



使用者指南

AWS CloudHSM



AWS CloudHSM: 使用者指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS CloudHSM ?	1
使用案例	2
運作方式	4
叢集	4
中的使用者 AWS CloudHSM	5
中的金鑰 AWS CloudHSM	5
用戶端 SDK	6
備份	7
的支援區域 AWS CloudHSM	8
的定價 AWS CloudHSM	8
開始使用	9
建立 IAM 管理員	9
建立 IAM 使用者和管理員群組	10
建立 VPC	11
建立叢集	12
檢閱叢集安全群組	16
啟動 EC2 用戶端	17
設定 EC2 執行個體安全群組	19
步驟 1. 修改預設安全群組	19
步驟 2. 將 Amazon EC2 執行個體連接至 AWS CloudHSM 叢集	20
建立 HSM	21
驗證 HSM 身分 (選用)	22
步驟 1. 從 HSM 取得憑證	25
步驟 2. 取得根憑證	28
步驟 3. 驗證憑證鏈	28
步驟 4. 擷取和比較公有金鑰	29
初始化叢集	30
步驟 1. 取得叢集 CSR	31
步驟 2. 簽署 CSR	33
步驟 3. 初始化叢集	35
安裝 CloudHSM CLI	36
啟用叢集	40
設定 mTLS (建議)	43
步驟 1. 在 HSM 上建立並註冊信任錨點	43

步驟 2. 為 啟用 mTLS AWS CloudHSM	47
步驟 3. 設定的 mTLS 強制執行 AWS CloudHSM	52
在 中建立和使用金鑰 AWS CloudHSM	53
最佳實務	55
叢集管理	55
擴展叢集以處理尖峰流量	55
架構您的叢集以獲得高可用性	55
至少有三個 HSMs 以確保新產生的金鑰的耐久性	55
安全存取您的叢集	56
根據您的需求擴展以降低成本	56
使用者管理	56
保護 HSM 使用者的登入資料	56
至少有兩個管理員以防止鎖定	57
為所有使用者管理操作啟用規定人數	57
建立多個加密使用者，每個使用者具有有限的許可	57
金鑰管理	57
選擇正確的金鑰類型	57
管理金鑰儲存限制	58
管理和保護金鑰包裝	58
應用程式整合	59
引導您的用戶端 SDK	59
驗證以執行 操作	59
有效管理應用程式中的金鑰	59
使用多執行緒	60
處理調節錯誤	60
整合叢集操作的重試	61
實作災難復原策略	61
監控	61
監控用戶端日誌	62
監控稽核日誌	62
監控 AWS CloudTrail	62
監控 Amazon CloudWatch 指標	62
叢集	64
叢集架構	64
叢集同步	66
叢集高可用性和負載平衡	66

叢集模式	67
HSM 類型	68
連接至叢集	69
在每個 EC2 執行個體上安裝發行憑證	70
指定憑證的位置。	70
引導用戶端 SDK	72
擴展 HSMs	75
新增 HSM	76
移除 HSM	77
刪除叢集	78
從備份建立叢集	79
從備份建立叢集 (主控台)	80
從備份建立叢集 (AWS CLI)	80
從備份建立叢集 (AWS CloudHSM API)	81
遷移 HSM 叢集類型	82
從 hsm1.medium 遷移至 hsm2m.medium	82
HSM 使用者	90
使用 CloudHSM CLI 進行使用者管理	90
先決條件	91
使用者類型	92
許可表	93
建立管理員	95
建立 CU	96
列出所有使用者	97
變更密碼	98
刪除使用者	100
管理使用者 MFA	101
管理規定人數身分驗證 (M 為 N)	115
使用 CMU 進行使用者管理	137
先決條件	138
使用者類型	142
許可表	143
建立使用者	145
列出所有使用者	147
變更密碼	149
刪除使用者	152

管理使用者 2FA	153
使用 CMU 管理規定人數身分驗證	161
金鑰	180
金鑰同步與持久性	180
概念	181
了解金鑰同步	181
變更用戶端金鑰持久性設定	182
同步複製的叢集之間的金鑰	188
AES 金鑰包裝	188
支援的演算法	188
在 中使用 AES 金鑰包裝 AWS CloudHSM	190
可信任金鑰	191
了解可信任金鑰	191
可信任的金鑰屬性	191
如何使用可信任金鑰來包裝資料金鑰	192
如何使用可信任金鑰取包裝資料金鑰	194
使用 CloudHSM CLI 進行金鑰管理	195
產生金鑰	195
刪除金鑰	201
共用和取消共用金鑰	204
依金鑰篩選	211
將金鑰標示為信任	218
管理規定人數身分驗證 (M 為 N)	219
使用 KMU 進行金鑰管理	239
產生金鑰	239
匯入金鑰	241
匯出金鑰	243
刪除金鑰	245
共用和取消共用金鑰	245
將金鑰標示為信任	246
叢集備份	247
使用備份	247
移除過期金鑰或非作用中使用者	248
考量災難復原	248
刪除備份	248
還原備份	250

設定備份保留	251
受管備份保留	251
跨區域複製備份	254
將備份複製到不同的區域 (控制台)	254
將備份複製到不同的區域 (AWS CLI)	255
將備份複製到不同的區域 (AWS CloudHSM API)	255
使用共用備份	255
共用備份的先決條件	256
共用備份	256
取消共用共用備份	259
識別共用備份	260
共用備份的許可	260
計費和計量	260
複製的叢集	261
取得 HSM 的 IP 地址	262
相關主題	263
標籤資源	264
新增或更新標籤	264
列出標籤	265
移除標籤	266
命令列工具	268
設定工具	269
用戶端 SDK 5 設定工具	269
用戶端 SDK 3 設定工具	295
CloudHSM CLI	304
支援平台	304
從 CMU 和 KMU 遷移至 CloudHSM CLI	305
開始使用	306
命令模式	313
金鑰屬性	315
進階組態	320
參考資料	326
AWS CloudHSM 管理公用程式	560
支援平台	561
開始使用	561
安裝用戶端 (Linux)	566

安裝用戶端 (Windows)	569
參考資料	570
金鑰管理公用程式	625
開始使用	625
安裝用戶端 (Linux)	629
安裝用戶端 (Windows)	632
參考資料	633
用戶端 SDK	749
檢查您的版本	750
比較元件支援	751
PKCS #11 程式庫	752
CloudHSM 管理公用程式 (CMU)	752
金鑰管理公用程式 (KMU)	753
JCE 提供者	753
OpenSSL 動態引擎	753
金鑰儲存提供者 (KSP)	753
遷移至最新的 SDK	754
遷移 PKCS #11 程式庫	754
遷移 OpenSSL 動態引擎	757
遷移金鑰儲存提供者 (KSP)	759
遷移 JCE 供應商	766
用戶端 SDK 5	776
最新 SDK 的優點	777
支援平台	778
PKCS #11 程式庫	780
OpenSSL 動態引擎	828
金鑰儲存提供者 (KSP)	835
JCE 提供者	863
先前版本	895
升級用戶端 SDK 3	896
支援平台	905
PKCS #11 程式庫	907
OpenSSL 動態引擎	947
JCE 提供者	951
KSP 和 CNG 提供者	978
整合第三方應用程式	990

SSL/TLS 卸載	990
運作方式	991
使用 OpenSSL 在 Linux 上卸載	992
使用 JSSE 在 Linux 上卸載	1059
在 Windows 上卸載	1068
新增負載平衡器 (選用)	1082
Windows Server CA	1088
用戶端 SDK 5 搭配 Windows Server CA	1088
具有 Windows Server CA 的用戶端 SDK 3	1093
Oracle 資料庫加密	1097
設定先決條件	1098
步驟 3：產生 Oracle TDE 主加密金鑰	1099
Microsoft SignTool	1101
用戶端 SDK 5 搭配 Microsoft SignTool	1101
用戶端 SDK 3 搭配 Microsoft SignTool	1105
Java Keytool 和 Jarsigner	1110
用戶端 SDK 5 搭配 Java Keytool 和 Jarsigner	1110
用戶端 SDK 3 搭配 Java Keytool 和 Jarsigner	1120
Microsoft 資訊清單產生和編輯工具	1136
步驟 1：設定先決條件	1136
步驟 2：建立簽署憑證	1137
步驟 3：簽署檔案	1138
其他第三方廠商整合	1139
監控	1141
用戶端 SDK 日誌	1141
用戶端 SDK 5 記錄	1142
用戶端 SDK 3 記錄	1143
AWS CloudTrail	1144
AWS CloudHSM CloudTrail 中的資訊	1145
了解 AWS CloudHSM 日誌檔案項目	1145
稽核日誌	1147
記錄的運作方式	1147
檢視日誌	1148
解譯日誌	1151
日誌參考	1165
CloudWatch 指標	1167

效能	1169
效能資料	1169
.....	1169
HSM 調節	1170
安全	1171
使用 IAM 政策控制 API 存取	1171
將 IAM 政策升級至 IPv6	1171
資料保護	1175
靜態加密	1176
傳輸中加密	1176
端對端加密	1176
叢集備份	1177
身分與存取管理	1178
使用 IAM 政策授予許可	1178
的 API 動作 AWS CloudHSM	1179
的條件索引鍵 AWS CloudHSM	1180
的預先定義 AWS 受管政策 AWS CloudHSM	1180
的客戶受管政策 AWS CloudHSM	1180
服務連結角色	1183
合規	1185
PCI-PIN 常見問答集	1186
棄用	1188
恢復能力	1189
基礎架構安全	1189
網路隔離	1190
使用者的授權	1190
VPC 端點 (AWS PrivateLink)	1190
AWS CloudHSM VPC 端點的考量事項	1190
為 AWS CloudHSM 建立介面 VPC 端點	1190
為 建立 VPC 端點政策 AWS CloudHSM	1191
更新管理	1192
疑難排解	1193
AWS CloudHSM 已知問題	1193
所有 HSM 執行個體的已知問題	1194
hsm1.medium 的已知問題	1198
hsm2m.medium 的已知問題	1198

PKCS #11 程序庫的已知問題	1200
JCE 開發套件的已知問題	1205
OpenSSL 動態引擎的已知問題	1209
金鑰儲存提供者 (KSP) 的已知問題	1211
執行 Amazon Linux 2 的 Amazon EC2 執行個體的已知問題	1213
整合第三方應用程式的已知問題	1213
叢集修改的已知問題	1214
在 hsm2.medium 上使用 AWS CloudHSM 用戶端 5.12.0 版的已知操作失敗問題	1215
用戶端 SDK 3 金鑰同步失敗	1215
用戶端 SDK 3 驗證效能	1216
測試建議	1217
pkpspeed 工具的可設定選項	1218
可以使用 pkpspeed 工具執行的測試	1218
範例	1219
用戶端 SDK 5 使用者包含不一致的值	1222
用戶端 SDK 5 使用者複寫失敗	1228
問題：所選使用者不會在整個叢集中同步	1228
問題：使用者存在於具有不同屬性的目的地叢集上	1230
用戶端 SDK 5 金鑰複寫失敗	1230
問題：所選金鑰不會在整個叢集中同步	1230
問題：具有不同資訊或屬性的目的地叢集中存在具有相同參考的金鑰	1232
AWS CloudHSM 在金鑰可用性檢查期間看到的錯誤	1232
使用 JCE 擷取金鑰	1233
getEncoded、getPrivateExponent 或 getS 傳回 Null	1233
getEncoded、getPrivateExponent 或 getS 返回 HSM 之外的金鑰位元組	1234
HSM 調節	1234
Resolution	1235
讓 HSM 使用者保持同步	1235
連線中斷	1236
CloudWatch 中缺少 AWS CloudHSM 稽核日誌	1239
不合規的 AES 金鑰包裝	1239
確定代碼是否生成不可復原的包裝金鑰。	1239
如果代碼生成不可復原的包裝金鑰，則必須採取的動作	1240
解決 AWS CloudHSM 叢集建立失敗	1241
新增遺失的許可	1242
手動建立服務連結角色	1242

使用非聯合身分使用者	1242
擷取 AWS CloudHSM 用戶端組態日誌	1243
用戶端 SDK 5 支援工具	1243
用戶端 SDK 3 支援工具	1245
配額	1247
下載	1249
最新版本	1249
用戶端 SDK 5 版本 : 5.16.1 版	1249
上一個版本	1255
淘汰版本	1279
已棄用的用戶端 SDK 5 版本	1279
已棄用的用戶端 SDK 3 版本	1293
終止命週期的版本	1303
文件歷史紀錄	1304
最近更新	1304
舊版更新	1309
.....	mccccxi

什麼是 AWS CloudHSM ?

AWS CloudHSM 結合了 AWS 雲端的優勢與硬體安全模組 (HSMs) 的安全性。硬體安全模組 (HSM) 是一種運算裝置，可處理密碼編譯操作，並為密碼編譯金鑰提供安全的儲存空間。透過 AWS CloudHSM，您可以完全控制 AWS 雲端中的高可用性 HSMs、具有低延遲存取，以及自動化 HSM 管理的安全信任根（包括備份、佈建、組態和維護）。

AWS CloudHSM 為客戶提供各種好處：

存取 FIPS 和非 FIPS 叢集

AWS CloudHSM 以兩種模式提供叢集：FIPS 和非 FIPS。在 FIPS 模式中，只能使用經聯邦資訊處理標準 (FIPS) 驗證的金鑰和演算法。非 FIPS 模式提供支援的所有金鑰和演算法 AWS CloudHSM，無論 FIPS 核准為何。如需詳細資訊，請參閱[AWS CloudHSM 叢集模式](#)。

HSMs 是一般用途、單一租用戶，以及 FIPS 140-2 Level-3 或 FIPS 140-3 Level-3，在 FIPS 模式下針對叢集進行驗證

AWS CloudHSM 使用一般用途 HSMs，相較於具有預先定義演算法和應用程式金鑰長度的全受管 AWS 服務，可提供更高的彈性。我們提供符合標準的 HSMs、單一租戶，以及 FIPS 140-2 Level-3 或 FIPS 140-3 Level-3 驗證，可用於 FIPS 模式的叢集。對於使用案例超出 FIPS 140-2 或 FIPS 140-3 層級 3 驗證限制的客戶，AWS CloudHSM 也提供非 FIPS 模式的叢集。如需更多資訊，請參閱[AWS CloudHSM 叢集](#)。

AWS 看不到 E2E 加密

由於您的資料平面經過端對端 (E2E) 加密，而且 AWS 看不到，因此您可以控制自己的使用者管理 (IAM 角色之外)。與使用受管 AWS 服務相比，此控制項的折衷之處在於您的責任更大。

完全控制金鑰、演算法和應用程式開發

AWS CloudHSM 可讓您完全控制所使用的演算法和金鑰。您可以產生、存放、匯出、匯入、管理和使用密碼編譯金鑰 (包括工作階段金鑰、字符金鑰、對稱金鑰和非對稱金鑰對)。此外，AWS CloudHSM SDKs 可讓您完全控制應用程式開發、應用程式語言、執行緒，以及應用程式實際存在的位置。

將加密編譯工作負載遷移到雲端

客戶遷移使用公有金鑰密碼編譯標準 #11 (PKCS #11)、Java 密碼編譯延伸模組 (JCE)、密碼編譯 API：新一代 (CNG) 或金鑰儲存提供者 (KSP) 的公有金鑰基礎設施可以遷移至，AWS CloudHSM 而其應用程式的變更較少。

若要進一步了解您可以使用哪些 AWS CloudHSM，請參閱下列主題。當您準備好開始使用時 AWS CloudHSM，請參閱 [開始使用](#)。

 Note

如果您需要受管服務，用於建立和控制您的加密金鑰，但您不想要或不需要操作自己的 HSM，請考慮使用 [AWS Key Management Service](#)。

如果您正在尋找一種彈性服務來管理雲端支付 HSM 和付款處理應用程式的金鑰，請考慮使用 [AWS 付款加密技術](#)。

目錄

- [AWS CloudHSM 使用案例](#)
- [AWS CloudHSM 運作方式](#)
- [的定價 AWS CloudHSM](#)

AWS CloudHSM 使用案例

AWS CloudHSM 可用來實現各種目標。本主題中的內容概述了您可以如何使用 AWS CloudHSM。

達成法規合規

需要符合企業安全標準的企業可以使用 AWS CloudHSM 來管理保護高度機密資料的私有金鑰。提供的 HSMs AWS CloudHSM 經過 FIPS 140-2 第 3 級認證，並符合 PCI DSS。此外，AWS CloudHSM 是否符合 PCI PIN 和 PCI-3DS 規範。如需詳細資訊，請參閱 [合規](#)。

加密和解密資料

使用 AWS CloudHSM 管理保護高度機密資料、傳輸中加密和靜態加密的私有金鑰。此外，AWS CloudHSM 提供與多個密碼編譯 SDKs 的標準相容整合。

使用私有金鑰和公有金鑰簽署和驗證文件

在密碼編譯中，使用私有金鑰簽署文件可讓收件者使用公有金鑰來驗證您 (而非其他人) 是否確實傳送文件。使用 AWS CloudHSM 建立專為此目的設計的非對稱公有和私有金鑰對。

使用 HMAC 和 CMAC 進行訊息驗證

在密碼編譯中，加密式訊息驗證程式碼 (CMAC) 和雜湊訊息驗證碼 (HMAC) 用於驗證並確保透過不安全網路傳送訊息的完整性。透過 AWS CloudHSM，您可以安全地建立和管理支援 HMACs 和 CMACs 對稱金鑰。

利用 AWS CloudHSM 和 的優點 AWS Key Management Service

客戶可以結合 AWS CloudHSM 和 [AWS KMS](#)，將金鑰材料存放在單一租用戶環境中，同時獲得的金鑰管理、擴展和雲端整合優勢 AWS KMS。如需如何執行此操作的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的 [AWS CloudHSM 金鑰存放區](#)。

卸載 Web 伺服器的 SSL/TLS 處理

為了透過網際網路安全地傳送資料，Web 伺服器會使用公有金鑰和私有金鑰對和 SSL/TLS 公有金鑰憑證來建立 HTTPS 工作階段。此程序涉及許多 Web 伺服器的運算，但您可以將其中一些內容卸載至 AWS CloudHSM 叢集，藉此減輕運算負擔，同時提供額外安全性。如需使用 設定 SSL/TLS 卸載的資訊 AWS CloudHSM，請參閱 [SSL/TLS 卸載](#)。

啟用透明資料加密 (TDE)

透明資料加密 (TDE) 可用來加密資料庫檔案。使用 TDE，資料庫軟體將資料存儲在磁盤上之前對其進行加密。您可以將 TDE 主加密金鑰儲存在 AWS CloudHSM 叢集的 HSM 中，以達到更高的安全性。如需使用 設定 Oracle TDE 的詳細資訊 AWS CloudHSM，請參閱 [Oracle 資料庫加密](#)。

管理發行憑證授權機構 (CA) 的私有金鑰

憑證授權機構 (CA) 是一種受信任的實體，會發出將公有金鑰繫結至身分 (個人或組織) 的數位憑證。若要操作 CA，您必須保護簽署 CA 所發行憑證的私有金鑰，以維護信任。您可以在 AWS CloudHSM 叢集中存放這類私有金鑰，然後使用 HSMs 來執行密碼編譯簽署操作。

生成隨機數字

產生隨機數字以建立加密金鑰是線上安全的核心。AWS CloudHSM 可用來在您控制的 HSMs 中安全地產生隨機數字，而且只有您可見。

AWS CloudHSM 運作方式

本主題概述了您用來安全地加密資料並在 HSMs 中執行密碼編譯操作的基本概念和架構。在您自己的 Amazon Virtual Private Cloud (VPC) 中 AWS CloudHSM 操作。您必須先 AWS CloudHSM 建立叢集、將 HSMs 新增至叢集、建立使用者和金鑰，然後使用用戶端 SDKs 整合 HSMs 與應用程式，才能使用。完成後，您可以使用用戶端 SDK 日誌 AWS CloudTrail、稽核日誌和 Amazon CloudWatch 進行[監控 AWS CloudHSM](#)。

了解 AWS CloudHSM 基本概念及其如何協同運作，以協助保護您的資料。

主題

- [AWS CloudHSM 叢集](#)
- [中的使用者 AWS CloudHSM](#)
- [中的金鑰 AWS CloudHSM](#)
- [適用於 SDKs AWS CloudHSM](#)
- [AWS CloudHSM 叢集備份](#)
- [的支援區域 AWS CloudHSM](#)

AWS CloudHSM 叢集

讓個別 HSMs 以同步、備援和高可用性的方式一起運作可能很困難，但透過在叢集中提供硬體安全模組 (HSMs) 來 AWS CloudHSM 為您處理繁重工作。叢集是 AWS CloudHSM 保持同步的個別 HSMs 集合。當您在叢集的一個 HSM 上執行任務或操作時，該叢集的其他 HSM 會自動保持在最新狀態。

AWS CloudHSM 以兩種模式提供叢集：FIPS 和非 FIPS。在 FIPS 模式中，只能使用經聯邦資訊處理標準 (FIPS) 驗證的金鑰和演算法。非 FIPS 模式提供支援的所有金鑰和演算法 AWS CloudHSM，無論 FIPS 核准為何。AWS CloudHSM 也提供兩種 HSMs 類型：hsm1.medium 和 hsm2m.medium。如需每個 HSM 類型和叢集模式間差異的詳細資訊，請參閱 [AWS CloudHSM 叢集模式](#)。hsm1.medium HSM 類型即將終止支援，因此無法使用此類型建立新叢集。如需詳細資訊，請參閱[棄用通知](#)以取得詳細資訊。

為了滿足可用性、耐久性和可擴展性目標，您可以在多個可用區域中設定叢集中的 HSM 數量。您可以建立具有 1 到 28 個 HSMs 叢集 ([預設限制](#)為每個 [AWS 區域](#) 每個 AWS 帳戶 6 個 HSMs)。您可以將 HSMs 放置在 AWS 區域中的不同 [可用區域](#)。將更多 HSM 新增到叢集可提高效能。將叢集分散於可用區域可提供備援和高可用性。

如需叢集的詳細資訊，請參閱 [中的叢集 AWS CloudHSM](#)。

若要建立叢集，請參閱[開始使用](#)。

中的使用者 AWS CloudHSM

與大多數 AWS 服務和資源不同，您不會使用 AWS Identity and Access Management (IAM) 使用者或 IAM 政策來存取 AWS CloudHSM 叢集中的資源。反之，您可以直接在 AWS CloudHSM 叢集的 HSM HSMs HSM 使用者。

HSM 使用者與 IAM 使用者不同。擁有正確憑證的 IAM 使用者可利用 AWS API 與資源進行互動來建立 HSM。由於 AWS 看不到 E2E 加密，因此您必須使用 HSM 使用者憑證來驗證 HSM 上的操作，因為憑證會直接在 HSM 上進行。HSM 會透過您定義和管理的憑證來驗證每個 HSM 使用者。每個 HSM 使用者都有類型，可決定使用者在 HSM 上執行的操作。每個 HSM 都會透過您使用 [CloudHSM CLI](#) 定義的憑證來驗證每個 HSM 使用者。

如果您使用的是[舊版 SDK 系列](#)，則將使用 [CloudHSM 管理公用程式 \(CMU\)](#)。

中的金鑰 AWS CloudHSM

AWS CloudHSM 可讓您安全地在 AWS CloudHSM HSMs 中產生、存放和管理加密金鑰。金鑰可以是對稱或非對稱的，可以是單一工作階段的工作階段金鑰（暫時性金鑰），長期使用的權杖金鑰（持久性金鑰），而且可以從 AWS CloudHSM 匯出和匯入 AWS CloudHSM。金鑰也可以用來完成常見的密碼編譯任務和函數：

- 使用對稱和非對稱加密演算法執行加密資料簽署和簽章驗證。
- 使用雜湊函數來計算訊息摘要和雜湊訊息驗證碼 (HMAC)。
- 包裝並保護其他金鑰。
- 訪問以密碼編譯方式保護的隨機資料。

叢集可以擁有的最大金鑰取決於叢集中的 HSMs 類型。例如，hsm2m.medium 儲存的金鑰比 hsm1，medium 多。如需比較，請參閱 [AWS CloudHSM 配額](#)。

此外，AWS CloudHSM 遵循幾個關鍵用量和管理的基本原則：

許多金鑰類型和演算法可供選擇

為了讓您自訂自己的解決方案，AWS CloudHSM 提供許多金鑰類型和演算法供您選擇。演算法支援各種金鑰大小。如需詳細資訊，請參閱每個 [使用 AWS CloudHSM 用戶端 SDKs 操作](#) 的屬性和機制頁面。

如何管理金鑰

AWS CloudHSM 金鑰是透過 SDKs和命令列工具來管理。如需如何使用這些工具管理金鑰的詳細資訊，請參閱 [中的金鑰 AWS CloudHSM](#) 和 [的最佳實務 AWS CloudHSM](#)。

誰擁有金鑰

在 中 AWS CloudHSM，建立金鑰的加密使用者 (CU) 擁有金鑰。擁有者可以使用 key share 和 key unshare 命令來與其他 CU 共用和取消共用金鑰。如需詳細資訊，請參閱 [使用 CloudHSM CLI 共用和取消共用金鑰](#)。

存取和使用可以通過基於屬性的加密來控制

AWS CloudHSM 可讓您使用屬性型加密，這是一種加密形式，可讓您使用金鑰屬性來控制誰可以根據政策解密資料。

適用於 SDKs AWS CloudHSM

使用 時 AWS CloudHSM，您可以使用[AWS CloudHSM 用戶端軟體開發套件 \(SDKs\)](#)執行密碼編譯操作。AWS CloudHSM 用戶端 SDKs包括：

- 公有金鑰密碼編譯標準 #11 (PKCS #11)
- JCE 提供者
- OpenSSL 動態引擎
- Microsoft Windows 的金鑰儲存提供者 (KSP)

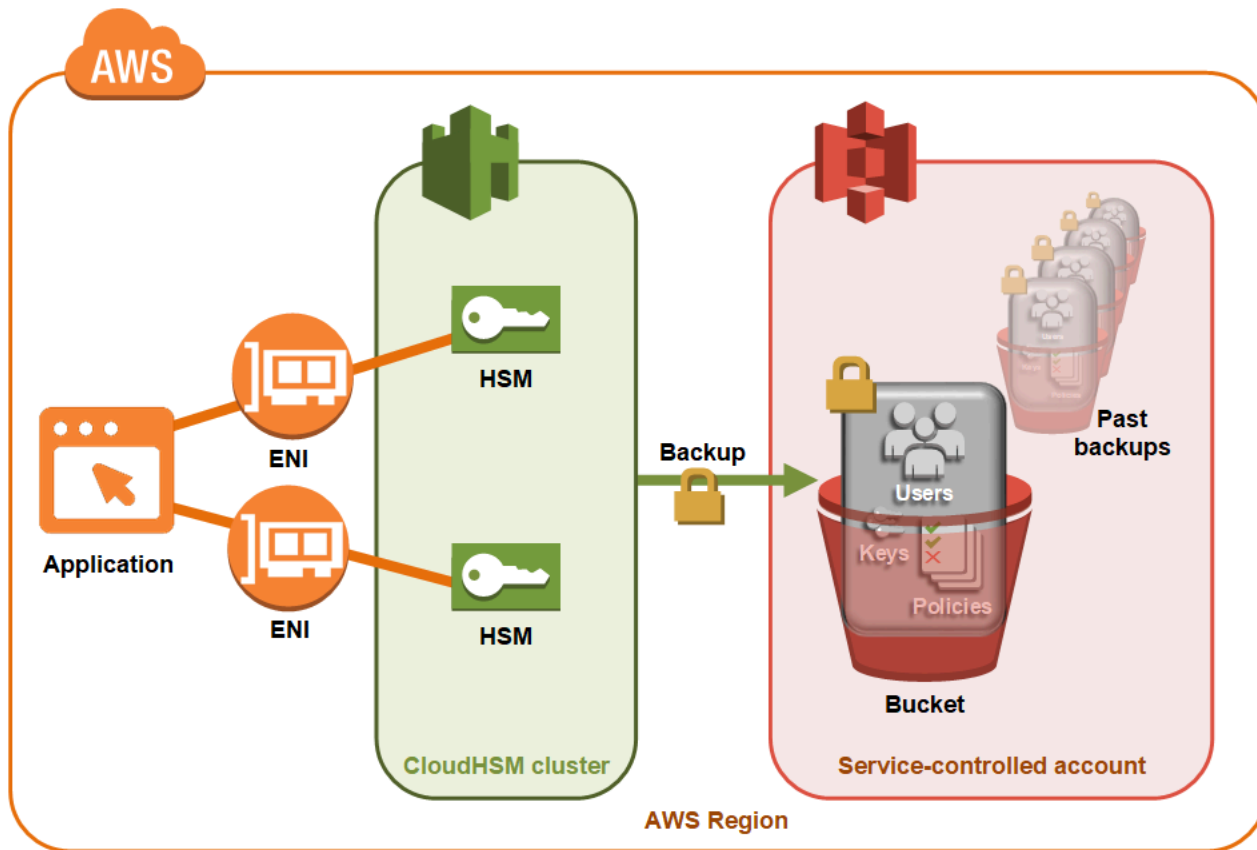
您可以在 AWS CloudHSM 叢集中使用這些 SDKS 的任何或所有。撰寫您的應用程式碼，以使用這些 SDK 在 HSM 中執行密碼編譯作業。若要查看哪些平台和 HSM 類型支援每個 SDK，請參閱 [AWS CloudHSM 用戶端 SDK 5 支援的平台](#)

公用程式和命令列工具不僅需要使用 SDK，還需要設定應用程式的憑證、政策和設定。如需詳細資訊，請參閱 [AWS CloudHSM 命令列工具](#)。

如需關於安裝和使用客戶端 SDK 或用戶端連線安全性的詳細資訊，請參閱 [用戶端 SDK](#) 和 [端對端加密](#)。

AWS CloudHSM 叢集備份

AWS CloudHSM 會定期備份叢集中的使用者、金鑰和政策。備份既安全又耐用，並按可預測的排程進行更新。下圖顯示備份與叢集的關係。



如需使用備份的詳細資訊，請參閱 [叢集備份](#)。

安全性

當從 HSM AWS CloudHSM 進行備份時，HSM 會先加密其所有資料，再將其傳送至 AWS CloudHSM。資料永遠不會以純文字格式離開 HSM。此外，備份無法由解密，AWS 因為 AWS 無法存取用來解密備份的金鑰。如需詳細資訊，請參閱[叢集備份的安全性](#)

耐久性

AWS CloudHSM 會將備份存放在與叢集相同區域中的服務控制 Amazon Simple Storage Service (Amazon S3) 儲存貯體中。備份具有 99.999999999% 的耐久性層級，與存放在 Amazon S3 中的任何物件相同。

的支援區域 AWS CloudHSM

如需 支援區域的相關資訊 AWS CloudHSM，請參閱 中的[AWS CloudHSM 區域和端點](#) AWS 一般參考，或[區域資料表](#)。

AWS CloudHSM 可能無法在指定區域中的所有可用區域中使用。不過，這不應影響效能，因為 會在叢集中的所有 HSMs 之間 AWS CloudHSM 自動負載平衡。

與大多數 AWS 資源一樣，叢集和 HSMs 是區域資源。您不能跨區域重複使用或擴展叢集。您必須執行[入門 AWS CloudHSM](#)中列出的所有必要步驟，才能在新區域中建立叢集。

基於災難復原目的，AWS CloudHSM 可讓您將 AWS CloudHSM 叢集備份從一個區域複製到另一個區域。如需詳細資訊，請參閱[AWS CloudHSM 叢集備份](#)。

的定價 AWS CloudHSM

使用 時 AWS CloudHSM，您按小時支付，無需長期承諾或預付款項。如需詳細資訊，請參閱 AWS 網站上的[AWS CloudHSM 定價](#)。

入門 AWS CloudHSM

下列主題可協助您在 中建立、初始化和啟用叢集 AWS CloudHSM。完成這些程序之後，您就能管理使用者、管理叢集，以及使用隨附的軟體程式庫執行密碼編譯操作。為了獲得最佳體驗，請依照列出的順序遵循主題。

目錄

- [建立的 IAM 管理群組 AWS CloudHSM](#)
- [建立的虛擬私有雲端 \(VPC\) AWS CloudHSM](#)
- [在 中建立叢集 AWS CloudHSM](#)
- [在 中檢閱叢集的安全群組 AWS CloudHSM](#)
- [啟動 Amazon EC2 用戶端執行個體以與 互動 AWS CloudHSM](#)
- [設定的用戶端 Amazon EC2 執行個體安全群組 AWS CloudHSM](#)
- [在 中建立 HSM AWS CloudHSM](#)
- [在 AWS CloudHSM \(選用\) 中驗證叢集 HSM 的身分和真實性](#)
- [在 中初始化叢集 AWS CloudHSM](#)
- [下載和設定 CloudHSM CLI](#)
- [在 中啟用叢集 AWS CloudHSM](#)
- [在用戶端和 AWS CloudHSM 之間設定交互 TLS \(建議\)](#)
- [在 中建立和使用金鑰 AWS CloudHSM](#)

建立的 IAM 管理群組 AWS CloudHSM

開始使用 的第一步 AWS CloudHSM 是設定 IAM 許可。

根據[最佳實務](#)，請勿使用 AWS 帳戶根使用者與 互動 AWS，包括 AWS CloudHSM。反之，請使用 AWS Identity and Access Management (IAM) 來建立 IAM 使用者、IAM 角色或聯合身分使用者。依照[建立 IAM 使用者和管理員群組](#) 區段中的步驟來建立管理員群組，並附加 AdministratorAccess 政策。然後建立新管理使用者，並將該使用者新增到群組。視需要將其他使用者新增至該群組。您新增的每位使用者都會繼承群組的 AdministratorAccess 政策。

另一個最佳實務是建立只有執行所需許可的 AWS CloudHSM 管理員群組 AWS CloudHSM。視需要將個別使用者新增至此群組。每位使用者都會繼承已連接至群組的有限許可，而不是完整的 AWS 存取權。以下的[客戶受管政策 AWS CloudHSM](#) 章節包含您應連接至 AWS CloudHSM 管理員群組的政策。

AWS CloudHSM 會為 AWS 您的帳戶定義[服務連結角色](#)。服務連結角色目前定義許可，允許您的帳戶記錄 AWS CloudHSM 事件。角色可以由 自動建立，AWS CloudHSM 也可以由您手動建立。您無法編輯此角色，但可以刪除。如需詳細資訊，請參閱[的服務連結角色 AWS CloudHSM](#)。

建立 IAM 使用者和管理員群組

首先，建立 IAM 使用者以及該使用者的管理員群組。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。
2. 請遵循線上指示進行。

註冊程序的一部分包括接聽電話或文字訊息，並在電話鍵盤上輸入驗證碼。

當您註冊時 AWS 帳戶，AWS 帳戶根使用者會建立。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行[需要根使用者存取權的任務](#)。

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

註冊後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center 和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者[AWS Management Console](#)身分登入。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的[以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需說明，請參閱《IAM 使用者指南》中的[為您的 AWS 帳戶 根使用者（主控台）啟用虛擬 MFA 裝置](#)。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center 《使用者指南》中的[使用預設值設定使用者存取 IAM Identity Center 目錄](#)。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《使用者指南》中的[登入 AWS 存取入口網站](#)。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[建立許可集](#)。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[新增群組](#)。

如需可連接至 IAM 使用者群組 AWS CloudHSM 的 政策範例，請參閱 [的身分和存取管理 AWS CloudHSM](#)。

建立 的虛擬私有雲端 (VPC) AWS CloudHSM

您需要 中的叢集虛擬私有雲端 (VPC) AWS CloudHSM。如果您還沒有 VPC，請遵循本主題中的步驟來建立 VPC。

Note

按照這些步驟將建立公有和私有子網路。

建立 VPC

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽列上，使用區域選擇器來選擇 [AWS CloudHSM 目前支援的其中一個區域](#)。
3. 選取建立 VPC 按鈕。
4. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
5. 針對名稱標籤自動產生，請輸入可識別的名稱，例如 **CloudHSM**。
6. 針對 IPv6 CIDR 區塊，選取 Amazon 提供的 IPv6 CIDR 區塊，以使用 HSMs 的 IPv6 連線，並為您的叢集 AWS 配置 IPv6 CIDR 區塊。此設定支援雙堆疊網路類型。如果您不需要 IPv6 連線，請保留預設設定。
7. 所有其他選項保持設定為預設值。
8. 選擇建立 VPC。
9. 建立 VPC 之後，選取檢視 VPC 以檢視您剛建立的 VPC。

在 中建立叢集 AWS CloudHSM

叢集是個別硬體安全模組 (HSMs) 的集合。會 AWS CloudHSM 同步每個叢集中的 HSMs，使其做為邏輯單位運作。AWS CloudHSM 提供兩種 HSMs 類型：hsm1.medium 和 hsm2m.medium。建立叢集時，您可以選擇叢集中的兩個。如需每個 HSM 類型和叢集模式間差異的詳細資訊，請參閱 [AWS CloudHSM 叢集模式](#)。

當您建立叢集時，AWS CloudHSM 會代表您建立叢集的安全群組。此安全群組會控制對叢集中 HSM 的網路存取。該群組僅允許來自安全群組中 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的傳入連接。在預設情況下，此安全群組不包含任何執行個體。您之後會 [啟動用戶端執行個體](#) 並 [設定叢集的安全群組](#)，以允許與 HSM 進行通訊並連線。

Important

當您建立叢集時，會 AWS CloudHSM 建立名為 AWSServiceRoleForCloudHSM [的服務連結角色](#)。如果 AWS CloudHSM 無法建立角色或角色尚未存在，您可能無法建立叢集。如需詳細資訊，請參閱 [解決 AWS CloudHSM 叢集建立失敗](#)。如需服務連結角色的詳細資訊，請參閱 [的服務連結角色 AWS CloudHSM](#)。

⚠ Important

如果您使用 [AWS CloudHSM 雙堆疊端點](#) (即 `cloudhsmv2.<region>.api.aws`)，請確定您的 IAM 政策已更新以處理 IPv6。如需詳細資訊，請參閱 [安全性下的將 IAM 政策升級至 IPv6 一節](#)。

您可以從 [AWS CloudHSM 主控台](#)、[AWS Command Line Interface \(AWS CLI\)](#) 或 AWS CloudHSM API 建立叢集。

ℹ Note

如需叢集引數和 APIs 的詳細資訊，請參閱《AWS CLI 命令參考[create-cluster](#)》中的。

Console

建立叢集 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 在導覽列上，使用區域選擇器來選擇 [AWS CloudHSM 目前支援的其中一個區域](#)。
3. 選擇建立叢集。
4. 在叢集組態區段中，執行下列操作：
 - a. 對於 VPC，請選取您在 [建立的虛擬私有雲端 \(VPC\) AWS CloudHSM](#) 建立的 VPC。
 - b. 對於可用區域，請在每個可用區域旁選擇您建立的私有子網路。

ℹ Note

即使指定的可用區域 AWS CloudHSM 不支援，效能也不應受到影響，因為會在叢集中的所有 HSMs 之間 AWS CloudHSM 自動負載平衡。請參閱 [AWS CloudHSM 區域和端點](#) 中的 AWS 一般參考，以查看的可用區域支援 AWS CloudHSM。

- c. 針對 HSM 類型，選取可在叢集中建立的 HSM 類型，以及叢集所需的模式。若要查看每個區域支援哪些 HSM 類型，請參閱 [AWS CloudHSM 定價計算器](#)。

 Important

建立叢集之後，就無法變更叢集模式。如需適合您使用案例的類型和模式資訊，請參閱 [AWS CloudHSM 叢集模式](#)。

- d. 針對網路類型，選擇用於存取 HSMs IP 地址通訊協定。IPv4 會將應用程式與 HSMs 之間的通訊限制為僅限 IPv4。此為預設選項。雙堆疊可同時啟用 IPv4 和 IPv6 通訊。若要使用雙堆疊，請將 IPv4 和 IPv6 CIDRs 新增至您的 VPC 和子網路組態。網路類型在初始設定後很難變更。若要修改它，請建立現有叢集的備份，並使用所需的網路類型還原新的叢集。如需詳細資訊，請參閱[從備份建立 AWS CloudHSM 叢集](#)
 - e. 針對叢集來源，指定您要建立新的叢集，還是從現有的備份還原叢集。
 - 非 FIPS 模式的叢集備份只能用來還原處於非 FIPS 模式的叢集。
 - 處於 FIPS 模式的叢集備份只能用來還原處於 FIPS 模式的叢集。
5. 選擇下一步。
 6. 指定服務應保留備份的時間長度。

 Note

接受預設保留期 90 天，或輸入介於 7 到 379 天之間的新值。服務會自動刪除此叢集中超過您在此指定值的備份。您之後可以變更這個設定。如需詳細資訊，請參閱[設定備份保留](#)。

7. 選擇下一步。
8. (選用) 輸入標籤索引鍵和選用標籤值。若要將多個標籤新增至叢集，請選擇新增標籤。
9. 選擇檢閱。
10. 檢閱您的叢集組態，然後選擇建立叢集。

如果您嘗試建立叢集失敗，這可能與服務 AWS CloudHSM 連結角色的問題有關。如需解決失敗的協助，請參閱 [解決 AWS CloudHSM 叢集建立失敗](#)。

AWS CLI

建立叢集 ([AWS CLI](#))

- 在命令提示中，執行 [create-cluster](#) 命令。指定您計劃建立 HSM 所在子網路的 HSM 執行個體類型、備份保留時長和子網路 ID。使用您建立之私有子網路的子網路 ID。僅能對每個可用區域指定一個子網路。

```
$ aws cloudhsmv2 create-cluster --hsm-type hsm2m.medium \
                                --backup-retention-policy Type=DAYS,Value=<number of days> \
                                --subnet-ids <subnet ID> \
                                --mode <FIPS> \
                                --network-type <IPv4>

{
  "Cluster": {
    "BackupPolicy": "DEFAULT",
    "BackupRetentionPolicy": {
      "Type": "DAYS",
      "Value": 90
    },
    "VpcId": "vpc-50ae0636",
    "SubnetMapping": {
      "us-west-2b": "subnet-49a1bc00",
      "us-west-2c": "subnet-6f950334",
      "us-west-2a": "subnet-fd54af9b"
    },
    "SecurityGroup": "sg-6cb2c216",
    "HsmType": "hsm2m.medium",
    "NetworkType": "IPv4",
    "Certificates": {},
    "State": "CREATE_IN_PROGRESS",
    "Hsms": [],
    "ClusterId": "cluster-igklspoyj5v",
    "ClusterMode": "FIPS",
    "CreateTimestamp": 1502423370.069
  }
}
```

 Note

ClusterMode 是除 hsm1.medium 以外的所有 hsm 類型的必要參數。--mode :


```
$ aws cloudhsmv2 create-cluster --hsm-type hsm2m.medium \
    --backup-retention-policy Type=DAYS,Value=<number of days> \
    --subnet-ids <subnet ID> \
    --mode NON_FIPS
```

如果您嘗試建立叢集失敗，這可能與服務 AWS CloudHSM 連結角色的問題有關。如需解決失敗的協助，請參閱 [解決 AWS CloudHSM 叢集建立失敗](#)。

AWS CloudHSM API

建立叢集 (AWS CloudHSM API)

- 傳送 [CreateCluster](#) 要求。指定您計劃建立 HSM 所在子網路的 HSM 執行個體類型、備份保留政策和子網路 ID。使用您建立之私有子網路的子網路 ID。僅能對每個可用區域指定一個子網路。

如果您嘗試建立叢集失敗，這可能與服務 AWS CloudHSM 連結角色的問題有關。如需解決失敗的協助，請參閱 [解決 AWS CloudHSM 叢集建立失敗](#)。

在中檢閱叢集的安全群組 AWS CloudHSM

當您建立叢集時，會 AWS CloudHSM 建立名為的安全群組 `cloudhsm-cluster-<clusterID>-sg`。此安全群組包含預先設定的 TCP 規則，其允許叢集安全群組內透過連接埠 2223-2225 的傳入和傳出通訊。此 SG 可讓您的 EC2 執行個體使用 VPC 與叢集中的 HSM 進行通訊。

Warning

- 請勿刪除或修改預先設定的 TCP 規則 (已填入叢集安全群組中)。這個規則可以防止連線問題和對 HSM 未經授權的存取。
- 叢集安全群組可防止對 HSM 未經授權的存取。可以存取安全群組中執行個體的任何人都可以存取您的 HSM。大多數操作需要使用者登入 HSM，但可能會在未經驗證的情況下就將 HSM 歸零，而將金鑰資料、憑證和其他資料銷毀。如果發生這種情況，在最新的備份之後建立或修改的資料會遺失且無法復原。為了避免未經授權的存取，請確保只有受信任的管理員可以修改或存取預設安全群組中的執行個體。

- `hsm2m.medium` 叢集引進 mTLS 功能，以限制未經授權的使用者連線至叢集。未經授權的使用者需要有效的 mTLS 登入資料才能成功連線到叢集，然後再嘗試歸零。

在下一個步驟中，您可以[啟動 Amazon EC2 執行個體](#)，並將其[連接叢集安全群組](#)以將它連接到您的 HSM。

啟動 Amazon EC2 用戶端執行個體以與 互動 AWS CloudHSM

若要與 AWS CloudHSM 叢集和 HSM 執行個體互動和管理，您必須能夠與 HSMs 的彈性網路介面通訊。最簡單的方式是使用與您的叢集位於相同 VPC 的 EC2 執行個體。您也可以使用下列 AWS 資源來連線至叢集：

- [Amazon VPC 對等互連](#)
- [AWS Direct Connect](#)
- [VPN 連接](#)

Note

本指南提供如何將 EC2 執行個體連接至 AWS CloudHSM 叢集的簡化範例。如需安全網路組態的最佳實務，請參閱 [安全存取您的叢集](#)。

AWS CloudHSM 文件通常會假設您在建立叢集的相同 VPC 和可用區域 (AZ) 中使用 EC2 執行個體。

建立 EC2 執行個體

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 EC2 儀表板。
2. 選取啟動執行個體。從下拉式選單中，選擇啟動執行個體。
3. 在名稱欄位中，輸入 EC2 執行個體的名稱。
4. 在應用程式和 OS 影像 (Amazon Machine Image) 區段，選擇與 CloudHSM 支援平台相對應的 Amazon Machine Image (AMI)。如需詳細資訊，請參閱[AWS CloudHSM 用戶端 SDK 5 支援的平台](#)。
5. 在執行個體類型區段中，選取執行個體類型。
6. 在金鑰對區段中，使用現有金鑰對，或選取建立新金鑰配對並完成下列步驟：

- a. 在金鑰對名稱中，輸入新金鑰對的名稱。
- b. 在金鑰對類型中，選擇一個金鑰對類型。
- c. 在私有金鑰檔案格式中，選擇私有金鑰的儲存格式。
- d. 選取建立金鑰對。
- e. 下載並存儲私有金鑰檔案。

 Important

這是您儲存私有金鑰檔案的唯一機會。將檔案下載並儲存於安全處。當您啟動執行個體時，必須提供金鑰對的名稱。此外，每次連接至執行個體，您都必須提供對應的私有金鑰，同時要選擇您在設定時建立的金鑰對。

7. 在網路設定中選取編輯。
8. 在 VPC 中，選擇先前為叢集建立的 VPC。
9. 在子網路中，選擇先前為 VPC 建立的公有子網路。
10. 在 Auto-assign Public IP (自動指派公有 IP) 中，選擇 Enable (啟用)。
11. 針對自動指派 IPv6 IP，選擇啟用以將 IPv6 連線與叢集和雙堆疊 NetworkType 搭配使用。如果您啟用此選項，請更新 Amazon EC2 執行個體的安全群組規則、VPC 和子網路路由表，以及網路 ACLs，以允許從執行個體到 HSMs IPv6 傳出流量。
12. 選擇 Select an existing security group (選取現有的安全群組)。
13. 在一般安全群組中，從下拉式選單中選取預設安全群組。
14. 在設定儲存中，使用下拉式功能表選擇儲存組態。
15. 在彙總視窗中，選取啟動執行個體。

 Note

完成此步驟後，將開始建立 EC2 執行個體的執执行程序。

如需建立 Linux Amazon EC2 用戶端的詳細資訊，請參閱 [Amazon EC2 Linux 執行個體入門](#)。如需連接到執行中用戶端的詳細資訊，請參閱下列主題：

- [使用 SSH 連接至您的 Linux 執行個體](#)
- [使用 PuTTY 從 Windows 連接至您的 Linux 執行個體](#)

Amazon EC2 使用者指南包含設定和使用 Amazon EC2 執行個體的詳細說明。以下清單提供適用於 Linux 和 Windows Amazon EC2 用戶端的可用文件概觀：

- 若要建立 Linux Amazon EC2 用戶端，請參閱 [Amazon EC2 Linux 執行個體入門](#)。

如需連接到執行中用戶端的詳細資訊，請參閱下列主題：

- [使用 SSH 連接至您的 Linux 執行個體](#)
- [使用 PuTTY 從 Windows 連接至您的 Linux 執行個體](#)
- 若要建立 Windows Amazon EC2 用戶端，請參閱 [Amazon EC2 Windows 執行個體入門](#)。如需連接到您的 Windows 用戶端的詳細資訊，請參閱 [連接到您的 Windows 執行個體](#)。

Note

您的 EC2 執行個體可以執行本指南中包含的所有 AWS CLI 命令。如果未安裝 AWS CLI，您可以從 [AWS Command Line Interface](#) 下載。如果您使用 Windows，可以下載及執行 64 位元或 32 位元 Windows 安裝程式。如果您使用 Linux 或 macOS，可以使用 pip 安裝 CLI。

設定 的用戶端 Amazon EC2 執行個體安全群組 AWS CloudHSM

當您在 中啟動叢集的 Amazon EC2 執行個體時 AWS CloudHSM，您會將其與預設的 Amazon VPC 安全群組建立關聯。本主題說明如何將叢集安全群組與 EC2 執行個體建立關聯。此關聯可讓在 EC2 執行個體上執行的 AWS CloudHSM 用戶端與您的 HSMs 通訊。若要將 EC2 執行個體連線至 AWS CloudHSM 叢集，您必須正確設定 VPC 預設安全群組，並將叢集安全群組與執行個體建立關聯。

使用下列步驟來完成組態變更。

主題

- [步驟 1. 修改預設安全群組](#)
- [步驟 2. 將 Amazon EC2 執行個體連接至 AWS CloudHSM 叢集](#)

步驟 1. 修改預設安全群組

您需要修改預設安全群組，允許 SSH 或 RDP 連線，以便下載及安裝用戶端軟體，並與您的 HSM 互動。

修改預設安全群組

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 EC2 儀表板。
2. 選取執行個體（執行中），然後選取您要安裝 AWS CloudHSM 用戶端之 EC2 執行個體旁的核取方塊。
3. 在安全標籤下方，選擇名稱為預設的安全群組。
4. 在頁面頂端，依序選擇 Actions (動作) 和 Edit Inbound Rules (編輯傳入規則)。
5. 選取 Add Rule (新增規則)。
6. 針對 Type (類型)，執行下列其中一項操作：
 - 若是 Windows Server Amazon EC2 執行個體，請選擇 RDP。即會自動填入連接埠 3389。
 - 若是 Linux EC2 執行個體，請選擇 SSH。即會自動填入連接埠範圍 22。
7. 對於任意一個選項，請將來源設定為我的 IP，以便與 Amazon EC2 執行個體進行通訊。

Important

請不要將 0.0.0.0/0 指定為 CIDR 範圍，避免其他人存取您的執行個體。

8. 選擇儲存。

步驟 2. 將 Amazon EC2 執行個體連接至 AWS CloudHSM 叢集

您必須將叢集安全群組連接到 EC2 執行個體，以便 EC2 執行個體可以與叢集中的 HSM 通訊。叢集安全群組包含預先設定的規則，其允許透過連接埠 2223-2225 的傳入通訊。

將 EC2 執行個體連線至 AWS CloudHSM 叢集

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 EC2 儀表板。
2. 選取執行個體（執行中），然後選取您要安裝 AWS CloudHSM 用戶端之 EC2 執行個體的核取方塊。
3. 在頁面頂端，依序選擇動作、聯網和變更安全群組。
4. 選取群組名稱符合您叢集 ID 的安全群組，例如 `cloudhsm-cluster-<clusterID>-sg`。
5. 選擇新增安全群組。
6. 選取 Save (儲存)。

Note

您最多可以指派 5 個安全群組給 Amazon EC2 執行個體。如果您已達到上限，則必須修改 Amazon EC2 執行個體的預設安全群組和叢集安全群組：

在預設安全群組中，執行下列動作：

- 新增傳入規則，允許使用 TCP 通訊協定、來自叢集安全群組，且透過連接埠 2223-2225 的流量。

在叢集安全群組中，執行下列動作：

- 新增傳入規則，允許使用 TCP 通訊協定、來自預設安全群組，且透過連接埠 2223-2225 的流量。

在 中建立 HSM AWS CloudHSM

在 中建立叢集後 AWS CloudHSM，您可以建立硬體安全模組 (HSM)。不過，叢集必須在未初始化狀態，您才能在叢集建立 HSM。若要判斷叢集的狀態，[請在 AWS CloudHSM 主控台中檢視叢集頁面](#)、使用 AWS CLI 執行 [describe-clusters](#) 命令，或在 AWS CloudHSM API 中傳送 [DescribeClusters](#) 請求。您可以從 [AWS CloudHSM 主控台](#)、[AWS CLI](#) 或 AWS CloudHSM API 建立 HSM。

Console

建立 HSM (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 在您要為其建立 HSM 的叢集 ID 旁邊，選取選項按鈕。
3. 選取動作。從下拉式功能表中，選擇初始化。
4. 針對您要建立的 HSM 選擇可用區域 (AZ)。
5. 選取建立。

在建立叢集和 HSM 之後，您可以選擇[驗證 HSM 的身分](#)，或直接開始[初始化叢集](#)。

AWS CLI

建立 HSM ([AWS CLI](#))

- 在命令提示中，執行 [create-hsm](#) 命令。指定您先前建立之叢集的叢集 ID，以及 HSM 的可用區域。指定可用區域，格式為 us-west-2a、us-west-2b 等。

```
$ aws cloudhsmv2 create-hsm --cluster-id <cluster ID> --availability-  
zone <Availability Zone>  
  
{  
  "Hsm": {  
    "HsmId": "hsm-ted36yp5b2x",  
    "EniIp": "10.0.1.12",  
    "EniIpV6": "2600:113f:404:be09:310e:ed34:3412:f733",  
    "AvailabilityZone": "us-west-2a",  
    "ClusterId": "cluster-igklspoyj5v",  
    "EniId": "eni-5d7ade72",  
    "SubnetId": "subnet-fd54af9b",  
    "State": "CREATE_IN_PROGRESS"  
  }  
}
```

在建立叢集和 HSM 之後，您可以選擇[驗證 HSM 的身分](#)，或直接開始[初始化叢集](#)。

AWS CloudHSM API

建立 HSM (AWS CloudHSM API)

- 傳送 [CreateHsm](#) 要求。指定您先前建立之叢集的叢集 ID，以及 HSM 的可用區域。

在建立叢集和 HSM 之後，您可以選擇[驗證 HSM 的身分](#)，或直接開始[初始化叢集](#)。

在 AWS CloudHSM（選用）中驗證叢集 HSM 的身分和真實性

若要在中初始化叢集 AWS CloudHSM，您需要簽署叢集第一個硬體安全模組 (HSM) 所產生的憑證簽署請求 (CSR)。在這樣做之前，您可能需要驗證 HSM 的身分和真偽。

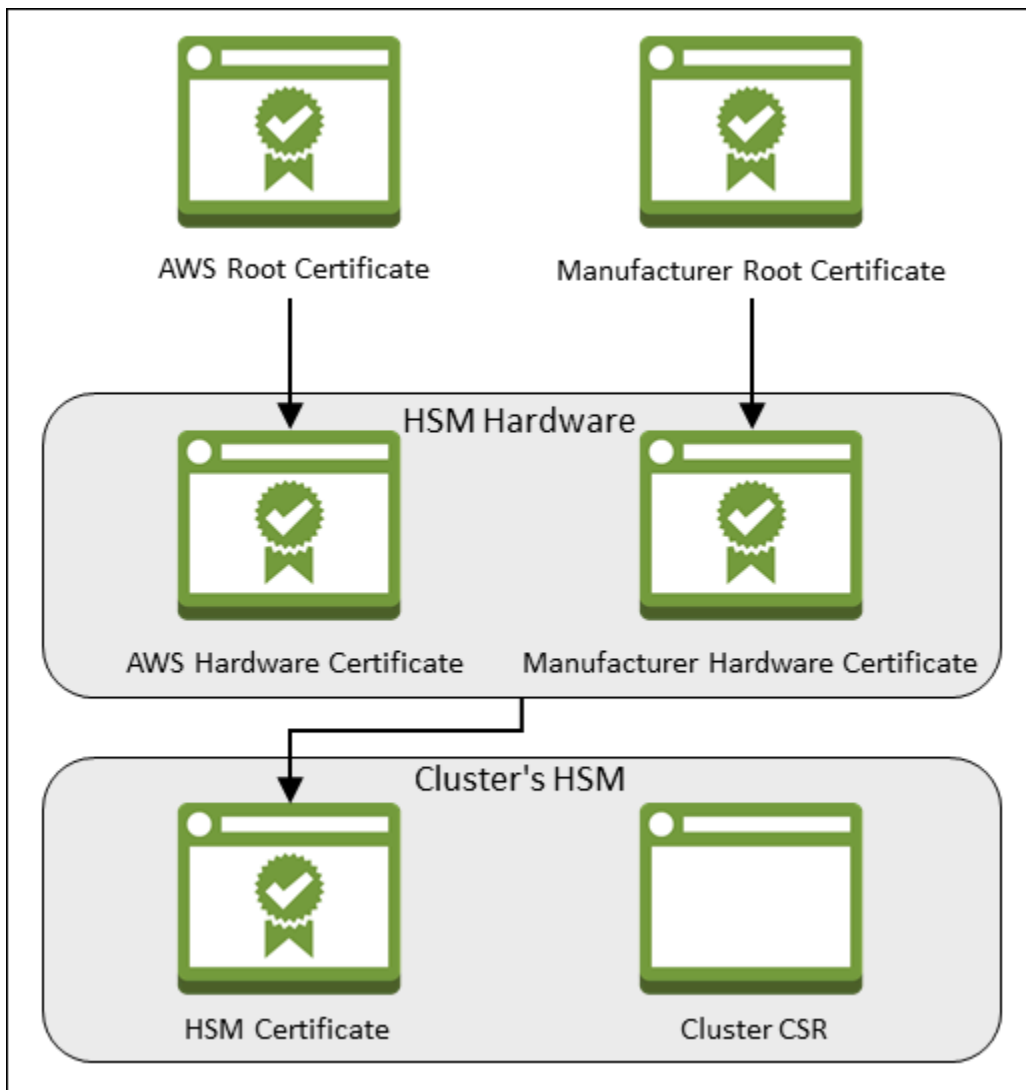
Note

此為選用程序。然而只在叢集初始化之前適用。叢集初始化之後，您就無法使用此程序來取得憑證或驗證 HSM。

若要驗證叢集第一個 HSM 的身分，請完成以下步驟：

1. [取得憑證和 CSR](#)：在此步驟中，您從 HSM 取得三個憑證和一個 CSR。您也可以取得兩個根憑證，一個來自 HSM 硬體製造商 AWS CloudHSM，另一個來自 HSM 硬體製造商。
2. [驗證憑證鏈](#) – 在此步驟中，您會建構兩個憑證鏈，一個是 AWS CloudHSM 根憑證，另一個是製造商根憑證。然後，您可以使用這些憑證鏈驗證 HSM 憑證，以確定 AWS CloudHSM 和硬體製造商都證明 HSM 的身分和真實性。
3. [比較公有金鑰](#)：在此步驟中，您擷取並比較 HSM 憑證和叢集 CSR 中的公有金鑰，以確保金鑰相同。這樣可讓您確信 CSR 是由真實可信任的 HSM 所產生。

下圖顯示 CSR、憑證及其相互關係。後續清單定義每個憑證。



AWS 根憑證

這是 AWS CloudHSM 根憑證。

製造商根憑證

這是硬體製造商的根憑證。

AWS 硬體憑證

AWS CloudHSM 會在 HSM 硬體新增至機群時建立此憑證。此憑證宣告 AWS CloudHSM 擁有硬體。

製造商硬體憑證

HSM 硬體製造商在製造 HSM 硬體時建立此憑證。此憑證聲明製造商建立此硬體。

HSM 憑證

當您在叢集中建立第一個 HSM 時，通過 FIPS 驗證的硬體會產生 HSM 憑證。此憑證聲明 HSM 硬體建立此 HSM。

叢集 CSR

第一個 HSM 建立叢集 CSR。當您[簽署叢集 CSR](#)時，您即宣稱擁有叢集。然後，您可以使用已簽署的 CSR 來[初始化叢集](#)。

步驟 1. 從 HSM 取得憑證

若要驗證 HSM 的身分和真偽，請先取得一個 CSR 和 5 個 HSM。您可以從 HSM 取得三個憑證，您可以使用 [AWS CloudHSM 主控台](#)、[AWS Command Line Interface \(AWS CLI\)](#) 或 AWS CloudHSM API 來執行。

Console

取得 CSR 和 HSM 憑證 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 選取您要驗證的 HSM 叢集 ID 旁的選項按鈕。
3. 選取動作。從下拉式功能表中，選擇初始化。
4. 如果您未完成[上一個步驟](#)來建立 HSM，請為您正在建立的 HSM 選擇一個可用區域 (AZ)。然後選取建立。
5. 當憑證和 CSR 準備好時，您會看到下載連結。

Certificate signing request

To initialize the cluster, you must download a certificate signing request (CSR) and then [sign it](#) .

 **Cluster CSR**

Cluster verification certificate

Optionally, you may wish to download the HSM certificate below which generated this Cluster CSR and [verify its authenticity](#) .

 **HSM certificate**

6. 選擇每個連結來下載和儲存 CSR 和憑證。為了簡化後續步驟，請將所有檔案儲存到相同目錄，並使用預設的檔案名稱。

AWS CLI

取得 CSR 和 HSM 憑證 ([AWS CLI](#))

- 在命令提示字元中，執行 [describe-clusters](#) 命令四次，每次都擷取 CSR 和不同的憑證，並將其儲存到檔案。
 - a. 發出下列命令來擷取叢集 CSR。將 *<cluster ID>* 取代為您先前建立的叢集 ID。

```
$ aws cloudhsmv2 describe-clusters --filters clusterIds=<cluster ID> \
                                     --output text \
                                     --query
'Clusters[].Certificates.ClusterCsr' \
                                     > <cluster ID>_ClusterCsr.csr
```

- b. 發出下列命令來擷取 HSM 憑證。將 *<cluster ID>* 取代為您先前建立的叢集 ID。

```
$ aws cloudhsmv2 describe-clusters --filters clusterIds=<cluster ID> \
                                     --output text \
                                     --query
'Clusters[].Certificates.HsmCertificate' \
                                     > <cluster ID>_HsmCertificate.crt
```

- c. 發出下列命令來擷取 AWS 硬體憑證。將 *<cluster ID>* 取代為您先前建立的叢集 ID。

```
$ aws cloudhsmv2 describe-clusters --filters clusterIds=<cluster ID> \
                                     --output text \
                                     --query
'Clusters[].Certificates.AwsHardwareCertificate' \
                                     > <cluster ID>_AwsHardwareCertificate.crt
```

- d. 發出下列命令來擷取製造商硬體憑證。將 *<cluster ID>* 取代為您先前建立的叢集 ID。

```
$ aws cloudhsmv2 describe-clusters --filters clusterIds=<cluster ID> \
                                     --output text \
                                     --query
'Clusters[].Certificates.ManufacturerHardwareCertificate' \
                                     > <cluster
ID>_ManufacturerHardwareCertificate.crt
```

AWS CloudHSM API

取得 CSR 和 HSM 憑證 (AWS CloudHSM API)

- 傳送 [DescribeClusters](#) 請求，然後從回應中擷取並儲存 CSR 和憑證。

步驟 2. 取得根憑證

請依照下列步驟取得 AWS CloudHSM 和 製造商的根憑證。將根憑證檔案儲存到包含 CSR 和 HSM 憑證檔案的目錄。

取得 AWS CloudHSM 和製造商根憑證

1. 下載 AWS CloudHSM 根憑證：[AWS_CloudHSM_Root-G1.zip](#)
2. 為您的 HSM 類型下載正確的製造商根憑證：
 - hsm1.medium 製造商根憑證：[liquid_security_certificate.zip](#)
 - hsm2m.medium 製造商根憑證：[liquid_security_certificate.zip](#)

Note

若要從其登陸頁面下載每個憑證，請使用以下連結：

- hsm1.medium [製造商根憑證](#) 的登陸頁面
- hsm2m.medium [製造商根憑證](#) 的登陸頁面

您可能需要用滑鼠右鍵按一下 Download Certificate (下載憑證) 連結，然後選擇 Save Link As...(另存連結為...) 以儲存憑證檔案。

3. 下載檔案之後，將其內容解壓縮 (unzip)。

步驟 3. 驗證憑證鏈

在此步驟中，您會建構兩個憑證鏈，一個是 AWS CloudHSM 根憑證，另一個是製造商根憑證。然後，使用 OpenSSL 根據每個憑證鏈來驗證 HSM 憑證。

若要建立憑證鏈，請開啟 Linux shell。您需要 OpenSSL (大多數的 Linux shell 中都有)，還需要您下載的[根憑證](#)和[HSM 憑證檔案](#)。不過，您不需要此步驟 AWS CLI 的，而且 shell 不需要與 AWS 您的帳戶建立關聯。

使用 AWS CloudHSM 根憑證驗證 HSM 憑證

1. 導覽至您下載的[根憑證](#)和[HSM 憑證檔案](#)的儲存目錄。以下命令假設所有憑證都在目前的目錄中，且使用預設的檔案名稱。

使用下列命令，依該順序建立包含 AWS 硬體憑證和 AWS CloudHSM 根憑證的憑證鏈。將 *<cluster ID>* 取代為您先前建立的叢集 ID。

```
$ cat <cluster ID>_AwsHardwareCertificate.crt \  
    AWS_CloudHSM_Root-G1.crt \  
    > <cluster ID>_AWS_chain.crt
```

2. 使用下列 OpenSSL 命令，根據 AWS 憑證鏈來驗證 HSM 憑證。將 *<cluster ID>* 取代為您先前建立的叢集 ID。

```
$ openssl verify -CAfile <cluster ID>_AWS_chain.crt <cluster ID>_HsmCertificate.crt  
<cluster ID>_HsmCertificate.crt: OK
```

根據製造商根憑證來驗證 HSM 憑證

1. 使用下列命令來建立憑證鏈，其中依序包含製造商硬體憑證和製造商根憑證。將 *<cluster ID>* 取代為您先前建立的叢集 ID。

```
$ cat <cluster ID>_ManufacturerHardwareCertificate.crt \  
    liquid_security_certificate.crt \  
    > <cluster ID>_manufacturer_chain.crt
```

2. 使用以下 OpenSSL 命令，根據製造商憑證鏈來驗證 HSM 憑證。將 *<cluster ID>* 取代為您先前建立的叢集 ID。

```
$ openssl verify -CAfile <cluster ID>_manufacturer_chain.crt <cluster  
ID>_HsmCertificate.crt  
<cluster ID>_HsmCertificate.crt: OK
```

步驟 4. 擷取和比較公有金鑰

使用 OpenSSL 來擷取並比較 HSM 憑證和叢集 CSR 中的公有金鑰，以確保金鑰相同。

若要比較公有金鑰，請使用 Linux shell。您需要 OpenSSL，這可在大多數 Linux shell 中使用，但此步驟不需要 AWS CLI。shell 不需要與 AWS 您的帳戶建立關聯。

擷取和比較公有金鑰

1. 使用下列命令從 HSM 憑證中擷取公有金鑰。

```
$ openssl x509 -in <cluster ID>_HsmCertificate.crt -pubkey -noout > <cluster ID>_HsmCertificate.pub
```

2. 使用下列命令從叢集 CSR 中擷取公有金鑰。

```
$ openssl req -in <cluster ID>_ClusterCsr.csr -pubkey -noout > <cluster ID>_ClusterCsr.pub
```

3. 使用下列命令來比較公有金鑰。如果公有金鑰相同，以下命令不會產生任何輸出。

```
$ diff <cluster ID>_HsmCertificate.pub <cluster ID>_ClusterCsr.pub
```

驗證 HSM 的身分和真偽之後，請繼續[初始化叢集](#)。

在 中初始化叢集 AWS CloudHSM

建立叢集並在 中新增硬體安全模組 (HSM) 之後 AWS CloudHSM，您可以初始化叢集。完成下列主題中的步驟來初始化 叢集。

Note

初始化叢集之前，請檢閱您可以用來[驗證 HSM 的身分和真實性](#)的程序。此程序為選擇性，且只能在叢集初始化前使用。將叢集初始化後，您無法使用此程序來取得您的憑證或驗證 HSM。

主題

- [步驟 1. 取得叢集 CSR](#)
- [步驟 2. 簽署 CSR](#)
- [步驟 3. 初始化叢集](#)

步驟 1. 取得叢集 CSR

初始化叢集之前，您必須下載並簽署憑證簽署請求 (CSR)，CSR 是由叢集的第一個 HSM 產生。如果您之前已依照[驗證叢集的 HSM 身分](#)中的步驟操作，則您已有 CSR，可以直接簽署。否則，請使用[AWS CloudHSM 主控台](#)、[AWS Command Line Interface \(AWS CLI\)](#) 或 AWS CloudHSM API 立即取得 CSR。

Important

如要初始化叢集，您的信任錨點必須符合 [RFC 5280](#) 並符合下列需求：

- 如使用 X509v3 延伸功能，則必須存在 X509v3 基本限制條件延伸。
- 信任錨點必須是自我簽署的憑證。
- 延伸值不得相互衝突。

Console

取得 CSR (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 選取您要驗證的 HSM 叢集 ID 旁的選項按鈕。
3. 選取動作。從下拉式功能表中，選擇初始化。
4. 如果您未完成[上一個步驟](#)來建立 HSM，請為您正在建立的 HSM 選擇一個可用區域 (AZ)。然後選取建立。
5. 當 CSR 準備好，您會看到可下載它的連結。

Certificate signing request

To initialize the cluster, you must download a certificate signing request (CSR) and then [sign it](#).

 **Cluster CSR**

Cluster verification certificate

Optionally, you may wish to download the HSM certificate below which generated this Cluster CSR and [verify its authenticity](#).

 **HSM certificate**

6. 選擇 Cluster CSR (叢集 CSR) 以下載並儲存 CSR。

AWS CLI

取得 CSR ([AWS CLI](#))

- 在命令提示字元，執行下列 [describe-clusters](#) 命令，其會擷取 CSR 並將它儲存到檔案。將 **<cluster ID>** 取代為[先前建立](#)的叢集 ID。

```
$ aws cloudhsmv2 describe-clusters --filters clusterIds=<cluster ID> \
                                     --output text \
                                     --query 'Clusters[].Certificates.ClusterCsr' \
```



```
> <cluster ID>_ClusterCsr.csr
```

AWS CloudHSM API

取得 CSR (AWS CloudHSM API)

1. 傳送 [DescribeClusters](#) 要求。
2. 擷取並儲存來自回應的 CSR。

步驟 2. 簽署 CSR

現在，您必須建立自我簽署的簽署憑證，並使用它來簽署您的叢集 CSR。此步驟不需要 AWS CLI，而且 shell 不需要與 AWS 您的帳戶建立關聯。若要簽署 CSR，您必須執行以下操作：

1. 完成上一節 (請參閱 [步驟 1. 取得叢集 CSR](#))。
2. 建立私有金鑰。
3. 使用私有金鑰來建立簽署憑證。
4. 簽署您的叢集 CSR。

建立私有金鑰。

Note

針對生產叢集，應使用信任的隨機來源以安全的方式建立您想建立的金鑰。我們建議您使用安全的離站和離線 HSM 或其他同等項目。安全地存放金鑰。金鑰會建立叢集的身分識別，以及您對叢集所包含的 HSM 的唯一控制權。

在開發和測試時，您可以使用任何方便的工具 (如 OpenSSL) 來建立和簽署叢集憑證。下列範例說明如何建立金鑰。在使用該金鑰建立自我簽署憑證 (請見以下) 後，您應該妥善存放它。若要登入 AWS CloudHSM 執行個體，憑證必須存在，但私有金鑰不會存在。

使用下列命令來建立私有金鑰。初始化 AWS CloudHSM 叢集時，您必須使用 RSA 2048 憑證或 RSA 4096 憑證。

```
$ openssl genrsa -aes256 -out customerCA.key 2048  
Generating RSA private key, 2048 bit long modulus
```

```

.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for customerCA.key:
Verifying - Enter pass phrase for customerCA.key:

```

使用私有金鑰來建立自我簽署憑證。

您用來建立生產叢集私有金鑰的信任硬體，也應該提供軟體工具來產生使用該金鑰的自我簽署憑證。以下範例使用 OpenSSL 和您在上個步驟中建立的私有金鑰來建立簽署憑證。憑證有效期限是 10 年 (3652 天)。請閱讀畫面上的指示，並依照提示操作。

```

$ openssl req -new -x509 -days 3652 -key customerCA.key -out customerCA.crt
Enter pass phrase for customerCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

```

此命令會建立名為 `customerCA.crt` 的憑證檔案。將此憑證放在您要從中連線到 AWS CloudHSM 叢集的每個主機上。如果您替檔案取了其他名稱，或將其存放在主機根目錄以外的路徑，請據此編輯您的用戶端組態檔案。使用您剛建立的憑證和私有金鑰來簽署後續步驟中的叢集憑證簽署請求 (CSR)。

簽署叢集 CSR

您用來建立生產叢集私有金鑰的信任硬體，也應該提供工具來簽署使用該金鑰的 CSR。以下範例會使用 OpenSSL 來簽署叢集的 CSR。範例會使用您的私有金鑰和以及在先前步驟中建立的自我簽署憑證。

```

$ openssl x509 -req -days 3652 -in <cluster ID>_ClusterCsr.csr \

```

```
-CA customerCA.crt \
-CAkey customerCA.key \
-CAcreateserial \
-out <cluster ID>_CustomerHsmCertificate.crt
```

Signature ok

subject=/C=US/ST=CA/O=Cavium/OU=N3FIPS/L=SanJose/CN=HSM:<HSM
identifier>:PARTN:<partition number>, for FIPS mode

Getting CA Private Key

Enter pass phrase for customerCA.key:

此命令會建立名為 *<cluster ID>_CustomerHsmCertificate.crt* 的檔案。初始化叢集時，使用這個檔案做為已簽署的憑證。

步驟 3。初始化叢集

使用已簽署的 HSM 憑證和簽署憑證來初始化您的叢集。您可以使用 [AWS CloudHSM 主控台](#)、[AWS CLI](#)、或 AWS CloudHSM API。

Console

初始化叢集 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 選取您要驗證的 HSM 叢集 ID 旁的選項按鈕。
3. 選取動作。從下拉式功能表中，選擇初始化。
4. 如果您未完成 [上一個步驟](#) 來建立 HSM，請為您正在建立的 HSM 選擇一個可用區域 (AZ)。然後選取建立。
5. 在 Download certificate signing request (下載憑證簽署請求) 頁面上，選擇 Next (下一步)。如果無法使用 Next (下一步)，先選擇其中一個 CSR 或憑證連結。然後選擇下一步。
6. 在 Sign certificate signing request (簽署憑證簽署請求) 頁面上，選擇 Next (下一步)。
7. 在 Upload the certificates (上傳憑證) 頁面上，執行下列動作：
 - a. 選擇 Cluster certificate (叢集憑證) 旁的 Upload file (上傳檔案)。然後，尋找並選取您之前簽署的 HSM 憑證。如果您已完成先前區段的步驟，請選取 *<cluster ID>_CustomerHsmCertificate.crt* 檔案。
 - b. 選擇 Issuing certificate (發行憑證) 旁的 Upload file (上傳檔案)。然後選擇您的簽署憑證。如果您已完成先前區段的步驟，請選取 customerCA.crt 檔案。
 - c. 選擇 Upload and initialize (上傳並初始化)。

AWS CLI

初始化叢集 ([AWS CLI](#))

- 在命令提示中，執行 [initialize-cluster](#) 命令。提供下列資訊：
 - 您先前建立之叢集的 ID。
 - 您先前簽署的 HSM 憑證。如果您已完成先前區段的步驟，它會儲存在名為 **<cluster ID>_CustomerHsmCertificate.crt** 的檔案中。
 - 您的簽署憑證。如果您已完成先前區段的步驟，簽署憑證會儲存在名為 customerCA.crt 的檔案中。

```
$ aws cloudhsmv2 initialize-cluster --cluster-id <cluster ID> \
                                     --signed-cert file://<cluster
                                     ID>_CustomerHsmCertificate.crt \
                                     --trust-anchor file://customerCA.crt
{
  "State": "INITIALIZE_IN_PROGRESS",
  "StateMessage": "Cluster is initializing. State will change to INITIALIZED
upon completion."
}
```

AWS CloudHSM API

初始化叢集 (AWS CloudHSM API)

- 使用下列項目傳送 [InitializeCluster](#) 請求：
 - 您先前建立之叢集的 ID。
 - 您先前簽署的 HSM 憑證。
 - 您的簽署憑證。

下載和設定 CloudHSM CLI

若要與 AWS CloudHSM 叢集中的 HSM 互動，您需要 CloudHSM CLI。

連線至您的用戶端執行個體並執行下列命令，以下載並安裝 AWS CloudHSM 命令列工具。如需詳細資訊，請參閱[啟動 Amazon EC2 用戶端執行個體以與 互動 AWS CloudHSM](#)。

Amazon Linux 2023

x86_64 架構上的 Amazon Linux 2023 :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-cli-latest.amzn2023.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.amzn2023.x86_64.rpm
```

ARM64 架構上的 Amazon Linux 2023 :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-cli-latest.amzn2023.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.amzn2023.aarch64.rpm
```

Amazon Linux 2

Amazon Linux 2 (x86_64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-cli-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el7.x86_64.rpm
```

Amazon Linux 2 (ARM64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-cli-latest.el7.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el7.aarch64.rpm
```

RHEL 9 (9.2+)

x86_64 架構上的 RHEL 9 :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-cli-latest.el9.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el9.x86_64.rpm
```

ARM64 架構上的 RHEL 9 :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-cli-latest.el9.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el9.aarch64.rpm
```

RHEL 8 (8.3+)

RHEL 8 (x86_64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-cli-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el8.x86_64.rpm
```

Ubuntu 24.04 LTS

x86_64 架構上的 Ubuntu 24.04 LTS :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/cloudhsm-cli_latest_u24.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u24.04_amd64.deb
```

ARM64 架構上的 Ubuntu 24.04 LTS :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/cloudhsm-cli_latest_u24.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u24.04_arm64.deb
```

Ubuntu 22.04 LTS

Ubuntu 22.04 LTS (x86_64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/cloudhsm-  
cli_latest_u22.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u22.04_amd64.deb
```

ARM64 架構上的 Ubuntu 22.04 LTS :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/cloudhsm-  
cli_latest_u22.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u22.04_arm64.deb
```

Ubuntu 20.04 LTS

Ubuntu 20.04 LTS (x86_64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Focal/cloudhsm-  
cli_latest_u20.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u20.04_amd64.deb
```

Windows Server 2022

對於 x86_64 架構上的 Windows Server 2022，請以管理員身分開啟 PowerShell，並執行下列命令：

```
PS C:\> wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Windows/  
AWSCloudHSMCLI-latest.msi -Outfile C:\AWSCloudHSMCLI-latest.msi
```

```
PS C:\> Start-Process msixexec.exe -ArgumentList '/i C:\AWSCloudHSMCLI-latest.msi /  
quiet /norestart /log C:\client-install.txt' -Wait
```

Windows Server 2019

對於 Windows Server 2019 (x86_64 架構)，請以系統管理員身分開啟 PowerShell，然後執行下列命令：

```
PS C:\> wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Windows/AWSCloudHSMCLI-latest.msi -Outfile C:\AWSCloudHSMCLI-latest.msi
```

```
PS C:\> Start-Process msixec.exe -ArgumentList '/i C:\AWSCloudHSMCLI-latest.msi /quiet /norestart /log C:\client-install.txt' -Wait
```

Windows Server 2016

對於 Windows Server 2016 (x86_64 架構)，請以系統管理員身分開啟 PowerShell，然後執行下列命令：

```
PS C:\> wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Windows/AWSCloudHSMCLI-latest.msi -Outfile C:\AWSCloudHSMCLI-latest.msi
```

```
PS C:\> Start-Process msixec.exe -ArgumentList '/i C:\AWSCloudHSMCLI-latest.msi /quiet /norestart /log C:\client-install.txt' -Wait
```

使用下列命令來設定 CloudHSM CLI。

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用設定工具指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-cli -a <The ENI IPv4 / IPv6 addresses of the HSMs>
```

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用設定工具指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" -a <The ENI IPv4 / IPv6 addresses of the HSMs>
```

在中啟用叢集 AWS CloudHSM

當您啟用 AWS CloudHSM 叢集時，叢集的狀態會從初始化變更為作用中。然後，您就可以[管理硬體安全模組 \(HSM\) 的使用者](#)和[使用 HSM](#)。

⚠ Important

在啟動叢集之前，您必須先將簽發的憑證複製到連線至叢集的每個 EC2 執行個體平台的預設位置 (您可以在初始化叢集時建立發行憑證)。

Linux

```
/opt/cloudhsm/etc/customerCA.crt
```

Windows

```
C:\ProgramData\Amazon\CloudHSM\customerCA.crt
```

放置簽發的憑證後，請安裝 CloudHSM CLI，並在您的第一個 HSM 上執行 [cluster activate](#) 命令。您會注意到叢集中第一個 HSM 上的管理員帳戶具有 [未啟用的管理員](#) 角色。這是僅在叢集啟動之前暫時存在的角色。當您啟動叢集時，未啟用的管理員角色會變更為管理員。

啟用叢集

1. 連接到您先前啟動的用戶端執行個體。如需詳細資訊，請參閱[啟動 Amazon EC2 用戶端執行個體以與 互動 AWS CloudHSM](#)。您可以啟動 Linux 執行個體或 Windows Server。
2. 以互動式模式執行 CloudHSM CLI。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

3. (選用) 使用 user list 命令來顯示現有的使用者。

```
aws-cloudhsm > user list
{
  "error_code": 0,
  "data": {
    "users": [
      {
```

```

    "username": "admin",
    "role": "unactivated-admin",
    "locked": "false",
    "mfa": [],
    "cluster-coverage": "full"
  },
  {
    "username": "app_user",
    "role": "internal(APPLIANCE_USER)",
    "locked": "false",
    "mfa": [],
    "cluster-coverage": "full"
  }
]
}
}

```

4. 使用 `cluster activate` 命令設定初始管理員密碼。

```

aws-cloudhsm > cluster activate
Enter
password:<NewPassword>
Confirm password:<NewPassword>
{
  "error_code": 0,
  "data": "Cluster activation successful"
}

```

建議您將新密碼寫在密碼工作表。不要遺失此工作表。建議您列印一份密碼工作表，用來記錄重要的 HSM 密碼，並存放於安全之處。另外也建議您將一份這個工作表存放於安全的離站儲存區。

5. (選用) 使用 `user list` 命令，確認使用者的類型已變更為[管理員/CO](#)。

```

aws-cloudhsm > user list
{
  "error_code": 0,
  "data": {
    "users": [
      {
        "username": "admin",
        "role": "admin",

```

```
    "locked": "false",
    "mfa": [],
    "cluster-coverage": "full"
  },
  {
    "username": "app_user",
    "role": "internal(APPLIANCE_USER)",
    "locked": "false",
    "mfa": [],
    "cluster-coverage": "full"
  }
]
```

6. 使用 `quit` 命令來停止 CloudHSM CLI 工具。

```
aws-cloudhsm > quit
```

如需使用 CloudHSM CLI 或 CMU 的詳細資訊，請參閱[了解 HSM 使用者](#)和[了解使用 CMU 的 HSM 使用者管理](#)。

在用戶端和 AWS CloudHSM 之間設定交互 TLS（建議）

下列主題說明您必須完成的步驟，才能在用戶端與之間啟用交互 TLS (mTLS) AWS CloudHSM。目前此功能僅適用於 `hsm2m.medium`。如需 HSM 類型的詳細資訊，請參閱 [AWS CloudHSM 叢集模式](#)。

主題

- [步驟 1. 在 HSM 上建立並註冊信任錨點](#)
- [步驟 2. 為啟用 mTLS AWS CloudHSM](#)
- [步驟 3. 設定的 mTLS 強制執行 AWS CloudHSM](#)

步驟 1. 在 HSM 上建立並註冊信任錨點

在啟用 mTLS 之前，必須先在 HSM 上建立並註冊信任錨點。這是一個兩步驟的程序：

主題

- [建立私有金鑰和自我簽署根憑證](#)
- [在 HSM 上註冊信任錨點](#)

建立私有金鑰和自我簽署根憑證

Note

針對生產叢集，應使用信任的隨機來源以安全的方式建立您想建立的金鑰。我們建議您使用安全的離站和離線 HSM 或其他同等項目。安全地存放金鑰。

對於開發和測試，您可以使用任何方便的工具（例如 OpenSSL）來建立金鑰並自我簽署根憑證。您將需要金鑰和根憑證，才能在[啟用 mTLS AWS CloudHSM](#)中簽署用戶端憑證。

下列範例示範如何使用 [OpenSSL](#) 建立私有金鑰和自我簽署根憑證。

Example – 使用 OpenSSL 建立私有金鑰

使用下列命令來建立以 AES-256 演算法加密的 4096 位元 RSA 金鑰。若要使用此範例，請將 `<mtls_ca_root_1.key>` 取代為您要存放金鑰的檔案名稱。

```
$ openssl genrsa -out <mtls_ca_root_1.key> -aes256 4096
Generating RSA private key, 4096 bit long modulus
.....+++
.+++
e is 65537 (0x10001)
Enter pass phrase for mtls_ca_root_1.key:
Verifying - Enter pass phrase for mtls_ca_root_1.key:
```

Example – 使用 OpenSSL 建立自我簽署根憑證

使用下列命令，`mtls_ca_root_1.crt` 從您剛建立的私有金鑰建立名為 `mtls_ca_root_1.crt` 的自我簽署根憑證。憑證有效期為 25 年 (9130 天)。請閱讀畫面上的指示，並依照提示操作。

```
$ openssl req -new -x509 -days 9130 -key mtls_ca_root_1.key -out mtls_ca_root_1.crt
Enter pass phrase for mtls_ca_root_1.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
```

For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

在 HSM 上註冊信任錨點

建立自我簽署根憑證之後，管理員必須將憑證註冊為 AWS CloudHSM 叢集的信任錨點。

向 HSM 註冊信任錨點

1. 使用下列命令來啟動 CloudHSM CLI：

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 CloudHSM CLI，以管理員身分登入。

```
aws-cloudhsm > login --username <admin> --role admin
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "<admin>",
    "role": "admin"
  }
}
```

3. 使用 [向 CloudHSM CLI 註冊信任錨點](#) 命令來註冊信任錨點。如需詳細資訊，請參閱下列範例或使用 `help cluster mtls register-trust-anchor` 命令。

Example – 向 AWS CloudHSM 叢集註冊信任錨點

下列範例示範如何在 CloudHSM CLI 中使用 `cluster mtls register-trust-anchor` 命令，將信任錨點註冊到 HSM。若要使用此命令，管理員必須登入 HSM。以您自己的值取代這些值：

```
aws-cloudhsm > cluster mtls register-trust-anchor --path </path/mtls_ca_root_1.crt>
{
  "error_code": 0,
  "data": {
    "trust_anchor": {
      "certificate-reference": "0x01",
      "certificate": "<PEM Encoded Certificate>",
      "cluster-coverage": "full"
    }
  }
}
```

Note

AWS CloudHSM 支援將中繼憑證註冊為信任錨點。在這種情況下，整個 PEM 編碼的憑證鏈檔案需要註冊到 HSM，並以階層順序使用憑證。
AWS CloudHSM 支援 6980 位元組的憑證鏈。

成功註冊信任錨點後，您可以執行 `cluster mtls list-trust-anchors` 命令來檢查目前註冊的信任錨點，如下所示：

```
aws-cloudhsm > cluster mtls list-trust-anchors
{
  "error_code": 0,
  "data": {
    "trust_anchors": [
      {
        "certificate-reference": "0x01",
        "certificate": "<PEM Encoded Certificate>",
        "cluster-coverage": "full"
      }
    ]
  }
}
```

Note

可以在 hsm2m.medium 上註冊的信任錨數上限為兩 (2) 個。

步驟 2. 為 啟用 mTLS AWS CloudHSM

若要為 啟用 mTLS AWS CloudHSM，您需要建立私有金鑰和由我們在建立中產生的根憑證簽署的用戶端憑證，[並將信任錨點註冊到 HSM](#)，然後使用任何用戶端 SDK 5 設定工具來設定私有金鑰路徑和用戶端憑證鏈路徑。

主題

- [建立私有金鑰和用戶端憑證鏈](#)
- [設定用戶端 SDK 5 的 mTLS](#)

建立私有金鑰和用戶端憑證鏈

Example – 使用 OpenSSL 建立私有金鑰

使用下列命令來建立 4096 位元 RSA 金鑰。若要使用此範例，請將 *<ssl-client.key>* 取代為您要存放金鑰的檔案名稱。

```
$ openssl genrsa -out <ssl-client.key> 4096
Generating RSA private key, 4096 bit long modulus
.....+++
.+++
e is 65537 (0x10001)
```

Example – 使用 OpenSSL 產生憑證簽署請求 (CSR)

使用下列命令，從您剛建立的私有金鑰產生憑證簽署請求 (CSR)。請閱讀畫面上的指示，並依照提示操作。

```
$ openssl req -new -key <ssl-client.key> -out <ssl-client.csr>
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

Example – 使用根憑證簽署 CSR

使用以下命令，以我們在[建立信任錨點並將其註冊到 HSM 中建立和註冊的根憑證簽署 CSR](#)，並建立名為 `ssl-client.crt` 的用戶端憑證。憑證有效期為 5 年 (1826 天)。

```
$ openssl x509 -req -days 1826 -in <ssl-client.csr> -CA <mtls_ca_root_1.crt> -
CAkey <mtls_ca_root_1.key> -CAcreateserial -out <ssl-client.crt>
```

Example – 建立用戶端憑證鏈

使用以下命令來結合我們在[建立和註冊信任錨點到 HSM](#) 中建立和註冊的用戶端憑證和根憑證，並建立名為 `ssl-client.pem` 的用戶端憑證鏈，用於在下一個步驟中設定。

```
$ cat <ssl-client.crt> <mtls_ca_root_1.crt> > <ssl-client.pem>
```

Note

如果您在[建立中繼憑證並在 HSM 上註冊信任錨點](#)做為信任錨點，請務必將用戶端憑證與整個憑證鏈結合，以建立用戶端憑證鏈。

設定用戶端 SDK 5 的 mTLS

使用任何用戶端 SDK 5 設定工具，透過提供正確的用戶端金鑰路徑和用戶端憑證鏈路徑來啟用交互 TLS。如需設定用戶端 SDK 5 工具的詳細資訊，請參閱[???](#)。

PKCS #11 library

使用自訂憑證和金鑰搭配 Linux 上的用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。


```
$ sudo cp ssl-client.pem </opt/cloudhsm/etc>
$ sudo cp ssl-client.key </opt/cloudhsm/etc>
```

2. 使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 \
    --client-cert-hsm-tls-file </opt/cloudhsm/etc/ssl-client.pem> \
    --client-key-hsm-tls-file </opt/cloudhsm/etc/ssl-client.key>
```

在 Windows 上使用自訂憑證和金鑰與用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
cp ssl-client.pem <C:\ProgramData\Amazon\CloudHSM\ssl-client.pem>
cp ssl-client.key <C:\ProgramData\Amazon\CloudHSM\ssl-client.key>
```

2. 使用 PowerShell 解譯器時，請使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" `
    --client-cert-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.pem> `
    --client-key-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.key>
```

OpenSSL Dynamic Engine

使用自訂憑證和金鑰搭配 Linux 上的用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
$ sudo cp ssl-client.pem </opt/cloudhsm/etc>
$ sudo cp ssl-client.key </opt/cloudhsm/etc>
```

2. 使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
$ sudo /opt/cloudhsm/bin/configure-dyn \
    --client-cert-hsm-tls-file </opt/cloudhsm/etc/ssl-client.pem> \
```

```
--client-key-hsm-tls-file </opt/cloudhsm/etc/ssl-client.key>
```

Key Storage Provider (KSP)

在 Windows 上使用自訂憑證和金鑰與用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
cp ssl-client.pem <C:\ProgramData\Amazon\CloudHSM\ssl-client.pem>
cp ssl-client.key <C:\ProgramData\Amazon\CloudHSM\ssl-client.key>
```

2. 使用 PowerShell 解譯器時，請使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" `
    --client-cert-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.pem> `
    --client-key-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.key>
```

JCE provider

使用自訂憑證和金鑰搭配 Linux 上的用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
$ sudo cp ssl-client.pem </opt/cloudhsm/etc>
sudo cp ssl-client.key </opt/cloudhsm/etc>
```

2. 使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
$ sudo /opt/cloudhsm/bin/configure-jce \
    --client-cert-hsm-tls-file </opt/cloudhsm/etc/ssl-client.pem> \
    --client-key-hsm-tls-file </opt/cloudhsm/etc/ssl-client.key>
```

在 Windows 上使用自訂憑證和金鑰與用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
cp ssl-client.pem <C:\ProgramData\Amazon\CloudHSM\ssl-client.pem>
cp ssl-client.key <C:\ProgramData\Amazon\CloudHSM\ssl-client.key>
```

2. 使用 PowerShell 解譯器時，請使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" `
    --client-cert-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.pem> `
    --client-key-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.key>
```

CloudHSM CLI

使用自訂憑證和金鑰搭配 Linux 上的用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
$ sudo cp ssl-client.pem </opt/cloudhsm/etc>
sudo cp ssl-client.key </opt/cloudhsm/etc>
```

2. 使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
$ sudo /opt/cloudhsm/bin/configure-cli \
    --client-cert-hsm-tls-file </opt/cloudhsm/etc/ssl-client.pem> \
    --client-key-hsm-tls-file </opt/cloudhsm/etc/ssl-client.key>
```

在 Windows 上使用自訂憑證和金鑰與用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
cp ssl-client.pem <C:\ProgramData\Amazon\CloudHSM\ssl-client.pem>
cp ssl-client.key <C:\ProgramData\Amazon\CloudHSM\ssl-client.key>
```

2. 使用 PowerShell 解譯器時，請使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" `
```

```
--client-cert-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-  
client.pem>`  
--client-key-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-  
client.key>
```

步驟 3。設定 的 mTLS 強制執行 AWS CloudHSM

使用任何用戶端 SDK 5 設定工具設定之後，用戶端與之間的連線 AWS CloudHSM 將成為叢集中的交互 TLS。不過，從組態檔案移除私有金鑰路徑和用戶端憑證鏈路徑將再次將連線轉換為一般 TLS。您可以使用 CloudHSM CLI 完成下列步驟，在叢集中設定 mtls 強制執行：

1. 使用下列命令來啟動 CloudHSM CLI：

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 CloudHSM CLI，以管理員身分登入。

```
aws-cloudhsm > login --username <admin> --role admin  
Enter password:  
{  
  "error_code": 0,  
  "data": {  
    "username": "<admin>",  
    "role": "admin"  
  }  
}
```

Note

1. 請確定您已設定 CloudHSM CLI，並在 mTLS 連線下啟動 CloudHSM CLI。
2. 在設定 mTLS 強制執行之前，您必須以使用者名稱為 admin 的預設管理員使用者身分登入。

3. 使用 [使用 CloudHSM CLI 設定 mTLS 強制執行層級](#) 命令來設定強制執行。如需詳細資訊，請參閱下列範例或使用 `help cluster mtls set-enforcement` 命令。

Example – 使用 AWS CloudHSM 叢集設定 mTLS 強制執行

下列範例示範如何在 CloudHSM CLI 中使用 `cluster mtls set-enforcement` 命令，透過 HSM 設定 mTLS 強制執行。若要使用此命令，使用者名稱為 `admin` 的管理員必須登入 HSM。

```
aws-cloudhsm > cluster mtls set-enforcement --level cluster
{
  "error_code": 0,
  "data": {
    "message": "Mtls enforcement level set to Cluster successfully"
  }
}
```

 Warning

在叢集中強制執行 mTLS 用量後，所有現有的非 mTLS 連線都會遭到捨棄，而且您只能使用 mTLS 憑證連線到叢集。

在 中建立和使用金鑰 AWS CloudHSM

在新叢集中建立和使用金鑰之前，請使用 AWS CloudHSM CLI 建立硬體安全模組 (HSM) 使用者。如需詳細資訊，請參閱[了解 HSM 使用者管理任務](#)、[AWS CloudHSM 命令列界面 \(CLI\) 入門](#)，以及[如何管理 HSM 使用者](#)。

 Note

如使用用戶端 SDK 3，請使用 [CloudHSM 管理公用程式 \(CMU\)](#) 而不是 CloudHSM CLI。

建立 HSM 使用者之後，您可以使用下列任一選項登入 HSM 和管理金鑰：

- 使用[金鑰管理公用程式，命令列工具](#)
- 使用[PKCS #11 程式庫](#)建立 C 應用程式
- 使用[JCE 提供程序](#)建立 Java 應用程式

- 使用[直接從命令列使用 OpenSSL 動態引擎](#)
- 使用 OpenSSL 動態引擎在 [NGINX 和 Apache Web 伺服器](#)上進行 TLS 卸載
- 使用的金鑰儲存提供者 (KSP) AWS CloudHSM 搭配 [Microsoft Windows Server 憑證授權機構 \(CA\)](#)
- 將的金鑰儲存提供者 (KSP) AWS CloudHSM 與 [Microsoft Sign Tool](#) 搭配使用
- 透過[網際網路資訊伺服器 \(IIS\) Web 伺服器](#)使用 TLS 卸載的金鑰儲存提供者 (KSP)

的最佳實務 AWS CloudHSM

執行本主題中的最佳實務以有效使用 AWS CloudHSM。

目錄

- [AWS CloudHSM 叢集管理最佳實務](#)
- [AWS CloudHSM 使用者管理最佳實務](#)
- [AWS CloudHSM 金鑰管理最佳實務](#)
- [AWS CloudHSM 應用程式整合最佳實務](#)
- [AWS CloudHSM 監控最佳實務](#)

AWS CloudHSM 叢集管理最佳實務

建立、存取和管理 AWS CloudHSM 叢集時，請遵循本節中的最佳實務。

擴展叢集以處理尖峰流量

有幾個因素可能會影響叢集可處理的最大輸送量，包括用戶端執行個體大小、叢集大小、網路拓撲，以及使用案例所需的密碼編譯操作。

做為起點，請參閱主題[AWS CloudHSM 效能資訊](#)，以取得常見叢集大小和組態的效能預估。我們建議您使用預期的尖峰負載來測試叢集，以判斷目前的架構是否具有彈性且規模正確。

架構您的叢集以獲得高可用性

將備援新增至維護帳戶：AWS 可以取代您的 HSM 進行排定的維護，或如果它偵測到問題。一般而言，您的叢集大小應至少具有 +1 備援。例如，如果您需要兩個 HSMs 讓您的服務在尖峰時間運作，則理想的叢集大小將是三個。如果您遵循與可用性相關的最佳實務，這些 HSM 替換不應影響您的服務。不過，已取代 HSM 的進行中操作可能會失敗，必須重試。

將您的 HSMs 分散到多個可用區域：考慮您的服務如何在可用區域中斷期間運作。AWS 建議您將 HSMs 分散到盡可能多的可用區域。對於具有三個 HSMs 叢集，您應該將 HSMs 分散到三個可用區域。根據您的系統，您可能需要額外的備援。

至少有三個 HSMs 以確保新產生的金鑰的耐久性

對於需要新產生的金鑰耐久性的應用程式，我們建議在一個區域的不同可用區域中至少分佈三個 HSMs。

安全存取您的叢集

使用私有子網路來限制對執行個體的存取：在 VPC 的私有子網路中啟動 HSMs 和用戶端執行個體。這會限制從外部世界存取您的 HSMs。

使用 VPC 端點存取 APIs：AWS CloudHSM 資料平面設計用於操作，而不需要存取網際網路或 AWS APIs。如果您的用戶端執行個體需要存取 AWS CloudHSM API，您可以使用 VPC 端點來存取 API，而不需要用戶端執行個體上的網際網路存取。如需詳細資訊，請參閱[AWS CloudHSM 和 VPC 端點](#)。

根據您的需求擴展以降低成本

無需預付費用即可使用 AWS CloudHSM。您需為啟動的每個 HSM 支付每小時費用，直到您終止 HSM 為止。如果您的服務不需要持續使用 AWS CloudHSM，您可以將 HSMs 縮減（刪除）為零，以降低成本。當再次需要 HSMs 時，您可以從備份還原 HSMs。例如，如果您有一個工作負載需要您每月簽署一次程式碼，特別是在當月的最後一天，您可以在之前擴展叢集，在工作完成後刪除 HSMs 將其縮減，然後在下個月結束時還原叢集以再次執行簽署操作。

AWS CloudHSM 會自動定期備份叢集中的 HSMs。在稍後日期新增新的 HSM 時，AWS CloudHSM 會將最新的備份還原到新的 HSM，以便您可以從您離開的相同位置恢復使用。若要計算 AWS CloudHSM 架構成本，請參閱 [AWS CloudHSM 定價](#)。

相關資源：

- [備份的一般概觀](#)
- [備份保留政策](#)
- [跨 AWS 區域複製 AWS CloudHSM 叢集備份](#)

AWS CloudHSM 使用者管理最佳實務

遵循本節中的最佳實務，有效管理 AWS CloudHSM 叢集中的使用者。HSM 使用者與 IAM 使用者不同。透過 AWS API 與資源互動，具有具有適當許可之身分型政策的 IAM 使用者和實體可以建立 HSMs。HSM 建立後，您必須使用 HSM 使用者憑證來驗證 HSM 上的操作。如需 HSM 使用者的詳細指南，請參閱 [中的 HSM 使用者 AWS CloudHSM](#)。

保護 HSM 使用者的登入資料

請務必保護 HSM 使用者的登入資料的安全，因為 HSM 使用者是可在 HSM 上存取和執行密碼編譯和管理操作的實體。AWS CloudHSM 無法存取您的 HSM 使用者登入資料，而且如果您無法存取這些登入資料，將無法提供協助。

至少有兩個管理員以防止鎖定

為了避免您的叢集遭到鎖定，我們建議您至少有兩個管理員，以防遺失一個管理員密碼。如果發生這種情況，您可以使用其他管理員來重設密碼。

Note

用戶端 SDK 5 中的管理員與用戶端 SDK 3 中的加密主管 (COs) 同義。

為所有使用者管理操作啟用規定人數

Quorum 可讓您設定最低數量的管理員，這些管理員必須核准使用者管理操作，才能進行該操作。由於管理員擁有的權限，我們建議您為所有使用者管理操作啟用規定人數。如果您的其中一個管理員密碼洩露，這可能會限制影響的可能性。如需詳細資訊，請參閱[管理配額](#)。

建立多個加密使用者，每個使用者具有有限的許可

透過區隔加密使用者的責任，沒有人可以完全控制整個系統。因此，我們建議您建立多個加密使用者，並限制每個使用者的許可。通常，這是透過給予不同的加密使用者完全不同的責任和他們執行的動作來完成的（例如，有一個加密使用者負責產生金鑰，並與其他加密使用者共用金鑰，然後在您的應用程式中使用這些金鑰）。

相關資源：

- [使用 CloudHSM CLI 共用金鑰](#)
- [使用 CloudHSM CLI 取消共用金鑰](#)

AWS CloudHSM 金鑰管理最佳實務

管理金鑰時，請遵循本節中的最佳實務 AWS CloudHSM。

選擇正確的金鑰類型

使用工作階段金鑰時，每秒交易數 (TPS) 將僅限於金鑰存在的一個 HSM。叢集中的額外 HSMs 不會增加該金鑰的請求輸送量。如果您針對相同的應用程式使用權杖金鑰，您的請求將在叢集中的所有可用 HSMs 之間進行負載平衡。如需詳細資訊，請參閱[中的金鑰同步和持久性設定 AWS CloudHSM](#)。

管理金鑰儲存限制

HSMs 對可在 HSM 上一次存放的字符和工作階段金鑰數目上限有限制。如需金鑰儲存限制的資訊，請參閱 [AWS CloudHSM 配額](#)。如果您的應用程式需要超過限制，您可以使用下列一或多個策略來有效管理金鑰：

使用信任的包裝將您的金鑰存放在外部資料存放區：使用信任的金鑰包裝，您可以透過將包裝在外部資料存放區中的所有金鑰存放區來克服金鑰儲存限制。當您需要使用此金鑰時，您可以將金鑰取消包裝至 HSM 做為工作階段金鑰，使用金鑰進行必要的操作，然後捨棄工作階段金鑰。原始金鑰資料會安全地存放在資料存放區中，以便在需要時使用。使用信任的金鑰來執行此操作可最大化您的保護。

在叢集之間分配金鑰：克服金鑰儲存限制的另一個策略是將金鑰儲存在多個叢集中。在此方法中，您會維護儲存在每個叢集中的金鑰映射。使用此映射將用戶端請求路由到具有所需金鑰的叢集。如需如何從相同用戶端應用程式連線至多個叢集的資訊，請參閱下列主題：

- [使用 JCE 供應商連線至多個 AWS CloudHSM 叢集](#)
- [適用於的 PKCS #11 程式庫的多個槽組態 AWS CloudHSM](#)

管理和保護金鑰包裝

金鑰可透過 EXTRACTABLE 屬性標示為可擷取或不可擷取。根據預設，HSM 金鑰會標示為可擷取。

可擷取金鑰是允許透過金鑰包裝從 HSM 匯出的金鑰。包裝的金鑰會加密，必須先使用相同的包裝金鑰取消包裝，才能使用。在任何情況下，都不能從 HSM 匯出無法擷取的金鑰。無法擷取不可擷取的金鑰。因此，請務必考慮是否需要擷取金鑰，並相應地設定對應的金鑰屬性。

如果您在應用程式中需要金鑰包裝，您應該利用信任的金鑰包裝來限制 HSM 使用者只能包裝/取消包裝已被管理員明確標記為信任的金鑰。如需詳細資訊，請參閱 [中受信任金鑰包裝的主題](#) [中的金鑰 AWS CloudHSM](#)。

相關資源

- [包裝和解包函數](#)
- [JCE 的加密函數](#)
- [用戶端 SDK AWS CloudHSM 5 支援的 Java 金鑰屬性](#)
- [CloudHSM CLI 的金鑰屬性](#)

AWS CloudHSM 應用程式整合最佳實務

遵循本節中的最佳實務，以最佳化應用程式與 AWS CloudHSM 叢集的整合方式。

引導您的用戶端 SDK

用戶端 SDK 可以連線到叢集之前，必須先將其引導。將 IP 地址引導至叢集時，建議您盡可能使用 `--cluster-id` 參數。此方法會將叢集中的所有 HSM IP 地址填入您的組態，而不需要追蹤每個個別地址。如果 HSM 正在進行維護或在可用區域中斷期間，這樣做會為您的應用程式初始化增加額外的彈性。如需詳細資訊，請參閱[引導用戶端 SDK](#)。

驗證以執行 操作

在 中 AWS CloudHSM，您必須先向叢集進行身分驗證，才能執行大多數操作，例如密碼編譯操作。

使用 CloudHSM CLI 驗證：您可以使用 CloudHSM CLI 的[單一命令模式](#)或[互動式模式](#)進行驗證。使用[使用 CloudHSM CLI 登入 HSM](#) 命令在互動式模式下進行身分驗證。若要在單一命令模式下進行身分驗證，您必須設定環境變數 `CLOUDHSM_ROLE` 和 `CLOUDHSM_PIN`。如需執行此操作的詳細資訊，請參閱[單一命令模式](#)。AWS CloudHSM 建議您在應用程式未使用時安全地存放 HSM 登入資料。

使用 PKCS #11 驗證：在 PKCS #11 中，您在使用 `C_OpenSession` 開啟工作階段後，使用 `C_Login` API 登入。每個插槽（叢集）只需要執行一個 `C_Login`。成功登入後，您可以使用 `C_OpenSession` 開啟其他工作階段，而不需要執行其他登入操作。如需驗證為 PKCS #11 的範例，請參閱[用戶端 SDK AWS CloudHSM 5 的 PKCS #11 程式庫程式碼範例](#)。

使用 JCE 驗證：AWS CloudHSM JCE 提供者支援隱含和明確登入。適合您的方法取決於您的使用案例。如果可能，我們建議您使用隱含登入，因為如果您的應用程式與您的叢集中斷連線且需要重新驗證，開發套件將自動處理身分驗證。使用隱含登入也可讓您在無法控制應用程式程式碼的整合時，提供登入資料給應用程式。如需登入方法的詳細資訊，請參閱[步驟 2：提供登入資料給 JCE 供應商](#)。

使用 OpenSSL 驗證：使用 OpenSSL 動態引擎，您可以透過環境變數提供登入資料。AWS CloudHSM 建議在應用程式未使用時安全地存放 HSM 登入資料。如果可能，您應該將環境設定為系統性地擷取和設定這些環境變數，而不需要手動輸入。如需使用 OpenSSL 驗證的詳細資訊，請參閱[安裝適用於用戶端 SDK 5 的 AWS CloudHSM OpenSSL 動態引擎](#)。

使用 KSP 驗證：您可以使用 Windows 登入資料管理員或環境變數向金鑰儲存提供者 (KSP) 進行驗證，請參閱[安裝 AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 \(KSP\)](#)。

有效管理應用程式中的金鑰

使用金鑰屬性來控制金鑰可以執行的動作：產生金鑰時，請使用金鑰屬性來定義一組許可，以允許或拒絕該金鑰的特定操作類型。我們建議您使用完成其任務所需的最少屬性來產生金鑰。例如，也不應允許用於加密的 AES 金鑰將金鑰包裝出 HSM。如需詳細資訊，請參閱下列用戶端 SDKs 的屬性頁面：

- [PKCS #11 金鑰屬性](#)
- [JCE 金鑰屬性](#)

如果可能，快取金鑰物件以將延遲降至最低：金鑰尋找操作將查詢叢集中的每個 HSM。此操作非常昂貴，而且不會隨著叢集中的 HSM 計數而擴展。

- 透過 PKCS #11，您可以使用 `C_FindObjects` API 找到金鑰。
- 透過 JCE，您可以使用 `KeyStore` 找到金鑰。

為了獲得最佳效能，AWS 建議您在應用程式啟動期間僅使用金鑰尋找命令（例如 [使用 KMU 依屬性搜尋 AWS CloudHSM 索引鍵](#) 和 [使用 CloudHSM CLI 列出使用者的金鑰](#)）一次，並快取應用程式記憶體中傳回的金鑰物件。如果您稍後需要此金鑰物件，您應該從快取擷取物件，而不是查詢每個操作的此物件，這會增加大量的效能額外負荷。

使用多執行緒

AWS CloudHSM 支援多執行緒應用程式，但多執行緒應用程式需要謹記某些事項。

使用 PKCS #11，您應該只初始化 PKCS #11 程式庫（呼叫 `C_Initialize`）一次。每個執行緒都應指派自己的工作階段（`C_OpenSession`）。不建議在多個執行緒中使用相同的工作階段。

使用 JCE 時，AWS CloudHSM 供應商只能初始化一次。請勿跨執行緒共用 SPI 物件的執行個體。例如，`Cipher`、`Signature`、`Digest`、`Mac`、`KeyFactory` 或 `KeyGenerator` 物件應該只在自己的執行緒內容中使用。

處理調節錯誤

在下列情況下，您可能會遇到 HSM 調節錯誤：

- 您的叢集未正確擴展以管理尖峰流量。
- 在維護事件期間，您的叢集大小不會有 +1 備援。
- 可用區域中斷會導致叢集中可用 HSMs 的數量減少。

如需如何處理此案例的詳細資訊[HSM 調節](#)，請參閱。

為了確保您的叢集大小適當且不會受到調節，AWS 建議您使用預期的尖峰流量在環境中載入測試。

整合叢集操作的重試

AWS 可能會因為操作或維護原因而取代您的 HSM。為了讓您的應用程式適應這類情況，AWS 建議您在路由至叢集的所有操作上實作用戶端重試邏輯。因取代而失敗操作的後續重試預期會成功。

實作災難復原策略

為了回應事件，您可能需要將流量移離整個叢集或區域。下列各節說明執行此操作的多種策略。

使用 VPC 對等互連從另一個帳戶或區域存取叢集：您可以使用 VPC 對等互連從另一個帳戶或區域存取 AWS CloudHSM 叢集。如需如何設定的詳細資訊，請參閱 [《VPC 對等互連指南》中的什麼是 VPC 對等互連？](#)。建立對等連線並適當設定安全群組後，您可以像平常一樣與 HSM IP 地址通訊。

從相同的應用程式連線至多個叢集：用戶端 SDK 5 中的 JCE 提供者、PKCS #11 程式庫和 CloudHSM CLI 支援從相同的應用程式連線至多個叢集。例如，您可以有兩個作用中叢集，每個叢集位於不同區域，而您的應用程式可以一次連線到這兩個叢集，並在正常操作中同時連線到負載平衡。如果您的應用程式未使用用戶端 SDK 5（最新的 SDK），則您無法從相同的應用程式連線至多個叢集。或者，您可以保持另一個叢集正常運作，如果發生區域性中斷，請將流量轉移到另一個叢集，以將停機時間降至最低。如需詳細資訊，請參閱個別頁面：

- [適用於的 PKCS #11 程式庫的多個槽組態 AWS CloudHSM](#)
- [使用 JCE 供應商連線至多個 AWS CloudHSM 叢集](#)
- [使用 CloudHSM CLI 連線至多個叢集](#)

從備份還原叢集：您可以從現有叢集的備份建立新的叢集。如需詳細資訊，請參閱[中的叢集備份 AWS CloudHSM](#)。

AWS CloudHSM 監控最佳實務

本節說明您可以用來監控叢集和應用程式的多種機制。如需監控的其他詳細資訊，請參閱 [監控 AWS CloudHSM](#)。

監控用戶端日誌

每個用戶端 SDK 都會寫入您可以監控的日誌。如需用戶端記錄的資訊，請參閱 [使用 AWS CloudHSM 用戶端 SDK 日誌](#)。

在設計為暫時性的平台上，例如 Amazon ECS 和 AWS Lambda，從檔案收集用戶端日誌可能很困難。在這些情況下，最佳實務是設定用戶端 SDK 記錄以將日誌寫入主控台。大多數服務會自動收集此輸出，並將其發佈至 Amazon CloudWatch logs，供您保留和檢視。

如果您在 AWS CloudHSM 用戶端 SDK 之外使用任何第三方整合，您應該確保設定該軟體套件，將其輸出記錄到主控台。AWS CloudHSM 用戶端 SDK 的輸出可能由此套件擷取，否則會寫入自己的日誌檔案。

如需如何在應用程式中設定記錄選項的資訊，[AWS CloudHSM 用戶端 SDK 5 設定工具](#)請參閱。

監控稽核日誌

AWS CloudHSM 會將稽核日誌發佈到您的 Amazon CloudWatch 帳戶。稽核日誌來自 HSM，並追蹤特定操作以進行稽核。

您可以使用稽核日誌來追蹤 HSM 上叫用的任何管理命令。例如，您可以在發現執行非預期的管理操作時觸發警示。

如需詳細資訊，請參閱[HSM 稽核記錄的運作方式](#)。

監控 AWS CloudTrail

AWS CloudHSM 已與服務整合 AWS CloudTrail，此服務提供由使用者、角色或 in. AWS CloudTrail captures AWS 服務所採取動作的記錄 AWS CloudHSM。會將的所有 API 呼叫擷取 AWS CloudHSM 為事件。擷取的呼叫包括來自 AWS CloudHSM 主控台的呼叫，以及對 AWS CloudHSM API 操作的程式碼呼叫。

您可以使用 AWS CloudTrail 來稽核對 AWS CloudHSM 控制平面所做的任何 API 呼叫，以確保您的帳戶中不會發生不必要的活動。

如需詳細資訊，請參閱 [使用 AWS CloudTrail 和 AWS CloudHSM](#)。

監控 Amazon CloudWatch 指標

您可以使用 Amazon CloudWatch 指標來即時監控 AWS CloudHSM 叢集。指標可以依區域、叢集 ID 或 HSM ID 和叢集 ID 分組。

您可以使用 Amazon CloudWatch 指標來設定 Amazon CloudWatch 警示，以提醒您任何可能影響服務的潛在問題。我們建議您設定警示來監控下列項目：

- 在 HSM 上接近您的金鑰限制
- 接近 HSM 上的 HSM 工作階段計數限制
- 接近 HSM 上的 HSM 使用者計數限制
- HSM 使用者或金鑰計數的差異，以識別同步問題
- 運作狀態不佳HSMs 可向上擴展叢集，直到 AWS CloudHSM 可以解決問題為止

如需詳細資訊，請參閱[使用 Amazon CloudWatch Logs 和 AWS CloudHSM Audit Logs](#)。

中的叢集 AWS CloudHSM

叢集是 AWS CloudHSM 保持同步的個別硬體安全模組 (HSM) 集合。當您在叢集的一個 HSM 上執行任務或操作時，該叢集的其他 HSM 會自動保持在最新狀態。

您可以從 [AWS CloudHSM 主控台](#) 或其中一個 [AWS SDKs 或命令列工具](#) 管理您的 AWS CloudHSM 叢集。如需詳細資訊，請參閱下列主題。

若要建立叢集，請參閱[開始使用](#)。

下列主題提供有關叢集的詳細資訊。

主題

- [AWS CloudHSM 叢集架構](#)
- [AWS CloudHSM 叢集同步](#)
- [AWS CloudHSM 叢集高可用性和負載平衡](#)
- [AWS CloudHSM 叢集模式](#)
- [中的 HSM 類型 AWS CloudHSM](#)
- [將用戶端 SDK 連接至 AWS CloudHSM 叢集](#)
- [擴展 AWS CloudHSM 叢集中的 HSMs](#)
- [刪除 AWS CloudHSM 叢集](#)
- [從備份建立 AWS CloudHSM 叢集](#)
- [叢集 HSM 類型遷移](#)

AWS CloudHSM 叢集架構

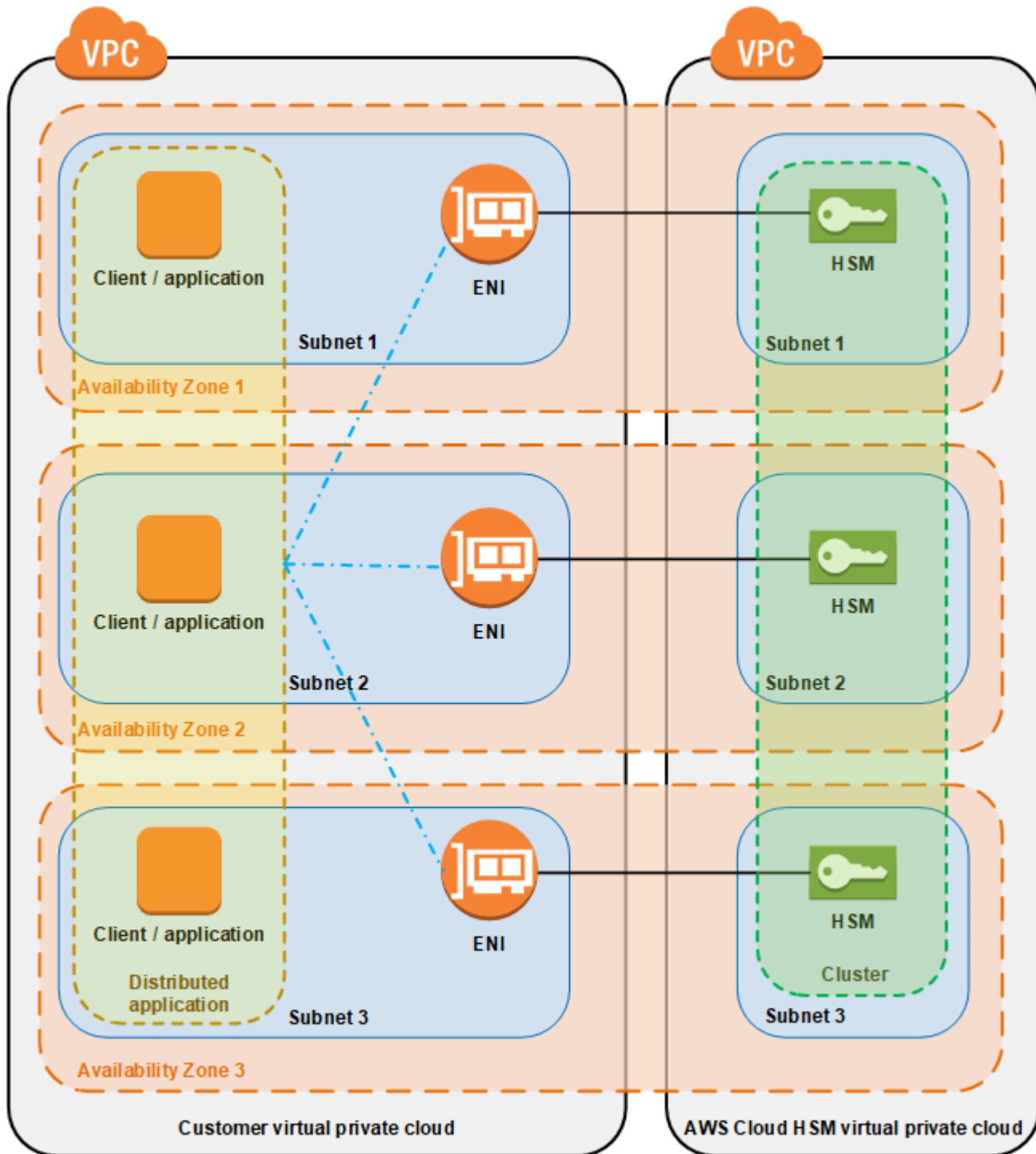
建立叢集時，您可以在 AWS 帳戶中指定 Amazon Virtual Private Cloud (VPC)，並在該 VPC 中指定一或多個子網路。建議您在所選 AWS 區域中的每個可用區域 (AZ) 中建立一個子網路。您可以在建立 VPC 時建立私有子網路。如需詳細資訊，請參閱 [建立的虛擬私有雲端 \(VPC\) AWS CloudHSM](#)。

每次建立 HSM 時，您都需要指定 HSM 的叢集和可用區域。只要將 HSM 放在不同的可用區域，萬一某個可用區域無法使用，就能發揮備援和高可用性。

當您建立 HSM 時，會在您 AWS 帳戶中的指定子網路中 AWS CloudHSM 輸入彈性網路界面 (ENI)。彈性網路界面是用來與 HSM 互動的界面。HSM 位於由擁有 AWS 的帳戶中的個別 VPC 中 AWS CloudHSM。HSM 及其對應的網路界面位於相同的可用區域。

若要與叢集中的 HSMs 互動，您需要 AWS CloudHSM 用戶端軟體。一般而言，您會將用戶端安裝在 Amazon EC2 執行個體 (稱為用戶端執行個體)，而這些執行個體與 HSM ENI 位於相同的 VPC，如下圖所示。在技術上不必如此；在任何相容的電腦上，只要可連接到 HSM ENI，都可以安裝用戶端。用戶端會透過 ENI 來與叢集的個別 HSM 通訊。

下圖代表具有三個 HSMs AWS CloudHSM 叢集，每個在 VPC 的不同可用區域中。



AWS CloudHSM 叢集同步

在 AWS CloudHSM 叢集中，會同步 AWS CloudHSM 保留個別 HSMs 上的金鑰。您不需要做任何動作來同步 HSM 上的金鑰。若要讓每個 HSM 上的使用者和政策保持同步，請在[管理 HSM 使用者](#)之前更新 AWS CloudHSM 用戶端組態檔案。如需詳細資訊，請參閱[讓 HSM 使用者保持同步](#)。

當您將新的 HSM 新增至叢集時，AWS CloudHSM 會備份現有 HSM 上的所有金鑰、使用者和政策。然後將該備份還原到新的 HSM。這樣就可讓兩個 HSM 保持同步。

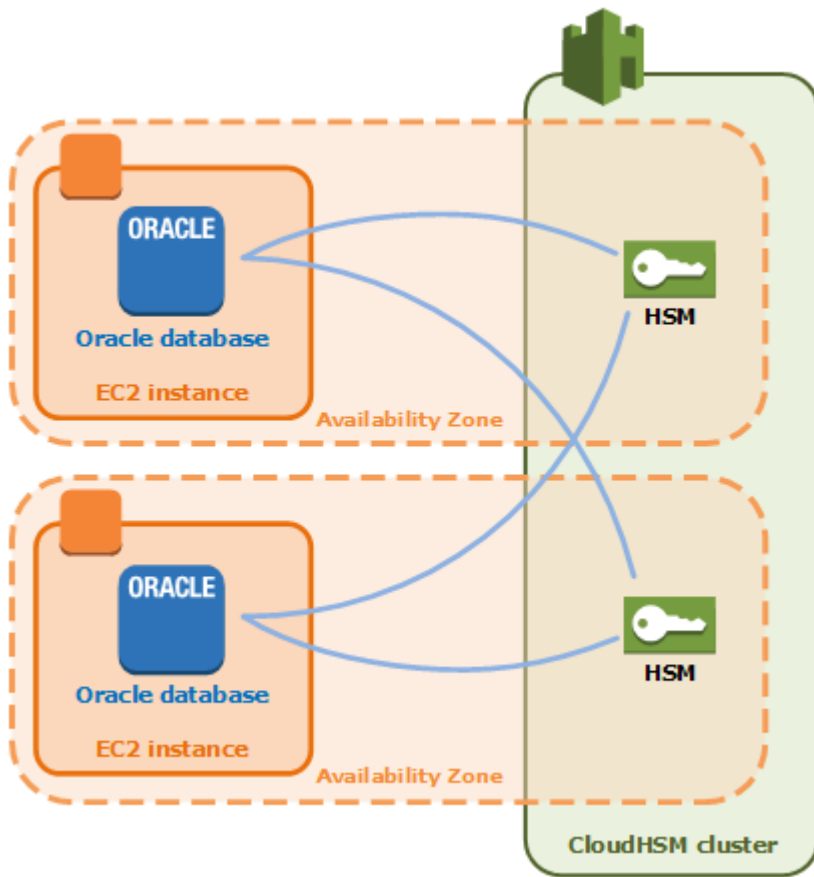
如果叢集中的 HSMs 不同步，AWS CloudHSM 會自動重新同步它們。若要啟用此功能，AWS CloudHSM 會使用[設備使用者](#)的登入資料。此使用者存在於提供的所有 HSMs 上 AWS CloudHSM，並且具有有限的許可。這個使用者可以取得 HSM 上的物件雜湊，並可以擷取和插入遮罩 (加密) 物件。AWS 無法檢視或修改您的使用者或金鑰，也無法使用這些金鑰執行任何加密操作。

AWS CloudHSM 叢集高可用性和負載平衡

當您建立具有多個 HSM 的 AWS CloudHSM 叢集時，會自動取得負載平衡。負載平衡表示 [AWS CloudHSM 用戶端](#) 會根據每個 HSM 的額外處理能力，將密碼編譯操作分散給叢集中的所有 HSM 用戶端。

當您在不同 AWS 可用區域中建立 HSMs 時，會自動取得高可用性。高可用性表示您可以獲得更高的可靠性，因為沒有任何一個 HSM 會發生單點失效。我們建議您在每個叢集中至少有兩個 HSMs，其中每個 HSM 位於 AWS 區域內的不同可用區域。

例如，下圖顯示 Oracle 資料庫應用程式分佈至兩個不同的可用區域。資料庫執行個體會將主金鑰存放在叢集中，該叢集在每個可用區域中包含 HSM。AWS CloudHSM 會自動將金鑰同步到兩個 HSMs，以便立即存取和備援。



AWS CloudHSM 叢集模式

AWS CloudHSM 以兩種模式提供叢集：FIPS 和非 FIPS。在 FIPS 模式中，只能使用經聯邦資訊處理標準 (FIPS) 驗證的金鑰和演算法。非 FIPS 模式提供支援的所有金鑰和演算法 AWS CloudHSM，無論 FIPS 核准為何。

在決定哪個叢集模式和 HSM 類型適合您的需求之前，請檢閱此頁面的詳細資訊。

Note

2024 年 6 月 10 日之前建立的所有叢集都處於 FIPS 模式，並具有 HSM 類型 hsm1.medium。

若要查看叢集的模式和 HSM 類型，請使用 [describe-clusters](#) 命令。

下表列出每個叢集模式之間的主要差異：

區分功能	FIPS 模式	非 FIPS 模式
HSM 類型相容性	適用於 hsm1.medium 和 hsm2m.medium。	hsm2m.medium 提供。
備份相容性	只能用於在 FIPS 模式下備份還原叢集。	只能用於在非 FIPS 模式下備份還原叢集。
金鑰選擇	支援產生和使用具有 FIPS 核准機制的金鑰 ¹ 。	除了其他未驗證的機制之外，還支援產生和使用具有所有 FIPS 驗證機制的金鑰。
演算法	支援 FIPS 核准的 AWS CloudHSM 演算法 ¹ 。	支援 FIPS 核准和未核准 FIPS 的 AWS CloudHSM 演算法。

【1】如需詳細資訊，請參閱[棄用通知](#)。

在選擇叢集模式之前，請注意，叢集的模式 (FIPS 或非 FIPS) 無法在建立之後變更，因此請務必選擇符合您需求的正確模式。

中的 HSM 類型 AWS CloudHSM

AWS CloudHSM 也提供兩種硬體安全模組 (HSM) 類型：hsm1.medium 和 hsm2m.medium。請先檢閱此頁面的詳細資訊，再決定哪種 HSM 類型適合您的需求。

除了叢集模式之外，AWS CloudHSM 還提供兩種 HSM 類型：hsm1.medium 和 hsm2m.medium。每個 HSM 類型都使用不同的硬體，而且每個叢集只能包含一種 HSM 類型。下表列出兩者之間的主要差異：

區分功能	hsm1.medium	hsm2m.medium
叢集模式相容性	適用於 FIPS 模式的叢集。	適用於 FIPS 或非 FIPS 模式的叢集。
網路類型相容性	無	適用於 FIPS 或非 FIPS 模式的叢集。

區分功能	hsm1.medium	hsm2m.medium
備份相容性	可用於在 FIPS 模式下備份和還原至 hsm1.medium 和 hsm2m.medium 叢集。	只能用於備份和還原 hsm2m.medium 叢集。
金鑰容量	每個叢集 3,300 個。	總共 16,666 個金鑰，每個叢集具有最多 3,333 個非對稱金鑰。
用戶端 SDKs	支援所有用戶端 SDKs。	支援所有用戶端 SDKs。
用戶端 SDK 版本	與 SDK 3.1.0 版及更新版本相容。	與用戶端 SDK 5.9.0 版及更新版本相容。
區域可用性	CloudHSM 不再支援在任何區域中建立新的叢集 AWS。如需詳細資訊，請參閱 棄用通知 以取得詳細資訊。	AWS 區域 可在該 CloudHSM 中使用 。
效能	若要查看每個 HSM 類型的效能，請參閱 AWS CloudHSM 效能資訊 。	
認證	FIPS 140-2、PCI DSS、PCI PIN、SOC2 和 PCI-3DS 相容。	FIPS 140-3、PCI DSS、PCI PIN 和 SOC2 相容。

將用戶端 SDK 連接至 AWS CloudHSM 叢集

如要使用用戶端 SDK 5 或用戶端 SDK 3 連接至叢集，您必須先執行兩項操作：

- 在 EC2 執行個體上擁有發行憑證
- 將用戶端 SDK 引導至叢集

在每個 EC2 執行個體上安裝發行憑證

您可以在初始化叢集時建立發行憑證。將發行憑證複製到連接至叢集每個 EC2 執行個體平台的預設位置。

Linux

```
/opt/cloudhsm/etc/customerCA.crt
```

Windows

```
C:\ProgramData\Amazon\CloudHSM\customerCA.crt
```

指定憑證的位置。

如果是用戶端 SDK 5，您可使用設定工具指定簽發憑證的位置。

PKCS #11 library

將用戶端 SDK 5 的簽發憑證安裝於 Linux 上

- 使用設定工具指定簽發憑證的位置。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --hsm-ca-cert <customerCA certificate file>
```

將用戶端 SDK 5 的簽發憑證安裝於 Windows 上

- 使用設定工具指定簽發憑證的位置。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" --hsm-ca-cert <customerCA certificate file>
```

OpenSSL Dynamic Engine

將用戶端 SDK 5 的簽發憑證安裝於 Linux 上

- 使用設定工具指定簽發憑證的位置。

```
$ sudo /opt/cloudhsm/bin/configure-dyn --hsm-ca-cert <customerCA certificate file>
```

Key Storage Provider (KSP)

將用戶端 SDK 5 的簽發憑證安裝於 Windows 上

- 使用設定工具指定簽發憑證的位置。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --hsm-ca-cert <customerCA certificate file>
```

JCE provider

將用戶端 SDK 5 的簽發憑證安裝於 Linux 上

- 使用設定工具指定簽發憑證的位置。

```
$ sudo /opt/cloudhsm/bin/configure-jce --hsm-ca-cert <customerCA certificate file>
```

將用戶端 SDK 5 的簽發憑證安裝於 Windows 上

- 使用設定工具指定簽發憑證的位置。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" --hsm-ca-cert <customerCA certificate file>
```

CloudHSM CLI

將用戶端 SDK 5 的簽發憑證安裝於 Linux 上

- 使用設定工具指定簽發憑證的位置。

```
$ sudo /opt/cloudhsm/bin/configure-cli --hsm-ca-cert <customerCA certificate file>
```

將用戶端 SDK 5 的簽發憑證安裝於 Windows 上

- 使用設定工具指定簽發憑證的位置。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" --hsm-ca-  
cert <customerCA certificate file>
```

如需詳細資訊，請參閱[設定工具](#)。

如需有關初始化叢集或建立和簽署憑證的詳細資訊，請參閱[初始化叢集](#)。

引導用戶端 SDK

用戶端 SDK 版本不同，啟動程序也不一樣，但您必須擁有叢集中其中一個硬體安全性模組 (HSM) 的 IP 地址。您可以使用任何連接至叢集的 HSM 的 IP 地址。用戶端 SDK 連接之後，會擷取其他任何 HSM 的 IP 地址，並執行負載平衡和用戶端金鑰同步處理操作。

取得叢集的 IP 地址

取得 HSM 的 IP 地址 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 若要開啟叢集詳細資訊頁面，請在叢集表格中選擇叢集 ID。
4. 若要取得 IP 地址，請前往 HSMs 索引標籤。對於 IPv4 叢集，請選擇 ENI IPv4 地址下列出的地址。對於雙堆疊叢集，請使用 ENI IPv4 或 ENI IPv6 地址。

取得 HSM 的 IP 地址 (AWS CLI)

- 使用 AWS CLI 中的 [describe-clusters](#) 命令取得 HSM 的 IP 地址。在 命令的輸出中，HSMs 的 IP 地址是 `EniIp` 和 的值 `EniIPv6` (如果是雙堆疊叢集) 。

```
$ aws cloudhsmv2 describe-clusters  
{  
  "Clusters": [  
    { ... }  
    "Hsms": [  
      {  
        ...
```



```
        "EniIp": "10.0.0.9",
    ...
    },
    {
    ...
        "EniIp": "10.0.1.6",
        "EniIpV6": "2600:113f:404:be09:310e:ed34:3412:f733",
    ...
    }
```

如需有關啟動程序的詳細資訊，請參閱[設定工具](#)。

如要啟用用戶端 SDK 5

PKCS #11 library

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 -a <HSM IP addresses>
```

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" -a <HSM IP  
addresses>
```

OpenSSL Dynamic Engine

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-dyn -a <HSM IP addresses>
```

Key Storage Provider (KSP)

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" -a <HSM IP addresses>
```

JCE provider

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-jce -a <HSM IP addresses>
```

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" -a <HSM IP addresses>
```

CloudHSM CLI

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用設定工具指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-cli -a <The ENI IPv4 / IPv6 addresses of the HSMs>
```

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用設定工具指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" -a <The ENI  
IPv4 / IPv6 addresses of the HSMs>
```

Note

您可以使用 `--cluster-id` 參數來代替 `-a <HSM_IP_ADDRESSES>`。若要查看使用 `--cluster-id` 的需求，請參閱 [AWS CloudHSM 用戶端 SDK 5 設定工具](#)。

如要啟用用戶端 SDK 3

為用戶端 SDK 3 引導 Linux EC2 執行個體

- 使用 `configure` 指定叢集中 HSM 的 IP 地址。

```
sudo /opt/cloudhsm/bin/configure -a <IP address>
```

為用戶端 SDK 3 引導 Windows EC2 執行個體

- 使用 `configure` 指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" -a <HSM IP address>
```

如需設定的詳細資訊，請參閱 [???](#)。

擴展 AWS CloudHSM 叢集中的 HSMs

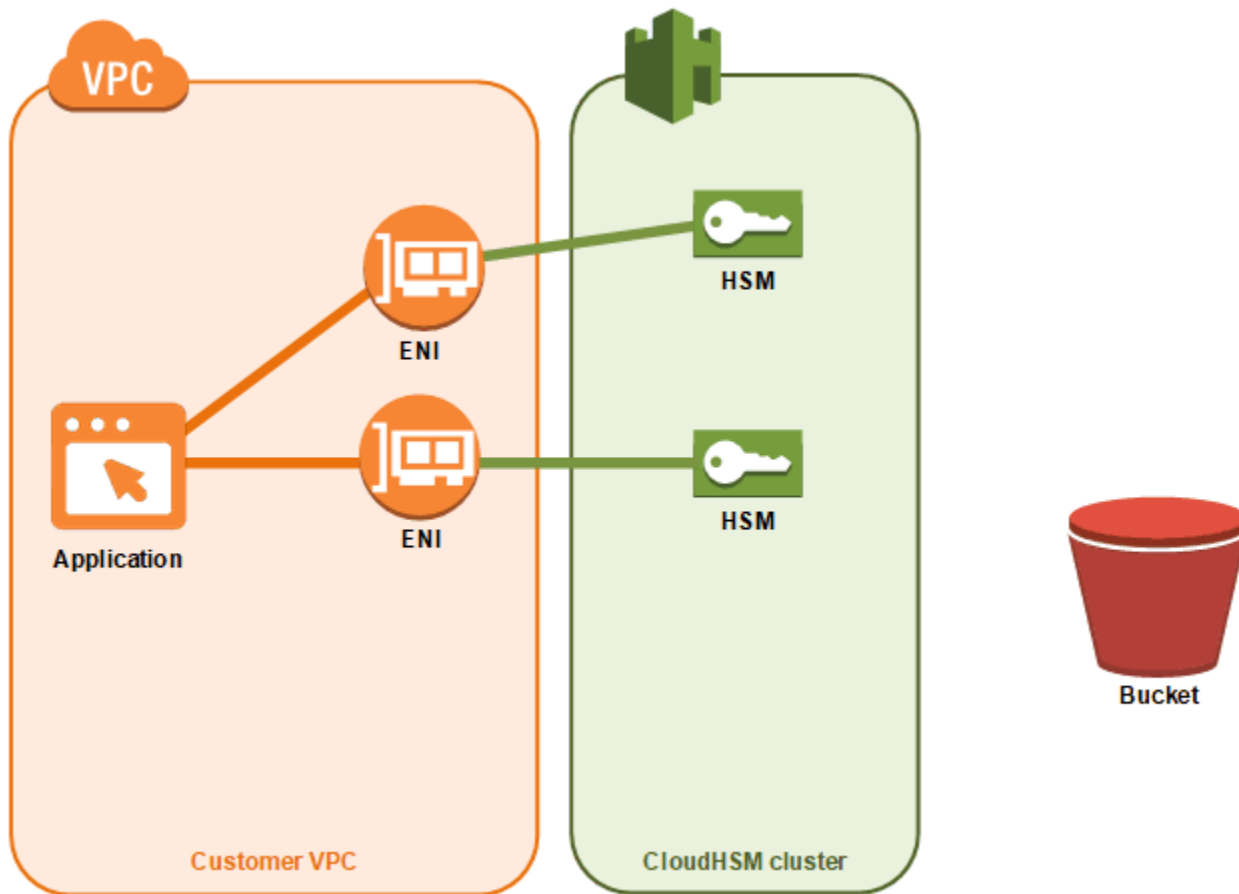
若要擴展或縮減 AWS CloudHSM 叢集，請使用 [AWS CloudHSM 主控台](#) 或其中一個 [AWS SDKs 或命令列工具](#) 來新增或移除 HSMs。我們建議您測試叢集的負載，以確定您應預期的尖峰負載，然後在叢集中再新增一個 HSM 以確保高可用性。

主題

- [將 HSM 新增至 AWS CloudHSM 叢集](#)
- [從 AWS CloudHSM 叢集移除 HSM](#)

將 HSM 新增至 AWS CloudHSM 叢集

下圖說明將 HSM 新增到叢集時發生的事件。



1. 您將新的 HSM 新增到叢集。下列程序說明如何從 [AWS CloudHSM 主控台](#)、[AWS Command Line Interface \(AWS CLI\)](#) 和 [AWS CloudHSM API](#) 執行此作業。

您只需要執行這個動作。剩餘的事件會自動發生。

2. AWS CloudHSM 會建立叢集中現有 HSM 的備份複本。如需詳細資訊，請參閱[備份](#)。
3. AWS CloudHSM 會將備份還原到新的 HSM。這可確保此 HSM 與叢集的其他 HSM 同步。
4. 叢集中的現有 HSMs 會通知 AWS CloudHSM 用戶端叢集中有新的 HSM。
5. 用戶端會對新的 HSM 建立連線。

新增 HSM (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 針對您要新增的 HSM 選擇叢集。

3. 在 HSM 標籤上，選擇 Create HSM (建立 HSM)。
4. 針對您要建立的 HSM 選擇可用區域 (AZ)。然後選擇 Create (建立)。

新增 HSM (AWS CLI)

- 在命令提示字元中，發出 [create-hsm](#) 命令，並指定您要建立之 HSM 的叢集 ID 和可用區域。如果您不知道慣用叢集的叢集 ID，請發出 [describe-clusters](#) 命令。指定可用區域，格式為 us-east-2a、us-east-2b 等。

```
$ aws cloudhsmv2 create-hsm --cluster-id <cluster ID> --availability-  
zone <Availability Zone>  
{  
  "Hsm": {  
    "State": "CREATE_IN_PROGRESS",  
    "ClusterId": "cluster-5a73d5qzrdh",  
    "HsmId": "hsm-lgavqitns2a",  
    "SubnetId": "subnet-0e358c43",  
    "AvailabilityZone": "us-east-2c",  
    "EniId": "eni-bab18892",  
    "EniIp": "10.0.3.10",  
    "EniIPv6": "2600:113f:404:be09:310e:ed34:3412:f733"  
  }  
}
```

新增 HSM (AWS CloudHSM API)

- 傳送 [CreateHsm](#) 請求，並指定您要建立之 HSM 的叢集 ID 和可用區域。

從 AWS CloudHSM 叢集移除 HSM

您可以使用 [AWS CloudHSM 主控台](#)、[AWS CLI](#) 或 AWS CloudHSM API 來移除 HSM。

移除 HSM (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 選擇叢集，其中包含您要移除的 HSM。
3. 在 HSM 標籤中，選擇您要移除的 HSM。然後選擇 Delete HSM (刪除 HSM)。
4. 確認您要刪除 HSM。然後選擇 Delete (刪除)。

移除 HSM (AWS CLI)

- 在命令提示字元中，發出 [delete-hsm](#) 命令。傳遞叢集 (包含您要刪除的 HSM) 的 ID 和以下其中一個 HSM 識別符：
 - HSM ID (`--hsm-id`)
 - HSM IP 地址 (`--eni-ip`)
 - HSM 的彈性網路界面 ID (`--eni-id`)

如果您不知道這些識別符的值，請發出 [describe-clusters](#) 命令。

```
$ aws cloudhsmv2 delete-hsm --cluster-id <cluster ID> --eni-ip <HSM IP address>
{
  "HsmId": "hsm-lgavqitns2a"
}
```

移除 HSM (AWS CloudHSM API)

- 傳送 [DeleteHsm](#) 請求，並指定您要刪除之 HSM 的叢集 ID 和識別符。

刪除 AWS CloudHSM 叢集

您必須先移除叢集中的所有 HSM 後，才能刪除叢集。如需詳細資訊，請參閱[從 AWS CloudHSM 叢集移除 HSM](#)。

移除所有 HSMs 之後，您可以使用 [AWS CloudHSM 主控台](#)、[AWS Command Line Interface \(AWS CLI\)](#) 或 AWS CloudHSM API 刪除叢集。

刪除叢集 (主控台)

- 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
- 選擇您要刪除的叢集。然後選擇刪除叢集。
- 確認您要刪除叢集，然後選擇刪除。

刪除叢集 (AWS CLI)

- 在命令提示字元中，發出 [delete-cluster](#) 命令，並傳遞您要刪除的叢集 ID。如果您不知道叢集 ID，請發出 [describe-clusters](#) 命令。

```
$ aws cloudhsmv2 delete-cluster --cluster-id <cluster ID>
{
  "Cluster": {
    "Certificates": {
      "ClusterCertificate": "<certificate string>"
    },
    "SourceBackupId": "backup-rtq2dwi2gq6",
    "SecurityGroup": "sg-40399d28",
    "CreateTimestamp": 1504903546.035,
    "SubnetMapping": {
      "us-east-2a": "subnet-f1d6e798",
      "us-east-2c": "subnet-0e358c43",
      "us-east-2b": "subnet-40ed9d3b"
    },
    "ClusterId": "cluster-kdmrayrc7gi",
    "VpcId": "vpc-641d3c0d",
    "State": "DELETE_IN_PROGRESS",
    "HsmType": "hsm1.medium",
    "StateMessage": "The cluster is being deleted.",
    "Hsms": [],
    "BackupPolicy": "DEFAULT"
  }
}
```

刪除AWS CloudHSM 叢集 (API)

- 傳送 [DeleteCluster](#) 請求，指定您要刪除的叢集 ID。

從備份建立 AWS CloudHSM 叢集

若要從備份還原 AWS CloudHSM 叢集，請遵循本主題中的步驟。您的叢集會包含備份中的相同使用者、金鑰資料、憑證、組態和政策。如需管理備份的詳細資訊，請參閱 [叢集備份](#)。

從備份建立叢集 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 選擇建立叢集。
3. 在叢集組態區段中，執行下列操作：
 - a. 對於 VPC，選擇您要建立叢集的 VPC。
 - b. 對於 AZ，為您要新增至叢集的每個可用區域選擇私有子網路。
 - c. 針對網路類型，選擇 HSMs 用於連線的 IP 通訊協定。
4. 在叢集來源區段中，執行下列操作：
 - a. 選擇從當前備份還原。
 - b. 選擇您要還原的備份。
5. 選擇下一步：檢閱。
6. 檢閱您的叢集組態，然後選擇建立叢集。
7. 指定服務應保留備份的時間長度。

接受預設保留期 90 天，或輸入介於 7 到 379 天之間的新值。服務會自動刪除此叢集中超過您在此指定值的備份。您之後可以變更這個設定。如需詳細資訊，請參閱[設定備份保留](#)。

8. 選擇下一步。
9. (選用) 輸入標籤索引鍵和選用標籤值。若要將多個標籤新增至叢集，請選擇新增標籤。
10. 選擇檢閱。
11. 檢閱您的叢集組態，然後選擇建立叢集。

Tip

若要在叢集中建立 HSM，其中包含與您還原之備份中相同的使用者、金鑰材料、憑證、組態和政策，請將 [HSM](#) 新增至叢集。

從備份建立叢集 (AWS CLI)

若要確定備份 ID，請執行 [describe-backups](#) 命令。

- 在命令提示字元中，發出 [create-cluster](#) 命令。指定 HSM 執行個體類型、您計劃在其中建立 HSM 子網路的子網路 ID，以及您要還原之備份的備份 ID。

```
$ aws cloudhsmv2 create-cluster --hsm-type hsm2m.medium \
                                --subnet-ids <subnet ID 1> <subnet ID 2> <subnet ID
N> \
                                --source-backup-id <backup ID>
                                --mode <FIPS> \
                                --network-type <IPV4>

{
  "Cluster": {
    "HsmType": "hsm2m.medium",
    "VpcId": "vpc-641d3c0d",
    "Hsms": [],
    "State": "CREATE_IN_PROGRESS",
    "SourceBackupId": "backup-rtq2dwi2gq6",
    "BackupPolicy": "DEFAULT",
    "BackupRetentionPolicy": {
      "Type": "DAYS",
      "Value": 90
    },
    "NetworkType": "IPV4",
    "SecurityGroup": "sg-640fab0c",
    "CreateTimestamp": 1504907311.112,
    "SubnetMapping": {
      "us-east-2c": "subnet-0e358c43",
      "us-east-2a": "subnet-f1d6e798",
      "us-east-2b": "subnet-40ed9d3b"
    },
    "Certificates": {
      "ClusterCertificate": "<certificate string>"
    },
    "ClusterId": "cluster-jxhlf7644ne"
  }
}
```

從備份建立叢集 (AWS CloudHSM API)

請參閱下列主題，了解如何使用 API 從備份創建叢集。

- [CreateCluster](#)

叢集 HSM 類型遷移

AWS CloudHSM 提供變更現有叢集 HSM 類型的功能。檢閱此頁面上的資料表，判斷是否允許修改 HSM 類型。

如需支援的 HSMs 類型及其功能的詳細資訊，請參閱 [中的 HSM 類型 AWS CloudHSM](#)。

Note

您無法在此操作期間變更叢集的 FIPS 模式。

從	到	註解
hsm1.medium	hsm2m.medium	允許
hsm2m.medium	hsm1.medium	條件式。您可以在遷移開始後 24 小時內，從 hsm2m.medium 復原至 hsm1.medium。

主題

- [從 hsm1.medium 遷移至 hsm2m.medium](#)

從 hsm1.medium 遷移至 hsm2m.medium

您可以將 AWS CloudHSM 叢集從 hsm1.medium 遷移至 hsm2m.medium。本主題說明先決條件、遷移程序和轉返程序。

開始遷移之前，請確定您的應用程式遵循 [中的建議架構您的叢集以獲得高可用性](#)。這有助於避免程序期間的停機時間。

hsm1.medium 到 hsm2m.medium 遷移程序概觀

您可以使用 AWS CloudHSM 主控台、AWS CLI 或 AWS CloudHSM API 開始遷移。無論您在何處啟動，AWS CloudHSM 叢集遷移都會使用 `modify-cluster` API 端點。一旦遷移開始，您的整個叢集就會進入有限寫入模式。如需詳細資訊，請參閱 [叢集有限寫入模式](#)。

為了將影響降至最低，會將 HSMs 從 hsm1.medium AWS CloudHSM 變更為 hsm2m.medium，一次一個。替換 HSMs 會維護相同的 IP 地址，因此在遷移期間或之後不需要變更組態。

以下是遷移的運作方式：

1. 在遷移第一個 HSM 之前，AWS CloudHSM 會建立整個叢集的完整備份。
2. 使用此備份，AWS CloudHSM 會建立請求類型 (hsm2m.medium) 的新 HSM，以取代第一個 HSM。
3. 在遷移每個後續 HSM 之前，會 AWS CloudHSM 建立整個叢集的新完整備份。
4. AWS CloudHSM 針對叢集中的每個 HSM 重複步驟 3 和 4，一次遷移一個 HSM。
5. 每個個別 HSM 遷移大約需要 30 分鐘。

AWS CloudHSM 會監控叢集運作狀態，並在整個遷移過程中執行驗證。如果 AWS CloudHSM 偵測到錯誤增加或驗證檢查失敗，它會自動停止遷移，並將叢集還原為其原始 HSM 類型。您也可以在開始遷移後最多 24 小時內手動復原。在復原之前，請參閱 [HSM 類型復原考量](#)。

遷移至 hsm2m.medium 的先決條件

您現有的 AWS CloudHSM 叢集必須符合這些需求，才能遷移至 hsm2m.medium。如果在驗證檢查期間不符合任何條件，AWS CloudHSM 會自動將叢集還原為其原始 HSM 類型。

如需已知遷移問題的清單，請參閱 [???](#)

- 在過去 7 天內：
 - 所有用戶端連線都已使用 SDK 5.9 或更新版本。
 - 如果執行 ECDSA 驗證，所有用戶端連線都已使用 SDK 5.13 或更新版本。
 - AWS CloudHSM 執行個體只使用支援（且沒有已棄用）的功能。如需詳細資訊，請參閱[棄用通知](#)。
 - 您必須在過去 7 天內使用 SDK 與叢集中至少一個 HSM 連線。
- 叢集處於 ACTIVE 狀態。
- 叢集有 27 HSMs 或更少。
- HSM 操作的錯誤率在遷移期間不會增加。

 Note

先前防止具有字符金鑰工作負載的客戶遷移的限制已移除。

叢集有限寫入模式

當您開始叢集遷移時，它會進入有限寫入模式。可變更 HSM 狀態的操作會遭到拒絕。所有讀取操作都不會受到影響。

在遷移期間，您的應用程式在嘗試這些操作時收到來自 HSM 的錯誤：

- 產生和刪除字符金鑰（工作階段金鑰工作負載會繼續運作）。
- 所有使用者建立、刪除或修改。
- 配額操作。
- HSM 內金鑰的修改，例如變更金鑰屬性。
- mTLS 註冊。

AWS CloudHSM 也會在遷移期間將您的叢集置於 MODIFY_IN_PROGRESS 狀態。在此期間，您無法從叢集新增或移除 HSMs。

開始遷移

叢集遷移程序會逐一取代叢集中的個別 HSMs。持續時間取決於叢集中的 HSMs 數目。每個 HSM 平均需要約 30 分鐘。您可以透過監控叢集中個別 HSM HSMs 已遷移至新類型。

Console

變更 HSM 類型（主控台）

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 選取您要變更之叢集 ID 旁的選項按鈕
3. 從動作功能表中，選擇 Modify HSM Type 並選取所需的 HSM 類型

此程序會讓您的叢集進入 MODIFY_IN_PROGRESS 狀態。遷移後，您的叢集會返回 ACTIVE 狀態。

AWS CLI

變更 HSM 類型 ([AWS CLI](#))

- 在命令提示中，執行 [modify-cluster](#) 命令。指定叢集 ID 和所需的 HSM 類型。

```
$ aws cloudhsmv2 modify-cluster --cluster-id <cluster ID> --hsm-type <HSM Type>

{
  "Cluster": {
    "BackupPolicy": "DEFAULT",
    "BackupRetentionPolicy": {
      "Type": "DAYS",
      "Value": 90
    },
    "VpcId": "vpc-50ae0636",
    "SubnetMapping": {
      "us-west-2b": "subnet-49a1bc00",
      "us-west-2c": "subnet-6f950334",
      "us-west-2a": "subnet-fd54af9b"
    },
    "SecurityGroup": "sg-6cb2c216",
    "HsmType": "hsm2m.medium",
    "HsmTypeRollbackExpiration": 1730383180.000,
    "Certificates": {},
    "State": "MODIFY_IN_PROGRESS",
    "Hsms": [],
    "ClusterId": "cluster-igklspoyj5v",
    "ClusterMode": "FIPS",
    "CreateTimestamp": 1502423370.069
  }
}
```

此程序會讓您的叢集進入 MODIFY_IN_PROGRESS 狀態。遷移後，您的叢集會返回 ACTIVE 狀態。

AWS CloudHSM API

變更 HSM 類型 (AWS CloudHSM API)

- 傳送 [ModifyCluster](#) 要求。指定叢集 ID 和叢集所需的 HSM 類型。

此程序會讓您的叢集進入 MODIFY_IN_PROGRESS 狀態。遷移後，您的叢集會返回 ACTIVE 狀態。

復原遷移

AWS CloudHSM 會監控提高的錯誤率，並在整個遷移過程中執行持續驗證檢查。如果 AWS CloudHSM 偵測到服務品質降低或任何驗證失敗，它會自動啟動復原至叢集的原始 HSM 類型。在復原期間，針對叢集中的每個 HSM：

- AWS CloudHSM 使用在該 HSM 遷移開始時取得的備份。
- 它會一次取代一個 HSM，直到所有 HSMs 都傳回原始類型為止。
- 在整個過程中，您的叢集會保持有限寫入模式。

您可以在啟動遷移的 24 小時內復原遷移。若要檢查轉返截止日期：

- 執行 [describe-clusters](#) 命令。
- 尋找 HsmTypeRollbackExpiration 值。此時間戳記是您的轉返截止日期。

如果您決定轉返，請在此截止日期之前完成。復原會使用原始 HSM 類型的最新備份。

Warning

遷移完成後，請謹慎轉返。如果您完成遷移，然後使用 AWS CloudHSM 建立新的金鑰或使用者，轉返可能會導致資料遺失。請參閱[在復原後同步資料](#)，了解如何在復原後緩解資料遺失。

Console

復原 HSM 類型 (主控台)

- 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。

2. 選取您要復原的叢集 ID。
3. 從動作功能表中，選擇Modify HSM Type並選取原始 HSM 類型

此程序會讓您的叢集進入 ROLLBACK_IN_PROGRESS 狀態。復原後，您的叢集會返回 ACTIVE 狀態。

AWS CLI

若要轉返 HSM 類型 ([AWS CLI](#))

- 在命令提示中，執行 [modify-cluster](#) 命令。指定叢集 ID 和原始 HSM 類型。

```
$ aws cloudhsmv2 modify-cluster --cluster-id <cluster ID> --hsm-type <HSM Type>

{
  "Cluster": {
    "BackupPolicy": "DEFAULT",
    "BackupRetentionPolicy": {
      "Type": "DAYS",
      "Value": 90
    },
    "VpcId": "vpc-50ae0636",
    "SubnetMapping": {
      "us-west-2b": "subnet-49a1bc00",
      "us-west-2c": "subnet-6f950334",
      "us-west-2a": "subnet-fd54af9b"
    },
    "SecurityGroup": "sg-6cb2c216",
    "HsmType": "hsm1.medium",
    "HsmTypeRollbackExpiration": 1730383180.000,
    "Certificates": {},
    "State": "ROLLBACK_IN_PROGRESS",
    "Hsms": [],
    "ClusterId": "cluster-igklspoyj5v",
    "ClusterMode": "FIPS",
    "CreateTimestamp": 1502423370.069
  }
}
```

此程序會讓您的叢集進入 ROLLBACK_IN_PROGRESS 狀態。復原後，您的叢集會返回 ACTIVE 狀態。

AWS CloudHSM API

復原 HSM 類型 (AWS CloudHSM API)

- 傳送 [ModifyCluster](#) 要求。指定叢集 ID 和叢集的原始 HSM 類型。

此程序會讓您的叢集進入 ROLLBACK_IN_PROGRESS 狀態。復原後，您的叢集會返回 ACTIVE 狀態。

在復原後同步資料

在遷移期間，HSMs處於有限寫入模式，防止 HSM 狀態變更。如果您在這段時間內轉返（當叢集為時MODIFY_IN_PROGRESS），會產生與原始叢集內容相同的叢集。

叢集返回 ACTIVE 狀態後，就會解除有限寫入模式。如果您在處於 ACTIVE 狀態時建立金鑰或使用者，然後轉返，則該金鑰或使用者將不會出現在您的轉返叢集中。

若要解決此問題，請使用 CloudHSM CLI 的[金鑰複寫](#)命令，在兩個叢集之間複寫金鑰。如果您尚未安裝，請參閱 [中的指示](#)。

在復原後同步金鑰

完成轉返後，請遵循下列步驟。我們會使用下列術語：

- "cluster-1"：您的復原叢集（現在為 hsm1.medium）
- "cluster-2"：您將建立的新暫時 hsm2m.medium 叢集

1. 使用來自 cluster-1 的最新 hsm2m.medium 備份建立新的 hsm2m.medium 叢集 (cluster-2)：

```
aws cloudhsmv2 create-cluster --hsm-type hsm2m.medium \
                                --subnet-ids <subnet ID 1> <subnet ID 2> <subnet ID
N> \
                                --source-backup-id <backup ID>
                                --mode <FIPS>
```

2. 在 cluster-2 中建立 HSM：


```
aws cloudhsmv2 create-hsm --cluster-id <cluster-2 ID>
```

3. 列出 cluster-2 中需要複寫的金鑰：

```
cloudhsm-cli key list --cluster-id <cluster-2 ID>
```

4. 將每個金鑰從 cluster-2 複寫到 cluster-1：

```
cloudhsm-cli key replicate --source-cluster-id <cluster-2 ID> \  
                           --destination-cluster-id <cluster-1 ID> \  
                           --filter attr.label=<key ID>
```

5. 針對需要複製的每個金鑰重複步驟 4。
6. 刪除 cluster-2 中的 HSM：

```
aws cloudhsmv2 delete-hsm --cluster-id <cluster-2 ID> --hsm-id <HSM ID>
```

7. 刪除 cluster-2：

```
aws cloudhsmv2 delete-cluster --cluster-id <cluster-2 ID>
```

中的 HSM 使用者 AWS CloudHSM

您必須先在 AWS CloudHSM 叢集中的硬體安全模組 (HSM) 上建立使用者和[金鑰](#)，才能使用叢集進行加密處理。

Note

HSM 使用者與 IAM 使用者不同。擁有正確憑證的 IAM 使用者可利用 AWS API 與資源進行互動來建立 HSM。HSM 建立後，您必須使用 HSM 使用者憑證來驗證 HSM 上的操作。

在 中 AWS CloudHSM，您必須使用 [CloudHSM CLI](#) 或 [CloudHSM Management Utility \(CMU\)](#) 命令列工具來建立和管理 HSM 上的使用者。CloudHSM CLI 可與[最新的 SDK 版本系列](#)搭配使用，而 CMU 則可與[先前的 SDK 版本系列](#)搭配使用。

如需在 中管理 HSM 使用者的詳細資訊，請參閱下列主題 AWS CloudHSM。您也可以了解如何使用規定人數身分驗證 (也稱為 M of N 存取控制)。

主題

- [使用 CloudHSM CLI 進行 HSM 使用者管理](#)
- [使用 CloudHSM 管理公用程式 \(CMU\) 進行 HSM 使用者管理](#)

使用 CloudHSM CLI 進行 HSM 使用者管理

若要在 中管理硬體安全模組 (HSM) 使用者 AWS CloudHSM，您必須使用[管理員](#)的使用者名稱和密碼登入 HSM。只有管理員可以管理使用者。HSM 包含名為 admin 的預設管理員。您可以在[啟用叢集](#)時設定 admin 管理員的密碼。

本主題提供使用 CloudHSM CLI 管理 HSM 使用者的step-by-step說明和詳細資訊。

主題

- [CloudHSM CLI 中使用者管理的先決條件](#)
- [CloudHSM CLI 的 HSM 使用者類型](#)
- [CloudHSM CLI 的 HSM 使用者許可表](#)
- [使用 CloudHSM CLI 建立 HSM 使用者管理員](#)

- [使用 CloudHSM CLI 建立 HSM 加密使用者](#)
- [使用 CloudHSM CLI 列出叢集中的所有 HSM 使用者](#)
- [使用 CloudHSM CLI 變更 HSM 使用者密碼](#)
- [使用 CloudHSM CLI 刪除 HSM 使用者](#)
- [使用 CloudHSM CLI 管理 HSM 使用者的 MFA](#)
- [使用 CloudHSM CLI 管理規定人數身分驗證 \(M of N 存取控制\)](#)

CloudHSM CLI 中使用者管理的先決條件

在使用 CloudHSM CLI 管理硬體安全模組 (HSM) 使用者之前 AWS CloudHSM，您必須先完成這些先決條件。下列主題說明 CloudHSM CLI 入門。

主題

- [在 中取得 HSM 的 IP 地址 AWS CloudHSM](#)
- [下載 CloudHSM CLI](#)

在 中取得 HSM 的 IP 地址 AWS CloudHSM

如要使用 CloudHSM CLI，您必須使用設定工具來更新本機組態。如需使用 CloudHSM CLI 執行設定工具的說明，請參閱 [開始使用 AWS CloudHSM 命令列界面 \(CLI\)](#)。 -a 參數需要在叢集中新增 HSM 的 IP 地址。如果您有多個 HSM，則可以使用任何 IP 地址。這可確保 CloudHSM CLI 可在整個叢集中傳播您所做的任何變更。請記住，CloudHSM CLI 會使用其本機檔案來追蹤叢集資訊。如果自上次從特定主機使用 CloudHSM CLI 後叢集已發生變更，則必須將這些變更新增至儲存在該主機上的本機組態檔案中。使用 CloudHSM CLI 時，請勿移除 HSM。

取得 HSM 的 IP 地址（主控台）

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 若要開啟叢集詳細資訊頁面，請在叢集表格中選擇叢集 ID。
4. 若要取得 IP 地址，請前往 HSMs 索引標籤。對於 IPv4 叢集，請選擇 ENI IPv4 地址下列出的地址。對於雙堆疊叢集，請使用 ENI IPv4 或 ENI IPv6 地址。

取得 HSM 的 IP 地址 (AWS CLI)

- 使用 AWS CLI 中的 [describe-clusters](#) 命令取得 HSM 的 IP 地址。在 命令的輸出中，HSMs 的 IP 地址是 `EniIp` 和 的值 `EniIPv6` (如果是雙堆疊叢集)。

```
$ aws cloudhsmv2 describe-clusters
{
  "Clusters": [
    { ... }
    "Hsms": [
      {
...
        "EniIp": "10.0.0.9",
...
      },
      {
...
        "EniIp": "10.0.1.6",
        "EniIPv6": "2600:113f:404:be09:310e:ed34:3412:f733",
...
    }
```

下載 CloudHSM CLI

最新版本的 CloudHSM CLI 適用於用戶端 SDK 5 的 HSM 使用者管理任務。若要下載並安裝 CloudHSM CLI，請按照[安裝和設定 CloudHSM CLI](#) 中的說明進行操作。

CloudHSM CLI 的 HSM 使用者類型

您在硬體安全模組 (HSM) 上執行的大多數操作都需要 AWS CloudHSM anHSM 使用者的登入資料。HSM 會驗證每個 HSM 使用者，且每個 HSM 使用者都有一種類型，決定您可以該使用者身分在 HSM 上執行哪些操作。

Note

HSM 使用者與 IAM 使用者不同。擁有正確憑證的 IAM 使用者可利用 AWS API 與資源進行互動來建立 HSM。HSM 建立後，您必須使用 HSM 使用者憑證來驗證 HSM 上的操作。

使用者類型

- [未激活的管理員](#)

- [管理員](#)
- [加密使用者 \(CU\)](#)
- [設備使用者 \(AU\)](#)

未激活的管理員

在 CloudHSM CLI 中，未激活的管理員是暫時使用者，僅存在於尚未激活的 AWS CloudHSM 叢集中的第一個 HSM 上。如要[啟動叢集](#)，請執行 CloudHSM CLI 中的 `cluster activate` 命令。運行此命令後，系統將提示未激活的管理員更改密碼。更改密碼後，未激活的管理員將成為管理員。

管理員

在 CloudHSM CLI 中，管理員可以執行使用者管理操作。例如，管理員可以建立和刪除使用者，也可以變更使用者密碼。如需管理員的詳細資訊，請參閱 [CloudHSM CLI 的 HSM 使用者許可表](#)。

加密使用者 (CU)

加密使用者 (CU) 可以執行以下的金鑰管理和密碼編譯操作。

- 金鑰管理：建立、刪除、共用、匯入和匯出密碼編譯金鑰。
- 密碼編譯操作：使用密碼編譯金鑰進行加密、解密、簽署、驗證及其他操作。

如需更多資訊，請參閱[CloudHSM CLI 的 HSM 使用者許可表](#)。

設備使用者 (AU)

設備使用者 (AU) 可以在叢集的 HSMs 上執行複製和同步操作。AWS CloudHSM 會使用 AU 來同步 AWS CloudHSM 叢集中的 HSMs。AU 存在於提供的所有 HSMs 上 AWS CloudHSM，並且具有有限的許可。如需更多資訊，請參閱[CloudHSM CLI 的 HSM 使用者許可表](#)。

AWS 無法在 HSMs 上執行任何操作。AWS 無法檢視或修改您的使用者或金鑰，也無法使用這些金鑰執行任何密碼編譯操作。

CloudHSM CLI 的 HSM 使用者許可表

下表列出硬體安全模組 (HSM) 操作，依可在其中執行操作的 HSM 使用者或工作階段類型排序 AWS CloudHSM。

	管理員	加密使用者 (CU)	設備使用者 (AU)	已驗證的工作階段
取得基本叢集資訊 ¹	 是	 是	 是	 是
變更自己的密碼	 是	 是	 是	不適用
變更任何使用者的密碼	 是	 否	 否	 否
新增、移除使用者	 是	 否	 否	 否
取得同步狀態 ²	 是	 是	 是	 否
擷取、插入遮罩物件 ³	 是	 是	 是	 否

	管理員	加密使用者 (CU)	設備使用者 (AU)	已驗證的工作階段
金鑰管理功能 ⁴	 否	 是	 否	 否
加密、解密	 否	 是	 否	 否
簽署、驗證	 否	 是	 否	 否
產生摘要和 HMAC	 否	 是	 否	 否

- [1] 基本叢集資訊包括叢集的 HSM 數目，以及每個 HSM 的 IP 地址、型號、序號、裝置 ID、韌體 ID 等。
- [2] 使用者可以取得一組摘要 (雜湊)，這組摘要會對應到 HSM 上的金鑰。應用程式可以比較這幾組摘要，以了解叢集中的 HSM 的同步狀態。
- [3] 遮罩物件就是在離開 HSM 之前加密的金鑰。這些金鑰無法在 HSM 外部解密。將金鑰插入 HSM，而且此 HSM 與先前從中擷取金鑰的 HSM 必須在同一個叢集，金鑰才會解密。應用程式可以擷取和插入遮罩物件，以同步叢集的 HSM。
- [4] 金鑰管理功能包括建立、刪除、包裝、取消包裝及修改金鑰的屬性。

使用 CloudHSM CLI 建立 HSM 使用者管理員

請依照下列步驟，使用 CloudHSM CLI 建立硬體安全模組 (HSM) 管理員使用者。

1. 使用下列命令啟動 CloudHSM CLI 互動式模式。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 login 命令並以管理員身分登入叢集。

```
aws-cloudhsm > login --username <username> --role admin
```

3. 系統會提示您輸入密碼。輸入密碼，然後輸出會顯示命令已成功執行。

```
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "<username>",
    "role": "admin"
  }
}
```

4. 輸入下列命令建立管理員。

```
aws-cloudhsm > user create --username <username> --role admin
```

5. 輸入新使用者的密碼。
6. 重新輸入密碼以確認您輸入的密碼正確無誤。

使用 CloudHSM CLI 建立 HSM 加密使用者

請依照下列步驟，使用 CloudHSM CLI 建立硬體安全模組 (HSM) 加密使用者 (CU)。

1. 使用下列命令啟動 CloudHSM CLI 互動式模式。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 login 命令並以管理員身分登入叢集。

```
aws-cloudhsm > login --username <username> --role admin
```

3. 系統會提示您輸入密碼。輸入密碼，然後輸出會顯示命令已成功執行。

```
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "<USERNAME>",
    "role": "admin"
  }
}
```

4. 輸入以下命令來建立加密使用者：

```
aws-cloudhsm > user create --username <username> --role crypto-user
```

5. 輸入新加密使用者的密碼。
6. 重新輸入密碼以確認您輸入的密碼正確無誤。

使用 CloudHSM CLI 列出叢集中的所有 HSM 使用者

在 CloudHSM CLI 中使用 user list 命令來列出 AWS CloudHSM 叢集中的所有使用者。您無需登入即可執行 user list。所有使用者類型均可列出使用者。

請依照下列步驟列出叢集中的所有使用者

1. 使用下列命令啟動 CloudHSM CLI 互動式模式。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 輸入下列命令列出叢集中的所有使用者：

```
aws-cloudhsm > user list
```

如需 user list 的詳細資訊，請參閱[使用者清單](#)。

使用 CloudHSM CLI 變更 HSM 使用者密碼

使用 CloudHSM CLI 中的 user change-password 命令來變更硬體安全模組 (HSM) 使用者的密碼。

使用者類型和密碼需區分大小寫，但使用者名稱不區分大小寫。

管理員、加密使用者 (CU) 和設備使用者 (AU) 只能變更自己的密碼。如要變更其他使用者的密碼，您必須以管理員身分登入。您無法變更目前已登入使用者的密碼。

如要變更您自己的密碼

1. 使用下列命令啟動 CloudHSM CLI 互動式模式。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 login 命令並以要變更密碼的使用者身份登入。

```
aws-cloudhsm > login --username <username> --role <role>
```

3. 輸入使用者的密碼。

```
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "<username>",
    "role": "<role>"
  }
}
```

4. 輸入 user change-password 命令。

```
aws-cloudhsm > user change-password --username <username> --role <role>
```

5. 輸入新密碼。

6. 再次輸入新密碼。

如要變更其他使用者的密碼

1. 使用下列命令啟動 CloudHSM CLI 互動式模式。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 CloudHSM CLI，以管理員身分登入。

```
aws-cloudhsm > login --username <admin> --role admin
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "<admin>",
    "role": "admin"
  }
}
```

```
}
```

- 輸入 `user change-password` 命令以及要變更密碼的使用者的使用者名稱。

```
aws-cloudhsm > user change-password --username <username> --role <role>
```

- 輸入新密碼。
- 再次輸入新密碼。

如需 `user change-password` 的詳細資訊，請參閱 [user change-password](#)。

使用 CloudHSM CLI 刪除 HSM 使用者

在 CloudHSM CLI `user delete` 中使用 刪除硬體安全模組 (HSM) 使用者。您必須以管理員身分登入才能刪除其他使用者。

Tip

您無法刪除擁有金鑰的加密使用者 (CU)。

如要刪除使用者

- 使用下列命令啟動 CloudHSM CLI 互動式模式。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

- 使用 `login` 命令並以管理員身分登入叢集。

```
aws-cloudhsm > login --username <username> --role admin
```

- 系統會提示您輸入密碼。輸入密碼，然後輸出會顯示命令已成功執行。

```
Enter password:
```

```
{
  "error_code": 0,
  "data": {
    "username": "<username>",
    "role": "admin"
  }
}
```

4. 使用 `user delete` 命令來刪除使用者。

```
aws-cloudhsm > user delete --username <username> --role <role>
```

如需 `user delete` 的詳細資訊，請參閱 [deleteUser](#)。

使用 CloudHSM CLI 管理 HSM 使用者的 MFA

為了提高安全性，您可以為使用者設定多重驗證 (MFA)，以協助保護 AWS CloudHSM 叢集。

當您使用啟用 MFA 的硬體安全模組 (HSM) 使用者帳戶登入叢集時，您會向 CloudHSM CLI 提供密碼，這是您所知的第一個因素，而 CloudHSM CLI 會為您提供權杖，並提示您簽署權杖。

如要提供第二個要素 (您擁有的)，請使用您已經建立並與 HSM 使用者相關聯的金鑰對中的私有金鑰來簽署權杖。如要訪問叢集，請將已簽署的權杖提供給 CloudHSM CLI。

如需為使用者設定 MFA 的詳細資訊，請參閱 [為 CloudHSM CLI 設定 MFA](#)

下列主題提供在 中使用規定人數身分驗證的詳細資訊 AWS CloudHSM。

主題

- [使用 CloudHSM CLI 的叢集中的 AWS CloudHSM 配額身分驗證和 MFA](#)
- [AWS CloudHSM 使用 CloudHSM CLI 的 MFA 金鑰對需求](#)
- [為 CloudHSM CLI 設定 MFA](#)
- [為 CloudHSM CLI 建立已啟用 MFA 的使用者](#)
- [為 CloudHSM CLI 啟用 MFA 的登入使用者](#)
- [針對 CloudHSM CLI 啟用 MFA 的使用者輪換金鑰](#)
- [使用 CloudHSM CLI 取消註冊 MFA 公有金鑰](#)
- [使用 CloudHSM CLI 的 MFA 字符檔案參考](#)

使用 CloudHSM CLI 的叢集中的 AWS CloudHSM 配額身分驗證和 MFA

AWS CloudHSM 叢集針對規定人數身分驗證和多重要素驗證 (MFA) 使用相同的金鑰。這表示已啟用 MFA 的使用者已有效註冊 MofN 或規定人數存取控制。如要為同一 HSM 使用者成功使用 MFA 和規定人數驗證，請考慮下列幾點：

- 如果您今天要為使用者使用規定人數驗證，則應使用您為規定人數使用者建立的同一個金鑰對來為該使用者啟用 MFA。
- 如果您為非規定人數身分驗證使用者的非 MFA 使用者新增 MFA 要求，則會將該使用者註冊為使用 MFA 身分驗證的規定人數 (MofN) 註冊使用者。
- 如果您要為兼具規定人數驗證使用者身分的 MFA 使用者移除 MFA 要求或變更其密碼，您也會同時移除規定人數使用者作為規定人數 (MofN) 使用者的註冊。
- 如果您要為兼具規定人數驗證使用者身分的 MFA 使用者移除 MFA 要求或變更其密碼，但仍想保留該使用者的規定人數驗證，則您須將該使用者註冊為規定人數 (MofN) 使用者。

如需規定人數驗證的詳細資訊，請參閱 [管理規定人數身分驗證 \(M 為 N\)](#)。

AWS CloudHSM 使用 CloudHSM CLI 的 MFA 金鑰對需求

若要在 中為硬體安全模組 (HSM) 使用者啟用多重要素驗證 (MFA) AWS CloudHSM，您可以建立新的金鑰對，或使用符合下列要求的現有金鑰：

- 金鑰類型：非對稱金鑰
- 金鑰用途：簽署和驗證
- 金鑰規格：RSA_2048
- 簽名算法包括：sha256WithRSAEncryption

Note

如果您正在使用規定人數驗證或計劃使用法定驗證，請參閱 [使用 CloudHSM CLI 的叢集中的 AWS CloudHSM 配額身分驗證和 MFA](#)

您可以使用 CloudHSM CLI 和金鑰對來建立已啟用 MFA 的新管理員使用者。

為 CloudHSM CLI 設定 MFA

請依照下列步驟設定 CloudHSM CLI 的多重驗證 (MFA)。

1. 如要使用字符簽署策略設定 MFA，您必須先產生 2048 位元的 RSA 私有鍵和關聯的公有金鑰。

```
$ openssl genrsa -out officer1.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)

$ openssl rsa -in officer1.key -outform PEM -pubout -out officer1.pub
writing RSA key
```

2. 在互動式模式中輸入下列命令啟動 CLI。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

3. 使用 CloudHSM CLI 登入您的使用者帳戶。

```
aws-cloudhsm > login --username <admin> --role <admin> --cluster-id <cluster ID>
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "<admin>",
    "role": "<admin>"
  }
}
```

4. 接下來，執行命令以變更 MFA 策略。您必須提供參數 --token。此參數指定將寫入未簽署權杖的檔案。

```
aws-cloudhsm > user change-mfa token-sign --token unsigned-tokens.json --
username <username> --role crypto-user --change-quorum
```

```
Enter password:
Confirm password:
```

5. 您現在有一個包含需要簽署但還未簽署權杖的檔案：`unsigned-tokens.json`。此檔案中的權杖數量取決於叢集中的 HSM 數目。每個權杖代表一個 HSM。這個檔案是 JSON 格式，包含需要簽署以證明您擁有私有金鑰的權杖。

```
$ cat unsigned-tokens.json
{
  "version": "2.0",
  "tokens": [
    {
      {
        "unsigned": "Vtf/9Q0FY45v/E1osvpEMr59JsnP/hLDm4It002vqL8=",
        "signed": ""
      },
      {
        "unsigned": "wVbC0/5IKwjyZK2NBpdFLyI7BiayZ24YcdUdlcxLwZ4=",
        "signed": ""
      },
      {
        "unsigned": "z6aW9RzErJBL5KqFG5h8lhTVt9oLbxppjod0Ebysydw=",
        "signed": ""
      }
    ]
  }
}
```

6. 接下來，使用步驟 1 中建立的私有金鑰來簽署這些權杖。將簽署的權杖放回檔案中。首先，您必須擷取和解碼 base64 編碼的權杖。

```
$ echo "Vtf/9Q0FY45v/E1osvpEMr59JsnP/hLDm4It002vqL8=" > token1.b64
$ echo "wVbC0/5IKwjyZK2NBpdFLyI7BiayZ24YcdUdlcxLwZ4=" > token2.b64
$ echo "z6aW9RzErJBL5KqFG5h8lhTVt9oLbxppjod0Ebysydw=" > token3.b64
$ base64 -d token1.b64 > token1.bin
$ base64 -d token2.b64 > token2.bin
$ base64 -d token3.b64 > token3.bin
```

7. 現在，您擁有了可以使用步驟 1 中建立的 RSA 私有金鑰進行簽署的二進位權杖。

```
$ openssl pkeyutl -sign \
    -inkey officer1.key \
    -pkeyopt digest:sha256 \
    -keyform PEM \
```



```

    -in token1.bin \
    -out token1.sig.bin
$ openssl pkeyutl -sign \
    -inkey officer1.key \
    -pkeyopt digest:sha256 \
    -keyform PEM \
    -in token2.bin \
    -out token2.sig.bin
$ openssl pkeyutl -sign \
    -inkey officer1.key \
    -pkeyopt digest:sha256 \
    -keyform PEM \
    -in token3.bin \
    -out token3.sig.bin

```

8. 現在，您有字符的二進位簽章。您必須使用 base64 進行編碼，然後將它們放回權杖檔案中。

```

$ base64 -w0 token1.sig.bin > token1.sig.b64
$ base64 -w0 token2.sig.bin > token2.sig.b64
$ base64 -w0 token3.sig.bin > token3.sig.b64

```

9. 最後，您可以將 base64 值複製並粘貼回權杖檔案中：

```

{
  "version": "2.0",
  "tokens": [
    {
      "unsigned": "1jqwx9bJ0UUQLiNb7mxXS1uBJsEXh0B9nj05BqnPsE=",
      "signed": "eiw3fZeCKIY50C4zPeg9Rt90M1Qlq3WlJh6Yw7xXm4nF6e9ETLE39+9M
+rUqDWMRZjaBfaMbg5d9yDkz5p13U7ch2t1F9LoYabsWutkT014KRq/rcYMvFsU9n/Ey/
TK0PVaxLN42X+pebV4juwMhN4mK4CzdFAJgM+UGB0j4yB9recp0BB9K8QFSpJZALSEdDgUc/
mS1eDq3rU0int6+4NKuLQjpR
+LSEIWRZ6g6+MND2vXGskxHjadCQ09L7Tz8VcWjKDbxJcBiGKvkqyozl9zrGo8fA3WHBmwiAgS61Merx77ZGY4PFR37
YMSC14prCN15DtMRv2xA1SGSb4w=="
    },
    {
      "unsigned": "LMMFc34ASpvnNPFzBbMbr9FProS/Zu2P8zF/xzk5hVQ=",
      "signed": "HBImKnHmw+6R2TpFEpfiAg4+hu2pFNwn43ClhKPkn2higbEhUD0JVi
+4MerSyvU/NN79iWVxDvJ9Ito+jpiRQjTfTGEoIteyuAr1v/Bzh+Hjmr0530QpZaJ/VXGIgApD0myuu/
ZGNKQTCskkL7+V81FG7yR1Nm22jUeGa735zvm/E+cenvZdy0VVx6A7WeWr13JEKKBweHbi+7BwbaW
+PTdCuIRd4Ug76Sy+cFhsvcG1k7cMwDh8MgXzIZ2m1f/hdy2j8qAx0RTLlmyU0YvPY0vUhc
+s83hx36QpGwGcD7RA0bPT50rTx7PHd0N1CL+Wwy91We8yIOFBS6nxo1R7w=="
    }
  ],
}

```

```

    {
      "unsigned": "dzeHbwhiVXQqcUGj563z51/7sLUdxjL93Sb0UyZRjH8=",
      "signed": "VgQPvrTsvGljVBFxHnsduq16x8ZrnxfcYVYGf/
N7gEzI4At3GDs2EVZWTRdvS0uGHdkFYp1apHgJZ7PDVmGcTkIXVD2lFYppcgNlSzkYlfttr5E0jqS9ZjYEggGuB4g//
MxaBaRbJai/6BlcE92NIdBusTtreIm3yTpjIXNAVoeRSnkfuw7wZcL96Qok1Nb1WUuSHw
+psUyeIVtIwFMHEfFoRC0t
+Vhmn1nFnkjGPb9W3Aprw2dRRvFM3R2ZTDvMCi0YDzUCd43GftGq2LfxH3qSD51oFHg1HQV0Y0jyVzz1Avub5HQdt00
    }
  ]
}

```

10. 現在，您的權杖文件已全部簽署，您可以繼續操作。輸入包含已簽署權杖的檔案名稱，然後按 Enter 鍵。最後，輸入您公有金鑰的路徑。

```

Enter signed token file path (press enter if same as the unsigned token file):
Enter public key PEM file path:officer1.pub
{
  "error_code": 0,
  "data": {
    "username": "<username>",
    "role": "crypto-user"
  }
}

```

現在，您已經使用 MFA 設定了您的使用者。

```

{
  "username": "<username>",
  "role": "crypto-user",
  "locked": "false",
  "mfa": [
    {
      "strategy": "token-sign",
      "status": "enabled"
    }
  ],
  "cluster-coverage": "full"
},

```

為 CloudHSM CLI 建立已啟用 MFA 的使用者

請依照下列步驟建立已啟用多重要素驗證 (MFA) AWS CloudHSM 的使用者。

1. 使用 CloudHSM CLI 以管理員身分登入 HSM。
2. 使用 [user create](#) 命令建立您選擇的使用者。然後依照 [為 CloudHSM CLI 設定 MFA](#) 的步驟為使用者設定 MFA。

為 CloudHSM CLI 啟用 MFA 的登入使用者

請依照下列步驟，在啟用多重要素驗證 (MFA) 的情況下登入 AWS CloudHSM 使用者。

1. 使用 CloudHSM CLI 中的 [login mfa-token-sign](#) 命令，針對已啟用 MFA 的使用者啟動登入程序。

```
aws-cloudhsm > login --username <username> --role <role> mfa-token-sign --  
token <unsigned-tokens.json>  
Enter password:
```

2. 輸入您的密碼。然後，系統將提示您輸入包含未簽署/已簽署權杖對的權杖檔案路徑，其中已簽署權杖是使用您私有金鑰產生的權杖。

```
aws-cloudhsm > login --username <username> --role <role> mfa-token-sign --  
token <unsigned-tokens.json>  
Enter password:  
Enter signed token file path (press enter if same as the unsigned token file):
```

3. 當提示輸入已簽署權杖文件路徑時，您可以在單獨的終端中檢查未簽署的權杖檔案。識別具有需要簽署但尚未權杖的檔案：[<unsigned-tokens.json>](#)。此檔案中的權杖數量取決於叢集中的 HSM 數目。每個權杖代表一個 HSM。這個檔案是 JSON 格式，包含需要簽署以證明您擁有私有金鑰的權杖。

```
$ cat <unsigned-tokens.json>  
{  
  "version": "2.0",  
  "tokens": [  
    {  
      "unsigned": "Vtf/9Q0FY45v/E1osvpEMr59JsnP/hLDm4It002vqL8=",  
      "signed": ""  
    },  
    {  
      "unsigned": "wVbC0/5IKwjyZK2NBpdFLyI7BiayZ24YcdUd1cxLwZ4=",
```

```

    "signed": ""
  },
  {
    "unsigned": "z6aW9RzErJBL5KqFG5h8lhTVt9oLbxppjod0Ebysydw=",
    "signed": ""
  }
]
}

```

4. 使用在步驟 2 中建立的私有金鑰簽署尚未簽署的權杖。首先，您必須擷取和解碼 base64 編碼的權杖。

```

$ echo "Vtf/9Q0FY45v/E1osvpEMr59JsnP/hLDm4It002vqL8=" > token1.b64
$ echo "wVbC0/5IKwjyZK2NBpdFLyI7BiayZ24YcdUdlcxLwZ4=" > token2.b64
$ echo "z6aW9RzErJBL5KqFG5h8lhTVt9oLbxppjod0Ebysydw=" > token3.b64
$ base64 -d token1.b64 > token1.bin
$ base64 -d token2.b64 > token2.bin
$ base64 -d token3.b64 > token3.bin

```

5. 您現在有二進制權杖。使用您先前在 [MFA 設定步驟 1](#) 中建立的 RSA 私有金鑰來簽署這些權杖。

```

$ openssl pkeyutl -sign \
  -inkey officer1.key \
  -pkeyopt digest:sha256 \
  -keyform PEM \
  -in token1.bin \
  -out token1.sig.bin
$ openssl pkeyutl -sign \
  -inkey officer1.key \
  -pkeyopt digest:sha256 \
  -keyform PEM \
  -in token2.bin \
  -out token2.sig.bin
$ openssl pkeyutl -sign \
  -inkey officer1.key \
  -pkeyopt digest:sha256 \
  -keyform PEM \
  -in token3.bin \
  -out token3.sig.bin

```

6. 現在，您有了已簽署的二進位權杖。使用 base64 對這些權杖進行編碼，然後將它們放回權杖檔案中。

```
$ base64 -w0 token1.sig.bin > token1.sig.b64
$ base64 -w0 token2.sig.bin > token2.sig.b64
$ base64 -w0 token3.sig.bin > token3.sig.b64
```

7. 最後，將 base64 值複製並粘貼回權杖檔案中：

```
{
  "version": "2.0",
  "tokens": [
    {
      "unsigned": "1jqwx9b9J0UUQLiNb7mxXS1uBJsEXh0B9nj05BqnPsE=",
      "signed": "eiw3fZeCKIY50C4zPeg9Rt90M1Q1q3W1Jh6Yw7xXm4nF6e9ETLE39+9M
+rUqDWMRZjaBfaMbg5d9yDkz5p13U7ch2t1F9LoYabsWutkT014KRq/rcYMvFsU9n/Ey/
TK0PVaxLN42X+pebV4juwMhN4mK4CzdFAJgM+UGB0j4yB9recp0BB9K8QFSpJZALSEdDgUc/
mS1eDq3rU0int6+4NKuLQjpR
+LSEIWRZ6g6+MND2vXGskxHjadCQ09L7Tz8VcWjKDbxJcBiGKvkqyozl9zrGo8fA3WHBmwiAgS61Merx77ZGY4PFR37
YM5C14prCN15DtMRv2xA1SGSb4w=="
    },
    {
      "unsigned": "LMMFc34ASpNvNPFzBbMbr9FProS/Zu2P8zF/xzk5hVQ=",
      "signed": "HBImKnHmw+6R2TpFEpfiAg4+hu2pFNwn43ClhKPkn2higbEhUD0JVi
+4MerSyvU/NN79iWVxDvJ9Ito+jpiRQjTfTGEoIteyuAr1v/Bzh+Hjmr0530QpZaJ/VXGIgApD0myuu/
ZGNKQTCSSkL7+V81FG7yR1Nm22jUeGa735zvm/E+cenvZdy0VVx6A7WeWrl3JEKKBweHbi+7BwbaW
+PTdCuIRd4Ug76Sy+cFhsvcG1k7cMwDh8MgXzIZ2m1f/hdy2j8qAx0RTLlmyU0YvPY0vUhc
+s83hx36QpGwGcD7RA0bPT50rTx7PHd0N1CL+Wwy91We8yIOFBS6nxo1R7w=="
    },
    {
      "unsigned": "dzeHbwhiVXQqcUGj563z51/7sLUdxjL93Sb0UyZRjH8=",
      "signed": "VgQPvrTsvGljVBFxHnsduq16x8ZrnxfcYVYGf/
N7gEzI4At3GDs2EVZWTRdvS0uGHdkFYp1apHgJZ7PDVmGcTkIXVD21FYppcgN1SzkY1ftr5E0jqS9ZjYEggGuB4g//
MxaBaRbJai/6BlcE92NIdBusTtreIm3yTpjIXNAVoeRSnkfuw7wZcL96Qok1Nb1WUuSHw
+psUyeIVtIwFMHEfFoRC0t
+VhmnlnFnkjGPb9W3Aprw2dRRvFM3R2ZTDvMCi0YDzUCd43GftGq2LfxH3qSD51oFHglHQV0Y0jyVzz1Avub5HQdt0Q
    }
  ]
}
```

8. 現在，您的權杖文件已全部簽署，您可以繼續操作。輸入包含已簽署權杖的檔案名稱，然後按 Enter 鍵。您現在應該成功登錄。

```
aws-cloudhsm > login --username <username> --role <role> mfa-token-sign --
token <unsigned-tokens.json>
```

```

Enter password:
Enter signed token file path (press enter if same as the unsigned token file):
{
  "error_code": 0,
  "data": {
    "username": "<username>",
    "role": "<role>"
  }
}

```

針對 CloudHSM CLI 啟用 MFA 的使用者輪換金鑰

請依照下列步驟，為啟用多重要素驗證 (MFA) AWS CloudHSM 的使用者輪換金鑰。

<result>

您已使用私有金鑰簽署了產生的 JSON 格式的權杖文件檔案，並註冊了新的 MFA 公有金鑰。

</result>

1. 使用 CloudHSM CLI 以任何管理員或已啟用 MFA 的特定使用者身分登入 HSM (如需詳細資訊，請參閱[已啟用 MFA 的登入使用者](#))。
2. 接下來，執行命令以變更 MFA 策略。您必須提供參數 `--token`。此參數指定將寫入未簽署權杖的檔案。

```

aws-cloudhsm > user change-mfa token-sign --token unsigned-tokens.json --
username <username> --role crypto-user --change-quorum
Enter password:
Confirm password:

```

3. 識別具有需要簽署但尚未權杖的檔案：`unsigned-tokens.json`。此檔案中的權杖數量取決於叢集中的 HSM 數目。每個權杖代表一個 HSM。這個檔案是 JSON 格式，包含需要簽署以證明您擁有私有金鑰的權杖。這將是新 RSA 公有/私有金鑰對中的新私有金鑰 (您想要用其輪換目前已註冊公有金鑰)。

```

$ cat unsigned-tokens.json
{
  "version": "2.0",
  "tokens": [
    {
      "unsigned": "Vtf/9Q0FY45v/E1osvpEMr59JsnP/hLDm4It002vqL8=",
      "signed": ""
    }
  ]
}

```

```

    },
    {
      "unsigned": "wVbC0/5IKwjyZK2NBpdFLyI7BiayZ24YcdUd1cxLwZ4=",
      "signed": ""
    },
    {
      "unsigned": "z6aW9RzErJBL5KqFG5h81hTVt9oLbxppjod0Ebysydw=",
      "signed": ""
    }
  ]
}

```

4. 使用您先前在設置過程中建立的私有金鑰來簽署這些權杖。首先，必須擷取和解碼 base64 編碼的權杖。

```

$ echo "Vtf/9Q0FY45v/E1osvpEMr59JsnP/hLDm4It002vqL8=" > token1.b64
$ echo "wVbC0/5IKwjyZK2NBpdFLyI7BiayZ24YcdUd1cxLwZ4=" > token2.b64
$ echo "z6aW9RzErJBL5KqFG5h81hTVt9oLbxppjod0Ebysydw=" > token3.b64
$ base64 -d token1.b64 > token1.bin
$ base64 -d token2.b64 > token2.bin
$ base64 -d token3.b64 > token3.bin

```

5. 您現在有二進制權杖。使用您先前在設定過程中建立的 RSA 私有金鑰來簽署這些權杖。

```

$ openssl pkeyutl -sign \
  -inkey officer1.key \
  -pkeyopt digest:sha256 \
  -keyform PEM \
  -in token1.bin \
  -out token1.sig.bin
$ openssl pkeyutl -sign \
  -inkey officer1.key \
  -pkeyopt digest:sha256 \
  -keyform PEM \
  -in token2.bin \
  -out token2.sig.bin
$ openssl pkeyutl -sign \
  -inkey officer1.key \
  -pkeyopt digest:sha256 \
  -keyform PEM \
  -in token3.bin \
  -out token3.sig.bin

```

6. 現在，您有了已簽署的二進位權杖。使用 base64 對這些權杖進行編碼，然後將它們放回權杖檔案中。

```
$ base64 -w0 token1.sig.bin > token1.sig.b64
$ base64 -w0 token2.sig.bin > token2.sig.b64
$ base64 -w0 token3.sig.bin > token3.sig.b64
```

7. 最後，將 base64 值複製並粘貼回權杖檔案中：

```
{
  "version": "2.0",
  "tokens": [
    {
      "unsigned": "1jqwxb9bJ0UUQLiNb7mxXS1uBJsEXh0B9nj05BqnPsE=",
      "signed": "eiw3fZeCKIY50C4zPeg9Rt90M1Q1q3W1Jh6Yw7xXm4nF6e9ETLE39+9M
+rUqDWMRZjaBfaMbg5d9yDkz5p13U7ch2t1F9LoYabsWutkT014KRq/rcYMvFsU9n/Ey/
TK0PVaxLN42X+pebV4juwMhN4mK4CzdFAJgM+UGB0j4yB9recp0BB9K8QFSpJZALSEdDgUc/
mS1eDq3rU0int6+4NKuLQjpR
+LSEIWRZ6g6+MND2vXGskxHjadCQ09L7Tz8VcWjKDbxJcBiGKvkqyozl9zrGo8fA3WHBmwiAgS61Merx77ZGY4PFR37
YM5C14prCN15DtMRv2xA1SGSb4w=="
    },
    {
      "unsigned": "LMMFc34ASpNvNPFzBbMbr9FProS/Zu2P8zF/xzk5hVQ=",
      "signed": "HBImKnHmw+6R2TpFEpfiAg4+hu2pFNwn43ClhKPkn2higbEhUD0JVi
+4MerSyvU/NN79iWVxDvJ9Ito+jpiRQjTfTGEoIteyuAr1v/Bzh+Hjmr0530QpZaJ/VXGIgApD0myuu/
ZGNKQTCsKkL7+V81FG7yR1Nm22jUeGa735zvm/E+cenvZdy0VVx6A7WeWr13JEKKBweHbi+7BwbaW
+PTdCuIRd4Ug76Sy+cFhsvcG1k7cMwDh8MgXzIZ2m1f/hdy2j8qAx0RTL1mwyU0YvPY0vUhc
+s83hx36QpGwGcD7RA0bPT50rTx7PHd0N1CL+Wwy91We8yIOFBS6nxo1R7w=="
    },
    {
      "unsigned": "dzeHbwhiVXQqcUGj563z51/7sLUdxjL93Sb0UyZRjH8=",
      "signed": "VgQPvrTsvG1jVBFxHnsduq16x8ZrnxfcYVYGf/
N7gEzI4At3GDs2EVZWTRdvS0uGHdkFYp1apHgJZ7PDVmGcTkIXVD21FYppcgN1SzkY1ftr5E0jqS9ZjYEggGuB4g//
MxaBaRbJai/6BlcE92NIdBusTtreIm3yTpjIXNAVoeRSnkfuw7wZcL96Qok1Nb1WUuSHw
+psUyeIVtIwFMHEfFoRC0t
+VhmnlnFnkjGPb9W3Aprw2dRRvFM3R2ZTDvMCi0YDzUCd43GftGq2LfxH3qSD51oFHg1HQV0Y0jyVzz1Avub5HQdt0Q
    }
  ]
}
```

8. 現在，您的權杖文件已全部簽署，您可以繼續操作。輸入包含已簽署權杖的檔案名稱，然後按 Enter 鍵。最後，輸入您新公有金鑰的路徑。現在，您會看到以下 [用戶列表](#) 部分輸出的內容。


```

Enter signed token file path (press enter if same as the unsigned token file):
Enter public key PEM file path:officer1.pub
{
  "error_code": 0,
  "data": {
    "username": "<username>",
    "role": "crypto-user"
  }
}

```

現在，您已經使用 MFA 設定了您的使用者。

```

{
  "username": "<username>",
  "role": "crypto-user",
  "locked": "false",
  "mfa": [
    {
      "strategy": "token-sign",
      "status": "enabled"
    }
  ],
  "cluster-coverage": "full"
},

```

使用 CloudHSM CLI 取消註冊 MFA 公有金鑰

請依照下列步驟，在註冊 MFA 公有金鑰時，取消 AWS CloudHSM 註冊管理使用者的多重驗證 (MFA) 公有金鑰。

1. 使用 CloudHSM CLI 以啟用 MFA 的管理員身分登入 HSM。
2. 使用 `user change-mfa token-sign` 命令為使用者移除 MFA。

```

aws-cloudhsm > user change-mfa token-sign --username <username> --role admin --
deregister --change-quorum
Enter password:
Confirm password:
{
  "error_code": 0,
  "data": {

```

```

    "username": "<username>",
    "role": "admin"
  }
}

```

使用 CloudHSM CLI 的 MFA 字符檔案參考

註冊多重要素驗證 (MFA) 公有金鑰或嘗試使用 MFA 登入 CloudHSM CLI 時產生的字符檔案包含下列項目：

- 權杖：一組以 JSON 物件文字形式表示的 base64 編碼的未簽署/已簽署權杖對。
- 未簽署：一個 base64 編碼和 SHA256 雜湊的權杖。
- 已簽署：使用 RSA 2048 位元私有金鑰對未簽署權杖進行 base64 編碼的已簽署權杖 (簽章)。

```

{
  "version": "2.0",
  "tokens": [
    {
      "unsigned": "1jqwx b9bJ0UUQLiNb7mxXS1uBJsEXh0B9nj05BqnPsE=",
      "signed": "eiw3fZeCKIY50C4zPeg9Rt90M1Q1q3W1Jh6Yw7xXm4nF6e9ETLE39+9M
+rUqDWMRZjaBfaMbg5d9yDkz5p13U7ch2t1F9LoYabsWutkT014KRq/rcYMvFsU9n/Ey/TK0PVaxLN42X
+pebV4juwMhN4mK4CzdFAJgM+UGB0j4yB9recp0BB9K8QFSpJZALSEdDgUc/mS1eDq3rU0int6+4NKuLQjpR
+LSEIWRZ6g6+MND2vXGskxHjadCQ09L7Tz8VcWjKDbxJcBiGKvkqyozl9zrGo8fA3WHBmwiAgS61Merx77ZGY4PFR37+j/
YMSC14prCN15DtMRv2xA1SGSb4w=="
    },
    {
      "unsigned": "LMMFc34ASpvnNPFzBbMbr9FProS/Zu2P8zF/xzk5hVQ=",
      "signed": "HBImKnHmw+6R2TPePfiAg4+hu2pFNwn43ClhKPkn2higbEhUD0JVi
+4MerSyvU/NN79iWVxDvJ9Ito+jpiRQjTfTGEoIteyuAr1v/Bzh+Hjmr0530QpZaJ/VXGIgApD0myuu/
ZGNKQTCSkkL7+V81FG7yR1Nm22jUeGa735zvm/E+cenvZdy0VVx6A7WeWr13JEKKBweHbi+7BwbaW
+PTdCuIRd4Ug76Sy+cFhsvcG1k7cMwDh8MgXzIZ2m1f/hdy2j8qAx0RTLlmwyU0YvPY0vUhc
+s83hx36QpGwGcD7RA0bPT50rTx7PHd0N1CL+Wwy91We8yIOFBS6nxo1R7w=="
    },
    {
      "unsigned": "dzeHbwhiVXQqcUGj563z51/7sLUdxjL93Sb0UyZRjH8=",
      "signed": "VgQPvrTsvGljVBFxHnsduq16x8ZrnxfcYVYGf/
N7gEzI4At3GDs2EVZWTRdvS0uGHdkFYp1apHgJZ7PDVmGcTkIXVD2lFYppcgN1SzkYlftR5E0jqS9ZjYEggGuB4g//
MxaBaRbJai/6BlcE92NIdBusTtreIm3yTpjIXNAVoeRSnkfuw7wZcL96Qok1Nb1WUuSHw
+psUyeIVtIwFMHEfFoRC0t
+VhmnlnFnkjGPb9W3Aprw2dRRvFM3R2ZTDvMCi0YDzUCd43GftGq2LfxH3qSD51oFHg1HQV0Y0jyVzz1Avub5HQdt0QdErI

```

```
}  
]  
}
```

使用 CloudHSM CLI 管理規定人數身分驗證 (M of N 存取控制)

AWS CloudHSM 叢集支援規定人數身分驗證，也稱為 M of N 存取控制。此功能需要 HSM 使用者配合某些操作，增加額外的保護層。

透過規定人數身分驗證，HSM 上的單一使用者都無法在 HSM 上執行規定人數控制的操作。相對地，必須有最低數量的 HSM 使用者 (至少 2 個) 合作來執行這些操作。

規定人數身分驗證可以控制以下操作：

- [管理員](#)的 HSM 使用者管理：建立和刪除 HSM 使用者或變更不同的 HSM 使用者密碼。如需詳細資訊，請參閱[AWS CloudHSM 使用 CloudHSM CLI 啟用規定人數身分驗證的使用者管理](#)。

有關規定人數身分驗證的要點 AWS CloudHSM。

- HSM 使用者可以簽署自己的規定人數字符，也就是提供規定人數身分驗證所需的其中一項核准。
- 您可以選擇最低人數的仲裁核准者，範圍從兩 (2) 到八 (8)。
- HSMs 最多可存放 1024 個規定人數字符。達到此限制時，HSM 會清除過期的權杖以建立新的權杖。
- 根據預設，權杖會在建立後 10 分鐘過期。
- 對於啟用 MFA 的叢集，相同的金鑰用於規定人數身分驗證和多重要素驗證 (MFA)。如需詳細資訊，[請參閱使用 CloudHSM CLI 管理 MFA](#)。
- 每個 HSM 每個 Admin 服務可以包含一個字符，每個 Crypto 使用者服務可以包含多個字符。

下列主題提供 AWS CloudHSM 中的規定人數身分驗證的詳細資訊。

主題

- [CloudHSM CLI 的配額身分驗證程序](#)
- [支援使用 CloudHSM CLI 進行規定人數身分驗證 AWS CloudHSM 的服務名稱和類型](#)
- [使用 CloudHSM CLI 為 AWS CloudHSM 管理員設定規定人數身分驗證](#)
- [AWS CloudHSM 使用 CloudHSM CLI 啟用規定人數身分驗證的使用者管理](#)

- [變更使用 CloudHSM CLI 的 AWS CloudHSM 規定人數最小值](#)

CloudHSM CLI 的配額身分驗證程序

下列步驟摘要說明 CloudHSM CLI 的規定人數身分驗證程序。如需特定步驟和工具，請參閱 [AWS CloudHSM 使用 CloudHSM CLI 啟用規定人數身分驗證的使用者管理](#)。

1. 每個硬體安全模組 (HSM) 使用者都會建立非對稱金鑰以進行簽署。使用者會在 HSM 外部執行此動作，以適當方式保護金鑰。
2. 每個 HSM 使用者會登入 HSM，並向 HSM 註冊使用者的簽署金鑰 (公有金鑰) 的公有部分。
3. HSM 使用者想要執行由規定人數控制的操作時，使用者會登入 HSM，並取得規定人數權杖。
4. HSM 使用者會將規定人數字符提供給一或多個其他 HSM 使用者，並要求其核准。
5. 其他 HSM 使用者透過使用自己的金鑰以密碼編譯方式簽署規定人數字符來進行核准。這是在 HSM 外部進行。
6. 當 HSM 使用者具有所需的核准數目時，相同的使用者會登入 HSM 並使用 --approval 引數執行規定人數控制的操作，並提供已簽署的規定人數權杖檔案，其中包含所有必要的核准 (簽章)。
7. HSM 會使用每個簽署者註冊的公有金鑰來驗證簽章。如果簽章有效，HSM 會核准權杖，並執行規定人數控制的操作。

支援使用 CloudHSM CLI 進行規定人數身分驗證 AWS CloudHSM 的服務名稱和類型

管理員服務：規定人數身分驗證用於管理員特殊權限服務，例如建立使用者、刪除使用者、變更使用者密碼、設定規定人數值，以及停用規定人數和 MFA 功能。

加密使用者服務：配額身分驗證用於與特定金鑰相關聯的加密使用者特殊權限服務，例如使用金鑰簽署、共用/取消共用金鑰、包裝/取消包裝金鑰，以及設定金鑰的屬性。產生、匯入或取消包裝金鑰時，會設定關聯金鑰的仲裁值。規定人數值必須等於或小於與金鑰相關聯的使用者數量，其中包括與金鑰共用的使用者和金鑰擁有者。

每種服務類型都會進一步細分為合格的服務名稱，這包含一組特定的可執行法定人數支援的服務操作。

服務名稱	服務類型	服務操作
使用者	管理員	• 建立使用者 • 刪除使用者

服務名稱	服務類型	服務操作
		- 變更使用者密碼 - 變更使用者 MFA
規定人數	管理員	規定人數字符簽署 設定規定人數值
cluster ¹	管理員	- 叢集 mtls register-trust-anchor - 叢集 mtls deregister-trust-anchor - 叢集 mtls set-enforcement
金鑰管理	加密使用者	- 金鑰包裝 - 金鑰取消包裝 - 共用金鑰 - 取消共用金鑰 - 設定金鑰屬性
key-usage	加密使用者	金鑰符號

【1】 叢集服務僅在 hsm2m.medium 上提供

使用 CloudHSM CLI 為 AWS CloudHSM 管理員設定規定人數身分驗證

下列主題說明您必須完成的步驟，才能設定硬體安全模組 (HSM)，以便 AWS CloudHSM [管理員](#) 可以使用規定人數身分驗證。第一次針對管理員設定規定人數身分驗證時，您只需要執行一次下列步驟。完成這些步驟之後，請參閱 [AWS CloudHSM 使用 CloudHSM CLI 啟用規定人數身分驗證的使用者管理](#)。

主題

- [先決條件](#)
- [步驟 1. 建立和註冊用於簽署的金鑰](#)
- [步驟 2. 設定 HSM 上的規定人數最小值](#)
- [配額最小值](#)

先決條件

若要了解此範例，您應該熟悉 [CloudHSM CLI](#)。

步驟 1. 建立和註冊用於簽署的金鑰

若要使用規定人數身分驗證，每個管理員都必須完成下列所有步驟：

主題

- [建立 RSA 金鑰對](#)
- [建立並簽署註冊權杖](#)
- [用 HSM 註冊公有金鑰](#)

建立 RSA 金鑰對

建立和保護金鑰對有許多不同的方式。下列範例示範使用 [OpenSSL](#) 的做法。

Example – 使用 OpenSSL 建立私有金鑰

下列範例示範如何使用 OpenSSL 建立 2048 位元 RSA 金鑰。若要使用這個範例，請將 *<admin.key>* 以您要存放金鑰的檔案名稱來加以取代。

```
$ openssl genrsa -out <admin.key>
Generating RSA private key, 2048 bit long modulus
.....+++
.+++
e is 65537 (0x10001)
```

接下來，使用您剛建立的私有金鑰來產生公有金鑰。

Example – 使用 OpenSSL 建立一個公有金鑰

下列範例會示範如何使用 OpenSSL 根據您剛建立的私有金鑰建立公有金鑰。

```
$ openssl rsa -in admin.key -outform PEM -pubout -out admin1.pub
writing RSA key
```

建立並簽署註冊權杖

您可以建立一個權杖並使用在上一步中剛產生的私有金鑰簽署該權杖。

Example – 建立一個註冊權杖

1. 使用以下命令來啟動 CloudHSM CLI：

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 透過執行[產生規定人數權杖簽署](#)命令建立註冊權杖：

```
aws-cloudhsm > quorum token-sign generate --service registration --token /path/
tokenfile
{
  "error_code": 0,
  "data": {
    "path": "/path/tokenfile"
  }
}
```

3. [產生規定人數權杖簽署](#)命令在指定的檔案路徑產生註冊權杖。檢查權杖檔案：

```
$ cat /path/tokenfile
{
  "version": "2.0",
  "tokens": [
    {
      "approval_data": <approval data in base64 encoding>,
      "unsigned": <unsigned token in base64 encoding>,
      "signed": ""
    }
  ]
}
```

權杖檔案由以下項目組成：

- approval_data：一個 base64 編碼的隨機資料權杖，其原始資料不超過 245 個位元組的最大值。

- **unsigned** : 核准資料的 base64 編碼和 SHA256 雜湊權杖。
- **signed** : 未簽署的權杖的 base64 編碼簽名權杖 (簽名)，使用先前使用 OpenSSL 產生的 RSA 2048 位元私有金鑰。

您可以使用私有金鑰簽署未簽署的權杖，以證明您可以訪問私有金鑰。您需要完整填入簽章和公有金鑰的註冊字符檔案，才能向 AWS CloudHSM 叢集將管理員註冊為規定人數使用者。

Example — 簽署未簽署的註冊權杖

1. 解碼 base64 編碼的未簽署權杖並將其放入二進位檔案中：

```
$ echo -n '6BMUj6mUjjko6ZLCEdzG1WpR5sILhFJfqhW1ej30q1g=' | base64 -d > admin.bin
```

2. 使用 OpenSSL 和私有金鑰來簽署現在的二進位未簽署註冊權杖，並建立一個二進位簽署檔案：

```
$ openssl pkeyutl -sign \  
-inkey admin.key \  
-pkeyopt digest:sha256 \  
-keyform PEM \  
-in admin.bin \  
-out admin.sig.bin
```

3. 將二進位簽章編碼為 base64：

```
$ base64 -w0 admin.sig.bin > admin.sig.b64
```

4. 將 base64 編碼的簽名複製並粘貼到權杖檔案中：

```
{  
  "version": "2.0",  
  "tokens": [  
    {  
      "approval_data": <approval data in base64 encoding>,  
      "unsigned": <unsigned token in base64 encoding>,  
      "signed": <signed token in base64 encoding>  
    }  
  ]  
}
```


用 HSM 註冊公有金鑰

建立金鑰後，管理員必須向 AWS CloudHSM 叢集註冊公有金鑰。

向 HSM 註冊公有金鑰

1. 使用下列命令來啟動 CloudHSM CLI：

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 CloudHSM CLI，以管理員身分登入。

```
aws-cloudhsm > login --username <admin> --role admin
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "<admin>",
    "role": "admin"
  }
}
```

3. 使用 [使用 CloudHSM CLI 註冊使用者的字符簽署規定人數策略](#) 命令來註冊公有金鑰。如需詳細資訊，請參閱下列範例或使用 `help user change-quorum token-sign register` 命令。

Example – 向 AWS CloudHSM 叢集註冊公有金鑰

下列範例顯示如何在 CloudHSM CLI 中使用 `user change-quorum token-sign register` 命令，以向 HSM 註冊管理員的公有金鑰。若要使用此命令，管理員必須登入 HSM。以您自己的值取代這些值：

```
aws-cloudhsm > user change-quorum token-sign register --public-key </path/admin.pub> --
signed-token </path/tokenfile>
{
  "error_code": 0,
  "data": {
    "username": "admin",
```

```
    "role": "admin"
  }
}
```

Note

/path/admin.pub : 公有金鑰 PEM 檔案的檔案路徑

必要 : 是

/path/tokenfile : 帶有權杖由用戶私有金鑰簽名的檔案路徑

必要 : 是

在所有管理員註冊其公有金鑰之後，`user list` 命令的輸出會在規定人數欄位中顯示此資訊，說明使用中已啟用的規定人數策略，如下所示：

```
aws-cloudhsm > user list
{
  "error_code": 0,
  "data": {
    "users": [
      {
        "username": "admin",
        "role": "admin",
        "locked": "false",
        "mfa": [],
        "quorum": [
          {
            "strategy": "token-sign",
            "status": "enabled"
          }
        ],
        "cluster-coverage": "full"
      },
      {
        "username": "admin2",
        "role": "admin",
        "locked": "false",
        "mfa": [],
        "quorum": [
          {
            "strategy": "token-sign",
            "status": "enabled"
          }
        ]
      }
    ]
  }
}
```

```

    }
  ],
  "cluster-coverage": "full"
},
{
  "username": "admin3",
  "role": "admin",
  "locked": "false",
  "mfa": [],
  "quorum": [
    {
      "strategy": "token-sign",
      "status": "enabled"
    }
  ],
  "cluster-coverage": "full"
},
{
  "username": "admin4",
  "role": "admin",
  "locked": "false",
  "mfa": [],
  "quorum": [
    {
      "strategy": "token-sign",
      "status": "enabled"
    }
  ],
  "cluster-coverage": "full"
},
{
  "username": "app_user",
  "role": "internal(APPLIANCE_USER)",
  "locked": "false",
  "mfa": [],
  "quorum": [],
  "cluster-coverage": "full"
}
]
}
}

```

在此範例中，AWS CloudHSM 叢集有兩個 HSMs，每個 HSM 都有相同的管理員，如 `user list` 命令的下列輸出所示。如需建立使用者的詳細資訊，請參閱 [使用 CloudHSM CLI 進行使用者管理](#)

步驟 2. 設定 HSM 上的規定人數最小值

若要使用規定人數身分驗證，管理員必須登入 HSM，然後設定規定人數最小值。這是執行 HSM 使用者管理操作所需的的管理員核准數下限。HSM 上的任何管理員 (包括尚未註冊用於簽署的金鑰的管理員) 可以設定規定人數最小值。您可以隨時變更規定人數最小值。如需詳細資訊，請參閱[變更最小值](#)。

設定 HSM 上的規定人數最小值

1. 使用下列命令來啟動 CloudHSM CLI：

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 CloudHSM CLI，以管理員身分登入。

```
aws-cloudhsm > login --username <admin> --role admin
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "<admin>",
    "role": "admin"
  }
}
```

3. 使用 [使用 CloudHSM CLI 更新規定人數值](#) 命令來設定規定人數最小值。--service 旗標可識別您要為其設定值的 HSM 服務。如需詳細資訊，請參閱下列範例或使用 `help quorum token-sign set-quorum-value` 命令。

Example – 設定 HSM 上的規定人數最小值

此範例使用值為 2 的規定人數最小值。您可以選擇二 (2) 到八 (8) 之間的任何值，最多可到 HSM 上的管理員總數。在此範例中，HSM 有四 (4) 個管理員，因此最大可能值為四 (4) 個。

若要使用以下範例命令，請將最終數字 (**<2>**) 以您偏好的規定人數最小值加以取代。

```
aws-cloudhsm > quorum token-sign set-quorum-value --service user --value <2>
{
  "error_code": 0,
  "data": "Set quorum value successful"
}
```

在此範例中，[使用 CloudHSM CLI 顯示規定人數值](#) 命令會列出服務中包含的 HSM 服務類型、名稱和描述。

配額最小值

使用 `quorum token-sign list-quorum-values` 命令取得服務的規定人數最小值。

```
aws-cloudhsm > quorum token-sign list-quorum-values
{
  "error_code": 0,
  "data": {
    "user": 2,
    "quorum": 1
  }
}
```

上述 `quorum token-sign list-quorum-values` 命令的輸出顯示 HSM 使用者服務 (負責使用者管理操作) 的規定人數最小值現在是 2。完成這些步驟之後，請參閱 [使用規定人數進行使用者管理 \(M 為 N\)](#)。

管理員服務：規定人數身分驗證用於管理員特殊權限服務，例如建立使用者、刪除使用者、變更使用者密碼、設定規定人數值，以及停用規定人數和 MFA 功能。

加密使用者服務：配額身分驗證用於與特定金鑰相關聯的加密使用者特殊權限服務，例如使用金鑰簽署、共用/取消共用金鑰、包裝/取消包裝金鑰，以及設定金鑰的屬性。產生、匯入或取消包裝金鑰時，會設定關聯金鑰的仲裁值。規定人數值必須等於或小於與金鑰相關聯的使用者數量，其中包括與金鑰共用的使用者和金鑰擁有者。

每種服務類型都會進一步細分為合格的服務名稱，這包含一組特定的可執行法定人數支援的服務操作。

服務名稱	服務類型	服務操作
使用者	管理員	建立使用者

服務名稱	服務類型	服務操作
		- 刪除使用者 - 變更使用者密碼 - 變更使用者 MFA
規定人數	管理員	規定人數字符簽署 設定規定人數值
cluster ¹	管理員	- 叢集 mtls register-trust-anchor - 叢集 mtls deregister-trust-anchor - 叢集 mtls set-enforcement
金鑰管理	加密使用者	- 金鑰包裝 - 金鑰取消包裝 - 共用金鑰 - 取消共用金鑰 - 設定金鑰屬性
key-usage	加密使用者	金鑰符號

【1】 叢集服務僅在 hsm2m.medium 上提供

AWS CloudHSM 使用 CloudHSM CLI 啟用規定人數身分驗證的使用者管理

硬體安全模組 (HSM) 上的 AWS CloudHSM [管理員](#) 可以為 AWS CloudHSM 叢集中的下列操作設定規定人數身分驗證：

- [使用 CloudHSM CLI 建立 AWS CloudHSM 使用者](#)
- [使用 CloudHSM CLI 刪除 AWS CloudHSM 使用者](#)
- [使用 CloudHSM CLI 變更使用者的密碼](#)
- [CloudHSM CLI 中的使用者 change-mfa 類別](#)

AWS CloudHSM 叢集設定為規定人數身分驗證之後，管理員就無法自行執行 HSM 使用者管理操作。以下範例示範當管理員嘗試在 HSM 上建立新使用者時的輸出。命令失敗並顯示錯誤，指出需要進行規定人數身分驗證。

```
aws-cloudhsm > user create --username user1 --role crypto-user
Enter password:
Confirm password:
{
  "error_code": 1,
  "data": "Quorum approval is required for this operation"
}
```

若要執行 HSM 使用者管理操作，管理員必須完成下列工作：

主題

- [步驟 1. 取得規定人數字符](#)
- [步驟 2. 取得核准管理員的簽章](#)
- [步驟 3. 核准 AWS CloudHSM 叢集上的權杖並執行使用者管理操作](#)

步驟 1. 取得規定人數字符

首先，管理員必須使用 CloudHSM CLI 來請求規定人數權杖。

取得規定人數權杖

1. 使用下列命令來啟動 CloudHSM CLI。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 CloudHSM CLI，以管理員身分登入。

```
aws-cloudhsm > login --username <admin> --role admin
Enter password:
{
```

```

    "error_code": 0,
    "data": {
      "username": "<admin>",
      "role": "admin"
    }
  }
}

```

3. 使用 `quorum token-sign generate` 命令來產生規定人數權杖。如需詳細資訊，請參閱下列範例或使用 `help quorum token-sign generate` 命令。

Example – 產生規定人數權杖

此範例會取得使用者名稱為 `admin` 的管理員的規定人數權杖並將權杖儲存至名為 `admin.token` 的檔案中。若要使用範例命令，請將這些值取代為您自己的值：

- `<admin>`：取得權杖的管理員名稱。此使用者必須是登入 HSM 的相同管理員並正在執行此命令。
- `<admin.token>`：用於存放規定人數權杖的檔案名稱。

在以下命令中，`user` 會識別您可以對其使用要生成權杖的服務名稱。在此情況下，此權杖可用於 HSM 使用者管理操作 (`user` 服務)。

```

aws-cloudhsm > login --username <admin> --role admin --password <password>
{
  "error_code": 0,
  "data": {
    "username": "<admin>",
    "role": "admin"
  }
}

```

```

aws-cloudhsm > quorum token-sign generate --service user --token </path/admin.token>
{
  "error_code": 0,
  "data": {
    "path": "/home/tfile"
  }
}

```

`quorum token-sign generate` 命令會在指定的檔案路徑產生使用者服務規定人數權杖。可以檢查權杖文件：


```
$ cat </path/admin.token>
{
  "version": "2.0",
  "service": "user-management",
  "approval_data": "AAEAAwAAABgAAAAAAAAAAJ9eFkfcP3mNzJA1fK
+0WbNhZG1pbgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABj5vbeAAAAAAAAAAAAQADAAAFQAAAAAAAAAAW/
v5Euk83amq1fij0zyvD2FkbWluAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGPm9t4AAAAAAAAAAAAABAAMAAAAUA
+b23gAAAAAAAA",
  "token": "012LZkmAHZyAc1hPhyck0oVW33aGrgG77qmDHWQ3CJ8=",
  "signatures": []
}
```

權杖檔案由以下項目組成：

- 服務：與權杖相關聯的規定人數服務識別符。
- approval_data：由 HSM 產生的 base64 編碼原始資料權杖。
- token：approval_data 的 base64 編碼和 SHA-256 雜湊權杖
- signatures：base64 編碼的簽名權杖 (簽名) 陣列，其中核准者的每個簽名均採用 JSON 物件常值的形式：

```
{
  "username": "<APPROVER_USERNAME>",
  "role": "<APPROVER_ROLE>",
  "signature": "<APPROVER_RSA2048_BIT_SIGNATURE>"
}
```

每個簽章都是從核准者的結果使用其對應的 RSA 2048 位元私有金鑰建立，其公有金鑰已向 HSM 註冊。

執行 `quorum token-sign list` 命令，可確認產生的使用者服務規定人數權杖在於 CloudHSM 叢集中是否存在：

```
aws-cloudhsm > quorum token-sign list
{
  "error_code": 0,
  "data": {
    "tokens": [
      {
        "username": "admin",
```

```

    "service": "user",
    "approvals-required": {
      "value": 2
    },
    "number-of-approvals": {
      "value": 0
    },
    "token-timeout-seconds": {
      "value": 597
    },
    "cluster-coverage": "full"
  }
]
}
}

```

token-timeout-seconds 時間表示過期前需核准的所產生權杖的超時期 (以秒為單位)。

步驟 2. 取得核准管理員的簽章

具有規定人數權杖的管理員必須取得其他管理員核准的權杖。為了提供核准，其他管理員會使用其簽署金鑰來以密碼編譯形式簽署權杖。他們會在 HSM 外部執行此操作。

簽署權杖的方式有很多。下列範例示範使用 [OpenSSL](#) 的做法。若要使用不同的簽署工具，請確認工具使用管理員的私有金鑰 (簽署金鑰) 來簽署權杖的 SHA-256 摘要。

Example 取得核准管理員的簽章

在這個範例中，具有權杖 (admin) 的管理員需要至少兩 (2) 個核准。以下範例命令示範兩 (2) 個管理員如何使用 OpenSSL 來以密碼編譯方式簽署權杖。

1. 解碼 base64 編碼的未簽署權杖並將其放入二進位檔案中：

```
$ echo -n '012LZkmAHZyAc1hPhyck0oVW33aGrgG77qmDHWQ3CJ8=' | base64 -d > admin.bin
```

2. 使用 OpenSSL 和核准者 (admin3) 各自的私有金鑰來簽署使用者服務的現在二進位規定人數未簽署的權杖，並建立二進位簽章檔案：

```
$ openssl pkeyutl -sign \
-inkey admin3.key \
-pkeyopt digest:sha256 \
-keyform PEM \
```

```
-in admin.bin \
-out admin.sig.bin
```

3. 將二進位簽章編碼為 base64：

```
$ base64 -w0 admin.sig.bin > admin.sig.b64
```

4. 最後，將 base64 編碼的簽名複製並粘貼到權杖檔案中，遵循先前為核准者簽名指定的 JSON 物件常值格式：

```
{
  "version": "2.0",
  "approval_data": "AAEAAwAAABgAAAAAAAAAAJ9eFkfcP3mNzJA1fK
+0WbNhZG1pbGAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABj5vbeAAAAAAAAAAAAAQADAAAFQAAAAAAAAAAW
v5Euk83amq1fij0zyvD2FkbWluAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGPm9t4AAAAAAAAAAAAABAAMAA
+b23gAAAAAAAA",
  "token": "012LZkmAHZyAc1hPhyck0oVW33aGrgG77qmDHWQ3CJ8=",
  "signatures": [
    {
      "username": "admin2",
      "role": "admin",
      "signature": "06qx7/mUaVkyYYVr1PW7l8JJko+Kh3e8zBIqdk3tAiNy+1rW
+0sDtvYujhEU4a0FVLcrUFmyB/CX90QmgJLgx/pyK+ZPEH+GoJGqk9YZ7X1n0XwZRP9g7hKV
+7XCtg9TuDFtHYWDpBfz2jWiu2fXfX4/
jTs4f2xIfFPIDKcSP8fhxjQ63xEcCf1jzGha6rDQMu4xUWwdtDgft7um7EJ9dXNoHqLB7cTzphaubNaEFbFPXQ1siGm
ssktwyruGFLpXs1n0tJ0EglGhx2qbYTs+omKWZd0R15WIWEXW3IXw/
Dg5vV0brNpvG0eZK08nSMc27+cyPySc+ZbNw=="
    },
    {
      "username": "admin3",
      "role": "admin",
      "signature": "06qx7/mUaVkyYYVr1PW7l8JJko+Kh3e8zBIqdk3tAiNy+1rW
+0sDtvYujhEU4a0FVLcrUFmyB/CX90QmgJLgx/pyK+ZPEH+GoJGqk9YZ7X1n0XwZRP9g7hKV
+7XCtg9TuDFtHYWDpBfz2jWiu2fXfX4/
jTs4f2xIfFPIDKcSP8fhxjQ63xEcCf1jzGha6rDQMu4xUWwdtDgft7um7EJ9dXNoHqLB7cTzphaubNaEFbFPXQ1siGm
ssktwyruGFLpXs1n0tJ0EglGhx2qbYTs+omKWZd0R15WIWEXW3IXw/
Dg5vV0brNpvG0eZK08nSMc27+cyPySc+ZbNw=="
    }
  ]
}
```

步驟 3. 核准 AWS CloudHSM 叢集上的權杖並執行使用者管理操作

管理員擁有必要的核准/簽名後 (詳見上一節)，管理員可以將該權杖提供給 AWS CloudHSM 叢集，以及下列其中一項使用者管理操作：

- [建立](#)
- [刪除](#)
- [變更密碼](#)
- [user change-mfa](#)

如需使用這些命令的詳細資訊，請參閱[使用 CloudHSM CLI 進行使用者管理](#)。

在交易期間，字符將在 AWS CloudHSM 叢集內核准，並執行請求的使用者管理操作。使用者管理操作的成功取決於有效的已核准規定人數權杖和有效的使用者管理操作。

管理員僅可以使用該權杖來進行一個操作。當該操作成功，該字符即不再有效。若要執行其他 HSM 使用者管理操作，管理員必須重複上述程序。即：管理員必須產生新的規定人數權杖、向核准者取得新簽章，在 HSM 上核准新權杖並執行要求的使用者管理操作。

Note

規定人數權杖僅在您目前的登入工作階段開啟時才有效。如果您登出 CloudHSM CLI 或網路中斷連線，則該權杖將不再有效。同樣地，授權的權杖只能在 CloudHSM CLI 中使用。其不能用於其他應用程式中進行身分驗證。

Example 以管理員身分建立新使用者

在下列範例命令中，登入的管理員會在 HSM 上建立新使用者。

```
aws-cloudhsm > user create --username user1 --role crypto-user --approval /path/
admin.token
Enter password:
Confirm password:
{
  "error_code": 0,
  "data": {
    "username": "user1",
    "role": "crypto-user"
  }
}
```

```
}
```

然後，管理員輸入 `user list` 命令以確認新使用者的建立：

```
aws-cloudhsm > user list
{
  "error_code": 0,
  "data": {
    "users": [
      {
        "username": "admin",
        "role": "admin",
        "locked": "false",
        "mfa": [],
        "quorum": [
          {
            "strategy": "token-sign",
            "status": "enabled"
          }
        ],
        "cluster-coverage": "full"
      },
      {
        "username": "admin2",
        "role": "admin",
        "locked": "false",
        "mfa": [],
        "quorum": [
          {
            "strategy": "token-sign",
            "status": "enabled"
          }
        ],
        "cluster-coverage": "full"
      },
      {
        "username": "admin3",
        "role": "admin",
        "locked": "false",
        "mfa": [],
        "quorum": [
          {
            "strategy": "token-sign",
```

```

        "status": "enabled"
      }
    ],
    "cluster-coverage": "full"
  },
  {
    "username": "admin4",
    "role": "admin",
    "locked": "false",
    "mfa": [],
    "quorum": [
      {
        "strategy": "token-sign",
        "status": "enabled"
      }
    ],
    "cluster-coverage": "full"
  },
  {
    "username": "user1",
    "role": "crypto-user",
    "locked": "false",
    "mfa": [],
    "quorum": [],
    "cluster-coverage": "full"
  },
  {
    "username": "app_user",
    "role": "internal(APPLIANCE_USER)",
    "locked": "false",
    "mfa": [],
    "quorum": [],
    "cluster-coverage": "full"
  }
]
}
}

```

如果管理員嘗試執行另一個 HSM 使用者管理操作，會因規定人數身分驗證錯誤而失敗，如以下範例所示。

```

aws-cloudhsm > user delete --username user1 --role crypto-user
{

```

```
"error_code": 1,  
"data": "Quorum approval is required for this operation"  
}
```

如下所示，`quorum token-sign list` 命令顯示管理員沒有核准的權杖。若要執行另一個 HSM 使用者管理操作，管理員必須產生新的規定人數權杖、向核准者取得新簽章，並使用核准引數執行所需的使用者管理操作，以提供要在執行使用者管理操作期間核准和使用的規定人數權杖。

```
aws-cloudhsm > quorum token-sign list  
{  
  "error_code": 0,  
  "data": {  
    "tokens": []  
  }  
}
```

變更使用 CloudHSM CLI 的 AWS CloudHSM 規定人數最小值

設定 CloudHSM [管理員的規定人數最小值](#) 之後，您可能需要調整規定人數最小值。HSM 只有在核准者數目符合或超過目前值時，才允許變更規定人數最小值。例如，如果規定人數最小值為兩 (2)，則至少兩 (2) 個管理員必須核准任何變更。

Note

使用者服務的規定人數值必須永遠小於規定人數服務的規定人數值。如需服務名稱的資訊，請參閱 [支援使用 CloudHSM CLI 進行規定人數身分驗證 AWS CloudHSM 的服務名稱和類型](#)。

若要取得規定人數核准來變更規定人數最小值，您需要規定人數權杖來用於使用 `quorum token-sign set-quorum-value` 命令的 `quorum service`。若要為使用 `quorum token-sign set-quorum-value` 命令的 `quorum service` 產生規定人數權杖，規定人數服務必須大於一 (1)。這表示您可能需要變更規定人數服務的規定人數最小值才能變更使用者服務的規定人數最小值。

變更管理員規定人數最小值的步驟

1. 啟動 CloudHSM CLI 互動式模式。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 CloudHSM CLI，以管理員身分登入。

```
aws-cloudhsm > login --username <admin> --role admin
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "<admin>",
    "role": "admin"
  }
}
```

3. 檢查目前的規定人數最小值：

```
aws-cloudhsm > quorum token-sign list-quorum-values
```

4. 如果規定人數服務的規定人數最小值低於使用者服務的值，請變更規定人數服務值：

```
aws-cloudhsm > quorum token-sign set-quorum-value --service quorum --value <3>
```

5. [產生規定人數服務的規定人數字符](#)。
6. [向其他管理員取得核准 \(簽章\)](#)。
7. 在 [CloudHSM 叢集上核准權杖](#)，並執行使用者管理操作。
8. 變更使用者服務的規定人數最小值：

```
aws-cloudhsm > quorum token-sign set-quorum-value
```

Example 調整規定人數服務最小值

1. 檢查目前值。此範例顯示使用者服務的規定人數最小值目前為兩 (2) 個。

```
aws-cloudhsm > quorum token-sign list-quorum-values
{
  "error_code": 0,
  "data": {
```



```
"user": 2,
"quorum": 1
}
}
```

2. 變更規定人數服務值。將規定人數服務的規定人數最小值設定為等於或高於使用者服務值的值。此範例將規定人數服務的規定人數最小值設定為兩個 (2)，與先前範例中為使用者服務設定的值相同。

```
aws-cloudhsm > quorum token-sign set-quorum-value --service quorum --value 2
{
  "error_code": 0,
  "data": "Set quorum value successful"
}
```

3. 驗證變更。此範例顯示，使用者服務和規定人數服務的規定人數最小值現在為兩 (2)。

```
aws-cloudhsm > quorum token-sign list-quorum-values
{
  "error_code": 0,
  "data": {
    "user": 2,
    "quorum": 2
  }
}
```

使用 CloudHSM 管理公用程式 (CMU) 進行 HSM 使用者管理

若要管理硬體安全模組 (HSM) 使用者 AWS CloudHSM，您必須使用[密碼編譯主管 \(CO\)](#) 的使用者名稱和密碼登入 HSM。只有 CO 可以管理使用者。HSM 包含名為 admin 的預設 CO。您可以在[啟用叢集](#)時設定 admin 管理員的密碼。

本主題提供使用 AWS CloudHSM Management Utility (CMU) 管理 HSM step-by-step 說明和詳細資訊。

主題

- [Management AWS CloudHSM Utility 中使用者管理的先決條件](#)
- [AWS CloudHSM Management Utility 的 HSM 使用者類型](#)
- [AWS CloudHSM Management Utility 的 HSM 使用者許可表](#)
- [使用 AWS CloudHSM Management Utility 建立 HSM 使用者](#)

- [使用 AWS CloudHSM Management Utility 列出叢集中的所有 HSM 使用者](#)
- [使用 AWS CloudHSM Management Utility 變更 HSM 使用者密碼](#)
- [使用 AWS CloudHSM Management Utility 刪除 HSM 使用者](#)
- [使用 Management Utility 為使用者 AWS CloudHSM 管理 2FA](#)
- [使用 CloudHSM 管理公用程式 \(CMU\) 管理規定人數身分驗證 \(M/N 個存取控制\)](#)

Management AWS CloudHSM Utility 中使用者管理的先決條件

在使用 AWS CloudHSM Management Utility (CMU) 在中管理硬體安全模組 (HSM) 使用者之前 AWS CloudHSM，您必須先完成這些先決條件。下列主題說明 CMU 入門。

章節

- [在中取得 HSM 的 IP 地址 AWS CloudHSM](#)
- [將 CMU 與用戶端 SDK 3.2.1 及更早版本搭配使用](#)
- [下載 CloudHSM 管理公用程式](#)

在中取得 HSM 的 IP 地址 AWS CloudHSM

如要使用 CMU，您必須使用設定工具來更新本機組態。CMU 會建立自己的與叢集的連接，且該連接不支援叢集。為追蹤叢集資訊，CMU 會維護本機組態檔案。這表示每次使用 CMU 時，您都應先透過執行帶有 `--cmu` 參數的[設定](#)命令列工具來更新組態檔案。如果您使用的是用戶端 SDK 3.2.1 或更早版本，則必須將 `--cmu` 換成其他參數。如需詳細資訊，請參閱 [the section called “將 CMU 與用戶端 SDK 3.2.1 及更早版本搭配使用”](#)。

`--cmu` 參數需要在叢集中新增 HSM 的 IP 地址。如果您有多個 HSM，則可以使用任何 IP 地址。這可確保 CMU 可在整個叢集中傳播您所做的任何變更。請記住，CMU 會使用其本機檔案來追蹤叢集資訊。如果自上次從特定主機使用 CMU 後叢集已發生變更，則必須將這些變更新增至儲存在該主機上的本機組態檔案中。使用 CMU 時，請勿新增或移除 HSM。

取得 HSM 的 IP 地址（主控台）

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 若要開啟叢集詳細資訊頁面，請在叢集表格中選擇叢集 ID。
4. 若要取得 IP 地址，請前往 HSMs 索引標籤。對於 IPv4 叢集，請選擇 ENI IPv4 地址下列出的地址。對於雙堆疊叢集，請使用 ENI IPv4 或 ENI IPv6 地址。

取得 HSM 的 IP 地址 (AWS CLI)

- 使用 AWS CLI 中的 [describe-clusters](#) 命令取得 HSM 的 IP 地址。在 命令的輸出中，HSMs 的 IP 地址是 `EniIp` 和 的值 `EniIPv6` (如果是雙堆疊叢集)。

```
$ aws cloudhsmv2 describe-clusters
{
  "Clusters": [
    { ... }
    "Hsms": [
      {
...
        "EniIp": "10.0.0.9",
...
      },
      {
...
        "EniIp": "10.0.1.6",
        "EniIPv6": "2600:113f:404:be09:310e:ed34:3412:f733",
...
      }
    ]
  }
}
```

將 CMU 與用戶端 SDK 3.2.1 及更早版本搭配使用

透過用戶端 SDK 3.3.0，AWS CloudHSM 新增了對 `--cmu` 參數的支援，可簡化更新 CMU 組態檔案的程序。如果您使用的是用戶端 SDK 3.2.1 或更早版本的 CMU，您必須繼續使用 `-a` 和 `-m` 參數來更新組態檔案。如需這些參數的詳細資訊，請參閱[設定工具](#)。

下載 CloudHSM 管理公用程式

無論您使用的是用戶端 SDK 5 還是用戶端 SDK 3，HSM 使用者管理任務均可使用最新版本的 CMU。

如要下載並安裝 CMU

- 下載並安裝 CMU。

Amazon Linux

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-
mgmt-util-latest.el6.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-mgmt-util-latest.el6.x86_64.rpm
```

Amazon Linux 2

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-mgmt-util-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-mgmt-util-latest.el7.x86_64.rpm
```

CentOS 7.8+

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-mgmt-util-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-mgmt-util-latest.el7.x86_64.rpm
```

CentOS 8.3+

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-mgmt-util-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-mgmt-util-latest.el8.x86_64.rpm
```

RHEL 7 (7.8+)

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-mgmt-util-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-mgmt-util-latest.el7.x86_64.rpm
```

RHEL 8 (8.3+)

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-mgmt-util-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-mgmt-util-latest.el8.x86_64.rpm
```

Ubuntu 16.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-mgmt-util_latest_amd64.deb
```

```
$ sudo apt install ./cloudhsm-mgmt-util_latest_amd64.deb
```

Ubuntu 18.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Bionic/cloudhsm-mgmt-util_latest_u18.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-mgmt-util_latest_u18.04_amd64.deb
```

Windows Server 2012

1. 下載 [CloudHSM 管理公用程式](#)。
2. 以 Windows 管理權限執行 CMU 安裝程式 (AWSCloudHSMMManagementUtil-latest.msi)。

Windows Server 2012 R2

1. 下載 [CloudHSM 管理公用程式](#)。
2. 以 Windows 管理權限執行 CMU 安裝程式 (AWSCloudHSMMManagementUtil-latest.msi)。

Windows Server 2016

1. 下載 [CloudHSM 管理公用程式](#)。
2. 以 Windows 管理權限執行 CMU 安裝程式 (AWSCloudHSMMManagementUtil-latest.msi)。

AWS CloudHSM Management Utility 的 HSM 使用者類型

您在硬體安全模組 (HSM) 上執行的大多數操作都需要 AWS CloudHSM anHSM 使用者的登入資料。HSM 會驗證每個 HSM 使用者，且每個 HSM 使用者都有一種類型，決定您可以該使用者身分在 HSM 上執行哪些操作。

Note

HSM 使用者與 IAM 使用者不同。擁有正確憑證的 IAM 使用者可利用 AWS API 與資源進行互動來建立 HSM。HSM 建立後，您必須使用 HSM 使用者憑證來驗證 HSM 上的操作。

使用者類型

- [準加密員 \(PRECO\)](#)
- [加密管理員 \(CO\)](#)
- [加密使用者 \(CU\)](#)
- [設備使用者 \(AU\)](#)

準加密員 (PRECO)

在雲端管理公用程式 (CMU) 和金鑰管理公用程式 (KMU) 中，PRECO 是暫時使用者，僅存在於 AWS CloudHSM 叢集中的第一個 HSM 上。新叢集中的第一個 HSM 包含一個 PRECO 使用者，這表示此叢集尚未啟用。若要[啟用叢集](#)，請執行 cloudhsm-cli 並執行 cluster activate 命令。登入 HSM 並變更 PRECO 的密碼。當您變更密碼時，此使用者會變成加密管理員 (CO)。

加密管理員 (CO)

在雲端管理公用程式 (CMU) 和金鑰管理公用程式 (KMU) 中，加密管理員 (CO) 可以執行使用者管理操作。例如，管理員可以建立和刪除使用者，也可以變更使用者密碼。如需有關加密使用者的詳細資訊，請參閱 [AWS CloudHSM Management Utility 的 HSM 使用者許可表](#)。當您啟用新叢集時，使用者會由[準加密員](#) (PRECO) 變成加密管理員 (CO)。-->

加密使用者 (CU)

加密使用者 (CU) 可以執行以下的金鑰管理和密碼編譯操作。

- 金鑰管理：建立、刪除、共用、匯入和匯出密碼編譯金鑰。
- 密碼編譯操作：使用密碼編譯金鑰進行加密、解密、簽署、驗證及其他操作。

如需更多資訊，請參閱[AWS CloudHSM Management Utility 的 HSM 使用者許可表](#)。

設備使用者 (AU)

設備使用者 (AU) 可以在叢集的 HSMs 上執行複製和同步操作。AWS CloudHSM 會使用 AU 來同步 AWS CloudHSM 叢集中的 HSMs。AU 存在於 提供的所有 HSMs 上 AWS CloudHSM，並且具有有限的許可。如需更多資訊，請參閱[AWS CloudHSM Management Utility 的 HSM 使用者許可表](#)。

AWS 無法在 HSMs 上執行任何操作。AWS 無法檢視或修改您的使用者或金鑰，也無法使用這些金鑰執行任何密碼編譯操作。

AWS CloudHSM Management Utility 的 HSM 使用者許可表

下表列出硬體安全模組 (HSM) 操作依可在其中執行操作的 HSM 使用者或工作階段類型排序 AWS CloudHSM。

	加密管理員 (CO)	加密使用者 (CU)	設備使用者 (AU)	已驗證的工作階段
取得基本叢集資訊 ¹	 是	 是	 是	 是
變更自己的密碼	 是	 是	 是	不適用
變更任何使用者的密碼	 是	 否	 否	 否
新增、移除使用者	 是	 否	 否	 否

	加密管理員 (CO)	加密使用者 (CU)	設備使用者 (AU)	已驗證的工作階段
取得同步狀態 ²	 是	 是	 是	 否
擷取、插入遮罩物件 ³	 是	 是	 是	 否
金鑰管理功能 ⁴	 否	 是	 否	 否
加密、解密	 否	 是	 否	 否
簽署、驗證	 否	 是	 否	 否
產生摘要和 HMAC	 否	 是	 否	 否

- [1] 基本叢集資訊包括叢集的 HSM 數目，以及每個 HSM 的 IP 地址、型號、序號、裝置 ID、韌體 ID 等。

- [2] 使用者可以取得一組摘要 (雜湊)，這組摘要會對應到 HSM 上的金鑰。應用程式可以比較這幾組摘要，以了解叢集中的 HSM 的同步狀態。
- [3] 遮罩物件就是在離開 HSM 之前加密的金鑰。這些金鑰無法在 HSM 外部解密。將金鑰插入 HSM，而且此 HSM 與先前從中擷取金鑰的 HSM 必須在同一個叢集，金鑰才會解密。應用程式可以擷取和插入遮罩物件，以同步叢集的 HSM。
- [4] 金鑰管理功能包括建立、刪除、包裝、取消包裝及修改金鑰的屬性。

使用 AWS CloudHSM Management Utility 建立 HSM 使用者

在 AWS CloudHSM Management Utility (CMU) createUser 中使用 在硬體安全模組 (HSM) 上建立新的使用者。您必須以 CO 的身份登入才能建立使用者。

如要建立新的 CO 使用者

1. 使用設定工具來更新 CMU 組態。

Linux

```
$ sudo /opt/cloudhsm/bin/configure --cmu <IP address>
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" --cmu <IP address>
```

2. 啟動 CMU。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cloudhsm_mgmt_util.exe" C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_mgmt_util.cfg
```

3. 以 CO 使用者身分登入 HSM。

```
aws-cloudhsm > loginHSM CO admin co12345
```

請確定連線 CMU 清單的數目與叢集中的 HSM 數目相符。如不符，請登出並重新啟動。

4. 使用 `createUser` 來建立名為 **example_officer** 的 CO 使用者，密碼為 **password1**。

```
aws-cloudhsm > createUser CO example_officer password1
```

CMU 會提示您建立使用者操作。

```
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
*****

Do you want to continue(y/n)?
```

5. 輸入 **y**。

如要建立新的 CU 使用者

1. 使用設定工具來更新 CMU 組態。

Linux

```
$ sudo /opt/cloudhsm/bin/configure --cmu <IP address>
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" --cmu <IP address>
```

2. 啟動 CMU。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cloudhsm_mgmt_util.exe" C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_mgmt_util.cfg
```

3. 以 CO 使用者身分登入 HSM。

```
aws-cloudhsm > loginHSM CO admin co12345
```

請確定連線 CMU 清單的數目與叢集中的 HSM 數目相符。如不符，請登出並重新啟動。

4. 使用 `createUser` 來建立名為 **example_user** 的 CU 使用者，密碼為 **password1**。

```
aws-cloudhsm > createUser CU example_user password1
```

CMU 會提示您建立使用者操作。

```
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
*****
Do you want to continue(y/n)?
```

5. 輸入 **y**。

如需 `createUser` 的詳細資訊，請參閱 [createUser](#)。

使用 AWS CloudHSM Management Utility 列出叢集中的所有 HSM 使用者

在 AWS CloudHSM Management Utility (CMU) 中使用 `listUsers` 命令來列出 AWS CloudHSM 叢集中的所有使用者。您無需登入即可執行 `listUsers` 且所有使用者類型都可以列出使用者。

如要列出叢集中的所有使用者

1. 使用設定工具來更新 CMU 組態。

Linux

```
$ sudo /opt/cloudhsm/bin/configure --cmu <IP address>
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" --cmu <IP address>
```

2. 啟動 CMU。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cloudhsm_mgmt_util.exe" C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_mgmt_util.cfg
```

3. 用 listUsers 來列出叢集上的所有使用者。

```
aws-cloudhsm > listUsers
```

CMU 列出了叢集上的所有使用者。

Users on server 0(10.0.2.9):

Number of users found:4

User Id	User Type	User Name	
MofnPubKey	LoginFailureCnt	2FA	
1	AU	app_user	NO
	0		NO
2	CO	example_officer	NO
	0		NO
3	CU	example_user	NO
	0		NO

Users on server 1(10.0.3.11):

Number of users found:4

User Id	User Type	User Name	
MofnPubKey	LoginFailureCnt	2FA	
1	AU	app_user	N0
	0		N0
2	CO	example_officer	N0
	0		N0
3	CU	example_user	N0
	0		N0
Users on server 2(10.0.1.12):			
Number of users found:4			
User Id	User Type	User Name	
MofnPubKey	LoginFailureCnt	2FA	
1	AU	app_user	N0
	0		N0
2	CO	example_officer	N0
	0		N0
3	CU	example_user	N0
	0		N0

如需 listUsers 的詳細資訊，請參閱 [listUsers](#)。

使用 AWS CloudHSM Management Utility 變更 HSM 使用者密碼

在 AWS CloudHSM Management Utility (CMU) changePswd 中使用 變更硬體安全模組 (HSM) 使用者的密碼。

使用者類型和密碼需區分大小寫，但使用者名稱不區分大小寫。

管理員、加密使用者 (CU) 和設備使用者 (AU) 只能變更自己的密碼。若要變更其他使用者的密碼，您必須以 CO 身分登入。您無法變更目前已登入使用者的密碼。

如要變更您自己的密碼

1. 使用設定工具來更新 CMU 組態。

Linux

```
$ sudo /opt/cloudhsm/bin/configure --cmu <IP address>
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" --cmu <IP address>
```

2. 啟動 CMU。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cloudhsm_mgmt_util.exe" C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_mgmt_util.cfg
```

3. 登入 HSM。

```
aws-cloudhsm > loginHSM C0 admin co12345
```

請確定連線 CMU 清單的數目與叢集中的 HSM 數目相符。如不符，請登出並重新啟動。

4. 使用 changePswd 變更您自己的密碼。

```
aws-cloudhsm > changePswd C0 example_officer <new password>
```

CMU 會提示您變更密碼的操作。

```
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
*****

Do you want to continue(y/n)?
```

5. 輸入 y。

CMU 會提示您變更密碼的操作。

```
Changing password for example_officer(C0) on 3 nodes
```

如要變更其他使用者的密碼

1. 使用設定工具來更新 CMU 組態。

Linux

```
$ sudo /opt/cloudhsm/bin/configure --cmu <IP address>
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" --cmu <IP address>
```

2. 啟動 CMU。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cloudhsm_mgmt_util.exe" C:\  
\ProgramData\Amazon\CloudHSM\data\cloudhsm_mgmt_util.cfg
```

3. 以 CO 使用者身分登入 HSM。

```
aws-cloudhsm > loginHSM C0 admin co12345
```

請確定連線 CMU 清單的數目與叢集中的 HSM 數目相符。如不符，請登出並重新啟動。

4. 使用 changePswd 變更其他使用者的密碼。

```
aws-cloudhsm > changePswd CU example_user <new password>
```

CMU 會提示您變更密碼的操作。

```
*****CAUTION*****
```

```
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
*****
```

```
Do you want to continue(y/n)?
```

5. 輸入 **y**。

CMU 會提示您變更密碼的操作。

```
Changing password for example_user(CU) on 3 nodes
```

如需 changePswd 的詳細資訊，請參閱 [changePswd](#)。

使用 AWS CloudHSM Management Utility 刪除 HSM 使用者

在 AWS CloudHSM Management Utility (CMU) deleteUser 中使用 刪除硬體安全模組 (HSM) 使用者。您必須以 CO 身分登入才能刪除其他使用者。



Tip

您無法刪除擁有金鑰的加密使用者 (CU)。

如要刪除使用者

1. 使用設定工具來更新 CMU 組態。

Linux

```
$ sudo /opt/cloudhsm/bin/configure --cmu <IP address>
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" --cmu <IP address>
```

2. 啟動 CMU。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cloudhsm_mgmt_util.exe" C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_mgmt_util.cfg
```

3. 以 CO 使用者身分登入 HSM。

```
aws-cloudhsm > loginHSM C0 admin co12345
```

請確定連線 CMU 清單的數目與叢集中的 HSM 數目相符。如不符，請登出並重新啟動。

4. 使用 deleteUser 刪除使用者。

```
aws-cloudhsm > deleteUser C0 example_officer
```

CMU 會刪除使用者。

```
Deleting user example_officer(C0) on 3 nodes
deleteUser success on server 0(10.0.2.9)
deleteUser success on server 1(10.0.3.11)
deleteUser success on server 2(10.0.1.12)
```

如需 deleteUser 的詳細資訊，請參閱 [deleteUser](#)。

使用 Management Utility 為使用者 AWS CloudHSM 管理 2FA

為了提高安全性，您可以設定雙重驗證 (2FA)，以協助保護 AWS CloudHSM 叢集。您只能為加密管理員 (CO) 啟用 2FA。

當您以啟用 2FA 的硬體服務模組 (HSM) 帳戶登入叢集時，您需向 cloudhsm_mgmt_util (CMU) 提供您的密碼 (第一個要素，這是您已知的內容)，然後 CMU 會提供給您一個權杖並提示您簽署該權杖。如要提供第二個要素 (您擁有的)，請使用您已經建立並與 HSM 使用者相關聯的金鑰對中的私有金鑰來簽署權杖。如要訪問叢集，請將已簽署的權杖提供給 CMU。

 Note

您無法為加密使用者 (CU) 或應用程式啟用 2FA。雙重要素驗證 (2FA) 僅適用於 CO 使用者。

主題

- [使用 AWS CloudHSM Management Utility 的 AWS CloudHSM 叢集中的配額身分驗證和 2FA](#)
- [AWS CloudHSM 使用 AWS CloudHSM Management Utility 的 2FA 金鑰對需求](#)
- [為 AWS CloudHSM Management Utility 使用者建立已啟用 2FA 的使用者](#)
- [使用 Management Utility 管理 HSM 使用者的 AWS CloudHSM 2FA](#)
- [使用 AWS CloudHSM Management Utility 停用 HSM 使用者的 2FA](#)
- [使用 AWS CloudHSM Management Utility 的 2FA 組態參考](#)

使用 AWS CloudHSM Management Utility 的 AWS CloudHSM 叢集中的配額身分驗證和 2FA

叢集對規定人數身分驗證和雙重身分驗證 2FA 使用相同的金鑰)。這意味著啟用了 2FA 的使用者可以有效地註冊了 M-of-N-access-control (MofN)。如要為同一 HSM 使用者成功使用 2FA 和規定人數驗證，請考慮下列幾點：

- 如果您今天要為使用者使用規定人數驗證，則應使用您為規定人數使用者建立的同一個金鑰對來為該使用者啟用 2FA。
- 如果您為非規定人數驗證使用者身分的非 2FA 使用者新增 2FA 要求，則您應將該使用者註冊為具有 2FA 驗證的 MofN 使用者。
- 如果您要為兼具規定人數驗證使用者身分的 2FA 使用者移除 2FA 要求或變更其密碼，您也會同時移除規定人數使用者作為 MofN 使用者的註冊。
- 如果您要為兼具規定人數驗證使用者身分的 2FA 使用者移除 2FA 要求或變更其密碼，但仍想保留該使用者的規定人數驗證，則您須將該使用者註冊為 MofN 使用者。

如需規定人數驗證的詳細資訊，請參閱 [使用 CMU 管理規定人數身分驗證](#)。

AWS CloudHSM 使用 AWS CloudHSM Management Utility 的 2FA 金鑰對需求

若要為 AWS CloudHSM 硬體安全模組 (HSM) 使用者啟用雙重驗證 (2FA)，請使用符合下列需求的金鑰。

您可建立新的金鑰對，或使用符合下列要求的現有金鑰。

- 金鑰類型：非對稱金鑰
- 金鑰用途：簽署和驗證
- 金鑰規格：RSA_2048
- 簽署演算法包括：
 - sha256WithRSAEncryption

Note

如果您正在使用規定人數驗證或計劃使用法定驗證，請參閱 [the section called “配額身分驗證”](#)。

為 AWS CloudHSM Management Utility 使用者建立已啟用 2FA 的使用者

使用 AWS CloudHSM Management Utility CMU (CMU) 和金鑰對來建立新的加密辦公室 (CO) 使用者，並啟用雙重驗證 (2FA)。

如建立已啟用 2FA 的 CO 使用者

1. 如在一個終端中，請執行下列步驟：
 - a. 訪問您的 HSM 並登入 CloudHSM 管理公用程式：

```
/opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

- b. 以 CO 身分登入，並使用下列命令建立含有 2FA 的新使用者 MFA：

```
aws-cloudhsm > createUser CO MFA <CO USER NAME> -2fa /home/ec2-user/authdata
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
*****

Do you want to continue(y/n)? y
```

Creating User exampleuser3(C0) on 1 nodesAuthentication data written to: "/home/ec2-user/authdata"Generate Base64-encoded signatures for SHA256 digests in the authentication datafile.

To generate the signatures, use the RSA private key, which is the second factor ofauthentication for this user. Paste the signatures and the corresponding public keyinto the authentication data file and provide the file path below.Leave this field blank to use the path initially provided.Enter filename:

c. 將上述終端保留在此狀態。請勿按回車鍵或輸入任何檔案名稱。

2. 如在其他終端中，請執行下列步驟：

a. 訪問您的 HSM 並登入 CloudHSM 管理公用程式：

```
/opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

b. 使用下列指令產生公有/私有金鑰對：

```
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt  
rsa_keygen_bits:2048
```

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

c. 執行下列命令以安裝 Json 查詢功能，以便從 AuthData 檔案中擷取摘要：

```
sudo yum install jq
```

d. 如要擷取摘要值，請先在 AuthData 檔案中尋找下列資料：

```
{  
  "Version": "1.0",  
  "PublicKey": "",  
  "Data": [  
    {  
      "HsmId": <"HSM ID">,  
      "Digest": <"DIGEST">,  
      "Signature": ""  
    }  
  ]  
}
```

Note

已獲得的摘要要是 base64 編碼的，但如要簽署該摘要，您需要先解碼該文件，然後簽署該文件。以下命令將解碼摘要並將解碼的內容存儲在「digest1.bin」中。

```
cat authdata | jq '.Data[0].Digest' | cut -c2- | rev | cut -c2- | rev |
base64 -d > digest1.bin
```

- e. 如要轉換公用金鑰的內容，請添加「\n」並刪除空格，如下所示：

```
-----BEGIN PUBLIC KEY-----\n<PUBLIC KEY>\n-----END PUBLIC KEY-----
```

Important

以上命令顯示如何在 BEGIN PUBLIC KEY----- 後立即添加「\n」，如何刪除「\n」和公用金鑰第一個字元之間的空格，如何在 -----END PUBLIC KEY 之前添加「\n」，以及如何刪除「\n」和公用金鑰結尾的空格。

這是在 AuthData 文件中已接受的公用金鑰的 PEM 格式。

- f. 將公有金鑰 PEM 格式的內容粘貼到 AuthData 文件的公用金鑰部分。

```
vi authdata
```

```
{
  "Version": "1.0",
  "PublicKey": "-----BEGIN PUBLIC KEY-----\n<"PUBLIC KEY">\n-----END PUBLIC
KEY-----",
  "Data": [
    {
      "HsmId": "<"HSM ID">",
      "Digest": "<"DIGEST">",
      "Signature": ""
    }
  ]
}
```

- g. 請使用下列指令簽署權杖：

```
openssl pkeyutl -sign -in digest1.bin -inkey private_key.pem -pkeyopt
digest:sha256 | base64
```

Output Expected:

```
<"THE SIGNATURE">
```

Note

如以上命令所示，請改用 `openssl pkeyutl` 而不是 `openssl dgst` 來簽署。

- h. 在「簽名」欄位的 AuthData File 中新增已簽署的摘要。

```
vi authdata
```

```
{
  "Version": "1.0",
  "PublicKey": "-----BEGIN PUBLIC KEY----- ... -----END PUBLIC KEY-----",
  "Data": [
    {
      "HsmId": <"HSM ID">,
      "Digest": <"DIGEST">,
      "Signature": <"Kkd1 ... rkrvJ6Q==">
    },
    {
      "HsmId": <"HSM ID">,
      "Digest": <"DIGEST">,
      "Signature": <"K1hxy ... Q261Q==">
    }
  ]
}
```

3. 返回到第一個終端，然後按 **Enter**：

Generate Base64-encoded signatures for SHA256 digests in the authentication datafile. To generate the signatures, use the RSA private key, which is the second factor of authentication for this user. Paste the signatures and the corresponding public key into the authentication data file and provide the file path below. Leave this field blank to use the path initially provided.

Enter filename: >>>> Press Enter here

```
createUser success on server 0(10.0.1.11)
```

使用 Management Utility 管理 HSM 使用者的 AWS CloudHSM 2FA

在 AWS CloudHSM Management Utility (CMU) `changePswd` 中使用 來修改使用者的雙重驗證 (2FA)。每次啟用 2FA 時，您都必須提供 2FA 登入的公用金鑰。

`changePswd` 會執行下列任一案例：

- 變更 2FA 使用者的密碼
- 變更 2FA 使用者的密碼
- 為非 2FA 使用者新增 2FA
- 移除 2FA 使用者的 2FA
- 輪換 2FA 使用者的金鑰

您也可以合併任務。例如，您可以移除使用者的 2FA 並同時變更密碼，或輪換 2FA 金鑰並變更使用者密碼。

如要為已啟用 2FA 的 CO 使用者變更密碼或輪換金鑰

1. 使用 CMU 以已啟用 2FA 的 CO 身分登入 HSM。
2. 用 `changePswd` 變更密碼或向已啟用 2FA 的 CO 使用者輪換金鑰。使用 `-2fa` 參數並在檔案系統中指定一個位置，以便系統寫入 `authdata` 檔案。此檔案包含叢集中每個 HSM 的摘要。

```
aws-cloudhsm > changePswd CO example-user <new-password> -2fa /path/to/authdata
```

CMU 會提示您使用私有金鑰簽署 `authdata` 檔案中的摘要，並傳回含有公有金鑰的簽章。

3. 使用私有金鑰簽署 `authdata` 檔案中的摘要、將簽章和公有金鑰新增至 JSON 格式的 `authdata` 檔案，然後將 `authdata` 檔案位置提供給 CMU。如需詳細資訊，請參閱 [the section called “組態參考”](#)。

Note

叢集使用同一金鑰進行規定人數驗證和雙重要素驗證 (2FA)。如果您正在使用規定人數驗證或計劃使用法定驗證，請參閱 [the section called “配額身分驗證”](#)。

使用 AWS CloudHSM Management Utility 停用 HSM 使用者的 2FA

使用 AWS CloudHSM Management Utility (CMU) 來停用硬體安全模組 HSM 使用者的雙重驗證 (2FA) AWS CloudHSM。

如要為已啟用 2FA 的 CO 使用者停用 2FA

1. 使用 CMU 以已啟用 2FA 的 CO 身分登入 HSM。
2. 使用 `changePswd` 從已啟用 2FA 的 CO 使用者中移除 2FA。

```
aws-cloudhsm > changePswd CO example-user <new password>
```

CMU 會提示您確認變更密碼操作。

Note

如果您要為兼具規定人數驗證使用者身分的 2FA 使用者移除 2FA 要求或變更其密碼，您也會同時移除規定人數使用者作為 MofN 使用者的註冊。如需規定人數使用者和 2FA 的詳細資訊，請參閱 [the section called “配額身分驗證”](#)。

3. 輸入 `y`。

CMU 會確認變更密碼操作。

使用 AWS CloudHSM Management Utility 的 2FA 組態參考

以下是 AWS CloudHSM Management Utility (CMU) 產生的請求和您的回應在 `authdata` 檔案中的雙重驗證 (2FA) 屬性範例。

```
{
  "Version": "1.0",
  "PublicKey": "-----BEGIN PUBLIC KEY----- ... -----END PUBLIC KEY-----",
  "Data": [
    {
      "HsmId": "hsm-lgavqitns2a",
      "Digest": "k501p3f6foQRVQH7S8Rrjcau6h3TYqsSdr16A54+qG8=",
      "Signature": "Kkd1 ... rkrvJ6Q=="
    },
    {
      "HsmId": "hsm-lgavqitns2a",
```



```

        "Digest": "IyBcx4I5Vyx1jztwvXinCBQd9lDx8oQe7iRrWjBAi1w=",
        "Signature": "K1hxy ... Q261Q=="
    }
]
}

```

資料

頂層節點。包含叢集中每個 HSM 的次級節點。出現在所有 2FA 命令的請求和回應中。

摘要

這是您必須簽署後才能提供驗證的第二個要素。在所有 2FA 命令請求中產生 CMU。

HsmId

您 HSM 的識別碼。出現在所有 2FA 命令的請求和回應中。

PublicKey

您所產生金鑰對的公開金鑰部分會作為 PEM 格式字串插入。您要在 createUser 和 changePswd 的回應中輸入此內容。

Signature

Base 64 編碼的已簽署摘要。您要在所有 2FA 回應中輸入此內容。

版本

驗證資料的格式為 JSON 格式檔案。出現在所有 2FA 命令的請求和回應中。

使用 CloudHSM 管理公用程式 (CMU) 管理規定人數身分驗證 (M/N 個存取控制)

AWS CloudHSM 叢集中的 HSMs 支援規定人數身分驗證，也稱為 M of N 存取控制。有了規定人數身分驗證，HSM 上沒有任何單一使用者可以在 HSM 上執行由規定人數控制的操作。相對地，必須有最低數量的 HSM 使用者 (至少 2 個) 合作來執行這些操作。有了規定人數身分驗證，您可以透過要求來自一個以上 HSM 使用者的核准來新增一層額外的保護。

規定人數身分驗證可以控制以下操作：

- 由[加密管理員 \(CO\)](#)管理的 HSM 使用者：會建立和刪除 HSM 使用者，以及變更不同 HSM 使用者的密碼。如需詳細資訊，請參閱[針對 Management Utility 啟用規定人數身分驗證的使用者 AWS CloudHSM 管理](#)。

請注意關於在 AWS CloudHSM 中使用規定人數身分驗證的下列額外資訊。

- HSM 使用者可以簽署自己的規定人數權杖，即：要求的使用者可以針對規定人數身分驗證提供其中一個需要的核准。
- 您可以針對由規定人數控制的操作選擇最低數量的規定人數核准者。您可以選擇的最小數字是二 (2)，您可以選擇的最大數字是八 (8)。
- HSM 最多可存放最多 1024 個規定人數字符。當您嘗試建立新的字符時，如果 HSM 已經有 1024 個字符，HSM 會清除其中一個過期的字符。在預設情況下，字符會在建立後的十分鐘後過期。
- 叢集使用相同的金鑰進行規定人數身分驗證和雙重要素驗證 (2FA)。如需關於使用規定人數身分驗證和 2FA 的詳細資訊，請參閱[規定人數身分驗證和 2FA](#)。

下列主題提供 AWS CloudHSM 中的規定人數身分驗證的詳細資訊。

主題

- [AWS CloudHSM Management Utility 的配額身分驗證程序](#)
- [為 AWS CloudHSM 加密主管設定規定人數身分驗證](#)
- [針對 Management Utility 啟用規定人數身分驗證的使用者 AWS CloudHSM 管理](#)
- [使用 AWS CloudHSM Management Utility 變更規定人數最小值](#)

AWS CloudHSM Management Utility 的配額身分驗證程序

下列步驟彙總規定人數身分驗證程序。如需特定步驟和工具，請參閱[針對 Management Utility 啟用規定人數身分驗證的使用者 AWS CloudHSM 管理](#)。

1. 每個 HSM 使用者會建立非對稱金鑰供簽署使用。使用者會在 HSM 外部執行此動作，以適當方式保護金鑰。
2. 每個 HSM 使用者會登入 HSM，並向 HSM 註冊使用者的簽署金鑰 (公有金鑰) 的公有部分。
3. HSM 使用者想要執行由規定人數控制的操作時，每個使用者會登入 HSM，並取得規定人數權杖。
4. HSM 使用者會將規定人數字符提供給一或多個其他 HSM 使用者，並要求其核准。
5. 其他 HSM 使用者透過使用自己的金鑰以密碼編譯方式簽署規定人數字符來進行核准。這是在 HSM 外部進行。
6. 當 HSM 使用者擁有需要的核准數量時，相同的使用者會登入 HSM，並向 HSM 提供規定人數權杖和核准 (簽章)。
7. HSM 會使用每個簽署者註冊的公有金鑰來驗證簽章。如果簽章有效，HSM 會核准字符。

8. HSM 使用者現在可以執行由規定人數控制的操作。

為 AWS CloudHSM 加密主管設定規定人數身分驗證

下列主題說明您必須完成的步驟，才能設定硬體安全模組 (HSM)，以便 AWS CloudHSM [加密主管 \(COs\)](#) 可以使用規定人數身分驗證。第一次針對 CO 設定規定人數身分驗證時，您只需要執行一次下列步驟。完成這些步驟之後，請參閱 [針對 Management Utility 啟用規定人數身分驗證的使用者 AWS CloudHSM 管理](#)。

主題

- [先決條件](#)
- [步驟 1. 建立和註冊用於簽署的金鑰](#)
- [步驟 2. 設定 HSM 上的規定人數最小值](#)

先決條件

若要了解此範例，您應熟悉 [cloudhsm_mgmt_util \(CMU\) 命令列工具](#)。在此範例中，AWS CloudHSM 叢集有兩個 HSMs，每個都有相同的 COs，如 listUsers 命令的下列輸出所示。如需有關建立使用者的詳細資訊，請參閱 [HSM 使用者](#)。

```
aws-cloudhsm > listUsers
```

```
Users on server 0(10.0.2.14):
```

```
Number of users found:7
```

User Id	User Type	User Name	MofnPubKey
LoginFailureCnt	2FA		
1	PRECO	admin	N0
0	N0		
2	AU	app_user	N0
0	N0		
3	CO	officer1	N0
0	N0		
4	CO	officer2	N0
0	N0		
5	CO	officer3	N0
0	N0		
6	CO	officer4	N0
0	N0		
7	CO	officer5	N0
0	N0		

Users on server 1(10.0.1.4):

Number of users found:7

User Id	User Type	User Name	MofnPubKey
LoginFailureCnt	2FA		
1	PRECO	admin	NO
0	NO		
2	AU	app_user	NO
0	NO		
3	CO	officer1	NO
0	NO		
4	CO	officer2	NO
0	NO		
5	CO	officer3	NO
0	NO		
6	CO	officer4	NO
0	NO		
7	CO	officer5	NO
0	NO		

步驟 1. 建立和註冊用於簽署的金鑰

若要使用規定人數身分驗證，每個管理員都必須執行下列所有步驟：

主題

- [建立 RSA 金鑰對](#)
- [建立並簽署註冊權杖](#)
- [用 HSM 註冊公有金鑰](#)

建立 RSA 金鑰對

建立和保護金鑰對有許多不同的方式。下列範例示範使用 [OpenSSL](#) 的做法。

Example – 使用 OpenSSL 建立私有金鑰

以下範例示範如何使用 OpenSSL 來建立受到密碼短語保護的 2048 位元 RSA 金鑰。若要使用這個範例，請將 *officer1.key* 以您要存放金鑰的檔案名稱來加以取代。

```
$ openssl genrsa -out <officer1.key> -aes256 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.+++
```

```
e is 65537 (0x10001)
Enter pass phrase for officer1.key:
Verifying - Enter pass phrase for officer1.key:
```

接下來，使用您剛建立的私有金鑰來產生公有金鑰。

Example – 使用 OpenSSL 建立一個公有金鑰

下列範例會示範如何使用 OpenSSL 根據您剛建立的私有金鑰建立公有金鑰。

```
$ openssl rsa -in officer1.key -outform PEM -pubout -out officer1.pub
Enter pass phrase for officer1.key:
writing RSA key
```

建立並簽署註冊權杖

您可以建立一個權杖並使用在上一步中剛產生的私有金鑰簽署該權杖。

Example – 建立權杖

註冊權杖只是一個最大不超過 245 位元組的任何隨機資料的檔案。您可以使用私有金鑰簽署權杖，以證明您可以訪問私有金鑰。下列命令使用 echo 將字串重新導向到一個檔案。

```
$ echo <token to be signed> > officer1.token
```

簽署權杖並將其儲存至簽章檔案。您需要已簽署的權杖、未簽署的權杖和公有金鑰，才能在 HSM 中將 CO 註冊為 MofN 使用者。

Example – 簽署權杖

使用 OpenSSL 和私有金鑰來簽署註冊權杖並建立簽章檔案。

```
$ openssl dgst -sha256 \
    -sign officer1.key \
    -out officer1.token.sig officer1.token
```

用 HSM 註冊公有金鑰

建立金鑰之後，CO 必須向 HSM 註冊金鑰的公有部分 (公有金鑰)。

向 HSM 註冊公有金鑰

1. 使用下列命令來啟動 cloudhsm_mgmt_util 命令列工具。

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

2. 使用 loginHSM 命令以 CO 身分登入 HSM。如需詳細資訊，請參閱 [???](#)。
3. 使用 [registerQuorumPubKey](#) 命令來註冊公有金鑰。如需詳細資訊，請參閱下列範例或使用 help registerQuorumPubKey 命令。

Example – 向 HSM 註冊公有金鑰

下列範例顯示如何在 cloudhsm_mgmt_util 命令列工具中使用 registerQuorumPubKey 命令，以向 HSM 註冊 CO 的公有金鑰。若要使用此命令，CO 必須登入 HSM。以您自己的值取代這些值：

```
aws-cloudhsm > registerQuorumPubKey
CO <officer1> <officer1.token> <officer1.token.sig> <officer1.pub>
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
*****

Do you want to continue(y/n)? y
registerQuorumPubKey success on server 0(10.0.2.14)
```

<officer1.token>

包含未簽署註冊權杖的檔案路徑。可包含最大 245 個位元組的任何隨機資料。

必要：是

<officer1.token.sig>

包含註冊權杖的 SHA256_PKCS 機制簽名雜湊的檔案路徑。

必要：是

<officer1.pub>

包含非對稱 RSA-2048 金鑰對的公有金鑰的檔案路徑。使用私有金鑰簽署註冊權杖。

必要：是

在所有 CO 註冊其公有金鑰之後，來自 `listUsers` 命令的輸出會在 `MofnPubKey` 欄中顯示此資訊，如下列範例所示。

```
aws-cloudhsm > listUsers
```

```
Users on server 0(10.0.2.14):
```

```
Number of users found:7
```

User Id	User Type	User Name	MofnPubKey
LoginFailureCnt	2FA		
1	PRECO	admin	NO
0	NO		
2	AU	app_user	NO
0	NO		
3	CO	officer1	YES
0	NO		
4	CO	officer2	YES
0	NO		
5	CO	officer3	YES
0	NO		
6	CO	officer4	YES
0	NO		
7	CO	officer5	YES
0	NO		

```
Users on server 1(10.0.1.4):
```

```
Number of users found:7
```

User Id	User Type	User Name	MofnPubKey
LoginFailureCnt	2FA		
1	PRECO	admin	NO
0	NO		
2	AU	app_user	NO
0	NO		
3	CO	officer1	YES
0	NO		
4	CO	officer2	YES
0	NO		
5	CO	officer3	YES
0	NO		
6	CO	officer4	YES
0	NO		
7	CO	officer5	YES
0	NO		

步驟 2. 設定 HSM 上的規定人數最小值

若要對 CO 使用規定人數身分驗證，CO 必須登入 HSM，然後設定規定人數最小值，也稱為 m 值。這是執行 HSM 使用者管理操作所需的 CO 核准數下限。HSM 上的任何 CO (包括尚未註冊用於簽署的金鑰的 CO) 可以設定規定人數最小值。您隨時可以變更規定人數最小值。如需更多資訊，請參閱 [變更最小值](#)。

設定 HSM 上的規定人數最小值

1. 使用下列命令來啟動 cloudhsm_mgmt_util 命令列工具。

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

2. 使用 loginHSM 命令以 CO 身分登入 HSM。如需詳細資訊，請參閱[???](#)。
3. 使用 setMValue 命令來設定規定人數最小值。如需詳細資訊，請參閱下列範例或使用 help setMValue 命令。

Example – 設定 HSM 上的規定人數最小值

此範例使用值為 2 的規定人數最小值。您可以選擇二 (2) 到八 (8) 之間的任何值，最多可到 HSM 上的 CO 總數。在這個範例中，HSM 有 6 個 CO，因此最大的可能值為 6。

若要使用以下範例命令，請將最終數字 (2) 以您偏好的規定人數最小值加以取代。

```
aws-cloudhsm > setMValue 3 <2>
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
*****

Do you want to continue(y/n)? y
Setting M Value(2) for 3 on 2 nodes
```

在上述範例中，第一個數字 (3) 表示您要設定之規定人數最小值的 HSM 服務。

HSM 服務識別符及其名稱、說明和服務中包含的命令如下表所列。

服務識別符	服務名稱	服務描述	HSM 命令
3	USER_MGMT	HSM 使用者管理	• createUser • deleteUser • changePswd (僅在變更不同 HSM 使用者的密碼時適用)
4	MISC_CO	其他 CO 服務	• setMValue

若要取得服務的規定人數最小值，請使用 getMValue 命令，如下列範例所示。

```
aws-cloudhsm > getMValue 3
MValue of service 3[USER_MGMT] on server 0 : [2]
MValue of service 3[USER_MGMT] on server 1 : [2]
```

來自上述 getMValue 命令的輸出顯示 HSM 使用者管理操作 (服務 3) 的規定人數最小值現在是 2。

完成這些步驟之後，請參閱 [針對 Management Utility 啟用規定人數身分驗證的使用者 AWS CloudHSM 管理](#)。

針對 Management Utility 啟用規定人數身分驗證的使用者 AWS CloudHSM 管理

硬體安全模組 AWS CloudHSM ([HSM](#)) 上的[加密主管 \(CO\)](#) 可以為 HSM 上的下列操作設定規定人數身分驗證：

- 建立 HSM 使用者
- 刪除 HSM 使用者
- 變更另一個 HSM 使用者的密碼

在將 HSM 設定為使用規定人數身分驗證之後，CO 無法自行執行 HSM 使用者管理操作。以下範例示範當 CO 嘗試在 HSM 上建立新使用者時的輸出。命令失敗，出現 RET_MXN_AUTH_FAILED 錯誤，這表示規定人數身分驗證失敗。

```
aws-cloudhsm > createUser CU user1 password
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
```

```
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
```

```
*****
```

```
Do you want to continue(y/n)? y
Creating User user1(CU) on 2 nodes
createUser failed: RET_MXN_AUTH_FAILED
creating user on server 0(10.0.2.14) failed
```

```
Retry/Ignore/Abort?(R/I/A): A
```

若要執行 HSM 使用者管理操作，CO 必須完成下列工作：

1. [取得規定人數字符](#)。
2. [取得其他 CO 的核准 \(簽章\)](#)。
3. [在 HSM 上核准字符](#)。
4. [執行 HSM 使用者管理操作](#)。

如果您尚未將 HSM 設定為使用 CO 的規定人數身分驗證，請立即設定。如需詳細資訊，請參閱[首次設定](#)。

步驟 1. 取得規定人數字符

首先，CO 必須使用 `cloudhsm_mgmt_util` 命令列工具，以請求規定人數權杖。

取得規定人數權杖

1. 使用下列命令來啟動 `cloudhsm_mgmt_util` 命令列工具。

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

2. 使用 `loginHSM` 命令以 CO 身分登入 HSM。如需詳細資訊，請參閱[???](#)。
3. 使用 `getToken` 命令來取得規定人數權杖。如需詳細資訊，請參閱下列範例或使用 `help getToken` 命令。

Example – 取得規定人數字符

此範例會取得使用者名稱 `officer1` 之 CO 的規定人數字符，並將字符儲存至名為 `officer1.token` 的檔案。若要使用範例命令，請將這些值取代為您自己的值：

- **officer1**：取得權杖的 CO 名稱。此使用者必須是登入到 HSM 的相同 CO 並正在執行此命令。
- **officer1.token**：用於存放規定人數權杖的檔案名稱。

在以下命令中，3 會識別您可以對其使用要取得字符的服務。在此情況下，此字符可用於 HSM 使用者管理操作 (服務 3)。如需詳細資訊，請參閱[步驟 2. 設定 HSM 上的規定人數最小值](#)。

```
aws-cloudhsm > getToken 3 officer1 officer1.token
getToken success on server 0(10.0.2.14)
Token:
Id:1
Service:3
Node:1
Key Handle:0
User:officer1
getToken success on server 1(10.0.1.4)
Token:
Id:1
Service:3
Node:0
Key Handle:0
User:officer1
```

步驟 2. 取得核准 CO 的簽章

具有規定人數字符的 CO 必須取得其他 CO 核准的字符。為了提供核准，其他 CO 會使用其簽署金鑰來以密碼編譯形式簽署字符。他們會在 HSM 外部執行此操作。

簽署權杖的方式有很多。下列範例示範使用 [OpenSSL](#) 的做法。若要使用不同的簽署工具，請確定工具使用 CO 的私有金鑰 (簽署金鑰) 來簽署字符的 SHA-256 摘要。

Example – 取得核准 CO 的簽章

在這個範例中，具有字符 (officer1) 的 CO 需要至少兩個核准。以下範例命令示範兩個 CO 如何使用 OpenSSL 來以密碼編譯方式簽署字符。

在第一個命令中，officer1 會簽署自己的字符。若要使用下列範例命令，請將這些值取代為您自己的值：

- **officer1.key** 和 **officer2.key**：包含 CO 簽署金鑰的檔案名稱。
- **officer1.token.sig1** 和 **officer1.token.sig2**：用於存放簽章的檔案名稱。務必將每個簽章儲存在不同的檔案中。

- ***officer1.token*** : 包含 CO 要簽署的權杖的檔案名稱。

```
$ openssl dgst -sha256 -sign officer1.key -out officer1.token.sig1 officer1.token
Enter pass phrase for officer1.key:
```

在以下命令中，**officer2** 會簽署相同的字符。

```
$ openssl dgst -sha256 -sign officer2.key -out officer1.token.sig2 officer1.token
Enter pass phrase for officer2.key:
```

步驟 3. 在 HSM 上核准簽署的權杖

CO 在向其他 CO 取得最低數量的核准 (簽章) 後，必須在 HSM 上核准簽署的字符。

在 HSM 上核准簽署的字符

1. 建立字符核准檔案。如需詳細資訊，請參閱下列範例。
2. 使用下列命令來啟動 `cloudhsm_mgmt_util` 命令列工具。

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

3. 使用 `loginHSM` 命令以 CO 身分登入 HSM。如需詳細資訊，請參閱[???。](#)
4. 使用 `approveToken` 命令來核准已簽署的字符，以便傳遞字符核准檔案。如需詳細資訊，請參閱下列範例。

Example – 在 HSM 上建立權杖核准檔案和核准簽署的權杖

字符核准檔案是一個文字檔案，採用 HSM 要求的特定格式。該檔案包含有關該字符、其核准者和核准者簽章的資訊。以下範例示範的是範例字符核准檔案。

```
# For "Multi Token File Path", type the path to the file that contains
# the token. You can type the same value for "Token File Path", but
# that's not required. The "Token File Path" line is required in any
# case, regardless of whether you type a value.
Multi Token File Path = officer1.token;
Token File Path = ;

# Total number of approvals
Number of Approvals = 2;
```

```
# Approver 1
# Type the approver's type, name, and the path to the file that
# contains the approver's signature.
Approver Type = 2; # 2 for CO, 1 for CU
Approver Name = officer1;
Approval File = officer1.token.sig1;

# Approver 2
# Type the approver's type, name, and the path to the file that
# contains the approver's signature.
Approver Type = 2; # 2 for CO, 1 for CU
Approver Name = officer2;
Approval File = officer1.token.sig2;
```

建立字符核准檔案之後，CO 會使用 `cloudhsm_mgmt_util` 命令列工具來登入 HSM。接著 CO 會使用 `approveToken` 命令來核准字符，如下列範例所示。將 *approval.txt* 取代為字符核准檔案的名稱。

```
aws-cloudhsm > approveToken approval.txt
approveToken success on server 0(10.0.2.14)
approveToken success on server 1(10.0.1.4)
```

此命令成功時，HSM 即已核准規定人數字符。若要檢查字符的狀態，請使用 `listTokens` 命令，如下列範例所示。命令的輸出顯示字符擁有所需的核准數。

字符有效時間指出字符會維持在 HSM 上的保證時間。即使已超過字符有效時間 (零秒)，您仍可繼續使用該字符。

```
aws-cloudhsm > listTokens
=====
      Server 0(10.0.2.14)
=====
----- Token - 0 -----
Token:
Id:1
Service:3
Node:1
Key Handle:0
User:officer1
Token Validity: 506 sec
Required num of approvers : 2
Current num of approvals : 2
Approver-0: officer1
```

```

Approver-1: officer2
Num of tokens = 1

=====
    Server 1(10.0.1.4)
=====
----- Token - 0 -----
Token:
Id:1
Service:3
Node:0
Key Handle:0
User:officer1
Token Validity: 506 sec
Required num of approvers : 2
Current num of approvals : 2
Approver-0: officer1
Approver-1: officer2
Num of tokens = 1

listTokens success

```

步驟 4. 針對使用者管理操作使用權杖

在 CO 具有所需核准數的字符之後，如先前區段中所示，CO 可以執行以下其中一個 HSM 使用者管理操作：

- 使用 [createUser](#) 命令建立 HSM 使用者
- 使用 deleteUser 命令來刪除 HSM 使用者
- 使用 changePswd 命令來變更不同 HSM 使用者的密碼

如需使用這些命令的詳細資訊，請參閱[HSM 使用者](#)。

CO 僅可以使用該字符來進行一個操作。當該操作成功，該字符即不再有效。為了執行其他 HSM 使用者管理操作，CO 必須取得新的規定人數字符、向核准者取得新簽章，並在 HSM 上核准該新字符。

Note

MofN 權杖僅在您目前的登入工作階段開啟時才有效。如果您登出 cloudhsm_mgmt_util 或網路連線中斷連線，則該權杖會失效。同樣地，授權的權杖只能在 cloudhsm_mgmt_util 中使用，而不能用於其他應用程式中進行身分驗證。

在下列範例命令中，CO 會在 HSM 上建立新使用者。

```
aws-cloudhsm > createUser CU user1 <password>
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
*****

Do you want to continue(y/n)? y
Creating User user1(CU) on 2 nodes
```

先前命令成功之後，後續的 listUsers 命令會顯示新使用者。

```
aws-cloudhsm > listUsers
Users on server 0(10.0.2.14):
Number of users found:8
```

User Id	User Type	User Name	MofnPubKey
LoginFailureCnt	2FA		
1	PCO	admin	N0
0	N0		
2	AU	app_user	N0
0	N0		
3	CO	officer1	YES
0	N0		
4	CO	officer2	YES
0	N0		
5	CO	officer3	YES
0	N0		
6	CO	officer4	YES
0	N0		
7	CO	officer5	YES
0	N0		

8	CU	user1	NO
0	NO		
Users on server 1(10.0.1.4):			
Number of users found:8			
User Id	User Type	User Name	MofnPubKey
LoginFailureCnt	2FA		
1	PCO	admin	NO
0	NO		
2	AU	app_user	NO
0	NO		
3	CO	officer1	YES
0	NO		
4	CO	officer2	YES
0	NO		
5	CO	officer3	YES
0	NO		
6	CO	officer4	YES
0	NO		
7	CO	officer5	YES
0	NO		
8	CU	user1	NO
0	NO		

如果 CO 嘗試執行其他 HSM 使用者管理操作，會因為規定人數身分驗證錯誤而失敗，如以下範例所示。

```
aws-cloudhsm > deleteUser CU user1
Deleting user user1(CU) on 2 nodes
deleteUser failed: RET_MXN_AUTH_FAILED
deleteUser failed on server 0(10.0.2.14)

Retry/rollBack/Ignore?(R/B/I): I
deleteUser failed: RET_MXN_AUTH_FAILED
deleteUser failed on server 1(10.0.1.4)

Retry/rollBack/Ignore?(R/B/I): I
```

listTokens 命令顯示 CO 沒有已核准的憑證，如下列範例所示。為了執行其他 HSM 使用者管理操作，CO 必須取得新的規定人數字符、向核准者取得新的簽章，並在 HSM 上核准該新字符。

```
aws-cloudhsm > listTokens
=====
```



```

    Server 0(10.0.2.14)
    =====
    Num of tokens = 0

    =====
    Server 1(10.0.1.4)
    =====
    Num of tokens = 0

listTokens success

```

使用 AWS CloudHSM Management Utility 變更規定人數最小值

[設定規定人數最小值](#)之後，讓 AWS CloudHSM [加密主管 \(COs\)](#) 可以使用規定人數身分驗證，您可能想要變更規定人數最小值。只有當核准者數目等於或大於目前規定人數最小值時，HSM 才允許您變更規定人數最小值。例如，如果規定人數最小值是 2，則至少兩個 CO 必須核准，才能變更規定人數最小值。

若要取得規定人數核准來變更規定人數最小值，您需要規定人數字符來用於 setMValue 命令 (服務 4)。若要取得 setMValue 命令的規定人數字符 (服務 4)，服務 4 的規定人數最小值必須大於 1。這表示您可能需要變更服務 4 的規定人數最小值，才能變更 CO 的規定人數最小值 (服務 3)。

HSM 服務識別符及其名稱、說明和服務中包含的命令如下表所列。

服務識別符	服務名稱	服務描述	HSM 命令
3	USER_MGMT	HSM 使用者管理	• createUser • deleteUser • changePswd (僅在變更不同 HSM 使用者的密碼時適用)
4	MISC_CO	其他 CO 服務	• setMValue

變更加密主管的規定人數最小值

1. 使用下列命令來啟動 cloudhsm_mgmt_util 命令列工具。

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

2. 使用 loginHSM 命令以 CO 身分登入 HSM。如需詳細資訊，請參閱 [???](#)。
3. 使用 getMValue 命令取得服務 3 的規定人數最小值。如需詳細資訊，請參閱下列範例。
4. 使用 getMValue 命令取得服務 4 的規定人數最小值。如需詳細資訊，請參閱下列範例。
5. 如果服務 4 的規定人數最小值低於服務 3 的值，請使用 setMValue 命令來變更服務 4 的值。將服務 4 的值變更為等於或大於服務 3 的值。如需詳細資訊，請參閱下列範例。
6. [取得規定人數權杖](#)，且應該指定服務 4 做為您可將字串用於其中的服務。
7. [取得其他 CO 的核准 \(簽章\)](#)。
8. [在 HSM 上核准字串](#)。
9. 使用 setMValue 命令來變更服務 3 (由 CO 執行的使用者管理操作) 的規定人數最小值。

Example – 取得規定人數最小值並變更服務 4 的值

以下範例命令顯示服務 3 的規定人數最小值目前是 2。

```
aws-cloudhsm > getMValue 3
MValue of service 3[USER_MGMT] on server 0 : [2]
MValue of service 3[USER_MGMT] on server 1 : [2]
```

以下範例命令顯示服務 4 的規定人數最小值目前是 1。

```
aws-cloudhsm > getMValue 4
MValue of service 4[MISC_CO] on server 0 : [1]
MValue of service 4[MISC_CO] on server 1 : [1]
```

若要變更服務 4 的規定人數最小值，請使用 setMValue 命令，並設定等於或大於服務 3 之值的值。以下範例將服務 4 的規定人數最小值設為 2，與為服務 3 設定的值相同。

```
aws-cloudhsm > setMValue 4 2
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
*****

Do you want to continue(y/n)? y
Setting M Value(2) for 4 on 2 nodes
```

以下命令顯示服務 3 和服務 4 的規定人數最小值現在是 2。

```
aws-cloudhsm > getMValue 3  
MValue of service 3[USER_MGMT] on server 0 : [2]  
MValue of service 3[USER_MGMT] on server 1 : [2]
```

```
aws-cloudhsm > getMValue 4  
MValue of service 4[MISC_C0] on server 0 : [2]  
MValue of service 4[MISC_C0] on server 1 : [2]
```

中的金鑰 AWS CloudHSM

您必須先在 AWS CloudHSM 叢集中的硬體安全模組 (HSM) 上建立[使用者](#)和金鑰，才能使用叢集進行加密處理。

在 中 AWS CloudHSM，使用下列任何一項來管理叢集中 HSMs 上的金鑰：

- PKCS #11 程式庫
- JCE 提供者
- CNG 和 KSP 提供者
- CloudHSM CLI

在管理金鑰前，請以加密使用者 (CU) 的使用者名稱和密碼登入 HSM。只有 CU 才可建立金鑰。建立金鑰的 CU 擁有並管理該金鑰。

如需在 中管理金鑰的詳細資訊，請參閱下列主題 AWS CloudHSM。

主題

- [中的金鑰同步和持久性設定 AWS CloudHSM](#)
- [中的 AES 金鑰包裝 AWS CloudHSM](#)
- [在 中使用信任的金鑰 AWS CloudHSM](#)
- [使用 CloudHSM CLI 進行金鑰管理](#)
- [使用 AWS CloudHSM KMU 進行金鑰管理](#)

中的金鑰同步和持久性設定 AWS CloudHSM

AWS CloudHSM 會同步您建立的每個字符金鑰。金鑰同步主要是自動程序，但您可以在叢集中至少使用兩個硬體安全模組 (HSM)，讓金鑰更耐久。本主題說明金鑰同步處理設定、客戶在叢集上使用金鑰時所面臨的常見問題，以及讓金鑰更耐久的策略。

本主題說明 中的金鑰同步設定 AWS CloudHSM、客戶在叢集上使用金鑰時遇到的常見問題，以及讓金鑰更持久的策略。

主題

- [AWS CloudHSM 關鍵概念](#)

- [了解 AWS CloudHSM 金鑰同步](#)
- [變更 AWS CloudHSM 用戶端金鑰耐久性設定](#)
- [在複製的 AWS CloudHSM 叢集之間同步金鑰](#)

AWS CloudHSM 關鍵概念

以下是在 中使用金鑰時需要注意的概念 AWS CloudHSM。

權杖金鑰

您在金鑰產生、匯入或取消包裝操作期間建立的持久性金鑰。會 AWS CloudHSM 同步叢集中的權杖金鑰。

工作階段金鑰

僅存在於叢集中一個硬體安全模組 (HSM) 上的暫時性金鑰。AWS CloudHSM 不會跨叢集同步工作階段金鑰。

用戶端金鑰同步

一種用戶端程序，可複製您在金鑰產生、匯入或解除包裝作業期間建立的權杖金鑰。您可以透過執行至少兩個 HSM 的叢集，使權杖金鑰更耐久。

伺服器端金鑰同步

定期將金鑰複製到叢集中的每個 HSM。不需要管理。

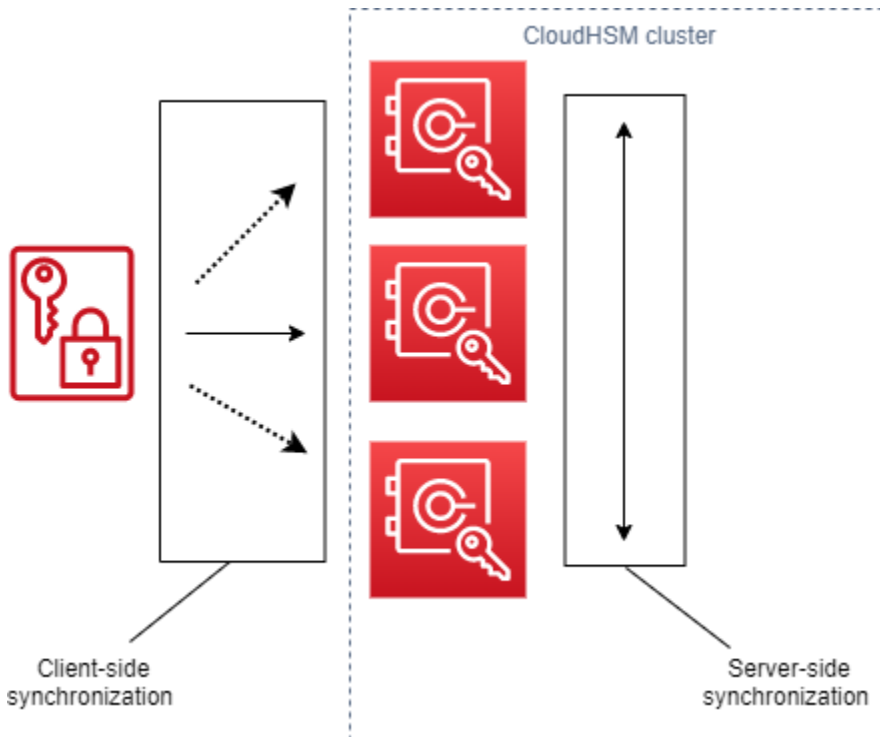
用戶端金鑰耐久性設定

您在用戶端上設定的會影響金鑰耐久性的設定。這些設定在用戶端 SDK 5 和用戶端 SDK 3 中的運作方式不同。

- 在用戶端 SDK 5 中，使用此設定來執行單一 HSM 叢集。
- 在用戶端 SDK 3 中，使用此設定可指定金鑰建立作業成功所需的 HSM 數目。

了解 AWS CloudHSM 金鑰同步

AWS CloudHSM 使用金鑰同步來複製叢集中所有硬體安全模組 (HSM) 的權杖金鑰。您可以在金鑰產生、匯入或解除包裝作業期間，將權杖金鑰建立為持久性金鑰。為了在叢集中分配這些金鑰，CloudHSM 提供用戶端和伺服器端金鑰同步處理。



金鑰同步處理 (伺服器端和用戶端) 的目標是在建立新金鑰之後，儘快在叢集中散發新金鑰。這很重要，因為您後續使用新金鑰所進行的呼叫可以路由傳送至叢集中任何可用的 HSM。如果您進行的呼叫路由到沒有金鑰的 HSM，則呼叫會失敗。您可以指定應用程式重試在金鑰建立作業之後進行的後續呼叫，藉此減輕這些類型的失敗。同步處理所需的時間可能會有所不同，具體取決於叢集的工作負載和其他無形資產。使用 CloudWatch 指標來判斷應用程式在這種情況下應採用的時間。如需詳細資訊，請參閱 [CloudWatch 指標](#)。

在雲端環境中，金鑰同步處理的挑戰在於金鑰的耐久性。您可以在單一 HSM 上建立金鑰，並且通常會立即開始使用這些金鑰。如果您建立金鑰的 HSM 在將金鑰複製到叢集中的其他 HSM 前失敗，您將遺失金鑰並存取金鑰所加密的任何項目。為了減輕此風險，我們提供用戶端同步處理。用戶端同步處理是用戶端程序，可複製您在金鑰產生、匯入或解除包裝作業期間建立的金鑰。在建立金鑰時複製金鑰會讓金鑰更耐久。當然，您無法使用單一 HSM 複製叢集中的金鑰。為了讓金鑰更耐久，我們也建議您將叢集設定為至少使用兩個 HSM。透過用戶端同步處理和具有兩個 HSM 的叢集，您可以在雲端環境中應對金鑰耐久性的挑戰。

變更 AWS CloudHSM 用戶端金鑰耐久性設定

金鑰同步處理大部分是自動程序，但您可以管理用戶端金鑰耐久性設定。用戶端金鑰耐久性設定在用戶端 SDK 5 和用戶端 SDK 3 中的運作方式不同。

- 在用戶端 SDK 5 中，我們介紹了金鑰可用性定額組的概念。此概念要求您至少使用兩個 HSM 執行叢集。您可以使用用戶端金鑰持久性設定來選擇退出兩個 HSM 需求。如需定額組的詳細資訊，請參閱 [the section called “用戶端 SDK 5 概念”](#)。
- 在用戶端 SDK 3 中，您可以使用用戶端金鑰持久性設定來指定必須成功建立金鑰的 HSM 數目，整體作業才會視為成功。

用戶端 SDK 5 用戶端金鑰持久性設定

在用戶端 SDK 5 中，金鑰同步處理是完全自動的程序。透過金鑰可用性定額組，新建立的金鑰在您的應用程式使用金鑰前必須存在於叢集中的兩個 HSM 上。若要使用金鑰可用性定額組，您的叢集必須至少要有兩個 HSM。

如果您的叢集組態不符合金鑰持久性需求，則建立或使用權杖金鑰的任何嘗試都會失敗，並在日誌中顯示下列錯誤訊息：

```
Key <key handle> does not meet the availability requirements - The key must be
available on at least 2 HSMs before being used.
```

您可以使用用戶端組態設定來選擇退出金鑰可用性定額組。例如，您可能想要選擇退出以單一 HSM 執行叢集。

用戶端 SDK 5 概念

金鑰可用性定額組

AWS CloudHSM 會指定叢集中的 HSMs 數目，在應用程式可以使用金鑰之前，金鑰必須存在於其中。需要至少有兩個 HSM 的叢集。

管理用戶端金鑰持久性設定

若要管理用戶端金鑰持久性設定，您必須使用用戶端 SDK 5 的設定工具。

PKCS #11 library

在 Linux 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --disable-key-availability-check
```

在 Windows 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" --disable-key-availability-check
```

OpenSSL Dynamic Engine

在 Linux 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
$ sudo /opt/cloudhsm/bin/configure-dyn --disable-key-availability-check
```

Key Storage Provider (KSP)

在 Windows 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --disable-key-availability-check
```

JCE provider

在 Linux 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
$ sudo /opt/cloudhsm/bin/configure-jce --disable-key-availability-check
```

在 Windows 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。


```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" --disable-key-availability-check
```

CloudHSM CLI

在 Linux 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
$ sudo /opt/cloudhsm/bin/configure-cli --disable-key-availability-check
```

在 Windows 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" --disable-key-availability-check
```

用戶端 SDK 3 用戶端金鑰持久性設定

在用戶端 SDK 3 中，金鑰同步處理大部分是自動程序，但您可以使用用戶端金鑰持久性設定，讓金鑰更耐久。您需要指定必須成功建立金鑰的 HSM 數目，整體作業才會視為成功。無論您選擇何種設定，用戶端同步處理始終都會盡最大努力嘗試將金鑰複製到叢集中的每個 HSM。您的設定會對您指定的 HSM 數量強制建立金鑰。如果您指定一個值，但系統無法將金鑰複製到該數目的 HSM，則系統會自動清除任何不需要的金鑰材料，您可以再試一次。

Important

如果您未設定用戶端金鑰持久性設定 (或使用預設值 1)，您的金鑰容易遺失。如果您目前的 HSM 應該在伺服器端服務將該金鑰複製到另一個 HSM 之前失敗，您就會遺失金鑰材料。

若要最大化金鑰持久性，請考慮為用戶端同步處理指定至少兩個 HSM。請記住，無論您指定了多少 HSM，叢集上的工作負載都保持不變。用戶端同步處理一律會盡最大努力嘗試將金鑰複製到叢集中的每個 HSM。

建議

- 最小值：每個叢集兩個 HSM
- 最大值：少於叢集中 HSM 總數的一個值

如果用戶端同步處理失敗，用戶端服務會清除任何可能已建立且現在不需要的多餘金鑰。這種清理是盡力而為的回應，可能並非不總是有效。如果清理失敗，您可能必須刪除不需要的金鑰材料。如需詳細資訊，請參閱[金鑰同步處理失敗](#)。

設定用戶端金鑰耐久性的組態檔案

若要指定用戶端金鑰耐久性設定，您必須編輯 `cloudhsm_client.cfg`。

編輯用戶端組態檔案

1. 打開 `cloudhsm_client.cfg`。

Linux：

```
/opt/cloudhsm/etc/cloudhsm_client.cfg
```

Windows：

```
C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_client.cfg
```

2. 在檔案的 `client` 節點中，新增 `create_object_minimum_nodes` 並指定 HSMs 數目下限的值，該值 AWS CloudHSM 必須成功建立金鑰，金鑰建立操作才能成功。

```
"create_object_minimum_nodes" : 2
```

Note

`key_mgmt_util` (KMU) 命令列工具有用戶端金鑰耐久性的額外設定。如需詳細資訊，請參閱[the section called “KMU 與用戶端同步”](#)

組態參考

以下是用戶端同步處理屬性，如 `cloudhsm_client.cfg` 的摘錄所示：

```
{
  "client": {
    "create_object_minimum_nodes" : 2,
    ...
  },
  ...
}
```

create_object_minimum_nodes

指定認為金鑰產生、金鑰匯入或金鑰解除包裝作業成功所需的 HSM 數目下限。如果設定，則預設值為 1。即：對於每個金鑰建立作業，用戶端服務都會嘗試在叢集中的每個 HSM 上建立金鑰，但若要傳回成功，只需要在叢集中的一個 HSM 上建立單一金鑰。

KMU 與用戶端同步

如果您使用 key_mgmt_util (KMU) 命令列工具建立金鑰，您可以使用選用的命令列參數 (-min_srv) 來限制需要複製金鑰的 HSM 數目。如果您指定命令列參數和組態檔案中的值，會 AWS CloudHSM 認可兩個值的 LARGER。

如需詳細資訊，請參閱下列主題：

- [genDSAKeyPair](#)
- [genECCKeypair](#)
- [genRSAKeyPair](#)
- [genSymKey](#)
- [importPrivateKey](#)
- [importPubKey](#)
- [imSymKey](#)
- [insertMaskedObject](#)
- [unWrapKey](#)

在複製的 AWS CloudHSM 叢集之間同步金鑰

用戶端和伺服器端同步僅適用於同步相同 AWS CloudHSM 叢集中的金鑰。如果您將叢集備份複製到另一個區域，您可以使用 `cloudhsm_mgmt_util` (CMU) 的 `syncKey` 命令來同步叢集之間的金鑰。您可以使用複製的叢集進行跨區域備援，或簡化災難復原程序。如需詳細資訊，請參閱 [syncKey](#)。

中的 AES 金鑰包裝 AWS CloudHSM

本主題說明 中的 AES 金鑰包裝選項 AWS CloudHSM。AES 金鑰包裝使用 AES 金鑰 (包裝金鑰) 來包裝任何類型的另一個金鑰 (目標金鑰)。您可以使用金鑰包裝來保護儲存的金鑰，或透過不安全的網路傳輸金鑰。

主題

- [支援的演算法](#)
- [在 中使用 AES 金鑰包裝 AWS CloudHSM](#)

支援的演算法

AWS CloudHSM 提供三種 AES 金鑰包裝選項，每個選項都根據目標金鑰在包裝前的填充方式而定。當您呼叫金鑰包裝時，會根據您使用的演算法自動完成填補。下表列出支援的演算法和相關詳細資訊，可協助您為應用程式選擇適當的包裝機制。

AES 金鑰包裝演算法	規格	支援的目標金鑰類型	填補方案	AWS CloudHSM 用戶端可用性
AES 金鑰包裝，零填補	RFC 5649 和 SP 800-38F	全部	如果需要，在金鑰位元後增加零，以對齊區塊	SDK 3.1 及更新版本
AES 金鑰包裝，無填補	RFC 3394 和 SP 800-38F	區塊對齊的金鑰，例如 AES 和 3DES	無	SDK 3.1 及更新版本
AES 金鑰包裝與 PKCS #5 填補	無	全部	根據 PKCS #5 填補方案新增至少 8 個位元組以對齊區塊	全部

若要了解如何在應用程式中使用上表的 AES 金鑰包裝演算法，請參閱 [AWS CloudHSM 中的使用 AES 金鑰包裝](#)。

了解 AES 金鑰包裝中的初始化向量

在包裝之前，CloudHSM 會將初始化向量 (IV) 附加到目標金鑰，以確保資料完整性。每個金鑰包裝演算法對於允許什麼類型的 IV 都有特定的限制。若要在 中設定 IV AWS CloudHSM，您有兩個選項：

- 隱含：將 IV 設定為 NULL，CloudHSM 會使用該演算法的預設值進行包裝和取消包裝操作 (建議)
- 明確：透過將預設 IV 值傳遞給金鑰包裝函數來設定 IV

Important

您必須了解在您應用程式中使用什麼 IV。若要取消包裝金鑰，您必須提供您用來包裝金鑰的相同 IV。如果您使用隱含 IV 來包裝，則請使用隱含 IV 來取消包裝。對於隱含 IV，CloudHSM 將使用預設值來取消包裝。

下表說明包裝演算法指定之 IV 的允許值。

AES 金鑰包裝演算法	隱含 IV	明確 IV
AES 金鑰包裝，零填補	必要 預設值：(根據規格在內部計算 IV)	不允許
AES 金鑰包裝，無填補	允許 (建議使用) 預設值：0xA6A6A6A6A6A6A6A6	允許 只接受此值：0xA6A6A6A6A6A6A6A6
AES 金鑰包裝與 PKCS #5 填補	允許 (建議使用) 預設值：0xA6A6A6A6A6A6A6A6	允許 只接受此值：0xA6A6A6A6A6A6A6A6

在 中使用 AES 金鑰包裝 AWS CloudHSM

如下所示包裝和取消包裝金鑰：

- 在 [PKCS #11 程式庫](#) 中，為 C_WrapKey 和 C_UnWrapKey 函數選取適當的機制，如下表所示。
- 在 [JCE 提供者](#) 中，選取適當的演算法、模式和填補組合，實作加密方法 Cipher.WRAP_MODE 和 Cipher.UNWRAP_MODE，如下表所示。
- 在 [CloudHSM CLI](#) 中，從支援的 [CloudHSM CLI 中的金鑰包裝命令](#) 和 演算法清單中選擇適當的 [CloudHSM CLI 中的金鑰展開命令](#) 演算法，如下表所示。
- 在 [key_mgmt_util \(KMU\)](#) 中，使用 [使用 KMU 取消包裝 AWS CloudHSM 金鑰](#) 和 [使用 KMU 匯出 AWS CloudHSM 金鑰](#) 命令搭配適當的 m 值，如下表所示。

AES 金鑰包裝演算法	PKCS #11 機制	Java 方法	CloudHSM CLI 子命令	金鑰管理公用程式 (KMU) 引數
AES 金鑰包裝，零填補	CKM_CLOUD_HSM_AES_KEY_WRAP_ZERO_PAD (供應商定義的機制)	AESWrap/ECB/ZeroPadding	aes-zero-pad	m = 6
AES 金鑰包裝，無填補	CKM_CLOUD_HSM_AES_KEY_WRAP_NO_PAD (供應商定義的機制)	AESWrap/ECB/NoPadding	aes-no-pad	m = 5
AES 金鑰包裝與 PKCS #5 填補	CKM_CLOUD_HSM_AES_KEY_WRAP_PKCS5_PAD (供應商定義的機制)	AESWrap/ECB/PKCS5Padding	aes-pkcs5-pad	m = 4

在 中使用信任的金鑰 AWS CloudHSM

AWS CloudHSM 支援受信任的金鑰包裝，以保護資料金鑰免受內部威脅。本主題說明如何建立可信任金鑰來保護資料安全。

主題

- [了解 中的信任金鑰 AWS CloudHSM](#)
- [中的信任金鑰屬性 AWS CloudHSM](#)
- [如何使用信任的金鑰在 中包裝資料金鑰 AWS CloudHSM](#)
- [如何使用 的信任金鑰來取消包裝資料金鑰 AWS CloudHSM](#)

了解 中的信任金鑰 AWS CloudHSM

可信任金鑰是用來包裝其他金鑰的金鑰，管理員和加密管理員 (COs) 會使用屬性 `CKA_TRUSTED` 明確識別為可信任。此外，管理員和加密管理員 (CO) 會使用 `CKA_UNWRAP_TEMPLATE` 和相關屬性來指定可信任金鑰取消資料金鑰包裝後可執行的動作。由可信任金鑰取消資料金鑰包裝也必須包含這些屬性，取消包裝的操作才能成功，其有助於確保只允許已取消包裝的資料金鑰用於您想要的用途。

使用屬性 `CKA_WRAP_WITH_TRUSTED` 來識別您要使用可信任金鑰包裝的所有資料金鑰。這樣做可讓您限制資料金鑰，讓應用程式只能使用可信任金鑰來取消包裝。一旦您在資料金鑰上設定此屬性，屬性就會變成唯讀，而且無法變更。設定這些屬性後，應用程式只能使用您信任的金鑰來取消資料金鑰包裝，並且取消包裝一律會產生具有會限制這些金鑰使用方式屬性的資料金鑰。

中的信任金鑰屬性 AWS CloudHSM

下列屬性可讓您將 AWS CloudHSM 金鑰標示為受信任、指定只能使用受信任金鑰包裝和取消包裝的資料金鑰，以及控制資料金鑰在取消包裝後可以執行的動作：

- `CKA_TRUSTED`：將此屬性 (除 `CKA_UNWRAP_TEMPLATE` 外) 套用於將會包裝資料金鑰的金鑰，以表明管理員或加密管理員 (CO) 已完成必要的盡職調查並信任此金鑰。只有管理員或 CO 可以設定 `CKA_TRUSTED`。加密使用者 (CU) 擁有金鑰，但只有 CO 可以設置其 `CKA_TRUSTED` 屬性。
- `CKA_WRAP_WITH_TRUSTED`：將此屬性套用於可匯出的資料金鑰，以表明只能使用標記為 `CKA_TRUSTED` 的金鑰包裝此金鑰。一旦設定 `CKA_WRAP_WITH_TRUSTED` 為 `true`，屬性就會變成唯讀，而且您無法變更或移除屬性。
- `CKA_UNWRAP_TEMPLATE`：將此屬性套用於包裝金鑰 (除 `CKA_TRUSTED` 外)，以指定服務必須自動套用於服務取消包裝資料金鑰的屬性名稱和值。當應用程式提交金鑰以取消包裝時，還可提供自有的

取消包裝範本。如果您指定取消包裝範本，且應用程式提供了自有的取消包裝範本，則 HSM 會使用這兩個範本將屬性名稱和值套用於金鑰。但是，如果用於包裝金鑰的 `CKA_UNWRAP_TEMPLATE` 中的值與應用程式在取消包裝請求期間提供的屬性衝突，取消包裝請求會失敗。

如需關於屬性的詳細資訊，請參閱下列主題：

- [PKCS #11 金鑰屬性](#)
- [JCE 金鑰屬性](#)
- [CloudHSM CLI 金鑰屬性](#)

如何使用信任的金鑰在 中包裝資料金鑰 AWS CloudHSM

若要使用信任的金鑰來包裝資料金鑰 AWS CloudHSM，您必須完成三個基本步驟：

1. 對於您計劃使用可信任金鑰包裝的資料金鑰，請將其 `CKA_WRAP_WITH_TRUSTED` 屬性設定為 `true`。
2. 對於您計劃用來包裝資料金鑰的可信任金鑰，請將其 `CKA_TRUSTED` 屬性設定為 `true`。
3. 使用可受信任金鑰來包裝資料金鑰。

步驟 1：將資料金鑰的 `CKA_WRAP_WITH_TRUSTED` 設定為 `true`

對於要包裝的資料金鑰，選擇以下選項之一以將金鑰的 `CKA_WRAP_WITH_TRUSTED` 屬性設定為 `true`。這樣做會限制資料金鑰，因此應用程式只能使用可信任金鑰來包裝。

選項 1：如果產生一個新的金鑰，將 `CKA_WRAP_WITH_TRUSTED` 設定為 `true`

使用 [PKCS #11](#)、[JCE](#) 或 [CloudHSM CLI](#) 產生金鑰。如需詳細資訊，請參閱下列範例。

PKCS #11

若要使用 PKCS #11 產生金鑰，您需要將金鑰的 `CKA_WRAP_WITH_TRUSTED` 屬性設定為 `true`。為此，請先將此屬性包含在金鑰的 `CK_ATTRIBUTE` `template` 中，然後將屬性設定為 `true`，如下列範例所示：

```
CK_BYTE_PTR label = "test_key";
CK_ATTRIBUTE template[] = {
    {CKA_WRAP_WITH_TRUSTED, &true_val,      sizeof(CK_BBOOL)},
```



```

        {CKA_LABEL,          label,          strlen(label)},
        ...
    };

```

如需詳細資訊，請參閱[使用 PKCS #11 產生金鑰的公開示範範例](#)。

JCE

若要使用 JCE 產生金鑰，您需要將金鑰的 `WRAP_WITH_TRUSTED` 屬性設定為 `true`。為此，請先將此屬性包含在金鑰的 `KeyAttributesMap` 中，然後將屬性設定為 `true`，如下列範例所示：

```

final String label = "test_key";
final KeyAttributesMap keySpec = new KeyAttributesMap();
keySpec.put(KeyAttribute.WRAP_WITH_TRUSTED, true);
keySpec.put(KeyAttribute.LABEL, label);
...

```

如需詳細資訊，請參閱[使用 JCE 產生金鑰的公開示範範例](#)。

CloudHSM CLI

若要使用 CloudHSM CLI 產生金鑰，您需要將金鑰的 `wrap-with-trusted` 屬性設定為 `true`。為此，請將 `wrap-with-trusted=true` 包含在適合金鑰產生命令的引數：

- 對於對稱金鑰，請將 `wrap-with-trusted` 新增至 `attributes` 引數中。
- 對於公有金鑰，請將 `wrap-with-trusted` 新增至 `public-attributes` 引數中。
- 對於私有金鑰，請將 `wrap-with-trusted` 新增至 `private-attributes` 引數中。

如需關於產生金鑰對的詳細資訊，請參閱 [CloudHSM CLI 中的 `generate-asymmetric-pair` 類別](#)。

如需關於產生對稱金鑰的詳細資訊，請參閱 [CloudHSM CLI 中的產生對稱類別](#)。

選項 2：如果使用現有金鑰，請使用 CloudHSM CLI 將其 **`CKA_WRAP_WITH_TRUSTED`** 設定為 `true`

若要將現有金鑰的 `CKA_WRAP_WITH_TRUSTED` 屬性設定為 `true`，請依照下列步驟執行：

1. 使用 [使用 CloudHSM CLI 登入 HSM](#) 命令以加密使用者 (CU) 身分登入。
2. 使用 [使用 CloudHSM CLI 設定金鑰的屬性](#) 命令將金鑰的 `wrap-with-trusted` 屬性設定為 `true`。

```
aws-cloudhsm > key set-attribute --filter attr.label=test_key --name wrap-with-trusted --value true
{
  "error_code": 0,
  "data": {
    "message": "Attribute set successfully"
  }
}
```

步驟 2：將可信任金鑰的 **CKA_TRUSTED** 設定為 true

若要讓金鑰成為可信任金鑰，其 CKA_TRUSTED 屬性必須設定為 true。您可以使用 CloudHSM CLI 或 CloudHSM 管理公用程式 (CMU) 來執行此操作。

- 如果使用 CloudHSM CLI 設定金鑰的 CKA_TRUSTED 屬性，請參閱 [使用 CloudHSM CLI 將金鑰標記為信任](#)。
- 如果使用 CMU 來設定金鑰的 CKA_TRUSTED 屬性，請參閱 [如何使用 AWS CloudHSM Management Utility 將金鑰標記為受信任](#)。

步驟 3。使用可受信任金鑰來包裝資料金鑰

若要使用您在步驟 2 中設定的可信任金鑰來包裝步驟 1 所述的資料金鑰，請參閱下列連結以取得程式碼範例。每個都示範如何包裝金鑰。

- [AWS CloudHSM PKCS #11 範例](#)
- [AWS CloudHSM JCE 範例](#)

如何使用 的信任金鑰來取消包裝資料金鑰 AWS CloudHSM

若要在 中取消包裝資料金鑰 AWS CloudHSM，您需要已 CKA_UNWRAP 設定為 true 的信任金鑰。若要成為金鑰，其還必須滿足下列條件：

- 金鑰的 CKA_TRUSTED 屬性必須設定為 true。
- 金鑰必須使用 CKA_UNWRAP_TEMPLATE 和相關屬性來指定資料金鑰在取消包裝後可以執行的動作。例如，如果您希望取消包裝的金鑰不可匯出，您可以將 CKA_EXPORTABLE = FALSE 設定為 CKA_UNWRAP_TEMPLATE 的一部分。

 Note

CKA_UNWRAP_TEMPLATE 僅可與 PKCS #11 一同使用。

當應用程式提交要取消包裝的金鑰時，應用程式也可以提供自有的取消包裝範本。如果您指定取消包裝範本，且應用程式提供了自有的取消包裝範本，則 HSM 會使用這兩個範本將屬性名稱和值套用於金鑰。但是，如果在取消包裝請求期間，可信任金鑰中的值與應用程式提供的屬性 CKA_UNWRAP_TEMPLATE 衝突，則取消包裝請求會失敗。

若要查看關於使用可信任金鑰取消包裝金鑰的範例，請參閱[此 PKCS #11 範例](#)。

使用 CloudHSM CLI 進行金鑰管理

如果使用[最新的 SDK 版本系列](#)，請使用 [CloudHSM CLI](#) 來管理 AWS CloudHSM 叢集中的金鑰。如需詳細資訊，請參閱下列主題。

- [使用信任的金鑰](#)說明如何使用 CloudHSM CLI 建立信任的金鑰來保護資料。
- [產生金鑰](#)包括建立金鑰的說明，包括對稱金鑰、RSA 金鑰和 EC 金鑰。
- [刪除金鑰](#)會說明金鑰擁有者如何刪除金鑰。
- [共用和取消共用金鑰](#)詳細說明金鑰擁有者如何共用和取消共用金鑰。
- [篩選金鑰](#)提供如何使用篩選條件尋找金鑰的準則。
- [管理金鑰規定人數身分驗證 \(M of N\)](#) 提供如何設定和使用規定人數身分驗證與金鑰的指導方針。

使用 CloudHSM CLI 產生金鑰

您必須先啟動 [CloudHSM CLI](#) 並以加密使用者 (CU) 身分登入，才能產生金鑰。若要在 HSM 中產生金鑰，請使用與您想產生之金鑰類型對應的命令。

主題

- [使用 CloudHSM CLI 產生對稱金鑰](#)
- [使用 CloudHSM CLI 產生非對稱金鑰](#)
- [AWS CloudHSM 金鑰相關主題](#)

使用 CloudHSM CLI 產生對稱金鑰

使用 中列出的命令 [CloudHSM CLI 中的產生對稱類別](#) 來產生 的對稱金鑰 AWS CloudHSM。若要查看所有可用的選項，請使用 `help key generate-symmetric` 命令。

產生 AES 金鑰

使用 `key generate-symmetric aes` 命令產生 AES 金鑰。若要查看所有可用的選項，請使用 `help key generate-symmetric aes` 命令。

Example

下列範例會產生 32 位元組 AES 金鑰。

```
aws-cloudhsm > key generate-symmetric aes \  
  --label aes-example \  
  --key-length-bytes 32
```

引數

<LABEL>

指使用者定義的 AES 金鑰標籤。

必要：是

<KEY-LENGTH-BYTES>

指金鑰長度 (以位元組為單位)。

有效值：

- 16、24 和 32

必要：是

<KEY_ATTRIBUTES>

指定一個空格分隔的金鑰屬性清單，對產生的 AES 金鑰進行設定，格式為 `KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` (例如，`sign=true`)

如需支援的 AWS CloudHSM 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

<SESSION>

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

如要將工作階段金鑰更改為永久 (權杖) 金鑰，請使用[金鑰設定屬性](#)。

根據預設，產生的金鑰是持久性/權杖金鑰。使用 <SESSION> 會變更此項目，確保使用此引數產生的金鑰是工作階段/暫時性的

必要：否

產生一般私密金鑰

使用 `key generate-symmetric generic-secret` 命令產生一般私密金鑰。若要查看所有可用的選項，請使用 `help key generate-symmetric generic-secret` 命令。

Example

下列範例會產生 32 位元組的一般私密金鑰。

```
aws-cloudhsm > key generate-symmetric generic-secret \  
  --label generic-secret-example \  
  --key-length-bytes 32
```

引數**<LABEL>**

為一般私密金鑰指定使用者定義的標籤。

必要：是

<KEY-LENGTH-BYTES>

指金鑰長度 (以位元組為單位)。

有效值：

- 1 到 800

必要：是

<KEY_ATTRIBUTES>

指一個空格分隔的金鑰屬性清單，以 KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE (例如，sign=true) 的形式為產生的一般私密金鑰設定

如需支援的 AWS CloudHSM 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

<SESSION>

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

如要將工作階段金鑰更改為永久 (權杖) 金鑰，請使用 [金鑰設定屬性](#)。

根據預設，產生的金鑰是持久性/權杖金鑰。使用 <SESSION> 會變更此項目，確保使用此引數產生的金鑰是工作階段/暫時性的

必要：否

使用 CloudHSM CLI 產生非對稱金鑰

使用 中列出的命令 [CloudHSM CLI 中的 generate-asymmetric-pair 類別](#) 來產生 AWS CloudHSM 叢集的非對稱金鑰對。

產生 RSA 金鑰

使用 key generate-asymmetric-pair rsa 命令來產生 RSA 金鑰對。若要查看所有可用的選項，請使用 help key generate-asymmetric-pair rsa 命令。

Example

以下範例會產生 RSA 2048 位元金鑰對。

```
aws-cloudhsm > key generate-asymmetric-pair rsa \  
  --public-exponent 65537 \  
  --modulus-size-bits 2048 \  
  --public-label rsa-public-example \  
  --private-label rsa-private-example
```

引數

<PUBLIC_LABEL>

指使用者定義的公有金鑰標籤。

必要：是

<PRIVATE_LABEL>

指使用者定義的私有金鑰標籤。

必要：是

<MODULUS_SIZE_BITS>

指模數的長度 (以位元為單位)。最小值為 2048。

必要：是

<PUBLIC_EXPONENT>

指公有指數。值必須為大於或等於 65537 的奇數。

必要：是

<PUBLIC_KEY_ATTRIBUTES>

指以空格分隔的金鑰屬性清單，以 KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE (例如，sign=true) 的形式為產生的 RSA 公有金鑰設定。

如需支援的 AWS CloudHSM 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

<SESSION>

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

如要將工作階段金鑰更改為永久 (權杖) 金鑰，請使用 [金鑰設定屬性](#)。

根據預設，產生的金鑰是持久性/權杖金鑰。使用 <SESSION> 會變更此項目，確保使用此引數產生的金鑰是工作階段/暫時性的

必要：否

產生 EC (橢圓曲線密碼編譯) 金鑰對

使用 `key generate-asymmetric-pair ec` 命令來產生金鑰對。若要查看所有可用的選項，包括支援的橢圓曲線清單，請使用 `help key generate-asymmetric-pair ec` 命令。

Example

下列範例會使用 `Secp384r1` 橢圓曲線產生 EC 金鑰對。

```
aws-cloudhsm > key generate-asymmetric-pair ec \  
  --curve secp384r1 \  
  --public-label ec-public-example \  
  --private-label ec-private-example
```

引數

<PUBLIC_LABEL>

指使用者定義的公有金鑰標籤。用戶端 SDK label 5.11 和更新版本允許的大小上限為 127 個字元。用戶端 SDK 5.10 和以前的 限制為 126 個字元。

必要：是

<PRIVATE_LABEL>

指使用者定義的私有金鑰標籤。用戶端 SDK label 5.11 和更新版本允許的大小上限為 127 個字元。用戶端 SDK 5.10 和以前的 限制為 126 個字元。

必要：是

<CURVE>

指橢圓曲線的識別符。

有效值：

- prime256v1
- secp256r1
- secp224r1
- secp384r1
- secp256k1
- secp521r1

必要：是

<PUBLIC_KEY_ATTRIBUTES>

指以空格分隔的金鑰屬性清單，以 KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE (例如，verify=true) 的形式為產生的 EC 公開金鑰設定。

如需支援的 AWS CloudHSM 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

<PRIVATE_KEY_ATTRIBUTES>

指以空格分隔的金鑰屬性清單，以 KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE (例如，sign=true) 的形式為產生的 EC 私有金鑰設定。

如需支援的 AWS CloudHSM 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

<SESSION>

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

如要將工作階段金鑰更改為永久 (權杖) 金鑰，請使用 [金鑰設定屬性](#)。

根據預設，產生的金鑰是持久性 (權杖) 金鑰。在 <SESSION> 傳遞會變更此情況，確保使用此參數生成的金鑰是工作階段 (臨時) 金鑰。

必要：否

AWS CloudHSM 金鑰相關主題

如需 中金鑰的其他資訊，請參閱下列各節 AWS CloudHSM。

- [CloudHSM CLI 的金鑰屬性](#)
- [CloudHSM CLI 中的 generate-asymmetric-pair 類別](#)
- [CloudHSM CLI 中的產生對稱類別](#)

使用 CloudHSM CLI 刪除金鑰

使用本主題中的範例，透過 [CloudHSM CLI](#) 刪除金鑰。只有金鑰擁有者可以刪除金鑰。

主題

- [範例：刪除金鑰](#)
- [相關主題](#)

範例：刪除金鑰

1. 執行 `key list` 命令以識別您要刪除的金鑰：

```
aws-cloudhsm > key list --filter attr.label="my_key_to_delete" --verbose
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x00000000000540011",
        "key-info": {
          "key-owners": [
            {
              "username": "my_crypto_user",
              "key-coverage": "full"
            }
          ],
          "shared-users": [],
          "key-quorum-values": {
            "manage-key-quorum-value": 0,
            "use-key-quorum-value": 0
          },
          "cluster-coverage": "full"
        },
        "attributes": {
          "key-type": "rsa",
          "label": "my_key_to_delete",
          "id": "",
          "check-value": "0x29bbd1",
          "class": "private-key",
          "encrypt": false,
          "decrypt": true,
          "token": true,
          "always-sensitive": true,
          "derive": false,
          "destroyable": true,
          "extractable": true,
```

```

        "local": true,
        "modifiable": true,
        "never-extractable": false,
        "private": true,
        "sensitive": true,
        "sign": true,
        "trusted": false,
        "unwrap": true,
        "verify": false,
        "wrap": false,
        "wrap-with-trusted": false,
        "key-length-bytes": 1217,
        "public-exponent": "0x010001",
        "modulus":
"0x8b3a7c20618e8be08220ed8ab2c8550b65fc1aad8d4cf04fbf2be685f97eeb78fcbbad9b02cd91a3b15e990
        "modulus-size-bits": 2048
    }
}
],
"total_key_count": 1,
"returned_key_count": 1
}

```

2. 識別金鑰後，執行具有金鑰的唯一 label 屬性的 key delete 以刪除金鑰：

```

aws-cloudhsm > key delete --filter attr.label="my_key_to_delete"
{
  "error_code": 0,
  "data": {
    "message": "Key deleted successfully"
  }
}

```

3. 執行具有金鑰的唯一 label 屬性的 key list 命令並確認金鑰已被刪除。如下列範例所示，HSM 叢集中沒有含標籤 my_key_to_delete 的金鑰：

```

aws-cloudhsm > key list --filter attr.label="my_key_to_delete"
{
  "error_code": 0,
  "data": {
    "matched_keys": [],
    "total_key_count": 0,
    "returned_key_count": 0
  }
}

```

```
}  
}
```

相關主題

- [CloudHSM CLI 的金鑰屬性](#)
- [使用 CloudHSM CLI 刪除金鑰](#)

使用 CloudHSM CLI 共用和取消共用金鑰

使用本主題中的命令在 [CloudHSM CLI](#) 中共用和取消共用金鑰。在 AWS CloudHSM 中，建立金鑰的加密使用者 (CU) 擁有金鑰。擁有者可以使用 `key share` 和 `key unshare` 命令來與其他 CU 共用和取消共用金鑰。共用金鑰的使用者可以在密碼編譯操作中使用此金鑰，但無法匯出金鑰、刪除金鑰，或再與其他使用者共用。

共用金鑰前，請以擁有金鑰的加密使用者 (CU) 身分登入 HSM。

主題

- [範例：共用和停止共用金鑰](#)
- [相關主題](#)

範例：共用和停止共用金鑰

Example

以下示例顯示如何與加密使用者 (CU) `alice` 共用和取消共用金鑰。除 `key share` 和 `key unshare` 命令外，共用和取消共用命令還需要使用 [CloudHSM CLI 金鑰篩選條件](#) 的特定金鑰以及要與之共用或取消共用金鑰的使用者的特定使用者名稱。

1. 先用篩選條件執行 `key list` 命令以傳回特定金鑰並查看已與誰共用金鑰。

```
aws-cloudhsm > key list --filter attr.label="rsa_key_to_share" --verbose  
{  
  "error_code": 0,  
  "data": {  
    "matched_keys": [  
      {  
        "key-reference": "0x000000000001c0686",
```

```
"key-info": {
  "key-owners": [
    {
      "username": "cu3",
      "key-coverage": "full"
    }
  ],
  "shared-users": [
    {
      "username": "cu2",
      "key-coverage": "full"
    },
    {
      "username": "cu1",
      "key-coverage": "full"
    },
    {
      "username": "cu4",
      "key-coverage": "full"
    },
    {
      "username": "cu5",
      "key-coverage": "full"
    },
    {
      "username": "cu6",
      "key-coverage": "full"
    },
    {
      "username": "cu7",
      "key-coverage": "full"
    }
  ],
  "key-quorum-values": {
    "manage-key-quorum-value": 0,
    "use-key-quorum-value": 0
  },
  "cluster-coverage": "full"
},
"attributes": {
  "key-type": "rsa",
  "label": "rsa_key_to_share",
  "id": "",
  "check-value": "0xae8ff0",
```

```

        "class": "private-key",
        "encrypt": false,
        "decrypt": true,
        "token": true,
        "always-sensitive": true,
        "derive": false,
        "destroyable": true,
        "extractable": true,
        "local": true,
        "modifiable": true,
        "never-extractable": false,
        "private": true,
        "sensitive": true,
        "sign": true,
        "trusted": false,
        "unwrap": true,
        "verify": false,
        "wrap": false,
        "wrap-with-trusted": false,
        "key-length-bytes": 1219,
        "public-exponent": "0x010001",
        "modulus":
"0xa8855cba933cec0c21a4df0450ec31675c024f3e65b2b215a53d2bda6dcd191f75729150b59b4d86df58254
        "modulus-size-bits": 2048
    }
}
],
"total_key_count": 1,
"returned_key_count": 1
}
}

```

2. 檢視 `shared-users` 輸出以識別金鑰目前與誰共用。
3. 如要與加密使用者 (CU) `alice` 共享此金鑰，請輸入以下命令：

```

aws-cloudhsm > key share --filter attr.label="rsa_key_to_share" attr.class=private-
key --username alice --role crypto-user
{
  "error_code": 0,
  "data": {
    "message": "Key shared successfully"
  }
}

```

請注意，除 key share 命令外，此命令還使用金鑰的唯一標籤以及與其共用金鑰的使用者名稱。

4. 執行 key list 命令以確認金鑰已與 alice 共用：

```
aws-cloudhsm > key list --filter attr.label="rsa_key_to_share" --verbose
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x000000000001c0686",
        "key-info": {
          "key-owners": [
            {
              "username": "cu3",
              "key-coverage": "full"
            }
          ],
          "shared-users": [
            {
              "username": "cu2",
              "key-coverage": "full"
            },
            {
              "username": "cu1",
              "key-coverage": "full"
            },
            {
              "username": "cu4",
              "key-coverage": "full"
            },
            {
              "username": "cu5",
              "key-coverage": "full"
            },
            {
              "username": "cu6",
              "key-coverage": "full"
            },
            {
              "username": "cu7",
              "key-coverage": "full"
            }
          ]
        }
      }
    ]
  }
}
```

```

        {
            "username": "alice",
            "key-coverage": "full"
        }
    ],
    "key-quorum-values": {
        "manage-key-quorum-value": 0,
        "use-key-quorum-value": 0
    },
    "cluster-coverage": "full"
},
"attributes": {
    "key-type": "rsa",
    "label": "rsa_key_to_share",
    "id": "",
    "check-value": "0xae8ff0",
    "class": "private-key",
    "encrypt": false,
    "decrypt": true,
    "token": true,
    "always-sensitive": true,
    "derive": false,
    "destroyable": true,
    "extractable": true,
    "local": true,
    "modifiable": true,
    "never-extractable": false,
    "private": true,
    "sensitive": true,
    "sign": true,
    "trusted": false,
    "unwrap": true,
    "verify": false,
    "wrap": false,
    "wrap-with-trusted": false,
    "key-length-bytes": 1219,
    "public-exponent": "0x010001",
    "modulus":
"0xa8855cba933cec0c21a4df0450ec31675c024f3e65b2b215a53d2bda6dcd191f75729150b59b4d86df58254
    "modulus-size-bits": 2048
}
}
],
"total_key_count": 1,

```



```
    "returned_key_count": 1
  }
}
```

5. 若要與 alice 取消共用相同的金鑰，請執行下列 unshare 命令：

```
aws-cloudhsm > key unshare --filter attr.label="rsa_key_to_share"
attr.class=private-key --username alice --role crypto-user
{
  "error_code": 0,
  "data": {
    "message": "Key unshared successfully"
  }
}
```

請注意，除 key unshare 命令外，此命令還使用金鑰的唯一標籤以及與其共用金鑰的使用者名稱。

6. 再次執行 key list 命令並確認是否未與加密使用者 alice 共用金鑰：

```
aws-cloudhsm > key list --filter attr.label="rsa_key_to_share" --verbose
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x000000000001c0686",
        "key-info": {
          "key-owners": [
            {
              "username": "cu3",
              "key-coverage": "full"
            }
          ],
          "shared-users": [
            {
              "username": "cu2",
              "key-coverage": "full"
            },
            {
              "username": "cu1",
              "key-coverage": "full"
            }
          ]
        }
      }
    ]
  }
}
```

```
        "username": "cu4",
        "key-coverage": "full"
    },
    {
        "username": "cu5",
        "key-coverage": "full"
    },
    {
        "username": "cu6",
        "key-coverage": "full"
    },
    {
        "username": "cu7",
        "key-coverage": "full"
    },
],
"key-quorum-values": {
    "manage-key-quorum-value": 0,
    "use-key-quorum-value": 0
},
"cluster-coverage": "full"
},
"attributes": {
    "key-type": "rsa",
    "label": "rsa_key_to_share",
    "id": "",
    "check-value": "0xae8ff0",
    "class": "private-key",
    "encrypt": false,
    "decrypt": true,
    "token": true,
    "always-sensitive": true,
    "derive": false,
    "destroyable": true,
    "extractable": true,
    "local": true,
    "modifiable": true,
    "never-extractable": false,
    "private": true,
    "sensitive": true,
    "sign": true,
    "trusted": false,
    "unwrap": true,
    "verify": false,
```

```
        "wrap": false,
        "wrap-with-trusted": false,
        "key-length-bytes": 1219,
        "public-exponent": "0x010001",
        "modulus":
    "0xa8855cba933cec0c21a4df0450ec31675c024f3e65b2b215a53d2bda6dcd191f75729150b59b4d86df58254",
        "modulus-size-bits": 2048
    }
}
],
"total_key_count": 1,
"returned_key_count": 1
}
}
```

相關主題

- [CloudHSM CLI 的金鑰屬性](#)
- [使用 CloudHSM CLI 共用金鑰](#)
- [使用 CloudHSM CLI 取消共用金鑰](#)
- [使用 CloudHSM CLI 篩選金鑰](#)

使用 CloudHSM CLI 篩選金鑰

使用下列主要命令，將標準化金鑰篩選機制用於 [CloudHSM CLI](#)。

- key list
- key delete
- key share
- key unshare
- key set-attribute

若要使用 CloudHSM CLI 選取和/或篩選金鑰，主要命令會根據 [CloudHSM CLI 的金鑰屬性](#) 使用標準化篩選機制。金鑰或一組金鑰可以使用可識別單一金鑰或多個金鑰的一或多個 AWS CloudHSM 屬性，在金鑰命令中指定。金鑰篩選機制只會在目前登入使用者擁有和共用的金鑰，以及 AWS CloudHSM 叢集中的所有公有金鑰上運作。

主題

- [要求](#)
- [篩選以尋找單一金鑰](#)
- [篩選錯誤](#)
- [相關主題](#)

要求

若要篩選金鑰，您必須以加密使用者 (CU) 的身分登入。

篩選以尋找單一金鑰

請注意，在下面的範例中，用作篩選條件的每個屬性都必須以 `attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` 的形式寫入。例如，如果您想透過標籤屬性進行篩選，您會寫入 `attr.label=my_label`。

Example 使用單個屬性來尋找單一金鑰

此範例示範如何篩選為僅使用單一識別屬性的單一唯一金鑰。

```
aws-cloudhsm > key list --filter attr.label="my_unique_key_label" --verbose
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x000000000001c0686",
        "key-info": {
          "key-owners": [
            {
              "username": "cu1",
              "key-coverage": "full"
            }
          ],
          "shared-users": [
            {
              "username": "alice",
              "key-coverage": "full"
            }
          ],
          "key-quorum-values": {
```

```

        "manage-key-quorum-value": 0,
        "use-key-quorum-value": 0
    },
    "cluster-coverage": "full"
},
"attributes": {
    "key-type": "rsa",
    "label": "my_unique_key_label",
    "id": "",
    "check-value": "0xae8ff0",
    "class": "private-key",
    "encrypt": false,
    "decrypt": true,
    "token": true,
    "always-sensitive": true,
    "derive": false,
    "destroyable": true,
    "extractable": true,
    "local": true,
    "modifiable": true,
    "never-extractable": false,
    "private": true,
    "sensitive": true,
    "sign": true,
    "trusted": false,
    "unwrap": true,
    "verify": false,
    "wrap": false,
    "wrap-with-trusted": false,
    "key-length-bytes": 1219,
    "public-exponent": "0x010001",
    "modulus":
"0xa8855cba933cec0c21a4df0450ec31675c024f3e65b2b215a53d2bda6dcd191f75729150b59b4d86df58254c8f5
    "modulus-size-bits": 2048
}
}
],
"total_key_count": 1,
"returned_key_count": 1
}
}

```

Example 使用多個屬性尋找單一金鑰

以下範例示範如何使用多個金鑰屬性尋找單一金鑰。

```
aws-cloudhsm > key list --filter attr.key-type=rsa attr.class=private-key attr.check-  
value=0x29bbd1 --verbose  
{  
  "error_code": 0,  
  "data": {  
    "matched_keys": [  
      {  
        "key-reference": "0x00000000000540011",  
        "key-info": {  
          "key-owners": [  
            {  
              "username": "cu3",  
              "key-coverage": "full"  
            }  
          ],  
          "shared-users": [  
            {  
              "username": "cu2",  
              "key-coverage": "full"  
            }  
          ],  
          "key-quorum-values": {  
            "manage-key-quorum-value": 0,  
            "use-key-quorum-value": 0  
          },  
          "cluster-coverage": "full"  
        },  
        "attributes": {  
          "key-type": "rsa",  
          "label": "my_crypto_user",  
          "id": "",  
          "check-value": "0x29bbd1",  
          "class": "my_test_key",  
          "encrypt": false,  
          "decrypt": true,  
          "token": true,  
          "always-sensitive": true,  
          "derive": false,  
          "destroyable": true,  
          "extractable": true,  
        }  
      }  
    ]  
  }  
}
```

```

        "local": true,
        "modifiable": true,
        "never-extractable": false,
        "private": true,
        "sensitive": true,
        "sign": true,
        "trusted": false,
        "unwrap": true,
        "verify": false,
        "wrap": false,
        "wrap-with-trusted": false,
        "key-length-bytes": 1217,
        "public-exponent": "0x010001",
        "modulus":
"0x8b3a7c20618e8be08220ed8ab2c8550b65fc1aad8d4cf04fbf2be685f97eeb78fcbbad9b02cd91a3b15e990c2a7
        "modulus-size-bits": 2048
    }
}
],
"total_key_count": 1,
"returned_key_count": 1
}
}

```

Example 篩選以尋找一組金鑰

以下範例示範如何篩選以尋找一組私有 rsa 金鑰。

```

aws-cloudhsm > key list --filter attr.key-type=rsa attr.class=private-key --verbose
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x000000000001c0686",
        "key-info": {
          "key-owners": [
            {
              "username": "my_crypto_user",
              "key-coverage": "full"
            }
          ],
          "shared-users": [
            {

```

```

        "username": "cu2",
        "key-coverage": "full"
    },
    {
        "username": "cu1",
        "key-coverage": "full"
    },
],
"key-quorum-values": {
    "manage-key-quorum-value": 0,
    "use-key-quorum-value": 0
},
"cluster-coverage": "full"
},
"attributes": {
    "key-type": "rsa",
    "label": "rsa_key_to_share",
    "id": "",
    "check-value": "0xae8ff0",
    "class": "private-key",
    "encrypt": false,
    "decrypt": true,
    "token": true,
    "always-sensitive": true,
    "derive": false,
    "destroyable": true,
    "extractable": true,
    "local": true,
    "modifiable": true,
    "never-extractable": false,
    "private": true,
    "sensitive": true,
    "sign": true,
    "trusted": false,
    "unwrap": true,
    "verify": false,
    "wrap": false,
    "wrap-with-trusted": false,
    "key-length-bytes": 1219,
    "public-exponent": "0x010001",
    "modulus":
"0xa8855cba933cec0c21a4df0450ec31675c024f3e65b2b215a53d2bda6dcd191f75729150b59b4d86df58254c8f5
    "modulus-size-bits": 2048
}

```



```
},
{
  "key-reference": "0x00000000000540011",
  "key-info": {
    "key-owners": [
      {
        "username": "my_crypto_user",
        "key-coverage": "full"
      }
    ],
    "shared-users": [
      {
        "username": "cu2",
        "key-coverage": "full"
      }
    ],
    "key-quorum-values": {
      "manage-key-quorum-value": 0,
      "use-key-quorum-value": 0
    },
    "cluster-coverage": "full"
  },
  "attributes": {
    "key-type": "rsa",
    "label": "my_test_key",
    "id": "",
    "check-value": "0x29bbd1",
    "class": "private-key",
    "encrypt": false,
    "decrypt": true,
    "token": true,
    "always-sensitive": true,
    "derive": false,
    "destroyable": true,
    "extractable": true,
    "local": true,
    "modifiable": true,
    "never-extractable": false,
    "private": true,
    "sensitive": true,
    "sign": true,
    "trusted": false,
    "unwrap": true,
    "verify": false,
```

```

        "wrap": false,
        "wrap-with-trusted": false,
        "key-length-bytes": 1217,
        "public-exponent": "0x010001",
        "modulus":
"0x8b3a7c20618e8be08220ed8ab2c8550b65fc1aad8d4cf04fbf2be685f97eeb78fcbbad9b02cd91a3b15e990c2a7
        "modulus-size-bits": 2048
    }
}
],
"total_key_count": 2,
"returned_key_count": 2
}
}

```

篩選錯誤

某些金鑰作業一次只能在單一金鑰上執行。對於這些操作，CloudHSM CLI 會在篩選條件未充分細化且多個金鑰符合準則時報錯。一個此類範例與金鑰刪除如下所示。

Example 匹配太多金鑰時篩選錯誤

```

aws-cloudhsm > key delete --filter attr.key-type=rsa
{
  "error_code": 1,
  "data": "Key selection criteria matched 48 keys. Refine selection criteria to select
a single key."
}

```

相關主題

- [CloudHSM CLI 的金鑰屬性](#)

使用 CloudHSM CLI 將金鑰標記為信任

本節中的內容提供如何使用 CloudHSM CLI 將金鑰標記為可信任的說明。

1. 使用 [CloudHSM CLI login 命令](#)，以加密使用者 (CU) 身分登入。
2. 使用 `key list` 命令來識別您要標記為可信任的金鑰的金鑰參照。下列範例會列出含有標籤 `key_to_be_trusted` 的金鑰。

```
aws-cloudhsm > key list --filter attr.label=test_aes_trusted
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x00000000000200333",
        "attributes": {
          "label": "test_aes_trusted"
        }
      }
    ],
    "total_key_count": 1,
    "returned_key_count": 1
  }
}
```

3. 使用 [使用 CloudHSM CLI 登出 HSM](#) 命令，以加密使用者 (CU) 的身分登出。
4. 使用 [使用 CloudHSM CLI 登入 HSM](#) 命令，以管理員身分登入。
5. 使用 [key set-attribute](#) 命令搭配您在步驟 2 中識別的金鑰參照，將金鑰的信任值設定為 true：

```
aws-cloudhsm > key set-attribute --filter key-reference=<Key Reference> --name
trusted --value true
{
  "error_code": 0,
  "data": {
    "message": "Attribute set successfully"
  }
}
```

使用 CloudHSM CLI 管理規定人數身分驗證 (M of N 存取控制)

AWS CloudHSM 叢集中的硬體安全模組 (HSMs) 支援規定人數身分驗證，也稱為 M of N 存取控制。透過規定人數身分驗證，HSM 上沒有任何單一使用者可以執行規定人數控制的操作。相對地，必須有最低數量的 HSM 使用者 (至少 2 個) 合作來執行這些操作。配額身分驗證需要多個 HSM 使用者的核准，以新增額外的保護層。

規定人數身分驗證可以控制以下操作：

- [加密使用者的 HSM 金鑰使用和管理](#) – 使用金鑰建立簽章，或包裝、取消包裝、共用、取消共用和設定金鑰的屬性。

重要考量

- HSM 使用者可以簽署自己的規定人數權杖，即：要求的使用者可以針對規定人數身分驗證提供其中一個需要的核准。
- 您可以針對由規定人數控制的操作選擇最低數量的規定人數核准者。您可以選擇的最小數字是二 (2)，您可以選擇的最大數字是八 (8)。
- HSM 最多可存放 1,024 個規定人數字符。如果您在嘗試建立新的字符時 HSM 已有 1,024 個字符，HSM 會清除其中一個過期字符。在預設情況下，字符會在建立後的十分鐘後過期。
- 如果啟用多重要素驗證 (MFA)，叢集會使用相同的金鑰進行規定人數身分驗證和 MFA。如需使用規定人數身分驗證和 MFA 的詳細資訊，請參閱[使用 CloudHSM CLI 管理 MFA](#)。
- 每個 HSM 一次只能包含一個字符，但每個加密使用者服務只能包含多個字符。

下列主題提供 AWS CloudHSM 中的規定人數身分驗證的詳細資訊。

主題

- [CloudHSM CLI 的配額身分驗證程序](#)
- [支援使用 CloudHSM CLI 進行規定人數身分驗證 AWS CloudHSM 的服務名稱和類型](#)
- [使用 CloudHSM CLI 為 AWS CloudHSM 加密使用者設定規定人數身分驗證](#)
- [啟用規定人數身分驗證以 AWS CloudHSM 使用 CloudHSM CLI 的金鑰管理和用量](#)

CloudHSM CLI 的配額身分驗證程序

下列步驟摘要說明 CloudHSM CLI 的規定人數身分驗證程序。如需特定步驟和工具，請參閱 [啟用規定人數身分驗證以 AWS CloudHSM 使用 CloudHSM CLI 的金鑰管理和用量](#)。

1. 每個硬體安全模組 (HSM) 使用者都會建立非對稱金鑰以進行簽署。使用者會在 HSM 外部執行此動作，以適當方式保護金鑰。
2. 每個 HSM 使用者會登入 HSM，並向 HSM 註冊使用者的簽署金鑰 (公有金鑰) 的公有部分。
3. HSM 使用者想要執行由規定人數控制的操作時，使用者會登入 HSM，並取得規定人數權杖。
4. HSM 使用者會將規定人數字符提供給一或多個其他 HSM 使用者，並要求其核准。

5. 其他 HSM 使用者透過使用自己的金鑰以密碼編譯方式簽署規定人數字符來進行核准。這是在 HSM 外部進行。
6. 當 HSM 使用者具有所需的核准數目時，相同的使用者會登入 HSM 並使用 --approval 引數執行規定人數控制的操作，並提供已簽署的規定人數權杖檔案，其中包含所有必要的核准 (簽章)。
7. HSM 會使用每個簽署者註冊的公有金鑰來驗證簽章。如果簽章有效，HSM 會核准權杖，並執行規定人數控制的操作。

支援使用 CloudHSM CLI 進行規定人數身分驗證 AWS CloudHSM 的服務名稱和類型

管理員服務：規定人數身分驗證用於管理員特殊權限服務，例如建立使用者、刪除使用者、變更使用者密碼、設定規定人數值，以及停用規定人數和 MFA 功能。

加密使用者服務：Quorum 身分驗證用於與特定金鑰相關聯的加密使用者權限服務，例如使用金鑰簽署、共用/取消共用金鑰、包裝/取消包裝金鑰，以及設定金鑰的屬性。產生、匯入或取消包裝金鑰時，會設定關聯金鑰的規定人數值。規定人數值必須等於或小於與金鑰相關聯的使用者數量，其中包括與金鑰共用的使用者和金鑰擁有者。

每種服務類型都會進一步細分為合格的服務名稱，這包含一組特定的可執行法定人數支援的服務操作。

服務名稱	服務類型	服務操作
使用者	管理員	• 建立使用者 • 刪除使用者 • 變更使用者密碼 • 變更使用者 MFA
規定人數	管理員	• 規定人數字符簽署 設定規定人數值
cluster ¹	管理員	• 叢集 mtls register-trust-anchor • 叢集 mtls deregister-trust-anchor • 叢集 mtls 設定強制執行
金鑰管理	加密使用者	• 金鑰包裝 • 金鑰取消包裝

服務名稱	服務類型	服務操作
		• 共用金鑰 • 取消共用金鑰 • 設定金鑰屬性
key-usage	加密使用者	• 鍵符號

【1】叢集服務僅在 hsm2m.medium 上提供

使用 CloudHSM CLI 為 AWS CloudHSM 加密使用者設定規定人數身分驗證

這些主題說明如何將 CloudHSM 設定為由[加密使用者](#)進行規定人數身分驗證。在初始設定期間執行這些步驟一次。如需後續金鑰管理和使用，請參閱[啟用規定人數身分驗證以 AWS CloudHSM 使用 CloudHSM CLI 的金鑰管理和用量](#)。

主題

- [先決條件](#)
- [步驟 1. 建立和註冊用於簽署的金鑰](#)
- [步驟 2. 在產生金鑰期間設定金鑰規定人數值](#)

先決條件

- 熟悉 [CloudHSM CLI](#)

步驟 1. 建立和註冊用於簽署的金鑰

若要使用規定人數身分驗證，每個加密使用者都必須完成所有以下步驟：

主題

- [建立 RSA 金鑰對](#)
- [建立註冊字符](#)
- [簽署未簽署的註冊字符](#)
- [用 HSM 註冊公有金鑰](#)

建立 RSA 金鑰對

建立和保護金鑰對有許多不同的方式。下列範例示範使用 [OpenSSL](#) 的做法。

Example – 使用 OpenSSL 建立私有金鑰

下列範例示範如何使用 OpenSSL 建立 2048 位元 RSA 金鑰。若要使用此範例，請將 `<crypto_user1.key>` 取代為您要存放金鑰的檔案名稱。

```
$ openssl genrsa -out <crypto_user1.key>
Generating RSA private key, 2048 bit long modulus
.....+++
.+++
e is 65537 (0x10001)
```

接下來，使用您剛建立的私有金鑰來產生公有金鑰。

Example – 使用 OpenSSL 建立一個公有金鑰

下列範例會示範如何使用 OpenSSL 根據您剛建立的私有金鑰建立公有金鑰。

```
$ openssl rsa -in crypto_user1.key -outform PEM -pubout -out crypto_user1.pub
writing RSA key
```

建立註冊字符

您可以建立一個權杖並使用在上一步中剛產生的私有金鑰簽署該權杖。

建立註冊字符

1. 使用以下命令來啟動 CloudHSM CLI：

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 透過執行[產生規定人數權杖簽署](#)命令建立註冊權杖：

```
aws-cloudhsm > quorum token-sign generate --service registration --token /path/
tokenfile
{
  "error_code": 0,
  "data": {
    "path": "/path/tokenfile"
  }
}
```

3. [產生規定人數權杖簽署](#)命令在指定的檔案路徑產生註冊權杖。檢查權杖檔案：

```
$ cat /path/tokenfile
{
  "version": "2.0",
  "tokens": [
    {
      "approval_data": <approval data in base64 encoding>,
      "unsigned": <unsigned token in base64 encoding>,
      "signed": ""
    }
  ]
}
```

權杖檔案由以下項目組成：

- approval_data：一個 base64 編碼的隨機資料權杖，其原始資料不超過 245 個位元組的最大值。
- unsigned：核准資料的 base64 編碼和 SHA256 雜湊權杖。
- signed：未簽署的權杖的 base64 編碼簽名權杖 (簽名)，使用先前使用 OpenSSL 產生的 RSA 2048 位元私有金鑰。

您可以使用私有金鑰簽署未簽署的權杖，以證明您可以訪問私有金鑰。您需要完整填入簽章和公有金鑰的註冊字符檔案，才能向 AWS CloudHSM 叢集將加密使用者註冊為規定人數使用者。

簽署未簽署的註冊字符

1. 解碼 base64 編碼的未簽署權杖並將其放入二進位檔案中：


```
$ echo -n '6BMUj6mUjjko6ZLCEdzG1WpR5sILhFJfqhW1ej30q1g=' | base64 -d >
crypto_user.bin
```

2. 使用 OpenSSL 和私有金鑰來簽署現在的二進位未簽署註冊權杖，並建立一個二進位簽署檔案：

```
$ openssl pkeyutl -sign \
-inkey crypto_user1.key \
-pkeyopt digest:sha256 \
-keyform PEM \
-in crypto_user.bin \
-out crypto_user.sig.bin
```

3. 將二進位簽章編碼為 base64：

```
$ base64 -w0 crypto_user.sig.bin > crypto_user.sig.b64
```

4. 將 base64 編碼的簽名複製並粘貼到權杖檔案中：

```
{
  "version": "2.0",
  "tokens": [
    {
      "approval_data": <approval data in base64 encoding>,
      "unsigned": <unsigned token in base64 encoding>,
      "signed": <signed token in base64 encoding>
    }
  ]
}
```

用 HSM 註冊公有金鑰

建立金鑰後，加密使用者必須向 AWS CloudHSM 叢集註冊公有金鑰。

1. 啟動 CloudHSM CLI：

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 以您要註冊其公有金鑰的加密使用者身分登入。

```
aws-cloudhsm > login --username crypto_user1 --role crypto-user
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "crypto_user1",
    "role": "crypto-user"
  }
}
```

3. 向註冊公有金鑰使用 [CloudHSM CLI 註冊使用者的字符簽署規定人數策略](#)。如需詳細資訊，請參閱下列範例或使用 `help user change-quorum token-sign register` 命令。

Example – 向 AWS CloudHSM 叢集註冊公有金鑰

下列範例顯示如何在 CloudHSM CLI 中使用 `user change-quorum token-sign register` 命令向 HSM 註冊加密使用者公有金鑰。若要使用此命令，加密使用者必須登入 HSM。以您自己的值取代這些值：

```
aws-cloudhsm > user change-quorum token-sign register --public-key </path/
crypto_user.pub> --signed-token </path/tokenfile>
{
  "error_code": 0,
  "data": {
    "username": "crypto_user1",
    "role": "crypto-user"
  }
}
```

Note

/path/crypto_user.pub：公有金鑰 PEM 檔案的檔案路徑

必要：是

/path/token_file：具有使用者私有金鑰簽署字符的 filepath

必要：是

4. 所有加密使用者註冊其公有金鑰後，`user list`命令的輸出會在規定人數欄位中顯示，指出使用中的啟用規定人數策略。

在此範例中，AWS CloudHSM 叢集有兩個 HSMs，每個 HSM 都有相同的加密使用者，如 `user list`命令的下列輸出所示。如需有關建立使用者的詳細資訊，請參閱[使用 CloudHSM CLI 進行使用者管理](#)。

```
aws-cloudhsm > user list
{
  "error_code": 0,
  "data": {
    "users": [
      {
        "username": "admin",
        "role": "admin",
        "locked": "false",
        "mfa": [],
        "quorum": [],
        "cluster-coverage": "full"
      },
      {
        "username": "crypto_user1",
        "role": "crypto-user",
        "locked": "false",
        "mfa": [],
        "quorum": [
          {
            "strategy": "token-sign",
            "status": "enabled"
          }
        ],
        "cluster-coverage": "full"
      },
      {
        "username": "crypto_user2",
        "role": "crypto-user",
        "locked": "false",
        "mfa": [],
        "quorum": [
          {
            "strategy": "token-sign",
```

```

        "status": "enabled"
    },
    ],
    "cluster-coverage": "full"
},
{
    "username": "crypto_user3",
    "role": "crypto-user",
    "locked": "false",
    "mfa": [],
    "quorum": [
        {
            "strategy": "token-sign",
            "status": "enabled"
        }
    ],
    "cluster-coverage": "full"
},
{
    "username": "app_user",
    "role": "internal(APPLIANCE_USER)",
    "locked": "false",
    "mfa": [],
    "quorum": [],
    "cluster-coverage": "full"
}
]
}
}

```

步驟 2. 在產生金鑰期間設定金鑰規定人數值

若要使用規定人數身分驗證，加密使用者必須登入 HSM，然後設定相關聯的金鑰規定人數值。這是執行 HSM 金鑰管理/用量操作所需的加密使用者核准數目下限。如需與金鑰管理或金鑰用量相關聯之金鑰命令的詳細資訊，請參閱 [支援的服務和類型](#)。

產生已設定金鑰規定人數值的金鑰對

1. 使用下列命令來啟動 CloudHSM CLI：

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 CloudHSM CLI，以加密使用者身分登入。

```
aws-cloudhsm > login --username crypto_user1 --role crypto-user
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "crypto_user1",
    "role": "crypto-user"
  }
}
```

此範例會產生 RSA 金鑰對，其針對金鑰管理和金鑰使用操作設定了兩 (2) 個金鑰規定人數值。您可以選擇從零 (0) 到八 (8) 的任何值，直到 HSM 上的加密使用者總數為止。在此範例中，HSM 有三 (3) 個加密使用者，因此可能的值上限為三 (3) 個。請注意，在此範例中，我們會在金鑰產生期間與 *<crypto_user2>* 共用金鑰。另請注意，公有金鑰沒有規定人數值。

```
aws-cloudhsm > key generate-asymmetric-pair rsa \
--public-exponent 65537 \
--modulus-size-bits 2048 \
--public-label rsa-public-key-example \
--private-label rsa-private-key-example \
--public-attributes verify=true \
--private-attributes sign=true
--share-crypto-users crypto_user2 \
--manage-private-key-quorum-value 2 \
--use-private-key-quorum-value 2
{
  "error_code": 0,
  "data": {
    "public_key": {
      "key-reference": "0x00000000000640006",
```

```

"key-info": {
  "key-owners": [
    {
      "username": "crypto_user",
      "key-coverage": "full"
    }
  ],
  "shared-users": [],
  "key-quorum-values": {
    "manage-key-quorum-value": 0,
    "use-key-quorum-value": 0
  },
  "cluster-coverage": "full"
},
"attributes": {
  "key-type": "rsa",
  "label": "rsa-public-key-example",
  "id": "0x",
  "check-value": "0x218f50",
  "class": "public-key",
  "encrypt": false,
  "decrypt": false,
  "token": true,
  "always-sensitive": false,
  "derive": false,
  "destroyable": true,
  "extractable": true,
  "local": true,
  "modifiable": true,
  "never-extractable": false,
  "private": true,
  "sensitive": false,
  "sign": false,
  "trusted": false,
  "unwrap": false,
  "verify": true,
  "wrap": false,
  "wrap-with-trusted": false,
  "key-length-bytes": 512,
  "public-exponent": "0x010001",
  "modulus":
"0xbdf471a3d2a869492f51c767bece8780730ae6479a9a75efffe7cea3594fb28ca518630e7b1d988b45d2fedc830",
  "modulus-size-bits": 2048
}

```

```
},
"private_key": {
  "key-reference": "0x00000000000640007",
  "key-info": {
    "key-owners": [
      {
        "username": "crypto_user",
        "key-coverage": "full"
      }
    ],
    "shared-users": [
      {
        "username": "crypto_user2",
        "key-coverage": "full"
      }
    ],
    "key-quorum-values": {
      "manage-key-quorum-value": 2,
      "use-key-quorum-value": 2
    },
    "cluster-coverage": "full"
  },
  "attributes": {
    "key-type": "rsa",
    "label": "rsa-private-key-example",
    "id": "0x",
    "check-value": "0x218f50",
    "class": "private-key",
    "encrypt": false,
    "decrypt": false,
    "token": true,
    "always-sensitive": true,
    "derive": false,
    "destroyable": true,
    "extractable": true,
    "local": true,
    "modifiable": true,
    "never-extractable": false,
    "private": true,
    "sensitive": true,
    "sign": true,
    "trusted": false,
    "unwrap": false,
    "verify": false,
```

```

    "wrap": false,
    "wrap-with-trusted": false,
    "key-length-bytes": 1216,
    "public-exponent": "0x010001",
    "modulus":
      "0xbdf471a3d2a869492f51c767bece8780730ae6479a9a75efffe7cea3594fb28ca518630e7b1d988b45d2fedc830
      "modulus-size-bits": 2048
  }
}
}
}

```

使用規定人數控制產生金鑰時，該金鑰必須與等於最大金鑰規定人數值的最小使用者數目相關聯。關聯的使用者包括金鑰擁有者和與金鑰共用的加密使用者。若要判斷要共用金鑰的最小使用者數量，請取得金鑰使用量值與金鑰管理規定人數值之間的最大規定人數值，並減去 1 以考慮金鑰擁有者，該擁有者預設與金鑰相關聯。若要與更多使用者共用金鑰，請使用 [使用 CloudHSM CLI 共用金鑰](#) 命令。

無法在金鑰產生時與足夠的使用者共用金鑰會導致失敗，如下所示。

```

aws-cloudhsm > key generate-asymmetric-pair rsa \
--public-exponent 65537 \
--modulus-size-bits 2048 \
--public-label rsa-public-key-example \
--private-label rsa-private-key-example \
--public-attributes verify=true \
--private-attributes sign=true
--share-crypto-users crypto_user2 crypto_user3 \
--manage-private-key-quorum-value 3 \
--use-private-key-quorum-value 4
{
  "error_code": 1,
  "data": "Invalid quorum value provided."
}

```

啟用規定人數身分驗證以 AWS CloudHSM 使用 CloudHSM CLI 的金鑰管理和用量

為 AWS CloudHSM 叢集設定規定人數身分驗證之後，如果加密使用者的金鑰具有相關聯的規定人數值，則無法自行執行 HSM 金鑰管理或使用操作。本主題說明加密使用者如何取得臨時字符來執行 HSM 金鑰管理或金鑰使用操作。

Note

每個規定人數字符對一個操作有效。當該操作成功時，字符不再有效，且加密使用者必須取得新的字符。規定人數字符僅在您目前的登入工作階段期間有效。如果您登出 CloudHSM CLI 或網路中斷連線，字符將不再有效，您需要取得新的字符。您只能在 CloudHSM CLI 中使用 CloudHSM 字符。您無法用它在不同的應用程式中進行身分驗證。

下列範例顯示設定規定人數身分驗證後，加密使用者嘗試在 HSM 上建立具有規定人數相關金鑰的簽章時的輸出。命令失敗並出現 Quorum Failed 錯誤，這表示規定人數身分驗證失敗：

```
aws-cloudhsm > crypto sign rsa-pkcs --key-filter attr.label=rsa-private-key-example --  
hash-function sha256 --data YWJjMTIz  
{  
  "error_code": 1,  
  "data": "Quorum Failed"  
}
```

加密使用者必須完成下列任務，才能取得在 HSM 上執行金鑰管理或金鑰使用操作的臨時權杖：

步驟

- [步驟 1. 取得規定人數字符](#)
- [步驟 2. 從核准加密使用者取得簽章](#)
- [步驟 3. 在 CloudHSM 叢集上核准權杖並執行操作](#)

步驟 1. 取得規定人數字符

1. 啟動 CloudHSM CLI。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 以加密使用者身分登入叢集。

```
aws-cloudhsm > login --username <crypto_user1> --role crypto-user --
password password123
```

此範例使用 `crypto-user` 角色 `crypto_user1` 登入 CloudHSM CLI。將這些值取代為您自己的值。

```
{
  "error_code": 0,
  "data": {
    "username": "crypto_user1",
    "role": "crypto-user"
  }
}
```

3. 使用 `quorum token-sign generate` 命令產生規定人數字符。

在下列命令中，`key-usage` 識別您要用來產生字符的服務名稱。在此情況下，字符適用於金鑰使用操作 (`key-usage` 服務) 此範例使用 `--filter` 旗標將字符與特定金鑰建立關聯。

```
aws-cloudhsm > quorum token-sign generate --service key-usage --token </path/
crypto_user1.token> --filter attr.label=rsa-private-key-example
{
  "error_code": 0,
  "data": {
    "path": "/home/crypto_user1.token"
  }
}
```

此範例會使用使用者名稱取得加密使用者的規定人數字符，`crypto_user1` 並將字符儲存至名為的檔案 `crypto_user1.token`。若要使用範例命令，請將這些值取代為您自己的值：

`quorum token-sign generate` 命令會在指定的檔案路徑產生金鑰使用量服務規定人數字符。您可以檢查權杖檔案：

```
$ cat </path/crypto_user1.token>
{
  "version": "2.0",
  "service": "key-usage",
  "key_reference": "0x00000000000680006",
```

```

    "approval_data":
    "AAIABQAAABkAAAAAGgABi5CDa9x9VyyRIaFbkSrHgJjcnlwdG9fdXNlcmgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
+GJj8gXo9lKuANGNyeXB0b191c2VyAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGc9AEsAAAAAAAAAAAAAA==",
    "token": "5GlgoW0lQU4fw4QIlbxkPGZV0VoDugFGuSKE/k67ncM=",
    "signatures": []
}

```

權杖檔案由以下項目組成：

- 服務：與權杖相關聯的規定人數服務識別符。
- key_reference：與此規定人數字符相關聯的金鑰識別符。
- approval_data：由 HSM 產生的 base64 編碼原始資料權杖。
- token：approval_data 的 base64 編碼和 SHA-256 雜湊權杖
- 簽章：未簽署字符的 base64 編碼簽署字符（簽章）陣列。每個核准者簽章的格式都是 JSON 物件常值：

```

{
    "username": "<APPROVER_USERNAME>",
    "role": "<APPROVER_ROLE>",
    "signature": "<APPROVER_RSA2048_BIT_SIGNATURE>"
}

```

每個簽章都是從核准者的結果，使用其對應的 RSA 2048 位元私有金鑰，其公有金鑰已向 HSM 註冊。

4. 驗證新的使用者服務規定人數字符。quorum token-sign list 命令會確認字符存在於 CloudHSM 上。

```

aws-cloudhsm > quorum token-sign list
{
    "error_code": 0,
    "data": {
        "tokens": [
            {
                "username": "crypto_user",
                "service": "key-usage",
                "key-reference": "0x000000000000680006",
                "minimum-token-count": 2
            }
        ]
    }
}

```

```
}
```

minimum-token-count 會顯示從叢集中單一 HSM 擷取的對應使用者名稱、服務和金鑰參考的最小可用金鑰字符數量的彙總叢集檢視。

例如，假設有一個 2-HSM 叢集，如果我們收到使用者 crypto_user1 為金鑰產生的兩 (2) 個金鑰用量權杖，其中包含叢集中 0x0000000000680006 第一個 HSM 的參考，而我們收到使用者 crypto_user1 為金鑰產生的一 (1) 個金鑰用量權杖，其中包含叢集中另一個 HSM 0x0000000000680006 的參考，則會顯示 "minimum-token-count": 1。

步驟 2. 從核准加密使用者取得簽章

具有規定人數字符的加密使用者必須取得其他加密使用者核准的字符。為了提供核准，另一個加密 users 會使用其簽署金鑰在 HSM 外部以密碼編譯方式簽署字符。

簽署權杖的方式有很多。下列範例示範如何使用 [OpenSSL](#) 簽署權杖。若要使用不同的簽署工具，請確定工具使用 crypto-user 的私有金鑰（簽署金鑰）來簽署權杖的 SHA-256 摘要。

在此範例中，具有字符 (crypto-user) 的加密使用者需要至少兩 (2) 個核准。下列範例命令顯示兩 (2) 個加密使用者如何使用 OpenSSL 以密碼編譯方式簽署字符。

1. 解碼 base64 編碼的未簽署權杖並將其放入二進位檔案中：

```
$echo -n '5G1goW01QU4fw4QI1bxkPGZV0VoDugFGuSKE/k67ncM=' | base64 -d >
crypto_user1.bin
```

2. 使用 OpenSSL 和核准者的私有金鑰來簽署使用者服務的二進位規定人數未簽署字符，並建立二進位簽章檔案：

```
$openssl pkeyutl -sign \
-inkey crypto_user1.key \
-pkeyopt digest:sha256 \
-keyform PEM \
-in crypto_user1.bin \
-out crypto_user1.sig.bin
```

3. 將二進位簽章編碼為 base64：

```
$ base64 -w0 crypto_user1.sig.bin > crypto_user1.sig.b64
```

4. 使用先前為核准者簽章指定的 JSON 物件常值格式，將 base64 編碼的簽章複製並貼到權杖檔案中：

```
{
  "version": "2.0",
  "service": "key-usage",
  "key_reference": "0x00000000000680006",
  "approval_data":
    "AAIABQAAABkAAAAAGgABi5CDa9x9VyyRIaFbkSrHgJjcnlwdG9fdXNlcmgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    +GJj8gXo9lKuANGNyeXB0b191c2VyAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGc9AEsAAAAAAAAAAAAA==",
  "token": "5GlgoW0lQU4fw4QIlbXkPGZV0VoDugFGuSKE/k67ncM=",
  "signatures": [
    {
      "username": "crypto_user1",
      "role": "crypto-user",
      "signature": "wa7aPzmGwBjcEoZ6jAzYASp841Afg0vcI27Y/
tGlCj1E9DawnFw5Uf0IJT2Ca7T5XD2ThVkuI0B+dhAomdqYNl6aUUFrJyH9GBJ
+E0PmA5jNVm25tzeRWBjzneTg4/
zTeE2reNqrHFHicWnttQLe9jS09J1znuDGWDe0HaBKWUaz2gUInJRqmeXDszYdSvZksrqUH5dci/
RsaDE2+tGiS9g0RcIkFbsPW4HpGe2e5HVzGsqrV803PK1YQv6+fymfcNTTuoxKcHAK0jpl43QSuSIu2gVq7KI8mSmmW
+oiukaNfLJr+MoDKzAvCGDg4cDArg=="
    },
    {
      "username": "crypto_user2",
      "role": "crypto-user",
      "signature": "wa7aPzmGwBjcEoZ6jAzYASp841Afg0vcI27Y/
tGlCj1E9DawnFw5Uf0IJT2Ca7T5XD2ThVkuI0B+dhAomdqYNl6aUUFrJyH9GBJ
+E0PmA5jNVm25tzeRWBjzneTg4/
zTeE2reNqrHFHicWnttQLe9jS09J1znuDGWDe0HaBKWUaz2gUInJRqmeXDszYdSvZksrqUH5dci/
RsaDE2+tGiS9g0RcIkFbsPW4HpGe2e5HVzGsqrV803PK1YQv6+fymfcNTTuoxKcHAK0jpl43QSuSIu2gVq7KI8mSmmW
+oiukaNfLJr+MoDKzAvCGDg4cDArg=="
    }
  ]
}
```

步驟 3。在 CloudHSM；叢集上核准權杖並執行 操作

在加密使用者擁有必要的核准和簽章之後，他們可以將該字符連同金鑰管理或金鑰使用操作一起提供給 CloudHSM 叢集。

請確定金鑰操作對應至與規定人數字符相關聯的適當規定人數服務。如需詳細資訊，請參閱 [支援的服務和類型](#)。

在交易期間，字符將在 AWS CloudHSM 叢集內核准，並執行請求的金鑰操作。金鑰操作的成功取決於有效的核准規定人數字符和有效的金鑰操作。

Example 使用 RSA-PKCS 機制產生簽章

在下列範例中，登入的 `crypto-user` 會在 HSM 上建立具有金鑰的簽章：

```
aws-cloudhsm > crypto sign rsa-pkcs --key-filter attr.label=rsa-private-key-example --
hash-function sha256 --data YWJjMTIz --approval /path/crypto_user1.token

{
  "error_code": 0,
  "data": {
    "key-reference": "0x00000000000640007",
    "signature":
    "h6hMqXacBrT3x3MXV13RXHdQno0+IQ6iy0kVrGzo23+eoWT0ZZgrSpBCu5KcuP6IYYHw9goQ5CfPf4jI1n05m/
    IUJtF1A1lmcz0HjEy1CJ7ICXNReDRye0U8m43dkJzt0UdkbtkDJGAcxkbKHLZ02uWsGXaQ8b0KhoGwsRAHHF6nldTXquIC
    +pZmUS38ythybney94Wj6fzY0ER8v7VIY5ijQGa3LfxrjSG4aw6QijEEbno5LSf18ahEaVKmVEnDBL54tylCJBGvGsYSY9H
    TDd2wfvP4PaxbFRyyHaw=="
  }
}
```

如果加密使用者嘗試使用相同的字符執行另一個 HSM 金鑰使用操作，它會失敗：

```
aws-cloudhsm > crypto sign rsa-pkcs --key-filter attr.label=rsa-private-key-example --
hash-function sha256 --data YWJjMTIz --approval /home/crypto_user1.token

{
  "error_code": 1,
  "data": "Quorum approval is required for this operation"
}
```

若要執行另一個 HSM 金鑰操作，加密使用者必須產生新的規定人數字符、從核准者取得新的簽章，並使用 `--核准引數` 執行所需的金鑰操作，以提供規定人數字符。

使用 `quorum token-sign list` 來檢查可用的字符。此範例顯示 `crypto-user` 沒有核准的字符。

```
aws-cloudhsm > quorum token-sign list

{
  "error_code": 0,
  "data": {
    "tokens": []
  }
}
```

```
}
```

使用 AWS CloudHSM KMU 進行金鑰管理

如果使用[最新的 SDK 版本系列](#)，請使用 [CloudHSM CLI](#) 來管理 AWS CloudHSM 叢集中的金鑰。

如果使用[先前的 SDK 版本系列](#)，您可以使用 key_mgmt_util (KMU) 命令列工具來管理 AWS CloudHSM 叢集中硬體安全模組 (HSM) 的金鑰。您必須先啟動 AWS CloudHSM 用戶端、啟動 key_mgmt_util，然後登入 HSMs，才能管理金鑰。如需詳細資訊，請參閱 [key_mgmt_util 的入門指南](#)。

- [使用可信任金鑰](#)說明如何使用 PKCS #11 程式庫屬性和 CMU 來建立可信任金鑰以保護資料的安全。
- [產生金鑰](#)具有產生金鑰的說明，包括對稱金鑰、RSA 金鑰和 EC 金鑰。
- [匯入金鑰](#)提供金鑰擁有者如何匯入金鑰的詳細資訊。
- [匯出金鑰](#)提供金鑰擁有者如何匯出金鑰的詳細資訊。
- [刪除金鑰](#)提供金鑰擁有者如何刪除金鑰的詳細資訊。
- [共用和取消共用金鑰](#)詳細說明金鑰擁有者如何共用和取消共用金鑰。

使用 AWS CloudHSM KMU 產生金鑰

若要在硬體安全模組 (HSM) 上產生金鑰，請在 AWS CloudHSM key_mgmt_util (KMU) 中使用對應於您要產生之金鑰類型的命令。

主題

- [使用 AWS CloudHSM KMU 產生對稱金鑰](#)
- [使用 AWS CloudHSM KMU 產生 RSA 金鑰對](#)
- [使用 AWS CloudHSM KMU 產生 ECC \(橢圓曲線密碼編譯\) 金鑰對](#)

使用 AWS CloudHSM KMU 產生對稱金鑰

使用 AWS CloudHSM key_mgmt_util (KMU) 中的 [genSymKey](#) 命令來產生 AES 和其他類型的對稱金鑰 AWS CloudHSM。若要查看所有可用的選項，請使用 genSymKey -h 命令。

以下範例建立 256 位元 AES 金鑰。

```
Command: genSymKey -t 31 -s 32 -l aes256  
Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS
```

```
Symmetric Key Created. Key Handle: 524295
```

Cluster Error Status

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS  
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS  
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

使用 AWS CloudHSM KMU 產生 RSA 金鑰對

若要產生的 RSA 金鑰對 AWS CloudHSM，請使用 AWS CloudHSM `key_mgmt_util` 中的 [genRSAKeyPair](#) 命令。若要查看所有可用的選項，請使用 `genRSAKeyPair -h` 命令。

以下範例會產生 RSA 2048 位元金鑰對。

```
Command: genRSAKeyPair -m 2048 -e 65537 -l rsa2048  
Cfm3GenerateKeyPair returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3GenerateKeyPair: public key handle: 524294 private key handle: 524296
```

Cluster Error Status

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS  
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS  
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

使用 AWS CloudHSM KMU 產生 ECC（橢圓曲線密碼編譯）金鑰對

若要產生的 ECC 金鑰對 AWS CloudHSM，請在 AWS CloudHSM `key_mgmt_util` 中使用 [genECCKeyPair](#) 命令。若要查看所有可用的選項，包括支援的橢圓曲線清單，請使用 `genECCKeyPair -h` 命令。

以下範例使用 [NIST FIPS 出版物 186-4](#) 中定義的 P-384 橢圓曲線來產生 ECC 金鑰對。

```
Command: genECCKeyPair -i 14 -l ecc-p384  
Cfm3GenerateKeyPair returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3GenerateKeyPair: public key handle: 524297 private key handle: 524298
```

Cluster Error Status

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```



```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

使用 AWS CloudHSM KMU 匯入金鑰

若要使用 key AWS CloudHSM _mgmt_util 將對稱金鑰和非對稱私有金鑰匯入硬體安全模組 (HSM)，您必須先在 HSM 上建立包裝金鑰。您可以直接匯入公有金鑰，而不需包裝金鑰。

主題

- [使用 AWS CloudHSM KMU 匯入私密金鑰](#)
- [使用 AWS CloudHSM KMU 匯入公有金鑰](#)

使用 AWS CloudHSM KMU 匯入私密金鑰

完成下列步驟，AWS CloudHSM 使用 key_mgmt_util (KMU) 將私密金鑰匯入。匯入私密金鑰之前，請先儲存為檔案。將對稱金鑰儲存為原始位元組，將非對稱私有金鑰儲存為 PEM 格式。

此範例示範如何將檔案中的純文字私密金鑰匯入 HSM。若要將檔案中的加密金鑰匯入 HSM，請使用 [unWrapKey](#) 命令。

匯入私密金鑰

1. 使用 [genSymKey](#) 命令來建立包裝金鑰。以下命令會建立僅對目前工作階段而言有效的 128 位元 AES 包裝金鑰。您可以使用工作階段金鑰或持久性金鑰做為包裝金鑰。

```
Command: genSymKey -t 31 -s 16 -sess -l import-wrapping-key
Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS

Symmetric Key Created. Key Handle: 524299

Cluster Error Status
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

2. 依據您要匯入的私密金鑰類型而定，使用以下其中一個命令。
 - 若要匯入對稱金鑰，請使用 [imSymKey](#) 命令。以下命令使用上個步驟中建立的包裝金鑰，從名為 aes256.key 的檔案匯入 AES 金鑰。若要查看所有可用的選項，請使用 `imSymKey -h` 命令。

```
Command: imSymKey -f aes256.key -t 31 -l aes256-imported -w 524299
```

```
Cfm3WrapHostKey returned: 0x00 : HSM Return: SUCCESS

Cfm3CreateUnwrapTemplate returned: 0x00 : HSM Return: SUCCESS

Cfm3UnWrapKey returned: 0x00 : HSM Return: SUCCESS

Symmetric Key Unwrapped.  Key Handle: 524300

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

- 若要匯入非對稱私有金鑰，請使用 [importPrivateKey](#) 命令。以下命令使用上個步驟中建立的包裝金鑰，從名為 `rsa2048.key` 的檔案匯入私有金鑰。若要查看所有可用的選項，請使用 `importPrivateKey -h` 命令。

```
Command: importPrivateKey -f rsa2048.key -l rsa2048-imported -w 524299
BER encoded key length is 1216

Cfm3WrapHostKey returned: 0x00 : HSM Return: SUCCESS

Cfm3CreateUnwrapTemplate returned: 0x00 : HSM Return: SUCCESS

Cfm3UnWrapKey returned: 0x00 : HSM Return: SUCCESS

Private Key Unwrapped.  Key Handle: 524301

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

使用 AWS CloudHSM KMU 匯入公有金鑰

使用 AWS CloudHSM `key_mgmt_util` (KMU) 中的 [importPubKey](#) 命令來匯入公有金鑰。若要查看所有可用的選項，請使用 `importPubKey -h` 命令。

以下範例會從名為 `rsa2048.pub` 的檔案匯入 RSA 公有金鑰。

```
Command: importPubKey -f rsa2048.pub -l rsa2048-public-imported
Cfm3CreatePublicKey returned: 0x00 : HSM Return: SUCCESS
```

```
Public Key Handle: 524302
```

Cluster Error Status

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

使用 AWS CloudHSM KMU 匯出金鑰

若要使用 key AWS CloudHSM _mgmt_util (KMU) 從硬體安全模組 (HSM) 匯出 AWS CloudHSM 私密金鑰，也就是對稱金鑰和非對稱私有金鑰，您必須先建立包裝金鑰。您可以直接匯出公有金鑰，而不需包裝金鑰。

只有金鑰擁有者可以匯出金鑰。共用金鑰的使用者可以在密碼編譯操作中使用此金鑰，但無法匯出此金鑰。執行這個範例時，請務必匯出您建立的金鑰。

Important

[exSymKey](#) 命令可將私密金鑰的純文字 (未加密) 複本寫入檔案。匯出程序需要包裝金鑰，但檔案中的金鑰不是包裝金鑰。若要匯出金鑰的包裝 (加密) 複本，請使用 [wrapKey](#) 命令。

主題

- [使用 AWS CloudHSM KMU 匯出私密金鑰](#)
- [使用 AWS CloudHSM KMU 匯出公有金鑰](#)

使用 AWS CloudHSM KMU 匯出私密金鑰

完成下列步驟，AWS CloudHSM 使用 key_mgmt_util (KMU) 從 匯出私密金鑰。

匯出私密金鑰

1. 使用 [genSymKey](#) 命令來建立包裝金鑰。以下命令會建立僅對目前工作階段而言有效的 128 位元 AES 包裝金鑰。

```
Command: genSymKey -t 31 -s 16 -sess -l export-wrapping-key  
Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS
```

```
Symmetric Key Created. Key Handle: 524304
```

Cluster Error Status

Node id 2 and err state 0x00000000 : HSM Return: SUCCESS

2. 依據您要匯出的私密金鑰類型而定，使用以下其中一個命令。

- 若要匯出對稱金鑰，請使用 [exSymKey](#) 命令。以下命令會將 AES 金鑰匯出到名為 `aes256.key.exp` 的檔案。若要查看所有可用的選項，請使用 `exSymKey -h` 命令。

```
Command: exSymKey -k 524295 -out aes256.key.exp -w 524304
```

```
Cfm3WrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
Wrapped Symmetric Key written to file "aes256.key.exp"
```

 Note

命令的輸出顯示「包裝對稱金鑰」已寫入輸出檔。不過，輸出檔案包含純文字 (而非包裝) 金鑰。若要將包裝 (加密) 金鑰匯出到檔案，請使用 [wrapKey](#) 命令。

- 若要匯出私有金鑰，請使用 `exportPrivateKey` 命令。以下命令會將私有金鑰匯出到名為 `rsa2048.key.exp` 的檔案。若要查看所有可用的選項，請使用 `exportPrivateKey -h` 命令。

```
Command: exportPrivateKey -k 524296 -out rsa2048.key.exp -w 524304
```

```
Cfm3WrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
PEM formatted private key is written to rsa2048.key.exp
```

使用 AWS CloudHSM KMU 匯出公有金鑰

使用 AWS CloudHSM `key_mgmt_util` (KMU) 中的 `exportPubKey` 命令匯出公有金鑰。若要查看所有可用的選項，請使用 `exportPubKey -h` 命令。

以下範例將 RSA 公有金鑰匯出到名為 `rsa2048.pub.exp` 的檔案。

```
Command: exportPubKey -k 524294 -out rsa2048.pub.exp
```

```
PEM formatted public key is written to rsa2048.pub.key
```

```
Cfm3ExportPubKey returned: 0x00 : HSM Return: SUCCESS
```

使用 KMU 和 CMU 刪除金鑰

使用 [deleteKey](#) 命令來刪除金鑰，如下列範例所示。只有金鑰擁有者可以刪除金鑰。

```
Command: deleteKey -k 524300
```

```
Cfm3DeleteKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

與 KMU 和 CMU 共用和取消共用金鑰

在 AWS CloudHSM 中，建立金鑰的 CU 擁有該金鑰。擁有者可以管理金鑰、匯出和刪除金鑰，以及可在密碼編譯操作中使用金鑰。擁有者還可以向其他 CU 使用者共用金鑰。共用金鑰的使用者可以在密碼編譯操作中使用此金鑰，但無法匯出或刪除此金鑰，或再與其他使用者共用。

當您建立金鑰時，您可以與其他 CU 使用者共用金鑰，例如使用 [genSymKey](#) 或 [genRSAKeyPair](#) 命令的 `-u` 參數。若要將現有的金鑰共用給另一個 HSM 使用者，請使用 [cloudhsm_mgmt_util](#) 命令列工具。這不同於本區段中大多數使用 [key_mgmt_util](#) 命令列工具的任務。

您必須啟動 `cloudhsm_mgmt_util`、啟用端對端加密，並且登入 HSM，才能共用金鑰。若要共用金鑰，請以擁有金鑰的加密使用者 (CU) 身分登入 HSM。只有金鑰擁有者可以共用金鑰。

使用 `shareKey` 命令，並指定金鑰控點及一或多位使用者的 ID，以共用或取消共用金鑰。若要與多個使用者共用或取消共用，請指定以逗號分隔的使用者 ID 清單。若要共用金鑰，請使用 1 做為命令的最後一個參數，如下列範例所示。若要取消共用，請使用 0。

```
aws-cloudhsm > shareKey 524295 4 1
```

```
*****CAUTION*****
```

```
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
```

```
*****
```

```
Do you want to continue(y/n)? y
shareKey success on server 0(10.0.2.9)
shareKey success on server 1(10.0.3.11)
shareKey success on server 2(10.0.1.12)
```

下列顯示 shareKey 命令的語法。

```
aws-cloudhsm > shareKey <key handle> <user ID> <Boolean: 1 for share, 0 for unshare>
```

如何使用 AWS CloudHSM Management Utility 將金鑰標記為受信任

本節中的內容提供使用 AWS CloudHSM Management Utility (CMU) 將金鑰標記為信任的指示。

1. 使用 [loginHSM](#) 命令，以加密管理員 (CO) 身分登入。
2. 使用 [使用 CMU 設定 AWS CloudHSM 金鑰的屬性](#) 命令，將 OBJ_ATTR_TRUSTED (值 134) 設定為 true (1)。

```
aws-cloudhsm > setAttribute <Key Handle> 134 1
```

中的叢集備份 AWS CloudHSM

AWS CloudHSM 至少每 24 小時會定期備份您的叢集一次。每個備份包含以下資料的加密複本：

- 使用者 (CO、CU 和 AU)
- 金鑰資料與憑證
- 硬體安全模組 (HSM) 組態與原則

您無法指示服務進行備份，但您可以執行某些操作強制服務建立備份。這項服務會在您執行下列任一動作時，進行備份：

- 啟用叢集
- 將 HSM 新增至作用中叢集
- 從叢集移除 HSM

AWS CloudHSM 根據您在建立叢集時設定的備份保留政策刪除備份。如需管理備份保留原則的詳細資訊，請參閱 [設定備份保留](#)。

主題

- [使用 AWS CloudHSM 叢集備份](#)
- [刪除 AWS CloudHSM 叢集備份](#)
- [還原 AWS CloudHSM 備份](#)
- [設定 AWS CloudHSM 備份保留政策](#)
- [跨 AWS 區域複製 AWS CloudHSM 叢集備份](#)
- [在中使用共用備份 AWS CloudHSM](#)

使用 AWS CloudHSM 叢集備份

當您將硬體安全模組 (HSM) 新增至先前包含一或多個作用中 HSMs AWS CloudHSM 的叢集時，服務會將最新的備份還原至新的 HSM。使用備份來管理您不常使用的 HSM。當您刪除不需要使用的 HSM 時，會觸發備份。之後，如果您需要使用 HSM，請在同一叢集中建立新的 HSM，此動作會還原先您刪除 HSM 操作時建立的備份。

移除過期金鑰或非作用中使用者

您可能會想從您的環境移除不需要的密碼編譯資料，例如過期金鑰或非作用中使用者。這個程序需要兩個步驟：首先，從 HSM 中刪除這些材料。然後，刪除所有現有的備份。此步驟可確保您從備份初始化新叢集時，不會還原備份中的已刪除資訊。如需詳細資訊，請參閱[the section called “刪除備份”](#)。

考量災難復原

您可以從備份中建立叢集。您可能需要執行此操作來設定叢集的復原點。指定一份包含復原點中所需的所有使用者、金鑰資料和憑證的備份，然後使用該備份建立新叢集。如需從備份中建立叢集的詳細資訊，請參閱[從備份建立叢集](#)。

您也可以將叢集的備份複製到另一個區域中，然後可在該區域建立新的叢集，做為原始叢集的複本。您可能出於多種原因而希望這樣做，包括簡化災難復原程序。如需將備份複製到區域的詳細資訊，請參閱[跨區域複製備份](#)。

刪除 AWS CloudHSM 叢集備份

刪除 AWS CloudHSM 叢集備份後，服務會保留備份七天，在此期間您可以還原備份。七天後，您無法再還原備份。如需管理備份的詳細資訊，請參閱[叢集備份](#)。

下表說明如何刪除備份。

Console

刪除備份原則 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 如要變更 AWS 區域，請使用頁面右上角的 區域選擇器。
3. 在導覽窗格中，選擇備份。
4. 選擇要刪除的備份。
5. 如要刪除選取的備份，請選擇 Actions, Delete。

刪除備份對話方塊隨即出現。

6. 選擇 刪除。

備份的狀態會變更為 PENDING_DELETE。您最多可以在請求刪除備份後的 7 天內，還原待刪除的備份。

如要列出備份 (AWS CLI)

- 如要查看 PENDING_DELETION 狀態下的所有備份清單，請執行 `describe-backups` 命令並指定 `states=PENDING_DELETION` 做為篩選條件。

```
$ aws cloudhsmv2 describe-backups --filters states=PENDING_DELETION
{
  "Backups": [
    {
      "BackupId": "backup-ro5c4er4aac",
      "BackupState": "PENDING_DELETION",
      "ClusterId": "cluster-dygnwhmscg5",
      "CreateTimestamp": 1534461854.64,
      "DeleteTimestamp": 1536339805.522,
      "HsmType": "hsm2m.medium",
      "Mode": "NON_FIPS",
      "NeverExpires": false,
      "TagList": []
    }
  ]
}
```

AWS CLI

使用 AWS CLI 中的 [describe-backups](#) 命令檢查備份狀態或尋找其 ID。

如要刪除備份 (AWS CLI)

- 在命令提示字元下，執行 [delete-backup](#) 命令，傳遞要刪除的備份 ID。

```
$ aws cloudhsmv2 delete-backup --backup-id <backup ID>
{
  "Backup": {
    "CreateTimestamp": 1534461854.64,
    "ClusterId": "cluster-dygnwhmscg5",
    "BackupId": "backup-ro5c4er4aac",
    "BackupState": "PENDING_DELETION",
    "DeleteTimestamp": 1536339805.522,
    "HsmType": "hsm1.medium",
    "Mode": "FIPS"
  }
}
```

AWS CloudHSM API

請參閱 [DeleteBackup](#) 了解如何使用 API 刪除備份。

還原 AWS CloudHSM 備份

AWS CloudHSM 會保留已刪除的備份七天，在此期間您可以還原備份。七天後，您無法再還原備份。如需管理備份的詳細資訊，請參閱 [叢集備份](#)。

下表說明如何刪除備份。

Console

如要備份原則 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 如要變更 AWS 區域，請使用頁面右上角的 區域選擇器。
3. 在導覽窗格中，選擇備份。
4. 選擇 PENDING_DELETE 狀態下的備份進行還原。
5. 如要還原選取的備份，請選擇 Actions, Restore。

AWS CLI

如要還原備份 (AWS CLI)

- 若要還原備份，請發出 [restore-backup](#) 命令，傳遞處於 PENDING_DELETION 狀態的備份 ID。

```
$ aws cloudhsmv2 restore-backup --backup-id <backup ID>
{
  "Backup": {
    "ClusterId": "cluster-dygnwhmscg5",
    "CreateTimestamp": 1534461854.64,
    "BackupState": "READY",
    "BackupId": "backup-ro5c4er4aac"
  }
}
```

AWS CloudHSM API

請參閱 [RestoreBackup](#)，了解如何使用 API 還原備份。

設定 AWS CloudHSM 備份保留政策

AWS CloudHSM 根據您在建立叢集時設定的備份保留政策清除備份。備份保留原則適用於叢集。如果您將備份移至其他區域，該備份就不再與叢集產生關聯，也不再適用備份保留原則。您必須手動刪除任何與叢集無關的備份。AWS CloudHSM 不會刪除叢集的上次備份。

[AWS CloudTrail](#) 會報告標記為刪除的備份。您可以還原服務清除的備份，跟還原[手動刪除的備份](#)一樣。如要防止競爭，您應該先變更叢集的備份保留原則，然後再還原由服務刪除的備份。如果您不想變更原則但又想保留選取的備份，您可以指定服務從叢集備保留原則中[排除備份](#)。

受管備份保留

對於 2020 年 11 月 18 日之前建立的叢集，其備份保留原則還要加上額外 90 天叢集的保留期限。例如，如果您在 2019 年 11 月 18 日建立叢集，服務會為您的叢集指派一年的備份保留原則，再加上 90 天 (一共 455 天)。您可以將此期間設定為 7 到 379 天之間的任何數字。AWS CloudHSM 不會刪除叢集的上次備份。如需管理備份的詳細資訊，請參閱 [叢集備份](#)。

Note

您可以聯絡支援人員 (<https://aws.amazon.com/support>)，選擇退出管理備份保留。

下表說明如何設定備份保留。

Console

如要設定備份保留 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 按一下載作用中狀態下叢集的叢集 ID，即可管理該叢集的備份保留原則。
4. 如要變更備份保留原則，請選擇 Actions, Change backup retention period。

這時系統會顯示變更備份保留期限的對話方塊。

5. 在 Backup retention period (in days)，輸入介於 7 到 379 天之間的數字。

6. 選擇 Change backup retention period。

如要從備份保留原則 (主控台) 排除或包含一個備份

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 若要檢視備份，請在導覽窗格中選擇 Backups。
3. 按一下處於「就緒」狀態的備份 ID 以排除或包含某個備份。
4. 在 Backup details 頁面上，採取下列其中一項動作。
 - 如要排除日期為 Expiration time 的備份，請選擇 Actions, Disable expiration。
 - 如要包含未過期備份，請選擇 Actions, Use cluster retention policy。

AWS CLI

如要設定備份保留 (AWS CLI)

- 在命令提示字元中，發出 modify-cluster 命令。指定叢集 ID 和備份保留原則。

```
$ aws cloudhsmv2 modify-cluster --cluster-id <cluster ID> \
                                --backup-retention-policy
                                Type=DAYS,Value=<number of days to retain backups>
{
  "Cluster": {
    "BackupPolicy": "DEFAULT",
    "BackupRetentionPolicy": {
      "Type": "DAYS",
      "Value": 90
    },
    "Certificates": {},
    "ClusterId": "cluster-kdmrayrc7gi",
    "CreateTimestamp": 1504903546.035,
    "Hsms": [],
    "HsmType": "hsm1.medium",
    "SecurityGroup": "sg-40399d28",
    "State": "ACTIVE",
    "SubnetMapping": {
      "us-east-2a": "subnet-f1d6e798",
      "us-east-2c": "subnet-0e358c43",
      "us-east-2b": "subnet-40ed9d3b"
    }
  }
}
```

```

    },
    "TagList": [
      {
        "Key": "Cost Center",
        "Value": "12345"
      }
    ],
    "VpcId": "vpc-641d3c0d"
  }
}

```

如要從備份保留原則 (AWS CLI) 排除或包含一個備份

- 在命令提示字元中，發出 `modify-backup-attributes` 命令。指定備份 ID 並設定永不過期旗標以保留備份。

```

$ aws cloudhsmv2 modify-backup-attributes --backup-id <backup ID> \
                                           --never-expires
{
  "Backup": {
    "BackupId": "backup-ro5c4er4aac",
    "BackupState": "READY",
    "ClusterId": "cluster-dygnwhmscg5",
    "NeverExpires": true
  }
}

```

如要在備份保留原則中包含一個備份 (AWS CLI)

- 在命令提示字元中，發出 `modify-backup-attributes` 命令。指定備份 ID 並設定永不過期旗標，將備份包含在備份保留原則中，這表示服務最終不會刪除備份。

```

$ aws cloudhsmv2 modify-backup-attributes --backup-id <backup ID> \
                                           --no-never-expires
{
  "Backup": {
    "BackupId": "backup-ro5c4er4aac",
    "BackupState": "READY",
    "ClusterId": "cluster-dygnwhmscg5",
    "NeverExpires": false
  }
}

```

```
}  
}
```

AWS CloudHSM API

請參閱下列主題，了解如何使用 API 管理備份原則。

- [ModifyCluster](#)
- [ModifyBackupAttributes](#)

跨 AWS 區域複製 AWS CloudHSM 叢集備份

您可以基於許多原因跨區域複製 AWS CloudHSM 叢集備份，包括跨區域彈性、全球工作負載和[災難復原](#)。複製備份後，備份會以 CREATE_IN_PROGRESS 狀態顯示在目標區域。成功複製後，備份狀態會變成 READY。如果複製失敗，備份的狀態會變更為 DELETED。請檢查您輸入的參數是否有誤，並確保指定的來源備份處於 DELETED 狀態，然後再重新執行操作。如需備份或如何從備份建立叢集的資訊，請參閱 [叢集備份](#) 或 [從備份建立叢集](#)。

注意下列事項：

- 若要複製叢集備份到目標區域，您的帳戶必須擁有適當的 IAM 政策許可。為將備份複製到其他區域，您的 IAM 政策必須允許訪問備份所在的來源區域。跨區域複製之後，您的 IAM 政策必須允許訪問目標區域，才能和複製的備份互動，其中包含使用 [CreateCluster](#) 操作。如需詳細資訊，請參閱[建立 IAM 管理員](#)。
- 原始叢集和可從目標區域中備份建立的叢集並未連結。您必須分別管理每個叢集。如需詳細資訊，請參閱[叢集](#)。
- 限制 AWS 區域和標準區域之間無法複製備份。您可以在 AWS GovCloud（美國東部）和 AWS GovCloud（美國西部）區域之間複製備份。

將備份複製到不同的區域 (控制台)

將備份複製到不同的區域 (控制台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 如要變更 AWS 區域，請使用頁面右上角的 區域選擇器。
3. 在導覽窗格中，選擇備份。

4. 將備份複製到不同區域。
5. 如要複製所選備份，請選擇動作，複製到另一個區域。

將會顯示 [將備份複製到其他區域] 對話方塊。

6. 在目標區域中，從選取一個區域選擇一個區域。
7. (選用) 輸入標籤索引鍵和選用標籤值。若要將多個標籤新增至叢集，請選擇新增標籤。
8. 選擇複製備份。

將備份複製到不同的區域 (AWS CLI)

如要確定備份 ID，請執行 [describe-backups](#) 命令。

將備份複製到不同的區域 (AWS CLI)

- 在命令提示中，執行 [copy-backup-to-region](#) 命令。指定目標區域以及來源備份的備份 ID。如果指定備份 ID，則會複製關聯的備份。

```
$ aws cloudhsmv2 copy-backup-to-region --destination-region <destination region> \
                                     --backup-id <backup ID>
```

將備份複製到不同的區域 (AWS CloudHSM API)

請參閱下列主題，了解如何使用 API 將備份複製到不同區域。

- [CopyBackupToRegion](#)

在 中 使用共用備份 AWS CloudHSM

CloudHSM 與 AWS Resource Access Manager (AWS RAM) 整合以啟用資源共用。AWS RAM 是一項服務，可讓您與其他 AWS 帳戶 或透過 共用一些 CloudHSM 資源 AWS Organizations。您可以使用 AWS RAM 建立資源共享，以共享您擁有的資源。資源共享指定要共用的資源，以及共用它們的消費者。消費者可包括：

- 中的特定組織 AWS 帳戶 內部或外部 AWS Organizations
- 中的組織單位 AWS Organizations

- 中的整個組織 AWS Organizations

如需詳細資訊 AWS RAM，請參閱 [AWS RAM 使用者指南](#)。

本主題說明如何共用您擁有的資源，以及如何使用與您共用的資源。

目錄

- [共用備份的先決條件](#)
- [共用備份](#)
- [取消共用共用備份](#)
- [識別共用備份](#)
- [共用備份的許可](#)
- [計費和計量](#)

共用備份的先決條件

- 若要共用備份，您必須在 中擁有備份 AWS 帳戶。這表示必須在您的帳戶中配置或佈建資源。您無法共用已與您共用的備份。
- 若要共用備份，它必須處於 READY 狀態。
- 若要與 中的組織或組織單位共用備份 AWS Organizations，您必須啟用與 共用 AWS Organizations。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的[透過 AWS Organizations 啟用共用](#)。

共用備份

當您與其他人共用備份時 AWS 帳戶，您可以讓它們從備份還原叢集，其中包含存放在備份中的金鑰和使用者。

若要共用備份，您必須將其新增至資源共用。資源共用是可讓您在 AWS 帳戶之間共用資源的一種 AWS RAM 資源。資源共享指定要共用的資源，以及共用它們的消費者。當您使用 CloudHSM 主控台共用備份時，您可以將其新增至現有的資源共用。若要將備份新增至新的資源共享，您必須先使用 [AWS RAM 主控台](#) 建立資源共享。

如果您是 中組織的一部分，AWS Organizations 且已啟用組織內的共用，則組織中的消費者會自動獲得共用備份的存取權。否則，消費者會收到加入資源共享的邀請，並在接受邀請後授予共用備份的存取權。

您可以使用 AWS RAM 主控台或 共用您擁有的備份 AWS CLI。

使用 AWS RAM 主控台共用您擁有的備份

請參閱《AWS RAM 使用者指南》中的[建立資源共享](#)。

共用您擁有的備份 (AWS RAM 命令)

使用 [create-resource-share](#) 命令。

共用您擁有的備份 (CloudHSM 命令)

Important

雖然您可以使用 CloudHSM PutResourcePolicy 操作共用備份，但我們建議您改用 AWS Resource Access Manager (AWS RAM)。使用 可在為您建立政策時 AWS RAM 提供多項優點、允許一次共用多個資源，並提高共用資源的可探索性。如果您使用 PutResourcePolicy，並希望消費者能夠描述您與其共用的備份，您必須使用 AWS RAM PromoteResourceShareCreatedFromPolicy API 操作將備份提升為標準 AWS RAM 資源共享。

使用 [put-resource-policy](#) 命令。

1. 建立名為 的檔案，policy.json並將下列政策複製到其中。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "<consumer-aws-account-id-or-user>"
      },
      "Action": [
        "cloudhsm:CreateCluster",
        "cloudhsm:DescribeBackups"
      ],
      "Resource": "<arn-of-backup-to-share>"
    }
  ]
}
```

2. policy.json 使用備份 ARN 和識別符進行更新，以便與之共用。下列範例授予 123456789012 所識別 AWS 帳戶的根使用者的唯讀存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "account-id"
      ]
    },
    "Action": [
      "cloudhsm:CreateCluster",
      "cloudhsm:DescribeBackups"
    ],
    "Resource": "arn:aws:cloudhsm:us-west-2:123456789012:backup/backup-123"
  }]
}
```

Important

您只能將許可授予帳戶層級的 DescribeBackups。當您與其他客戶共用備份時，在該帳戶中具有 DescribeBackups 許可的任何主體都可以描述備份。

3. 執行 `put-resource-policy` 命令。

```
$ aws cloudhsmv2 put-resource-policy --resource-arn <resource-arn> --policy file://policy.json
```

Note

此時，消費者可以使用備份，但不會在 DescribeBackups 回應中顯示共用參數。後續步驟說明如何提升 AWS RAM 資源共享，以便將備份包含在回應中。

4. 取得 AWS RAM 資源共享 ARN。

```
$ aws ram list-resources --resource-owner SELF --resource-arns <backup-arn>
```

這會傳回類似以下的回應：

```
{
  "resources": [
```

```
{
  "arn": "<project-arn>",
  "type": "<type>",
  "resourceShareArn": "<resource-share-arn>",
  "creationTime": "<creation-time>",
  "lastUpdatedTime": "<last-update-time>"
}
```

從回應中，複製要在後續步驟中使用的 *<resource-share-arn>* 值。

5. 執行 AWS RAM [promote-resource-share-created-from-policy](#) 命令。

```
$ aws ram promote-resource-share-created-from-policy --resource-share-arn <resource-share-arn>
```

6. 若要驗證資源共享是否已提升，您可以執行 AWS RAM [get-resource-shares](#) 命令。

```
$ aws ram get-resource-shares --resource-owner SELF --resource-share-arns <resource-share-arn>
```

政策提升後，回應中 `featureSet` 列出的 為 STANDARD。這也表示備份可由政策中的新帳戶描述。

取消共用共用備份

當您取消共用資源時，消費者可能無法再使用它來還原叢集。消費者仍然可以存取從共用備份還原的任何叢集。

若要取消共用您擁有的共用備份，您必須將其從資源共用中移除。您可以使用 AWS RAM 主控台或 執行此操作 AWS CLI。

使用 AWS RAM 主控台取消共用您擁有的共用備份

請參閱《AWS RAM 使用者指南》中的[更新資源共享](#)。

取消共用您擁有的共用備份 (AWS RAM 命令)

使用 [disassociate-resource-share](#) 命令。

取消共用您擁有的共用備份 (CloudHSM 命令)

使用 [delete-resource-policy](#) 命令。

```
$ aws cloudhsmv2 delete-resource-policy --resource-arn <resource-arn>
```

識別共用備份

消費者可以使用 CloudHSM 主控台和 來識別與其共用的備份 AWS CLI。

使用 CloudHSM 主控台識別與您共用的備份

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 在導覽窗格中，選擇備份。
4. 在表格中，選擇共用備份索引標籤。

使用 識別與您共用的備份 AWS CLI

使用 [describe-backups](#) 命令搭配 `--shared` 參數來傳回與您共用的備份。

共用備份的許可

擁有者的許可

備份擁有者可以描述和管理共用備份，並使用它來還原叢集。

消費者的許可

備份取用者無法修改共用備份，但他們可以描述它，並使用它來還原叢集。

計費和計量

共用備份無需額外費用。

中的複製叢集 AWS CloudHSM

如果該區域中的叢集最初是從另一個區域中的叢集備份建立的，請使用 AWS CloudHSM Management Utility (CMU) 來同步遠端區域中的叢集。比如，您將叢集複製到另一個區域 (目的地)，然後您想要同步原始叢集 (來源) 的變更。在這種情況下，您可以使用 CMU 同步處理叢集。您可以建立新的 CMU 組態檔案，從新檔案中的兩個叢集指定硬體安全性模組 (HSM)，然後使用 CMU 連線至具有該檔案的叢集。

在複製的叢集間使用 CMU

1. 建立當前組態檔案的複本，並將複本的名稱更改為其他名稱。

例如，使用下列檔案位置來尋找並建立目前組態檔案的複本，然後將複本名稱從 `cloudhsm_mgmt_config.cfg` 變更為 `syncConfig.cfg`。

- Linux : `/opt/cloudhsm/etc/cloudhsm_mgmt_config.cfg`
- Windows : `C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_mgmt_config.cfg`

2. 在重新命名的複本中，新增目的地 HSM (需要同步的外部區域中的 HSM) 的彈性網路介面 (ENI) IP。建議您在來源 HSM 下方新增目的地 HSM。

```
{
  ...
  "servers": [
    {
      ...
      "hostname": "<ENI Source IP>",
      ...
    },
    {
      ...
      "hostname": "<ENI Destination IP>",
      ...
    }
  ]
}
```

如需如何取得 IP 地址的詳細資訊，請參閱 [the section called “取得 HSM 的 IP 地址”](#)。

3. 使用新的組態檔來初始化 CMU：

Linux

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/userSync.cfg
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cloudhsm_mgmt_util.exe" C:\ProgramData\Amazon\CloudHSM\data\userSync.cfg
```

4. 檢查傳回的狀態訊息，確認 CMU 連線到所需的全部 HSM，並判斷傳回的 ENI IP 對應到哪個叢集。使用 syncUser 和 syncKey 手動同步處理使用者和金鑰。如需詳細資訊，請參閱 [syncUser](#) 和 [syncKey](#)。

取得 HSM 的 IP 地址

使用本節取得 HSM 的 IP 地址。

取得 HSM 的 IP 地址（主控台）

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 若要開啟叢集詳細資訊頁面，請在叢集表格中選擇叢集 ID。
4. 若要取得 IP 地址，請前往 HSMs 索引標籤。對於 IPv4 叢集，請選擇 ENI IPv4 地址下列出的地址。對於雙堆疊叢集，請使用 ENI IPv4 或 ENI IPv6 地址。

取得 HSM 的 IP 地址 (AWS CLI)

- 使用 AWS CLI 中的 [describe-clusters](#) 命令取得 HSM 的 IP 地址。在命令的輸出中，HSMs 的 IP 地址是 EniIp 和 的值 EniIPv6（如果是雙堆疊叢集）。

```
$ aws cloudhsmv2 describe-clusters
{
  "Clusters": [
    { ... }
    "Hsms": [
      {
        ...
        "EniIp": "10.0.0.9",
```

```
...
    },
    {
...
        "EniIp": "10.0.1.6",
        "EniIPv6": "2600:113f:404:be09:310e:ed34:3412:f733",
...
    }
```

相關主題

- [syncUser](#)
- [syncKey](#)
- [跨區域複製備份](#)

標籤 AWS CloudHSM 資源

標籤是您指派給 AWS 資源的標籤。您可以將標籤指派給 AWS CloudHSM 叢集。每個標籤皆包含由您定義的標籤索引鍵和標籤值。例如，標籤索引鍵可能是 Cost Center，而標籤值是 12345。每個叢集的標籤索引鍵必須是唯一的。

您可以將標籤用於各種用途。使用標籤來分類和追蹤 AWS 成本是常見的用途之一。您可以套用代表業務類別 (例如成本中心、應用程式名稱或擁有者) 的標籤，來整理多個服務中的成本。當您將標籤新增至 AWS 資源時，AWS 會產生成本分配報告，其中包含標籤彙總的用量和成本。您可以使用此報告來檢視專案或應用程式 AWS CloudHSM 的成本，而不是以單一明細項目檢視所有 AWS CloudHSM 成本。

如需有關使用成本配置標籤的詳細資訊，請參閱《AWS Billing 使用者指南》中的[使用成本分配標籤](#)。

您可以使用 [AWS CloudHSM 主控台](#) 或 [AWS 開發套件或命令列工具](#) 的其中一個，來新增、更新、列出或移除標籤。

主題

- [新增或更新 AWS CloudHSM 資源的標籤](#)
- [列出 AWS CloudHSM 資源的標籤](#)
- [從 AWS CloudHSM 資源移除標籤](#)

新增或更新 AWS CloudHSM 資源的標籤

您可以從 [AWS CloudHSM 主控台](#)、[AWS Command Line Interface \(AWS CLI\)](#) 或 AWS CloudHSM API 新增或更新標籤。

新增或更新標籤 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 選擇您要新增標籤的叢集。
3. 選擇標籤。
4. 若要新增標籤，請執行以下操作：
 - a. 選擇 Edit Tag (編輯標籤)，然後選擇 Add Tag (新增標籤)。
 - b. 在 Key (索引鍵) 中，指定標籤的索引鍵。

- c. (選用) 在 Value (值) 中，輸入標籤的值。
 - d. 選擇儲存。
5. 若要更新標籤，請執行以下操作：
 - a. 選擇 Edit Tag (編輯標籤)。

 Note

如果您更新現有標籤的標籤索引鍵，主控台會刪除現有的標籤，並建立新的標籤。

- b. 輸入新的標籤值。
 - c. 選擇儲存。

新增或更新標籤 (AWS CLI)

1. 在命令提示字元，發出 [tag-resource](#) 命令來指定標籤以及您要加上標籤的叢集 ID。如果您不知道叢集 ID，請發出 [describe-clusters](#) 命令。

```
$ aws cloudhsmv2 tag-resource --resource-id <cluster ID> \  
--tag-list Key="<tag key>",Value="<tag value>"
```

2. 若要更新標籤，請使用相同的命令，但指定現有的標籤索引鍵。當您為現有標籤指定新的標籤值，新值會覆寫原標籤。

新增或更新標籤 (AWS CloudHSM API)

- 傳送 [TagResource](#) 要求。指定標籤以及您要加上標籤的叢集 ID。

列出 AWS CloudHSM 資源的標籤

您可以從[AWS CloudHSM 主控台](#)、[AWS CLI](#)或 AWS CloudHSM API 列出叢集的標籤。

列出標籤 (主控台)

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 選擇您要列出其標籤的叢集。
3. 選擇標籤。

列出標籤 (AWS CLI)

- 在命令提示字元，發出 [list-tags](#) 命令來指定您要列出其標籤的叢集 ID。如果您不知道叢集 ID，請發出 [describe-clusters](#) 命令。

```
$ aws cloudhsmv2 list-tags --resource-id <cluster ID>
{
  "TagList": [
    {
      "Key": "Cost Center",
      "Value": "12345"
    }
  ]
}
```

列出標籤 (AWS CloudHSM API)

- 傳送 [ListTags](#) 請求，以便指定您要列出標籤的叢集 ID。

從 AWS CloudHSM 資源移除標籤

您可以使用 [AWS CloudHSM 主控台](#)、[AWS CLI](#) 或 AWS CloudHSM API 從 AWS CloudHSM 叢集移除標籤。

移除標籤 (主控台)

- 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
- 選擇您要移除其標籤的叢集。
- 選擇標籤。
- 選擇 Edit Tag (編輯標籤)，然後針對您要移除的標籤，選擇 Remove tag (移除標籤)。
- 選擇儲存。

移除標籤 (AWS CLI)

- 在命令提示字元，發出 [untag-resource](#) 命令來指定要移除之標籤的標籤索引鍵，以及您要移除其標籤的叢集 ID。當您使用 AWS CLI 移除標籤時，請僅指定標籤索引鍵，而非標籤值。

```
$ aws cloudhsmv2 untag-resource --resource-id <cluster ID> \  
                                --tag-key-list "<tag key>"
```

移除標籤 (AWS CloudHSM API)

- 在 AWS CloudHSM API 中傳送 [UntagResource](#) 請求，指定叢集的 ID 和您要移除的標籤。

AWS CloudHSM 命令列工具

除了您用來管理 AWS 資源的 AWS Command Line Interface (AWS CLI) 之外，AWS CloudHSM 還提供命令列工具，用於在 HSMs 上建立和管理硬體安全模組 (HSM) 使用者和金鑰。在 AWS CloudHSM，您可以使用熟悉的 CLI 來管理叢集，並使用 CloudHSM 命令列工具來管理 HSM。

這些是各種命令列工具：

管理叢集和 HSM

[AWS CLI 中的 CloudHSMv2 命令](#)和 [AWS PowerShell 模組中的 HSM2 PowerShell cmdlets](#)

- 這些工具會取得、建立、刪除和標記 AWS CloudHSM 叢集和 HSMs：
- 若要在 [CLI 的 CloudHSMv2 命令中使用](#)命令，您需要[安裝](#)和[設定](#) AWS CLI。
- 可在 Windows PowerShell 模組和跨平台 PowerShell Core 模組中使用 [AWS PowerShell 模組中的 HSM2 PowerShell cmdlets](#)。

如何管理 HSM 使用者。

[CloudHSM CLI](#)

- 使用 [CloudHSM CLI](#) 建立使用者、刪除使用者、列出使用者、變更使用者密碼，以及更新使用者多重要素驗證 (MFA)。AWS CloudHSM 用戶端軟體中不包含此工具。如需有關安裝此工具的指引，請參閱[安裝和設定 CloudHSM CLI](#)。

協助程式工具

兩種工具可協助您使用 AWS CloudHSM 工具和軟體程式庫：

- [設定工具](#)可更新您的 CloudHSM 用戶端組態檔案。這可讓 AWS CloudHSM 同步叢集中的 HSMs。

AWS CloudHSM 提供兩個主要版本，而用戶端 SDK 5 是最新的。與用戶端 SDK 3 (上一個系列) 相比，用戶端 SDK 5 具有多種優勢。

- [pkpspeed](#) 可衡量 HSM 硬體的效能 (與軟體程式庫無關)。

適用於先前 SDK 的工具

使用金鑰管理工具 (KMU) 建立、刪除、匯入和匯出對稱金鑰和非對稱金鑰對：

- [key_mgmt_util](#)。此工具包含在 AWS CloudHSM 用戶端軟體之中。

使用 CloudHSM 管理工具 (CMU) 建立和刪除 HSM 使用者，包括執行使用者管理工作的規定人數身分驗證

- [cloudhsm_mgmt_util](#)。此工具包含在 AWS CloudHSM 用戶端軟體之中。

下列主題進一步描述可用於管理和使用的命令列工具 AWS CloudHSM。

主題

- [AWS CloudHSM 設定工具](#)
- [AWS CloudHSM 命令列界面 \(CLI\)](#)
- [AWS CloudHSM Management Utility \(CMU\)](#)
- [AWS CloudHSM 金鑰管理公用程式 \(KMU\)](#)

AWS CloudHSM 設定工具

AWS CloudHSM 會自動同步叢集中所有硬體安全模組 (HSM) 之間的資料。configure 工具會更新同步機制所使用之組態檔案中的 HSM 資料。在您使用此命令列工具之前 (特別是在叢集中的 HSM 已變更時)，請使用 configure 重新整理 HSM 資料。

AWS CloudHSM 包含兩個主要用戶端 SDK 版本：

- 用戶端 SDK 5：這是我們最新預設的用戶端 SDK。如需有關其優點和優勢的資訊，請參閱 [AWS CloudHSM 用戶端 SDK 5 的優點](#)。
- 用戶端 SDK 3：這是我們較舊的用戶端 SDK。它包括一組完整的組件，用於基於平台和語言的應用程序兼容性和管理工具。

如需從用戶端 SDK 3 遷移至用戶端 SDK 5 的指示，請參閱 [從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)。

主題

- [AWS CloudHSM 用戶端 SDK 5 設定工具](#)
- [AWS CloudHSM 用戶端 SDK 3 設定工具](#)

AWS CloudHSM 用戶端 SDK 5 設定工具

使用 AWS CloudHSM 用戶端 SDK 5 設定工具更新用戶端組態檔案。

用戶端 SDK 5 中的每個元件都包含一個設定工具，其中包含設定工具檔案名稱中的元件指示項。例如，用戶端 SDK 5 的 PKCS #11 程式庫包含一個名為 Linux `configure-pkcs11` 或 Windows `configure-pkcs11.exe` 的設定工具。

主題

- [AWS CloudHSM 用戶端 SDK 5 組態語法](#)
- [AWS CloudHSM 用戶端 SDK 5 組態參數](#)
- [AWS CloudHSM 用戶端 SDK 5 組態範例](#)
- [用戶端 SDK 5 設定工具的進階組態](#)
- [AWS CloudHSM 用戶端 SDK 5 相關主題](#)

AWS CloudHSM 用戶端 SDK 5 組態語法

下表說明 用戶端 SDK 5 AWS CloudHSM 組態檔案的語法。

PKCS #11

```
configure-pkcs11[ .exe ]
    -a <ENI IP address>
    [--hsm-ca-cert <customerCA certificate file path>]
    [--cluster-id <cluster ID>]
    [--endpoint <endpoint>]
    [--region <region>]
    [--client-cert-hsm-tls-file <client certificate hsm tls path>]
    [--client-key-hsm-tls-file <client key hsm tls path>]
    [--log-level <error | warn | info | debug | trace>]
        Default is <info>
    [--log-rotation <daily | weekly>]
        Default is <daily>
    [--log-file <file name with path>]
        Default is </opt/cloudhsm/run/cloudhsm-pkcs11.log>
        Default for Windows is <C:\\Program Files\\Amazon\\CloudHSM\\
\\cloudhsm-pkcs11.log>
    [--log-type <file | term>]
        Default is <file>
    [-h | --help]
    [-V | --version]
    [--disable-key-availability-check]
    [--enable-key-availability-check]
    [--disable-validate-key-at-init]
```

```
[--enable-validate-key-at-init]
    This is the default for PKCS #11
```

OpenSSL

```
configure-dyn[ .exe ]
    -a <ENI IP address>
    [--hsm-ca-cert <customerCA certificate file path>]
    [--cluster-id <cluster ID>]
    [--endpoint <endpoint>]
    [--region <region>]
    [--client-cert-hsm-tls-file <client certificate hsm tls path>]
    [--client-key-hsm-tls-file <client key hsm tls path>]
    [--log-level <error | warn | info | debug | trace>]
        Default is <error>
    [--log-type <file | term>]
        Default is <term>
    [-h | --help]
    [-V | --version]
    [--disable-key-availability-check]
    [--enable-key-availability-check]
    [--disable-validate-key-at-init]
        This is the default for OpenSSL
    [--enable-validate-key-at-init]
```

KSP

```
configure-ksp[ .exe ]
    -a <ENI IP address>
    [--hsm-ca-cert <customerCA certificate file path>]
    [--cluster-id <cluster ID>]
    [--endpoint <endpoint>]
    [--region <region>]
    [--client-cert-hsm-tls-file <client certificate hsm tls path>]
    [--client-key-hsm-tls-file <client key hsm tls path>]
    [--log-level <error | warn | info | debug | trace>]
        Default is <info>
    [--log-rotation <daily | weekly>]
        Default is <daily>
    [--log-file <file name with path>]
        Default is <C:\\Program Files\\Amazon\\CloudHSM\\cloudhsm-ksp.log>
    [--log-type <file | term>]
        Default is <file>
```

```

[-h | --help]
[-V | --version]
[--disable-key-availability-check]
[--enable-key-availability-check]
[--disable-validate-key-at-init]
    This is the default for KSP
[--enable-validate-key-at-init]

```

JCE

```

configure-jce[ .exe ]
    -a <ENI IP address>
    [--hsm-ca-cert <customerCA certificate file path>]
    [--cluster-id <cluster ID>]
    [--endpoint <endpoint>]
    [--region <region>]
    [--client-cert-hsm-tls-file <client certificate hsm tls path>]
    [--client-key-hsm-tls-file <client key hsm tls path>]
    [--log-level <error | warn | info | debug | trace>]
        Default is <info>
    [--log-rotation <daily | weekly>]
        Default is <daily>
    [--log-file <file name with path>]
        Default is </opt/cloudhsm/run/cloudhsm-jce.log>
        Default for Windows is <C:\\Program Files\\Amazon\\CloudHSM\\
\\cloudhsm-jce.log>
    [--log-type <file | term>]
        Default is <file>
    [-h | --help]
    [-V | --version]
    [--disable-key-availability-check]
    [--enable-key-availability-check]
    [--disable-validate-key-at-init]
        This is the default for JCE
    [--enable-validate-key-at-init]

```

CloudHSM CLI

```

configure-cli[ .exe ]
    -a <ENI IP address>
    [--hsm-ca-cert <customerCA certificate file path>]
    [--cluster-id <cluster ID>]
    [--endpoint <endpoint>]

```



```

[--region <region>]
[--client-cert-hsm-tls-file <client certificate hsm tls path>]
[--client-key-hsm-tls-file <client key hsm tls path>]
[--log-level <error | warn | info | debug | trace>]
    Default is <info>
[--log-rotation <daily | weekly>]
    Default is <daily>
[--log-file <file name with path>]
    Default for Linux is </opt/cloudhsm/run/cloudhsm-cli.log>
    Default for Windows is <C:\\Program Files\\Amazon\\CloudHSM\\
\\cloudhsm-cli.log>
[--log-type <file | term>]
    Default setting is <file>
[-h | --help]
[-V | --version]
[--disable-key-availability-check]
[--enable-key-availability-check]
[--disable-validate-key-at-init]
[--enable-validate-key-at-init]
    This is the default for CloudHSM CLI

```

AWS CloudHSM 用戶端 SDK 5 組態參數

以下是設定 AWS CloudHSM 用戶端 SDK 5 的參數清單。

-a **<ENI IP address>**

將指定的 IP 地址新增至用戶端 SDK 5 設定檔案。從叢集輸入 HSM 的任何 ENI IP 地址。如需如何使用此選項的詳細資訊，請參閱[引導用戶端 SDK 5](#)。

必要：是

--hsm-ca-cert **<customerCA certificate file path>**

儲存用於將 EC2 用戶端執行個體連接到叢集的憑證授權機構 (CA) 憑證目錄的路徑。您可在初始化叢集時建立此檔案。按照預設，系統會在下列位置尋找此檔案：

Linux

```
/opt/cloudhsm/etc/customerCA.crt
```

Windows

```
C:\ProgramData\Amazon\CloudHSM\customerCA.crt
```

如需有關初始化叢集或放置憑證的詳細資訊，請參閱 [???](#) 和 [???](#)。

必要：否

`--cluster-id <cluster ID>`

進行 DescribeClusters 呼叫以尋找叢集中與叢集 ID 關聯的所有 HSM 彈性網路介面 (ENI) IP 地址。系統會將 ENI IP 地址新增至 AWS CloudHSM 組態檔案。

 Note

如果您在無法存取公有網際網路的 VPC 中使用來自 EC2 執行個體的 `--cluster-id` 參數，則必須建立要連線的介面 VPC 端點 AWS CloudHSM。如需 VPC 端點的詳細資訊，請參閱 [???](#)。

必要：否

`--endpoint <endpoint>`

指定用於進行 DescribeClusters 呼叫的 AWS CloudHSM API 端點。您必須結合 `--cluster-id` 設定此選項。

必要：否

`--region <region>`

指您叢集的區域。您必須結合 `--cluster-id` 設定此選項。

如果您未提供 `--region` 參數，系統會嘗試讀取 `AWS_DEFAULT_REGION` 或 `AWS_REGION` 環境變數來選擇區域。如果未設定這些變數，則除非您在 `AWS_CONFIG_FILE` 環境變數中指定了不同的檔案，否則系統會檢查 AWS config 檔案中 (通常是 `~/.aws/config`) 與您的設定檔相關聯的區域。如果未設定上述任何變數，系統會預設為 `us-east-1` 區域。

必要：否

`--client-cert-hsm-tls-file <client certificate hsm tls ###>`

用於 TLS 用戶端-HSM 交互身分驗證的用戶端憑證路徑。

只有在您已使用 CloudHSM CLI 在 HSM 上註冊至少一個信任錨點時，才使用此選項。您必須結合 `--client-key-hsm-tls-file` 設定此選項。

必要：否

`--client-key-hsm-tls-file ##### hsm tls ###`

用於 TLS 用戶端-HSM 交互身分驗證的用戶端金鑰路徑。

只有在您已使用 CloudHSM CLI 在 HSM 上註冊至少一個信任錨點時，才使用此選項。您必須結合 `--client-cert-hsm-tls-file` 設定此選項。

必要：否

`--log-level <error / warn / info / debug / trace>`

指定系統應寫入日誌檔的最低日誌層級。每個層級包括以前的層級，錯誤作為最低層級，追蹤為最高層級。這表示如果您指定錯誤，系統只會將錯誤寫入日誌。如果您指定追蹤，系統會將錯誤、警告、資訊 (info) 和偵錯訊息寫入日誌檔。如需詳細資訊，請參閱[用戶端 SDK 5 記錄](#)。

必要：否

`--log-rotation <daily / weekly>`

指系統輪換日誌檔的頻率。如需詳細資訊，請參閱[用戶端 SDK 5 記錄](#)。

必要：否

`--log-file <file name with path>`

指系統將寫入日誌檔的位置。如需詳細資訊，請參閱[用戶端 SDK 5 記錄](#)。

必要：否

`--log-type <term / file>`

指系統是否將日誌寫入檔案或終端。如需詳細資訊，請參閱[用戶端 SDK 5 記錄](#)。

必要：否

`-h | --help`

顯示幫助。

必要：否

`-v | --version`

顯示版本。

必要：否

`--disable-key-availability-check`

停用金鑰可用性仲裁的旗標。使用此旗標表示 AWS CloudHSM 應該停用金鑰可用性仲裁，而且您只能使用叢集中一個 HSM 上存在的金鑰。如需有關使用此旗標設定金鑰可用性仲裁的詳細資訊，請參閱 [???](#)。

必要：否

`--enable-key-availability-check`

啟動金鑰可用性仲裁的旗標。使用此旗標表示 AWS CloudHSM 應該使用金鑰可用性規定人數，而且在叢集中的兩個 HSMs 上存在這些金鑰之前，都不允許您使用金鑰。如需有關使用此旗標設定金鑰可用性仲裁的詳細資訊，請參閱 [???](#)。

預設啟用。

必要：否

`--disable-validate-key-at-init`

指定您可以跳過初始化呼叫來驗證後續呼叫之金鑰的權限，以此改善效能。請謹慎使用。

背景：PKCS #11 程式庫中的某些機制支援多部分操作，其中初始化呼叫會驗證您是否可以將金鑰用於後續呼叫。這一操作需要對 HSM 進行驗證呼叫，這會增加整體操作的延遲。此選項可讓您停用後續呼叫，並可能改善效能。

必要：否

`--disable-validate-key-at-init`

指您應該使用初始化呼叫來驗證後續呼叫的金鑰權限。此為預設選項。使用 `disable-validate-key-at-init` 暫停這些初始化呼叫後，再使用 `enable-validate-key-at-init` 恢復這些初始化呼叫。

必要：否

AWS CloudHSM 用戶端 SDK 5 組態範例

這些範例示範如何使用 AWS CloudHSM 用戶端 SDK 5 的設定工具。

引導用戶端 SDK 5

Example

此範例使用 `-a` 參數來更新用戶端 SDK 5 的 HSM 資料。若要使用此 `-a` 參數，您必須擁有叢集中其中一個 HSM 的 IP 地址。

PKCS #11 library

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 -a <HSM IP addresses>
```

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" -a <HSM IP addresses>
```

OpenSSL Dynamic Engine

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-dyn -a <HSM IP addresses>
```

Key Storage Provider (KSP)

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" -a <HSM IP addresses>
```

JCE provider

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-jce -a <HSM IP addresses>
```

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用 設定工具來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" -a <HSM IP addresses>
```

CloudHSM CLI

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用設定工具指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-cli -a <The ENI IPv4 / IPv6 addresses of the HSMs>
```

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用設定工具指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" -a <The ENI IPv4 / IPv6 addresses of the HSMs>
```

Note

您可以使用 `--cluster-id` 參數來代替 `-a <HSM_IP_ADDRESSES>`。若要查看使用 `--cluster-id` 的需求，請參閱 [AWS CloudHSM 用戶端 SDK 5 設定工具](#)。

如需 `-a` 參數的詳細資訊，請參閱 [the section called “參數”](#)。

指定用戶端 SDK 5 的叢集、區域和端點

Example

此範例會使用 `cluster-id` 參數，以 `DescribeClusters` 撥打呼叫的方式來啟動用戶端 SDK 5。

PKCS #11 library

使用 **cluster-id** 為用戶端 SDK 5 啟動 Linux EC2 執行個體

- 使用叢集 ID `cluster-1234567`來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --cluster-id <cluster-1234567>
```

使用 **cluster-id** 為用戶端 SDK 5 啟動 Windows EC2 執行個體

- 使用叢集 ID `cluster-1234567`來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" --cluster-id <cluster-1234567>
```

OpenSSL Dynamic Engine

使用 **cluster-id** 為用戶端 SDK 5 啟動 Linux EC2 執行個體

- 使用叢集 ID `cluster-1234567`來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-dyn --cluster-id <cluster-1234567>
```

Key Storage Provider (KSP)

使用 **cluster-id** 為用戶端 SDK 5 啟動 Windows EC2 執行個體

- 使用叢集 ID `cluster-1234567`來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --cluster-id <cluster-1234567>
```

JCE provider

使用 **cluster-id** 為用戶端 SDK 5 啟動 Linux EC2 執行個體

- 使用叢集 ID `cluster-1234567` 來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-jce --cluster-id <cluster-1234567>
```

使用 **cluster-id** 為用戶端 SDK 5 啟動 Windows EC2 執行個體

- 使用叢集 ID `cluster-1234567` 來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" --cluster-id <cluster-1234567>
```

CloudHSM CLI

使用 **cluster-id** 為用戶端 SDK 5 啟動 Linux EC2 執行個體

- 使用叢集 ID `cluster-1234567` 來指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-cli --cluster-id <cluster-1234567>
```

使用 **cluster-id** 為用戶端 SDK 5 啟動 Windows EC2 執行個體

- 使用叢集 ID `cluster-1234567` 來指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" --cluster-id <cluster-1234567>
```

您可以將 `--region` 和 `--endpoint` 參數與 `cluster-id` 參數結合使用，以指定系統進行 `DescribeClusters` 呼叫的方式。例如，如果叢集區域與設定為 AWS CLI 預設的區域不同，則應使用該 `--region` 參數來使用該區域。此外，您可以指定用於呼叫的 AWS CloudHSM API 端點，這對於各種網路設定而言可能是必要的，例如使用不使用預設 DNS 主機名稱的 VPC 介面端點 AWS CloudHSM。

PKCS #11 library

使用自訂端點和區域啟動 Linux EC2 執行個體

- 使用 設定工具指定叢集中具有自訂區域和端點的 HSM IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --cluster-id <cluster-1234567> --  
region <us-east-1> --endpoint <https://cloudhsmv2.us-east-1.amazonaws.com>
```

使用端點和區域啟動 Windows EC2 執行個體

- 使用 設定工具指定叢集中具有自訂區域和端點的 HSM IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" --cluster-  
id <cluster-1234567>--region <us-east-1> --endpoint <https://cloudhsmv2.us-  
east-1.amazonaws.com>
```

OpenSSL Dynamic Engine

使用自訂端點和區域啟動 Linux EC2 執行個體

- 使用 設定工具指定叢集中具有自訂區域和端點的 HSM IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-dyn --cluster-id <cluster-1234567> --  
region <us-east-1> --endpoint <https://cloudhsmv2.us-east-1.amazonaws.com>
```

Key Storage Provider (KSP)

使用端點和區域啟動 Windows EC2 執行個體

- 使用 設定工具指定叢集中具有自訂區域和端點的 HSM IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --cluster-  
id <cluster-1234567> --region <us-east-1> --endpoint <https://cloudhsmv2.us-  
east-1.amazonaws.com>
```

JCE provider

使用自訂端點和區域啟動 Linux EC2 執行個體

- 使用 設定工具指定叢集中具有自訂區域和端點的 HSM IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-jce --cluster-id <cluster-1234567> --  
region <us-east-1> --endpoint <https://cloudhsmv2.us-east-1.amazonaws.com>
```

使用端點和區域啟動 Windows EC2 執行個體

- 使用 設定工具指定叢集中具有自訂區域和端點的 HSM IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" --cluster-  
id <cluster-1234567> --region <us-east-1> --endpoint <https://cloudhsmv2.us-  
east-1.amazonaws.com>
```

CloudHSM CLI

使用自訂端點和區域啟動 Linux EC2 執行個體

- 使用 設定工具指定叢集中具有自訂區域和端點的 HSM IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-cli --cluster-id <cluster-1234567> --  
region <us-east-1> --endpoint <https://cloudhsmv2.us-east-1.amazonaws.com>
```

使用端點和區域啟動 Windows EC2 執行個體

- 使用 設定工具指定叢集中具有自訂區域和端點的 HSM IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" --cluster-  
id <cluster-1234567> --region <us-east-1> --endpoint <https://cloudhsmv2.us-  
east-1.amazonaws.com>
```

如需 --cluster-id、--region 和 --endpoint 參數的詳細資訊，請參閱 [the section called “參數”](#)。

更新 TLS 用戶端-HSM 交互身分驗證的用戶端憑證和金鑰

Example

此範例示範如何使用 `--client-cert-hsm-tls-file` 和 `--client-key-hsm-tls-file` 參數，透過指定的自訂金鑰和 SSL 憑證來重新設定 SSL AWS CloudHSM

PKCS #11 library

使用自訂憑證和金鑰搭配 Linux 上的用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
$ sudo cp ssl-client.pem </opt/cloudhsm/etc>
$ sudo cp ssl-client.key </opt/cloudhsm/etc>
```

2. 使用設定工具來指定 `ssl-client.pem` 和 `ssl-client.key`。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 \
    --client-cert-hsm-tls-file </opt/cloudhsm/etc/ssl-client.pem> \
    --client-key-hsm-tls-file </opt/cloudhsm/etc/ssl-client.key>
```

在 Windows 上使用自訂憑證和金鑰與用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
cp ssl-client.pem <C:\ProgramData\Amazon\CloudHSM\ssl-client.pem>
cp ssl-client.key <C:\ProgramData\Amazon\CloudHSM\ssl-client.key>
```

2. 使用 PowerShell 解釋器時，請使用設定工具來指定 `ssl-client.pem` 和 `ssl-client.key`。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" `
    --client-cert-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.pem> `
    --client-key-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.key>
```

OpenSSL Dynamic Engine

使用自訂憑證和金鑰搭配 Linux 上的用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
$ sudo cp ssl-client.pem </opt/cloudhsm/etc>
sudo cp ssl-client.key </opt/cloudhsm/etc>
```

2. 使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
$ sudo /opt/cloudhsm/bin/configure-dyn \
    --client-cert-hsm-tls-file </opt/cloudhsm/etc/ssl-client.pem> \
    --client-key-hsm-tls-file </opt/cloudhsm/etc/ssl-client.key>
```

Key Storage Provider (KSP)

在 Windows 上使用自訂憑證和金鑰與用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
cp ssl-client.pem <C:\ProgramData\Amazon\CloudHSM\ssl-client.pem>
cp ssl-client.key <C:\ProgramData\Amazon\CloudHSM\ssl-client.key>
```

2. 使用 PowerShell 解譯器時，請使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" `
    --client-cert-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.pem> `
    --client-key-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.key>
```

JCE provider

使用自訂憑證和金鑰搭配 Linux 上的用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
$ sudo cp ssl-client.pem </opt/cloudhsm/etc>
```

```
sudo cp ssl-client.key </opt/cloudhsm/etc>
```

2. 使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
$ sudo /opt/cloudhsm/bin/configure-jce \  
    --client-cert-hsm-tls-file </opt/cloudhsm/etc/ssl-client.pem> \  
    --client-key-hsm-tls-file </opt/cloudhsm/etc/ssl-client.key>
```

在 Windows 上使用自訂憑證和金鑰與用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
cp ssl-client.pem <C:\ProgramData\Amazon\CloudHSM\ssl-client.pem>  
cp ssl-client.key <C:\ProgramData\Amazon\CloudHSM\ssl-client.key>
```

2. 使用 PowerShell 解譯器時，請使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" \  
    --client-cert-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-  
client.pem> \  
    --client-key-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-  
client.key>
```

CloudHSM CLI

使用自訂憑證和金鑰搭配 Linux 上的用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
$ sudo cp ssl-client.pem </opt/cloudhsm/etc>  
sudo cp ssl-client.key </opt/cloudhsm/etc>
```

2. 使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
$ sudo /opt/cloudhsm/bin/configure-cli \  
    --client-cert-hsm-tls-file </opt/cloudhsm/etc/ssl-client.pem> \  
    --client-key-hsm-tls-file </opt/cloudhsm/etc/ssl-client.key>
```

在 Windows 上使用自訂憑證和金鑰與用戶端 SDK 5 進行 TLS 用戶端-HSM 交互身分驗證

1. 將您的金鑰和憑證複製到適當的目錄。

```
cp ssl-client.pem <C:\ProgramData\Amazon\CloudHSM\ssl-client.pem>
cp ssl-client.key <C:\ProgramData\Amazon\CloudHSM\ssl-client.key>
```

2. 使用 PowerShell 解譯器時，請使用設定工具來指定 ssl-client.pem 和 ssl-client.key。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" `
        --client-cert-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.pem> `
        --client-key-hsm-tls-file <C:\ProgramData\Amazon\CloudHSM\ssl-
client.key>
```

如需 --client-cert-hsm-tls-file 和 --client-key-hsm-tls-file 參數的詳細資訊，請參閱 [the section called “參數”](#)。

停用用戶端金鑰持久性設定

Example

此範例使用 --disable-key-availability-check 參數來停用用戶端金鑰持久性設定。如要使用單一 HSM 執行叢集，您必須停用用戶端金鑰持久性設定。

PKCS #11 library

在 Linux 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --disable-key-availability-check
```

在 Windows 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" --disable-key-availability-check
```

OpenSSL Dynamic Engine

在 Linux 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
$ sudo /opt/cloudhsm/bin/configure-dyn --disable-key-availability-check
```

Key Storage Provider (KSP)

在 Windows 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --disable-key-availability-check
```

JCE provider

在 Linux 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
$ sudo /opt/cloudhsm/bin/configure-jce --disable-key-availability-check
```

在 Windows 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" --disable-key-availability-check
```

CloudHSM CLI

在 Linux 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
$ sudo /opt/cloudhsm/bin/configure-cli --disable-key-availability-check
```

在 Windows 上停用用戶端 SDK 5 的用戶端金鑰持久性

- 使用設定工具來停用用戶端金鑰持久性設定。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" --disable-key-availability-check
```

如需 `--disable-key-availability-check` 參數的詳細資訊，請參閱 [the section called “參數”](#)。

管理日誌選項

Example

用戶端 SDK 5 會使用 `log-file`、`log-level`、`log-rotation` 和 `log-type` 參數來管理記錄。

Note

若要為 AWS Fargate 或 AWS Lambda 等無伺服器環境設定開發套件，建議您將 AWS CloudHSM 日誌類型設定為 `term`。用戶端日誌將輸出到 `stderr` 並會擷取到為該環境設定的 CloudWatch Logs 日誌群組中。

PKCS #11 library

預設日誌位置

- 如果您未指定檔案的位置，系統會將日誌寫入下列預設位置：

Linux

```
/opt/cloudhsm/run/cloudhsm-pkcs11.log
```


Windows

```
C:\Program Files\Amazon\CloudHSM\cloudhsm-pkcs11.log
```

設定日誌層級，並將其他日誌選項設定為預設值

- ```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --log-level info
```

設定檔案日誌選項

- ```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --log-type file --log-file <file name with path> --log-rotation daily --log-level info
```

設定終端日誌選項

- ```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --log-type term --log-level info
```

## OpenSSL Dynamic Engine

預設日誌位置

- 如果您未指定檔案的位置，系統會將日誌寫入下列預設位置：

Linux

```
stderr
```

設定日誌層級，並將其他日誌選項設定為預設值

- ```
$ sudo /opt/cloudhsm/bin/configure-dyn --log-level info
```

設定檔案日誌選項

- ```
$ sudo /opt/cloudhsm/bin/configure-dyn --log-type <file name> --log-file file --log-rotation daily --log-level info
```

## 設定終端日誌選項

- ```
$ sudo /opt/cloudhsm/bin/configure-dyn --log-type term --log-level info
```

Key Storage Provider (KSP)

預設日誌位置

- 如果您未指定檔案的位置，系統會將日誌寫入下列預設位置：

Windows

```
C:\Program Files\Amazon\CloudHSM\cloudhsm-ksp.log
```

設定日誌層級，並將其他日誌選項設定為預設值

- ```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --log-level info
```

## 設定檔案日誌選項

- ```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --log-type file --log-file <file name> --log-rotation daily --log-level info
```

設定終端日誌選項

- ```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --log-type term --log-level info
```

## JCE provider

### 預設日誌位置

- 如果您未指定檔案的位置，系統會將日誌寫入下列預設位置：

#### Linux

```
/opt/cloudhsm/run/cloudhsm-jce.log
```

#### Windows

```
C:\Program Files\Amazon\CloudHSM\cloudhsm-jce.log
```

### 設定日誌層級，並將其他日誌選項設定為預設值

- ```
$ sudo /opt/cloudhsm/bin/configure-jce --log-level info
```

設定檔案日誌選項

- ```
$ sudo /opt/cloudhsm/bin/configure-jce --log-type file --log-file <file name> --log-rotation daily --log-level info
```

### 設定終端日誌選項

- ```
$ sudo /opt/cloudhsm/bin/configure-jce --log-type term --log-level info
```

CloudHSM CLI

預設日誌位置

- 如果您未指定檔案的位置，系統會將日誌寫入下列預設位置：

Linux

```
/opt/cloudhsm/run/cloudhsm-cli.log
```

Windows

```
C:\Program Files\Amazon\CloudHSM\cloudhsm-cli.log
```

設定日誌層級，並將其他日誌選項設定為預設值

- ```
$ sudo /opt/cloudhsm/bin/configure-cli --log-level info
```

設定檔案日誌選項

- ```
$ sudo /opt/cloudhsm/bin/configure-cli --log-type file --log-file <file name> --log-rotation daily --log-level info
```

設定終端日誌選項

- ```
$ sudo /opt/cloudhsm/bin/configure-cli --log-type term --log-level info
```

如需 log-file、log-level、log-rotation 和 log-type 參數的詳細資訊，請參閱 [the section called “參數”](#)。

放置用戶端 SDK 5 的簽發憑證

## Example

此範例使用 --hsm-ca-cert 參數來更新用戶端 SDK 5 的簽發憑證位置。

## PKCS #11 library

將用戶端 SDK 5 的簽發憑證安裝於 Linux 上

- 使用設定工具指定簽發憑證的位置。

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --hsm-ca-cert <customerCA certificate file>
```

將用戶端 SDK 5 的簽發憑證安裝於 Windows 上

- 使用設定工具指定簽發憑證的位置。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" --hsm-ca-cert <customerCA certificate file>
```

## OpenSSL Dynamic Engine

將用戶端 SDK 5 的簽發憑證安裝於 Linux 上

- 使用設定工具指定簽發憑證的位置。

```
$ sudo /opt/cloudhsm/bin/configure-dyn --hsm-ca-cert <customerCA certificate file>
```

## Key Storage Provider (KSP)

將用戶端 SDK 5 的簽發憑證安裝於 Windows 上

- 使用設定工具指定簽發憑證的位置。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --hsm-ca-cert <customerCA certificate file>
```

## JCE provider

將用戶端 SDK 5 的簽發憑證安裝於 Linux 上

- 使用設定工具指定簽發憑證的位置。

```
$ sudo /opt/cloudhsm/bin/configure-jce --hsm-ca-cert <customerCA certificate file>
```

將用戶端 SDK 5 的簽發憑證安裝於 Windows 上

- 使用設定工具指定簽發憑證的位置。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" --hsm-ca-cert <customerCA certificate file>
```

## CloudHSM CLI

將用戶端 SDK 5 的簽發憑證安裝於 Linux 上

- 使用設定工具指定簽發憑證的位置。

```
$ sudo /opt/cloudhsm/bin/configure-cli --hsm-ca-cert <customerCA certificate file>
```

將用戶端 SDK 5 的簽發憑證安裝於 Windows 上

- 使用設定工具指定簽發憑證的位置。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" --hsm-ca-cert <customerCA certificate file>
```

如需 `--hsm-ca-cert` 參數的詳細資訊，請參閱 [the section called “參數”](#)。

## 用戶端 SDK 5 設定工具的進階組態

AWS CloudHSM 用戶端 SDK 5 設定工具包含進階組態，這些組態不屬於大多數客戶使用的一般功能。進階組態提供額外的功能。

### Important

變更組態後，您需要重新啟動應用程式才能使變更生效。

- PKCS #11 的進階組態
  - [適用於的 PKCS #11 程式庫的多個槽組態 AWS CloudHSM](#)

- [的 PKCS #11 程式庫重試命令 AWS CloudHSM](#)
- OpenSSL 的進階組態
  - [的 OpenSSL 重試命令 AWS CloudHSM](#)
- KSP 的進階組態
  - [適用於的金鑰儲存提供者 \(KSP\) 的 SDK3 相容性模式 AWS CloudHSM](#)
- 適用於 JCE 的進階組態
  - [使用 JCE 供應商連線至多個 AWS CloudHSM 叢集](#)
  - [重試適用於的 JCE 命令 AWS CloudHSM](#)
  - [使用 JCE for 擷取金鑰 AWS CloudHSM](#)
- AWS CloudHSM 命令列界面 (CLI) 的進階組態
  - [使用 CloudHSM CLI 連線至多個叢集](#)

## AWS CloudHSM 用戶端 SDK 5 相關主題

請參閱下列相關主題，進一步了解 AWS CloudHSM 用戶端 SDK 5。

- [DescribeClusters](#) API 操作
- [describe-clusters](#) AWS CLI
- [Get-HSM2Cluster](#) PowerShell cmdlet
- [引導用戶端 SDK 5](#)
- [AWS CloudHSM VPC 端點](#)
- [管理用戶端 SDK 5 金鑰持久性設定](#)
- [用戶端 SDK 5 記錄](#)
- [設定 mTLS \(建議\)](#)

## AWS CloudHSM 用戶端 SDK 3 設定工具

使用 AWS CloudHSM 用戶端 SDK 3 設定工具來引導用戶端協助程式，並設定 CloudHSM 管理公用程式 (CMU)。

### 主題

- [AWS CloudHSM 用戶端 SDK 3 組態語法](#)
- [AWS CloudHSM 用戶端 SDK 3 組態參數](#)

- [AWS CloudHSM 用戶端 SDK 3 組態範例](#)
- [AWS CloudHSM 用戶端 SDK 3 組態相關主題](#)

## AWS CloudHSM 用戶端 SDK 3 組態語法

下表說明 用戶端 SDK 3 AWS CloudHSM 組態檔案的語法。

```
configure -h | --help
-a <ENI IP address>
-m [-i <daemon_id>]
--ssl --pkey <private key file> --cert <certificate file>
--cmu <ENI IP address>
```

## AWS CloudHSM 用戶端 SDK 3 組態參數

以下是設定 AWS CloudHSM 用戶端 SDK 3 的參數清單。

-h | --help

顯示命令的語法。

必要：是

-a <ENI IP address>

將指定的 HSM 彈性網路界面 (ENI) IP 地址新增至 AWS CloudHSM 組態檔案。輸入叢集中任何一個 HSM 的 ENI IP 地址。選擇哪一個都可以。

若要取得您叢集中 HSM 的 ENI IP 地址，請使用 [DescribeClusters](#) 操作、[describe-clusters](#) AWS CLI 命令，或是 [Get-HSM2Cluster](#) PowerShell Cmdlet。

### Note

執行 `-aconfigure` 命令之前，請先停止 AWS CloudHSM 用戶端。然後，當 `-a` 命令完成時，重新啟動 AWS CloudHSM 用戶端。如需詳細資訊，[請參閱範例](#)。

此參數會編輯以下組態檔案：

- `/opt/cloudhsm/etc/cloudhsm_client.cfg`：由 AWS CloudHSM 用戶端和 [key\\_mgmt\\_util](#) 使用。
- `/opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg`：由 [cloudhsm\\_mgmt\\_util](#) 使用。



當 AWS CloudHSM 用戶端啟動時，它會使用其組態檔案中的 ENI IP 地址來查詢叢集，並使用叢集中所有 HSMs 的正確 ENI IP 地址更新 `cluster.info` 檔案 (`/opt/cloudhsm/daemon/1/cluster.info`)。

必要：是

-m

更新 CMU 所使用組態檔案中的 HSM ENI IP 地址。

 Note

此 -m 參數可與用戶端 SDK 3.2.1 及更早版本的 CMU 搭配使用。對於用戶端 SDK 3.3.0 及更新版本的 CMU，請參閱 --cmu 參數，該參數可簡化更新 CMU 的 HSM 資料的程序。

當您更新 -a 參數 `configure` 並啟動 AWS CloudHSM 用戶端時，用戶端協助程式會查詢叢集，並使用叢集中所有 HSM 的正確 HSMs IP 地址來更新 `cluster.info` 檔案。將 HSM IP 地址從 `cluster.info` 複製到 `cloudhsm_mgmt_util` 使用的 `cloudhsm_mgmt_util.cfg` 組態檔案，從而執行 -m `configure` 命令並完成更新。

在執行 -a `configure` 命令之前，請務必執行 -m 命令並重新啟動 AWS CloudHSM 用戶端。這可確保從 `cluster.info` 複製到 `cloudhsm_mgmt_util.cfg` 檔案的資料既完整且準確。

必要：是

-i

指定替代的用戶端常駐程式。預設值代表 AWS CloudHSM 用戶端。

預設：1

必要：否

--ssl

以指定的私有金鑰和憑證取代叢集的 SSL 金鑰和憑證。使用此參數時，需要 --pkey 和 --cert 參數。

必要：否

--pkey

指定新的私有金鑰。輸入包含私有金鑰之檔案的路徑和名稱。

必要：如果指定 `--ssl` 則為是。否則不應使用此項目。

`--cert`

指定新的憑證。輸入包含憑證之檔案的路徑和名稱。此憑證應會鏈結至 `customerCA.crt` 憑證，即用於初始化叢集的自簽憑證。如需詳細資訊，請參閱[初始化叢集](#)。

必要：如果指定 `--ssl` 則為是。否則不應使用此項目。

`--cmu <ENI IP address>`

將 `-a` 和 `-m` 參數合併為一個參數。將指定的 HSM 彈性網路介面 (ENI) IP 地址新增至 AWS CloudHSM 組態檔案，然後更新 CMU 組態檔案。輸入叢集中任何 HSM 的任何 IP 地址。如需用戶端 SDK 3.2.1 及更早版本，請參閱[使用用戶端 SDK 3.2.1 及更早版本隨附的 CMU](#)。

必要：是

## AWS CloudHSM 用戶端 SDK 3 組態範例

這些範例示範如何使用適用於 AWS CloudHSM 用戶端 SDK 3 `configure` 的工具。

Example：更新 AWS CloudHSM 用戶端和 `key_mgmt_util` 的 HSM 資料

此範例使用的 `-a` 參數 `configure` 來更新 AWS CloudHSM 用戶端和 `key_mgmt_util` 的 HSM 資料。若要使用此 `-a` 參數，您必須擁有叢集中其中一個 HSM 的 IP 地址。使用主控台或 AWS CLI 取得 IP 地址。

取得 HSM 的 IP 地址（主控台）

1. 在 <https://console.aws.amazon.com/cloudhsm/home> 開啟 AWS CloudHSM 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 若要開啟叢集詳細資訊頁面，請在叢集表格中選擇叢集 ID。
4. 若要取得 IP 地址，請前往 HSMs 索引標籤。對於 IPv4 叢集，請選擇 ENI IPv4 地址下列出的地址。對於雙堆疊叢集，請使用 ENI IPv4 或 ENI IPv6 地址。

取得 HSM 的 IP 地址 (AWS CLI)

- 使用 AWS CLI 中的 [describe-clusters](#) 命令取得 HSM 的 IP 地址。在命令的輸出中，HSMs 的 IP 地址是 `EniIp` 和 `EniIpV6` (如果是雙堆疊叢集)。

```
$ aws cloudhsmv2 describe-clusters
```

```
{
 "Clusters": [
 { ... }
 "Hsms": [
 {
...
 "EniIp": "10.0.0.9",
...
 },
 {
...
 "EniIp": "10.0.1.6",
 "EniIpV6": "2600:113f:404:be09:310e:ed34:3412:f733",
...
 }
]
 }
}
```

## : 更新 HSM 資料

1. 更新 `-a` 參數之前，請先停止 AWS CloudHSM 用戶端。這可防止在 `configure` 編輯用戶端的組態檔案時可能發生的衝突。如果用戶端已停止，而此命令不會帶來任何影響，因此您可以在指令碼中使用它。

### Amazon Linux

```
$ sudo stop cloudhsm-client
```

### Amazon Linux 2

```
$ sudo service cloudhsm-client stop
```

### CentOS 7

```
$ sudo service cloudhsm-client stop
```

### CentOS 8

```
$ sudo service cloudhsm-client stop
```

## RHEL 7

```
$ sudo service cloudhsm-client stop
```

## RHEL 8

```
$ sudo service cloudhsm-client stop
```

## Ubuntu 16.04 LTS

```
$ sudo service cloudhsm-client stop
```

## Ubuntu 18.04 LTS

```
$ sudo service cloudhsm-client stop
```

## Windows

- 用於 Windows 用戶端 1.1.2+ :

```
C:\Program Files\Amazon\CloudHSM>net.exe stop AWSCloudHSMClient
```

- 用於 Windows 用戶端 1.1.1 和更早版本 :

在您啟動 AWS CloudHSM 用戶端的命令視窗中使用 Ctrl + C。

2. 此步驟使用 configure 的 -a 參數，來將 10.0.0.9 ENI IP 地址新增至組態檔案。

## Amazon Linux

```
$ sudo /opt/cloudhsm/bin/configure -a 10.0.0.9
```

## Amazon Linux 2

```
$ sudo /opt/cloudhsm/bin/configure -a 10.0.0.9
```

## CentOS 7

```
$ sudo /opt/cloudhsm/bin/configure -a 10.0.0.9
```

## CentOS 8

```
$ sudo /opt/cloudhsm/bin/configure -a 10.0.0.9
```

## RHEL 7

```
$ sudo /opt/cloudhsm/bin/configure -a 10.0.0.9
```

## RHEL 8

```
$ sudo /opt/cloudhsm/bin/configure -a 10.0.0.9
```

## Ubuntu 16.04 LTS

```
$ sudo /opt/cloudhsm/bin/configure -a 10.0.0.9
```

## Ubuntu 18.04 LTS

```
$ sudo /opt/cloudhsm/bin/configure -a 10.0.0.9
```

## Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" -a 10.0.0.9
```

3. 接著，重新啟動 AWS CloudHSM 用戶端。用戶端啟動時，會使用組態檔案中的 ENI IP 地址來查詢叢集。接著會將叢集中所有 HSM 的 ENI IP 地址新增至 `cluster.info` 檔案。

## Amazon Linux

```
$ sudo start cloudhsm-client
```

## Amazon Linux 2

```
$ sudo service cloudhsm-client start
```

## CentOS 7

```
$ sudo service cloudhsm-client start
```

## CentOS 8

```
$ sudo service cloudhsm-client start
```

## RHEL 7

```
$ sudo service cloudhsm-client start
```

## RHEL 8

```
$ sudo service cloudhsm-client start
```

## Ubuntu 16.04 LTS

```
$ sudo service cloudhsm-client start
```

## Ubuntu 18.04 LTS

```
$ sudo service cloudhsm-client start
```

## Windows

- 用於 Windows 用戶端 1.1.2+ :

```
C:\Program Files\Amazon\CloudHSM>net.exe start AWSCloudHSMClient
```

- 用於 Windows 用戶端 1.1.1 和更早版本 :

```
C:\Program Files\Amazon\CloudHSM>start "cloudhsm_client" cloudhsm_client.exe
C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_client.cfg
```

當命令完成時，AWS CloudHSM 用戶端和 key\_mgmt\_util 使用的 HSM 資料完整且準確。

Example：從用戶端 SDK 3.2.1 及更早版本更新 CMU 的 HSM 資料

此範例使用 `-m configure` 命令，將來自 `cluster.info` 檔案的更新 HSM 資料複製到 `cloudhsm_mgmt_util` 使用的 `cloudhsm_mgmt_util.cfg` 檔案。請搭配用戶端 SDK 3.2.1 及更早版本隨附的 CMU 使用此功能。

- 在執行之前 `-m`，請停止 AWS CloudHSM 用戶端、執行 `-a` 命令，然後重新啟動 AWS CloudHSM 用戶端，如[上一個範例](#)所示。這可確保從 `cluster.info` 檔案複製到 `cloudhsm_mgmt_util.cfg` 檔案的資料既完整且準確。

Linux

```
$ sudo /opt/cloudhsm/bin/configure -m
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" -m
```

Example：從用戶端 SDK 3.3.0 及更新版本更新 CMU 的 HSM 資料

此範例使用 `configure` 的 `--cmu` 參數來更新 CMU 的 HSM 資料。請搭配用戶端 SDK 3.3.0 及更新版本隨附的 CMU 使用此功能。如需有關使用 CMU 的詳細資訊，請參閱[使用 CloudHSM 管理公用程式 \(CMU\) 管理使用者](#)和[使用用戶端 SDK 3.2.1 及更早版本隨附的 CMU](#)。

- 使用此 `--cmu` 參數傳遞叢集中 HSM 的 IP 地址。

Linux

```
$ sudo /opt/cloudhsm/bin/configure --cmu <IP address>
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" --cmu <IP address>
```

## AWS CloudHSM 用戶端 SDK 3 組態相關主題

請參閱下列相關主題，進一步了解 AWS CloudHSM 用戶端 SDK 3。

- [設定 AWS CloudHSM key\\_mgmt\\_util](#)

## AWS CloudHSM 命令列界面 (CLI)

CloudHSM CLI 可協助管理員管理其叢集中的使用者和加密使用者管理金鑰 AWS CloudHSM。CLI 包含可用於建立、刪除和列出使用者、變更使用者密碼、更新使用者多重要素驗證 (MFA) 的工具。它還包括產生、刪除、匯入和匯出金鑰、取得和設定屬性、尋找金鑰和執行密碼編譯操作的命令。

如需已定義的 CloudHSM CLI 使用者清單，請參閱 [使用 CloudHSM CLI 進行 HSM 使用者管理](#)。如需 CloudHSM CLI 金鑰屬性的定義清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。如需有關如何使用 CloudHSM CLI 管理金鑰的資訊，請參閱 [使用 CloudHSM CLI 進行金鑰管理](#)。

如需快速入門，請參閱 [開始使用 AWS CloudHSM 命令列界面 \(CLI\)](#)。如需 CloudHSM CLI 命令的詳細資訊以及使用命令的範例，請參閱 [CloudHSM CLI 命令的參考資料](#)。

### 主題

- [AWS CloudHSM 支援命令列界面 \(CLI\) 的平台](#)
- [從 AWS CloudHSM 用戶端 SDK 3 CMU 和 KMU 遷移至用戶端 SDK 5 CloudHSM CLI](#)
- [開始使用 AWS CloudHSM 命令列界面 \(CLI\)](#)
- [CloudHSM CLI 中的命令模式](#)
- [CloudHSM CLI 的金鑰屬性](#)
- [CloudHSM CLI 的進階組態](#)
- [CloudHSM CLI 命令的參考資料](#)

## AWS CloudHSM 支援命令列界面 (CLI) 的平台

本主題說明 CLI 支援的 Linux 和 Windows AWS CloudHSM 平台。

### Linux 支援

| 支援平台              | X86_64 架構 | ARM 架構 |
|-------------------|-----------|--------|
| Amazon Linux 2    | 是         | 是      |
| Amazon Linux 2023 | 是         | 是      |



| 支援平台                              | X86_64 架構 | ARM 架構 |
|-----------------------------------|-----------|--------|
| Red Hat Enterprise Linux 8 (8.3+) | 是         | 否      |
| Red Hat Enterprise Linux 9 (9.2+) | 是         | 是      |
| Ubuntu 22.04 LTS                  | 是         | 是      |
| Ubuntu 24.04 LTS                  | 是         | 是      |

- SDK 5.16 是提供 Ubuntu 20.04 LTS 平台支援的最後版本。如需詳細資訊，請參閱 [Ubuntu 網站](#)。
- SDK 5.12 是提供 CentOS 7 (7.8+) 平台支援的最後版本。如需詳細資訊，請參閱 [CentOS 網站](#)。
- SDK 5.12 是提供 Red Hat Enterprise Linux 7 (7.8+) 平台支援的最後版本。如需詳細資訊，請參閱 [Red Hat 網站](#)。
- SDK 5.4.2 是提供 CentOS 8 平台支援的最後版本。如需詳細資訊，請參閱 [CentOS 網站](#)。

## Windows 支援

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

## 從 AWS CloudHSM 用戶端 SDK 3 CMU 和 KMU 遷移至用戶端 SDK 5 CloudHSM CLI

使用此主題遷移使用 AWS CloudHSM 用戶端 SDK 3 命令列工具、CloudHSM Management Utility (CMU) 和 Key Management Utility (KMU) 的工作流程，以改為使用用戶端 SDK 5 命令列工具 CloudHSM CLI。

在 中 AWS CloudHSM，客戶應用程式會使用 AWS CloudHSM 用戶端軟體開發套件 (SDK) 執行密碼編譯操作。用戶端 SDK 5 是持續新增新功能和平台支援的主要 SDK。本主題提供從用戶端 SDK 3 遷移到用戶端 SDK 5 的命令列工具的特定詳細資訊。

用戶端 SDK 3 包含兩個不同的命令列工具：用於管理使用者的 CMU，以及用於管理金鑰和使用金鑰執行操作的 KMU。用戶端 SDK 5 會將 CMU 和 KMU（用戶端 SDK 3 隨附的工具）的函數合併為單一

工具 [AWS CloudHSM 命令列界面 \(CLI\)](#)。您可以在 子命令 [CloudHSM CLI 中的使用者類別](#) 和 下找到使用者管理操作 [CloudHSM CLI 中的規定人數類別](#)。金鑰管理操作可在 [金鑰子命令](#) 下找到，而密碼編譯操作可在 [密碼子命令](#) 下找到。如需命令的完整清單，[CloudHSM CLI 命令的參考資料](#) 請參閱。

如需遷移至用戶端 SDK 5 的指示，請參閱 [從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)。如需遷移的優勢，請參閱 [AWS CloudHSM 用戶端 SDK 5 的優點](#)。

## 開始使用 AWS CloudHSM 命令列界面 (CLI)

使用 CloudHSM CLI 命令列界面 (CLI)，您可以管理 AWS CloudHSM 叢集中的使用者。使用此主題來開始使用基本硬體安全模組 (HSM) 使用者管理任務，例如建立使用者、列出使用者，以及將 CloudHSM CLI 連線至叢集。

### 主題

- [安裝 CloudHSM CLI](#)
- [使用 CloudHSM CLI](#)

## 安裝 CloudHSM CLI

使用下列命令來下載並安裝的 CloudHSM CLI AWS CloudHSM。

### Amazon Linux 2023

x86\_64 架構上的 Amazon Linux 2023：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-cli-latest.amzn2023.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.amzn2023.x86_64.rpm
```

ARM64 架構上的 Amazon Linux 2023：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-cli-latest.amzn2023.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.amzn2023.aarch64.rpm
```

## Amazon Linux 2

Amazon Linux 2 (x86\_64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-cli-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el7.x86_64.rpm
```

Amazon Linux 2 (ARM64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-cli-latest.el7.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el7.aarch64.rpm
```

## RHEL 9 (9.2+)

x86\_64 架構上的 RHEL 9 :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-cli-latest.el9.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el9.x86_64.rpm
```

ARM64 架構上的 RHEL 9 :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-cli-latest.el9.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el9.aarch64.rpm
```

## RHEL 8 (8.3+)

RHEL 8 (x86\_64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-cli-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-cli-latest.el8.x86_64.rpm
```

## Ubuntu 24.04 LTS

x86\_64 架構上的 Ubuntu 24.04 LTS :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/cloudhsm-
cli_latest_u24.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u24.04_amd64.deb
```

ARM64 架構上的 Ubuntu 24.04 LTS :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/cloudhsm-
cli_latest_u24.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u24.04_arm64.deb
```

## Ubuntu 22.04 LTS

Ubuntu 22.04 LTS (x86\_64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/cloudhsm-
cli_latest_u22.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u22.04_amd64.deb
```

ARM64 架構上的 Ubuntu 22.04 LTS :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/cloudhsm-
cli_latest_u22.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u22.04_arm64.deb
```

## Ubuntu 20.04 LTS

Ubuntu 20.04 LTS (x86\_64 架構) :

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Focal/cloudhsm-
cli_latest_u20.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-cli_latest_u20.04_amd64.deb
```

## Windows Server 2022

對於 x86\_64 架構上的 Windows Server 2022，請以管理員身分開啟 PowerShell，並執行下列命令：

```
PS C:\> wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Windows/
AWSCloudHSMCLI-latest.msi -Outfile C:\AWSCloudHSMCLI-latest.msi
```

```
PS C:\> Start-Process msixexec.exe -ArgumentList '/i C:\AWSCloudHSMCLI-latest.msi /
quiet /norestart /log C:\client-install.txt' -Wait
```

## Windows Server 2019

對於 Windows Server 2019 (x86\_64 架構)，請以系統管理員身分開啟 PowerShell，然後執行下列命令：

```
PS C:\> wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Windows/
AWSCloudHSMCLI-latest.msi -Outfile C:\AWSCloudHSMCLI-latest.msi
```

```
PS C:\> Start-Process msixexec.exe -ArgumentList '/i C:\AWSCloudHSMCLI-latest.msi /
quiet /norestart /log C:\client-install.txt' -Wait
```

## Windows Server 2016

對於 Windows Server 2016 (x86\_64 架構)，請以系統管理員身分開啟 PowerShell，然後執行下列命令：

```
PS C:\> wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Windows/
AWSCloudHSMCLI-latest.msi -Outfile C:\AWSCloudHSMCLI-latest.msi
```

```
PS C:\> Start-Process msixexec.exe -ArgumentList '/i C:\AWSCloudHSMCLI-latest.msi /
quiet /norestart /log C:\client-install.txt' -Wait
```

使用下列命令來設定 CloudHSM CLI。

為用戶端 SDK 5 引導 Linux EC2 執行個體

- 使用設定工具指定叢集中 HSM 的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure-cli -a <The ENI IPv4 / IPv6 addresses of the HSMs>
```

為用戶端 SDK 5 引導 Windows EC2 執行個體

- 使用設定工具指定叢集中 HSM 的 IP 地址。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" -a <The ENI IPv4 / IPv6 addresses of the HSMs>
```

## 使用 CloudHSM CLI

使用下列命令來啟動和使用 CloudHSM CLI。

1. 使用下列命令來啟動 CloudHSM CLI。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

2. 使用 login 命令登入叢集。所有使用者都可以使用此命令。

以下範例中的命令將 admin 登入，這是預設的[管理員](#)帳戶。您已在[啟用叢集](#)時設定此使用者的密碼。

```
aws-cloudhsm > login --username admin --role admin
```

系統會提示您輸入密碼。您輸入密碼，然後輸出顯示命令已成功。

```
Enter password:
```

```
{
 "error_code": 0,
 "data": {
 "username": "admin",
 "role": "admin"
 }
}
```

3. 執行 `user list` 命令以列出叢集上的所有使用者。

```
aws-cloudhsm > user list
{
 "error_code": 0,
 "data": {
 "users": [
 {
 "username": "admin",
 "role": "admin",
 "locked": "false",
 "mfa": [],
 "cluster-coverage": "full"
 },
 {
 "username": "app_user",
 "role": "internal(APPLIANCE_USER)",
 "locked": "false",
 "mfa": [],
 "cluster-coverage": "full"
 }
]
 }
}
```

4. 用於 `user create` 建立名為 **example\_user** 的 CU 使用者。

您可以建立 CU，因為在上一個步驟中，您以系統管理員使用者身分登入。只有管理員使用者可以執行使用者管理工作，例如建立和刪除使用者，以及變更其他使用者的密碼。

```
aws-cloudhsm > user create --username example_user --role crypto-user
Enter password:
```

```
Confirm password:
{
 "error_code": 0,
 "data": {
 "username": "example_user",
 "role": "crypto-user"
 }
}
```

5. 用 `user list` 來列出叢集上的所有使用者。

```
aws-cloudhsm > user list
{
 "error_code": 0,
 "data": {
 "users": [
 {
 "username": "admin",
 "role": "admin",
 "locked": "false",
 "mfa": [],
 "cluster-coverage": "full"
 },
 {
 "username": "example_user",
 "role": "crypto_user",
 "locked": "false",
 "mfa": [],
 "cluster-coverage": "full"
 },
 {
 "username": "app_user",
 "role": "internal(APPLIANCE_USER)",
 "locked": "false",
 "mfa": [],
 "cluster-coverage": "full"
 }
]
 }
}
```

6. 使用 `logout` 命令登出 AWS CloudHSM 叢集。



```
aws-cloudhsm > logout
{
 "error_code": 0,
 "data": "Logout successful"
}
```

7. 使用 quit 命令停止 CLI。

```
aws-cloudhsm > quit
```

## CloudHSM CLI 中的命令模式

在 CloudHSM CLI 中，您可以使用兩種不同的方式執行命令，分別是：單一命令模式和互動式模式。互動式模式專為使用者設計，而單一命令模式則是專為指令碼設計。

### Note

所有命令均在互動式模式和單一命令模式下工作。

## 互動式模式

使用以下命令來啟動 CloudHSM CLI 互動式模式。

Linux

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive
```

在互動式模式下使用 CLI 時，您可使用 login 命令登入使用者帳戶。

```
aws-cloudhsm > login --username <USERNAME> --role <ROLE>
```

若要列出所有 CloudHSM CLI 命令，請執行以下命令：

```
aws-cloudhsm > help
```

若要取得某一 CloudHSM CLI 命令的語法，請執行以下命令：

```
aws-cloudhsm > help <command-name>
```

若要取得 HSM 上的使用者清單，請輸入 user list。

```
aws-cloudhsm > user list
```

若要結束 CloudHSM CLI 工作階段，請執行以下命令：

```
aws-cloudhsm > quit
```

## 單一命令模式

如要在單一命令模式下執行 CloudHSM CLI，則需設定兩個環境變數以提供憑證：CLOUDHSM\_PIN 和 CLOUDHSM\_ROLE：

```
$ export CLOUDHSM_ROLE=admin
```

```
$ export CLOUDHSM_PIN=admin_username:admin_password
```

環境變數設定完成後，您可使用儲存在環境中的憑證來執行命令。

```
$ cloudhsm-cli user change-password --username alice --role crypto-user
Enter password:
Confirm password:
{
 "error_code": 0,
 "data": {
 "username": "alice",
 "role": "crypto-user"
 }
}
```

## CloudHSM CLI 的金鑰屬性

本主題旨在說明如何使用 CloudHSM CLI 設定金鑰屬性。CloudHSM CLI 中的金鑰屬性可以定義金鑰的類型、金鑰的運作方式或金鑰的標記方式。某些屬性定義唯一的特性 (例如，金鑰的類型)。其他屬性可以設定為 true 或 false (變更它們會啟動或停用金鑰功能的一部分)。

如需展示如何使用金鑰屬性的範例，請參閱父命令 [CloudHSM CLI 中的金鑰類別](#) 下列出的命令。

下列主題提供 CloudHSM CLI 中關鍵屬性的其他詳細資訊。

### 主題

- [CloudHSM CLI 支援的屬性](#)
- [在 CloudHSM CLI 中檢查值](#)
- [CloudHSM CLI 的相關主題](#)

## CloudHSM CLI 支援的屬性

最佳實務是，只為您希望更有限制性的屬性設定值。如果您未指定值，CloudHSM CLI 會使用下表中指定的預設值。

下表列出 CloudHSM CLI 的關鍵屬性、可能的值、預設值和相關備註。值欄位中的空白儲存格表示屬性沒有獲派指定預設值。

| CloudHSM CLI屬性   | Value                                        | 可以使用 <a href="#">密鑰集屬性</a> 進行修改 | 可在建立金鑰時設定 |
|------------------|----------------------------------------------|---------------------------------|-----------|
| always-sensitive | 如果 sensitive 一直被設置為 True 並且從未更改過，則該值是 True。  | 否                               | 否         |
| check-value      | 金鑰的金鑰檢查值。如需詳細資訊，請參閱 <a href="#">其他詳細資訊</a> 。 | 否                               | 否         |
| class            | 可能的值：secret-key、public-                      | 否                               | 是         |

| CloudHSM CLI屬性 | Value                                                                                                          | 可以使用 <a href="#">密鑰集屬性</a> 進行修改                          | 可在建立金鑰時設定       |
|----------------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|-----------------|
|                | key 和 private-key 。                                                                                            |                                                          |                 |
| curve          | 用於產生 EC 金鑰對的橢圓曲線。<br><br>有效值：secp224r1<br>、secp256r1<br>、prime256v1<br>、secp384r1<br>、secp256k1<br>和 secp521r1 | 否                                                        | 可設定 EC，不可設定 RSA |
| decrypt        | 預設：False                                                                                                       | 是                                                        | 是               |
| derive         | 預設：False                                                                                                       | 您可以在 hsm2medium 執行個體上設定衍生。無法在 hsm1medium 執行個體上設定 RSA 金鑰。 | 是               |
| destroyable    | 預設：True                                                                                                        | 是                                                        | 是               |
| ec-point       | 如果是 EC 金鑰，則以十六進位格式對 ANSI X9.62 ECPoint 值「Q」進行 DER 編碼。<br><br>對於其他金鑰類型，這個屬性不存在。                                 | 否                                                        | 否               |
| encrypt        | 預設：False                                                                                                       | 是                                                        | 是               |
| extractable    | 預設：True                                                                                                        | 否                                                        | 是               |

| CloudHSM CLI屬性    | Value                                          | 可以使用 <a href="#">密鑰集屬性</a> 進行修改                   | 可在建立金鑰時設定                |
|-------------------|------------------------------------------------|---------------------------------------------------|--------------------------|
| id                | 預設值：空                                          | ID 可在 hsm2medium 執行個體上設定。它無法在 hsm1medium 執行個體上設定。 | 是                        |
| key-length-bytes  | 產生 AES 密鑰所需。<br>有效值：16、24 和 32 位元組。            | 否                                                 | 否                        |
| key-type          | 可能的值：aes、rsa 和 ec。                             | 否                                                 | 是                        |
| label             | 預設值：空                                          | 是                                                 | 是                        |
| local             | 預設值：True 適用於在 HSM 中產生的金鑰，False 適用於匯入至 HSM 的金鑰。 | 否                                                 | 否                        |
| modifiable        | 預設：True                                        | 可以從 true 變更為 false，但不能從 false 變更為 true。           | 是                        |
| modulus           | 用於產生 RSA 金鑰對的模數。對於其他金鑰類型，這個屬性不存在。              | 否                                                 | 否                        |
| modulus-size-bits | 產生 RSA 金鑰對時需要。<br>最小值為 2048。                   | 否                                                 | 可使用 RSA 設定，而無法使用 EC 進行設定 |

| CloudHSM CLI屬性    | Value                                                                                                                                   | 可以使用 <a href="#">密鑰集屬性</a> 進行修改 | 可在建立金鑰時設定                |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|--------------------------|
| never-extractable | <p>如果可擷取值從未設置為 False，則該值為 True。</p> <p>如果可擷取值已被設置為 True，則該值為 False。</p>                                                                 | 否                               | 否                        |
| private           | 預設：True                                                                                                                                 | 否                               | 是                        |
| public-exponent   | <p>產生 RSA 金鑰對時需要。</p> <p>有效值：值必須為大於或等於 65537 的奇數。</p>                                                                                   | 否                               | 可使用 RSA 設定，而無法使用 EC 進行設定 |
| sensitive         | <p>預設：</p> <ul style="list-style-type: none"> <li>此值為 True，適用於 AES 金鑰以及 EC 和 RSA 私有金鑰。</li> <li>此值為 False，適用於 EC 和 RSA 公有金鑰。</li> </ul> | 否                               | 可使用私有金鑰設定，而不能使用公有金鑰設定。   |
| sign              | <p>預設：</p> <ul style="list-style-type: none"> <li>此值為 True，適用於 AES 金鑰。</li> <li>此值為 False，適用於 RSA 和 EC 金鑰。</li> </ul>                   | 是                               | 是                        |

| CloudHSM CLI屬性    | Value                                                                                                          | 可以使用 <a href="#">密鑰集屬性</a> 進行修改         | 可在建立金鑰時設定  |
|-------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------|------------|
| token             | 預設：True                                                                                                        | 可以從 false 變更為 true，但不能從 true 變更為 false。 | 是          |
| trusted           | 預設：False                                                                                                       | 只有管理員使用者可以設定此參數。                        | 否          |
| unwrap            | 預設：False                                                                                                       | 是                                       | 是，但公有金鑰除外。 |
| unwrap-template   | 這些值應使用已套用於以此包裝金鑰取消包裝之任何金鑰的屬性範本。                                                                                | 是                                       | 否          |
| verify            | 預設： <ul style="list-style-type: none"> <li>此值為 True，適用於 AES 金鑰。</li> <li>此值為 False，適用於 RSA 和 EC 金鑰。</li> </ul> | 是                                       | 是          |
| wrap              | 預設：False                                                                                                       | 是                                       | 是，私有金鑰除外。  |
| wrap-template     | 這些值應使用屬性範本來匹配使用此包裝金鑰所包裝的金鑰。                                                                                    | 是                                       | 否          |
| wrap-with-trusted | 預設：False                                                                                                       | 是                                       | 是          |

## 在 CloudHSM CLI 中檢查值

CloudHSM CLI 中的檢查值是 HSM 匯入或產生金鑰時產生的金鑰的 3 位元組雜湊或檢查總和。您也可以 HSM 之外計算檢查值，例如在匯出金鑰之後。然後，您可以比較檢查值以確認金鑰的身分和完整性。如需獲取金鑰的檢查值，請使用帶有詳細標誌的[金鑰列表](#)。

AWS CloudHSM 使用以下標準方法產生檢查值：

- 對稱密鑰：使用金鑰加密零塊的結果的前 3 個位元組。
- 非對稱金鑰配對：公有金鑰 SHA-1 雜湊的前 3 個位元組。
- HMAC 金鑰：目前不支援 HMAC 金鑰的 KCV。

## CloudHSM CLI 的相關主題

如需 CloudHSM CLI 的詳細資訊，請參閱下列主題。

- [CloudHSM CLI 中的金鑰類別](#)
- [CloudHSM CLI 命令的參考資料](#)

## CloudHSM CLI 的進階組態

Command AWS CloudHSM Line Interface (CLI) 包含下列進階組態，這不屬於大多數客戶使用的一般組態。這些組態提供額外的功能。

- [連接至多個叢集](#)

## 使用 CloudHSM CLI 連線至多個叢集

透過 AWS CloudHSM 用戶端 SDK 5，您可以設定 CloudHSM CLI，以允許從單一 CLI 執行個體連線至多個 CloudHSM 叢集。

下列主題說明如何使用 CloudHSM CLI 多叢集功能來連接多個叢集。

### 主題

- [的多叢集先決條件 AWS CloudHSM](#)
- [為多叢集功能設定 CloudHSM CLI](#)
- [將叢集新增至您的 AWS CloudHSM 組態](#)



- [從 AWS CloudHSM 組態中移除叢集](#)
- [在 中與多個叢集互動 AWS CloudHSM](#)

## 的多叢集先決條件 AWS CloudHSM

在 中設定叢集 AWS CloudHSM 以連線至多個叢集之前，您必須符合下列先決條件：

- 您要連線的兩個或多個 AWS CloudHSM 叢集及其叢集憑證。
- 具有安全群組的 EC2 執行個體正確設定為連線到上述所有叢集。如需如何設定叢集和用戶端執行個體的詳細資訊，請參閱 [入門 AWS CloudHSM](#)。
- 若要設定多叢集功能，您必須已下載並安裝 CloudHSM CLI。若您尚未完成此動作，請參閱 [???](#) 中的說明。
- 您將無法存取使用設定的叢集，`./configure-cli[.exe] -a`因為它不會與 建立關聯cluster-id。您可以`config-cli add-cluster`依照本指南所述，依照 重新設定它。

## 為多叢集功能設定 CloudHSM CLI

若要為多叢集功能設定 CloudHSM CLI，請遵循下列步驟：

1. 識別您要連線的叢集。
2. 使用 [configure-cli](#) 子命令將這些叢集新增至 CloudHSM CLI 組態`add-cluster`，如下所述。
3. 重新啟動任何 CloudHSM CLI 程序，新組態才會生效。

## 將叢集新增至您的 AWS CloudHSM 組態

連線至多個叢集時，請使用 `configure-cli add-cluster`命令將叢集新增至您的組態。

## 語法

```
configure-cli add-cluster [OPTIONS]
 --cluster-id <CLUSTER ID>
 [--region <REGION>]
 [--endpoint <ENDPOINT>]
 [--hsm-ca-cert <HSM CA CERTIFICATE FILE>]
 [--client-cert-hsm-tls-file <CLIENT CERTIFICATE FILE>]
 [--client-key-hsm-tls-file <CLIENT KEY FILE>]
 [-h, --help]
```

## 範例

### 使用 **cluster-id** 參數新增叢集

#### Example

搭配使用 `configure-cli add-cluster` 和 `cluster-id` 參數，將叢集 (ID 為 `cluster-1234567`) 新增至您的組態。

#### Linux

```
$ sudo /opt/cloudhsm/bin/configure-cli add-cluster --cluster-id <cluster-1234567>
```

#### Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" add-cluster --cluster-id <cluster-1234567>
```

#### Tip

如果 `configure-cli add-cluster` 與 `cluster-id` 參數搭配使用不會導致新增叢集，請參閱下列範例，以取得此命令的更長版本，此命令也需要 `--region` 和 `--endpoint` 參數來識別要新增的叢集。例如，如果叢集區域與設定為 AWS CLI 預設值的區域不同，則應使用 `--region` 參數來使用正確的區域。此外，您可以指定用於呼叫的 AWS CloudHSM API 端點，這對於各種網路設定而言可能是必要的，例如使用不使用預設 DNS 主機名稱的 VPC 介面端點 AWS CloudHSM。

### 使用 **cluster-id**、**endpoint** 和 **region** 參數新增叢集

#### Example

搭配使用 `configure-cli add-cluster` 以及 `cluster-id`、`endpoint` 和 `region` 參數將叢集 (ID 為 `cluster-1234567`) 新增至您的組態。

#### Linux

```
$ sudo /opt/cloudhsm/bin/configure-cli add-cluster --cluster-id <cluster-1234567> --region <us-east-1> --endpoint <https://cloudhsmv2.us-east-1.amazonaws.com>
```

## Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" add-cluster --
cluster-id <cluster-1234567> --region <us-east-1> --endpoint <https://cloudhsmv2.us-
east-1.amazonaws.com>
```

如需 `--cluster-id`、`--region` 和 `--endpoint` 參數的詳細資訊，請參閱 [the section called “參數”](#)。

### 參數

`--cluster-id` **<Cluster ID>**

進行 `DescribeClusters` 呼叫以尋找叢集中與叢集 ID 關聯的所有 HSM 彈性網路介面 (ENI) IP 地址。系統會將 ENI IP 地址新增至 AWS CloudHSM 組態檔案。

#### Note

如果您從無法存取公有網際網路的 VPC 內 EC2 執行個體使用 `--cluster-id` 參數，則必須建立要連線的介面 VPC 端點 AWS CloudHSM。如需 VPC 端點的詳細資訊，請參閱 [???](#)。

必要：是

`--endpoint` **<Endpoint>**

指定用於進行 `DescribeClusters` 呼叫的 AWS CloudHSM API 端點。您必須結合 `--cluster-id` 設定此選項。

必要：否

`--hsm-ca-cert` **<HsmCA Certificate Filepath>**

指定 HSM CA 憑證的檔案路徑。

必要：否

`--region` **<Region>**

指您叢集的區域。您必須結合 `--cluster-id` 設定此選項。

如果您未提供 `--region` 參數，系統會嘗試讀取 `AWS_DEFAULT_REGION` 或 `AWS_REGION` 環境變數來選擇區域。如果未設定這些變數，則除非您在 `AWS_CONFIG_FILE` 環境變數中指定了不同的檔案，否則系統會檢查 AWS config 檔案中 (通常是 `~/.aws/config`) 與您的設定檔相關聯的區域。如果未設定上述任何變數，系統會預設為 `us-east-1` 區域。

必要：否

`--client-cert-hsm-tls-file` *<client certificate hsm tls>###*

用於 TLS 用戶端-HSM 交互身分驗證的用戶端憑證路徑。

只有在您已使用 CloudHSM CLI 在 HSM 上註冊至少一個信任錨點時，才使用此選項。您必須結合 `--client-key-hsm-tls-file` 設定此選項。

必要：否

`--client-key-hsm-tls-file` *<client key hsm tls>###*

用於 TLS 用戶端-HSM 交互身分驗證的用戶端金鑰路徑。

只有在您已使用 CloudHSM CLI 在 HSM 上註冊至少一個信任錨點時，才使用此選項。您必須結合 `--client-cert-hsm-tls-file` 設定此選項。

必要：否

## 從 AWS CloudHSM 組態中移除叢集

使用 CloudHSM CLI 連線至多個叢集時，請使用 `configure-cli remove-cluster` 命令從您的組態中移除叢集。

### 語法

```
configure-cli remove-cluster [OPTIONS]
 --cluster-id <CLUSTER ID>
 [-h, --help]
```

### 範例

使用 **cluster-id** 參數移除叢集

#### Example

搭配使用 `configure-cli remove-cluster` 和 `cluster-id` 參數，從您的組態中移除叢集 (ID 為 `cluster-1234567`)。

## Linux

```
$ sudo /opt/cloudhsm/bin/configure-cli remove-cluster --cluster-id <cluster-1234567>
```

## Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-cli.exe" remove-cluster --cluster-id <cluster-1234567>
```

如需 `--cluster-id` 參數的詳細資訊，請參閱 [the section called “參數”](#)。

## 參數

`--cluster-id` **<Cluster ID>**

要從組態中移除的叢集 ID。

必要：是

## 在中與多個叢集互動 AWS CloudHSM

使用 CloudHSM CLI 設定多個叢集之後，請使用 `cloudhsm-cli` 命令與其互動。

## 範例

使用互動式模式 `cluster-id` 時設定預設值

## Example

使用 [???](#) 搭配 `cluster-id` 參數，從您的組態設定預設叢集 (ID 為 `cluster-1234567`)。

## Linux

```
$ cloudhsm-cli interactive --cluster-id <cluster-1234567>
```

## Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" interactive --cluster-id <cluster-1234567>
```

## 在執行單一命令 **cluster-id** 時設定

### Example

使用 `cluster-id` 參數來設定要[從](#)中取得的叢集 (ID 為 `cluster-1234567`)。

#### Linux

```
$ cloudhsm-cli cluster hsm-info --cluster-id <cluster-1234567>
```

#### Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" cluster hsm-info
--cluster-id <cluster-1234567>
```

## CloudHSM CLI 命令的參考資料

CloudHSM CLI 可協助管理員管理其 AWS CloudHSM 叢集中的使用者。CloudHSM CLI 可以在兩種模式下執行：互動式模式和單一命令模式。如需快速入門，請參閱 [開始使用 AWS CloudHSM 命令列界面 \(CLI\)](#)。

若要執行大多數 CloudHSM CLI 命令，您必須啟動 CloudHSM CLI 並登入 HSM。如果您新增或刪除 HSM，請更新 CloudHSM CLI 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

下列各主題說明 CloudHSM CLI 中的命令。

| Command                  | 描述                                        | 使用者類型                                    |
|--------------------------|-------------------------------------------|------------------------------------------|
| <a href="#">activate</a> | 啟動 CloudHSM 叢集並確認叢集是新的叢集。完成此操作後，方可執行其他操作。 | 未激活的管理員                                  |
| <a href="#">hsm-info</a> | 列出叢集中的 HSMs。                              | 所有 <a href="#">1</a> ，包括未經身分驗證的使用者。無需登入。 |
| <a href="#">ECDSA</a>    | 使用 EC 私有金鑰和 ECDSA 簽署機制產生簽章。               | 加密使用者 (CU)                               |

| Command                      | 描述                                                                                                      | 使用者類型 |
|------------------------------|---------------------------------------------------------------------------------------------------------|-------|
| <a href="#">rsa-pkcs</a>     | 使用 RSA 私有金鑰和 RSA-PKCS 簽署機制產生簽章。                                                                         | 加密使用者 |
| <a href="#">rsa-pkcs-pss</a> | 使用 RSA 私有金鑰和 RSA-PKCS-PSS 簽署機制產生簽章。                                                                     | 加密使用者 |
| <a href="#">ecdsa</a>        | 確認檔案已由指定的公有金鑰在 HSM 中登入。驗證簽章是否使用 ECDSA 簽署機制產生。比較已簽章的檔案與來源檔案，並根據指定的 ecdsa 公有金鑰和簽署機制，判斷兩者是否在密碼編譯上相關。       | 加密使用者 |
| <a href="#">rsa-pkcs</a>     | 確認檔案已由指定的公有金鑰在 HSM 中登入。驗證簽章是否使用 RSA-PKCS 簽署機制產生。比較已簽章的檔案與來源檔案，並根據指定的 rsa 公有金鑰和簽署機制，判斷兩者是否以密碼編譯方式相關。     | 加密使用者 |
| <a href="#">rsa-pkcs-pss</a> | 確認檔案已由指定的公有金鑰在 HSM 中登入。驗證簽章是否使用 RSA-PKCS-PSS 簽署機制產生。比較已簽章的檔案與來源檔案，並根據指定的 rsa 公有金鑰和簽署機制，判斷兩者是否以密碼編譯方式相關。 | 加密使用者 |
| <a href="#">刪除金鑰</a>         | 從 AWS CloudHSM 叢集刪除金鑰。                                                                                  | 加密使用者 |
| <a href="#">產生金鑰的檔案</a>      | 在您的 AWS CloudHSM 叢集中產生金鑰檔案。                                                                             | 加密使用者 |

| Command                       | 描述                                          | 使用者類型                       |
|-------------------------------|---------------------------------------------|-----------------------------|
| <a href="#">產生非對稱 RSA 金鑰對</a> | 在您的 AWS CloudHSM 叢集中產生非對稱 RSA 金鑰對。          | 加密使用者                       |
| <a href="#">產生非對稱 EC 金鑰對</a>  | 在您的 AWS CloudHSM 叢集中產生非對稱橢圓曲線 (EC) 金鑰對。     | 加密使用者                       |
| <a href="#">產生對稱 AES 金鑰</a>   | 在 AWS CloudHSM 叢集中產生對稱 AES 金鑰。              | 加密使用者                       |
| <a href="#">產生對稱通用私密金鑰</a>    | 在 AWS CloudHSM 叢集中產生對稱的一般私密金鑰。              | 加密使用者                       |
| <a href="#">金鑰匯入 pem</a>      | 將 PEM 格式金鑰匯入 HSM。您可以使用此命令匯入在 HSM 之外產生的公有金鑰。 | 加密使用者                       |
| <a href="#">列出金鑰</a>          | 尋找 AWS CloudHSM 叢集中目前使用者的所有金鑰。              | 加密使用者                       |
| <a href="#">金鑰複寫</a>          | 將金鑰從來源叢集複寫到複製的目的地叢集。                        | 加密使用者                       |
| <a href="#">設定金鑰屬性</a>        | 設定 AWS CloudHSM 叢集中金鑰的屬性。                   | 加密使用者可以執行此命令，管理員可以設定受信任的屬性。 |
| <a href="#">共用金鑰</a>          | 與 AWS CloudHSM 叢集中的其他 CUs 共用金鑰。             | 加密使用者                       |
| <a href="#">取消共用金鑰</a>        | 取消與 AWS CloudHSM 叢集中其他 CUs 共用金鑰。            | 加密使用者                       |
| <a href="#">aes-gcm</a>       | 使用 AES 包裝金鑰和 AES-GCM 取消包裝機制，將承載金鑰取消包裝到叢集中。  | 加密使用者                       |



| Command                          | 描述                                                  | 使用者類型 |
|----------------------------------|-----------------------------------------------------|-------|
| <a href="#">aes-no-pad</a>       | 使用 AES 包裝金鑰和 AES-NO-PAD 取消包裝機制，將承載金鑰取消包裝到叢集中。       | 加密使用者 |
| <a href="#">aes-pkcs5-pad</a>    | 使用 AES 包裝金鑰和 AES-PKCS5-PAD 取消包裝機制來取消包裝承載金鑰。         | 加密使用者 |
| <a href="#">aes-zero-pad</a>     | 使用 AES 包裝金鑰和 AES-ZERO-PAD 取消包裝機制，將承載金鑰取消包裝到叢集中。     | 加密使用者 |
| <a href="#">cloudhsm-aes-gcm</a> | 使用 AES 包裝金鑰和 CLOUDHSM-AES-GCM 取消包裝機制，將承載金鑰取消包裝到叢集中。 | 加密使用者 |
| <a href="#">rsa-aes</a>          | 使用 RSA 私有金鑰和 RSA-AES 取消包裝機制來取消包裝承載金鑰。               | 加密使用者 |
| <a href="#">rsa-oaep</a>         | 使用 RSA 私有金鑰和 RSA-OAEP 取消包裝機制來取消包裝承載金鑰。              | 加密使用者 |
| <a href="#">rsa-pkcs</a>         | 使用 RSA 私有金鑰和 RSA-PKCS 取消包裝機制來取消包裝承載金鑰。              | 加密使用者 |
| <a href="#">aes-gcm</a>          | 使用 HSM 上的 AES 金鑰和 AES-GCM 包裝機制來包裝承載金鑰。              | 加密使用者 |
| <a href="#">aes-no-pad</a>       | 使用 HSM 上的 AES 金鑰和 AES-NO-PAD 包裝機制來包裝承載金鑰。           | 加密使用者 |

| Command                          | 描述                                              | 使用者類型 |
|----------------------------------|-------------------------------------------------|-------|
| <a href="#">aes-pkcs5-pad</a>    | 使用 HSM 上的 AES 金鑰和 AES-PKCS5-PAD 包裝機制來包裝承載金鑰。    | 加密使用者 |
| <a href="#">aes-zero-pad</a>     | 使用 HSM 上的 AES 金鑰和 AES-ZERO-PAD 包裝機制來包裝承載金鑰。     | 加密使用者 |
| <a href="#">cloudhsm-aes-gcm</a> | 使用 HSM 上的 AES 金鑰和 CLOUDHSM-AES-GCM 包裝機制來包裝承載金鑰。 | CUs   |
| <a href="#">rsa-aes</a>          | 使用 HSM 上的 RSA 公有金鑰和 RSA-AES 包裝機制來包裝承載金鑰。        | 加密使用者 |
| <a href="#">rsa-oaep</a>         | 使用 HSM 上的 RSA 公有金鑰和 RSA-OAEP 包裝機制來包裝承載金鑰。       | 加密使用者 |

| Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 描述                                               | 使用者類型        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|--------------|
| <p>在 CloudHSM CLI 中使用 <code>key wrap rsa-pkcs</code> 命令，在硬體安全模組 (HSM) 和包裝機制上使用 RSA 公有金鑰 RSA-PKCS 來包裝承載金鑰。承載金鑰的 <code>extractable</code> 屬性必須設定為 <code>true</code>。</p> <p>只有建立金鑰的加密使用者 (CU) 金鑰擁有者才能包裝金鑰。共用金鑰的使用者可以在密碼編譯操作中使用金鑰。</p> <p>若要使用 <code>key wrap rsa-pkcs</code> 命令，您必須先在 AWS CloudHSM 叢集中擁有 RSA 金鑰。您可以使用 CloudHSM CLI 中的 <code>generate-asymmetric-pair</code> 類別命令和設定為 <code>wrap</code> 屬性來產生 RSA 金鑰對 <code>true</code>。</p> <p>使用者類型</p> <p>下列類型的使用者可以執行此命令。</p> <ul style="list-style-type: none"><li>加密使用者 (CU)</li></ul> <p>要求</p> <ul style="list-style-type: none"><li>若要執行此命令，必須以 CU 的身分登入。</li></ul> <p>語法</p> <div><pre>aws-cloudhsm &gt; help key wrap rsa-pkcs</pre><pre>Usage: key wrap rsa-pkcs</pre></div> | <p>使用 HSM 上的 RSA 公有金鑰和 RSA-PKCS 包裝機制來包裝承載金鑰。</p> | <p>加密使用者</p> |

wrap rsa-pkcs

Usage: key wrap rsa-pkcs

| Command                          | 描述                                              | 使用者類型                                    |
|----------------------------------|-------------------------------------------------|------------------------------------------|
| <a href="#">登入</a>               | 登入您的 AWS CloudHSM 叢集。                           | 管理員、加密使用者 (CU) 和設備使用者 (AU)               |
| <a href="#">登出</a>               | 登出您的 AWS CloudHSM 叢集。                           | 管理員、加密使用者和設備使用者 (AU)                     |
| <a href="#">刪除規定人數字符簽署</a>       | 刪除規定人數授權服務的一個或多個權杖。                             | 管理員                                      |
| <a href="#">產生規定人數字符簽署</a>       | 產生規定人數授權服務的權杖。                                  | 管理員                                      |
| <a href="#">列出規定人數字符簽署</a>       | 列出 CloudHSM 叢集中所有權杖簽署的規定人數權杖。                   | 所有 <a href="#">1</a> ，包括未經身分驗證的使用者。無需登入。 |
| <a href="#">規定人數字符簽署 列出規定人數值</a> | 列出 CloudHSM 叢集中規定人數值集。                          | 所有 <a href="#">1</a> ，包括未經身分驗證的使用者。無需登入。 |
| <a href="#">規定人數字符簽署 設定規定人數值</a> | 為規定人數授權服務設定新的規定人數值。                             | 管理員                                      |
| <a href="#">變更使用者 MFA</a>        | 變更使用者的多重要素驗證 (MFA) 策略。                          | 管理員、加密使用者                                |
| <a href="#">變更使用者密碼</a>          | 變更 HSM 上使用者的密碼。任何使用者都可以變更自己的密碼。加密使用者可以變更任何人的密碼。 | 管理員、加密使用者                                |
| <a href="#">建立使用者</a>            | 在 AWS CloudHSM 叢集中建立使用者。                        | 管理員                                      |
| <a href="#">刪除使用者</a>            | 刪除 AWS CloudHSM 叢集中的使用者。                        | 管理員                                      |
| <a href="#">使用者清單</a>            | 列出 AWS CloudHSM 叢集中的使用者。                        | 所有 <a href="#">1</a> ，包括未經身分驗證的使用者。無需登入。 |

| Command                          | 描述                     | 使用者類型 |
|----------------------------------|------------------------|-------|
| <a href="#">變更規定人數使用者 註冊字符簽署</a> | 為使用者註冊規定人數字符簽署的規定人數策略。 | 管理員   |

## 註釋

- [1] 所有使用者都包含所有列出的角色和未登入的使用者。

## CloudHSM CLI 中的叢集類別

在 CloudHSM CLI 中，cluster 是一組命令的父類別，當與父類別結合時，會建立叢集特有的命令。目前，叢集類別包含下列命令：

### 主題

- [使用 CloudHSM CLI 啟用叢集](#)
- [使用 HSMsCLI 列出 HSM CloudHSM](#)
- [CloudHSM CLI 中的叢集 mtls 類別](#)

## 使用 CloudHSM CLI 啟用叢集

在 CloudHSM CLI 中使用 cluster activate 命令來[啟用新的叢集](#) AWS CloudHSM。必須先執行此命令，叢集才可以用於執行密碼編譯操作。

### 使用者類型

下列類型的使用者可以執行此命令。

- 未激活的管理員

### 語法

此命令沒有任何參數。

```
aws-cloudhsm > help cluster activate
Activate a cluster
```

This command will set the initial Admin password. This process will cause your CloudHSM cluster to move into the ACTIVE state.

**USAGE:**

```
cloudhsm-cli cluster activate [OPTIONS] [--password <PASSWORD>]
```

**Options:**

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--password <PASSWORD>
```

Optional: Plaintext activation password If you do not include this argument you will be prompted for it

```
-h, --help
```

Print help (see a summary with '-h')

## 範例

此命令會為您的管理員使用者設定初始密碼來啟動叢集。

```
aws-cloudhsm > cluster activate
Enter password:
Confirm password:
{
 "error_code": 0,
 "data": "Cluster activation successful"
}
```

## 相關主題

- [建立使用者](#)
- [刪除使用者](#)
- [變更使用者密碼](#)

## 使用 HSMsCLI 列出 HSM CloudHSM

使用 CloudHSM CLI 中的 `cluster hsm-info` 命令來列出 AWS CloudHSM 叢集中的硬體安全模組 (HSMs)。您無須登入 CloudHSM CLI 即可執行此命令。

### Note

如果您新增或刪除 HSMs，請更新 AWS CloudHSM 用戶端和命令列工具使用的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列類型的使用者可以執行此命令。

- 所有使用者。您無須登入即可執行此命令。

## 語法

```
aws-cloudhsm > help cluster hsm-info
List info about each HSM in the cluster

Usage: cloudhsm-cli cluster hsm-info [OPTIONS]

Options:
 --cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in the
 config file to run the operation against. If not provided, will fall back to the value
 provided when interactive mode was started, or error
 -h, --help Print help
```

## 範例

此命令會列出 AWS CloudHSM 叢集中存在 HSMs。

```
aws-cloudhsm > cluster hsm-info
{
 "error_code": 0,
 "data": {
 "hsm": [
 {
```

```

 "vendor": "Marvell Semiconductors, Inc.",
 "model": "NITROX-III CNN35XX-NFBE",
 "serial-number": "5.3G1941-ICM000590",
 "hardware-version-major": "5",
 "hardware-version-minor": "3",
 "firmware-version-major": "2",
 "firmware-version-minor": "6",
 "firmware-build-number": "16",
 "firmware-id": "CNN35XX-NFBE-FW-2.06-16"
 "fips-state": "2 [FIPS mode with single factor authentication]"
 },
 {
 "vendor": "Marvell Semiconductors, Inc.",
 "model": "NITROX-III CNN35XX-NFBE",
 "serial-number": "5.3G1941-ICM000625",
 "hardware-version-major": "5",
 "hardware-version-minor": "3",
 "firmware-version-major": "2",
 "firmware-version-minor": "6",
 "firmware-build-number": "16",
 "firmware-id": "CNN35XX-NFBE-FW-2.06-16"
 "fips-state": "2 [FIPS mode with single factor authentication]"
 },
 {
 "vendor": "Marvell Semiconductors, Inc.",
 "model": "NITROX-III CNN35XX-NFBE",
 "serial-number": "5.3G1941-ICM000663",
 "hardware-version-major": "5",
 "hardware-version-minor": "3",
 "firmware-version-major": "2",
 "firmware-version-minor": "6",
 "firmware-build-number": "16",
 "firmware-id": "CNN35XX-NFBE-FW-2.06-16"
 "fips-state": "2 [FIPS mode with single factor authentication]"
 }
]
}
}

```

輸出具有下列屬性：

- 廠商：HSM 的廠商名稱。
- 型號：HSM 的型號。



- 序號：HSM 的序號。其可能會因更換而改變。
- Hardware-version-major：主要硬體版本。
- Hardware-version-minor：次要硬體版本。
- Firmware-version-major：主要韌體版本。
- Firmware-version-minor：次要韌體版本。
- Firmware-build-number：韌體建置編號。
- Firmware-id：韌體 ID，其中包括主要和次要版本以及建置編號。
- FIPS-state：叢集及其中的 HSMs 的 FIPS 模式。如果處於 FIPS 模式，則輸出為「2【FIPS 模式，使用單一因素身分驗證】」。如果處於非 FIPS 模式，則輸出為「0【具有單一因素身分驗證的非 FIPS 模式】」。

## 相關主題

- [使用 CloudHSM CLI 啟用叢集](#)

## CloudHSM CLI 中的叢集 mtls 類別

在 CloudHSM CLI 中，cluster mtls 是一組命令的父類別，當與父類別結合時，會建立叢集特有 AWS CloudHSM 的命令。目前，此類別由以下命令組成：

## 主題

- [使用 CloudHSM CLI 取消註冊信任錨點](#)
- [使用 CloudHSM CLI 取得 mTLS 強制執行層級](#)
- [使用 CloudHSM CLI 列出信任錨點](#)
- [向 CloudHSM CLI 註冊信任錨點](#)
- [使用 CloudHSM CLI 設定 mTLS 強制執行層級](#)

## 使用 CloudHSM CLI 取消註冊信任錨點

使用 CloudHSM CLI 中的 cluster mtls deregister-trust-anchor 命令，取消註冊用戶端與 之間相互 TLS 的信任錨點 AWS CloudHSM。

## 使用者類型

下列使用者可以執行此命令。

- 管理員

## 要求

- 若要執行此命令，您必須以管理員使用者身分登入。

## 語法

```
aws-cloudhsm > help cluster mtls deregister-trust-anchor
```

Deregister a trust anchor for mtls

Usage: cluster mtls deregister-trust-anchor [OPTIONS] --certificate-reference [**<CERTIFICATE\_REFERENCE>**...]

Options:

    --certificate-reference **<CERTIFICATE\_REFERENCE>** A hexadecimal or decimal certificate reference

    --cluster-id **<CLUSTER\_ID>** Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

    --approval **<APPROVAL>** Filepath of signed quorum token file to approve operation

    -h, --help Print help

## 範例

### Example

在下列範例中，此命令會從 HSM 移除信任錨點。

```
aws-cloudhsm > cluster mtls deregister-trust-anchor --certificate-reference 0x01
```

```
{
 "error_code": 0,
 "data": {
 "message": "Trust anchor with reference 0x01 deregistered successfully"
 }
}
```

然後，您可以執行 `list-trust-anchors` 命令，確認信任錨點已從 取消註冊 AWS CloudHSM：

```
aws-cloudhsm > cluster mtls list-trust-anchors

{
 "error_code": 0,
 "data": {
 "trust_anchors": []
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <CERTIFICATE\_REFERENCE>

十六進位或十進位憑證參考。

必要：是

#### Warning

取消註冊叢集中的信任錨點後，使用該信任錨點簽署的用戶端憑證的所有現有 mTLS 連線都會遭到捨棄。

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在規定人數叢集服務規定人數值大於 1 時才需要。

## 相關主題

- [叢集 mtls reregister-trust-anchor](#)
- [叢集 mtls list-trust-anchors](#)

- [設定 mTLS \(建議\)](#)

使用 CloudHSM CLI 取得 mTLS 強制執行層級

在 CloudHSM CLI 中使用 `cluster mtls get-enforcement` 命令，以取得用戶端與 之間相互 TLS 用量的強制執行層級 AWS CloudHSM。

使用者類型

下列使用者可以執行此命令。

- 管理員
- 加密使用者 (CU)

要求

- 若要執行此命令，您必須以管理員使用者或加密使用者 (CUs 身分登入。

語法

```
aws-cloudhsm > help cluster mtls get-enforcement
```

```
Get the status of mtls enforcement in the cluster
```

```
Usage: cluster mtls get-enforcement [OPTIONS]
```

```
Options:
```

```
 --cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in the
config file to run the operation against. If not provided, will fall back to the value
provided when interactive mode was started, or error
```

```
 -h, --help Print help
```

範例

Example

在下列範例中，此命令會列出 的 mTLS 強制執行層級 AWS CloudHSM。

```
aws-cloudhsm > cluster mtls get-enforcement
```

```
{
 "error_code": 0,
 "data": {
 "mtls-enforcement-level": "none"
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

## 相關主題

- [叢集 mtls 設定強制執行](#)
- [設定 mTLS \( 建議 \)](#)

## 使用 CloudHSM CLI 列出信任錨點

使用 CloudHSM CLI 中的 `cluster mtls list-trust-anchors` 命令，列出可用於用戶端與 之間相互 TLS 的所有信任錨點 AWS CloudHSM。

## 使用者類型

下列使用者可以執行此命令。

- 所有使用者。您無須登入即可執行此命令。

## 語法

```
aws-cloudhsm > help cluster mtls list-trust-anchors

List all trust anchors for mtls

Usage: cluster mtls list-trust-anchors [OPTIONS]
```

**Options:**

`--cluster-id <CLUSTER_ID>` Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

`-h, --help` Print help

**範例****Example**

在下列範例中，此命令會從 列出所有已註冊的信任錨點 AWS CloudHSM。

```
aws-cloudhsm > cluster mtls list-trust-anchors

{
 "error_code": 0,
 "data": {
 "trust_anchors": [
 {
 "certificate-reference": "0x01",
 "certificate": "<PEM Encoded Certificate 1>",
 "cluster-coverage": "full"
 },
 {
 "certificate-reference": "0x02",
 "certificate": "<PEM Encoded Certificate 2>",
 "cluster-coverage": "full"
 }
]
 }
}
```

**引數****<CLUSTER\_ID>**

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

## 相關主題

- [叢集 mtls reregister-trust-anchor](#)
- [叢集 mtls deregister-trust-anchor](#)
- [設定 mTLS \( 建議 \)](#)

## 向 CloudHSM CLI 註冊信任錨點

使用 CloudHSM CLI 中的 `cluster mtls register-trust-anchor` 命令，為用戶端與 之間的相互 TLS 註冊信任錨點 AWS CloudHSM。

## 使用者類型

下列使用者可以執行此命令。

- 管理員

## 要求

AWS CloudHSM 接受具有下列金鑰類型的信任錨點：

| 金鑰類型 | 描述                                                          |
|------|-------------------------------------------------------------|
| EC   | secp256r1 (P-256)、secp384r1 (P-384) 和 secp521r1 (P-521) 曲線。 |
| RSA  | 2048 位元、3072 位元和 4096 位元 RSA 金鑰。                            |

## 語法

```
aws-cloudhsm > help cluster mtls register-trust-anchor

Register a trust anchor for mtls

Usage: cluster mtls register-trust-anchor [OPTIONS] --path [<PATH>...]

Options:
```

```

--cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in the
config file to run the operation against. If not provided, will fall back to the value
provided when interactive mode was started, or error
--path <PATH> Filepath of the trust anchor to register
--approval <APPROVAL> Filepath of signed quorum token file to approve operation
-h, --help Print help

```

## 範例

### Example

在下列範例中，此命令會將信任錨點註冊到 HSM。可註冊的信任錨點數量上限為兩 (2) 個。

```
aws-cloudhsm > cluster mtls register-trust-anchor --path /home/rootCA
```

```

{
 "error_code": 0,
 "data": {
 "trust_anchor": {
 "certificate-reference": "0x01",
 "certificate": "<PEM Encoded Certificate>",
 "cluster-coverage": "full"
 }
 }
}

```

然後，您可以執行 list-trust-anchors 命令，確認信任錨點已註冊到 AWS CloudHSM：

```
aws-cloudhsm > cluster mtls list-trust-anchors
```

```

{
 "error_code": 0,
 "data": {
 "trust_anchors": [
 {
 "certificate-reference": "0x01",
 "certificate": "<PEM Encoded Certificate>",
 "cluster-coverage": "full"
 }
]
 }
}

```



```
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <PATH>

要註冊之信任錨點的 Filepath。

必要：是

#### Note

AWS CloudHSM 支援將中繼憑證註冊為信任錨點。在這種情況下，整個 PEM 編碼的憑證鏈檔案需要註冊到 HSM，並以階層順序排列憑證。  
AWS CloudHSM 支援 6980 位元組的憑證鏈。

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在規定人數叢集服務規定人數值大於 1 時才需要。

## 相關主題

- [叢集 mtls deregister-trust-anchor](#)
- [叢集 mtls list-trust-anchors](#)
- [設定 mTLS \(建議\)](#)

## 使用 CloudHSM CLI 設定 mTLS 強制執行層級

在 CloudHSM CLI 中使用 `cluster mtls set-enforcement` 命令，設定用戶端與 之間相互 TLS 用量的強制執行層級 AWS CloudHSM。

## 使用者類型

下列使用者可以執行此命令。

- 使用者名稱為 admin 的管理員

## 要求

若要執行此命令：

- 至少有一個信任錨點已成功註冊到 AWS CloudHSM。
- 使用正確的私有金鑰和用戶端憑證來設定 CloudHSM CLI，並在相互 TLS 連線下啟動 CloudHSM CLI。
- 您必須以使用者名稱為 "admin" 的預設管理員身分登入。任何其他管理員使用者將無法執行此命令。

## 語法

```
aws-cloudhsm > help cluster mtls set-enforcement
```

Set mtls enforcement policy in the cluster

Usage: cluster mtls set-enforcement [OPTIONS] --level [**<LEVEL>**...]

Options:

    --cluster-id **<CLUSTER\_ID>** Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

    --level **<LEVEL>** Level to be set for mtls in the cluster [possible values: none, cluster]

    --approval **<APPROVAL>** Filepath of signed quorum token file to approve operation

    -h, --help Print help

## 範例

### Example

在下列範例中，此命令會將 AWS CloudHSM 的 mtls 強制執行層級設定為叢集。set-enforcement 命令只能在相互 TLS 連線中執行，並以使用者名稱為 admin 的管理員使用者身分登入，請參閱[設定 mTLS 強制執行 AWS CloudHSM](#)。

```
aws-cloudhsm > cluster mtls set-enforcement --level cluster

{
 "error_code": 0,
 "data": {
 "message": "Mtls enforcement level set to Cluster successfully"
 }
}
```

然後，您可以執行 get-enforcement 命令，確認強制執行層級已設定為叢集：

```
aws-cloudhsm > cluster mtls get-enforcement

{
 "error_code": 0,
 "data": {
 "mtls-enforcement-level": "cluster"
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <LEVEL>

叢集中 mtl 要設定的關卡。

有效值

- 叢集：在叢集中強制執行用戶端和之間相互 TLS 的使用 AWS CloudHSM。
- 無：請勿在用戶端和叢集 AWS CloudHSM 中強制使用相互 TLS。

必要：是

**⚠ Warning**

在叢集中強制執行 mTLS 用量之後，所有現有的非 mTLS 連線都會遭到捨棄，而且您只能使用 mTLS 憑證連線到叢集。

**<APPROVAL>**

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在規定人數叢集服務規定人數值大於 1 時才需要。

**相關主題**

- [叢集 mtls get-enforcement](#)
- [設定 mTLS \(建議\)](#)

**CloudHSM CLI 中的加密類別**

在 CloudHSM CLI 中，crypto 是一組命令的父類別，當與父類別結合時，會建立密碼編譯操作特有的命令。目前，此類別由以下命令組成：

- [sign](#)
  - [ECDSA](#)
  - [rsa-pkcs](#)
  - [rsa-pkcs-pss](#)
- [驗證](#)
  - [ecdsa](#)
  - [rsa-pkcs](#)
  - [rsa-pkcs-pss](#)

**CloudHSM CLI 中的加密簽署類別**

在 CloudHSM CLI 中，crypto sign 是一組命令的父類別，當與父類別結合時，會在叢集 AWS CloudHSM 中使用所選的私有金鑰來產生簽章。crypto sign 具有下列子命令：

- [在 CloudHSM CLI 中使用 ECDSA 機制產生簽章](#)

- [在 CloudHSM CLI 中使用 RSA-PKCS 機制產生簽章](#)
- [在 CloudHSM CLI 中使用 RSA-PKCS-PSS 機制產生簽章](#)

若要使用 `crypto sign`，您必須在 HSM 中擁有私有金鑰。您可以使用下列命令產生私有金鑰：

- [產生非對稱 EC 金鑰對](#)
- [產生非對稱 RSA 金鑰對](#)

在 CloudHSM CLI 中使用 ECDSA 機制產生簽章

在 CloudHSM CLI 中使用 `crypto sign ecdsa` 命令，使用 EC 私有金鑰和 ECDSA 簽署機制產生簽章。

若要使用 `crypto sign ecdsa` 命令，您必須先在 AWS CloudHSM 叢集中擁有 EC 私有金鑰。您可以使用 `sign` 屬性設定為的 [使用 CloudHSM CLI 產生非對稱 EC 金鑰對](#) 命令來產生 EC 私有金鑰 `true`。

#### Note

可以使用 [CloudHSM CLI 中的加密驗證類別](#) 子命令 AWS CloudHSM 在 中驗證簽章。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help crypto sign ecdsa
```

Sign with the ECDSA mechanism

```
Usage: crypto sign ecdsa --key-filter [<KEY_FILTER>>...] --hash-
function <HASH_FUNCTION> <--data-path <DATA_PATH>|--data <DATA>>
```

## Options:

**--cluster-id** *<CLUSTER\_ID>*

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

**--key-filter** [*<KEY\_FILTER>*...]

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key

**--hash-function** *<HASH\_FUNCTION>*

[possible values: sha1, sha224, sha256, sha384, sha512]

**--data-path** *<DATA\_PATH>*

The path to the file containing the data to be signed

**--data** *<DATA>*

Base64 Encoded data to be signed

**--approval** *<APPROVAL>*

Filepath of signed quorum token file to approve operation

**--data-type** *<DATA\_TYPE>*

The type of data passed in, either raw or digest [possible values: raw, digest]

**-h, --help**

Print help

## 範例

這些範例示範如何使用 ECDSA 簽署機制和SHA256雜湊函數crypto sign ecdsa來產生簽章。此命令在 HSM 中使用私有金鑰。

Example 範例：產生基礎 64 編碼資料的簽章

```
aws-cloudhsm > crypto sign ecdsa --key-filter attr.label=ec-private --hash-function
sha256 --data YWJjMTIz
{
 "error_code": 0,
 "data": {
 "key-reference": "0x0000000000007808dd",
 "signature": "4zki+Fzjhp7Z/KqoQvh4ueMAxQQVp7FQguZ2w0S3Q5bzk
+Hc5irV5iTkuxQbropPttVFZ8V6FgR2fz+sPegwCw=="
 }
}
```

## Example 範例：產生資料檔案的簽章

```
aws-cloudhsm > crypto sign ecdsa --key-filter attr.label=ec-private --hash-function
sha256 --data-path data.txt
{
 "error_code": 0,
 "data": {
 "key-reference": "0x0000000000007808dd",
 "signature": "4zki+FzjhP7Z/KqoQvh4ueMAxQQVp7FQguZ2w0S3Q5bzk
+Hc5irV5iTkuxQbropPttVFZ8V6FgR2fz+sPegwCw=="
 }
}
```

### 引數

#### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

#### <DATA>

要簽署的 Base64 編碼資料。

必要：是（除非透過資料路徑提供）

#### <DATA\_PATH>

指定要簽署的資料位置。

必要：是（除非透過資料路徑提供）

#### <HASH\_FUNCTION>

指定雜湊函數。

有效值：

- sha1
- sha224
- sha256
- sha384

- sha512

必要：是

### <KEY\_FILTER>

索引鍵參考（例如，key-reference=0xabc）或以 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 格式分隔的索引鍵屬性清單，以選取相符的索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 CloudHSM CLI 的金鑰屬性。

必要：是

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在私有金鑰的金鑰用量服務規定人數值大於 1 時才需要。

### <DATA\_TYPE>

指定是否應將資料參數的值雜湊為簽署演算法的一部分。raw 用於未雜湊的資料；digest 用於已雜湊的摘要。

有效值：

- raw
- 摘要

### 相關主題

- [CloudHSM CLI 中的加密簽署類別](#)
- [CloudHSM CLI 中的加密驗證類別](#)

在 CloudHSM CLI 中使用 RSA-PKCS 機制產生簽章

在 CloudHSM CLI 中使用 crypto sign rsa-pkcs 命令，使用 RSA 私有金鑰和 RSA-PKCS 簽署機制產生簽章。

若要使用 crypto sign rsa-pkcs 命令，您必須先在 AWS CloudHSM 叢集中擁有 RSA 私有金鑰。您可以使用 sign 屬性設定為的 [使用 CloudHSM CLI 產生非對稱 RSA 金鑰對](#) 命令來產生 RSA 私有金鑰 true。



 Note

可以使用 [CloudHSM CLI 中的加密驗證類別](#) 子命令 AWS CloudHSM 在 中驗證簽章。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help crypto sign rsa-pkcs
```

Sign with the RSA-PKCS mechanism

Usage: crypto sign rsa-pkcs --key-filter [**<KEY\_FILTER>**...] --hash-function **<HASH\_FUNCTION>** <--data-path **<DATA\_PATH>**|--data **<DATA>**>

Options:

--cluster-id **<CLUSTER\_ID>**

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

--key-filter [**<KEY\_FILTER>**...]

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key

--hash-function **<HASH\_FUNCTION>**

[possible values: sha1, sha224, sha256, sha384, sha512]

--data-path **<DATA\_PATH>**

The path to the file containing the data to be signed

--data **<DATA>**

Base64 Encoded data to be signed

--approval **<APPROVAL>**

Filepath of signed quorum token file to approve operation

--data-type **<DATA\_TYPE>**

```

 The type of data passed in, either raw or digest [possible values: raw,
 digest]
 -h, --help
 Print help

```

## 範例

這些範例示範如何使用 RSA-PKCS 簽署機制和 SHA256 雜湊函數 `crypto sign rsa-pkcs` 產生簽章。此命令在 HSM 中使用私有金鑰。

### Example 範例：產生基礎 64 編碼資料的簽章

```

aws-cloudhsm > crypto sign rsa-pkcs --key-filter attr.label=rsa-private --hash-function sha256 --data YWJjMTIz
{
 "error_code": 0,
 "data": {
 "key-reference": "0x000000000007008db",
 "signature": "XJ7mRyHnDRYrDWTQuuNb
+5mhoXx7VTsPMjg0QW4iMN7E42eNHj2Q0oovMmBdHUEH0F4HYG8FBj0BhvGuM8J/
z6y41GbowVpUT6WzjnIQs79K9i7i6oR1TYjLnIS3r/zkimuXcS8/ZxyDzru+G09BUT9FFU/
of9cvu40yn6a5+IXuCbKNQs19uASuFARUTZ0a0Ny1CB1MulxUpqGTmI91J6evlP7k/2khwDmJ5E8FEar5/
Cvbn9t21p3Uj561ngTXrYbIZ2KHpef9jQh/cEIVFLG61sexJjQi8EdTxeDA
+I3IT00qrvvESvA9+Sj7kdG2ceIicFS8/8LwyxiIC31UHQ=="
 }
}

```

### Example 範例：產生資料檔案的簽章

```

aws-cloudhsm > crypto sign rsa-pkcs --key-filter attr.label=rsa-private --hash-function sha256 --data-path data.txt
{
 "error_code": 0,
 "data": {
 "key-reference": "0x000000000007008db",
 "signature": "XJ7mRyHnDRYrDWTQuuNb
+5mhoXx7VTsPMjg0QW4iMN7E42eNHj2Q0oovMmBdHUEH0F4HYG8FBj0BhvGuM8J/
z6y41GbowVpUT6WzjnIQs79K9i7i6oR1TYjLnIS3r/zkimuXcS8/ZxyDzru+G09BUT9FFU/
of9cvu40yn6a5+IXuCbKNQs19uASuFARUTZ0a0Ny1CB1MulxUpqGTmI91J6evlP7k/2khwDmJ5E8FEar5/
Cvbn9t21p3Uj561ngTXrYbIZ2KHpef9jQh/cEIVFLG61sexJjQi8EdTxeDA
+I3IT00qrvvESvA9+Sj7kdG2ceIicFS8/8LwyxiIC31UHQ=="
 }
}

```

```
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <DATA>

要簽署的 Base64 編碼資料。

必要：是（除非透過資料路徑提供）

### <DATA\_PATH>

指定要簽署的資料位置。

必要：是（除非透過資料提供）

### <HASH\_FUNCTION>

指定雜湊函數。

有效值：

- sha1
- sha224
- sha256
- sha384
- sha512

必要：是

### <KEY\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 以選取相符的索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 CloudHSM CLI 的金鑰屬性。

必要：是

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在私有金鑰的金鑰用量服務規定人數值大於 1 時才需要。

### <DATA\_TYPE>

指定是否應將資料參數的值雜湊為簽署演算法的一部分。raw 用於未雜湊的資料；digest 用於已雜湊的摘要。

對於 RSA-PKCS，資料必須以 DER 編碼格式傳遞，[如 RFC 8017 第 9.2 節](#)所述

有效值：

- raw
- 摘要

### 相關主題

- [CloudHSM CLI 中的加密簽署類別](#)
- [CloudHSM CLI 中的加密驗證類別](#)

在 CloudHSM CLI 中使用 RSA-PKCS-PSS 機制產生簽章

在 CloudHSM CLI 中使用 `crypto sign rsa-pkcs-pss` 命令，使用 RSA 私有金鑰和 RSA-PKCS-PSS 簽署機制產生簽章。

若要使用 `crypto sign rsa-pkcs-pss` 命令，您必須先在 AWS CloudHSM 叢集中擁有 RSA 私有金鑰。您可以使用 `sign` 屬性設定為的 [使用 CloudHSM CLI 產生非對稱 RSA 金鑰對](#) 命令來產生 RSA 私有金鑰 `true`。

#### Note

可以使用 [CloudHSM CLI 中的加密驗證類別](#) 子命令 AWS CloudHSM 在 中驗證簽章。

### 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help crypto sign rsa-pkcs-pss
```

Sign with the RSA-PKCS-PSS mechanism

```
Usage: crypto sign rsa-pkcs-pss [OPTIONS] --key-filter [<KEY_FILTER>...] --
hash-function <HASH_FUNCTION> --mgf <MGF> --salt-length <SALT_LENGTH> <--data-
path <DATA_PATH>|--data <DATA>>
```

Options:

```
--cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in the
config file to run the operation against. If not provided, will fall back to the value
provided when interactive mode was started, or error
--key-filter [<KEY_FILTER>...] Key reference (e.g. key-
reference=0xabc) or space separated list of key attributes in the form of
attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a matching key
--hash-function <HASH_FUNCTION> [possible values: sha1, sha224, sha256, sha384,
sha512]
--data-path <DATA_PATH> The path to the file containing the data to be
signed
--data <DATA> Base64 Encoded data to be signed
--mgf <MGF> The mask generation function [possible values:
mgf1-sha1, mgf1-sha224, mgf1-sha256, mgf1-sha384, mgf1-sha512]
--salt-length <SALT_LENGTH> The salt length
--approval <APPROVAL> Filepath of signed quorum token file to approve
operation
--data-type <DATA_TYPE> The type of data passed in, either raw or digest
[possible values: raw, digest]
-h, --help Print help
```

## 範例

這些範例示範如何使用RSA-PKCS-PSS簽署機制和SHA256雜湊函數crypto sign rsa-pkcs-pss來產生簽章。此命令在 HSM 中使用私有金鑰。

## Example 範例：產生基礎 64 編碼資料的簽章

```
aws-cloudhsm > crypto sign rsa-pkcs-pss --key-filter attr.label=rsa-private --hash-
function sha256 --data YWJjMTIz --salt-length 10 --mgf mgf1-sha256
{
 "error_code": 0,
 "data": {
 "key-reference": "0x000000000007008db",
 "signature": "H/z1rYVMzNAa31K4amE5MTiwGxDdCTgQXCJXRBKV0Vm7ZuyI0fGE4sT/BUN
+977mQEV2TqtWpTsiF2IpwGM1VfSBRT7h/g4o6YERm1tTQL17q+AJ7uGGK37zCsWQrAo7Vy8NzPSHxekePo/
ZegrB1aHWN1fE8H3IPUKqLuMDI9o1Jq6kM986ExS7Yme0Ic1cZkyykTWqHLQVL2C3+A2bHJZBqRcM5XoIpk8HkPypjpN
+m4FNUds30GAemo0M16asSrEJSthaZWV530BsD0qzA8Rt8JdhXS+GZp3vNLdL10TBELDPweXVgAu4dBX0F0vpw/
gg6sNvuaDK4Y0Bv2fqKg=="
 }
}
```

## Example 範例：產生資料檔案的簽章

```
aws-cloudhsm > crypto sign rsa-pkcs-pss --key-filter attr.label=rsa-private --hash-
function sha256 --data-path data.txt --salt-length 10 --mgf mgf1-sha256
{
 "error_code": 0,
 "data": {
 "key-reference": "0x000000000007008db",
 "signature": "H/z1rYVMzNAa31K4amE5MTiwGxDdCTgQXCJXRBKV0Vm7ZuyI0fGE4sT/BUN
+977mQEV2TqtWpTsiF2IpwGM1VfSBRT7h/g4o6YERm1tTQL17q+AJ7uGGK37zCsWQrAo7Vy8NzPSHxekePo/
ZegrB1aHWN1fE8H3IPUKqLuMDI9o1Jq6kM986ExS7Yme0Ic1cZkyykTWqHLQVL2C3+A2bHJZBqRcM5XoIpk8HkPypjpN
+m4FNUds30GAemo0M16asSrEJSthaZWV530BsD0qzA8Rt8JdhXS+GZp3vNLdL10TBELDPweXVgAu4dBX0F0vpw/
gg6sNvuaDK4Y0Bv2fqKg=="
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <DATA>

要簽署的 Base64 編碼資料。

必要：是（除非透過資料路徑提供）

### <DATA\_PATH>

指定要簽署的資料位置。

必要：是（除非透過資料提供）

### <HASH\_FUNCTION>

指定雜湊函數。

有效值：

- sha1
- sha224
- sha256
- sha384
- sha512

必要：是

### <KEY\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 以選取相符的索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 CloudHSM CLI 的金鑰屬性。

必要：是

### <MGF>

指定遮罩產生函數。

#### Note

遮罩產生函數雜湊函數必須符合簽署機制雜湊函數。

有效值：

- mgf1-sha1
- mgf1-sha224

- mgf1-sha256
- mgf1-sha384
- mgf1-sha512

必要：是

### <SALT\_LENGTH>

指定 salt 長度。

必要：是

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在私有金鑰的金鑰用量服務規定人數值大於 1 時才需要。

### <DATA\_TYPE>

指定是否應將資料參數的值雜湊為簽署演算法的一部分。raw 用於未雜湊的資料；digest 用於已雜湊的摘要。

有效值：

- raw
- 摘要

## 相關主題

- [CloudHSM CLI 中的加密簽署類別](#)
- [CloudHSM CLI 中的加密驗證類別](#)

## 相關主題

- [CloudHSM CLI 中的加密驗證類別](#)

## CloudHSM CLI 中的加密驗證類別

在 CloudHSM CLI 中，crypto verify 是一組命令的父類別，當與父類別結合時，會確認檔案是否已由指定的金鑰簽署。crypto verify 具有下列子命令：

- [crypto 驗證 ecdsa](#)



- [加密驗證 rsa-pkcs](#)
- [加密驗證 rsa-pkcs-pss](#)

crypto verify 命令會比較已簽章的檔案與來源檔案，並根據指定的公有金鑰和簽署機制，分析它們是否與密碼編譯相關。

 Note

檔案可以使用 AWS CloudHSM [CloudHSM CLI 中的加密簽署類別](#)操作登入。

在 CloudHSM CLI 中驗證使用 ECDSA 機制簽署的簽章

在 CloudHSM CLI 中使用 crypto verify ecdsa命令來完成下列操作：

- 確認檔案已由指定的公有金鑰在 HSM 中簽署。
- 驗證簽章是否使用 ECDSA 簽署機制產生。
- 比較已簽章的檔案與來源檔案，並根據指定的 ecdsa 公有金鑰和簽署機制，判斷兩者是否在密碼編譯上相關。

若要使用 crypto verify ecdsa命令，您必須先在 AWS CloudHSM 叢集中擁有 EC 公有金鑰。您可以使用 verify 屬性設定為的 [使用 CloudHSM CLI 匯入 PEM 格式金鑰](#)命令來匯入 EC 公有金鑰true。

 Note

您可以使用[CloudHSM CLI 中的加密簽署類別](#)子命令在 CloudHSM CLI 中產生簽章。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help crypto verify ecdsa
```

Verify with the ECDSA mechanism

Usage: crypto verify ecdsa --key-filter [<KEY\_FILTER>...] --hash-function <HASH\_FUNCTION> <--data-path <DATA\_PATH>|--data <DATA>> <--signature-path <SIGNATURE\_PATH>|--signature <SIGNATURE>>

Options:

--cluster-id <CLUSTER\_ID>

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

--key-filter [<KEY\_FILTER>...]

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key

--hash-function <HASH\_FUNCTION>

[possible values: sha1, sha224, sha256, sha384, sha512]

--data-path <DATA\_PATH>

The path to the file containing the data to be verified

--data <DATA>

Base64 encoded data to be verified

--signature-path <SIGNATURE\_PATH>

The path to where the signature is located

--signature <SIGNATURE>

Base64 encoded signature to be verified

--data-type <DATA\_TYPE>

The type of data passed in, either raw or digest [possible values: raw, digest]

-h, --help

Print help

## 範例

這些範例示範如何使用 crypto verify ecdsa 驗證使用 ECDSA 簽署機制和SHA256雜湊函數產生的簽章。此命令在 HSM 中使用公有金鑰。

## Example 範例：使用 Base64 編碼資料驗證 Base64 編碼簽章

```
aws-cloudhsm > crypto verify ecdsa --hash-function sha256 --key-filter attr.label=ec-public --data YWJjMTIz --signature 4zki+FzjhP7Z/KqoQvh4ueMAxQQVp7FQguZ2w0S3Q5bzk+Hc5irV5iTkuxQbropPttVFZ8V6FgR2fz+sPegwCw==
{
 "error_code": 0,
 "data": {
 "message": "Signature verified successfully"
 }
}
```

## Example 範例：使用資料檔案驗證簽章檔案

```
aws-cloudhsm > crypto verify ecdsa --hash-function sha256 --key-filter attr.label=ec-public --data-path data.txt --signature-path signature-file
{
 "error_code": 0,
 "data": {
 "message": "Signature verified successfully"
 }
}
```

## Example 範例：證明錯誤簽署關係

此命令會使用 ECDSA /home/data簽署機制來產生位於 中的簽章，驗證位於 的資料是否由具有 標籤ecdsa-public的公有金鑰簽署/home/signature。由於指定的引數不會構成真正的簽署關係，因此 命令會傳回錯誤訊息。

```
aws-cloudhsm > crypto verify ecdsa --hash-function sha256 --key-filter attr.label=ec-public --data aW52YWxpZA== --signature +ogk7M7S3iTqFg3SndJfd91dZFr5Qo6YixJl8JwcvqqVgsVu06o+VKvTRjz0/V05kf3JJbBLr87Q+wLWcMAJfA==
{
 "error_code": 1,
 "data": "Signature verification failed"
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <DATA>

要簽署的 Base64 編碼資料。

必要：是（除非透過資料路徑提供）

### <DATA\_PATH>

指定要簽署的資料位置。

必要：是（除非透過資料路徑提供）

### <HASH\_FUNCTION>

指定雜湊函數。

有效值：

- sha1
- sha224
- sha256
- sha384
- sha512

必要：是

### <KEY\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 以選取相符的索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 CloudHSM CLI 的金鑰屬性。

必要：是

**<SIGNATURE>**

Base64 編碼簽章。

必要：是（除非透過簽章路徑提供）

**<SIGNATURE\_PATH>**

指定簽章的位置。

必要：是（除非透過簽章路徑提供）

**<DATA\_TYPE>**

指定是否應將資料參數的值雜湊為簽署演算法的一部分。raw 用於未雜湊的資料；digest 用於已雜湊的摘要。

有效值：

- raw
- 摘要

**相關主題**

- [CloudHSM CLI 中的加密簽署類別](#)
- [CloudHSM CLI 中的加密驗證類別](#)

在 CloudHSM CLI 中驗證使用 RSA-PKCS 機制簽署的簽章

在 CloudHSM CLI 中使用 `crypto verify rsa-pkcs` 命令完成下列操作：

- 確認檔案已由指定的公有金鑰在 HSM 中簽署。
- 驗證簽章是否使用 RSA-PKCS 簽署機制產生。
- 比較已簽章的檔案與來源檔案，並根據指定的 rsa 公有金鑰和簽署機制，判斷兩者是否在密碼編譯上相關。

若要使用 `crypto verify rsa-pkcs` 命令，您必須先在 AWS CloudHSM 叢集中擁有 RSA 公有金鑰。

**Note**

您可以使用 CloudHSM CLI 搭配 [CloudHSM CLI 中的加密簽署類別](#) 子命令來產生簽章。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help crypto verify rsa-pkcs
```

Verify with the RSA-PKCS mechanism

Usage: crypto verify rsa-pkcs --key-filter [*<KEY\_FILTER>*...] --hash-function *<HASH\_FUNCTION>* [--data-path *<DATA\_PATH>*|--data *<DATA>*] [--signature-path *<SIGNATURE\_PATH>*|--signature *<SIGNATURE>*]

Options:

--cluster-id *<CLUSTER\_ID>*

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

--key-filter [*<KEY\_FILTER>*...]

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key

--hash-function *<HASH\_FUNCTION>*

[possible values: sha1, sha224, sha256, sha384, sha512]

--data-path *<DATA\_PATH>*

The path to the file containing the data to be verified

--data *<DATA>*

Base64 encoded data to be verified

--signature-path *<SIGNATURE\_PATH>*

The path to where the signature is located

--signature *<SIGNATURE>*

Base64 encoded signature to be verified

--data-type *<DATA\_TYPE>*

The type of data passed in, either raw or digest [possible values: raw, digest]

-h, --help

Print help

## 範例

這些範例示範如何使用 `crypto verify rsa-pkcs` 驗證使用 RSA-PKCS 簽署機制和 SHA256 雜湊函數產生的簽章。此命令在 HSM 中使用公有金鑰。

Example 範例：使用 Base64 編碼資料驗證 Base64 編碼簽章

```
aws-cloudhsm > crypto verify rsa-pkcs --hash-function sha256 --key-filter
attr.label=rsa-public --data YWJjMTIz --signature XJ7mRyHnDRYrDWTQuuNb
+5mhoXx7VTsPMjg0QW4iMN7E42eNHj2Q0oovMmBdHUEH0F4HYG8FBj0BhvGuM8J/
z6y41GbowVpUT6WzjnIQs79K9i7i6oR1TYjLnIS3r/zkimuXcS8/ZxyDzru+G09BUT9FFU/
of9cvu40yn6a5+IXuCbKNQs19uASuFARUTZ0a0Ny1CB1MulxUpqGTmI91J6evlP7k/2khwDmJ5E8FEar5/
Cvbn9t21p3Uj561ngTXrYbIZ2KHpef9jQh/cEIvFLG61sexJjQi8EdTxeDA
+I3IT00qrvvESvA9+Sj7kdG2ceIicFS8/8LwyxiIC31UHQ==
{
 "error_code": 0,
 "data": {
 "message": "Signature verified successfully"
 }
}
```

Example 範例：使用資料檔案驗證簽章檔案

```
aws-cloudhsm > crypto verify rsa-pkcs --hash-function sha256 --key-filter
attr.label=rsa-public --data-path data.txt --signature-path signature-file
{
 "error_code": 0,
 "data": {
 "message": "Signature verified successfully"
 }
}
```

Example 範例：證明錯誤簽署關係

此命令 `rsa-public` 會使用 RSAPKCS 簽署機制來產生位於 `/home/signature` 中的簽章，驗證無效資料是否由具有 `attr.label=rsa-public` 標籤的公有金鑰簽署。由於指定的引數不會構成真正的簽署關係，因此命令會傳回錯誤訊息。

```
aws-cloudhsm > crypto verify rsa-pkcs --hash-function sha256 --key-filter
attr.label=rsa-public --data aW52YWxpZA== --signature XJ7mRyHnDRYrDWTQuuNb
```

```
+5mhoXx7VTsPMjg0QW4iMN7E42eNHj2Q0oovMmBdHUEH0F4HYG8FBj0BhvGuM8J/
z6y41GbowVpUT6WzjnIQs79K9i7i6oR1TYjLnIS3r/zkimuXcS8/ZxyDzru+G09BUT9FFU/
of9cvu40yn6a5+IXuCbKNQs19uASuFARUTZ0a0Ny1CB1MulxUpqGTmI91J6ev1P7k/2khwDmJ5E8FEar5/
Cvbn9t21p3Uj561ngTXrYbIZ2KHpef9jQh/cEivFLG61sexJjQi8EdTxeDA
+I3IT00qrvvESvA9+Sj7kdG2ceIicFS8/8LwyxiIC31UHQ==
{
 "error_code": 1,
 "data": "Signature verification failed"
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <DATA>

要簽署的 Base64 編碼資料。

必要：是（除非透過資料路徑提供）

### <DATA\_PATH>

指定要簽署的資料位置。

必要：是（除非透過資料路徑提供）

### <HASH\_FUNCTION>

指定雜湊函數。

有效值：

- sha1
- sha224
- sha256
- sha384
- sha512

必要：是



**<KEY\_FILTER>**

索引鍵參考 ( 例如 key-reference=0xabc) 或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 以選取相符的索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 CloudHSM CLI 的金鑰屬性。

必要：是

**<SIGNATURE>**

Base64 編碼簽章。

必要：是 ( 除非透過簽章路徑提供 )

**<SIGNATURE\_PATH>**

指定簽章的位置。

必要：是 ( 除非透過簽章路徑提供 )

**<DATA\_TYPE>**

指定是否應將資料參數的值雜湊為簽署演算法的一部分。raw 用於未雜湊的資料；digest 用於已雜湊的摘要。

對於 RSA-PKCS，資料必須以 [RFC 8017 第 9.2 節](#) 中指定的 DER 編碼格式傳遞

有效值：

- raw
- 摘要

**相關主題**

- [CloudHSM CLI 中的加密簽署類別](#)
- [CloudHSM CLI 中的加密驗證類別](#)

在 CloudHSM CLI 中驗證使用 RSA-PKCS-PSS 機制簽署的簽章

使用 CloudHSM CLI 中的 crypto sign rsa-pkcs-pss 命令來完成下列操作。

- 確認檔案已透過指定的公有金鑰在 HSM 中簽署。

- 驗證簽章是否使用 RSA-PKCS-PSS 簽署機制產生。
- 比較已簽章的檔案與來源檔案，並根據指定的 rsa 公有金鑰和簽署機制，判斷兩者是否與密碼編譯相關。

若要使用 `crypto verify rsa-pkcs-pss` 命令，您必須先在 AWS CloudHSM 叢集中擁有 RSA 公有金鑰。您可以使用金鑰匯入 `pem` 命令 `ADD UNWRAP LINK HERE`) 匯入 RSA 公有金鑰，並將 `verify` 屬性設定為 `true`。

#### Note

您可以使用 CloudHSM CLI 搭配 [CloudHSM CLI 中的加密簽署類別](#) 子命令來產生簽章。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help crypto verify rsa-pkcs-pss
```

Verify with the RSA-PKCS-PSS mechanism

```
Usage: crypto verify rsa-pkcs-pss --key-filter [<KEY_FILTER>...] --hash-
function <HASH_FUNCTION> --mgf <MGF> --salt-length >SALT_LENGTH< <--data-
path <DATA_PATH>|--data <DATA> <--signature-path <SIGNATURE_PATH>|--
signature <SIGNATURE>
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--key-filter [<KEY_FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key

--hash-function *<HASH\_FUNCTION>*

[possible values: sha1, sha224, sha256, sha384, sha512]

--data-path *<DATA\_PATH>*

The path to the file containing the data to be verified

--data *<DATA>*

Base64 encoded data to be verified

--signature-path *<SIGNATURE\_PATH>*

The path to where the signature is located

--signature *<SIGNATURE>*

Base64 encoded signature to be verified

--data-type *<DATA\_TYPE>*

The type of data passed in, either raw or digest [possible values: raw, digest]

--mgf *<MGF>*

The mask generation function [possible values: mgf1-sha1, mgf1-sha224, mgf1-sha256, mgf1-sha384, mgf1-sha512]

--salt-length *<SALT\_LENGTH>*

The salt length

-h, --help

Print help

## 範例

這些範例示範如何使用 `crypto verify rsa-pkcs-pss` 驗證使用 RSA-PKCS-PSS 簽署機制和 SHA256 雜湊函數產生的簽章。此命令在 HSM 中使用公有金鑰。

Example 範例：使用 Base64 編碼資料驗證 Base64 編碼簽章

```
aws-cloudhsm > crypto verify rsa-pkcs-pss --key-filter attr.label=rsa-public
--hash-function sha256 --data YWJjMTIz --salt-length 10 --mgf mgf1-sha256
--signature H/z1rYVMzNAa31K4amE5MTiwGxDdCTgQXCJXRBKV0Vm7ZuyI0fGE4sT/BUN
+977mQEV2TqtWpTsiF2IpwGM1VfSBRT7h/g4o6YERm1tTQL17q+AJ7uGGK37zCsWQrAo7Vy8NzPShxekePo/
ZegrB1aHWN1fE8H3IPUKqLuMDI9o1Jq6kM986ExS7Yme0Ic1cZkyykTWqHLQVL2C3+A2bHJZBqRcM5XoIpk8HkPypjpN
+m4FNUds30GAemo0M16asSrEJSthaZWV530BsD0qzA8Rt8JdhXS+GZp3vNLdL10TBELDPweXVgAu4dBX0F0vpw/
gg6sNvuaDK4Y0Bv2fqKg==
{
 "error_code": 0,
 "data": {
 "message": "Signature verified successfully"
 }
}
```

```
}
```

### Example 範例：使用資料檔案驗證簽章檔案

```
aws-cloudhsm > crypto verify rsa-pkcs-pss --key-filter attr.label=rsa-public --hash-
function sha256 --data-path data.txt --salt-length 10 --mgf mgf1-sha256 --signature
signature-file
{
 "error_code": 0,
 "data": {
 "message": "Signature verified successfully"
 }
}
```

### Example 範例：證明錯誤簽署關係

此命令 `rsa-public` 會使用 RSAPKCS PSS 簽署機制來產生位於 `/home/signature` 中的簽章，驗證無效資料是否由具有標籤的公有金鑰簽署。由於指定的引數不會構成真正的簽署關係，因此命令會傳回錯誤訊息。

```
aws-cloudhsm > crypto verify rsa-pkcs-pss --key-filter attr.label=rsa-public
--hash-function sha256 --data aW52YWxpZA== --salt-length 10 --mgf mgf1-sha256
--signature H/z1rYVMzNAa31K4amE5MTiwGxDdCTgQXCJXRBKV0Vm7ZuyI0fGE4sT/BUN
+977mQEV2TqtWpTsiF2IpwGM1VfSBRT7h/g4o6YERm1tTQL17q+AJ7uGGK37zCsWQrAo7Vy8NzPSHxekePo/
ZegrB1aHWN1fE8H3IPUKqLuMDI9o1Jq6kM986ExS7Yme0Ic1cZkyykTWqHLQVL2C3+A2bHJZBqRcM5XoIpk8HkPypjpN
+m4FNUds30GAemo0M16asSrEJSthaZWV530BsD0qzA8Rt8JdhXS+GZp3vNLdL10TBELDPweXVgAu4dBX0F0vpw/
gg6sNvuaDK4Y0Bv2fqKg==
{
 "error_code": 1,
 "data": "Signature verification failed"
}
```

### 引數

#### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

#### <DATA>

要簽署的 Base64 編碼資料。

必要：是（除非透過資料路徑提供）

### <DATA\_PATH>

指定要簽署的資料位置。

必要：是（除非透過資料路徑提供）

### <HASH\_FUNCTION>

指定雜湊函數。

有效值：

- sha1
- sha224
- sha256
- sha384
- sha512

必要：是

### <KEY\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 以選取相符的索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 CloudHSM CLI 的金鑰屬性。

必要：是

### <MFG>

指定遮罩產生函數。

#### Note

遮罩產生函數雜湊函數必須符合簽署機制雜湊函數。

有效值：

- mgf1-sha1
- mgf1-sha224

- mgf1-sha256
- mgf1-sha384
- mgf1-sha512

必要：是

### <SIGNATURE>

Base64 編碼簽章。

必要：是（除非透過簽章路徑提供）

### <SIGNATURE\_PATH>

指定簽章的位置。

必要：是（除非透過簽章路徑提供）

### <DATA\_TYPE>

指定是否應將資料參數的值雜湊為簽署演算法的一部分。raw 用於未雜湊的資料；digest 用於已雜湊的摘要。

有效值：

- raw
- 摘要

## 相關主題

- [CloudHSM CLI 中的加密簽署類別](#)
- [CloudHSM CLI 中的加密驗證類別](#)

## CloudHSM CLI 中的金鑰類別

在 CloudHSM CLI 中，key 是一組命令的父類別，當與父類別結合時，會建立金鑰特有的命令。目前，此類別由以下命令組成：

- [刪除](#)
- [產生的檔案](#)
- [產生非對稱金鑰對](#)

- [產生非對稱 RSA 金鑰對](#)
- [產生非對稱 EC 金鑰對](#)
- [產生對稱金鑰](#)
  - [產生對稱 AES 金鑰](#)
  - [產生對稱通用私密金鑰](#)
- [匯入 pem](#)
- [列出](#)
- [複寫](#)
- [設定屬性](#)
- [共用](#)
- [取消共用](#)
- [取消包裝](#)
- [包裝](#)

## 使用 CloudHSM CLI 刪除金鑰

使用 CloudHSM CLI 中的 `key delete` 命令，從 AWS CloudHSM 叢集刪除金鑰。您一次只能刪除一個金鑰。刪除金鑰對中的一個金鑰，對金鑰對中的另一個金鑰沒有影響。

只有建立金鑰並因此擁有金鑰的 CU 才能刪除金鑰。共用金鑰但卻未擁有金鑰的使用者可以在密碼編譯操作中使用金鑰，但不能刪除它。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key delete
```

Delete a key in the HSM cluster

Usage: key delete [OPTIONS] --filter [**<FILTER>**...]

Options:

--cluster-id **<CLUSTER\_ID>** Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

--filter [**<FILTER>**...] Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key for deletion

-h, --help Print help

## 範例

```
aws-cloudhsm > key delete --filter attr.label="ec-test-public-key"
{
 "error_code": 0,
 "data": {
 "message": "Key deleted successfully"
 }
}
```

## 引數

### **<CLUSTER\_ID>**

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### **#####**

索引鍵參考 (例如 key-reference=0xabc) 或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要刪除的相符索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)

必要：是

## 相關主題

- [使用 CloudHSM CLI 列出使用者的金鑰](#)



- [使用 CloudHSM CLI 匯出非對稱金鑰](#)
- [使用 CloudHSM CLI 取消共用金鑰](#)
- [CloudHSM CLI 的金鑰屬性](#)
- [使用 CloudHSM CLI 篩選金鑰](#)

## 使用 CloudHSM CLI 匯出非對稱金鑰

在 CloudHSM CLI 中使用 `key generate-file` 命令，從硬體安全模組 (HSM) 匯出非對稱金鑰。如果目標是私有金鑰，則會以仿造 PEM 格式匯出私有金鑰的參考。如果目標是公有金鑰，則會以 PEM 格式匯出公有金鑰位元組。

仿造 PEM 檔案不包含實際的私有金鑰材料，而是參考 HSM 中的私有金鑰，可用來從 Web 伺服器建立 SSL/TLS 卸載 AWS CloudHSM。如需詳細資訊，請參閱 [SSL/TLS 卸載](#)。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key generate-file
```

```
Generate a key file from a key in the HSM cluster. This command does not export any private key data from the HSM
```

```
Usage: key generate-file --encoding <ENCODING> --path <PATH> --filter [<FILTER>...]
```

```
Options:
```

```
--cluster-id <CLUSTER_ID>
```

```
Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error
```

```
--encoding <ENCODING>
```

```
Encoding format for the key file
```

Possible values:

- reference-pem: PEM formatted key reference (supports private keys)
- pem: PEM format (supports public keys)

**--path** *<PATH>*

Filepath where the key file will be written

**--filter** [*<FILTER>*...]

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key for file generation

**-h, --help**

Print help (see a summary with '-h')

## 範例

此範例示範如何使用 在 AWS CloudHSM 叢集中key generate-file產生金鑰檔案。

## Example

```
aws-cloudhsm > key generate-file --encoding reference-pem --path /tmp/ec-private-key.pem --filter attr.label="ec-test-private-key"
{
 "error_code": 0,
 "data": {
 "message": "Successfully generated key file"
 }
}
```

## 引數

### **<CLUSTER\_ID>**

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### **#####**

索引鍵參考 ( 例如 key-reference=0xabc) 或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要刪除的相符索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)

必要：否

### <ENCODING>

指金鑰檔案的編碼格式

必要：是

### <PATH>

指要寫入金鑰檔案的檔案路徑

必要：是

產生 KSP 金鑰參考 (Windows)

#### Note

此功能僅適用於 SDK 5.16.0 版及更新版本。

先決條件

- 您只能在 Windows 平台上產生 KSP 金鑰參考。
- 您必須以加密使用者 (CU) 身分登入。

檔案位置

根據預設，AWS CloudHSM 會將產生的檔案存放在：`C:\Users\Default\AppData\Roaming\Microsoft\Crypto\CaviumKSP\GlobalPartition`

若要指定不同的位置，請使用 `--path` 參數。

語法

```
aws-cloudhsm > help key generate-file --encoding ksp-key-reference
```

Generate a key file from a key in the HSM cluster. This command does not export any private key data from the HSM

Usage: key generate-file --encoding *<ENCODING>* --path *<PATH>* --filter [*<FILTER>*...]

#### Options:

--encoding *<ENCODING>*

Encoding format for the key file

Possible values:

- reference-pem: PEM formatted key reference (supports private keys)
- pem: PEM format (supports public keys)
- ksp-key-reference: KSP key reference format

--cluster-id *<CLUSTER\_ID>*

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided with multiple clusters configured, will error

--path *<PATH>*

Directory path where the key file will be written

--filter [*<FILTER>*...]

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key for file generation

--all

Generate ksp key reference for all available key pairs in HSM

-h, --help

Print help (see a summary with '-h')

### 範例 – 使用私有金鑰的屬性篩選條件產生 KSP 金鑰參考

下列範例會為具有特定標籤的私有金鑰產生 KSP 金鑰參考。

#### Example

```
aws-cloudhsm > key generate-file --encoding ksp-key-reference --path --filter
attr.label="ec-test-private-key"
{
 "error_code": 0,
 "data": {
 "message": "Successfully generated key file"
 }
}
```

```
}
```

## 範例 – 產生所有金鑰對的 KSP 金鑰參考

下列範例會為叢集中的所有金鑰對產生 KSP 金鑰參考。

### Example

```
aws-cloudhsm > key generate-file --encoding ksp-key-reference --all
{
 "error_code": 0,
 "data": {
 "message": "Successfully generated key file"
 }
}
```

### 相關主題

- [CloudHSM CLI 的金鑰屬性](#)
- [使用 CloudHSM CLI 篩選金鑰](#)
- [CloudHSM CLI 中的 generate-asymmetric-pair 類別](#)
- [CloudHSM CLI 中的產生對稱類別](#)

### CloudHSM CLI 中的 generate-asymmetric-pair 類別

在 CloudHSM CLI 中，key generate-asymmetric-pair 是一組命令的父類別，當與父類別結合時，會建立產生非對稱金鑰對的命令。目前，此類別由以下命令組成：

- [產生非對稱 EC 金鑰對](#)
- [產生非對稱 RSA 金鑰對](#)

### 使用 CloudHSM CLI 產生非對稱 EC 金鑰對

在 CloudHSM CLI 中使用 key asymmetric-pair ec 命令，在您的 AWS CloudHSM 叢集中產生非對稱橢圓曲線 (EC) 金鑰對。

### 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key generate-asymmetric-pair ec
Generate an Elliptic-Curve Cryptography (ECC) key pair

Usage: key generate-asymmetric-pair ec [OPTIONS] --public-label <PUBLIC_LABEL> --
private-label <PRIVATE_LABEL> --curve <CURVE>

Options:
 --cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error
 --public-label <PUBLIC_LABEL>
 Label for the public key
 --private-label <PRIVATE_LABEL>
 Label for the private key
 --session
 Creates a session key pair that exists only in the current session. The key
 cannot be recovered after the session ends
 --curve <CURVE>
 Elliptic curve used to generate the key pair [possible values: prime256v1,
 secp256r1, secp224r1, secp384r1, secp256k1, secp521r1]
 --public-attributes [<PUBLIC_KEY_ATTRIBUTES>...]
 Space separated list of key attributes to set for the generated EC public key
 in the form of KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE
 --private-attributes [<PRIVATE_KEY_ATTRIBUTES>...]
 Space separated list of key attributes to set for the generated EC private
 key in the form of KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE
 --share-crypto-users [<SHARE_CRYPTO_USERS>...]
 Space separated list of Crypto User usernames to share the EC private key
 with
 --manage-private-key-quorum-value <MANAGE_PRIVATE_KEY_QUORUM_VALUE>
 The quorum value for key management operations for the private key
 --use-private-key-quorum-value <USE_PRIVATE_KEY_QUORUM_VALUE>
 The quorum value for key usage operations for the private key
 -h, --help
```

[Print help](#)

## 範例

下列範例示範如何使用 `key generate-asymmetric-pair ec` 命令來建立 EC 金鑰對。

Example 範例：建立 EC 金鑰對

```
aws-cloudhsm > key generate-asymmetric-pair ec \
 --curve secp224r1 \
 --public-label ec-public-key-example \
 --private-label ec-private-key-example
{
 "error_code": 0,
 "data": {
 "public_key": {
 "key-reference": "0x0000000000012000b",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "ec",
 "label": "ec-public-key-example",
 "id": "",
 "check-value": "0xd7c1a7",
 "class": "public-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 }
 }
 }
}
```

```

 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 57,
 "ec-point":
"0x047096513df542250a6b228fd9cb67fd0c903abc93488467681974d6f371083fce1d79da8ad1e9ede745fb9f38a
 "curve": "secp224r1"
 }
},
"private_key": {
 "key-reference": "0x0000000000012000c",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "ec",
 "label": "ec-private-key-example",
 "id": "",
 "check-value": "0xd7c1a7",
 "class": "private-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,

```



```

 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 122,
 "ec-point":
"0x047096513df542250a6b228fd9cb67fd0c903abc93488467681974d6f371083fce1d79da8ad1e9ede745fb9f38a
 "curve": "secp224r1"
 }
}
}
}

```

Example 範例：建立具有選用屬性的 EC 金鑰對

```

aws-cloudhsm > key generate-asymmetric-pair ec \
 --curve secp224r1 \
 --public-label ec-public-key-example \
 --private-label ec-private-key-example \
 --public-attributes encrypt=true \
 --private-attributes decrypt=true
{
 "error_code": 0,
 "data": {
 "public_key": {
 "key-reference": "0x000000000002806eb",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],

```

```

 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "ec",
 "label": "ec-public-key-example",
 "id": "",
 "check-value": "0xedef86",
 "class": "public-key",
 "encrypt": true,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 57,
 "ec-point":
"0x0487af31882189ec29eddf17a48e8b9cebb075b7b5afc5522fe9c83a029a450cc68592889a1ebf45f32240da514",
 "curve": "secp224r1"
 }
},
"private_key": {
 "key-reference": "0x0000000000280c82",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
]
 }
}

```

```

],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
},
"attributes": {
 "key-type": "ec",
 "label": "ec-private-key-example",
 "id": "",
 "check-value": "0xedef86",
 "class": "private-key",
 "encrypt": false,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 122,
 "ec-point":
"0x0487af31882189ec29eddf17a48e8b9cebb075b7b5afc5522fe9c83a029a450cc68592889a1ebf45f32240da514
 "curve": "secp224r1"
}
}
}
}

```

## Example 範例：使用規定人數值建立 EC 金鑰對

使用規定人數控制產生金鑰時，該金鑰必須與等於最大金鑰規定人數值的最小使用者數目相關聯。相關聯的使用者包括金鑰擁有者和與金鑰共用的加密使用者。若要判斷要共用金鑰的最小使用者數量，請在金鑰使用量值與金鑰管理量值之間取得最大的量值，並減去 1 以考慮金鑰擁有者，該擁有者預設為與金鑰相關聯的使用者。若要與更多使用者共用金鑰，請使用 [使用 CloudHSM CLI 共用金鑰](#) 命令。

```
aws-cloudhsm > key generate-asymmetric-pair ec \
 --curve secp224r1 \
 --public-label ec-public-key-example \
 --private-label ec-private-key-example \
 --public-attributes verify=true \
 --private-attributes sign=true
 --share-crypto-users cu2 cu3 cu4 \
 --manage-private-key-quorum-value 4 \
 --use-private-key-quorum-value 2
{
 "error_code": 0,
 "data": {
 "public_key": {
 "key-reference": "0x000000000002806eb",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "ec",
 "label": "ec-public-key-example",
 "id": "",
 "check-value": "0xedef86",
 "class": "public-key",
 "encrypt": false,
 "decrypt": false,
```

```

 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 57,
 "ec-point":
"0x0487af31882189ec29eddf17a48e8b9cebb075b7b5afc5522fe9c83a029a450cc68592889a1ebf45f32240da514
 "curve": "secp224r1"
 }
},
"private_key": {
 "key-reference": "0x00000000000280c82",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [
 {
 "username": "cu2",
 "key-coverage": "full"
 },
 {
 "username": "cu3",
 "key-coverage": "full"
 },
 {
 "username": "cu4",
 "key-coverage": "full"
 }
]
 }
},

```

```

],
 "key-quorum-values": {
 "manage-key-quorum-value": 4,
 "use-key-quorum-value": 2
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "ec",
 "label": "ec-private-key-example",
 "id": "",
 "check-value": "0xedef86",
 "class": "private-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 122,
 "ec-point":
 "0x0487af31882189ec29eddf17a48e8b9cebb075b7b5afc5522fe9c83a029a450cc68592889a1ebf45f32240da514",
 "curve": "secp224r1"
 }
}
}
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <CURVE>

指橢圓曲線的識別符。

- prime256v1
- secp256r1
- secp224r1
- secp384r1
- secp256k1
- secp521r1

必要：是

### <PUBLIC\_KEY\_ATTRIBUTES>

指一個空格分隔的金鑰屬性清單，以 KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE (例如，verify=true) 的形式為產生的 EC 公有金鑰設定

如需支援的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

### <PUBLIC\_LABEL>

指使用者定義的公有金鑰標籤。用戶端 SDK label 5.11 和更新版本允許的大小上限為 127 個字元。用戶端 SDK 5.10 和以前的 限制為 126 個字元。

必要：是

### <PRIVATE\_KEY\_ATTRIBUTES>

指一個空格分隔的金鑰屬性清單，以 KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE (例如，sign=true) 的形式為產生的 EC 私有金鑰設定

如需支援的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

### <PRIVATE\_LABEL>

指使用者定義的私有金鑰標籤。用戶端 SDK label 5.11 和更新版本允許的大小上限為 127 個字元。用戶端 SDK 5.10 和以前的 限制為 126 個字元。

必要：是

### <SESSION>

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

根據預設，產生的金鑰是持久性 (權杖) 金鑰。在 <SESSION> 傳遞會變更此情況，確保使用此參數生成的金鑰是工作階段 (臨時) 金鑰。

必要：否

### <SHARE\_CRYPTO\_USERS>

指定要與 共用 EC 私有金鑰的加密使用者名稱清單，以空格分隔

必要：否

### <MANAGE\_PRIVATE\_KEY\_QUORUM\_VALUE>

私有金鑰金鑰管理操作的規定人數值。此值必須小於或等於與金鑰相關聯的使用者數目。這包括與之共用金鑰的使用者，以及金鑰擁有者。最大值為 8。

必要：否

### <USE\_PRIVATE\_KEY\_QUORUM\_VALUE>

私有金鑰金鑰使用量操作的規定人數值。此值必須小於或等於與金鑰相關聯的使用者數目。這包括與之共用金鑰的使用者，以及金鑰擁有者。最大值為 8。

必要：否

## 相關主題

- [CloudHSM CLI 的金鑰屬性](#)
- [使用 CloudHSM CLI 篩選金鑰](#)



## 使用 CloudHSM CLI 產生非對稱 RSA 金鑰對

在 CloudHSM CLI 中使用 `key generate-asymmetric-pair rsa` 命令，在您的 AWS CloudHSM 叢集中產生非對稱 RSA 金鑰對。

### 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

### 要求

若要執行此命令，必須以 CU 的身分登入。

### 語法

```
aws-cloudhsm > help key generate-asymmetric-pair rsa
```

Generate an RSA key pair

```
Usage: key generate-asymmetric-pair rsa [OPTIONS] --public-label <PUBLIC_LABEL>
--private-label <PRIVATE_LABEL> --modulus-size-bits <MODULUS_SIZE_BITS> --public-
exponent <PUBLIC_EXPONENT>
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--public-label <PUBLIC_LABEL>
```

Label for the public key

```
--private-label <PRIVATE_LABEL>
```

Label for the private key

```
--session
```

Creates a session key pair that exists only in the current session. The key cannot be recovered after the session ends

```
--modulus-size-bits <MODULUS_SIZE_BITS>
```

Modulus size in bits used to generate the RSA key pair

```
--public-exponent <PUBLIC_EXPONENT>
```

Public exponent used to generate the RSA key pair

```
--public-attributes [<PUBLIC_KEY_ATTRIBUTES>...]
```

Space separated list of key attributes to set for the generated RSA public key in the form of KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE

```

--private-attributes [<PRIVATE_KEY_ATTRIBUTES>...]
 Space separated list of key attributes to set for the generated RSA private
 key in the form of KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE
--share-crypto-users [<SHARE_CRYPTO_USERS>...]
 Space separated list of Crypto User usernames to share the RSA key with
--manage-private-key-quorum-value <MANAGE_PRIVATE_KEY_QUORUM_VALUE>
 The quorum value for key management operations for the private key
--use-private-key-quorum-value <USE_PRIVATE_KEY_QUORUM_VALUE>
 The quorum value for key usage operations for the private key
-h, --help
 Print help

```

## 範例

下列範例示範如何使用 `key generate-asymmetric-pair rsa` 來建立 RSA 金鑰對。

Example 範例：建立 RSA 金鑰對

```

aws-cloudhsm > key generate-asymmetric-pair rsa \
--public-exponent 65537 \
--modulus-size-bits 2048 \
--public-label rsa-public-key-example \
--private-label rsa-private-key-example
{
 "error_code": 0,
 "data": {
 "public_key": {
 "key-reference": "0x000000000000160010",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "rsa",

```

```

 "label": "rsa-public-key-example",
 "id": "",
 "check-value": "0x498e1f",
 "class": "public-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 512,
 "public-exponent": "0x010001",
 "modulus":
 "0xdfca0669dc8288ed3bad99509bd21c7e6192661407021b3f4cdf4a593d939dd24f4d641af8e4e73b04c847731c6
 e89a065e7d1a46ced96b46b909db2ab6be871ee700fd0a448b6e975bb64cae77c49008749212463e37a577baa57ce3e
 bcebb7d20bd6df1948ae336ae23b52d73b7f3b6acc254edb6358e08d326d280ce489571f4d34e316a2ea1904d513ca
 "modulus-size-bits": 2048
 }
},
"private_key": {
 "key-reference": "0x00000000000160011",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 }
 }
}

```

```

 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "rsa",
 "label": "rsa-private-key-example",
 "id": "",
 "check-value": "0x498e1f",
 "class": "private-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 1217,
 "public-exponent": "0x010001",
 "modulus":
 "0xdfca0669dc8288ed3bad99509bd21c7e6192661407021b3f4cdf4a593d939dd24f4d641af8e4e73b04c847731c6",
 "modulus-size-bits": 2048
 }
}
}
}
}

```

Example 範例：建立具有選用屬性的 RSA 金鑰對

```

aws-cloudhsm > key generate-asymmetric-pair rsa \
--public-exponent 65537 \
--modulus-size-bits 2048 \
--public-label rsa-public-key-example \

```

```
--private-label rsa-private-key-example \
--public-attributes encrypt=true \
--private-attributes decrypt=true
{
 "error_code": 0,
 "data": {
 "public_key": {
 "key-reference": "0x00000000000280cc8",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "rsa",
 "label": "rsa-public-key-example",
 "id": "",
 "check-value": "0x01fe6e",
 "class": "public-key",
 "encrypt": true,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
```

```

 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 512,
 "public-exponent": "0x010001",
 "modulus":
 "0xb1d27e857a876f4e9fd5de748a763c539b359f937eb4b4260e30d1435485a732c878cdad9c72538e2215351b1d4
 73a80fdb457aa7b20cd61e486c326e2cfd5e124a7f6a996437437812b542e3caf85928aa866f0298580f7967ee6aa01
 f6e6296d6c116d5744c6d60d14d3bf3cb978fe6b75ac67b7089bafd50d8687213b31abc7dc1bad422780d29c851d510
 133022653225bd129f8491101725e9ea33e1ded83fb57af35f847e532eb30cd7e726f23910d2671c6364092e834697e
 ac3160f0ca9725d38318b7",
 "modulus-size-bits": 2048
 },
 "private_key": {
 "key-reference": "0x00000000000280cc7",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "rsa",
 "label": "rsa-private-key-example",
 "id": "",
 "check-value": "0x01fe6e",
 "class": "private-key",
 "encrypt": false,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,

```

```

 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 1217,
 "public-exponent": "0x010001",
 "modulus":
"0xb1d27e857a876f4e9fd5de748a763c539b359f937eb4b4260e30d1435485a732c878cdad9c72538e2215351b1d4
 "modulus-size-bits": 2048
 }
}
}
}

```

#### Example 範例：使用規定人數值建立 RSA 金鑰對

使用規定人數控制產生金鑰時，該金鑰必須與等於最大金鑰規定人數值的最小使用者數目相關聯。相關聯的使用者包括金鑰擁有者和與金鑰共用的加密使用者。若要判斷要共用金鑰的最小使用者數量，請在金鑰使用量值與金鑰管理量值之間取得最大的量值，並減去 1 以考慮金鑰擁有者，該擁有者預設為與金鑰相關聯的使用者。若要與更多使用者共用金鑰，請使用 [使用 CloudHSM CLI 共用金鑰](#) 命令。

```

aws-cloudhsm > key generate-asymmetric-pair rsa \
--public-exponent 65537 \
--modulus-size-bits 2048 \
--public-label rsa-public-key-example \
--private-label rsa-private-key-example \
--public-attributes verify=true \
--private-attributes sign=true
--share-crypto-users cu2 cu3 cu4 \
--manage-private-key-quorum-value 4 \
--use-private-key-quorum-value 2
{
 "error_code": 0,
 "data": {
 "public_key": {
 "key-reference": "0x00000000000280cc8",
 "key-info": {
 "key-owners": [

```

```

 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
},
"attributes": {
 "key-type": "rsa",
 "label": "rsa-public-key-example",
 "id": "",
 "check-value": "0x01fe6e",
 "class": "public-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 512,
 "public-exponent": "0x010001",
 "modulus":

```

```

 "0xb1d27e857a876f4e9fd5de748a763c539b359f937eb4b4260e30d1435485a732c878cdad9c72538e2215351b1d4
73a80fdb457aa7b20cd61e486c326e2cfd5e124a7f6a996437437812b542e3caf85928aa866f0298580f7967ee6aa01
f6e6296d6c116d5744c6d60d14d3bf3cb978fe6b75ac67b7089bafd50d8687213b31abc7dc1bad422780d29c851d510
133022653225bd129f8491101725e9ea33e1ded83fb57af35f847e532eb30cd7e726f23910d2671c6364092e834697e
ac3160f0ca9725d38318b7",

```



```
 "modulus-size-bits": 2048
 },
},
"private_key": {
 "key-reference": "0x00000000000280cc7",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [
 {
 "username": "cu2",
 "key-coverage": "full"
 },
 {
 "username": "cu3",
 "key-coverage": "full"
 },
 {
 "username": "cu4",
 "key-coverage": "full"
 }
],
 "key-quorum-values": {
 "manage-key-quorum-value": 4,
 "use-key-quorum-value": 2
 },
 "cluster-coverage": "full"
 },
},
"attributes": {
 "key-type": "rsa",
 "label": "rsa-private-key-example",
 "id": "",
 "check-value": "0x01fe6e",
 "class": "private-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
```

```

 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 1217,
 "public-exponent": "0x010001",
 "modulus":
"0xb1d27e857a876f4e9fd5de748a763c539b359f937eb4b4260e30d1435485a732c878cdad9c72538e2215351b1d4
 "modulus-size-bits": 2048
 }
}
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <MODULUS\_SIZE\_BITS>

指模數的長度 (以位元為單位)。最小值為 2048。

必要：是

### <PRIVATE\_KEY\_ATTRIBUTES>

指一個空格分隔的金鑰屬性清單，以 KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE (例如，sign=true) 的形式為產生的 RSA 私有金鑰設定

如需支援的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

**<PRIVATE\_LABEL>**

指使用者定義的私有金鑰標籤。用戶端 SDK label 5.11 和更新版本允許的大小上限為 127 個字元。用戶端 SDK 5.10 和以前的 限制為 126 個字元。

必要：是

**<PUBLIC\_EXPONENT>**

指公有指數。值必須為大於或等於 65537 的奇數。

必要：是

**<PUBLIC\_KEY\_ATTRIBUTES>**

指一個空格分隔的金鑰屬性清單，以 KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE (例如，verify=true) 的形式為產生的 RSA 公有金鑰設定

如需支援的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

**<PUBLIC\_LABEL>**

指使用者定義的公有金鑰標籤。用戶端 SDK label 5.11 和更新版本允許的大小上限為 127 個字元。用戶端 SDK 5.10 和以前的 限制為 126 個字元。

必要：是

**<SESSION>**

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

根據預設，產生的金鑰是持久性 (權杖) 金鑰。在 <SESSION> 傳遞會變更此情況，確保使用此參數生成的金鑰是工作階段 (臨時) 金鑰。

必要：否

**<SHARE\_CRYPTO\_USERS>**

指定要與 共用 RSA 私有金鑰的加密使用者名稱的空格分隔清單

必要：否

### <MANAGE\_PRIVATE\_KEY\_QUORUM\_VALUE>

私有金鑰金鑰管理操作的規定人數值。此值必須小於或等於與金鑰相關聯的使用者數目。這包括與之共用金鑰的使用者，以及金鑰擁有者。最大值為 8。

必要：否

### <USE\_PRIVATE\_KEY\_QUORUM\_VALUE>

私有金鑰金鑰使用量操作的規定人數值。此值必須小於或等於與金鑰相關聯的使用者數目。這包括與之共用金鑰的使用者，以及金鑰擁有者。最大值為 8。

必要：否

## 相關主題

- [CloudHSM CLI 的金鑰屬性](#)
- [使用 CloudHSM CLI 篩選金鑰](#)

## CloudHSM CLI 中的產生對稱類別

在 CloudHSM CLI 中，key generate-symmetric 是一組命令的父類別，當與父類別結合時，會建立產生對稱金鑰的命令。目前，此類別由以下命令組成：

- [產生對稱 AES 金鑰](#)
- [產生對稱通用私密金鑰](#)

## 使用 CloudHSM CLI 產生對稱 AES 金鑰

在 CloudHSM CLI 中使用 key generate-symmetric aes 命令，在您的 AWS CloudHSM 叢集中產生對稱 AES 金鑰。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key generate-symmetric aes
```

Generate an AES key

Usage: key generate-symmetric aes [OPTIONS] --label *<LABEL>* --key-length-bytes *<KEY\_LENGTH\_BYTES>*

Options:

--cluster-id *<CLUSTER\_ID>*

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

--label *<LABEL>*

Label for the key

--session

Creates a session key that exists only in the current session. The key cannot be recovered after the session ends

--key-length-bytes *<KEY\_LENGTH\_BYTES>*

Key length in bytes

--attributes [*<KEY\_ATTRIBUTES>*...]

Space separated list of key attributes to set for the generated AES key in the form of KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE

--share-crypto-users [*<SHARE\_CRYPTO\_USERS>*...]

Space separated list of Crypto User usernames to share the AES key with

--manage-key-quorum-value *<MANAGE\_KEY\_QUORUM\_VALUE>*

The quorum value for key management operations

--use-key-quorum-value *<USE\_KEY\_QUORUM\_VALUE>*

The quorum value for key usage operations

-h, --help

Print help

## 範例

下列範例示範如何使用 key generate-symmetric aes 命令來建立 AES 金鑰。

Example 範例：建立 AES 金鑰

```
aws-cloudhsm > key generate-symmetric aes \
--label example-aes \
--key-length-bytes 24
{
 "error_code": 0,
```

```
"data": {
 "key": {
 "key-reference": "0x000000000002e06bf",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "example-aes",
 "id": "",
 "check-value": "0x9b94bd",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 24
 }
 }
}
```

```
}
}
```

### Example 範例：建立具有選用屬性的 AES 金鑰

```
aws-cloudhsm > key generate-symmetric aes \
--label example-aes \
--key-length-bytes 24 \
--attributes decrypt=true encrypt=true
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000002e06bf",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "example-aes",
 "id": "",
 "check-value": "0x9b94bd",
 "class": "secret-key",
 "encrypt": true,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,

```

```

 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 24
 }
}
}
}

```

### Example 範例：建立具有規定人數值的 AES 金鑰

使用規定人數控制產生金鑰時，該金鑰必須與等於最大金鑰規定人數值的最小使用者數目相關聯。相關聯的使用者包括金鑰擁有者和與金鑰共用的加密使用者。若要判斷要共用金鑰的最小使用者數量，請在金鑰使用量值與金鑰管理量值之間取得最大的量值，並減去 1 以考慮金鑰擁有者，該擁有者預設為與金鑰相關聯的使用者。若要與更多使用者共用金鑰，請使用 [使用 CloudHSM CLI 共用金鑰](#) 命令。

```

aws-cloudhsm > key generate-symmetric aes \
--label example-aes \
--key-length-bytes 24 \
--attributes decrypt=true encrypt=true
--share-crypto-users cu2 cu3 cu4 \
--manage-key-quorum-value 4 \
--use-key-quorum-value 2
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000002e06bf",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [
 {

```



```
 "username": "cu2",
 "key-coverage": "full"
 },
 {
 "username": "cu3",
 "key-coverage": "full"
 },
 {
 "username": "cu4",
 "key-coverage": "full"
 },
],
"key-quorum-values": {
 "manage-key-quorum-value": 4,
 "use-key-quorum-value": 2
},
"cluster-coverage": "full"
},
"attributes": {
 "key-type": "aes",
 "label": "example-aes",
 "id": "",
 "check-value": "0x9b94bd",
 "class": "secret-key",
 "encrypt": true,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 24
}
```

```
}
}
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <KEY\_ATTRIBUTES>

指定一個空格分隔的金鑰屬性清單，對產生的 AES 金鑰進行設定，格式為 KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE (例如，sign=true)。

如需支援的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

### <KEY-LENGTH-BYTES>

指金鑰長度 (以位元組為單位)。

有效值：

- 16、24 和 32

必要：是

### <LABEL>

指定使用者定義的 AES 金鑰標籤。用戶端 SDK label 5.11 和更新版本允許的大小上限為 127 個字元。用戶端 SDK 5.10 和以前的 限制為 126 個字元。

必要：是

### <SESSION>

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

根據預設，產生的金鑰是持久性 (權杖) 金鑰。在 <SESSION> 傳遞會變更此情況，確保使用此參數生成的金鑰是工作階段 (臨時) 金鑰。

必要：否

### <SHARE\_CRYPTO\_USERS>

指定要與 共用 AES 金鑰的加密使用者名稱的空格分隔清單

必要：否

### <MANAGE\_KEY\_QUORUM\_VALUE>

金鑰管理操作的規定人數值。此值必須小於或等於與金鑰相關聯的使用者數目。這包括與之共用金鑰的使用者，以及金鑰擁有者。最大值為 8。

必要：否

### <USE\_KEY\_QUORUM\_VALUE>

金鑰用量操作的規定人數值。此值必須小於或等於與金鑰相關聯的使用者數目。這包括與之共用金鑰的使用者，以及金鑰擁有者。最大值為 8。

必要：否

## 相關主題

- [CloudHSM CLI 的金鑰屬性](#)
- [使用 CloudHSM CLI 篩選金鑰](#)

## 使用 CloudHSM CLI 產生對稱一般私密金鑰

在 CloudHSM CLI 中使用 `key generate-asymmetric-pair` 命令，在您的 AWS CloudHSM 叢集中產生對稱的一般秘密金鑰。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > key help generate-symmetric generic-secret
```

Generate a generic secret key

Usage: key generate-symmetric generic-secret [OPTIONS] --label *<LABEL>* --key-length-bytes *<KEY\_LENGTH\_BYTES>*

Options:

--cluster-id *<CLUSTER\_ID>*

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

--label *<LABEL>*

Label for the key

--session

Creates a session key that exists only in the current session. The key cannot be recovered after the session ends

--key-length-bytes *<KEY\_LENGTH\_BYTES>*

Key length in bytes

--attributes [*<KEY\_ATTRIBUTES>*...]

Space separated list of key attributes to set for the generated generic secret key in the form of KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE

--share-crypto-users [*<SHARE\_CRYPTO\_USERS>*...]

Space separated list of Crypto User usernames to share the generic secret key with

--manage-key-quorum-value *<MANAGE\_KEY\_QUORUM\_VALUE>*

The quorum value for key management operations

--use-key-quorum-value *<USE\_KEY\_QUORUM\_VALUE>*

The quorum value for key usage operations

-h, --help

Print help

## 範例

下列範例示範如何使用 key generate-symmetric generic-secret 命令來建立一組通用私密金鑰。

Example 範例：建立一組通用私密金鑰

```
aws-cloudhsm > key generate-symmetric generic-secret \
--label example-generic-secret \
--key-length-bytes 256
{
```

```
"error_code": 0,
"data": {
 "key": {
 "key-reference": "0x000000000002e08fd",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "generic-secret",
 "label": "example-generic-secret",
 "id": "",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 256
 }
 }
}
```

```
}
}
```

### Example 範例：建立一組無選用屬性的通用私密金鑰

```
aws-cloudhsm > key generate-symmetric generic-secret \
--label example-generic-secret \
--key-length-bytes 256 \
--attributes encrypt=true
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000002e08fd",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "generic-secret",
 "label": "example-generic-secret",
 "id": "",
 "class": "secret-key",
 "encrypt": true,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 }
 }
 }
}
```

```

 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 256
 }
}
}
}

```

### Example 範例：建立具有規定人數值的一般私密金鑰

使用規定人數控制產生金鑰時，該金鑰必須與等於最大金鑰規定人數值的最小使用者數目相關聯。相關聯的使用者包括金鑰擁有者和與金鑰共用的加密使用者。若要判斷要共用金鑰的最小使用者數量，請在金鑰使用量值與金鑰管理量值之間取得最大的量值，並減去 1 以考慮金鑰擁有者，該擁有者預設為與金鑰相關聯的使用者。若要與更多使用者共用金鑰，請使用 [使用 CloudHSM CLI 共用金鑰](#) 命令。

```

aws-cloudhsm > key generate-symmetric generic-secret \
--label example-generic-secret \
--key-length-bytes 256 \
--attributes encrypt=true
--share-crypto-users cu2 cu3 cu4 \
--manage-key-quorum-value 4 \
--use-key-quorum-value 2
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000002e08fd",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [
 {
 "username": "cu2",

```

```
 "key-coverage": "full"
 },
 {
 "username": "cu3",
 "key-coverage": "full"
 },
 {
 "username": "cu4",
 "key-coverage": "full"
 },
],
 "key-quorum-values": {
 "manage-key-quorum-value": 4,
 "use-key-quorum-value": 2
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "generic-secret",
 "label": "example-generic-secret",
 "id": "",
 "class": "secret-key",
 "encrypt": true,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 256
 }
}
```



```
}
```

引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <KEY\_ATTRIBUTES>

指定一個空格分隔的金鑰屬性清單，對產生的 AES 金鑰進行設定，格式為 KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE (例如，sign=true)。

如需支援的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

### <KEY-LENGTH-BYTES>

指金鑰長度 (以位元組為單位)。

有效值：

- 1 到 800

必要：是

### <LABEL>

指定使用者定義的通用私密金鑰標籤。用戶端 SDK label 5.11 和更新版本允許的大小上限為 127 個字元。用戶端 SDK 5.10 和以前的 限制為 126 個字元。

必要：是

### <SESSION>

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

根據預設，產生的金鑰是持久性 (權杖) 金鑰。在 <SESSION> 傳遞會變更此情況，確保使用此參數生成的金鑰是工作階段 (臨時) 金鑰。

必要：否

### <SHARE\_CRYPTO\_USERS>

加密使用者名稱的空格分隔清單，以與 共用一般私密金鑰

必要：否

### <MANAGE\_KEY\_QUORUM\_VALUE>

金鑰管理操作的規定人數值。此值必須小於或等於與金鑰相關聯的使用者數目。這包括與之共用金鑰的使用者，以及金鑰擁有者。最大值為 8。

必要：否

### <USE\_KEY\_QUORUM\_VALUE>

金鑰用量操作的規定人數值。此值必須小於或等於與金鑰相關聯的使用者數目。這包括與之共用金鑰的使用者，以及金鑰擁有者。最大值為 8。

必要：否

## 相關主題

- [CloudHSM CLI 的金鑰屬性](#)
- [使用 CloudHSM CLI 篩選金鑰](#)

## 使用 CloudHSM CLI 匯入 PEM 格式金鑰

在 中使用 `key import pem` 命令 AWS CloudHSM，將 PEM 格式金鑰匯入硬體安全模組 (HSM)。您可以使用此命令匯入在 HSM 之外產生的公有金鑰。

### Note

使用 [使用 CloudHSM CLI 匯出非對稱金鑰](#) 命令從公有金鑰建立標準 PEM 檔案，或從私有金鑰建立參考 PEM 檔案。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key import pem
```

Import key from a PEM file

Usage: key import pem [OPTIONS] --path <PATH> --label <LABEL> --key-type-class <KEY\_TYPE\_CLASS>

Options:

    --cluster-id <CLUSTER\_ID>

        Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

    --path <PATH>

        Path where the key is located in PEM format

    --label <LABEL>

        Label for the imported key

    --key-type-class <KEY\_TYPE\_CLASS>

        Key type and class of the imported key [possible values: ec-public, rsa-public]

    --attributes [<IMPORT\_KEY\_ATTRIBUTES>...]

        Space separated list of key attributes in the form of KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE for the imported key

    -h, --help

        Print help

## 範例

這些範例示範如何使用 key import pem 命令，從 PEM 格式的檔案匯入 RSA 公有金鑰。

Example 範例：匯入 RSA 公有金鑰

```
aws-cloudhsm > key import pem --path /home/example --label example-imported-key --key-type-class rsa-public
```

```
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001e08e3",
 "key-info": {
```

```

 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "rsa",
 "label": "example-imported-key",
 "id": "0x",
 "check-value": "0x99fe93",
 "class": "public-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 512,
 "public-exponent": "0x010001",
 "modulus":
 "0x8e9c172c37aa22ed1ce25f7c3a7c936dadcd532201400128b044ebb4b96#..3e4930ab910df5a2896eae8853cfe",
 "modulus-size-bits": 2048
 }
},

```

```
 "message": "Successfully imported key"
 }
}
```

### Example 範例：匯入具有選用屬性的 RSA 公有金鑰

```
aws-cloudhsm > key import pem --path /home/example --label example-imported-key-with-
attributes --key-type-class rsa-public --attributes verify=true
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001e08e3",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "rsa",
 "label": "example-imported-key-with-attributes",
 "id": "0x",
 "check-value": "0x99fe93",
 "class": "public-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
```

```

 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 512,
 "public-exponent": "0x010001",
 "modulus":
"0x8e9c172c37aa22ed1ce25f7c3a7c936dad532201400128b044ebb4b96#..3e4930ab910df5a2896eaeb8853cfe
 "modulus-size-bits": 2048
 }
},
"message": "Successfully imported key"
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <PATH>

指定金鑰檔案所在的檔案路徑。

必要：是

### <LABEL>

指定匯入金鑰的使用者定義標籤。label 的大小上限為 126 個字元。

必要：是

### <KEY\_TYPE\_CLASS>

包裝金鑰的金鑰類型和類別。

可能的值如下：

- ec-public
- rsa-public

必要：是

### <IMPORT\_KEY\_ATTRIBUTES>

指定要為匯入金鑰設定之金鑰屬性的空格分隔清單，格式為 KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE ( 例如 sign=true)。如需支援的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：否

### 相關主題

- [CloudHSM CLI 中的加密簽署類別](#)
- [CloudHSM CLI 中的加密驗證類別](#)

### 使用 CloudHSM CLI 列出使用者的金鑰

使用 CloudHSM CLI 中的 key list 命令，尋找 AWS CloudHSM 叢集中目前使用者的所有金鑰。輸出包含使用者擁有和共用的金鑰，以及 CloudHSM 叢集中的所有公有金鑰。

### 使用者類型

下列類型的使用者可以執行此命令。

- 管理員 (COs)
- 加密使用者 (CU)

### 語法

```
aws-cloudhsm > help key list
List the keys the current user owns, shares, and all public keys in the HSM cluster

Usage: key list [OPTIONS]

Options:
 --cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error
 --filter [<FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select matching key(s) to list

`--max-items <MAX_ITEMS>`

The total number of items to return in the command's output. If the total number of items available is more than the value specified, a next-token is provided in the command's output. To resume pagination, provide the next-token value in the starting-token argument of a subsequent command [default: 10]

`--starting-token <STARTING_TOKEN>`

A token to specify where to start paginating. This is the next-token from a previously truncated response

`-v, --verbose`

If included, prints all attributes and key information for each matched key. By default each matched key only displays its key-reference and label attribute. This flag when used by Admins has no effect

`-h, --help`

Print help

## 範例

下列範例顯示執行 key list 命令的不同方式。下列範例以加密使用者身分顯示輸出。

Example 範例：尋找所有金鑰 – 預設

此命令會列出 AWS CloudHSM 叢集中存在的已登入使用者的金鑰。

### Note

根據預設，僅顯示目前登入使用者的 10 個金鑰，且只顯示 key-reference 和 label 作為輸出。使用適當的分頁選項來顯示更多或更少的金鑰作為輸出。

```
aws-cloudhsm > key list
{
 "error_code": 0,
 "data": {
 "matched_keys": [
 {
 "key-reference": "0x000000000000003d5",
 "attributes": {
 "label": "test_label_1"
 }
 }
],
 },
}
```



```

 {
 "key-reference": "0x00000000000000626",
 "attributes": {
 "label": "test_label_2"
 }
 },
 ...8 keys later...
],
 "total_key_count": 56,
 "returned_key_count": 10,
 "next_token": "10"
}

```

### Example 範例：尋找所有金鑰 – 詳細資訊

輸出包含使用者擁有和共用的金鑰，以及 HSMs 中的所有公有金鑰。

#### Note

注意：按照預設，僅顯示目前登入使用者的 10 個金鑰。使用適當的分頁選項來顯示更多或更少的金鑰作為輸出。

```

aws-cloudhsm > key list --verbose
{
 "error_code": 0,
 "data": {
 "matched_keys": [
 {
 "key-reference": "0x0000000000012000c",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 }
 }
 }
]
 }
}

```

```

 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "ec",
 "label": "ec-test-private-key",
 "id": "",
 "check-value": "0x2a737d",
 "class": "private-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 122,
 "ec-point":
"0x0442d53274a6c0ec1a23c165dcb9ccdd72c64e98ae1a9594bb5284e752c746280667e11f1e983493c1c605e0a80
 "curve": "secp224r1"
 }
},
{
 "key-reference": "0x0000000000012000d",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {

```

```

 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
},
"attributes": {
 "key-type": "ec",
 "label": "ec-test-public-key",
 "id": "",
 "check-value": "0x2a737d",
 "class": "public-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 57,
 "ec-point":
"0x0442d53274a6c0ec1a23c165dcb9ccdd72c64e98ae1a9594bb5284e752c746280667e11f1e983493c1c605e0a80
 "curve": "secp224r1"
}
}
],
 ...8 keys later...
 "total_key_count": 1580,
 "returned_key_count": 10
}
}

```

## Example 範例：分頁傳回

下列範例將顯示僅顯示兩個金鑰的金鑰分頁子集。然後，此範例會提供後續呼叫，以顯示接下來的兩個金鑰。

```
aws-cloudhsm > key list --verbose --max-items 2
{
 "error_code": 0,
 "data": {
 "matched_keys": [
 {
 "key-reference": "0x00000000000000030",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "98a6688d1d964ed7b45b9cec5c4b1909",
 "id": "",
 "check-value": "0xb28a46",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
```

```
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 32
 }
},
{
 "key-reference": "0x00000000000000042",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "4ad6cdcbc02044e09fa954143efde233",
 "id": "",
 "check-value": "0xc98104",
 "class": "secret-key",
 "encrypt": true,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
```

```

 "trusted": false,
 "unwrap": true,
 "verify": true,
 "wrap": true,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
},
"total_key_count": 1580,
"returned_key_count": 2,
"next_token": "2"
}
}

```

若要顯示接下來的兩個金鑰，可以進行後續呼叫：

```

aws-cloudhsm > key list --verbose --max-items 2 --starting-token 2
{
 "error_code": 0,
 "data": {
 "matched_keys": [
 {
 "key-reference": "0x00000000000000081",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "6793b8439d044046982e5b895791e47f",
 "id": "",
 "check-value": "0x3f986f",

```

```

 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 32
 }
},
{
 "key-reference": "0x00000000000000089",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 }
 },
 "cluster-coverage": "full"
},
{
 "attributes": {
 "key-type": "aes",
 "label": "56b30fa05c6741faab8f606d3b7fe105",
 "id": "",
 "check-value": "0xe9201a",
 "class": "secret-key",

```

```

 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 32
 }
},
"total_key_count": 1580,
"returned_key_count": 2,
"next_token": "4"
}
}

```

如需更多有關 CloudHSM CLI 中金鑰篩選機制工作原理的演示範例，請參閱 [使用 CloudHSM CLI 篩選金鑰](#)。

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### #####

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要列出的相符索引鍵 (s)。



如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)

必要：否

### <MAX\_ITEMS>

要在命令輸出中傳回的總項目數。若可傳回的總項目數超過指定值，會在命令的輸出中提供 next-token。若要繼續分頁，請在後續 starting-token 命令引數中提供 next-token 值。

必要：否

### <STARTING\_TOKEN>

用以指定分頁開始位置的字符。這是來自先前已截斷回應的 next-token。

必要：否

### <VERBOSE>

如已包含，則會列印每個相符金鑰的所有屬性和金鑰資訊。根據預設，每個相符金鑰僅顯示其金鑰參考和標籤屬性。管理員使用時，此旗標沒有作用。

必要：否

## 相關主題

- [使用 CloudHSM CLI 刪除金鑰](#)
- [使用 CloudHSM CLI 匯出非對稱金鑰](#)
- [使用 CloudHSM CLI 取消共用金鑰](#)
- [CloudHSM CLI 的金鑰屬性](#)
- [使用 CloudHSM CLI 篩選金鑰](#)

## 使用 CloudHSM CLI 複寫金鑰

在 CloudHSM CLI 中使用 key replicate 命令，將金鑰從來源 AWS CloudHSM 叢集複寫到目的地 AWS CloudHSM 叢集。

## 使用者類型

下列類型的使用者可以執行此命令。

- 管理員 (COs)

- 加密使用者 (CU)

 Note

加密 使用者必須擁有金鑰才能使用此命令。

## 要求

- 來源和目的地叢集必須是複製。這表示一個是從另一個備份建立的，或者兩者都是從通用備份建立的。如需詳細資訊，請參閱[從備份建立叢集](#)。
- 金鑰的擁有者必須存在於目的地叢集上。此外，如果與任何使用者共用金鑰，這些使用者也必須存在於目的地叢集上。
- 若要執行此命令，您必須以加密使用者或來源和目的地叢集上的管理員身分登入。
  - 在單一命令模式中，命令將使用 CLOUDHSM\_PIN 和 CLOUDHSM\_ROLE 環境變數在來源叢集上進行驗證。如需詳細資訊，請參閱[單一命令模式](#)。若要提供目的地叢集的登入資料，您需要設定兩個額外的環境變數：DESTINATION\_CLOUDHSM\_PIN 和 DESTINATION\_CLOUDHSM\_ROLE：

```
$ export DESTINATION_CLOUDHSM_ROLE=<role>
```

```
$ export DESTINATION_CLOUDHSM_PIN=<username:password>
```

- 在互動式模式中，使用者需要明確登入來源和目的地叢集。

## 語法

```
aws-cloudhsm > help key replicate
```

Replicate a key from a source to a destination cluster

Usage: key replicate --filter [<FILTER>...] --source-cluster-id <SOURCE\_CLUSTER\_ID> --destination-cluster-id <DESTINATION\_CLUSTER\_ID>

Options:

```
--filter [<FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select matching key on the source cluster

```
--source-cluster-id <SOURCE_CLUSTER_ID>
```

Source cluster ID

```
--destination-cluster-id <DESTINATION_CLUSTER_ID>
 Destination cluster ID
-h, --help
 Print help
```

## 範例

### Example 範例：複寫金鑰

此命令會將金鑰從來源叢集與 複寫到複製的目的地叢集。以下範例示範在兩個叢集上以加密使用者身分登入時的輸出。

```
crypto-user-1@cluster-1234abcdefg > key replicate \
 --filter attr.label=example-key \
 --source-cluster-id cluster-1234abcdefg \
 --destination-cluster-id cluster-2345bcdefgh
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000000300006",
 "key-info": {
 "key-owners": [
 {
 "username": "crypto-user-1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "example-key",
 "id": "0x",
 "check-value": "0x5e118e",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
```

```

 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": true,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
},
"message": "Successfully replicated key"
}
}

```

## 引數

### #####

索引鍵參考 ( 例如 key-reference=0xabc) 或以 形式分隔的索引鍵屬性清單attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取來源叢集上的相符索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)

必要：是

### <SOURCE\_CLUSTER\_ID>

來源叢集 ID。

必要：是

### <DESTINATION\_CLUSTER\_ID>

目的地叢集 ID。

必要：是

## 相關主題

- [使用 CloudHSM CLI 連線至多個叢集](#)

### 使用 CloudHSM CLI 設定金鑰的屬性

使用 CloudHSM CLI 中的 `key set-attribute` 命令來設定 AWS CloudHSM 叢集中金鑰的屬性。只有建立金鑰並因此擁有金鑰的加密使用者才能變更金鑰的屬性。

如需可在 CloudHSM CLI 中使用的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

### 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU) 可以執行此命令。
- 管理員可設定受信任的屬性。

### 要求

若要執行此命令，必須以 CU 的身分登入。若要設定受信任屬性，您必須以管理員使用者身分登入。

### 語法

```
aws-cloudhsm > help key set-attribute
```

```
Set an attribute for a key in the HSM cluster
```

```
Usage: cloudhsm-cli key set-attribute [OPTIONS] --filter [<FILTER>...] --
name <KEY_ATTRIBUTE> --value <KEY_ATTRIBUTE_VALUE>
```

Options:

```
 --cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in
the config file to run the operation against. If not provided, will fall back to the
value provided when interactive mode was started, or error
 --filter [<FILTER>...] Key reference (e.g. key-
reference=0xabc) or space separated list of key attributes in the form of
attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a matching key to modify
 --name <KEY_ATTRIBUTE> Name of attribute to be set
 --value <KEY_ATTRIBUTE_VALUE>... Attribute value to be set
 --approval <APPROVAL> Filepath of signed quorum token file to approve
operation
```

`-h, --help`

Print help

## 範例：設定金鑰屬性

下列範例示範如何使用 `key set-attribute` 命令來設定標籤。

### Example

1. 使用帶有標籤 `my_key` 的金鑰，如下所示：

```
aws-cloudhsm > key set-attribute --filter attr.label=my_key --name encrypt --value false
{
 "error_code": 0,
 "data": {
 "message": "Attribute set successfully"
 }
}
```

2. 使用 `key list` 命令確認 `encrypt` 屬性已變更：

```
aws-cloudhsm > key list --filter attr.label=my_key --verbose
{
 "error_code": 0,
 "data": {
 "matched_keys": [
 {
 "key-reference": "0x000000000006400ec",
 "key-info": {
 "key-owners": [
 {
 "username": "bob",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
```

```

 "key-type": "aes",
 "label": "my_key",
 "id": "",
 "check-value": "0x6bd9f7",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": true,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": true,
 "unwrap": true,
 "verify": true,
 "wrap": true,
 "wrap-with-trusted": false,
 "key-length-bytes": 32
 }
},
"total_key_count": 1,
"returned_key_count": 1
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <KEY\_ATTRIBUTES>

指金鑰屬性的名稱。

必要：是

#####

索引鍵參考（例如 `key-reference=0xabc`）或以形式分隔的索引鍵屬性清單 `attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE`，以選取要刪除的相符索引鍵。

如需支援的 CloudHSM CLI 金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)

必要：否

**<KEY\_ATTRIBUTE\_VALUE>**

指金鑰屬性的名稱。

必要：是

**<KEY\_REFERENCE>**

金鑰的十六進位或十進位表示法。（例如金鑰控制代碼）。

必要：否

**<APPROVAL>**

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [使用 CloudHSM CLI 篩選金鑰](#)
- [CloudHSM CLI 的金鑰屬性](#)

## 使用 CloudHSM CLI 共用金鑰

在 CloudHSM CLI 中使用 `key share` 命令，與 AWS CloudHSM 叢集中的其他 CUs 共用金鑰。

只有建立金鑰並因此擁有金鑰的加密使用者才能共用金鑰。共用金鑰的使用者可以在密碼編譯操作中使用此金鑰，但無法刪除、匯出、共用金鑰或取消共用金鑰。此外，這些使用者無法變更 [金鑰屬性](#)。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)



## 要求

若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key share
```

Share a key in the HSM cluster with another user

Usage: key share --filter [**<FILTER>**...] --username **<USERNAME>** --role **<ROLE>**

Options:

**--cluster-id <CLUSTER\_ID>**

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

**--filter [**<FILTER>**...]**

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key for sharing

**--username <USERNAME>**

A username with which the key will be shared

**--role <ROLE>**

Role the user has in the cluster

Possible values:

- crypto-user: A CryptoUser has the ability to manage and use keys
- admin: An Admin has the ability to manage user accounts

**--approval <APPROVAL>**

Filepath of signed quorum token file to approve operation

**-h, --help**

Print help (see a summary with '-h')

## 範例：與另一個加密使用者共用金鑰

下列範例顯示如何使用 key share 命令與加密使用者 alice 共用金鑰。

## Example

1. 執行 key share 命令與 alice 共用金鑰。

```
aws-cloudhsm > key share --filter attr.label="rsa_key_to_share" attr.class=private-
key --username alice --role crypto-user
{
 "error_code": 0,
 "data": {
 "message": "Key shared successfully"
 }
}
```

2. 執行 key list 命令。

```
aws-cloudhsm > key list --filter attr.label="rsa_key_to_share" attr.class=private-
key --verbose
{
 "error_code": 0,
 "data": {
 "matched_keys": [
 {
 "key-reference": "0x000000000001c0686",
 "key-info": {
 "key-owners": [
 {
 "username": "cu3",
 "key-coverage": "full"
 }
],
 "shared-users": [
 {
 "username": "cu2",
 "key-coverage": "full"
 },
 {
 "username": "cu1",
 "key-coverage": "full"
 },
 {
 "username": "cu4",
 "key-coverage": "full"
 }
]
 }
 }
]
 }
}
```

```
{
 "username": "cu5",
 "key-coverage": "full"
},
{
 "username": "cu6",
 "key-coverage": "full"
},
{
 "username": "cu7",
 "key-coverage": "full"
},
{
 "username": "alice",
 "key-coverage": "full"
}
],
"key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
},
"cluster-coverage": "full"
},
"attributes": {
 "key-type": "rsa",
 "label": "rsa_key_to_share",
 "id": "",
 "check-value": "0xae8ff0",
 "class": "private-key",
 "encrypt": false,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": true,
```

```

 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 1219,
 "public-exponent": "0x010001",
 "modulus":
 "0xa8855cba933cec0c21a4df0450ec31675c024f3e65b2b215a53d2bda6dcd191f75729150b59b4d86df58254
 "modulus-size-bits": 2048
 }
}
],
"total_key_count": 1,
"returned_key_count": 1
}
}

```

3. 以上列表中，驗證 alice 在列表 shared-users 中

引數

**<CLUSTER\_ID>**

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

**#####**

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要刪除的相符索引鍵。

如需支援的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：是

**<USERNAME>**

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。在此命令中，使用者名稱不區分大小寫，使用者名稱始終以小寫顯示。

必要：是

**<ROLE>**

指定指派給此使用者的角色。此為必要參數。若要取得使用者的角色，請使用使用者清單命令。如需 HSM 上使用者類型的詳細資訊，請參閱 [CloudHSM CLI 的 HSM 使用者類型](#)。

必要：是

**<APPROVAL>**

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在金鑰的金鑰管理服務規定人數值大於 1 時才需要。

**相關主題**

- [使用 CloudHSM CLI 篩選金鑰](#)
- [CloudHSM CLI 的金鑰屬性](#)

**使用 CloudHSM CLI 取消共用金鑰**

使用 CloudHSM CLI 中的 `key unshare` 命令，取消與 AWS CloudHSM 叢集中其他 CUs 共用金鑰。

只有建立金鑰並因此擁有金鑰的加密使用者才能取消共用金鑰。共用金鑰的使用者可以在密碼編譯操作中使用此金鑰，但無法刪除、匯出、共用金鑰或取消共用金鑰。此外，這些使用者無法變更 [金鑰屬性](#)。

**使用者類型**

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

**要求**

若要執行此命令，必須以 CU 的身分登入。

**語法**

```
aws-cloudhsm > help key unshare
Unshare a key in the HSM cluster with another user

Usage: key unshare --filter [<FILTER>...] --username <USERNAME> --role <ROLE>

Options:
```

`--cluster-id <CLUSTER_ID>`

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

`--filter [<FILTER>...]`

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a matching key for unsharing

`--username <USERNAME>`

A username with which the key will be unshared

`--role <ROLE>`

Role the user has in the cluster

Possible values:

- crypto-user: A CryptoUser has the ability to manage and use keys
- admin: An Admin has the ability to manage user accounts

`--approval <APPROVAL>`

Filepath of signed quorum token file to approve operation

`-h, --help`

Print help (see a summary with '-h')

範例：取消與另一個加密使用者共用金鑰

下列範例顯示如何使用 key unshare 命令取消與加密使用者 alice 共用的金鑰。

Example

1. 執行 key list 命令並篩選出您想取消與 alice 共用的金鑰。

```
aws-cloudhsm > key list --filter attr.label="rsa_key_to_share" attr.class=private-
key --verbose
{
 "error_code": 0,
 "data": {
 "matched_keys": [
 {
 "key-reference": "0x000000000001c0686",
 "key-info": {
 "key-owners": [
```

```
{
 "username": "cu3",
 "key-coverage": "full"
},
"shared-users": [
 {
 "username": "cu2",
 "key-coverage": "full"
 },
 {
 "username": "cu1",
 "key-coverage": "full"
 },
 {
 "username": "cu4",
 "key-coverage": "full"
 },
 {
 "username": "cu5",
 "key-coverage": "full"
 },
 {
 "username": "cu6",
 "key-coverage": "full"
 },
 {
 "username": "cu7",
 "key-coverage": "full"
 },
 {
 "username": "alice",
 "key-coverage": "full"
 }
],
"key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
},
"cluster-coverage": "full"
},
"attributes": {
 "key-type": "rsa",
 "label": "rsa_key_to_share",
```

```

 "id": "",
 "check-value": "0xae8ff0",
 "class": "private-key",
 "encrypt": false,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": true,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 1219,
 "public-exponent": "0x010001",
 "modulus":
"0xa8855cba933cec0c21a4df0450ec31675c024f3e65b2b215a53d2bda6dcd191f75729150b59b4d86df58254
 "modulus-size-bits": 2048
 }
],
 "total_key_count": 1,
 "returned_key_count": 1
}

```

2. 確認 `alice` 在 `shared-users` 輸出中，並運行下列 `key unshare` 命令以取消與 `alice` 共用的金鑰。

```

aws-cloudhsm > key unshare --filter attr.label="rsa_key_to_share"
attr.class=private-key --username alice --role crypto-user
{
 "error_code": 0,
 "data": {
 "message": "Key unshared successfully"
 }
}

```



```
}
}
```

3. 再次執行 `key list` 命令以確認已取消與 `alice` 共用該金鑰。

```
aws-cloudhsm > key list --filter attr.label="rsa_key_to_share" attr.class=private-
key --verbose
{
 "error_code": 0,
 "data": {
 "matched_keys": [
 {
 "key-reference": "0x000000000001c0686",
 "key-info": {
 "key-owners": [
 {
 "username": "cu3",
 "key-coverage": "full"
 }
],
 "shared-users": [
 {
 "username": "cu2",
 "key-coverage": "full"
 },
 {
 "username": "cu1",
 "key-coverage": "full"
 },
 {
 "username": "cu4",
 "key-coverage": "full"
 },
 {
 "username": "cu5",
 "key-coverage": "full"
 },
 {
 "username": "cu6",
 "key-coverage": "full"
 },
 {
 "username": "cu7",
 "key-coverage": "full"
 }
]
 }
 }
]
 }
}
```

```

 },
],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
},
"attributes": {
 "key-type": "rsa",
 "label": "rsa_key_to_share",
 "id": "",
 "check-value": "0xae8ff0",
 "class": "private-key",
 "encrypt": false,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": true,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 1219,
 "public-exponent": "0x010001",
 "modulus":
"0xa8855cba933cec0c21a4df0450ec31675c024f3e65b2b215a53d2bda6dcd191f75729150b59b4d86df58254
 "modulus-size-bits": 2048
 }
}
],
"total_key_count": 1,
"returned_key_count": 1
}

```

```
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### #####

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要刪除的相符索引鍵。

如需支援的金鑰屬性清單，請參閱 [CloudHSM CLI 的金鑰屬性](#)。

必要：是

### <USERNAME>

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。在此命令中，使用者名稱不區分大小寫，使用者名稱始終以小寫顯示。

必要：是

### <ROLE>

指定指派給此使用者的角色。此為必要參數。若要取得使用者的角色，請使用使用者清單命令。如需 HSM 上使用者類型的詳細資訊，請參閱 [CloudHSM CLI 的 HSM 使用者類型](#)。

必要：是

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [使用 CloudHSM CLI 篩選金鑰](#)
- [CloudHSM CLI 的金鑰屬性](#)

## CloudHSM CLI 中的金鑰展開命令

CloudHSM CLI 中的 `key unwrap` 父命令會將加密（包裝）對稱或非對稱私有金鑰從檔案匯入 HSM。此命令旨在匯入由 [CloudHSM CLI 中的金鑰包裝命令](#) 命令包裝的加密金鑰，但也可以用來取消包裝與其他工具包裝的金鑰。不過，在這些情況下，我們建議您使用 PKCS#11 或 JCE 軟體程式庫來取消包裝金鑰。

- [aes-gcm](#)
- [aes-no-pad](#)
- [aes-pkcs5-pad](#)
- [aes-zero-pad](#)
- [cloudhsm-aes-gcm](#)
- [rsa-aes](#)
- [rsa-oaep](#)
- [rsa-pkcs](#)

### 使用 CloudHSM CLI 以 AES-GCM 取消包裝金鑰

在 CloudHSM CLI 中使用 `key unwrap aes-gcm` 命令，使用 AES 包裝金鑰和取消包裝機制，將承載金鑰 AES-GCM 取消包裝到叢集中。

未包裝金鑰的使用方式與產生的金鑰相同 AWS CloudHSM。若要表示它們不是在本機產生，其 `local` 屬性會設定為 `false`。

若要使用 `key unwrap aes-gcm` 命令，您必須在 AWS CloudHSM 叢集中具有 AES 包裝金鑰，且其 `unwrap` 屬性必須設定為 `true`。

### 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

### 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key unwrap aes-gcm
```

```
Usage: key unwrap aes-gcm [OPTIONS] --filter [<FILTER>...] --tag-length-bits
<TAG_LENGTH_BITS> --key-type-class <KEY_TYPE_CLASS> --label <LABEL> --iv <IV> <--
data-path <DATA_PATH>|--data <DATA>>
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--filter [<FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a key to unwrap with

```
--data-path <DATA_PATH>
```

Path to the binary file containing the wrapped key data

```
--data <DATA>
```

Base64 encoded wrapped key data

```
--attributes [<UNWRAPPED_KEY_ATTRIBUTES>...]
```

Space separated list of key attributes in the form of KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE for the unwrapped key

```
--share-crypto-users [<SHARE_CRYPTO_USERS;...]
```

Space separated list of Crypto User usernames to share the unwrapped key with

```
--manage-key-quorum-value <MANAGE_KEY_QUORUM_VALUE;
```

The quorum value for key management operations for the unwrapped key

```
--use-key-quorum-value <USE_KEY_QUORUM_VALUE;
```

The quorum value for key usage operations for the unwrapped key

```
--aad <AAD>
```

Aes GCM Additional Authenticated Data (AAD) value, in hex

```
--tag-length-bits <TAG_LENGTH_BITS>
```

Aes GCM tag length in bits

```
--key-type-class <KEY_TYPE_CLASS>
```

Key type and class of wrapped key [possible values: aes, des3, ec-private, generic-secret, rsa-private]

```
--label <LABEL>
```

Label for the unwrapped key

```
--session
```

Creates a session key that exists only in the current session. The key cannot be recovered after the session ends

```
--iv <IV>
```

Initial value used to wrap the key, in hex

```
--approval <APPROVAL>
```

```

 Filepath of signed quorum token file to approve operation
-h, --help
 Print help

```

## 範例

這些範例示範如何使用 `key unwrap aes-gcm` 命令，其 `unwrap` 屬性值設為 `true` 的 AES 金鑰。

**Example 範例：**從 Base64 編碼的包裝金鑰資料中取消包裝承載金鑰

```

aws-cloudhsm > key unwrap aes-gcm --key-type-class aes --label aes-unwrapped
--filter attr.label=aes-example --tag-length-bits 64 --aad 0x10 --iv
0xf90613bb8e337ec0339aad21 --data xvslgrtg8kHrzrvekny97tLSieokpPwV8
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001808e4",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,

```

```

 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

Example 範例：取消包裝透過資料路徑提供的承載金鑰

```

aws-cloudhsm > key unwrap aes-gcm --key-type-class aes --label aes-unwrapped
--filter attr.label=aes-example --tag-length-bits 64 --aad 0x10 --iv
0xf90613bb8e337ec0339aad21 --data-path payload-key.pem
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001808e4",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {

```

```

 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### #####

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，以attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE選取要取消包裝的索引鍵。

必要：是



**<DATA\_PATH>**

包含包裝金鑰資料的二進位檔案路徑。

必要：是（除非透過 Base64 編碼資料提供）

**<DATA>**

Base64 編碼的包裝金鑰資料。

必要：是（除非透過資料路徑提供）

**<ATTRIBUTES>**

以的形式KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE為包裝金鑰以空格分隔的金鑰屬性清單。

必要：否

**<AAD>**

Aes GCM 其他已驗證資料 (AAD) 值，以十六進位表示。

必要：否

**<TAG\_LENGTH\_BITS>**

Aes GCM 標籤長度，以位元為單位。

必要：是

**<KEY\_TYPE\_CLASS>**

封裝金鑰的金鑰類型和類別【可能值：aes、des3、ec-private、generic-secret、rsa-private】。

必要：是

**<LABEL>**

未包裝金鑰的標籤。

必要：是

**<SESSION>**

建立僅存在於目前工作階段的工作階段金鑰。工作階段結束後，金鑰無法復原。

必要：否

**<IV>**

用來以十六進位包裝金鑰的初始值。

必要：否

**<APPROVAL>**

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在未包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

**相關主題**

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

**使用 CloudHSM CLI 以 AES-NO-PAD 取消包裝金鑰**

在 CloudHSM CLI 中使用 `key unwrap aes-no-pad` 命令，使用 AES 包裝金鑰和取消包裝機制，將承載金鑰 AES-NO-PAD 解包裝至 AWS CloudHSM 叢集。

未包裝金鑰的使用方式與產生的金鑰相同 AWS CloudHSM。若要表示它們不是在本機產生，其 `local` 屬性會設為 `false`。

若要使用 `key unwrap aes-no-pad` 命令，您必須在 AWS CloudHSM 叢集中具有 AES 包裝金鑰，且其 `unwrap` 屬性必須設定為 `true`。

**使用者類型**

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

**要求**

- 若要執行此命令，必須以 CU 的身分登入。

**語法**

```
aws-cloudhsm > help key unwrap aes-no-pad
```

```
Usage: key unwrap aes-no-pad [OPTIONS] --filter [<FILTER>...] --key-type-
class <KEY_TYPE_CLASS> --label <LABEL> <--data-path <DATA_PATH>|--data <DATA>>
```

#### Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--filter [<FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a key to unwrap with

```
--data-path <DATA_PATH>
```

Path to the binary file containing the wrapped key data

```
--data <DATA>
```

Base64 encoded wrapped key data

```
--attributes [<UNWRAPPED_KEY_ATTRIBUTES>...]
```

Space separated list of key attributes in the form of KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE for the unwrapped key

```
--share-crypto-users [<SHARE_CRYPTO_USERS>...]
```

Space separated list of Crypto User usernames to share the unwrapped key with

```
--manage-key-quorum-value <MANAGE_KEY_QUORUM_VALUE>;
```

The quorum value for key management operations for the unwrapped key

```
--use-key-quorum-value <USE_KEY_QUORUM_VALUE>;
```

The quorum value for key usage operations for the unwrapped key

```
--key-type-class <KEY_TYPE_CLASS>
```

Key type and class of wrapped key [possible values: aes, des3, ec-private, generic-secret, rsa-private]

```
--label <LABEL>
```

Label for the unwrapped key

```
--session
```

Creates a session key that exists only in the current session. The key cannot be recovered after the session ends

```
--approval <APPROVAL>
```

Filepath of signed quorum token file to approve operation

```
-h, --help
```

Print help

## 範例

這些範例示範如何使用 key unwrap aes-no-pad命令，其unwrap屬性值設為的 AES 金鑰true。

**Example 範例：從 Base64 編碼的包裝金鑰資料中取消包裝承載金鑰**

```
aws-cloudhsm > key unwrap aes-no-pad --key-type-class aes --label aes-unwrapped --
filter attr.label=aes-example --data eXK3PMA0nKM9y3YX6brbhtMoC060E0H9
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001c08ec",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
```

```

 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

### Example 範例：取消包裝透過資料路徑提供的承載金鑰

```

aws-cloudhsm > key unwrap aes-no-pad --key-type-class aes --label aes-unwrapped --
filter attr.label=aes-example --data-path payload-key.pem
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001c08ec",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,

```

```

 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### #####

索引鍵參考（例如 key-reference=0xabc）或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要取消包裝的索引鍵。

必要：是

### <DATA\_PATH>

包含包裝金鑰資料的二進位檔案路徑。

必要：是（除非透過 Base64 編碼資料提供）

### <DATA>

Base64 編碼的包裝金鑰資料。

必要：是（除非透過資料路徑提供）

### <ATTRIBUTES>

以的形式KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE為包裝金鑰以空格分隔的金鑰屬性清單。

必要：否

### <KEY\_TYPE\_CLASS>

封裝金鑰的金鑰類型和類別【可能值：aes、des3、ec-private、generic-secret、rsa-private】。

必要：是

### <LABEL>

未包裝金鑰的標籤。

必要：是

### <SESSION>

建立僅存在於目前工作階段的工作階段金鑰。工作階段結束後，金鑰無法復原。

必要：否

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在未包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

## 使用 CloudHSM CLI 使用 AES-PKCS5-PAD 取消包裝金鑰

在 CloudHSM CLI 中使用 key unwrap aes-pkcs5-pad命令，使用 AES 包裝金鑰和AES-PKCS5-PAD取消包裝機制來取消包裝承載金鑰。

未包裝金鑰的使用方式與產生的金鑰相同 AWS CloudHSM。若要表示它們不是在本機產生，其local屬性會設為 false。

若要使用 `key unwrap aes-pkcs5-pad` 命令，您必須在 AWS CloudHSM 叢集中具有 AES 包裝金鑰，且其 `unwrap` 屬性必須設定為 `true`。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key unwrap aes-pkcs5-pad
```

```
Usage: key unwrap aes-pkcs5-pad [OPTIONS] --filter [<FILTER>...] --key-type-
class <KEY_TYPE_CLASS> --label <LABEL> <--data-path <DATA_PATH>|--data <DATA>>
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--filter [<FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a key to unwrap with

```
--data-path <DATA_PATH>
```

Path to the binary file containing the wrapped key data

```
--data <DATA>
```

Base64 encoded wrapped key data

```
--attributes [<UNWRAPPED_KEY_ATTRIBUTES>...]
```

Space separated list of key attributes in the form of KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE for the unwrapped key

```
--share-crypto-users [<SHARE_CRYPTO_USERS>...]
```

Space separated list of Crypto User usernames to share the unwrapped key with

```
--manage-key-quorum-value <MANAGE_KEY_QUORUM_VALUE>;
```

The quorum value for key management operations for the unwrapped key

```
--use-key-quorum-value <USE_KEY_QUORUM_VALUE>;
```

The quorum value for key usage operations for the unwrapped key

```
--key-type-class <KEY_TYPE_CLASS>
```



```

 Key type and class of wrapped key [possible values: aes, des3, ec-private,
generic-secret, rsa-private]
 --label <LABEL>
 Label for the unwrapped key
 --session
 Creates a session key that exists only in the current session. The key cannot
be recovered after the session ends
 --approval <APPROVAL>
 Filepath of signed quorum token file to approve operation
-h, --help
 Print help

```

## 範例

這些範例示範如何使用 `key unwrap aes-pkcs5-pad` 命令，其 `unwrap` 屬性值設為 `true` 的 AES 金鑰。

Example 範例：從 Base64 編碼的包裝金鑰資料中取消包裝承載金鑰

```

aws-cloudhsm > key unwrap aes-pkcs5-pad --key-type-class aes --label aes-unwrapped --
filter attr.label=aes-example --data MbuYNresf0KyGNnxKwen88nSfX+uUE/0qmGofSisicY=
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001c08e3",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",

```

```

 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

### Example 範例：取消包裝透過資料路徑提供的承載金鑰

```

aws-cloudhsm > key unwrap aes-pkcs5-pad --key-type-class aes --label aes-unwrapped --
filter attr.label=aes-example --data-path payload-key.pem
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001c08e3",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {

```

```

 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
},
"attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
}
}
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

**#####**

索引鍵參考 ( 例如 `key-reference=0xabc`) 或以空格分隔的索引鍵屬性清單，  
以 `attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` 選取要取消包裝的索引鍵。

必要：是

**<DATA\_PATH>**

包含包裝金鑰資料的二進位檔案路徑。

必要：是 ( 除非透過 Base64 編碼資料提供 )

**<DATA>**

Base64 編碼的包裝金鑰資料。

必要：是 ( 除非透過資料路徑提供 )

**<ATTRIBUTES>**

以 的形式 `KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` 為包裝金鑰以空格分隔的金鑰屬性清單。

必要：否

**<KEY\_TYPE\_CLASS>**

封裝金鑰的金鑰類型和類別 【可能值：aes、des3、ec-private、generic-secret、rsa-private】。

必要：是

**<LABEL>**

未包裝金鑰的標籤。

必要：是

**<SESSION>**

建立僅存在於目前工作階段的工作階段金鑰。工作階段結束後，金鑰無法復原。

必要：否

**<APPROVAL>**

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在未包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

### 使用 CloudHSM CLI 使用 AES-ZERO-PAD 取消包裝金鑰

在 CloudHSM CLI 中使用 `key unwrap aes-zero-pad` 命令，使用 AES 包裝金鑰和取消包裝機制，將承載金鑰 AES-ZERO-PAD 解包裝至 AWS CloudHSM 叢集。

未包裝金鑰的使用方式與產生的金鑰相同 AWS CloudHSM。若要表示它們不是在本機產生，其 `local` 屬性會設為 `false`。

若要使用 `key unwrap aes-no-pad` 命令，您必須在 AWS CloudHSM 叢集中具有 AES 包裝金鑰，且其 `unwrap` 屬性必須設定為 `true`。

### 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

### 要求

- 若要執行此命令，必須以 CU 的身分登入。

### 語法

```
aws-cloudhsm > help key unwrap aes-zero-pad
Usage: key unwrap aes-zero-pad [OPTIONS] --filter [<FILTER>...] --key-type-
class <KEY_TYPE_CLASS> --label <LABEL> <--data-path <DATA_PATH>|--data <DATA>>

Options:
 --cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error
 --filter [<FILTER>...]
 Key reference (e.g. key-reference=0xabc) or space separated list of key
 attributes in the form of attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a key
 to unwrap with
```

```

--data-path <DATA_PATH>
 Path to the binary file containing the wrapped key data
--data <DATA>
 Base64 encoded wrapped key data
--attributes [<UNWRAPPED_KEY_ATTRIBUTES>...]
 Space separated list of key attributes in the form of
KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE for the unwrapped key
--share-crypto-users [<SHARE_CRYPTO_USERS>;...]
 Space separated list of Crypto User usernames to share the unwrapped key with
--manage-key-quorum-value <MANAGE_KEY_QUORUM_VALUE>;
 The quorum value for key management operations for the unwrapped key
--use-key-quorum-value <USE_KEY_QUORUM_VALUE>;
 The quorum value for key usage operations for the unwrapped key
--key-type-class <KEY_TYPE_CLASS>
 Key type and class of wrapped key [possible values: aes, des3, ec-private,
generic-secret, rsa-private]
--label <LABEL>
 Label for the unwrapped key
--session
 Creates a session key that exists only in the current session. The key cannot
be recovered after the session ends
--approval <APPROVAL>
 Filepath of signed quorum token file to approve operation
-h, --help
 Print help

```

## 範例

這些範例示範如何使用 `key unwrap aes-zero-pad` 命令，其 `unwrap` 屬性值設為 `true` 的 AES 金鑰。

Example 範例：從 Base64 編碼的包裝金鑰資料中取消包裝承載金鑰

```

aws-cloudhsm > key unwrap aes-zero-pad --key-type-class aes --label aes-unwrapped --
filter attr.label=aes-example --data L1wVlL/YeBNVAw6Mpk3owFJZXBzDL0nt
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001c08e7",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
]
 }
 }
 }
}

```

```

 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
},
"attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
}
}
}
}

```

Example 範例：取消包裝透過資料路徑提供的承載金鑰

```
aws-cloudhsm > key unwrap aes-zero-pad --key-type-class aes --label aes-unwrapped --
filter attr.label=aes-example --data-path payload-key.pem
```

```
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001c08e7",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
 }
 }
}
```



```

 }
 }
}
}

```

引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

#####

索引鍵參考（例如 key-reference=0xabc）或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要取消包裝的索引鍵。

必要：是

### <DATA\_PATH>

包含包裝金鑰資料的二進位檔案路徑。

必要：是（除非透過 Base64 編碼資料提供）

### <DATA>

Base64 編碼的包裝金鑰資料。

必要：是（除非透過資料路徑提供）

### <ATTRIBUTES>

以的形式 KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 為包裝金鑰以空格分隔的金鑰屬性清單。

必要：否

### <KEY\_TYPE\_CLASS>

封裝金鑰的金鑰類型和類別【可能值：aes、des3、ec-private、generic-secret、rsa-private】。

必要：是

**<LABEL>**

未包裝金鑰的標籤。

必要：是

**<SESSION>**

建立僅存在於目前工作階段的工作階段金鑰。工作階段結束後，金鑰無法復原。

必要：否

**<APPROVAL>**

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在未包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

**相關主題**

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

**使用 CloudHSM CLI 以 CLOUDHSM-AES-GCM 取消包裝金鑰**

在 CloudHSM CLI 中使用 `key unwrap cloudhsm-aes-gcm` 命令，使用 AES 包裝金鑰和取消包裝機制，將承載金鑰 CLOUDHSM-AES-GCM 解包裝至 AWS CloudHSM 叢集。

未包裝金鑰的使用方式與產生的金鑰相同 AWS CloudHSM。若要表示它們不是在本機產生，其 `local` 屬性會設定為 `false`。

若要使用 `key unwrap cloudhsm-aes-gcm` 命令，您必須在 AWS CloudHSM 叢集中具有 AES 包裝金鑰，且其 `unwrap` 屬性必須設定為 `true`。

**使用者類型**

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

**要求**

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key unwrap cloudhsm-aes-gcm
```

```
Usage: key unwrap cloudhsm-aes-gcm [OPTIONS] --filter [<FILTER>...] --tag-length-bits <TAG_LENGTH_BITS> --key-type-class <KEY_TYPE_CLASS> --label <LABEL> <--data-path <DATA_PATH>|--data <DATA>>
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--filter [<FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a key to unwrap with

```
--data-path <DATA_PATH>
```

Path to the binary file containing the wrapped key data

```
--data <DATA>
```

Base64 encoded wrapped key data

```
--attributes [<UNWRAPPED_KEY_ATTRIBUTES>...]
```

Space separated list of key attributes in the form of KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE for the unwrapped key

```
--share-crypto-users [<SHARE_CRYPTO_USERS>...]
```

Space separated list of Crypto User usernames to share the unwrapped key with

```
--manage-key-quorum-value <MANAGE_KEY_QUORUM_VALUE>;
```

The quorum value for key management operations for the unwrapped key

```
--use-key-quorum-value <USE_KEY_QUORUM_VALUE>;
```

The quorum value for key usage operations for the unwrapped key

```
--aad <AAD>
```

Aes GCM Additional Authenticated Data (AAD) value, in hex

```
--tag-length-bits <TAG_LENGTH_BITS>
```

Aes GCM tag length in bits

```
--key-type-class <KEY_TYPE_CLASS>
```

Key type and class of wrapped key [possible values: aes, des3, ec-private, generic-secret, rsa-private]

```
--label <LABEL>
```

Label for the unwrapped key

```
--session
```

Creates a session key that exists only in the current session. The key cannot be recovered after the session ends

```
--approval <APPROVAL>
```

Filepath of signed quorum token file to approve operation

```
-h, --help
```

Print help

## 範例

這些範例示範如何使用 `key unwrap cloudhsm-aes-gcm` 命令，其 `unwrap` 屬性值設為 `true` 的 AES 金鑰。

Example 範例：從 Base64 編碼的包裝金鑰資料中取消包裝承載金鑰

```
aws-cloudhsm > key unwrap cloudhsm-aes-gcm --key-type-class aes --label aes-
unwrapped --filter attr.label=aes-example --tag-length-bits 64 --aad 0x10 --data
6Rn8nkjEriDYlnP3P8nPkYQ8hp10EJ899zsrF+aTB0i/f1lZ
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001408e8",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
```

```

 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

Example 範例：取消包裝透過資料路徑提供的承載金鑰

```

aws-cloudhsm > key unwrap cloudhsm-aes-gcm --key-type-class aes --label aes-unwrapped
--filter attr.label=aes-example --tag-length-bits 64 --aad 0x10 --data-path payload-
key.pem
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001408e8",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {

```

```

 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### #####

索引鍵參考（例如 key-reference=0xabc）或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要取消包裝的索引鍵。

必要：是

**<DATA\_PATH>**

包含包裝金鑰資料的二進位檔案路徑。

必要：是（除非透過 Base64 編碼資料提供）

**<DATA>**

Base64 編碼的包裝金鑰資料。

必要：是（除非透過資料路徑提供）

**<ATTRIBUTES>**

以的形式KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE為包裝金鑰以空格分隔的金鑰屬性清單。

必要：否

**<AAD>**

Aes GCM 其他已驗證資料 (AAD) 值，以十六進位表示。

必要：否

**<TAG\_LENGTH\_BITS>**

Aes GCM 標籤長度，以位元為單位。

必要：是

**<KEY\_TYPE\_CLASS>**

封裝金鑰的金鑰類型和類別【可能值：aes、des3、ec-private、generic-secret、rsa-private】。

必要：是

**<LABEL>**

未包裝金鑰的標籤。

必要：是

**<SESSION>**

建立僅存在於目前工作階段的工作階段金鑰。工作階段結束後，金鑰無法復原。

必要：否

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在未包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

### 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

### 使用 CloudHSM CLI 以 RSA-AES 取消包裝金鑰

在 CloudHSM CLI 中使用 `key unwrap rsa-aes` 命令，使用 RSA 私有金鑰和 RSA-AES 取消包裝機制來取消包裝承載金鑰。

未包裝金鑰的使用方式與產生的金鑰相同 AWS CloudHSM。若要表示它們不是在本機產生，其 `local` 屬性會設定為 `false`。

若要使用 `key unwrap rsa-aes`，您必須在 AWS CloudHSM 叢集中擁有 RSA 公有包裝金鑰的 RSA 私有金鑰，且其 `unwrap` 屬性必須設定為 `true`。

### 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

### 要求

- 若要執行此命令，必須以 CU 的身分登入。

### 語法

```
aws-cloudhsm > help key unwrap rsa-aes
Usage: key unwrap rsa-aes [OPTIONS] --filter [<FILTER>...] --hash-
function <HASH_FUNCTION> --mgf <MGF> --key-type-class <KEY_TYPE_CLASS> --label <LABEL>
<--data-path <DATA_PATH>|--data <DATA>>
```



## Options:

```

--cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error
--filter [<FILTER>...]
 Key reference (e.g. key-reference=0xabc) or space separated list of key
 attributes in the form of attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a key
 to unwrap with
--data-path <DATA_PATH>
 Path to the binary file containing the wrapped key data
--data <DATA>
 Base64 encoded wrapped key data
--attributes [<UNWRAPPED_KEY_ATTRIBUTES>...]
 Space separated list of key attributes in the form of
 KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE for the unwrapped key
--share-crypto-users [<SHARE_CRYPTO_USERS>...]
 Space separated list of Crypto User usernames to share the unwrapped key with
--manage-key-quorum-value <MANAGE_KEY_QUORUM_VALUE>;
 The quorum value for key management operations for the unwrapped key
--use-key-quorum-value <USE_KEY_QUORUM_VALUE>;
 The quorum value for key usage operations for the unwrapped key
--hash-function <HASH_FUNCTION>
 Hash algorithm [possible values: sha1, sha224, sha256, sha384, sha512]
--mgf <MGF>
 Mask Generation Function algorithm [possible values: mgf1-sha1, mgf1-sha224,
 mgf1-sha256, mgf1-sha384, mgf1-sha512]
--key-type-class <KEY_TYPE_CLASS>
 Key type and class of wrapped key [possible values: aes, des3, ec-private,
 generic-secret, rsa-private]
--label <LABEL>
 Label for the unwrapped key
--session
 Creates a session key that exists only in the current session. The key cannot
 be recovered after the session ends
--approval <APPROVAL>
 Filepath of signed quorum token file to approve operation
-h, --help
 Print help

```

## 範例

這些範例示範如何使用 RSA 私有金鑰搭配 unwrap 屬性值設為 true 的 key unwrap rsa-aes 命令。

## Example 範例：從 Base64 編碼的包裝金鑰資料中取消包裝承載金鑰

```
aws-cloudhsm > key unwrap rsa-aes --key-type-class aes --label aes-unwrapped
--filter attr.label=rsa-private-key-example --hash-function sha256 --
mgf mgf1-sha256 --data HrSE1DEyLjIeyGdPa9R+ebiqB5TIJGyamPker31ZebPwRA
+NcerbAJ08DJ1lXPYgZcI21vIFSZJuWMEiWpe1R9D/5WSYgxLVKex30xCFqebtEzxbKuv4D0mU4meSofqREYvtb3EoIKwjy
+RL5WGxKe4nAboAkC5G07veI5yHL1SaKlssSJtTL/CFpbSLsAFuYbv/NUCWwMY5mwyVTCSlw+HlgKK
+5TH1MzBaSi8fpfyepLT8sHy2Q/VRl6ifb49p6m0KQFbRVvz/0WUd6l4d97BdgtaEz6ueg==
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001808e2",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,

```

```

 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

Example 範例：取消包裝透過資料路徑提供的承載金鑰

```

aws-cloudhsm > key unwrap rsa-aes --key-type-class aes --label aes-unwrapped --filter
attr.label=rsa-private-key-example --hash-function sha256 --mgf mgf1-sha256 --data-
path payload-key.pem
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x0000000000001808e2",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",

```

```

 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### #####

索引鍵參考（例如 key-reference=0xabc）或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要取消包裝的索引鍵。

必要：是

### <DATA\_PATH>

包含包裝金鑰資料的二進位檔案路徑。

必要：是（除非透過 Base64 編碼資料提供）

**<DATA>**

Base64 編碼的包裝金鑰資料。

必要：是（除非透過資料路徑提供）

**<ATTRIBUTES>**

以的形式KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE為包裝金鑰以空格分隔的金鑰屬性清單。

必要：否

**<KEY\_TYPE\_CLASS>**

封裝金鑰的金鑰類型和類別【可能值：aes、des3、ec-private、generic-secret、rsa-private】。

必要：是

**<HASH\_FUNCTION>**

指定雜湊函數。

有效值：

- sha1
- sha224
- sha256
- sha384
- sha512

必要：是

**<MGF>**

指定遮罩產生函數。

 Note

遮罩產生函數雜湊函數必須符合簽署機制雜湊函數。

有效值：

- mgf1-sha1
- mgf1-sha224
- mgf1-sha256
- mgf1-sha384
- mgf1-sha512

必要：是

### <LABEL>

未包裝金鑰的標籤。

必要：是

### <SESSION>

建立僅存在於目前工作階段的工作階段金鑰。工作階段結束後，金鑰無法復原。

必要：否

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在未包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

## 使用 CloudHSM CLI 以 RSA-OAEP 取消包裝金鑰

在 CloudHSM CLI 中使用 `key unwrap rsa-oaep` 命令，使用 RSA 私有金鑰和取消包裝機制來 RSA-OAEP 取消包裝承載金鑰。

未包裝金鑰的使用方式與產生的金鑰相同 AWS CloudHSM。為了表示它們不是在本機產生，其 `local` 屬性設定為 `false`。

若要使用 `key unwrap rsa-oaep` 命令，您必須在 AWS CloudHSM 叢集中具有 RSA 公有包裝金鑰的 RSA 私有金鑰，且其 `unwrap` 屬性必須設定為 `true`。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key unwrap rsa-oaep
```

```
Usage: key unwrap rsa-oaep [OPTIONS] --filter [<FILTER>...] --hash-
function <HASH_FUNCTION> --mgf <MGF> --key-type-class <KEY_TYPE_CLASS> --label <LABEL>
--data-path <DATA_PATH>|--data <DATA>
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--filter [<FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a key to unwrap with

```
--data-path <DATA_PATH>
```

Path to the binary file containing the wrapped key data

```
--data <DATA>
```

Base64 encoded wrapped key data

```
--attributes [<UNWRAPPED_KEY_ATTRIBUTES>...]
```

Space separated list of key attributes in the form of KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE for the unwrapped key

```
--share-crypto-users [<SHARE_CRYPTO_USERS>...]
```

Space separated list of Crypto User usernames to share the unwrapped key with

```
--manage-key-quorum-value <MANAGE_KEY_QUORUM_VALUE>;
```

The quorum value for key management operations for the unwrapped key

```
--use-key-quorum-value <USE_KEY_QUORUM_VALUE>;
```

The quorum value for key usage operations for the unwrapped key

```
--hash-function <HASH_FUNCTION>
```

Hash algorithm [possible values: sha1, sha224, sha256, sha384, sha512]

```
--mgf <MGF>
```

```

Mask Generation Function algorithm [possible values: mgf1-sha1, mgf1-sha224,
mgf1-sha256, mgf1-sha384, mgf1-sha512]
--key-type-class <KEY_TYPE_CLASS>
 Key type and class of wrapped key [possible values: aes, des3, ec-private,
generic-secret, rsa-private]
--label <LABEL>
 Label for the unwrapped key
--session
 Creates a session key that exists only in the current session. The key cannot
be recovered after the session ends
--approval <APPROVAL>
 Filepath of signed quorum token file to approve operation
-h, --help
 Print help

```

## 範例

這些範例示範如何使用 RSA 私有金鑰搭配 `unwrap` 屬性值設為 `true` 的 `key unwrap rsa-oaep` 命令。

Example 範例：從 Base64 編碼的包裝金鑰資料中取消包裝承載金鑰

```

aws-cloudhsm > key unwrap rsa-oaep --key-type-class aes --label aes-unwrapped --filter
attr.label=rsa-private-example-key --hash-function sha256 --mgf mgf1-sha256 --data
OjJe4msobPLz9TuSAdULEu17T5rMDWtS1LyBSkLbaZnYzzpdrhsbGLbwZJCtB/jGkDNdB4qyTA0QwEpggGf6v
+Yx6JcesNeKKNU8XZa1/YBoHC8noTGUSDi2qr+u2tDc84NPv6d+F2K00NXsSxMhmxzzNG/
gzTVIJh0uy/B1yHjGP4m0XoDZf5+7f5M1CjxBmz4Vva/wrWHGCSG0y0aWb1Ev0iHAI3UBdyKmU+/
My4xjfJv7WGGu3DFUUIZ06TihRtKQhUYU1M9u6NPF9riJJfHsk6QCUSZ9yWThDT9as6i7e3htnyDhIhGWaoK8JU855cN/
YNKAUqkNpC4FPL3iw==
{
 "data": {
 "key": {
 "key-reference": "0x000000000001808e9",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 }
 }
 }
 }
}

```



```

 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}
}

```

Example 範例：取消包裝透過資料路徑提供的承載金鑰

```

aws-cloudhsm > key unwrap rsa-oaep --key-type-class aes --label aes-unwrapped --filter
attr.label=rsa-private-example-key --hash-function sha256 --mgf mgf1-sha256 --data-
path payload-key.pem
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x0000000000001808e9",
 "key-info": {

```

```
"key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
"shared-users": [],
"key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
},
"cluster-coverage": "full"
},
"attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
}
}
}
```

## 引數

### <CLUSTER\_ID>

執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### #####

索引鍵參考（例如，key-reference=0xabc）或以形式分隔的索引鍵屬性清單attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要取消包裝的索引鍵。

必要：是

### <DATA\_PATH>

包含包裝金鑰資料的二進位檔案路徑。

必要：是（除非透過 Base64 編碼資料提供）

### <DATA>

Base64 編碼的包裝金鑰資料。

必要：是（除非透過資料路徑提供）

### <ATTRIBUTES>

以空格分隔的金鑰屬性清單，格式KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE為的包裝金鑰。

必要：否

### <KEY\_TYPE\_CLASS>

包裝金鑰的金鑰類型和類別【可能值：aes、des3、ec-private、generic-secret、rsa-private】。

必要：是

### <HASH\_FUNCTION>

指定雜湊函數。

有效值：

- sha1

- sha224
- sha256
- sha384
- sha512

必要：是

### <MGF>

指定遮罩產生函數。

#### Note

遮罩產生函數雜湊函數必須符合簽署機制雜湊函數。

有效值：

- mgf1-sha1
- mgf1-sha224
- mgf1-sha256
- mgf1-sha384
- mgf1-sha512

必要：是

### <LABEL>

未包裝金鑰的標籤。

必要：是

### <SESSION>

建立僅存在於目前工作階段的工作階段金鑰。工作階段結束後，金鑰無法復原。

必要：否

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在取消包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

## 使用 CloudHSM CLI 以 RSA-PKCS 取消包裝金鑰

在 CloudHSM CLI 中使用 `key unwrap rsa-pkcs` 命令，使用 RSA 私有金鑰和 RSA-PKCS 取消包裝機制來取消包裝承載金鑰。

未包裝金鑰的使用方式與產生的金鑰相同 AWS CloudHSM。若要表示它們不是在本機產生，其 `local` 屬性會設為 `false`。

若要使用金鑰 `unwrap rsa-pkcs` 命令，您必須在 AWS CloudHSM 叢集中具有 RSA 公有包裝金鑰的 RSA 私有金鑰，且其 `unwrap` 屬性必須設定為 `true`。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key unwrap rsa-pkcs
Usage: key unwrap rsa-pkcs [OPTIONS] --filter [<FILTER>...] --key-type-
class <KEY_TYPE_CLASS> --label <LABEL> <--data-path <DATA_PATH>|--data <DATA>>

Options:
 --cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error
 --filter [<FILTER>...]
 Key reference (e.g. key-reference=0xabc) or space separated list of key
 attributes in the form of attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a key
 to unwrap with
```

```

--data-path <DATA_PATH>
 Path to the binary file containing the wrapped key data
--data <DATA>
 Base64 encoded wrapped key data
--attributes [<UNWRAPPED_KEY_ATTRIBUTES>...]
 Space separated list of key attributes in the form of
KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE for the unwrapped key
--share-crypto-users [<SHARE_CRYPTO_USERS>;...]
 Space separated list of Crypto User usernames to share the unwrapped key with
--manage-key-quorum-value <MANAGE_KEY_QUORUM_VALUE>;
 The quorum value for key management operations for the unwrapped key
--use-key-quorum-value <USE_KEY_QUORUM_VALUE>;
 The quorum value for key usage operations for the unwrapped key
--key-type-class <KEY_TYPE_CLASS>
 Key type and class of wrapped key [possible values: aes, des3, ec-private,
generic-secret, rsa-private]
--label <LABEL>
 Label for the unwrapped key
--session
 Creates a session key that exists only in the current session. The key cannot
be recovered after the session ends
--approval <APPROVAL>
 Filepath of signed quorum token file to approve operation
-h, --help
 Print help

```

## 範例

這些範例示範如何使用 `key unwrap rsa-oaep` 命令，其 `unwrap` 屬性值設為 `true` 的 AES 金鑰。

Example 範例：從 Base64 編碼的包裝金鑰資料中取消包裝承載金鑰

```

aws-cloudhsm > key unwrap rsa-pkcs --key-type-class aes --label
aes-unwrapped --filter attr.label=rsa-private-key-example --data
am0Nc7+YE8FWs+5HvU7sIBcXVb24QA0165nbNAD+1bK+e18BpSfnaI3P+r8Dp+pLu1ofoUy/
vtzRjZoCiDofcz4EqCFnG14GdcJ1/3W/5WRvMatCa2d7cx02swaeZcjKsermPXYR01lG1fq6NskwMeeTkV8R7Rx9artFrs1
c3XdFJ2+0Bo94c6og/
yfPcp00obJlITCoXhtMRepSd040ggYq/6nUDuHCtJ86pPGnNahyr7+sAaSI3a5ECQLUjwaIARUCyoRh7EFK3qPXcg==
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001c08ef",
 "key-info": {

```

```
"key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
"shared-users": [],
"key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
},
"cluster-coverage": "full"
},
"attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
}
}
}
```

**Example 範例：取消包裝透過資料路徑提供的承載金鑰**

```
aws-cloudhsm > key unwrap rsa-pkcs --key-type-class aes --label aes-unwrapped --filter
attr.label=rsa-private-key-example --data-path payload-key.pem
{
 "error_code": 0,
 "data": {
 "key": {
 "key-reference": "0x000000000001c08ef",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "aes-unwrapped",
 "id": "0x",
 "check-value": "0x8d9099",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": false,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
```



```

 "verify": true,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
}
}
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### #####

索引鍵參考（例如 key-reference=0xabc）或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取要取消包裝的索引鍵。

必要：是

### <DATA\_PATH>

包含包裝金鑰資料的二進位檔案路徑。

必要：是（除非透過 Base64 編碼資料提供）

### <DATA>

Base64 編碼的包裝金鑰資料。

必要：是（除非透過資料路徑提供）

### <ATTRIBUTES>

以的形式 KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 為包裝金鑰以空格分隔的金鑰屬性清單。

必要：否

### <KEY\_TYPE\_CLASS>

封裝金鑰的金鑰類型和類別【可能值：aes、des3、ec-private、generic-secret、rsa-private】。

必要：是

### <LABEL>

未包裝金鑰的標籤。

必要：是

### <SESSION>

建立僅存在於目前工作階段的工作階段金鑰。工作階段結束後，金鑰無法復原。

必要：否

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在未包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

## CloudHSM CLI 中的金鑰包裝命令

CloudHSM CLI 中的 `key wrap` 命令會將對稱或非對稱私有金鑰的加密副本從硬體安全模組 (HSM) 匯出至 檔案。當您執行 `key wrap`，您可以指定兩件事：要匯出的金鑰和輸出檔案。要匯出的金鑰是 HSM 上的金鑰，它會加密（包裝）您要匯出的金鑰。

`key wrap` 命令不會從 HSM 移除金鑰，也不會阻止您在密碼編譯操作中使用金鑰。您可以多次匯出相同的金鑰。若要將加密的金鑰匯入回 HSM，請使用 [CloudHSM CLI 中的金鑰展開命令](#)。只有建立金鑰的加密使用者 (CU) 金鑰擁有者，才能包裝金鑰。與之共用金鑰的使用者只能在密碼編譯操作中使用金鑰。

`key wrap` 命令包含下列子命令：

- [aes-gcm](#)
- [aes-no-pad](#)
- [aes-pkcs5-pad](#)

- [aes-zero-pad](#)
- [cloudhsm-aes-gcm](#)
- [rsa-aes](#)
- [rsa-oaep](#)
- [rsa-pkcs](#)

## 使用 CloudHSM CLI 使用 AES-GCM 包裝金鑰

在 CloudHSM CLI 中使用 `key wrap aes-gcm` 命令，在硬體安全模組 (HSM) 和包裝機制上使用 AES 金鑰 AES-GCM 來包裝承載金鑰。承載金鑰的 `extractable` 屬性必須設定為 `true`。

只有金鑰擁有者，也就是建立金鑰的加密使用者 (CU)，才能包裝金鑰。共用金鑰的使用者可以在密碼編譯操作中使用金鑰。

若要使用 `key wrap aes-gcm` 命令，您必須先在 AWS CloudHSM 叢集中擁有 AES 金鑰。您可以產生 AES 金鑰來包裝 [使用 CloudHSM CLI 產生對稱 AES 金鑰](#) 命令，並將 `wrap` 屬性設定為 `true`。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key wrap aes-gcm
Usage: key wrap aes-gcm [OPTIONS] --payload-filter [<PAYLOAD_FILTER>...] --wrapping-
filter [<WRAPPING_FILTER>...] --tag-length-bits <TAG_LENGTH_BITS>

Options:
 --cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error
 --payload-filter [<PAYLOAD_FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a payload key

--wrapping-filter [**<WRAPPING\_FILTER>**...]

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a wrapping key

--path **<PATH>**

Path to the binary file where the wrapped key data will be saved

--wrapping-approval **<WRAPPING\_APPROVAL>**

File path of signed quorum token file to approve operation for wrapping key

--payload-approval **<PAYLOAD\_APPROVAL>**

File path of signed quorum token file to approve operation for payload key

--aad **<AAD>**

Aes GCM Additional Authenticated Data (AAD) value, in hex

--tag-length-bits **<TAG\_LENGTH\_BITS>**

Aes GCM tag length in bits

-h, --help

Print help

## 範例

此範例示範如何使用 AES 金鑰來使用 key wrap aes-gcm 命令。

## Example

```
aws-cloudhsm > key wrap aes-gcm --payload-filter attr.label=payload-key --wrapping-
filter attr.label=aes-example --tag-length-bits 64 --aad 0x10
{
 "error_code": 0,
 "data": {
 "payload_key_reference": "0x000000000001c08f1",
 "wrapping_key_reference": "0x000000000001c08ea",
 "iv": "0xf90613bb8e337ec0339aad21",
 "wrapped_key_data": "xvslgrtg8kHrzveky97tLSIeokpPwV8"
 }
}
```

## 引數

### **<CLUSTER\_ID>**

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

#### <PAYLOAD\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 以選取承載索引鍵。

必要：是

#### <PATH>

二進位檔案的路徑，其中會儲存包裝的金鑰資料。

必要：否

#### <WRAPPING\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 以選取包裝索引鍵。

必要：是

#### <AAD>

AES GCM 其他已驗證資料 (AAD) 值，以十六進位表示。

必要：否

#### <TAG\_LENGTH\_BITS>

以位元為單位的 AES GCM 標籤長度。

必要：是

#### <WRAPPING\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准包裝金鑰的操作。只有在包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

#### <PAYLOAD\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准承載金鑰的操作。只有在承載金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)

- [CloudHSM CLI 中的金鑰展開命令](#)

## 使用 CloudHSM CLI 使用 AES-NO-PAD 包裝金鑰

在 CloudHSM CLI 中使用 `key wrap aes-no-pad` 命令，在硬體安全模組 (HSM) 和包裝機制上使用 AES 金鑰 AES-NO-PAD 來包裝承載金鑰。承載金鑰的 `extractable` 屬性必須設定為 `true`。

只有金鑰擁有者，也就是建立金鑰的加密使用者 (CU)，才能包裝金鑰。共用金鑰的使用者可以在密碼編譯操作中使用金鑰。

若要使用 `key wrap aes-no-pad` 命令，您必須先在 AWS CloudHSM 叢集中擁有 AES 金鑰。您可以使用 [使用 CloudHSM CLI 產生對稱 AES 金鑰](#) 命令和 `wrap` 屬性設定為 `true` 來產生 AES 金鑰以進行包裝。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key wrap aes-no-pad
Usage: key wrap aes-no-pad [OPTIONS] --payload-filter [<PAYLOAD_FILTER>...] --wrapping-
filter [<WRAPPING_FILTER>...]

Options:
 --cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error
 --payload-filter [<PAYLOAD_FILTER>...]
 Key reference (e.g. key-reference=0xabc) or space separated list of key
 attributes in the form of attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a
 payload key
 --wrapping-filter [<WRAPPING_FILTER>...]
```

```

 Key reference (e.g. key-reference=0xabc) or space separated list of key
 attributes in the form of attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a
 wrapping key
 --path <PATH>
 Path to the binary file where the wrapped key data will be saved
 --wrapping-approval <WRAPPING_APPROVAL>
 File path of signed quorum token file to approve operation for wrapping key
 --payload-approval <PAYLOAD_APPROVAL>
 File path of signed quorum token file to approve operation for payload key
 -h, --help
 Print help

```

## 範例

此範例說明如何使用wrap屬性值設為 的 AES 金鑰來使用 key wrap aes-no-pad命令true。

## Example

```

aws-cloudhsm > key wrap aes-no-pad --payload-filter attr.label=payload-key --wrapping-
filter attr.label=aes-example
{
 "error_code": 0,
 "data": {
 "payload_key_reference": "0x000000000001c08f1",
 "wrapping_key_reference": "0x000000000001c08ea",
 "wrapped_key_data": "eXK3PMA0nKM9y3YX6brbhtMoC060E0H9"
 }
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <PAYLOAD\_FILTER>

索引鍵參考 ( 例如 key-reference=0xabc) 或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE以選取承載索引鍵。

必要：是

**<PATH>**

二進位檔案的路徑，其中會儲存包裝的金鑰資料。

必要：否

**<WRAPPING\_FILTER>**

索引鍵參考（例如 `key-reference=0xabc`）或以空格分隔的索引鍵屬性清單，格式為 `attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` 以選取包裝索引鍵。

必要：是

**<WRAPPING\_APPROVALR>**

指定已簽署規定人數字符檔案的檔案路徑，以核准包裝金鑰的操作。只有在包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

**<PAYLOAD\_APPROVALR>**

指定已簽署規定人數字符檔案的檔案路徑，以核准承載金鑰的操作。只有在承載金鑰的金鑰管理服務規定人數值大於 1 時才需要。

**相關主題**

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

**使用 CloudHSM CLI 使用 AES-PKCS5-PAD 包裝金鑰**

在 CloudHSM CLI 中使用 `key wrap aes-pkcs5-pad` 命令，在硬體安全模組 (HSM) 和包裝機制上使用 AES 金鑰 AES-PKCS5-PAD 來包裝承載金鑰。承載金鑰的 `extractable` 屬性必須設定為 `true`。

只有建立金鑰的加密使用者 (CU) 金鑰擁有者，才能包裝金鑰。共用金鑰的使用者可以在密碼編譯操作中使用金鑰。

若要使用 `key wrap aes-pkcs5-pad` 命令，您必須先在 AWS CloudHSM 叢集中擁有 AES 金鑰。您可以使用 [使用 CloudHSM CLI 產生對稱 AES 金鑰](#) 命令和設定為 `wrap` 屬性來產生 AES 金鑰以進行包裝 `true`。

**使用者類型**

下列類型的使用者可以執行此命令。



- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key wrap aes-pkcs5-pad
```

```
Usage: key wrap aes-pkcs5-pad [OPTIONS] --payload-filter [<PAYLOAD_FILTER>...] --
wrapping-filter [<WRAPPING_FILTER>...]
```

Options:

`--cluster-id <CLUSTER_ID>`

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

`--payload-filter [<PAYLOAD_FILTER>...]`

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a payload key

`--wrapping-filter [<WRAPPING_FILTER>...]`

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a wrapping key

`--path <PATH>`

Path to the binary file where the wrapped key data will be saved

`--wrapping-approval <WRAPPING_APPROVALR>`

File path of signed quorum token file to approve operation for wrapping key

`--payload-approval <PAYLOAD_APPROVALR>`

File path of signed quorum token file to approve operation for payload key

`-h, --help`

Print help

## 範例

此範例示範如何使用 key wrap aes-pkcs5-pad 命令，其 AES 金鑰的 wrap 屬性值設為 true。

## Example

```
aws-cloudhsm > key wrap aes-pkcs5-pad --payload-filter attr.label=payload-key --
wrapping-filter attr.label=aes-example
```

```
{
 "error_code": 0,
 "data": {
 "payload_key_reference": "0x000000000001c08f1",
 "wrapping_key_reference": "0x000000000001c08ea",
 "wrapped_key_data": "MbuYNresf0KyGNnxKWen88nSfX+uUE/0qmGofSisicY="
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <PAYLOAD\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取承載索引鍵。

必要：是

### <PATH>

儲存包裝金鑰資料的二進位檔案路徑。

必要：否

### <WRAPPING\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取包裝索引鍵。

必要：是

### <WRAPPING\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准包裝金鑰的操作。只有在包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

### <PAYLOAD\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准承載金鑰的操作。只有在承載金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

## 使用 CloudHSM CLI 使用 AES-ZERO-PAD 包裝金鑰

在 CloudHSM CLI 中使用 `key wrap aes-zero-pad` 命令，在硬體安全模組 (HSM) 和包裝機制上使用 AES 金鑰 AES-ZERO-PAD 來包裝承載金鑰。承載金鑰的 `extractable` 屬性必須設定為 `true`。

只有建立金鑰的加密使用者 (CU) 金鑰擁有者才能包裝金鑰。共用金鑰的使用者可以在密碼編譯操作中使用金鑰。

若要使用 `key wrap aes-zero-pad` 命令，您必須先在 AWS CloudHSM 叢集中擁有 AES 金鑰。您可以使用 `wrap` 屬性設為的 [使用 CloudHSM CLI 產生對稱 AES 金鑰](#) 命令來產生 AES 金鑰以進行包裝 `true`。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key wrap aes-zero-pad
Usage: key wrap aes-zero-pad [OPTIONS] --payload-filter [<PAYLOAD_FILTER>...] --
wrapping-filter [<WRAPPING_FILTER>...]

Options:
 --cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error
 --payload-filter [<PAYLOAD_FILTER>...]
```

```

 Key reference (e.g. key-reference=0xabc) or space separated list of key
 attributes in the form of attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a
 payload key
 --wrapping-filter [<WRAPPING_FILTER>...]
 Key reference (e.g. key-reference=0xabc) or space separated list of key
 attributes in the form of attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a
 wrapping key
 --path <PATH>
 Path to the binary file where the wrapped key data will be saved
 --wrapping-approval <WRAPPING_APPROVALR>
 File path of signed quorum token file to approve operation for wrapping key
 --payload-approval <PAYLOAD_APPROVALR>
 File path of signed quorum token file to approve operation for payload key
 -h, --help
 Print help

```

## 範例

此範例說明如何使用wrap屬性值設為 的 AES 金鑰來使用 key wrap aes-zero-pad 命令true。

## Example

```

aws-cloudhsm > key wrap aes-zero-pad --payload-filter attr.label=payload-key --
wrapping-filter attr.label=aes-example
{
 "error_code": 0,
 "data": {
 "payload_key_reference": "0x000000000001c08f1",
 "wrapping_key_reference": "0x000000000001c08ea",
 "wrapped_key_data": "L1wV1L/YeBNVAw6Mpk3owFJZXBzDL0Nt"
 }
}

```

## 引數

### **<CLUSTER\_ID>**

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

**<PAYLOAD\_FILTER>**

索引鍵參考 (例如 `key-reference=0xabc`) 或以形式分隔的索引鍵屬性清單 `attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` , 以選取承載索引鍵。

必要：是

**<PATH>**

二進位檔案的路徑，其中會儲存包裝的金鑰資料。

必要：否

**<WRAPPING\_FILTER>**

索引鍵參考 (例如 `key-reference=0xabc`) 或以空格分隔的索引鍵屬性清單，格式為 `attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` 以選取包裝索引鍵。

必要：是

**<WRAPPING\_APPROVALR>**

指定已簽署規定人數字符檔案的檔案路徑，以核准包裝金鑰的操作。只有在包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

**<PAYLOAD\_APPROVALR>**

指定已簽署規定人數字符檔案的檔案路徑，以核准承載金鑰的操作。只有在承載金鑰的金鑰管理服務規定人數值大於 1 時才需要。

**相關主題**

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

**使用 CloudHSM CLI 使用 CLOUDHSM-AES-GCM 包裝金鑰**

在 CloudHSM CLI 中使用 `key wrap cloudhsm-aes-gcm` 命令，在硬體安全模組 (HSM) 和包裝機制上使用 AES 金鑰 CLOUDHSM-AES-GCM 來包裝承載金鑰。承載金鑰的 `extractable` 屬性必須設定為 `true`。

只有建立金鑰的加密使用者 (CU) 金鑰擁有者，才能包裝金鑰。共用金鑰的使用者可以在密碼編譯操作中使用金鑰。

若要使用 `key wrap cloudhsm-aes-gcm` 命令，您必須先在 AWS CloudHSM 叢集中擁有 AES 金鑰。您可以產生 AES 金鑰來包裝 [使用 CloudHSM CLI 產生對稱 AES 金鑰](#) 命令，並將 `wrap` 屬性設定為 `true`。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key wrap cloudhsm-aes-gcm
```

```
Usage: key wrap cloudhsm-aes-gcm [OPTIONS] --payload-filter [<PAYLOAD_FILTER>...] --
wrapping-filter [<WRAPPING_FILTER>...] --tag-length-bits <TAG_LENGTH_BITS>
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--payload-filter [<PAYLOAD_FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a payload key

```
--wrapping-filter [<WRAPPING_FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a wrapping key

```
--path <PATH>
```

Path to the binary file where the wrapped key data will be saved

```
--wrapping-approval <WRAPPING_APPROVAL>
```

File path of signed quorum token file to approve operation for wrapping key

```
--payload-approval <PAYLOAD_APPROVAL>
```

File path of signed quorum token file to approve operation for payload key

```
--aad <AAD>
```

Aes GCM Additional Authenticated Data (AAD) value, in hex

```
--tag-length-bits <TAG_LENGTH_BITS>
```

```

 Aes GCM tag length in bits
-h, --help
 Print help

```

## 範例

此範例示範如何使用 AES 金鑰來使用 key wrap cloudhsm-aes-gcm 命令。

## Example

```

aws-cloudhsm > key wrap cloudhsm-aes-gcm --payload-filter attr.label=payload-key --
wrapping-filter attr.label=aes-example --tag-length-bits 64 --aad 0x10
{
 "error_code": 0,
 "data": {
 "payload_key_reference": "0x000000000001c08f1",
 "wrapping_key_reference": "0x000000000001c08ea",
 "wrapped_key_data": "6Rn8nkjEriDYlnP3P8nPkYQ8hp10EJ899zsrF+aTB0i/fI1Z"
 }
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <PAYLOAD\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取承載索引鍵。

必要：是

### <PATH>

二進位檔案的路徑，其中會儲存包裝的金鑰資料。

必要：否

### <WRAPPING\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 以選取包裝索引鍵。

必要：是

#### <AAD>

AES GCM 其他已驗證資料 (AAD) 值，以十六進位表示。

必要：否

#### <TAG\_LENGTH\_BITS>

以位元為單位的 AES GCM 標籤長度。

必要：是

#### <WRAPPING\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准包裝金鑰的操作。只有在包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

#### <PAYLOAD\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准承載金鑰的操作。只有在承載金鑰的金鑰管理服務規定人數值大於 1 時才需要。

### 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

### 使用 CloudHSM CLI 使用 RSA-AES 包裝金鑰

在 CloudHSM CLI 中使用 `key wrap rsa-aes` 命令，在硬體安全模組 (HSM) 和 RSA-AES 包裝機制上使用 RSA 公有金鑰來包裝承載金鑰。承載金鑰的 `extractable` 屬性必須設定為 `true`。

只有建立金鑰的加密使用者 (CU) 金鑰擁有者，才能包裝金鑰。共用金鑰的使用者可以在密碼編譯操作中使用金鑰。

若要使用 `key wrap rsa-aes` 命令，您必須先在 AWS CloudHSM 叢集中擁有 RSA 金鑰。您可以使用 [CloudHSM CLI 中的 `generate-asymmetric-pair` 類別](#) 命令和設定為 `wrap` 的屬性來產生 RSA 金鑰對 `true`。

### 使用者類型

下列類型的使用者可以執行此命令。



- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key wrap rsa-aes
```

```
Usage: key wrap rsa-aes [OPTIONS] --payload-filter [<PAYLOAD_FILTER>...] --wrapping-
filter [<WRAPPING_FILTER>...] --hash-function <HASH_FUNCTION> --mgf <MGF>
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--payload-filter [<PAYLOAD_FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a payload key

```
--wrapping-filter [<WRAPPING_FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a wrapping key

```
--path <PATH>
```

Path to the binary file where the wrapped key data will be saved

```
--wrapping-approval <WRAPPING_APPROVALR>
```

File path of signed quorum token file to approve operation for wrapping key

```
--payload-approval <PAYLOAD_APPROVALR>
```

File path of signed quorum token file to approve operation for payload key

```
--hash-function <HASH_FUNCTION>
```

Hash algorithm [possible values: sha1, sha224, sha256, sha384, sha512]

```
--mgf <MGF>
```

Mask Generation Function algorithm [possible values: mgf1-sha1, mgf1-sha224, mgf1-sha256, mgf1-sha384, mgf1-sha512]

```
-h, --help
```

Print help

## 範例

此範例示範如何使用 wrap 屬性值設為的 RSA 公有金鑰來使用 key wrap rsa-ae命令true。

## Example

```
aws-cloudhsm > key wrap rsa-aes --payload-filter attr.label=payload-key --wrapping-
filter attr.label=rsa-public-key-example --hash-function sha256 --mgf mgf1-sha256
{
 "error_code": 0,
 "data": {
 "payload-key-reference": "0x000000000001c08f1",
 "wrapping-key-reference": "0x000000000007008da",
 "wrapped-key-data": "HrSE1DEyLjIeyGdPa9R+ebiqB5TIJGyamPker31ZebPwRA
+NcerbAJ08DJ1lXPYgZcI21vIFSZJuWMEiWpe1R9D/5WSYgxLVKex30xCFqebtEzxbKuv4D0mU4meSofqREYvtb3EoIKwjy
+RL5WGXXKe4nAboAkC5G07veI5yHL1SaKlssSJtTL/CFpbSLsAFuYbv/NUCWwMY5mwyVTCSlw+HlgKK
+5TH1MzBaSi8fpfyepLT8sHy2Q/VRl6ifb49p6m0KQFbRVvz/0WUd6l4d97BdgtaEz6ueg=="
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <PAYLOAD\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取承載索引鍵。

必要：是

### <PATH>

二進位檔案的路徑，其中會儲存包裝的金鑰資料。

必要：否

### <WRAPPING\_FILTER>

索引鍵參考（例如 key-reference=0xabc）或以空格分隔的索引鍵屬性清單，格式為 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE 以選取包裝索引鍵。

必要：是

**<MGF>**

指定遮罩產生函數。

**Note**

遮罩產生函數雜湊函數必須符合簽署機制雜湊函數。

有效值

- mgf1-sha1
- mgf1-sha224
- mgf1-sha256
- mgf1-sha384
- mgf1-sha512

必要：是

**<WRAPPING\_APPROVALR>**

指定已簽署規定人數字符檔案的檔案路徑，以核准包裝金鑰的操作。只有在包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

**<PAYLOAD\_APPROVALR>**

指定已簽署規定人數字符檔案的檔案路徑，以核准承載金鑰的操作。只有在承載金鑰的金鑰管理服務規定人數值大於 1 時才需要。

相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

使用 CloudHSM CLI 以 RSA-OAEP 包裝金鑰

在 CloudHSM CLI 中使用 `key wrap rsa-oaep` 命令，在硬體安全模組 (HSM) 和包裝機制上使用 RSA 公有金鑰 RSA-OAEP 來包裝承載金鑰。承載金鑰的 `extractable` 屬性必須設定為 `true`。

只有金鑰擁有者，也就是建立金鑰的加密使用者 (CU)，才能包裝金鑰。共用金鑰的使用者可以在密碼編譯操作中使用金鑰。

若要使用 `key wrap rsa-oaep` 命令，您必須先在 AWS CloudHSM 叢集中擁有 RSA 金鑰。您可以使用 [CloudHSM CLI 中的 `generate-asymmetric-pair` 類別](#) 命令和設定為 `wrap` 屬性來產生 RSA 金鑰對 `true`。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key wrap rsa-oaep
```

```
Usage: key wrap rsa-oaep [OPTIONS] --payload-filter [<PAYLOAD_FILTER>...] --wrapping-
filter [<WRAPPING_FILTER>...] --hash-function <HASH_FUNCTION> --mgf <MGF>
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--payload-filter [<PAYLOAD_FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a payload key

```
--wrapping-filter [<WRAPPING_FILTER>...]
```

Key reference (e.g. key-reference=0xabc) or space separated list of key attributes in the form of attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE to select a wrapping key

```
--path <PATH>
```

Path to the binary file where the wrapped key data will be saved

```
--wrapping-approval <WRAPPING_APPROVAL>
```

File path of signed quorum token file to approve operation for wrapping key

```
--payload-approval <PAYLOAD_APPROVAL>
```

File path of signed quorum token file to approve operation for payload key

```
--hash-function <HASH_FUNCTION>
```

Hash algorithm [possible values: sha1, sha224, sha256, sha384, sha512]

```
--mgf <MGF>
```

```
Mask Generation Function algorithm [possible values: mgf1-sha1, mgf1-sha224,
mgf1-sha256, mgf1-sha384, mgf1-sha512]
-h, --help
 Print help
```

## 範例

此範例示範如何使用 wrap 屬性值設定為的 RSA 公有金鑰來使用 key wrap rsa-*oaep* 命令 *true*。

## Example

```
aws-cloudhsm > key wrap rsa-oaep --payload-filter attr.label=payload-key --wrapping-
filter attr.label=rsa-public-key-example --hash-function sha256 --mgf mgf1-sha256
{
 "error_code": 0,
 "data": {
 "payload-key-reference": "0x000000000001c08f1",
 "wrapping-key-reference": "0x000000000007008da",
 "wrapped-key-data": "0jJe4msobPLz9TuSAdULEu17T5rMDWtS1LyBSkLbaZnYzzpdrhsbGLbwZJCtB/
jGkDNdB4qyTA0QwEpggGf6v+Yx6JcesNeKKNU8XZa1/YBoHC8noTGUSDI2qr+u2tDc84NPv6d
+F2K00NXsSxMhmxzzNG/gzTVIJh0uy/B1yHjGP4m0XoDZf5+7f5M1CjxBmz4Vva/
wrWHGCSG0y0aWblEv0iHAIIt3UBdyKmU+/
My4xjfJv7WGGu3DFUUIZ06TihRtKQhUYU1M9u6NPf9riJJfHsk6QCuSZ9yWThDT9as6i7e3htnyDhIhGWaoK8JU855cN/
YNKAUqkNpC4FPL3iw=="
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <PAYLOAD\_FILTER>

索引鍵參考（例如 *key-reference=0xabc*）或以空格分隔的索引鍵屬性清單，格式為 *attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE* 以選取承載索引鍵。

必要：是

### <PATH>

二進位檔案的路徑，其中會儲存包裝的金鑰資料。

必要：否

### <WRAPPING\_FILTER>

索引鍵參考（例如 `key-reference=0xabc`）或以空格分隔的索引鍵屬性清單，格式為 `attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` 以選取包裝索引鍵。

必要：是

### <MGF>

指定遮罩產生函數。

#### Note

遮罩產生函數雜湊函數必須符合簽署機制雜湊函數。

有效值

- `mgf1-sha1`
- `mgf1-sha224`
- `mgf1-sha256`
- `mgf1-sha384`
- `mgf1-sha512`

必要：是

### <WRAPPING\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准包裝金鑰的操作。只有在包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

### <PAYLOAD\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准承載金鑰的操作。只有在承載金鑰的金鑰管理服務規定人數值大於 1 時才需要。

相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)

- [CloudHSM CLI 中的金鑰展開命令](#)

## 使用 CloudHSM CLI 使用 RSA-PKCS 包裝金鑰

在 CloudHSM CLI 中使用 `key wrap rsa-pkcs` 命令，在硬體安全模組 (HSM) 和包裝機制上使用 RSA 公有金鑰 RSA-PKCS 來包裝承載金鑰。承載金鑰的 `extractable` 屬性必須設定為 `true`。

只有建立金鑰的加密使用者 (CU) 金鑰擁有者才能包裝金鑰。共用金鑰的使用者可以在密碼編譯操作中使用金鑰。

若要使用 `key wrap rsa-pkcs` 命令，您必須先在 AWS CloudHSM 叢集中擁有 RSA 金鑰。您可以使用 [CloudHSM CLI 中的 `generate-asymmetric-pair` 類別](#) 命令和設定為 `wrap` 屬性來產生 RSA 金鑰對 `true`。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 要求

- 若要執行此命令，必須以 CU 的身分登入。

## 語法

```
aws-cloudhsm > help key wrap rsa-pkcs
```

```
Usage: key wrap rsa-pkcs [OPTIONS] --payload-filter [<PAYLOAD_FILTER>...] --wrapping-filter [<WRAPPING_FILTER>...]
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--payload-filter [<PAYLOAD_FILTER>...]
```

Key reference (e.g. `key-reference=0xabc`) or space separated list of key attributes in the form of `attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` to select a payload key

```
--wrapping-filter [<WRAPPING_FILTER>...]
```

```

 Key reference (e.g. key-reference=0xabc) or space separated list of key
 attributes in the form of attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE to select a
 wrapping key
 --path <PATH>
 Path to the binary file where the wrapped key data will be saved
 --wrapping-approval <WRAPPING_APPROVAL>
 File path of signed quorum token file to approve operation for wrapping key
 --payload-approval <PAYLOAD_APPROVAL>
 File path of signed quorum token file to approve operation for payload key
 -h, --help
 Print help

```

## 範例

此範例示範如何使用 RSA 公有金鑰來使用 key wrap rsa-pkcs 命令。

## Example

```

aws-cloudhsm > key wrap rsa-pkcs --payload-filter attr.label=payload-key --wrapping-
filter attr.label=rsa-public-key-example
{
 "error_code": 0,
 "data": {
 "payload_key_reference": "0x000000000001c08f1",
 "wrapping_key_reference": "0x000000000007008da",
 "wrapped_key_data": "am0Nc7+YE8FWs+5HvU7sIBcXVb24QA0l65nbNAD+1bK+e18BpSfnaI3P+r8Dp
+Lu1ofoUy/
vtzRjZoCiDofcz4EqCFnG14GdcJ1/3W/5WRvMatCa2d7cx02swaeZcjKsermPXYR01lG1fq6NskwMeeTkV8R7Rx9artFrs1
c3XdFJ2+0Bo94c6og/
yfPcp00obJlITCoXhtMRepSd040ggYq/6nUDuHCtJ86pPGnNahyr7+sAaSI3a5ECQLUjwaIARUCyoRh7EFK3qPXcg=="
 }
}

```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <PAYLOAD\_FILTER>

索引鍵參考 (例如 key-reference=0xabc) 或以形式分隔的索引鍵屬性清單 attr.KEY\_ATTRIBUTE\_NAME=KEY\_ATTRIBUTE\_VALUE，以選取承載索引鍵。



必要：是

### <PATH>

二進位檔案的路徑，其中會儲存包裝的金鑰資料。

必要：否

### <WRAPPING\_FILTER>

索引鍵參考（例如 `key-reference=0xabc`）或以空格分隔的索引鍵屬性清單，格式為 `attr.KEY_ATTRIBUTE_NAME=KEY_ATTRIBUTE_VALUE` 以選取包裝索引鍵。

必要：是

### <WRAPPING\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准包裝金鑰的操作。只有在包裝金鑰的金鑰管理服務規定人數值大於 1 時才需要。

### <PAYLOAD\_APPROVALR>

指定已簽署規定人數字符檔案的檔案路徑，以核准承載金鑰的操作。只有在承載金鑰的金鑰管理服務規定人數值大於 1 時才需要。

## 相關主題

- [CloudHSM CLI 中的金鑰包裝命令](#)
- [CloudHSM CLI 中的金鑰展開命令](#)

## 使用 CloudHSM CLI 登入 HSM

您可以使用 CloudHSM CLI 中的 `login` 命令來登入和登出 AWS CloudHSM 叢集中的每個硬體安全 (HSM)。此命令具有下列子命令：

- [簽署 mfa 權杖](#)

### Note

如果您錯誤登入超過 5 次，系統將鎖定您的帳戶。如要解除鎖定，管理員須使用 `cloudhsm_cli` 中的 [user change-password](#) 命令來重設您的密碼。

## 登入和登出疑難排解

如果您在叢集中有多個 HSM，系統將允許您再嘗試登入幾次，若均登入錯誤，系統才會鎖定您的賬戶。這是因為 CloudHSM 用戶端可平衡各個 HSM 之間的負載。因此，每次登入嘗試可能會在不同的 HSM 上開始。如果您正在測試此功能，建議您在只有一個作用中 HSM 的叢集上執行此操作。

如果您在 2018 年 2 月前建立叢集，則系統將在您 20 次錯誤登入後鎖定您的賬戶。

## 使用者類型

下列使用者可以執行這些命令。

- 未激活的管理員
- 管理員
- 加密使用者 (CU)

## 語法

```
aws-cloudhsm > help login
```

```
Login to your cluster
```

```
USAGE:
```

```
cloudhsm-cli login [OPTIONS] --username <USERNAME> --role <ROLE> [COMMAND]
```

```
Commands:
```

```
mfa-token-sign Login with token-sign mfa
```

```
help Print this message or the help of the given subcommand(s)
```

```
OPTIONS:
```

```
--cluster-id <CLUSTER_ID>
```

```
Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error
```

```
--username <USERNAME>
```

```
Username to access the Cluster
```

```
--role <ROLE>
```

```
Role the user has in the Cluster
```

```
Possible values:
```

```
- crypto-user: A CryptoUser has the ability to manage and use keys
```

```
- admin: An Admin has the ability to manage user accounts

--password <PASSWORD>
 Optional: Plaintext user's password. If you do not include this argument you
 will be prompted for it

-h, --help
 Print help (see a summary with '-h')
```

## 範例

### Example

此命令可允許您使用以 admin1 的管理員使用者登入憑證，來登入叢集中的所有 HSM。

```
aws-cloudhsm > login --username admin1 --role admin
Enter password:
{
 "error_code": 0,
 "data": {
 "username": "admin1",
 "role": "admin"
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <USERNAME>

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。在此命令中，使用者名稱不區分大小寫，使用者名稱始終以小寫顯示。

必要：是

### <ROLE>

指定指派給此使用者的角色。此為必要參數。有效值為 admin、crypto-user。

若要取得使用者的角色，請使用 `user list` 命令。如需 HSM 上使用者類型的詳細資訊，請參閱[了解 HSM 使用者](#)。

### <PASSWORD>

指定登入 HSM 使用者的密碼。

### 相關主題

- [開始使用 CloudHSM CLI](#)
- [啟用叢集](#)

### 使用 CloudHSM CLI 使用 MFA 登入 HSM

使用 `aws cloudhsm login mfa-token-sign` 命令，使用多重驗證 (MFA) 登入硬體安全模組 (HSM)。若要使用此命令，您必須先設定 [MFA 的 CloudHSM CLI](#)。

### 使用者類型

下列使用者可以執行這些命令。

- 管理員
- 加密使用者 (CU)

### 語法

```
aws-cloudhsm > help login mfa-token-sign
```

```
Login with token-sign mfa
```

#### USAGE:

```
login --username <username> --role <role> mfa-token-sign --token <token>
```

#### OPTIONS:

```
--cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in the
config file to run the operation against. If not provided, will fall back to the value
provided when interactive mode was started, or error
--token <TOKEN> Filepath where the unsigned token file will be written
-h, --help Print help
```

## 範例

### Example

```
aws-cloudhsm > login --username test_user --role admin mfa-token-sign --token /home/valid.token
Enter password:
Enter signed token file path (press enter if same as the unsigned token file):
{
 "error_code": 0,
 "data": {
 "username": "test_user",
 "role": "admin"
 }
}
```

## 引數

### <CLUSTER\_ID>

執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <TOKEN>

將寫入未簽署權杖檔案的檔案路徑。

必要：是

## 相關主題

- [開始使用 CloudHSM CLI](#)
- [啟用叢集](#)
- [使用 CloudHSM CLI 管理 MFA](#)

## 使用 CloudHSM CLI 登出 HSM

使用 CloudHSM CLI 中的 logout 命令來登出 AWS CloudHSM 叢集中的每個硬體安全模組 (HSM)。

## 使用者類型

下列使用者可以執行此命令。

- 管理員
- 加密使用者 (CU)

## 語法

```
aws-cloudhsm > help logout
Logout of your cluster

USAGE:
 logout

OPTIONS:
 --cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in the
 config file to run the operation against. If not provided, will fall back to the value
 provided when interactive mode was started, or error
 -h, --help Print help information
 -V, --version Print version information
```

## 範例

### Example

此命令會讓您登出叢集中的所有 HSM。

```
aws-cloudhsm > logout
{
 "error_code": 0,
 "data": "Logout successful"
}
```

## 相關主題

- [開始使用 CloudHSM CLI](#)
- [啟用叢集](#)

## CloudHSM CLI 中的使用者類別

在 CloudHSM CLI 中，`user` 是一組命令的父類別，當與父類別結合時，會建立使用者專屬的命令。目前，用戶類別由以下命令組成：

- [變更使用者 MFA](#)
- [變更使用者密碼](#)
- [建立使用者](#)
- [刪除使用者](#)
- [使用者清單](#)
- [使用者複寫](#)

### CloudHSM CLI 中的使用者 `change-mfa` 類別

在 CloudHSM CLI 中，`user change-mfa` 是一組命令的父類別，當與父類別結合時，會為使用者建立特定於變更多重要素驗證 (MFA) 的命令。

目前，此類別由以下子命令組成：

- [字符簽署](#)

### 使用 CloudHSM CLI 變更使用者的 MFA 設定

在 CloudHSM CLI 中使用 `user change-mfa token-sign` 命令來更新使用者帳戶的多重驗證 (MFA) 設定。任何使用者帳戶均可執行此命令。具有管理員角色的帳戶可以為其他使用者執行此命令。

### 使用者類型

下列使用者可以執行此命令。

- 管理員
- 加密使用者

### 語法

目前，只有單一多重因素策略可供使用者使用：字符簽署。

```
aws-cloudhsm > help user change-mfa
```

## Change a user's Mfa Strategy

### Usage:

```
user change-mfa <COMMAND>
```

### Commands:

```
token-sign Register or Deregister a public key using token-sign mfa strategy
help Print this message or the help of the given subcommand(s)
```

Token Sign 策略需要一個權杖檔案將未簽署的權杖寫入其中。

```
aws-cloudhsm > help user change-mfa token-sign
```

```
Register or Deregister a public key using token-sign mfa strategy
```

```
Usage: user change-mfa token-sign [OPTIONS] --username <USERNAME> --role <ROLE> <--
token <TOKEN>|--deregister>
```

### Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--username <USERNAME>
```

Username of the user that will be modified

```
--role <ROLE>
```

Role the user has in the cluster

Possible values:

- crypto-user: A CryptoUser has the ability to manage and use keys
- admin: An Admin has the ability to manage user accounts

```
--change-password <CHANGE_PASSWORD>
```

Optional: Plaintext user's password. If you do not include this argument you will be prompted for it

```
--token <TOKEN>
```

Filepath where the unsigned token file will be written. Required for enabling MFA for a user

```
--approval <APPROVAL>
```



Filepath of signed quorum token file to approve operation

**--deregister**

Deregister the MFA public key, if present

**--change-quorum**

Change the Quorum public key along with the MFA key

**-h, --help**

Print help (see a summary with '-h')

## 範例

此命令會將叢集中每個 HSM 的未簽署權杖寫入 token 指定的檔案。當系統提示您時，請在檔案中簽署權杖。

Example：寫入叢集中每個 HSM 的未簽署權杖

```
aws-cloudhsm > user change-mfa token-sign --username cu1 --change-password password --
role crypto-user --token /path/myfile
```

Enter signed token file path (press enter if same as the unsigned token file):

Enter public key PEM file path:/path/mypemfile

```
{
 "error_code": 0,
 "data": {
 "username": "test_user",
 "role": "admin"
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <ROLE>

指賦予使用者帳戶的角色。此為必要參數。如需 HSM 上使用者類型的詳細資訊，請參閱[了解 HSM 使用者](#)。

有效值

- 管理員：管理員可以管理使用者，但無法管理金鑰。
- 加密使用者：加密使用者可以建立管理金鑰並在密碼編譯操作時使用該金鑰。

### <USERNAME>

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。

建立使用者之後，您就無法再變更使用者的名稱。在 CloudHSM CLI 命令中，角色和密碼需區分大小寫，但使用者名稱不區分大小寫。

必要：是

### <CHANGE\_PASSWORD>

指正在註冊/取消註冊 MFA 使用者的純文字新密碼。

必要：是

### <TOKEN>

將寫入未簽署權杖檔案的檔案路徑。

必要：是

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在規定人數使用者服務規定人數值大於 1 時才需要執行此操作。

### <DEREGISTER>

取消註冊 MFA 公有金鑰 (如有)。

### <CHANGE-QUORUM>

變更規定人數公有金鑰以及 MFA 金鑰。

## 相關主題

- [了解 HSM 使用者的 2FA](#)

## 使用 CloudHSM CLI 變更使用者的密碼

使用 CloudHSM CLI 中的 `user change-password` 命令來變更 AWS CloudHSM 叢集中現有使用者的密碼。若要為使用者啟用 MFA，請使用 `user change-mfa` 命令。

任何使用者都可以變更自己的密碼。此外，具有管理員角色的使用者可以變更叢集中其他使用者的密碼。您無需輸入目前的密碼即可進行變更。

 Note

您無法變更目前已登入叢集使用者的密碼。

## 使用者類型

下列使用者可以執行此命令。

- 管理員
- 加密使用者 (CU)

## 語法

 Note

若要為使用者啟用多重要素驗證 (MFA)，請使用 `user change-mfa` 命令。

```
aws-cloudhsm > help user change-password
```

Change a user's password

Usage:

```
cloudhsm-cli user change-password [OPTIONS] --username <USERNAME> --role <ROLE>
[--password <PASSWORD>]
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--username <USERNAME>
```

Username of the user that will be modified

```
--role <ROLE>
```

Role the user has in the cluster

```

Possible values:
- crypto-user: A CryptoUser has the ability to manage and use keys
- admin: An Admin has the ability to manage user accounts

--password <PASSWORD>
 Optional: Plaintext user's password. If you do not include this argument you
will be prompted for it

--approval <APPROVAL>
 Filepath of signed quorum token file to approve operation

--deregister-mfa <DEREGISTER-MFA>
 Deregister the user's mfa public key, if present

--deregister-quorum <DEREGISTER-QUORUM>
 Deregister the user's quorum public key, if present
-h, --help
 Print help (see a summary with '-h')
```

## 範例

以下範例說明如何使用 `user change-password` 重設叢集中目前使用者或其他任何使用者的密碼。

Example：變更您的密碼

叢集中的任何使用者均可使用 `user change-password` 變更自己的密碼。

以下輸出顯示 Bob 目前正以加密使用者 (CU) 的身分登入。

```

aws-cloudhsm > user change-password --username bob --role crypto-user
Enter password:
Confirm password:
{
 "error_code": 0,
 "data": {
 "username": "bob",
 "role": "crypto-user"
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在規定人數使用者服務規定人數值大於 1 時才需要執行此操作。

### <DEREGISTER-MFA>

取消註冊 MFA 公有金鑰 (如有)。

### <DEREGISTER-QUORUM>

取消註冊規定人數公有鑰 (如有)。

### <PASSWORD>

指使用者的純文字新密碼。不允許下列字元 ' : '。

必要：是

### <ROLE>

指賦予使用者帳戶的角色。此為必要參數。如需 HSM 上使用者類型的詳細資訊，請參閱[了解 HSM 使用者](#)。

有效值

- 管理員：管理員可以管理使用者，但無法管理金鑰。
- 加密使用者：加密使用者可以建立管理金鑰並在密碼編譯操作時使用該金鑰。

### <USERNAME>

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。

建立使用者之後，您就無法再變更使用者的名稱。在 CloudHSM CLI 命令中，角色和密碼需區分大小寫，但使用者名稱不區分大小寫。

必要：是

## 相關主題

- [使用者清單](#)
- [建立使用者](#)
- [刪除使用者](#)

### CloudHSM CLI 中的使用者變更量子類別

在 CloudHSM CLI 中，`user change-quorum` 是一組命令的父類別，當與父類別結合時，會建立使用者變更規定人數的特定命令。

`user change-quorum` 用於使用特定的規定人數策略註冊使用者規定人數驗證。如下所示：從 SDK 5.8.0 開始，使用者只能使用一種規定人數策略。

目前，此類別由以下類別和子命令組成：

- [字符簽署](#)
  - [註冊](#)

### CloudHSM CLI 中的使用者 `change-quorum token-sign` 類別

在 CloudHSM CLI 中，`user change-quorum token-sign` 是命令的父類別，當與此父類別結合時，會建立權杖簽署規定人數操作專用的命令。

目前，此類別由以下命令組成：

- [註冊](#)

### 使用 CloudHSM CLI 註冊使用者的字符簽署規定人數策略

使用 CloudHSM CLI 中的 `user change-quorum token-sign register` 命令為管理員使用者註冊規定人數字符簽署策略。

### 使用者類型

下列使用者可以執行此命令。

- 管理員

## 語法

```
aws-cloudhsm > help user change-quorum token-sign register
```

Register a user for quorum authentication with a public key

Usage: user change-quorum token-sign register --public-key *<PUBLIC\_KEY>* --signed-token *<SIGNED\_TOKEN>*

Options:

--cluster-id *<CLUSTER\_ID>* Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

--public-key *<PUBLIC\_KEY>* Filepath to public key PEM file

--signed-token *<SIGNED\_TOKEN>* Filepath with token signed by user private key

-h, --help Print help (see a summary with '-h')

## 範例

### Example

若要執行此命令，您須以您希望的使用者身分登入 register quorum token-sign。

```
aws-cloudhsm > login --username admin1 --role admin
```

Enter password:

```
{
 "error_code": 0,
 "data": {
 "username": "admin1",
 "role": "admin"
 }
}
```

此 user change-quorum token-sign register 命令會向 HSM 註冊您的公有金鑰。因此，該命令可讓您作為規定人數核准人執行必要的核准操作，這些操作需要使用者取得規定人數簽章，以此滿足必要的規定人數值閾值。

```
aws-cloudhsm > user change-quorum token-sign register \
--public-key /home/mypemfile \
--signed-token /home/mysignedtoken
{
 "error_code": 0,
```

```
"data": {
 "username": "admin1",
 "role": "admin"
}
```

您現在可以執行 `user list` 命令，並確認已為此使用者註冊規定人數字符簽署。

```
aws-cloudhsm > user list
{
 "error_code": 0,
 "data": {
 "users": [
 {
 "username": "admin",
 "role": "admin",
 "locked": "false",
 "mfa": [],
 "quorum": [],
 "cluster-coverage": "full"
 },
 {
 "username": "admin1",
 "role": "admin",
 "locked": "false",
 "mfa": [],
 "quorum": [
 {
 "strategy": "token-sign",
 "status": "enabled"
 }
],
 "cluster-coverage": "full"
 }
]
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。



必要：如果已[設定多個叢集](#)。

### <PUBLIC-KEY>

公有金鑰 PEM 檔案的檔案路徑。

必要：是

### <SIGNED-TOKEN>

帶有由使用者私有金鑰簽署的權杖的文件路徑。

必要：是

## 相關主題

- [使用 CloudHSM CLI 管理規定人數驗證](#)
- [對管理員使用規定人數身分驗證：首次設定](#)
- [變更管理員的規定人數最小值](#)
- [支援規定人數身分驗證的服務名稱和類型](#)

## 使用 CloudHSM CLI 建立 AWS CloudHSM 使用者

CloudHSM CLI 中的 `user create` 命令會在 AWS CloudHSM 叢集中建立使用者。只有具有管理員角色的使用者帳戶可以執行此命令。

## 使用者類型

下列類型的使用者可以執行此命令。

- 管理員

## 要求

若要執行此命令，必須以管理員使用者的身分登入。

## 語法

```
aws-cloudhsm > help user create
Create a new user
```

```
Usage: cloudhsm-cli user create [OPTIONS] --username <USERNAME> --role <ROLE> [--password <PASSWORD>]
```

Options:

```
--cluster-id <CLUSTER_ID>
```

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

```
--username <USERNAME>
```

Username to access the HSM cluster

```
--role <ROLE>
```

Role the user has in the cluster

Possible values:

- crypto-user: A CryptoUser has the ability to manage and use keys
- admin: An Admin has the ability to manage user accounts

```
--password <PASSWORD>
```

Optional: Plaintext user's password. If you do not include this argument you will be prompted for it

```
--approval <APPROVAL>
```

Filepath of signed quorum token file to approve operation

```
-h, --help
```

Print help (see a summary with '-h')

## 範例

下列範例顯示如何使用 `user create` 在您的 HSM 中建立新使用者。

Example : 建立加密使用者

此範例會在具有加密使用者角色的 AWS CloudHSM 叢集中建立 帳戶。

```
aws-cloudhsm > user create --username alice --role crypto-user
Enter password:
Confirm password:
{
 "error_code": 0,
```

```
"data": {
 "username": "alice",
 "role": "crypto-user"
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <USERNAME>

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。在此命令中，使用者名稱不區分大小寫，使用者名稱始終以小寫顯示。

必要：是

### <ROLE>

指定指派給此使用者的角色。此為必要參數。有效值為 admin、crypto-user。

若要取得使用者的角色，請使用 user list 命令。如需 HSM 上使用者類型的詳細資訊，請參閱[了解 HSM 使用者](#)。

### <PASSWORD>

指定登入 HSM 使用者的密碼。不允許使用下列字元 ':'

必要：是

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在規定人數使用者服務規定人數值大於 1 時才需要執行此操作。

## 相關主題

- [使用者清單](#)
- [刪除使用者](#)

- [變更使用者密碼](#)

## 使用 CloudHSM CLI 刪除 AWS CloudHSM 使用者

CloudHSM CLI 中的 `user delete` 命令會從 AWS CloudHSM 叢集中刪除使用者。只有具有管理員角色的使用者帳戶可以執行此命令。您無法刪除目前登入 HSM 的使用者。

## 使用者類型

下列類型的使用者可以執行此命令。

- 管理員

## 要求

- 您無法刪除擁有金鑰的使用者帳戶。
- 您的使用者帳戶必須具有管理員角色才能執行此命令。

## 語法

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
aws-cloudhsm > help user delete
Delete a user

Usage: user delete [OPTIONS] --username <USERNAME> --role <ROLE>

Options:
 --cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error

 --username <USERNAME>
 Username to access the HSM cluster

 --role <ROLE>
 Role the user has in the cluster

Possible values:
 - crypto-user: A CryptoUser has the ability to manage and use keys
```

```
- admin: An Admin has the ability to manage user accounts

--approval <APPROVAL>
 Filepath of signed quorum token file to approve operation
```

## 範例

```
aws-cloudhsm > user delete --username alice --role crypto-user
{
 "error_code": 0,
 "data": {
 "username": "alice",
 "role": "crypto-user"
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <USERNAME>

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。在此命令中，使用者名稱不區分大小寫，使用者名稱始終以小寫顯示。

必要：是

### <ROLE>

指定指派給此使用者的角色。此為必要參數。有效值為 admin、crypto-user。

若要取得使用者的角色，請使用 user list 命令。如需 HSM 上使用者類型的詳細資訊，請參閱[了解 HSM 使用者](#)。

必要：是

### <APPROVAL>

指要核准操作的已簽署規定人數權杖檔案的檔案路徑。只有在規定人數使用者服務規定人數值大於 1 時才需要執行此操作。

必要：是

## 相關主題

- [使用者清單](#)
- [建立使用者](#)
- [變更使用者密碼](#)

使用 CloudHSM CLI 列出 AWS CloudHSM 所有使用者

CloudHSM CLI 中的 `user list` 命令會列出 AWS CloudHSM 叢集中存在的使用者帳戶。您無須登入 CloudHSM CLI 即可執行此命令。

### Note

如果您新增或刪除 HSMs，請更新 AWS CloudHSM 用戶端和命令列工具使用的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列類型的使用者可以執行此命令。

- 所有使用者。您無須登入即可執行此命令。

## 語法

```
aws-cloudhsm > help user list
List the users in your cluster
```

### USAGE:

```
user list
```

### Options:

```
--cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in the
config file to run the operation against. If not provided, will fall back to the value
provided when interactive mode was started, or error
-h, --help Print help
```

## 範例

此命令會列出 CloudHSM 叢集中的使用者。

```
aws-cloudhsm > user list
{
 "error_code": 0,
 "data": {
 "users": [
 {
 "username": "admin",
 "role": "admin",
 "locked": "false",
 "mfa": [],
 "cluster-coverage": "full"
 },
 {
 "username": "test_user",
 "role": "admin",
 "locked": "false",
 "mfa": [
 {
 "strategy": "token-sign",
 "status": "enabled"
 }
],
 "cluster-coverage": "full"
 },
 {
 "username": "app_user",
 "role": "internal(APPLIANCE_USER)",
 "locked": "false",
 "mfa": [],
 "cluster-coverage": "full"
 }
]
 }
}
```

輸出包含下列使用者屬性：

- 使用者名稱：顯示使用者定義的使用者易記名稱。使用者名稱一律以小寫顯示。
- 角色：決定使用者在 HSM 上可執行的操作。

- 已鎖定：表示此使用者帳戶是否已鎖定。
- MFA：表示此使用者帳戶支援的多重要素驗證機制。
- 叢集涵蓋範圍：表示此使用者帳戶在叢集範圍內的可用性。

## 相關主題

- key\_mgmt\_util 中的 [listUsers](#)
- [建立使用者](#)
- [刪除使用者](#)
- [變更使用者密碼](#)

## 使用 CloudHSM CLI 複寫使用者

使用 CloudHSM CLI 中的 user replicate 命令，將使用者從來源 AWS CloudHSM 叢集複寫到目的地 AWS CloudHSM 叢集。

## 使用者類型

下列類型的使用者可以執行此命令。

- 管理員 (COs)

## 要求

- 來源和目的地叢集必須是複製。這表示一個是從另一個備份建立的，或者兩者都是從通用備份建立的。如需詳細資訊，請參閱[從備份建立叢集](#)。
- 若要執行此命令，您必須在來源和目的地叢集上以管理員身分登入。
  - 在單一命令模式中，命令將使用 CLOUDHSM\_PIN 和 CLOUDHSM\_ROLE 環境變數在來源叢集上進行驗證。如需詳細資訊，請參閱[單一命令模式](#)。若要提供目的地叢集的登入資料，您需要設定兩個額外的環境變數：DESTINATION\_CLOUDHSM\_PIN 和 DESTINATION\_CLOUDHSM\_ROLE：

```
$ export DESTINATION_CLOUDHSM_ROLE=<role>
```

```
$ export DESTINATION_CLOUDHSM_PIN=<username:password>
```

- 在互動式模式中，使用者將需要明確登入來源和目的地叢集。



## 語法

```
aws-cloudhsm > help user replicate
```

Replicate a user from a source to a destination cluster

Usage: user replicate --username *<USERNAME>* --role *<ROLE>* --source-cluster-id *<SOURCE\_CLUSTER\_ID>* --destination-cluster-id *<DESTINATION\_CLUSTER\_ID>*

Options:

--username *<USERNAME>*

Username of the user to replicate

--role *<ROLE>*

Role the user has in the cluster

Possible values:

- crypto-user: A CryptoUser has the ability to manage and use keys
- admin: An Admin has the ability to manage user accounts

--source-cluster-id *<SOURCE\_CLUSTER\_ID>*

Source cluster ID

--destination-cluster-id *<DESTINATION\_CLUSTER\_ID>*

Destination cluster ID

-h, --help

Print help (see a summary with '-h')

## 範例

Example 範例：複寫使用者

此命令會將使用者從具有 的來源叢集複寫到複製的目的地叢集。以下範例示範在兩個叢集上以管理員身分登入時的輸出。

```
admin-user@cluster-1234abcdefg > user replicate \
 --username example-admin \
 --role admin \
 --source-cluster-id cluster-1234abcdefg \
 --destination-cluster-id cluster-2345bcdefgh
{
 "error_code": 0,
 "data": {
```

```
{
 "user": {
 "username": "example-admin",
 "role": "admin",
 "locked": "false",
 "mfa": [],
 "quorum": [],
 "cluster-coverage": "full"
 },
 "message": "Successfully replicated user"
}
```

## 引數

### <USERNAME>

指定要在來源叢集中複寫的使用者名稱。

必要：是

### <ROLE>

指定指派給此使用者的角色。此為必要參數。有效值為 admin、crypto-user。

若要取得使用者的角色，請使用 user list 命令。如需 HSM 上使用者類型的詳細資訊，請參閱[了解 HSM 使用者](#)。

必要：是

### <SOURCE\_CLUSTER\_ID>

來源叢集 ID。

必要：是

### <DESTINATION\_CLUSTER\_ID>

目的地叢集 ID。

必要：是

## 相關主題

- [使用 CloudHSM CLI 連線至多個叢集](#)

## CloudHSM CLI 中的規定人數類別

在 CloudHSM CLI 中，quorum 是一組命令的父類別，當與 `結合時quorum`，會建立特定於規定人數身分驗證或 M 的 N 操作的命令。目前，此類別由 token-sign 子類別組成，該子類別由其自己的命令組成。按一下以下連結了解詳細資訊。

- [字符簽署](#)

**管理員服務：**規定人數身分驗證用於管理員特殊權限服務，例如建立使用者、刪除使用者、變更使用者密碼、設定規定人數值，以及停用規定人數和 MFA 功能。

**加密使用者服務：**Quorum 身分驗證用於與特定金鑰相關聯的加密使用者權限服務，例如使用金鑰簽署、共用/取消共用金鑰、包裝/取消包裝金鑰，以及設定金鑰的屬性。產生、匯入或取消包裝金鑰時，會設定關聯金鑰的規定人數值。規定人數值必須等於或小於與金鑰相關聯的使用者數量，其中包括與金鑰共用的使用者和金鑰擁有者。

每種服務類型都會進一步細分為合格的服務名稱，這包含一組特定的可執行法定人數支援的服務操作。

| 服務名稱                 | 服務類型  | 服務操作                                                                                                                                                   |
|----------------------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用者                  | 管理員   | <ul style="list-style-type: none"> <li>• 建立使用者</li> <li>• 刪除使用者</li> <li>• 變更使用者密碼</li> <li>• 變更使用者 MFA</li> </ul>                                     |
| 規定人數                 | 管理員   | <ul style="list-style-type: none"> <li>• 規定人數字符簽署 設定規定人數值</li> </ul>                                                                                   |
| cluster <sup>1</sup> | 管理員   | <ul style="list-style-type: none"> <li>• 叢集 mtls register-trust-anchor</li> <li>• 叢集 mtls deregister-trust-anchor</li> <li>• 叢集 mtls 設定強制執行</li> </ul> |
| 金鑰管理                 | 加密使用者 | <ul style="list-style-type: none"> <li>• 金鑰包裝</li> <li>• 金鑰取消包裝</li> <li>• 共用金鑰</li> </ul>                                                             |

| 服務名稱      | 服務類型  | 服務操作                                                                     |
|-----------|-------|--------------------------------------------------------------------------|
|           |       | <ul style="list-style-type: none"> <li>取消共用金鑰</li> <li>設定金鑰屬性</li> </ul> |
| key-usage | 加密使用者 | <ul style="list-style-type: none"> <li>鍵符號</li> </ul>                    |

【1】叢集服務僅在 hsm2m.medium 上提供

## 相關主題

- [使用 CloudHSM CLI 為 AWS CloudHSM 管理員設定規定人數身分驗證](#)
- [使用 CloudHSM CLI 管理規定人數身分驗證 \(M of N 存取控制\)](#)

## CloudHSM CLI 中的規定人數字符簽署類別

在 CloudHSM CLI 中，quorum token-sign 是一組命令的類別，當與 結合時quorum token-sign，會建立規定人數身分驗證或 N 操作的 M 特定命令。

目前，此類別由以下命令組成：

- [刪除](#)
- [產生](#)
- [列出](#)
- [列出規定人數值](#)
- [設定規定人數值](#)

## 使用 CloudHSM CLI 刪除規定人數字符

使用 CloudHSM CLI 中的 quorum token-sign delete 命令刪除規定人數授權服務的一個或多個權杖。

## 使用者類型

下列使用者可以執行此命令。

- 管理員

## 語法

```
aws-cloudhsm > help quorum token-sign delete
```

Delete one or more Quorum Tokens

Usage: quorum token-sign delete --scope *<SCOPE>*

Options:

**--cluster-id** *<CLUSTER\_ID>*

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

**--scope** *<SCOPE>*

Scope of which token(s) will be deleted

Possible values:

- user: Deletes all token(s) of currently logged in user
- all: Deletes all token(s) on the HSM

**-h, --help**

Print help (see a summary with '-h')

## 範例

下列範例顯示了如何使用 CloudHSM CLI 中的 quorum token-sign delete 命令刪除規定人數授權服務的一個或多個權杖。

Example：刪除規定人數授權服務的一個或多個權杖

```
aws-cloudhsm > quorum token-sign delete --scope all
{
 "error_code": 0,
 "data": "Deletion of quorum token(s) successful"
}
```

## 引數

***<CLUSTER\_ID>***

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

## <SCOPE>

AWS CloudHSM 叢集中將刪除字符的範圍 (s)。

有效值

- 使用者：僅用於刪除登入使用者擁有的權杖。
- 全部：用於刪除 AWS CloudHSM 叢集中的所有字符。

相關主題

- [使用者清單](#)
- [建立使用者](#)
- [刪除使用者](#)

使用 CloudHSM CLI 產生規定人數權杖

使用 CloudHSM CLI 中的 `quorum token-sign generate` 命令為規定人數授權服務產生一個權杖。

對於服務使用者 and 規定人數而言，HSM 叢集上，每位使用者每種服務取得作用中權杖有一定限制。此限制不適用於與金鑰服務相關的字符。

### Note

只有管理員和加密使用者可以產生特定的服務權杖。如需服務類型和名稱的詳細資訊，請參閱 [支援規定人數身分驗證的服務名稱和類型](#)

**管理員服務：**規定人數身分驗證用於管理員特殊權限服務，例如建立使用者、刪除使用者、變更使用者密碼、設定規定人數值，以及停用規定人數和 MFA 功能。

**加密使用者服務：**Quorum 身分驗證用於與特定金鑰相關聯的加密使用者權限服務，例如使用金鑰簽署、共用/取消共用金鑰、包裝/取消包裝金鑰，以及設定金鑰的屬性。產生、匯入或取消包裝金鑰時，會設定關聯金鑰的規定人數值。規定人數值必須等於或小於與金鑰相關聯的使用者數量，其中包括與金鑰共用的使用者和金鑰擁有者。

每種服務類型都會進一步細分為合格的服務名稱，這包含一組特定的可執行法定人數支援的服務操作。

| 服務名稱                 | 服務類型  | 服務操作                                                                                                                                                   |
|----------------------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用者                  | 管理員   | <ul style="list-style-type: none"> <li>• 建立使用者</li> <li>• 刪除使用者</li> <li>• 變更使用者密碼</li> <li>• 變更使用者 MFA</li> </ul>                                     |
| 規定人數                 | 管理員   | <ul style="list-style-type: none"> <li>• 規定人數字符簽署 設定規定人數值</li> </ul>                                                                                   |
| cluster <sup>1</sup> | 管理員   | <ul style="list-style-type: none"> <li>• 叢集 mtls register-trust-anchor</li> <li>• 叢集 mtls deregister-trust-anchor</li> <li>• 叢集 mtls 設定強制執行</li> </ul> |
| 金鑰管理                 | 加密使用者 | <ul style="list-style-type: none"> <li>• 金鑰包裝</li> <li>• 金鑰取消包裝</li> <li>• 共用金鑰</li> <li>• 取消共用金鑰</li> <li>• 設定金鑰屬性</li> </ul>                         |
| key-usage            | 加密使用者 | <ul style="list-style-type: none"> <li>• 鍵符號</li> </ul>                                                                                                |

【1】 叢集服務僅在 hsm2m.medium 上提供

## 使用者類型

下列使用者可以執行此命令。

- 管理員
- 加密使用者 (CU)

## 語法

```
aws-cloudhsm > help quorum token-sign generate
```

Generate a token

Usage: quorum token-sign generate --service *<SERVICE>* --token *<TOKEN>*

Options:

--cluster-id *<CLUSTER\_ID>*

Unique Id to choose which of the clusters in the config file to run the operation against. If not provided, will fall back to the value provided when interactive mode was started, or error

--service *<SERVICE>*

Service the token will be used for

Possible values:

- user:

User management service is used for executing quorum authenticated user management operations

- quorum:

Quorum management service is used for setting quorum values for any quorum service

- cluster:

Cluster management service is used for executing quorum for cluster wide configuration managements like mtls enforcement, mtls registration and mtls deregistration

- registration:

Registration service is used for registering a public key for quorum authentication

- key-usage:

Key usage service is used for executing quorum authenticated key usage operations

- key-management:

Key management service is used for executing quorum authenticated key management operations

--token *<TOKEN>*

Filepath where the unsigned token file will be written

-h, --help

Print help

## 範例

此命令會將叢集中每個 HSM 的未簽署權杖寫入 token 指定的檔案。



Example：寫入叢集中每個 HSM 的未簽署權杖

```
aws-cloudhsm > quorum token-sign generate --service user --token /home/tfile
{
 "error_code": 0,
 "data": {
 "filepath": "/home/tfile"
 }
}
```

引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <SERVICE>

指定要產生字符的規定人數授權服務。此為必要參數。

有效值

- 使用者：指使用者管理服務，用於執行規定人數授權的使用者管理操作。
- 規定人數：指規定人數管理服務，用於為任何規定人數授權服務設定規定人數授權的規定人數值。
- cluster：用於執行 mtls 強制執行、mtls 註冊和 mtls 取消註冊等叢集範圍組態管理的法定人數的叢集管理服務。
- 登記：產生一個未簽署權杖，用於登記規定人數授權的公有金鑰。
- key-usage：產生未簽署的字符，用於執行規定人數授權金鑰用量操作。
- 金鑰管理：產生未簽署的權杖，用於執行規定人數授權金鑰管理操作。

必要：是

### <TOKEN>

將寫入未簽署權杖檔案的檔案路徑。

必要：是

## 相關主題

- [支援規定人數身分驗證的服務名稱和類型](#)

### 使用 CloudHSM CLI 列出規定人數字符

使用 CloudHSM CLI 中的 `quorum token-sign list` 命令，列出 AWS CloudHSM 叢集中存在的所有字符簽署規定人數字符。這包括其他使用者產生的字符。權杖綁定到使用者，因此雖然您可能會看到其他使用者的權杖，但您只能使用與目前登入使用者相關聯的權杖。

如需有關服務類型和名稱的詳細資訊，請參閱[支援規定人數身分驗證的服務名稱和類型](#)。如需從列出的字符顯示的內容詳細資訊，請參閱 [the section called “具有規定人數的金鑰管理和用量 \(M 為 N\)”](#) 以取得與 key-management key-usage 服務相關聯的字符，請參閱 [the section called “使用規定人數進行使用者管理 \(M 為 N\)”](#) 以取得與 user、quorum 或 cluster 服務相關聯的字符。

### 使用者類型

下列使用者可以執行此命令。

- 管理員
- 加密使用者 (CU)

### 語法

```
aws-cloudhsm > help quorum token-sign list
List the token-sign tokens in your cluster

Usage: quorum token-sign list

Options:
 --cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in the
 config file to run the operation against. If not provided, will fall back to the value
 provided when interactive mode was started, or error
 -h, --help Print help
```

### 範例

此命令會列出 AWS CloudHSM 叢集中存在的所有字符-簽章字符。這包括其他使用者產生的字符。權杖綁定到使用者，因此雖然您可能會看到其他使用者的權杖，但您只能使用與目前登入使用者相關聯的權杖。

## Example

```
aws-cloudhsm > quorum token-sign list
{
 "error_code": 0,
 "data": {
 "tokens": [
 {
 "username": "admin",
 "service": "quorum",
 "approvals-required": 2,
 "number-of-approvals": 0,
 "token-timeout-seconds": 397,
 "cluster-coverage": "full"
 },
 {
 "username": "admin",
 "service": "user",
 "approvals-required": 2,
 "number-of-approvals": 0,
 "token-timeout-seconds": 588,
 "cluster-coverage": "full"
 },
 {
 "username": "crypto_user1",
 "service": "key-management",
 "key-reference": "0x000000000002c33f7",
 "minimum-token-count": 1
 },
 {
 "username": "crypto_user1",
 "service": "key-usage",
 "key-reference": "0x000000000002c33f7",
 "minimum-token-count": 1
 }
]
 }
}
```

## 相關主題

- [產生規定人數字符簽署](#)

## 使用 CloudHSM CLI 顯示規定人數值

使用 CloudHSM CLI 中的 `quorum token-sign list-quorum-values` 命令來列出 AWS CloudHSM 叢集中設定的規定人數值。

### 使用者類型

下列使用者可以執行此命令。

- 所有使用者。您無須登入即可執行此命令。

### 語法

```
aws-cloudhsm > help quorum token-sign list-quorum-values
List current quorum values

Usage: quorum token-sign list-quorum-values

Options:
 --cluster-id <CLUSTER_ID> Unique Id to choose which of the clusters in the
 config file to run the operation against. If not provided, will fall back to the value
 provided when interactive mode was started, or error
 -h, --help Print help
```

### 範例

此命令會列出叢集中 AWS CloudHSM 針對每個服務設定的規定人數值。

#### Example

hsm1.medium :

```
aws-cloudhsm > quorum token-sign list-quorum-values
{
 "error_code": 0,
 "data": {
 "user": 1,
 "quorum": 1
 }
}
```

hsm2m.medium :

```
aws-cloudhsm > quorum token-sign list-quorum-values
{
 "error_code": 0,
 "data": {
 "user": 1,
 "quorum": 1,
 "cluster": 1
 }
}
```

## 相關主題

- [支援規定人數身分驗證的服務名稱和類型](#)
- [設定 mTLS \( 建議 \)](#)

## 使用 CloudHSM CLI 更新規定人數值

使用 CloudHSM CLI 中的 `quorum token-sign set-quorum-value` 命令為規定人數授權服務設定一個新的規定人數值。

## 使用者類型

下列使用者可以執行此命令。

- 管理員

## 語法

```
aws-cloudhsm > help quorum token-sign set-quorum-value
Set a quorum value

Usage: quorum token-sign set-quorum-value [OPTIONS] --service <SERVICE> --value <VALUE>

Options:
 --cluster-id <CLUSTER_ID>
 Unique Id to choose which of the clusters in the config file to run the
 operation against. If not provided, will fall back to the value provided when
 interactive mode was started, or error

 --service <SERVICE>
 Service the token will be used for
```

```
Possible values:
- user:
 User management service is used for executing quorum authenticated user
management operations
- quorum:
 Quorum management service is used for setting quorum values for any quorum
service
- cluster:
 Cluster management service is used for executing quorum for cluster
wide configuration managements like mtls enforcement, mtls registration and mtls
deregistration

--value <VALUE>
 Value to set for service

--approval <APPROVAL>
 Filepath of signed quorum token file to approve operation

-h, --help
 Print help (see a summary with '-h')
```

## 範例

### Example

下列範例中，此命令會將叢集中每個 HSM 的未簽署權杖寫入權杖指定的檔案。當系統提示您時，請在檔案中簽署權杖。

```
aws-cloudhsm > quorum token-sign set-quorum-value --service quorum --value 2
{
 "error_code": 0,
 "data": "Set Quorum Value successful"
}
```

然後，您可以執行 `list-quorum-values` 命令來確認規定人數管理服務的規定人數值已設定完成。

hsm1.medium :

```
aws-cloudhsm > quorum token-sign list-quorum-values
{
 "error_code": 0,
```

```
"data": {
 "user": 1,
 "quorum": 2
}
```

hsm2m.medium :

```
aws-cloudhsm > quorum token-sign list-quorum-values
{
 "error_code": 0,
 "data": {
 "user": 1,
 "quorum": 2,
 "cluster": 1
 }
}
```

## 引數

### <CLUSTER\_ID>

要執行此操作的叢集 ID。

必要：如果已[設定多個叢集](#)。

### <APPROVAL>

HSM 上待核准的已簽署權杖檔案的檔案路徑。

### <SERVICE>

指定要產生字符的規定人數授權服務。此為必要參數。如需有關服務類型和名稱的詳細資訊，請參閱[支援規定人數身分驗證的服務名稱和類型](#)。

#### 有效值

- 使用者：使用者管理服務。用於執行規定人數授權的使用者管理操作的服務。
- 規定人數：規定人數管理服務。用於為任何規定人數授權服務而設定規定人數授權的規定人數值。
- cluster：用於執行 mtls 強制執行、mtls 註冊和 mtls 取消註冊等叢集範圍組態管理的法定人數的叢集管理服務。

- 登記：產生一個未簽署權杖，用於登記規定人數授權的公有金鑰。

必要：是

<VALUE>

指定要設定的規定人數值。最大規定人數值為八 (8)。

必要：是

## 相關主題

- [規定人數字符簽署 列出規定人數值](#)
- [支援規定人數身分驗證的服務名稱和類型](#)
- [設定 mTLS \(建議\)](#)

## AWS CloudHSM Management Utility (CMU)

cloudhsm\_mgmt\_util 命令列工具可協助加密管理員管理 AWS CloudHSM 叢集硬體安全模組 (HSMs) 中的使用者。AWS CloudHSM Management Utility (CMU) 包含建立、刪除和列出使用者的工具，以及變更使用者密碼。

CMU 和金鑰管理公用程式 (KMU) 是[用戶端 SDK 3 套件](#)的一部分。用戶端 SDK 3 及其相關的命令列工具（金鑰管理公用程式和 CloudHSM 管理公用程式）僅適用於 HSM 類型 hsm1.medium。

cloudhsm\_mgmt\_util 還包含允許加密使用者 (CU) 共用金鑰以及取得和設定金鑰屬性的命令。這些命令可以補充主索引鍵管理工具 [key\\_mgmt\\_util](#) 中的金鑰管理命令。

如需快速入門，請參閱 [中的複製叢集 AWS CloudHSM](#)。如需 cloudhsm\_mgmt\_util 命令的詳細資訊以及使用命令的範例，請參閱 [AWS CloudHSM Management Utility 命令的參考](#)。

## 主題

- [AWS CloudHSM Management Utility 支援的平台](#)
- [Management AWS CloudHSM Utility \(CMU\) 入門](#)
- [安裝和設定 CMU \(Linux\) 的 AWS CloudHSM 用戶端](#)
- [安裝和設定 CMU 的 AWS CloudHSM 用戶端 \(Windows\)](#)
- [AWS CloudHSM Management Utility 命令的參考](#)



# AWS CloudHSM Management Utility 支援的平台

本主題說明 AWS CloudHSM Management Utility (CMU) 支援的 Linux 和 Windows 平台。

## Linux 支援

- Amazon Linux
- Amazon Linux 2
- CentOS 6.10+
- CentOS 7.3+
- CentOS 8
- Red Hat Enterprise Linux (RHEL) 6.10+
- Red Hat Enterprise Linux (RHEL) 7.9+
- Red Hat Enterprise Linux (RHEL) 8
- Ubuntu 16.04 LTS
- Ubuntu 18.04 LTS

## Windows 支援

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

## Management AWS CloudHSM Utility (CMU) 入門

AWS CloudHSM Management Utility (CMU) 可讓您管理硬體安全模組 (HSM) 使用者。使用本主題可開始進行基本的 HSM 使用者管理工作，例如建立使用者、列出使用者以及將 CMU 連線到叢集。

1. 若要使用 CMU，您必須先使用設定工具，以 `--cmu` 參數和叢集中其中一個 HSM 的 IP 地址來更新本機 CMU 組態。每次使用 CMU 時，執行此操作，以確保您管理叢集中每個 HSM 上的 HSM 使用者。

## Linux

```
$ sudo /opt/cloudhsm/bin/configure --cmu <IP address>
```

## Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" --cmu <IP address>
```

2. 在互動式模式中輸入下列命令啟動 CLI。

## Linux

```
$ /opt/cloudhsm/bin/cloudhsm_mgmt_util /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

## Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cloudhsm_mgmt_util.exe" C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_mgmt_util.cfg
```

輸出應該類似如下，視您有多少個 HSM 而定。

```
Connecting to the server(s), it may take time
depending on the server(s) load, please wait...

Connecting to server '10.0.2.9': hostname '10.0.2.9', port 2225...
Connected to server '10.0.2.9': hostname '10.0.2.9', port 2225.

Connecting to server '10.0.3.11': hostname '10.0.3.11', port 2225...
Connected to server '10.0.3.11': hostname '10.0.3.11', port 2225.

Connecting to server '10.0.1.12': hostname '10.0.1.12', port 2225...
Connected to server '10.0.1.12': hostname '10.0.1.12', port 2225.
```

cloudhsm\_mgmt\_util 執行時，系統提示會切換至 aws-cloudhsm>。

3. 使用 loginHSM 命令登入叢集。任何類型的使用者都可以使用此命令來登入叢集。

以下範例中的命令以 admin 登入，這是預設的[加密管理員 \(CO\)](#)。您已在啟用叢集時設定此使用者的密碼。您可以使用 -hpswd 參數來隱藏您的密碼。

```
aws-cloudhsm>loginHSM C0 admin -hpswd
```

系統會提示您輸入密碼。您輸入密碼時，系統會隱藏密碼，並且輸出顯示命令已成功，並顯示您已連線至叢集上的所有 HSM。

```
Enter password:

loginHSM success on server 0(10.0.2.9)
loginHSM success on server 1(10.0.3.11)
loginHSM success on server 2(10.0.1.12)
```

4. 用 listUsers 來列出叢集上的所有使用者。

```
aws-cloudhsm>listUsers
```

CMU 列出了叢集上的所有使用者。

```
Users on server 0(10.0.2.9):
Number of users found:2

 User Id User Type User Name
MofnPubKey LoginFailureCnt 2FA
 1 C0 admin NO
 0 NO
 2 AU app_user NO
 0 NO

Users on server 1(10.0.3.11):
Number of users found:2

 User Id User Type User Name
MofnPubKey LoginFailureCnt 2FA
 1 C0 admin NO
 0 NO
 2 AU app_user NO
 0 NO

Users on server 2(10.0.1.12):
Number of users found:2
```

| User Id    | User Type       | User Name |    |
|------------|-----------------|-----------|----|
| MofnPubKey | LoginFailureCnt | 2FA       |    |
| 1          | CO              | admin     | NO |
|            | 0               |           | NO |
| 2          | AU              | app_user  | NO |
|            | 0               |           | NO |

5. 使用 `createUser` 來建立名為 **example\_user** 的 CU 使用者，密碼為 **password1**。

您可以在應用程式中使用 CU 使用者來執行密碼編譯和金鑰管理操作。您可以建立 CU 使用者，因為在步驟 3 中您是以 CO 使用者身分登入的。只有 CO 使用者可以使用 CMU 執行使用者管理工作，例如建立和刪除使用者，以及變更其他使用者的密碼。

```
aws-cloudhsm>createUser CU example_user password1
```

CMU 會提示您建立使用者操作。

```
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.

Do you want to continue(y/n)?
```

6. 若要建立 CU 使用者 **example\_user**，請輸入 **y**。
7. 用 `listUsers` 來列出叢集上的所有使用者。

```
aws-cloudhsm>listUsers
```

CMU 會列出叢集上的所有使用者，包括您剛建立的新 CU 使用者。

```
Users on server 0(10.0.2.9):
Number of users found:3
```

| User Id    | User Type       | User Name |
|------------|-----------------|-----------|
| MofnPubKey | LoginFailureCnt | 2FA       |

|   |   |    |    |              |  |    |
|---|---|----|----|--------------|--|----|
| 1 |   | C0 |    | admin        |  | N0 |
|   | 0 |    | N0 |              |  |    |
| 2 |   | AU |    | app_user     |  | N0 |
|   | 0 |    | N0 |              |  |    |
| 3 |   | CU |    | example_user |  | N0 |
|   | 0 |    | N0 |              |  |    |

Users on server 1(10.0.3.11):  
Number of users found:3

| User Id    |                 | User Type |     | User Name    |  |    |
|------------|-----------------|-----------|-----|--------------|--|----|
| MofnPubKey | LoginFailureCnt |           | 2FA |              |  |    |
| 1          |                 | C0        |     | admin        |  | N0 |
|            | 0               |           | N0  |              |  |    |
| 2          |                 | AU        |     | app_user     |  | N0 |
|            | 0               |           | N0  |              |  |    |
| 3          |                 | CU        |     | example_user |  | N0 |
|            | 0               |           | N0  |              |  |    |

Users on server 2(10.0.1.12):  
Number of users found:3

| User Id    |                 | User Type |     | User Name    |  |    |
|------------|-----------------|-----------|-----|--------------|--|----|
| MofnPubKey | LoginFailureCnt |           | 2FA |              |  |    |
| 1          |                 | C0        |     | admin        |  | N0 |
|            | 0               |           | N0  |              |  |    |
| 2          |                 | AU        |     | app_user     |  | N0 |
|            | 0               |           | N0  |              |  |    |
| 3          |                 | CU        |     | example_user |  | N0 |
|            | 0               |           | N0  |              |  |    |

8. 使用 logoutHSM 命令來登出 HSM。

```
aws-cloudhsm>logoutHSM

logoutHSM success on server 0(10.0.2.9)
logoutHSM success on server 1(10.0.3.11)
logoutHSM success on server 2(10.0.1.12)
```

9. 使用 quit 命令來停止 cloudhsm\_mgmt\_util。

```
aws-cloudhsm>quit
```

```
disconnecting from servers, please wait...
```

## 安裝和設定 CMU (Linux) 的 AWS CloudHSM 用戶端

若要使用 cloudhsm\_mgmt\_util (CMU) 與 AWS CloudHSM 叢集中的硬體安全模組 (HSM) 互動，您需要 Linux 的 AWS CloudHSM 用戶端軟體。您應該將它安裝在您先前建立的 Linux Amazon EC2 用戶端執行個體上。如果是使用 Windows，您也可以安裝用戶端。如需詳細資訊，請參閱[安裝和設定 CMU 的 AWS CloudHSM 用戶端 \(Windows\)](#)。

### 任務

- [步驟 1. 安裝 AWS CloudHSM 用戶端和命令列工具](#)
- [步驟 2. 編輯用戶端組態](#)

### 步驟 1. 安裝 AWS CloudHSM 用戶端和命令列工具

連線至您的用戶端執行個體並執行下列命令，以下載並安裝 AWS CloudHSM 用戶端和命令列工具。

#### Amazon Linux

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-latest.el6.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el6.x86_64.rpm
```

#### Amazon Linux 2

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-latest.el7.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el7.x86_64.rpm
```

#### CentOS 7

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-latest.el7.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el7.x86_64.rpm
```

## CentOS 8

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-latest.el8.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el8.x86_64.rpm
```

## RHEL 7

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-latest.el7.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el7.x86_64.rpm
```

## RHEL 8

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-latest.el8.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el8.x86_64.rpm
```

## Ubuntu 16.04 LTS

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-client_latest_amd64.deb
```

```
sudo apt install ./cloudhsm-client_latest_amd64.deb
```

## Ubuntu 18.04 LTS

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Bionic/cloudhsm-client_latest_u18.04_amd64.deb
```

```
sudo apt install ./cloudhsm-client_latest_u18.04_amd64.deb
```

## 步驟 2. 編輯用戶端組態

您必須編輯 AWS CloudHSM 用戶端組態，才能使用用戶端連線至叢集。

### 編輯用戶端組態

1. 如果在 cloudhsm\_mgmt\_util 上安裝用戶端 SDK 3，請完成下列步驟以確保叢集中的所有節點均已同步。
  - a. 執行 `configure -a <IP of one of the HSMs>`。
  - b. 重新啟動用戶端服務。
  - c. 執行 `configure -m`。
2. 將您的發行憑證 ([您使用此憑證來簽署叢集憑證](#)) 複製到用戶端執行個體上的這個位置：`/opt/cloudhsm/etc/customerCA.crt`。您的用戶端執行個體上需要有執行個體根使用者許可，才能將憑證複製到此位置。
3. 使用下列 [configure](#) 命令來更新 AWS CloudHSM 用戶端和命令列工具的組態檔案，並在叢集中指定 HSM 的 IP 地址。若要取得 HSM 的 IP 地址，請在 [AWS CloudHSM 主控台](#) 中檢視叢集，或執行 [describe-clusters](#) AWS CLI 命令。在命令輸出中，HSM 的 IP 地址是 `EniIp` 欄位的值。如果您有多個 HSM，請選擇任何 HSM 的 IP 地址；任何一個都可以。

```
sudo /opt/cloudhsm/bin/configure -a <IP address>
```

```
Updating server config in /opt/cloudhsm/etc/cloudhsm_client.cfg
```

```
Updating server config in /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

4. 前往 [在中啟用叢集 AWS CloudHSM](#)。



## 安裝和設定 CMU 的 AWS CloudHSM 用戶端 (Windows)

若要使用 cloudhsm\_mgmt\_util (CMU) 在 Windows 上的 AWS CloudHSM 叢集中使用硬體安全模組 (HSM)，您需要適用於 Windows 的 AWS CloudHSM 用戶端軟體。應將此軟體安裝到您先前建立的 Windows Server 執行個體。

### Note

- 如果您正在更新用戶端，系統將不會覆寫前一次安裝的現有組態檔案。
- 適用於 Windows 的 AWS CloudHSM 用戶端安裝程式會自動註冊密碼編譯 API：新一代 (CNG) 和金鑰儲存提供者 (KSP)。若要解除安裝用戶端，請再次執行安裝程式並依照解除安裝指示操作。
- 如果您使用的 Linux，也可以安裝 Linux 用戶端。如需詳細資訊，請參閱[安裝和設定 CMU \(Linux\) 的 AWS CloudHSM 用戶端](#)。

### 安裝 (或更新) 最新 Windows 用戶端和命令列工具

1. 連接至您的 Windows Server 執行個體。
2. 下載 [AWSCloudHSMClient-latest.msi installer](#)。
3. 如果在 cloudhsm\_mgmt\_util 上安裝用戶端 SDK 3，請完成下列步驟以確保叢集中的所有節點均已同步。
  - a. 執行 `configure.exe -a <IP of one of the HSMs>`。
  - b. 重新啟動用戶端服務。
  - c. 執行 `configure.exe -m`。
4. 前往下載位置，並以管理權限執行安裝程式 `AWSCloudHSMClient-latest.msi`。
5. 依照安裝程式指示操作，然後在安裝程式完成後選擇關閉。
6. 將您自己簽署的發行憑證 ([用於簽署叢集憑證的憑證](#)) 複製到 `C:\ProgramData\Amazon\CloudHSM` 資料夾。
7. 使用下列命令以更新組態檔案。如果您正在更新用戶端，務必在重新組態時停止和啟動用戶端。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" -a <HSM IP address>
```

8. 前往 [在中啟用叢集 AWS CloudHSM](#)。

## AWS CloudHSM Management Utility 命令的參考

AWS CloudHSM `cloudhsm_mgmt_util` 命令列工具可協助加密管理員管理 AWS CloudHSM 叢集硬體安全模組 (HSMs) 中的使用者。此工具還包含允許加密使用者 (CU) 共用金鑰以及取得和設定金鑰屬性的命令。這些命令可以補充 [key\\_mgmt\\_util](#) 命令列工具中的主索引鍵管理命令。

如需快速入門，請參閱 [中的複製叢集 AWS CloudHSM](#)。

您必須先啟動 `cloudhsm_mgmt_util` 並登入 HSM 後，才能執行任何 `cloudhsm_mgmt_util` 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

若要列出所有 `cloudhsm_mgmt_util` 命令，請執行以下命令：

```
aws-cloudhsm> help
```

若要取得任一 `cloudhsm_mgmt_util` 命令的語法，請執行以下命令：

```
aws-cloudhsm> help <command-name>
```

### Note

根據文件使用語法。雖然內建的軟體說明可以提供其他選項，但您不應將這些選項視為支援選項，亦不應在生產程式碼中使用。

若要執行某個命令，請輸入命令名稱，或輸入該命令與 `cloudhsm_mgmt_util` 其他命令的名稱相區別的名稱。

例如，輸入 `listUsers` 或 `listU` 均可取得 HSM 上的使用者清單。

```
aws-cloudhsm> listUsers
```

若要結束 `cloudhsm_mgmt_util` 工作階段，請執行以下命令：

```
aws-cloudhsm> quit
```

如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

下列各主題說明 `cloudhsm_mgmt_util` 中的命令。

**Note**

key\_mgmt\_util 和 cloudhsm\_mgmt\_util 中的某些命令，名稱相同。但是，這些命令通常具有不同的語法，不同的輸出和略微不同的功能。

| Command                      | 描述                                            | 使用者類型    |
|------------------------------|-----------------------------------------------|----------|
| <a href="#">changePswd</a>   | 變更 HSM 上使用者的密碼。任何使用者都可以變更自己的密碼。CO 可以變更任何人的密碼。 | CO       |
| <a href="#">createUser</a>   | 在 HSM 上建立所有類型的使用者。                            | CO       |
| <a href="#">deleteUser</a>   | 從 HSM 刪除所有類型的使用者。                             | CO       |
| <a href="#">findAllKeys</a>  | 取得使用者擁有或共用的金鑰。也可取得每個 HSM 上所有金鑰的金鑰擁有權和共用資料的雜湊。 | CO、AU    |
| <a href="#">getAttribute</a> | 取得 AWS CloudHSM 金鑰的屬性值，並將其寫入檔案或 stdout（標準輸出）。 | 加密使用者    |
| <a href="#">getHSMInfo</a>   | 取得 HSM 執行所在硬體的相關資訊。                           | 全部。無需登入。 |
| <a href="#">getKeyInfo</a>   | 取得金鑰的擁有者、共用使用者和仲裁身分驗證的狀態。                     | 全部。無需登入。 |
| <a href="#">info</a>         | 取得 HSM 的資訊，包括 IP 地址、主機名稱、連接埠和目前的使用者。          | 全部。無需登入。 |

| Command                              | 描述                               | 使用者類型    |
|--------------------------------------|----------------------------------|----------|
| <a href="#">listUsers</a>            | 取得每個 HSM 中的使用者、使用者類型和 ID，以及其他屬性。 | 全部。無需登入。 |
| <a href="#">loginHSM 和 logoutHSM</a> | 登入及登出 HSM。                       | 全部。      |
| <a href="#">quit</a>                 | 結束 cloudhsm_mgmt_util。           | 全部。無需登入。 |
| <a href="#">伺服器</a>                  | 由 HSM 上進入及結束伺服器模式。               | 全部。      |
| <a href="#">registerQuorumPubKey</a> | 將 HSM 使用者與非對稱 RSA-2048 金鑰對產生關聯。  | CO       |
| <a href="#">setAttribute</a>         | 變更現有金鑰的標籤、加密、解密、包裝和取消包裝屬性的值。     | 加密使用者    |
| <a href="#">shareKey</a>             | 與其他使用者共用現有的金鑰。                   | 加密使用者    |
| <a href="#">syncKey</a>              | 跨複製的 AWS CloudHSM 叢集同步金鑰。        | CU、CO    |
| <a href="#">syncUser</a>             | 跨複製 AWS CloudHSM 叢集同步使用者。        | CO       |

## 使用 CMU 變更使用者的密碼

使用 AWS CloudHSM cloudhsm\_mgmt\_util (CMU) 中的 changePswd 命令，變更 AWS CloudHSM 叢集中硬體安全模組 (HSM) 上現有使用者的密碼。

任何使用者都可以變更自己的密碼。此外，加密管理員 (CO 和 PCO) 可以變更其他加密管理員或加密使用者 (CU) 的密碼。您無需輸入目前的密碼即可進行變更。

 Note

您無法變更目前登入 AWS CloudHSM 用戶端或 key\_mgmt\_util 之使用者的密碼。

## changePswd 疑難排解

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列使用者可以執行此命令。

- 加密管理員 (CO)
- 加密使用者 (CU)

## 語法

依照語法圖表中指定的順序輸入引數。使用 -hpswd 參數來遮罩您的密碼。若要為 CO 使用者啟用雙重要素驗證 (2FA)，請使用 -2fa 參數並包含檔案路徑。如需詳細資訊，請參閱 [the section called “引數”](#)。

```
changePswd <user-type> <user-name> <password> [-hpswd] [-2fa </path/to/authdata>]
```

## 範例

以下範例說明如何使用 changePassword 重設 HSM 中目前使用者或任何其他使用者的密碼。

Example：變更您的密碼

HSM 上的任何使用者均可使用 changePswd 變更自己的密碼。變更密碼之前，請使用 [info](#) 取得叢集中每個 HSM 的資訊，包括使用者名稱和登入使用者的使用者類型。

以下輸出顯示 Bob 目前正以加密使用者 (CU) 的身分登入。

```
aws-cloudhsm> info server 0
```

| Id | Name       | Hostname   | Port | State     | Partition       |
|----|------------|------------|------|-----------|-----------------|
| 0  | 10.1.9.193 | 10.1.9.193 | 2225 | Connected | hsm-jqici4covtv |

LoginState  
Logged in as 'bob(CU)'

```
aws-cloudhsm> info server 1
```

| Id | Name      | Hostname  | Port | State     | Partition       |
|----|-----------|-----------|------|-----------|-----------------|
| 1  | 10.1.10.7 | 10.1.10.7 | 2225 | Connected | hsm-ogi3sywxbqx |

LoginState  
Logged in as 'bob(CU)'

為了變更密碼，Bob 執行 `changePswd` 後接使用者類型、使用者名稱和新的密碼。

```
aws-cloudhsm> changePswd CU bob newPassword
```

```
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.

```

```
Do you want to continue(y/n)?y
Changing password for bob(CU) on 2 nodes
```

Example：變更其他使用者的密碼

您必須是 CO 或 PCO 才能變更 HSM 上其他 CO 或 CU 的密碼。在變更其他使用者的密碼之前，請先使用 [info](#) 命令確認您的使用者類型為 CO 或 PCO。

以下輸出確認 Alice 目前已登入，且她是 CO。

```
aws-cloudhsm>info server 0
```

| Id | Name       | Hostname | Port | State | Partition |
|----|------------|----------|------|-------|-----------|
|    | LoginState |          |      |       |           |

```
0 10.1.9.193 10.1.9.193 2225 Connected hsm-jqici4covtv
Logged in as 'alice(C0)'
```

```
aws-cloudhsm>info server 1
```

```
Id Name Hostname Port State Partition
LoginState
0 10.1.10.7 10.1.10.7 2225 Connected hsm-ogi3sywxbqx
Logged in as 'alice(C0)'
```

Alice 想要重設其他使用者 (John) 的密碼。在變更密碼之前，她先使用 [listUsers](#) 命令來驗證 John 的使用者類型。

以下輸出列出 John 為 CO 使用者。

```
aws-cloudhsm> listUsers
```

```
Users on server 0(10.1.9.193):
```

```
Number of users found:5
```

| User Id         | User Type | User Name | MofnPubKey |   |
|-----------------|-----------|-----------|------------|---|
| LoginFailureCnt | 2FA       |           |            |   |
| 1               | PCO       | admin     | YES        | 0 |
| NO              |           |           |            |   |
| 2               | AU        | jane      | NO         | 0 |
| NO              |           |           |            |   |
| 3               | CU        | bob       | NO         | 0 |
| NO              |           |           |            |   |
| 4               | CU        | alice     | NO         | 0 |
| NO              |           |           |            |   |
| 5               | CO        | john      | NO         | 0 |
| NO              |           |           |            |   |

```
Users on server 1(10.1.10.7):
```

```
Number of users found:5
```

| User Id         | User Type | User Name | MofnPubKey |   |
|-----------------|-----------|-----------|------------|---|
| LoginFailureCnt | 2FA       |           |            |   |
| 1               | PCO       | admin     | YES        | 0 |
| NO              |           |           |            |   |
| 2               | AU        | jane      | NO         | 0 |
| NO              |           |           |            |   |

|    |    |       |    |   |
|----|----|-------|----|---|
| 3  | CU | bob   | NO | 0 |
| NO |    |       |    |   |
| 4  | CO | alice | NO | 0 |
| NO |    |       |    |   |
| 5  | CO | john  | NO | 0 |
| NO |    |       |    |   |

為了變更密碼，Alice 執行 `changePswd` 後接 John 的使用者類型、使用者名稱和新的密碼。

```
aws-cloudhsm>changePswd CO john newPassword
```

```
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.

```

```
Do you want to continue(y/n)?y
Changing password for john(CO) on 2 nodes
```

## 引數

依照語法圖表中指定的順序輸入引數。使用 `-hpswd` 參數來遮罩您的密碼。若要為 CO 使用者啟用雙重要素驗證 (2FA)，請使用 `-2fa` 參數並包含檔案路徑。如需使用 2FA 的詳細資訊，請參閱 [管理使用者 2FA](#)。

```
changePswd <user-type> <user-name> <password> [-hpswd] [-2fa </path/to/authdata>]
```

### <user-type>

指您要變更密碼之使用者的目前類型。您不能使用 `changePswd` 來變更使用者類型。

有效值為 CO、CU、PCO、PRECO。

若要取得使用者類型，請使用 [listUsers](#)。如需 HSM 上使用者類型的詳細資訊，請參閱 [AWS CloudHSM Management Utility 的 HSM 使用者類型](#)。

必要：是

### <user-name>

指使用者的易記名稱。此參數不區分大小寫。您不能使用 `changePswd` 來變更使用者名稱。



必要：是

<密碼 | -hpswd >

為使用者指定新密碼。輸入長度 7 到 32 個字元的字串。此值區分大小寫。輸入密碼時，密碼會以純文字顯示。要隱藏您的密碼，請使用 -hpswd 參數代替密碼，然後按照提示進行操作。

必要：是

[-2fa </path/to/authdata>]

指為此 CO 使用者啟用 2FA。若要取得設定 2FA 所需的資料，請在 -2fa 參數後加入檔案系統帶有檔案名稱位置的路徑。如需使用 2FA 的詳細資訊，請參閱 [管理使用者 2FA](#)。

必要：否

## 相關主題

- [info](#)
- [listUsers](#)
- [createUser](#)
- [deleteUser](#)

## 使用 CMU 建立 AWS CloudHSM 使用者

在 cloudhsm\_mgmt\_util (CMU) 中使用 createUser 命令，在 AWS CloudHSM 叢集的硬體安全模組 (HSM) 上建立使用者。只有加密管理員 (CO 和 PRECO) 可以執行此命令。命令成功時，它會在叢集的所有 HSM 中建立使用者。

### createUser 疑難排解

如果您的 HSM 組態不準確，可能不會在所有 HSM 上建立使用者。若要將使用者新增至未包含該使用者的任何 HSM，請僅在遺漏該使用者的 HSM 上使用 [syncUser](#) 或 [createUser](#) 命令。為了避免組態錯誤，請執行 [configure](#) 工具搭配 -m 選項。

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密管理員 (CO、PRECO)

## 語法

依照語法圖表中指定的順序輸入引數。使用 `-hpswd` 參數來遮罩您的密碼。若要為 CO 使用者啟用雙重要素身分驗證 (2FA)，請使用 `-2fa` 參數並包含檔案路徑。如需詳細資訊，請參閱[the section called “引數”](#)。

```
createUser <user-type> <user-name> <password> [-hpswd> [-2fa </path/to/authdata>]
```

## 範例

下列範例顯示如何使用 `createUser` 在您的 HSM 中建立新使用者。

Example：建立加密管理員

此範例會在叢集中的 HSM 上建立加密管理員 (CO)。第一個命令會使用 [loginHSM](#) 以加密管理員的身分登入 HSM。

```
aws-cloudhsm> loginHSM CO admin 735782961
```

```
loginHSM success on server 0(10.0.0.1)
```

```
loginHSM success on server 1(10.0.0.2)
```

```
loginHSM success on server 1(10.0.0.3)
```

第二個命令會使用 `createUser` 命令來建立 `alice` (即 HSM 上新的加密管理員)。

警告訊息說明該命令會在叢集中的所有 HSM 上建立使用者。但如果此命令在任何 HSM 上失敗，使用者將不會存在於那些 HSM 上。若要繼續，請輸入 `y`。

輸出顯示已在叢集中的所有三個 HSM 上建立新使用者。

```
aws-cloudhsm> createUser CO alice 391019314
```

```
*****CAUTION*****
```

```
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
```

```
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
```

```

```

```
Do you want to continue(y/n)?Invalid option, please type 'y' or 'n'
```

```
Do you want to continue(y/n)?y
```

```
Creating User alice(C0) on 3 nodes
```

命令完成時，alice 會擁有與 HSM 上與 admin CO 使用者相同的許可，包括變更 HSM 上任何使用者的密碼。

最後一個命令會使用 [listUsers](#) 命令，來驗證在叢集的所有三個 HSM 上是否存在 alice。輸出也會顯示 alice 已獲指派使用者 ID 3。您可以使用使用者 ID 來識別其他命令中的 alice，例如 [findAllKeys](#)。

```
aws-cloudhsm> listUsers
```

```
Users on server 0(10.0.0.1):
```

```
Number of users found:3
```

| User Id         | User Type | User Name | MofnPubKey |
|-----------------|-----------|-----------|------------|
| LoginFailureCnt | 2FA       |           |            |
| 1               | PRECO     | admin     | YES        |
| 0               | NO        |           |            |
| 2               | AU        | app_user  | NO         |
| 0               | NO        |           |            |
| 3               | CO        | alice     | NO         |
| 0               | NO        |           |            |

```
Users on server 1(10.0.0.2):
```

```
Number of users found:3
```

| User Id         | User Type | User Name | MofnPubKey |
|-----------------|-----------|-----------|------------|
| LoginFailureCnt | 2FA       |           |            |
| 1               | PRECO     | admin     | YES        |
| 0               | NO        |           |            |
| 2               | AU        | app_user  | NO         |
| 0               | NO        |           |            |
| 3               | CO        | alice     | NO         |
| 0               | NO        |           |            |

```
Users on server 1(10.0.0.3):
```

```
Number of users found:3
```

| User Id         | User Type | User Name | MofnPubKey |
|-----------------|-----------|-----------|------------|
| LoginFailureCnt | 2FA       |           |            |
| 1               | PRECO     | admin     | YES        |
| 0               | NO        |           |            |
| 2               | AU        | app_user  | NO         |
| 0               | NO        |           |            |
| 3               | CO        | alice     | NO         |
| 0               | NO        |           |            |

### Example：建立加密使用者

此範例會在 HSM 上建立加密使用者 (CU) bob。加密使用者可以建立和管理金鑰，但不能管理使用者。

在您輸入 y 來回應警告訊息之後，輸出會顯示已在叢集中的全部三個 HSM 上建立 bob。新 CU 可以登入 HSM 來建立和管理金鑰。

此命令使用 defaultPassword 的密碼值。之後，bob 或任何 CO 可以使用 [changePswd](#) 命令來變更他的密碼。

```
aws-cloudhsm> createUser CU bob defaultPassword
```

```
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.

Do you want to continue(y/n)?Invalid option, please type 'y' or 'n'

Do you want to continue(y/n)?y
Creating User bob(CU) on 3 nodes
```

### 引數

依照語法圖表中指定的順序輸入引數。使用 -hpswd 參數來遮罩您的密碼。若要建立啟用雙重要素驗證 (2FA) 的 CO 使用者，請使用 -2fa 參數並包含檔案路徑。如需 2FA 的詳細資訊，請參閱 [管理使用者 2FA](#)。

```
createUser <user-type> <user-name> <password> [-hpswd] [-2fa </path/to/authdata>]
```

## <user-type>

指使用者的類型。此為必要參數。

如需 HSM 上使用者類型的詳細資訊，請參閱 [AWS CloudHSM Management Utility 的 HSM 使用者類型](#)。

有效值：

- CO：加密管理員可以管理使用者，但不能管理金鑰。
- CU：加密使用者可以建立管理金鑰並在密碼編譯操作時使用該金鑰。

當您在 [HSM 啟用](#) 期間指派密碼時，PRECO 會轉換為 CO。

必要：是

## <user-name>

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。

建立使用者之後，您就無法再變更使用者的名稱。在 cloudhsm\_mgmt\_util 命令中，使用者類型和密碼需區分大小寫，但使用者名稱不區分大小寫。

必要：是

## <密碼 | -hpswd >

為使用者指定密碼。輸入長度 7 到 32 個字元的字串。此值區分大小寫。輸入密碼時，密碼會以純文字顯示。要隱藏您的密碼，請使用 -hpswd 參數代替密碼，然後按照提示進行操作。

若要變更使用者密碼，請使用 [changePswd](#)。任何 HSM 使用者可以變更自己的密碼，但 CO 使用者可以變更 HSM 上任何使用者 (任何類型) 的密碼。

必要：是

## [-2fa </path/to/authdata>]

指建立已啟用 2FA 的 CO 使用者。若要取得設定 2FA 驗證所需資料，請在 -2fa 參數後加入檔案系統帶有檔案名稱位置的路徑。如需設定並使用 2FA 的詳細資訊，請參閱 [管理使用者 2FA](#)。

必要：否

## 相關主題

- [listUsers](#)

- [deleteUser](#)
- [syncUser](#)
- [changePswd](#)

## 使用 CMU 刪除 AWS CloudHSM 使用者

使用 AWS CloudHSM `cloudhsm_mgmt_util` (CMU) 中的 `deleteUser` 命令，從 AWS CloudHSM 叢集中的硬體安全模組 (HSM) 刪除使用者。只有加密管理員 (CO) 可以執行此命令。您無法刪除目前登入 HSM 的使用者。如需刪除使用者的詳細資訊，請參閱[如何刪除 HSM 使用者](#)。



Tip

您無法刪除擁有金鑰的加密使用者 (CU)。

## 使用者類型

下列類型的使用者可以執行此命令。

- CO

## 語法

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
deleteUser <user-type> <user-name>
```

## 範例

此範例會從叢集的 HSM 刪除加密管理員 (CO)。第一個命令使用 [listUsers](#) 列出 HSM 上的所有使用者。

輸出顯示使用者 3 (alice) 是 HSM 上的 CO。

```
aws-cloudhsm> listUsers
Users on server 0(10.0.0.1):
Number of users found:3
```

| User Id | User Type | User Name | MofnPubKey |
|---------|-----------|-----------|------------|
| 1       | PC0       | admin     | YES        |
| 0       | N0        |           |            |
| 2       | AU        | app_user  | N0         |
| 0       | N0        |           |            |
| 3       | C0        | alice     | N0         |
| 0       | N0        |           |            |

Users on server 1(10.0.0.2):

Number of users found:3

| User Id | User Type | User Name | MofnPubKey |
|---------|-----------|-----------|------------|
| 1       | PC0       | admin     | YES        |
| 0       | N0        |           |            |
| 2       | AU        | app_user  | N0         |
| 0       | N0        |           |            |
| 3       | C0        | alice     | N0         |
| 0       | N0        |           |            |

Users on server 1(10.0.0.3):

Number of users found:3

| User Id | User Type | User Name | MofnPubKey |
|---------|-----------|-----------|------------|
| 1       | PC0       | admin     | YES        |
| 0       | N0        |           |            |
| 2       | AU        | app_user  | N0         |
| 0       | N0        |           |            |
| 3       | C0        | alice     | N0         |
| 0       | N0        |           |            |

第二個命令使用 `deleteUser` 命令以從 HSM 刪除 `alice`。

輸出顯示命令在叢集中的三個 HSM 上均成功。

```
aws-cloudhsm> deleteUser C0 alice
Deleting user alice(C0) on 3 nodes
deleteUser success on server 0(10.0.0.1)
deleteUser success on server 0(10.0.0.2)
deleteUser success on server 0(10.0.0.3)
```

最後一個命令使用 `listUsers` 命令，來驗證已從叢集上的所有三個 HSM 中刪除 `alice`。

```
aws-cloudhsm> listUsers
```

```
Users on server 0(10.0.0.1):
```

```
Number of users found:2
```

| User Id         | User Type | User Name | MofnPubKey |
|-----------------|-----------|-----------|------------|
| LoginFailureCnt | 2FA       |           |            |
| 1               | PC0       | admin     | YES        |
| 0               | N0        |           |            |
| 2               | AU        | app_user  | N0         |
| 0               | N0        |           |            |

```
Users on server 1(10.0.0.2):
```

```
Number of users found:2
```

| User Id         | User Type | User Name | MofnPubKey |
|-----------------|-----------|-----------|------------|
| LoginFailureCnt | 2FA       |           |            |
| 1               | PC0       | admin     | YES        |
| 0               | N0        |           |            |
| 2               | AU        | app_user  | N0         |
| 0               | N0        |           |            |

```
Users on server 1(10.0.0.3):
```

```
Number of users found:2
```

| User Id         | User Type | User Name | MofnPubKey |
|-----------------|-----------|-----------|------------|
| LoginFailureCnt | 2FA       |           |            |
| 1               | PC0       | admin     | YES        |
| 0               | N0        |           |            |
| 2               | AU        | app_user  | N0         |
| 0               | N0        |           |            |

## 引數

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
deleteUser <user-type> <user-name>
```

### <user-type>

指使用者的類型。此為必要參數。

#### Tip

您無法刪除擁有金鑰的加密使用者 (CU)。



有效值為 CO、CU。

若要取得使用者類型，請使用 [listUsers](#)。如需 HSM 上使用者類型的詳細資訊，請參閱 [AWS CloudHSM Management Utility 的 HSM 使用者類型](#)。

必要：是

<user-name>

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。

建立使用者之後，您就無法再變更使用者的名稱。在 cloudhsm\_mgmt\_util 命令中，使用者類型和密碼需區分大小寫，但使用者名稱不區分大小寫。

必要：是

## 相關主題

- [listUsers](#)
- [createUser](#)
- [syncUser](#)
- [changePswd](#)

## 列出 AWS CloudHSM 加密使用者使用 CMU 擁有的金鑰

使用 AWS CloudHSM cloudhsm\_mgmt\_util (CMU) 中的 findAllKeys 命令，取得指定加密使用者 (CU) AWS CloudHSM 擁有或共用的金鑰。命令也會傳回每個 HSMs 上使用者資料的雜湊。有關使用者、金鑰擁有權和金鑰共用資料在叢集的所有 HSM 上是否都相同，此雜湊可讓您一目了然。在輸出中，由使用者擁有的金鑰會由 (o) 註釋，且共用金鑰會由 (s) 註釋。

即使 HSM 上的所有 CU 可以使用任何公有金鑰，只有當指定的 CU 擁有金鑰時，findAllKeys 才會傳回公有金鑰。此行為不同於 key\_mgmt\_util 中的 [findKey](#)，此命令會傳回所有 CU 使用者的公有金鑰。

只有加密主管 (CO 和 PCO) 和設備使用者 (AU) 才可以執行此命令。加密使用者 (CU) 可執行以下命令：

- [listUsers](#) 尋找所有使用者
- 在 key\_mgmt\_util 中 [findKey](#) 可查找他們可以使用的金鑰
- 在 [key\\_mgmt\\_util](#) 中 getKeyInfo 查找他們擁有或共用的特定金鑰的擁有者或共用使用者

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列使用者可以執行此命令。

- 加密管理員 (CO、PCO)
- 設備使用者 (AU)

## 語法

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
findAllKeys <user id> <key hash (0/1)> [<output file>]
```

## 範例

這些範例示範如何使用 `findAllKeys` 尋找每個 HSM 上使用者的所有金鑰，以及取得金鑰使用者資訊的雜湊。

### Example：尋找 CU 的金鑰

此範例使用 `findAllKeys`，在 HSM 中尋找使用者 4 所擁有和共用的金鑰。此命令使用 0 做為第二個引數的值，以隱藏雜湊值。由於省略選用的檔案名稱，此命令會寫入 `stdout` (標準輸出)。

輸出顯示使用者 4 可以使用 6 個金鑰：8、9、17、262162、19 和 31。輸出會使用 (s) 指出由使用者明確共用的金鑰。使用者擁有的金鑰由 (o) 指定，並包含使用者不共享的對稱和私有金鑰，以及可供所有加密使用者使用的公有金鑰。

```
aws-cloudhsm> findAllKeys 4 0
Keys on server 0(10.0.0.1):
Number of keys found 6
number of keys matched from start index 0::6
8(s),9(s),17,262162(s),19(o),31(o)
findAllKeys success on server 0(10.0.0.1)

Keys on server 1(10.0.0.2):
```

```
Number of keys found 6
number of keys matched from start index 0::6
8(s),9(s),17,262162(s),19(o),31(o)
findAllKeys success on server 1(10.0.0.2)
```

```
Keys on server 1(10.0.0.3):
Number of keys found 6
number of keys matched from start index 0::6
8(s),9(s),17,262162(s),19(o),31(o)
findAllKeys success on server 1(10.0.0.3)
```

### Example：驗證使用者資料已同步

此範例使用 `findAllKeys`，以驗證叢集中的所有 HSM 是否包含相同的使用者、金鑰擁有權和金鑰共用值。為了這樣做，此範例取得每個 HSM 上的金鑰使用者資料雜湊並比較雜湊值。

為了取得金鑰雜湊，此命令使用第二個引數中的 1 值。由於選用的檔案名稱已遭省略，此命令會將金鑰雜湊寫入 `stdout`。

此範例指定使用者 6，但對於 HSM 上擁有或共用任何金鑰的任何使用者，雜湊值都相同。如果指定的使用者未擁有或共用任何金鑰，例如 CO，則此命令不會傳回雜湊值。

輸出顯示叢集內的兩個 HSM 具有相同的金鑰雜湊。如果其中一個 HSM 有不同的使用者、不同的金鑰擁有者或不同的共用使用者，則雜湊值就不相等。

```
aws-cloudhsm> findAllKeys 6 1
Keys on server 0(10.0.0.1):
Number of keys found 3
number of keys matched from start index 0::3
8(s),9(s),11,17(s)
Key Hash:
55655676c95547fd4e82189a072ee1100eccfca6f10509077a0d6936a976bd49

findAllKeys success on server 0(10.0.0.1)
Keys on server 1(10.0.0.2):
Number of keys found 3
number of keys matched from start index 0::3
8(s),9(s),11(o),17(s)
Key Hash:
55655676c95547fd4e82189a072ee1100eccfca6f10509077a0d6936a976bd49

findAllKeys success on server 1(10.0.0.2)
```

此命令示範雜湊值代表 HSM 上所有金鑰的使用者資料。此命令針對使用者 3 使用 `findAllKeys`。與使用者 6 不同 (只擁有或共用 3 個金鑰)，使用者 3 擁有或共用 17 個金鑰，但金鑰雜湊值相同。

```
aws-cloudhsm> findAllKeys 3 1
Keys on server 0(10.0.0.1):
Number of keys found 17
number of keys matched from start index 0::17
6(o),7(o),8(s),11(o),12(o),14(o),262159(o),262160(o),17(s),262162(s),19(s),20(o),21(o),262177(o)
Key Hash:
55655676c95547fd4e82189a072ee1100eccfca6f10509077a0d6936a976bd49

findAllKeys success on server 0(10.0.0.1)
Keys on server 1(10.0.0.2):
Number of keys found 17
number of keys matched from start index 0::17
6(o),7(o),8(s),11(o),12(o),14(o),262159(o),262160(o),17(s),262162(s),19(s),20(o),21(o),262177(o)
Key Hash:
55655676c95547fd4e82189a072ee1100eccfca6f10509077a0d6936a976bd49

findAllKeys success on server 1(10.0.0.2)
```

## 引數

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
findAllKeys <user id> <key hash (0/1)> [<output file>]
```

### <user id>

取得指定之使用者擁有或共用的所有金鑰。輸入 HSM 上某個使用者的使用者 ID。若要尋找所有使用者的使用者 ID，請使用 [listUsers](#)。

所有使用者 ID 都有效，但 `findAllKeys` 只會傳回加密使用者 (CU) 的金鑰。

必要：是

### <key hash>

納入 (1) 或排除 (0) 每個 HSM 中所有金鑰的使用者擁有權和共用資料的雜湊。

`user id` 引數代表擁有或共用金鑰的使用者時，將會填入金鑰雜湊。對於 HSM 上擁有或共用金鑰的所有使用者，即使他們擁有和共用不同的金鑰，金鑰雜湊值也都相同。不過，當 `user id` 代表未擁有或共用任何金鑰的使用者時 (例如 CO)，就不會填入雜湊值。

必要：是

<output file>

將輸出寫入指定的檔案。

必要：否

預設：Stdout

## 相關主題

- [changePswd](#)
- [deleteUser](#)
- [listUsers](#)
- [syncUser](#)
- key\_mgmt\_util 中的 [findKey](#)
- key\_mgmt\_util 中的 [getKeyInfo](#)

## 使用 CMU 取得 AWS CloudHSM 金鑰屬性值

使用 AWS CloudHSM cloudhsm\_mgmt\_util (CMU) 中的 `getAttribute` 命令，從 AWS CloudHSM 叢集中的所有硬體安全模組 (HSM) 取得金鑰的一個屬性值，並將其寫入 stdout (標準輸出) 或檔案。只有加密使用者 (CU) 可以執行此命令。

金鑰屬性是金鑰的屬性。其中包括的特性，例如金鑰類型、類別、標籤和 ID，以及代表您可對金鑰執行之動作的值，例如加密、解密、包裝、取消包裝和驗證。

您只可以對您擁有的金鑰和與您共用的金鑰使用 `getAttribute`。您可以執行此命令或 `key_mgmt_util` 中的 [getAttribute](#) 命令，將金鑰的一個或所有屬性值寫入檔案。

若要取得屬性的清單和代表它們的常數，請使用 [listAttributes](#) 命令。若要變更現有金鑰的屬性值，請使用 `key_mgmt_util` 中的 [setAttribute](#) 和 `cloudhsm_mgmt_util` 中的 [setAttribute](#)。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列使用者可以執行此命令。

- 加密使用者 (CU)

## 語法

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
getAttribute <key handle> <attribute id> [<filename>]
```

## 範例

此範例在 HSM 中取得金鑰之可擷取屬性的值。您可以使用如下命令，以判斷您是否可以從 HSM 匯出金鑰。

第一個命令使用 [listAttributes](#)，以尋找代表可擷取之屬性的常數。輸出顯示 OBJ\_ATTR\_EXTRACTABLE 的常數是 354。您也可以在此[AWS CloudHSM KMU 的金鑰屬性參考](#)中找到這項資訊以及屬性和其值的描述。

```
aws-cloudhsm> listAttributes
```

Following are the possible attribute values for getAttribute:

|                    |       |
|--------------------|-------|
| OBJ_ATTR_CLASS     | = 0   |
| OBJ_ATTR_TOKEN     | = 1   |
| OBJ_ATTR_PRIVATE   | = 2   |
| OBJ_ATTR_LABEL     | = 3   |
| OBJ_ATTR_TRUSTED   | = 134 |
| OBJ_ATTR_KEY_TYPE  | = 256 |
| OBJ_ATTR_ID        | = 258 |
| OBJ_ATTR_SENSITIVE | = 259 |
| OBJ_ATTR_ENCRYPT   | = 260 |
| OBJ_ATTR_DECRYPT   | = 261 |
| OBJ_ATTR_WRAP      | = 262 |
| OBJ_ATTR_UNWRAP    | = 263 |
| OBJ_ATTR_SIGN      | = 264 |
| OBJ_ATTR_VERIFY    | = 266 |
| OBJ_ATTR_DERIVE    | = 268 |
| OBJ_ATTR_LOCAL     | = 355 |

|                            |              |
|----------------------------|--------------|
| OBJ_ATTR_MODULUS           | = 288        |
| OBJ_ATTR_MODULUS_BITS      | = 289        |
| OBJ_ATTR_PUBLIC_EXPONENT   | = 290        |
| OBJ_ATTR_VALUE_LEN         | = 353        |
| OBJ_ATTR_EXTRACTABLE       | = 354        |
| OBJ_ATTR_NEVER_EXTRACTABLE | = 356        |
| OBJ_ATTR_ALWAYS_SENSITIVE  | = 357        |
| OBJ_ATTR_DESTROYABLE       | = 370        |
| OBJ_ATTR_KCV               | = 371        |
| OBJ_ATTR_WRAP_WITH_TRUSTED | = 528        |
| OBJ_ATTR_WRAP_TEMPLATE     | = 1073742353 |
| OBJ_ATTR_UNWRAP_TEMPLATE   | = 1073742354 |
| OBJ_ATTR_ALL               | = 512        |

第二個命令使用 `getAttribute`，在 HSM 中取得金鑰 (金鑰控點為 262170) 之可擷取屬性的值。為了指定可擷取屬性，此命令使用 354，這是代表屬性的常數。因為此命令未指定檔案名稱，所以 `getAttribute` 會將輸出寫入 `stdout`。

輸出顯示在所有 HSM 上，可擷取之屬性的值都是 1。這個值表示金鑰擁有者可以匯出金鑰。當值為 0 (0x0) 時，表示無法從 HSM 匯出金鑰。您在建立金鑰時會設定可擷取屬性的值，但無法變更。

```
aws-cloudhsm> getAttribute 262170 354
```

```
Attribute Value on server 0(10.0.1.10):
```

```
OBJ_ATTR_EXTRACTABLE
0x00000001
```

```
Attribute Value on server 1(10.0.1.12):
```

```
OBJ_ATTR_EXTRACTABLE
0x00000001
```

```
Attribute Value on server 2(10.0.1.7):
```

```
OBJ_ATTR_EXTRACTABLE
0x00000001
```

## 引數

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
getAttribute <key handle> <attribute id> [<filename>]
```

## <key-handle>

指定目標金鑰的金鑰控制代碼。每一個命令中只能指定一個金鑰。若要取得金鑰的金鑰控制代碼，請在 `key_mgmt_util` 中使用 [findKey](#)。

您必須擁有或共用指定的金鑰。若要尋找金鑰的使用者，請在 `key_mgmt_util` 中使用 [getKeyInfo](#)。

必要：是

## <attribute id>

識別屬性。輸入代表屬性的常數，或輸入 512 來代表所有屬性。例如，若要取得金鑰類型，請輸入 256，此常數代表 `OBJ_ATTR_KEY_TYPE` 屬性。

若要列出屬性及其常數，請使用 [listAttributes](#)。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

必要：是

## <filename>

將輸出寫入指定的檔案。輸入檔案路徑。

如果指定的檔案已存在，`getAttribute` 會覆寫檔案且不會警告。

必要：否

預設：Stdout

## 相關主題

- `key_mgmt_util` 中的 [getAttribute](#)
- [listAttributes](#)
- `cloudhsm_mgmt_util` 中的 [setAttribute](#)
- `key_mgmt_util` 中的 [setAttribute](#)
- [金鑰屬性參考](#)

## 使用 CMU 取得 AWS CloudHSM 叢集中每個 HSM 的硬體資訊

使用 AWS CloudHSM `cloudhsm_mgmt_util` (CMU) 中的 `getHSMInfo` 命令，取得每個硬體安全模組 (HSM) 執行之硬體的相關資訊，包括硬體和韌體的模型、序號、FIPS 狀態、記憶體、溫度和版本編號。此資訊還包括可讓 `cloudhsm_mgmt_util` 用來參考 HSM 的伺服器 ID。



啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列類型的使用者可以執行此命令。

- 所有使用者。您無須登入即可執行此命令。

## 語法

此命令沒有任何參數。

```
getHSMInfo
```

## 範例

此範例使用 `getHSMInfo`，以取得叢集中 HSM 的相關資訊。

```
aws-cloudhsm> getHSMInfo
Getting HSM Info on 3 nodes
*** Server 0 HSM Info ***

Label :cavium
Model :NITROX-III CNN35XX-NFBE

Serial Number :3.0A0101-ICM000001
HSM Flags :0
FIPS state :2 [FIPS mode with single factor authentication]

Manufacturer ID :
Device ID :10
Class Code :100000
System vendor ID :177D
SubSystem ID :10

TotalPublicMemory :560596
FreePublicMemory :294568
```

```

TotalPrivateMemory :0
FreePrivateMemory :0

Hardware Major :3
Hardware Minor :0

Firmware Major :2
Firmware Minor :03

Temperature :56 C

Build Number :13

Firmware ID :xxxxxxxxxxxxxxxx

```

...

## 相關主題

- [info](#)

## 使用 CMU 取得金鑰的使用者 AWS CloudHSM 資訊

使用 AWS CloudHSM `key_mgmt_util` (KMU) 中的 `getKeyInfo` 命令，傳回可以使用金鑰之使用者的硬體安全模組 (HSM) 使用者 IDs，包括共用金鑰的擁有者和加密使用者 (CU)。對金鑰啟用規定人數身分驗證時，`getKeyInfo` 也會傳回必須核准使用該金鑰的加密操作的使用者數量。您只可以對您擁有的金鑰以及與您共用的金鑰執行 `getKeyInfo`。

當您對公有金鑰執行 `getKeyInfo` 時，即使 HSM 的所有使用者都可以使用該公有金鑰，`getKeyInfo` 只會傳回該金鑰擁有者。若要尋找 HSM 中使用者的 HSM 使用者 ID，請使用 [listUsers](#)。若要找出特定使用者的金鑰，請使用 `key_mgmt_util` 中的 [findKey](#) -u。加密管理員可以在 `cloudhsm_mgmt_util` 中使用 [findAllKeys](#)。

您擁有您建立的金鑰。您可以在建立金鑰時與其他使用者共用金鑰。之後，若要共用或取消共用現有的金鑰，請使用 `cloudhsm_mgmt_util` 中的 [shareKey](#)。

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 語法

```
getKeyInfo -k <key-handle> [<output file>]
```

## 範例

這些範例顯示如何使用 getKeyInfo，以取得金鑰使用者的相關資訊。

Example：取得非對稱金鑰的使用者

此命令會取得可以對金鑰控制代碼 262162 使用 AES (非對稱) 金鑰的使用者。輸出顯示使用者 3 擁有金鑰，並且已將它與使用者 4 和使用者 6 共用。

只有使用者 3、4 和 6 可以對金鑰 262162 執行 getKeyInfo。

```
aws-cloudhsm>getKeyInfo 262162
Key Info on server 0(10.0.0.1):

 Token/Flash Key,

 Owned by user 3

 also, shared to following 2 user(s):

 4
 6
Key Info on server 1(10.0.0.2):

 Token/Flash Key,

 Owned by user 3

 also, shared to following 2 user(s):

 4
```

**Example**：取得對稱金鑰對的使用者

這些命令使用 `getKeyInfo`，以取得可以在 [ECC \(對稱\) 金鑰對](#) 中使用金鑰的使用者。公有金鑰具有金鑰控制代碼 262179。私有金鑰具有金鑰控制代碼 262177。

對私有金鑰 (262177) 執行 `getKeyInfo` 時，它會傳回金鑰擁有者 (3) 以及與其共用金鑰的加密使用者 (CU) 4。

```
aws-cloudhsm>getKeyInfo -k 262177
Key Info on server 0(10.0.0.1):

 Token/Flash Key,

 Owned by user 3

 also, shared to following 1 user(s):

 4
Key Info on server 1(10.0.0.2):

 Token/Flash Key,

 Owned by user 3

 also, shared to following 1 user(s):

 4
```

對公有金鑰 (262179) 執行 `getKeyInfo` 時，只會傳回金鑰擁有者 (使用者 3)。

```
aws-cloudhsm>getKeyInfo -k 262179
Key Info on server 0(10.0.3.10):

 Token/Flash Key,

 Owned by user 3

Key Info on server 1(10.0.3.6):

 Token/Flash Key,
```

Owned by user 3

若要確認使用者 4 可以使用該公有金鑰 (和 HSM 上的所有公開金鑰)，請使用 `key_mgmt_util` 中 [findKey](#) 的 `-u` 參數。

輸出示範使用者 4 可以同時使用金鑰對中的公開 (262179) 與私密 (262177) 金鑰。使用者 4 也可以使用它們所建立或與其共用的所有其他公開金鑰和任何私密金鑰。

```
Command: findKey -u 4
```

```
Total number of keys present 8
```

```
number of keys matched from start index 0::7
11, 12, 262159, 262161, 262162, 19, 20, 21, 262177, 262179
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS
```

Example：取得金鑰的規定人數身分驗證值 (`m_value`)

此範例示範如何取得金鑰的 `m_value`。`m_value` 為規定人數中的使用者數量，這些使用者必須核准使用該金鑰的任何密碼編譯操作與共用和取消共用金鑰的操作。

對金鑰啟用了仲裁身分驗證時，必須有仲裁的使用者核准使用該金鑰的任何密碼編譯操作。若要啟用規定人數驗證並設定規定人數數量，建立金鑰時請使用 `-m_value` 參數。

此命令會使用 [genSymKey](#) 來建立與使用者 4 共用的 256 位元 AES 金鑰對。它會使用 `m_value` 參數來啟用規定人數驗證，並將仲裁大小設定為兩個使用者。必須有足夠多的使用者，才能提供所需的核准。

輸出顯示此命令建立了金鑰 10。

```
Command: genSymKey -t 31 -s 32 -l aes256m2 -u 4 -m_value 2
```

```
Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS
```

```
Symmetric Key Created. Key Handle: 10
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

此命令使用 `cloudhsm_mgmt_util` 中的 `getKeyInfo` 以取得金鑰 10 使用者的相關資訊。輸出顯示使用者 3 擁有該金鑰，並且將它與使用者 4 共用。它還示範兩個使用者的規定人數必須核准使用該金鑰的每個密碼編譯操作。

```
aws-cloudhsm>getKeyInfo 10

Key Info on server 0(10.0.0.1):

 Token/Flash Key,

 Owned by user 3

 also, shared to following 1 user(s):

 4
 2 Users need to approve to use/manage this key
Key Info on server 1(10.0.0.2):

 Token/Flash Key,

 Owned by user 3

 also, shared to following 1 user(s):

 4
 2 Users need to approve to use/manage this key
```

## 引數

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
getKeyInfo -k <key-handle> <output file>
```

### <key-handle>

指定 HSM 中某個金鑰的金鑰控制代碼。輸入您擁有或共用的金鑰的金鑰控制代碼。此為必要參數。

必要：是

## <output file>

將輸出寫入指定的檔案，而非 stdout。如果檔案存在，命令會覆寫檔案且不會有任何警告。

必要：否

預設：stdout

## 相關主題

- key\_mgmt\_util 中的 [getKeyInfo](#)
- key\_mgmt\_util 中的 [findKey](#)
- cloudhsm\_mgmt\_util 中的 [findAllKeys](#)
- [listUsers](#)
- [shareKey](#)

## 使用 CMU 取得 AWS CloudHSM 叢集中每個 HSM 的資訊

使用 AWS CloudHSM cloudhsm\_mgmt\_util (CMU) 中的 info 命令，取得 AWS CloudHSM 叢集中每個硬體安全模組 (HSM) 的相關資訊，包括主機名稱、連接埠、IP 地址，以及登入 HSM 上的 cloudhsm\_mgmt\_util 之使用者的名稱和類型。

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列類型的使用者可以執行此命令。

- 所有使用者。您無須登入即可執行此命令。

## 語法

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
info server <server ID>
```

## 範例

此範例使用 `info`，以取得叢集中 HSM 的相關資訊。此命令使用 0 表示叢集中的第一個 HSM。輸出顯示 IP 地址、連接埠以及目前使用者的類型和名稱。

```
aws-cloudhsm> info server 0
```

| Id | Name                        | Hostname | Port | State     | Partition       |
|----|-----------------------------|----------|------|-----------|-----------------|
|    | LoginState                  |          |      |           |                 |
| 0  | 10.0.0.1                    | 10.0.0.1 | 2225 | Connected | hsm-udw0tkfg1ab |
|    | Logged in as 'testuser(CU)' |          |      |           |                 |

## 引數

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
info server <server ID>
```

### <server id>

指定 HSM 的伺服器 ID。序號指派給 HSM，代表 HSM 新增到叢集的順序 (從 0 開始)。若要尋找 HSM 的伺服器 ID，請使用 `getHSMInfo`。

必要：是

## 相關主題

- [getHSMInfo](#)
- [loginHSM 和 logoutHSM](#)

## 使用 CMU 列出 AWS CloudHSM 金鑰的屬性

使用 AWS CloudHSM `cloudhsm_mgmt_util` (CMU) 中的 `listAttributes` 命令來列出 AWS CloudHSM 金鑰的屬性以及代表它們的常數。您可以使用這些常數來識別 [getAttribute](#) 和 [setAttribute](#) 命令中的屬性。

如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。



## 使用者類型

下列使用者可以執行此命令。

- 所有使用者。您無須登入即可執行此命令。

## 語法

```
listAttributes [-h]
```

## 範例

此命令可列出您在 `key_mgmt_util` 中可取得和變更的金鑰屬性，以及代表這些屬性的常數。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。若要代表所有屬性，請使用 512。

Command: **listAttributes**

Description

=====

The following are all of the possible attribute values for `getAttribute`.

|                          |       |
|--------------------------|-------|
| OBJ_ATTR_CLASS           | = 0   |
| OBJ_ATTR_TOKEN           | = 1   |
| OBJ_ATTR_PRIVATE         | = 2   |
| OBJ_ATTR_LABEL           | = 3   |
| OBJ_ATTR_TRUSTED         | = 134 |
| OBJ_ATTR_KEY_TYPE        | = 256 |
| OBJ_ATTR_ID              | = 258 |
| OBJ_ATTR_SENSITIVE       | = 259 |
| OBJ_ATTR_ENCRYPT         | = 260 |
| OBJ_ATTR_DECRYPT         | = 261 |
| OBJ_ATTR_WRAP            | = 262 |
| OBJ_ATTR_UNWRAP          | = 263 |
| OBJ_ATTR_SIGN            | = 264 |
| OBJ_ATTR_VERIFY          | = 266 |
| OBJ_ATTR_DERIVE          | = 268 |
| OBJ_ATTR_LOCAL           | = 355 |
| OBJ_ATTR_MODULUS         | = 288 |
| OBJ_ATTR_MODULUS_BITS    | = 289 |
| OBJ_ATTR_PUBLIC_EXPONENT | = 290 |
| OBJ_ATTR_VALUE_LEN       | = 353 |
| OBJ_ATTR_EXTRACTABLE     | = 354 |

|                            |              |
|----------------------------|--------------|
| OBJ_ATTR_NEVER_EXTRACTABLE | = 356        |
| OBJ_ATTR_ALWAYS_SENSITIVE  | = 357        |
| OBJ_ATTR_DESTROYABLE       | = 370        |
| OBJ_ATTR_KCV               | = 371        |
| OBJ_ATTR_WRAP_WITH_TRUSTED | = 528        |
| OBJ_ATTR_WRAP_TEMPLATE     | = 1073742353 |
| OBJ_ATTR_UNWRAP_TEMPLATE   | = 1073742354 |
| OBJ_ATTR_ALL               | = 512        |

## 參數

-h

顯示命令的說明。

必要：是

## 相關主題

- [getAttribute](#)
- [setAttribute](#)
- [金鑰屬性參考](#)

## 列出使用 CMU 的 AWS CloudHSM 所有使用者

使用 AWS CloudHSM `cloudhsm_mgmt_util` 中的 `listUsers` 命令，取得每個硬體安全模組 (HSM) 中的使用者，以及其使用者類型和其他屬性。所有類型的使用者可以執行此命令。您甚至不需要登入 `cloudhsm_mgmt_util` 即可執行此命令。

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列類型的使用者可以執行此命令。

- 所有使用者。您無須登入即可執行此命令。

## 語法

此命令沒有任何參數。

```
listUsers
```

## 範例

此命令列出叢集的每一個 HSM 上的使用者，並顯示其屬性。您可以在其他命令中 (例如 deleteUser、changePswd 和 findAllKeys) 使用 User ID 屬性來識別使用者。

```
aws-cloudhsm> listUsers
Users on server 0(10.0.0.1):
Number of users found:6
```

| User Id | User Type | User Name    | MofnPubKey |   |
|---------|-----------|--------------|------------|---|
| 1       | PC0       | admin        | YES        | 0 |
| NO      |           |              |            |   |
| 2       | AU        | app_user     | N0         | 0 |
| NO      |           |              |            |   |
| 3       | CU        | crypto_user1 | N0         | 0 |
| NO      |           |              |            |   |
| 4       | CU        | crypto_user2 | N0         | 0 |
| NO      |           |              |            |   |
| 5       | C0        | officer1     | YES        | 0 |
| NO      |           |              |            |   |
| 6       | C0        | officer2     | N0         | 0 |
| NO      |           |              |            |   |

```
Users on server 1(10.0.0.2):
Number of users found:5
```

| User Id | User Type | User Name    | MofnPubKey |   |
|---------|-----------|--------------|------------|---|
| 1       | PC0       | admin        | YES        | 0 |
| NO      |           |              |            |   |
| 2       | AU        | app_user     | N0         | 0 |
| NO      |           |              |            |   |
| 3       | CU        | crypto_user1 | N0         | 0 |
| NO      |           |              |            |   |

|    |    |              |     |   |
|----|----|--------------|-----|---|
| 4  | CU | crypto_user2 | NO  | 0 |
| NO |    |              |     |   |
| 5  | CO | officer1     | YES | 0 |
| NO |    |              |     |   |

輸出包含下列使用者屬性：

- 使用者 ID：在 `key_mgmt_util` 和 [cloudhsm\\_mgmt\\_util](#) 命令中識別使用者。
- [使用者類型](#)：決定使用者在 HSM 上可執行的操作。
- 使用者名稱：顯示使用者定義的使用者易記名稱。
- `MofnPubKey`：指出使用者是否已註冊金鑰對來簽署[仲裁身分驗證權杖](#)。
- `LoginFailureCnt`：表示使用者登入失敗的次數。
- `2FA`：指出使用者已啟用多重要素驗證。

## 相關主題

- `key_mgmt_util` 中的 [listUsers](#)
- [createUser](#)
- [deleteUser](#)
- [changePswd](#)

## 使用 AWS CloudHSM Management Utility 登入和登出 HSM

使用 `cloudhsm_mgmt_util` 中的 AWS CloudHSM `loginHSM` 和 `logoutHSM` 命令來登入和登出叢集中的每個 HSM。任何類型的任何使用者都可以使用這些命令。

### Note

如果您錯誤登入超過 5 次，系統將鎖定您的帳戶。若要解除鎖定帳戶，加密管理員 (CO) 必須在 `cloudhsm_mgmt_util` 中使用 [changePswd](#) 命令來重設您的密碼。

## loginHSM 和 logoutHSM 疑難排解

您必須先啟動 `cloudhsm_mgmt_util`，然後再執行這些 `cloudhsm_mgmt_util` 命令。

如果您新增或刪除 HSMs，請更新 AWS CloudHSM 用戶端和命令列工具使用的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

如果您在叢集中有多個 HSM，系統將允許您再嘗試登入幾次，若均登入錯誤，系統才會鎖定您的賬戶。這是因為 CloudHSM 用戶端可平衡各個 HSM 之間的負載。因此，每次登入嘗試可能會在不同的 HSM 上開始。如果您正在測試此功能，建議您在只有一個作用中 HSM 的叢集上執行此操作。

如果您在 2018 年 2 月前建立叢集，則系統將在您 20 次錯誤登入後鎖定您的賬戶。

## 使用者類型

下列使用者可以執行這些命令。

- 加密前主管 (PRECO)
- 加密管理員 (CO)
- 加密使用者 (CU)

## 語法

依照語法圖表中指定的順序輸入引數。使用 `-hpswd` 參數來遮罩您的密碼。若要啟用雙重要素驗證 (2FA)，請使用 `-2fa` 參數並包含檔案路徑。如需詳細資訊，請參閱[the section called “引數”](#)。

```
loginHSM <user-type> <user-name> <password> [-hpswd] [-2fa </path/to/authdata>]
```

```
logoutHSM
```

## 範例

這些範例顯示如何使用 `loginHSM` 和 `logoutHSM` 登入和登出叢集中的所有 HSM。

Example：登入叢集中的 HSM

此命令會使用名為 `admin`、密碼為 `co12345` 的 CO 使用者登入憑證資訊，來登入叢集中的所有 HSM。輸出會顯示您已成功執行此命令，且已連接到 HSM (在此案例中是 `server 0` 和 `server 1`)。

```
aws-cloudhsm>loginHSM CO admin co12345

loginHSM success on server 0(10.0.2.9)
loginHSM success on server 1(10.0.3.11)
```

## Example：使用隱藏密碼登入

此命令與以上範例相同，只不過這次您指定系統應該隱藏密碼。

```
aws-cloudhsm>loginHSM C0 admin -hpswd
```

系統會提示您輸入密碼。您輸入密碼時後，系統會隱藏密碼，並且輸出會顯示您已成功執行此命令，並顯示您已連線至叢集上的所有 HSM。

```
Enter password:

loginHSM success on server 0(10.0.2.9)
loginHSM success on server 1(10.0.3.11)

aws-cloudhsm>
```

## Example：登出 HSM

此命令會登出您目前登入的 HSM (在此案例中是 server 0 和 server 1)。輸出會顯示已成功執行此命令，且使用者已從 HSM 中斷開連線。

```
aws-cloudhsm>logoutHSM

logoutHSM success on server 0(10.0.2.9)
logoutHSM success on server 1(10.0.3.11)
```

## 引數

依照語法圖表中指定的順序輸入引數。使用 `-hpswd` 參數來遮罩您的密碼。若要啟用雙重要素驗證 (2FA)，請使用 `-2fa` 參數並包含檔案路徑。如需使用 2FA 的詳細資訊，請參閱 [管理使用者 2FA](#)。

```
loginHSM <user-type> <user-name> <password> |-hpswd> [-2fa </path/to/authdata>]
```

### <user type>

指登入 HSM 的使用者類型。如需詳細資訊，請參閱上面的[使用者類型](#)。

必要：是

### <user name>

指登入 HSM 使用者的使用者名稱。

必要：是

< 密碼 | -hpswd >

指定登入 HSM 使用者的密碼。要隱藏您的密碼，請使用 -hpswd 參數代替密碼，然後按照提示進行操作。

必要：是

[-2fa </path/to/authdata>]

指系統應使用第二個要素來驗證該啟用 2FA 的 CO 使用者。若要取得啟用 2FA 登入的所需資料，請在 -2fa 參數後加入檔案系統帶有檔案名稱位置的路徑。如需使用 2FA 的詳細資訊，請參閱 [管理使用者 2FA](#)。

必要：否

## 相關主題

- [cloudhsm\\_mgmt\\_util 入門](#)
- [啟用叢集](#)

## 使用 CMU 將 AWS CloudHSM 使用者與金鑰建立關聯

使用 AWS CloudHSM cloudhsm\_mgmt\_util 中的 registerQuorumPubKey 命令，將硬體安全模組 (HSM) 使用者與非對稱 RSA-2048 金鑰對建立關聯。您將 HSM 使用者與金鑰建立關聯後，這些使用者就可以使用私有金鑰來核准規定人數要求，且叢集可以使用已註冊的公有金鑰來確認簽章是否來自使用者。如需有關規定人數身分驗證的詳細資訊，請參閱 [管理規定人數身分驗證 \(M/N 存取控制\)](#)。

### Tip

在 AWS CloudHSM 文件中，規定人數身分驗證有時稱為 M of N (MofN)，這表示 N 個核准者總數中至少有 M 個核准者。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密管理員 (CO)

## 語法

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
registerQuorumPubKey <user-type> <user-name> <registration-token> <signed-registration-token> <public-key>
```

## 範例

此範例說明如何使用 registerQuorumPubKey 將加密管理員 (CO) 註冊為規定人數身分驗證要求的核准者。若要執行此命令，您須擁有非對稱 RSA-2048 金鑰對、已簽署權杖和未簽署權杖。有關這些需求的詳細資訊，請參閱 [the section called “引數”](#)。

Example：註冊 HSM 使用者以進行規定人數身分驗證

此範例會將名為 quorum\_officer 的 CO 註冊為核准人，以進行規定人數身分驗證。

```
aws-cloudhsm> registerQuorumPubKey CO <quorum_officer> </path/to/quorum_officer.token> </path/to/quorum_officer.token.sig> </path/to/quorum_officer.pub>
```

```
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.

```

```
Do you want to continue(y/n)?y
registerQuorumPubKey success on server 0(10.0.0.1)
```

最終命令使用 [listUsers](#) 命令來驗證 quorum\_officer 已註冊為 MofN 使用者。

```
aws-cloudhsm> listUsers
Users on server 0(10.0.0.1):
Number of users found:3
```

| User Id         | User Type | User Name | MofnPubKey |
|-----------------|-----------|-----------|------------|
| LoginFailureCnt | 2FA       |           |            |
| 1               | PCO       | admin     | NO         |
| 0               | NO        |           |            |
| 2               | AU        | app_user  | NO         |
| 0               | NO        |           |            |



|   |    |                |     |
|---|----|----------------|-----|
| 3 | CO | quorum_officer | YES |
| 0 | NO |                |     |

## 引數

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
registerQuorumPubKey <user-type> <user-name> <registration-token> <signed-registration-token> <public-key>
```

### <user-type>

指使用者的類型。此為必要參數。

如需 HSM 上使用者類型的詳細資訊，請參閱 [AWS CloudHSM Management Utility 的 HSM 使用者類型](#)。

有效值：

- CO：加密管理者可以管理使用者，但不能管理金鑰。

必要：是

### <user-name>

為使用者指定易記的名稱。長度上限為 31 個字元。允許的唯一特殊字元是底線 (\_)。

建立使用者之後，您就無法再變更使用者的名稱。在 cloudhsm\_mgmt\_util 命令中，使用者類型和密碼需區分大小寫，但使用者名稱不區分大小寫。

必要：是

### <registration-token>

指定包含未簽署註冊權杖檔案的路徑。可包含最大 245 個位元組的任何隨機資料。如需有關建立未簽署註冊權杖的詳細資訊，請參閱[建立並簽署註冊權杖](#)。

必要：是

### <signed-registration-token>

指包含註冊權杖的 SHA256\_PKCS 機制簽署雜湊的文件的路徑。如需詳細資訊，請參閱[建立並簽署註冊權杖](#)。

必要：是

<public-key>

指包含非對稱 RSA-2048 金鑰對的公有金鑰檔案的路徑。使用私有金鑰簽署註冊權杖。如需詳細資訊，請參閱[建立 RSA 金鑰對](#)。

必要：是

 Note

叢集使用相同的金鑰進行規定人數身分驗證和雙重要素驗證 (2FA)。這表示您無法為使用 `registerQuorumPubKey` 啟用 2FA 的使用者輪換規定人數金鑰。若要輪換金鑰，您必須使用 `changePswd`。如需關於使用規定人數身分驗證和 2FA 的詳細資訊，請參閱[規定人數身分驗證和 2FA](#)。

## 相關主題

- [建立 RSA 金鑰對](#)
- [建立並簽署註冊權杖](#)
- [用 HSM 註冊公有金鑰](#)
- [管理規定人數身分驗證 \(M/N 存取控制\)](#)
- [規定人數驗證和 2FA](#)
- [listUsers](#)

## 使用 CMU 與 AWS CloudHSM 叢集中的一個 HSM 互動

在 AWS CloudHSM `cloudhsm_mgmt_util` 中使用 `server` 命令來進入伺服器模式，並直接與特定硬體安全模組 (HSM) 執行個體互動。

一般而言，當您從 `cloudhsm_mgmt_util` 中發出命令時，該命令將會影響指定的叢集 (全域模式) 內的所有 HSM。不過，有時您可能需要向單一 HSM 發出命令。例如，若自動同步失敗，您可能需要同步某個 HSM 上的金鑰和使用者，以維持整個叢集的一致性。

成功啟動後，`aws-cloudhsm >` 命令提示將取代為 `server >` 命令提示。

若要結束伺服器模式，請使用 `exit` 命令。成功退出後，您即會返回 `cloudhsm_mgmt_util` 命令提示。

您必須先啟動 `cloudhsm_mgmt_util`，然後再執行任何 `cloudhsm_mgmt_util` 命令。

## 使用者類型

下列使用者可以執行此命令。

- 所有使用者。

## 先決條件

若要進入伺服器模式，您必須事先得知目標 HSM 的伺服器編號。伺服器編號會列示於 `cloudhsm_mgmt_util` 在啟動時所產生的追蹤輸出中。伺服器編號將按照 HSM 顯示在組態檔案中的相同順序進行指派。本範例假設 `server 0` 是與所需 HSM 相對應的伺服器。

## 語法

啟動伺服器模式：

```
server <server-number>
```

結束伺服器模式：

```
server> exit
```

## 範例

此命令使用伺服器編號 0 由 HSM 上進入伺服器模式。

```
aws-cloudhsm> server 0

Server is in 'E2' mode...
```

若要結束伺服器模式，請使用 `exit` 命令。

```
server0> exit
```

## 引數

```
server <server-number>
```

<server-number>

指定目標 HSM 的伺服器編號。

必要：是

exit 命令沒有任何引數。

## 相關主題

- [syncKey](#)
- [createUser](#)
- [deleteUser](#)

## 使用 CMU 設定 AWS CloudHSM 金鑰的屬性

使用 AWS CloudHSM `cloudhsm_mgmt_util` 中的 `setAttribute` 命令來變更 HSMs 中金鑰的標籤值、加密、解密、包裝和取消包裝屬性。您也可以在 `key_mgmt_util` 中使用 [setAttribute](#) 命令，將工作階段金鑰轉換為持久性金鑰。您只能變更您所擁有金鑰的屬性。

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列使用者可以執行此命令。

- 加密使用者 (CU)

## 語法

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
setAttribute <key handle> <attribute id>
```

## 範例

此範例說明如何停用對稱金鑰的解密功能。您可使用這樣的命令來設定包裝金鑰，該金鑰應該能夠包裝和取消包裝其他金鑰，但不能加密或解密資料。

第一步是建立包裝金鑰。此命令在 `key_mgmt_util` 中使用 [genSymKey](#) 來產生 256 位元 AES 對稱金鑰。輸出顯示新金鑰的金鑰控制代碼是 14。

```
$ genSymKey -t 31 -s 32 -l aes256

Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS

Symmetric Key Created. Key Handle: 14

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

接著，我們想要確認目前解密屬性的值。若要取得解密屬性的屬性 ID，請使用 [listAttributes](#)。輸出顯示代表 OBJ\_ATTR\_DECRYPT 屬性的常數是 261。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

```
aws-cloudhsm> listAttributes

Following are the possible attribute values for getAttribute:

OBJ_ATTR_CLASS = 0
OBJ_ATTR_TOKEN = 1
OBJ_ATTR_PRIVATE = 2
OBJ_ATTR_LABEL = 3
OBJ_ATTR_TRUSTED = 134
OBJ_ATTR_KEY_TYPE = 256
OBJ_ATTR_ID = 258
OBJ_ATTR_SENSITIVE = 259
OBJ_ATTR_ENCRYPT = 260
OBJ_ATTR_DECRYPT = 261
OBJ_ATTR_WRAP = 262
OBJ_ATTR_UNWRAP = 263
OBJ_ATTR_SIGN = 264
OBJ_ATTR_VERIFY = 266
OBJ_ATTR_DERIVE = 268
OBJ_ATTR_LOCAL = 355
OBJ_ATTR_MODULUS = 288
```

```

OBJ_ATTR_MODULUS_BITS = 289
OBJ_ATTR_PUBLIC_EXPONENT = 290
OBJ_ATTR_VALUE_LEN = 353
OBJ_ATTR_EXTRACTABLE = 354
OBJ_ATTR_NEVER_EXTRACTABLE = 356
OBJ_ATTR_ALWAYS_SENSITIVE = 357
OBJ_ATTR_DESTROYABLE = 370
OBJ_ATTR_KCV = 371
OBJ_ATTR_WRAP_WITH_TRUSTED = 528
OBJ_ATTR_WRAP_TEMPLATE = 1073742353
OBJ_ATTR_UNWRAP_TEMPLATE = 1073742354
OBJ_ATTR_ALL = 512

```

若要取得金鑰 14 目前解密屬性的值，下一個命令會在 `cloudhsm_mgmt_util` 中使用 [getAttribute](#)。

輸出顯示在叢集的兩個 HSM 上，解密屬性的值均為 `true (1)`。

```

aws-cloudhsm> getAttribute 14 261

Attribute Value on server 0(10.0.0.1):
OBJ_ATTR_DECRYPT
0x00000001

Attribute Value on server 1(10.0.0.2):
OBJ_ATTR_DECRYPT
0x00000001

```

此命令使用 `setAttribute`，將金鑰 14 的解密屬性 (屬性 261) 的值變更為 0。這將停用該金鑰的解密功能。

輸出顯示該命令在叢集中的兩個 HSM 上均成功執行。

```

aws-cloudhsm> setAttribute 14 261 0
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.

Do you want to continue(y/n)? y

```

```
setAttribute success on server 0(10.0.0.1)
setAttribute success on server 1(10.0.0.2)
```

最後的命令會重複 `getAttribute` 命令。同樣地，執行該命令會取得金鑰 14 的解密屬性 (屬性 261)。

此時，輸出顯示在叢集中的兩個 HSM 上，解密屬性的值均為 `false (0)`。

```
aws-cloudhsm > getAttribute 14 261
Attribute Value on server 0(10.0.3.6):
OBJ_ATTR_DECRYPT
0x00000000

Attribute Value on server 1(10.0.1.7):
OBJ_ATTR_DECRYPT
0x00000000
```

## 引數

```
setAttribute <key handle> <attribute id>
```

### <key-handle>

指定您擁有金鑰的金鑰控制代碼。每一個命令中只能指定一個金鑰。若要取得金鑰的金鑰控制代碼，請在 `key_mgmt_util` 中使用 [findKey](#)。如要尋找金鑰的使用者，請使用 [getKeyInfo](#)。

必要：是

### <attribute id>

指定常數，其代表您要變更的屬性。每一個命令中只能指定一個屬性。如要取得屬性及其整數值，請使用 [listAttributes](#)。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

有效值：

- 3 : OBJ\_ATTR\_LABEL。
- 134 : OBJ\_ATTR\_TRUSTED。
- 260 : OBJ\_ATTR\_ENCRYPT。
- 261 : OBJ\_ATTR\_DECRYPT。
- 262 : OBJ\_ATTR\_WRAP。

- 263 : OBJ\_ATTR\_UNWRAP。
- 264 : OBJ\_ATTR\_SIGN。
- 266 : OBJ\_ATTR\_VERIFY。
- 268 : OBJ\_ATTR\_DERIVE。
- 370 : OBJ\_ATTR\_DESTROYABLE。
- 528 : OBJ\_ATTR\_WRAP\_WITH\_TRUSTED。
- 1073742353 : OBJ\_ATTR\_WRAP\_TEMPLATE。
- 1073742354 : OBJ\_ATTR\_UNWRAP\_TEMPLATE。

必要：是

## 相關主題

- key\_mgmt\_util 中的 [setAttribute](#)
- [getAttribute](#)
- [listAttributes](#)
- [金鑰屬性參考](#)

## 結束 CMU

使用 AWS CloudHSM cloudhsm\_mgmt\_util 中的 quit 命令退出 cloudhsm\_mgmt\_util。任何類型的任何使用者均可使用此命令。

您必須先啟動 cloudhsm\_mgmt\_util，然後再執行任何 cloudhsm\_mgmt\_util 命令。

## 使用者類型

下列使用者可以執行此命令。

- 所有使用者。您無須登入即可執行此命令。

## 語法

```
quit
```



## 範例

這個命令會結束 `cloudhsm_mgmt_util`。成功結束後，您將返回慣常的命令列。此命令沒有任何輸出參數。

```
aws-cloudhsm> quit

disconnecting from servers, please wait...
```

## 相關主題

- [cloudhsm\\_mgmt\\_util 入門](#)

## 使用 CMU 共用 AWS CloudHSM 金鑰

使用 AWS CloudHSM `cloudhsm_mgmt_util` 中的 `shareKey` 命令，與其他加密使用者共用和取消共用您擁有的金鑰。只有金鑰擁有者可以共用和取消共用金鑰。您也可以在建立金鑰時共用金鑰。

共用金鑰的使用者可在加密操作中使用此金鑰，但無法刪除、匯出、共用、取消共用此金鑰，或變更其屬性。對金鑰啟用規定人數身分驗證時，任何會共用或取消共用此金鑰的操作，都必須經過規定人數核准。

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密使用者 (CU)

## 語法

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

使用者類型：加密使用者 (CU)

```
shareKey <key handle> <user id> <(share/unshare key?) 1/0>
```

## 範例

以下範例示範如何使用 `shareKey`，將您擁有的金鑰與其他加密使用者共用，也可以與其他加密使用者取消共用。

### Example：共用金鑰

此範例使用 `shareKey`，將目前使用者擁有的 [ECC 私密金鑰](#) 與 HSM 上的另一位加密使用者共用。HSM 的所有使用者都能使用公開金鑰，因此您無法共用或取消共用公開金鑰。

第一個命令使用 [getKeyInfo](#)，以取得金鑰 262177 (HSM 上的 ECC 私密金鑰) 的使用者資訊。

輸出顯示金鑰 262177 由使用者 3 擁有，但不共用。

```
aws-cloudhsm>getKeyInfo 262177

Key Info on server 0(10.0.3.10):

 Token/Flash Key,

 Owned by user 3

Key Info on server 1(10.0.3.6):

 Token/Flash Key,

 Owned by user 3
```

此命令使用 262177 與 HSMs 上的另一個加密使用者 4 共用金鑰。最後一個引數使用的值是 1，表示共用操作。

輸出顯示該操作在叢集的兩個 HSM 上均成功執行。

```
aws-cloudhsm>shareKey 262177 4 1
*****CAUTION*****
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.

Do you want to continue(y/n)?y
shareKey success on server 0(10.0.3.10)
```

```
shareKey success on server 1(10.0.3.6)
```

為確認操作成功，範例會重複第一個 `getKeyInfo` 命令。

輸出顯示金鑰 262177 現在已共用給使用者 4。

```
aws-cloudhsm>getKeyInfo 262177
```

```
Key Info on server 0(10.0.3.10):
```

```
Token/Flash Key,
```

```
Owned by user 3
```

```
also, shared to following 1 user(s):
```

```
4
```

```
Key Info on server 1(10.0.3.6):
```

```
Token/Flash Key,
```

```
Owned by user 3
```

```
also, shared to following 1 user(s):
```

```
4
```

#### Example：取消共用金鑰

此範例取消共用對稱金鑰，即：從金鑰的共用使用者清單中移除加密使用者。

此命令使用 `shareKey` 從金鑰 6 的共用使用者清單中移除使用者 4。最後一個引數使用的值是 0，表示取消共用操作。

輸出顯示命令在兩個 HSM 上均成功執行。因此，使用者 4 無法再於加密操作中使用金鑰 6。

```
aws-cloudhsm>shareKey 6 4 0
```

```
*****CAUTION*****
```

```
This is a CRITICAL operation, should be done on all nodes in the
cluster. AWS does NOT synchronize these changes automatically with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
```

```

```

```
Do you want to continue(y/n)?y
shareKey success on server 0(10.0.3.10)
shareKey success on server 1(10.0.3.6)
```

## 引數

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
shareKey <key handle> <user id> <(share/unshare key?) 1/0>
```

### <key-handle>

指定您擁有金鑰的金鑰控制代碼。每一個命令中只能指定一個金鑰。若要取得金鑰的金鑰控制代碼，請在 `key_mgmt_util` 中使用 [findKey](#)。如要證實您擁有金鑰，請使用 [getKeyInfo](#)。

必要：是

### <user id>

指定加密使用者 (CU) 的使用者 ID，表示您要將金鑰共用或取消共用給此使用者。如要尋找使用者的使用者 ID，請使用 [listUsers](#)。

必要：是

### <share 1 or unshare 0>

如要將金鑰共用給指定的使用者，請輸入 1。如要取消共用金鑰，即：從金鑰的共用使用者清單中移除指定的使用者，請輸入 0。

必要：是

## 相關主題

- [getKeyInfo](#)

## 使用 CMU 跨 AWS CloudHSM 叢集同步金鑰

使用 AWS CloudHSM `cloudhsm_mgmt_util` 中的 `syncKey` 命令，在叢集內的 HSM 執行個體或複製的叢集之間手動同步金鑰。一般而言，您不需要使用此命令，這是因為叢集中的 HSM 執行個體會自動同步金鑰。但是您須手動同步複製叢集之間的金鑰。複製的叢集通常在不同 AWS 區域中建立，以簡化全域擴展和災難復原程序。

您不能用 `syncKey` 在任意叢集之間同步金鑰：其中一個叢集必須是從另一個叢集的備份建立而來。此外，兩個叢集必須擁有一致的 CO 和 CU 登入資料，操作才能成功。如需詳細資訊，請參閱 [HSM 使用者](#)。

若要使用 `syncKey`，您必須先[建立 AWS CloudHSM 組態檔案](#)，指定來源叢集中的一個 HSM，以及目的地叢集中的一個 HSM。這可讓 `cloudhsm_mgmt_util` 連線到兩個 HSM 執行個體。使用此組態檔案啟動 `cloudhsm_mgmt_util`。然後，使用擁有您要同步金鑰的 CO 或 CU 登入資料登入。

## 使用者類型

下列類型的使用者可以執行此命令。

- 加密管理員 (CO)
- 加密使用者 (CU)

### Note

CO 可以在任何金鑰上使用 `syncKey`，而 CU 只能在他們擁有的金鑰上使用此命令。如需詳細資訊，請參閱[the section called “使用者類型”](#)。

## 先決條件

開始之前，您須知道來源 HSM 上要與目標 HSM 同步之金鑰的 `key handle`。如要尋找 `key handle`，請使用 [listUsers](#) 命令列出具名使用者的所有識別符。然後，使用 [findAllKeys](#) 命令尋找屬於特定使用者的所有金鑰。

您也需了解指派給來源及目標 HSM 的 `server IDs`，這會顯示在啟動時由 `cloudhsm_mgmt_util` 所傳回的追蹤輸出中的具體內容。這些項目的指派順序就是 HSM 顯示在組態檔案中的順序。

遵循[複製叢集間使用 CMU](#)的說明，並使用新的組態檔案初始化 `cloudhsm_mgmt_util`。然後，發出 [server](#) 命令，在來源 HSM 上進入伺服器模式。

## 語法

### Note

若要執行 `syncKey`，請先在包含要同步金鑰的 HSM 上進入伺服器模式。

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

使用者類型：加密使用者 (CU)

```
syncKey <key handle> <destination hsm>
```

## 範例

執行 `server` 命令，登入來源 HSM 並進入伺服器模式。在該範例中，我們假設 `server 0` 是來源 HSM。

```
aws-cloudhsm> server 0
```

現在執行 `syncKey` 命令。在這個範例中，我們假設金鑰 261251 要同步到 `server 1`。

```
aws-cloudhsm> syncKey 261251 1
syncKey success
```

## 引數

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
syncKey <key handle> <destination hsm>
```

### <key handle>

指定要同步金鑰的金鑰控制代碼。每一個命令中只能指定一個金鑰。若要取得金鑰的金鑰控制代碼，請在登入 HSM 伺服器時使用 [findAllKeys](#)。

必要：是

### <destination hsm>

指定您要同步金鑰的伺服器數量。

必要：是

## 相關主題

- [listUsers](#)

- [findAllKeys](#)
- [describe-clusters](#) in AWS CLI
- [server](#)

## 使用 CMU 同步 AWS CloudHSM 叢集中的使用者

使用 AWS CloudHSM `cloudhsm_mgmt_util` 中的 `syncUser` 命令，在叢集內的 HSM 執行個體或複製的叢集之間手動同步加密使用者 (CUs) 或加密管理員 (COs)。AWS CloudHSM 不會自動同步使用者。一般而言，您可以在全域模式中管理使用者，這樣，叢集中的所有 HSM 可以一起更新。如果 HSM 意外取消同步 (例如，由於密碼變更)，或者，如果您想要在複製叢集間輪換使用者憑證，您可能需要使用 `syncUser`。複製的叢集通常在不同 AWS 區域中建立，以簡化全域擴展和災難復原程序。

啟動 CMU 並登入 HSM 後，方可執行任何 CMU 命令。請確認您所登入的使用者帳戶類型能夠執行您要使用的命令。

如果您新增或刪除 HSM，請更新 CMU 的組態檔案。否則，您所進行的變更可能無法在叢集中的所有 HSM 上生效。

### 使用者類型

下列類型的使用者可以執行此命令。

- 加密管理員 (CO)

### 先決條件

開始之前，您必須知道來源 HSM 上要與目標 HSM 同步使用者的 `user ID`。如要尋找 `user ID`，請使用 [listUsers](#) 命令列出叢集中 HSM 上的所有使用者。

您也需了解指派給來源及目標 HSM 的 `server ID`，這會顯示在啟動時由 `cloudhsm_mgmt_util` 所傳回的追蹤輸出中的具體內容。這些項目的指派順序就是 HSM 顯示在組態檔案中的順序。

如果您要同步複製叢集間的 HSM，請遵循[複製叢集間使用 CMU](#)中的說明操作，並使用新的組態檔案初始化 `cloudhsm_mgmt_util`。

當您準備好執行 `syncUser` 時，請發出 [server](#) 命令，在來源 HSM 上進入伺服器模式。

### 語法

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
syncUser <user ID> <server ID>
```

## 範例

執行 `server` 命令，登入來源 HSM 並進入伺服器模式。在該範例中，我們假設 `server 0` 是來源 HSM。

```
aws-cloudhsm> server 0
```

現在執行 `syncUser` 命令。在這個範例中，我們假設使用者 6 是要同步的使用者，而 `server 1` 是目標 HSM。

```
server 0> syncUser 6 1
ExtractMaskedObject: 0x0 !
InsertMaskedObject: 0x0 !
syncUser success
```

## 引數

因為此命令未指明具體參數，所以您須依照語法圖表中指定的順序輸入引數。

```
syncUser <user ID> <server ID>
```

### <user ID>

指定要同步的使用者 ID。每一個命令中只能指定一個使用者。若要取得使用者的 ID，請使用 [listUsers](#)。

必要：是

### <server ID>

指定您要同步使用者的 HSM 伺服器編號。

必要：是

## 相關主題

- [listUsers](#)



- [describe-clusters](#) in AWS CLI
- [server](#)

## AWS CloudHSM 金鑰管理公用程式 (KMU)

金鑰管理公用程式 (KMU) 是 的命令列工具 AWS CloudHSM，可協助加密使用者 (CU) 管理硬體安全模組 (HSM) 上的金鑰。KMU 包含多個命令，可產生、刪除、匯入和匯出金鑰、取得和設定屬性、尋找金鑰，以及執行密碼編譯操作。

KMU 和 CMU 系統是[用戶端 SDK 3 套件](#)的一部分。

如需快速入門，請參閱 [key\\_mgmt\\_util 入門 AWS CloudHSM](#)。如需命令的詳細資訊，請參閱 [AWS CloudHSM Key Management Utility 命令的參考](#)。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

如果您使用的是 Linux，若要使用 key\_mgmt\_util，請連接到您的用戶端執行個體，然後請參閱[安裝和設定 KMU \(Linux\) 的 AWS CloudHSM 用戶端](#)。如果您使用的是 Windows，請參閱 [安裝和設定 KMU 的 AWS CloudHSM 用戶端 \(Windows\)](#)。

### 主題

- [key\\_mgmt\\_util 入門 AWS CloudHSM](#)
- [安裝和設定 KMU \(Linux\) 的 AWS CloudHSM 用戶端](#)
- [安裝和設定 KMU 的 AWS CloudHSM 用戶端 \(Windows\)](#)
- [AWS CloudHSM Key Management Utility 命令的參考](#)

## key\_mgmt\_util 入門 AWS CloudHSM

AWS CloudHSM 包含兩個命令列工具與[AWS CloudHSM 用戶端軟體](#)。[cloudhsm\\_mgmt\\_util](#) 工具包含管理 HSM 使用者的命令。[key\\_mgmt\\_util](#) 工具包含管理金鑰的命令。若要開始使用 key\_mgmt\_util 命令列工具，請參閱下列主題。

### 主題

- [設定 AWS CloudHSM key\\_mgmt\\_util](#)
- [使用 KMU 登入 AWS CloudHSM 叢集中的 HSMs](#)
- [使用 KMU 從 AWS CloudHSM 叢集中的 HSMs 登出](#)

- [停止 AWS CloudHSM key\\_mgmt\\_util](#)

如果您使用命令時遇到錯誤訊息或未預期的結果，請參閱[故障診斷 AWS CloudHSM](#) 主題以取得協助。如需 key\_mgmt\_util 命令的詳細資訊，請參閱 [AWS CloudHSM Key Management Utility 命令的參考](#)。

## 設定 AWS CloudHSM key\_mgmt\_util

請先完成下列設定，再使用 AWS CloudHSM key\_mgmt\_util (KMU)。

### 主題

- [步驟 1. 啟動 AWS CloudHSM 用戶端](#)
- [步驟 2. 啟動 key\\_mgmt\\_util](#)

### 步驟 1. 啟動 AWS CloudHSM 用戶端

在使用 key\_mgmt\_util 之前，您必須先啟動 AWS CloudHSM 用戶端。用戶端為一項協助程式，其會與您的叢集中的 HSM 建立端對端加密的通訊。key\_mgmt\_util 工具會使用用戶端連線來與叢集中的 HSM 通訊。如果沒有連線，key\_mgmt\_util 便無法運作。

### 啟動 AWS CloudHSM 用戶端

使用下列命令來啟動 AWS CloudHSM 用戶端。

#### Amazon Linux

```
$ sudo start cloudhsm-client
```

#### Amazon Linux 2

```
$ sudo service cloudhsm-client start
```

#### CentOS 7

```
$ sudo service cloudhsm-client start
```

#### CentOS 8

```
$ sudo service cloudhsm-client start
```

## RHEL 7

```
$ sudo service cloudhsm-client start
```

## RHEL 8

```
$ sudo service cloudhsm-client start
```

## Ubuntu 16.04 LTS

```
$ sudo service cloudhsm-client start
```

## Ubuntu 18.04 LTS

```
$ sudo service cloudhsm-client start
```

## Windows

- 用於 Windows 用戶端 1.1.2+ :

```
C:\Program Files\Amazon\CloudHSM>net.exe start AWSCloudHSMClient
```

- 用於 Windows 用戶端 1.1.1 和更早版本 :

```
C:\Program Files\Amazon\CloudHSM>start "cloudhsm_client" cloudhsm_client.exe C:
\ProgramData\Amazon\CloudHSM\data\cloudhsm_client.cfg
```

## 步驟 2. 啟動 key\_mgmt\_util

啟動 AWS CloudHSM 用戶端後，請使用下列命令來啟動 key\_mgmt\_util。

## Amazon Linux

```
$ /opt/cloudhsm/bin/key_mgmt_util
```

## Amazon Linux 2

```
$ /opt/cloudhsm/bin/key_mgmt_util
```

## CentOS 7

```
$ /opt/cloudhsm/bin/key_mgmt_util
```

## CentOS 8

```
$ /opt/cloudhsm/bin/key_mgmt_util
```

## RHEL 7

```
$ /opt/cloudhsm/bin/key_mgmt_util
```

## RHEL 8

```
$ /opt/cloudhsm/bin/key_mgmt_util
```

## Ubuntu 16.04 LTS

```
$ /opt/cloudhsm/bin/key_mgmt_util
```

## Ubuntu 18.04 LTS

```
$ /opt/cloudhsm/bin/key_mgmt_util
```

## Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\key_mgmt_util.exe"
```

key\_mgmt\_util 執行時，提示會切換至 Command:。

如果命令失敗 (例如傳回 Daemon socket connection error 訊息)，請嘗試[更新您的組態檔](#)。

## 使用 KMU 登入 AWS CloudHSM 叢集中的 HSMs

使用 key\_mgmt\_util (KMU) 中的 loginHSM 命令來登入 AWS CloudHSM 叢集中的硬體安全模組 (HSM)。以下命令會以名為 example\_user 的[加密使用者 \(CU\) 身分登入](#)：輸出指出叢集中的所有三個 HSM 已成功登入。

```
Command: loginHSM -u CU -s example_user -p <PASSWORD>
```

```
Cfm3LoginHSM returned: 0x00 : HSM Return: SUCCESS
```

#### Cluster Error Status

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

下列顯示 loginHSM 命令的語法。

```
Command: loginHSM -u <USER TYPE> -s <USERNAME> -p <PASSWORD>
```

## 使用 KMU 從 AWS CloudHSM 叢集中的 HSMs 登出

使用 key\_mgmt\_util (KMU) 中的 logoutHSM 命令，從 AWS CloudHSM 叢集中的硬體安全模組 (HSM) 登出。

```
Command: logoutHSM
```

```
Cfm3LogoutHSM returned: 0x00 : HSM Return: SUCCESS
```

#### Cluster Error Status

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

## 停止 AWS CloudHSM key\_mgmt\_util

使用 exit 命令來停止 AWS CloudHSM key\_mgmt\_util。

```
Command: exit
```

## 安裝和設定 KMU (Linux) 的 AWS CloudHSM 用戶端

若要使用 key\_mgmt\_util (KMU) 與 AWS CloudHSM 叢集中的硬體安全模組 (HSM) 互動，您需要 Linux 的 AWS CloudHSM 用戶端軟體。應該將此軟體安裝到您先前建立的 Linux EC2 用戶端執行個體。如果是使用 Windows，您也可以安裝用戶端。如需詳細資訊，請參閱[安裝和設定 KMU 的 AWS CloudHSM 用戶端 \(Windows\)](#)。

### 任務

- [步驟 1. 安裝 AWS CloudHSM 用戶端和命令列工具](#)

- [步驟 2. 編輯用戶端組態](#)

## 步驟 1. 安裝 AWS CloudHSM 用戶端和命令列工具

連線至您的用戶端執行個體並執行下列命令，以下載並安裝 AWS CloudHSM 用戶端和命令列工具。

### Amazon Linux

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-latest.el6.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el6.x86_64.rpm
```

### Amazon Linux 2

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-latest.el7.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el7.x86_64.rpm
```

### CentOS 7

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-latest.el7.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el7.x86_64.rpm
```

### CentOS 8

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-latest.el8.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el8.x86_64.rpm
```

## RHEL 7

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-latest.el7.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el7.x86_64.rpm
```

## RHEL 8

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-latest.el8.x86_64.rpm
```

```
sudo yum install ./cloudhsm-client-latest.el8.x86_64.rpm
```

## Ubuntu 16.04 LTS

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-client_latest_amd64.deb
```

```
sudo apt install ./cloudhsm-client_latest_amd64.deb
```

## Ubuntu 18.04 LTS

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Bionic/cloudhsm-client_latest_u18.04_amd64.deb
```

```
sudo apt install ./cloudhsm-client_latest_u18.04_amd64.deb
```

## 步驟 2. 編輯用戶端組態

您必須編輯 AWS CloudHSM 用戶端組態，才能使用用戶端連線至叢集。

## 編輯用戶端組態

1. 將您的發行憑證 ([您使用此憑證來簽署叢集憑證](#)) 複製到用戶端執行個體上的這個位置：`/opt/cloudhsm/etc/customerCA.crt`。您的用戶端執行個體上需要有執行個體根使用者許可，才能將憑證複製到此位置。
2. 使用下列 [configure](#) 命令來更新 AWS CloudHSM 用戶端和命令列工具的組態檔案，並在叢集中指定 HSM 的 IP 地址。若要取得 HSM 的 IP 地址，請在 [AWS CloudHSM 主控台](#) 中檢視叢集，或執行 [describe-clusters](#) AWS CLI 命令。在命令輸出中，HSM 的 IP 地址是 `EniIp` 欄位的值。如果您有多個 HSM，請選擇任何 HSM 的 IP 地址；任何一個都可以。

```
sudo /opt/cloudhsm/bin/configure -a <IP address>

Updating server config in /opt/cloudhsm/etc/cloudhsm_client.cfg
Updating server config in /opt/cloudhsm/etc/cloudhsm_mgmt_util.cfg
```

3. 前往 [在中啟用叢集 AWS CloudHSM](#)。

## 安裝和設定 KMU 的 AWS CloudHSM 用戶端 (Windows)

若要在 Windows 上使用 `key_mgmt_util` (KMU)，在 AWS CloudHSM 叢集中使用硬體安全模組 (HSM)，您需要適用於 Windows 的 AWS CloudHSM 用戶端軟體。應將此軟體安裝到您先前建立的 Windows Server 執行個體。

### 安裝 (或更新) 最新 Windows 用戶端和命令列工具

1. 連接至您的 Windows Server 執行個體。
2. 從[下載頁面](#)下載最新 (`AWSCloudHSMClient-latest.msi`)。
3. 前往下載位置，並以管理權限執行安裝程式 (`AWSCloudHSMClient-latest.msi`)。
4. 依照安裝程式指示操作，然後在安裝程式完成後選擇關閉。
5. 將您自己簽署的發行憑證 ([用於簽署叢集憑證的憑證](#)) 複製到 `C:\ProgramData\Amazon\CloudHSM` 資料夾。
6. 使用下列命令以更新組態檔案。如果您正在更新用戶端，務必在重新組態時停止和啟動用戶端。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" -a <HSM IP address>
```

7. 前往 [在中啟用叢集 AWS CloudHSM](#)。



**備註：**

- 如果您正在更新用戶端，系統將不會覆寫前一次安裝的現有組態檔案。
- 適用於 Windows 的 AWS CloudHSM 用戶端安裝程式會自動註冊密碼編譯 API：新一代 (CNG) 和金鑰儲存提供者 (KSP)。若要解除安裝用戶端，請再次執行安裝程式並依照解除安裝指示操作。
- 如果您使用的 Linux，也可以安裝 Linux 用戶端。如需詳細資訊，請參閱[安裝和設定 KMU \(Linux\) 的 AWS CloudHSM 用戶端](#)。

## AWS CloudHSM Key Management Utility 命令的參考

key\_mgmt\_util 命令列工具可協助您管理 AWS CloudHSM 叢集中硬體安全模組 (HSM) 中的金鑰，包括建立、刪除和尋找金鑰及其屬性。它包含多個命令，這個主題中詳細說明每個命令。

如需快速入門，請參閱[key\\_mgmt\\_util 入門 AWS CloudHSM](#)。如需金鑰屬性的解譯說明，請參閱[AWS CloudHSM KMU 的金鑰屬性參考](#)。如需 cloudhsm\_mgmt\_util 命令列工具 (其中包含用來管理叢集中 HSM 和使用者的命令) 的詳細資訊，請參閱[AWS CloudHSM Management Utility \(CMU\)](#)。

執行任何 key\_mgmt\_util 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

如要列出所有 key\_mgmt\_util 命令，請輸入：

```
Command: help
```

若要取得特定 key\_mgmt\_util 命令的說明，請輸入：

```
Command: <command-name> -h
```

若要結束您的 key\_mgmt\_util 工作階段，請輸入：

```
Command: exit
```

下列各主題說明 key\_mgmt\_util 中的命令。

### Note

key\_mgmt\_util 和 cloudhsm\_mgmt\_util 中的某些命令，名稱相同。但是，這些命令通常具有不同的語法，不同的輸出和略微不同的功能。

| Command                             | 描述                                                               |
|-------------------------------------|------------------------------------------------------------------|
| <a href="#">aesWrapUnwrap</a>       | 加密和解密檔案中金鑰的內容。                                                   |
| <a href="#">deleteKey</a>           | 從 HSM 刪除金鑰。                                                      |
| <a href="#">Error2String</a>        | 取得與 key_mgmt_util 十六進位錯誤碼對應的錯誤。                                  |
| <a href="#">exit</a>                | 結束 key_mgmt_util。                                                |
| <a href="#">exportPrivateKey</a>    | 將私有金鑰的複本 從 HSM 匯出至磁碟上的檔案。                                        |
| <a href="#">exportPubKey</a>        | 從 HSM 匯出公有金鑰的複本至檔案。                                              |
| <a href="#">exSymKey</a>            | 將對稱金鑰的純文字複本從 HSM 匯出到檔案。                                          |
| <a href="#">extractMaskedObject</a> | 從做為遮罩物件檔案的 HSM 擷取金鑰。                                             |
| <a href="#">findKey</a>             | 依金鑰屬性值搜尋金鑰。                                                      |
| <a href="#">findSingleKey</a>       | 驗證叢集中所有 HSM 上存在金鑰。                                               |
| <a href="#">genDSAKeyPair</a>       | 在 HSM 中產生 <a href="#">數位簽署演算法</a> (DSA) 金鑰對。                     |
| <a href="#">genECCKeyPair</a>       | 在 HSM 中產生 <a href="#">Elliptic Curve Cryptography</a> (ECC) 金鑰對。 |
| <a href="#">genRSAKeyPair</a>       | 在 HSM 中產生 <a href="#">RSA</a> 非對稱金鑰對。                            |
| <a href="#">genSymKey</a>           | 在 HSM 中產生對稱金鑰                                                    |
| <a href="#">getAttribute</a>        | 取得 AWS CloudHSM 金鑰的屬性值並將值寫入檔案。                                   |
| <a href="#">getCaviumPrivKey</a>    | 建立私有金鑰的仿造 PEM 格式版本，並將它匯出至檔案。                                     |
| <a href="#">getCert</a>             | 擷取 HSM 的分割區憑證，並將它們儲存至檔案。                                         |

| Command                              | 描述                                                                       |
|--------------------------------------|--------------------------------------------------------------------------|
| <a href="#">getKeyInfo</a>           | 取得可以使用金鑰之使用者的 HSM 使用者 ID。<br><br>如果金鑰是受規定人數控制，它會取得規定人數中的使用者數目。           |
| <a href="#">help</a>                 | 顯示在 key_mgmt_util 中可用命令的 help 資訊。                                        |
| <a href="#">importPrivateKey</a>     | 將私有金鑰匯入 HSM。                                                             |
| <a href="#">importPubKey</a>         | 將公有金鑰匯入 HSM。                                                             |
| <a href="#">imSymKey</a>             | 將對稱金鑰的純文字複本從檔案匯入 HSM。                                                    |
| <a href="#">insertMaskedObject</a>   | 從磁碟上的檔案將遮罩物件插入由相關叢集包含到物件原始叢集的 HSM。相關叢集是以 <a href="#">原始叢集備份產生的</a> 任何叢集。 |
| <a href="#">???</a>                  | 決定指定檔案是否包含真正的私有金鑰或範例 PEM 金鑰。                                             |
| <a href="#">listAttributes</a>       | 列出 AWS CloudHSM 金鑰的屬性和代表它們的常數。                                           |
| <a href="#">listUsers</a>            | 取得 HSM 中的使用者、其使用者類型和 ID，以及其他屬性。                                          |
| <a href="#">loginHSM 和 logoutHSM</a> | 登入和登出叢集中的 HSM。                                                           |
| <a href="#">setAttribute</a>         | 將工作階段金鑰轉換為持久性金鑰。                                                         |
| <a href="#">sign</a>                 | 使用所選的私有金鑰產生檔案的簽章。                                                        |
| <a href="#">unWrapKey</a>            | 將包裝 (加密) 的金鑰從檔案匯入到 HSM。                                                  |
| <a href="#">驗證</a>                   | 驗證指定的金鑰是否用於簽署指定的檔案。                                                      |
| <a href="#">wrapKey</a>              | 將金鑰的加密複本從 HSM 匯出到檔案。                                                     |

## 使用 KMU 加密和解密 AWS CloudHSM 檔案

使用 AWS CloudHSM `key_mgmt_util` 中的 `aesWrapUnwrap` 命令來加密或解密磁碟上的檔案內容。此命令旨在包裝和取消包裝加密金鑰，但您可以對包含小於 4 KB (4096 個位元組) 資料的任何檔案使用它。

`aesWrapUnwrap` 使用 [AES 金鑰包裝](#)。它會在 HSM 上使用 AES 金鑰做為包裝或取消包裝金鑰。然後，它會將結果寫入到磁碟上的另一個檔案。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

### 語法

```
aesWrapUnwrap -h

aesWrapUnwrap -m <wrap-unwrap mode>
 -f <file-to-wrap-unwrap>
 -w <wrapping-key-handle>
 [-i <wrapping-IV>]
 [-out <output-file>]
```

### 範例

這些範例示範如何使用 `aesWrapUnwrap` 來加密和解密檔案中的加密金鑰。

#### Example：包裝加密金鑰

此命令使用 `aesWrapUnwrap` 來包裝[從 HSM 以純文字匯出](#)的三重 DES 對稱金鑰到 `3DES.key` 檔案。您可以使用類似命令來包裝在檔案中儲存的任何金鑰。

此命令會使用 `-m` 參數搭配 1 值來指出包裝模式。它使用 `-w` 參數來指定 HSM 中的 AES 金鑰 (金鑰控制代碼 6) 做為包裝金鑰。它會將產生的包裝金鑰寫入 `3DES.key.wrapped` 檔案。

輸出顯示命令已成功，而操作使用了預設的 IV，這是慣用的操作。

```
Command: aesWrapUnwrap -f 3DES.key -w 6 -m 1 -out 3DES.key.wrapped
```

```
Warning: IV (-i) is missing.
```

```
0xA6A6A6A6A6A6A6A6 is considered as default IV
```

```
result data:
```

```
49 49 E2 D0 11 C1 97 22
```

```
17 43 BD E3 4E F4 12 75
8D C1 34 CF 26 10 3A 8D
6D 0A 7B D5 D3 E8 4D C2
79 09 08 61 94 68 51 B7
```

```
result written to file 3DES.key.wrapped
```

```
Cfm3WrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

### Example：取消包裝加密金鑰

此範例示範如何使用 `aesWrapUnwrap` 來將檔案中已包裝 (加密) 的金鑰取消包裝 (解密)。在將金鑰匯入至 HSM 之前，您可能想要執行這類的操作。例如，如果您嘗試使用 [imSymKey](#) 命令來匯入加密金鑰，因為加密金鑰沒有該類型的純文字金鑰所需的格式，則會傳回錯誤。

此命令會取消包裝 `3DES.key.wrapped` 檔案中的金鑰，並將純文字寫入 `3DES.key.unwrapped` 檔案。此命令會使用 `-m` 參數搭配 `0` 值來指出取消包裝模式。它使用 `-w` 參數來指定 HSM 中的 AES 金鑰 (金鑰控制代碼 6) 做為包裝金鑰。它會將產生的包裝金鑰寫入 `3DES.key.unwrapped` 檔案。

```
Command: aesWrapUnwrap -m 0 -f 3DES.key.wrapped -w 6 -out 3DES.key.unwrapped
```

```
Warning: IV (-i) is missing.
```

```
0xA6A6A6A6A6A6A6A6 is considered as default IV
```

```
result data:
```

```
14 90 D7 AD D6 E4 F5 FA
A1 95 6F 24 89 79 F3 EE
37 21 E6 54 1F 3B 8D 62
```

```
result written to file 3DES.key.unwrapped
```

```
Cfm3UnWrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

### 參數

`-h`

顯示命令的說明。

必要：是

`-m`

指定模式。若要包裝 (加密) 檔案內容，請輸入 1；若要取消包裝 (解密) 檔案內容，請輸入 0。

必要：是

-f

指定要包裝的檔案。輸入包含小於 4 KB (4096 個位元組) 資料的檔案。此操作旨在包裝和取消包裝加密金鑰。

必要：是

-w

指定包裝金鑰。輸入 HSM 上 AES 金鑰的金鑰控制代碼。此為必要參數。若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

要建立包裝金鑰，請使用 [genSymKey](#) 以產生 AES 金鑰 (輸入 31)。

必要：是

-i

指定演算法的替代初始值 (IV)。除非您有需要替代方案的特殊條件，否則請使用預設值。

預設：0xA6A6A6A6A6A6A6A6。預設值是在 [AES 金鑰包裝](#) 演算法規格中所定義。

必要：否

-out

指定包含已包裝或取消包裝金鑰之輸出檔的替代名稱。本機目錄中的預設值是 wrapped\_key (針對包裝操作) 和 unwrapped\_key (針對取消包裝操作)。

如果檔案存在，aesWrapUnwrap 會覆寫檔案且不會有任何警告。如果命令失敗，aesWrapUnwrap 會建立沒有內容的輸出檔。

預設值：針對包裝：wrapped\_key。針對取消包裝：unwrapped\_key。

必要：否

## 相關主題

- [exSymKey](#)
- [imSymKey](#)
- [unWrapKey](#)
- [wrapKey](#)

## 使用 KMU 刪除 AWS CloudHSM 金鑰

使用 AWS CloudHSM `key_mgmt_util` 中的 `deleteKey` 命令，從 AWS CloudHSM 叢集中的硬體安全模組 (HSM) 刪除金鑰。您一次只能刪除一個金鑰。刪除金鑰對中的一個金鑰，對金鑰對中的另一個金鑰沒有影響。

只有金鑰擁有者可以刪除金鑰。共用金鑰的使用者可以在密碼編譯操作中使用它，但不能刪除它。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

### 語法

```
deleteKey -h
```

```
deleteKey -k
```

### 範例

下列範例示範如何使用 `deleteKey` 來刪除 HSM 中的金鑰。

#### Example：刪除金鑰

此命令會刪除金鑰控制代碼為 6 的金鑰。當命令成功時，`deleteKey` 會從叢集中每個 HSM 傳回成功訊息。

```
Command: deleteKey -k 6
```

```
Cfm3DeleteKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

#### Example：刪除金鑰 (失敗)

若因為沒有金鑰有指定的金鑰控制代碼而導致命令失敗，`deleteKey` 會傳回無效的物件控制代碼錯誤訊息。

```
Command: deleteKey -k 252126
```

```
Cfm3FindKey returned: 0xa8 : HSM Error: Invalid object handle is passed to this operation
```

#### Cluster Error Status

```
Node id 1 and err state 0x000000a8 : HSM Error: Invalid object handle is passed to this operation
```

```
Node id 2 and err state 0x000000a8 : HSM Error: Invalid object handle is passed to this operation
```

若因為目前的使用者不是金鑰擁有者而導致命令失敗，命令會傳回存取遭拒錯誤。

```
Command: deleteKey -k 262152
```

```
Cfm3DeleteKey returned: 0xc6 : HSM Error: Key Access is denied.
```

## 參數

**-h**

顯示命令的命令列說明。

必要：是

**-k**

指定要刪除之金鑰的金鑰控制代碼。若要尋找 HSM 中金鑰的金鑰控制代碼，請使用 [findKey](#)。

必要：是

## 相關主題

- [findKey](#)

## 使用 KMU 描述 AWS CloudHSM 錯誤

使用 AWS CloudHSM `key_mgmt_util` 中的 `Error2String` helper 命令，傳回對應至 `key_mgmt_util` 十六進位錯誤代碼的錯誤。針對命令和指令碼進行疑難排解時，您可以使用此命令。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。



## 語法

```
Error2String -h

Error2String -r <response-code>
```

## 範例

這些範例示範如何使用 Error2String，以取得 key\_mgmt\_util 錯誤碼的錯誤字串。

### Example：取得錯誤描述

此命令取得 0xdb 錯誤代碼的錯誤描述。描述中說明嘗試登入 key\_mgmt\_util 失敗，因為使用者的使用者類型錯誤。只有加密使用者 (CU) 可以登入 key\_mgmt\_util。

```
Command: Error2String -r 0xdb

Error Code db maps to HSM Error: Invalid User Type.
```

### Example：尋找錯誤碼

此範例顯示在 key\_mgmt\_util 錯誤中尋找錯誤碼的位置。錯誤代碼 0xc6 出現在此字串後面：Cfm3*<command-name>* returned: 。

在這個範例中，[getKeyInfo](#) 指出目前使用者 (使用者 4) 可以在密碼編譯操作中使用該金鑰。不過，當使用者嘗試使用 [deleteKey](#) 刪除金鑰時，命令會傳回錯誤代碼 0xc6。

```
Command: deleteKey -k 262162

Cfm3DeleteKey returned: <0xc6> : HSM Error: Key Access is denied

Cluster Error Status

Command: getKeyInfo -k 262162

Cfm3GetKey returned: 0x00 : HSM Return: SUCCESS

Owned by user 3

also, shared to following 1 user(s):
```

4

如果您收到 0xc6 錯誤報告，您可以使用如下的 Error2String 命令來查詢錯誤。在此案例中，deleteKey 命令失敗，發生存取遭拒錯誤，因為金鑰與目前使用者共用，但擁有的使用者不同。只有金鑰擁有者有權刪除金鑰。

```
Command: Error2String -r 0xa8
```

```
Error Code c6 maps to HSM Error: Key Access is denied
```

## 參數

-h

顯示命令的說明。

必要：是

-r

指定十六進位錯誤代碼。需要 0x 十六進位指標。

必要：是

## 結束 AWS CloudHSM KMU

使用 AWS CloudHSM key\_mgmt\_util 中的 exit 命令退出 key\_mgmt\_util。成功退出後，您即會返回您的標準命令列。

執行任何 key\_mgmt\_util 命令前，您必須先[啟動 key\\_mgmt\\_util](#)。

## 語法

```
exit
```

## 參數

此命令沒有任何參數。

## 相關主題

- [啟動 key\\_mgmt\\_util](#)

## 使用 KMU 匯出私有 AWS CloudHSM 金鑰

使用 AWS CloudHSM `key_mgmt_util` 中的 `exportPrivateKey` 命令，將非對稱私有金鑰從硬體安全模組 (HSM) 匯出至檔案。HSM 不允許以純文字形式直接匯出金鑰。該命令使用您指定的 AES 包裝密鑰來包裝私有金鑰，解密包裝的位元組，並以純文字形式將私有金鑰複製到檔案中。

`exportPrivateKey` 命令不會從 HSM 移除金鑰、變更其[金鑰屬性](#)，也不會阻止您在進一步的密碼編譯操作中使用該金鑰。您可以多次匯出相同的金鑰。

您只能匯出私有金鑰具有 `OBJ_ATTR_EXTRACTABLE` 屬性值 1。您須指定具有 `OBJ_ATTR_WRAP` 和 `OBJ_ATTR_DECRYPT` 屬性值 1 的 AES 包裝金鑰。若要尋找金鑰的屬性，請使用 [getAttribute](#) 命令。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
exportPrivateKey -h

exportPrivateKey -k <private-key-handle>
 -w <wrapping-key-handle>
 -out <key-file>
 [-m <wrapping-mechanism>]
 [-wk <wrapping-key-file>]
```

## 範例

此範例顯示如何使用 `exportPrivateKey` 從 HSM 匯出私有金鑰。

Example：匯出私有金鑰

此命令以包含控制代碼 16 的包裝金鑰，將包含控制代碼 15 的私有金鑰匯出至稱為 `exportKey.pem` 的 PEM 檔案。當命令成功時，`exportPrivateKey` 會傳回成功訊息。

```
Command: exportPrivateKey -k 15 -w 16 -out exportKey.pem
```

```
Cfm3WrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
PEM formatted private key is written to exportKey.pem
```

## 參數

此命令會使用下列參數。

### -h

顯示命令的命令列說明。

必要：是

### -k

指定要匯出之私有金鑰的金鑰控制代碼。

必要：是

### -w

指定包裝金鑰的金鑰控制代碼。此為必要參數。若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

若要判斷金鑰是否可以做為包裝金鑰使用，請使用 [getAttribute](#) 取得 OBJ\_ATTR\_WRAP 屬性 (262) 的值。若要建立包裝金鑰，請使用 [genSymKey](#) 建立 AES 金鑰 (類型 31)。

如果您使用 -wk 參數來指定外部的取消包裝金鑰，則在匯出期間會使用 -w 包裝金鑰來進行包裝，但不會用來取消包裝。

必要：是

### -out

指定將寫入匯出之私有金鑰的檔案名稱。

必要：是

### -m

指定用來包裝匯出之私有金鑰的包裝機制。唯一的有效值是 4，這代表 NIST\_AES\_WRAP mechanism.。

預設：4 (NIST\_AES\_WRAP)

必要：否

## **-wk**

指定用於將匯出之金鑰取消包裝的金鑰。輸入包含純文字 AES 金鑰的檔案路徑和名稱。

當您加入此參數時，`exportPrivateKey` 會使用在 `-w` 檔案中的金鑰來包裝要匯出的金鑰，並使用 `-wk` 參數指定的金鑰來取消包裝此金鑰。

預設：使用在 `-w` 參數中指定的包裝金鑰來進行包裝和取消包裝。

必要：否

## 相關主題

- [importPrivateKey](#)
- [wrapKey](#)
- [unWrapKey](#)
- [genSymKey](#)

## 使用 KMU 匯出公有 AWS CloudHSM 金鑰

使用 AWS CloudHSM `key_mgmt_util` 中的 `exportPubKey` 命令，將 HSM 中的公有金鑰匯出至 檔案。您可以使用此命令匯出在 HSM 上產生的公有金鑰。您也可以使用此命令匯出之前匯入 HSM 的公有金鑰，例如使用 [importPubKey](#) 命令匯入的公有金鑰。command.

`exportPubKey` 操作會複製金鑰材料至您指定的檔案。但不會從 HSM 移除金鑰、變更其[金鑰屬性](#)，或避免您將金鑰用於進一步的密碼編譯操作。您可以多次匯出相同的金鑰。

您僅可匯出具有 1 之 `OBJ_ATTR_EXTRACTABLE` 值的公有金鑰。若要尋找金鑰的屬性，請使用 [getAttribute](#) 命令。

執行任何 `key_mgmt_util` 命令之前，您必須[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
exportPubKey -h

exportPubKey -k <public-key-handle>
 -out <key-file>
```

## 範例

此範例顯示如何使用 `exportPubKey` 從 HSM 匯出公有金鑰。

### Example：匯出公有金鑰

此命令將包含控制代碼 10 的公有金鑰匯出至稱為 `public.pem` 的檔案。當命令成功時，`exportPubKey` 會傳回成功訊息。

```
Command: exportPubKey -k 10 -out public.pem

PEM formatted public key is written to public.pem

Cfm3ExportPubKey returned: 0x00 : HSM Return: SUCCESS
```

## 參數

此命令會使用下列參數。

### **-h**

顯示命令的命令列說明。

必要：是

### **-k**

指定要匯出之公有金鑰的金鑰控制代碼。

必要：是

### **-out**

指定將寫入匯出之公有金鑰的檔案名稱。

必要：是

## 相關主題

- [importPubKey](#)
- [產生金鑰](#)

## 使用 KMU 匯出 AWS CloudHSM 金鑰的純文字副本

使用 AWS CloudHSM `key_mgmt_util` 工具中的 `exSymKey` 命令，從硬體安全模組 (HSM) 匯出對稱金鑰的純文字副本，並將其儲存在磁碟上的檔案中。若要匯出金鑰的加密 (包裝) 複本，請使用 [wrapKey](#) 命令。若要匯入純文字金鑰 (像是 `exSymKey` 匯出的金鑰)，請使用 [imSymKey](#)。

在匯出程序時，`exSymKey` 會使用您指定要包裝 (加密) 的 AES 金鑰 (包裝金鑰)，然後將金鑰取消包裝 (解密) 以便匯出。不過，匯出操作的結果是磁碟上的純文字 (取消包裝) 金鑰。

只有金鑰的擁有者 (也就是建立金鑰的 CU 使用者) 可以匯出金鑰。共用金鑰的使用者可以在密碼編譯操作中使用它，但不能將它匯出。

`exSymKey` 操作會將金鑰資料複製到您指定的檔案，但不會從 HSM 中移除該金鑰、變更其[金鑰屬性](#)、或阻止您在密碼編譯操作中使用金鑰。您可以多次匯出相同的金鑰。

`exSymKey` 只會匯出對稱金鑰。若要匯出公有金鑰，請使用 [exportPubKey](#)。若要匯出私有金鑰，請使用 [exportPrivateKey](#)。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

### 語法

```
exSymKey -h

exSymKey -k <key-to-export>
 -w <wrapping-key>
 -out <key-file>
 [-m 4]
 [-wk <unwrapping-key-file>]
```

### 範例

下列範例示範如何從 HSM 使用 `exSymKey` 來匯出您擁有的對稱金鑰。

#### Example：匯出 3DES 對稱金鑰

此命令會將三重 DES (3DES) 對稱金鑰 (金鑰控制代碼 7) 匯出。它使用 HSM 中的現有 AES 金鑰 (金鑰控制代碼 6) 做為包裝金鑰。然後，將純文字的 3DES 金鑰寫入 `3DES.key` 檔案。

輸出顯示已成功將金鑰 7 (3DES 金鑰) 包裝和取消包裝，然後將其寫入 `3DES.key` 檔案。

**⚠ Warning**

雖然輸出寫著已將 "Wrapped Symmetric Key"(包裝的對稱金鑰) 寫入輸出檔，但輸出檔中包含純文字 (取消包裝) 金鑰。

```
Command: exSymKey -k 7 -w 6 -out 3DES.key
```

```
Cfm3WrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
Wrapped Symmetric Key written to file "3DES.key"
```

**Example : 匯出僅限工作階段的包裝金鑰**

此範例示範如何使用只存在於工作階段中的金鑰做為包裝金鑰。因為要匯出的金鑰會被包裝、再立即取消包裝，然後以純文字傳送，所以不需要保留包裝金鑰。

這一系列的命令會從 HSM 匯出金鑰控制代碼為 8 的 AES 金鑰。它會使用特別為此目的建立的 AES 工作階段金鑰。

第一個命令使用 [genSymKey](#) 來建立 256 位元的 AES 金鑰。它會使用 `-sess` 參數來建立只在目前工作階段中存在的金鑰。

輸出顯示 HSM 建立了金鑰 262168。

```
Command: genSymKey -t 31 -s 32 -l AES-wrapping-key -sess
```

```
Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS
```

```
Symmetric Key Created. Key Handle: 262168
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

接著，範例會驗證金鑰 8 (要匯出的金鑰) 是可擷取的對稱金鑰。它也會驗證包裝金鑰 (金鑰 262168) 是只存在於工作階段中的 AES 金鑰。您可以使用 [findKey](#) 命令，而本範例則是將兩個金鑰的屬性匯出到檔案，然後使用 `grep` 在檔案中尋找相關的屬性值。



這些命令使用 `getAttribute`，再加上 `-a` 的值為 512 (所有)，來取得 8 和 262168 金鑰的所有屬性。如需有關這些金鑰屬性的詳細資訊，請參閱[the section called “金鑰屬性參考”](#)。

```
getAttribute -o 8 -a 512 -out attributes/attr_8
getAttribute -o 262168 -a 512 -out attributes/attr_262168
```

這些命令使用 `grep` 來驗證要匯出金鑰 (金鑰 8) 的屬性，以及僅限工作階段的包裝金鑰 (金鑰 262168)。

```
// Verify that the key to be exported is a symmetric key.
$ grep -A 1 "OBJ_ATTR_CLASS" attributes/attr_8
OBJ_ATTR_CLASS
0x04

// Verify that the key to be exported is extractable.
$ grep -A 1 "OBJ_ATTR_KEY_TYPE" attributes/attr_8
OBJ_ATTR_EXTRACTABLE
0x00000001

// Verify that the wrapping key is an AES key
$ grep -A 1 "OBJ_ATTR_KEY_TYPE" attributes/attr_262168
OBJ_ATTR_KEY_TYPE
0x1f

// Verify that the wrapping key is a session key
$ grep -A 1 "OBJ_ATTR_TOKEN" attributes/attr_262168
OBJ_ATTR_TOKEN
0x00

// Verify that the wrapping key can be used for wrapping
$ grep -A 1 "OBJ_ATTR_WRAP" attributes/attr_262168
OBJ_ATTR_WRAP
0x00000001
```

最後，我們使用工作階段金鑰 (金鑰 262168) 做為包裝金鑰，來使用 `exSymKey` 命令匯出金鑰 8。

當工作階段結束時，金鑰 262168 便不再存在。

```
Command: exSymKey -k 8 -w 262168 -out aes256_H8.key
```

```
Cfm3WrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
Wrapped Symmetric Key written to file "aes256_H8.key"
```

### Example：使用外部取消包裝金鑰

此範例示範如何使用外部取消包裝金鑰來從 HSM 匯出金鑰。

當您從 HSM 匯出金鑰時，會指定 HSM 上的 AES 金鑰做為包裝金鑰。依預設，此包裝金鑰會用於將要匯出的金鑰進行包裝和取消包裝。不過，您可以使用 `-wk` 參數來告訴 `exSymKey` 使用磁碟上檔案中的外部金鑰來取消包裝。當您這麼做時，由 `-w` 參數指定的金鑰會包裝目標金鑰，而 `-wk` 參數指定檔案中的金鑰會將金鑰取消包裝。

因為包裝金鑰必須是 AES 金鑰 (其為對稱)，在 HSM 中的包裝金鑰和磁碟上的取消包裝金鑰必須有相同的金鑰資料。為此，您必須在匯出操作前將包裝金鑰匯入 HSM，或從 HSM 匯出包裝金鑰。

此範例會在 HSM 外建立金鑰，並將其匯入 HSM。它使用內部的金鑰複本來包裝要匯出的對稱金鑰，然後複製檔案中的金鑰來將其取消包裝。

第一個命令會使用 OpenSSL 來產生 256 位元的 AES 金鑰。此命令會將金鑰儲存到 `aes256-forImport.key` 檔案。OpenSSL 命令不會傳回任何輸出，但您可以使用多種命令來確認操作是否成功。此範例使用 `wc` (字數) 工具，確認包含 32 個位元組資料的檔案。

```
$ openssl rand -out keys/aes256-forImport.key 32
```

```
$ wc keys/aes256-forImport.key
0 2 32 keys/aes256-forImport.key
```

此命令會使用 [imSymKey](#) 命令將 AES 金鑰從 `aes256-forImport.key` 檔案匯入 HSM。命令完成後，HSM 中便有該金鑰，金鑰控制代碼為 262167，並位於 `aes256-forImport.key` 檔案中。

```
Command: imSymKey -f keys/aes256-forImport.key -t 31 -l aes256-imported -w 6
```

```
Cfm3WrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3CreateUnwrapTemplate returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Symmetric Key Unwrapped. Key Handle: 262167
```

## Cluster Error Status

Node id 1 and err state 0x00000000 : HSM Return: SUCCESS

Node id 0 and err state 0x00000000 : HSM Return: SUCCESS

此命令在匯出操作時使用該金鑰。命令使用 `exSymKey` 來匯出金鑰 21，後者是 192 位元的 AES 金鑰。若要包裝金鑰，它使用金鑰 262167，這是之前匯入 HSM 的複本。為了要將金鑰取消包裝，它使用 `aes256-forImport.key` 檔案中的相同金鑰資料。命令完成時，會將金鑰 21 匯出到 `aes192_h21.key` 檔案。

```
Command: exSymKey -k 21 -w 262167 -out aes192_H21.key -wk aes256-forImport.key
```

```
Cfm3WrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Wrapped Symmetric Key written to file "aes192_H21.key"
```

## 參數

**-h**

顯示命令的說明。

必要：是

**-k**

指定要匯出之金鑰的金鑰控制代碼。此為必要參數。輸入您擁有之對稱金鑰的金鑰控制代碼。此為必要參數。若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

若要確認金鑰是否匯出，請使用 [getAttribute](#) 命令取得 `OBJ_ATTR_EXTRACTABLE` 屬性的值 (以常數 354 表示)。此外，您只能匯出您擁有的金鑰。若要尋找金鑰的擁有者，請使用 [getKeyInfo](#) 命令。

必要：是

**-w**

指定包裝金鑰的金鑰控制代碼。此為必要參數。若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

包裝金鑰 是 HSM 中的金鑰，用於將要匯出的金鑰進行加密 (包裝) 然後解密 (取消包裝)。只有 AES 金鑰可以做為包裝金鑰。

您可以使用任何 AES 金鑰 (任何大小) 做為包裝金鑰。因為包裝金鑰將目標金鑰包裝後又立即取消包裝，您可以使用僅限工作階段的 AES 金鑰做為包裝金鑰。若要判斷金鑰是否可做為包裝金鑰，

使用 [getAttribute](#) 取得 OBJ\_ATTR\_WRAP 屬性之值 (以常數 262 表示)。要建立包裝金鑰，請使用 [genSymKey](#) 以建立 AES 金鑰 (輸入 31)。

如果您使用 `-wk` 參數來指定外部的取消包裝金鑰，則在匯出期間會使用 `-w` 包裝金鑰來進行包裝，但不會用來取消包裝。

 Note

Key 4 代表不支援的內部金鑰。建議您使用您所建立並做為包裝金鑰管理的 AES 金鑰。

必要：是

`-out`

指定輸出檔案的路徑和名稱。命令成功時，這個檔案中會包含匯出的純文字金鑰。如果檔案已存在，命令會覆寫檔案且不會有任何警告。

必要：是

`-m`

指定包裝機制。唯一的有效值是 4，這代表 NIST\_AES\_WRAP 機制。

必要：否

預設：4

`-wk`

使用指定檔案中的 AES 金鑰來將要匯出的金鑰取消包裝。輸入包含純文字 AES 金鑰的檔案路徑和名稱。

當您加入此參數時，`exSymKey` 會使用 `-w` 參數在 HSM 指定的金鑰來包裝要匯出的金鑰，並使用 `-wk` 檔案中的金鑰來取消包裝此金鑰。`-w` 和 `-wk` 參數值必須解析為相同的純文字金鑰。

必要：否

預設：使用 HSM 上的包裝金鑰來取消包裝。

## 相關主題

- [genSymKey](#)

- [imSymKey](#)
- [wrapKey](#)

## 使用 KMU 擷取 AWS CloudHSM 金鑰

使用 AWS CloudHSM `key_mgmt_util` 中的 `extractMaskedObject` 命令，從硬體安全模組 (HSM) 擷取金鑰，並將其儲存為遮罩物件的檔案。遮罩物件是「複製的」物件，僅可在使用 [insertMaskedObject](#) 命令將這些物件插回原始叢集後才可使用。您僅能將遮罩物件插入之前從中產生的相同叢集，或該叢集的複製品。這包括透過[複製跨區域備份](#)和[使用該備份建立新叢集](#)而產生之叢集的任何複製版本。

遮罩物件是卸載及同步金鑰的有效方式，包括無法擷取的金鑰 (即：具有 0 的 [OBJ\\_ATTR\\_EXTRACTABLE](#) 值的金鑰)。如此一來，金鑰就可以在不同區域的相關叢集之間安全地同步，而不需要更新 AWS CloudHSM [組態檔案](#)。

### Important

插入後，即將遮罩物件解密，並給予不同於原始金鑰之金鑰控制代碼的金鑰控制代碼。遮罩物件包括與原始金鑰關聯的所有中繼資料，包括屬性、所有權和分享資訊，以及仲裁設定。如果您需要同步處理應用程式中叢集間的金鑰，請改用 `cloudhsm_mgmt_util` 中的 [syncKey](#)。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並[登入](#) HSM。擁有金鑰的 CU 或任何 CO 都可使用 `extractMaskedObject` 命令。

### 語法

```
extractMaskedObject -h

extractMaskedObject -o <object-handle>
 -out <object-file>
```

### 範例

此範例顯示如何使用 `extractMaskedObject` 命令從 HSM 擷取做為遮罩物件的金鑰。

Example：擷取遮罩物件

此命令從包含控制代碼 524295 的金鑰，自 HSM 擷取遮罩物件，並另存為稱為 `maskedObj` 的檔案。當命令成功時，`extractMaskedObject` 會傳回成功訊息。

```
Command: extractMaskedObject -o 524295 -out maskedObj
```

```
Object was masked and written to file "maskedObj"
```

```
Cfm3ExtractMaskedObject returned: 0x00 : HSM Return: SUCCESS
```

## 參數

此命令會使用下列參數。

### **-h**

顯示命令的命令列說明。

必要：是

### **-o**

指定金鑰的控制代碼，以做為遮罩物件擷取。

必要：是

### **-out**

指定將儲存遮罩物件的檔案名稱。

必要：是

## 相關主題

- [insertMaskedObject](#)
- [syncKey](#)
- [跨區域複製備份](#)
- [從先前的備份建立 AWS CloudHSM 叢集](#)

## 使用 KMU 依屬性搜尋 AWS CloudHSM 索引鍵

使用 AWS CloudHSM `key_mgmt_util` 中的 `findKey` 命令，依金鑰屬性的值搜尋金鑰。當一個金鑰符合您設定的所有條件時，`findKey` 會傳回金鑰控制代碼。若不指定任何參數，`findKey` 會傳回您在 HSM 中可使用之所有金鑰的金鑰控制代碼。若要尋找特定金鑰的屬性值，請使用 [getAttribute](#)。

就像所有 `key_mgmt_util` 命令一樣，`findKey` 也是針對特定使用者。只會傳回目前的使用者在密碼編譯操作中可以使用的金鑰。這包括目前使用者擁有的金鑰，以及已經與目前使用者共用的金鑰。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入 HSM](#)。

## 語法

```
findKey -h

findKey [-c <key class>]
 [-t <key type>]
 [-l <key label>]
 [-id <key ID>]
 [-sess (0 | 1)]
 [-u <user-ids>]
 [-m <modulus>]
 [-kcv <key_check_value>]
```

## 範例

下列範例示範如何使用 `findKey` 以在 HSM 中尋找和識別金鑰。

### Example：尋找所有金鑰

此命令在 HSM 中找出目前使用者的所有金鑰。輸出包含使用者擁有和共用的金鑰，以及 HSM 中的所有公有金鑰。

若要取得具有特定金鑰控制代碼之金鑰的屬性，請使用 [getAttribute](#)。如要判斷目前使用者是否擁有或共用特定金鑰，請使用 `cloudhsm_mgmt_util` 中的 [getKeyInfo](#) 和 [findAllKeys](#)。

Command: **findKey**

Total number of keys present 13

number of keys matched from start index 0::12

6, 7, 524296, 9, 262154, 262155, 262156, 262157, 262158, 262159, 262160, 262161, 262162

Cluster Error Status

Node id 1 and err state 0x00000000 : HSM Return: SUCCESS

Node id 0 and err state 0x00000000 : HSM Return: SUCCESS

Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS

### Example：依類型、使用者和工作階段尋找金鑰

此命令會尋找目前使用者和使用者 3 可使用的持久性 AES 金鑰。(使用者 3 或許能夠使用目前使用者看不到的其他金鑰。)

```
Command: findKey -t 31 -sess 0 -u 3
```

### Example：依類別和標籤尋找金鑰

此命令針對目前使用者找出具有 2018-sept 標籤的所有公有金鑰。

```
Command: findKey -c 2 -l 2018-sept
```

### Example：依模數尋找 RSA 金鑰

此命令會針對目前的使用者，尋找以 m4.txt 檔案中的模數所建立之 RSA 金鑰 (類型 0)。

```
Command: findKey -t 0 -m m4.txt
```

## 參數

-h

顯示命令的說明。

必要：是

-t

尋找指定類型的金鑰。輸入代表金鑰類別的常數。例如，若要尋找 3DES 金鑰，請輸入 -t 21。

有效值：

- 0 : [RSA](#)
- 1 : [DSA](#)
- 3 : [EC](#)
- 16 : [GENERIC\\_SECRET](#)
- 18 : [RC4](#)
- 21 : [三重 DES \(3DES\)](#)
- 31 : [AES](#)



必要：否

-c

尋找指定類別中的金鑰。輸入代表金鑰類別的常數。例如，若要尋找公有金鑰，請輸入 -c 2。

每個金鑰類型的有效值：

- 2：公有。此類別包含公有/私有金鑰對中的公有金鑰。
- 3：私有。此類別包含公有/私有金鑰對中的私有金鑰。
- 4：私密。此類別包含所有對稱金鑰。

必要：否

-l

尋找具有指定標籤的金鑰。輸入確切的標籤。--l 值中不可使用萬用字元或規則表達式。

必要：否

-id

尋找具有指定 ID 的金鑰。輸入確切的 ID 字串。-id 值中不可使用萬用字元或規則表達式。

必要：否

-sess

依工作階段狀態尋找金鑰。若要尋找只在目前工作階段中有效的金鑰，請輸入 1。若要尋找持久性金鑰，請輸入 0。

必要：否

-u

尋找指定的使用者和目前的使用者共用的金鑰。輸入以逗號分隔的 HSM 使用者 ID 清單，例如 -u 3 或 -u 4,7。若要尋找 HSM 上的使用者 ID，請使用 [listUsers](#)。

當您指定一個使用者 ID 時，findKey 會傳回該使用者的金鑰。當您指定多個使用者 ID 時，findKey 會傳回所有指定之使用者可以使用的金鑰。

由於 findKey 只會傳回目前使用者可以使用的金鑰，-u 結果一律與目前使用者的金鑰相同或為其中一部分。如要取得任何使用者所擁有或共用的所有金鑰，加密管理員 (CO) 可使用 cloudhsm\_mgmt\_util 中的 [findAllKeys](#)。

必要：否

## -m

尋找透過指定檔案中的 RSA 模數所建立的金鑰。輸入存放模數之檔案的路徑。

-m 指定要匹配包含 RSA 模數的二進位檔案 (選用)。

必要：否

## -kcv

尋找具有指定之金鑰檢查值的金鑰。

金鑰檢查值 (KCV) 是 HSM 匯入或產生金鑰時所產生之金鑰的 3 位元組雜湊或總和檢查碼。您也可以 HSM 之外計算 KCV，例如在匯出金鑰之後。然後，您可以比較 KCV 值以確認金鑰的身分和完整性。若要取得金鑰的 KCV，請使用 [getAttribute](#)。

AWS CloudHSM 使用以下標準方法產生金鑰檢查值：

- 對稱密鑰：使用金鑰加密零塊的結果的前 3 個位元組。
- 非對稱金鑰配對：公有金鑰 SHA-1 雜湊的前 3 個位元組。
- HMAC 金鑰：目前不支援 HMAC 金鑰的 KCV。

必要：否

## 輸出

findKey 輸出會列出相符金鑰的總數及其金鑰控制代碼。

```
Command: findKey
Total number of keys present 10

number of keys matched from start index 0::9
6, 7, 8, 9, 10, 11, 262156, 262157, 262158, 262159

Cluster Error Status
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS

Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS
```

## 相關主題

- [findSingleKey](#)

- [getKeyInfo](#)
- [getAttribute](#)
- cloudhsm\_mgmt\_util 中的 [findAllKeys](#)
- [金鑰屬性參考](#)

## 使用 KMU 驗證 AWS CloudHSM 金鑰

使用 AWS CloudHSM key\_mgmt\_util 工具中的 findSingleKey 命令來驗證 AWS CloudHSM 叢集中所有硬體安全模組 (HSM) 上是否存在金鑰。

執行任何 key\_mgmt\_util 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

### 語法

```
findSingleKey -h

findSingleKey -k <key-handle>
```

### 範例

#### Example

此命令可驗證叢集中所有三個 HSM 上存在金鑰 252136。

```
Command: findSingleKey -k 252136
Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS

Cluster Error Status
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

### 參數

-h

顯示命令的說明。

必要：是

-k

指定 HSM 中某個金鑰的金鑰控制代碼。此為必要參數。

若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

必要：是

## 相關主題

- [findKey](#)
- [getKeyInfo](#)
- [getAttribute](#)

## 使用 KMU 產生 AWS CloudHSM DSA 金鑰對

使用 AWS CloudHSM `key_mgmt_util` 工具中的 `genDSAKeyPair` 命令，在您的硬體安全模組 (HSM) 中產生 [數位簽署演算法](#) (DSA) 金鑰對。您必須指定模數長度；命令會產生模數值。您還可以指派 ID、將金鑰與其他 HSM 使用者共用、建立不可擷取的金鑰，以及建立當工作階段結束時就過期的金鑰。命令成功時會傳回 HSM 指派給公有和私有金鑰的金鑰控制代碼。您可以使用金鑰控制代碼來向其他命令識別金鑰。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

### Tip

如要尋找您已建立之金鑰的屬性，例如類型、長度、標籤和 ID，請使用 [getAttribute](#)。如要尋找特定使用者的金鑰，請使用 [getKeyInfo](#)。如要根據金鑰屬性值來尋找金鑰，請使用 [findKey](#)。

## 語法

```
genDSAKeyPair -h

genDSAKeyPair -m <modulus length>
 -l <label>
 [-id <key ID>]
```

```

[-min_srv <minimum number of servers>]
[-m_value <0..8>]
[-nex]
[-sess]
[-timeout <number of seconds>]
[-u <user-ids>]
[-attest]

```

## 範例

下列範例示範如何使用 `genDSAKeyPair` 來建立 DSA 金鑰對。

### Example：建立 DSA 金鑰對

此命令建立標籤為 DSA 的 DSA 金鑰對。輸出顯示公有金鑰的金鑰控制代碼是 19，而私有金鑰的控制代碼是 21。

Command: **genDSAKeyPair -m 2048 -l DSA**

```

Cfm3GenerateKeyPair: returned: 0x00 : HSM Return: SUCCESS

Cfm3GenerateKeyPair: public key handle: 19 private key handle: 21

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS

```

### Example：建立僅限工作階段的 DSA 金鑰對

此命令會建立只在目前工作階段中有效的 DSA 金鑰對。除了必要的 (非唯一) 標籤，此命令還會指派 `DSA_temp_pair` 的唯一 ID。您可以建立像這樣的金鑰對，以簽署和驗證僅限工作階段的字符。輸出顯示公有金鑰的金鑰控制代碼是 12，而私有金鑰的控制代碼是 14。

Command: **genDSAKeyPair -m 2048 -l DSA-temp -id DSA\_temp\_pair -sess**

```

Cfm3GenerateKeyPair: returned: 0x00 : HSM Return: SUCCESS

Cfm3GenerateKeyPair: public key handle: 12 private key handle: 14

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS

```

若要確認金鑰對只存在於工作階段中，請使用 `-sessfindKey` [的](#) 參數，且值為 1 (true)。

```
Command: findKey -sess 1
```

```
Total number of keys present 2
```

```
number of keys matched from start index 0::1
12, 14
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS
```

### Example : 建立共用、不可擷取的 DSA 金鑰對

此命令建立 DSA 金鑰對。私有金鑰共用給其他三個使用者，且無法從 HSM 匯出。公有金鑰可供任何使用者使用，且一律可擷取。

```
Command: genDSAKeyPair -m 2048 -l DSA -id DSA_shared_pair -nex -u 3,5,6
```

```
Cfm3GenerateKeyPair: returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3GenerateKeyPair: public key handle: 11 private key handle: 19
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

### Example : 建立規定人數控制的金鑰對

此命令建立標籤為 DSA-mV2 的 DSA 金鑰對。此命令使用 -u 參數，將私有金鑰共用給使用者 4 和 6。此命令使用 -m\_value 參數，針對任何使用私有金鑰的加密操作，要求至少兩次核准的仲裁。此命令還使用 -attest 參數，以驗證用來產生金鑰對的韌體完整性。

輸出顯示命令已產生金鑰控制代碼為 12 的公用金鑰，以及金鑰控制代碼 17 的私有金鑰，且已通過對叢集韌體的證實檢查。

```
Command: genDSAKeyPair -m 2048 -l DSA-mV2 -m_value 2 -u 4,6 -attest
```

```
Cfm3GenerateKeyPair: returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3GenerateKeyPair: public key handle: 12 private key handle: 17
```

```
Attestation Check : [PASS]
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

此命令使用私有金鑰 (金鑰控制代碼 17) 上的 [getKeyInfo](#)。輸出確認金鑰由目前的使用者 (使用者 3) 擁有，且共用給使用者 4 和 6 (沒有其他任何人)。輸出也顯示規定人數身分驗證已啟用，且規定人數為 2。

```
Command: getKeyInfo -k 17
```

```
Cfm3GetKey returned: 0x00 : HSM Return: SUCCESS
```

```
Owned by user 3
```

```
also, shared to following 2 user(s):
```

```
4
```

```
6
```

```
2 Users need to approve to use/manage this key
```

## 參數

**-h**

顯示命令的說明。

必要：是

**-m**

指定模數的長度 (以位元為單位)。唯一有效的值為 2048。

必要：是

**-l**

指使用者定義的金鑰對標籤。輸入一個字串。相同標籤套用至金鑰對中的兩個金鑰。label 的大小上限為 127 個字元。

您可以使用任何可以幫助您識別金鑰的片語。標籤不具唯一性，因此您可使用標籤將金鑰進行分組和分類。

必要：是

-id

指使用者定義的金鑰對識別符。輸入叢集中唯一的字串。預設為空字串。您指定的 ID 會套用至金鑰對中的兩個金鑰。

預設：無 ID 值。

必要：否

-min\_srv

指在 -timeout 參數值過期之前同步金鑰所需的 HSM 數量下限。如果未在規定時間內同步至指定數量的伺服器，金鑰就不會建立。

AWS CloudHSM 會自動將每個金鑰同步到叢集中的每個 HSM。要加速流程，請將 min\_srv 值設定為少於叢集中之 HSM 的數量，並設定低逾時值。然而，請注意有些請求可能不會產生金鑰。

預設：1

必要：否

-m\_value

指須核准使用金鑰對中私有金鑰之密碼編譯操作的使用者數量。輸入 0 到 8 之間的值。

此參數會建立私有金鑰的規定人數驗證要求。預設值 0 會停用金鑰的規定人數驗證功能。啟用規定人數驗證時，指定數目的使用者必須簽署權杖，才能核准使用私用金鑰的密碼編譯操作，以及核准共用或取消共用私有金鑰的操作。

如要尋找金鑰的 m\_value，請使用 [getKeyInfo](#)。

只有當命令中的 -u 參數與一定數量的使用者共用金鑰對以符合 m\_value 要求時，此參數才有效。

預設：0

必要：否

-nex

使私有金鑰無法擷取。產生的私有金鑰無法[從 HSM 匯出](#)。公有金鑰始終可擷取。



預設：金鑰對中的公有金鑰和私有金鑰均可擷取。

必要：否

-sess

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

若要將工作階段金鑰更改為持久性 (權杖) 金鑰，請使用 [setAttribute](#)。

預設：此金鑰是持久性金鑰。

必要：否

-timeout

指命令等待金鑰同步到 min\_srv 參數指定數目的 HSM 的時長 (以秒為單位)。

此參數只有在命令中同時使用 min\_srv 參數時才有效。

預設：無逾時。該命令會無限期等待，並且僅在將金鑰同步到最小數目的伺服器時才返回。

必要：否

-u

與指定使用者共用金鑰對中的私有金鑰。此參數允許其他 HSM 加密使用者 (CU) 在密碼編譯操作中使用此金鑰。任何使用者均可在無需共用的情況下使用公有金鑰。

輸入以逗號分隔的 HSM 使用者 ID 清單，例如 -u 5,6。請勿包含現行使用者的 HSM 使用者 ID。若要尋找 HSM 上 CU 的 HSM 使用者 ID，請使用 [listUsers](#)。之後，如要共用或取消共用現有金鑰，請使用 cloudhsm\_mgmt\_util 中的 [shareKey](#)。

預設：只有目前使用者能使用匯入的私有金鑰。

必要：否

-attest

執行完整性檢查，以驗證執行叢集的韌體未被篡改。

預設：無認證檢查。

必要：否

## 相關主題

- [genRSAKeyPair](#)
- [genSymKey](#)
- [genECCKeyPair](#)

## 使用 KMU 產生 AWS CloudHSM ECC 金鑰對

使用 AWS CloudHSM `key_mgmt_util` 工具中的 `genECCKeyPair` 命令，在您的硬體安全模組 (HSM) 中產生 [橢圓曲線密碼編譯 \(ECC\)](#) 金鑰對。執行 `genECCKeyPair` 命令時，您必須指定橢圓曲線識別碼和金鑰對的標籤。您也可以將私有金鑰共用給其他 CU 使用者、建立不可擷取的金鑰、由規定人數控制的金鑰及工作階段結束時就過期的金鑰。命令成功時會傳回 HSM 指派給公有和私有 ECC 金鑰的金鑰控制代碼。您可以使用金鑰控制代碼來向其他命令識別金鑰。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

### Tip

如要尋找您已建立之金鑰的屬性，例如類型、長度、標籤和 ID，請使用 [getAttribute](#)。如要尋找特定使用者的金鑰，請使用 [getKeyInfo](#)。如要根據金鑰屬性值來尋找金鑰，請使用 [findKey](#)。

## 語法

```
genECCKeyPair -h

genECCKeyPair -i <EC curve id>
 -l <label>
 [-id <key ID>]
 [-min_srv <minimum number of servers>]
 [-m_value <0..8>]
 [-nex]
 [-sess]
 [-timeout <number of seconds>]
 [-u <user-ids>]
```

`[-attest]`

## 範例

以下範例示範如何使用 `genECCKeypair` 在 HSM 中建立 ECC 金鑰對。

Example：建立和檢查 ECC 金鑰對

此命令使用 `NID_secp384r1` 橢圓曲線和 `ecc14` 標籤建立 ECC 金鑰對。輸出顯示私有金鑰的金鑰控制代碼是 262177，而公有金鑰的金鑰控制代碼是 262179。公有和私有金鑰都會套用此標籤。

```
Command: genECCKeypair -i 14 -l ecc14
```

```
Cfm3GenerateKeyPair returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3GenerateKeyPair: public key handle: 262179 private key handle: 262177
```

```
Cluster Error Status
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

產生金鑰後，您可以檢查其屬性。使用 [getAttribute](#)，將新 ECC 私有金鑰的所有屬性 (以常數 512 表示) 寫入 `attr_262177` 檔案。

```
Command: getAttribute -o 262177 -a 512 -out attr_262177
```

```
got all attributes of size 529 attr cnt 19
```

```
Attributes dumped into attr_262177
```

```
Cfm3GetAttribute returned: 0x00 : HSM Return: SUCCESS
```

然後使用 `cat` 命令來檢視 `attr_262177` 屬性檔案的內容。輸出顯示金鑰是橢圓曲線私有金鑰，可用於簽署，但不可用於加密、解密、包裝、取消包裝或驗證。金鑰為持久性且可匯出。

```
$ cat attr_262177
```

```
OBJ_ATTR_CLASS
```

```
0x03
```

```
OBJ_ATTR_KEY_TYPE
```

```
0x03
```

```
OBJ_ATTR_TOKEN
```

```
0x01
```

```

OBJ_ATTR_PRIVATE
0x01
OBJ_ATTR_ENCRYPT
0x00
OBJ_ATTR_DECRYPT
0x00
OBJ_ATTR_WRAP
0x00
OBJ_ATTR_UNWRAP
0x00
OBJ_ATTR_SIGN
0x01
OBJ_ATTR_VERIFY
0x00
OBJ_ATTR_LOCAL
0x01
OBJ_ATTR_SENSITIVE
0x01
OBJ_ATTR_EXTRACTABLE
0x01
OBJ_ATTR_LABEL
ecc2
OBJ_ATTR_ID

OBJ_ATTR_VALUE_LEN
0x00000008a
OBJ_ATTR_KCV
0xbbb32a
OBJ_ATTR_MODULUS
044a0f9d01d10f7437d9fa20995f0cc742552e5ba16d3d7e9a65a33e20ad3e569e68eb62477a9960a87911e6121d112
OBJ_ATTR_MODULUS_BITS
0x00000019f

```

### Example 使用無效的 EEC 曲線

此命令嘗試使用 NID\_X9\_62\_prime192v1 曲線建立 ECC 金鑰對。由於該橢圓曲線不適用於 FIPS 模式的 HSM，命令會失敗。訊息報告叢集內有一部伺服器無法使用，但這通常不表示叢集內的 HSM 有問題。

Command: **genECCKeypair -i 1 -l ecc1**

```

Cfm3GenerateKeyPair returned: 0xb3 : HSM Error: This operation violates the
current configured/FIPS policies

```

**Cluster Error Status**

Node id 0 and err state 0x30000085 : HSM CLUSTER ERROR: Server in cluster is unavailable

**參數**

**-h**

顯示命令的說明。

必要：是

**-i**

指定橢圓曲線的識別符。輸入識別符。

有效值：

- 2: NID\_X9\_62\_prime256v1
- 14: NID\_secp384r1
- 16: NID\_secp256k1

必要：是

**-l**

指使用者定義的金鑰對標籤。輸入一個字串。相同標籤套用至金鑰對中的兩個金鑰。label 的大小上限為 127 個字元。

您可以使用任何可以幫助您識別金鑰的片語。標籤不具唯一性，因此您可使用標籤將金鑰進行分組和分類。

必要：是

**-id**

指使用者定義的金鑰對識別符。輸入叢集中唯一的字串。預設為空字串。您指定的 ID 會套用至金鑰對中的兩個金鑰。

預設：無 ID 值。

必要：否

## `-min_srv`

指在 `-timeout` 參數值過期之前同步金鑰所需的 HSM 數量下限。如果未在規定時間內同步至指定數量的伺服器，金鑰就不會建立。

AWS CloudHSM 會自動將每個金鑰同步到叢集中的每個 HSM。要加速流程，請將 `min_srv` 值設定為少於叢集中之 HSM 的數量，並設定低逾時值。然而，請注意有些請求可能不會產生金鑰。

預設：1

必要：否

## `-m_value`

指須核准使用金鑰對中私有金鑰之密碼編譯操作的使用者數量。輸入 0 到 8 之間的值。

此參數會建立私有金鑰的規定人數驗證要求。預設值 0 會停用金鑰的規定人數驗證功能。啟用規定人數驗證時，指定數目的使用者必須簽署權杖，才能核准使用私用金鑰的密碼編譯操作，以及核准共用或取消共用私有金鑰的操作。

如要尋找金鑰的 `m_value`，請使用 [getKeyInfo](#)。

只有當命令中的 `-u` 參數與一定數量的使用者共用金鑰對以符合 `m_value` 要求時，此參數才有效。

預設：0

必要：否

## `-nex`

使私有金鑰無法擷取。產生的私有金鑰無法[從 HSM 匯出](#)。公有金鑰始終可擷取。

預設：金鑰對中的公有金鑰和私有金鑰均可擷取。

必要：否

## `-sess`

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

若要將工作階段金鑰更改為持久性 (權杖) 金鑰，請使用 [setAttribute](#)。

預設：此金鑰是持久性金鑰。

必要：否

-timeout

指命令等待金鑰同步到 min\_srv 參數指定數目的 HSM 的時長 (以秒為單位)。

此參數只有在命令中同時使用 min\_srv 參數時才有效。

預設：無逾時。該命令會無限期等待，並且僅在將金鑰同步到最小數目的伺服器時才返回。

必要：否

-u

與指定使用者共用金鑰對中的私有金鑰。此參數允許其他 HSM 加密使用者 (CU) 在密碼編譯操作中使用此金鑰。任何使用者均可在無需共用的情況下使用公有金鑰。

輸入以逗號分隔的 HSM 使用者 ID 清單，例如 -u 5,6。請勿包含現行使用者的 HSM 使用者 ID。若要尋找 HSM 上 CU 的 HSM 使用者 ID，請使用 [listUsers](#)。之後，如要共用或取消共用現有金鑰，請使用 cloudhsm\_mgmt\_util 中的 [shareKey](#)。

預設：只有目前使用者能使用匯入的私有金鑰。

必要：否

-attest

執行完整性檢查，以驗證執行叢集的韌體未被篡改。

預設：無認證檢查。

必要：否

## 相關主題

- [genSymKey](#)
- [genRSAKeyPair](#)
- [genDSAKeyPair](#)

## 使用 KMU 產生 AWS CloudHSM RSA 金鑰對

使用 AWS CloudHSM key\_mgmt\_util 工具中的 genRSAKeyPair 命令來產生 [RSA](#) 非對稱金鑰對。您需要指定金鑰類型、模數長度及公有指數。此命令產生指定長度的模數並建立金鑰對。您可以指派 ID、

將金鑰與其他 HSM 使用者共用、建立不可擷取的金鑰及工作階段結束時就過期的金鑰。命令成功時會傳回 HSM 指派給金鑰的金鑰控制代碼。您可以使用金鑰控制代碼來向其他命令識別金鑰。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

#### Tip

如要尋找您已建立之金鑰的屬性，例如類型、長度、標籤和 ID，請使用 [getAttribute](#)。如要尋找特定使用者的金鑰，請使用 [getKeyInfo](#)。如要根據金鑰屬性值來尋找金鑰，請使用 [findKey](#)。

## 語法

```
genRSAKeyPair -h

genRSAKeyPair -m <modulus length>
 -e <public exponent>
 -l <label>
 [-id <key ID>]
 [-min_srv <minimum number of servers>]
 [-m_value <0..8>]
 [-nex]
 [-sess]
 [-timeout <number of seconds>]
 [-u <user-ids>]
 [-attest]
```

## 範例

下列範例示範如何使用 `genRSAKeyPair` 在 HSM 中建立非對稱金鑰對。

Example：建立和檢查 RSA 金鑰對

此命令建立具有 2048 位元模數和指數為 65537 的 RSA 金鑰對。輸出顯示公有金鑰控制代碼是 2100177，私有金鑰控制代碼是 2100426。

```
Command: genRSAKeyPair -m 2048 -e 65537 -l rsa_test
```

```
Cfm3GenerateKeyPair returned: 0x00 : HSM Return: SUCCESS
```



```
Cfm3GenerateKeyPair: public key handle: 2100177 private key handle:
2100426
```

```
Cluster Status:
```

```
Node id 0 status: 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 status: 0x00000000 : HSM Return: SUCCESS
```

下一個命令會使用 [getAttribute](#)，以取得剛建立之公有金鑰的屬性。此命令會將輸出寫入 `attr_2100177` 檔案。接著以 `cat` 命令來取得屬性檔案的內容。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

產生的十六進制值可確認這是類型為 RSA (OBJ\_ATTR\_CLASS 0x02) 的公有金鑰 (OBJ\_ATTR\_KEY\_TYPE 0x00)。您可以使用此公有金鑰來加密 (OBJ\_ATTR\_ENCRYPT 0x01)，但不能解密 (OBJ\_ATTR\_DECRYPT 0x00)。結果還包括金鑰長度 (512, 0x200)、模數、模數長度 (2048, 0x800) 及公有指數 (65537, 0x10001)。

```
Command: getAttribute -o 2100177 -a 512 -out attr_2100177
```

```
Attribute size: 801, count: 26
```

```
Written to: attr_2100177 file
```

```
Cfm3GetAttribute returned: 0x00 : HSM Return: SUCCESS
```

```
$ cat attr_2100177
```

```
OBJ_ATTR_CLASS
```

```
0x02
```

```
OBJ_ATTR_KEY_TYPE
```

```
0x00
```

```
OBJ_ATTR_TOKEN
```

```
0x01
```

```
OBJ_ATTR_PRIVATE
```

```
0x01
```

```
OBJ_ATTR_ENCRYPT
```

```
0x01
```

```
OBJ_ATTR_DECRYPT
```

```
0x00
```

```
OBJ_ATTR_WRAP
```

```
0x01
```

```
OBJ_ATTR_UNWRAP
```

```
0x00
```

```
OBJ_ATTR_SIGN
```

```
0x00
OBJ_ATTR_VERIFY
0x01
OBJ_ATTR_LOCAL
0x01
OBJ_ATTR_SENSITIVE
0x00
OBJ_ATTR_EXTRACTABLE
0x01
OBJ_ATTR_LABEL
rsa_test
OBJ_ATTR_ID

OBJ_ATTR_VALUE_LEN
0x00000200
OBJ_ATTR_KCV
0xc51c18
OBJ_ATTR_MODULUS
0xbb9301cc362c1d9724eb93da8adab0364296bde7124a241087d9436b9be57e4f7780040df03c2c
1c0fe6e3b61aa83c205280119452868f66541bbbffacbbe787b8284fc81deaef2b8ec0ba25a077d
6983c77a1de7b17cbe8e15b203868704c6452c2810344a7f2736012424cf0703cf15a37183a1d2d0
97240829f8f90b063dd3a41171402b162578d581980976653935431da0c1260bfe756d85dca63857
d9f27a541676cb9c7def0ef6a2a89c9b9304bcac16fdf8183c0a555421f9ad5dfefb534cf26b65873
970cdf1a07484f1c128b53e10209cc6f7ac308669112968c81a5de408e7f644fe58b1a9ae1286fec
b3e4203294a96fae06f8f0db7982cb5d7f
OBJ_ATTR_MODULUS_BITS
0x00000800
OBJ_ATTR_PUBLIC_EXPONENT
0x010001
OBJ_ATTR_TRUSTED
0x00
OBJ_ATTR_WRAP_WITH_TRUSTED
0x00
OBJ_ATTR_DESTROYABLE
0x01
OBJ_ATTR_DERIVE
0x00
OBJ_ATTR_ALWAYS_SENSITIVE
0x00
OBJ_ATTR_NEVER_EXTRACTABLE
0x00
```

## Example：產生共用 RSA 金鑰對

此命令會產生 RSA 金鑰對，並將私有金鑰向使用者 4 (HSM 上的另一個 CU) 共用。此命令會使用 `m_value` 參數來要求至少兩次核准，才能將金鑰對的私有金鑰用於密碼編譯操作。當您使用 `m_value` 參數時，您在命令中還必須使用 `-u`，且 `m_value` 不可超過使用者總數 (`-u` 的值個數 + 擁有者)。

```
Command: genRSAKeyPair -m 2048 -e 65537 -l rsa_mofn -id rsa_mv2 -u 4 -m_value 2
```

```
Cfm3GenerateKeyPair returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3GenerateKeyPair: public key handle: 27 private key handle: 28
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

## 參數

`-h`

顯示命令的說明。

必要：是

`-m`

指模數的長度 (以位元為單位)。最小值為 2048。

必要：是

`-e`

指公有指數。值必須為大於或等於 65537 的奇數。

必要：是

`-l`

指使用者定義的金鑰對標籤。輸入一個字串。相同標籤套用至金鑰對中的兩個金鑰。label 的大小上限為 127 個字元。

您可以使用任何可以幫助您識別金鑰的片語。標籤不具唯一性，因此您可使用標籤將金鑰進行分組和分類。

必要：是

-id

指使用者定義的金鑰對識別符。輸入叢集中唯一的字串。預設為空字串。您指定的 ID 會套用至金鑰對中的兩個金鑰。

預設：無 ID 值。

必要：否

-min\_srv

指在 -timeout 參數值過期之前同步金鑰所需的 HSM 數量下限。如果未在規定時間內同步至指定數量的伺服器，金鑰就不會建立。

AWS CloudHSM 會自動將每個金鑰同步到叢集中的每個 HSM。要加速流程，請將 min\_srv 值設定為少於叢集中之 HSM 的數量，並設定低逾時值。然而，請注意有些請求可能不會產生金鑰。

預設：1

必要：否

-m\_value

指須核准使用金鑰對中私有金鑰之密碼編譯操作的使用者數量。輸入 0 到 8 之間的值。

此參數會建立私有金鑰的規定人數驗證要求。預設值 0 會停用金鑰的規定人數驗證功能。啟用規定人數驗證時，指定數目的使用者必須簽署權杖，才能核准使用私用金鑰的密碼編譯操作，以及核准共用或取消共用私有金鑰的操作。

如要尋找金鑰的 m\_value，請使用 [getKeyInfo](#)。

只有當命令中的 -u 參數與一定數量的使用者共用金鑰對以符合 m\_value 要求時，此參數才有效。

預設：0

必要：否

-nex

使私有金鑰無法擷取。產生的私有金鑰無法[從 HSM 匯出](#)。公有金鑰始終可擷取。

預設：金鑰對中的公有金鑰和私有金鑰均可擷取。

必要：否

#### -sess

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

若要將工作階段金鑰更改為持久性 (權杖) 金鑰，請使用 [setAttribute](#)。

預設：此金鑰是持久性金鑰。

必要：否

#### -timeout

指命令等待金鑰同步到 min\_srv 參數指定數目的 HSM 的時長 (以秒為單位)。

此參數只有在命令中同時使用 min\_srv 參數時才有效。

預設：無逾時。該命令會無限期等待，並且僅在將金鑰同步到最小數目的伺服器時才返回。

必要：否

#### -u

與指定使用者共用金鑰對中的私有金鑰。此參數允許其他 HSM 加密使用者 (CU) 在密碼編譯操作中使用此金鑰。任何使用者均可在無需共用的情況下使用公有金鑰。

輸入以逗號分隔的 HSM 使用者 ID 清單，例如 -u 5,6。請勿包含現行使用者的 HSM 使用者 ID。若要尋找 HSM 上 CU 的 HSM 使用者 ID，請使用 [listUsers](#)。之後，如要共用或取消共用現有金鑰，請使用 cloudhsm\_mgmt\_util 中的 [shareKey](#)。

預設：只有目前使用者能使用匯入的私有金鑰。

必要：否

#### -attest

執行完整性檢查，以驗證執行叢集的韌體未被篡改。

預設：無認證檢查。

必要：否

## 相關主題

- [genSymKey](#)
- [genDSAKeyPair](#)
- [genECCKeyPair](#)

## 使用 KMU AWS CloudHSM 產生對稱金鑰

使用 AWS CloudHSM `key_mgmt_util` 工具中的 `genSymKey` 命令，在您的硬體安全模組 (HSM) 中產生對稱金鑰。您可以指定金鑰類型和大小、指派 ID 和標籤，以及與其他 HSM 使用者共用金鑰。您也可以建立不可擷取的金鑰，以及工作階段結束時就過期的金鑰。命令成功時會傳回 HSM 指派給金鑰的金鑰控制代碼。您可以使用金鑰控制代碼來向其他命令識別金鑰。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
genSymKey -h

genSymKey -t <key-type>
 -s <key-size>
 -l <label>
 [-id <key-ID>]
 [-min_srv <minimum-number-of-servers>]
 [-m_value <0..8>]
 [-nex]
 [-sess]
 [-timeout <number-of-seconds>]
 [-u <user-ids>]
 [-attest]
```

## 範例

下列範例示範如何使用 `genSymKey` 在 HSM 中建立對稱金鑰。

**Tip**

如要使用您在這些範例中建立的金鑰進行 HMAC 操作，您必須在產生金鑰後將 OBJ\_ATTR\_SIGN 和 OBJ\_ATTR\_VERIFY 設為 TRUE。如要設定這些值，請使用 CloudHSM 管理公用程式 (CMU) 中的 setAttribute。如需詳細資訊，請參閱 [setAttribute](#)。

**Example : 產生 AES 金鑰**

此命令建立標籤為 aes256 的 256 位元 AES 金鑰。輸出顯示新金鑰的金鑰控制代碼是 6。

```
Command: genSymKey -t 31 -s 32 -l aes256
```

```
Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS
```

```
Symmetric Key Created. Key Handle: 6
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

**Example : 建立工作階段金鑰**

此命令會建立不可擷取的 192 位元 AES 金鑰，此金鑰只在目前的工作階段中有效。您可以建立像這樣的金鑰來包裝 (然後立即拆封) 正在匯出的金鑰。

```
Command: genSymKey -t 31 -s 24 -l tmpAES -id wrap01 -nex -sess
```

**Example : 快速返回**

此命令會建立標籤為 IT\_test\_key 的一般 512 位元組金鑰。此命令不會等待金鑰同步至叢集內的所有 HSM。相反地，一旦在任何一個 HSM 上建立金鑰 (-min\_srv 1) 或 1 秒之內 (-timeout 1) 就立即返回，以最快者為準。如果在逾時到期之前金鑰未同步至指定的 HSM 最少數量，金鑰就不會建立。您可以在指令碼中使用像這樣的命令來建立許多金鑰，例如下列範例中的 for 迴圈。

```
Command: genSymKey -t 16 -s 512 -l IT_test_key -min_srv 1 -timeout 1
```

```
$ for i in {1..30};
do /opt/cloudhsm/bin/key_mgmt_util singlecmd loginHSM -u CU -s example_user -p
example_pwd genSymKey -l aes -t 31 -s 32 -min_srv 1 -timeout 1;
done;
```

**Example : 建立規定人數授權的一般金鑰**

此命令會建立標籤為 generic-mV2 的 2048 位元一般私密金鑰。此命令使用 -u 參數來與另一個 CU (使用者 6) 共用金鑰。此命令使用 -m\_value 參數，針對任何使用金鑰的密碼編譯操作，要求至少兩次核准的仲裁。此命令還使用 -attest 參數來驗證所產生金鑰的韌體完整性。

輸出顯示命令已產生金鑰控制代碼為 9 的金鑰，且已通過對叢集韌體的證實檢查。

```
Command: genSymKey -t 16 -s 2048 -l generic-mV2 -m_value 2 -u 6 -
attest

Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS

Symmetric Key Created. Key Handle: 9

Attestation Check : [PASS]

Cluster Error Status
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

**Example : 建立和檢查金鑰**

此命令會建立標籤為 3DES\_shared 和 ID 為 IT-02 的三重 DES 金鑰。金鑰可供目前使用者及使用者 4 和 5 使用。如果 ID 在叢集內不是唯一的，或目前使用者是使用者 4 或 5，命令會失敗。

輸出顯示新金鑰的金鑰控制代碼是 7。

```
Command: genSymKey -t 21 -s 24 -l 3DES_shared -id IT-02 -u 4,5

Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS

Symmetric Key Created. Key Handle: 7

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

若要驗證新的 3DES 金鑰是否為目前使用者所擁有，並與使用者 4 和 5 共用，請使用 [getKeyInfo](#)。此命令會使用指派給新金鑰的控制代碼 (Key Handle: 7)。



輸出確認金鑰為使用者 3 所擁有，且與使用者 4 和 5 共用。

```
Command: getKeyInfo -k 7
```

```
Cfm3GetKey returned: 0x00 : HSM Return: SUCCESS
```

```
Owned by user 3
```

```
also, shared to following 2 user(s):
```

```
4, 5
```

若要確認金鑰的其他屬性，請使用 [getAttribute](#)。第一個命令使用 `getAttribute` 來取得金鑰控制代碼 7 (-o 7) 的所有屬性 (-a 512)。然後將屬性寫入 `attr_7` 檔案。第二個命令使用 `cat` 以取得 `attr_7` 檔案的內容。

此命令確認金鑰 7 是 192 位元 (OBJ\_ATTR\_VALUE\_LEN 0x00000018 或 24 位元組) 3DES (OBJ\_ATTR\_KEY\_TYPE 0x15) 對稱金鑰 (OBJ\_ATTR\_CLASS 0x04)，標籤為 3DES\_shared (OBJ\_ATTR\_LABEL 3DES\_shared)，ID 為 IT\_02 (OBJ\_ATTR\_ID IT-02)。金鑰是持久性 (OBJ\_ATTR\_TOKEN 0x01) 且可擷取 (OBJ\_ATTR\_EXTRACTABLE 0x01)，還可以用於加密、解密和包裝。

#### Tip

如要尋找您已建立之金鑰的屬性，例如類型、長度、標籤和 ID，請使用 [getAttribute](#)。如要尋找特定使用者的金鑰，請使用 [getKeyInfo](#)。如要根據金鑰屬性值來尋找金鑰，請使用 [findKey](#)。

如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

```
Command: getAttribute -o 7 -a 512 -out attr_7
```

```
got all attributes of size 444 attr cnt 17
```

```
Attributes dumped into attr_7 file
```

```
Cfm3GetAttribute returned: 0x00 : HSM Return: SUCCESS
```

```
$ cat attr_7
```

```
OBJ_ATTR_CLASS
0x04
OBJ_ATTR_KEY_TYPE
0x15
OBJ_ATTR_TOKEN
0x01
OBJ_ATTR_PRIVATE
0x01
OBJ_ATTR_ENCRYPT
0x01
OBJ_ATTR_DECRYPT
0x01
OBJ_ATTR_WRAP
0x00
OBJ_ATTR_UNWRAP
0x00
OBJ_ATTR_SIGN
0x00
OBJ_ATTR_VERIFY
0x00
OBJ_ATTR_LOCAL
0x01
OBJ_ATTR_SENSITIVE
0x01
OBJ_ATTR_EXTRACTABLE
0x01
OBJ_ATTR_LABEL
3DES_shared
OBJ_ATTR_ID
IT-02
OBJ_ATTR_VALUE_LEN
0x00000018
OBJ_ATTR_KCV
0x59a46e
```

 Tip

如要使用您在這些範例中建立的金鑰進行 HMAC 操作，您必須在產生金鑰後將 OBJ\_ATTR\_SIGN 和 OBJ\_ATTR\_VERIFY 設為 TRUE。若要設定這些值，請使用 CMU 中的 `setAttribute`。如需詳細資訊，請參閱 [setAttribute](#)。

## 參數

-h

顯示命令的說明。

必要：是

-t

指對稱金鑰的類型。輸入代表金鑰類型的常數。例如，若要建立 AES 金鑰，請輸入 -t 31。

有效值：

- 16：[GENERIC\\_SECRET](#)。一般私密金鑰是位元組陣列，不符合任何特定標準，例如，AES 金鑰的需求。
- 18：[RC4](#)。RC4 金鑰不適用於 FIPS 模式的 HSM
- 21：[三重 DES \(3DES\)](#)。根據 NIST 指引，2023 年之後處於 FIPS 模式的叢集不允許這樣做。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。
- 31：[AES](#)

必要：是

-s

指定金鑰大小 (位元組)。例如，若要建立 192 位元金鑰，請輸入 24。

每個金鑰類型的有效值：

- AES：16 (128 位元)、24 (192 位元)、32 (256 位元)
- 3DES：24 (192 位元)
- 一般密碼：<3584 (28672 位元)

必要：是

-l

指使用者定義的金鑰對標籤。輸入一個字串。

您可以使用任何可以幫助您識別金鑰的片語。標籤不具唯一性，因此您可使用標籤將金鑰進行分組和分類。

必要：是

-attest

執行完整性檢查，以驗證執行叢集的韌體未被篡改。

預設：無認證檢查。

必要：否

-id

指使用者定義的金鑰識別符。輸入叢集中唯一的字串。預設為空字串。

預設：無 ID 值。

必要：否

-min\_srv

指在 -timeout 參數值過期之前同步金鑰所需的 HSM 數量下限。如果未在規定時間內同步至指定數量的伺服器，金鑰就不會建立。

AWS CloudHSM 會自動將每個金鑰同步到叢集中的每個 HSM。要加速流程，請將 min\_srv 值設定為少於叢集中之 HSM 的數量，並設定低逾時值。然而，請注意有些請求可能不會產生金鑰。

預設：1

必要：否

-m\_value

指須核准使用金鑰之密碼編譯操作的使用者數量。輸入 0 到 8 之間的值。

此參數會建立私有金鑰的規定人數驗證要求。預設值 0 會停用金鑰的規定人數驗證功能。啟用規定人數驗證時，指定數目的使用者必須簽署權杖，才能核准使用金鑰的密碼編譯操作，以及核准共用或取消共用金鑰的操作。

如要尋找金鑰的 m\_value，請使用 [getKeyInfo](#)。

只有當命令中的 -u 參數與足夠的使用者共享金鑰以符合 m\_value 要求，此參數才有效。

預設：0

必要：否

**-nex**

使金鑰無法擷取。產生的金鑰無法[從 HSM 匯出](#)。

預設：此金鑰可擷取。

必要：否

**-sess**

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

若要將工作階段金鑰更改為持久性 (權杖) 金鑰，請使用 [setAttribute](#)。

預設：此金鑰是持久性金鑰。

必要：否

**-timeout**

指命令等待金鑰同步到 `min_srv` 參數指定數目的 HSM 的時長 (以秒為單位)。

此參數只有在命令中同時使用 `min_srv` 參數時才有效。

預設：無逾時。該命令會無限期等待，並且僅在將金鑰同步到最小數目的伺服器時才返回。

必要：否

**-u**

將金鑰共用給指定的使用者。此參數授與其他 HSM 密碼使用者 (CU) 在密碼編譯操作中使用此金鑰的許可。

輸入以逗號分隔的 HSM 使用者 ID 清單，例如 `-u 5,6`。請勿包含現行使用者的 HSM 使用者 ID。若要尋找 HSM 上 CU 的 HSM 使用者 ID，請使用 [listUsers](#)。之後，如要共用或取消共用現有金鑰，請使用 `cloudhsm_mgmt_util` 中的 [shareKey](#)。

預設：只有現行使用者能夠使用此金鑰。

必要：否

## 相關主題

- [exSymKey](#)
- [genRSAKeyPair](#)
- [genDSAKeyPair](#)
- [genECCKeyPair](#)
- [setAttribute](#)

## 使用 KMU 取得 AWS CloudHSM 金鑰屬性

使用 AWS CloudHSM `key_mgmt_util` 中的 `getAttribute` 命令，將 AWS CloudHSM 金鑰的一或多個屬性值寫入檔案。如果您所指定金鑰類型的屬性不存在 (例如 AES 金鑰的模數)，則 `getAttribute` 會傳回錯誤。

金鑰屬性是金鑰的屬性。其中包括特性 (例如金鑰類型、類別、標籤和 ID)，以及代表您可對金鑰執行之動作的值 (例如加密、解密、包裝、取消包裝和驗證)。

您只可以對您擁有的金鑰和與您共用的金鑰使用 `getAttribute`。您可以執行此命令或 `cloudhsm_mgmt_util` 中的 [getAttribute](#) 命令，如此可從叢集中的所有 HSM 取得金鑰的一個屬性值，並將其寫入 `stdout` 或檔案。

若要取得屬性的清單和代表它們的常數，請使用 [listAttributes](#) 命令。若要變更現有金鑰的屬性值，請使用 `key_mgmt_util` 中的 [setAttribute](#) 和 `cloudhsm_mgmt_util` 中的 [setAttribute](#)。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
getAttribute -h

getAttribute -o <key handle>
 -a <attribute constant>
 -out <file>
```

## 範例

這些範例示範如何使用 `getAttribute` 來取得 HSM 中金鑰的屬性。

**Example : 取得金鑰類型**

此範例會取得金鑰的類型，例如 AES、3DES 或一般金鑰或 RSA 或橢圓曲線金鑰對。

第一個命令會執行 [listAttributes](#)，它會取得金鑰屬性和代表它們的常數。輸出顯示金鑰類型的常數是 256。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

Command: **listAttributes**

Description

=====

The following are all of the possible attribute values for getAttributes.

|                          |       |
|--------------------------|-------|
| OBJ_ATTR_CLASS           | = 0   |
| OBJ_ATTR_TOKEN           | = 1   |
| OBJ_ATTR_PRIVATE         | = 2   |
| OBJ_ATTR_LABEL           | = 3   |
| OBJ_ATTR_KEY_TYPE        | = 256 |
| OBJ_ATTR_ID              | = 258 |
| OBJ_ATTR_SENSITIVE       | = 259 |
| OBJ_ATTR_ENCRYPT         | = 260 |
| OBJ_ATTR_DECRYPT         | = 261 |
| OBJ_ATTR_WRAP            | = 262 |
| OBJ_ATTR_UNWRAP          | = 263 |
| OBJ_ATTR_SIGN            | = 264 |
| OBJ_ATTR_VERIFY          | = 266 |
| OBJ_ATTR_LOCAL           | = 355 |
| OBJ_ATTR_MODULUS         | = 288 |
| OBJ_ATTR_MODULUS_BITS    | = 289 |
| OBJ_ATTR_PUBLIC_EXPONENT | = 290 |
| OBJ_ATTR_VALUE_LEN       | = 353 |
| OBJ_ATTR_EXTRACTABLE     | = 354 |
| OBJ_ATTR_KCV             | = 371 |

第二個命令會執行 `getAttribute`。它會要求金鑰控制代碼 524296 的金鑰類型 (屬性 256)，並將它寫入 `attribute.txt` 檔案。

Command: **getAttribute -o 524296 -a 256 -out attribute.txt**

Attributes dumped into attribute.txt file

最終命令會取得金鑰檔案的內容。輸出顯示金鑰類型為 0x15 或 21，它是三重 DES (3DES) 金鑰。對於類別和類型值的定義，請參閱[金鑰屬性參考](#)。

```
$ cat attribute.txt
OBJ_ATTR_KEY_TYPE
0x00000015
```

Example：取得金鑰的所有屬性

此命令會取得金鑰控制代碼 6 之金鑰的所有屬性，並將它們寫入 attr\_6 檔案。它使用 512 的屬性值，其代表所有屬性。

```
Command: getAttribute -o 6 -a 512 -out attr_6
```

```
got all attributes of size 444 attr cnt 17
Attributes dumped into attribute.txt file
```

```
Cfm3GetAttribute returned: 0x00 : HSM Return: SUCCESS>
```

此命令示範範例屬性檔案的內容與所有屬性值。在值當中，其報告該金鑰是 256 位元 AES 金鑰並具有 ID test\_01 和標籤 aes256。該金鑰可擷取且具持久性，亦即，不是僅限工作階段的金鑰。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

```
$ cat attribute.txt

OBJ_ATTR_CLASS
0x04
OBJ_ATTR_KEY_TYPE
0x15
OBJ_ATTR_TOKEN
0x01
OBJ_ATTR_PRIVATE
0x01
OBJ_ATTR_ENCRYPT
0x01
OBJ_ATTR_DECRYPT
0x01
OBJ_ATTR_WRAP
0x01
OBJ_ATTR_UNWRAP
0x01
OBJ_ATTR_SIGN
0x00
OBJ_ATTR_VERIFY
0x00
```



```
OBJ_ATTR_LOCAL
0x01
OBJ_ATTR_SENSITIVE
0x01
OBJ_ATTR_EXTRACTABLE
0x01
OBJ_ATTR_LABEL
aes256
OBJ_ATTR_ID
test_01
OBJ_ATTR_VALUE_LEN
0x00000020
OBJ_ATTR_KCV
0x1a4b31
```

## 參數

-h

顯示命令的說明。

必要：是

-o

指定目標金鑰的金鑰控制代碼。每一個命令中只能指定一個金鑰。若要取得金鑰的金鑰控制代碼，請使用 [findKey](#)。

同時，您必須擁有該指定的金鑰或與您共用該金鑰。如要尋找金鑰的使用者，請使用 [getKeyInfo](#)。

必要：是

-a

識別屬性。輸入代表屬性的常數，或輸入 512 來代表所有屬性。例如，若要取得金鑰類型，請輸入 256，這是代表 OBJ\_ATTR\_KEY\_TYPE 屬性的常數。

若要列出屬性及其常數，請使用 [listAttributes](#)。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

必要：是

-out

將輸出寫入指定的檔案。輸入檔案路徑。您不能將輸出寫入 stdout。

如果指定的檔案已存在，`getAttribute` 會覆寫檔案且不會警告。

必要：是

## 相關主題

- `cloudhsm_mgmt_util` 中的 [getAttribute](#)
- [listAttributes](#)
- [setAttribute](#)
- [findKey](#)
- [金鑰屬性參考](#)

## 使用 KMU 匯出 AWS CloudHSM 金鑰以仿造 PEM 格式

使用 AWS CloudHSM `key_mgmt_util` 中的 `getCaviumPrivKey` 命令，從硬體安全模組 (HSM) 以仿造 PEM 格式匯出私有金鑰。未包含實際私有金鑰材料，而是參照 HSM 中私有金鑰的仿造 PEM 檔案，之後可以用於從您的 Web 伺服器建立至 AWS CloudHSM 的 SSL/TLS 卸載。如需詳細資訊，請參閱[使用 Tomcat 的 Linux 上的 SSL/TLS 卸載](#)，或使用[NGINX 或 Apache 的 Linux 上的 SSL/TLS 卸載](#)。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
getCaviumPrivKey -h

getCaviumPrivKey -k <private-key-handle>
 -out <fake-PEM-file>
```

## 範例

此範例顯示如何使用 `getCaviumPrivKey`，以仿造 PEM 格式匯出私有金鑰。

Example：匯出偽 PEM 檔案

此命令建立並匯出包含控制代碼 15 的仿造 PEM 版私有金鑰，並將它儲存至稱為 `cavKey.pem` 的檔案。當命令成功時，`exportPrivateKey` 會傳回成功訊息。

```
Command: getCaviumPrivKey -k 15 -out cavKey.pem
```

```
Private Key Handle is written to cavKey.pem in fake PEM format
```

```
getCaviumPrivKey returned: 0x00 : HSM Return: SUCCESS
```

## 參數

此命令會使用下列參數。

### -h

顯示命令的命令列說明。

必要：是

### -k

指定要以仿造 PEM 格式匯出之私有金鑰的金鑰控制代碼。

必要：是

### -out

指定將寫入仿造 PEM 金鑰的檔案名稱。

必要：是

## 相關主題

- [importPrivateKey](#)
- [使用 Tomcat 在 Linux 上卸載 SSL/TLS](#)
- [使用 NGINX 或 Apache 在 Linux 上卸載 SSL/TLS](#)

## 使用 AWS CloudHSM KMU 取得 HSM 分割區憑證

使用 AWS CloudHSM key\_mgmt\_util 中的 getCert 命令來擷取硬體安全模組的 (HSM) 分割區憑證，並將其儲存至 檔案。執行此命令時，請指定欲擷取的憑證類型。若要執行此操作，請使用 [參數](#) 一節所述的其中一個對應整數。若要了解該節所述各類憑證的角色，請參閱 [驗證 HSM 身分](#)。

執行任何 key\_mgmt\_util 命令之前，您必須先 [啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分 [登入](#) HSM。

## 語法

```
getCert -h

getCert -f <file-name>
 -t <certificate-type>
```

## 範例

此範例說明如何使用 `getCert` 擷取叢集的客戶根憑證，並將它儲存為檔案。

Example：擷取客戶根憑證

此命令會匯出客戶根憑證 (由整數 4 表示)，並將它儲存到名為 `userRoot.crt` 的檔案。當命令成功時，`getCert` 會傳回成功訊息。

```
Command: getCert -f userRoot.crt -s 4

Cfm3GetCert() returned 0 :HSM Return: SUCCESS
```

## 參數

此命令會使用下列參數。

### -h

顯示命令的命令列說明。

必要：是

### -f

指定要用來儲存擷取憑證的檔案名稱。

必要：是

### -s

以整數指定欲擷取的分割區憑證類型。各整數及其對應的憑證類型如下所示：

- 1：製造商根憑證
- 2：製造商硬體憑證
- 4：客戶根憑證

- 8：叢集憑證 (由客戶根憑證進行簽署)
- 16：叢集憑證 (鏈結到製造商根憑證)

必要：是

## 相關主題

- [驗證 HSM 身分](#)

## 使用 KMU 取得 AWS CloudHSM 金鑰的使用者

使用 AWS CloudHSM `key_mgmt_util` 中的 `getKeyInfo` 命令，傳回可以使用金鑰之使用者的硬體安全模組 (HSM) 使用者 IDs，包括與金鑰共用的擁有者和加密使用者 (CU)。對金鑰啟用規定人數身分驗證時，`getKeyInfo` 也會傳回必須核准使用該金鑰的加密操作的使用者數量。您只可以對您擁有的金鑰以及與您共用的金鑰執行 `getKeyInfo`。

當您對公有金鑰執行 `getKeyInfo` 時，即使 HSM 的所有使用者都可以使用該公有金鑰，`getKeyInfo` 只會傳回該金鑰擁有者。若要尋找 HSM 中使用者的 HSM 使用者 ID，請使用 [listUsers](#)。若要找出特定使用者的金鑰，請使用 [findKey](#) -u。

您擁有您建立的金鑰。您可以在建立金鑰時與其他使用者共用金鑰。之後，若要共用或取消共用現有的金鑰，請使用 `cloudhsm_mgmt_util` 中的 [shareKey](#)。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
getKeyInfo -h

getKeyInfo -k <key-handle>
```

## 範例

這些範例顯示如何使用 `getKeyInfo`，以取得金鑰使用者的相關資訊。

Example：取得對稱金鑰的使用者

此命令會取得可以對金鑰控制代碼 9 使用 AES (對稱) 金鑰的使用者。輸出顯示使用者 3 擁有該金鑰，並且已將它與使用者 4 共用。

Command: **getKeyInfo -k 9**

```
Cfm3GetKey returned: 0x00 : HSM Return: SUCCESS
```

```
Owned by user 3
```

```
also, shared to following 1 user(s):
```

```
4
```

Example：取得非對稱金鑰對的使用者

這些命令使用 `getKeyInfo`，以取得可以在 RSA (非對稱) 金鑰對中使用金鑰的使用者。公有金鑰具有金鑰控制代碼 21。私有金鑰具有金鑰控制代碼 20。

對私有金鑰 (20) 執行 `getKeyInfo` 時，它會傳回金鑰擁有者 (3) 和與其共用金鑰的加密使用者 (CU) 4 和 5。

Command: **getKeyInfo -k 20**

```
Cfm3GetKey returned: 0x00 : HSM Return: SUCCESS
```

```
Owned by user 3
```

```
also, shared to following 2 user(s):
```

```
4
```

```
5
```

對公有金鑰 (21) 執行 `getKeyInfo` 時，只會傳回金鑰擁有者 (3)。

Command: **getKeyInfo -k 21**

```
Cfm3GetKey returned: 0x00 : HSM Return: SUCCESS
```

```
Owned by user 3
```

若要確認使用者 4 可以使用該公有金鑰 (和 HSM 上的所有公有金鑰)，請使用 `-ufindKey` [的](#) 參數。

輸出示範使用者 4 可以同時使用金鑰對中的公開 (21) 與私密 (20) 金鑰。使用者 4 也可以使用它們所建立或與其共用的所有其他公開金鑰和任何私密金鑰。

```
Command: findKey -u 4
```

```
Total number of keys present 8
```

```
number of keys matched from start index 0::7
```

```
11, 12, 262159, 262161, 262162, 19, 20, 21
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS
```

Example：取得金鑰的規定人數身分驗證值 (m\_value)

此範例示範如何取得金鑰的 m\_value，也就是在規定人數中的使用者數量，這些人必須核准使用該金鑰的任何密碼編譯操作。

對金鑰啟用了仲裁身分驗證時，必須有仲裁的使用者核准使用該金鑰的任何密碼編譯操作。若要啟用規定人數驗證並設定規定人數數量，建立金鑰時請使用 -m\_value 參數。

此命令會使用 [genRSAKeyPair](#) 來建立與使用者 4 共用的 RSA 金鑰對。它使用 m\_value 參數來啟用金鑰中私有金鑰的規定人數身分驗證，並將規定人數大小設為兩個使用者。必須有足夠多的使用者，才能提供所需的核准。

輸出顯示命令建立了公有金鑰 27 和私有金鑰 28。

```
Command: genRSAKeyPair -m 2048 -e 195193 -l rsa_mofn -id rsa_mv2 -u 4 -m_value 2
```

```
Cfm3GenerateKeyPair returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3GenerateKeyPair: public key handle: 27 private key handle: 28
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

此命令使用 getKeyInfo 以取得私有金鑰使用者的相關資訊。輸出顯示使用者 3 擁有該金鑰，並且將它與使用者 4 共用。它還示範兩個使用者的規定人數必須核准使用該金鑰的每個密碼編譯操作。

```
Command: getKeyInfo -k 28
```

```
Cfm3GetKey returned: 0x00 : HSM Return: SUCCESS
```

```
Owned by user 3

also, shared to following 1 user(s):

 4
2 Users need to approve to use/manage this key
```

## 參數

-h

顯示命令的命令列說明。

必要：是

-k

指定 HSM 中某個金鑰的金鑰控制代碼。輸入您擁有或共用的金鑰的金鑰控制代碼。此為必要參數。

若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

必要：是

## 相關主題

- cloudhsm\_mgmt\_util 中的 [getKeyInfo](#)
- [listUsers](#)
- [findKey](#)
- cloudhsm\_mgmt\_util 中的 [findAllKeys](#)

## 顯示 AWS CloudHSM KMU 的說明資訊

使用 AWS CloudHSM key\_mgmt\_util 中的 help 命令，以顯示所有可用 key\_mgmt\_util 命令的相關資訊。

執行 help 前，您必須先[啟動 key\\_mgmt\\_util](#)。

## 語法

```
help
```



## 範例

此範例顯示 help 命令的輸出。

### Example

Command: **help**

Help Commands Available:

Syntax: <command> -h

| Command                          | Description                              |
|----------------------------------|------------------------------------------|
| =====                            | =====                                    |
| exit                             | Exits this application                   |
| help                             | Displays this information                |
| Configuration and Admin Commands |                                          |
| getHSMInfo                       | Gets the HSM Information                 |
| getPartitionInfo                 | Gets the Partition Information           |
| listUsers                        | Lists all users of a partition           |
| loginStatus                      | Gets the Login Information               |
| loginHSM                         | Login to the HSM                         |
| logoutHSM                        | Logout from the HSM                      |
| M of N commands                  |                                          |
| getToken                         | Initiate an MxN service and get Token    |
| delToken                         | delete Token(s)                          |
| approveToken                     | Approves an MxN service                  |
| listTokens                       | List all Tokens in the current partition |
| Key Generation Commands          |                                          |
| Asymmetric Keys:                 |                                          |
| genRSAKeyPair                    | Generates an RSA Key Pair                |
| genDSAKeyPair                    | Generates a DSA Key Pair                 |
| genECCKeyPair                    | Generates an ECC Key Pair                |
| Symmetric Keys:                  |                                          |
| genPBEKey                        | Generates a PBE DES3 key                 |
| genSymKey                        | Generates a Symmetric keys               |

## Key Import/Export Commands

|                               |                                                      |
|-------------------------------|------------------------------------------------------|
| <code>createPublicKey</code>  | Creates an RSA public key                            |
| <code>importPubKey</code>     | Imports RSA/DSA/EC Public key                        |
| <code>exportPubKey</code>     | Exports RSA/DSA/EC Public key                        |
| <code>importPrivateKey</code> | Imports RSA/DSA/EC private key                       |
| <code>exportPrivateKey</code> | Exports RSA/DSA/EC private key                       |
| <code>imSymKey</code>         | Imports a Symmetric key                              |
| <code>exSymKey</code>         | Exports a Symmetric key                              |
| <code>wrapKey</code>          | Wraps a key from from HSM using the specified handle |
| <code>unwrapKey</code>        | UnWraps a key into HSM using the specified handle    |

## Key Management Commands

|                            |                                          |
|----------------------------|------------------------------------------|
| <code>deleteKey</code>     | Delete Key                               |
| <code>setAttribute</code>  | Sets an attribute of an object           |
| <code>getKeyInfo</code>    | Get Key Info about shared users/sessions |
| <code>findKey</code>       | Find Key                                 |
| <code>findSingleKey</code> | Find single Key                          |
| <code>getAttribute</code>  | Reads an attribute from an object        |

## Certificate Setup Commands

|                      |                                           |
|----------------------|-------------------------------------------|
| <code>getCert</code> | Gets Partition Certificates stored on HSM |
|----------------------|-------------------------------------------|

## Key Transfer Commands

|                                  |                          |
|----------------------------------|--------------------------|
| <code>insertMaskedObject</code>  | Inserts a masked object  |
| <code>extractMaskedObject</code> | Extracts a masked object |

## Management Crypto Commands

|                            |                           |
|----------------------------|---------------------------|
| <code>sign</code>          | Generates a signature     |
| <code>verify</code>        | Verifies a signature      |
| <code>aesWrapUnwrap</code> | Does NIST AES Wrap/Unwrap |

## Helper Commands

|                                                 |                                                                |
|-------------------------------------------------|----------------------------------------------------------------|
| <code>Error2String</code>                       | Converts Error codes to Strings                                |
| <code>save key handle in fake PEM format</code> |                                                                |
| <code>getCaviumPrivKey</code>                   | Saves an RSA private key handle in fake PEM format             |
| <code>IsValidKeyHandlefile</code>               | Checks if private key file has an HSM key handle or a real key |
| <code>listAttributes</code>                     | List all attributes for getAttributes                          |
| <code>listECCCurveIds</code>                    | List HSM supported ECC CurveIds                                |

## 參數

此命令沒有任何參數。

## 相關主題

- [loginHSM 和 logoutHSM](#)

## 使用 AWS CloudHSM KMU 匯入私有金鑰

使用 AWS CloudHSM `key_mgmt_util` 中的 `importPrivateKey` 命令，將非對稱私有金鑰從檔案匯入硬體安全模組 (HSM)。HSM 不允許以純文字形式直接匯入金鑰。此命令會使用您指定的 AES 包裝金鑰來加密私有金鑰，並在 HSM 內將該金鑰取消包裝。如果您嘗試將 AWS CloudHSM 金鑰與憑證建立關聯，請參閱[本主題](#)。

### Note

您無法使用對稱或私有金鑰匯入受密碼保護的 PEM 金鑰。

您須指定具有 `OBJ_ATTR_UNWRAP` 和 `OBJ_ATTR_ENCRYPT` 屬性值 1 的 AES 包裝金鑰。若要尋找金鑰的屬性，請使用 [getAttribute](#) 命令。

### Note

此命令不提供將匯入金鑰標記為不可匯出的選項。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
importPrivateKey -h

importPrivateKey -l <label>
 -f <key-file>
 -w <wrapping-key-handle>
 [-sess]
 [-id <key-id>]
 [-m_value <0...8>]
 [min_srv <minimum-number-of-servers>]
 [-timeout <number-of-seconds>]
 [-u <user-ids>]
```

```
[-wk <wrapping-key-file>]
[-attest]
```

## 範例

此範例顯示如何使用 `importPrivateKey` 將私有金鑰匯入 HSM。

### Example：匯入私有金鑰

此命令會從名為 `rsa2048.key` 且包含標籤 `rsa2048-imported` 的檔案，以及包含控制代碼 524299 的包裝金鑰，匯入私有金鑰。命令成功時，`importPrivateKey` 會傳回已匯入金鑰的金鑰控制代碼和成功訊息。

```
Command: importPrivateKey -f rsa2048.key -l rsa2048-imported -w 524299
```

```
BER encoded key length is 1216
```

```
Cfm3WrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3CreateUnwrapTemplate returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Private Key Unwrapped. Key Handle: 524301
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

## 參數

此命令會使用下列參數。

### -h

顯示命令的命令列說明。

必要：是

### -l

指定使用者定義的私有金鑰標籤。

必要：是

## **-f**

指定要匯入之金鑰的檔案名稱。

必要：是

## **-w**

指定包裝金鑰的金鑰控制代碼。此為必要參數。若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

若要判斷金鑰是否可以做為包裝金鑰使用，請使用 [getAttribute](#) 取得 OBJ\_ATTR\_WRAP 屬性 (262) 的值。若要建立包裝金鑰，請使用 [genSymKey](#) 建立 AES 金鑰 (類型 31)。

如果您使用 -wk 參數來指定外部的取消包裝金鑰，則在匯入期間會使用 -w 包裝金鑰來進行包裝，但不會用來取消包裝。

必要：是

## **-sess**

將已匯入金鑰指定為工作階段金鑰。

預設：匯入的金鑰在叢集中保留為持久性 (符記) 金鑰。

必要：否

## **-id**

指定要匯入之金鑰的 ID。

預設：無 ID 值。

必要：否

## **-m\_value**

指定必須核准使用匯入金鑰之密碼編譯操作的使用者數量。輸入從 **0** 到 **8** 的值。

只有當命令中的 -u 參數與足夠的使用者共享金鑰以符合 m\_value 要求，此參數才有效。

預設：0

必要：否

**-min\_srv**

指定在 `-timeout` 參數值過期之前同步匯入金鑰所需的 HSM 數量下限。如果未在規定時間內同步至指定數量的伺服器，金鑰就不會建立。

AWS CloudHSM 會自動將每個金鑰同步到叢集中的每個 HSM。要加速流程，請將 `min_srv` 值設定為少於叢集中之 HSM 的數量，並設定低逾時值。然而，請注意有些請求可能不會產生金鑰。

預設：1

必要：否

**-timeout**

指定當加入 `min-serv` 參數時要等待金鑰在 HSM 之間同步的秒數。如果未指定秒數，將持續輪詢下去。

預設：無限制

必要：否

**-u**

指定要分享匯入之私有金鑰的使用者清單。此參數授與其他 HSM 密碼使用者 (CU) 在密碼編譯操作中使用匯入金鑰的許可。

輸入 HSM 使用者 ID 清單並以逗號分隔，例如 `-u 5,6`。請勿包含現行使用者的 HSM 使用者 ID。若要找出 HSM 上 CU 的 HSM 使用者 ID，請使用 [listUsers](#)。

預設：只有現行使用者能夠使用匯入的金鑰。

必要：否

**-wk**

指定用於將匯入之金鑰包裝的金鑰。輸入包含純文字 AES 金鑰的檔案路徑和名稱。

當您加入此參數時，`importPrivateKey` 會使用 `-wk` 檔案中的金鑰來包裝匯入的金鑰。它也會使用 `-w` 參數指定的金鑰。

預設：使用在 `-w` 參數中指定的包裝金鑰來進行包裝和取消包裝。

必要：否

**-attest**

請對韌體回應進行證明檢查，以確保上面有叢集執行的韌體並未遭到盜用。

必要：否

## 相關主題

- [wrapKey](#)
- [unwrapKey](#)
- [genSymKey](#)
- [exportPrivateKey](#)

## 使用 AWS CloudHSM KMU 匯入公有金鑰

使用 AWS CloudHSM `key_mgmt_util` 中的 `importPubKey` 命令，將 PEM 格式公有金鑰匯入硬體安全模組 (HSM)。您可以使用此命令匯入在 HSM 之外產生的公有金鑰。您也可以使用此命令匯入之前從 HSM 匯出的金鑰，例如使用 [exportPubKey](#) 命令匯出的金鑰。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
importPubKey -h

importPubKey -l <label>
 -f <key-file>
 [-sess]
 [-id <key-id>]
 [min_srv <minimum-number-of-servers>]
 [-timeout <number-of-seconds>]
```

## 範例

此範例顯示如何使用 `importPubKey` 將公有金鑰匯入 HSM。

### Example：匯入公有金鑰

此命令從名為 `public.pem` 且包含標籤 `importedPublicKey` 的檔案匯入公有金鑰。命令成功時，`importPubKey` 會傳回已匯入金鑰的金鑰控制代碼和成功訊息。

```
Command: importPubKey -l importedPublicKey -f public.pem
```

```
Cfm3CreatePublicKey returned: 0x00 : HSM Return: SUCCESS
```

```
Public Key Handle: 262230
```

```
Cluster Error Status
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

## 參數

此命令會使用下列參數。

### **-h**

顯示命令的命令列說明。

必要：是

### **-l**

指定使用者定義的公有金鑰標籤。

必要：是

### **-f**

指定要匯入之金鑰的檔案名稱。

必要：是

### **-sess**

將已匯入金鑰指定為工作階段金鑰。

預設：匯入的金鑰在叢集中保留為持久性 (符記) 金鑰。

必要：否

### **-id**

指定要匯入之金鑰的 ID。

預設：無 ID 值。



必要：否

### **-min\_srv**

指定在 -timeout 參數值過期之前同步匯入金鑰所需的 HSM 數量下限。如果未在規定時間內同步至指定數量的伺服器，金鑰就不會建立。

AWS CloudHSM 會自動將每個金鑰同步到叢集中的每個 HSM。要加速流程，請將 min\_srv 值設定為少於叢集中之 HSM 的數量，並設定低逾時值。然而，請注意有些請求可能不會產生金鑰。

預設：1

必要：否

### **-timeout**

指定當加入 min-serv 參數時要等待金鑰在 HSM 之間同步的秒數。如果未指定秒數，將持續輪詢下去。

預設：無限制

必要：否

### 相關主題

- [exportPubKey](#)
- [產生金鑰](#)

## 使用 AWS CloudHSM KMU 匯入純文字對稱金鑰

使用 AWS CloudHSM key\_mgmt\_util 工具中的 imSymKey 命令，將對稱金鑰的純文字副本從檔案匯入硬體安全模組 (HSM)。您可以使用此命令匯入您在 HSM 外部以任何方法產生的金鑰，以及從 HSM 匯出的金鑰，例如 [exSymKey](#) 命令寫入檔案中的金鑰。

在匯入過程中，imSymKey 會使用您選取的 AES 金鑰 (「包裝金鑰」) 來「包裝」(加密) 然後「取消包裝」(解密) 要匯入的金鑰。不過，imSymKey 僅適用於包含純文字金鑰的檔案。若要匯出和匯入已加密的金鑰，請使用 [wrapKey](#) 和 [unWrapKey](#) 命令。

此外，imSymKey 命令只匯出對稱金鑰。若要匯入公有金鑰，請使用 [importPubKey](#)。若要匯入私有金鑰，請使用 [importPrivateKey](#) 或 [wrapKey](#)。

**Note**

您無法使用對稱或私有金鑰匯入受密碼保護的 PEM 金鑰。

匯入的金鑰運作方式非常類似於 HSM 中產生的金鑰。不過，[OBJ\\_ATTR\\_LOCAL](#) 屬性的值為零，表示其不是在本機產生。當您匯入對稱金鑰時，您可以使用以下命令來共用金鑰。匯入金鑰之後，您可以在 `shareKeycloudhsm_mgmt_util` [中使用](#) 命令來共用金鑰。

```
imSymKey -l aesShared -t 31 -f kms.key -w 3296 -u 5
```

在您匯入金鑰之後，請務必標記或刪除金鑰檔案。此命令不會阻止您將相同的金鑰資料匯入許多次。結果 (具有不同金鑰控制代碼和相同金鑰資料的多個金鑰) 會難以追蹤金鑰資料的使用情形，也就很難防止超過其加密限制。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

**語法**

```
imSymKey -h

imSymKey -f <key-file>
 -w <wrapping-key-handle>
 -t <key-type>
 -l <label>
 [-id <key-ID>]
 [-sess]
 [-wk <wrapping-key-file>]
 [-attest]
 [-min_srv <minimum-number-of-servers>]
 [-timeout <number-of-seconds>]
 [-u <user-ids>]
```

**範例**

以下範例示範如何使用 `imSymKey` 將對稱金鑰匯入 HSM。

Example：匯入 AES 對稱金鑰

這個範例使用 `imSymKey` 將 AES 對稱金鑰匯入 HSM。

第一個命令使用 OpenSSL 產生隨機 256 位元 AES 對稱金鑰。此命令將金鑰儲存在 `aes256.key` 檔案中。

```
$ openssl rand -out aes256-forImport.key 32
```

第二個命令使用 `imSymKey`，將 `aes256.key` 檔案中的 AES 金鑰匯入 HSM。此命令使用金鑰 20 (HSM 中的 AES 金鑰) 作為包裝金鑰，並指定標籤為 `imported`。與 ID 不同，標籤在叢集內不需要是唯一的。`-t` (類型) 參數的值是 31，代表 AES。

輸出顯示檔案中的金鑰已包裝和取消包裝，然後匯入 HSM 中，並於其中指派金鑰控制代碼 262180。

```
Command: imSymKey -f aes256.key -w 20 -t 31 -l imported
```

```
Cfm3WrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3CreateUnwrapTemplate returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Symmetric Key Unwrapped. Key Handle: 262180
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

下一個命令使用 [getAttribute](#)，以取得新匯入之金鑰的 `OBJ_ATTR_LOCAL` 屬性 ([屬性 355](#))，並將此屬性寫入 `attr_262180` 檔案。

```
Command: getAttribute -o 262180 -a 355 -out attributes/attr_262180
```

```
Attributes dumped into attributes/attr_262180_imported file
```

```
Cfm3GetAttribute returned: 0x00 : HSM Return: SUCCESS
```

當您檢查屬性檔案時，您可以看到 `OBJ_ATTR_LOCAL` 屬性值為零，這表示在金鑰資料不是在 HSM 中產生。

```
$ cat attributes/attr_262180_local
```

```
OBJ_ATTR_LOCAL
```

```
0x00000000
```

### Example：在叢集之間移動對稱金鑰

此範例說明如何使用 [exSymKey](#) 和 `imSymKey`，在叢集之間移動純文字 AES 金鑰。您可以使用像這樣的程序來建立 AES 包裝，而此 AES 包裝同時存在於兩個叢集的 HSM 上。當共用包裝金鑰備妥後，您就可以使用 [wrapKey](#) 和 [unWrapKey](#)，在叢集之間移動已加密的金鑰。

執行此操作的 CU 使用者必須有許可，而能夠登入兩個叢集上的 HSM。

第一個命令使用 [exSymKey](#)，從叢集 1 將金鑰 14 (32 位元 AES 金鑰) 匯出到 `aes.key` 檔案。此命令使用金鑰 6 (叢集 1 的 HSM 上的 AES 金鑰) 作為包裝金鑰。

```
Command: exSymKey -k 14 -w 6 -out aes.key
```

```
Cfm3WrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
Wrapped Symmetric Key written to file "aes.key"
```

接著，使用者在叢集 2 登入 `key_mgmt_util`，並執行 `imSymKey` 命令，將 `aes.key` 檔案中的金鑰匯入叢集 2 的 HSM。此命令使用金鑰 252152 (叢集 2 的 HSM 上的 AES 金鑰) 作為包裝金鑰。

由於 [exSymKey](#) 和 `imSymKey` 使用的包裝金鑰會包裝目標金鑰，並立即取消包裝，所以不同叢集上的包裝金鑰不需要相同。

輸出顯示金鑰已成功匯入叢集 2，且指派的金鑰控制代碼為 21。

```
Command: imSymKey -f aes.key -w 262152 -t 31 -l xcluster
```

```
Cfm3WrapHostKey returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3CreateUnwrapTemplate returned: 0x00 : HSM Return: SUCCESS
```

```
Cfm3UnWrapKey returned: 0x00 : HSM Return: SUCCESS
```

```
Symmetric Key Unwrapped. Key Handle: 21
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

若要證明叢集 1 的金鑰 14 和叢集 2 的金鑰 21 有相同的金鑰資料，請取得每個金鑰的金鑰檢查值 (KCV)。如果 KCV 值相同，即表示金鑰資料相同。

以下命令在叢集 1 使用 [getAttribute](#)，將金鑰 14 的 KCV 屬性 (屬性 371) 的值寫入 attr\_14\_kcv 檔案。然後，使用 cat 命令取得 attr\_14\_kcv 檔案的內容。

```
Command: getAttribute -o 14 -a 371 -out attr_14_kcv
Attributes dumped into attr_14_kcv file

$ cat attr_14_kcv
OBJ_ATTR_KCV
0xc33cbd
```

以下類似的命令在叢集 2 使用 [getAttribute](#)，將金鑰 21 的 KCV 屬性 (屬性 371) 的值寫入 attr\_21\_kcv 檔案。然後，使用 cat 命令取得 attr\_21\_kcv 檔案的內容。

```
Command: getAttribute -o 21 -a 371 -out attr_21_kcv
Attributes dumped into attr_21_kcv file

$ cat attr_21_kcv
OBJ_ATTR_KCV
0xc33cbd
```

輸出顯示兩個金鑰的 KCV 值相同，這證明金鑰資料相同。

由於相同的金鑰資料同時存在於兩個叢集的 HSM 中，您現在可以在叢集之間共用加密的金鑰，而完全不需要公有純文字金鑰。例如，您可以對包裝金鑰 14 使用 wrapKey 命令，從叢集 1 匯出加密的金鑰，然後對包裝金鑰 21 使用 unwrapKey，將加密的金鑰匯入叢集 2。

#### Example：匯入工作階段金鑰

此命令使用 imSymKey 的 -sess 參數，以匯入只在目前工作階段中有效的 192 位元三重 DES 金鑰。

此命令使用 -f 參數來指定包含要匯入之金鑰的檔案、使用 -t 參數來指定金鑰類型，以及使用 -w 參數來指定包裝金鑰。此命令使用 -l 參數來指定金鑰的分類標籤，也使用 -id 參數來建立金鑰的易記 (且唯一的) 識別符。另外還使用 -attest 參數來驗證用於匯入金鑰的韌體。

輸出顯示金鑰已成功包裝和取消包裝、已匯入 HSM 中，且指派的金鑰控制代碼為 37。此外，也已通過證實檢查，表示韌體未被篡改。

```
Command: imSymKey -f 3des192.key -w 6 -t 21 -l temp -id test01 -sess -attest
```

```

Cfm3WrapHostKey returned: 0x00 : HSM Return: SUCCESS

Cfm3CreateUnwrapTemplate returned: 0x00 : HSM Return: SUCCESS

Cfm3UnWrapKey returned: 0x00 : HSM Return: SUCCESS

Symmetric Key Unwrapped. Key Handle: 37

Attestation Check : [PASS]

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS

```

接著，您可以使用 [getAttribute](#) 或 [findKey](#) 命令，以驗證新匯入之金鑰的屬性。以下命令使用 `findKey`，以驗證金鑰 37 具有命令所指定的類型、標籤和 ID，而且是工作階段金鑰。如輸出的第 5 行所示，`findKey` 報告唯一符合所有屬性的金鑰是金鑰 37。

```

Command: findKey -t 21 -l temp -id test01 -sess 1
Total number of keys present 1

 number of keys matched from start index 0::0
37

Cluster Error Status
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS

Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS

```

## 參數

### -attest

執行完整性檢查，以驗證執行叢集的韌體未被篡改。

預設：無認證檢查。

必要：否

### -f

指定檔案，其中包含要匯入的金鑰。

這個檔案必須包含具有指定長度之 AES 或三重 DES 金鑰的純文字副本。RC4 和 DES 金鑰不適用於 FIPS 模式的 HSM。

- AES：16、24 或 32 位元組
- 三重 DES (3DES)：24 位元組

必要：是

-h

顯示命令的說明。

必要：是

-id

指使用者定義的金鑰識別符。輸入叢集中唯一的字串。預設為空字串。

預設：無 ID 值。

必要：否

-l

指使用者定義的金鑰對標籤。輸入一個字串。

您可以使用任何可以幫助您識別金鑰的片語。標籤不具唯一性，因此您可使用標籤將金鑰進行分組和分類。

必要：是

-min\_srv

指在 -timeout 參數值過期之前同步金鑰所需的 HSM 數量下限。如果未在規定時間內同步至指定數量的伺服器，金鑰就不會建立。

AWS CloudHSM 會自動將每個金鑰同步到叢集中的每個 HSM。要加速流程，請將 min\_srv 值設定為少於叢集中之 HSM 的數量，並設定低逾時值。然而，請注意有些請求可能不會產生金鑰。

預設：1

必要：否

-sess

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

若要將工作階段金鑰更改為持久性 (權杖) 金鑰，請使用 [setAttribute](#)。

預設：此金鑰是持久性金鑰。

必要：否

-timeout

指命令等待金鑰同步到 min\_srv 參數指定數目的 HSM 的時長 (以秒為單位)。

此參數只有在命令中同時使用 min\_srv 參數時才有效。

預設：無逾時。該命令會無限期等待，並且僅在將金鑰同步到最小數目的伺服器時才返回。

必要：否

-t

指對稱金鑰的類型。輸入代表金鑰類型的常數。例如，若要建立 AES 金鑰，請輸入 -t 31。

有效值：

- 21：[三重 DES \(3DES\)](#)。
- 31：[AES](#)

必要：是

-u

將您匯入的金鑰共用給指定的使用者。此參數授與其他 HSM 密碼使用者 (CU) 在密碼編譯操作中使用此金鑰的許可。

輸入一個 ID，或以逗號分隔的 HSM 使用者 ID 清單，例如 -u 5,6。請勿包含現行使用者的 HSM 使用者 ID。若要尋找 ID，您可以在 cloudhsm\_mgmt\_util 命令列工具中使用 [listUsers](#) 命令，或在 key\_mgmt\_util 命令列工具中使用 [listUsers](#) 命令。

必要：否

-w

指定包裝金鑰的金鑰控制代碼。此為必要參數。若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

包裝金鑰是 HSM 中的金鑰，用於匯入過程中加密 (包裝) 然後解密 (取消包裝) 金鑰。只有 AES 金鑰可以做為包裝金鑰。



您可以使用任何 AES 金鑰 (任何大小) 做為包裝金鑰。因為包裝金鑰將目標金鑰包裝後又立即取消包裝，您可以使用僅限工作階段的 AES 金鑰做為包裝金鑰。若要判斷金鑰是否可作為包裝金鑰，請使用 [getAttribute](#) 以取得 OBJ\_ATTR\_WRAP 屬性 (262) 的值。要建立包裝金鑰，請使用 [genSymKey](#) 以建立 AES 金鑰 (輸入 31)。

如果您使用 `-wk` 參數來指定外部包裝金鑰，則會使用 `-w` 包裝金鑰來取消包裝 (而不是包裝) 要匯入的金鑰。

**Note**

金鑰 4 是不支援的內部金鑰。建議您使用您所建立並做為包裝金鑰管理的 AES 金鑰。

必要：是

`-wk`

使用指定檔案中的 AES 金鑰來包裝要匯入的金鑰。輸入包含純文字 AES 金鑰的檔案路徑和名稱。

當您加入此參數時，`imSymKey` 會使用 `-wk` 檔案中的金鑰來包裝要匯入的金鑰，並使用由 `-w` 參數在 HSM 中指定的金鑰來取消包裝此金鑰。`-w` 和 `-wk` 參數值必須解析為相同的純文字金鑰。

預設：使用 HSM 上的包裝金鑰來取消包裝。

必要：否

## 相關主題

- [genSymKey](#)
- [exSymKey](#)
- [wrapKey](#)
- [unWrapKey](#)
- [exportPrivateKey](#)
- [exportPubKey](#)

## 使用 AWS CloudHSM KMU 插入遮罩物件

使用 AWS CloudHSM `key_mgmt_util` 中的 `insertMaskedObject` 命令，將遮罩的物件從檔案插入指定的硬體安全模組 (HSM)。遮罩物件是使用 [extractMaskedObject](#) 命令從 HSM 擷取的複製物件。它們僅可

在插回原先的叢集後使用。您僅能將遮罩物件插入之前從中產生的相同叢集，或該叢集的複製品。這包括透過[複製跨區域備份](#)和[使用該備份建立新叢集](#)而產生之原始叢集的任何複製版本。

遮罩物件是卸載及同步金鑰的有效方式，包括無法擷取的金鑰 (即：具有 0 的 [OBJ\\_ATTR\\_EXTRACTABLE](#) 值的金鑰)。如此一來，金鑰就可以在不同區域的相關叢集之間安全地同步，而不需要更新 AWS CloudHSM [組態檔案](#)。

執行任何 key\_mgmt\_util 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
insertMaskedObject -h

insertMaskedObject -f <filename>
 [-min_srv <minimum-number-of-servers>]
 [-timeout <number-of-seconds>]
```

## 範例

此範例顯示如何使用 insertMaskedObject 將遮罩物件檔案插入 HSM。

Example：插入遮罩物件

此命令會從名為 maskedObj 的檔案將遮罩物件插入 HSM。命令成功時，insertMaskedObject 會傳回從遮罩物件解密之金鑰的金鑰控制代碼，以及成功訊息。

```
Command: insertMaskedObject -f maskedObj

Cfm3InsertMaskedObject returned: 0x00 : HSM Return: SUCCESS
 New Key Handle: 262433

Cluster Error Status
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

## 參數

此命令會使用下列參數。

**-h**

顯示命令的命令列說明。

必要：是

**-f**

指定要插入之遮罩物件的檔案名稱。

必要：是

**-min\_srv**

指定在 `-timeout` 參數值過期之前同步所插入遮罩物件所需的伺服器數量下限。如果未在規定時間內同步至指定數量的伺服器，物件就不會插入。

預設：1

必要：否

**-timeout**

指定當加入 `min-serv` 參數時要等待金鑰在伺服器之間同步的秒數。如果未指定秒數，將持續輪詢下去。

預設：無限制

必要：否

**相關主題**

- [extractMaskedObject](#)
- [syncKey](#)
- [跨區域複製備份](#)
- [從先前的備份建立 AWS CloudHSM 叢集](#)

**使用 AWS CloudHSM KMU 驗證金鑰檔案**

使用 AWS CloudHSM `key_mgmt_util` 中的 `IsValidKeyHandlefile` 命令，來了解金鑰檔案是否包含真正的私有金鑰或仿造 RSA PEM 金鑰。仿造 PEM 檔案不含實際的私有金鑰材料，而是參照 HSM 中的私有金鑰。諸如此類的檔案可以用於從您的 Web 伺服器建立至 AWS CloudHSM 的 SSL/TLS 卸載。如需

詳細資訊，請參閱[使用 Tomcat 的 Linux 上的 SSL/TLS 卸載](#)，或使用 [NGINX 或 Apache 的 Linux 上的 SSL/TLS 卸載](#)。

 Note

IsValidKeyHandlefile 僅適用於 RSA 金鑰。

執行任何 key\_mgmt\_util 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
IsValidKeyHandlefile -h

IsValidKeyHandlefile -f <rsa-private-key-file>
```

## 範例

這些範例顯示如何使用 IsValidKeyHandlefile 判斷指定的金鑰檔案是否包含真實的金鑰材料或仿造的 PEM 金鑰材料。

### Example：驗證真實的私有金鑰

此命令確認稱為 privateKey.pem 的檔案包含真實的金鑰材料。

```
Command: IsValidKeyHandlefile -f privateKey.pem

Input key file has real private key
```

### Example：驗證仿造的 PEM 金鑰

此命令確認稱為 caviumKey.pem 的檔案包含以金鑰控制代碼 15 製作的仿造 PEM 金鑰材料。

```
Command: IsValidKeyHandlefile -f caviumKey.pem

Input file has invalid key handle: 15
```

## 參數

此命令會使用下列參數。

## -h

顯示命令的命令列說明。

必要：是

## -f

指定要檢查有效金鑰材料的 RSA 私有金鑰檔案。

必要：是

## 相關主題

- [getCaviumPrivKey](#)
- [使用 Tomcat 在 Linux 上卸載 SSL/TLS](#)
- [使用 NGINX 或 Apache 在 Linux 上卸載 SSL/TLS](#)

## 使用 KMU 列出 AWS CloudHSM 金鑰的屬性

使用 AWS CloudHSM key\_mgmt\_util 中的 listAttributes 命令來列出 AWS CloudHSM 金鑰的屬性以及代表它們的常數。您可以使用這些常數來識別 [getAttribute](#) 和 [setAttribute](#) 命令中的屬性。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

執行任何 key\_mgmt\_util 命令之前，您必須先[啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

此命令沒有任何參數。

```
listAttributes
```

## 範例

此命令可列出您在 key\_mgmt\_util 中可取得和變更的金鑰屬性，以及代表這些屬性的常數。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

若要表示 key\_mgmt\_util 中 [getAttribute](#) 命令中所有屬性，請使用 512。

```
Command: listAttributes
```

Following are the possible attribute values for `getAttributes`:

|                                       |                    |
|---------------------------------------|--------------------|
| <code>OBJ_ATTR_CLASS</code>           | <code>= 0</code>   |
| <code>OBJ_ATTR_TOKEN</code>           | <code>= 1</code>   |
| <code>OBJ_ATTR_PRIVATE</code>         | <code>= 2</code>   |
| <code>OBJ_ATTR_LABEL</code>           | <code>= 3</code>   |
| <code>OBJ_ATTR_KEY_TYPE</code>        | <code>= 256</code> |
| <code>OBJ_ATTR_ENCRYPT</code>         | <code>= 260</code> |
| <code>OBJ_ATTR_DECRYPT</code>         | <code>= 261</code> |
| <code>OBJ_ATTR_WRAP</code>            | <code>= 262</code> |
| <code>OBJ_ATTR_UNWRAP</code>          | <code>= 263</code> |
| <code>OBJ_ATTR_SIGN</code>            | <code>= 264</code> |
| <code>OBJ_ATTR_VERIFY</code>          | <code>= 266</code> |
| <code>OBJ_ATTR_LOCAL</code>           | <code>= 355</code> |
| <code>OBJ_ATTR_MODULUS</code>         | <code>= 288</code> |
| <code>OBJ_ATTR_MODULUS_BITS</code>    | <code>= 289</code> |
| <code>OBJ_ATTR_PUBLIC_EXPONENT</code> | <code>= 290</code> |
| <code>OBJ_ATTR_VALUE_LEN</code>       | <code>= 353</code> |
| <code>OBJ_ATTR_EXTRACTABLE</code>     | <code>= 354</code> |
| <code>OBJ_ATTR_KCV</code>             | <code>= 371</code> |

## 相關主題

- `cloudhsm_mgmt_util` 中的 [listAttributes](#)
- [getAttribute](#)
- [setAttribute](#)
- [金鑰屬性參考](#)

## 列出使用 KMU 的 AWS CloudHSM 所有使用者

使用 AWS CloudHSM `key_mgmt_util` 中的 `listUsers` 命令，取得硬體安全模組 (HSM) 中的使用者，以及其使用者類型和其他屬性。

在 `key_mgmt_util` 中，`listUsers` 會傳回輸出，其代表叢集內的所有 HSM (即使不一致)。若要取得每個 HSM 中之使用者的相關資訊，請使用 `cloudhsm_mgmt_util` 中的 [listUsers](#) 命令。

`key_mgmt_util` 中的使用者命令、`listUsers` 和 [getKeyInfo](#) 是唯讀命令，加密使用者 (CU) 有權執行該命令。剩餘的使用者管理命令是 `cloudhsm_mgmt_util` 的一部分。由具有使用者管理許可的加密主管 (CO) 執行。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入 HSM](#)。

## 語法

```
listUsers

listUsers -h
```

## 範例

此命令列出叢集內的 HSM 使用者及其屬性。您可以在其他命令中 (例如 [findKey](#)、[getAttribut](#) 和 [getKeyInfo](#)) 使用 User ID 屬性來識別使用者。

Command: `listUsers`

Number Of Users found 4

| Index | User ID | User Type | User Name | MofnPubKey |
|-------|---------|-----------|-----------|------------|
| 0     | 1       | PCO       | admin     | NO         |
| 0     | 2       | AU        | app_user  | NO         |
| 0     | 3       | CU        | alice     | YES        |
| 0     | 4       | CU        | bob       | NO         |
| 0     | 5       | CU        | trent     | YES        |

Cfm3ListUsers returned: 0x00 : HSM Return: SUCCESS

輸出包含下列使用者屬性：

- 使用者 ID：在 `key_mgmt_util` 和 [cloudhsm\\_mgmt\\_util](#) 命令中識別使用者。
- [使用者類型](#)：決定使用者在 HSM 上可執行的操作。
- 使用者名稱：顯示使用者定義的使用者易記名稱。
- MofnPubKey：指出使用者是否已註冊金鑰對來簽署[仲裁身分驗證權杖](#)。
- LoginFailureCnt：表示使用者登入失敗的次數。

- 2FA：指出使用者已啟用多重要素驗證。

## 參數

-h

顯示命令的說明。

必要：是

## 相關主題

- cloudhsm\_mgmt\_util 中的 [listUsers](#)
- [findKey](#)
- [getAttribute](#)
- [getKeyInfo](#)

## 使用 AWS CloudHSM KMU 登入和登出 HSM

使用 key\_mgmt\_util 中的 AWS CloudHSM loginHSM 和 logoutHSM 命令來登入和登出叢集中的硬體安全模組 (HSM)。登入 HSM 後，您即可使用 key\_mgmt\_util 執行各式各樣的金鑰管理操作，包括公有和私有金鑰產生、同步處理和包裝。

執行任何 key\_mgmt\_util 命令前，您必須先[啟動 key\\_mgmt\\_util](#)。為使用 key\_mgmt\_util 管理金鑰，您必須以[加密使用者 \(CU\)](#) 的身分登入 HSM。

### Note

如果您錯誤登入超過 5 次，系統將鎖定您的帳戶。如果您在 2018 年 2 月前建立叢集，則系統將在您 20 次錯誤登入後鎖定您的帳戶。若要解除鎖定帳戶，加密管理員 (CO) 必須在 cloudhsm\_mgmt\_util 中使用 [changePswd](#) 命令來重設您的密碼。

如果您在叢集中有多個 HSM，系統將允許您再嘗試登入幾次，若均登入錯誤，系統才會鎖定您的帳戶。這是因為 CloudHSM 用戶端可平衡各個 HSM 之間的負載。因此，每次登入嘗試可能會在不同的 HSM 上開始。如果您正在測試此功能，建議您在只有一個作用中 HSM 的叢集上執行此操作。



## 語法

```
loginHSM -h

loginHSM -u <user type>
 { -p | -hpswd } <password>
 -s <username>
```

## 範例

此範例顯示如何使用 loginHSM 和 logoutHSM 命令登入和登出叢集內的 HSM。

### Example：登入 HSM

此命令以使用者名稱為 example\_user 和密碼為 aws 的加密使用者 (CU) 身分，登入 HSM。輸出顯示您已登入叢集中的所有 HSM。

```
Command: loginHSM -u CU -s example_user -p aws

Cfm3LoginHSM returned: 0x00 : HSM Return: SUCCESS

Cluster Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

### Example：使用隱藏密碼登入

此命令與以上範例相同，只不過這次您指定系統應該隱藏密碼。

```
Command: loginHSM -u CU -s example_user -hpswd
```

系統會提示您輸入密碼。您輸入密碼時後，系統會隱藏密碼，並且輸出會顯示您已成功執行此命令，並顯示您已連線至叢集上的所有 HSM。

```
Enter password:

Cfm3LoginHSM returned: 0x00 : HSM Return: SUCCESS

Cluster Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

Command:

Example : 登出 HSM。

此命令用於登出 HSM。輸出顯示您已登出叢集中的所有 HSM。

Command: **logoutHSM**

```
Cfm3LogoutHSM returned: 0x00 : HSM Return: SUCCESS
```

Cluster Status

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

## 參數

-h

顯示此命令的說明。

-u

指定登入使用者的類型。為使用 key\_mgmt\_util，您必須以 CU 的身分登入。

必要：是

-s

指定登入使用者名稱。

必要：是

{ -p | -hpswd }

指帶 -p 的登入密碼。輸入密碼時，密碼會以純文字顯示。如要隱藏您的密碼，請使用 -hpswd 參數代替 -p，然後按照提示進行操作。

必要：是

## 相關主題

- [exit](#)

## 使用 KMU 設定 AWS CloudHSM 金鑰的屬性

使用 AWS CloudHSM `key_mgmt_util` 中的 `setAttribute` 命令，將僅在目前工作階段中有效的金鑰轉換為持久性金鑰，直到您將其刪除為止。在作法上，此命令將金鑰的字符屬性值 (`OBJ_ATTR_TOKEN`) 從 `false` (0) 變更為 `true` (1)。您只能變更您自己金鑰的屬性。

您也可以使用 `cloudhsm_mgmt_util` 中的 `setAttribute` 命令，以變更標籤、包裝、取消包裝、加密和解密屬性。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

### 語法

```
setAttribute -h

setAttribute -o <object handle>
 -a 1
```

### 範例

此範例示範如何將工作階段金鑰轉換為持久性金鑰。

第一個命令使用 [genSymKey](#) 的 `-sess` 參數，以建立只在目前工作階段中有效的 192 位元 AES 金鑰。輸出顯示新工作階段金鑰的金鑰控制代碼是 262154。

```
Command: genSymKey -t 31 -s 24 -l tmpAES -sess

Cfm3GenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS

Symmetric Key Created. Key Handle: 262154

Cluster Error Status
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

此命令使用 [findKey](#) 來尋找目前工作階段中的工作階段金鑰。輸出確認金鑰 262154 是工作階段金鑰。

```
Command: findKey -sess 1
```

```
Total number of keys present 1
```

```
number of keys matched from start index 0::0
262154
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS
```

此命令使用 `setAttribute`，以將金鑰 262154 從工作階段金鑰轉換為持久性金鑰。在作法上，此命令將金鑰的權杖屬性值 (`OBJ_ATTR_TOKEN`) 從 0 (false) 變更為 1 (true)。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

此命令使用 `-o` 參數來指定金鑰控制代碼 (262154)，並使用 `-a` 參數來指定代表字符屬性的常數 (1)。執行此命令時會提示您輸入字符屬性的值。唯一的有效值是 1 (true)，此值代表持久性金鑰。

```
Command: setAttribute -o 262154 -a 1
```

```
This attribute is defined as a boolean value.
```

```
Enter the boolean attribute value (0 or 1):1
```

```
Cfm3SetAttribute returned: 0x00 : HSM Return: SUCCESS
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

為了確認金鑰 262154 現在是持久性，此命令使用 `findKey` 來搜尋工作階段金鑰 (`-sess 1`) 和持久性金鑰 (`-sess 0`)。這一次，命令不會尋找任何工作階段金鑰，而是傳回在持久性金鑰清單中的 262154。

```
Command: findKey -sess 1
```

```
Total number of keys present 0
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS
```

```
Command: findKey -sess 0
```

```
Total number of keys present 5
```

```
number of keys matched from start index 0::4
6, 7, 524296, 9, 262154
```

```
Cluster Error Status
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS
```

## 參數

-h

顯示命令的說明。

必要：是

-o

指定目標金鑰的金鑰控制代碼。每一個命令中只能指定一個金鑰。若要取得金鑰的金鑰控制代碼，請使用 [findKey](#)。

必要：是

-a

指定常數，其代表您要變更的屬性。唯一的有效值是 1，這代表字符屬性 OBJ\_ATTR\_TOKEN。

如要取得屬性及其整數值，請使用 [listAttributes](#)。

必要：是

## 相關主題

- cloudhsm\_mgmt\_util 中的 [setAttribute](#)
- [getAttribute](#)
- [listAttributes](#)

- [金鑰屬性參考](#)

## 使用 AWS CloudHSM KMU 產生簽章

使用 AWS CloudHSM `key_mgmt_util` 中的 `sign` 命令，使用所選的私有金鑰來產生檔案的簽章。

為使用 `sign`，您必須先在 HSM 中擁有私有金鑰。您可以使用 [genSymKey](#)、[genRSAKeyPair](#) 或 [genECCKeypair](#) 命令產生私有金鑰。您也可以使用 [importPrivateKey](#) 命令匯入私有金鑰。如需關於這些金鑰的詳細資訊，請參閱[產生金鑰](#)。

`sign` 命令採用使用者指定的簽署機制 (以整數代表) 來簽署訊息檔案。如需可能的簽署機制清單，請參閱[參數](#)。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

### 語法

```
sign -h

sign -f <file name>
 -k <private key handle>
 -m <signature mechanism>
 -out <signed file name>
```

### 範例

此範例顯示如何使用 `sign` 簽署檔案。

#### Example：簽署檔案

此命令以包含控制代碼 266309 的私有金鑰簽署名為 `messageFile` 的檔案。此命令使用 SHA256\_RSA\_PKCS (1) 簽署機制，並將產生的簽署檔案另存為 `signedFile`。

```
Command: sign -f messageFile -k 266309 -m 1 -out signedFile
```

```
Cfm3Sign returned: 0x00 : HSM Return: SUCCESS
```

```
signature is written to file signedFile
```

```
Cluster Error Status
```

```
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

```
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

## 參數

此命令會使用下列參數。

### **-f**

待簽署檔案的名稱。

必要：是

### **-k**

要用於簽署之私有金鑰的控制代碼。

必要：是

### **-m**

代表用於簽署之簽署機制的整數。對應下列整數的可能機制：

| 簽署機制                | 對應整數 |
|---------------------|------|
| SHA1_RSA_PKCS       | 0    |
| SHA256_RSA_PKCS     | 1    |
| SHA384_RSA_PKCS     | 2    |
| SHA512_RSA_PKCS     | 3    |
| SHA224_RSA_PKCS     | 4    |
| SHA1_RSA_PKCS_PSS   | 5    |
| SHA256_RSA_PKCS_PSS | 6    |
| SHA384_RSA_PKCS_PSS | 7    |
| SHA512_RSA_PKCS_PSS | 8    |
| SHA224_RSA_PKCS_PSS | 9    |

| 簽署機制         | 對應整數 |
|--------------|------|
| ECDSA_SHA1   | 15   |
| ECDSA_SHA224 | 16   |
| ECDSA_SHA256 | 17   |
| ECDSA_SHA384 | 18   |
| ECDSA_SHA512 | 19   |

必要：是

### **-out**

將儲存簽署檔案的檔案名稱。

必要：是

### 相關主題

- [驗證](#)
- [importPrivateKey](#)
- [genRSAKeyPair](#)
- [genECCKeyPair](#)
- [genSymKey](#)
- [產生金鑰](#)

## 使用 KMU 取消包裝 AWS CloudHSM 金鑰

使用 AWS CloudHSM `key_mgmt_util` 工具中的 `unWrapKey` 命令，將包裝（加密）對稱或私有金鑰從檔案匯入 HSM。此命令旨在匯入由 `key_mgmt_util` 中 [wrapKey](#) 命令包裝的加密金鑰，同時也可對使用其他工具包裝的金鑰取消包裝。不過，在這些情況下，我們建議您使用 [PKCS#11](#) 或 [JCE](#) 軟體程式庫來取消包裝金鑰。

匯入的金鑰的運作方式與產生的金鑰相同 AWS CloudHSM。不過，其 [OBJ\\_ATTR\\_LOCAL](#) 屬性值為零，表示其不是在本機產生。



匯入金鑰後，請務必標示或刪除金鑰檔案。此命令不會阻止您將相同的金鑰資料匯入許多次。結果 (具有不同金鑰控制代碼和相同金鑰資料的多個金鑰) 會難以追蹤金鑰資料的使用情形，也就很難防止超過其加密限制。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入 HSM](#)。

## 語法

```
unWrapKey -h

unWrapKey -f <key-file-name>
 -w <wrapping-key-handle>
 [-sess]
 [-min_srv <minimum-number-of-HSMs>]
 [-timeout <number-of-seconds>]
 [-aad <additional authenticated data filename>]
 [-tag_size <tag size>]
 [-iv_file <IV file>]
 [-attest]
 [-m <wrapping-mechanism>]
 [-t <hash-type>]
 [-nex]
 [-u <user id list>]
 [-m_value <number of users needed for approval>]
 [-noheader]
 [-l <key-label>]
 [-id <key-id>]
 [-kt <key-type>]
 [-kc <key-class>]
 [-i <unwrapping-IV>]
```

## 範例

這些範例示範如何使用 `unWrapKey` 將檔案的包裝金鑰匯入 HSM。在第一個範例中，我們取消包裝由 [wrapKey](#) `key_mgmt_util` 命令包裝的金鑰，因此有標頭。在第二個範例中，我們取消包裝在 `key_mgmt_util` 外部包裝的金鑰，因此不會有標頭。

**Example : 取消包裝金鑰 (含標頭)**

此命令可將 3DES 對稱金鑰的包裝複本匯入 HSM。此金鑰是使用標籤為 6 的 AES 金鑰取消包裝，其加密方式與用來包裝 3DES 金鑰的金鑰相同。此輸出說明檔案中的金鑰已取消包裝並匯入，且匯入金鑰的控制代碼為 29。

```
Command: unWrapKey -f 3DES.key -w 6 -m 4

Cfm3UnWrapKey returned: 0x00 : HSM Return: SUCCESS

Key Unwrapped. Key Handle: 29

Cluster Error Status
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

**Example : 取消包裝金鑰 (無標頭)**

此命令可將 3DES 對稱金鑰的包裝複本匯入 HSM。此金鑰是使用標籤為 6 的 AES 金鑰取消包裝，其加密方式與用來包裝 3DES 金鑰的金鑰相同。由於這個 3DES 金鑰並非使用 key\_mgmt\_util 包裝，因此指定了 noheader 參數，以及其必要的相關參數：金鑰標籤 (unwrapped3DES)、金鑰類別 (4) 和金鑰類型 (21)。此輸出說明檔案中的金鑰已取消包裝並匯入，且匯入金鑰的控制代碼為 8。

```
Command: unWrapKey -f 3DES.key -w 6 -noheader -l unwrapped3DES -kc 4 -kt 21 -m 4

Cfm3CreateUnwrapTemplate2 returned: 0x00 : HSM Return: SUCCESS
Cfm2UnWrapWithTemplate3 returned: 0x00 : HSM Return: SUCCESS

Key Unwrapped. Key Handle: 8

Cluster Error Status
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
```

**參數**

-h

顯示命令的說明。

必要：是

-f

包含包裝金鑰的檔案路徑和名稱。

必要：是

-w

指定包裝金鑰。輸入 HSM 上 AES 金鑰或 RSA 金鑰的金鑰控制代碼。此為必要參數。若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

如要創建一個包裝密鑰，請使用 [genSymKey](#) 產生一個 AES 金鑰 (類型 31) 或使用 [genRSAKeyPair](#) 產生一個 RSA 金鑰對 (類型 0)。如果您使用 RSA 金鑰對，請務必使用其中一個金鑰包裝該金鑰，並使用另一個金鑰對其取消包裝。如要驗證金鑰是否可做為包裝金鑰，請使用 [getAttribute](#) 取得 OBJ\_ATTR\_WRAP 的屬性值 (以常數 262 表示)。

必要：是

-sess

建立只在目前工作階段中存在的金鑰。工作階段結束後，金鑰無法復原。

當您僅短暫需要金鑰 (例如，加密後快速解密另一個金鑰的包裝金鑰) 時，請使用此參數。請勿使用工作階段金鑰來加密工作階段結束後可能需要解密的資料。

若要將工作階段金鑰更改為持久性 (權杖) 金鑰，請使用 [setAttribute](#)。

預設：此金鑰是持久性金鑰。

必要：否

-min\_srv

指在 -timeout 參數值過期之前同步金鑰所需的 HSM 數量下限。如果未在規定時間內同步至指定數量的伺服器，金鑰就不會建立。

AWS CloudHSM 會自動將每個金鑰同步到叢集中的每個 HSM。要加速流程，請將 min\_srv 值設定為少於叢集中之 HSM 的數量，並設定低逾時值。然而，請注意有些請求可能不會產生金鑰。

預設：1

必要：否

-timeout

指命令等待金鑰同步到 min\_srv 參數指定數目的 HSM 的時長 (以秒為單位)。

此參數只有在命令中同時使用 `min_srv` 參數時才有效。

預設：無逾時。該命令會無限期等待，並且僅在將金鑰同步到最小數目的伺服器時才返回。

必要：否

#### `-attest`

執行完整性檢查，以驗證執行叢集的韌體未被篡改。

預設：無認證檢查。

必要：否

#### `-nex`

使金鑰無法擷取。產生的金鑰無法[從 HSM 匯出](#)。

預設：此金鑰可擷取。

必要：否

#### `-m`

表示包裝機制的值。CloudHSM 支援以下機制：

| Mechanism                      | Value |
|--------------------------------|-------|
| AES_KEY_WRAP_PAD_PKCS5         | 4     |
| NIST_AES_WRAP_NO_PAD           | 5     |
| NIST_AES_WRAP_PAD              | 6     |
| RSA_AES                        | 7     |
| RSA_OAEP (如需資料大小上限，請參閱本節後文的備註) | 8     |
| AES_GCM                        | 10    |
| CLOUDHSM_AES_GCM               | 11    |

| Mechanism                                                           | Value |
|---------------------------------------------------------------------|-------|
| RSA_PKCS (如需資料大小上限，請參閱本節後文的備註)。請參閱下列備註 <a href="#">1</a> 查看即將進行的變更。 | 12    |

必要：是

#### Note

使用 RSA\_OAEP 包裝機制時，您可以包裝的金鑰大小上限取決於 RSA 金鑰的模數和指定雜湊的長度，如下所示：金鑰大小上限 =  $\text{modulusLengthInBytes} - (2 * \text{hashLengthInBytes}) - 2$ 。使用 RSA\_PKCS 包裝機制時，您可以包裝的金鑰大小上限取決於 RSA 金鑰的模數，如下所示：金鑰大小上限 =  $(\text{modulusLengthInBytes} - 11)$ 。

-t

| 雜湊演算法                              | Value |
|------------------------------------|-------|
| SHA1                               | 2     |
| SHA256                             | 3     |
| SHA384                             | 4     |
| SHA512                             | 5     |
| SHA224 (對 RSA_AES 和 RSA_OAEP 機制有效) | 6     |

必要：否

-noheader

如果您的金鑰是在 key\_mgmt\_util 外部包裝，則您必須指定此參數和所有其他相關參數。

必要：否

 Note

指定此參數時，您也必須指定下列 `-noheader` 參數：

- `-l`

指定要新增到取消包裝金鑰的標籤。

必要：是

- `-kc`

指定要取消包裝的金鑰類別。以下是可接受的值：

3 = 來自公私金鑰對的私有金鑰

4 = 私密 (對稱) 金鑰

必要：是

- `-kt`

指定要取消包裝的金鑰類型。以下是可接受的值：

0 = RSA

1 = DSA

3 = ECC

16 = GENERIC\_SECRET

21 = DES3

31 = AES

必要：是

您也可以選擇指定以下 `-noheader` 參數：

- `-id`

必要：否

- -i

要使用的取消包裝初始化向量 (IV)。

必要：否

【1】根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## 相關主題

- [wrapKey](#)
- [exSymKey](#)
- [imSymKey](#)

## 使用 AWS CloudHSM KMU 驗證檔案的簽章

使用 AWS CloudHSM `key_mgmt_util` 中的 `verify` 命令來確認檔案是否已由指定的金鑰簽署。若要進行這些操作，`verify` 命令會依照來源檔案比較簽署的檔案，然後根據指定的公有金鑰和簽署機制，分析檔案是否在密碼編譯上相關。檔案可以使用 AWS CloudHSM [sign](#) 操作登入。

參數機制以列於 [參數](#) 區段中的整數代表。

執行任何 `key_mgmt_util` 命令之前，您必須先 [啟動 key\\_mgmt\\_util](#) 並以加密使用者 (CU) 的身分 [登入](#) HSM。

## 語法

```
verify -h

verify -f <message-file>
 -s <signature-file>
 -k <public-key-handle>
 -m <signature-mechanism>
```

## 範例

這些範例顯示如何使用 `verify` 來檢查特定公有金鑰是否用於簽署指定的檔案。

### Example：驗證文件簽名

此命令會嘗試驗證是否使用 SHA256\_RSA\_PKCS 簽署機制產生 hardwareCertSigned 簽署檔案，以公有金鑰 262276 簽署名為 hardwareCert.crt 的檔案。由於指定的參數代表真實的簽署關係，因此命令會傳回成功訊息。

```
Command: verify -f hardwareCert.crt -s hardwareCertSigned -k 262276 -m 1
```

```
Signature verification successful
```

```
Cfm3Verify returned: 0x00 : HSM Return: SUCCESS
```

### Example：證明 False 簽署關係

此命令驗證是否使用 SHA256\_RSA\_PKCS 簽署機制產生 userCertSigned 簽署檔案，以公有金鑰 262276 簽署名為 hardwareCert.crt 的檔案。由於指定的參數並未組成真實的簽署關係，因此命令會傳回錯誤訊息。

```
Command: verify -f hardwarecert.crt -s usercertsigned -k 262276 -m 1
```

```
Cfm3Verify returned: 0x1b
```

```
CSP Error: ERR_BAD_PKCS_DATA
```

### 參數

此命令會使用下列參數。

#### **-f**

原始訊息檔案名稱。

必要：是

#### **-s**

簽署檔案的名稱。

必要：是

#### **-k**

被視為是用來簽署檔案的公有金鑰控制代碼。



必要：是

-m

整數代表用來簽署檔案之提出的簽署機制。對應下列整數的可能機制：

| 簽署機制                | 對應整數 |
|---------------------|------|
| SHA1_RSA_PKCS       | 0    |
| SHA256_RSA_PKCS     | 1    |
| SHA384_RSA_PKCS     | 2    |
| SHA512_RSA_PKCS     | 3    |
| SHA224_RSA_PKCS     | 4    |
| SHA1_RSA_PKCS_PSS   | 5    |
| SHA256_RSA_PKCS_PSS | 6    |
| SHA384_RSA_PKCS_PSS | 7    |
| SHA512_RSA_PKCS_PSS | 8    |
| SHA224_RSA_PKCS_PSS | 9    |
| ECDSA_SHA1          | 15   |
| ECDSA_SHA224        | 16   |
| ECDSA_SHA256        | 17   |
| ECDSA_SHA384        | 18   |
| ECDSA_SHA512        | 19   |

必要：是

## 相關主題

- [sign](#)
- [getCert](#)
- [產生金鑰](#)

## 使用 KMU 匯出 AWS CloudHSM 金鑰

使用 AWS CloudHSM `key_mgmt_util` 中的 `wrapKey` 命令，將對稱或私有金鑰的加密複本從硬體安全模組 (HSM) 匯出至 檔案。執行 `wrapKey` 時，您會指定要匯出的金鑰、HSM 上用來加密 (包裝) 您要匯出之金鑰的金鑰，以及輸出檔。

`wrapKey` 命令會將加密金鑰寫入您指定的檔案，但不會從 HSM 中移除該金鑰，或阻止您在密碼編譯操作中使用該金鑰。您可以多次匯出相同的金鑰。

只有金鑰的擁有者 (也就是建立金鑰的加密使用者 (CU)) 可以匯出金鑰。共用金鑰的使用者可以在密碼編譯操作中使用它，但不能將它匯出。

若要將加密金鑰匯回 HSM，請使用 [unWrapKey](#)。若要從 HSM 匯出純文字金鑰，請視需要使用 [exSymKey](#) 或 [exportPrivateKey](#)。[aesWrapUnwrap](#) 命令無法解密 (取消包裝) `wrapKey` 所加密的金鑰。

執行任何 `key_mgmt_util` 命令之前，您必須先[啟動 `key\_mgmt\_util`](#) 並以加密使用者 (CU) 的身分[登入](#) HSM。

## 語法

```
wrapKey -h

wrapKey -k <exported-key-handle>
 -w <wrapping-key-handle>
 -out <output-file>
 [-m <wrapping-mechanism>]
 [-aad <additional authenticated data filename>]
 [-t <hash-type>]
 [-noheader]
 [-i <wrapping IV>]
 [-iv_file <IV file>]
 [-tag_size <num_tag_bytes>]
```

## 範例

### Example

此命令會將 192 位元的三重 DES (3DES) 對稱金鑰 (金鑰控制代碼 7) 匯出。它使用 HSM 中的 256 位元 AES 金鑰 (金鑰控制代碼 14) 來包裝金鑰 7。然後它會將加密的 3DES 金鑰寫入 3DES-encrypted.key 檔案。

輸出顯示金鑰 7 (3DES 金鑰) 已成功包裝並寫入指定的檔案。加密金鑰的長度為 307 個位元組。

```
Command: wrapKey -k 7 -w 14 -out 3DES-encrypted.key -m 4

Key Wrapped.

Wrapped Key written to file "3DES-encrypted.key length 307

Cfm2WrapKey returned: 0x00 : HSM Return: SUCCESS
```

## 參數

-h

顯示命令的說明。

必要：是

-k

您要匯出之金鑰的金鑰控制代碼。輸入您擁有之對稱或私有金鑰的金鑰控制代碼。若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

若要確認金鑰是否匯出，請使用 [getAttribute](#) 命令取得 OBJ\_ATTR\_EXTRACTABLE 屬性的值 (以常數 354 表示)。如需金鑰屬性的解譯說明，請參閱 [AWS CloudHSM KMU 的金鑰屬性參考](#)。

您只能匯出您擁有的金鑰。若要尋找金鑰的擁有者，請使用 [getKeyInfo](#) 命令。

必要：是

-w

指定包裝金鑰。輸入 HSM 上 AES 金鑰或 RSA 金鑰的金鑰控制代碼。此為必要參數。若要找出金鑰控制代碼，請使用 [findKey](#) 命令。

如要創建一個包裝密鑰，請使用 [genSymKey](#) 產生一個 AES 金鑰 (類型 31) 或使用 [genRSAKeyPair](#) 產生一個 RSA 金鑰對 (類型 0)。如果您使用 RSA 金鑰對，請務必使用其中一個金鑰包裝該金鑰，並使用另一個金鑰對其取消包裝。如要驗證金鑰是否可做為包裝金鑰，請使用 [getAttribute](#) 取得 OBJ\_ATTR\_WRAP 的屬性值 (以常數 262 表示)。

必要：是

-out

輸出檔案的路徑和名稱。命令成功時，這個檔案會包含匯出金鑰的加密複本。如果檔案已存在，命令會覆寫檔案且不會有任何警告。

必要：是

-m

表示包裝機制的值。CloudHSM 支援以下機制：

| Mechanism                                                           | Value |
|---------------------------------------------------------------------|-------|
| AES_KEY_WRAP_PAD_PKCS5                                              | 4     |
| NIST_AES_WRAP_NO_PAD                                                | 5     |
| NIST_AES_WRAP_PAD                                                   | 6     |
| RSA_AES                                                             | 7     |
| RSA_OAEP (如需資料大小上限，請參閱本節後文的備註)                                      | 8     |
| AES_GCM                                                             | 10    |
| CLOUDHSM_AES_GCM                                                    | 11    |
| RSA_PKCS (如需資料大小上限，請參閱本節後文的備註)。請參閱下列備註 <a href="#">1</a> 查看即將進行的變更。 | 12    |

必要：是

**Note**

使用 RSA\_OAEP 包裝機制時，您可以包裝的金鑰大小上限取決於 RSA 金鑰的模數和指定雜湊的長度，如下所示：金鑰大小上限 = (modulusLengthInBytes-2\*hashLengthInBytes-2)。  
 使用 RSA\_PKCS 包裝機制時，您可以包裝的金鑰大小上限取決於 RSA 金鑰的模數，如下所示：金鑰大小上限 = (modulusLengthInBytes -11)。

-t

表示雜湊演算法的值。CloudHSM 支援以下演算法：

| 雜湊演算法                              | Value |
|------------------------------------|-------|
| SHA1                               | 2     |
| SHA256                             | 3     |
| SHA384                             | 4     |
| SHA512                             | 5     |
| SHA224 (對 RSA_AES 和 RSA_OAEP 機制有效) | 6     |

必要：否

-aad

檔案名稱包含 AAD。

**Note**

僅對 AES\_GCM 和 CLOUDHSM\_AES\_GCM 機制有效。

必要：否

## -noheader

忽略標頭，其指定 CloudHSM 特定的[金鑰屬性](#)。僅限您要使用 key\_mgmt\_util 以外的工具來取消包裝金鑰時，才使用此參數。

必要：否

-i

初始向量 (IV) (十六進位值)。

### Note

只在使用 CLOUDHSM\_AES\_KEY\_WRAP 和 NIST\_AES\_WRAP 機制的 -noheader 參數傳遞時有效。

必要：否

-iv\_file

您要寫入回應中包含之 IV 值的檔案。

### Note

只在使用 AES\_GCM 機制的 -noheader 參數傳遞時有效。

必要：否

-tag\_size

要與包裝的 Blob 一起儲存的標籤大小。

### Note

只在使用 AES\_GCM 和 CLOUDHSM\_AES\_GCM 機制的 -noheader 參數傳遞時有效。標籤大小下限為 8。

必要：否

【1】根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## 相關主題

- [exSymKey](#)
- [imSymKey](#)
- [unWrapKey](#)

## AWS CloudHSM KMU 的金鑰屬性參考

AWS CloudHSM `key_mgmt_util` 命令使用常數來表示硬體安全模組 (HSM) 中金鑰的屬性。這個主題可協助您識別屬性、尋找在命令中代表這些屬性的常數，以及了解屬性的值。

您在建立金鑰時會設定金鑰的屬性。如要變更權杖屬性 (指明金鑰是持久性金鑰還是工作階段金鑰)，請使用 `key_mgmt_util` 中的 [setAttribute](#) 命令。如要變更標籤、包裝、取消包裝、加密和解密屬性，請使用 `cloudhsm_mgmt_util` 中的 `setAttribute` 命令。

若要取得屬性及其常數的清單，請使用 [listAttributes](#)。若要取得金鑰的屬性值，請使用 [getAttribute](#)。

下表列出金鑰屬性、其常數及其有效值。

| 屬性                        | 常數  | 值                                                             |
|---------------------------|-----|---------------------------------------------------------------|
| OBJ_ATTR_ALL              | 512 | 代表所有屬性。                                                       |
| OBJ_ATTR_ALWAYS_SENSITIVE | 357 | 0 : False。<br>1 : True。                                       |
| OBJ_ATTR_CLASS            | 0   | 2 : 公有/私有金鑰對中的公有金鑰。<br>3 : 公有/私有金鑰對中的私有金鑰。<br>4 : 私密 (對稱) 金鑰。 |
| OBJ_ATTR_DECRYPT          | 261 | 0 : False。                                                    |

| 屬性                   | 常數  | 值                                            |
|----------------------|-----|----------------------------------------------|
|                      |     | 1 : True。金鑰可用來解密資料。                          |
| OBJ_ATTR_DERIVE      | 268 | 0 : False。<br><br>1 : True。此函數將衍生金鑰。         |
| OBJ_ATTR_DESTROYABLE | 370 | 0 : False。<br><br>1 : True。                  |
| OBJ_ATTR_ENCRYPT     | 260 | 0 : False。<br><br>1 : True。金鑰可用來加密資料。        |
| OBJ_ATTR_EXTRACTABLE | 354 | 0 : False。<br><br>1 : True。可以從 HSM 匯出金鑰。     |
| OBJ_ATTR_ID          | 258 | 使用者定義的字串。在叢集內必須是唯一的。預設為空字串。                  |
| OBJ_ATTR_KCV         | 371 | 金鑰的金鑰檢查值。如需詳細資訊，請參閱 <a href="#">其他詳細資訊</a> 。 |



| 屬性                    | 常數  | 值                                                                                               |
|-----------------------|-----|-------------------------------------------------------------------------------------------------|
| OBJ_ATTR_KEY_TYPE     | 256 | 0 : RSA。<br>1 : DSA。<br>3 : EC。<br>16 : 一般機密。<br>18 : RC4。<br>21 : 三重 DES (3DES)。<br>31 : AES。  |
| OBJ_ATTR_LABEL        | 3   | 使用者定義的字串。在叢集內不必是唯一的。                                                                            |
| OBJ_ATTR_LOCAL        | 355 | 0。False。金鑰已匯入到 HSM。<br>1 : True。                                                                |
| OBJ_ATTR_MODULUS      | 288 | 用於產生 RSA 金鑰對的模數。如果是 EC 金鑰，這個值則代表以十六進位格式表示 ANSI X9.62 ECPoint 值「Q」的 DER 編碼。<br>對於其他金鑰類型，這個屬性不存在。 |
| OBJ_ATTR_MODULUS_BITS | 289 | 用於產生 RSA 金鑰對的模數長度。如果是 EC 金鑰，則代表用於產生金鑰的橢圓曲線的 ID。<br>對於其他金鑰類型，這個屬性不存在。                            |

| 屬性                             | 常數  | 值                                                                                                                     |
|--------------------------------|-----|-----------------------------------------------------------------------------------------------------------------------|
| OBJ_ATTR_NEVER_EXT<br>RACTABLE | 356 | 0 : False。<br><br>1 : True。金鑰無法從 HSM 匯出。                                                                              |
| OBJ_ATTR_PUBLIC_EX<br>PONENT   | 290 | 用於產生 RSA 金鑰對的公有指數。<br><br>對於其他金鑰類型，這個屬性不存在。                                                                           |
| OBJ_ATTR_PRIVATE               | 2   | 0 : False。<br><br>1 : True。此屬性指出未經授權的使用者可以索引鍵屬性。由於 CloudHSM PKCS # 11 供應商目前不支援公有工作階段，所有金鑰 (包括公有金鑰的公有私有金鑰對) 有此屬性設定為 1。 |
| OBJ_ATTR_SENSITIVE             | 259 | 0 : False。公有/私有金鑰對中的公有金鑰。<br><br>1 : True。                                                                            |
| OBJ_ATTR_SIGN                  | 264 | 0 : False。<br><br>1 : True。金鑰可用於簽署 (私有金鑰)。                                                                            |
| OBJ_ATTR_TOKEN                 | 1   | 0 : False。工作階段金鑰。<br><br>1 : True。持久性金鑰。                                                                              |
| OBJ_ATTR_TRUSTED               | 134 | 0 : False。<br><br>1 : True。                                                                                           |

| 屬性                         | 常數         | 值                                          |
|----------------------------|------------|--------------------------------------------|
| OBJ_ATTR_UNWRAP            | 263        | 0 : False。<br><br>1 : True。金鑰可用來解密金鑰。      |
| OBJ_ATTR_UNWRAP_TEMPLATE   | 1073742354 | 這些值應使用已套用於以此包裝金鑰取消包裝之任何金鑰的屬性範本。            |
| OBJ_ATTR_VALUE_LEN         | 353        | 金鑰長度 (以位元組為單位)。                            |
| OBJ_ATTR_VERIFY            | 266        | 0 : False。<br><br>1 : True。金鑰可用於驗證 (公有金鑰)。 |
| OBJ_ATTR_WRAP              | 262        | 0 : False。<br><br>1 : True。金鑰可用來加密金鑰。      |
| OBJ_ATTR_WRAP_TEMPLATE     | 1073742353 | 這些值應使用屬性範本來匹配使用此包裝金鑰所包裝的金鑰。                |
| OBJ_ATTR_WRAP_WITH_TRUSTED | 528        | 0 : False。<br><br>1 : True。                |

## 其他詳細資訊

### 金鑰檢查值 (kcv)

金鑰檢查值 (KCV) 是 HSM 匯入或產生金鑰時所產生之金鑰的 3 位元組雜湊或總和檢查碼。您也可以 HSM 之外計算 KCV，例如在匯出金鑰之後。然後，您可以比較 KCV 值以確認金鑰的身分和完整性。若要取得金鑰的 KCV，請使用 [getAttribute](#)。

AWS CloudHSM 使用以下標準方法產生金鑰檢查值：

- 對稱密鑰：使用金鑰加密零塊的結果的前 3 個位元組。
- 非對稱金鑰配對：公有金鑰 SHA-1 雜湊的前 3 個位元組。
- HMAC 金鑰：目前不支援 HMAC 金鑰的 KCV。

# 使用 AWS CloudHSM 用戶端 SDKs 操作

使用用戶端 SDK 將密碼編譯作業從平台或語言型應用程式卸載到硬體安全模組 (HSM)。

AWS CloudHSM 提供兩個主要版本，而用戶端 SDK 5 是最新的。與用戶端 SDK 3 (上一個系列) 相比，用戶端 SDK 5 具有多種優勢。如需詳細資訊，請參閱[用戶端 SDK 5 的優點](#)。如需關於平台支援的詳細資訊，請參閱[AWS CloudHSM 用戶端 SDK 5 支援的平台](#)。

下列主題說明如何使用 AWS CloudHSM 用戶端 SDKs。

AWS CloudHSM 支援下列元件：

## [the section called “PKCS #11 程式庫”](#)

PKCS #11 是在硬體安全模組 (HSMs) 上執行加密作業的標準。AWS CloudHSM 提供與 PKCS #11 2.40 版相容的 PKCS #11 程式庫的實作方式。

## [the section called “OpenSSL 動態引擎”](#)

AWS CloudHSM OpenSSL 動態引擎可讓您透過 OpenSSL API 將密碼編譯操作卸載至 CloudHSM 叢集。

## [the section called “JCE 提供者”](#)

AWS CloudHSM JCE 提供者符合 Java 密碼編譯架構 (JCA)。提供者可讓您在 HSM 上執行密碼編譯作業。

## [the section called “金鑰儲存提供者 \(KSP\)”](#)

適用於 Windows 的 AWS CloudHSM 用戶端包含 CNG 和 KSP 提供者。目前，只有用戶端 SDK 3 支援 CNG 和 KSP 提供者。

## 主題

- [檢查您的 AWS CloudHSM 用戶端 SDK 版本](#)
- [比較 AWS CloudHSM 用戶端 SDK 元件支援](#)
- [從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)
- [使用用戶端 SDK 5 來使用 AWS CloudHSM](#)
- [使用先前的 SDK 版本來使用 AWS CloudHSM](#)

## 檢查您的 AWS CloudHSM 用戶端 SDK 版本

使用下列命令來驗證您搭配使用的用戶端 SDK 版本 AWS CloudHSM。

### Amazon Linux

使用下列命令：

```
rpm -qa | grep ^cloudhsm
```

### Amazon Linux 2

使用下列命令：

```
rpm -qa | grep ^cloudhsm
```

### CentOS 6

使用下列命令：

```
rpm -qa | grep ^cloudhsm
```

### CentOS 7

使用下列命令：

```
rpm -qa | grep ^cloudhsm
```

### CentOS 8

使用下列命令：

```
rpm -qa | grep ^cloudhsm
```

### RHEL 6

使用下列命令：

```
rpm -qa | grep ^cloudhsm
```

## RHEL 7

使用下列命令：

```
rpm -qa | grep ^cloudhsm
```

## RHEL 8

使用下列命令：

```
rpm -qa | grep ^cloudhsm
```

## Ubuntu 16.04 LTS

使用下列命令：

```
apt list --installed | grep ^cloudhsm
```

## Ubuntu 18.04 LTS

使用下列命令：

```
apt list --installed | grep ^cloudhsm
```

## Ubuntu 20.04 LTS

使用下列命令：

```
apt list --installed | grep ^cloudhsm
```

## Windows Server

使用下列命令：

```
wmic product get name,version
```

## 比較 AWS CloudHSM 用戶端 SDK 元件支援

除了命令列工具之外，用戶端 SDK 3 還包含可從各種基於平台或語言的應用程式對 HSM 進行卸載密碼編譯操作的元件。用戶端 SDK 5 與用戶端 SDK 3 相同，但尚未支援 CNG 和 KSP 提供者。下表旨在比較用戶端 SDK 3 和用戶端 SDK 5 中的元件可用性。

| 元件                                 | 用戶端 SDK 5 | 用戶端 SDK 3 |
|------------------------------------|-----------|-----------|
| PKCS #11 程式庫                       | 是         | 是         |
| JCE 提供者                            | 是         | 是         |
| OpenSSL 動態引擎                       | 是         | 是         |
| 金鑰儲存提供者 (KSP)                      | 是         | 是         |
| CloudHSM 管理公用程式 (CMU) <sup>1</sup> | 是         | 是         |
| 金鑰管理公用程式 (KMU) <sup>1</sup>        | 是         | 是         |
| 設定工具                               | 是         | 是         |

[1] CMU 和 KMU 元件包含在 CloudHSM CLI 與用戶端 SDK 5 中。

下列各節說明元件。

## PKCS #11 程式庫

PKCS #11 是對硬體安全模組 (HSMs) 執行密碼編譯操作的標準。AWS CloudHSM 提供符合 PKCS #11 2.40 版的 PKCS #11 程式庫實作。

- 對於用戶端 SDK 3，PKCS #11 程式庫是唯一符合 Linux 基礎支援的 Linux 元件。如需詳細資訊，請參閱[the section called “Linux 支援用戶端 SDK 3”](#)。
- 對於用戶端 SDK 5，PKCS #11 程式庫是符合 Linux 和 Windows 用戶端 SDK 5 基本支援的跨平台元件。如需詳細資訊，請參閱[the section called “Linux 支援用戶端 SDK 5”](#)及[the section called “Windows 支援用戶端 SDK 5”](#)。

## CloudHSM 管理公用程式 (CMU)

CloudHSM Management Utility (CMU) 命令列工具可協助加密主管管理 HSMs 中的使用者。它包括可建立、刪除和列出使用者，以及變更使用者密碼的工具。如需詳細資訊，請參閱[AWS CloudHSM Management Utility \(CMU\)](#)。



## 金鑰管理公用程式 (KMU)

Key Management Utility (KMU) 是一種命令列工具，可協助加密使用者 (CU) 管理硬體安全模組 (HSM) 上的金鑰。如需詳細資訊，請參閱[AWS CloudHSM 金鑰管理公用程式 \(KMU\)](#)。

## JCE 提供者

AWS CloudHSM JCE 提供者符合 Java 密碼編譯架構 (JCA)。提供者可讓您在 HSM 上執行密碼編譯作業。

JCE 提供者是 Linux 唯一符合 Linux 基礎支援的元件。如需詳細資訊，請參閱[the section called “Linux 支援用戶端 SDK 3”](#)。

- 對於用戶端 SDK 3，需要 OpenJDK 1.8

## OpenSSL 動態引擎

AWS CloudHSM OpenSSL 動態引擎可讓您透過 OpenSSL API 將密碼編譯操作卸載至 CloudHSM 叢集。

- 對於用戶端 SDK 3，OpenSSL 動態引擎是 Linux 唯一不符合 Linux 基礎支援的元件。請參閱以下排除項目。
  - 需要 OpenSSL 1.0.2 [f+]

不支援的平台：

- CentOS 8
- Red Hat Enterprise Linux (RHEL) 8
- Ubuntu 18.04 LTS

這些平台隨附的 OpenSSL 版本與用戶端 SDK 3 的 OpenSSL 動態引擎不相容。AWS CloudHSM 使用適用於用戶端 SDK 5 的 OpenSSL 動態引擎支援這些平台。

- 對於用戶端 SDK 5，OpenSSL 動態引擎是僅限 Linux 的元件，需要 OpenSSL 1.0.2、1.1.1 或 3.x。

## 金鑰儲存提供者 (KSP)

金鑰儲存提供者 (KSP) 是 Microsoft Windows 作業系統特有的密碼編譯 API。

對於用戶端 SDK 3，CNG 和 KSP 提供者是符合 Windows 基礎支援的 Windows 限定元件。如需詳細資訊，請參閱[Windows 支援 AWS CloudHSM 用戶端 SDK 3](#)。

對於用戶端 SDK 5，金鑰儲存提供者 (KSP) 是符合 Windows 基礎支援的 Windows 專用元件。如需詳細資訊，請參閱[Windows 支援 AWS CloudHSM 用戶端 SDK 5](#)。

## 從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5

如需從用戶端 SDK 3 遷移至用戶端 SDK 5 的詳細說明，請參閱下列主題。

對於 CloudHSM CLI 不支援的功能或使用案例，請聯絡 [支援](#)。

- [將您的 AWS CloudHSM PKCS #11 程式庫從用戶端 SDK 3 遷移至用戶端 SDK 5](#)
- [將您的 OpenSSL 動態引擎從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)
- [將您的金鑰儲存提供者 \(KSP\) 從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)
- [將您的 JCE 供應商從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)
- [從 AWS CloudHSM 用戶端 SDK 3 CMU 和 KMU 遷移至用戶端 SDK 5 CloudHSM CLI](#)

## 將您的 AWS CloudHSM PKCS #11 程式庫從用戶端 SDK 3 遷移至用戶端 SDK 5

使用此主題將 AWS CloudHSM [PKCS #11 程式庫](#)從用戶端 SDK 3 遷移至用戶端 SDK 5。如需遷移的優勢，請參閱 [AWS CloudHSM 用戶端 SDK 5 的優點](#)。

在 中 AWS CloudHSM，客戶應用程式會使用 AWS CloudHSM 用戶端軟體開發套件 (SDK) 執行密碼編譯操作。用戶端 SDK 5 是持續新增新功能和平台支援的主要 SDK。

若要檢閱所有提供者的遷移說明，請參閱 [從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)。

### 解決重大變更以做好準備

檢閱這些重大變更，並相應地更新開發環境中的應用程式。

包裝機制已變更

| 用戶端 SDK 3 機制     | 同等用戶端 SDK 5 機制                          |
|------------------|-----------------------------------------|
| CKM_AES_KEY_WRAP | CKM_CLOUDHSM_AES_KEY_WRAP_P<br>KCS5_PAD |

| 用戶端 SDK 3 機制                        | 同等用戶端 SDK 5 機制                      |
|-------------------------------------|-------------------------------------|
| CKM_AES_KEY_WRAP_PAD                | CKM_CLOUDHSM_AES_KEY_WRAP_ZERO_PAD  |
| CKM_CLOUDHSM_AES_KEY_WRAP_PKCS5_PAD | CKM_CLOUDHSM_AES_KEY_WRAP_PKCS5_PAD |
| CKM_CLOUDHSM_AES_KEY_WRAP_NO_PAD    | CKM_CLOUDHSM_AES_KEY_WRAP_NO_PAD    |
| CKM_CLOUDHSM_AES_KEY_WRAP_ZERO_PAD  | CKM_CLOUDHSM_AES_KEY_WRAP_ZERO_PAD  |

## ECDH

在用戶端 SDK 3 中，您可以使用 ECDH 並指定 KDF。此功能目前無法在用戶端 SDK 5 中使用。如果您的應用程式需要此功能，請聯絡 [支援](#)。

金鑰控點現在是工作階段特定的

若要將金鑰控制代碼成功用於用戶端 SDK 5，您必須在每次執行應用程式時取得金鑰控制代碼。如果您有現有的應用程式會在不同的工作階段中使用相同的金鑰控制代碼，您必須修改程式碼，才能在每次執行應用程式時取得金鑰控制代碼。如需擷取金鑰控點的資訊，請參閱[此 AWS CloudHSM PKCS #11 範例](#)。此變更符合 [PKCS #11 2.40 規格](#)。

## 遷移至用戶端 SDK 5

遵循本節中的指示，從用戶端 SDK 3 遷移到用戶端 SDK 5。

### Note

用戶端 SDK 5 目前不支援 Amazon Linux、Ubuntu 16.04、Ubuntu 18.04、CentOS 6、CentOS 8 和 RHEL 6。如果您目前使用其中一個平台搭配用戶端 SDK 3，則需要在遷移至用戶端 SDK 5 時選擇不同的平台。

1. 解除安裝用戶端 SDK 3 的 PKCS #11 程式庫。

## Amazon Linux 2

```
$ sudo yum remove cloudhsm-client-pkcs11
```

## CentOS 7

```
$ sudo yum remove cloudhsm-client-pkcs11
```

## RHEL 7

```
$ sudo yum remove cloudhsm-client-pkcs11
```

## RHEL 8

```
$ sudo yum remove cloudhsm-client-pkcs11
```

## 2. 解除安裝 Client Daemon for Client SDK 3。

### Amazon Linux 2

```
$ sudo yum remove cloudhsm-client
```

### CentOS 7

```
$ sudo yum remove cloudhsm-client
```

### RHEL 7

```
$ sudo yum remove cloudhsm-client
```

### RHEL 8

```
$ sudo yum remove cloudhsm-client
```

 Note

需要再次啟用自訂組態。

3. 依照中的步驟安裝用戶端 SDK PKCS #11 程式庫[安裝 AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫](#)。
4. 用戶端 SDK 5 推出新的組態檔案格式和命令列引導工具。若要引導您的用戶端 SDK 5 PKCS #11 程式庫，請遵循下使用者指南中列出的說明[引導用戶端 SDK](#)。
5. 在您的開發環境中，測試您的應用程式。更新現有程式碼，以在最終遷移之前解決重大變更。

## 相關主題

- [的最佳實務 AWS CloudHSM](#)

## 將您的 OpenSSL 動態引擎從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5

使用此主題將您的 [OpenSSL 動態引擎](#)從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5。如需遷移的優勢，請參閱 [AWS CloudHSM 用戶端 SDK 5 的優點](#)。

在 中 AWS CloudHSM，客戶應用程式會使用 AWS CloudHSM 用戶端軟體開發套件 (SDK) 執行密碼編譯操作。用戶端 SDK 5 是持續新增新功能和平台支援的主要 SDK。

 Note

使用 OpenSSL 動態引擎的用戶端 SDK 5 目前不支援隨機數產生。

若要檢閱所有提供者的遷移說明，請參閱 [從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)。

## 遷移至用戶端 SDK 5

遵循本節中的指示，從用戶端 SDK 3 遷移到用戶端 SDK 5。

 Note

用戶端 SDK 5 目前不支援 Amazon Linux、Ubuntu 16.04、Ubuntu 18.04、CentOS 6、CentOS 8 和 RHEL 6。如果您目前使用其中一個平台搭配用戶端 SDK 3，則需要在遷移至用戶端 SDK 5 時選擇不同的平台。

## 1. 解除安裝適用於用戶端 SDK 3 的 OpenSSL 動態引擎。

### Amazon Linux 2

```
$ sudo yum remove cloudhsm-client-dyn
```

### CentOS 7

```
$ sudo yum remove cloudhsm-client-dyn
```

### RHEL 7

```
$ sudo yum remove cloudhsm-client-dyn
```

### RHEL 8

```
$ sudo yum remove cloudhsm-client-dyn
```

## 2. 解除安裝 Client Daemon for Client SDK 3。

### Amazon Linux 2

```
$ sudo yum remove cloudhsm-client
```

### CentOS 7

```
$ sudo yum remove cloudhsm-client
```

### RHEL 7

```
$ sudo yum remove cloudhsm-client
```

## RHEL 8

```
$ sudo yum remove cloudhsm-client
```

 Note

需要再次啟用自訂組態。

3. 依照中的步驟安裝用戶端 SDK OpenSSL 動態引擎[安裝適用於用戶端 SDK 5 的 AWS CloudHSM OpenSSL 動態引擎](#)。
4. 用戶端 SDK 5 推出新的組態檔案格式和命令列引導工具。若要引導您的用戶端 SDK 5 OpenSSL 動態引擎，請遵循下使用者指南中列出的說明[引導用戶端 SDK](#)。
5. 在您的開發環境中，測試您的應用程式。更新現有程式碼，以在最終遷移之前解決重大變更。

## 相關主題

- [的最佳實務 AWS CloudHSM](#)

## 將您的金鑰儲存提供者 (KSP) 從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5

本主題說明如何將[金鑰儲存提供者 \(KSP\)](#) 從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5。如需遷移優點的詳細資訊，請參閱 [AWS CloudHSM 用戶端 SDK 5 的優點](#)。

在 中 AWS CloudHSM，您可以使用 AWS CloudHSM 用戶端軟體開發套件 (SDK) 來執行密碼編譯操作。用戶端 SDK 5 是接收新功能和平台支援更新的主要 SDK。

如需所有供應商的遷移說明，請參閱 [從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)。

### 遷移至用戶端 SDK 5

1. 在 Windows Server 執行個體上安裝用戶端 SDK 5 金鑰儲存提供者 (KSP)。如需說明，請參閱[安裝 AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 \(KSP\)](#)。
2. 使用新的組態檔案格式和命令列引導工具來設定用戶端 SDK 5 金鑰儲存提供者 (KSP)。如需說明，請參閱[引導用戶端 SDK](#)。

3. AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 (KSP) 包含 SDK3 相容性模式，以支援 SDK3 中產生的金鑰參考檔案。如需詳細資訊，請參閱[適用於的金鑰儲存提供者 \(KSP\) 的 SDK3 相容性模式 AWS CloudHSM](#)。

 Note

搭配用戶端 SDK3 使用用戶端 SDK 3 產生的金鑰參考檔案時，您必須啟用 SDK3 相容性模式。

## 遷移至新的 Windows Server 執行個體

1. 在新的 Windows Server 執行個體上完成[遷移至用戶端 SDK 5](#)中的所有步驟。
2. 檢查現有的金鑰參考檔案

在原始 Windows Server 執行個體上，檢查 中是否有金鑰參考檔案C:\Users\Default\AppData\Roaming\Microsoft\Crypto\CaviumKSP\GlobalPartition。

- 如果金鑰參考檔案存在，請將C:\Users\Default\AppData\Roaming\Microsoft\Crypto\CaviumKSP包含的所有內容複製到新 Windows Server 執行個體上的GlobalPartition相同目錄路徑。如果目錄不存在，請建立目錄。
- 如果金鑰參考檔案不存在，請在新的 Windows Server 執行個體cloudhsm-cli key generate-file --encoding ksp-key-reference上使用 來建立它們。如需說明，請參閱[產生 KSP 金鑰參考 \(Windows\)](#)。

3. 驗證根憑證

在信任的根憑證授權單位中檢查您的根憑證：

```
PS C:\Users\Administrator\Desktop> certutil -store Root

Root "Trusted Root Certification Authorities"
===== Certificate 0 =====
Serial Number: certificate-serial-number
Issuer: CN=MYRootCA
NotBefore: 2/5/2020 1:38 PM
NotAfter: 2/5/2021 1:48 PM
Issuer: CN=MYRootCA
Signature matches Public Key
Root Certificate: Subject matches Issuer
```



```
Cert Hash(sha1): cert-hash
No key provider information
Cannot find the certificate and private key for decryption.
CertUtil: -store command completed successfully.
```

#### Note

請注意用於下一個步驟的憑證序號。

## 4. 匯出根憑證

將根憑證匯出至檔案：

```
certutil -store Root certificate-serial-number root-certificate-name.cer
```

## 5. 驗證 HSM 後端憑證

在個人憑證存放區中檢查您的 HSM 後端憑證：

```
PS C:\Users\Administrator\Desktop> certutil -store My

my "Personal"
===== Certificate 0 =====
Serial Number: certificate-serial-number
Issuer: CN=MYRootCA
NotBefore: 2/5/2020 1:38 PM
NotAfter: 2/5/2021 1:48 PM
Subject: CN=www.mydomain.com, OU=Certificate Management, O=Information Technology,
L=Houston, S=Texas, C=US
Non-root Certificate
Cert Hash(sha1): cert-hash
Key Container = key-container-name
Provider = Cavium Key Storage Provider
Private key is NOT exportable
Encryption test passed
CertUtil: -store command completed successfully.
```

#### Note

請注意用於下一個步驟的憑證序號。

## 6. 匯出 HSM 後端憑證

將 HSM 後端憑證匯出至 檔案：

```
certutil -store My certificate-serial-number signed-certificate-name.cer
```

## 7. 匯入根憑證

在您的新 Windows 執行個體上：

1. 將根 CA 檔案複製到新的 Windows 執行個體
2. 匯入憑證：

```
certutil -addstore Root root-certificate-name.cer
```

## 8. 驗證根憑證安裝

確認根憑證已正確安裝：

```
PS C:\Users\Administrator\Desktop> certutil -store Root

Root "Trusted Root Certification Authorities"
===== Certificate 0 =====
Serial Number: certificate-serial-number
Issuer: CN=MYRootCA
NotBefore: 2/5/2020 1:38 PM
NotAfter: 2/5/2021 1:48 PM
Issuer: CN=MYRootCA
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): cert-hash
No key provider information
Cannot find the certificate and private key for decryption.
CertUtil: -store command completed successfully.
```

## 9. 匯入 HSM 後端憑證

在您的新 Windows 執行個體上：

1. 將 HSM 後端憑證複製到新的 Windows 執行個體
2. 匯入憑證：

```
certutil -addstore My signed-certificate-name.cer
```

## 10. 驗證 HSM 後端憑證安裝

確認 HSM 後端憑證已正確安裝：

```
PS C:\Users\Administrator\Desktop> certutil -store My

my "Personal"
===== Certificate 0 =====
Serial Number: certificate-serial-number
Issuer: CN=MYRootCA
NotBefore: 2/5/2020 1:38 PM
NotAfter: 2/5/2021 1:48 PM
Subject: CN=www.mydomain.com, OU=Certificate Management, O=Information Technology,
L=Houston, S=Texas, C=US
Non-root Certificate
Cert Hash(sha1): cert-hash
No key provider information
Cannot find the certificate and private key for decryption.
CertUtil: -store command completed successfully.
```

### Note

請注意要在後續步驟中使用的憑證序號。

## 11. 建立金鑰參考檔案（選用）

只有在您需要建立新的金鑰參考檔案時，才完成此步驟。否則，請繼續執行下一個步驟。

### Note

此功能僅適用於 SDK 5.16.0 版及更新版本。

### 1. 安裝 [OpenSSL](#) 並擷取模數：

```
openssl x509 -in signed-certificate-name.cer -modulus -noout
```

 Note

OpenSSL 命令會以 格式輸出模數：Modulus=*modulus-value*。請注意用於下一個命令的###。

2. 使用 CloudHSM CLI 建立金鑰參考檔案，請參閱[產生 KSP 金鑰參考 \(Windows\)](#)：

```
& "C:\Program Files\Amazon\CloudHSM\bin\cloudhsm-cli.exe" key generate-
file --encoding ksp-key-reference --filter attr.class=private-key
attr.modulus=0xmodulus-value
```

 Note

CloudHSM CLI 命令引數中的###必須以 為字首0x，表示十六進位格式。  
金鑰參考檔案是在 中建立C:\Users\Default\AppData\Roaming\Microsoft\Crypto\CaviumKSP\GlobalPartition。

## 12. 建立修復組態

建立名為 repair.txt 且具有下列內容的檔案：

```
[Properties]
11 = "" ; Add friendly name property
2 = "{text}" ; Add Key Provider Information property
continue="Container=key-container-name&"
continue="Provider=Cavium Key Storage Provider&"
continue="Flags=0&"
continue="KeySpec=2"
```

 Note

將 *key-container-name* 取代為來自 的金鑰參考檔案名稱C:\Users\Default\AppData\Roaming\Microsoft\Crypto\CaviumKSP\GlobalPartition。

## 13. 修復憑證存放區

執行修復命令：

```
certutil -repairstore My certificate-serial-number repair.txt
```

#### Note

驗證 HSM 後端憑證安裝時，會從先前的步驟取得憑證序號。

## 14. 驗證憑證關聯

確認憑證已正確關聯：

```
PS C:\Users\Administrator\Desktop> certutil -store My

my "Personal"
===== Certificate 0 =====
Serial Number: certificate-serial-number
Issuer: CN=MYRootCA
NotBefore: 2/5/2020 1:38 PM
NotAfter: 2/5/2021 1:48 PM
Subject: CN=www.mydomain.com, OU=Certificate Management, O=Information Technology,
L=Houston, S=Texas, C=US
Non-root Certificate
Cert Hash(sha1): cert-hash
Key Container = key-container-name
Provider = Cavium Key Storage Provider
Private key is NOT exportable
ERROR: Could not verify certificate public key against private key
CertUtil: -store command completed successfully.
```

確認輸出顯示：

- 正確的金鑰容器名稱
- Cavium 金鑰儲存供應商
- ERROR: Could not verify certificate public key against private key 是已知問題，請參閱 [問題：憑證存放區的驗證失敗](#)

## 15. 測試您的應用程式

在完成遷移之前：

1. 在開發環境中測試您的應用程式

2. 更新您的程式碼以解決任何重大變更
3. 如需應用程式特定的指引，請參閱 [整合第三方應用程式與 AWS CloudHSM](#)

## 驗證遷移

完成遷移步驟後，請確認：

- 您的憑證已正確安裝在正確的憑證存放區中
- 金鑰參考檔案位於正確位置
- 您的應用程式可以使用遷移的憑證執行密碼編譯操作

## 故障診斷

如果您在遷移期間遇到問題，請驗證：

- 從來源系統正確匯出所有憑證
- 系統之間的憑證序號相符
- repair.txt 檔案中的金鑰容器名稱符合您的金鑰參考檔案
- 如果使用 SDK3 SDK3-generated 相容性模式

## 相關主題

- [的最佳實務 AWS CloudHSM](#)

## 將您的 JCE 供應商從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5

使用此主題將 [JCE 供應商](#) 從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5。如需遷移的優點，請參閱 [AWS CloudHSM 用戶端 SDK 5 的優點](#)。

在中 AWS CloudHSM，客戶應用程式會使用 AWS CloudHSM 用戶端軟體開發套件 (SDK) 執行密碼編譯操作。用戶端 SDK 5 是主要 SDK，會持續新增新功能和平台支援。

用戶端 SDK 3 JCE 提供者使用不屬於標準 JCE 規格的自訂類別和 APIs。適用於 JCE 提供者的用戶端 SDK 5 會抱怨 JCE 規格，且與特定區域的用戶端 SDK 3 回溯不相容。在遷移至用戶端 SDK 5 的過程中，客戶應用程式可能需要變更。本節概述成功遷移所需的變更。

若要檢閱所有供應商的遷移指示，請參閱 [從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)。

## 主題

- [解決重大變更以做好準備](#)
- [遷移至用戶端 SDK 5](#)
- [相關主題](#)

## 解決重大變更以做好準備

檢閱這些重大變更，並相應地更新開發環境中的應用程式。

### 供應商類別和名稱已變更

| 已變更的內容   | 用戶端 SDK 3 中的內容                                                                       | 用戶端 SDK 5 中的內容                                                                       | 範例                                                                                           |
|----------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| 供應商類別和名稱 | 用戶端 SDK 3 中的 JCE 提供者類別稱為 <code>CaviumProvider</code> ，且具有提供者名稱 <code>Cavium</code> 。 | 在用戶端 SDK 5 中，稱為提供者類別 <code>CloudHsmProvider</code> ，且具有提供者名稱 <code>CloudHSM</code> 。 | 有關如何初始化 <code>CloudHsmProvider</code> 物件的範例可在 <a href="#">AWS CloudHSM GitHub 範例儲存庫</a> 中找到。 |

### 明確登入已變更，隱含 尚未

| 已變更的內容 | 用戶端 SDK 3 中的內容                                                 | 用戶端 SDK 5 中的內容                                                                                                                  | 範例                                                                                                                                          |
|--------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 明確登入   | 用戶端 SDK 3 使用 <code>LoginManager</code> 類別進行明確登入 <sup>1</sup> 。 | 在用戶端 SDK 5 中， <code>CloudHSM</code> 提供者會實作 <code>AuthProvider</code> 以進行明確登入。 <code>AuthProvider</code> 是標準 Java 類別，並遵循 Java 的慣 | 如需如何搭配用戶端 SDK 5 使用明確登入的範例，請參閱 <a href="#">AWS CloudHSM GitHub 範例儲存庫</a> 中的 <code>LoginRunner</code> 範例。 <a href="#">AWS CloudHSM GitHub</a> |

| 已變更的內容 | 用戶端 SDK 3 中的內容                                               | 用戶端 SDK 5 中的內容                                                            | 範例                                                                                        |
|--------|--------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
|        |                                                              | 用方式登入提供者。<br>透過改善用戶端 SDK 5 中的登入狀態管理，應用程式不再需要在重新連線期間監控和執行登入 <sup>2</sup> 。 |                                                                                           |
| 隱含登入   | 隱含登入不需要變更。從用戶端 SDK 3 遷移至用戶端 SDK 5 時，相同的屬性檔案和所有環境變數將繼續用於隱含登入。 |                                                                           | 如需如何搭配用戶端 SDK 5 使用隱含登入的範例，請參閱 AWS CloudHSM GitHub <a href="#">範例儲存庫中的 LoginRunner</a> 範例。 |

- **【1】** 用戶端 SDK 3 程式碼片段：

```
LoginManager lm = LoginManager.getInstance();

lm.login(partition, user, pass);
```

- **【2】** 用戶端 SDK 5 程式碼片段：

```
// Construct or get the existing provider object
AuthProvider provider = new CloudHsmProvider();

// Call login method on the CloudHsmProvider object
// Here loginHandler is a CallbackHandler
provider.login(null, loginHandler);
```

如需如何搭配用戶端 SDK 5 使用明確登入的範例，請參閱 AWS CloudHSM GitHub [範例儲存庫中的 LoginRunner](#) 範例。



## 金鑰產生已變更

| 已變更的內容 | 用戶端 SDK 3 中的內容                                                                                    | 用戶端 SDK 5 中的內容                                                               | 範例                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 金鑰產生   | 在用戶端 SDK 3 中，Cavium[Key-type]AlgorithmParameterSpec 用於指定金鑰產生參數。如需程式碼片段，請參閱註腳 <a href="#">1</a> 。  | 在用戶端 SDK 5 中，KeyAttributesMap 用於指定金鑰產生屬性。如需程式碼片段，請參閱註腳 <a href="#">2</a> 。   | 如需如何使用 KeyAttributesMap 產生對稱金鑰的範例，請參閱 AWS CloudHSM GitHub <a href="#">範例儲存庫</a> 中的 <a href="#">SymmetricKeys</a> 範例。   |
| 產生金鑰對  | 在用戶端 SDK 3 中，Cavium[Key-type]AlgorithmParameterSpec 用於指定金鑰對產生參數。如需程式碼片段，請參閱註腳 <a href="#">3</a> 。 | 在用戶端 SDK 5 中，KeyPairAttributesMap 用於指定這些參數。如需程式碼片段，請參閱註腳 <a href="#">4</a> 。 | 如需如何使用 KeyAttributesMap 產生非對稱金鑰的範例，請參閱 AWS CloudHSM GitHub <a href="#">範例儲存庫</a> 中的 <a href="#">AsymmetricKeys</a> 範例。 |

- **【1】** 用戶端 SDK 3 金鑰產生程式碼片段：

```
KeyGenerator keyGen = KeyGenerator.getInstance("AES", "Cavium");
CaviumAESKeyGenParameterSpec aesSpec = new CaviumAESKeyGenParameterSpec(
 keySizeInBits,
 keyLabel,
 isExtractable,
 isPersistent);
keyGen.init(aesSpec);
SecretKey aesKey = keyGen.generateKey();
```

- **【2】** 用戶端 SDK 5 金鑰產生程式碼片段：

```
KeyGenerator keyGen = KeyGenerator.getInstance("AES",
 CloudHsmProvider.PROVIDER_NAME);
```

```
final KeyAttributesMap aesSpec = new KeyAttributesMap();
aesSpec.put(KeyAttribute.LABEL, keyLabel);
aesSpec.put(KeyAttribute.SIZE, keySizeInBits);
aesSpec.put(KeyAttribute.EXTRACTABLE, isExtractable);
aesSpec.put(KeyAttribute.TOKEN, isPersistent);

keyGen.init(aesSpec);
SecretKey aesKey = keyGen.generateKey();
```

- **【3】 用戶端 SDK 3 金鑰對產生程式碼片段：**

```
KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("rsa", "Cavium");
CaviumRSAKeyGenParameterSpec spec = new CaviumRSAKeyGenParameterSpec(
 keySizeInBits,
 new BigInteger("65537"),
 label + ":public",
 label + ":private",
 isExtractable,
 isPersistent);

keyPairGen.initialize(spec);

keyPairGen.generateKeyPair();
```

- **【4】 用戶端 SDK 5 金鑰對產生程式碼片段：**

```
KeyPairGenerator keyPairGen =
 KeyPairGenerator.getInstance("RSA", providerName);

// Set attributes for RSA public key
final KeyAttributesMap publicKeyAttrsMap = new KeyAttributesMap();
publicKeyAttrsMap.putAll(additionalPublicKeyAttributes);
publicKeyAttrsMap.put(KeyAttribute.LABEL, label + ":Public");
publicKeyAttrsMap.put(KeyAttribute.MODULUS_BITS, keySizeInBits);
publicKeyAttrsMap.put(KeyAttribute.PUBLIC_EXPONENT,
 new BigInteger("65537").toByteArray());

// Set attributes for RSA private key
final KeyAttributesMap privateKeyAttrsMap = new KeyAttributesMap();
privateKeyAttrsMap.putAll(additionalPrivateKeyAttributes);
privateKeyAttrsMap.put(KeyAttribute.LABEL, label + ":Private");
```

```
// Create KeyPairAttributesMap and use that to initialize the
// keyPair generator
KeyPairAttributesMap keyPairSpec =
new KeyPairAttributesMapBuilder()
.withPublic(publicKeyAttrsMap)
.withPrivate(privateKeyAttrsMap)
.build();

keyPairGen.initialize(keyPairSpec);
keyPairGen.generateKeyPair();
```

尋找、刪除和參考金鑰已變更

AWS CloudHSM 使用 KeyStore 尋找已產生的金鑰。用戶端 SDK 3 有兩種 KeyStore 類型：Cavium和 CloudHSM。用戶端 SDK 5 只有一種 KeyStore 類型：CloudHSM。

從 Cavium KeyStore 移至 CloudHSM KeyStore 需要變更 KeyStore 類型。此外，用戶端 SDK 3 使用金鑰控制代碼來參考金鑰，而用戶端 SDK 5 則使用金鑰標籤。產生的行為變更如下所示。

| 已變更的內容 | 用戶端 SDK 3 中的內容                                                                           | 用戶端 SDK 5 中的內容                                                                                                                                                                | 範例 |
|--------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 金鑰參考   | 透過用戶端 SDK 3，應用程式會使用金鑰標籤或金鑰控制代碼來參考 HSM 中的金鑰。他們使用標籤搭配 KeyStore 來尋找金鑰，或使用控點並建立CaviumKey 物件。 | 在用戶端 SDK 5 中，應用程式可以使用 <a href="#">用戶端 SDK 5 的AWS CloudHSM KeyStore Java 類別</a> 依標籤尋找金鑰。若要依控制代碼尋找金鑰，請使用 AWS CloudHSM KeyStoreWithAttributes 搭配 AWS CloudHSM KeyReferenceSpec 。 |    |
| 尋找多個項目 | 在 KeyStore 中存<br>在多個條件相同的                                                                | 使用 AWS CloudHSM KeyStore和                                                                                                                                                     |    |

| 已變更的內容 | 用戶端 SDK 3 中的內容                                                            | 用戶端 SDK 5 中的內容                                                                                                                                                                                 | 範例                                                                                               |
|--------|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
|        | 項目getCertificate 的情況<br>下getKey，使用<br>getEntry、或搜尋Cavium金鑰時，只會傳回找到的第一個項目。 | 時KeyStoreWithAttributes，這個相同的案例會導致擲回例外狀況。若要修正此問題，建議您使用 CloudHSM CLI 中的 <a href="#">使用 CloudHSM CLI 設定金鑰的屬性</a> 命令來設定金鑰的唯一標籤。或使用 KeyStoreWithAttributes#getKeys 傳回符合條件的所有金鑰。                    |                                                                                                  |
| 尋找所有金鑰 | 您可以在用戶端 SDK 3 中使用 尋找 HSM 中的所有金鑰Util.findAllKeys() 。                       | 用戶端 SDK 5 使用 KeyStoreWithAttributes 類別，讓尋找金鑰變得更簡單且更有效率。盡可能快取您的金鑰，將延遲降至最低。如需詳細資訊，請參閱 <a href="#">有效管理應用程式中的金鑰</a> 。當您需要從 HSM 擷取所有金鑰時，請使用 KeyStoreWithAttributes#getKeys 搭配空的 KeyAttributesMap 。 | 使用 KeyStoreWithAttributes 類別尋找金鑰的範例可在 <a href="#">AWS CloudHSM GitHub 範例儲存庫</a> 中使用，程式碼片段會顯示在中1。 |

| 已變更的內容 | 用戶端 SDK 3 中的內容                                   | 用戶端 SDK 5 中的內容                                                                            | 範例                                                                                                |
|--------|--------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| 刪除金鑰   | 用戶端 SDK 3 使用 <code>Util.deleteKey()</code> 刪除金鑰。 | 用戶端 SDK 5 中的 Key 物件實作 <code>Destroyable</code> 介面，允許使用此介面的 <code>destroy()</code> 方法刪除金鑰。 | 您可以在 <a href="#">CloudHSM GitHub 範例儲存庫</a> 中找到顯示刪除金鑰功能的範例程式碼。每個 SDK 的範例程式碼片段會顯示在 中 <sup>2</sup> 。 |

- **【1】** 程式碼片段如下所示：

```
KeyAttributesMap findSpec = new KeyAttributesMap();
findSpec.put(KeyAttribute.LABEL, label);
findSpec.put(KeyAttribute.KEY_TYPE, keyType);
KeyStoreWithAttributes keyStore = KeyStoreWithAttributes.getInstance("CloudHSM");

keyStore.load(null, null);
keyStore.getKey(findSpec);
```

- **【2】** 在用戶端 SDK 3 中刪除金鑰：

```
Util.deleteKey(key);
```

在用戶端 SDK 5 中刪除金鑰：

```
((Destroyable) key).destroy();
```

密碼取消包裝操作已變更，其他密碼操作尚未

#### Note

密碼 `encrypt/decrypt/wrap` 操作不需要變更。

取消包裝操作需要將用戶端 SDK 3 `CaviumUnwrapParameterSpec` 類別取代為下列密碼編譯操作專用的其中一個類別。

- GCMUnwrapKeySpec 用於 AES/GCM/NoPadding 取消包裝
- IvUnwrapKeySpec 適用於 AESWrap unwrap 和 的 AES/CBC/NoPadding unwrap
- 適用於 RSA OAEP unwrap 的 OAEPUnwrapKeySpec

的範例程式碼片段 OAEPUnwrapKeySpec :

```
OAEPParameterSpec oaepParameterSpec =
new OAEPParameterSpec(
 "SHA-256",
 "MGF1",
 MGF1ParameterSpec.SHA256,
 PSpecified.DEFAULT);

KeyAttributesMap keyAttributesMap =
 new KeyAttributesMap(KeyAttributePermissiveProfile.KEY_CREATION);
keyAttributesMap.put(KeyAttribute.TOKEN, true);
keyAttributesMap.put(KeyAttribute.EXTRACTABLE, false);

OAEPUnwrapKeySpec spec = new OAEPUnwrapKeySpec(oaepParameterSpec,
 keyAttributesMap);

Cipher hsmCipher =
 Cipher.getInstance(
 "RSA/ECB/OAEPPadding",
 CloudHsmProvider.PROVIDER_NAME);
hsmCipher.init(Cipher.UNWRAP_MODE, key, spec);
```

簽章操作尚未變更

Signature 操作不需要變更。

## 遷移至用戶端 SDK 5

遵循本節中的指示，從用戶端 SDK 3 遷移至用戶端 SDK 5。

### Note

用戶端 SDK 5 目前不支援 Amazon Linux、Ubuntu 16.04、Ubuntu 18.04 CentOS 6、CentOS 8 和 RHEL 6。如果您目前正在將其中一個平台與用戶端 SDK 3 搭配使用，則需要在遷移至用戶端 SDK 5 時選擇不同的平台。

## 1. 解除安裝用戶端 SDK 3 的 JCE 提供者。

### Amazon Linux 2

```
$ sudo yum remove cloudhsm-client-jce
```

### CentOS 7

```
$ sudo yum remove cloudhsm-client-jce
```

### RHEL 7

```
$ sudo yum remove cloudhsm-client-jce
```

### RHEL 8

```
$ sudo yum remove cloudhsm-client-jce
```

## 2. 解除安裝 Client Daemon for Client SDK 3。

### Amazon Linux 2

```
$ sudo yum remove cloudhsm-client
```

### CentOS 7

```
$ sudo yum remove cloudhsm-client
```

### RHEL 7

```
$ sudo yum remove cloudhsm-client
```

### RHEL 8

```
$ sudo yum remove cloudhsm-client
```

 Note

需要再次啟用自訂組態。

3. 依照中的步驟安裝用戶端 SDK JCE 提供者[安裝 AWS CloudHSM 用戶端 SDK 5 的 JCE 提供者](#)。
4. 用戶端 SDK 5 推出新的組態檔案格式和命令列引導工具。若要引導您的用戶端 SDK 5 JCE 供應商，請遵循下使用者指南中列出的說明[引導用戶端 SDK](#)。
5. 在您的開發環境中，測試您的應用程式。更新現有程式碼，以在最終遷移之前解決重大變更。

## 相關主題

- [的最佳實務 AWS CloudHSM](#)

## 使用用戶端 SDK 5 來使用 AWS CloudHSM

AWS CloudHSM 包含兩個主要用戶端 SDK 版本：

- 用戶端 SDK 5：這是我們最新預設的用戶端 SDK。如需有關其優點和優勢的資訊，請參閱 [AWS CloudHSM 用戶端 SDK 5 的優點](#)。
- 用戶端 SDK 3：這是我們較舊的用戶端 SDK。它包括一組完整的組件，用於基於平台和語言的應用程式兼容性和管理工具。

如需從用戶端 SDK 3 遷移至用戶端 SDK 5 的指示，請參閱 [從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)。

本主題說明用戶端 SDK 5。若要檢查您正在使用的用戶端 SDK 版本，請參閱

### 主題

- [AWS CloudHSM 用戶端 SDK 5 的優點](#)
- [AWS CloudHSM 用戶端 SDK 5 支援的平台](#)
- [AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫](#)
- [適用於 AWS CloudHSM 用戶端 SDK 5 的 OpenSSL 動態引擎](#)
- [AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 \(KSP\)](#)



- [AWS CloudHSM 用戶端 SDK 5 的 JCE 提供者](#)

## AWS CloudHSM 用戶端 SDK 5 的優點

AWS CloudHSM 與用戶端 SDK 3 相比，用戶端 SDK 5 更易於管理，提供卓越的可設定性和更高的可靠性。用戶端 SDK 5 還為用戶端 SDK 3 提供了一些額外的關鍵優勢。

### 專為無伺服器架構所設計

用戶端 SDK 5 不需要用戶端常駐程式，因此您不再需要管理背景服務。其可以通過幾種重要方式幫助用戶：

- 簡化應用程式的啟動程序。開始使用 CloudHSM 需在執行應用程式之前先設定 SDK。
- 無需持續執执行程序，可更輕鬆地與 Lambda 和彈性容器服務 (ECS) 等無伺服器元件的集成。

### 更好的第三方集成和更輕鬆的可攜性

用戶端 SDK 5 嚴格遵循 JCE 規範，並在不同的 JCE 提供者和更好的第三方集成之間提供了更輕鬆的可移植性

### 改善使用者體驗和可設定性

用戶端 SDK 5 提高了日誌消息的可讀性，並提供了更清晰的異常和錯誤處理機制，讓使用者更容易進行自助分類。SDK 5 還提供了各種組態，這些組態列在[設定工具頁面](#)中。

### 更廣泛的平台支援

用戶端 SDK 5 為現代作業平台提供了更多支援。其包括對 ARM 技術的支援，以及對 [JCE](#)、[PKCS #11](#) 和 [OpenSSL](#) 的更多支援。如需詳細資訊，請參閱[支援的平台](#)。

### IPv6 連線支援

用戶端 SDK 5.14+ 支援使用 IPv6 連線至雙堆疊 HSMs。

### 附加功能和機制

用戶端 SDK 5 包含用戶端 SDK 3 中無法使用的其他功能和機制，而用戶端 SDK 5 未來會繼續新增更多機制。

## AWS CloudHSM 用戶端 SDK 5 支援的平台

AWS CloudHSM 用戶端 SDK 的每個版本的基本支援都不同。SDK 中元件的平台支援通常符合基礎支援，但並非總是如此。若要判斷特定元件的平台支援，請先確定您想要的平台出現在 SDK 的基礎區段中，然後檢查元件區段中是否有任何排除或任何其他相關資訊。

AWS CloudHSM 僅支援 64 位元作業系統。

平台支援會隨時間變更。舊版 CloudHSM 用戶端 SDK 可能不支援此處列出的所有作業系統。使用版本說明來判斷舊版 CloudHSM 用戶端 SDK 的作業系統支援。如需詳細資訊，請參閱 [AWS CloudHSM 用戶端 SDK 的下載](#)。

如需先前用戶端 SDK 支援的平台，請參閱 [AWS CloudHSM 用戶端 SDK 3 支援的平台](#)

用戶端 SDK 5 不需要用戶端常駐程式。

### 主題

- [Linux 支援 AWS CloudHSM 用戶端 SDK 5](#)
- [Windows 支援 AWS CloudHSM 用戶端 SDK 5](#)
- [AWS CloudHSM 用戶端 SDK 5 的無伺服器支援](#)
- [AWS CloudHSM 用戶端 SDK 5 的 HSM 相容性](#)

## Linux 支援 AWS CloudHSM 用戶端 SDK 5

AWS CloudHSM 用戶端 SDK 5 支援下列 Linux 作業系統和平台。

| 支援平台                              | X86_64 架構 | ARM 架構 |
|-----------------------------------|-----------|--------|
| Amazon Linux 2                    | 是         | 是      |
| Amazon Linux 2023                 | 是         | 是      |
| Red Hat Enterprise Linux 8 (8.3+) | 是         | 否      |
| Red Hat Enterprise Linux 9 (9.2+) | 是         | 是      |
| Ubuntu 22.04 LTS                  | 是         | 是      |

| 支援平台             | X86_64 架構 | ARM 架構 |
|------------------|-----------|--------|
| Ubuntu 24.04 LTS | 是         | 是      |

- SDK 5.16 是提供 Ubuntu 20.04 LTS 平台支援的最後版本。如需詳細資訊，請參閱 [Ubuntu 網站](#)。
- SDK 5.12 是提供 CentOS 7 (7.8+) 平台支援的最後版本。如需詳細資訊，請參閱 [CentOS 網站](#)。
- SDK 5.12 是提供 Red Hat Enterprise Linux 7 (7.8+) 平台支援的最後版本。如需詳細資訊，請參閱 [Red Hat 網站](#)。
- SDK 5.4.2 是提供 CentOS 8 平台支援的最後版本。如需詳細資訊，請參閱 [CentOS 網站](#)。

## Windows 支援 AWS CloudHSM 用戶端 SDK 5

AWS CloudHSM 用戶端 SDK 5 支援下列版本的 Windows Server。

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2025

## AWS CloudHSM 用戶端 SDK 5 的無伺服器支援

AWS CloudHSM 用戶端 SDK 5 支援下列無 AWS 伺服器服務。

- AWS Lambda
- Docker/ECS

## AWS CloudHSM 用戶端 SDK 5 的 HSM 相容性

下表說明 HSMs 的 AWS CloudHSM 用戶端 SDK 5 相容性。

| hsm1.medium              | hsm2m.medium             |
|--------------------------|--------------------------|
| 與用戶端 SDK 5.0.0 版及更新版本相容。 | 與用戶端 SDK 5.9.0 版及更新版本相容。 |

## AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫

PKCS #11 是在硬體安全模組 (HSMs) 上執行加密作業的標準。AWS CloudHSM 提供與 PKCS #11 2.40 版相容的 PKCS #11 程式庫的實作方式。

如需關於啟動載入的資訊，請參閱 [連接至叢集](#)。如需故障診斷，請參閱 [PKCS #11 程式庫的已知問題 AWS CloudHSM](#)。

如需關於使用用戶端 SDK 3 的資訊，請參閱 [使用先前的 SDK 版本來使用 AWS CloudHSM](#)。

### 主題

- [安裝 AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫](#)
- [驗證至用戶端 SDK 5 的 AWS CloudHSM PKCS #11 程式庫](#)
- [用戶端 SDK 5 的 PKCS #11 程式庫 AWS CloudHSM 支援的金鑰類型](#)
- [用戶端 SDK AWS CloudHSM 5 的 PKCS #11 程式庫支援的機制](#)
- [用戶端 SDK 5 的 PKCS #11 程式庫 AWS CloudHSM 支援的 API 操作](#)
- [用戶端 SDK 5 的 AWS CloudHSM PKCS #11 程式庫中的金鑰屬性](#)
- [用戶端 SDK AWS CloudHSM 5 的 PKCS #11 程式庫程式碼範例](#)
- [PKCS #11 程式庫的進階組態 AWS CloudHSM](#)
- [具有 PKCS #11 程式庫的憑證儲存](#)

## 安裝 AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫

本主題提供安裝 AWS CloudHSM 用戶端 SDK 5 版本系列的最新版 PKCS #11 程式庫的說明。如需關於用戶端 SDK 或 PKCS #11 程式庫的詳細資訊，請參閱[使用用戶端 SDK](#) 和 [PKCS #11 程式庫](#)。

使用用戶端 SDK 5 時，您無需安裝或執行用戶端常駐程式。

若要使用用戶端 SDK 5 執行單一 HSM 叢集，您必須先將 `disable_key_availability_check` 設定為 `True` 來管理用戶端金鑰持久性。如需詳細資訊，請參閱[金鑰同步處理](#)和[用戶端 SDK 5 設定工具](#)。

如需關於用戶端 SDK 5 中 PKCS #11 程式庫的詳細資訊，請參閱 [PKCS #11 程式庫](#)。

**Note**

若要使用用戶端 SDK 5 執行單一 HSM 叢集，您必須先將 `disable_key_availability_check` 設定為 `True` 來管理用戶端金鑰持久性。如需詳細資訊，請參閱[金鑰同步處理](#)和[用戶端 SDK 5 設定工具](#)。

若要安裝和設定 PKCS #11 程式庫

1. 使用以下命令來下載和安裝 PKCS #11 程式庫。

### Amazon Linux 2023

在 X86\_64 架構上安裝 Amazon Linux 2023 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-pkcs11-latest.amzn2023.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-pkcs11-latest.amzn2023.x86_64.rpm
```

在 ARM64 架構上安裝 Amazon Linux 2023 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-pkcs11-latest.amzn2023.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-pkcs11-latest.amzn2023.aarch64.rpm
```

### Amazon Linux 2

安裝適用於 Amazon Linux 2 (X86\_64 架構) 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-pkcs11-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-pkcs11-latest.el7.x86_64.rpm
```

安裝適用於 Amazon Linux 2 (ARM64 架構) 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-pkcs11-latest.el7.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-pkcs11-latest.el7.aarch64.rpm
```

## RHEL 9 (9.2+)

在 X86\_64 架構上安裝 RHEL 9 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-pkcs11-latest.el9.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-pkcs11-latest.el9.x86_64.rpm
```

在 ARM64 架構上安裝 RHEL 9 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-pkcs11-latest.el9.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-pkcs11-latest.el9.aarch64.rpm
```

## RHEL 8 (8.3+)

在 X86\_64 架構上安裝 RHEL 8 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-pkcs11-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-pkcs11-latest.el8.x86_64.rpm
```

## Ubuntu 24.04 LTS

在 X86\_64 架構上安裝適用於 Ubuntu 24.04 LTS 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/cloudhsm-pkcs11_latest_u24.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-pkcs11_latest_u24.04_amd64.deb
```

在 ARM64 架構上安裝適用於 Ubuntu 24.04 LTS 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/
cloudhsm-pkcs11_latest_u24.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-pkcs11_latest_u24.04_arm64.deb
```

## Ubuntu 22.04 LTS

安裝適用於 Ubuntu 22.04 LTS (X86\_64 架構) 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/
cloudhsm-pkcs11_latest_u22.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-pkcs11_latest_u22.04_amd64.deb
```

在 ARM64 架構上安裝適用於 Ubuntu 22.04 LTS 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/
cloudhsm-pkcs11_latest_u22.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-pkcs11_latest_u22.04_arm64.deb
```

## Ubuntu 20.04 LTS

安裝適用於 Ubuntu 20.04 LTS (X86\_64 架構) 的 PKCS #11 程式庫：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Focal/
cloudhsm-pkcs11_latest_u20.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-pkcs11_latest_u20.04_amd64.deb
```

## Windows Server

在 X86\_64 架構上安裝適用於 Windows Server 的 PKCS #11 程式庫：

1. 下載[適用於用戶端 SDK 5 的 PKCS #11 程式庫](#)。
2. 以 Windows 管理權限執行 PKCS #11 程式庫安裝程式 (AWSCloudHSMPKCS11-latest.msi)。
2. 使用設定工具指定發行憑證的位置。如需說明，請參閱 [指定憑證的位置](#)。
3. 若要連線到您的叢集，請參閱 [引導用戶端 SDK](#)。
4. 您可於下列位置找到 PKCS #11 程式庫檔案：
  - Linux 二進位檔案、組態指令碼和日誌文檔：

```
/opt/cloudhsm
```

Windows 二進位檔案：

```
C:\Program Files\Amazon\CloudHSM
```

Windows組態指令碼和日誌檔案：

```
C:\ProgramData\Amazon\CloudHSM
```

## 驗證至用戶端 SDK 5 的 AWS CloudHSM PKCS #11 程式庫

當您使用 PKCS #11 程式庫時，您的應用程式會在 HSMs 中以特定[加密使用者 \(CU\)](#) 身分執行 AWS CloudHSM。您的應用程式只能檢視和管理 CU 所擁有和共用的金鑰。您可以使用 HSM 中現有的 CU，或為應用程式建立新的 CU。如需關於管理 CU 的資訊，請參閱[使用 CloudHSM CLI 管理 HSM 使用者](#)和[使用 CloudHSM 管理公用程式 \(CMU\) 管理 HSM 使用者](#)。

若要將 CU 指定給 PKCS #11 程式庫，請使用 PKCS #11 [C\\_Login 函數](#)的 pin 參數。對於 AWS CloudHSM，接腳參數的格式如下：

```
<CU_user_name>:<password>
```

例如，以下命令會將 PKCS #11 程式庫 pin 設定給使用者名為 CryptoUser 和密碼為 CUPassword123! 的 CU。



```
CryptoUser:CUPassword123!
```

## 用戶端 SDK 5 的 PKCS #11 程式庫 AWS CloudHSM 支援的金鑰類型

AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫支援下列金鑰類型。

| 金鑰類型                      | 描述                                                                                                          |
|---------------------------|-------------------------------------------------------------------------------------------------------------|
| AES                       | 產生 128 位元、192 位元和 256 位元的 AES 金鑰。                                                                           |
| Triple DES (3DES, DESede) | 產生 192 位元的三重 DES 金鑰。請參閱下列備註 <a href="#">1</a> 查看即將進行的變更。                                                    |
| EC                        | 使用 secp224r1 (P-224)、secp256r1 (P-256)、secp256k1 (Blockchain)、secp384r1 (P-384) 和 secp521r1 (P-521) 曲線產生金鑰。 |
| GENERIC_SECRET            | 產生 1 到 800 位元組的一般機密。                                                                                        |
| RSA                       | 產生 2048 位元至 4096 位元的 RSA 金鑰，以 256 位元為單位遞增。                                                                  |

**【1】** 根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## 用戶端 SDK AWS CloudHSM 5 的 PKCS #11 程式庫支援的機制

PKCS #11 程式庫與 PKCS #11 規格的 2.40 版相容。若要使用 PKCS #11 叫用加密功能，請利用指定機制呼叫函數。下列各節摘要了 AWS CloudHSM 用戶端 SDK 5 支援的函數和機制組合。

PKCS #11 程式庫支援下列演算法：

- 加密和解密：AES-CBC、AES-CTR、AES-ECB、AES-GCM、DES3-CBC、DES3-ECB、RSA-OAEP 和 RSA-PKCS
- 簽署和驗證：RSA、HMAC 和 ECDSA；無論是否使用雜湊皆不影響
- 雜湊/摘要：SHA1、SHA224、SHA256、SHA384 和 SHA512
- 金鑰包裝：AES 金鑰包裝、[1](#) AES-GCM、RSA-AES 和 RSA-OAEP

- 金鑰衍生 – SP800-108 計數器 KDF 和 ECDH 搭配 KDF (支援的 KDF 演算法為 X9.63 搭配 SHA1, SHA224, SHA256, SHA384, SHA512)

## 主題

- [產生金鑰與金鑰對函數](#)
- [簽署和驗證函數](#)
- [簽名恢復和驗證復原函數](#)
- [Digest 函數](#)
- [加密和解密函數](#)
- [衍生金鑰函數](#)
- [包裝和解包函數](#)
- [每個機制的資料大小上限](#)
- [機制註釋](#)

## 產生金鑰與金鑰對函數

PKCS #11 程式庫 AWS CloudHSM 的軟體程式庫可讓您使用下列機制來產生金鑰和金鑰對函數。

- CKM\_RSA\_PKCS\_KEY\_PAIR\_GEN
- CKM\_RSA\_X9\_31\_KEY\_PAIR\_GEN：此機制的功能與 CKM\_RSA\_PKCS\_KEY\_PAIR\_GEN 機制完全相同，但在產生 p 和 q 時提供更強大的保證。
- CKM\_EC\_KEY\_PAIR\_GEN
- CKM\_GENERIC\_SECRET\_KEY\_GEN
- CKM\_AES\_KEY\_GEN
- CKM\_DES3\_KEY\_GEN：註腳 [5](#) 所列的即將進行的變更。

## 簽署和驗證函數

PKCS #11 程式庫 AWS CloudHSM 的軟體程式庫可讓您針對 Sign and Verify 函數使用下列機制。使用用戶端 SDK 5，資料會在軟體中進行本機雜湊處理。這意味著 SDK 可以對任何大小的資料進行雜湊處理。

使用用戶端 SDK 5 RSA 和 ECDSA 時，雜湊在本機完成，因此沒有資料限制。使用 HMAC 時，會有資料限制。如需詳細諮詢，請參閱註腳 [2](#)。

## RSA

- CKM\_RSA\_X\_509
- CKM\_RSA\_PKCS：僅限單一部分操作。
- CKM\_RSA\_PKCS\_PSS：僅限單一部分操作。
- CKM\_SHA1\_RSA\_PKCS
- CKM\_SHA224\_RSA\_PKCS
- CKM\_SHA256\_RSA\_PKCS
- CKM\_SHA384\_RSA\_PKCS
- CKM\_SHA512\_RSA\_PKCS
- CKM\_SHA512\_RSA\_PKCS
- CKM\_SHA1\_RSA\_PKCS\_PSS
- CKM\_SHA224\_RSA\_PKCS\_PSS
- CKM\_SHA256\_RSA\_PKCS\_PSS
- CKM\_SHA384\_RSA\_PKCS\_PSS
- CKM\_SHA512\_RSA\_PKCS\_PSS

## ECDSA

- CKM\_ECDSA：僅限單一部分操作。
- CKM\_ECDSA\_SHA1
- CKM\_ECDSA\_SHA224
- CKM\_ECDSA\_SHA256
- CKM\_ECDSA\_SHA384
- CKM\_ECDSA\_SHA512

## HMAC

- CKM\_SHA\_1\_HMAC<sup>2</sup>
- CKM\_SHA224\_HMAC<sup>2</sup>
- CKM\_SHA256\_HMAC<sup>2</sup>

- CKM\_SHA384\_HMAC<sup>2</sup>
- CKM\_SHA512\_HMAC<sup>2</sup>

## CMAC

- CKM\_AES\_CMAC

## 簽名恢復和驗證復原函數

用戶端 SDK 5 不支援簽名恢復和驗證復原函數。

## Digest 函數

適用於 PKCS #11 程式庫 AWS CloudHSM 的軟體程式庫可讓您針對摘要函數使用下列機制。使用用戶端 SDK 5，資料會在軟體中進行本機雜湊處理。這意味著 SDK 可以對任何大小的資料進行雜湊處理。

- CKM\_SHA\_1
- CKM\_SHA224
- CKM\_SHA256
- CKM\_SHA384
- CKM\_SHA512

## 加密和解密函數

適用於 PKCS #11 程式庫 AWS CloudHSM 的軟體程式庫可讓您針對加密和解密函數使用下列機制。

- CKM\_RSA\_X\_509
- CKM\_RSA\_PKCS：僅限單一部分操作。註腳 [5](#) 所列的即將進行的變更。
- CKM\_RSA\_PKCS\_OAEP：僅限單一部分操作。
- CKM\_AES\_ECB
- CKM\_AES\_CTR
- CKM\_AES\_CBC
- CKM\_AES\_CBC\_PAD
- CKM\_DES3\_CBC：註腳 [5](#) 所列的即將進行的變更。

- CKM\_DES3\_ECB：註腳 [5](#) 所列的即將進行的變更。
- CKM\_DES3\_CBC\_PAD：註腳 [5](#) 所列的即將進行的變更。
- CKM\_AES\_GCM [1](#), [2](#)
- CKM\_CLOUDHSM\_AES\_GCM [3](#)

## 衍生金鑰函數

PKCS #11 程式庫 AWS CloudHSM 的軟體程式庫支援下列金鑰衍生機制：

- CKM\_SP800\_108\_COUNTER\_KDF
- CKM\_ECDH1\_DERIVE - 支援下列廠商定義 KDF 類型的 ECDH 金鑰衍生 [6](#)：
  - CKD\_CLOUDHSM\_X963\_SHA1\_KDF - X9.63 KDF 搭配 SHA1 [7](#)
  - CKD\_CLOUDHSM\_X963\_SHA224\_KDF - X9.63 KDF 搭配 SHA224 [7](#)
  - CKD\_CLOUDHSM\_X963\_SHA256\_KDF - X9.63 KDF 搭配 SHA256 [7](#)
  - CKD\_CLOUDHSM\_X963\_SHA384\_KDF - X9.63 KDF 搭配 SHA384 [7](#)
  - CKD\_CLOUDHSM\_X963\_SHA512\_KDF - X9.63 KDF 搭配 SHA512 [7](#)

## 包裝和解包函數

PKCS #11 程式庫 AWS CloudHSM 的軟體程式庫可讓您針對包裝和取消包裝函數使用下列機制。

如需有關 AES 金鑰包裝的其他資訊，請參閱[AES 金鑰包裝](#)。

- CKM\_RSA\_PKCS：僅限單一部分操作。註腳 [5](#) 所列的即將進行的變更。
- CKM\_RSA\_PKCS\_OAEP [4](#)
- CKM\_AES\_GCM [1](#), [3](#)
- CKM\_CLOUDHSM\_AES\_GCM [3](#)
- CKM\_RSA\_AES\_KEY\_WRAP
- CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_NO\_PAD [3](#)
- CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_PKCS5\_PAD [3](#)
- CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_ZERO\_PAD [3](#)

## 每個機制的資料大小上限

下表列出每個機制設定的資料大小上限：

### 資料集大小上限

| Mechanism            | 資料大小上限 (位元組) |
|----------------------|--------------|
| CKM_SHA_1_HMAC       | 16288        |
| CKM_SHA224_HMAC      | 16256        |
| CKM_SHA256_HMAC      | 16288        |
| CKM_SHA384_HMAC      | 16224        |
| CKM_SHA512_HMAC      | 16224        |
| CKM_AES_CBC          | 16272        |
| CKM_AES_GCM          | 16224        |
| CKM_CLOUDHSM_AES_GCM | 16224        |
| CKM_DES3_CBC         | 16280        |

### 機制註釋

- [1] 當執行 AES-GCM 加密時，HSM 不會接受來自應用程式的初始化向量 (IV) 資料。請務必使用其產生的 IV。系統會將 HSM 所提供的 12 位元組 IV 寫入記憶體參考，該記憶體參考是由您提供的 CK\_GCM\_PARAMS 參數結構 pIV 元素所指向。為了確保使用者不會混淆，在初始化 AES-GCM 加密時，1.1.1 版和更新版本中的 PKCS # 11 開發套件會強制將該 pIV 指向歸零的緩衝區。
- [2] 當使用下列任一機制操作資料時，若資料緩衝區超過資料大小上限，該操作就會導致錯誤。對於這些機制，所有資料處理都必須在 HSM 內進行。如需每個機制的最大資料大小集資訊，請參閱 [每個機制的資料大小上限](#)。
- [3] 廠商定義的機制。為了能使用 CloudHSM 廠商定義的機制，編譯期間 PKCS #11 應用程式必須加入 /opt/cloudhsm/include/pkcs11t.h。

**CKM\_CLOUDHSM\_AES\_GCM**：這個專屬機制是標準 CKM\_AES\_GCM 程式設計更安全的替代方案。這將 HSM 生成的 IV 加入至加密文字的開頭，而不是將它寫回加密初始化期間提供的

CK\_GCM\_PARAMS 結構中。您可以搭配 C\_Encrypt、C\_WrapKey、C\_Decrypt 和 C\_UnwrapKey 函數搭配使用此機制。使用此機制時，CK\_GCM\_PARAMS 結構中的 pIV 變數必須設定為 NULL。與 C\_Decrypt 和 C\_UnwrapKey 搭配使用此機制時，IV 應至於取消包裝的加密文字之前。

**CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_PKCS5\_PAD** : AES 金鑰包裝與 PKCS #5 填補。

**CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_ZERO\_PAD** : AES 金鑰包裝，零填補。

- [4] 支援下列 CK\_MECHANISM\_TYPE 和 CK\_RSA\_PKCS\_MGF\_TYPE，作為 CKM\_RSA\_PKCS\_OAEP 的 CK\_RSA\_PKCS\_OAEP\_PARAMS：
  - CKM\_SHA\_1 使用 CKG\_MGF1\_SHA1
  - CKM\_SHA224 使用 CKG\_MGF1\_SHA224
  - CKM\_SHA256 使用 CKG\_MGF1\_SHA256
  - CKM\_SHA384 使用 CKM\_MGF1\_SHA384
  - CKM\_SHA512 使用 CKM\_MGF1\_SHA512
- 【5】 根據 NIST 指引，2023 年之後處於 FIPS 模式的叢集不允許這樣做。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。
- 【6】 供應商定義的類型。為了使用 CloudHSM 廠商定義的類型，PKCS#11 應用程式必須在編譯 cloudhsm\_pkcs11\_vendor\_defs.h 期間包含。這可在 /opt/cloudhsm/include/pkcs11/cloudhsm\_pkcs11\_vendor\_defs.h 適用於 Linux 型平台的 和 C:\Program Files\Amazon\CloudHSM\include\pkcs11\cloudhsm\_pkcs11\_vendor\_defs.h 適用於 Windows 型平台的 中找到
- 【7】 金鑰衍生函數 (KDFs) 會在 [RFC 8418 第 2.1 節](#) 中指定。

## 用戶端 SDK 5 的 PKCS #11 程式庫 AWS CloudHSM 支援的 API 操作

PKCS #11 程式庫支援 AWS CloudHSM 用戶端 SDK 5 的下列 PKCS #11 API 操作。

- C\_CloseAllSessions
- C\_CloseSession
- C\_CreateObject
- C\_Decrypt
- C\_DecryptFinal
- C\_DecryptInit
- C\_DecryptUpdate

- C\_DeriveKey
- C\_DestroyObject
- C\_Digest
- C\_DigestFinal
- C\_DigestInit
- C\_DigestUpdate
- C\_Encrypt
- C\_EncryptFinal
- C\_EncryptInit
- C\_EncryptUpdate
- C\_Finalize
- C\_FindObjects
- C\_FindObjectsFinal
- C\_FindObjectsInit
- C\_GenerateKey
- C\_GenerateKeyPair
- C\_GenerateRandom
- C\_GetAttributeValue
- C\_GetFunctionList
- C\_GetInfo
- C\_GetMechanismInfo
- C\_GetMechanismList
- C\_GetSessionInfo
- C\_GetSlotInfo
- C\_GetSlotList
- C\_GetTokenInfo
- C\_Initialize
- C\_Login
- C\_Logout
- C\_OpenSession



- C\_Sign
- C\_SignFinal
- C\_SignInit
- C\_SignUpdate
- C\_UnWrapKey
- C\_Verify
- C\_VerifyFinal
- C\_VerifyInit
- C\_VerifyUpdate
- C\_WrapKey

## 用戶端 SDK 5 的 AWS CloudHSM PKCS #11 程式庫中的金鑰屬性

AWS CloudHSM 金鑰物件可以是公有、私有或私密金鑰。系統會透過屬性來指定金鑰物件上允許的動作。金鑰物件建立時，即會一併建立屬性。當您使用 PKCS #11 程式庫時 AWS CloudHSM，我們會依 PKCS #11 標準指定預設值。

AWS CloudHSM 不支援 PKCS #11 規格中列出的所有屬性。我們會符合所有支援屬性的規格，並在個別表格中列出這些屬性。

用來建立、修改或複製物件的加密函數 (如

C\_CreateObject、C\_GenerateKey、C\_GenerateKeyPair、C\_UnwrapKey 和 C\_DeriveKey) 會採用屬性範本做為其中一個參數。如需關於在建立物件期間傳遞屬性範本的詳細資訊，請參閱[透過 PKCS #11 程式庫產生金鑰](#) (以此為例)。

下列主題提供有關 AWS CloudHSM 金鑰屬性的詳細資訊。

### 主題

- [AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫屬性資料表](#)
- [修改用戶端 SDK 5 的 AWS CloudHSM PKCS #11 程式庫屬性](#)
- [解譯用戶端 SDK 5 的 AWS CloudHSM PKCS #11 程式庫錯誤代碼](#)

## AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫屬性資料表

的 PKCS #11 程式庫資料表 AWS CloudHSM 包含因金鑰類型而異的屬性清單。它會指出使用特定密碼編譯函數時，特定金鑰類型是否支援指定的屬性 AWS CloudHSM。

圖例：

- ✓ 表示 CloudHSM 支援特定金鑰類型的屬性。
- ✕ 表示 CloudHSM 不支援特定金鑰類型的屬性。
- R 表示特定金鑰類型的屬性值設定為唯讀模式。
- S 表示屬性較為敏感，因此無法透過 GetAttributeValue 讀取。
- 預設值欄位中的空白儲存格表示屬性沒有獲派指定預設值。

## GenerateKeyPair

| 屬性               | 金鑰類型           |                |                |                | 預設值   |
|------------------|----------------|----------------|----------------|----------------|-------|
|                  | EC 私<br>有金鑰    | EC 公<br>有金鑰    | RSA 私<br>有金鑰   | RSA 公<br>有金鑰   |       |
| CKA_CLASS        | ✓              | ✓              | ✓              | ✓              |       |
| CKA_KEY_T<br>YPE | ✓              | ✓              | ✓              | ✓              |       |
| CKA_LABEL        | ✓              | ✓              | ✓              | ✓              |       |
| CKA_ID           | ✓              | ✓              | ✓              | ✓              |       |
| CKA_LOCAL        | R              | R              | R              | R              | True  |
| CKA_TOKEN        | ✓              | ✓              | ✓              | ✓              | False |
| CKA_PRIVA<br>TE  | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_ENCRY<br>PT  | ✕              | ✓              | ✕              | ✓              | False |

| 屬性                    | 金鑰類型 |   |   |   | 預設值   |
|-----------------------|------|---|---|---|-------|
| CKA_DECRYPT           | ✓    | ✗ | ✓ | ✗ | False |
| CKA_DERIVE            | ✓    | ✓ | ✓ | ✓ | False |
| CKA_MODIFIABLE        | ✓    | ✓ | ✓ | ✓ | True  |
| CKA_DESTROYABLE       | ✓    | ✓ | ✓ | ✓ | True  |
| CKA_SIGN              | ✓    | ✗ | ✓ | ✗ | False |
| CKA_SIGN_RECOVER      | ✗    | ✗ | ✗ | ✗ |       |
| CKA_VERIFY            | ✗    | ✓ | ✗ | ✓ | False |
| CKA_VERIFY_RECOVER    | ✗    | ✗ | ✗ | ✗ |       |
| CKA_WRAP              | ✗    | ✓ | ✗ | ✓ | False |
| CKA_WRAP_TEMPLATE     | ✗    | ✓ | ✗ | ✓ |       |
| CKA_TRUSTED           | ✗    | ✓ | ✗ | ✓ | False |
| CKA_WRAP_WITH_TRUSTED | ✓    | ✗ | ✓ | ✗ | False |
| CKA_UNWRAP            | ✓    | ✗ | ✓ | ✗ | False |

| 屬性                    | 金鑰類型           |   |                |                | 預設值  |
|-----------------------|----------------|---|----------------|----------------|------|
| CKA_UNWRAP_TEMPLATE   | ✓              | ✗ | ✓              | ✗              |      |
| CKA_SENSITIVE         | ✓ <sup>1</sup> | ✗ | ✓ <sup>1</sup> | ✗              | True |
| CKA_ALWAYS_SENSITIVE  | R              | ✗ | R              | ✗              |      |
| CKA_EXTRACTABLE       | ✓              | ✗ | ✓              | ✗              | True |
| CKA_NEVER_EXTRACTABLE | R              | ✗ | R              | ✗              |      |
| CKA_MODULUS           | ✗              | ✗ | ✗              | ✗              |      |
| CKA_MODULUS_BITS      | ✗              | ✗ | ✗              | ✓ <sup>2</sup> |      |
| CKA_PRIME_1           | ✗              | ✗ | ✗              | ✗              |      |
| CKA_PRIME_2           | ✗              | ✗ | ✗              | ✗              |      |
| CKA_COEFFICIENT       | ✗              | ✗ | ✗              | ✗              |      |
| CKA_EXPONENT_1        | ✗              | ✗ | ✗              | ✗              |      |

| 屬性                   | 金鑰類型 |                |   |                | 預設值 |
|----------------------|------|----------------|---|----------------|-----|
| CKA_EXPONENT_2       | ×    | ×              | × | ×              |     |
| CKA_PRIVATE_EXPONENT | ×    | ×              | × | ×              |     |
| CKA_PUBLIC_EXPONENT  | ×    | ×              | × | ✓ <sup>2</sup> |     |
| CKA_EC_PARAMS        | ×    | ✓ <sup>2</sup> | × | ×              |     |
| CKA_EC_POINT         | ×    | ×              | × | ×              |     |
| CKA_VALUE            | ×    | ×              | × | ×              |     |
| CKA_VALUE_LEN        | ×    | ×              | × | ×              |     |
| CKA_CHECK_VALUE      | R    | R              | R | R              |     |

## GenerateKey

| 屬性           | 金鑰類型 |      |      | 預設值 |
|--------------|------|------|------|-----|
|              | AES  | DES3 | 一般機密 |     |
| CKA_CLASS    | ✓    | ✓    | ✓    |     |
| CKA_KEY_TYPE | ✓    | ✓    | ✓    |     |

| 屬性                 | 金鑰類型 |                |                | 預設值            |
|--------------------|------|----------------|----------------|----------------|
| CKA_LABEL          |      | ✓              | ✓              | ✓              |
| CKA_ID             |      | ✓              | ✓              | ✓              |
| CKA_LOCAL          |      | R              | R              | R              |
| CKA_TOKEN          |      | ✓              | ✓              | ✓              |
| CKA_PRIVATE        |      | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> |
| CKA_ENCRYPT        |      | ✓              | ✓              | ✗              |
| CKA_DECRYPT        |      | ✓              | ✓              | ✗              |
| CKA_DERIVE         |      | ✓              | ✓              | ✓              |
| CKA_MODIFIABLE     |      | ✓              | ✓              | ✓              |
| CKA_DESTROYABLE    |      | ✓              | ✓              | ✓              |
| CKA_SIGN           |      | ✓              | ✓              | ✓              |
| CKA_SIGN_RECOVER   |      | ✗              | ✗              | ✗              |
| CKA_VERIFY         |      | ✓              | ✓              | ✓              |
| CKA_VERIFY_RECOVER |      | ✗              | ✗              | ✗              |

| 屬性                    | 金鑰類型 |   |   |   | 預設值   |
|-----------------------|------|---|---|---|-------|
| CKA_WRAP              |      | ✓ | ✓ | ✗ | False |
| CKA_WRAP_TEMPLATE     |      | ✓ | ✓ | ✗ |       |
| CKA_TRUSTED           |      | ✓ | ✓ | ✗ | False |
| CKA_WRAP_WITH_TRUSTED |      | ✓ | ✓ | ✓ | False |
| CKA_UNWRAP            |      | ✓ | ✓ | ✗ | False |
| CKA_UNWRAP_TEMPLATE   |      | ✓ | ✓ | ✗ |       |
| CKA_SENSITIVE         |      | ✓ | ✓ | ✓ | True  |
| CKA_ALWAYS_SENSITIVE  |      | ✗ | ✗ | ✗ |       |
| CKA_EXTRACTABLE       |      | ✓ | ✓ | ✓ | True  |
| CKA_NEVER_EXTRACTABLE |      | R | R | R |       |
| CKA_MODULUS           |      | ✗ | ✗ | ✗ |       |

| 屬性                   | 金鑰類型           |   |                | 預設值 |
|----------------------|----------------|---|----------------|-----|
| CKA_MODULUS_BITS     | ×              | × | ×              |     |
| CKA_PRIME_1          | ×              | × | ×              |     |
| CKA_PRIME_2          | ×              | × | ×              |     |
| CKA_COEFFICIENT      | ×              | × | ×              |     |
| CKA_EXPONENT_1       | ×              | × | ×              |     |
| CKA_EXPONENT_2       | ×              | × | ×              |     |
| CKA_PRIVATE_EXPONENT | ×              | × | ×              |     |
| CKA_PUBLIC_EXPONENT  | ×              | × | ×              |     |
| CKA_EC_PARAMS        | ×              | × | ×              |     |
| CKA_EC_POINT         | ×              | × | ×              |     |
| CKA_VALUE            | ×              | × | ×              |     |
| CKA_VALUE_LEN        | ✓ <sup>2</sup> | × | ✓ <sup>2</sup> |     |



| 屬性              | 金鑰類型 |   |   | 預設值 |
|-----------------|------|---|---|-----|
| CKA_CHECK_VALUE | R    | R | R |     |

## CreateObject

| 屬性           | 金鑰類型           |                |                 |                 |                |                |                | 預設值   |
|--------------|----------------|----------------|-----------------|-----------------|----------------|----------------|----------------|-------|
|              | EC 私<br>有金鑰    | EC 公<br>有金鑰    | RSA<br>私有<br>金鑰 | RSA<br>公有<br>金鑰 | AES            | DES3           | 一般<br>機密       |       |
| CKA_CLASS    | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup>  | ✓ <sup>2</sup>  | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_KEY_TYPE | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup>  | ✓ <sup>2</sup>  | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_LABEL    | ✓              | ✓              | ✓               | ✓               | ✓              | ✓              | ✓              |       |
| CKA_ID       | ✓              | ✓              | ✓               | ✓               | ✓              | ✓              | ✓              |       |
| CKA_LOCAL    | R              | R              | R               | R               | R              | R              | R              | False |
| CKA_TOKEN    | ✓              | ✓              | ✓               | ✓               | ✓              | ✓              | ✓              | False |
| CKA_PRIVATE  | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup>  | ✓ <sup>1</sup>  | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_ENCRYPT  | ✗              | ✗              | ✗               | ✓               | ✓              | ✓              | ✗              | False |
| CKA_DECRYPT  | ✗              | ✗              | ✓               | ✗               | ✓              | ✓              | ✗              | False |

| 屬性                    | 金鑰類型 |   |   |   |   |   |   | 預設值   |
|-----------------------|------|---|---|---|---|---|---|-------|
| CKA_DERIVE            | ✓    | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | False |
| CKA_MODIFIABLE        | ✓    | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | True  |
| CKA_DESTRUCTOYABLE    | ✓    | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | True  |
| CKA_SIGN              | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | False |
| CKA_SIGN_RECOVER      | ✗    | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | False |
| CKA_VERIFY            | ✗    | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | False |
| CKA_VERIFY_RECOVER    | ✗    | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |       |
| CKA_WRAP              | ✗    | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ | False |
| CKA_WRAP_TEMPLATE     | ✗    | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |       |
| CKA_TRUSTED           | ✗    | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | False |
| CKA_WRAP_WITH_TRUSTED | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | False |
| CKA_UNWRAP            | ✗    | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | False |

| 屬性                    | 金鑰類型 |   |                |                |   |   |   | 預設值  |
|-----------------------|------|---|----------------|----------------|---|---|---|------|
| CKA_UNWRAP_TEMPLATE   | ✓    | ✗ | ✓              | ✗              | ✓ | ✓ | ✗ |      |
| CKA_SENSITIVE         | ✓    | ✗ | ✓              | ✗              | ✓ | ✓ | ✓ | True |
| CKA_ALWAYS_SENSITIVE  | R    | ✗ | R              | ✗              | R | R | R |      |
| CKA_EXTRACTABLE       | ✓    | ✗ | ✓              | ✗              | ✓ | ✓ | ✓ | True |
| CKA_NEVER_EXTRACTABLE | R    | ✗ | R              | ✗              | R | R | R |      |
| CKA_MODULUS           | ✗    | ✗ | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✗ | ✗ | ✗ |      |
| CKA_MODULUS_BITS      | ✗    | ✗ | ✗              | ✗              | ✗ | ✗ | ✗ |      |
| CKA_PRIME_1           | ✗    | ✗ | ✓              | ✗              | ✗ | ✗ | ✗ |      |
| CKA_PRIME_2           | ✗    | ✗ | ✓              | ✗              | ✗ | ✗ | ✗ |      |
| CKA_COEFFICIENT       | ✗    | ✗ | ✓              | ✗              | ✗ | ✗ | ✗ |      |
| CKA_EXPONENT_1        | ✗    | ✗ | ✓              | ✗              | ✗ | ✗ | ✗ |      |

| 屬性                   | 金鑰類型           |                |                |                |                |                |                | 預設值 |
|----------------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|-----|
| CKA_EXPONENT_2       | ×              | ×              | ✓              | ×              | ×              | ×              | ×              |     |
| CKA_PRIVATE_EXPONENT | ×              | ×              | ✓ <sup>2</sup> | ×              | ×              | ×              | ×              |     |
| CKA_PUBLIC_EXPONENT  | ×              | ×              | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ×              | ×              | ×              |     |
| CKA_EC_PARAMS        | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ×              | ×              | ×              | ×              | ×              |     |
| CKA_EC_POINT         | ×              | ✓ <sup>2</sup> | ×              | ×              | ×              | ×              | ×              |     |
| CKA_VALUE            | ✓ <sup>2</sup> | ×              | ×              | ×              | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |     |
| CKA_VALUE_LEN        | ×              | ×              | ×              | ×              | ×              | ×              | ×              |     |
| CKA_CHECK_VALUE      | R              | R              | R              | R              | R              | R              | R              |     |

## UnwrapKey

| 屬性        | 金鑰類型 |                |                |                |                |                | 預設值 |
|-----------|------|----------------|----------------|----------------|----------------|----------------|-----|
|           |      | EC 私<br>有金鑰    | RSA 私<br>有金鑰   | AES            | DES3           | 一般機密           |     |
| CKA_CLASS |      | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |     |

| 屬性               | 金鑰類型           |                |                |                |                | 預設值   |
|------------------|----------------|----------------|----------------|----------------|----------------|-------|
| CKA_KEY_TYPE     | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_LABEL        | ✓              | ✓              | ✓              | ✓              | ✓              |       |
| CKA_ID           | ✓              | ✓              | ✓              | ✓              | ✓              |       |
| CKA_LOCAL        | R              | R              | R              | R              | R              | False |
| CKA_TOKEN        | ✓              | ✓              | ✓              | ✓              | ✓              | False |
| CKA_PRIVATE      | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_ENCRYPT      | ✗              | ✗              | ✓              | ✓              | ✗              | False |
| CKA_DECRYPT      | ✗              | ✓              | ✓              | ✓              | ✗              | False |
| CKA_DERIVE       | ✓              | ✓              | ✓              | ✓              | ✓              | False |
| CKA_MODIFIABLE   | ✓              | ✓              | ✓              | ✓              | ✓              | True  |
| CKA_DESTROYABLE  | ✓              | ✓              | ✓              | ✓              | ✓              | True  |
| CKA_SIGN         | ✓              | ✓              | ✓              | ✓              | ✓              | False |
| CKA_SIGN_RECOVER | ✗              | ✗              | ✗              | ✗              | ✗              | False |

| 屬性                    | 金鑰類型 |   |   |   |   |   | 預設值   |
|-----------------------|------|---|---|---|---|---|-------|
| CKA_VERIFY            |      | × | × | ✓ | ✓ | ✓ | False |
| CKA_VERIFY_RECOVER    |      | × | × | × | × | × |       |
| CKA_WRAP              |      | × | × | ✓ | ✓ | × | False |
| CKA_UNWRAP            |      | × | ✓ | ✓ | ✓ | × | False |
| CKA_SENSITIVE         |      | ✓ | ✓ | ✓ | ✓ | ✓ | True  |
| CKA_EXTRACTABLE       |      | ✓ | ✓ | ✓ | ✓ | ✓ | True  |
| CKA_NEVER_EXTRACTABLE |      | R | R | R | R | R |       |
| CKA_ALWAYS_SENSITIVE  |      | R | R | R | R | R |       |
| CKA_MODULUS           |      | × | × | × | × | × |       |
| CKA_MODULUS_BITS      |      | × | × | × | × | × |       |
| CKA_PRIME_1           |      | × | × | × | × | × |       |
| CKA_PRIME_2           |      | × | × | × | × | × |       |

| 屬性                   | 金鑰類型 |   |   |   |   | 預設值 |
|----------------------|------|---|---|---|---|-----|
| CKA_COEFFICIENT      | ×    | × | × | × | × |     |
| CKA_EXPONENT_1       | ×    | × | × | × | × |     |
| CKA_EXPONENT_2       | ×    | × | × | × | × |     |
| CKA_PRIVATE_EXPONENT | ×    | × | × | × | × |     |
| CKA_PUBLIC_EXPONENT  | ×    | × | × | × | × |     |
| CKA_EC_PARAMS        | ×    | × | × | × | × |     |
| CKA_EC_POINT         | ×    | × | × | × | × |     |
| CKA_VALUE            | ×    | × | × | × | × |     |
| CKA_VALUE_LEN        | ×    | × | × | × | × |     |
| CKA_CHECK_VALUE      | R    | R | R | R | R |     |

## DeriveKey

| 屬性              | 金鑰類型           |                |                | 預設值   |
|-----------------|----------------|----------------|----------------|-------|
|                 | AES            | DES3           | 一般機密           |       |
| CKA_CLASS       | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_KEY_TYPE    | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_LABEL       | ✓              | ✓              | ✓              |       |
| CKA_ID          | ✓              | ✓              | ✓              |       |
| CKA_LOCAL       | R              | R              | R              | True  |
| CKA_TOKEN       | ✓              | ✓              | ✓              | False |
| CKA_PRIVATE     | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_ENCRYPT     | ✓              | ✓              | ✗              | False |
| CKA_DECRYPT     | ✓              | ✓              | ✗              | False |
| CKA_DERIVE      | ✓              | ✓              | ✓              | False |
| CKA_MODIFIABLE  | ✓              | ✓              | ✓              | True  |
| CKA_DESTROYABLE | ✓              | ✓              | ✓              | True  |
| CKA_SIGN        | ✓              | ✓              | ✓              | False |



| 屬性                    | 金鑰類型 |   |   | 預設值   |
|-----------------------|------|---|---|-------|
| CKA_SIGN_RECOVER      | ✗    | ✗ | ✗ |       |
| CKA_VERIFY            | ✓    | ✓ | ✓ | False |
| CKA_VERIFY_RECOVER    | ✗    | ✗ | ✗ |       |
| CKA_WRAP              | ✓    | ✓ | ✗ | False |
| CKA_UNWRAP            | ✓    | ✓ | ✗ | False |
| CKA_SENSITIVE         | R    | R | R | True  |
| CKA_EXTRACTABLE       | ✓    | ✓ | ✓ | True  |
| CKA_NEVER_EXTRACTABLE | R    | R | R |       |
| CKA_ALWAYS_SENSITIVE  | R    | R | R |       |
| CKA_MODULUS           | ✗    | ✗ | ✗ |       |
| CKA_MODULUS_BITS      | ✗    | ✗ | ✗ |       |
| CKA_PRIME_1           | ✗    | ✗ | ✗ |       |

| 屬性                   | 金鑰類型           |   |                | 預設值 |
|----------------------|----------------|---|----------------|-----|
| CKA_PRIME_2          | ×              | × | ×              |     |
| CKA_COEFFICIENT      | ×              | × | ×              |     |
| CKA_EXPONENT_1       | ×              | × | ×              |     |
| CKA_EXPONENT_2       | ×              | × | ×              |     |
| CKA_PRIVATE_EXPONENT | ×              | × | ×              |     |
| CKA_PUBLIC_EXPONENT  | ×              | × | ×              |     |
| CKA_EC_PARAMS        | ×              | × | ×              |     |
| CKA_EC_POINT         | ×              | × | ×              |     |
| CKA_VALUE            | ×              | × | ×              |     |
| CKA_VALUE_LEN        | ✓ <sup>2</sup> | × | ✓ <sup>2</sup> |     |
| CKA_CHECK_VALUE      | R              | R | R              |     |

## GetAttributeValue

| 屬性                 | 金鑰類型           |                |                |                |                |                |                |  |
|--------------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|--|
|                    | EC 私<br>有金鑰    | EC 公<br>有金鑰    | RSA 私<br>有金鑰   | RSA 公<br>有金鑰   | AES            | DES3           | 一般<br>機密       |  |
| CKA_CLASS          | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |  |
| CKA_KEY_T<br>YPE   | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |  |
| CKA_LABEL          | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |  |
| CKA_ID             | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |  |
| CKA_LOCAL          | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |  |
| CKA_TOKEN          | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |  |
| CKA_PRIVATE<br>TE  | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> |  |
| CKA_ENCRY<br>PT    | ✗              | ✗              | ✗              | ✓              | ✓              | ✓              | ✗              |  |
| CKA_DECRY<br>PT    | ✗              | ✗              | ✓              | ✗              | ✓              | ✓              | ✗              |  |
| CKA_DERIV<br>E     | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |  |
| CKA_MODIF<br>IABLE | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |  |

| 屬性                            | 金鑰類型 |   |   |   |   |   |   |
|-------------------------------|------|---|---|---|---|---|---|
| CKA_DESTR<br>OYABLE           | ✓    | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| CKA_SIGN                      | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| CKA_SIGN_<br>RECOVER          | ✗    | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| CKA_VERIF<br>Y                | ✗    | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| CKA_VERIF<br>Y_RECOVER        | ✗    | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| CKA_WRAP                      | ✗    | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ |
| CKA_WRAP_<br>TEMPLATE         | ✗    | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |
| CKA_TRUST<br>ED               | ✗    | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| CKA_WRAP_<br>WITH_TRUS<br>TED | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| CKA_UNWRA<br>P                | ✗    | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |
| CKA_UNWRA<br>P_TEMPLAT<br>E   | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |
| CKA_SENSI<br>TIVE             | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |

| 屬性                    | 金鑰類型 |   |   |   |   |   |   |
|-----------------------|------|---|---|---|---|---|---|
| CKA_EXTRA_CTABLE      | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| CKA_NEVER_EXTRACTABLE | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| CKA_ALWAYS_SENSITIVE  | R    | R | R | R | R | R | R |
| CKA_MODULUS           | ✗    | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ |
| CKA_MODULUS_BITS      | ✗    | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| CKA_PRIME_1           | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |
| CKA_PRIME_2           | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |
| CKA_COEFFICIENT       | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |
| CKA_EXPONENT_1        | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |
| CKA_EXPONENT_2        | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |
| CKA_PRIVATE_EXPONENT  | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |

| 屬性                  | 金鑰類型 |   |   |   |   |   |   |
|---------------------|------|---|---|---|---|---|---|
| CKA_PUBLIC_EXPONENT | ×    | × | ✓ | ✓ | × | × | × |
| CKA_EC_PARAMS       | ✓    | ✓ | × | × | × | × | × |
| CKA_EC_POINT        | ×    | ✓ | × | × | × | × | × |
| CKA_VALUE           | S    | × | × | × | ✓ | ✓ | ✓ |
| CKA_VALUE_LEN       | ×    | × | × | × | ✓ | × | ✓ |
| CKA_CHECK_VALUE     | ✓    | ✓ | ✓ | ✓ | ✓ | ✓ | × |

### 屬性註釋

- [1] 此屬性受韌體部分支援，且需明確設定為僅限預設值。
- [2] 必要屬性。

### 修改用戶端 SDK 5 的 AWS CloudHSM PKCS #11 程式庫屬性

物件的某些 PKCS #11 程式庫屬性 AWS CloudHSM 可以在建立物件後修改，而有些則無法修改。若要修改屬性，請使用 CloudHSM CLI 中的[金鑰 set-attribute](#) 命令。您也可以使用 CloudHSM CLI 的[金鑰清單](#)命令來衍生屬性清單。

下列清單會顯示物件建立後可修改的屬性：

- CKA\_LABEL
- CKA\_TOKEN

 Note

只有在將工作階段金鑰變更為符記金鑰時，才允許進行修改。使用 CloudHSM CLI 的 [金鑰 set-attribute](#) 命令來變更屬性值。

- CKA\_ENCRYPT
- CKA\_DECRYPT
- CKA\_SIGN
- CKA\_VERIFY
- CKA\_WRAP
- CKA\_UNWRAP
- CKA\_LABEL
- CKA\_SENSITIVE
- CKA\_DERIVE

 Note

這個屬性支援金鑰衍生。所有公有金鑰的屬性須為 False，不能設定為 True。如果是私密金鑰和 EC 私有金鑰，則該屬性可設定為 True 或 False。

- CKA\_TRUSTED

 Note

唯有加密管理員 (CO) 可將這個屬性設定成 True 或 False。

- CKA\_WRAP\_WITH\_TRUSTED

 Note

將此屬性套用於可匯出的資料金鑰，以表明只能使用標記為 CKA\_TRUSTED 的金鑰包裝此金鑰。一旦設定 CKA\_WRAP\_WITH\_TRUSTED 為 true，屬性就會變成唯讀，而且您無法變更或移除屬性。

## 解釋用戶端 SDK 5 的 AWS CloudHSM PKCS #11 程式庫錯誤代碼

在範本中指定特定金鑰不支援的 PKCS #11 程式庫屬性會導致錯誤。下表包含違反規格時所產生的錯誤代碼：

| 錯誤代碼                       | Description                                           |
|----------------------------|-------------------------------------------------------|
| CKR_TEMPLATE_INCONSISTENT  | 當您在屬性範本中指定的屬性符合 PKCS #11 規格，卻不受 CloudHSM 支援時，就會收到此錯誤。 |
| CKR_ATTRIBUTE_TYPE_INVALID | 當您擷取的屬性值符合 PKCS #11 規格，卻不受 CloudHSM 支援時，就會收到此錯誤。      |
| CKR_ATTRIBUTE_INCOMPLETE   | 當您沒有在屬性範本中指定必要屬性時，就會收到此錯誤。                            |
| CKR_ATTRIBUTE_READ_ONLY    | 當您在屬性範本中指定唯讀屬性時，就會收到此錯誤。                              |

## 用戶端 SDK AWS CloudHSM 5 的 PKCS #11 程式庫程式碼範例

GitHub 上的程式碼範例示範如何使用 AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫來完成基本任務。

### 先決條件

執行範例之前，請執行以下步驟來設定您的環境：

- 安裝並設定適用於用戶端 SDK 5 的 [PKCS #11 程式庫](#)。
- 設定[密碼編譯使用者 \(CU\)](#)。您的應用程式會使用此 HSM 帳戶在 HSM 上執行程式碼範例。

### 程式碼範例

適用於 PKCS#11 AWS CloudHSM 的軟體程式庫程式碼範例可在 [GitHub](#) 上取得。此儲存庫包括如何使用 PKCS #11 執行一般作業的範例，包括加密、解密、簽署和驗證。

- [產生金鑰 \(AES、RSA、EC\)](#)



- [列出金鑰屬性](#)
- [使用 AES GCM 加密和解密資料](#)
- [使用 AES\\_CTR 加密和解密資料](#)
- [使用 3DES 加密和解密資料](#)
- [使用 RSA 簽署和驗證資料](#)
- [使用 HMAC KDF 衍生金鑰](#)
- [使用以 PKCS #5 填補的 AES 包裝和取消包裝金鑰](#)
- [使用不填補的 AES 包裝和取消包裝金鑰](#)
- [使用零填補的 AES 包裝和取消包裝金鑰](#)
- [使用 AES-GCM 包裝和取消包裝金鑰](#)
- [使用 RSA 包裝和取消包裝金鑰](#)

## PKCS #11 程式庫的進階組態 AWS CloudHSM

AWS CloudHSM PKCS #11 供應商包含下列進階組態，這不屬於大多數客戶使用的一般組態。這些組態提供額外的功能。

- [使用 PKCS #11 連線到多個插槽](#)
- [PKCS #11 的重試組態](#)

### 適用於 的 PKCS #11 程式庫的多個槽組態 AWS CloudHSM

用戶端 SDK 5 PKCS #11 程式庫中的單一插槽代表 AWS CloudHSM 中叢集的單一連線。使用用戶端 SDK 5，您可以將 PKCS11 程式庫設定為允許多個插槽，從單一 PKCS #11 應用程式將使用者連線到多個 CloudHSM 叢集。

使用本主題中的說明，讓您的應用程式使用多插槽功能來連線到多個叢集。

### 主題

- [適用於 的 PKCS #11 程式庫的多槽先決條件 AWS CloudHSM](#)
- [針對 的多槽功能設定 PKCS #11 程式庫 AWS CloudHSM](#)
- [為 新增具有多插槽功能的叢集 AWS CloudHSM](#)
- [移除具有 多插槽功能的叢集 AWS CloudHSM](#)

## 適用於 的 PKCS #11 程式庫的多槽先決條件 AWS CloudHSM

為 PKCS #11 程式庫設定多個插槽之前 AWS CloudHSM，請完成下列先決條件。

- 您要連線的兩個或多個 AWS CloudHSM 叢集及其叢集憑證。
- 具有安全群組的 EC2 執行個體正確設定為連線到上述所有叢集。如需如何設定叢集和用戶端執行個體的詳細資訊，請參閱 [入門 AWS CloudHSM](#)。
- 若要設定多插槽功能，您必須已下載並安裝 PKCS #11 程式庫。若您尚未完成此動作，請參閱 [???](#) 中的說明。

## 針對 的多槽功能設定 PKCS #11 程式庫 AWS CloudHSM

若要為 設定多槽功能的 PKCS #11 程式庫 AWS CloudHSM，請遵循下列步驟：

1. 使用多插槽功能識別要連線到的叢集。
2. 依照 [???](#) 中的說明，將這些叢集新增至 PKCS #11 組態
3. PKCS #11 應用程式下次執行時，其將具有多插槽功能。

## 為 新增具有多插槽功能的叢集 AWS CloudHSM

[使用 PKCS #11 for 連線至多個插槽](#)時 AWS CloudHSM，請使用 `configure-pkcs11 add-cluster` 命令將叢集新增至您的組態。

### 語法

```
configure-pkcs11 add-cluster [OPTIONS]
 --cluster-id <CLUSTER ID>
 [--region <REGION>]
 [--endpoint <ENDPOINT>]
 [--hsm-ca-cert <HSM CA CERTIFICATE FILE>]
 [--client-cert-hsm-tls-file <CLIENT CERTIFICATE FILE>]
 [--client-key-hsm-tls-file <CLIENT KEY FILE>]
 [-h, --help]
```

## 範例

### 使用 **cluster-id** 參數新增叢集

#### Example

搭配使用 `configure-pkcs11 add-cluster` 和 `cluster-id` 參數，將叢集 (ID 為 `cluster-1234567`) 新增至您的組態。

#### Linux

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 add-cluster --cluster-id <cluster-1234567>
```

#### Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" add-cluster --cluster-id <cluster-1234567>
```

#### Tip

如果 `configure-pkcs11 add-cluster` 與 `cluster-id` 參數搭配使用不會導致新增叢集，請參閱下列範例，以取得此命令的更長版本，此命令也需要 `--region` 和 `--endpoint` 參數來識別要新增的叢集。例如，如果叢集區域與設定為 AWS CLI 預設值的區域不同，則應使用 `--region` 參數來使用正確的區域。此外，您可以指定用於呼叫的 AWS CloudHSM API 端點，這對於各種網路設定而言可能是必要的，例如使用不使用預設 DNS 主機名稱的 VPC 介面端點 AWS CloudHSM。

### 使用 **cluster-id**、**endpoint** 和 **region** 參數新增叢集

#### Example

搭配使用 `configure-pkcs11 add-cluster` 以及 `cluster-id`、`endpoint` 和 `region` 參數將叢集 (ID 為 `cluster-1234567`) 新增至您的組態。

#### Linux

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 add-cluster --cluster-id <cluster-1234567>
--region <us-east-1> --endpoint <https://cloudhsmv2.us-east-1.amazonaws.com>
```

## Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" add-cluster --
cluster-id <cluster-1234567>--region <us-east-1> --endpoint <https://cloudhsmv2.us-
east-1.amazonaws.com>
```

如需 --cluster-id、--region 和 --endpoint 參數的詳細資訊，請參閱 [the section called “參數”](#)。

## 參數

--cluster-id **<Cluster ID>**

進行 DescribeClusters 呼叫以尋找叢集中與叢集 ID 關聯的所有 HSM 彈性網路介面 (ENI) IP 地址。系統會將 ENI IP 地址新增至 AWS CloudHSM 組態檔案。

### Note

如果您在無法存取公有網際網路的 VPC 中使用來自 EC2 執行個體的 --cluster-id 參數，則必須建立要連線的介面 VPC 端點 AWS CloudHSM。如需 VPC 端點的詳細資訊，請參閱 [???](#)。

必要：是

--endpoint **<Endpoint>**

指定用於進行 DescribeClusters 呼叫的 AWS CloudHSM API 端點。您必須結合 --cluster-id 設定此選項。

必要：否

--hsm-ca-cert **<HsmCA Certificate Filepath>**

指定 HSM CA 憑證的檔案路徑。

必要：否

`--region` *<Region>*

指您叢集的區域。您必須結合 `--cluster-id` 設定此選項。

如果您未提供 `--region` 參數，系統會嘗試讀取 `AWS_DEFAULT_REGION` 或 `AWS_REGION` 環境變數來選擇區域。如果未設定這些變數，則除非您在 `AWS_CONFIG_FILE` 環境變數中指定了不同的檔案，否則系統會檢查 AWS config 檔案中 (通常是 `~/.aws/config`) 與您的設定檔相關聯的區域。如果未設定上述任何變數，系統會預設為 `us-east-1` 區域。

必要：否

`--client-cert-hsm-tls-file` *<client certificate hsm tls ###>*

用於 TLS 用戶端-HSM 交互身分驗證的用戶端憑證路徑。

只有在您已使用 CloudHSM CLI 在 HSM 上註冊至少一個信任錨點時，才使用此選項。您必須結合 `--client-key-hsm-tls-file` 設定此選項。

必要：否

`--client-key-hsm-tls-file` *<client key hsm tls ###>*

用於 TLS 用戶端-HSM 交互身分驗證的用戶端金鑰路徑。

只有在您已使用 CloudHSM CLI 在 HSM 上註冊至少一個信任錨點時，才使用此選項。您必須結合 `--client-cert-hsm-tls-file` 設定此選項。

必要：否

移除具有 多插槽功能的叢集 AWS CloudHSM

[使用 PKCS #11 連線到多個插槽](#)時，請使用 `configure-pkcs11 remove-cluster` 命令從可用的 PKCS #11 插槽中移除叢集。

語法

```
configure-pkcs11 remove-cluster [OPTIONS]
 --cluster-id <CLUSTER ID>
 [-h, --help]
```

## 範例

### 使用 **cluster-id** 參數移除叢集

#### Example

搭配使用 `configure-pkcs11 remove-cluster` 和 `cluster-id` 參數，從您的組態中移除叢集 (ID 為 `cluster-1234567`)。

#### Linux

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 remove-cluster --cluster-id <cluster-1234567>
```

#### Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" remove-cluster --cluster-id <cluster-1234567>
```

如需 `--cluster-id` 參數的詳細資訊，請參閱 [the section called “參數”](#)。

#### 參數

`--cluster-id` **<Cluster ID>**

需從組態中移除的叢集的 ID

必要：是

#### 的 PKCS #11 程式庫重試命令 AWS CloudHSM

AWS CloudHSM 用戶端 SDK 5.8.0 和更新版本具有內建的自動重試策略，將從用戶端重試 HSM 限流操作。當 HSM 因過於忙於執行先前操作而無法接受更多要求而限制操作時，用戶端 SDK 會嘗試重試限流操作 (最多 3 次)，同時以指數形式回退。此自動重試策略可以設定為兩種模式中的其中一種：關閉模式和標準模式。

- 關閉：用戶端 SDK 將不會針對 HSM 的任何限流操作執行任何重試政策。
- 標準：這是用戶端 SDK 5.8.0 及更新版本的預設模式。在此模式下，用戶端 SDK 會以指數回退形式自動重試限流操作。

如需詳細資訊，請參閱[HSM 調節](#)。

將重試命令設定為關閉模式

## Linux

將 Linux 上用戶端 SDK 5 重試命令設定為 off

- 您可以使用下列命令將重試組態設定為 off 模式：

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --default-retry-mode off
```

## Windows

將 Windows 上用戶端 SDK 5 重試命令設定為 off

- 您可以使用下列命令將重試組態設定為 off 模式：

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" --default-retry-mode off
```

## 具有 PKCS #11 程式庫的憑證儲存

AWS CloudHSM PKCS #11 程式庫支援將公有金鑰憑證儲存為 hsm2m.medium 叢集上的「公有物件」（如 PKCS #11 2.40 所定義）。此功能允許公有和私有 PKCS #11 工作階段建立、擷取、修改和刪除公有金鑰憑證。

若要搭配 PKCS #11 程式庫使用憑證儲存，您需要在用戶端組態中啟用它。啟用後，您可以從 PKCS #11 應用程式管理憑證物件。同時套用到憑證和金鑰物件的操作，例如 [C\\_FindObjects](#)，將會傳回金鑰和憑證儲存的結果。

## 主題

- [啟用憑證儲存](#)
- [憑證儲存 API 操作](#)

- [憑證儲存屬性](#)
- [憑證儲存稽核日誌](#)

## 啟用憑證儲存

您可以使用 PKCS #11 程式庫組態工具，在 hsm2m.medium 叢集上啟用憑證儲存。此功能適用於 SDK 5.13 版和更新版本。如需支援憑證物件類型的操作清單，請參閱 [憑證儲存 API 操作](#)。

若要啟用憑證儲存，請依照下列步驟操作您的作業系統：

### Linux

- 啟用憑證儲存

執行以下命令：

```
$ sudo /opt/cloudhsm/bin/configure-pkcs11 --enable-certificate-storage
```

### Windows

- 啟用憑證儲存

開啟命令提示字元並執行下列命令：

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-pkcs11.exe" --enable-certificate-storage
```

## 憑證儲存 API 操作

下列 PKCS #11 操作支援憑證物件類型 (CKO\_CERTIFICATE)：

### 一般憑證操作

#### **C\_CreateObject**

建立新的憑證物件。

#### **C\_DestroyObject**

刪除現有的憑證物件。



## C\_GetAttributeValue

取得憑證物件的一或多個屬性的值。

## C\_SetAttributeValue

更新憑證物件的一或多個屬性的值。

## 憑證物件搜尋操作

## C\_FindObjectsInit

開始搜尋憑證物件。

## C\_FindObjects

繼續搜尋憑證物件。

## C\_FindObjectsFinal

結束憑證物件的搜尋。

## 憑證儲存屬性

下表列出支援的憑證物件屬性及其值：

| 屬性              | 預設值   | 描述                    |
|-----------------|-------|-----------------------|
| CKA_CLASS       | 必要    | 必須為 CKO_CERTIFICATE 。 |
| CKA_TOKEN       | True  | 必須為 True。             |
| CKA_MODIFIABLE  | True  | 必須為 True。             |
| CKA_PRIVATE     | False | 必須為 False。            |
| CKA_LABEL       | 空白    | 限制 127 個字元。           |
| CKA_COPYABLE    | False | 必須為 False。            |
| CKA_DESTROYABLE | True  | 必須為 True。             |

| 屬性                       | 預設值                                 | 描述                                        |
|--------------------------|-------------------------------------|-------------------------------------------|
| CKA_CERTIFICATE_TYPE     | 必要                                  | 必須為 CKC_X_509 。                           |
| CKA_TRUSTED              | False                               | 必須為 False。                                |
| CKA_CERTIFICATE_CATEGORY | CK_CERTIFICATE_CATEGORY_UNSPECIFIED | 必須為 CK_CERTIFICATE_CATEGORY_UNSPECIFIED 。 |
| CKA_CHECK_VALUE          | 衍生自 CKA_VALUE                       | 根據 自動設定 CKA_VALUE 。                       |
| CKA_START_DATE           | 空白                                  | 憑證 'not before' date。                     |
| CKA_END_DATE             | 空白                                  | 憑證 'not after' date。                      |
| CKA_PUBLIC_KEY_INFO      | 空白                                  | 大小上限為 16 KB。                              |
| CKA_SUBJECT              | 必要                                  | 憑證主體。                                     |
| CKA_ID                   | 空白                                  | 大小上限為 128 個位元組。不強制執行唯一性。                  |
| CKA_ISSUER               | 空白                                  | 憑證發行者。                                    |
| CKA_SERIAL_NUMBER        | 空白                                  | 憑證序號。                                     |
| CKA_VALUE                | 必要                                  | 大小上限為 32 KB。                              |

## 憑證儲存稽核日誌

AWS CloudHSM 會寫入憑證儲存操作的稽核日誌，以將資料修改為叢集 Amazon CloudWatch CloudWatch Events 日誌串流。此日誌串流是針對叢集命名，而不是針對叢集中的特定 HSM。

如需有關在 CloudWatch 中存取稽核日誌的資訊，請參閱 [使用 Amazon CloudWatch Logs 和 AWS CloudHSM Audit Logs](#)。

## 日誌項目欄位

### object\_handle

憑證物件的唯一識別符。

### op\_code

執行或嘗試的操作。可能的值如下：

- CreateObject
- DestroyObject
- SetAttributeValues

### response

OK 如果操作成功，或下列其中一個錯誤類型：

- DuplicateAttribute
- InvalidAttributeValue
- ObjectNotFound
- MaxObjectsReached
- InternalFailure

### attributes

已修改屬性，如果有的話。

### timestamp

操作發生的時間，以 Unix epoch 後的毫秒為單位。

## 稽核日誌範例

### CreateObject 範例

```
{
 "object_handle": 463180677312929947,
 "op_code": "CreateObject",
 "response": "OK",
 "attributes": null,
 "timestamp": 1725482483671
}
```

## DestroyObject 範例

```
{
 "object_handle": 463180677312929947,
 "op_code": "DestroyObject",
 "response": "OK",
 "attributes": null,
 "timestamp": 1725482484559
}
```

## SetAttributeValues 範例

```
{
 "object_handle": 463180678453346687,
 "op_code": "SetAttributeValues",
 "response": "OK",
 "attributes": [
 "Label"
],
 "timestamp": 1725482488004
}
```

## 不成功的 CreateObject 範例

```
{
 "object_handle": null,
 "op_code": "CreateObject",
 "response": "MaxObjectsReached",
 "attributes": null,
 "timestamp": 1726084937125
}
```

## 適用於 AWS CloudHSM 用戶端 SDK 5 的 OpenSSL 動態引擎

AWS CloudHSM OpenSSL 動態引擎可讓您透過 OpenSSL API 將密碼編譯操作卸載至 CloudHSM 叢集。

AWS CloudHSM 提供 OpenSSL 動態引擎，您可以在 [AWS CloudHSM 使用 Tomcat 搭配 JSSE 在 Linux 上卸載 SSL/TLS](#) 或 中閱讀相關文章 [AWS CloudHSM 使用 NGINX 或 Apache 搭配 OpenSSL 在 Linux 上卸載 SSL/TLS](#)。如需 AWS CloudHSM 搭配 OpenSSL 使用的範例，請參閱 [此 AWS 安全部落](#)

格。如需關於 SDK 平台支援的詳細資訊，請參閱 [the section called “支援平台”](#)。如需故障診斷，請參閱 [適用於的 OpenSSL 動態引擎的已知問題 AWS CloudHSM](#)。

使用下列各節，使用用戶端 SDK 5 安裝和設定 OpenSSL 的 AWS CloudHSM 動態引擎。

如需關於使用用戶端 SDK 3 的資訊，請參閱 [使用先前的 SDK 版本來使用 AWS CloudHSM](#)。

## 主題

- [安裝適用於用戶端 SDK 5 的 AWS CloudHSM OpenSSL 動態引擎](#)
- [用戶端 SDK 5 的 OpenSSL 動態引擎 AWS CloudHSM 支援的金鑰類型](#)
- [用戶端 SDK 5 的 OpenSSL 動態引擎 AWS CloudHSM 支援機制](#)
- [適用於的 OpenSSL 進階組態 AWS CloudHSM](#)

## 安裝適用於用戶端 SDK 5 的 AWS CloudHSM OpenSSL 動態引擎

使用下列章節安裝適用於 AWS CloudHSM 用戶端 SDK 5 的 OpenSSL 動態引擎。

### Note

若要使用用戶端 SDK 5 執行單一 HSM 叢集，您必須先將 `disable_key_availability_check` 設定為 `True` 來管理用戶端金鑰持久性。如需詳細資訊，請參閱 [金鑰同步處理](#) 和 [用戶端 SDK 5 設定工具](#)。

## 安裝和設定 OpenSSL 動態引擎

1. 使用以下命令來下載和安裝 OpenSSL 引擎。

### Amazon Linux 2023

在 x86\_64 架構上安裝適用於 Amazon Linux 2023 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-dyn-latest.amzn2023.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-dyn-latest.amzn2023.x86_64.rpm
```

在 ARM64 架構上安裝適用於 Amazon Linux 2023 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-dyn-latest.amzn2023.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-dyn-latest.amzn2023.aarch64.rpm
```

## Amazon Linux 2

在 x86\_64 架構上安裝適用於 Amazon Linux 2 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-dyn-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-dyn-latest.el7.x86_64.rpm
```

在 ARM64 架構上安裝適用於 Amazon Linux 2 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-dyn-latest.el7.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-dyn-latest.el7.aarch64.rpm
```

## RHEL 9 (9.2+)

在 x86\_64 架構上安裝適用於 RHEL 9 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-dyn-latest.el9.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-dyn-latest.el9.x86_64.rpm
```

在 ARM64 架構上安裝適用於 RHEL 9 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-dyn-latest.el9.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-dyn-latest.el9.aarch64.rpm
```

## RHEL 8 (8.3+)

在 x86\_64 架構上安裝適用於 RHEL 8 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-dyn-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-dyn-latest.el8.x86_64.rpm
```

## Ubuntu 24.04 LTS

在 x86\_64 架構上安裝適用於 Ubuntu 24.04 LTS 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/cloudhsm-dyn_latest_u24.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-dyn_latest_u24.04_amd64.deb
```

在 ARM64 架構上安裝適用於 Ubuntu 24.04 LTS 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/cloudhsm-dyn_latest_u24.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-dyn_latest_u24.04_arm64.deb
```

## Ubuntu 22.04 LTS

在 x86\_64 架構上安裝適用於 Ubuntu 22.04 LTS 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/cloudhsm-dyn_latest_u22.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-dyn_latest_u22.04_amd64.deb
```

在 ARM64 架構上安裝適用於 Ubuntu 22.04 LTS 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/cloudhsm-dyn_latest_u22.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-dyn_latest_u22.04_arm64.deb
```

## Ubuntu 20.04 LTS

在 x86\_64 架構上安裝適用於 Ubuntu 20.04 LTS 的 OpenSSL 動態引擎：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Focal/cloudhsm-dyn_latest_u20.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-dyn_latest_u20.04_amd64.deb
```

您已在 `/opt/cloudhsm/lib/libcloudhsm_openssl_engine.so` 中安裝動態引擎的共用程式庫。

2. 引導用戶端 SDK 5。如需關於啟動程序的詳細資訊，請參閱 [引導用戶端 SDK](#)。
3. 使用加密使用者 (CU) 的憑證設定環境變數。如需關於建立 CU 的資訊，請參閱 [使用 CMU 進行使用者管理](#)。

```
$ export CLOUDHSM_PIN=<HSM user name>:<password>
```

### Note

用戶端 SDK 5 引入了用於存儲 CU 憑證的 CLOUDHSM\_PIN 環境變量。在用戶端 SDK 3 中，您可以將 CU 憑證儲存在 `n3fips_password` 環境變數中。用戶端 SDK 5 支援這兩個環境變數，但建議使用 CLOUDHSM\_PIN。

4. 將您的 OpenSSL 動態引擎連接到叢集。如需詳細資訊，請參閱 [連接至叢集](#)。
5. 引導用戶端 SDK 5。如需詳細資訊，請參閱 [the section called “引導用戶端 SDK”](#)。



## 驗證用戶端 SDK 5 OpenSSL 的動態引擎

使用下面的命令來驗證您的 OpenSSL 動態引擎的安裝。

```
$ openssl engine -t cloudhsm
```

下列輸出會驗證組態：

```
(cloudhsm) CloudHSM OpenSSL Engine
[available]
```

## 用戶端 SDK 5 的 OpenSSL 動態引擎 AWS CloudHSM 支援的金鑰類型

AWS CloudHSM OpenSSL 動態引擎支援用戶端 SDK 5 的下列金鑰類型。

| 金鑰類型 | 描述                                                                                                                    |
|------|-----------------------------------------------------------------------------------------------------------------------|
| EC   | 對 P-256、P-384 和 secp256k1 金鑰類型進行 ECDSA 簽署/驗證。若要產生可與 OpenSSL 引擎互通的 EC 金鑰，請參閱 <a href="#">使用 CloudHSM CLI 匯出非對稱金鑰</a> 。 |
| RSA  | 2048、3072 和 4096 位元金鑰的 RSA 金鑰產生。RSA 簽署/驗證。驗證程序已卸載到 OpenSSL 軟件中。                                                       |

## 用戶端 SDK 5 的 OpenSSL 動態引擎 AWS CloudHSM 支援機制

AWS CloudHSM OpenSSL 動態引擎支援使用用戶端 SDK 5 簽署和驗證函數的下列機制。

### 簽署和驗證函數

使用用戶端 SDK 5，資料會在軟體中進行本機雜湊處理。這表示可以雜湊的資料大小沒有限制。

### RSA 簽章類型

- SHA1withRSA
- SHA224withRSA
- SHA256withRSA

- SHA384withRSA
- SHA512withRSA

## ECDSA 簽章類型

- SHA1withECDSA
- SHA224withECDSA
- SHA256withECDSA
- SHA384withECDSA
- SHA512withECDSA

## 適用於的 OpenSSL 進階組態 AWS CloudHSM

AWS CloudHSM OpenSSL 提供者包含下列進階組態，這不屬於大多數客戶使用的一般組態。這些組態提供額外的功能。

- [適用於 OpenSSL 的重試命令](#)

### 的 OpenSSL 重試命令 AWS CloudHSM

AWS CloudHSM 用戶端 SDK 5.8.0 和更新版本具有內建的自動重試策略，將從用戶端重試 HSM 限流操作。當 HSM 因過於忙於執行先前操作而無法接受更多要求而限制操作時，用戶端 SDK 會嘗試重試限流操作 (最多 3 次)，同時以指數形式回退。此自動重試策略可以設定為兩種模式中的其中一種：關閉模式和標準模式。

- 關閉：用戶端 SDK 將不會針對 HSM 的任何限流操作執行任何重試政策。
- 標準：這是用戶端 SDK 5.8.0 及更新版本的預設模式。在此模式下，用戶端 SDK 會以指數回退形式自動重試限流操作。

如需詳細資訊，請參閱[HSM 調節](#)。

將重試命令設定為關閉模式

您可以使用下列命令將重試命令設定為 off 模式：

```
$ sudo /opt/cloudhsm/bin/configure-dyn --default-retry-mode off
```

## AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 (KSP)

Key Storage Provider (KSP) 是 Microsoft Windows 作業系統特有的密碼編譯 API。Key Storage Provider (KSP) 可讓開發人員使用密碼編譯技術來保護 Windows 型應用程式。

如需關於啟動載入的資訊，請參閱 [連接至叢集](#)。

如需關於使用用戶端 SDK 3 的資訊，請參閱 [使用先前的 SDK 版本來使用 AWS CloudHSM](#)。

### 主題

- [安裝 AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 \(KSP\)](#)
- [向用戶端 SDK AWS CloudHSM 5 的金鑰儲存提供者 \(KSP\) 驗證](#)
- [用戶端 SDK 5 金鑰儲存提供者 \(KSP\) 支援的 AWS CloudHSM 金鑰類型](#)
- [用戶端 SDK AWS CloudHSM 5 支援的 API 操作金鑰儲存提供者 \(KSP\)](#)
- [適用於的 KSP 進階組態 AWS CloudHSM](#)

## 安裝 AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 (KSP)

使用下列各節來安裝 AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 (KSP)。

### Note

若要使用用戶端 SDK 5 執行單一 HSM 叢集，您必須先將 `disable_key_availability_check` 設定為 `True` 來管理用戶端金鑰持久性。如需詳細資訊，請參閱[金鑰同步處理](#)和[用戶端 SDK 5 設定工具](#)。

### 安裝和設定金鑰儲存提供者 (KSP)

1. 在 x86\_64 架構上安裝 Windows Server 的金鑰儲存提供者 (KSP)，以管理員身分開啟 PowerShell，然後執行下列命令：

```
PS C:\> wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Windows/AWSCloudHSMKSP-latest.msi -Outfile C:\AWSCloudHSMKSP-latest.msi
```

```
PS C:\> Start-Process msixexec.exe -ArgumentList '/i C:\AWSCloudHSMKSP-latest.msi /quiet /norestart /log C:\client-install.txt' -Wait
```

2. 使用設定工具指定發行憑證的位置。如需說明，請參閱 [指定憑證的位置](#)。
3. 若要連線到您的叢集，請參閱 [引導用戶端 SDK](#)。
4. 您可以在下列位置找到金鑰儲存提供者 (KSP) 檔案：

- Windows 二進位檔案：

```
C:\Program Files\Amazon\CloudHSM
```

Windows組態指令碼和日誌檔案：

```
C:\ProgramData\Amazon\CloudHSM
```

## 向用戶端 SDK AWS CloudHSM 5 的金鑰儲存提供者 (KSP) 驗證

使用 AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 (KSP) 之前，您必須在系統上設定 HSM 的登入憑證。您有兩種選擇：

- Windows Credentials Manager (建議提高安全性)
- 系統環境變數 (簡易設定)

### Windows 認證管理員

您可以使用 `set_cloudhsm_credentials` 公用程式或 Windows Credentials Manager 介面來設定登入資料。

- 使用 **`set_cloudhsm_credentials`** 公用程式：

Windows 安裝程式包含 `set_cloudhsm_credentials` 公用程式。您可以使用此公用程式，輕鬆地將 HSM 登入資料傳遞到 Windows 認證管理員。如果您想要從來源編譯此公用程式，您可以使用安裝程式中包含的 Python 程式碼。

1. 導覽至 `C:\Program Files\Amazon\CloudHSM\tools\`。
2. 執行以下命令：

```
set_cloudhsm_credentials.exe --username <CU USER> --password <CU PASSWORD>
```

- 使用認證管理員介面：
  1. 開啟登入資料管理員：

- credential manager 在任務列搜尋方塊中輸入
  - 選取登入資料管理員
2. 選取 Windows 認證以管理 Windows 認證。
  3. 選取新增一般登入資料
  4. 輸入下列詳細資訊：
    - 網路或網路地址：CLOUDHSM\_PIN。
    - 使用者名稱：*<CU USERNAME>*。
    - 密碼：*<CU PASSWORD>*。
  5. 選擇 OK (確定)。

## 系統環境變數

您可以設定系統環境變數來識別 HSM 和[加密使用者](#) (CU)。

### Warning

透過系統環境變數設定登入資料會將您的密碼以純文字形式存放在您的系統上。為了提高安全性，請改用 Windows Credential Manager。

您可以使用下列方式設定環境變數：

- [setx](#)。
- Windows 系統屬性控制面板（進階索引標籤）。
- 設定永久系統環境變數 [程式設計](#) 方法。

若要設定系統環境變數：

**CLOUDHSM\_PIN=*<CU USERNAME>*:*<CU PASSWORD>***

識別 HSM 中的[加密使用者](#) (CU)，並提供所有必要的登入資訊。您的應用程式會以這個 CU 的身分進行驗證和執行。這個應用程式具有此 CU 的許可，並僅可以檢視和管理該 CU 擁有和共用的金鑰。若要建立新的 CU，請使用 CloudHSM CLI 中的[使用者建立](#)命令。若要尋找現有的 CUs，請使用 CloudHSM CLI 中的[使用者清單](#)命令。

例如：

```
setx /m CLOUDHSM_PIN test_user:password123
```

## 用戶端 SDK 5 金鑰儲存提供者 (KSP) 支援的 AWS CloudHSM 金鑰類型

AWS CloudHSM 金鑰儲存提供者 (KSP) 支援用戶端 SDK 5 的下列金鑰類型。

| 金鑰類型 | 描述                                                                 |
|------|--------------------------------------------------------------------|
| EC   | 使用 secp256r1 (P-256)、secp384r1 (P-384) 和 secp521r1 (P-521) 曲線產生金鑰。 |
| RSA  | 產生 2048、3072 和 4096 位元 RSA 金鑰。                                     |

## 用戶端 SDK AWS CloudHSM 5 支援的 API 操作金鑰儲存提供者 (KSP)

KSP 中的參數由 Microsoft KSP 定義。如需詳細資訊，請參閱 [Microsoft 文件](#)。

Key Storage Provider (KSP) 支援 AWS CloudHSM 用戶端 SDK 5 的下列 KSP API 操作。

- [NCryptOpenStorageProvider](#)
- [NCryptOpenKey](#)
- [NCryptCreatePersistedKey](#)
- [NCryptGetProperty](#)
- [NCryptSetProperty](#)
- [NCryptFinalizeKey](#)
- [NCryptDeleteKey](#)
- [NCryptFreeObject](#)
- [NCryptFreeBuffer](#)
- [NCryptIsAlgSupported](#)
- [NCryptEnumAlgorithms](#)
- [NCryptEnumKeys](#)
- [NCryptExportKey](#)
- [NCryptSignHash](#)

- [NCryptVerifySignature](#)

NCryptOpenStorageProvider 函數與金鑰儲存提供者 (KSP)

NCryptOpenStorageProvider 函數會載入和初始化金鑰儲存提供者 (KSP)。

參數

phProvider 【輸出】

儲存提供者控點的NCRYPT\_PROV\_HANDLE變數指標。

pszProviderName 【in】

識別金鑰儲存提供者的 null 終止 Unicode 字串指標。AWS CloudHSM Key Storage Provider (KSP) 支援下列值：

| Value               | 意義                                 |
|---------------------|------------------------------------|
| L"CloudHSM 金鑰儲存提供者" | 識別用戶端 SDK 5 提供者名稱。根據預設，我們建議您使用此名稱。 |
| L"Cavium 金鑰儲存提供者"   | 識別用戶端 SDK 3 提供者名稱。支援回溯相容性。         |

 Note

值為廣字元字串常值，如常值前的 L 所示。

dwFlags 【in】

修改函數行為的旗標。此函數未定義任何旗標。

傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼                  | 描述        |
|-----------------------|-----------|
| ERROR_SUCCESS         | 操作已成功完成。  |
| NTE_INVALID_PARAMETER | 一或多個參數無效。 |
| NTE_FAIL              | 操作無法完成。   |

## NCryptOpenKey 與金鑰儲存提供者 (KSP)

NCryptOpenKey 函數會開啟金鑰儲存提供者 (KSP) 中存在的金鑰。

### 參數

**hProvider** 【in】

包含金鑰的 KSP 控點。使用 [NCryptOpenStorageProvider](#) 取得控點。

**phKey** 【輸出】

儲存金鑰控點的 NCrypt\_KEY\_HANDLE 變數指標。

**pszKeyName** 【in】

包含金鑰名稱的 null 終止 Unicode 字串指標。

**dwLegacyKeySpec** 【in、未使用】

AWS CloudHSM 金鑰儲存提供者 (KSP) 不會使用此參數。

**dwFlags** 【in】

修改函數行為的旗標。此函數未定義任何旗標。

### 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回碼包括：

| 傳回代碼          | 描述       |
|---------------|----------|
| ERROR_SUCCESS | 操作已成功完成。 |



| 傳回代碼                  | 描述                |
|-----------------------|-------------------|
| NTE_INVALID_PARAMETER | 一或多個參數無效。         |
| NTE_FAIL              | 操作無法完成。           |
| NTE_INVALID_HANDLE    | 中的控點hProvider 無效。 |
| NTE_BAD_KEYSET        | 提供的金鑰名稱未傳回唯一結果。   |

## NCryptCreatePersistedKey 與金鑰儲存提供者 (KSP)

NCryptCreatePersistedKey 函數會建立新的金鑰，並將其存放在金鑰儲存提供者 (KSP) 中。您可以使用 [NCryptSetProperty](#) 函數在建立後設定其屬性。您必須呼叫 [NCryptFinalizeKey](#) 才能使用金鑰。

### 參數

hProvider 【in】

您要建立金鑰的金鑰儲存提供者的控點。使用 [NCryptOpenStorageProvider](#) 取得此控點。

phKey 【輸出】

存放金鑰控點的NCRYPT\_KEY\_HANDLE變數地址。

pszAlgId 【in】

Null 終止 Unicode 字串的指標，指定用於建立金鑰的密碼編譯演算法識別符。

AWS CloudHSM Key Storage Provider (KSP) 支援下列演算法：

| 常數/值                        | 描述                                |
|-----------------------------|-----------------------------------|
| BCRYPT_RSA_ALGORITHM        | RSA 公有金鑰演算法。                      |
| "RSA"                       |                                   |
| BCRYPT_ECDSA_P256_ALGORITHM | 256 位元基本橢圓曲線數位簽章演算法 (FIPS 186-2)。 |
| "ECDSA_P256"                |                                   |

| 常數/值                                        | 描述                                |
|---------------------------------------------|-----------------------------------|
| BCRYPT_ECDSA_P384_ALGORITHM<br>"ECDSA_P384" | 384 位元主要橢圓曲線數位簽章演算法 (FIPS 186-2)。 |
| BCRYPT_ECDSA_P521_ALGORITHM<br>"ECDSA_P521" | 521 位元主要橢圓曲線數位簽章演算法 (FIPS 186-2)。 |

### pszKeyName 【in, 選用】

包含金鑰名稱的 null 終止 Unicode 字串指標。如果此參數為 NULL，則此函數會建立不會保留的暫時性金鑰。

### dwLegacyKeySpec 【in、未使用】

AWS CloudHSM 金鑰儲存提供者 (KSP) 不會使用此參數。

### dwFlags 【in】

用於修改函數行為的旗標。使用下列 0 或多個值：

| Value                     | 意義                                                          |
|---------------------------|-------------------------------------------------------------|
| NCRYPT_MACHINE_KEY_FLAG   | 此標記沒有效果。                                                    |
| NCRYPT_SILENT_FLAG        | 此標記沒有效果。                                                    |
| NCRYPT_OVERWRITE_KEY_FLAG | 指定此旗標會覆寫 HSM 中名稱相同的任何現有金鑰。<br><br>如果沒有此旗標，函數會傳回 NTE_EXISTS。 |

### 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回碼包括：

| 傳回代碼                  | 描述                                         |
|-----------------------|--------------------------------------------|
| ERROR_SUCCESS         | 函數已成功完成。                                   |
| NTE_INVALID_PARAMETER | 一或多個參數無效。                                  |
| NTE_FAIL              | 操作無法完成。                                    |
| NTE_BAD_FLAGS         | dwFlags 參數包含無效的值。                          |
| NTE_NOT_SUPPORTED     | pszAlgId 參數包含不支援的值。                        |
| NTE_EXISTS            | 具有指定名稱的金鑰已存在，且操作未使用 NCryptOverwriteKey 旗標。 |

## NCryptGetProperty 與金鑰儲存提供者 (KSP)

NCryptGetProperty 函數會擷取金鑰儲存物件的屬性值。

### 參數

hObject **【in】**

您要擷取其屬性的物件控點。您可以使用：

- 供應商控制代碼 (NCRYPT\_PROV\_HANDLE)
- 金鑰控制代碼 (NCRYPT\_KEY\_HANDLE)

pszProperty **【in】**

指向 null 終止的 Unicode 字串的指標，其中包含要擷取的屬性名稱。

使用時 NCRYPT\_PROV\_HANDLE，AWS CloudHSM 金鑰儲存提供者 (KSP) 支援下列 KSP 識別符：

| 識別符/值                     | 描述                      |
|---------------------------|-------------------------|
| NCRYPT_IMPL_TYPE_PROPERTY | 包含定義提供者實作詳細資訊之旗標的 DWORD |
| L"Impl 類型"                |                         |

| 識別符/值                                               | 描述                               |
|-----------------------------------------------------|----------------------------------|
| NCRYPT_MAX_NAME_LENGTH_PROPERTY<br>L"名稱長度上限"        | 包含持久性金鑰名稱長度上限（以字元為單位）的 DWORD。    |
| NCRYPT_NAME_PROPERTY<br>L"Name"                     | 包含 KSP 名稱的 null 終止 Unicode 字串指標。 |
| NCRYPT_VERSION_PROPERTY<br>L"版本"                    | 包含提供者版本的 DWORD（高字：主要版本、低字：次要版本）。 |
| NCRYPT_USE_CONTEXT_PROPERTY<br>L"使用內容"              | 描述操作內容的 null 終止 Unicode 字串指標。    |
| NCRYPT_SECURITY_DESCR_SUPPORT_PROPERTY<br>L"安全主管支援" | 指出提供者是否支援金鑰的安全描述項。               |

使用時 NCRYPT\_KEY\_HANDLE，AWS CloudHSM 金鑰儲存提供者 (KSP) 支援下列 KSP 識別符：

| 識別符/值                                    | 描述                             |
|------------------------------------------|--------------------------------|
| NCRYPT_ALGORITHM_PROPERTY<br>L"演算法名稱"    | 包含金鑰演算法名稱的 null 終止 Unicode 字串。 |
| NCRYPT_BLOCK_LENGTH_PROPERTY<br>L"區塊長度"  | 包含加密區塊長度的 DWORD，以位元組為單位。       |
| NCRYPT_EXPORT_POLICY_PROPERTY<br>L"匯出政策" | DWORD，其中包含指定持久金鑰匯出政策的旗標。       |

| 識別符/值                                       | 描述                                       |
|---------------------------------------------|------------------------------------------|
| NCRYPT_KEY_USAGE_PROPERTY<br>L"金鑰用量"        | 包含定義金鑰用量詳細資訊之旗標的 DWORD。                  |
| NCRYPT_KEY_TYPE_PROPERTY<br>L"金鑰類型"         | 包含定義金鑰類型的旗標的 DWORD。                      |
| NCRYPT_LENGTH_PROPERTY<br>L"長度"             | 以位元為單位包含金鑰長度的 DWORD。                     |
| NCRYPT_LENGTHS_PROPERTY<br>L"長度"            | 包含支援金鑰大小的 NCRYPT_SUPPORTED_LENGTHS 結構指標。 |
| NCRYPT_NAME_PROPERTY<br>L"Name"             | 包含金鑰名稱的 null 終止 Unicode 字串指標。            |
| NCRYPT_SECURITY_DESCR_PROPERTY<br>L"安全說明"   | 包含金鑰存取控制資訊的 SECURITY_DESCRIPTOR 結構指標。    |
| NCRYPT_ALGORITHM_GROUP_PROPERTY<br>L"演算法群組" | 包含物件演算法群組名稱的 null 終止 Unicode 字串。         |
| NCRYPT_UNIQUE_NAME_PROPERTY<br>L"唯一名稱"      | 包含金鑰唯一名稱的 null 終止 Unicode 字串指標。          |

 Note

值為廣字元字串常值，如常值前的 L 所示。

## pbOutput 【輸出】

儲存屬性值的緩衝區地址。使用 指定緩衝區大小cbOutput。

若要判斷所需的緩衝區大小，請將此參數設定為 NULL。函數會將所需的大小（以位元組為單位）存放在 指向的位置pcbResult。

## cbOutput 【in】

pbOutput 緩衝區的大小，以位元組為單位。

## pcbResult 【輸出】

DWORD 變數的指標，可存放複製到緩衝區的pbOutput位元組數。

如果 pbOutput是 NULL，這會存放所需的大小（以位元組為單位）。

## dwFlags 【in】

用於修改函數行為的旗標。您可以使用零或：

| Value              | 意義       |
|--------------------|----------|
| NCRYPT_SILENT_FLAG | 此旗標沒有效果。 |

當 pszProperty 為 時NCRYPT\_SECURITY\_DESCR\_PROPERTY，請使用下列其中一項或組合：

| Value                      | 意義       |
|----------------------------|----------|
| OWNER_SECURITY_INFORMATION | 此旗標沒有效果。 |
| GROUP_SECURITY_INFORMATION | 此旗標沒有效果。 |
| DACL_SECURITY_INFORMATION  | 此旗標沒有效果。 |
| LABEL_SECURITY_INFORMATION | 此旗標沒有效果。 |
| SACL_SECURITY_INFORMATION  | 此旗標沒有效果。 |

## 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼                  | 描述                   |
|-----------------------|----------------------|
| ERROR_SUCCESS         | 操作已成功完成。             |
| NTE_INVALID_PARAMETER | 一或多個參數無效。            |
| NTE_FAIL              | 操作無法完成。              |
| NTE_BAD_FLAGS         | dwFlags 參數包含無效的值。    |
| NTE_NOT_SUPPORTED     | pszAlgId 參數包含不支援的值。  |
| NTE_INVALID_HANDLE    | 中的控點hObject無效。       |
| NTE_BUFFER_TOO_SMALL  | cbOutput 參數太小，無法傳回值。 |

## NCryptSetProperty 與金鑰儲存提供者 (KSP)

NCryptSetProperty 函數會設定金鑰儲存物件的屬性值。

### 參數

hObject **【in】**

您要設定其屬性的物件控點。您可以使用：

- 供應商控制代碼 (NCRYPT\_PROV\_HANDLE)
- 金鑰控制代碼 (NCRYPT\_KEY\_HANDLE)

pszProperty **【in】**

指向 null 終止的 Unicode 字串的指標，其中包含要擷取的屬性名稱。

使用 時NCRYPT\_PROV\_HANDLE，AWS CloudHSM 金鑰儲存提供者 (KSP) 支援下列 KSP 識別符：

| 識別符/值                       | 描述                            |
|-----------------------------|-------------------------------|
| NCRYPT_USE_CONTEXT_PROPERTY | 描述操作內容的 null 終止 Unicode 字串指標。 |

| 識別符/值   | 描述 |
|---------|----|
| L"使用內容" |    |

使用時 NCryptKeyHandle，AWS CloudHSM 金鑰儲存提供者 (KSP) 支援下列 KSP 識別符：

| 識別符/值                                 | 描述                                                                                                                                                       |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| NCryptKeyUsageProperty<br>L"金鑰用量"     | DWORD，其中包含一組定義金鑰用量詳細資訊的旗標。此屬性僅適用於金鑰。這可以包含零或下列一或多個值的組合。<br><br>NCRYPT_ALLOW_DECRYPT_FLAG<br>(0x00000001)<br><br>NCRYPT_ALLOW_SIGNING_FLAG<br>(0x00000002) |
| NCryptLengthProperty<br>L"長度"         | 以位元為單位包含金鑰長度的 DWORD。                                                                                                                                     |
| NCryptExportPolicyProperty<br>L"匯出政策" | 包含指定持久金鑰匯出政策之旗標的 DWORD。這可以包含零或下列一或多個值的組合。<br><br>NCRYPT_ALLOW_EXPORT_FLAG<br>(0x00000001)                                                                |

 Note

值為廣字元字串常值，如常值前的 L 所示。

pbInput **【in】**

包含新屬性值的緩衝區地址。cbInput 包含緩衝區的大小。



**cbInput 【in】**

pbInput 緩衝區的大小，以位元組為單位。

**dwFlags 【in】**

修改函數行為的旗標。此函數未定義任何旗標。

**傳回值**

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼                  | 描述                        |
|-----------------------|---------------------------|
| ERROR_SUCCESS         | 操作已成功完成。                  |
| NTE_INVALID_PARAMETER | 一或多個參數無效。                 |
| NTE_FAIL              | 操作無法完成。                   |
| NTE_BAD_FLAGS         | dwFlags 參數包含無效的值。         |
| NTE_NOT_SUPPORTED     | pszProperty 參數包含不支援的值。    |
| NTE_INVALID_HANDLE    | 中的控點hObject無效。            |
| NTE_BAD_DATA          | 指向 pbInput和 的資料cbInput無效。 |

**NCryptFinalizeKey 與金鑰儲存提供者 (KSP)**

NCryptFinalizeKey 函數會完成 KSP 金鑰。您必須呼叫此函數，才能使用 金鑰。

**參數****hKey 【in】**

要完成的金鑰控點。呼叫 [NCryptCreatePersistedKey](#) 函數來取得此控制代碼。

**dwFlags 【in】**

用於修改函數行為的旗標。您可以使用零或這些值：

| Value                    | 意義       |
|--------------------------|----------|
| NCRYPT_SILENT_FLAG       | 此旗標沒有效果。 |
| NCRYPT_NO_KEY_VALIDATION | 此旗標沒有效果。 |

## 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼               | 描述                 |
|--------------------|--------------------|
| ERROR_SUCCESS      | 操作已成功完成。           |
| NTE_FAIL           | 操作無法完成。            |
| NTE_INVALID_HANDLE | 中的控點hKey無效。        |
| NTE_NOT_SUPPORTED  | dwFlags 參數包含不支援的值。 |
| NTE_BAD_FLAGS      | dwFlags 參數包含無效的值。  |

## NCryptDeleteKey 與金鑰儲存提供者 (KSP)

NCryptDeleteKey 函數會從金鑰儲存提供者 (KSP) 刪除 KSP 金鑰。

### 參數

**hKey 【in】**

要刪除之金鑰的控點。

**dwFlags 【in】**

用於修改函數行為的旗標。您可以使用下列零或多個值：

| Value              | 意義       |
|--------------------|----------|
| NCRYPT_SILENT_FLAG | 此標記沒有效果。 |

## 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回碼包括：

| 傳回代碼                  | 描述                |
|-----------------------|-------------------|
| ERROR_SUCCESS         | 函數已成功。            |
| NTE_INVALID_PARAMETER | 一或多個參數無效。         |
| NTE_BAD_FLAGS         | dwFlags 參數包含無效的值。 |
| NTE_FAIL              | 操作無法完成。           |
| NTE_INVALID_HANDLE    | 中的控點hKey無效。       |
| NTE_INTERNAL_ERROR    | 刪除金鑰時發生內部錯誤。      |

## NCryptFreeObject 與金鑰儲存提供者 (KSP)

NCryptFreeObject 函數會從金鑰儲存提供者 (KSP) 釋出提供者或金鑰控制代碼。

## 參數

### hObject 【in】

要釋放之物件的控點。您可以使用：

- 供應商控制代碼 (NCRYPT\_PROV\_HANDLE)
- 金鑰控制代碼 (NCRYPT\_KEY\_HANDLE)

## 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼               | 描述             |
|--------------------|----------------|
| ERROR_SUCCESS      | 操作已成功完成。       |
| NTE_INVALID_HANDLE | 中的控點hObject無效。 |

## NCryptFreeBuffer 與金鑰儲存提供者 (KSP)

NCryptFreeBuffer 函數會釋出金鑰儲存提供者 (KSP) 配置的記憶體區塊。

### 參數

pvInput **【in】**

要釋放的記憶體地址。

### 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼          | 描述       |
|---------------|----------|
| ERROR_SUCCESS | 操作已成功完成。 |
| NTE_FAIL      | 操作無法完成。  |

## 使用金鑰儲存提供者 (KSP) NCryptIsAlgSupported

NCryptIsAlgSupported 函數會判斷金鑰儲存提供者 (KSP) 是否支援特定的密碼編譯演算法。

### 參數

hProvider **【in】**

金鑰儲存提供者的控點。使用 [NCryptOpenStorageProvider](#) 取得控點。

**pszAlgId** 【in】

Null 終止 Unicode 字串的指標，其中包含用於建立金鑰的密碼編譯演算法識別符。AWS CloudHSM Key Storage Provider (KSP) 支援下列演算法：

| 常數/值                                        | 描述                                |
|---------------------------------------------|-----------------------------------|
| BCRYPT_RSA_ALGORITHM<br>"RSA"               | RSA 公有金鑰演算法。                      |
| BCRYPT_ECDSA_P256_ALGORITHM<br>"ECDSA_P256" | 256 位元主要橢圓曲線數位簽章演算法 (FIPS 186-2)。 |
| BCRYPT_ECDSA_P384_ALGORITHM<br>"ECDSA_P384" | 384 位元主要橢圓曲線數位簽章演算法 (FIPS 186-2)。 |
| BCRYPT_ECDSA_P521_ALGORITHM<br>"ECDSA_P521" | 521 位元主要橢圓曲線數位簽章演算法 (FIPS 186-2)。 |

**dwFlags** 【in】

修改函數行為的旗標。這可以是零或下列值：

| Value              | 意義       |
|--------------------|----------|
| NCRYPT_SILENT_FLAG | 此旗標沒有效果。 |

**傳回值**

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼                  | 描述                  |
|-----------------------|---------------------|
| ERROR_SUCCESS         | 操作已成功完成。            |
| NTE_INVALID_PARAMETER | 一或多個參數無效。           |
| NTE_BAD_FLAGS         | dwFlags 參數包含無效的值。   |
| NTE_NOT_SUPPORTED     | pszAlgId 參數包含不支援的值。 |
| NTE_INVALID_HANDLE    | 中的控點hProvider 無效。   |

具有金鑰儲存提供者 (KSP) 的 NCryptEnumAlgorithms

NCryptEnumAlgorithms 函數會擷取金鑰儲存提供者 (KSP) 支援的演算法名稱。

參數

hProvider 【in】

要列舉演算法之金鑰儲存提供者的控點。使用 [NCryptOpenStorageProvider](#) 函數來取得此控點。

dwAlgOperations 【in】

指定要列舉哪些演算法類別的一組值。您可以使用零列舉所有演算法，或結合下列一或多個值：

| Value                                                | 意義          |
|------------------------------------------------------|-------------|
| NCRYPT_ASYMMETRIC_ENCRYPTION_OPERATION<br>0x00000004 | 列出非對稱加密演算法。 |
| NCRYPT_SIGNATURE_OPERATION<br>0x00000010             | 列出數位簽章演算法。  |

pdwAlgCount 【輸出】

陣列中存放元素數量的 DWORD 地址ppAlgList。

## ppAlgList 【輸出】

儲存已註冊演算法名稱陣列的NCryptAlgorithmName結構指標地址。pdwAlgCount 參數指出此陣列中的元素數目。

## dwFlags 【in】

用於修改函數行為的旗標。使用零或下列值：

| Value              | 意義       |
|--------------------|----------|
| NCRYPT_SILENT_FLAG | 此標記沒有效果。 |

## 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回碼包括：

| 傳回代碼                  | 描述                         |
|-----------------------|----------------------------|
| ERROR_SUCCESS         | 操作已成功完成。                   |
| NTE_INVALID_PARAMETER | 一或多個參數無效。                  |
| NTE_FAIL              | 操作無法完成。                    |
| NTE_BAD_FLAGS         | dwFlags 參數包含無效的值。          |
| NTE_NOT_SUPPORTED     | dwAlgOperations 參數包含不支援的值。 |

## NCryptEnumKeys 與金鑰儲存提供者 (KSP)

NCryptEnumKeys 函數會列出儲存在金鑰儲存提供者 (KSP) 中的金鑰。

## 參數

### hProvider 【in】

金鑰儲存提供者處理。使用 [NCryptOpenStorageProvider](#)取得此控制代碼。

pszScope 【in、未使用】

將此參數設定為 NULL。

ppKeyName 【輸出】

儲存金鑰名稱的NCryptKeyName結構指標地址。若要在使用後釋放此記憶體，請呼叫 [NCryptFreeBuffer](#)。

ppEnumState 【輸入、輸出】

追蹤列舉進度的 VOID 指標地址。金鑰儲存提供者會在內部使用此資訊來管理列舉序列。若要從頭開始新的列舉，請將此指標設定為 NULL。

若要在完成列舉後釋放此記憶體，請將此指標傳遞至 [NCryptFreeBuffer](#)。

dwFlags 【in】

用於修改函數行為的旗標。此函數沒有旗標。

傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼                  | 描述                |
|-----------------------|-------------------|
| ERROR_SUCCESS         | 操作已成功完成。          |
| NTE_INVALID_PARAMETER | 一或多個參數無效。         |
| NTE_FAIL              | 操作無法完成。           |
| NTE_INVALID_HANDLE    | 中的控點hProvider 無效。 |
| NTE_NO_MORE_ITEMS     | 列舉已列出所有可用的金鑰。     |

NCryptExportKey 與金鑰儲存提供者 (KSP)

NCryptExportKey 函數會將 KSP 金鑰匯出至記憶體 BLOB。此函數僅支援匯出公有金鑰。



## 參數

### hKey 【in】

要匯出之金鑰的控制代碼。

### hExportKey 【in、未使用】

AWS CloudHSM 金鑰儲存提供者 (KSP) 不會使用此參數。

### pszBlobType 【in】

null 終止的 Unicode 字串，指定要匯出的BLOB類型。AWS CloudHSM 金鑰儲存提供者 (KSP) 支援下列值：

| Value                 | 意義                                                        |
|-----------------------|-----------------------------------------------------------|
| BCRYPT_RSAPUBLIC_BLOB | 匯出 RSA 公有金鑰。pbOutput 緩衝區包含BCRYPT_RSAKEY_BLOB 結構，後面接著金鑰資料。 |
| BCRYPT_ECCPUBLIC_BLOB | 匯出ECC公有金鑰。pbOutput 緩衝區包含BCRYPT_ECCKEY_BLOB 結構，後面接著金鑰資料。   |

### pParameterList 【in，未使用】

AWS CloudHSM 金鑰儲存提供者 (KSP) 不會使用此參數。

### pbOutput 【輸出，選用】

儲存金鑰 BLOB 的緩衝區地址。使用 指定緩衝區大小cbOutput。如果設定為 NULL，函數會將所需的大小（以位元組為單位）存放在 指向的 DWORD 中pcbResult。

### cbOutput 【in】

pbOutput 緩衝區的大小，以位元組為單位。

### pcbResult 【輸出】

存放複製到pbOutput緩衝區的位元組數的 DWORD 變數地址。如果 pbOutput是 NULL，則函數會以位元組為單位存放所需的緩衝區大小。

## dwFlags **【in】**

修改函數運作方式的旗標。您可以使用零或下列項目：

| Value              | 意義       |
|--------------------|----------|
| NCRYPT_SILENT_FLAG | 此旗標沒有效果。 |

## 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼                  | 描述                               |
|-----------------------|----------------------------------|
| ERROR_SUCCESS         | 操作已成功完成。                         |
| NTE_INVALID_PARAMETER | 一或多個參數無效。                        |
| NTE_FAIL              | 操作無法完成。                          |
| NTE_INVALID_HANDLE    | 中的控點hProvider 無效。                |
| NTE_BAD_FLAGS         | dwFlags 參數包含無效的值。                |
| NTE_BAD_KEY_STATE     | 金鑰狀態無效。                          |
| NTE_NOT_SUPPORTED     | pszBlobType 或 dwFlags 參數包含不支援的值。 |
| STATUS_INTERNAL_ERROR | 操作期間發生內部錯誤。                      |

## NCryptSignHash 與金鑰儲存提供者 (KSP)

NCryptSignHash 函數會建立雜湊值的簽章。

## 參數

### hKey 【in】

用來簽署雜湊的金鑰控點。

### pPaddingInfo 【in, 選用】

包含填補資訊的結構指標。結構類型取決於 dwFlags 值。僅將此參數與非對稱金鑰搭配使用；其他金鑰類型設定為 NULL。

### pbHashValue 【in】

緩衝區的指標，其中包含要簽署的雜湊值。使用 指定緩衝區大小 cbHashValue。

### cbHashValue 【in】

要簽署之 pbHashValue 緩衝區的大小，以位元組為單位。

### pbSignature 【輸出】

儲存簽章的緩衝區地址。使用 指定緩衝區大小 cbSignature。

若要判斷所需的緩衝區大小，請將此參數設定為 NULL。函數會將所需的大小（以位元組為單位）存放在 指向的位置 pcbResult。

### cbSignature 【in】

pbSignature 緩衝區的大小，以位元組為單位。如果 pbSignature 是 NULL，則函數會忽略此參數。

### pcbResult 【輸出】

DWORD 變數的指標，可存放複製到 pbSignature 緩衝區的位元組數。

如果 pbSignature 是 NULL，則會以位元組為單位存放所需的緩衝區大小。

### dwFlags 【in】

用於修改函數行為的旗標。允許的旗標取決於您的金鑰類型。使用下列其中一個值：

| Value            | 意義                                                             |
|------------------|----------------------------------------------------------------|
| BCRYPT_PAD_PKCS1 | 使用 PKCS1 填補方案。pPaddingInfo 設定為指向 BCRYPT_PKCS1_PADDING_INFO 結構。 |

| Value              | 意義                                                                   |
|--------------------|----------------------------------------------------------------------|
| BCRYPT_PAD_PSS     | 使用概率簽章方案 (PSS) 填補方案。設定 pPaddingInfo 參數以指向BCRYPT_PSS_PADDING_INFO 結構。 |
| NCRYPT_SILENT_FLAG | 此旗標沒有效果。                                                             |

## 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回代碼包括：

| 傳回代碼                  | 描述                    |
|-----------------------|-----------------------|
| ERROR_SUCCESS         | 操作已成功完成。              |
| NTE_INVALID_PARAMETER | 一或多個參數無效。             |
| NTE_FAIL              | 操作無法完成。               |
| NTE_INVALID_HANDLE    | 中的控點hKey無效。           |
| NTE_BAD_FLAGS         | dwFlags 參數包含無效的值。     |
| NTE_BUFFER_TOO_SMALL  | pcbOutput 參數太小，無法傳回值。 |
| NTE_BAD_KEY_STATE     | 金鑰狀態無效。               |
| NTE_INTERNAL_ERROR    | 簽署雜湊時發生內部錯誤。          |

## NCryptVerifySignature with Key Storage Provider (KSP)

NCryptVerifySignature 函數會確認簽章是否符合指定的雜湊。

## 參數

### hKey 【in】

用來解密簽章的金鑰控點。您必須使用用來使用 簽署資料的金鑰對公有金鑰部分 [NCryptSignHash](#)。

### pPaddingInfo 【in, 選用】

包含填補資訊的結構指標。結構類型取決於 dwFlags 值。僅將此參數與非對稱金鑰搭配使用；其他金鑰類型設定為 NULL。

### pbHashValue 【in】

緩衝區的指標，其中包含要簽署的雜湊值。使用 指定緩衝區大小 cbHashValue。

### cbHashValue 【in】

pbHashValue 緩衝區的大小，以位元組為單位。

### pbSignature 【輸出】

包含資料簽署雜湊的緩衝區地址。使用 [NCryptSignHash](#) 建立此簽章。使用 指定緩衝區大小 cbSignature。

### cbSignature 【in】

pbSignature 緩衝區的大小，以位元組為單位。使用 [NCryptSignHash](#) 建立簽章。

### dwFlags 【in】

用於修改函數行為的旗標。允許的旗標取決於您的金鑰類型。使用下列其中一個值：

| Value                 | 意義                                                                      |
|-----------------------|-------------------------------------------------------------------------|
| NCRYPT_PAD_PKCS1_FLAG | 指示簽章使用的 PKCS1 填充。pPaddingInfo 設定以指向 BCRYPT_PKCS1_PADDING_INFO 結構。       |
| NCRYPT_PAD_PSS_FLAG   | 指出使用的簽章概率簽章結構描述 (PSS) 填充。pPaddingInfo 設定以指向 BCRYPT_PSS_PADDING_INFO 結構。 |
| NCRYPT_SILENT_FLAG    | 此標記沒有效果。                                                                |

## 傳回值

函數會傳回狀態碼，表示成功或失敗。

常見的傳回碼包括：

| 傳回代碼                  | 描述                |
|-----------------------|-------------------|
| ERROR_SUCCESS         | 操作已成功完成。          |
| NTE_INVALID_PARAMETER | 一或多個參數無效。         |
| NTE_FAIL              | 操作無法完成。           |
| NTE_INVALID_HANDLE    | 中的控點hKey無效。       |
| NTE_BAD_FLAGS         | dwFlags 參數包含無效的值。 |
| NTE_BAD_SIGNATURE     | 簽章未驗證。            |
| NTE_BAD_KEY_STATE     | 金鑰狀態無效。           |
| NTE_INTERNAL_ERROR    | 驗證簽章時發生內部錯誤。      |

## 適用於 的 KSP 進階組態 AWS CloudHSM

Key AWS CloudHSM Storage Provider (KSP) 包含下列進階組態，這不屬於大多數客戶使用的一般組態。這些組態提供額外的功能。

- [KSP 的 SDK3 相容性模式](#)

## 適用於 的金鑰儲存提供者 (KSP) 的 SDK3 相容性模式 AWS CloudHSM

金鑰儲存提供者 (KSP) 實作 HSM 金鑰互動的不同方法：

- 用戶端 SDK 5：與存放在 HSM 中的金鑰直接通訊，無需本機參考檔案
- 用戶端 SDK 3：在 Windows 伺服器上維護本機檔案，做為 HSM 中所存放金鑰的參考，使用這些檔案來促進金鑰操作

對於從用戶端 SDK 3 遷移至用戶端 SDK 5 的客戶，啟用 SDK3 相容性模式選項支援使用現有金鑰參考檔案的操作，同時保留基礎 HSM 金鑰儲存架構。

## 啟用 SDK3 相容性模式

### Windows

在 Windows 中為用戶端 SDK3 5 啟用金鑰儲存提供者 (KSP) 的 SDK3 相容性模式

- 您可以使用下列命令來啟用 SDK3 相容性模式：

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --enable-sdk3-compatibility-mode
```

## 停用 SDK3 相容性模式

### Windows

在 Windows 中停用用戶端 SDK3 5 金鑰儲存提供者 (KSP) 的 SDK3 相容性模式

- 您可以使用下列命令來停用 SDK3 相容性模式：

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-ksp.exe" --disable-sdk3-compatibility-mode
```

## AWS CloudHSM 用戶端 SDK 5 的 JCE 提供者

AWS CloudHSM JCE 提供者是從 Java 密碼編譯延伸 (JCE) 提供者架構建置的提供者實作。JCE 可讓您使用 Java 開發套件 (JDK) 執行密碼編譯操作。在本指南中，AWS CloudHSM JCE 提供者有時稱為 JCE 提供者。使用 JCE 提供者和 JDK 將密碼編譯操作卸載至 HSM。如需故障診斷，請參閱[適用於的 JCE 開發套件的已知問題 AWS CloudHSM](#)。

如需關於使用用戶端 SDK 3 的資訊，請參閱[使用先前的 SDK 版本來使用 AWS CloudHSM](#)。

### 主題

- [安裝 AWS CloudHSM 用戶端 SDK 5 的 JCE 提供者](#)
- [用戶端 SDK 5 的 JCE 提供者 AWS CloudHSM 支援的金鑰類型](#)
- [AWS CloudHSM 用戶端 SDK 5 的 JCE 提供者中的金鑰管理基本概念](#)

- [用戶端 SDK 5 AWS CloudHSM 的 JCE 提供者支援的機制](#)
- [用戶端 SDK AWS CloudHSM 5 支援的 Java 金鑰屬性](#)
- [Java for Client SDK 5 AWS CloudHSM 軟體程式庫的程式碼範例](#)
- [AWS CloudHSM JCE 供應商 Javadocs](#)
- [用戶端 SDK 5 的 AWS CloudHSM KeyStore Java 類別](#)
- [AWS CloudHSM JCE for Client SDK 5 的進階組態](#)

## 安裝 AWS CloudHSM 用戶端 SDK 5 的 JCE 提供者

AWS CloudHSM 用戶端 SDK 5 的 JCE 提供者與 OpenJDK 8、OpenJDK 11、OpenJDK 17 和 OpenJDK 21 相容。您可以從 [OpenJDK 網站](#) 下載 OpenJDK 8 和 OpenJDK 11。

使用下列各節來安裝憑證並向供應商提供憑證。

### Note

若要使用用戶端 SDK 5 執行單一 HSM 叢集，您必須先將 `disable_key_availability_check` 設定為 `True` 來管理用戶端金鑰持久性。如需詳細資訊，請參閱 [金鑰同步處理](#) 和 [用戶端 SDK 5 設定工具](#)。

## 主題

- [步驟 1：安裝 JCE 提供者](#)
- [步驟 2：提供登入資料給 JCE 供應商](#)

### 步驟 1：安裝 JCE 提供者

1. 使用下列命令下載和安裝 JCE 提供者。

Amazon Linux 2023

在 x86\_64 架構上安裝 Amazon Linux 2023 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-jce-latest.amzn2023.x86_64.rpm
```



```
$ sudo yum install ./cloudhsm-jce-latest.amzn2023.x86_64.rpm
```

在 ARM64 架構上安裝 Amazon Linux 2023 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Amzn2023/cloudhsm-jce-latest.amzn2023.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-jce-latest.amzn2023.aarch64.rpm
```

## Amazon Linux 2

在 x86\_64 架構上安裝 Amazon Linux 2 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-jce-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-jce-latest.el7.x86_64.rpm
```

在 ARM64 架構上安裝 Amazon Linux 2 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-jce-latest.el7.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-jce-latest.el7.aarch64.rpm
```

## RHEL 9 (9.2+)

在 x86\_64 架構上安裝 RHEL 9 (9.2+) 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-jce-latest.el9.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-jce-latest.el9.x86_64.rpm
```

在 ARM64 架構上安裝 RHEL 9 (9.2+) 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL9/cloudhsm-jce-latest.el9.aarch64.rpm
```

```
$ sudo yum install ./cloudhsm-jce-latest.el9.aarch64.rpm
```

## RHEL 8 (8.3+)

在 x86\_64 架構上安裝 RHEL 8 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-jce-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-jce-latest.el8.x86_64.rpm
```

## Ubuntu 24.04 LTS

在 x86\_64 架構上安裝 Ubuntu 24.04 LTS 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/cloudhsm-jce_latest_u24.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-jce_latest_u24.04_amd64.deb
```

在 ARM64 架構上安裝 Ubuntu 24.04 LTS 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Noble/cloudhsm-jce_latest_u24.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-jce_latest_u24.04_arm64.deb
```

## Ubuntu 22.04 LTS

在 x86\_64 架構上安裝 Ubuntu 22.04 LTS 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/cloudhsm-jce_latest_u22.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-jce_latest_u22.04_amd64.deb
```

在 ARM64 架構上安裝 Ubuntu 22.04 LTS 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Jammy/cloudhsm-jce_latest_u22.04_arm64.deb
```

```
$ sudo apt install ./cloudhsm-jce_latest_u22.04_arm64.deb
```

## Ubuntu 20.04 LTS

在 x86\_64 架構上安裝 Ubuntu 20.04 LTS 的 JCE 提供者：

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Focal/cloudhsm-jce_latest_u20.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-jce_latest_u20.04_amd64.deb
```

## Windows Server

在 x86\_64 架構上安裝適用於 Windows Server 的 JCE 提供者，以管理員身分開啟 PowerShell，然後執行下列命令：

```
PS C:\> wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Windows/AWSCloudHSMJCE-latest.msi -Outfile C:\AWSCloudHSMJCE-latest.msi
```

```
PS C:\> Start-Process msixexec.exe -ArgumentList '/i C:\AWSCloudHSMJCE-latest.msi /quiet /norestart /log C:\client-install.txt' -Wait
```

2. 引導用戶端 SDK 5。如需有關啟動程序的詳細資訊，請參閱 [引導用戶端 SDK](#)。
3. 找出下列 JCE 提供者檔案：

## Linux

- /opt/cloudhsm/java/cloudhsm-*<version>*.jar
- /opt/cloudhsm/bin/configure-jce
- /opt/cloudhsm/bin/jce-info

## Windows

- C:\Program Files\Amazon\CloudHSM\java\cloudhsm-*<version>*.jar>
- C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe
- C:\Program Files\Amazon\CloudHSM\bin\jce\_info.exe

### 步驟 2：提供登入資料給 JCE 供應商

HSM 需要先驗證您的 Java 應用程式，應用程式才能使用 HSM。HSM 會使用明確登入或隱含登入方法，進行驗證。

**明確登入：**此方法可讓您直接在應用程式中提供 AWS CloudHSM 憑證。它使用 [AuthProvider](#) 中的方法，讓您可以在 pin 模式中傳遞 CU 使用者名稱和密碼。如需詳細資訊，請參閱[登入 HSM](#) 程式碼範例。

**隱含登入：**此方法可讓您在新的屬性檔案、系統屬性或環境變數中設定 AWS CloudHSM 憑證。

- **系統屬性：**執行應用程式時，您可以透過系統屬性設定憑證。以下範例示範兩種不同的作法：

## Linux

```
$ java -DHSM_USER=<HSM user name> -DHSM_PASSWORD=<password>
```

```
System.setProperty("HSM_USER", "<HSM user name>");
System.setProperty("HSM_PASSWORD", "<password>");
```

## Windows

```
PS C:\> java -DHSM_USER=<HSM user name> -DHSM_PASSWORD=<password>
```

```
System.setProperty("HSM_USER", "<HSM user name>");
System.setProperty("HSM_PASSWORD", "<password>");
```

- **環境變數：**將憑證設定為環境變數。

## Linux

```
$ export HSM_USER=<HSM user name>
```

```
$ export HSM_PASSWORD=<password>
```

## Windows

```
PS C:\> $Env:HSM_USER="<HSM user name>"
PS C:\> $Env:HSM_PASSWORD="<password>"
```

如果應用程式未提供登入資料，或者，如果您在 HSM 驗證工作階段之前嘗試操作，就可能無法使用登入資料。在這些情況下，適用於 Java 的 CloudHSM 軟體程式庫會按照以下順序，搜尋登入資料：

1. 系統屬性
2. 環境變數

## 用戶端 SDK 5 的 JCE 提供者 AWS CloudHSM 支援的金鑰類型

適用於 Java AWS CloudHSM 的軟體程式庫可讓您產生下列金鑰類型。

| 金鑰類型                      | 描述                                                                                                                      |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------|
| AES                       | 產生 128 位元、192 位元和 256 位元的 AES 金鑰。                                                                                       |
| Triple DES (3DES, DESede) | 產生 192 位元三重 DES 金鑰 <a href="#">請參閱即將進行變更 1 的註腳</a> 。                                                                    |
| EC                        | 產生 EC 金鑰對：NIST curves secp224r1 (P-224)、secp256r1 (P-256)、secp256k1 (Blockchain)、secp384r1 (P-384) 和 secp521r1 (P-521)。 |
| GENERIC_SECRET            | 產生 1 到 800 位元組的一般機密。                                                                                                    |
| HMAC                      | 支援 SHA1、SHA224、SHA256、SHA384 和 SHA512 雜湊。                                                                               |
| RSA                       | 產生 2048 位元至 4096 位元的 RSA 金鑰，以 256 位元為單位遞增。                                                                              |

【1】根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## AWS CloudHSM 用戶端 SDK 5 的 JCE 提供者中的金鑰管理基本概念

JCE 提供者的金鑰管理基本概念包括匯入金鑰、匯出金鑰、透過控制代碼載入金鑰或刪除金鑰。如需管理金鑰的詳細資訊，請參閱[管理金鑰](#)的程式碼範例。

您也可以[在 程式碼範例](#)中尋找更多 JCE 提供者程式碼範例。

## 用戶端 SDK 5 AWS CloudHSM 的 JCE 提供者支援的機制

本主題提供 JCE 供應商使用 AWS CloudHSM 用戶端 SDK 5 支援機制的相關資訊。如需支援的 Java 密碼編譯架構 (JCA) 介面和引擎類別的相關資訊 AWS CloudHSM，請參閱下列主題。

### 主題

- [產生金鑰與金鑰對函數](#)
- [密碼函數](#)
- [簽署和驗證函數](#)
- [Digest 函數](#)
- [雜湊訊息驗證碼 \(HMAC\) 函數](#)
- [加密式訊息驗證程式碼 \(CMAC\) 函數](#)
- [金鑰協議函數](#)
- [使用金鑰 Factory 將金鑰轉換為金鑰規格](#)
- [機制註釋](#)

### 產生金鑰與金鑰對函數

適用於 Java AWS CloudHSM 的軟體程式庫可讓您使用下列操作來產生金鑰和金鑰對函數。

- RSA
- EC
- AES
- DESede (Triple DES)<sup>請參閱備註 1</sup>
- GenericSecret

## 密碼函數

適用於 Java AWS CloudHSM 的軟體程式庫支援下列演算法、模式和填補組合。

| 演算法 | Mode | 填補                                            | 備註                                                                                                                                     |
|-----|------|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| AES | CBC  | AES/CBC/NoPadding<br><br>AES/CBC/PKCS5Padding | 實作 Cipher.ENCRYPT_MODE 和 Cipher.DECRYPT_MODE。<br><br>實作 Cipher.UNWRAP_MODE for AES/CBC NoPadding                                       |
| AES | ECB  | AES/ECB/PKCS5Padding<br><br>AES/ECB/NoPadding | 實作 Cipher.ENCRYPT_MODE 和 Cipher.DECRYPT_MODE。                                                                                          |
| AES | CTR  | AES/CTR/NoPadding                             | 實作 Cipher.ENCRYPT_MODE 和 Cipher.DECRYPT_MODE。                                                                                          |
| AES | GCM  | AES/GCM/NoPadding                             | 實作 Cipher.WRAP_MODE、Cipher.UNWRAP_MODE、Cipher.ENCRYPT_MODE 和 Cipher.DECRYPT_MODE。<br><br>執行 AES-GCM 加密時，HSM 會忽略請求中的初始化向量 (IV)，並使用自己產生的 |

| 演算法             | Mode | 填補                                                                           | 備註                                                                                                           |
|-----------------|------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
|                 |      |                                                                              | IV。操作完成後，您必須呼叫 <code>Cipher.getIV()</code> 以取得 IV。                                                           |
| AESWrap         | ECB  | AESWrap/ECB/NoPadding<br>AESWrap/ECB/PKCS5Padding<br>AESWrap/ECB/ZeroPadding | 實作 <code>Cipher.WRAP_MODE</code> 和 <code>Cipher.UNWRAP_MODE</code> 。                                         |
| DESede (三重 DES) | CBC  | DESede/CBC/PKCS5Padding<br>DESede/CBC/NoPadding                              | 實作 <code>Cipher.ENCRYPT_MODE</code> 和 <code>Cipher.DECRYPT_MODE</code> 。請參閱下列備註 <a href="#">1</a> 查看即將進行的變更。 |
| DESede (三重 DES) | ECB  | DESede/ECB/NoPadding<br>DESede/ECB/PKCS5Padding                              | 實作 <code>Cipher.ENCRYPT_MODE</code> 和 <code>Cipher.DECRYPT_MODE</code> 。請參閱下列備註 <a href="#">1</a> 查看即將進行的變更。 |



| 演算法 | Mode | 填補                                                | 備註                                                                                                       |
|-----|------|---------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| RSA | ECB  | RSA/ECB/P<br>KCS1Padding<br>閱備註 <a href="#">1</a> | 實作 Cipher.WR<br>AP_MODE、Cipher.UN<br>WRAP_MODE<br>、Cipher.EN<br>CRYPT_MODE<br>和 Cipher.DE<br>CRYPT_MODE。 |
|     |      | RSA/ECB/O<br>AEPPadding                           |                                                                                                          |
|     |      | RSA/ECB/O<br>AEPWithSH<br>A-1ANDMGF<br>1Padding   |                                                                                                          |
|     |      | RSA/ECB/O<br>AEPWithSH<br>A-224ANDM<br>GF1Padding |                                                                                                          |
|     |      | RSA/ECB/O<br>AEPWithSH<br>A-256ANDM<br>GF1Padding |                                                                                                          |
|     |      | RSA/ECB/O<br>AEPWithSH<br>A-384ANDM<br>GF1Padding |                                                                                                          |
|     |      | RSA/ECB/O<br>AEPWithSH<br>A-512ANDM<br>GF1Padding |                                                                                                          |
| RSA | ECB  | RSA/ECB/N<br>oPadding                             | 實作 Cipher.EN<br>CRYPT_MODE<br>和 Cipher.DE<br>CRYPT_MODE。                                                 |

| 演算法        | Mode | 填補                                                                                                                                                                                                                                                                                                                                                           | 備註                                        |
|------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| RSAAESWrap | ECB  | RSAAESWrap/ECB/<br>OAEPPadding<br><br>RSAAESWrap/ECB/<br>OAEPWithSHA-<br>1ANDMGF1P<br>adding<br><br>RSAAESWrap/ECB/<br>OAEPWithSHA-<br>224ANDMGF<br>1Padding<br><br>RSAAESWrap/ECB/<br>OAEPWithSHA-<br>256ANDMGF<br>1Padding<br><br>RSAAESWrap/ECB/<br>OAEPWithSHA-<br>384ANDMGF<br>1Padding<br><br>RSAAESWrap/ECB/<br>OAEPWithSHA-<br>512ANDMGF<br>1Padding | 實作 Cipher.WRAP_MODE 和 Cipher.UNWRAP_MODE。 |

## 簽署和驗證函數

適用於 Java AWS CloudHSM 的軟體程式庫支援以下類型的簽章和驗證。使用用戶端 SDK 5 和具有雜湊功能的簽章演算法，資料會先在軟體中進行本機雜湊處理，然後再傳送至 HSM 以進行簽章/驗證。這意味著 SDK 可以對任何大小的資料進行雜湊處理。

## RSA 簽章類型

- NONEwithRSA
- RSASSA-PSS
- SHA1withRSA
- SHA1withRSA/PSS
- SHA1withRSAandMGF1
- SHA224withRSA
- SHA224withRSAandMGF1
- SHA224withRSA/PSS
- SHA256withRSA
- SHA256withRSAandMGF1
- SHA256withRSA/PSS
- SHA384withRSA
- SHA384withRSAandMGF1
- SHA384withRSA/PSS
- SHA512withRSA
- SHA512withRSAandMGF1
- SHA512withRSA/PSS

## ECDSA 簽章類型

- NONEwithECDSA
- SHA1withECDSA
- SHA224withECDSA
- SHA256withECDSA
- SHA384withECDSA
- SHA512withECDSA

## Digest 函數

適用於 Java AWS CloudHSM 的軟體程式庫支援下列訊息摘要。使用用戶端 SDK 5，資料會在軟體中進行本機雜湊處理。這意味著 SDK 可以對任何大小的資料進行雜湊處理。

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

### 雜湊訊息驗證碼 (HMAC) 函數

適用於 Java AWS CloudHSM 的軟體程式庫支援下列 HMAC 演算法。

- HmacSHA1 ( 最大資料大小，以位元組為單位：16288)
- HmacSHA224 ( 最大資料大小，以位元組為單位：16256)
- HmacSHA256 ( 最大資料大小，以位元組為單位：16288)
- HmacSHA384 ( 最大資料大小，以位元組為單位：16224)
- HmacSHA512 ( 最大資料大小，以位元組為單位：16224)

### 加密式訊息驗證程式碼 (CMAC) 函數

CMAC (加密式訊息驗證程式碼) 使用區塊密碼和金鑰建立訊息驗證代碼 (MAC)。與 HMAC 不同之處在於，它們使用 MAC 區塊對稱金鑰方法而非雜湊方法。

適用於 Java AWS CloudHSM 的軟體程式庫支援下列 CMAC 演算法。

- AESCMAC

### 金鑰協議函數

適用於 Java AWS CloudHSM 的軟體程式庫支援具有金鑰衍生函數 (KDF) 的 ECDH。支援下列 KDF 類型：

- ECDHwithX963SHA1KDF 支援 X9.63 KDF SHA1 演算法<sup>2</sup>
- ECDHwithX963SHA224KDF 支援 X9.63 KDF SHA224 演算法<sup>2</sup>
- ECDHwithX963SHA256KDF 支援 X9.63 KDF SHA256 演算法<sup>2</sup>
- ECDHwithX963SHA384KDF 支援 X9.63 KDF SHA384 演算法<sup>2</sup>
- ECDHwithX963SHA512KDF 支援 X9.63 KDF SHA512 演算法<sup>2</sup>

## 使用金鑰 Factory 將金鑰轉換為金鑰規格

您可以使用金鑰工廠將金鑰轉換為金鑰規格。JCE AWS CloudHSM 有兩種類型的金鑰工廠：

**SecretKeyFactory:** 用於匯入或衍生對稱金鑰。使用 **SecretKeyFactory**，您可以傳遞支援的 Key 或支援的 KeySpec 將對稱金鑰匯入或衍生到 AWS CloudHSM。下列是 KeyFactory 支援的規格：

- 如採用 **SecretKeyFactory** 的 **generateSecret** 方法，可支援下列 [KeySpec](#) 類別：
  - **KeyAttributesMap** 可用來匯入具有額外屬性的金鑰位元組做為 CloudHSM 金鑰。可從[此處](#)查看範例。
  - [SecretKeySpec](#) 可將對稱 key spec 匯入為 CloudHSM Key 匯入。
  - **AesCmacKdfParameterSpec** 可使用另一個 CloudHSM AES Key 來衍生對稱金鑰。

### Note

**SecretKeyFactory** 的 **translateKey** 方法接受任何實現[金鑰](#)介面的金鑰。

**KeyFactory:** 用於匯入非對稱金鑰。使用 **KeyFactory**，您可以傳遞支援的 Key 或支援的 KeySpec 將對稱金鑰匯入到 AWS CloudHSM。如需詳細資訊，請參閱下列資源：

- 如採用 **KeyFactory** 的 **generatePublic** 方法，可支援下列 [KeySpec](#) 類別：
- 適用於 RSA 和 EC KeyTypes 的 CloudHSM **KeyAttributesMap** 包括：
  - 適用於 RSA 和 EC Public KeyTypes 的 CloudHSM **KeyAttributesMap** 包括：可從[此處](#)查看範例。
  - 適用於 RSA 和 EC Public Key 的 [X509EncodedKeySpec](#)
  - 適用於 RSA Public Key 的 [RSAPublicKeySpec](#)
  - 適用於 EC Public Key 的 [ECPublicKeySpec](#)
- 如採用 **KeyFactory** 的 **generatePrivate** 方法，可支援下列 [KeySpec](#) 類別：
- 適用於 RSA 和 EC KeyTypes 的 CloudHSM **KeyAttributesMap** 包括：
  - 適用於 RSA 和 EC Public KeyTypes 的 CloudHSM **KeyAttributesMap** 包括：可從[此處](#)查看範例。
  - 適用於 EC and RSA Private Key 的 [PKCS8EncodedKeySpec](#)
  - 適用於 RSA Private Key 的 [RSAPrivateCrtKeySpec](#)
  - 適用於 EC Private Key 的 [ECPrivateKeySpec](#)

如採用 **KeyFactory** 的 **translateKey** 方法，其可接受任何實現[金鑰](#)介面的金鑰。

## 機制註釋

【1】根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

【2】金鑰衍生函數 (KDFs) 會在 [RFC 8418 第 2.1 節](#) 中指定。

## 用戶端 SDK AWS CloudHSM 5 支援的 Java 金鑰屬性

本主題提供有關 AWS CloudHSM 用戶端 SDK 5 支援的 Java 金鑰屬性的資訊。本主題說明如何使用 JCE 提供程序的專屬擴充功能來設定金鑰屬性。請在以下操作期間，使用此擴充功能來設定支援的金鑰屬性及其值：

- 金鑰產生
- 金鑰匯入

如需如何使用金鑰屬性的範例，請參閱 [the section called “程式碼範例”](#)。

### 主題

- [了解屬性](#)
- [支援的屬性](#)
- [設定金鑰的屬性](#)

### 了解屬性

使用金鑰屬性來指定金鑰物件上允許的動作，包括公有金鑰、私有金鑰或秘密金鑰。在建立金鑰物件操作期間定義金鑰屬性和值。

Java Cryptography Extension (JCE) 未指定應該如何設定金鑰屬性的值，因此預設情況下會允許大部分動作。相反地，PKCS#11 標準定義了一組具有更嚴格預設值的完整屬性。從 JCE 提供者 3.1 開始，AWS CloudHSM 提供專屬延伸，可讓您為常用屬性設定更嚴格的值。

### 支援的屬性

您可以設定下表中屬性的值。最佳實務是，只為您希望更有限制性的屬性設定值。如果您未指定值，AWS CloudHSM 會使用下表中指定的預設值。預設值欄位中的空白儲存格表示屬性沒有獲派指定預設值。

| 屬性          | 預設值  |           |           | 備註                                                          |
|-------------|------|-----------|-----------|-------------------------------------------------------------|
|             | 對稱金鑰 | 金鑰對中的公有金鑰 | 金鑰對中的私有金鑰 |                                                             |
| DECRYPT     | TRUE |           | TRUE      | True 表示您可以使用金鑰來解密任何緩衝區。對於其 WRAP 設定為 true 的金鑰，通常將此設定為 FALSE。 |
| DERIVE      |      |           |           | 可以使用金鑰來衍生其他金鑰。                                              |
| ENCRYPT     | TRUE | TRUE      |           | True 表示您可以使用金鑰來加密任何緩衝區。                                     |
| EXTRACTABLE | TRUE |           | TRUE      | True 表示您可以從 HSM 匯出此金鑰。                                      |
| ID          |      |           |           | 用於識別金鑰的使用者定義值。                                              |
| KEY_TYPE    |      |           |           | 用於識別金鑰的類型 (AES、DESe de、一般私密錦綸、EC 或 RSA)。                    |
| LABEL       |      |           |           | 使用者定義的字串可方便您識別 HSM 上的金鑰。為了遵循最佳實                             |

| 屬性           | 預設值  |           |           | 備註                                                                                        |
|--------------|------|-----------|-----------|-------------------------------------------------------------------------------------------|
|              | 對稱金鑰 | 金鑰對中的公有金鑰 | 金鑰對中的私有金鑰 |                                                                                           |
|              |      |           |           | 務，請為每個金鑰使用唯一標籤，以便日後更容易找到。                                                                 |
| LOCAL        |      |           |           | 表示 HSM 產生的金鑰。                                                                             |
| OBJECT_CLASS |      |           |           | 用於識別金鑰 (SecretKey、PublicKey 或 PrivateKey) 的物件類別。                                          |
| PRIVATE      | TRUE | TRUE      | TRUE      | True 表示在使用者通過驗證之前，使用者可能無法存取金鑰。為了清楚起見，使用者在進行身分驗證 AWS CloudHSM 之前無法存取上的任何金鑰，即使此屬性設定為 FALSE。 |



| 屬性     | 預設值   |           |           | 備註                                                                           |
|--------|-------|-----------|-----------|------------------------------------------------------------------------------|
|        | 對稱金鑰  | 金鑰對中的公有金鑰 | 金鑰對中的私有金鑰 |                                                                              |
| SIGN   | TRUE  |           | TRUE      | True 表示您可以使用金鑰來簽署訊息摘要。對於公有金鑰和您已封存的私有金鑰，這通常會設定為 FALSE。                        |
| SIZE   |       |           |           | 定義金鑰大小的屬性。如需有關支援金鑰大小的詳細資訊，請參閱 <a href="#">用戶端 SDK 5 的支援機制</a> 。              |
| TOKEN  | FALSE | FALSE     | FALSE     | 永久金鑰，會跨叢集中的所有 HSM 進行複寫並包含在備份中。TOKEN = FALSE 代表一個暫時性金鑰，該金鑰會在與 HSM 的連接中斷時自動擦除。 |
| UNWRAP | TRUE  |           | TRUE      | True 表示您可以使用金鑰來取消包裝 (匯入) 另一個金鑰。                                              |

| 屬性                | 預設值   |           |           | 備註                                                                                                                                                     |
|-------------------|-------|-----------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | 對稱金鑰  | 金鑰對中的公有金鑰 | 金鑰對中的私有金鑰 |                                                                                                                                                        |
| VERIFY            | TRUE  | TRUE      |           | True 表示您可以使用金鑰來驗證簽章。對於私有金鑰，這通常被設定為 FALSE。                                                                                                              |
| WRAP              | TRUE  | TRUE      |           | True 表示您可以使用該金鑰來包裝另一個金鑰。對於私有金鑰，您通常將此設定為 FALSE。                                                                                                         |
| WRAP_WITH_TRUSTED | FALSE |           | FALSE     | True 表示金鑰只能與 TRUSTED 屬性為 True 的金鑰進行包裝和取消包裝。一旦金鑰 WRAP_WITH_TRUSTED 設置為 True，該屬性僅為只讀狀態，不能將其設置為 False。如要了解有關信任包裝的資訊，請參閱 <a href="#">使用受信任金鑰控制金鑰解除包裝</a> 。 |

**Note**

您可以在 PKCS #11 程式庫中獲得更廣泛的屬性支援。如需詳細資訊，請參閱[支援的 PKCS #11 屬性](#)。

## 設定金鑰的屬性

KeyAttributesMap 是類似 Java 映射的物件，您可以使用它來設定金鑰物件的屬性值。KeyAttributesMap 函數的方法類似於用於 Java 映射處理的方法。

若要設定屬性的自訂值，您有兩個選項：

- 使用下表中列出的方法
- 使用本文稍後示範的產生器模式

屬性映射物件支援以下列方法設定屬性：

| 作業            | 傳回值                                 | KeyAttributesMap 方法      |
|---------------|-------------------------------------|--------------------------|
| 獲取現有金鑰的金鑰屬性的值 | 物件 (包含值) 或 null                     | get(keyAttribute)        |
| 填入一個金鑰屬性的值    | 與金鑰屬性相關聯的先前值，<br>如果金鑰屬性沒有映射，則為 null | put(keyAttribute, value) |
| 填入多個金鑰屬性的值    | N/A                                 | putAll(keyAttributesMap) |
| 從屬性映射中刪除金鑰值對  | 與金鑰屬性相關聯的先前值，<br>如果金鑰屬性沒有映射，則為 null | remove(keyAttribute)     |

**Note**

您未明確指定的任何屬性都會設定為[the section called “支援的屬性”](#)中上表所列的預設值。

## 設定金鑰對的屬性

使用 Java 類別 `KeyPairAttributesMap` 來處理金鑰對的金鑰屬性。`KeyPairAttributesMap` 封裝了兩個 `KeyAttributesMap` 物件；一個用於公有金鑰，另一個用於私有金鑰。

若要分別為公有金鑰和私有金鑰設定個別屬性，您可以在該金鑰對應的 `KeyAttributes` 映射物件上使用 `put()` 方法。使用 `getPublic()` 方法來擷取公有金鑰的屬性映射，以及使用 `getPrivate()` 來擷取私有金鑰的屬性映射。使用 `putAll()` 與金鑰對屬性映射作為引數，填入公有金鑰和私有金鑰對的多個金鑰屬性值。

## Java for Client SDK 5 AWS CloudHSM 軟體程式庫的程式碼範例

本主題提供用戶端 SDK AWS CloudHSM 5 Java 程式碼範例的資源和資訊。

### 先決條件

執行範例之前，您必須先設定環境：

- 安裝並設定 [Java 密碼編譯延伸模組 \(JCE\) 提供者](#)。
- 設定有效的 [HSM 使用者名稱和密碼](#)。加密使用者 (CU) 許可足夠執行這些任務。在每個範例中，您的應用程式會使用這些登入資料來登入 HSM。
- 決定如何提供憑證給 [JCE 提供者](#)。

### 程式碼範例

下列程式碼範例會示範如何使用 [AWS CloudHSM JCE 提供者](#) 來執行基本任務。在 [GitHub](#) 可取得更多程式碼範例。

- [登入 HSM](#)
- [管理金鑰](#)
- [產生對稱金鑰](#)
- [產生非對稱金鑰](#)
- [使用 AES-GCM 進行加密和解密](#)
- [使用 AES-CTR 進行加密和解密](#)
- [使用 DESede-ECB 加密和解密](#) 請參閱附註 1
- [使用 RSA 金鑰簽署和驗證](#)
- [使用 EC 金鑰簽署和驗證](#)

- [使用支援的金鑰屬性](#)
- [使用 CloudHSM 金鑰存放區](#)

【1】根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## AWS CloudHSM JCE 供應商 Javadocs

使用 JCE 提供者 Javadocs 取得 AWS CloudHSM JCE SDK 中定義的 Java 類型和方法的使用資訊。若要下載最新的 Javadocs AWS CloudHSM，請參閱下載頁面上的 [AWS CloudHSM 最新的用戶端 SDK 版本](#) 一節。

您可以將 Javadocs 匯入整合式開發環境 (IDE)，或在網頁瀏覽器中檢視 Javadocs。

## 用戶端 SDK 5 的 AWS CloudHSM KeyStore Java 類別

類別 AWS CloudHSM KeyStore 提供特殊用途的 PKCS12 金鑰存放區。此金鑰存放區可與您的金鑰資料一起儲存憑證，並將其與在 AWS CloudHSM 儲存的金鑰資料連結在一起。KeyStore 類別會實作 Java AWS CloudHSM 密碼編譯延伸模組 (JCE) 的 KeyStore Service Provider Interface (SPI)。如需使用 KeyStore 的詳細資訊，請參閱 [Class KeyStore](#)。

### Note

由於憑證是公開資訊，並且為了最大化密碼編譯金鑰的儲存容量，AWS CloudHSM 不支援在 HSMs 上儲存憑證。

為 AWS CloudHSM 用戶端 SDK 5 選擇適當的金鑰存放區

AWS CloudHSM Java 密碼編譯延伸 (JCE) 供應商提供特殊用途的 AWS CloudHSM KeyStore。類別 AWS CloudHSM KeyStore 支援將金鑰操作卸載至 HSM、本機儲存憑證和以憑證為基礎的操作。

載入特殊用途的 CloudHSM 金鑰存放區，如下所示：

```
KeyStore ks = KeyStore.getInstance("CloudHSM")
```

## 初始化 AWS CloudHSM KeyStore 用戶端 SDK 5

以您登入 JCE 提供者的相同方式登入 AWS CloudHSM KeyStore。您可以使用環境變數或系統屬性檔案，並且在開始使用 CloudHSM 金鑰存放區之前應先登入。如需使用 JCE 提供者登入 HSM 的範例，請參閱[登入 HSM](#)。

如有需要，您可以指定一組密碼來加密保存金鑰儲存資料的本機 PKCS12 檔案。當您建立 AWS CloudHSM Keystore 時，您可以設定密碼，並在使用載入、設定和取得方法時提供密碼。

請依照以下方式，將新的 CloudHSM 金鑰存放區物件執行個體化：

```
ks.load(null, null);
```

使用 store 方法將金鑰存放區資料寫入檔案。從那時起，您可以依照以下方式，搭配來源檔案和密碼使用 load 方法載入現有的金鑰存放區：

```
ks.load(inputStream, password);
```

## Use AWS CloudHSM KeyStore 或 AWS CloudHSM 用戶端 SDK 5

AWS CloudHSM KeyStore 符合 JCE [類別 KeyStore](#) 規格，並提供下列函數。

- load

從特定的輸入串流載入金鑰存放區。如果在儲存金鑰存放區時設定了密碼，則必須提供相同的密碼才能成功載入。將這兩個參數設為 Null 以初始化一個新的空金鑰存放區。

```
KeyStore ks = KeyStore.getInstance("CloudHSM");
ks.load(inputStream, password);
```

- aliases

傳回特定的金鑰存放區執行個體中的所有項目別名名稱列舉。結果包括本機儲存在 PKCS12 檔案中的物件，以及常駐於 HSM 的物件。

範本程式碼：

```
KeyStore ks = KeyStore.getInstance("CloudHSM");
for(Enumeration<String> entry = ks.aliases(); entry.hasMoreElements();) {
 String label = entry.nextElement();
 System.out.println(label);
}
```

```
}
```

- `containsalias`

如果金鑰存放區可存取至少一個有指定別名的物件，則傳回 `True`。金鑰存放區會檢查本機儲存在 PKCS12 檔案中的物件，以及常駐於 HSM 的物件。

- `deleteEntry`

從本機 PKCS12 檔案刪除憑證項目。不支援使用 AWS CloudHSM KeyStore 刪除存放在 HSM 中的金鑰資料。您可以使用[可銷毀](#)介面 `destroy` 的銷毀方法刪除金鑰。

```
((Destroyable) key).destroy();
```

- `getCertificate`

如果可用，則傳回與別名相關聯的憑證。如果別名不存在或參考非憑證的物件，則函數會傳回 `NULL`。

```
KeyStore ks = KeyStore.getInstance("CloudHSM");
Certificate cert = ks.getCertificate(alias);
```

- `getCertificateAlias`

傳回第一個資料符合特定憑證的金鑰存放區項目名稱 (別名)。

```
KeyStore ks = KeyStore.getInstance("CloudHSM");
String alias = ks.getCertificateAlias(cert);
```

- `getCertificateChain`

傳回與特定別名相關聯的憑證鏈。如果別名不存在或參考非憑證的物件，則函數會傳回 `NULL`。

- `getCreationDate`

傳回由給定別名辨識的項目建立日期。如果沒有建立日期，則函數會傳回憑證生效的日期。

- `getKey`

`GetKey` 會傳遞給 HSM 並傳回與特定標籤對應的金鑰物件。由於 `getKey` 會直接查詢 HSM，因此無論金鑰存放區是否產生金鑰，都可用於 HSM 上的任何金鑰。

```
Key key = ks.getKey(keyLabel, null);
```

- `isCertificateEntry`

檢查有特定別名的項目是否代表憑證項目。

- `isKeyEntry`

檢查有特定別名的項目是否代表金鑰項目。此動作會在 PKCS12 檔案和 HSM 中搜尋別名。

- `setCertificateEntry`

指定特定憑證至特定別名。如果特定的別名已用於識別金鑰或憑證，則會擲出 `KeyStoreException`。您可以使用 JCE 程式碼來取得金鑰物件，然後使用金鑰存放區 `SetKeyEntry` 方法連結憑證至密鑰。

- 有 `byte[]` 金鑰的 `setKeyEntry`

用戶端 SDK 5 目前不支援此 API。

- 有 `Key` 物件的 `setKeyEntry`

指定特定金鑰至特定別名，並將其儲存在 HSM 內。如果該金鑰未儲存在 HSM 內，則該金鑰將做為可擷取的工作階段金鑰匯入至 HSM。

如果 `Key` 物件屬於類型 `PrivateKey`，則必須附有相對應的憑證鏈。

如果別名已經存在，則 `SetKeyEntry` 呼叫會擲出 `KeyStoreException` 並防止覆寫金鑰。如果必須覆寫金鑰，請使用 `KMU` 或 `JCE`。

- `engineSize`

傳回金鑰存放區中的項目數目。

- `store`

以 PKCS12 檔案格式儲存金鑰存放區至特定輸出串流，並使用特定的密碼加以保護。此外，它仍然保留載入的金鑰 (使用 `setKey` 呼叫的組合)。

## AWS CloudHSM JCE for Client SDK 5 的進階組態

AWS CloudHSM JCE 供應商包含下列進階組態，這些組態不屬於大多數客戶使用的一般組態。

- [連接至多個叢集](#)

- [使用 JCE 擷取金鑰](#)



- [重試適用於 JCE 的組態](#)

## 使用 JCE 供應商連線至多個 AWS CloudHSM 叢集

此組態允許單一用戶端執行個體與多個 AWS CloudHSM 叢集通訊。與單一執行個體僅能與單一叢集進行通訊相比，該組態可節省某些使用案例的成本。CloudHsmProvider 類別 AWS CloudHSM 是 [Java Security 提供者類別](#) 的實作。此類別的每個執行個體都代表整個 AWS CloudHSM 叢集的連線。您可以將此類別實例化，並將其新增至 Java 安全提供者清單中，以便您可以使用標準的 JCE 類別與其進行互動。

下面範例會將此類別實例化，並將其新增至 Java 安全提供者清單：

```
if (Security.getProvider(CloudHsmProvider.PROVIDER_NAME) == null) {
 Security.addProvider(new CloudHsmProvider());
}
```

可以使用下列兩種方式來對 CloudHsmProvider 進行設定：

1. 使用檔案進行設定 (預設組態)
2. 使用程式碼設定

下列主題說明這些組態，以及如何連線至多個叢集。

### 主題

- [使用 檔案設定 AWS CloudHSMCloudHsmProvider 類別 \(預設組態\)](#)
- [使用程式碼設定 AWS CloudHSMCloudHsmProvider 類別](#)
- [連線至多個 AWS CloudHSM 叢集](#)

## 使用 檔案設定 AWS CloudHSMCloudHsmProvider 類別 (預設組態)

設定類別 AWS CloudHSM CloudHsmProvider 的預設方法是使用 檔案。

當您使用預設建構函數實例化 CloudHsmProvider 時，根據預設，它會在 Linux 的 /opt/cloudhsm/etc/cloudhsm-jce.cfg 路徑中尋找組態檔案。可使用 configure-jce 設定此組態檔案。

使用預設的建構函數所建立的物件將會使用預設的 CloudHSM 提供者名稱 CloudHSM。提供者名稱有助於與 JCE 進行互動，以讓它了解各種作業應使用哪個提供者。以下為使用 CloudHSM 提供者名稱進行加密作業的範例：

```
Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding", "CloudHSM");
```

### 使用程式碼設定 AWS CloudHSM **CloudHsmProvider** 類別

從用戶端 SDK 5.8.0 版開始，您也可以使用 Java 程式碼來設定 AWS CloudHSM **CloudHsmProvider** 類別。使用 **CloudHsmProviderConfig** 類別的物件可以進行設定。您可以使用 **CloudHsmProviderConfigBuilder** 建置此物件。

**CloudHsmProvider** 有另一個接受 **CloudHsmProviderConfig** 物件的建構函數，如下列範例顯示。

#### Example

```
CloudHsmProviderConfig config = CloudHsmProviderConfig.builder()
 .withCluster(
 CloudHsmCluster.builder()
 .withHsmCAFilePath(hsmCAFilePath)

 .withClusterUniqueIdentifier("CloudHsmCluster1")
 .withServer(CloudHsmServer.builder().withHostIP(hostName).build())
 .build()
).build();
CloudHsmProvider provider = new CloudHsmProvider(config);
```

在此範例中，JCE 提供者的名稱為 **CloudHsmCluster1**。這是應用程式可用來與 JCE 互動的名稱：

#### Example

```
Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding", "CloudHsmCluster1");
```

或者，應用程式還可以使用上面建立的提供者物件，讓 JCE 了解要使用該提供者以進行作業：

```
Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding", provider);
```

如果未使用 **withClusterUniqueIdentifier** 方法指定唯一識別碼，則會為您建立一個隨機產生的提供者名稱。若要取得此隨機產生的識別碼，應用程式可以呼叫 **provider.getName()** 以取得識別碼。

## 連線至多個 AWS CloudHSM 叢集

每個 `CloudHsmProvider` 代表 AWS CloudHSM 叢集的連線。如果您想要從同一個應用程式與另一個叢集進行通訊，您可以使用其他叢集的組態建立另一個物件 `CloudHsmProvider`，然後您可以使用提供者物件或使用提供者名稱與該叢集互動，如下列範例所顯示。

### Example

```
CloudHsmProviderConfig config = CloudHsmProviderConfig.builder()
 .withCluster(
 CloudHsmCluster.builder()
 .withHsmCAFilePath(hsmCAFilePath)

.withClusterUniqueIdentifier("CloudHsmCluster1")
 .withServer(CloudHsmServer.builder().withHostIP(hostName).build())
 .build())
 .build();
CloudHsmProvider provider1 = new CloudHsmProvider(config);

if (Security.getProvider(provider1.getName()) == null) {
 Security.addProvider(provider1);
}

CloudHsmProviderConfig config2 = CloudHsmProviderConfig.builder()
 .withCluster(
 CloudHsmCluster.builder()
 .withHsmCAFilePath(hsmCAFilePath2)

.withClusterUniqueIdentifier("CloudHsmCluster2")
 .withServer(CloudHsmServer.builder().withHostIP(hostName2).build())
 .build())
 .build();
CloudHsmProvider provider2 = new CloudHsmProvider(config2);

if (Security.getProvider(provider2.getName()) == null) {
 Security.addProvider(provider2);
}
```

設定上述兩個提供者 (兩個叢集) 後，您可以使用提供者物件或使用提供者名稱與其進行互動。

此範例顯示了如何與 `cluster1` 進行通訊，在此基礎上，您可以使用下列範例進行 AES/GCM/NoPadding 操作。

```
Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding", provider1);
```

在同一個應用程式中使用提供者名稱在第二個叢集上產生「AES」金鑰，您還可以使用下列範例：

```
Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding", provider2.getName());
```

## 使用 JCE for 擷取金鑰 AWS CloudHSM

Java 密碼編譯延伸模組 (JCE) 使用允許插入不同密碼編譯實作的架構。會將密碼編譯操作卸載至 HSM 的其中一個 JCE 提供者 AWS CloudHSM 運送。對於使用儲存在 AWS CloudHSM 中金鑰的其他大多數 JCE 提供者，他們必須將金鑰位元組以純文字形式從 HSM 擷取到機器的記憶體中以供使用。HSM 通常僅允許將金鑰擷取為包裝物件，而非純文字。不過，為了支援供應商間整合使用案例，AWS CloudHSM 允許選擇加入組態選項，以明確地擷取金鑰位元組。

### Important

只要指定 AWS CloudHSM 供應商或使用 AWS CloudHSM 金鑰物件，JCE AWS CloudHSM 就會將操作卸載至。如果您預期在 HSM 內進行作業，則您不需要以純文字形式擷取金鑰。當您的應用程式因第三方程式庫或 JCE 提供者的限制而無法使用安全機制 (例如，包裝和取消包裝金鑰) 時，僅需要以純文字形式擷取金鑰。

根據預設，AWS CloudHSM JCE 提供者允許擷取公有金鑰以使用外部 JCE 提供者。一律允許使用下列方法：

| 類別                       | 方法                  | Format (getEncoded) |
|--------------------------|---------------------|---------------------|
| EcPublicKey              | getEncoded()        | X.509               |
|                          | getW()              | N/A                 |
| RSAPublicKey             | getEncoded()        | X.509               |
|                          | getPublicExponent() | N/A                 |
| CloudHsmRsaPrivateCrtKey | getPublicExponent() | N/A                 |

根據預設，AWS CloudHSM JCE 提供者不允許擷取私有或私密金鑰的清除金鑰位元組。如果您的使用案例需要，您可在下列情況下以純文字形式擷取私用金鑰或秘密金鑰的金鑰位元組：

1. 私用金鑰和秘密金鑰的 `EXTRACTABLE` 屬性設定為 `true`。
  - 根據預設，私用金鑰和秘密金鑰的 `EXTRACTABLE` 屬性設定為 `true`。`EXTRACTABLE` 金鑰是允許從 HSM 匯出的金鑰。如需詳細資訊，請參閱 [Client SDK 5](#) 支援的 Java 屬性。
2. 私用金鑰和私密金鑰的 `WRAP_WITH_TRUSTED` 屬性設定為 `false`。
  - `getEncoded`、`getPrivateExponent` 和 `getS` 不能與無法以純文字形式匯出的私用金鑰搭配使用。`WRAP_WITH_TRUSTED` 不允許您的私用金鑰以純文字形式匯出 HSM。如需詳細資訊，請參閱 [使用受信任的金鑰控制金鑰取消包裝](#)。

允許 JCE 供應商從 中擷取私有金鑰秘密 AWS CloudHSM

使用下列步驟允許 AWS CloudHSM JCE 提供者擷取您的私有金鑰秘密。

#### Important

變更此組態後，就可以從 HSM 叢集以純文字形式擷取所有 `EXTRACTABLE` 金鑰位元組。為了獲得更好的安全性，您應考慮使用 [金鑰包裝方法](#) 將金鑰安全地從 HSM 擷取出來。這可防止意外從 HSM 擷取金鑰位元組。

1. 使用下列命令，可在 JCE 中啟用您的私用金鑰或秘密金鑰：

Linux

```
$ /opt/cloudhsm/bin/configure-jce --enable-clear-key-extraction-in-software
```

Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" --enable-clear-key-extraction-in-software
```

2. 啟用以純文字形式擷取金鑰後，即可啟用下列方法將私用金鑰擷取至記憶體。

| 類別               | 方法                   | Format (getEncoded) |
|------------------|----------------------|---------------------|
| 金鑰               | getEncoded()         | RAW                 |
| ECPrivateKey     | getEncoded()         | PKCS#8              |
|                  | getS()               | N/A                 |
| RSAPrivateCrtKey | getEncoded()         | X.509               |
|                  | getPrivateExponent() | N/A                 |
|                  | getPrimeP()          | N/A                 |
|                  | getPrimeQ()          | N/A                 |
|                  | getPrimeExponentP()  | N/A                 |
|                  | getPrimeExponentQ()  | N/A                 |
|                  | getCrtCoefficient()  | N/A                 |

如果您想還原預設行為，且不允許 JCE 以純文字形式匯出金鑰，請執行下列命令：

#### Linux

```
$ /opt/cloudhsm/bin/configure-jce --disable-clear-key-extraction-in-software
```

#### Windows

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" --disable-clear-key-extraction-in-software
```

#### 重試適用於的 JCE 命令 AWS CloudHSM

AWS CloudHSM 用戶端 SDK 5.8.0 和更新版本具有內建的自動重試策略，將從用戶端重試 HSM 限流操作。當 HSM 因過於忙於執行先前操作而無法接受更多要求而限制操作時，用戶端 SDK 會嘗試重試

限流操作 (最多 3 次)，同時以指數形式回退。此自動重試策略可以設定為兩種模式中的其中一種：關閉模式和標準模式。

- 關閉：用戶端 SDK 將不會針對 HSM 的任何限流操作執行任何重試政策。
- 標準：這是用戶端 SDK 5.8.0 及更新版本的預設模式。在此模式下，用戶端 SDK 會以指數回退形式自動重試限流操作。

如需詳細資訊，請參閱[HSM 調節](#)。

將重試命令設定為關閉模式

Linux

將 Linux 上用戶端 SDK 5 重試命令設定為 off

- 您可以使用下列命令將重試組態設定為 off 模式：

```
$ sudo /opt/cloudhsm/bin/configure-jce --default-retry-mode off
```

Windows

將 Windows 上用戶端 SDK 5 重試命令設定為 off

- 您可以使用下列命令將重試組態設定為 off 模式：

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\configure-jce.exe" --default-retry-mode off
```

## 使用先前的 SDK 版本來使用 AWS CloudHSM

 SDK 5.8.0 版和更早版本已終止支援。2025 年 3 月 31 日之後，開發套件 3.4.4 版及更早版本的文件將不再提供。

AWS CloudHSM 包含兩個主要用戶端 SDK 版本：

- 用戶端 SDK 5：這是我們最新預設的用戶端 SDK。如需有關其優點和優勢的資訊，請參閱 [AWS CloudHSM 用戶端 SDK 5 的優點](#)。
- 用戶端 SDK 3：這是我們較舊的用戶端 SDK。它包括一組完整的組件，用於基於平台和語言的應用程序兼容性和管理工具。

如需從用戶端 SDK 3 遷移至用戶端 SDK 5 的指示，請參閱 [從 AWS CloudHSM 用戶端 SDK 3 遷移至用戶端 SDK 5](#)。

本主題說明用戶端 SDK 3。若要查看您正在使用的用戶端 SDK 版本，請參閱 [檢查您的 AWS CloudHSM 用戶端 SDK 版本](#)。

若要下載，請參閱 [下載](#)。

### 主題

- [在 Linux 上升級 AWS CloudHSM 用戶端 SDK 3](#)
- [AWS CloudHSM 用戶端 SDK 3 支援的平台](#)
- [AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫](#)
- [適用於 AWS CloudHSM 用戶端 SDK 3 的 OpenSSL 動態引擎](#)
- [AWS CloudHSM 用戶端 SDK 3 的 JCE 提供者](#)
- [密碼編譯 API：的新一代 \(CNG\) 和金鑰儲存供應商 \(KSP\) AWS CloudHSM](#)

## 在 Linux 上升級 AWS CloudHSM 用戶端 SDK 3

 SDK 5.8.0 版及更早版本已終止支援。2025 年 3 月 31 日之後，開發套件 3.4.4 版及更早版本的文件將不再提供。

使用 AWS CloudHSM 用戶端 SDK 3.1 和更新版本，用戶端協助程式的版本和您安裝的任何元件都必須相符才能升級。對於所有 Linux 系統，您必須使用單一命令，以相同版本的 PKCS #11 程式庫、Java 密碼編譯延伸模組 (JCE) 提供者或 OpenSSL 動態引擎來批次升級用戶端常駐程式。這項需求不適用於 Windows 系統，因為 CNG 和 KSP 提供者的二進位檔案已經包含在用戶端常駐程式套件中。

### 檢查用戶端常駐程式版本

- 在基於 Red Hat 的 Linux 系統 (包括 Amazon Linux 和 CentOS) 上，使用以下命令：



```
rpm -qa | grep ^cloudhsm
```

- 在基於 Debian 的 Linux 系統上，請使用下列命令：

```
apt list --installed | grep ^cloudhsm
```

- 在 Windows 系統上，請使用下列命令：

```
wmic product get name,version
```

## 主題

- [先決條件](#)
- [步驟 1：停止用戶端常駐程式](#)
- [步驟 2：升級用戶端 SDK](#)
- [步驟 3：啟動用戶端常駐程式](#)

## 先決條件

下載最新版本的 AWS CloudHSM 用戶端協助程式，然後選擇您的元件。

### Note

您不必安裝所有元件。對於已安裝的每個元件，您必須升級該元件以符合用戶端常駐程式的版本。

## 最新的 Linux 用戶端常駐程式

### Amazon Linux

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-latest.el6.x86_64.rpm
```

## Amazon Linux 2

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-latest.el7.x86_64.rpm
```

## CentOS 7

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-latest.el7.x86_64.rpm
```

## CentOS 8

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-latest.el8.x86_64.rpm
```

## RHEL 7

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-latest.el7.x86_64.rpm
```

## RHEL 8

```
sudo yum install wget
```

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-latest.el8.x86_64.rpm
```

## Ubuntu 16.04 LTS

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-client_latest_amd64.deb
```

## Ubuntu 18.04 LTS

```
wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Bionic/cloudhsm-client_latest_u18.04_amd64.deb
```

## 最新的 PKCS #11 程式庫

### Amazon Linux

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-pkcs11-latest.el6.x86_64.rpm
```

### Amazon Linux 2

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-pkcs11-latest.el7.x86_64.rpm
```

### CentOS 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-pkcs11-latest.el7.x86_64.rpm
```

### CentOS 8

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-pkcs11-latest.el8.x86_64.rpm
```

### RHEL 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-pkcs11-latest.el7.x86_64.rpm
```

### RHEL 8

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-pkcs11-latest.el8.x86_64.rpm
```

## Ubuntu 16.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-client-pkcs11_latest_amd64.deb
```

## Ubuntu 18.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Bionic/cloudhsm-client-pkcs11_latest_u18.04_amd64.deb
```

## 最新的 OpenSSL 動態引擎

## Amazon Linux

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-dyn-latest.el6.x86_64.rpm
```

## Amazon Linux 2

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-dyn-latest.el7.x86_64.rpm
```

## CentOS 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-dyn-latest.el7.x86_64.rpm
```

## RHEL 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-dyn-latest.el7.x86_64.rpm
```

## Ubuntu 16.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-client-dyn_latest_amd64.deb
```

## 最新的 JCE 提供者

### Amazon Linux

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-jce-latest.el6.x86_64.rpm
```

### Amazon Linux 2

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-jce-latest.el7.x86_64.rpm
```

### CentOS 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-jce-latest.el7.x86_64.rpm
```

### CentOS 8

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-jce-latest.el8.x86_64.rpm
```

### RHEL 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-jce-latest.el7.x86_64.rpm
```

### RHEL 8

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-jce-latest.el8.x86_64.rpm
```

### Ubuntu 16.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-client-jce_latest_amd64.deb
```

## Ubuntu 18.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Bionic/cloudhsm-client-jce_latest_u18.04_amd64.deb
```

### 步驟 1：停止用戶端常駐程式

使用以下命令來停止用戶端常駐程式。

#### Amazon Linux

```
$ sudo stop cloudhsm-client
```

#### Amazon Linux 2

```
$ sudo service cloudhsm-client stop
```

#### CentOS 7

```
$ sudo service cloudhsm-client stop
```

#### CentOS 8

```
$ sudo service cloudhsm-client stop
```

#### RHEL 7

```
$ sudo service cloudhsm-client stop
```

#### RHEL 8

```
$ sudo service cloudhsm-client stop
```

#### Ubuntu 16.04 LTS

```
$ sudo service cloudhsm-client stop
```

## Ubuntu 18.04 LTS

```
$ sudo service cloudhsm-client stop
```

## 步驟 2：升級用戶端 SDK

下列命令顯示升級用戶端常駐程式和元件所需的語法。執行命令之前，請先移除任何您不想升級的元件。

### Amazon Linux

```
$ sudo yum install ./cloudhsm-client-latest.el6.x86_64.rpm \
 <./cloudhsm-client-pkcs11-latest.el6.x86_64.rpm> \
 <./cloudhsm-client-dyn-latest.el6.x86_64.rpm> \
 <./cloudhsm-client-jce-latest.el6.x86_64.rpm>
```

### Amazon Linux 2

```
$ sudo yum install ./cloudhsm-client-latest.el7.x86_64.rpm \
 <./cloudhsm-client-pkcs11-latest.el7.x86_64.rpm> \
 <./cloudhsm-client-dyn-latest.el7.x86_64.rpm> \
 <./cloudhsm-client-jce-latest.el7.x86_64.rpm>
```

### CentOS 7

```
$ sudo yum install ./cloudhsm-client-latest.el7.x86_64.rpm \
 <./cloudhsm-client-pkcs11-latest.el7.x86_64.rpm> \
 <./cloudhsm-client-dyn-latest.el7.x86_64.rpm> \
 <./cloudhsm-client-jce-latest.el7.x86_64.rpm>
```

### CentOS 8

```
$ sudo yum install ./cloudhsm-client-latest.el8.x86_64.rpm \
 <./cloudhsm-client-pkcs11-latest.el8.x86_64.rpm> \
 <./cloudhsm-client-jce-latest.el8.x86_64.rpm>
```

### RHEL 7

```
$ sudo yum install ./cloudhsm-client-latest.el7.x86_64.rpm \
 <./cloudhsm-client-pkcs11-latest.el7.x86_64.rpm> \
 <./cloudhsm-client-jce-latest.el7.x86_64.rpm>
```

```
<./cloudhsm-client-pkcs11-latest.el7.x86_64.rpm> \
<./cloudhsm-client-dyn-latest.el7.x86_64.rpm> \
<./cloudhsm-client-jce-latest.el7.x86_64.rpm>
```

## RHEL 8

```
$ sudo yum install ./cloudhsm-client-latest.el8.x86_64.rpm \
 <./cloudhsm-client-pkcs11-latest.el8.x86_64.rpm> \
 <./cloudhsm-client-jce-latest.el8.x86_64.rpm>
```

## Ubuntu 16.04 LTS

```
$ sudo apt install ./cloudhsm-client_latest_amd64.deb \
 <cloudhsm-client-pkcs11_latest_amd64.deb> \
 <cloudhsm-client-dyn_latest_amd64.deb> \
 <cloudhsm-client-jce_latest_amd64.deb>
```

## Ubuntu 18.04 LTS

```
$ sudo apt install ./cloudhsm-client_latest_u18.04_amd64.deb \
 <cloudhsm-client-pkcs11_latest_amd64.deb> \
 <cloudhsm-client-jce_latest_amd64.deb>
```

## 步驟 3：啟動用戶端常駐程式

使用下列命令來啟動用戶端常駐程式。

### Amazon Linux

```
$ sudo start cloudhsm-client
```

### Amazon Linux 2

```
$ sudo service cloudhsm-client start
```

### CentOS 7

```
$ sudo service cloudhsm-client start
```



## CentOS 8

```
$ sudo service cloudhsm-client start
```

## RHEL 7

```
$ sudo service cloudhsm-client start
```

## RHEL 8

```
$ sudo service cloudhsm-client start
```

## Ubuntu 16.04 LTS

```
$ sudo service cloudhsm-client start
```

## Ubuntu 18.04 LTS

```
$ sudo service cloudhsm-client start
```

## Ubuntu 20.04 LTS

```
$ sudo service cloudhsm-client start
```

## Ubuntu 22.04 LTS

目前尚未提供對 OpenSSL 動態引擎的支援。

## AWS CloudHSM 用戶端 SDK 3 支援的平台

 SDK 5.8.0 版及更早版本已終止支援。2025 年 3 月 31 日之後，開發套件 3.4.4 版及更早版本的文件將不再提供。

AWS CloudHSM 用戶端 SDK 3 需要用戶端協助程式，並提供命令列工具，包括 CloudHSM Management Utility (CMU)、金鑰管理公用程式 (KMU) 和設定工具。

AWS CloudHSM 用戶端 SDK 的每個版本的基本支援都不同。SDK 中元件的平台通常支援與基礎支援相符，但並非總是如此。若要判斷特定元件的平台支援，請先確定您想要的平台出現在 SDK 的基礎區段中，然後檢查元件區段中是否有任何排除或任何其他相關資訊。

平台支援會隨時間變更。舊版 CloudHSM 用戶端 SDK 可能不支援此處列出的所有作業系統。使用版本說明來判斷舊版 CloudHSM 用戶端 SDK 的作業系統支援。如需詳細資訊，請參閱[AWS CloudHSM 用戶端 SDK 的下載](#)。

AWS CloudHSM 僅支援 64 位元作業系統。

## 主題

- [Linux 支援 AWS CloudHSM 用戶端 SDK 3](#)
- [Windows 支援 AWS CloudHSM 用戶端 SDK 3](#)
- [AWS CloudHSM 用戶端 SDK 3 的 HSM 相容性](#)

## Linux 支援 AWS CloudHSM 用戶端 SDK 3

AWS CloudHSM 用戶端 SDK 3 支援下列 Linux 作業系統和平台。

- Amazon Linux
- Amazon Linux 2
- CentOS 6.10+<sup>2</sup>
- CentOS 7.3+
- CentOS 8<sup>1,4</sup>
- Red Hat Enterprise Linux (RHEL) 6.10+<sup>2</sup>
- Red Hat Enterprise Linux (RHEL) 7.3+
- Red Hat Enterprise Linux (RHEL) 8<sup>1</sup>
- Ubuntu 16.04 LTS<sup>3</sup>
- Ubuntu 18.04 LTS<sup>1</sup>

[1] 不支援 OpenSSL 動態引擎。如需詳細資訊，請參閱 [OpenSSL 動態引擎](#)。

[2] 不支援用戶端 SDK 3.3.0 及更高版本。

[3] SDK 3.4 是 Ubuntu 16.04 上最後一個受支援的版本。

[4] SDK 3.4 是 CentOS 8.3+ 上最後一個受支援的版本。

## Windows 支援 AWS CloudHSM 用戶端 SDK 3

AWS CloudHSM 用戶端 SDK 3 支援下列版本的 Windows Server。

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

## AWS CloudHSM 用戶端 SDK 3 的 HSM 相容性

下表說明 HSMs 的 AWS CloudHSM 用戶端 SDK 3 相容性。

| hsm1.medium               | hsm2m.medium |
|---------------------------|--------------|
| 與用戶端版本 SDK 3.1.0 及更新版本相容。 | 不支援。         |

## AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫

PKCS #11 是對中的硬體安全模組 (HSM) 執行密碼編譯操作的標準 AWS CloudHSM。

如需關於啟動載入的資訊，請參閱 [連接至叢集](#)。

### 主題

- [安裝 AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫](#)
- [驗證用戶端 SDK 3 的 AWS CloudHSM PKCS #11 程式庫](#)
- [用戶端 SDK 3 的 PKCS #11 程式庫 AWS CloudHSM 支援的金鑰類型](#)
- [AWS CloudHSM 用戶端 SDK 3 支援的機制](#)
- [AWS CloudHSM 用戶端 SDK 3 支援的 API 操作](#)
- [用戶端 SDK 3 的 AWS CloudHSM PKCS #11 程式庫中的關鍵屬性](#)
- [用戶端 SDK AWS CloudHSM 3 的 PKCS #11 程式庫程式碼範例](#)

## 安裝 AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫

本主題提供安裝 AWS CloudHSM 用戶端 SDK 3 版本系列的 PKCS #11 程式庫的說明。如需關於用戶端 SDK 或 PKCS #11 程式庫的詳細資訊，請參閱[使用用戶端 SDK](#) 和 [PKCS #11 程式庫](#)。

用戶端 SDK 3 的先決條件

PKCS #11 程式庫需要 AWS CloudHSM 用戶端。

如果您尚未安裝和設定 AWS CloudHSM 用戶端，請現在依照 中的步驟執行[安裝用戶端 \(Linux\)](#)。安裝和設定用戶端之後，請使用以下命令來啟動用戶端。

Amazon Linux

```
$ sudo start cloudhsm-client
```

Amazon Linux 2

```
$ sudo systemctl cloudhsm-client start
```

CentOS 7

```
$ sudo systemctl cloudhsm-client start
```

CentOS 8

```
$ sudo systemctl cloudhsm-client start
```

RHEL 7

```
$ sudo systemctl cloudhsm-client start
```

RHEL 8

```
$ sudo systemctl cloudhsm-client start
```

Ubuntu 16.04 LTS

```
$ sudo systemctl cloudhsm-client start
```

## Ubuntu 18.04 LTS

```
$ sudo systemctl cloudhsm-client start
```

## Ubuntu 20.04 LTS

```
$ sudo systemctl cloudhsm-client start
```

## 安裝用戶端 SDK 3 的 PKCS #11 程式庫

下列命令會下載和安裝 PKCS #11 程式庫。

### Amazon Linux

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-pkcs11-latest.el6.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-pkcs11-latest.el6.x86_64.rpm
```

### Amazon Linux 2

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-pkcs11-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-pkcs11-latest.el7.x86_64.rpm
```

### CentOS 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-pkcs11-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-pkcs11-latest.el7.x86_64.rpm
```

### CentOS 8

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-pkcs11-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-pkcs11-latest.el8.x86_64.rpm
```

## RHEL 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-pkcs11-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-pkcs11-latest.el7.x86_64.rpm
```

## RHEL 8

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-pkcs11-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-pkcs11-latest.el8.x86_64.rpm
```

## Ubuntu 16.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-client-pkcs11_latest_amd64.deb
```

```
$ sudo apt install ./cloudhsm-client-pkcs11_latest_amd64.deb
```

## Ubuntu 18.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Bionic/cloudhsm-client-pkcs11_latest_u18.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-client-pkcs11_latest_u18.04_amd64.deb
```

- 如果您安裝了 PKCS #11 程式庫的 EC2 執行個體中沒有安裝用戶端 SDK 3 的其他元件，則您必須啟動用戶端 SDK 3。您只需要在每個執行個體上使用用戶端 SDK 3 的元件執行一次。
- 您可於下列位置找到 PKCS #11 程式庫檔案：

Linux 二進位檔案、組態指令碼、憑證和日誌檔案：

```
/opt/cloudhsm/lib
```

## 驗證用戶端 SDK 3 的 AWS CloudHSM PKCS #11 程式庫

當您使用 PKCS #11 程式庫時，您的應用程式會在 HSMs 中以特定[加密使用者 \(CU\)](#) 身分執行 AWS CloudHSM。您的應用程式只能檢視和管理 CU 所擁有和共用的金鑰。您可以使用 HSM 中現有的 CU，或建立新的 CU。如需關於管理 CU 的資訊，請參閱[使用 CloudHSM CLI 管理 HSM 使用者](#)和[使用 CloudHSM 管理公用程式 \(CMU\) 管理 HSM 使用者](#)。

若要將 CU 指定給 PKCS #11 程式庫，請使用 PKCS #11 [C\\_Login 函數](#) 的 pin 參數。對於 AWS CloudHSM，接腳參數的格式如下：

```
<CU_user_name>:<password>
```

例如，以下命令會將 PKCS #11 程式庫 pin 設定給使用者名稱為 CryptoUser 和密碼為 CUPassword123! 的 CU。

```
CryptoUser:CUPassword123!
```

## 用戶端 SDK 3 的 PKCS #11 程式庫 AWS CloudHSM 支援的金鑰類型

PKCS #11 程式庫支援用戶端 AWS CloudHSM SDK 3 的下列金鑰類型。

| 金鑰類型          | 描述                                                                                                          |
|---------------|-------------------------------------------------------------------------------------------------------------|
| RSA           | 產生 2048 位元至 4096 位元的 RSA 金鑰，以 256 位元為單位遞增。                                                                  |
| EC            | 使用 secp224r1 (P-224)、secp256r1 (P-256)、secp256k1 (Blockchain)、secp384r1 (P-384) 和 secp521r1 (P-521) 曲線產生金鑰。 |
| AES           | 產生 128 位元、192 位元和 256 位元的 AES 金鑰。                                                                           |
| DES3 (三重 DES) | 產生 192 位元 DES3 金鑰。請參閱下列備註 <a href="#">1</a> 查看即將進行的變更。                                                      |

| 金鑰類型           | 描述                  |
|----------------|---------------------|
| GENERIC_SECRET | 產生 1 到 64 位元組的一般機密。 |

- **【1】** 根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## AWS CloudHSM 用戶端 SDK 3 支援的機制

PKCS #11 程式庫支援 AWS CloudHSM 用戶端 SDK 3 的下列演算法：

- 加密和解密：AES-CBC、AES-CTR、AES-ECB、AES-GCM、DES3-CBC、DES3-ECB、RSA-OAEP 和 RSA-PKCS
- 簽署和驗證：RSA、HMAC 和 ECDSA；無論是否使用雜湊皆不影響
- 雜湊/摘要：SHA1、SHA224、SHA256、SHA384 和 SHA512
- 金鑰包裝：AES 金鑰包裝、<sup>4</sup> AES-GCM、RSA-AES 和 RSA-OAEP
- 金鑰派生：ECDH、<sup>5</sup> SP800-108 CTR KDF

### PKCS #11 程式庫機制功能表

PKCS #11 程式庫與 PKCS #11 規格的 2.40 版相容。若要使用 PKCS #11 叫用加密功能，請利用指定機制呼叫函數。下表總結說明 AWS CloudHSM 支援的函數和機制組合。

### 解譯支援的 PKCS #11 機制函數表

✓ 標記表示 AWS CloudHSM 支援函數的機制。並不是 PKCS #11 規格中所列的所有可能函數都受到支援。✗ 標記表示 AWS CloudHSM 尚不支援指定函數的機制，即使 PKCS #11 標準允許。空白儲存格表示 PKCS #11 標準不支援指定函數的機制。

### 支援的 PKCS #11 程式庫機制和函數

| Mechanism | 函數       |       |         |    |       |      |         |
|-----------|----------|-------|---------|----|-------|------|---------|
|           | 產生金鑰或金鑰對 | 簽署和驗證 | SR 和 VR | 摘要 | 加密和解密 | 衍生金鑰 | 包裝和取消包裝 |



| Mechanism                                    | 函數                             |                                    |   |  |                                |  |                                |
|----------------------------------------------|--------------------------------|------------------------------------|---|--|--------------------------------|--|--------------------------------|
| CKM_RSA_P<br>KCS_KEY_P<br>AIR_GEN            | ✓                              |                                    |   |  |                                |  |                                |
| CKM_RSA_X<br>9_31_KEY_<br>PAIR_GEN           | ✓ <sup><a href="#">2</a></sup> |                                    |   |  |                                |  |                                |
| CKM_RSA_X<br>_509                            |                                | ✓                                  |   |  | ✓                              |  |                                |
| CKM_RSA_P<br>KCS 請<br>參閱備註 <a href="#">8</a> |                                | ✓ <sup><a href="#">1</a></sup>     | ✗ |  | ✓ <sup><a href="#">1</a></sup> |  | ✓ <sup><a href="#">1</a></sup> |
| CKM_RSA_P<br>KCS_OAEP                        |                                |                                    |   |  | ✓ <sup><a href="#">1</a></sup> |  | ✓ <sup><a href="#">6</a></sup> |
| CKM_SHA1_<br>RSA_PKCS                        |                                | ✓ <sup><a href="#">3.2</a></sup>   |   |  |                                |  |                                |
| CKM_SHA22<br>4_RSA_PKC<br>S                  |                                | ✓ <sup><a href="#">3.2</a></sup>   |   |  |                                |  |                                |
| CKM_SHA25<br>6_RSA_PKC<br>S                  |                                | ✓ <sup><a href="#">3.2</a></sup>   |   |  |                                |  |                                |
| CKM_SHA38<br>4_RSA_PKC<br>S                  |                                | ✓ <sup><a href="#">2,3.2</a></sup> |   |  |                                |  |                                |
| CKM_SHA51<br>2_RSA_PKC<br>S                  |                                | ✓ <sup><a href="#">3.2</a></sup>   |   |  |                                |  |                                |

| Mechanism                  | 函數 |                         |  |  |  |  |  |
|----------------------------|----|-------------------------|--|--|--|--|--|
| CKM_RSA_PKCS_PSS           |    | ✓ <a href="#">1</a>     |  |  |  |  |  |
| CKM_SHA1_RSA_PKCS_PSS      |    | ✓ <a href="#">3.2</a>   |  |  |  |  |  |
| CKM_SHA224_RSA_PKCS_PSS    |    | ✓ <a href="#">3.2</a>   |  |  |  |  |  |
| CKM_SHA256_RSA_PKCS_PSS    |    | ✓ <a href="#">3.2</a>   |  |  |  |  |  |
| CKM_SHA384_RSA_PKCS_PSS    |    | ✓ <a href="#">2,3.2</a> |  |  |  |  |  |
| CKM_SHA512_RSA_PKCS_PSS    |    | ✓ <a href="#">3.2</a>   |  |  |  |  |  |
| CKM_EC_KEY_PAIR_GENERATION | ✓  |                         |  |  |  |  |  |
| CKM_ECDSA                  |    | ✓ <a href="#">1</a>     |  |  |  |  |  |
| CKM_ECDSA_SHA1             |    | ✓ <a href="#">3.2</a>   |  |  |  |  |  |
| CKM_ECDSA_SHA224           |    | ✓ <a href="#">3.2</a>   |  |  |  |  |  |

| Mechanism                  | 函數 |                       |  |  |                       |                     |   |
|----------------------------|----|-----------------------|--|--|-----------------------|---------------------|---|
| CKM_ECDSA_SHA256           |    | ✓ <a href="#">3.2</a> |  |  |                       |                     |   |
| CKM_ECDSA_SHA384           |    | ✓ <a href="#">3.2</a> |  |  |                       |                     |   |
| CKM_ECDSA_SHA512           |    | ✓ <a href="#">3.2</a> |  |  |                       |                     |   |
| CKM_ECDH1_DERIVE           |    |                       |  |  |                       | ✓ <a href="#">5</a> |   |
| CKM_SP800_108_COUNTER_KDF  |    |                       |  |  |                       | ✓                   |   |
| CKM_GENERIC_SECRET_KEY_GEN | ✓  |                       |  |  |                       |                     |   |
| CKM_AES_KEY_GEN            | ✓  |                       |  |  |                       |                     |   |
| CKM_AES_ECB                |    |                       |  |  | ✓                     |                     | ✗ |
| CKM_AES_CTR                |    |                       |  |  | ✓                     |                     | ✗ |
| CKM_AES_CBC                |    |                       |  |  | ✓ <a href="#">3.3</a> |                     | ✗ |
| CKM_AES_CBC_PAD            |    |                       |  |  | ✓                     |                     | ✗ |

| Mechanism                                           | 函數 |                       |  |                       |                                           |  |                       |
|-----------------------------------------------------|----|-----------------------|--|-----------------------|-------------------------------------------|--|-----------------------|
| CKM_DES3_<br>KEY_GEN<br>請參閱<br>備註 <a href="#">8</a> | ✓  |                       |  |                       |                                           |  |                       |
| CKM_DES3_<br>CBC<br>請參閱<br>備註 <a href="#">8</a>     |    |                       |  |                       | ✓ <a href="#">3.3</a>                     |  | ✗                     |
| CKM_DES3_<br>CBC_PAD<br>請參閱<br>備註 <a href="#">8</a> |    |                       |  |                       | ✓                                         |  | ✗                     |
| CKM_DES3_<br>ECB<br>請參閱<br>備註 <a href="#">8</a>     |    |                       |  |                       | ✓                                         |  | ✗                     |
| CKM_AES_G<br>CM                                     |    |                       |  |                       | ✓ <a href="#">3.3</a> , <a href="#">4</a> |  | ✓ <a href="#">7.1</a> |
| CKM_CLOUD<br>HSM_AES_G<br>CM                        |    |                       |  |                       | ✓ <a href="#">7.1</a>                     |  | ✓ <a href="#">7.1</a> |
| CKM_SHA_1                                           |    |                       |  | ✓ <a href="#">3.1</a> |                                           |  |                       |
| CKM_SHA_1<br>_HMAC                                  |    | ✓ <a href="#">3.3</a> |  |                       |                                           |  |                       |
| CKM_SHA22<br>4                                      |    |                       |  | ✓ <a href="#">3.1</a> |                                           |  |                       |

| Mechanism                        | 函數 |                       |  |                       |  |  |                       |
|----------------------------------|----|-----------------------|--|-----------------------|--|--|-----------------------|
| CKM_SHA224_HMAC                  |    | ✓ <a href="#">3.3</a> |  |                       |  |  |                       |
| CKM_SHA256                       |    |                       |  | ✓ <a href="#">3.1</a> |  |  |                       |
| CKM_SHA256_HMAC                  |    | ✓ <a href="#">3.3</a> |  |                       |  |  |                       |
| CKM_SHA384                       |    |                       |  | ✓ <a href="#">3.1</a> |  |  |                       |
| CKM_SHA384_HMAC                  |    | ✓ <a href="#">3.3</a> |  |                       |  |  |                       |
| CKM_SHA512                       |    |                       |  | ✓ <a href="#">3.1</a> |  |  |                       |
| CKM_SHA512_HMAC                  |    | ✓ <a href="#">3.3</a> |  |                       |  |  |                       |
| CKM_RSA_AES_KEY_WRAP             |    |                       |  |                       |  |  | ✓                     |
| CKM_AES_KEY_WRAP                 |    |                       |  |                       |  |  | ✓                     |
| CKM_AES_KEY_WRAP_PAD             |    |                       |  |                       |  |  | ✓                     |
| CKM_CLOUDHSM_AES_KEY_WRAP_NO_PAD |    |                       |  |                       |  |  | ✓ <a href="#">7.1</a> |

| Mechanism                                       | 函數 |  |  |  |  |  |                       |
|-------------------------------------------------|----|--|--|--|--|--|-----------------------|
| CKM_CLOUD<br>HSM_AES_K<br>EY_WRAP_P<br>KCS5_PAD |    |  |  |  |  |  | ✓ <a href="#">7.1</a> |
| CKM_CLOUD<br>HSM_AES_K<br>EY_WRAP_Z<br>ERO_PAD  |    |  |  |  |  |  | ✓ <a href="#">7.1</a> |

### 機制註釋

- [1] 僅限單一部分操作。
- [2] 此機制的功能與 CKM\_RSA\_PKCS\_KEY\_PAIR\_GEN 機制完全相同，但在產生 p 和 q 時提供更強大的保證。
- **【3.1】** 根據用戶端 SDK AWS CloudHSM 以不同方式處理雜湊。對於用戶端 SDK 3，我們執行雜湊的位置取決於資料大小以及您使用的是單一部分還是多部分操作。

### 用戶端 SDK 3 中的單一部分操作

用戶端 SDK 3 各機制的最大資料集大小如表 3.1 所列。整個雜湊會在 HSM 內計算。不支援大於 16KB 的資料。

表 3.1，單一部分操作的資料集大小上限

| Mechanism  | 資料大小上限 |
|------------|--------|
| CKM_SHA_1  | 16296  |
| CKM_SHA224 | 16264  |
| CKM_SHA256 | 16296  |
| CKM_SHA384 | 16232  |
| CKM_SHA512 | 16232  |

## 多部分操作用戶端 SDK 3

雖支援大於 16 KB 的資料，但資料大小會決定雜湊的發生位置。小於 16 KB 的資料緩衝區會在 HSM 內進行雜湊處理。16 KB 和系統資料大小上限之間的緩衝區會在軟體本機雜湊處理。請記住：雜湊函數不需要加密密碼編譯，因此您可以在 HSM 之外安全地計算。

- **【3.2】** 根據用戶端 SDK AWS CloudHSM 以不同方式處理雜湊。對於用戶端 SDK 3，我們執行雜湊的位置取決於資料大小以及您使用的是單一部分還是多部分操作。

## 單一部分操作用戶端 SDK 3

用戶端 SDK 3 各機制的最大資料集大小如表 3.2 所列。不支援大於 16KB 的資料。

表 3.2，單一部分操作的資料集大小上限

| Mechanism               | 資料大小上限 |
|-------------------------|--------|
| CKM_SHA1_RSA_PKCS       | 16296  |
| CKM_SHA224_RSA_PKCS     | 16264  |
| CKM_SHA256_RSA_PKCS     | 16296  |
| CKM_SHA384_RSA_PKCS     | 16232  |
| CKM_SHA512_RSA_PKCS     | 16232  |
| CKM_SHA1_RSA_PKCS_PSS   | 16296  |
| CKM_SHA224_RSA_PKCS_PSS | 16264  |
| CKM_SHA256_RSA_PKCS_PSS | 16296  |
| CKM_SHA384_RSA_PKCS_PSS | 16232  |
| CKM_SHA512_RSA_PKCS_PSS | 16232  |
| CKM_ECDSA_SHA1          | 16296  |
| CKM_ECDSA_SHA224        | 16264  |

| Mechanism        | 資料大小上限 |
|------------------|--------|
| CKM_ECDSA_SHA256 | 16296  |
| CKM_ECDSA_SHA384 | 16232  |
| CKM_ECDSA_SHA512 | 16232  |

### 多部分操作用戶端 SDK 3

雖支援大於 16 KB 的資料，但資料大小會決定雜湊的發生位置。小於 16 KB 的資料緩衝區會在 HSM 內進行雜湊處理。16 KB 和系統資料大小上限之間的緩衝區會在軟體本機雜湊處理。請記住：雜湊函數不需要加密密碼編譯，因此您可以在 HSM 之外安全地計算。

- [3.3] 當使用下列任一機制操作資料時，若資料緩衝區超過資料大小上限，該操作就會導致錯誤。對於這些機制，所有資料處理都必須在 HSM 內進行。下表列出每個機制設定的資料大小上限：

表 3.3，最大資料集大小

| Mechanism            | 資料大小上限 |
|----------------------|--------|
| CKM_SHA_1_HMAC       | 16288  |
| CKM_SHA224_HMAC      | 16256  |
| CKM_SHA256_HMAC      | 16288  |
| CKM_SHA384_HMAC      | 16224  |
| CKM_SHA512_HMAC      | 16224  |
| CKM_AES_CBC          | 16272  |
| CKM_AES_GCM          | 16224  |
| CKM_CLOUDHSM_AES_GCM | 16224  |
| CKM_DES3_CBC         | 16280  |

- [4] 當執行 AES-GCM 加密時，HSM 不會接受來自應用程式的初始化向量 (IV) 資料。請務必使用其產生的 IV。系統會將 HSM 所提供的 12 位元組 IV 寫入記憶體參考，該記憶體參考是由您提供的



CK\_GCM\_PARAMS 參數結構 pIV 元素所指向。為了確保使用者不會混淆，在初始化 AES-GCM 加密時，1.1.1 版和更新版本中的 PKCS # 11 開發套件會強制將該 pIV 指向歸零的緩衝區。

- [5] 僅限於用戶端 SDK 3。此機制的實作是為了支援 SSL/TLS 卸載案例，且在 HSM 內只會部分執行。使用此機制前，請參閱 [PKCS #11 程式庫的已知問題 AWS CloudHSM](#) 中的「問題：在 HSM 中 ECDH 金鑰衍生只會部分執行」。CKM\_ECDH1\_DERIVE 不支援 secp521r1 (P-521) 曲線。
- [6] 支援下列 CK\_MECHANISM\_TYPE 和 CK\_RSA\_PKCS\_MGF\_TYPE，作為 CKM\_RSA\_PKCS\_OAEP 的 CK\_RSA\_PKCS\_OAEP\_PARAMS：
  - CKM\_SHA\_1 使用 CKG\_MGF1\_SHA1
  - CKM\_SHA224 使用 CKG\_MGF1\_SHA224
  - CKM\_SHA256 使用 CKG\_MGF1\_SHA256
  - CKM\_SHA384 使用 CKM\_MGF1\_SHA384
  - CKM\_SHA512 使用 CKM\_MGF1\_SHA512
- [7.1] 廠商定義的機制。為了能使用 CloudHSM 廠商定義的機制，編譯期間 PKCS #11 應用程式必須加入 /opt/cloudhsm/include/pkcs11t.h。

**CKM\_CLOUDHSM\_AES\_GCM**：這個專屬機制是標準 CKM\_AES\_GCM 程式設計更安全的替代方案。這將 HSM 生成的 IV 加入至加密文字的開頭，而不是將它寫回加密初始化期間提供的 CK\_GCM\_PARAMS 結構中。您可以搭配 C\_Encrypt、C\_WrapKey、C\_Decrypt 和 C\_UnwrapKey 函數搭配使用此機制。使用此機制時，CK\_GCM\_PARAMS 結構中的 pIV 變數必須設定為 NULL。與 C\_Decrypt 和 C\_UnwrapKey 搭配使用此機制時，IV 應至於取消包裝的加密文字之前。

**CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_PKCS5\_PAD**：AES 金鑰包裝與 PKCS #5 填補

**CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_ZERO\_PAD**：AES 金鑰包裝，零填補

如需有關 AES 金鑰包裝的其他資訊，請參閱 [AES 金鑰包裝](#)。

- **【8】** 根據 NIST 指引，不允許在 2023 年之後處於 FIPS 模式的叢集執行此操作。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## AWS CloudHSM 用戶端 SDK 3 支援的 API 操作

PKCS #11 程式庫支援用戶端 AWS CloudHSM SDK 3 的下列 PKCS #11 API 操作。

- C\_CloseAllSessions
- C\_CloseSession
- C\_CreateObject

- C\_Decrypt
- C\_DecryptFinal
- C\_DecryptInit
- C\_DecryptUpdate
- C\_DeriveKey
- C\_DestroyObject
- C\_Digest
- C\_DigestFinal
- C\_DigestInit
- C\_DigestUpdate
- C\_Encrypt
- C\_EncryptFinal
- C\_EncryptInit
- C\_EncryptUpdate
- C\_Finalize
- C\_FindObjects
- C\_FindObjectsFinal
- C\_FindObjectsInit
- C\_GenerateKey
- C\_GenerateKeyPair
- C\_GenerateRandom
- C\_GetAttributeValue
- C\_GetFunctionList
- C\_GetInfo
- C\_GetMechanismInfo
- C\_GetMechanismList
- C\_GetSessionInfo
- C\_GetSlotInfo
- C\_GetSlotList
- C\_GetTokenInfo

- C\_Initialize
- C\_Login
- C\_Logout
- C\_OpenSession
- C\_Sign
- C\_SignFinal
- C\_SignInit
- C\_SignRecover (僅支援用戶端 SDK 3)
- C\_SignRecoverInit (僅支援用戶端 SDK 3)
- C\_SignUpdate
- C\_UnWrapKey
- C\_Verify
- C\_VerifyFinal
- C\_VerifyInit
- C\_VerifyRecover (僅支援用戶端 SDK 3)
- C\_VerifyRecoverInit (僅支援用戶端 SDK 3)
- C\_VerifyUpdate
- C\_WrapKey

## 用戶端 SDK 3 的 AWS CloudHSM PKCS #11 程式庫中的關鍵屬性

金鑰物件可以是公有金鑰、私有金鑰或私密金鑰。系統會透過屬性來指定金鑰物件上允許的動作。金鑰物件建立時，即會一併建立屬性。當您使用 PKCS #11 程式庫時 AWS CloudHSM，我們會指派 PKCS #11 標準指定的預設值。

AWS CloudHSM 不支援 PKCS #11 規格中列出的所有屬性。我們會符合所有支援屬性的規格，並在個別表格中列出這些屬性。

用來建立、修改或複製物件的加密函數 (如

C\_CreateObject、C\_GenerateKey、C\_GenerateKeyPair、C\_UnwrapKey 和 C\_DeriveKey) 會採用屬性範本做為其中一個參數。如需在建立物件期間傳遞屬性範本的詳細資訊，請參閱[透過 PKCS #11 程式庫產生金鑰範例](#)。

下列主題提供有關用戶端 SDK 3 AWS CloudHSM 金鑰屬性的詳細資訊。

## 主題

- [AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫屬性資料表](#)
- [修改 AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫屬性](#)
- [解譯 AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫錯誤代碼](#)

## AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫屬性資料表

AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫資料表包含因金鑰類型而異的屬性清單。它會指出搭配特定密碼編譯函數使用時，特定金鑰類型是否支援指定的屬性 AWS CloudHSM。

圖例：

- ✓ 表示 CloudHSM 支援特定金鑰類型的屬性。
- ✗ 表示 CloudHSM 不支援特定金鑰類型的屬性。
- R 表示特定金鑰類型的屬性值設定為唯讀模式。
- S 表示屬性較為敏感，因此無法透過 GetAttributeValue 讀取。
- 預設值欄位中的空白儲存格表示屬性沒有獲派指定預設值。

## GenerateKeyPair

| 屬性               | 金鑰類型        |             |              |              | 預設值 |
|------------------|-------------|-------------|--------------|--------------|-----|
|                  | EC 私<br>有金鑰 | EC 公<br>有金鑰 | RSA 私<br>有金鑰 | RSA 公<br>有金鑰 |     |
| CKA_CLASS        | ✓           | ✓           | ✓            | ✓            |     |
| CKA_KEY_T<br>YPE | ✓           | ✓           | ✓            | ✓            |     |
| CKA_LABEL        | ✓           | ✓           | ✓            | ✓            |     |
| CKA_ID           | ✓           | ✓           | ✓            | ✓            |     |

| 屬性                 | 金鑰類型 |                |                |                | 預設值            |
|--------------------|------|----------------|----------------|----------------|----------------|
| CKA_LOCAL          |      | R              | R              | R              | True           |
| CKA_TOKEN          |      | ✓              | ✓              | ✓              | False          |
| CKA_PRIVATE        |      | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True           |
| CKA_ENCRYPT        |      | ✗              | ✓              | ✗              | False          |
| CKA_DECRYPT        |      | ✓              | ✗              | ✓              | False          |
| CKA_DERIVE         |      | ✓              | ✓              | ✓              | False          |
| CKA_MODIFIABLE     |      | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True           |
| CKA_DESTROYABLE    |      | ✓              | ✓              | ✓              | True           |
| CKA_SIGN           |      | ✓              | ✗              | ✓              | False          |
| CKA_SIGN_RECOVER   |      | ✗              | ✗              | ✓ <sup>3</sup> | ✗              |
| CKA_VERIFY         |      | ✗              | ✓              | ✗              | ✓              |
| CKA_VERIFY_RECOVER |      | ✗              | ✗              | ✗              | ✓ <sup>4</sup> |
| CKA_WRAP           |      | ✗              | ✓              | ✗              | ✓              |

| 屬性                    | 金鑰類型 |   |   |                | 預設值   |
|-----------------------|------|---|---|----------------|-------|
| CKA_WRAP_TEMPLATE     | ×    | ✓ | × | ✓              |       |
| CKA_TRUSTED           | ×    | ✓ | × | ✓              | False |
| CKA_WRAP_WITH_TRUSTED | ✓    | × | ✓ | ×              | False |
| CKA_UNWRAP            | ✓    | × | ✓ | ×              | False |
| CKA_UNWRAP_TEMPLATE   | ✓    | × | ✓ | ×              |       |
| CKA_SENSITIVE         | ✓    | × | ✓ | ×              | True  |
| CKA_ALWAYS_SENSITIVE  | R    | × | R | ×              |       |
| CKA_EXTRACTABLE       | ✓    | × | ✓ | ×              | True  |
| CKA_NEVER_EXTRACTABLE | R    | × | R | ×              |       |
| CKA_MODULUS           | ×    | × | × | ×              |       |
| CKA_MODULUS_BITS      | ×    | × | × | ✓ <sup>2</sup> |       |

| 屬性                   | 金鑰類型 |                |   |                | 預設值 |
|----------------------|------|----------------|---|----------------|-----|
| CKA_PRIME_1          | ×    | ×              | × | ×              |     |
| CKA_PRIME_2          | ×    | ×              | × | ×              |     |
| CKA_COEFFICIENT      | ×    | ×              | × | ×              |     |
| CKA_EXPONENT_1       | ×    | ×              | × | ×              |     |
| CKA_EXPONENT_2       | ×    | ×              | × | ×              |     |
| CKA_PRIVATE_EXPONENT | ×    | ×              | × | ×              |     |
| CKA_PUBLIC_EXPONENT  | ×    | ×              | × | ✓ <sup>2</sup> |     |
| CKA_EC_PARAMS        | ×    | ✓ <sup>2</sup> | × | ×              |     |
| CKA_EC_POINT         | ×    | ×              | × | ×              |     |
| CKA_VALUE            | ×    | ×              | × | ×              |     |
| CKA_VALUE_LEN        | ×    | ×              | × | ×              |     |
| CKA_CHECK_VALUE      | R    | R              | R | R              |     |

## GenerateKey

| 屬性              | 金鑰類型           |                |                | 預設值   |
|-----------------|----------------|----------------|----------------|-------|
|                 | AES            | DES3           | 一般機密           |       |
| CKA_CLASS       | ✓              | ✓              | ✓              |       |
| CKA_KEY_TYPE    | ✓              | ✓              | ✓              |       |
| CKA_LABEL       | ✓              | ✓              | ✓              |       |
| CKA_ID          | ✓              | ✓              | ✓              |       |
| CKA_LOCAL       | R              | R              | R              | True  |
| CKA_TOKEN       | ✓              | ✓              | ✓              | False |
| CKA_PRIVATE     | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_ENCRYPT     | ✓              | ✓              | ✗              | False |
| CKA_DECRYPT     | ✓              | ✓              | ✗              | False |
| CKA_DERIVE      | ✓              | ✓              | ✓              | False |
| CKA_MODIFIABLE  | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_DESTROYABLE | ✓              | ✓              | ✓              | True  |
| CKA_SIGN        | ✓              | ✓              | ✓              | True  |



| 屬性                    | 金鑰類型 |   |   | 預設值   |
|-----------------------|------|---|---|-------|
| CKA_SIGN_RECOVER      | ✗    | ✗ | ✗ |       |
| CKA_VERIFY            | ✓    | ✓ | ✓ | True  |
| CKA_VERIFY_RECOVER    | ✗    | ✗ | ✗ |       |
| CKA_WRAP              | ✓    | ✓ | ✗ | False |
| CKA_WRAP_TEMPLATE     | ✓    | ✓ | ✗ |       |
| CKA_TRUSTED           | ✓    | ✓ | ✗ | False |
| CKA_WRAP_WITH_TRUSTED | ✓    | ✓ | ✓ | False |
| CKA_UNWRAP            | ✓    | ✓ | ✗ | False |
| CKA_UNWRAP_TEMPLATE   | ✓    | ✓ | ✗ |       |
| CKA_SENSITIVE         | ✓    | ✓ | ✓ | True  |
| CKA_ALWAYS_SENSITIVE  | ✗    | ✗ | ✗ |       |

| 屬性                    | 金鑰類型 |   |   |   | 預設值  |
|-----------------------|------|---|---|---|------|
| CKA_EXTRA_CTABLE      |      | ✓ | ✓ | ✓ | True |
| CKA_NEVER_EXTRACTABLE |      | R | R | R |      |
| CKA_MODULUS           |      | ✖ | ✖ | ✖ |      |
| CKA_MODULUS_BITS      |      | ✖ | ✖ | ✖ |      |
| CKA_PRIME_1           |      | ✖ | ✖ | ✖ |      |
| CKA_PRIME_2           |      | ✖ | ✖ | ✖ |      |
| CKA_COEFFICIENT       |      | ✖ | ✖ | ✖ |      |
| CKA_EXPONENT_1        |      | ✖ | ✖ | ✖ |      |
| CKA_EXPONENT_2        |      | ✖ | ✖ | ✖ |      |
| CKA_PRIVATE_EXPONENT  |      | ✖ | ✖ | ✖ |      |
| CKA_PUBLIC_EXPONENT   |      | ✖ | ✖ | ✖ |      |

| 屬性                  | 金鑰類型           |   |                | 預設值 |
|---------------------|----------------|---|----------------|-----|
| CKA_EC_PA<br>RAMS   | ×              | × | ×              |     |
| CKA_EC_PO<br>INT    | ×              | × | ×              |     |
| CKA_VALUE           | ×              | × | ×              |     |
| CKA_VALUE<br>_LEN   | ✓ <sup>2</sup> | × | ✓ <sup>2</sup> |     |
| CKA_CHECK<br>_VALUE | R              | R | R              |     |

## CreateObject

| 屬性               | 金鑰類型           |                |                 |                 |                |                |                | 預設值   |
|------------------|----------------|----------------|-----------------|-----------------|----------------|----------------|----------------|-------|
|                  | EC 私<br>有金鑰    | EC 公<br>有金鑰    | RSA<br>私有<br>金鑰 | RSA<br>公有<br>金鑰 | AES            | DES3           | 一般<br>機密       |       |
| CKA_CLASS        | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup>  | ✓ <sup>2</sup>  | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_KEY_T<br>YPE | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup>  | ✓ <sup>2</sup>  | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_LABEL        | ✓              | ✓              | ✓               | ✓               | ✓              | ✓              | ✓              |       |
| CKA_ID           | ✓              | ✓              | ✓               | ✓               | ✓              | ✓              | ✓              |       |
| CKA_LOCAL        | R              | R              | R               | R               | R              | R              | R              | False |

| 屬性                 | 金鑰類型           |                |                |                |                |                |                | 預設值   |
|--------------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|-------|
| CKA_TOKEN          | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | False |
| CKA_PRIVATE        | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_ENCRYPT        | ✗              | ✗              | ✗              | ✓              | ✓              | ✓              | ✗              | False |
| CKA_DECRYPT        | ✗              | ✗              | ✓              | ✗              | ✓              | ✓              | ✗              | False |
| CKA_DERIVE         | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | False |
| CKA_MODIFIABLE     | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_DESTROYABLE    | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | True  |
| CKA_SIGN           | ✓              | ✗              | ✓              | ✗              | ✓              | ✓              | ✓              | False |
| CKA_SIGN_RECOVER   | ✗              | ✗              | ✓ <sup>3</sup> | ✗              | ✗              | ✗              | ✗              | False |
| CKA_VERIFY         | ✗              | ✓              | ✗              | ✓              | ✓              | ✓              | ✓              | False |
| CKA_VERIFY_RECOVER | ✗              | ✗              | ✗              | ✓ <sup>4</sup> | ✗              | ✗              | ✗              |       |
| CKA_WRAP           | ✗              | ✗              | ✗              | ✓              | ✓              | ✓              | ✗              | False |
| CKA_WRAP_TEMPLATE  | ✗              | ✓              | ✗              | ✓              | ✓              | ✓              | ✗              |       |

| 屬性                    | 金鑰類型 |   |                |                |   |   |   | 預設值   |
|-----------------------|------|---|----------------|----------------|---|---|---|-------|
| CKA_TRUSTED           | ✗    | ✓ | ✗              | ✓              | ✓ | ✓ | ✗ | False |
| CKA_WRAP_WITH_TRUSTED | ✓    | ✗ | ✓              | ✗              | ✓ | ✓ | ✓ | False |
| CKA_UNWRAP            | ✗    | ✗ | ✓              | ✗              | ✓ | ✓ | ✗ | False |
| CKA_UNWRAP_TEMPLATE   | ✓    | ✗ | ✓              | ✗              | ✓ | ✓ | ✗ |       |
| CKA_SENSITIVE         | ✓    | ✗ | ✓              | ✗              | ✓ | ✓ | ✓ | True  |
| CKA_ALWAYS_SENSITIVE  | R    | ✗ | R              | ✗              | R | R | R |       |
| CKA_EXTRACTABLE       | ✓    | ✗ | ✓              | ✗              | ✓ | ✓ | ✓ | True  |
| CKA_NEVER_EXTRACTABLE | R    | ✗ | R              | ✗              | R | R | R |       |
| CKA_MODULUS           | ✗    | ✗ | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✗ | ✗ | ✗ |       |
| CKA_MODULUS_BITS      | ✗    | ✗ | ✗              | ✗              | ✗ | ✗ | ✗ |       |
| CKA_PRIME_1           | ✗    | ✗ | ✓              | ✗              | ✗ | ✗ | ✗ |       |

| 屬性                   | 金鑰類型           |                |                |                |                |                |                | 預設值 |
|----------------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|-----|
| CKA_PRIME_2          | ×              | ×              | ✓              | ×              | ×              | ×              | ×              |     |
| CKA_COEFFICIENT      | ×              | ×              | ✓              | ×              | ×              | ×              | ×              |     |
| CKA_EXPONENT_1       | ×              | ×              | ✓              | ×              | ×              | ×              | ×              |     |
| CKA_EXPONENT_2       | ×              | ×              | ✓              | ×              | ×              | ×              | ×              |     |
| CKA_PRIVATE_EXPONENT | ×              | ×              | ✓ <sup>2</sup> | ×              | ×              | ×              | ×              |     |
| CKA_PUBLIC_EXPONENT  | ×              | ×              | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ×              | ×              | ×              |     |
| CKA_EC_PARAMS        | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ×              | ×              | ×              | ×              | ×              |     |
| CKA_EC_POINT         | ×              | ✓ <sup>2</sup> | ×              | ×              | ×              | ×              | ×              |     |
| CKA_VALUE            | ✓ <sup>2</sup> | ×              | ×              | ×              | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |     |
| CKA_VALUE_LEN        | ×              | ×              | ×              | ×              | ×              | ×              | ×              |     |
| CKA_CHECK_VALUE      | R              | R              | R              | R              | R              | R              | R              |     |

## UnwrapKey

| 屬性                 | 金鑰類型           |                |                |                |                | 預設值   |
|--------------------|----------------|----------------|----------------|----------------|----------------|-------|
|                    | EC 私<br>有金鑰    | RSA 私<br>有金鑰   | AES            | DES3           | 一般機密           |       |
| CKA_CLASS          | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_KEY_T<br>YPE   | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_LABEL          | ✓              | ✓              | ✓              | ✓              | ✓              |       |
| CKA_ID             | ✓              | ✓              | ✓              | ✓              | ✓              |       |
| CKA_LOCAL          | R              | R              | R              | R              | R              | False |
| CKA_TOKEN          | ✓              | ✓              | ✓              | ✓              | ✓              | False |
| CKA_PRIVATE        | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_ENCRY<br>PT    | ✗              | ✗              | ✓              | ✓              | ✗              | False |
| CKA_DECRY<br>PT    | ✗              | ✓              | ✓              | ✓              | ✗              | False |
| CKA_DERIV<br>E     | ✓              | ✓              | ✓              | ✓              | ✓              | False |
| CKA_MODIF<br>IABLE | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |

| 屬性                            | 金鑰類型 |                |   |   |   | 預設值   |
|-------------------------------|------|----------------|---|---|---|-------|
| CKA_DESTR<br>OYABLE           | ✓    | ✓              | ✓ | ✓ | ✓ | True  |
| CKA_SIGN                      | ✓    | ✓              | ✓ | ✓ | ✓ | False |
| CKA_SIGN_<br>RECOVER          | ✗    | ✓ <sup>3</sup> | ✗ | ✗ | ✗ | False |
| CKA_VERIF<br>Y                | ✗    | ✗              | ✓ | ✓ | ✓ | False |
| CKA_VERIF<br>Y_RECOVER        | ✗    | ✗              | ✗ | ✗ | ✗ |       |
| CKA_WRAP                      | ✗    | ✗              | ✓ | ✓ | ✗ | False |
| CKA_UNWRA<br>P                | ✗    | ✓              | ✓ | ✓ | ✗ | False |
| CKA_SENSI<br>TIVE             | ✓    | ✓              | ✓ | ✓ | ✓ | True  |
| CKA_EXTRA<br>CTABLE           | ✓    | ✓              | ✓ | ✓ | ✓ | True  |
| CKA_NEVER<br>_EXTRACTA<br>BLE | R    | R              | R | R | R |       |
| CKA_ALWAY<br>S_SENSITI<br>VE  | R    | R              | R | R | R |       |
| CKA_MODUL<br>US               | ✗    | ✗              | ✗ | ✗ | ✗ |       |



| 屬性                   | 金鑰類型 |   |   |   |   | 預設值 |
|----------------------|------|---|---|---|---|-----|
| CKA_MODULUS_BITS     | ×    | × | × | × | × |     |
| CKA_PRIME_1          | ×    | × | × | × | × |     |
| CKA_PRIME_2          | ×    | × | × | × | × |     |
| CKA_COEFFICIENT      | ×    | × | × | × | × |     |
| CKA_EXPONENT_1       | ×    | × | × | × | × |     |
| CKA_EXPONENT_2       | ×    | × | × | × | × |     |
| CKA_PRIVATE_EXPONENT | ×    | × | × | × | × |     |
| CKA_PUBLIC_EXPONENT  | ×    | × | × | × | × |     |
| CKA_EC_PARAMS        | ×    | × | × | × | × |     |
| CKA_EC_POINT         | ×    | × | × | × | × |     |
| CKA_VALUE            | ×    | × | × | × | × |     |
| CKA_VALUE_LEN        | ×    | × | × | × | × |     |

| 屬性              | 金鑰類型 |   |   |   |   | 預設值 |
|-----------------|------|---|---|---|---|-----|
| CKA_CHECK_VALUE |      | R | R | R | R |     |

## DeriveKey

| 屬性             | 金鑰類型           |                |                | 預設值   |
|----------------|----------------|----------------|----------------|-------|
|                | AES            | DES3           | 一般機密           |       |
| CKA_CLASS      | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_KEY_TYPE   | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |       |
| CKA_LABEL      | ✓              | ✓              | ✓              |       |
| CKA_ID         | ✓              | ✓              | ✓              |       |
| CKA_LOCAL      | R              | R              | R              | True  |
| CKA_TOKEN      | ✓              | ✓              | ✓              | False |
| CKA_PRIVATE    | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_ENCRYPT    | ✓              | ✓              | ✗              | False |
| CKA_DECRYPT    | ✓              | ✓              | ✗              | False |
| CKA_DERIVE     | ✓              | ✓              | ✓              | False |
| CKA_MODIFIABLE | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |

| 屬性                            | 金鑰類型           |                |                | 預設值   |
|-------------------------------|----------------|----------------|----------------|-------|
| CKA_DESTR<br>OYABLE           | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | True  |
| CKA_SIGN                      | ✓              | ✓              | ✓              | False |
| CKA_SIGN_<br>RECOVER          | ✗              | ✗              | ✗              |       |
| CKA_VERIF<br>Y                | ✓              | ✓              | ✓              | False |
| CKA_VERIF<br>Y_RECOVER        | ✗              | ✗              | ✗              |       |
| CKA_WRAP                      | ✓              | ✓              | ✗              | False |
| CKA_UNWRA<br>P                | ✓              | ✓              | ✗              | False |
| CKA_SENSI<br>TIVE             | ✓              | ✓              | ✓              | True  |
| CKA_EXTRA<br>CTABLE           | ✓              | ✓              | ✓              | True  |
| CKA_NEVER<br>_EXTRACTA<br>BLE | R              | R              | R              |       |
| CKA_ALWAY<br>S_SENSITI<br>VE  | R              | R              | R              |       |
| CKA_MODUL<br>US               | ✗              | ✗              | ✗              |       |

| 屬性                   | 金鑰類型           |   |                | 預設值 |
|----------------------|----------------|---|----------------|-----|
| CKA_MODULUS_BITS     | ×              | × | ×              |     |
| CKA_PRIME_1          | ×              | × | ×              |     |
| CKA_PRIME_2          | ×              | × | ×              |     |
| CKA_COEFFICIENT      | ×              | × | ×              |     |
| CKA_EXPONENT_1       | ×              | × | ×              |     |
| CKA_EXPONENT_2       | ×              | × | ×              |     |
| CKA_PRIVATE_EXPONENT | ×              | × | ×              |     |
| CKA_PUBLIC_EXPONENT  | ×              | × | ×              |     |
| CKA_EC_PARAMS        | ×              | × | ×              |     |
| CKA_EC_POINT         | ×              | × | ×              |     |
| CKA_VALUE            | ×              | × | ×              |     |
| CKA_VALUE_LEN        | ✓ <sup>2</sup> | × | ✓ <sup>2</sup> |     |

| 屬性              | 金鑰類型 |   |   | 預設值 |
|-----------------|------|---|---|-----|
| CKA_CHECK_VALUE | R    | R | R |     |

## GetAttributeValue

| 屬性           | 金鑰類型           |                |                |                |                |                |                |
|--------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
|              | EC 私<br>有金鑰    | EC 公<br>有金鑰    | RSA 私<br>有金鑰   | RSA 公<br>有金鑰   | AES            | DES3           | 一般<br>機密       |
| CKA_CLASS    | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |
| CKA_KEY_TYPE | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |
| CKA_LABEL    | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |
| CKA_ID       | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |
| CKA_LOCAL    | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |
| CKA_TOKEN    | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              | ✓              |
| CKA_PRIVATE  | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> | ✓ <sup>1</sup> |
| CKA_ENCRYPT  | ✗              | ✗              | ✗              | ✓              | ✓              | ✓              | ✗              |
| CKA_DECRYPT  | ✗              | ✗              | ✓              | ✗              | ✓              | ✓              | ✗              |

| 屬性                    | 金鑰類型 |   |   |   |   |   |   |
|-----------------------|------|---|---|---|---|---|---|
| CKA_DERIVE            | ✓    | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| CKA_MODIFIABLE        | ✓    | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| CKA_DESTROYABLE       | ✓    | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| CKA_SIGN              | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| CKA_SIGN_RECOVER      | ✗    | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| CKA_VERIFY            | ✗    | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| CKA_VERIFY_RECOVER    | ✗    | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| CKA_WRAP              | ✗    | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ |
| CKA_WRAP_TEMPLATE     | ✗    | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |
| CKA_TRUSTED           | ✗    | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| CKA_WRAP_WITH_TRUSTED | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| CKA_UNWRAP            | ✗    | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |

| 屬性                    | 金鑰類型 |   |   |   |   |   |   |
|-----------------------|------|---|---|---|---|---|---|
| CKA_UNWRAPP_TEMPLATE  | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |
| CKA_SENSITIVE         | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| CKA_EXTRACTABLE       | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| CKA_NEVER_EXTRACTABLE | ✓    | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| CKA_ALWAYS_SENSITIVE  | R    | R | R | R | R | R | R |
| CKA_MODULUS           | ✗    | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ |
| CKA_MODULUS_BITS      | ✗    | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| CKA_PRIME_1           | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |
| CKA_PRIME_2           | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |
| CKA_COEFFICIENT       | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |
| CKA_EXPONENT_1        | ✗    | ✗ | S | ✗ | ✗ | ✗ | ✗ |

| 屬性                   | 金鑰類型 |   |   |   |                |                |                |
|----------------------|------|---|---|---|----------------|----------------|----------------|
| CKA_EXPONENT_2       | ×    | × | S | × | ×              | ×              | ×              |
| CKA_PRIVATE_EXPONENT | ×    | × | S | × | ×              | ×              | ×              |
| CKA_PUBLIC_EXPONENT  | ×    | × | ✓ | ✓ | ×              | ×              | ×              |
| CKA_EC_PARAMS        | ✓    | ✓ | × | × | ×              | ×              | ×              |
| CKA_EC_POINT         | ×    | ✓ | × | × | ×              | ×              | ×              |
| CKA_VALUE            | S    | × | × | × | ✓ <sup>2</sup> | ✓ <sup>2</sup> | ✓ <sup>2</sup> |
| CKA_VALUE_LEN        | ×    | × | × | × | ✓              | ×              | ✓              |
| CKA_CHECK_VALUE      | ✓    | ✓ | ✓ | ✓ | ✓              | ✓              | ×              |

### 屬性註釋

- [1] 此屬性受韌體部分支援，且需明確設定為僅限預設值。
- [2] 必要屬性。
- [3] 僅限於用戶端 SDK 3。CKA\_SIGN\_RECOVER 屬性由 CKA\_SIGN 屬性衍生而來。若已設定，該屬性就僅能設定為與 CKA\_SIGN 相同的值。若未設定，則該屬性會衍生 CKA\_SIGN 的預設值。CloudHSM 只支援以 RSA 為基礎的可復原簽章機制，因此屬性目前僅適用於 RSA 公有金鑰。
- [4] 僅限於用戶端 SDK 3。CKA\_VERIFY\_RECOVER 屬性由 CKA\_VERIFY 屬性衍生而來。若已設定，該屬性就僅能設定為與 CKA\_VERIFY 相同的值。若未設定，則該屬性會衍生 CKA\_VERIFY 的



預設值。CloudHSM 只支援以 RSA 為基礎的可復原簽章機制，因此此屬性目前僅適用於 RSA 公有金鑰。

### 修改 AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫屬性

有些物件屬性可在物件建立後進行修改，但有些不行。若要修改屬性，請使用來自 `cloudhsm_mgmt_util` 的 [setAttribute](#) 命令。您也可以使用來自 `cloudhsm_mgmt_util` 的 [listAttribute](#) 命令，來衍生屬性和代表這些屬性的常數清單。

下列清單會顯示物件建立後可修改的屬性：

- CKA\_LABEL
- CKA\_TOKEN

#### Note

只有在將工作階段金鑰變更為符記金鑰時，才允許進行修改。使用 `key_mgmt_util` 中的 [setAttribute](#) 命令來變更屬性值。

- CKA\_ENCRYPT
- CKA\_DECRYPT
- CKA\_SIGN
- CKA\_VERIFY
- CKA\_WRAP
- CKA\_UNWRAP
- CKA\_LABEL
- CKA\_SENSITIVE
- CKA\_DERIVE

#### Note

這個屬性支援金鑰衍生。所有公有金鑰的屬性須為 `False`，不能設定為 `True`。如果是私密金鑰和 EC 私有金鑰，則該屬性可設定為 `True` 或 `False`。

- CKA\_TRUSTED

**Note**

唯有加密管理員 (CO) 可將這個屬性設定成 True 或 False。

- CKA\_WRAP\_WITH\_TRUSTED

**Note**

將此屬性套用於可匯出的資料金鑰，以表明只能使用標記為 CKA\_TRUSTED 的金鑰包裝此金鑰。一旦設定 CKA\_WRAP\_WITH\_TRUSTED 為 true，屬性就會變成唯讀，而且您無法變更或移除屬性。

## 解譯 AWS CloudHSM 用戶端 SDK 3 的 PKCS #11 程式庫錯誤代碼

在範本中指定特定金鑰不支援的 PKCS #11 程式庫屬性會導致錯誤。下表包含違反規格時所產生的錯誤代碼：

| 錯誤代碼                       | Description                                           |
|----------------------------|-------------------------------------------------------|
| CKR_TEMPLATE_INCONSISTENT  | 當您在屬性範本中指定的屬性符合 PKCS #11 規格，卻不受 CloudHSM 支援時，就會收到此錯誤。 |
| CKR_ATTRIBUTE_TYPE_INVALID | 當您擷取的屬性值符合 PKCS #11 規格，卻不受 CloudHSM 支援時，就會收到此錯誤。      |
| CKR_ATTRIBUTE_INCOMPLETE   | 當您沒有在屬性範本中指定必要屬性時，就會收到此錯誤。                            |
| CKR_ATTRIBUTE_READ_ONLY    | 當您在屬性範本中指定唯讀屬性時，就會收到此錯誤。                              |

## 用戶端 SDK AWS CloudHSM 3 的 PKCS #11 程式庫程式碼範例

GitHub 上的程式碼範例示範如何使用適用於 的 PKCS #11 程式庫來完成基本任務 AWS CloudHSM。

## 範本程式碼先決條件

執行範例之前，請執行以下步驟來設定您的環境：

- 安裝並設定適用於用戶端 SDK 3 的 [PKCS #11 程式庫](#)。
- 設定[密碼編譯使用者 \(CU\)](#)。您的應用程式會使用此 HSM 帳戶在 HSM 上執行程式碼範例。

## 程式碼範例

適用於 PKCS#11 AWS CloudHSM 的軟體程式庫程式碼範例可在 [GitHub](#) 上取得。此儲存庫包括如何使用 PKCS #11 執行一般作業的範例，包括加密、解密、簽署和驗證。

- [產生金鑰 \(AES、RSA、EC\)](#)
- [列出金鑰屬性](#)
- [使用 AES GCM 加密和解密資料](#)
- [使用 AES\\_CTR 加密和解密資料](#)
- [使用 3DES 加密和解密資料](#)
- [使用 RSA 簽署和驗證資料](#)
- [使用 HMAC KDF 衍生金鑰](#)
- [使用以 PKCS #5 填補的 AES 包裝和取消包裝金鑰](#)
- [使用不填補的 AES 包裝和取消包裝金鑰](#)
- [使用零填補的 AES 包裝和取消包裝金鑰](#)
- [使用 AES-GCM 包裝和取消包裝金鑰](#)
- [使用 RSA 包裝和取消包裝金鑰](#)

## 適用於 AWS CloudHSM 用戶端 SDK 3 的 OpenSSL 動態引擎

AWS CloudHSM OpenSSL 動態引擎可讓您透過 OpenSSL API 將密碼編譯操作卸載至 CloudHSM 叢集。

AWS CloudHSM 用戶端 SDK 3 確實需要用戶端協助程式才能連線至叢集。其支援：

- 產生 2048 位元、3072 位元和 4096 位元金鑰的 RSA 金鑰
- RSA 簽署/驗證。

- RSA 加密/解密。
- 產生隨機數字，經過安全性密碼編譯並通過 FIPS 驗證。

使用下列各節來安裝和設定 OpenSSL 的 AWS CloudHSM 動態引擎。

## 主題

- [搭配 AWS CloudHSM 用戶端 SDK 3 的 OpenSSL 動態引擎先決條件](#)
- [安裝適用於用戶端 SDK 3 的 AWS CloudHSM OpenSSL 動態引擎](#)
- [使用適用於用戶端 SDK 3 的 AWS CloudHSM OpenSSL 動態引擎](#)

## 搭配 AWS CloudHSM 用戶端 SDK 3 的 OpenSSL 動態引擎先決條件

如需關於平台支援的詳細資訊，請參閱 [AWS CloudHSM 用戶端 SDK 3 支援的平台](#)。

您需要 AWS CloudHSM 用戶端，才能將 OpenSSL 的 AWS CloudHSM 動態引擎與用戶端 SDK 3 搭配使用。

用戶端是一種協助程式，可以與叢集內的 HSM 建立端對端加密通訊，而 OpenSSL 引擎會在本機與用戶端通訊。若要安裝和設定 AWS CloudHSM 用戶端，請參閱 [安裝用戶端 \(Linux\)](#)。使用下列命令來啟動。

### Amazon Linux

```
$ sudo start cloudhsm-client
```

### Amazon Linux 2

```
$ sudo systemctl cloudhsm-client start
```

### CentOS 6

```
$ sudo systemctl start cloudhsm-client
```

### CentOS 7

```
$ sudo systemctl cloudhsm-client start
```

## RHEL 6

```
$ sudo systemctl start cloudhsm-client
```

## RHEL 7

```
$ sudo systemctl cloudhsm-client start
```

## Ubuntu 16.04 LTS

```
$ sudo systemctl cloudhsm-client start
```

## 安裝適用於用戶端 SDK 3 的 AWS CloudHSM OpenSSL 動態引擎

下列步驟說明如何使用用戶端 SDK 3 安裝和設定 OpenSSL 的 AWS CloudHSM 動態引擎。如需關於升級的詳細資訊，請參閱 [升級用戶端 SDK 3](#)。

### 安裝和設定 OpenSSL 引擎

1. 使用以下命令來下載和安裝 OpenSSL 引擎。

#### Amazon Linux

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-dyn-latest.el6.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-dyn-latest.el6.x86_64.rpm
```

#### Amazon Linux 2

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-dyn-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-dyn-latest.el7.x86_64.rpm
```

## CentOS 6

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-dyn-latest.el6.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-dyn-latest.el6.x86_64.rpm
```

## CentOS 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-dyn-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-dyn-latest.el7.x86_64.rpm
```

## RHEL 6

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-dyn-latest.el6.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-dyn-latest.el6.x86_64.rpm
```

## RHEL 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-dyn-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-dyn-latest.el7.x86_64.rpm
```

## Ubuntu 16.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-client-dyn_latest_amd64.deb
```

```
$ sudo apt install ./cloudhsm-client-dyn_latest_amd64.deb
```

應將 OpenSSL 引擎安裝在 /opt/cloudhsm/lib/libcloudhsm\_openssl.so。

2. 使用下列命令來設定名為 n3fips\_password 的環境變數，其中包含加密使用者 (CU) 的登入資料。

```
$ export n3fips_password=<HSM user name>:<password>
```

## 使用適用於用戶端 SDK 3 的 AWS CloudHSM OpenSSL 動態引擎

若要從 OpenSSL 整合的應用程式使用 OpenSSL 的 AWS CloudHSM 動態引擎，請確定您的應用程式使用名為的 OpenSSL 動態引擎cloudhsm。動態引擎的共用程式庫位於 /opt/cloudhsm/lib/libcloudhsm\_openssl.so。

若要從 OpenSSL 命令列使用 OpenSSL 的 AWS CloudHSM 動態引擎，請使用 -engine選項指定名為的 OpenSSL 動態引擎cloudhsm。例如：

```
$ openssl s_server -cert <server.crt> -key <server.key> -engine cloudhsm
```

## AWS CloudHSM 用戶端 SDK 3 的 JCE 提供者

AWS CloudHSM JCE 提供者是從 Java 密碼編譯延伸 (JCE) 提供者架構建置的提供者實作。JCE 可讓您使用 Java 開發套件 (JDK) 執行密碼編譯操作。在本指南中，AWS CloudHSM JCE 提供者有時稱為 JCE 提供者。使用 JCE 提供者和 JDK 將密碼編譯操作卸載至 HSM。

### 主題

- [安裝 AWS CloudHSM 用戶端 SDK 3 的 JCE 提供者](#)
- [AWS CloudHSM 用戶端 SDK 3 的 JCE 提供者中的金鑰管理基本概念](#)
- [適用於用戶端 SDK 3 AWS CloudHSM 的用戶端 SDK 3 支援機制](#)
- [用戶端 SDK AWS CloudHSM 3 支援的 Java 金鑰屬性](#)
- [Java for Client SDK 3 AWS CloudHSM 軟體程式庫的程式碼範例](#)
- [用戶端 SDK 3 的AWS CloudHSM KeyStore Java 類別](#)

## 安裝 AWS CloudHSM 用戶端 SDK 3 的 JCE 提供者

您需要有 AWS CloudHSM 用戶端，才能使用 JCE 提供者。

用戶端為一項協助程式，其會與您的叢集中的 HSM 建立端對端加密的通訊。JCE 提供者會在本機與用戶端進行通訊。如果您尚未安裝並設定 AWS CloudHSM 用戶端套件，請立即依照 中的步驟執行。 [安裝用戶端 \(Linux\)](#) 安裝和設定用戶端之後，請使用以下命令來啟動用戶端。

僅 Linux 和相容的作業系統才支援 JCE 提供者。

#### Amazon Linux

```
$ sudo start cloudhsm-client
```

#### Amazon Linux 2

```
$ sudo systemctl cloudhsm-client start
```

#### CentOS 7

```
$ sudo systemctl cloudhsm-client start
```

#### CentOS 8

```
$ sudo systemctl cloudhsm-client start
```

#### RHEL 7

```
$ sudo systemctl cloudhsm-client start
```

#### RHEL 8

```
$ sudo systemctl cloudhsm-client start
```

#### Ubuntu 16.04 LTS

```
$ sudo systemctl cloudhsm-client start
```

#### Ubuntu 18.04 LTS

```
$ sudo systemctl cloudhsm-client start
```



## Ubuntu 20.04 LTS

```
$ sudo systemctl cloudhsm-client start
```

使用下列各節來安裝、驗證和提供登入資料給供應商。

### 主題

- [步驟 1：安裝 JCE 提供者](#)
- [步驟 2：驗證安裝](#)
- [步驟 3：提供登入資料給 JCE 供應商](#)

### 步驟 1：安裝 JCE 提供者

使用下列命令下載和安裝 JCE 提供者。僅 Linux 和相容的作業系統支援此提供者。

#### Note

如需升級，請參閱 [升級用戶端 SDK 3](#)。

## Amazon Linux

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL6/cloudhsm-client-jce-latest.el6.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-jce-latest.el6.x86_64.rpm
```

## Amazon Linux 2

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-jce-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-jce-latest.el7.x86_64.rpm
```

## CentOS 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-jce-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-jce-latest.el7.x86_64.rpm
```

## CentOS 8

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-jce-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-jce-latest.el8.x86_64.rpm
```

## RHEL 7

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-jce-latest.el7.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-jce-latest.el7.x86_64.rpm
```

## RHEL 8

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL8/cloudhsm-client-jce-latest.el8.x86_64.rpm
```

```
$ sudo yum install ./cloudhsm-client-jce-latest.el8.x86_64.rpm
```

## Ubuntu 16.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Xenial/cloudhsm-client-jce_latest_amd64.deb
```

```
$ sudo apt install ./cloudhsm-client-jce_latest_amd64.deb
```

## Ubuntu 18.04 LTS

```
$ wget https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/Bionic/cloudhsm-client-jce_latest_u18.04_amd64.deb
```

```
$ sudo apt install ./cloudhsm-client-jce_latest_u18.04_amd64.deb
```

當您執行上述命令後，您可以找到以下 JCE 提供者檔案：

- /opt/cloudhsm/java/cloudhsm-*<version>*.jar
- /opt/cloudhsm/java/cloudhsm-test-*<version>*.jar
- /opt/cloudhsm/java/hamcrest-all-1.3.jar
- /opt/cloudhsm/java/junit.jar
- /opt/cloudhsm/java/log4j-api-2.17.1.jar
- /opt/cloudhsm/java/log4j-core-2.17.1.jar
- /opt/cloudhsm/lib/libcaviumjca.so

### 步驟 2：驗證安裝

HSM 上執行基本操作以驗證安裝。

#### 驗證 JCE 提供者安裝

1. (選用) 如果您的環境中尚未安裝 Java，請使用下列命令來安裝。

Linux (and compatible libraries)

```
$ sudo yum install java-1.8.0-openjdk
```

Ubuntu

```
$ sudo apt-get install openjdk-8-jre
```

2. 使用下列命令來設定必要的環境變數。以加密使用者 (CU) 的登入資料取代 *<HSM user name>* 和 *<password>*。

```
$ export LD_LIBRARY_PATH=/opt/cloudhsm/lib
```

```
$ export HSM_PARTITION=PARTITION_1
```

```
$ export HSM_USER=<HSM user name>
```

```
$ export HSM_PASSWORD=<password>
```

3. 請使用以下命令執行基本功能測試。如果成功執行，您會看到類似如下的命令輸出。

```
$ java8 -classpath "/opt/cloudhsm/java/*" org.junit.runner.JUnitCore
TestBasicFunctionality
```

```
JUnit version 4.11
.2018-08-20 17:53:48,514 DEBUG [main] TestBasicFunctionality
 (TestBasicFunctionality.java:33) - Adding provider.
2018-08-20 17:53:48,612 DEBUG [main] TestBasicFunctionality
 (TestBasicFunctionality.java:42) - Logging in.
2018-08-20 17:53:48,612 INFO [main] cfm2.LoginManager (LoginManager.java:104) -
 Looking for credentials in HsmCredentials.properties
2018-08-20 17:53:48,612 INFO [main] cfm2.LoginManager (LoginManager.java:122) -
 Looking for credentials in System.properties
2018-08-20 17:53:48,613 INFO [main] cfm2.LoginManager (LoginManager.java:130) -
 Looking for credentials in System.env
SDK Version: 2.03
2018-08-20 17:53:48,655 DEBUG [main] TestBasicFunctionality
 (TestBasicFunctionality.java:54) - Generating AES Key with key size 256.
2018-08-20 17:53:48,698 DEBUG [main] TestBasicFunctionality
 (TestBasicFunctionality.java:63) - Encrypting with AES Key.
2018-08-20 17:53:48,705 DEBUG [main] TestBasicFunctionality
 (TestBasicFunctionality.java:84) - Deleting AES Key.
2018-08-20 17:53:48,707 DEBUG [main] TestBasicFunctionality
 (TestBasicFunctionality.java:92) - Logging out.
```

```
Time: 0.205
```

```
OK (1 test)
```

### 步驟 3：提供登入資料給 JCE 供應商

HSM 需要先驗證您的 Java 應用程式，應用程式才能使用這些 HSM。每個應用程式可以使用一個工作階段。HSM 會使用明確登入或隱含登入方法，驗證工作階段。

**明確登入：**此方法可讓您直接在應用程式中提供 CloudHSM 憑證。它使用 `LoginManager.login()` 方法；您可在其中傳遞 CU 使用者名稱、密碼和 HSM 分割區 ID。如需使用明確登入方法的詳細資訊，請參閱[登入 HSM](#) 的程式碼範例。

**隱含登入：**此方法可讓您在新的屬性檔案、系統屬性或環境變數中設定 CloudHSM 憑證。

- 新的屬性檔案：建立名為 `HsmCredentials.properties` 的新檔案，並將其新增到您應用程式的 CLASSPATH。檔案應包含以下內容：

```
HSM_PARTITION = PARTITION_1
HSM_USER = <HSM user name>
HSM_PASSWORD = <password>
```

- 系統屬性：執行應用程式時，您可以透過系統屬性設定憑證。以下範例示範兩種不同的作法：

```
$ java -DHSM_PARTITION=PARTITION_1 -DHSM_USER=<HSM user name> -
DHSM_PASSWORD=<password>
```

```
System.setProperty("HSM_PARTITION", "PARTITION_1");
System.setProperty("HSM_USER", "<HSM user name>");
System.setProperty("HSM_PASSWORD", "<password>");
```

- 環境變數：將憑證設定為環境變數。

```
$ export HSM_PARTITION=PARTITION_1
$ export HSM_USER=<HSM user name>
$ export HSM_PASSWORD=<password>
```

如果應用程式未提供登入資料，或者，如果您在 HSM 驗證工作階段之前嘗試操作，就可能無法使用登入資料。在這些情況下，適用於 Java 的 CloudHSM 軟體程式庫會按照以下順序，搜尋登入資料：

1. `HsmCredentials.properties`
2. 系統屬性
3. 環境變數

## 錯誤處理

使用明確登入會比隱含登入方法更容易處理錯誤。當您使用 LoginManager 類別時，您比較能控制應用程式如何處理失敗情況。隱含登入方法會讓處理錯誤時難以判斷到底是登入資料無效，或是 HSM 在驗證工作階段時發生問題。

## AWS CloudHSM 用戶端 SDK 3 的 JCE 提供者中的金鑰管理基本概念

JCE 提供者的金鑰管理基本概念包括匯入金鑰、匯出金鑰、透過控制代碼載入金鑰或刪除金鑰。如需管理金鑰的詳細資訊，請參閱[管理金鑰](#)的程式碼範例。

您也可以在此[程式碼範例](#)中尋找更多 JCE 提供者程式碼範例。

## 適用於用戶端 SDK 3 AWS CloudHSM 的用戶端 SDK 3 支援機制

本主題提供 AWS CloudHSM 用戶端 SDK 3 的 JCE 供應商支援機制的相關資訊。如需支援的 Java 密碼編譯架構 (JCA) 介面和引擎類別的相關資訊 AWS CloudHSM，請參閱下列主題。

### 主題

- [支援的金鑰](#)
- [受支援的密碼](#)
- [支援的摘要](#)
- [支援的雜湊訊息驗證碼 \(HMAC\) 演算法](#)
- [支援的登入/驗證機制](#)
- [機制註釋](#)

### 支援的金鑰

適用於 Java AWS CloudHSM 的軟體程式庫可讓您產生下列金鑰類型。

- AES：128 位元、192 位元和 256 位元 AES 金鑰。
- DESede：92 位元 3DES 金鑰。請參閱下列備註 [1](#) 查看即將進行的變更。
- NIST 曲線 secp256r1 (P-256)、secp384r1 (P-384) 和 secp256k1 (區塊鏈) 的 ECC 金鑰對。
- RSA：2048 位元至 4096 位元 RSA 金鑰，以 256 位元為單位遞增。

除了標準參數，我們也支援產生的每個金鑰使用下列參數。

- Label：金鑰標籤，您可以使用來搜尋金鑰。

- `isExtractable` : 指示是否可以從 HSM 匯出該金鑰。
- `isPersistent` : 指出在目前工作階段結束時，HSM 上是否保留金鑰。

### Note

Java 程式庫 3.1 版更詳細地提供指定參數的能力。如需詳細資訊，請參閱[支援的 Java 屬性](#)。

## 受支援的密碼

適用於 Java AWS CloudHSM 的軟體程式庫支援下列演算法、模式和填補組合。

| 演算法 | Mode | 填補                                                    | 備註                                                                                  |
|-----|------|-------------------------------------------------------|-------------------------------------------------------------------------------------|
| AES | CBC  | AES/CBC/N<br>oPadding<br><br>AES/CBC/P<br>KCS5Padding | 實作 Cipher.EN<br>CRYPT_MODE<br>和 Cipher.DE<br>CRYPT_MODE 。                           |
| AES | ECB  | AES/ECB/N<br>oPadding<br><br>AES/ECB/P<br>KCS5Padding | 實作 Cipher.EN<br>CRYPT_MODE<br>和 Cipher.DE<br>CRYPT_MODE 。使<br>用轉型 AES。              |
| AES | CTR  | AES/CTR/N<br>oPadding                                 | 實作 Cipher.EN<br>CRYPT_MODE<br>和 Cipher.DE<br>CRYPT_MODE 。                           |
| AES | GCM  | AES/GCM/N<br>oPadding                                 | 實作 Cipher.EN<br>CRYPT_MODE<br>和 Cipher.DE<br>CRYPT_MOD<br>E 、Cipher.WR<br>AP_MODE 和 |

| 演算法             | Mode | 填補                                                                                          | 備註                                                                                                                                                             |
|-----------------|------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |      |                                                                                             | <p>Cipher.UNWRAP_MODE 。</p> <p>執行 AES-GCM 加密時，HSM 會忽略請求中的初始化向量 (IV)，並使用自己產生的 IV。操作完成後，您必須呼叫 Cipher.getIV() 以取得 IV。</p>                                         |
| AESWrap         | ECB  | <p>AESWrap/ECB/ZeroPadding</p> <p>AESWrap/ECB/NoPadding</p> <p>AESWrap/ECB/PKCS5Padding</p> | <p>實作 Cipher.WRAP_MODE 和 Cipher.UNWRAP_MODE 。</p> <p>使用轉型 AES。</p>                                                                                             |
| DESede (三重 DES) | CBC  | <p>DESede/CBC/NoPadding</p> <p>DESede/CBC/PKCS5Padding</p>                                  | <p>實作 Cipher.ENCRYPT_MODE 和 Cipher.DECRYPT_MODE 。</p> <p>金鑰產生常式接受 168 或 192 位元的大小。不過，在內部所有 DESede 金鑰都是 192 位元。</p> <p>請參閱下列備註 <a href="#">1</a> 查看即將進行的變更。</p> |



| 演算法             | Mode | 填補                                                          | 備註                                                                                                                                                             |
|-----------------|------|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESede (三重 DES) | ECB  | DESede/ECB/<br>NoPadding<br><br>DESede/ECB/<br>PKCS5Padding | <p>實作 Cipher.ENCRYPT_MODE 和 Cipher.DECRYPT_MODE 。</p> <p>金鑰產生常式接受 168 或 192 位元的大小。不過，在內部所有 DESede 金鑰都是 192 位元。</p> <p>請參閱下列備註 <a href="#">1</a> 查看即將進行的變更。</p> |
| RSA             | ECB  | RSA/ECB/N<br>oPadding<br><br>RSA/ECB/P<br>KCS1Padding       | <p>實作 Cipher.ENCRYPT_MODE 和 Cipher.DECRYPT_MODE 。</p> <p>請參閱下列備註 <a href="#">1</a> 查看即將進行的變更。</p>                                                              |

| 演算法        | Mode | 填補                                                | 備註                                                                                                                                                           |
|------------|------|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RSA        | ECB  | RSA/ECB/0<br>AEPPadding                           | 實作 Cipher.EN<br>CRYPT_MOD<br>E 、Cipher.DE<br>CRYPT_MOD<br>E 、Cipher.WR<br>AP_MODE 和<br>Cipher.UN<br>WRAP_MODE 。<br><br>OAEPadding 是<br>OAEP，且填補類型是<br>SHA-1。 |
|            |      | RSA/ECB/0<br>AEPWithSH<br>A-1ANDMGF<br>1Padding   |                                                                                                                                                              |
|            |      | RSA/ECB/0<br>AEPWithSH<br>A-224ANDM<br>GF1Padding |                                                                                                                                                              |
|            |      | RSA/ECB/0<br>AEPWithSH<br>A-256ANDM<br>GF1Padding |                                                                                                                                                              |
|            |      | RSA/ECB/0<br>AEPWithSH<br>A-384ANDM<br>GF1Padding |                                                                                                                                                              |
|            |      | RSA/ECB/0<br>AEPWithSH<br>A-512ANDM<br>GF1Padding |                                                                                                                                                              |
|            |      |                                                   |                                                                                                                                                              |
| RSAAESWrap | ECB  | OAEPADDING                                        | 實作 Cipher.WR<br>AP_Mode 和<br>Cipher.UN<br>WRAP_MODE 。                                                                                                        |

## 支援的摘要

適用於 Java AWS CloudHSM 的軟體程式庫支援下列訊息摘要。

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

 Note

長度在 16 KB 下的資料是在 HSM 上進行雜湊處理，而較大的資料則是在本機軟體中進行雜湊處理。

### 支援的雜湊訊息驗證碼 (HMAC) 演算法

適用於 Java AWS CloudHSM 的軟體程式庫支援下列 HMAC 演算法。

- HmacSHA1
- HmacSHA224
- HmacSHA256
- HmacSHA384
- HmacSHA512

### 支援的登入/驗證機制

適用於 Java AWS CloudHSM 的軟體程式庫支援以下類型的簽章和驗證。

#### RSA 簽章類型

- NONEwithRSA
- SHA1withRSA
- SHA224withRSA
- SHA256withRSA
- SHA384withRSA
- SHA512withRSA
- SHA1withRSA/PSS

- SHA224withRSA/PSS
- SHA256withRSA/PSS
- SHA384withRSA/PSS
- SHA512withRSA/PSS

## ECDSA 簽章類型

- NONEwithECDSA
- SHA1withECDSA
- SHA224withECDSA
- SHA256withECDSA
- SHA384withECDSA
- SHA512withECDSA

## 機制註釋

**【1】** 根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## 用戶端 SDK AWS CloudHSM 3 支援的 Java 金鑰屬性

本主題說明如何使用 Java 程式庫 3.1 版的專屬延伸來設定 AWS CloudHSM 用戶端 SDK 3 的金鑰屬性。請在以下操作期間，使用此擴充功能來設定支援的金鑰屬性及其值：

- 金鑰產生
- 金鑰匯入
- 金鑰取消包裝

### Note

設定自訂金鑰屬性的擴充功能是選用功能。如果您具有在 Java 程式庫 3.0 版本中運作的程式碼，則不需要修改該程式碼。您建立的金鑰會繼續包含與之前相同的屬性。

## 主題

- [了解屬性](#)
- [支援的屬性](#)
- [設定金鑰的屬性](#)
- [整合練習](#)

## 了解屬性

您可以使用金鑰屬性來指定金鑰物件上允許的動作，包括公有金鑰、私有金鑰或秘密金鑰。您可以在建立金鑰物件操作期間定義金鑰屬性和值。

但是，Java Cryptography Extension (JCE) 未指定應該如何設定金鑰屬性的值，因此預設情況下會允許大部分動作。相反地，PKCS#11 標準定義了一組具有更嚴格預設值的完整屬性。從 Java 程式庫 3.1 版開始，CloudHSM 提供專屬的擴充功能，可讓您為常用的屬性設定更嚴格的值。

## 支援的屬性

您可以設定下表中列出之屬性的值。最佳實務是，只為您希望更有限制性的屬性設定值。如果您未指定值，CloudHSM 會使用下表中指定的預設值。預設值欄位中的空白儲存格表示屬性沒有獲派指定預設值。

| 屬性        | 預設值   |           |           | 備註                                                                                            |
|-----------|-------|-----------|-----------|-----------------------------------------------------------------------------------------------|
|           | 對稱金鑰  | 金鑰對中的公有金鑰 | 金鑰對中的私有金鑰 |                                                                                               |
| CKA_TOKEN | FALSE | FALSE     | FALSE     | 永久金鑰，會跨叢集中的所有 HSM 進行複寫並包含在備份中。CKA_TOKEN = FALSE 代表工作階段金鑰，該金鑰只被載入到一個 HSM 上，並在與 HSM 的连接中斷時自動擦除。 |

| 屬性              | 預設值  |      |      | 備註                                                              |
|-----------------|------|------|------|-----------------------------------------------------------------|
| CKA_LABEL       |      |      |      | 使用者定義的字串。它可讓您輕鬆識別 HSM 上的金鑰。                                     |
| CKA_EXTRACTABLE | TRUE |      | TRUE | True 表示您可以從 HSM 匯出此金鑰。                                          |
| CKA_ENCRYPT     | TRUE | TRUE |      | True 表示您可以使用金鑰來加密任何緩衝區。                                         |
| CKA_DECRYPT     | TRUE |      | TRUE | True 表示您可以使用金鑰來解密任何緩衝區。對於其 CKA_WRAP 設定為 true 的金鑰，通常將此設定為 FALSE。 |
| CKA_WRAP        | TRUE | TRUE |      | True 表示您可以使用該金鑰來包裝另一個金鑰。對於私有金鑰，您通常將此設定為 FALSE。                  |
| CKA_UNWRAP      | TRUE |      | TRUE | True 表示您可以使用金鑰來取消包裝 (匯入) 另一個金鑰。                                 |

| 屬性          | 預設值  |      |      | 備註                                                                                     |
|-------------|------|------|------|----------------------------------------------------------------------------------------|
| CKA_SIGN    | TRUE |      | TRUE | True 表示您可以使用金鑰來簽署訊息摘要。對於公有金鑰和您已封存的私有金鑰，這通常會設定為 FALSE。                                  |
| CKA_VERIFY  | TRUE | TRUE |      | True 表示您可以使用金鑰來驗證簽章。對於私有金鑰，這通常被設定為 FALSE。                                              |
| CKA_PRIVATE | TRUE | TRUE | TRUE | True 表示在使用者通過驗證之前，使用者可能無法存取金鑰。為了清楚起見，使用者在通過驗證之前無法存取 CloudHSM 上的任何金鑰，即使此屬性設為 FALSE 也一樣。 |

 Note

您可以在 PKCS #11 程式庫中獲得更廣泛的屬性支援。如需詳細資訊，請參閱[支援的 PKCS #11 屬性](#)。

## 設定金鑰的屬性

CloudHsmKeyAttributesMap 是類似 [Java 映射](#) 的物件，您可以使用它來設定金鑰物件的屬性值。CloudHsmKeyAttributesMap 函數的方法類似於用於 Java 映射處理的方法。

若要設定屬性的自訂值，您有兩個選項：

- 使用下表中列出的方法
- 使用本文稍後示範的產生器模式

屬性映射物件支援以下列方法設定屬性：

| 作業            | 傳回值                             | CloudHSMKeyAttributesMap 方法 |
|---------------|---------------------------------|-----------------------------|
| 獲取現有金鑰的金鑰屬性的值 | 物件 (包含值) 或 null                 | get(keyAttribute)           |
| 填入一個金鑰屬性的值    | 與金鑰屬性相關聯的先前值，如果金鑰屬性沒有映射，則為 null | put(keyAttribute, value)    |
| 填入多個金鑰屬性的值    | N/A                             | putAll(keyAttributesMap)    |
| 從屬性映射中刪除金鑰值對  | 與金鑰屬性相關聯的先前值，如果金鑰屬性沒有映射，則為 null | remove(keyAttribute)        |

### Note

您未明確指定的任何屬性都會設定為 [the section called “支援的屬性”](#) 中上表所列的預設值。

## 產生器模式範例

開發人員通常會發現，透過產生器模式利用類別更加方便。舉例來說：

```
import com.amazonaws.cloudhsm.CloudHsmKeyAttributes;
import com.amazonaws.cloudhsm.CloudHsmKeyAttributesMap;
```



```
import com.amazonaws.cloudhsm.CloudHsmKeyPairAttributesMap;

CloudHsmKeyAttributesMap keyAttributesSessionDecryptionKey =
 new CloudHsmKeyAttributesMap.Builder()
 .put(CloudHsmKeyAttributes.CKA_LABEL, "ExtractableSessionKeyEncryptDecrypt")
 .put(CloudHsmKeyAttributes.CKA_WRAP, false)
 .put(CloudHsmKeyAttributes.CKA_UNWRAP, false)
 .put(CloudHsmKeyAttributes.CKA_SIGN, false)
 .put(CloudHsmKeyAttributes.CKA_VERIFY, false)
 .build();

CloudHsmKeyAttributesMap keyAttributesTokenWrappingKey =
 new CloudHsmKeyAttributesMap.Builder()
 .put(CloudHsmKeyAttributes.CKA_LABEL, "TokenWrappingKey")
 .put(CloudHsmKeyAttributes.CKA_TOKEN, true)
 .put(CloudHsmKeyAttributes.CKA_ENCRYPT, false)
 .put(CloudHsmKeyAttributes.CKA_DECRYPT, false)
 .put(CloudHsmKeyAttributes.CKA_SIGN, false)
 .put(CloudHsmKeyAttributes.CKA_VERIFY, false)
 .build();
```

開發人員也可以利用預先定義的屬性集，作為在金鑰範本中強制執行最佳實務的便利方式。舉例來說：

```
//best practice template for wrapping keys

CloudHsmKeyAttributesMap commonKeyAttrs = new CloudHsmKeyAttributesMap.Builder()
 .put(CloudHsmKeyAttributes.CKA_EXTRACTABLE, false)
 .put(CloudHsmKeyAttributes.CKA_DECRYPT, false)
 .build();

// initialize a new instance of CloudHsmKeyAttributesMap by copying commonKeyAttrs
// but with an appropriate label

CloudHsmKeyAttributesMap firstKeyAttrs = new CloudHsmKeyAttributesMap(commonKeyAttrs);
firstKeyAttrs.put(CloudHsmKeyAttributes.CKA_LABEL, "key label");

// alternatively, putAll() will overwrite existing values to enforce conformance

CloudHsmKeyAttributesMap secondKeyAttrs = new CloudHsmKeyAttributesMap();
secondKeyAttrs.put(CloudHsmKeyAttributes.CKA_DECRYPT, true);
secondKeyAttrs.put(CloudHsmKeyAttributes.CKA_ENCRYPT, true);
secondKeyAttrs.put(CloudHsmKeyAttributes.CKA_LABEL, "safe wrapping key");
secondKeyAttrs.putAll(commonKeyAttrs); // will overwrite CKA_DECRYPT to be FALSE
```

## 設定金鑰對的屬性

使用 Java 類別 `CloudHsmKeyPairAttributesMap` 來處理金鑰對的金鑰屬性。`CloudHsmKeyPairAttributesMap` 封裝了兩個 `CloudHsmKeyAttributesMap` 物件；一個用於公有金鑰，另一個用於私有金鑰。

若要分別為公有金鑰和私有金鑰設定個別屬性，您可以在該金鑰對應的 `CloudHsmKeyAttributes` 映射物件上使用 `put()` 方法。使用 `getPublic()` 方法來擷取公有金鑰的屬性映射，以及使用 `getPrivate()` 來擷取私有金鑰的屬性映射。使用 `putAll()` 與金鑰對屬性映射作為引數，填入公有金鑰和私有金鑰對的多個金鑰屬性值。

## 產生器模式範例

開發人員通常會發現，透過產生器模式來設定金鑰屬性更加方便。例如：

```
import com.amazonaws.cloudhsm.CloudHsmKeyAttributes;
import com.amazonaws.cloudhsm.CloudHsmKeyAttributesMap;
import com.amazonaws.cloudhsm.CloudHsmKeyPairAttributesMap;

//specify attributes up-front
CloudHsmKeyAttributesMap keyAttributes =
 new CloudHsmKeyAttributesMap.Builder()
 .put(CloudHsmKeyAttributes.CKA_SIGN, false)
 .put(CloudHsmKeyAttributes.CKA_LABEL, "PublicCertSerial12345")
 .build();

CloudHsmKeyPairAttributesMap keyPairAttributes =
 new CloudHsmKeyPairAttributesMap.Builder()
 .withPublic(keyAttributes)
 .withPrivate(
 new CloudHsmKeyAttributesMap.Builder() //or specify them inline
 .put(CloudHsmKeyAttributes.CKA_LABEL, "PrivateCertSerial12345")
 .put(CloudHsmKeyAttributes.CKA_WRAP, FALSE)
 .build()
)
 .build();
```

### Note

如需此專屬擴充功能的詳細資訊，請參閱 [Javadoc](#) 封存和 GitHub 上的 [範例](#)。若要瀏覽 Javadoc，請下載並展開此封存。

## 整合練習

若需要使用金鑰操作指定金鑰屬性，請依照下列步驟執行：

1. 執行個體化對稱金鑰的 `CloudHsmKeyAttributesMap` 或金鑰對的 `CloudHsmKeyPairAttributesMap`。
2. 使用必要的金鑰屬性和值來定義步驟 1 的屬性物件。
3. 執行個體化對應至特定金鑰類型的 `Cavium*ParameterSpec` 類別，並在其建構函數中傳遞此設定好的屬性物件。
4. 將此 `Cavium*ParameterSpec` 物件傳遞到相應的加密類別或方法中。

如需參考，下表包含支援自定義金鑰屬性的 `Cavium*ParameterSpec` 類別和方法。

| 金鑰類型 | 參數規格類別                                          | 範例建構函數                                                                                                                               |
|------|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| 基本類別 | <code>CaviumKeyGenAlgorithmParameterSpec</code> | <code>CaviumKeyGenAlgorithmParameterSpec(CloudHsmKeyAttributesMap keyAttributesMap)</code>                                           |
| DES  | <code>CaviumDESKeyGenParameterSpec</code>       | <code>CaviumDESKeyGenParameterSpec(int keySize, byte[] iv, CloudHsmKeyAttributesMap keyAttributesMap)</code>                         |
| RSA  | <code>CaviumRSAKeyGenParameterSpec</code>       | <code>CaviumRSAKeyGenParameterSpec(int keysize, BigInteger publicExponent, CloudHsmKeyPairAttributesMap keyPairAttributesMap)</code> |

| 金鑰類型 | 參數規格類別                                 | 範例建構函數                                                                                          |
|------|----------------------------------------|-------------------------------------------------------------------------------------------------|
| 秘密   | CaviumGenericSecretKeyGenParameterSpec | CaviumGenericSecretKeyGenParameterSpec(int size, CloudHsmKeyAttributesMap keyAttributesMap)     |
| AES  | CaviumAESKeyGenParameterSpec           | CaviumAESKeyGenParameterSpec(int keySize, byte[] iv, CloudHsmKeyAttributesMap keyAttributesMap) |
| EC   | CaviumECGenParameterSpec               | CaviumECGenParameterSpec(String stdName, CloudHsmKeyPairAttributesMap keyPairAttributesMap)     |

範本程式碼：產生並包裝金鑰

這些簡短的程式碼範例示範兩個不同操作的步驟：金鑰產生和金鑰包裝：

```
// Set up the desired key attributes

KeyGenerator keyGen = KeyGenerator.getInstance("AES", "Cavium");
CaviumAESKeyGenParameterSpec keyAttributes = new CaviumAESKeyGenParameterSpec(
 256,
 new CloudHsmKeyAttributesMap.Builder()
 .put(CloudHsmKeyAttributes.CKA_LABEL, "MyPersistentAESKey")
 .put(CloudHsmKeyAttributes.CKA_EXTRACTABLE, true)
 .put(CloudHsmKeyAttributes.CKA_TOKEN, true)
 .build()
);
```

```
// Assume we already have a handle to the myWrappingKey
// Assume we already have the wrappedBytes to unwrap

// Unwrap a key using Custom Key Attributes

CaviumUnwrapParameterSpec unwrapSpec = new
 CaviumUnwrapParameterSpec(myInitializationVector, keyAttributes);

Cipher unwrapCipher = Cipher.getInstance("AESWrap", "Cavium");
unwrapCipher.init(Cipher.UNWRAP_MODE, myWrappingKey, unwrapSpec);
Key unwrappedKey = unwrapCipher.unwrap(wrappedBytes, "AES", Cipher.SECRET_KEY);
```

## Java for Client SDK 3 AWS CloudHSM 軟體程式庫的程式碼範例

本主題提供用戶端 SDK AWS CloudHSM 3 Java 程式碼範例的資源和資訊。

### 先決條件

執行範例之前，您必須先設定環境：

- 安裝並設定 [Java 密碼編譯延伸模組 \(JCE\) 提供者](#)和 [AWS CloudHSM 用戶端套件](#)。
- 設定有效的 [HSM 使用者名稱和密碼](#)。加密使用者 (CU) 許可足夠執行這些任務。在每個範例中，您的應用程式會使用這些登入資料來登入 HSM。
- 決定如何提供憑證給 [JCE 提供者](#)。

### 程式碼範例

下列程式碼範例會示範如何使用 [AWS CloudHSM JCE 提供者](#)來執行基本任務。在 [GitHub](#) 可取得更多程式碼範例。

- [登入 HSM](#)
- [管理金鑰](#)
- [產生 AES 金鑰](#)
- [使用 AES-GCM 進行加密和解密](#)
- [使用 AES-CTR 進行加密和解密](#)
- [使用 D3DES-ECB 加密和解密](#) 請參閱備註 1
- [使用 AES-GCM 包裝和取消包裝金鑰](#)

- [使用 AES 包裝和取消包裝金鑰](#)
- [使用 RSA 包裝和取消包裝金鑰](#)
- [使用支援的金鑰屬性](#)
- [列舉金鑰存放區中的金鑰](#)
- [使用 CloudHSM 金鑰存放區](#)
- [以多執行緒範例簽署訊息](#)
- [使用 EC 金鑰簽署和驗證](#)

**【1】** 根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## 用戶端 SDK 3 的 AWS CloudHSM KeyStore Java 類別

AWS CloudHSM KeyStore 類別提供特殊用途的 PKCS12 金鑰存放區，允許透過 AWS CloudHSM keytool 和 jarsigner 等應用程式存取金鑰。此金鑰存放區可與您的金鑰資料一起儲存憑證，並將其與在 AWS CloudHSM 儲存的金鑰資料連結在一起。

### Note

由於憑證是公開資訊，並且為了最大化密碼編譯金鑰的儲存容量，AWS CloudHSM 不支援在 HSMs 上儲存憑證。

類別實作 Java AWS CloudHSM KeyStore 密碼編譯延伸 (JCE) 的 KeyStore 服務提供者介面 (SPI)。如需使用 KeyStore 的詳細資訊，請參閱 [Class KeyStore](#)。

為 AWS CloudHSM 用戶端 SDK 3 選擇適當的金鑰存放區

AWS CloudHSM Java 密碼編譯延伸 (JCE) 供應商隨附預設的傳遞唯讀金鑰存放區，可將所有交易傳遞至 HSM。此預設金鑰存放區與特殊用途的 AWS CloudHSM 金鑰存放區不同。在大多數情況下，您會使用預設值取得較佳的執行階段效能和輸送量。除了將金鑰操作卸載至 HSM 之外，您應該只將 AWS CloudHSM KeyStore 用於需要憑證和憑證型操作支援的應用程式。

雖然這兩種金鑰存放區都使用 JCE 提供者進行操作，但它們是獨立的實體，且不會彼此交換資訊。

請依照下方步驟說明為您的 Java 應用程式載入預設的金鑰存放區：

```
KeyStore ks = KeyStore.getInstance("Cavium");
```

載入特殊用途的 CloudHSM 金鑰存放區，如下所示：

```
KeyStore ks = KeyStore.getInstance("CloudHSM")
```

### 初始化用戶端 SDK 3 的 AWS CloudHSM KeyStore

以您登入 JCE 供應商的相同方式登入 AWS CloudHSM KeyStore。您可以使用環境變數或系統屬性檔案，並且在開始使用 CloudHSM 金鑰存放區之前應先登入。如需使用 JCE 提供者登入 HSM 的範例，請參閱[登入 HSM](#)。

如有需要，您可以指定一組密碼來加密保存金鑰儲存資料的本機 PKCS12 檔案。當您建立 AWS CloudHSM 金鑰存放區時，您可以設定密碼，並在使用載入、設定和取得方法時提供密碼。

請依照以下方式，將新的 CloudHSM 金鑰存放區物件執行個體化：

```
ks.load(null, null);
```

使用 store 方法將金鑰存放區資料寫入檔案。從那時起，您可以依照以下方式，搭配來源檔案和密碼使用 load 方法載入現有的金鑰存放區：

```
ks.load(inputStream, password);
```

### 使用用戶端 SDK 3 的 AWS CloudHSM/AWS CloudHSM KeyStore

CloudHSM 金鑰存放區物件通常會透過第三方應用程式使用，例如：[jarsigner](#) 或 [keytool](#)。您也可以直接搭配程式碼存取物件。

AWS CloudHSM KeyStore 符合 JCE [類別 KeyStore](#) 規格，並提供下列函數。

- load

從特定的輸入串流載入金鑰存放區。如果在儲存金鑰存放區時設定了密碼，則必須提供相同的密碼才能成功載入。將這兩個參數設為 Null 以初始化一個新的空金鑰存放區。

```
KeyStore ks = KeyStore.getInstance("CloudHSM");
ks.load(inputStream, password);
```

- `aliases`

傳回特定的金鑰存放區執行個體中的所有項目別名名稱列舉。結果包括本機儲存在 PKCS12 檔案中的物件，以及常駐於 HSM 的物件。

範本程式碼：

```
KeyStore ks = KeyStore.getInstance("CloudHSM");
for(Enumeration<String> entry = ks.aliases(); entry.hasMoreElements();)
{
 String label = entry.nextElement();
 System.out.println(label);
}
```

- `ContainsAlias`

如果金鑰存放區可存取至少一個有指定別名的物件，則傳回 `True`。金鑰存放區會檢查本機儲存在 PKCS12 檔案中的物件，以及常駐於 HSM 的物件。

- `DeleteEntry`

從本機 PKCS12 檔案刪除憑證項目。不支援使用 AWS CloudHSM KeyStore 刪除存放在 HSM 中的金鑰資料。您可以使用 CloudHSM 的 [key\\_mgmt\\_util](#) 工具刪除金鑰。

- `GetCertificate`

如果可用，則傳回與別名相關聯的憑證。如果別名不存在或參考非憑證的物件，則函數會傳回 `NULL`。

```
KeyStore ks = KeyStore.getInstance("CloudHSM");
Certificate cert = ks.getCertificate(alias)
```

- `GetCertificateAlias`

傳回第一個資料符合特定憑證的金鑰存放區項目名稱 (別名)。

```
KeyStore ks = KeyStore.getInstance("CloudHSM");
String alias = ks.getCertificateAlias(cert)
```

- `GetCertificateChain`

傳回與特定別名相關聯的憑證鏈。如果別名不存在或參考非憑證的物件，則函數會傳回 `NULL`。

- `GetCreationDate`



傳回由給定別名辨識的項目建立日期。如果沒有建立日期，則函數會傳回憑證生效的日期。

- **GetKey**

GetKey 會傳遞給 HSM 並傳回與特定標籤對應的金鑰物件。由於 getKey 會直接查詢 HSM，因此無論金鑰存放區是否產生金鑰，都可用於 HSM 上的任何金鑰。

```
Key key = ks.getKey(keyLabel, null);
```

- **IsCertificateEntry**

檢查有特定別名的項目是否代表憑證項目。

- **IsKeyEntry**

檢查有特定別名的項目是否代表金鑰項目。此動作會在 PKCS12 檔案和 HSM 中搜尋別名。

- **SetCertificateEntry**

指定特定憑證至特定別名。如果特定的別名已用於識別金鑰或憑證，則會擲出 KeyStoreException。您可以使用 JCE 程式碼來取得金鑰物件，然後使用金鑰存放區 SetKeyEntry 方法連結憑證至密鑰。

- **有 byte[] 金鑰的 SetKeyEntry**

用戶端 SDK 3 目前不支援此 API。

- **有 Key 物件的 SetKeyEntry**

指定特定金鑰至特定別名，並將其儲存在 HSM 內。如果 Key 物件不是類型 CaviumKey，金鑰會以可擷取的工作階段金鑰匯入 HSM。

如果 Key 物件屬於類型 PrivateKey，則必須附有相對應的憑證鏈。

如果別名已經存在，則 SetKeyEntry 呼叫會擲出 KeyStoreException 並防止覆寫金鑰。如果必須覆寫金鑰，請使用 KMU 或 JCE。

- **EngineSize**

傳回金鑰存放區中的項目數目。

- **Store**

以 PKCS12 檔案格式儲存金鑰存放區至特定輸出串流，並使用特定的密碼加以保護。此外，它仍然保留載入的金鑰 (使用 setKey 呼叫的組合)。

# 密碼編譯 API：的新一代 (CNG) 和金鑰儲存供應商 (KSP) AWS CloudHSM

適用於 Windows 的 AWS CloudHSM 用戶端包含 CNG 和 KSP 提供者。

金鑰儲存提供者 (KSP) 可讓您儲存和擷取金鑰。例如，如果您將 Microsoft Active Directory Certificate Services (AD CS) 角色新增到您的 Windows 伺服器，並選擇為憑證授權機制 (CA) 建立新的私有金鑰，您可以選擇 KSP 來管理金鑰儲存。當您設定 AD CS 角色時，您可以選擇 KSP。如需詳細資訊，請參閱[建立 Windows Server CA](#)。

Cryptography API: Next Generation (CNG) 是一套專用於 Microsoft Windows 作業系統的密碼編譯 API。CNG 可讓開發人員使用密碼編譯技術來確保 Windows 應用程式的安全。在高階上，CNG 的 AWS CloudHSM 實作提供下列功能：

- 密碼編譯原則 – 可讓您執行基本密碼編譯操作。
- 金鑰匯入和匯出 – 可讓您匯入和匯出非對稱金鑰。
- 資料保護 API (CNG DPAPI) – 可讓您輕鬆加密和解密資料。
- 金鑰儲存和擷取 – 可讓您安全地儲存和隔離非對稱金鑰對的私有金鑰。

## 主題

- [驗證的 KSP 和 CNG 提供者 AWS CloudHSM](#)
- [使用 AWS CloudHSM Windows 用戶端的先決條件](#)
- [將 AWS CloudHSM 金鑰與憑證建立關聯](#)
- [的 CNG 提供者程式碼範例 AWS CloudHSM](#)

## 驗證的 KSP 和 CNG 提供者 AWS CloudHSM

安裝 Windows AWS CloudHSM 用戶端時會安裝 KSP 和 CNG 提供者。您可以依照在 [安裝用戶端 \(Windows\)](#) 的步驟安裝用戶端。

使用下列各節來驗證供應商的安裝。

### 設定和執行 Windows AWS CloudHSM 用戶端

若要啟動 Windows CloudHSM 用戶端，您必須先符合[先決條件](#)。然後，更新提供者使用的組態檔案，並完成以下步驟來啟動用戶端。在您首次使用 KSP 和 CNG 提供者時和在叢集中新增或移除 HSM 之後，您需要執行以下步驟。如此一來，AWS CloudHSM 就能同步資料並維持叢集中所有 HSMs 一致性。

## 步驟 1：停止 AWS CloudHSM 用戶端

更新提供者使用的組態檔案之前，請先停止 AWS CloudHSM 用戶端。如果用戶端已停止，執行停止命令並不會造成影響。

- 用於 Windows 用戶端 1.1.2+：

```
C:\Program Files\Amazon\CloudHSM>net.exe stop AWSCloudHSMClient
```

- 用於 Windows 用戶端 1.1.1 和更早版本：

在您啟動 AWS CloudHSM 用戶端的命令視窗中使用 Ctrl + C。

## 步驟 2：更新 AWS CloudHSM 組態檔案

此步驟使用 `-a` 設定工具 [的](#) 參數，將叢集的其中一個 HSM 的彈性網路界面 (ENI) IP 地址新增至組態檔案。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\configure.exe" -a <HSM ENI IP>
```

若要取得叢集中 HSM 的 ENI IP 地址，請導覽至 AWS CloudHSM 主控台，選擇叢集，然後選取所需的叢集。您也可以使用 [DescribeClusters](#) 操作、[describe-clusters](#) 命令或 [Get-HSM2Cluster](#) PowerShell cmdlet。僅輸入一個 ENI IP 地址。無論您使用哪個 ENI IP 地址都是如此。

## 步驟 3：啟動 AWS CloudHSM 用戶端

接著，啟動或重新啟動 AWS CloudHSM 用戶端。當 AWS CloudHSM 用戶端啟動時，它會使用其組態檔案中的 ENI IP 地址來查詢叢集。接著會將叢集的所有 HSM 的 ENI IP 地址，新增至叢集資訊檔案。

- 用於 Windows 用戶端 1.1.2+：

```
C:\Program Files\Amazon\CloudHSM>net.exe start AWSCloudHSMClient
```

- 用於 Windows 用戶端 1.1.1 和更早版本：

```
C:\Program Files\Amazon\CloudHSM>start "cloudhsm_client" cloudhsm_client.exe C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_client.cfg
```

## 檢查 KSP 和 CNG 提供者

您可以使用以下命令，以判斷哪些提供者已安裝在您的系統上。這些命令列出已註冊的 KSP 和 CNG 提供者。不需要執行 AWS CloudHSM 用戶端。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\ksp_config.exe" -enum
```

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cng_config.exe" -enum
```

如要驗證 KSP 和 CNG 提供者是否已安裝在 Windows Server EC2 執行個體上，您會在清單中看到下列項目：

```
Cavium CNG Provider
Cavium Key Storage Provider
```

如果缺少 CNG 提供者，請執行下列命令。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\cng_config.exe" -register
```

如果缺少 KSP 提供者，請執行下列命令。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\ksp_config.exe" -register
```

## 使用 AWS CloudHSM Windows 用戶端的先決條件

您必須先設定系統上 HSM 的登入憑證，才能啟動 Windows AWS CloudHSM 用戶端並使用 KSP 和 CNG 提供者。您可以透過 Windows 認證管理員或系統環境變數來設定登入資料。建議您使用 Windows 認證管理員來存放登入資料。此選項適用於 AWS CloudHSM 用戶端 2.0.4 版及更新版本。使用環境變數較容易設定，但比起使用 Windows 認證管理員較不安全。

### Windows 認證管理員

您可以使用 `set_cloudhsm_credentials` 公用程式或 Windows 認證管理員界面。

- 使用 **set\_cloudhsm\_credentials** 公用程式：

`set_cloudhsm_credentials` 公用程式包含在您的 Windows 安裝程式中。您可以使用此公用程式，輕鬆地將 HSM 登入資料傳遞到 Windows 認證管理員。如果您想要從來源編譯此公用程式，您可以使用安裝程式中包含的 Python 程式碼。

1. 前往 `C:\Program Files\Amazon\CloudHSM\tools\` 資料夾。

2. 使用 CU 使用者名稱和密碼參數執行 `set_cloudhsm_credentials.exe` 檔案。

```
set_cloudhsm_credentials.exe --username <CU USER> --password <CU PASSWORD>
```

- 使用認證管理員界面：

您可以使用認證管理員界面來手動管理您的登入資料。

1. 若要開啟認證管理員，請在工作列的搜尋方塊中輸入 `credential manager`，然後選取認證管理員。
2. 選取 Windows 認證以管理 Windows 認證。
3. 選取新增一般認證並填寫詳細資訊，如下所示：
  - 在網際網路或網路位址中，輸入目標名為 `cloudhsm_client`。
  - 在使用者名稱和密碼中，輸入 CU 登入資料。
  - 按一下 OK (確定)。

## 系統環境變數

您可以設定系統環境變數，用以識別 Windows 應用程式的 HSM 和 [加密使用者](#) (CU)。您可以使用 [setx 命令](#) 來設定系統環境變數，或 [以程式設計方式](#) 或是在 Windows 系統屬性控制台的進階標籤中設定永久性系統環境變數。

### Warning

當您透過系統環境變數設定登入資料時，密碼會在使用者的系統上以純文字提供。若要解決此問題，請使用 Windows 認證管理員。

設定下列系統環境變數：

**`n3fips_password=<CU USERNAME>:<CU PASSWORD>`**

識別 HSM 中的 [加密使用者](#) (CU)，並提供所有必要的登入資訊。您的應用程式會以這個 CU 的身分進行驗證和執行。這個應用程式具有此 CU 的許可，並僅可以檢視和管理該 CU 擁有和共用的金鑰。若要建立新 CU，請使用 [createUser](#)。若要尋找現有 CU，請使用 [listUsers](#)。

例如：

```
setx /m n3fips_password test_user:password123
```

## 將 AWS CloudHSM 金鑰與憑證建立關聯

您必須先將 AWS CloudHSM 金鑰的中繼資料匯入本機憑證存放區，並將中繼資料與憑證建立關聯，才能將金鑰與第三方工具搭配使用，例如 Microsoft 的 [SignTool](#)。若要匯入金鑰的中繼資料，請使用包含在 CloudHSM 3.0 以上版本中的 `import_key.exe` 公用程式。以下步驟提供額外資訊和範例輸出。

### 步驟 1：匯入您的憑證

在 Windows 中，您應可按兩下憑證，將其匯入至您的本機憑證存放區。

不過，如果按兩下無法執行，請使用 [Microsoft Certreq 工具](#) 將憑證匯入至憑證管理員。例如：

```
certreq -accept <certificatename>
```

如果這個動作失敗，且您收到錯誤訊息 `Key not found`，請繼續執行步驟 2。如果憑證出現在金鑰存放區，就表示您已完成任務，不需要進一步的動作。

### 步驟 2：收集憑證識別資訊

如果上一個步驟沒有成功，您需要建立您的私密金鑰與憑證之間的關聯。不過，在您可以建立關聯之前，您必須先找到憑證的唯一容器名稱和序號。使用等公用程式 `certutil` 來顯示所需的憑證資訊。的下列範例輸出 `certutil` 會顯示容器名稱和序號。

```
===== Certificate 1 ===== Serial Number:
72000000047f7f7a9d41851b4e000000000004Issuer: CN=Enterprise-CANotBefore: 10/8/2019
11:50
AM NotAfter: 11/8/2020 12:00 PMSubject: CN=www.example.com, OU=Certificate
Management,
O=Information Technology, L=Seattle, S=Washington, C=USNon-root CertificateCert
Hash(sha1): 7f d8 5c 00 27 bf 37 74 3d 71 5b 54 4e c0 94 20 45 75 bc 65No key
provider
information Simple container name: CertReq-39c04db0-6aa9-4310-93db-db0d9669f42c
Unique
container name: CertReq-39c04db0-6aa9-4310-93db-db0d9669f42c
```

### 步驟 3：將 AWS CloudHSM 私有金鑰與憑證建立關聯

若要將金鑰與憑證建立關聯，請務必先[啟動 AWS CloudHSM 用戶端協助程式](#)。然後，使用 `import_key.exe` (包含在 CloudHSM 3.0 以上版本中)，建立私有金鑰與憑證之間的關聯。指定憑證時，

請使用其簡易容器名稱。以下範例顯示命令和回應。此動作只會複製金鑰的中繼資料；金鑰會保留在 HSM 上。

```
$> import_key.exe -RSA CertReq-39c04db0-6aa9-4310-93db-db0d9669f42c
```

```
Successfully opened Microsoft Software Key Storage Provider : 0NCryptOpenKey failed : 80090016
```

#### 步驟 4：更新憑證存放區

確定 AWS CloudHSM 用戶端協助程式仍在執行中。然後，使用動certutil詞 -repairstore更新憑證序號。以下範例顯示命令和輸出。如需 [-repairstore 動詞](#)的相關資訊，請參閱 Microsoft 文件。

```
C:\Program Files\Amazon\CloudHSM>certutil -f -csp "Cavium Key Storage Provider"-
repairstore my "72000000047f7f7a9d41851b4e000000000004"
my "Personal"
===== Certificate 1 =====
Serial Number: 72000000047f7f7a9d41851b4e000000000004
Issuer: CN=Enterprise-CA
NotBefore: 10/8/2019 11:50 AM
NotAfter: 11/8/2020 12:00 PM
Subject: CN=www.example.com, OU=Certificate Management, O=Information Technology,
L=Seattle, S=Washington, C=US
Non-root CertificateCert Hash(sha1): 7f d8 5c 00 27 bf 37 74 3d 71 5b 54 4e c0 94 20 45
75 bc 65
SDK Version: 3.0
Key Container = CertReq-39c04db0-6aa9-4310-93db-db0d9669f42c
Provider = "Cavium Key Storage Provider"
Private key is NOT exportableEncryption test passedCertUtil: -repairstore command
completed successfully.
```

更新憑證序號後，您可以在 Windows 上將此憑證和對應的 AWS CloudHSM 私有金鑰與任何第三方簽署工具搭配使用。

#### 的 CNG 提供者程式碼範例 AWS CloudHSM

 \*\* 僅限範例程式碼 – 不適用於生產 \*\*

此範例程式碼僅供說明之用。不要在生產環境中執行此程式碼。

下列範例顯示如何列舉系統上已註冊加密提供者的程式碼範例，以尋找與適用於 Windows 的 CloudHSM 用戶端一起安裝的 CNG 提供者。此範例還示範如何建立非對稱金鑰對，以及如何使用金鑰對來簽署資料。

### Important

執行此範例之前，您必須先設定 HSM 登入資料，如先決條件中所述。如需詳細資訊，請參閱[使用 AWS CloudHSM Windows 用戶端的先決條件](#)。

```
// CloudHsmCngExampleConsole.cpp : Console application that demonstrates CNG
// capabilities.
// This example contains the following functions.
//
// VerifyProvider() - Enumerate the registered providers and retrieve Cavium
// KSP and CNG providers.
// GenerateKeyPair() - Create an RSA key pair.
// SignData() - Sign and verify data.
//
#include "stdafx.h"
#include <Windows.h>

#ifdef NT_SUCCESS
#define NT_SUCCESS(Status) ((NTSTATUS)(Status) >= 0)
#endif

#define CAVIUM_CNG_PROVIDER L"Cavium CNG Provider"
#define CAVIUM_KEYSTORE_PROVIDER L"Cavium Key Storage Provider"

// Enumerate the registered providers and determine whether the Cavium CNG provider
// and the Cavium KSP provider exist.
//
bool VerifyProvider()
{
 NTSTATUS status;
 ULONG cbBuffer = 0;
 PCRYPT_PROVIDERS pBuffer = NULL;
 bool foundCng = false;
 bool foundKeystore = false;
```



```

// Retrieve information about the registered providers.
// cbBuffer - the size, in bytes, of the buffer pointed to by pBuffer.
// pBuffer - pointer to a buffer that contains a CRYPT_PROVIDERS structure.
status = BCryptEnumRegisteredProviders(&cbBuffer, &pBuffer);

// If registered providers exist, enumerate them and determine whether the
// Cavium CNG provider and Cavium KSP provider have been registered.
if (NT_SUCCESS(status))
{
 if (pBuffer != NULL)
 {
 for (ULONG i = 0; i < pBuffer->cProviders; i++)
 {
 // Determine whether the Cavium CNG provider exists.
 if (wcscmp(CAVIUM_CNG_PROVIDER, pBuffer->rgpszProviders[i]) == 0)
 {
 printf("Found %S\n", CAVIUM_CNG_PROVIDER);
 foundCng = true;
 }

 // Determine whether the Cavium KSP provider exists.
 else if (wcscmp(CAVIUM_KEYSTORE_PROVIDER, pBuffer->rgpszProviders[i]) == 0)
 {
 printf("Found %S\n", CAVIUM_KEYSTORE_PROVIDER);
 foundKeystore = true;
 }
 }
 }
}
else
{
 printf("BCryptEnumRegisteredProviders failed with error code 0x%08x\n", status);
}

// Free memory allocated for the CRYPT_PROVIDERS structure.
if (NULL != pBuffer)
{
 BCryptFreeBuffer(pBuffer);
}

return foundCng == foundKeystore == true;
}

```

```
// Generate an asymmetric key pair. As used here, this example generates an RSA key
pair
// and returns a handle. The handle is used in subsequent operations that use the key
pair.
// The key material is not available.
//
// The key pair is used in the SignData function.
//
NTSTATUS GenerateKeyPair(BCRYPT_ALG_HANDLE hAlgorithm, BCRYPT_KEY_HANDLE *hKey)
{
 NTSTATUS status;

 // Generate the key pair.
 status = BCryptGenerateKeyPair(hAlgorithm, hKey, 2048, 0);
 if (!NT_SUCCESS(status))
 {
 printf("BCryptGenerateKeyPair failed with code 0x%08x\n", status);
 return status;
 }

 // Finalize the key pair. The public/private key pair cannot be used until this
 // function is called.
 status = BCryptFinalizeKeyPair(*hKey, 0);
 if (!NT_SUCCESS(status))
 {
 printf("BCryptFinalizeKeyPair failed with code 0x%08x\n", status);
 return status;
 }

 return status;
}

// Sign and verify data using the RSA key pair. The data in this function is hardcoded
// and is for example purposes only.
//
NTSTATUS SignData(BCRYPT_KEY_HANDLE hKey)
{
 NTSTATUS status;
 PBYTE sig;
 ULONG sigLen;
 ULONG resLen;
 BCRYPT_PKCS1_PADDING_INFO pInfo;

 // Hardcode the data to be signed (for demonstration purposes only).
```

```
PBYTE message = (PBYTE)"d83e7716bed8a20343d8dc6845e57447";
ULONG messageLen = strlen((char*)message);

// Retrieve the size of the buffer needed for the signature.
status = BCryptSignHash(hKey, NULL, message, messageLen, NULL, 0, &sigLen, 0);
if (!NT_SUCCESS(status))
{
 printf("BCryptSignHash failed with code 0x%08x\n", status);
 return status;
}

// Allocate a buffer for the signature.
sig = (PBYTE)HeapAlloc(GetProcessHeap(), 0, sigLen);
if (sig == NULL)
{
 return -1;
}

// Use the SHA256 algorithm to create padding information.
pInfo.pszAlgId = BCRYPT_SHA256_ALGORITHM;

// Create a signature.
status = BCryptSignHash(hKey, &pInfo, message, messageLen, sig, sigLen, &resLen,
BCRYPT_PAD_PKCS1);
if (!NT_SUCCESS(status))
{
 printf("BCryptSignHash failed with code 0x%08x\n", status);
 return status;
}

// Verify the signature.
status = BCryptVerifySignature(hKey, &pInfo, message, messageLen, sig, sigLen,
BCRYPT_PAD_PKCS1);
if (!NT_SUCCESS(status))
{
 printf("BCryptVerifySignature failed with code 0x%08x\n", status);
 return status;
}

// Free the memory allocated for the signature.
if (sig != NULL)
{
 HeapFree(GetProcessHeap(), 0, sig);
 sig = NULL;
}
```

```
}

return 0;
}

// Main function.
//
int main()
{
 NTSTATUS status;
 BCrypt_ALG_HANDLE hRsaAlg;
 BCrypt_KEY_HANDLE hKey = NULL;

 // Enumerate the registered providers.
 printf("Searching for Cavium providers...\n");
 if (VerifyProvider() == false) {
 printf("Could not find the CNG and Keystore providers\n");
 return 1;
 }

 // Get the RSA algorithm provider from the Cavium CNG provider.
 printf("Opening RSA algorithm\n");
 status = BCryptOpenAlgorithmProvider(&hRsaAlg, BCRYPT_RSA_ALGORITHM,
 CAVIUM_CNG_PROVIDER, 0);
 if (!NT_SUCCESS(status))
 {
 printf("BCryptOpenAlgorithmProvider RSA failed with code 0x%08x\n", status);
 return status;
 }

 // Generate an asymmetric key pair using the RSA algorithm.
 printf("Generating RSA Keypair\n");
 GenerateKeyPair(hRsaAlg, &hKey);
 if (hKey == NULL)
 {
 printf("Invalid key handle returned\n");
 return 0;
 }
 printf("Done!\n");

 // Sign and verify [hardcoded] data using the RSA key pair.
 printf("Sign/Verify data with key\n");
 SignData(hKey);
 printf("Done!\n");
}
```

```
// Remove the key handle from memory.
status = BCryptDestroyKey(hKey);
if (!NT_SUCCESS(status))
{
 printf("BCryptDestroyKey failed with code 0x%08x\n", status);
 return status;
}

// Close the RSA algorithm provider.
status = BCryptCloseAlgorithmProvider(hRsaAlg, NULL);
if (!NT_SUCCESS(status))
{
 printf("BCryptCloseAlgorithmProvider RSA failed with code 0x%08x\n", status);
 return status;
}

return 0;
}
```

# 整合第三方應用程式與 AWS CloudHSM

的一些[使用案例](#) AWS CloudHSM 涉及將第三方軟體應用程式與 AWS CloudHSM 叢集中的 HSM 整合。透過將第三方軟體與 整合 AWS CloudHSM，您可以實現各種與安全相關的目標。下列主題說明如何達成其中一些目標。

## 主題

- [在 中使用 SSL/TLS 卸載來改善您的 Web 伺服器安全性 AWS CloudHSM](#)
- [使用 AWS CloudHSM將 Windows Server 設定為憑證授權單位 \(CA\)](#)
- [Oracle 資料庫的透明資料加密 \(TDE\) 搭配 AWS CloudHSM](#)
- [搭配 使用 Microsoft SignTool AWS CloudHSM 來簽署檔案](#)
- [Java Keytool 和 Jarsigner 與 整合 AWS CloudHSM](#)
- [搭配 使用 Microsoft 資訊清單產生和編輯工具 \(Mage.exe\) AWS CloudHSM 來簽署檔案](#)
- [其他第三方廠商與 的整合 AWS CloudHSM](#)

## 在 中使用 SSL/TLS 卸載來改善您的 Web 伺服器安全性 AWS CloudHSM

Web 伺服器及其用戶端 (Web 瀏覽器) 可以使用 Secure Sockets Layer (SSL) 或 Transport Layer Security (TLS) 協議確認 Web 伺服器的身分，並建立通過 Internet 發送和接收網頁或其他數據的安全連接。這通常被稱為 HTTPS。Web 伺服器會使用公開-私有金鑰對以及 SSL/TLS 公開金鑰憑證，來和每個用戶端建立 HTTPS 工作階段。此程序涉及許多 Web 伺服器的運算，但您可以將其中一些卸載至 AWS CloudHSM 叢集，這稱為 SSL 加速。卸載可減少 Web 伺服器的計算負載，並藉由將伺服器的私有金鑰儲存在 HSM 中，提供額外的安全性。

下列主題提供 SSL/TLS 卸載搭配 AWS CloudHSM 運作方式的概觀，以及在 AWS CloudHSM 下列平台上使用 設定 SSL/TLS 卸載的教學課程。

對於 Linux，請在 [NGINX](#) 或 [Apache HTTP 伺服器](#) Web 伺服器軟件上使用 OpenSSL 動態引擎

對於 Windows，使用 [Internet Information Services \(IIS\) for Windows Server](#) Web 伺服器軟體。

## 主題

- [搭配的 SSL/TLS 卸載 AWS CloudHSM 運作方式](#)
- [AWS CloudHSM 使用 NGINX 或 Apache 搭配 OpenSSL 在 Linux 上卸載 SSL/TLS](#)

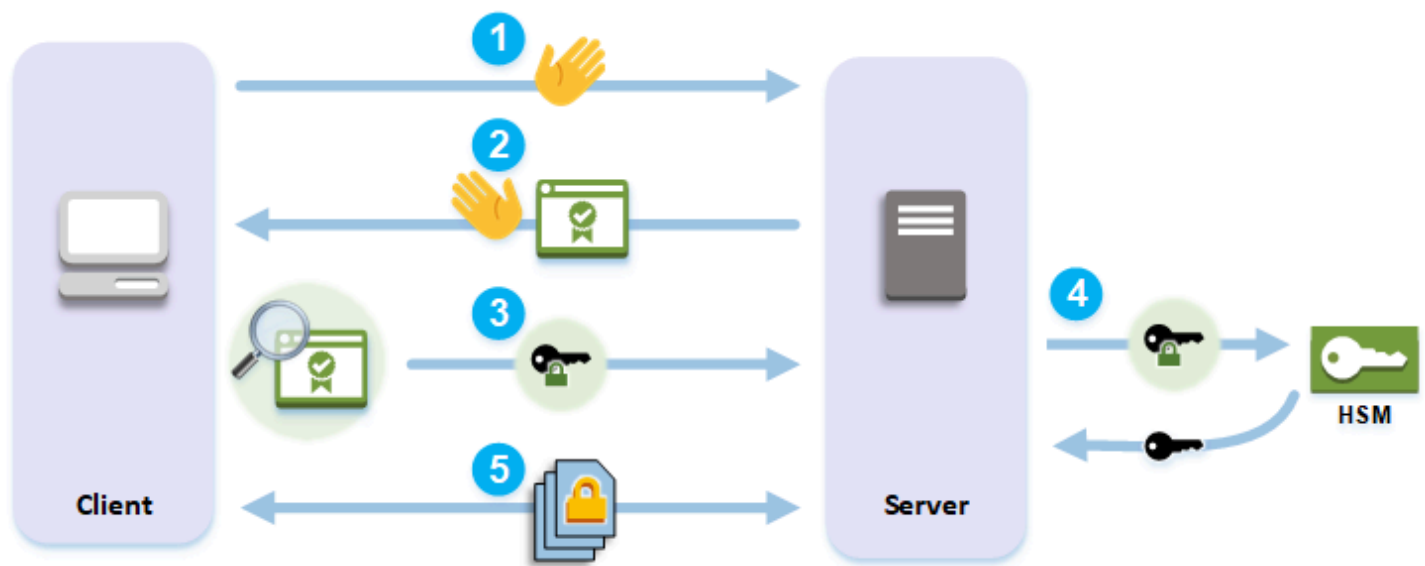
- [AWS CloudHSM 使用 Tomcat 搭配 JSSE 在 Linux 上卸載 SSL/TLS](#)
- [AWS CloudHSM 在 Windows 上使用 IIS 搭配 KSP 的 SSL/TLS 卸載](#)
- [使用 Elastic Load Balancing for 新增負載平衡器 AWS CloudHSM \(選用\)](#)

## 搭配的 SSL/TLS 卸載 AWS CloudHSM 運作方式

為了建立 HTTPS 連線，您的 Web 伺服器會與用戶端進行交握程序。在此程序中，伺服器會將部分密碼編譯處理卸載至 AWS CloudHSM 叢集中的 HSMs，如下圖所示。圖片下方有每個處理步驟的說明。

### Note

以下圖片和程序假設伺服器驗證和金鑰交換使用 RSA。使用 Diffie–Hellman 代替 RSA 時，程序略有不同。



1. 用戶端傳送 hello 訊息到伺服器。
2. 伺服器回應 hello 訊息並傳送伺服器的憑證。
3. 用戶端執行下列動作：
  - a. 確認 SSL/TLS 伺服器憑證是由客戶端信任的根憑證簽署。
  - b. 從伺服器憑證擷取公開金鑰。
  - c. 產生前置主機秘密，並使用伺服器的公有金鑰對其進行加密。
  - d. 將加密的前置主機秘密傳送至伺服器。

4. 若要解密用戶端的前置主機秘密，伺服器會將其傳送至 HSM。HSM 使用 HSM 中的私有金鑰來解密主機前秘密，然後將主機前秘密傳送至伺服器。用戶端和伺服器各自獨立地使用前置主機秘密和來自 hello 訊息的一些資訊來計算主要秘密。
5. 交握程序結束。在剩下來的工作階段中，在用戶端和伺服器之間傳送的所有訊息都會使用主要秘密的衍生產品加密。

若要了解如何使用 設定 SSL/TLS 卸載 AWS CloudHSM，請參閱下列其中一個主題：

- [AWS CloudHSM 使用 NGINX 或 Apache 搭配 OpenSSL 在 Linux 上卸載 SSL/TLS](#)
- [AWS CloudHSM 使用 Tomcat 搭配 JSSE 在 Linux 上卸載 SSL/TLS](#)
- [AWS CloudHSM 在 Windows 上使用 IIS 搭配 KSP 的 SSL/TLS 卸載](#)

## AWS CloudHSM 使用 NGINX 或 Apache 搭配 OpenSSL 在 Linux 上卸載 SSL/TLS

本主題提供在 Linux Web 伺服器上設定 SSL/TLS 卸載搭配 AWS CloudHSM 的逐步說明。

### 主題

- [概觀](#)
- [步驟 1：設定先決條件](#)
- [步驟 2：產生私有金鑰和 SSL/TLS 憑證](#)
- [步驟 3：設定 Web 伺服器](#)
- [步驟 4：啟用 HTTPS 流量並驗證憑證](#)

### 概觀

在 Linux 上，[NGINX](#) 和 [Apache HTTP Server](#) Web 伺服器軟體與 [OpenSSL](#) 整合以支援 HTTPS。[適用於 OpenSSL 之 AWS CloudHSM 動態引擎](#)提供的界面，可讓 Web 伺服器軟體使用叢集中的 HSM 進行密碼編譯卸載和金鑰儲存。OpenSSL 引擎是將 Web 伺服器連線到 AWS CloudHSM 叢集的橋樑。

若要完成此教學課程，您必須先選擇是否要在 Linux 上使用 NGINX 或 Apache Web 伺服器軟體。然後，教學課程會向您示範如何執行以下操作：

- 在 Amazon EC2 執行個體上安裝 Web 伺服器軟體。
- 將 Web 伺服器軟體設定為使用儲存在 AWS CloudHSM 叢集中的私有金鑰來支援 HTTPS。



- (選用) 使用 Amazon EC2 建立第二個 Web 伺服器執行個體，並使用 Elastic Load Balancing 建立負載平衡器。使用負載平衡器可將負載分散到多部伺服器，進而提升效能。它也可以在一或多個伺服器失敗時提供備援和高可用性。

當您準備好開始時，請移至[步驟 1：設定先決條件](#)。

## 步驟 1：設定先決條件

不同平台需要不同的先決條件。請使用下方符合您平台的先決條件區段。

### 用戶端 SDK 5 的先決條件

若要設定 Web 伺服器 SSL/TLS 卸載搭配 Client SDK 5，您需要下列項目：

- 具有至少兩個硬體安全模組 (HSM) 的作用中 AWS CloudHSM 叢集

#### Note

您可以使用單一 HSM 叢集，但必須先停用用戶端金鑰持久性。如需詳細資訊，請參閱[管理用戶端金鑰持久性設定](#)和[用戶端 SDK 5 設定工具](#)。

- 執行 Linux 作業系統的 Amazon EC2 執行個體，其中已安裝下列軟體：
  - 一個 Web 伺服器 (無論是 NGINX 或 Apache)
  - 適用於用戶端 SDK 5 的 OpenSSL 動態引擎
- [加密使用者](#) (CU)，擁有及管理 HSM 上 Web 伺服器的私有金鑰。

設定 Linux Web 伺服器執行個體，並在 HSM 上建立 CU

1. 安裝和設定的 OpenSSL 動態引擎 AWS CloudHSM。如需關於安裝 OpenSSL 動態引擎的詳細資訊，請參閱[用戶端 SDK 5 的 OpenSSL 動態引擎](#)。
2. 在可存取叢集的 EC2 Linux 執行個體上，安裝 NGINX 或 Apache Web 伺服器：

#### Amazon Linux

- NGINX

```
$ sudo yum install nginx
```

- Apache

```
$ sudo yum install httpd24 mod24_ssl
```

## Amazon Linux 2

- 如需如何在 Amazon Linux 2 上下載最新版本的 NGINX 的資訊，請參閱 [NGINX 網站](#)。

可用於 Amazon Linux 2 的最新版本 NGINX 使用的 OpenSSL 版本比系統版本的 OpenSSL 更新。安裝 NGINX 之後，您需要從 AWS CloudHSM OpenSSL 動態引擎程式庫建立符號連結，以連結到此版本的 OpenSSL 預期的位置

```
$ sudo ln -sf /opt/cloudhsm/lib/libcloudhsm_openssl_engine.so /usr/lib64/engines-1.1/cloudhsm.so
```

- Apache

```
$ sudo yum install httpd mod_ssl
```

## Amazon Linux 2023

- NGINX

```
$ sudo yum install nginx
```

- Apache

```
$ sudo yum install httpd mod_ssl
```

## CentOS 7

- 如需如何在 CentOS 7 上下載最新版本的 NGINX 的資訊，請參閱 [NGINX 網站](#)。

可用於 CentOS 7 的最新版本 NGINX 使用的 OpenSSL 版本比系統版本 OpenSSL 更新。安裝 NGINX 之後，您需要從 AWS CloudHSM OpenSSL 動態引擎程式庫建立符號連結，以連結到此版本的 OpenSSL 預期的位置

```
$ sudo ln -sf /opt/cloudhsm/lib/libcloudhsm_openssl_engine.so /usr/lib64/engines-1.1/cloudhsm.so
```

- Apache

```
$ sudo yum install httpd mod_ssl
```

## Red Hat 7

- 如需如何在 Red Hat 7 上下載最新版本的 NGINX 的資訊，請參閱 [NGINX 網站](#)。

可用於 Red Hat 7 的最新版本 NGINX 使用的 OpenSSL 版本比系統版本的 OpenSSL 更新。安裝 NGINX 之後，您需要從 AWS CloudHSM OpenSSL 動態引擎程式庫建立符號連結，以連結到此版本的 OpenSSL 預期的位置

```
$ sudo ln -sf /opt/cloudhsm/lib/libcloudhsm_openssl_engine.so /usr/lib64/engines-1.1/cloudhsm.so
```

- Apache

```
$ sudo yum install httpd mod_ssl
```

## CentOS 8

- NGINX

```
$ sudo yum install nginx
```

- Apache

```
$ sudo yum install httpd mod_ssl
```

## Red Hat 8

- NGINX

```
$ sudo yum install nginx
```

- Apache

```
$ sudo yum install httpd mod_ssl
```

## Ubuntu 18.04

- NGINX

```
$ sudo apt install nginx
```

- Apache

```
$ sudo apt install apache2
```

## Ubuntu 20.04

- NGINX

```
$ sudo apt install nginx
```

- Apache

```
$ sudo apt install apache2
```

## Ubuntu 22.04

- NGINX

```
$ sudo apt install nginx
```

- Apache

```
$ sudo apt install apache2
```

## Ubuntu 24.04

- NGINX

```
$ sudo apt install nginx
```

- Apache

```
$ sudo apt install apache2
```

3. 使用 CloudHSM CLI 建立[加密使用者](#)。如需關於管理 HSM 使用者的詳細資訊，請參閱[使用 CloudHSM CLI 管理 HSM 使用者](#)。

### Tip

保持追蹤 CU 使用者名稱和密碼。之後在為您的 Web 伺服器產生或匯入 HTTPS 私有金鑰和憑證時，您將會需要該資訊。

完成這些步驟之後，請移至 [步驟 2：產生私有金鑰和 SSL/TLS 憑證](#)。

### 備註

- 若要使用 Security-Enhanced Linux (SELinux) 和 Web 伺服器，您必須在連接埠 2223 上允許傳出 TCP 連線，也就是用戶端 SDK 5 用來與 HSM 通訊的連接埠。
- 若要建立和啟用叢集並授予 EC2 執行個體存取叢集的權限，請完成[AWS CloudHSM入門](#)中的步驟。入門提供使用 HSM 和 Amazon EC2 用戶端執行個體建立作用中叢集的逐步說明。可以使用此用戶端執行個體做為 Web 伺服器。
- 若要避免停用用戶端金鑰耐久性，請在叢集中新增多個 HSM。如需詳細資訊，請參閱[將 HSM 新增至 AWS CloudHSM 叢集](#)。
- 要連接到用戶端執行個體，可以使用 SSH 或 PuTTY。如需詳細資訊，請參閱 Amazon EC2 文件中的[使用 SSH 連接至您的 Linux 執行個體](#)或[使用 PuTTY 從 Windows 連接至您的 Linux 執行個體](#)。

## 步驟 2：產生私有金鑰和 SSL/TLS 憑證

若要啟用 HTTPS，您的 Web 伺服器應用程式 (NGINX 或 Apache) 需要私有金鑰和對應的 SSL/TLS 憑證。若要搭配使用 Web 伺服器 SSL/TLS 卸載 AWS CloudHSM，您必須將私有金鑰存放在 AWS

CloudHSM 叢集的 HSM 中。您會先產生私有金鑰，並使用金鑰來建立憑證簽署請求 (CSR)。然後，您從 HSM 匯出仿造 PEM 私有金鑰，這是 PEM 格式的私有金鑰檔案，其中包含 HSM 上存放之私有金鑰的參考（這不是實際的私有金鑰）。在 SSL/TLS 卸載期間，Web 伺服器會使用仿造的 PEM 私有金鑰檔案識別 HSM 上的私有金鑰。

## 產生私有金鑰和憑證

### 產生私有金鑰

本節說明如何使用 [CloudHSM CLI](#) 產生金鑰對。在 HSM 內產生金鑰對後，您可以將它匯出為仿造 PEM 檔案，並產生對應的憑證。

### 安裝和設定 CloudHSM CLI

1. [安裝和設定](#) CloudHSM CLI。
2. 使用下列命令來啟動 CloudHSM CLI。

```
$ /opt/cloudhsm/bin/cloudhsm-cli interactive
```

3. 執行以下命令來登入 HSM。將 *<user name>* 取代為您的 crypto-user 的使用者名稱

```
Command: login --username <user name> --role crypto-user
```

### 產生私有金鑰

根據您的使用案例，您可以產生 RSA 或 EC 金鑰對。執行以下任意一項：

- 在 HSM 上產生 RSA 私有金鑰

使用 [key generate-asymmetric-pair rsa](#) 命令來產生 RSA 金鑰對。此範例會產生一個 RSA 金鑰對，其模數為 2048、公有指數為 65537、公有金鑰標籤為 *tls\_rsa\_pub*，以及私有金鑰標籤為 *tls\_rsa\_private*。

```
aws-cloudhsm > key generate-asymmetric-pair rsa \
--public-exponent 65537 \
--modulus-size-bits 2048 \
--public-label tls_rsa_pub \
--private-label tls_rsa_private \
--private-attributes sign=true \
{
 "error_code": 0,
```

```

"data": {
 "public_key": {
 "key-reference": "0x00000000000280cc8",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "rsa",
 "label": "tls_rsa_pub",
 "id": "",
 "check-value": "0x01fe6e",
 "class": "public-key",
 "encrypt": true,
 "decrypt": false,
 "token": true,
 "always-sensitive": false,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 512,
 "public-exponent": "0x010001",
 "modulus":
 "0xb1d27e857a876f4e9fd5de748a763c539b359f937eb4b4260e30d1435485a732c878cdad9c72538e2215351b1
 73a80fdb457aa7b20cd61e486c326e2cfd5e124a7f6a996437437812b542e3caf85928aa866f0298580f7967ee6aa
 f6e6296d6c116d5744c6d60d14d3bf3cb978fe6b75ac67b7089bafd50d8687213b31abc7dc1bad422780d29c851d5
 133022653225bd129f8491101725e9ea33e1ded83fb57af35f847e532eb30cd7e726f23910d2671c6364092e83469

```

```

ac3160f0ca9725d38318b7",
 "modulus-size-bits": 2048
 }
},
"private_key": {
 "key-reference": "0x0000000000280cc7",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "rsa",
 "label": "tls_rsa_private",
 "id": "",
 "check-value": "0x01fe6e",
 "class": "private-key",
 "encrypt": false,
 "decrypt": true,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 1217,
 "public-exponent": "0x010001",
 "modulus":
 "0xb1d27e857a876f4e9fd5de748a763c539b359f937eb4b4260e30d1435485a732c878cdad9c72538e2215351b1

```



```

 "modulus-size-bits": 2048
 }
}
}
}

```

- 在 HSM 上產生 EC 私有金鑰

使用 [key generate-asymmetric-pair ec](#) 命令來產生 EC 金鑰對。此範例會產生具有 prime256v1 曲線（對應至 NID\_X9\_62\_prime256v1 曲線）的 EC 金鑰對、*tls\_ec\_pub* 的公有金鑰標籤，以及 *tls\_ec\_private* 的私有金鑰標籤。

```

aws-cloudhsm > key generate-asymmetric-pair ec \
 --curve prime256v1 \
 --public-label tls_ec_pub \
 --private-label tls_ec_private
 --private-attributes sign=true
{
 "error_code": 0,
 "data": {
 "public_key": {
 "key-reference": "0x0000000000012000b",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "cluster-coverage": "session"
 },
 "attributes": {
 "key-type": "ec",
 "label": "tls_ec_pub",
 "id": "",
 "check-value": "0xd7c1a7",
 "class": "public-key",
 "encrypt": false,
 "decrypt": false,
 "token": false,
 "always-sensitive": false,
 "derive": false,

```

```

 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": false,
 "sign": false,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 57,
 "ec-point":
"0x047096513df542250a6b228fd9cb67fd0c903abc93488467681974d6f371083fce1d79da8ad1e9ede745fb9f3
 "curve": "secp224r1"
 }
},
"private_key": {
 "key-reference": "0x0000000000012000c",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "cluster-coverage": "session"
 },
 "attributes": {
 "key-type": "ec",
 "label": "tls_ec_private",
 "id": "",
 "check-value": "0xd7c1a7",
 "class": "private-key",
 "encrypt": false,
 "decrypt": false,
 "token": false,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,

```

```

 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": true,
 "trusted": false,
 "unwrap": false,
 "verify": false,
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 122,
 "ec-point":
 "0x047096513df542250a6b228fd9cb67fd0c903abc93488467681974d6f371083fce1d79da8ad1e9ede745fb9f3
 "curve": "secp224r1"
 }
}
}
}

```

## 匯出仿造的 PEM 私有金鑰檔案

HSM 上擁有私有金鑰後，您必須匯出仿造的 PEM 私有金鑰檔案。此檔案不包含實際的金鑰資料，但可讓 OpenSSL 動態引擎識別 HSM 上的私有金鑰。接著，您可以使用私有金鑰來建立憑證簽署要求 (CSR)，簽署 CSR 來建立憑證。

使用 [key generate-file](#) 命令以仿造 PEM 格式匯出私有金鑰，並將其儲存至 檔案。以您自己的值取代下列值。

- `<private_key_label>` – 您在上一個步驟中產生的私有金鑰標籤。
- `<web_server_fake_pem.key>` – 要寫入仿造 PEM 金鑰的檔案名稱。

```

aws-cloudhsm > key generate-file --encoding reference-pem --
path <web_server_fake_pem.key> --filter attr.label=<private_key_label>
{
 "error_code": 0,
 "data": {
 "message": "Successfully generated key file"
 }
}

```

## 結束 CloudHSM CLI

執行下列命令來停止 CloudHSM CLI。

```
aws-cloudhsm > quit
```

您現在應該在系統上有一個新檔案，位於上述命令中 `<web_server_fake_pem.key>` 指定的路徑。此檔案是仿造的 PEM 私有金鑰檔案。

### 產生自簽憑證

產生仿造的 PEM 私有金鑰後，您可以使用此檔案來產生憑證簽署要求 (CSR) 和憑證。

在生產環境中，您通常會使用憑證授權單位 (CA) 從 CSR 建立憑證。測試環境不需要 CA。如果您確實使用 CA，請將 CSR 檔案發送給他們，並使用他們在 Web 伺服器中為您提供 HTTPS 的簽名 SSL/TLS 憑證。

除了使用 CA 之外，您也可以使用 AWS CloudHSM OpenSSL 動態引擎來建立自我簽署憑證。自簽憑證不受瀏覽器所信任，請勿用於生產環境。可以用於測試環境。

#### Warning

自簽憑證應該只用於測試環境。若為生產環境，請使用更安全的方法 (例如憑證授權單位) 來建立憑證。

### 安裝和設定 OpenSSL 動態引擎

1. 連接至您的用戶端執行個體。
2. [the section called “安裝”](#)

### 產生憑證

1. 取得先前步驟中產生的仿造的 PEM 檔案副本。
2. 建立 CSR

執行下列命令，使用 AWS CloudHSM OpenSSL 動態引擎來建立憑證簽署請求 (CSR)。以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_fake_pem.key>` 以包含 CSR 的檔案名稱取代 `<web_server.csr>`。

req 是互動式命令。回應每個欄位。欄位資訊會複製到您的 SSL/TLS 憑證。

```
$ openssl req -engine cloudhsm -new -key <web_server_fake_pem.key> -
out <web_server.csr>
```

### 3. 建立自簽憑證

執行下列命令，以使用 AWS CloudHSM OpenSSL 動態引擎在 HSM 上使用私有金鑰簽署 CSR。這會建立自簽憑證。在命令中，以您自己的值取代下列值。

- *<web\_server.csr>*：包含 CSR 的檔案名稱。
- *<web\_server\_fake\_pem.key>* – 包含仿造 PEM 私有金鑰的檔案名稱。
- *<web\_server.crt>*：包含 Web 伺服器憑證的檔案名稱。

```
$ openssl x509 -engine cloudhsm -req -days 365 -in <web_server.csr> -
signkey <web_server_fake_pem.key> -out <web_server.crt>
```

完成這些步驟之後，請移至 [步驟 3：設定 Web 伺服器](#)。

## 步驟 3：設定 Web 伺服器

更新 Web 伺服器軟體組態，以使用 HTTPS 憑證以及您在 [上一個步驟](#) 中建立的對應仿造 PEM 私有金鑰。請記得在開始之前備份現有的憑證和金鑰。這將完成針對 SSL/TLS 卸載搭配 AWS CloudHSM 設定您的 Linux Web 伺服器軟體。

完成以下其中一個區段中的步驟。

### 主題

- [設定 NGINX Web 伺服器](#)
- [設定 Apache Web 伺服器](#)

### 設定 NGINX Web 伺服器

使用此區段可在支援的平台上設定 NGINX。

## 更新 NGINX 的 Web 伺服器組態

1. 連接至您的用戶端執行個體。
2. 執行以下命令，為 Web 伺服器憑證和仿造 PEM 私有金鑰建立所需的目錄。

```
$ sudo mkdir -p /etc/pki/nginx/private
```

3. 執行以下命令，將您的 Web 伺服器憑證複製到所需的位置。以 Web 伺服器憑證的名稱取代 `<web_server.crt>`。

```
$ sudo cp <web_server.crt> /etc/pki/nginx/server.crt
```

4. 執行以下命令，將您的仿造 PEM 私有金鑰複製到所需的位置。以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_fake_pem.key>`。

```
$ sudo cp <web_server_example_pem.key> /etc/pki/nginx/private/server.key
```

5. 執行以下命令來變更檔案的擁有權，使得名為 nginx 的使用者可讀取這些檔案。

```
$ sudo chown nginx /etc/pki/nginx/server.crt /etc/pki/nginx/private/server.key
```

6. 執行以下命令來備份 `/etc/nginx/nginx.conf` 檔案。

```
$ sudo cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.backup
```

7. 更新 NGINX 組態。

### Note

每個叢集可以在所有 NGINX Web 伺服器上支持最多 1000 個 NGINX 工作者程序。

## Amazon Linux

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

然後將以下內容新增至檔案的 TLS 區段：

```
Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is *strongly* recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem 2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2;
 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-
RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-
RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;

 # Load configuration files for the default server block.
 include /etc/nginx/default.d/*.conf;

 location / {
 }

 error_page 404 /404.html;
 location = /40x.html {
 }

 error_page 500 502 503 504 /50x.html;
 location = /50x.html {
 }
}
```

## Amazon Linux 2

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

然後將以下內容新增至檔案的 TLS 區段：

```
Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is strongly recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem 2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2;
 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-
RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-
RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;

 # Load configuration files for the default server block.
 include /etc/nginx/default.d/*.conf;

 location / {

 }

 error_page 404 /404.html;
 location = /40x.html {
 }
}
```



```
error_page 500 502 503 504 /50x.html;
location = /50x.html {
}
}
```

## Amazon Linux 2023

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

然後將以下內容新增至檔案的 TLS 區段：

```
Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is *strongly* recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem 2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2;
 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;

 # Load configuration files for the default server block.
 include /etc/nginx/default.d/*.conf;
```

```
location / {
}

error_page 404 /404.html;
location = /40x.html {
}

error_page 500 502 503 504 /50x.html;
location = /50x.html {
}
}
```

## CentOS 7

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

然後將以下內容新增至檔案的 TLS 區段：

```
Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is *strongly* recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem 2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2;
 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-
```

```

SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;

 # Load configuration files for the default server block.
 include /etc/nginx/default.d/*.conf;

 location / {

 }

 error_page 404 /404.html;
 location = /40x.html {
 }

 error_page 500 502 503 504 /50x.html;
 location = /50x.html {
 }
}

```

## CentOS 8

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```

ssl_engine cloudhsm;
env CLOUDHSM_PIN;

```

然後將以下內容新增至檔案的 TLS 區段：

```

Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is *strongly* recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem 2048

```

```
#ssl_dhparam "/etc/pki/nginx/dhparams.pem";
ssl_session_cache shared:SSL:1m;
ssl_session_timeout 10m;
ssl_protocols TLSv1.2 TLSv1.3;
ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-
RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-
RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
ssl_prefer_server_ciphers on;

Load configuration files for the default server block.
include /etc/nginx/default.d/*.conf;

location / {

error_page 404 /404.html;
location = /40x.html {

error_page 500 502 503 504 /50x.html;
location = /50x.html {

}
}
```

## Red Hat 7

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

然後將以下內容新增至檔案的 TLS 區段：

```
Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
```

```

server_name _;
root /usr/share/nginx/html;

ssl_certificate "/etc/pki/nginx/server.crt";
ssl_certificate_key "/etc/pki/nginx/private/server.key";
It is strongly recommended to generate unique DH parameters
Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem 2048
#ssl_dhparam "/etc/pki/nginx/dhparams.pem";
ssl_session_cache shared:SSL:1m;
ssl_session_timeout 10m;
ssl_protocols TLSv1.2;
ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
ssl_prefer_server_ciphers on;

Load configuration files for the default server block.
include /etc/nginx/default.d/*.conf;

location / {

}

error_page 404 /404.html;
location = /40x.html {
}

error_page 500 502 503 504 /50x.html;
location = /50x.html {
}
}

```

## Red Hat 8

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```

ssl_engine cloudhsm;
env CLOUDHSM_PIN;

```

然後將以下內容新增至檔案的 TLS 區段：

```
Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is *strongly* recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem 2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2 TLSv1.3;
 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-
RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-
RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;

 # Load configuration files for the default server block.
 include /etc/nginx/default.d/*.conf;

 location / {
 }

 error_page 404 /404.html;
 location = /40x.html {
 }

 error_page 500 502 503 504 /50x.html;
 location = /50x.html {
 }
}
```

## Ubuntu 16.04 LTS

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```
ssl_engine cloudhsm;
 env n3fips_password;
```

然後將以下內容新增至檔案的 TLS 區段：

```
Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is strongly recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem
2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2;
 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;

 # Load configuration files for the default server block.
 include /etc/nginx/default.d/*.conf;

 location / {

 }

 error_page 404 /404.html;
 location = /40x.html {
```

```

 }

 error_page 500 502 503 504 /50x.html;
 location = /50x.html {
 }
}

```

## Ubuntu 18.04 LTS

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```

ssl_engine cloudhsm;
env CLOUDHSM_PIN;

```

然後將以下內容新增至檔案的 TLS 區段：

```

Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is *strongly* recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem
2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2 TLSv1.3;
 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;
}

```



```
Load configuration files for the default server block.
include /etc/nginx/default.d/*.conf;

location / {

}

error_page 404 /404.html;
location = /40x.html {
}

error_page 500 502 503 504 /50x.html;
location = /50x.html {
}
}
```

## Ubuntu 20.04 LTS

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

然後將以下內容新增至檔案的 TLS 區段：

```
Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is *strongly* recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem
2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2 TLSv1.3;
```

```

 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;

 # Load configuration files for the default server block.
 include /etc/nginx/default.d/*.conf;

 location / {

 }

 error_page 404 /404.html;
 location = /40x.html {
 }

 error_page 500 502 503 504 /50x.html;
 location = /50x.html {
 }
}

```

## Ubuntu 22.04 LTS

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```

ssl_engine cloudhsm;
env CLOUDHSM_PIN;

```

然後將以下內容新增至檔案的 TLS 區段：

```

Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";

```

```

 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is strongly recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem
2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2 TLSv1.3;
 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-
SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-
RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-
GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;

 # Load configuration files for the default server block.
 include /etc/nginx/default.d/*.conf;

 location / {

 }

 error_page 404 /404.html;
 location = /40x.html {
 }

 error_page 500 502 503 504 /50x.html;
 location = /50x.html {
 }
}

```

## Ubuntu 24.04 LTS

使用文字編輯器來編輯 `/etc/nginx/nginx.conf` 檔案。這需要 Linux 根許可。在檔案上方，新增下列行：

```

ssl_engine cloudhsm;
env CLOUDHSM_PIN;

```

然後將以下內容新增至檔案的 TLS 區段：

```
Settings for a TLS enabled server.
server {
 listen 443 ssl http2 default_server;
 listen [::]:443 ssl http2 default_server;
 server_name _;
 root /usr/share/nginx/html;

 ssl_certificate "/etc/pki/nginx/server.crt";
 ssl_certificate_key "/etc/pki/nginx/private/server.key";
 # It is strongly recommended to generate unique DH parameters
 # Generate them with: openssl dhparam -out /etc/pki/nginx/dhparams.pem
2048
 #ssl_dhparam "/etc/pki/nginx/dhparams.pem";
 ssl_session_cache shared:SSL:1m;
 ssl_session_timeout 10m;
 ssl_protocols TLSv1.2 TLSv1.3;
 ssl_ciphers "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA";
 ssl_prefer_server_ciphers on;

 # Load configuration files for the default server block.
 include /etc/nginx/default.d/*.conf;

 location / {
 }

 error_page 404 /404.html;
 location = /40x.html {
 }

 error_page 500 502 503 504 /50x.html;
 location = /50x.html {
 }
}
```

儲存檔案。

## 8. 備份 systemd 組態檔案，然後設定 EnvironmentFile 路徑。

### Amazon Linux

不需要採取行動。

### Amazon Linux 2

1. 備份 nginx.service 檔案。

```
$ sudo cp /lib/systemd/system/nginx.service /lib/systemd/system/
nginx.service.backup
```

2. 在文字編輯器中開啟 /lib/systemd/system/nginx.service 檔案，然後在 [Service] (服務) 區段中，新增以下路徑：

```
EnvironmentFile=/etc/sysconfig/nginx
```

### Amazon Linux 2023

1. 備份 nginx.service 檔案。

```
$ sudo cp /lib/systemd/system/nginx.service /lib/systemd/system/
nginx.service.backup
```

2. 在文字編輯器中開啟 /lib/systemd/system/nginx.service。在 【服務】 區段下，新增：

```
EnvironmentFile=/etc/sysconfig/nginx
```

### CentOS 7

不需要採取行動。

### CentOS 8

1. 備份 nginx.service 檔案。

```
$ sudo cp /lib/systemd/system/nginx.service /lib/systemd/system/
nginx.service.backup
```

2. 在文字編輯器中開啟 `/lib/systemd/system/nginx.service` 檔案，然後在 [Service] (服務) 區段中，新增以下路徑：

```
EnvironmentFile=/etc/sysconfig/nginx
```

## Red Hat 7

不需要採取行動。

## Red Hat 8

1. 備份 `nginx.service` 檔案。

```
$ sudo cp /lib/systemd/system/nginx.service /lib/systemd/system/
nginx.service.backup
```

2. 在文字編輯器中開啟 `/lib/systemd/system/nginx.service` 檔案，然後在 [Service] (服務) 區段中，新增以下路徑：

```
EnvironmentFile=/etc/sysconfig/nginx
```

## Ubuntu 16.04

1. 備份 `nginx.service` 檔案。

```
$ sudo cp /lib/systemd/system/nginx.service /lib/systemd/system/
nginx.service.backup
```

2. 在文字編輯器中開啟 `/lib/systemd/system/nginx.service` 檔案，然後在 [Service] (服務) 區段中，新增以下路徑：

```
EnvironmentFile=/etc/sysconfig/nginx
```

## Ubuntu 18.04

1. 備份 `nginx.service` 檔案。

```
$ sudo cp /lib/systemd/system/nginx.service /lib/systemd/system/
nginx.service.backup
```

2. 在文字編輯器中開啟 `/lib/systemd/system/nginx.service` 檔案，然後在 [Service] (服務) 區段中，新增以下路徑：

```
EnvironmentFile=/etc/sysconfig/nginx
```

## Ubuntu 20.04 LTS

1. 備份 `nginx.service` 檔案。

```
$ sudo cp /lib/systemd/system/nginx.service /lib/systemd/system/
nginx.service.backup
```

2. 在文字編輯器中開啟 `/lib/systemd/system/nginx.service` 檔案，然後在 [Service] (服務) 區段中，新增以下路徑：

```
EnvironmentFile=/etc/sysconfig/nginx
```

## Ubuntu 22.04 LTS

1. 備份 `nginx.service` 檔案。

```
$ sudo cp /lib/systemd/system/nginx.service /lib/systemd/system/
nginx.service.backup
```

2. 在文字編輯器中開啟 `/lib/systemd/system/nginx.service` 檔案，然後在 [Service] (服務) 區段中，新增以下路徑：

```
EnvironmentFile=/etc/sysconfig/nginx
```

## Ubuntu 24.04 LTS

1. 備份 `nginx.service` 檔案。

```
$ sudo cp /lib/systemd/system/nginx.service /lib/systemd/system/nginx.service.backup
```

- 在文字編輯器中開啟 `/lib/systemd/system/nginx.service` 檔案，然後在 [Service] (服務) 區段中，新增以下路徑：

```
EnvironmentFile=/etc/sysconfig/nginx
```

- 檢查 `/etc/sysconfig/nginx` 檔案是否存在，然後執行以下其中一項：

- 如果檔案存在，請執行下列命令來備份檔案：

```
$ sudo cp /etc/sysconfig/nginx /etc/sysconfig/nginx.backup
```

- 如果檔案不存在，請開啟文字編輯器，然後建立在 `/etc/sysconfig/` 資料夾中建立名為 `nginx` 的檔案。

- 設定 NGINX 環境。

#### Note

用戶端 SDK 5 引入了用於存儲 CU 憑證的 `CLOUDHSM_PIN` 環境變量。

## Amazon Linux

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

以 CU 憑證取代 `<CU #####>` 和 `<##>`。

儲存檔案。

## Amazon Linux 2

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：



```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

## Amazon Linux 2023

身為 Linux 根使用者，請在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。例如

```
sudo vi /etc/sysconfig/nginx
```

新增加密使用者 (CU) 憑證：

```
CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

## CentOS 7

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

## CentOS 8

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

## Red Hat 7

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

## Red Hat 8

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

## Ubuntu 16.04 LTS

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
n3fips_password=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

## Ubuntu 18.04 LTS

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
CLLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

#### Ubuntu 20.04 LTS

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
CLLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

#### Ubuntu 22.04 LTS

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
CLLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

#### Ubuntu 24.04 LTS

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
CLLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

儲存檔案。

### 11. 啟動 NGINX 伺服器。

## Amazon Linux

在文字編輯器中開啟 `/etc/sysconfig/nginx` 檔案。這需要 Linux 根許可。新增加密使用者 (CU) 憑證：

```
$ sudo service nginx start
```

## Amazon Linux 2

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

## Amazon Linux 2023

停止所有 NGINX 程序

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX

```
$ sudo systemctl start nginx
```

## CentOS 7

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

## CentOS 8

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

## Red Hat 7

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

## Red Hat 8

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

## Ubuntu 16.04 LTS

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

## Ubuntu 18.04 LTS

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

## Ubuntu 20.04 LTS

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

## Ubuntu 22.04 LTS

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

## Ubuntu 24.04 LTS

停止任何正在運行的 NGINX 進程

```
$ sudo systemctl stop nginx
```

重新載入 systemd 組態以取得最新的變更

```
$ sudo systemctl daemon-reload
```

啟動 NGINX 進程

```
$ sudo systemctl start nginx
```

12. (選用) 將平台設定為在啟動時啟動 NGINX。

Amazon Linux

```
$ sudo chkconfig nginx on
```

Amazon Linux 2

```
$ sudo systemctl enable nginx
```

Amazon Linux 2023

```
$ sudo systemctl enable nginx
```

CentOS 7

不需要採取行動。

CentOS 8

```
$ sudo systemctl enable nginx
```

Red Hat 7

不需要採取行動。

Red Hat 8

```
$ sudo systemctl enable nginx
```



## Ubuntu 16.04 LTS

```
$ sudo systemctl enable nginx
```

## Ubuntu 18.04 LTS

```
$ sudo systemctl enable nginx
```

## Ubuntu 20.04 LTS

```
$ sudo systemctl enable nginx
```

## Ubuntu 22.04 LTS

```
$ sudo systemctl enable nginx
```

## Ubuntu 24.04 LTS

```
$ sudo systemctl enable nginx
```

在更新您的 Web 伺服器組態之後，請移至 [步驟 4：啟用 HTTPS 流量並驗證憑證](#)。

## 設定 Apache Web 伺服器

使用此區段可在支援的平台上設定 Apache。

### 更新 Apache 的 Web 伺服器組態

1. 連線到 Amazon EC2 用戶端執行個體。
2. 為平台定義憑證和私有金鑰的預設位置。

## Amazon Linux

在 `/etc/httpd/conf.d/ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

## Amazon Linux 2

在 `/etc/httpd/conf.d/ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

## Amazon Linux 2023

開啟 `/etc/httpd/conf.d/ssl.conf` 檔案。如果這些值尚未存在，請新增這些值：

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

## CentOS 7

在 `/etc/httpd/conf.d/ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

## CentOS 8

在 `/etc/httpd/conf.d/ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

## Red Hat 7

在 `/etc/httpd/conf.d/ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

## Red Hat 8

在 `/etc/httpd/conf.d/ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
```

```
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

## Ubuntu 16.04 LTS

在 `/etc/apache2/sites-available/default-ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/ssl/certs/localhost.crt
SSLCertificateKeyFile /etc/ssl/private/localhost.key
```

## Ubuntu 18.04 LTS

在 `/etc/apache2/sites-available/default-ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/ssl/certs/localhost.crt
SSLCertificateKeyFile /etc/ssl/private/localhost.key
```

## Ubuntu 20.04 LTS

在 `/etc/apache2/sites-available/default-ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/ssl/certs/localhost.crt
SSLCertificateKeyFile /etc/ssl/private/localhost.key
```

## Ubuntu 22.04 LTS

在 `/etc/apache2/sites-available/default-ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateFile /etc/ssl/certs/localhost.crt
SSLCertificateKeyFile /etc/ssl/private/localhost.key
```

## Ubuntu 24.04 LTS

在 `/etc/apache2/sites-available/default-ssl.conf` 檔案中，請確定這些值存在：

```
SSLCertificateKeyFile /etc/ssl/private/localhost.key
```

### 3. 將 Web 伺服器憑證複製到平台所需的位置。

#### Amazon Linux

```
$ sudo cp <web_server.crt> /etc/pki/tls/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

#### Amazon Linux 2

```
$ sudo cp <web_server.crt> /etc/pki/tls/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

#### Amazon Linux 2023

```
$ sudo cp <web_server.crt> /etc/pki/tls/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

#### CentOS 7

```
$ sudo cp <web_server.crt> /etc/pki/tls/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

#### CentOS 8

```
$ sudo cp <web_server.crt> /etc/pki/tls/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

#### Red Hat 7

```
$ sudo cp <web_server.crt> /etc/pki/tls/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

## Red Hat 8

```
$ sudo cp <web_server.crt> /etc/pki/tls/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

## Ubuntu 16.04 LTS

```
$ sudo cp <web_server.crt> /etc/ssl/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

## Ubuntu 18.04 LTS

```
$ sudo cp <web_server.crt> /etc/ssl/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

## Ubuntu 20.04 LTS

```
$ sudo cp <web_server.crt> /etc/ssl/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

## Ubuntu 22.04 LTS

```
$ sudo cp <web_server.crt> /etc/ssl/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

## Ubuntu 24.04 LTS

```
$ sudo cp <web_server.crt> /etc/ssl/certs/localhost.crt
```

以 Web 伺服器憑證的名稱取代 *<web\_server.crt>*。

## 4. 將仿造 PEM 私有金鑰複製到平台所需的位置。

## Amazon Linux

```
$ sudo cp <web_server_example_pem.key> /etc/pki/tls/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

#### Amazon Linux 2

```
$ sudo cp <web_server_example_pem.key> /etc/pki/tls/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

#### Amazon Linux 2023

```
$ sudo cp <web_server_example_pem.key> /etc/pki/tls/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

#### CentOS 7

```
$ sudo cp <web_server_example_pem.key> /etc/pki/tls/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

#### CentOS 8

```
$ sudo cp <web_server_example_pem.key> /etc/pki/tls/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

#### Red Hat 7

```
$ sudo cp <web_server_example_pem.key> /etc/pki/tls/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

#### Red Hat 8

```
$ sudo cp <web_server_example_pem.key> /etc/pki/tls/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

#### Ubuntu 16.04 LTS

```
$ sudo cp <web_server_example_pem.key> /etc/ssl/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

Ubuntu 18.04 LTS

```
$ sudo cp <web_server_example_pem.key> /etc/ssl/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

Ubuntu 20.04 LTS

```
$ sudo cp <web_server_example_pem.key> /etc/ssl/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

Ubuntu 22.04 LTS

```
$ sudo cp <web_server_example_pem.key> /etc/ssl/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

Ubuntu 24.04 LTS

```
$ sudo cp <web_server_example_pem.key> /etc/ssl/private/localhost.key
```

以包含您仿造 PEM 私有金鑰的檔案名稱取代 `<web_server_example_pem.key>`#

5. 如果平台需要，請更改這些檔案的所有權。

Amazon Linux

```
$ sudo chown apache /etc/pki/tls/certs/localhost.crt /etc/pki/tls/private/localhost.key
```

提供讀取許可給名為 apache 的使用者。

Amazon Linux 2

```
$ sudo chown apache /etc/pki/tls/certs/localhost.crt /etc/pki/tls/private/localhost.key
```

提供讀取許可給名為 apache 的使用者。

## Amazon Linux 2023

```
$ sudo chown apache /etc/pki/tls/certs/localhost.crt /etc/pki/tls/private/localhost.key
```

提供讀取許可給名為 apache 的使用者。

## CentOS 7

```
$ sudo chown apache /etc/pki/tls/certs/localhost.crt /etc/pki/tls/private/localhost.key
```

提供讀取許可給名為 apache 的使用者。

## CentOS 8

```
$ sudo chown apache /etc/pki/tls/certs/localhost.crt /etc/pki/tls/private/localhost.key
```

提供讀取許可給名為 apache 的使用者。

## Red Hat 7

```
$ sudo chown apache /etc/pki/tls/certs/localhost.crt /etc/pki/tls/private/localhost.key
```

提供讀取許可給名為 apache 的使用者。

## Red Hat 8

```
$ sudo chown apache /etc/pki/tls/certs/localhost.crt /etc/pki/tls/private/localhost.key
```

提供讀取許可給名為 apache 的使用者。

## Ubuntu 16.04 LTS

不需要採取行動。

## Ubuntu 18.04 LTS

不需要採取行動。



## Ubuntu 20.04 LTS

不需要採取行動。

## Ubuntu 22.04 LTS

不需要採取行動。

## Ubuntu 24.04 LTS

不需要採取行動。

## 6. 為平台設定 Apache 指令。

### Amazon Linux

找到此平台的 SSL 檔案：

```
/etc/httpd/conf.d/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice cloudhsm
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
```

儲存檔案。

### Amazon Linux 2

找到此平台的 SSL 檔案：

```
/etc/httpd/conf.d/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice ccloudhsm
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
```

儲存檔案。

## Amazon Linux 2023

找到此平台的 SSL 檔案：

```
/etc/httpd/conf.d/ssl.conf
```

Apache 組態檔案會定義伺服器行為。使用根許可編輯此檔案。

更新或新增下列指令：

```
SSLCryptoDevice ccloudhsm
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
```

儲存檔案。

## CentOS 7

找到此平台的 SSL 檔案：

```
/etc/httpd/conf.d/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice ccloudhsm
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
```

儲存檔案。

## CentOS 8

找到此平台的 SSL 檔案：

```
/etc/httpd/conf.d/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice ccloudhsm
SSLProtocol TLSv1.2 TLSv1.3
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
SSLProxyCipherSuite HIGH:!aNULL
```

儲存檔案。

## Red Hat 7

找到此平台的 SSL 檔案：

```
/etc/httpd/conf.d/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice cloudhsm
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
```

儲存檔案。

## Red Hat 8

找到此平台的 SSL 檔案：

```
/etc/httpd/conf.d/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice cloudhsm
SSLProtocol TLSv1.2 TLSv1.3
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
SSLProxyCipherSuite HIGH:!aNULL
```

儲存檔案。

## Ubuntu 16.04 LTS

找到此平台的 SSL 檔案：

```
/etc/apache2/mods-available/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice cloudhsm
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
```

儲存檔案。

啟用 SSL 模組和預設 SSL 網站組態：

```
$ sudo a2enmod ssl
$ sudo a2ensite default-ssl
```

## Ubuntu 18.04 LTS

找到此平台的 SSL 檔案：

```
/etc/apache2/mods-available/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice cloudhsm
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-
```

```
SHA384:ECDSA-AES256-SHA384:ECDSA-AES128-GCM-SHA256:ECDSA-
AES128-SHA256:ECDSA-AES256-SHA:ECDSA-AES128-SHA
SSLProtocol TLSv1.2 TLSv1.3
```

儲存檔案。

啟用 SSL 模組和預設 SSL 網站組態：

```
$ sudo a2enmod ssl
$ sudo a2ensite default-ssl
```

## Ubuntu 20.04 LTS

找到此平台的 SSL 檔案：

```
/etc/apache2/mods-available/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice ccloudhsm
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDSA-AES256-GCM-SHA384:DHE-
RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDSA-AES256-SHA384:ECDSA-
RSA-AES128-SHA256:ECDSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDSA-AES256-GCM-
SHA384:ECDSA-AES256-SHA384:ECDSA-AES128-GCM-SHA256:ECDSA-
AES128-SHA256:ECDSA-AES256-SHA:ECDSA-AES128-SHA
SSLProtocol TLSv1.2 TLSv1.3
```

儲存檔案。

啟用 SSL 模組和預設 SSL 網站組態：

```
$ sudo a2enmod ssl
$ sudo a2ensite default-ssl
```

## Ubuntu 22.04 LTS

找到此平台的 SSL 檔案：

```
/etc/apache2/mods-available/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice cloudhsm
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
SSLProtocol TLSv1.2 TLSv1.3
```

儲存檔案。

啟用 SSL 模組和預設 SSL 網站組態：

```
$ sudo a2enmod ssl
$ sudo a2ensite default-ssl
```

## Ubuntu 24.04 LTS

找到此平台的 SSL 檔案：

```
/etc/apache2/mods-available/ssl.conf
```

該文件包含定義伺服器應該如何運行的 Apache 指令。指令顯示在左側，後面接著一個值。使用文字編輯器編輯此檔案。這需要 Linux 根許可。

使用這些值更新或輸入下列指令：

```
SSLCryptoDevice cloudhsm
```

```

SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-
RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-
RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-SHA:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
SSLProtocol TLSv1.2 TLSv1.3

```

儲存檔案。

啟用 SSL 模組和預設 SSL 網站組態：

```

$ sudo a2enmod ssl
$ sudo a2ensite default-ssl

```

## 7. 為平台設定環境值檔案。

### Amazon Linux

不需要採取行動。環境值要填入 `/etc/sysconfig/httpd`

### Amazon Linux 2

開啟 `httpd` 服務檔案：

```
/lib/systemd/system/httpd.service
```

將下列內容加入到 `[Service]` 區段：

```
EnvironmentFile=/etc/sysconfig/httpd
```

### Amazon Linux 2023

開啟 `/lib/systemd/system/httpd.service`

在 **【服務】** 區段下，新增：

```
EnvironmentFile=/etc/sysconfig/httpd
```

### CentOS 7

開啟 `httpd` 服務檔案：



```
/lib/systemd/system/httpd.service
```

將下列內容加入到 [Service] 區段：

```
EnvironmentFile=/etc/sysconfig/httpd
```

## CentOS 8

開啟 httpd 服務檔案：

```
/lib/systemd/system/httpd.service
```

將下列內容加入到 [Service] 區段：

```
EnvironmentFile=/etc/sysconfig/httpd
```

## Red Hat 7

開啟 httpd 服務檔案：

```
/lib/systemd/system/httpd.service
```

將下列內容加入到 [Service] 區段：

```
EnvironmentFile=/etc/sysconfig/httpd
```

## Red Hat 8

開啟 httpd 服務檔案：

```
/lib/systemd/system/httpd.service
```

將下列內容加入到 [Service] 區段：

```
EnvironmentFile=/etc/sysconfig/httpd
```

## Ubuntu 16.04 LTS

不需要採取行動。環境值要填入 `/etc/sysconfig/httpd`

## Ubuntu 18.04 LTS

不需要採取行動。環境值要填入 `/etc/sysconfig/httpd`

## Ubuntu 20.04 LTS

不需要採取行動。環境值要填入 `/etc/sysconfig/httpd`

## Ubuntu 22.04 LTS

不需要採取行動。環境值要填入 `/etc/sysconfig/httpd`

## Ubuntu 24.04 LTS

不需要採取行動。環境值要填入 `/etc/sysconfig/httpd`

8. 在儲存平台環境變數的檔案中，設定包含加密使用者 (CU) 憑證的環境變數：

## Amazon Linux

使用文字編輯器編輯 `/etc/sysconfig/httpd`。

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

以 CU 憑證取代 `<CU #####>` 和 `<##>`。

## Amazon Linux 2

使用文字編輯器編輯 `/etc/sysconfig/httpd`。

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

以 CU 憑證取代 `<CU #####>` 和 `<##>`。

## Amazon Linux 2023

開啟 `/etc/sysconfig/httpd`，新增：

```
CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

## CentOS 7

使用文字編輯器編輯 `/etc/sysconfig/httpd`。

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

## CentOS 8

使用文字編輯器編輯 `/etc/sysconfig/httpd`。

```
CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

## Red Hat 7

使用文字編輯器編輯 `/etc/sysconfig/httpd`。

```
ssl_engine cloudhsm;
env CLOUDHSM_PIN;
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

## Red Hat 8

使用文字編輯器編輯 `/etc/sysconfig/httpd`。

```
CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 **<CU #####>** 和 **<##>**。

### Note

用戶端 SDK 5 引入了用於存儲 CU 憑證的 CLOUDHSM\_PIN 環境變量。

## Ubuntu 16.04 LTS

使用文字編輯器編輯 /etc/apache2/envvars。

```
export n3fips_password=<CU user name>:<password>
```

以 CU 憑證取代 <CU #####> 和 <##>。

## Ubuntu 18.04 LTS

使用文字編輯器編輯 /etc/apache2/envvars。

```
export CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 <CU #####> 和 <##>。

### Note

用戶端 SDK 5 引入了用於存儲 CU 憑證的 CLOUDHSM\_PIN 環境變量。在用戶端 SDK 3 中，將 CU 憑證儲存在 n3fips\_password 環境變數中。用戶端 SDK 5 支援這兩個環境變數，但建議使用 CLOUDHSM\_PIN。

## Ubuntu 20.04 LTS

使用文字編輯器編輯 /etc/apache2/envvars。

```
export CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 <CU #####> 和 <##>。

### Note

用戶端 SDK 5 引入了用於存儲 CU 憑證的 CLOUDHSM\_PIN 環境變量。在用戶端 SDK 3 中，將 CU 憑證儲存在 n3fips\_password 環境變數中。用戶端 SDK 5 支援這兩個環境變數，但建議使用 CLOUDHSM\_PIN。

## Ubuntu 22.04 LTS

使用文字編輯器編輯 `/etc/apache2/envvars`。

```
export CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 `<CU #####>` 和 `<##>`。

### Note

用戶端 SDK 5 引入了用於存儲 CU 憑證的 `CLOUDHSM_PIN` 環境變量。在用戶端 SDK 3 中，將 CU 憑證儲存在 `n3fips_password` 環境變數中。用戶端 SDK 5 支援這兩個環境變數，但建議使用 `CLOUDHSM_PIN`。

## Ubuntu 24.04 LTS

使用文字編輯器編輯 `/etc/apache2/envvars`。

```
export CLOUDHSM_PIN=<CU user name>:<password>
```

以 CU 憑證取代 `<CU #####>` 和 `<##>`。

### Note

用戶端 SDK 5 引入了用於存儲 CU 憑證的 `CLOUDHSM_PIN` 環境變量。在用戶端 SDK 3 中，將 CU 憑證儲存在 `n3fips_password` 環境變數中。用戶端 SDK 5 支援這兩個環境變數，但建議使用 `CLOUDHSM_PIN`。

## 9. 啟動 Apache Web 伺服器。

### Amazon Linux

```
$ sudo systemctl daemon-reload
$ sudo service httpd start
```

## Amazon Linux 2

```
$ sudo systemctl daemon-reload
$ sudo service httpd start
```

## Amazon Linux 2023

```
$ sudo systemctl daemon-reload
$ sudo service httpd start
```

## CentOS 7

```
$ sudo systemctl daemon-reload
$ sudo service httpd start
```

## CentOS 8

```
$ sudo systemctl daemon-reload
$ sudo service httpd start
```

## Red Hat 7

```
$ sudo systemctl daemon-reload
$ sudo service httpd start
```

## Red Hat 8

```
$ sudo systemctl daemon-reload
$ sudo service httpd start
```

## Ubuntu 16.04 LTS

```
$ sudo service apache2 start
```

## Ubuntu 18.04 LTS

```
$ sudo service apache2 start
```

## Ubuntu 20.04 LTS

```
$ sudo service apache2 start
```

## Ubuntu 22.04 LTS

```
$ sudo service apache2 start
```

## Ubuntu 24.04 LTS

```
$ sudo service apache2 start
```

## 10. (選用) 將平台設定為在啟動時啟動 Apache。

### Amazon Linux

```
$ sudo chkconfig httpd on
```

### Amazon Linux 2

```
$ sudo chkconfig httpd on
```

### Amazon Linux 2023

```
$ sudo chkconfig httpd on
```

### CentOS 7

```
$ sudo chkconfig httpd on
```

### CentOS 8

```
$ systemctl enable httpd
```

### Red Hat 7

```
$ sudo chkconfig httpd on
```

## Red Hat 8

```
$ systemctl enable httpd
```

## Ubuntu 16.04 LTS

```
$ sudo systemctl enable apache2
```

## Ubuntu 18.04 LTS

```
$ sudo systemctl enable apache2
```

## Ubuntu 20.04 LTS

```
$ sudo systemctl enable apache2
```

## Ubuntu 22.04 LTS

```
$ sudo systemctl enable apache2
```

## Ubuntu 24.04 LTS

```
$ sudo systemctl enable apache2
```

在更新您的 Web 伺服器組態之後，請移至 [步驟 4：啟用 HTTPS 流量並驗證憑證](#)。

## 步驟 4：啟用 HTTPS 流量並驗證憑證

使用 設定 Web 伺服器進行 SSL/TLS 卸載後 AWS CloudHSM，請將 Web 伺服器執行個體新增至允許傳入 HTTPS 流量的安全群組。這可讓用戶端 (例如 Web 瀏覽器) 與 Web 伺服器建立 HTTPS 連線。然後建立與 Web 伺服器的 HTTPS 連線，並驗證其是否使用您為 SSL/TLS 卸載設定的憑證 AWS CloudHSM。

### 主題

- [啟用傳入 HTTPS 連線](#)
- [驗證 HTTPS 是否使用您已設定的憑證](#)



## 啟用傳入 HTTPS 連線

若要從用戶端 (例如 Web 瀏覽器) 連接到 Web 伺服器，請建立允許傳入 HTTPS 連接的安全群組。特別是應該允許連接埠 443 上的傳入 TCP 連線。將此安全群組指派到您的 Web 伺服器。

建立 HTTPS 的安全群組並將其指派至您的 Web 伺服器

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中選擇安全群組。
3. 選擇建立安全群組。
4. 對於 Create Security Group (建立安全群組)，執行下列動作：
  - a. 對於 Security group name (安全群組名稱)，輸入您要建立之安全群組的名稱。
  - b. (選用) 輸入您要建立之安全群組的描述。
  - c. 對於 VPC，選擇包含 Web 伺服器 Amazon EC2 執行個體的 VPC。
  - d. 選取 Add Rule (新增規則)。
  - e. 對於類型，從下拉式視窗中選取 HTTPS。
  - f. 對於來源，輸入來源位置。
  - g. 選擇建立安全群組。
5. 在導覽窗格中，選擇執行個體。
6. 選取 Web 伺服器執行個體旁的核取方塊。
7. 選取頁面頂端的動作下拉式選單。選取安全性，然後選取變更安全群組。
8. 對於關聯的安全群組，請選取搜尋方塊，然後選取您為 HTTPS 建立之安全群組。然後選擇新增安全群組。
9. 選取 Save (儲存)。

## 驗證 HTTPS 是否使用您已設定的憑證

將 Web 伺服器新增至安全群組後，您可以驗證 SSL/TLS 卸載是否使用您的自我簽署憑證。若要這樣做，您可以使用 Web 瀏覽器或使用 [OpenSSL s\\_client](#) 之類的工具。

## 使用 Web 瀏覽器驗證 SSL/TLS 卸載

1. 使用 Web 瀏覽器來透過伺服器的公有 DNS 名稱或 IP 地址連接到您的 Web 伺服器。請確定網址列中的 URL 開頭為 https://。例如 **https://ec2-52-14-212-67.us-east-2.compute.amazonaws.com/**。

**i** Tip

您可以使用 DNS 服務 (例如 Amazon Route 53)，將網站的網域名稱 (例如，https://www.example.com/) 路由到 Web 伺服器。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》或 DNS 服務文件中的[將流量路由到 Amazon EC2 執行個體](#)。

2. 使用您的 Web 瀏覽器來檢視 Web 伺服器憑證。如需詳細資訊，請參閱下列內容：

- 若為 Mozilla Firefox，請參閱 Mozilla 技術支援網站上的[檢視憑證](#)。
- 若為 Google Chrome，請參閱 Google Web 開發人員工具網站上的[了解安全問題](#)。

其他 Web 瀏覽器可能有類似的功能，可供您用來檢視 Web 伺服器憑證。

3. 確保 SSL/TLS 憑證是您設定 Web 伺服器所要使用的憑證。

使用 OpenSSL s\_client 來驗證 SSL/TLS 卸載

1. 執行以下 OpenSSL 命令來使用 HTTPS 連接至 Web 伺服器。以 Web 伺服器的公有 DNS 名稱或 IP 地址來取代 `<#####>`。

```
openssl s_client -connect <server name>:443
```

**i** Tip

您可以使用 DNS 服務 (例如 Amazon Route 53)，將網站的網域名稱 (例如，https://www.example.com/) 路由到 Web 伺服器。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》或 DNS 服務文件中的[將流量路由到 Amazon EC2 執行個體](#)。

2. 確保 SSL/TLS 憑證是您設定 Web 伺服器所要使用的憑證。

您現在有透過 HTTPS 而受到保護的網站。Web 伺服器的私有金鑰存放在 AWS CloudHSM 叢集的 HSM 中。

若要新增負載平衡器，請參閱 [使用 Elastic Load Balancing for 新增負載平衡器 AWS CloudHSM \(選用\)](#)。

# AWS CloudHSM 使用 Tomcat 搭配 JSSE 在 Linux 上卸載 SSL/TLS

本主題提供step-by-step說明。 AWS CloudHSM

## 主題

- [概觀](#)
- [步驟 1：設定先決條件](#)
- [步驟 2：產生或匯入私有金鑰和 SSL/TLS 憑證](#)
- [步驟 3：設定 Tomcat Web 伺服器](#)
- [步驟 4：啟用 HTTPS 流量並驗證憑證](#)

## 概觀

在 中 AWS CloudHSM，Tomcat Web 伺服器會在 Linux 上運作，以支援 HTTPS。AWS CloudHSM JCE 開發套件提供可與 JSSE (Java Secure Socket Extension) 搭配使用的界面，以啟用此類 Web 伺服器的 HSMs。AWS CloudHSM JCE 是將 JSSE 連接到 AWS CloudHSM 叢集的橋接器。JSSE 是適用於 Secure Sockets Layer (SSL) 和 Transport Layer Security (TLS) 通訊協定的 Java API。

## 步驟 1：設定先決條件

請遵循這些先決條件，將 Tomcat Web 伺服器與 Linux AWS CloudHSM 上的 SSL/TLS 卸載搭配使用。您必須符合這些先決條件，才能透過用戶端 SDK 5 和 Tomcat Web 伺服器來設定 Web 伺服器 SSL/TLS 卸載。

### Note

不同平台需要不同的先決條件。請務必遵循適用於平台的正確安裝步驟。

## 先決條件

- 執行 Linux 作業系統且安裝了 Tomcat Web 伺服器的 Amazon EC2 執行個體。
- [加密使用者](#) (CU)，擁有及管理 HSM 上 Web 伺服器的私有金鑰。
- 具有至少兩個硬體安全模組 (HSMs) 且已安裝並設定[用戶端 SDK 5 的 JCE](#)的作用中 AWS CloudHSM 叢集。

**Note**

您可以使用單一 HSM 叢集，但必須先停用用戶端金鑰持久性。如需詳細資訊，請參閱[管理用戶端金鑰持久性設定](#)和[用戶端 SDK 5 設定工具](#)。

**如何滿足先決條件**

1. 在具有至少兩個硬體安全模組 (HSMs) 的作用中 AWS CloudHSM 叢集 AWS CloudHSM 上安裝和設定的 JCE。如需關於安裝的詳細資訊，請參閱[用戶端 SDK 5 的 JCE](#)。
2. 在可存取 AWS CloudHSM 叢集的 EC2 Linux 執行個體上，遵循 [Apache Tomcat 指示](#) 下載並安裝 Tomcat Web 伺服器。
3. 使用 [CloudHSM CLI](#) 建立加密使用者 (CU)。如需關於管理 HSM 使用者的詳細資訊，請參閱[使用 CloudHSM CLI 管理 HSM 使用者](#)。

**Tip**

保持追蹤 CU 使用者名稱和密碼。之後在為您的 Web 伺服器產生或匯入 HTTPS 私有金鑰和憑證時，您將會需要該資訊。

4. 要使用 Java Keytool 設置 JCE，請按照 [使用用戶端 SDK 5 AWS CloudHSM 與 Java Keytool 和 Jarsigner 整合](#) 中的說明進行操作。

完成這些步驟之後，請移至 [步驟 2：產生或匯入私有金鑰和 SSL/TLS 憑證](#)。

**備註**

- 若要使用 Security-Enhanced Linux (SELinux) 和 Web 伺服器，您必須在連接埠 2223 上允許傳出 TCP 連線，也就是用戶端 SDK 5 用來與 HSM 通訊的連接埠。
- 若要建立和啟用叢集並授予 EC2 執行個體存取叢集的權限，請完成[AWS CloudHSM入門](#)中的步驟。本節提供使用一個 HSM 和 Amazon EC2 用戶端執行個體建立作用中叢集的逐步說明。可以使用此用戶端執行個體做為 Web 伺服器。
- 若要避免停用用戶端金鑰持久性，請在叢集中新增多個 HSM。如需詳細資訊，請參閱[將 HSM 新增至 AWS CloudHSM 叢集](#)。
- 要連接到用戶端執行個體，可以使用 SSH 或 PuTTY。如需詳細資訊，請參閱 Amazon EC2 文件中的[使用 SSH 連接至您的 Linux 執行個體](#)或[使用 PuTTY 從 Windows 連接至您的 Linux 執行個體](#)。

## 步驟 2：產生或匯入私有金鑰和 SSL/TLS 憑證

若要啟用 HTTPS，Tomcat Web 伺服器應用程式需要私有金鑰和對應 SSL/TLS 憑證。若要搭配使用 Web 伺服器 SSL/TLS 卸載 AWS CloudHSM，您必須將私有金鑰存放在 AWS CloudHSM 叢集的 HSM 中。

### Note

如果您還沒有私有金鑰和對應的憑證，可以在 HSM 中產生私有金鑰。您可以使用私有金鑰建立憑證簽署請求 (CSR)，以用來建立 SSL/TLS 憑證。

您可以建立 local AWS CloudHSM KeyStore 檔案，其中包含對 HSM 上私有金鑰和相關聯憑證的參考。在 SSL/TLS 卸載期間，您的 Web 伺服器會使用 AWS CloudHSM KeyStore 檔案來識別 HSM 上的私有金鑰。

### 主題

- [產生私有金鑰](#)
- [產生自簽憑證。](#)

### 產生私有金鑰

本節說明如何使用 JDK 的 KeyTool 產生金鑰對。在 HSM 內部產生金鑰對之後，您可以將其匯出為 KeyStore 檔案，然後產生對應的憑證。

根據您的使用案例，您可以產生 RSA 或 EC 金鑰對。下列步驟說明如何產生 RSA 金鑰對。

在 KeyTool 中使用 **genkeypair** 命令，以產生 RSA 金鑰對。

1. 用特定數據替換以下 **<VARIABLES>** 後，請使用下列命令產生名為 `jsse_keystore.keystore` 的金鑰存放區檔案，該檔案將具有 HSM 上私有金鑰的參考。

```
$ keytool -genkeypair -alias <UNIQUE ALIAS FOR KEYS> -keyalg <KEY ALGORITHM> -
keysize <KEY SIZE> -sigalg <SIGN ALGORITHM> \
-keystore <PATH>/<JSSE KEYSTORE NAME>.keystore -storetype CLOUDHSM \
-dname CERT_DOMAIN_NAME \
-J-classpath '-J'$JAVA_LIB'/*:/opt/cloudhsm/java/*:./*' \
-provider "com.amazonaws.cloudhsm.jce.provider.CloudHsmProvider" \
-providerpath "$CLOUDHSM_JCE_LOCATION" \

```

```
-keypass <KEY PASSWORD> -storepass <KEYSTORE PASSWORD>
```

- **<PATH>**：您要生成金鑰存放區檔案的路徑。
  - **<UNIQUE ALIAS FOR KEYS>**：這是用於唯一識別 HSM 上的金鑰。此別名將被設置為金鑰的 LABEL 屬性。
  - **<KEY PASSWORD>**：我們會將您金鑰的參考儲存在本機金鑰儲存檔案中，而此密碼會保護該本機參考。
  - **<KEYSTORE PASSWORD>**：這是本機金鑰存放區檔案的密碼。
  - **<JSSE KEYSTORE NAME>**：金鑰存放區檔案的名稱。
  - **<CERT DOMAIN NAME>**：X.500 辨別名稱。
  - **<KEY ALGORITHM>**：生成金鑰對的金鑰算法（例如，RSA 和 EC）。
  - **<KEY SIZE>**：要產生金鑰對的金鑰大小（例如，2048、3072 和 4096）。
  - **<SIGN ALGORITHM>**：要產生金鑰對的金鑰大小（例如，SHA1withRSA、SHA224withRSA、SHA256withRSA、SHA384withRSA 和 SHA512withRSA）。
2. 若要確認命令是否成功，請輸入下列命令，並確認您是否已成功產生 RSA 金鑰對。

```
$ ls <PATH>/<JSSE KEYSTORE NAME>.keystore
```

產生自簽憑證。

產生私有金鑰與金鑰存放區檔案後，您可以使用此檔案來產生憑證簽署要求 (CSR) 和憑證。

在生產環境中，您通常會使用憑證授權單位 (CA) 從 CSR 建立憑證。測試環境不需要 CA。如果您確實使用 CA，請將 CSR 檔案發送給他們，並使用他們在 Web 伺服器中為您提供 HTTPS 的簽名 SSL/TLS 憑證。

除了使用 CA，您也可以使用 KeyTool 建立自簽憑證。自簽憑證不受瀏覽器所信任，請勿用於生產環境。可以用於測試環境。

#### Warning

自簽憑證應該只用於測試環境。若為生產環境，請使用更安全的方法（例如憑證授權單位）來建立憑證。

## 產生憑證

1. 取得先前步驟中產生的金鑰存放區檔案的副本。
2. 執行下列命令，以使用 KeyTool 建立憑證簽署請求 (CSR)。

```
$ keytool -certreq -keyalg RSA -alias unique_alias_for_key -file certreq.csr \
 -keystore <JSSE KEYSTORE NAME>.keystore -storetype CLOUDHSM \
 -J-classpath '-J$JAVA_LIB/*:/opt/cloudhsm/java/*:./*' \
 -keypass <KEY PASSWORD> -storepass <KEYSTORE PASSWORD>
```

### Note

憑證簽署請求的輸出檔案為 certreq.csr。

## 簽署憑證

- 用特定數據替換以下 **<VARIABLES>** 後，請執行下列命令，以在 HSM 上的私有金鑰簽署 CSR。這會建立自簽憑證。

```
$ keytool -gencert -infile certreq.csr -outfile certificate.crt \
 -alias <UNIQUE ALIAS FOR KEYS> -keypass <KEY_PASSWORD> -
storepass <KEYSTORE_PASSWORD> -sigalg SIG_ALG \
 -storetype CLOUDHSM -J-classpath '-J$JAVA_LIB/*:/opt/cloudhsm/java/*:./*' \
 -keystore jsse_keystore.keystore
```

### Note

certificate.crt 是使用別名私有金鑰的簽署憑證。

## 在金鑰存放區中匯入憑證

- 用特定數據替換以下 **<VARIABLES>** 後，請執行下列命令，將已簽署的憑證匯入為受信任的憑證。此步驟會將憑證存放在別名識別的金鑰存放區項目中。

```
$ keytool -import -alias <UNIQUE ALIAS FOR KEYS> -keystore jsse_keystore.keystore \
 -file certificate.crt -storetype CLOUDHSM \
 -v -J-classpath '-J$JAVA_LIB/*:/opt/cloudhsm/java/*:./*' \
```

```
-keypass <KEY_PASSWORD> -storepass <KEYSTORE_PASSWORD>
```

## 將憑證轉換為 PEM

- 執行下列命令，將簽署的憑證檔案 (.crt) 轉換為 PEM。PEM 檔案將用於從 http 用戶端發送請求。

```
$ openssl x509 -inform der -in certificate.crt -out certificate.pem
```

完成這些步驟之後，前往[步驟 3：設定 Web 伺服器](#)。

## 步驟 3：設定 Tomcat Web 伺服器

更新 Web 伺服器軟體組態，以使用 HTTPS 憑證以及您在上一個步驟中建立的對應 PEM 檔案。請記得在開始之前備份現有的憑證和金鑰。這將完成針對 SSL/TLS 卸載搭配 AWS CloudHSM 設定您的 Linux Web 伺服器軟體。如需詳細資訊，請參閱 [Apache Tomcat 9 組態參考](#)。

### 停止伺服器

- 用特定數據替換以下 **<VARIABLES>** 後，請運行以下命令以在更新組態之前停止 Tomcat 伺服器。

```
$ /<TOMCAT DIRECTORY>/bin/shutdown.sh
```

- <TOMCAT DIRECTORY>**：Tomcat 安裝目錄。

### 更新 Tomcat classpath

- 連接至您的用戶端執行個體。
- 找到 Tomcat 安裝資料夾。
- 將以下 **<VARIABLES>** 取代為您的特定資料後，請使用下列命令，在 Tomcat 中新增位於 Tomcat/bin/catalina.sh 檔案 classpath 的 Java 程式庫和 AWS CloudHSM Java 路徑。

```
$ sed -i 's@CLASSPATH="$CLASSPATH"$CATALINA_HOME"/bin/bootstrap.jar@CLASSPATH="$CLASSPATH"$CATALINA_HOME"/bin/bootstrap.jar:"<JAVA LIBRARY>"'/*:/opt/cloudhsm/java/*:.*@' <TOMCAT PATH> /bin/catalina.sh
```



- **<JAVA LIBRARY>** : Java JRE 程式庫位置。
- **<TOMCAT PATH>** : Tomcat 安裝資料夾。

在伺服器組態中新增 HTTPS 連接器。

1. 前往 Tomcat 安裝資料夾。
2. 用特定數據替換下面的 **<VARIABLES>** 後，請使用下列命令新增 HTTPS 連接器，以使用必要條件中產生的憑證：

```
$ sed -i '/<Connector port="8080"/i <Connector port="\443\" maxThreads="\200\"
scheme="https\" secure="\true\" SSLEnabled="\true\" keystoreType="\CLOUDHSM\"
keystoreFile=\"
 <CUSTOM DIRECTORY>/<JSSE KEYSTORE NAME>.keystore\" keystorePass=\"<KEYSTORE
PASSWORD>\" keyPass=\"<KEY PASSWORD>
 \" keyAlias=\"<UNIQUE ALIAS FOR KEYS>\" clientAuth=\"false\" sslProtocol=
\"TLS\"/>' <TOMCAT PATH>/conf/server.xml
```

- **<CUSTOM DIRECTORY>** : 金鑰存放區檔案所在的目錄。
- **<JSSE KEYSTORE NAME>** : 金鑰存放區檔案的名稱。
- **<KEYSTORE PASSWORD>** : 這是本機金鑰存放區檔案的密碼。
- **<KEY PASSWORD>** : 我們會將您金鑰的參考儲存在本機金鑰儲存檔案中，而此密碼會保護該本機參考。
- **<UNIQUE ALIAS FOR KEYS>** : 這是用於唯一識別 HSM 上的金鑰。此別名將被設置為金鑰的 LABEL 屬性。
- **<TOMCAT PATH>** : Tomcat 資料夾的路徑。

## 啟動伺服器

- 用特定數據替換以下 **<VARIABLES>** 後，使用以下命令啟動 Tomcat 伺服器：

```
$ /<TOMCAT DIRECTORY>/bin/startup.sh
```

### Note

**<TOMCAT DIRECTORY>** 是您的 Tomcat 安裝目錄的名稱。

在更新您的 Web 伺服器組態之後，請前往 [步驟 4：啟用 HTTPS 流量並驗證憑證](#)。

## 步驟 4：啟用 HTTPS 流量並驗證憑證

使用設定 Web 伺服器進行 SSL/TLS 卸載後 AWS CloudHSM，請將 Web 伺服器執行個體新增至允許傳入 HTTPS 流量的安全群組。這可讓用戶端 (例如 Web 瀏覽器) 與 Web 伺服器建立 HTTPS 連線。然後建立與 Web 伺服器的 HTTPS 連線，並驗證其是否使用您為 SSL/TLS 卸載設定的憑證 AWS CloudHSM。

### 主題

- [啟用傳入 HTTPS 連線](#)
- [驗證 HTTPS 是否使用您已設定的憑證](#)

### 啟用傳入 HTTPS 連線

若要從用戶端 (例如 Web 瀏覽器) 連接到 Web 伺服器，請建立允許傳入 HTTPS 連接的安全群組。特別是應該允許連接埠 443 上的傳入 TCP 連線。將此安全群組指派到您的 Web 伺服器。

建立 HTTPS 的安全群組並將其指派至您的 Web 伺服器

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中選擇安全群組。
3. 選擇建立安全群組。
4. 對於 Create Security Group (建立安全群組)，執行下列動作：
  - a. 對於 Security group name (安全群組名稱)，輸入您要建立之安全群組的名稱。
  - b. (選用) 輸入您要建立之安全群組的描述。
  - c. 對於 VPC，選擇包含 Web 伺服器 Amazon EC2 執行個體的 VPC。
  - d. 選取 Add Rule (新增規則)。
  - e. 對於類型，從下拉式視窗中選取 HTTPS。
  - f. 對於來源，輸入來源位置。
  - g. 選擇建立安全群組。
5. 在導覽窗格中，選擇執行個體。
6. 選取 Web 伺服器執行個體旁的核取方塊。
7. 選取頁面頂端的動作下拉式選單。選取安全性，然後選取變更安全群組。

- 對於關聯的安全群組，請選取搜尋方塊，然後選取您為 HTTPS 建立之安全群組。然後選擇新增安全群組。
- 選取 Save (儲存)。

### 驗證 HTTPS 是否使用您已設定的憑證

將 Web 伺服器新增至安全群組後，您可以驗證 SSL/TLS 卸載是否使用您的自我簽署憑證。若要這樣做，您可以使用 Web 瀏覽器或使用 [OpenSSL s\\_client](#) 之類的工具。

#### 使用 Web 瀏覽器驗證 SSL/TLS 卸載

- 使用 Web 瀏覽器來透過伺服器的公有 DNS 名稱或 IP 地址連接到您的 Web 伺服器。請確定網址列中的 URL 開頭為 https://。例如 **https://ec2-52-14-212-67.us-east-2.compute.amazonaws.com/**。

#### Tip

您可以使用 DNS 服務 (例如 Amazon Route 53)，將網站的網域名稱 (例如，https://www.example.com/) 路由到 Web 伺服器。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》或 DNS 服務文件中的[將流量路由到 Amazon EC2 執行個體](#)。

- 使用您的 Web 瀏覽器來檢視 Web 伺服器憑證。如需詳細資訊，請參閱下列內容：
  - 若為 Mozilla Firefox，請參閱 Mozilla 技術支援網站上的[檢視憑證](#)。
  - 若為 Google Chrome，請參閱 Google Web 開發人員工具網站上的[了解安全問題](#)。

其他 Web 瀏覽器可能有類似的功能，可供您用來檢視 Web 伺服器憑證。

- 確保 SSL/TLS 憑證是您設定 Web 伺服器所要使用的憑證。

#### 使用 OpenSSL s\_client 來驗證 SSL/TLS 卸載

- 執行以下 OpenSSL 命令來使用 HTTPS 連接至 Web 伺服器。以 Web 伺服器的公有 DNS 名稱或 IP 地址來取代 **<server name>**。

```
openssl s_client -connect <server name>:443
```

 Tip

您可以使用 DNS 服務 (例如 Amazon Route 53)，將網站的網域名稱 (例如，https://www.example.com/) 路由到 Web 伺服器。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》或 DNS 服務文件中的[將流量路由到 Amazon EC2 執行個體](#)。

## 2. 確保 SSL/TLS 憑證是您設定 Web 伺服器所要使用的憑證。

您現在有透過 HTTPS 而受到保護的網站。Web 伺服器的私有金鑰存放在 AWS CloudHSM 叢集的 HSM 中。

若要新增負載平衡器，請參閱 [使用 Elastic Load Balancing for 新增負載平衡器 AWS CloudHSM \(選用\)](#)。

## AWS CloudHSM 在 Windows 上使用 IIS 搭配 KSP 的 SSL/TLS 卸載

本教學提供在 Windows Web 伺服器上設定 SSL/TLS 卸載搭配 AWS CloudHSM 的逐步說明。

### 主題

- [概觀](#)
- [步驟 1：設定先決條件](#)
- [步驟 2：建立憑證簽署要求 \(CSR\) 和憑證](#)
- [步驟 3：設定 Web 伺服器](#)
- [步驟 4：啟用 HTTPS 流量並驗證憑證](#)

### 概觀

在 Windows 上，[Internet Information Services \(IIS\) for Windows Server](#) Web 伺服器應用程式原本就支援 HTTPS。[適用於 Microsoft 加密 API 之 AWS CloudHSM 金鑰儲存供應商 \(KSP\)：下一代 \(CNG\)](#) 提供的界面，可讓 IIS 在您的叢集中使用 HSM，進行密碼編譯卸載和金鑰儲存。AWS CloudHSM KSP 是將 IIS 連接到 AWS CloudHSM 叢集的橋接器。

此教學課程會讓您了解如何執行以下操作：

- 在 Amazon EC2 執行個體上安裝 Web 伺服器軟體。
- 將 Web 伺服器軟體設定為使用儲存在 AWS CloudHSM 叢集中的私有金鑰來支援 HTTPS。

- (選用) 使用 Amazon EC2 建立第二個 Web 伺服器執行個體，並使用 Elastic Load Balancing 建立負載平衡器。使用負載平衡器可將負載分散到多部伺服器，進而提升效能。它也可以在一或多個伺服器失敗時提供備援和高可用性。

當您準備好開始時，請移至[步驟 1：設定先決條件](#)。

## 步驟 1：設定先決條件

不同平台需要不同的先決條件。請使用下方符合您平台的先決條件區段。

### 主題

- [用戶端 SDK 5 的先決條件](#)
- [用戶端 SDK 3 的先決條件](#)

### 用戶端 SDK 5 的先決條件

若要使用 設定 Web 伺服器 SSL/TLS 卸載 AWS CloudHSM，您需要下列項目：

- 具有至少一個 HSM 的作用中 AWS CloudHSM 叢集。
- 執行 Windows 作業系統的 Amazon EC2 執行個體，其中已安裝下列軟體：
  - 適用於 Windows 的 AWS CloudHSM 用戶端軟體。
  - Internet Information Services (IIS) for Windows Server。
- [加密使用者](#) (CU)，擁有及管理 HSM 上 Web 伺服器的私有金鑰。

#### Note

本教學課程使用 Microsoft Windows Server 2019。也支援 Microsoft Windows Server 2016 和 2022。

### 設定 Windows 伺服器執行個體，並在 HSM 上建立 CU

1. 完成「[開始使用](#)」中的步驟。當您啟動 Amazon EC2 用戶端時，請選擇 Windows Server 2019 AMI。當您完成這些步驟，便擁有至少包含一個 HSM 的作用中叢集。您也有執行 Windows Server 的 Amazon EC2 用戶端執行個體，其中已安裝適用於 Windows 的 AWS CloudHSM 用戶端軟體。

2. (選用) 在您的叢集中新增更多 HSM。如需詳細資訊，請參閱[將 HSM 新增至 AWS CloudHSM 叢集](#)。
3. 連接至 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
4. 使用 CloudHSM CLI 建立加密使用者 (CU)。保持追蹤 CU 使用者名稱和密碼。您需要它們來完成下一個步驟。

 Note

如需如何建立使用者的詳細資訊，請參閱[使用 CloudHSM CLI 管理 HSM 使用者](#)。

5. 使用您在先前步驟中建立的 CU 使用者名稱和密碼，[設定 HSM 的登入資料](#)。
6. 在步驟 5 中，如果您使用 Windows 認證管理員來設定 HSM 登入資料，請從 SysInternals 下載 [psexec.exe](#)，以 NT Authority\SYSTEM 的身分執行下列命令：

```
psexec.exe -s "C:\Program Files\Amazon\CloudHsm\tools\set_cloudhsm_credentials.exe"
--username <USERNAME> --password <PASSWORD>
```

以 HSM 憑證取代 **<#####>** 和 **<##>**。

## 在 Windows 伺服器上安裝 IIS

1. 如果您尚未這麼做，請連接至您的 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 在 Windows 伺服器上，啟動 Server Manager (伺服器管理員)。
3. 在 Server Manager (伺服器管理員) 儀表板中，選擇 Add roles and features (新增角色和功能)。
4. 閱讀 Before you begin (開始之前) 資訊，然後選擇 Next (下一步)。
5. 對於 Installation Type (安裝類型)，選擇 Role-based or feature-based installation (角色型或功能型安裝)。然後選擇下一步。
6. 對於 Server Selection (伺服器選項)，選擇 Select a server from the server pool (從伺服器集區選取伺服器)。然後選擇下一步。
7. 對於 Server Roles (伺服器角色)，執行下列動作：
  - a. 選取 Web Server (IIS) (Web 伺服器 (IIS))。

- b. 對於 Add features that are required for Web Server (IIS) (新增 Web 伺服器 (IIS) 需要的功能)，選擇 Add Features (新增功能)。
  - c. 選擇 Next (下一步) 來完成伺服器角色的選取。
8. 針對 Features (功能)，接受預設。然後選擇下一步。
  9. 閱讀 Web Server Role (IIS) (Web 伺服器角色 (IIS)) 資訊。然後選擇下一步。
  10. 對於 Select role services (選取角色服務)，接受預設值或變更為偏好的設定。然後選擇下一步。
  11. 針對 Confirmation (確認)，閱讀確認資訊。然後選擇 Install (安裝)。
  12. 完成安裝之後，請選擇 Close (關閉)。

完成這些步驟之後，請移至 [步驟 2：建立憑證簽署要求 \(CSR\) 和憑證](#)。

### 用戶端 SDK 3 的先決條件

若要使用 設定 Web 伺服器 SSL/TLS 卸載 AWS CloudHSM，您需要下列項目：

- 具有至少一個 HSM 的作用中 AWS CloudHSM 叢集。
- 執行 Windows 作業系統的 Amazon EC2 執行個體，其中已安裝下列軟體：
  - 適用於 Windows 的 AWS CloudHSM 用戶端軟體。
  - Internet Information Services (IIS) for Windows Server。
- [加密使用者](#) (CU)，擁有及管理 HSM 上 Web 伺服器的私有金鑰。

#### Note

本教學課程使用 Microsoft Windows Server 2016。也支援 Microsoft Windows Server 2012，但不支援 Microsoft Windows Server 2012 R2。

### 設定 Windows 伺服器執行個體，並在 HSM 上建立 CU

1. 完成「[開始使用](#)」中的步驟。當您啟動 Amazon EC2 用戶端時，請選擇 Windows Server 2016 或 Windows Server 2012 AMI。當您完成這些步驟，便擁有至少包含一個 HSM 的作用中叢集。您也有執行 Windows Server 的 Amazon EC2 用戶端執行個體，其中已安裝適用於 Windows 的 AWS CloudHSM 用戶端軟體。
2. (選用) 在您的叢集中新增更多 HSM。如需詳細資訊，請參閱[將 HSM 新增至 AWS CloudHSM 叢集](#)。



3. 連接至 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
4. 使用 CloudHSM CLI 建立加密使用者 (CU)。保持追蹤 CU 使用者名稱和密碼。您需要它們來完成下一個步驟。

 Note

如需如何建立使用者的詳細資訊，請參閱[使用 CloudHSM CLI 管理 HSM 使用者](#)。

5. 使用您在先前步驟中建立的 CU 使用者名稱和密碼，[設定 HSM 的登入資料](#)。
6. 在步驟 5 中，如果您使用 Windows 認證管理員來設定 HSM 登入資料，請從 SysInternals 下載 [psexec.exe](#)，以 NT Authority\SYSTEM 的身分執行下列命令：

```
psexec.exe -s "C:\Program Files\Amazon\CloudHsm\tools\set_cloudhsm_credentials.exe"
--username <USERNAME> --password <PASSWORD>
```

以 HSM 憑證取代 **<#####>** 和 **<##>**。

## 在 Windows 伺服器上安裝 IIS

1. 如果您尚未這麼做，請連接至您的 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 在 Windows 伺服器上，啟動 Server Manager (伺服器管理員)。
3. 在 Server Manager (伺服器管理員) 儀表板中，選擇 Add roles and features (新增角色和功能)。
4. 閱讀 Before you begin (開始之前) 資訊，然後選擇 Next (下一步)。
5. 對於 Installation Type (安裝類型)，選擇 Role-based or feature-based installation (角色型或功能型安裝)。然後選擇下一步。
6. 對於 Server Selection (伺服器選項)，選擇 Select a server from the server pool (從伺服器集區選取伺服器)。然後選擇下一步。
7. 對於 Server Roles (伺服器角色)，執行下列動作：
  - a. 選取 Web Server (IIS) (Web 伺服器 (IIS))。
  - b. 對於 Add features that are required for Web Server (IIS) (新增 Web 伺服器 (IIS) 需要的功能)，選擇 Add Features (新增功能)。
  - c. 選擇 Next (下一步) 來完成伺服器角色的選取。



8. 針對 Features (功能)，接受預設。然後選擇下一步。
9. 閱讀 Web Server Role (IIS) (Web 伺服器角色 (IIS)) 資訊。然後選擇下一步。
10. 對於 Select role services (選取角色服務)，接受預設值或變更為偏好的設定。然後選擇下一步。
11. 針對 Confirmation (確認)，閱讀確認資訊。然後選擇 Install (安裝)。
12. 完成安裝之後，請選擇 Close (關閉)。

完成這些步驟之後，請移至 [步驟 2：建立憑證簽署要求 \(CSR\) 和憑證](#)。

## 步驟 2：建立憑證簽署要求 (CSR) 和憑證

若要啟用 HTTPS，您的 Web 伺服器需要 SSL/TLS 憑證和對應私有金鑰。若要使用 SSL/TLS 卸載搭配 AWS CloudHSM，請將私有金鑰存放在叢集的 HSM 中 AWS CloudHSM。為此，請使用[適用於 Microsoft 密碼編譯 API 的 AWS CloudHSM 金鑰儲存供應商 \(KSP\)：下一代 \(CNG\)](#) 建立憑證簽署請求 (CSR)。然後，將 CSR 提供給憑證授權機構 (CA)，其會簽署 CSR 以產生憑證。

### 主題

- [使用用戶端 SDK 5 建立 CSR](#)
- [使用用戶端 SDK 3 建立 CSR](#)
- [取得已簽署的憑證並匯入它](#)

### 使用用戶端 SDK 5 建立 CSR

1. 在 Windows 伺服器上，使用文字編輯器來建立名為 IISCertRequest.inf 的憑證要求檔案。下列示範範例 IISCertRequest.inf 檔案的內容。如需您可在檔案中指定之區段、金鑰和數值的詳細資訊，請參閱 [Microsoft 文件](#)。請勿變更 ProviderName 值。

```
[Version]
Signature = "$Windows NT$"
[NewRequest]
Subject = "CN=example.com,C=US,ST=Washington,L=Seattle,O=ExampleOrg,OU=WebServer"
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "CloudHSM Key Storage Provider"
KeyUsage = 0xf0
MachineKeySet = True
[EnhancedKeyUsageExtension]
```

```
OID=1.3.6.1.5.5.7.3.1
```

2. 使用 [Windows certreq 命令](#) 從您在上一個步驟中建立 IISCertRequest.inf 的檔案建立 CSR。以下範例會將 CSR 儲存至名為 IISCertRequest.csr 的檔案。如果您對憑證要求檔案使用不同的檔案名稱，請將 *IISCertRequest.inf* 取代為適當的檔案名稱。您可以選擇性地將 *IISCertRequest.csr* 取代為 CSR 檔案的不同檔案名稱。

```
C:\>certreq -new IISCertRequest.inf IISCertRequest.csr
```

```
CertReq: Request Created
```

IISCertRequest.csr 檔案包含您的 CSR。您需要此 CSR 才能取得已簽署的憑證。

### 使用用戶端 SDK 3 建立 CSR

1. 如果您尚未這麼做，請連接至您的 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 使用下列命令啟動 AWS CloudHSM 用戶端常駐程式。

#### Amazon Linux

```
$ sudo start cloudhsm-client
```

#### Amazon Linux 2

```
$ sudo service cloudhsm-client start
```

#### CentOS 7

```
$ sudo service cloudhsm-client start
```

#### CentOS 8

```
$ sudo service cloudhsm-client start
```

#### RHEL 7

```
$ sudo service cloudhsm-client start
```

## RHEL 8

```
$ sudo service cloudhsm-client start
```

## Ubuntu 16.04 LTS

```
$ sudo service cloudhsm-client start
```

## Ubuntu 18.04 LTS

```
$ sudo service cloudhsm-client start
```

## Windows

- 用於 Windows 用戶端 1.1.2+ :

```
C:\Program Files\Amazon\CloudHSM>net.exe start AWSCloudHSMClient
```

- 用於 Windows 用戶端 1.1.1 和更早版本 :

```
C:\Program Files\Amazon\CloudHSM>start "cloudhsm_client" cloudhsm_client.exe
C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_client.cfg
```

3. 在 Windows 伺服器上，使用文字編輯器來建立名為 IISCertRequest.inf 的憑證要求檔案。下列示範範例 IISCertRequest.inf 檔案的內容。如需您可在檔案中指定之區段、金鑰和數值的詳細資訊，請參閱 [Microsoft 文件](#)。請勿變更 ProviderName 值。

```
[Version]
Signature = "$Windows NT$"
[NewRequest]
Subject = "CN=example.com,C=US,ST=Washington,L=Seattle,O=ExampleOrg,OU=WebServer"
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "Cavium Key Storage Provider"
KeyUsage = 0xf0
MachineKeySet = True
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
```

4. 使用 [Windows certreq 命令](#) 從您在上一個步驟中建立 IISCertRequest.inf 的檔案建立 CSR。以下範例會將 CSR 儲存至名為 IISCertRequest.csr 的檔案。如果您對憑證要求檔案使用不同的檔案名稱，請將 *IISCertRequest.inf* 取代為適當的檔案名稱。您可以選擇性地將 *IISCertRequest.csr* 取代為 CSR 檔案的不同檔案名稱。

```
C:\>certreq -new IISCertRequest.inf IISCertRequest.csr
 SDK Version: 2.03

CertReq: Request Created
```

IISCertRequest.csr 檔案包含您的 CSR。您需要此 CSR 才能取得已簽署的憑證。

### 取得已簽署的憑證並匯入它

在生產環境中，您通常會使用憑證授權單位 (CA) 從 CSR 建立憑證。測試環境不需要 CA。如果您使用 CA，請將 CSR 檔案 (IISCertRequest.csr) 傳送至其中，並使用 CA 來建立已簽署的 SSL/TLS 憑證。

除了使用 CA，您也可以使用 [OpenSSL](#) 之類的工具來建立自簽憑證。

#### Warning

自簽憑證不受瀏覽器所信任，請勿用於生產環境。可以用於測試環境。

以下程序示範如何建立自簽憑證，並使用它來簽署 Web 伺服器 CSR。

### 建立自簽憑證

1. 使用下列 OpenSSL 命令來建立私有金鑰。您可以選擇性地將 *SelfSignedCA.key* 取代為檔案名稱，以包含您的私有金鑰。

```
openssl genrsa -aes256 -out SelfSignedCA.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for SelfSignedCA.key:
Verifying - Enter pass phrase for SelfSignedCA.key:
```

2. 使用以下 OpenSSL 命令，以使用您在上一個步驟中建立之私有金鑰來建立自簽憑證。這是互動式命令。請閱讀畫面上的指示，並依照提示操作。將 *SelfSignedCA.key* 取代為包含私有金鑰之檔案的名稱 (若不同的話)。您可以選擇性地將 *SelfSignedCA.crt* 取代為檔案名稱，以包含您的自簽憑證。

```
openssl req -new -x509 -days 365 -key SelfSignedCA.key -out SelfSignedCA.crt
Enter pass phrase for SelfSignedCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

### 使用自簽憑證來簽署您的 Web 伺服器 CSR

- 使用以下 OpenSSL 命令來使用私有金鑰和自簽憑證以簽署 CSR。將以下名稱取代為包含對應資料之檔案的名稱 (若不同的話)。
  - *IISCertRequest.csr* : 包含 Web 伺服器 CSR 之檔案的名稱
  - *SelfSignedCA.crt* : 包含自簽憑證之檔案的名稱
  - *SelfSignedCA.key* : 包含私有金鑰之檔案的名稱
  - *IISCert.crt* : 包含 Web 伺服器已簽署憑證之檔案的名稱

```
openssl x509 -req -days 365 -in IISCertRequest.csr \
 -CA SelfSignedCA.crt \
 -CAkey SelfSignedCA.key \
 -CAcreateserial \
 -out IISCert.crt

Signature ok
subject=/ST=IIS-HSM/L=IIS-HSM/OU=IIS-HSM/O=IIS-HSM/CN=IIS-HSM/C=IIS-HSM
```

```
Getting CA Private Key
Enter pass phrase for SelfSignedCA.key:
```

在完成前一個步驟之後，您有一個適用於 Web 伺服器的自簽憑證 (IISCert.crt) 和自簽憑證 (SelfSignedCA.crt)。當您具有這些檔案，請移至[步驟 3：設定 Web 伺服器](#)。

### 步驟 3：設定 Web 伺服器

更新您的 IIS 網站組態，來使用您在[前一個步驟](#)結束時建立的 HTTPS 憑證。這將完成針對 SSL/TLS 卸載搭配 AWS CloudHSM 設定您的 Windows Web 伺服器軟體 (IIS)。

如果已使用自簽憑證來簽署 CSR，則您必須先將自簽憑證匯入至 Windows 受信任的根認證授權單位。

將自簽憑證匯入至 Windows 受信任的根認證授權單位

1. 如果您尚未這麼做，請連接至您的 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 將自簽憑證複製到 Windows 伺服器。
3. 在 Windows 伺服器上，開啟 Control Panel (控制台)。
4. 針對 Search Control Panel (搜尋控制台)，輸入 **certificates**。然後選擇 Manage computer certificates (管理電腦憑證)。
5. 在憑證 - 本機電腦視窗中，按兩下信任的根憑證授權機構。
6. 用滑鼠右鍵按一下 Certificates (憑證)，然後選擇 All Tasks (所有工作)、Import (匯入)。
7. 在 Certificate Import Wizard (憑證匯入精靈) 中，選擇 Next (下一步)。
8. 選擇 Browse (瀏覽)，然後尋找並選取您的自簽憑證。如果您已遵循[本教學課程前一個步驟](#)中的指示來建立自簽憑證，則您的自簽憑證即名為 SelfSignedCA.crt。選擇 Open (開啟)。
9. 選擇下一步。
10. 對於 Certificate Store (憑證存放區)，選擇 Place all certificates in the following store (將所有憑證放入以下存放區)。然後，確保選取 Trusted Root Certification Authorities (受信任的根認證授權單位) 做為 Certificate store (憑證存放區)。
11. 選擇 Next (下一步)，然後選擇 Finish (完成)。

### 更新 IIS 網站組態

1. 如果您尚未這麼做，請連接至您的 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。

2. 啟動 AWS CloudHSM 用戶端協助程式。
3. 將 Web 伺服器的已簽署憑證 (這是您在[本教學課程前一個步驟](#)結束時建立的憑證) 複製到 Windows 伺服器。
4. 在 Windows Server 上，使用 [Windows certreq 命令](#) 來接受簽署的憑證，如下列範例所示。將 *IISCert.crt* 取代為包含 Web 伺服器的已簽署憑證之檔案的名稱。

```
C:\>certreq -accept IISCert.crt
SDK Version: 2.03
```

5. 在 Windows 伺服器上，啟動 Server Manager (伺服器管理員)。
6. 在 Server Manager (伺服器管理員) 儀表板右上角，選擇 Tools (工具)、Internet Information Services (IIS) Manager (Internet Information Services (IIS) 管理員)。
7. 在 Internet Information Services (IIS) Manager (Internet Information Services (IIS) 管理員) 視窗中，按兩下您的伺服器名稱。然後按兩下 Sites (網站)。選取網站。
8. 選取 SSL Settings (SSL 設定)。然後，在視窗右側選擇 Bindings (繫結)。
9. 在 Site Bindings (網站繫結) 視窗中，選擇 Add (新增)。
10. 對於 Type (類型)，選擇 https (https)。對於 SSL certificate (SSL 憑證)，選擇您在[本教學課程前一個步驟](#)結束時建立的 HTTPS 憑證。

#### Note

如果您在此次憑證繫結中遇到錯誤，請重新啟動您的伺服器並重試此步驟。

11. 選擇確定。

在更新網站組態之後，請移至[步驟 4：啟用 HTTPS 流量並驗證憑證](#)。

## 步驟 4：啟用 HTTPS 流量並驗證憑證

使用 設定 Web 伺服器進行 SSL/TLS 卸載後 AWS CloudHSM，請將 Web 伺服器執行個體新增至允許傳入 HTTPS 流量的安全群組。這可讓用戶端 (例如 Web 瀏覽器) 與 Web 伺服器建立 HTTPS 連線。然後建立與 Web 伺服器的 HTTPS 連線，並驗證其是否使用您為 SSL/TLS 卸載設定的憑證 AWS CloudHSM。

### 主題

- [啟用傳入 HTTPS 連線](#)
- [驗證 HTTPS 是否使用您已設定的憑證](#)

## 啟用傳入 HTTPS 連線

若要從用戶端 (例如 Web 瀏覽器) 連接到 Web 伺服器，請建立允許傳入 HTTPS 連接的安全群組。特別是應該允許連接埠 443 上的傳入 TCP 連線。將此安全群組指派到您的 Web 伺服器。

建立 HTTPS 的安全群組並將其指派至您的 Web 伺服器

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中選擇安全群組。
3. 選擇建立安全群組。
4. 對於 Create Security Group (建立安全群組)，執行下列動作：
  - a. 對於 Security group name (安全群組名稱)，輸入您要建立之安全群組的名稱。
  - b. (選用) 輸入您要建立之安全群組的描述。
  - c. 對於 VPC，選擇包含 Web 伺服器 Amazon EC2 執行個體的 VPC。
  - d. 選取 Add Rule (新增規則)。
  - e. 對於類型，從下拉式視窗中選取 HTTPS。
  - f. 對於來源，輸入來源位置。
  - g. 選擇建立安全群組。
5. 在導覽窗格中，選擇執行個體。
6. 選取 Web 伺服器執行個體旁的核取方塊。
7. 選取頁面頂端的動作下拉式選單。選取安全性，然後選取變更安全群組。
8. 對於關聯的安全群組，請選取搜尋方塊，然後選取您為 HTTPS 建立之安全群組。然後選擇新增安全群組。
9. 選取 Save (儲存)。

## 驗證 HTTPS 是否使用您已設定的憑證

將 Web 伺服器新增至安全群組後，您可以驗證 SSL/TLS 卸載是否使用您的自我簽署憑證。若要這樣做，您可以使用 Web 瀏覽器或使用 [OpenSSL s\\_client](#) 之類的工具。

## 使用 Web 瀏覽器驗證 SSL/TLS 卸載

1. 使用 Web 瀏覽器來透過伺服器的公有 DNS 名稱或 IP 地址連接到您的 Web 伺服器。請確定網址列中的 URL 開頭為 https://。例如 **https://ec2-52-14-212-67.us-east-2.compute.amazonaws.com/**。



**i** Tip

您可以使用 DNS 服務 (例如 Amazon Route 53)，將網站的網域名稱 (例如，https://www.example.com/) 路由到 Web 伺服器。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》或 DNS 服務文件中的[將流量路由到 Amazon EC2 執行個體](#)。

2. 使用您的 Web 瀏覽器來檢視 Web 伺服器憑證。如需詳細資訊，請參閱下列內容：

- 若為 Mozilla Firefox，請參閱 Mozilla 技術支援網站上的[檢視憑證](#)。
- 若為 Google Chrome，請參閱 Google Web 開發人員工具網站上的[了解安全問題](#)。

其他 Web 瀏覽器可能有類似的功能，可供您用來檢視 Web 伺服器憑證。

3. 確保 SSL/TLS 憑證是您設定 Web 伺服器所要使用的憑證。

使用 OpenSSL s\_client 來驗證 SSL/TLS 卸載

1. 執行以下 OpenSSL 命令來使用 HTTPS 連接至 Web 伺服器。以 Web 伺服器的公有 DNS 名稱或 IP 地址來取代 `<#####>`。

```
openssl s_client -connect <server name>:443
```

**i** Tip

您可以使用 DNS 服務 (例如 Amazon Route 53)，將網站的網域名稱 (例如，https://www.example.com/) 路由到 Web 伺服器。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》或 DNS 服務文件中的[將流量路由到 Amazon EC2 執行個體](#)。

2. 確保 SSL/TLS 憑證是您設定 Web 伺服器所要使用的憑證。

您現在有透過 HTTPS 而受到保護的網站。Web 伺服器的私有金鑰會存放在 AWS CloudHSM 叢集的 HSM 中。

若要新增負載平衡器，請參閱 [使用 Elastic Load Balancing for 新增負載平衡器 AWS CloudHSM \(選用\)](#)。

## 使用 Elastic Load Balancing for 新增負載平衡器 AWS CloudHSM (選用)

對一個 Web 伺服器設定 SSL/TLS 卸載之後，您可以建立更多個 Web 伺服器和 Elastic Load Balancing 負載平衡器，將 HTTPS 流量路由到 Web 伺服器。負載平衡器可以平衡兩個或更多個伺服器之間的流量，以降低個別 Web 伺服器的負載。還可以提高網站的可用性，因為負載平衡器會監控 Web 伺服器的運作狀態，只將流量路由到運作狀態良好的伺服器。如果 Web 伺服器故障，負載平衡器會自動停止路由流量。

### 主題

- [步驟 1. 針對第二個 Web 伺服器建立子網路](#)
- [步驟 2. 建立第二個 Web 伺服器](#)
- [步驟 3. 建立負載平衡器](#)

### 步驟 1. 針對第二個 Web 伺服器建立子網路

您必須先在包含現有 Web 伺服器和 AWS CloudHSM 叢集的相同 VPC 中建立新的子網路，才能建立另一個 Web 伺服器。

#### 建立新的子網路

1. 開啟 [Amazon VPC 主控台的子網路區段](#)。
2. 選擇 Create Subnet (建立子網路)。
3. 在 Create Subnet (建立子網路) 對話方塊中，執行下列動作：
  - a. 在 Name tag (名稱標籤) 中，輸入子網路的名稱。
  - b. 針對 VPC，選擇包含現有 Web 伺服器和 AWS CloudHSM 叢集的 AWS CloudHSM VPC。
  - c. 在 Availability Zone (可用區域) 中，選擇一個不是現有 Web 伺服器所在的可用區域。
  - d. 在 IPv4 CIDR 區塊中，輸入要用於子網路 CIDR 區塊。例如，輸入 **10.0.10.0/24**。
  - e. 選擇 Yes, Create (是，建立)。
4. 選取包含現有 Web 伺服器之公有子網路旁的核取方塊。這與您在先前步驟中建立的公有子網路不同。
5. 在內容窗格中，選擇路由表標籤。然後選擇路由表的連結。

## subnet-1f358d78 | CloudHSM Public subnet



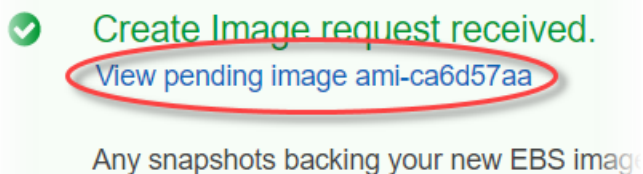
6. 選取路由表旁的核取方塊。
7. 選擇子網路關聯標籤。然後選擇 Edit (編輯)。
8. 選取您先前在此程序中建立之公用子網路旁的核取方塊。然後選擇 Save (儲存)。

## 步驟 2. 建立第二個 Web 伺服器

完成下列步驟，使用與現有 Web 伺服器相同的組態來建立第二個 Web 伺服器。

### 建立第二個 Web 伺服器

1. 開啟 Amazon EC2 主控台的[執行個體](#)區段。
2. 選取現有 Web 伺服器執行個體旁的核取方塊。
3. 依序選擇 Actions (動作)、Image (映像)、Create Image (建立映像)。
4. 在 Create Image (建立映像) 對話方塊中，執行下列動作：
  - a. 在 Image Name (映像名稱) 中，輸入映像的名稱。
  - b. 在 Image description (映像描述) 中，輸入映像的描述。
  - c. 選擇 Create Image (建立映像)。這個動作會重新啟動現有的 Web 伺服器。
  - d. 選擇檢視待處理映像 ami-**<AMI ID>**連結。



在狀態欄，注意您的映像狀態。當您的映像狀態是 available (可用) 時 (這可能需要幾分鐘)，請移至下一個步驟。

5. 在導覽窗格中，選擇執行個體。
6. 選取現有 Web 伺服器旁的核取方塊。
7. 選擇 Actions (動作)，然後選擇 Launch More Like This (啟動更多類似項目)。
8. 選擇 Edit AMI (編輯 AMI)。

#### ▼ AMI Details

Edit AMI



amzn-ami-hvm-2017.09.1.20171120-x86\_64-gp2 - ami-a51f27c5

Amazon Linux AMI 2017.09.1.20171120 x86\_64 HVM GP2

Root Device Type: ebs Virtualization type: hvm

9. 在左側導覽窗格中選擇我的 AMI。然後清除搜尋方塊中的文字。
10. 在 Web 伺服器映像旁，選擇 Select (選取)。
11. 選擇是，我想要繼續此 AMI (<####> - ami-<AMI ID>)。
12. 選擇下一步。
13. 選取執行個體類型，然後選擇 Next: Configure Instance Details (下一步：設定執行個體的詳細資訊)。
14. 在 Step 3: Configure Instance Details (步驟 3：設定執行個體詳細資訊) 中，執行下列動作：
  - a. 在 Network (網路) 中，選擇包含現有 Web 伺服器的 VPC。
  - b. 在 Subnet (子網路) 中，選擇您針對第二個 Web 伺服器建立的公有子網路。
  - c. 在 Auto-assign Public IP (自動指派公有 IP) 中，選擇 Enable (啟用)。
  - d. 依喜好變更剩餘的執行個體詳細資訊。然後選擇 Next: Add Storage (下一步：新增儲存體)。
15. 依喜好變更儲存設定。然後選擇 Next: Add Tags (下一步：新增標籤)。
16. 依喜好新增或編輯標籤。然後選擇 Next: Configure Security Group (下一步：設定安全群組)。
17. 在 Step 6: Configure Security Group (步驟 6：設定安全群組) 中，執行下列動作：
  - a. 在 Assign a security group (指派安全群組) 中，選擇 Select an existing security group (選取現有的安全群組)。
  - b. 選取名為 cloudhsm-####-sg 的安全群組旁邊的核取方塊。AWS CloudHSM 在 [建立叢集](#) 時代表您建立此安全群組。您必須選擇此安全群組，Web 伺服器執行個體才能連接到叢集內的 HSM。
  - c. 選取允許傳入 HTTPS 流量之安全群組旁的核取方塊。您 [先前已建立此安全群組](#)。

- d. (選用) 選取允許從您的網路傳入 SSH (Linux) 或 RDP (Windows) 流量之安全群組旁的核取方塊。也就是說，安全群組必須允許連接埠 22 (適用於 Linux 上的 SSH) 或連接埠 3389 (適用於 Windows 上的 RDP) 上的傳入 TCP 流量。否則，您無法連接到用戶端執行個體。如果您沒有像這樣的安全群組，則必須建立一個安全群組，並於稍後指派給用戶端執行個體。

選擇 Review and Launch (檢閱和啟動)。

18. 檢閱您的執行個體詳細資訊，然後選擇 Launch (啟動)。
19. 選擇是否以現有的金鑰對啟動執行個體、建立新的金鑰對，或在沒有金鑰對的情況下啟動執行個體。
  - 若要使用現有的金鑰對，請執行下列動作：
    1. 選擇 Choose an existing key pair (選擇現有金鑰對)。
    2. 在 Select a key pair (選取金鑰對) 中，選擇要使用的金鑰對。
    3. 選取我知道我能夠使用所選取的私有金鑰檔案 (<#####>.pem)，也知道如果沒有此檔案，我將無法登入我的執行個體) 旁的核取方塊。
  - 若要建立新的金鑰對，請執行下列動作：
    1. 選擇 Create a new key pair (建立新的金鑰對)。
    2. 在 Key pair name (金鑰對名稱) 中，輸入金鑰對名稱。
    3. 選擇 Download Key Pair (下載金鑰對)，然後將私有金鑰檔案儲存到安全又可存取的位置。

 Warning

此後，您就無法再次下載私有金鑰檔案。如果現在不下載私有金鑰檔案，您將無法存取用戶端執行個體。

- 若要在沒有金鑰對的情況下啟動執行個體，請執行下列動作：
  1. 選擇 Proceed without a key pair (不使用金鑰對而繼續)。
  2. 選取 I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI (我知道除非我已擁有內建於此 AMI 的密碼，否則我將無法連接至此執行個體) 旁的核取方塊。

選擇 Launch Instances (啟動執行個體)。

## 步驟 3。建立負載平衡器

完成以下步驟來建立 Elastic Load Balancing 負載平衡器，將 HTTPS 流量路由到您的 Web 伺服器。

### 建立負載平衡器

1. 開啟 Amazon EC2 主控台中的[負載平衡器](#)區段。
2. 選擇 Create Load Balancer (建立負載平衡器)。
3. 在 Network Load Balancer (網路負載平衡器) 區段中，選擇 Create (建立)。
4. 在 Step 1: Configure Load Balancer (步驟 1：設定負載平衡器) 中，執行下列動作：
  - a. 在 Name (名稱) 中，輸入您要建立之負載平衡器的名稱。
  - b. 在接聽程式區段中，將負載平衡器連接埠的值改為 **443**。
  - c. 在 Availability Zones (可用區域) 區段的 VPC 中，選擇包含您的 Web 伺服器的 VPC。
  - d. 在 Availability Zones (可用區域) 區段中，選擇包含您 Web 伺服器的子網路。
  - e. 選擇 Next: Configure Routing (下一步：設定路由)。
5. 在 Step 2: Configure Routing (步驟 2：設定路由) 中，執行下列動作：
  - a. 在 Name (名稱) 中，輸入您要建立之目標群組的名稱。
  - b. 將連接埠的值改為 **443**。
  - c. 選擇 Next: Register Targets (下一步：註冊目標)。
6. 在 Step 3: Register Targets (步驟 3：註冊目標) 中，執行下列動作：
  - a. 在執行個體區段中，選取您 Web 伺服器執行個體旁的核取方塊。然後選擇 Add to registered (新增至已註冊)。
  - b. 選擇下一步：檢閱。
7. 檢閱負載平衡器詳細資訊，然後選擇 Create (建立)。
8. 已成功建立負載平衡器時，請選擇 Close (關閉)。

當您完成前面的步驟後，Amazon EC2 主控台會顯示您的 Elastic Load Balancing 負載平衡器。

當負載平衡器的狀態為作用中，您可以確認負載平衡器是否在運作。也就是說，您可以確認負載平衡器是否將 HTTPS 流量傳送到 Web 伺服器 (使用 SSL/TLS 卸載搭配 AWS CloudHSM)。若要這樣做，您可以使用 Web 瀏覽器或 [OpenSSL s\\_client](#) 之類的工具。

## 使用 Web 瀏覽器來確認負載平衡器是否在運作

1. 在 Amazon EC2 主控台，尋找您剛建立之負載平衡器的 DNS 名稱。然後選取 DNS 名稱並將其複製。
2. 透過 Web 瀏覽器 (例如 Mozilla Firefox 或 Google Chrome)，使用負載平衡器的 DNS 名稱來連接到負載平衡器。請確定網址列中的 URL 開頭為 https://。

### Tip

您可以使用 DNS 服務 (例如 Amazon Route 53)，將網站的網域名稱 (例如，https://www.example.com/) 路由到 Web 伺服器。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》或 DNS 服務文件中的[將流量路由到 Amazon EC2 執行個體](#)。

3. 使用您的 Web 瀏覽器來檢視 Web 伺服器憑證。如需詳細資訊，請參閱下列內容：
  - 若為 Mozilla Firefox，請參閱 Mozilla 技術支援網站上的[檢視憑證](#)。
  - 若為 Google Chrome，請參閱 Google Web 開發人員工具網站上的[了解安全問題](#)。

其他 Web 瀏覽器可能有類似的功能，可供您用來檢視 Web 伺服器憑證。

4. 請確定憑證是您將 Web 伺服器設定為要使用的憑證。

## 使用 OpenSSL s\_client 來驗證負載平衡器是否在運作

1. 使用以下 OpenSSL 命令使用 HTTPS 連接負載平衡器。以負載平衡器的 DNS 名稱取代 **<DNS name>**。

```
openssl s_client -connect <DNS name>:443
```

### Tip

您可以使用 DNS 服務 (例如 Amazon Route 53)，將網站的網域名稱 (例如，https://www.example.com/) 路由到 Web 伺服器。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》或 DNS 服務文件中的[將流量路由到 Amazon EC2 執行個體](#)。

2. 請確定憑證是您將 Web 伺服器設定為要使用的憑證。



您現在有一個使用 HTTPS 保護的網站，其 Web 伺服器的私有金鑰存放在 AWS CloudHSM 叢集的 HSM 中。您的網站有兩個 Web 伺服器 and 一個負載平衡器，有助於提升效率和可用性。

## 使用 AWS CloudHSM 將 Windows Server 設定為憑證授權單位 (CA)

AWS CloudHSM 支援透過用戶端 SDK 3 和用戶端 SDK 5 將 Windows Server 設定為憑證授權機構 (CA)。使用這些工具的步驟會因您目前下載的用戶端 SDK 版本而異。下列各節提供每個 SDK 的資訊。

### 主題

- [使用用戶端 SDK 5 將 Windows Server 設定為憑證授權機構 \(CA\)](#)
- [使用用戶端 SDK 3 將 Windows Server 設定為憑證授權機構 \(CA\)](#)

## 使用用戶端 SDK 5 將 Windows Server 設定為憑證授權機構 (CA)

在公有金鑰基礎設施 (PKI) 中，憑證授權單位 (CA) 是發行數位憑證的受信任實體。這些數位憑證透過公有金鑰加密和數位簽章，將公有金鑰繫結至身分識別 (個人或組織)。若要操作 CA，您必須保護簽署 CA 所發行憑證的私有金鑰，以維護信任。您可以將私有金鑰儲存在 AWS CloudHSM 叢集中的 HSM 中，並使用 HSM 執行密碼編譯簽署作業。

在本教學課程中，您會使用 Windows Server 和 AWS CloudHSM 來設定 CA。您會在 Windows 伺服器上安裝適用於 Windows 的 AWS CloudHSM 用戶端軟體，然後將 Active Directory Certificate Services (AD CS) 角色新增到您的 Windows Server。設定此角色時，您可以使用 AWS CloudHSM 金鑰儲存提供者 (KSP) 在您的 AWS CloudHSM 叢集上建立和存放 CA 的私有金鑰。KSP 是將 Windows 伺服器連接到 AWS CloudHSM 叢集的橋接器。在最後一個步驟，您會使用 Windows Server CA 來簽署憑證簽署要求 (CSR)。

如需詳細資訊，請參閱下列主題：

### 主題

- [步驟 1：設定先決條件](#)
- [步驟 2：使用 建立 Windows Server CA AWS CloudHSM](#)
- [步驟 3：使用 Windows Server CA 簽署憑證簽署請求 \(CSR\) AWS CloudHSM](#)

## 步驟 1：設定先決條件

若要使用 將 Windows Server 設定為憑證授權機構 (CA) AWS CloudHSM，您需要下列項目：



- 具有至少一個 HSM 的作用中 AWS CloudHSM 叢集。
- 執行 Windows Server 作業系統並安裝 Windows AWS CloudHSM 用戶端軟體的 Amazon EC2 執行個體。本教學課程使用 Microsoft Windows Server 2016。
- 一位密碼編譯使用者 (CU)，擁有及管理 HSM 上的 CA 私有金鑰。

## 使用 設定 Windows Server CA 的先決條件 AWS CloudHSM

1. 完成「[開始使用](#)」中的步驟。當您啟動 Amazon EC2 用戶端時，請選擇 Windows Server AMI。本教學課程使用 Microsoft Windows Server 2016。當您完成這些步驟，便擁有至少包含一個 HSM 的作用中叢集。您也有執行 Windows Server 的 Amazon EC2 用戶端執行個體，其中已安裝 Windows 用戶端 AWS CloudHSM 軟體。
2. (選用) 在您的叢集中新增更多 HSM。如需詳細資訊，請參閱[將 HSM 新增至 AWS CloudHSM 叢集](#)。
3. 連接至您的用戶端執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
4. 使用[透過 CloudHSM CLI 管理 HSM 使用者](#)或使用 [CloudHSM Management Utility \(CMU\) 管理 HSM 使用者來建立加密使用者 \(CU\)](#)。保持追蹤 CU 使用者名稱和密碼。您需要它們來完成下一個步驟。
5. 使用您在先前步驟中建立的 CU 使用者名稱和密碼，[設定 HSM 的登入資料](#)。
6. 在步驟 5 中，如果您使用 Windows 認證管理員來設定 HSM 登入資料，請從 SysInternals 下載 [psexec.exe](#)，以 NT Authority\SYSTEM 的身分執行下列命令：

```
psexec.exe -s "C:\Program Files\Amazon\CloudHsm\tools\set_cloudhsm_credentials.exe"
--username <USERNAME> --password <PASSWORD>
```

以 HSM 憑證取代 <####> 和 <##>。

若要使用 建立 Windows Server CA AWS CloudHSM，請前往 [建立 Windows Server CA](#)。

## 步驟 2：使用 建立 Windows Server CA AWS CloudHSM

若要建立 Windows Server CA，您可以將 Active Directory Certificate Services (AD CS) 角色新增到您的 Windows Server。新增此角色時，您可以使用 AWS CloudHSM 金鑰儲存提供者 (KSP) 在您的 AWS CloudHSM 叢集上建立和存放 CA 的私有金鑰。

 Note

建立您的 Windows Server CA 時，您可以選擇建立根 CA 或次級 CA。您一般會根據組織的公有金鑰基礎設施和安全政策的設計進行此決策。本教學課程說明如何建立根 CA 以簡化程序。

將 AD CS 角色新增至您的 Windows Server 和建立 CA 的私有金鑰

1. 如果您尚未這麼做，請連接至您的 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 在 Windows 伺服器上，啟動 Server Manager (伺服器管理員)。
3. 在 Server Manager (伺服器管理員) 儀表板中，選擇 Add roles and features (新增角色和功能)。
4. 閱讀 Before you begin (開始之前) 資訊，然後選擇 Next (下一步)。
5. 對於 Installation Type (安裝類型)，選擇 Role-based or feature-based installation (角色型或功能型安裝)。然後選擇下一步。
6. 對於 Server Selection (伺服器選項)，選擇 Select a server from the server pool (從伺服器集區選取伺服器)。然後選擇下一步。
7. 對於 Server Roles (伺服器角色)，執行下列動作：
  - a. 選取 Active Directory Certificate Services (Active Directory Certificate Services)。
  - b. 對於 Add features that are required for Active Directory Certificate Services (新增 Active Directory Certificate Services 需要的功能)，選擇 Add Features (新增功能)。
  - c. 選擇 Next (下一步) 來完成伺服器角色的選取。
8. 對於 Features (功能)，接受預設值，然後選擇 Next (下一步)。
9. 對於 AD CS (AD CS)，執行下列動作：
  - a. 選擇下一步。
  - b. 選取 Certification Authority (憑證授權單位)，然後選擇 Next (下一步)。
10. 對於 Confirmation (確認)，閱讀確認資訊，然後選擇 Install (安裝)。請勿關閉視窗。
11. 選擇反白顯示的 Configure Active Directory Certificate Services on the destination server (在目的地伺服器上設定 Active Directory Certificate Services) 連結。
12. 對於 Credentials (登入資料)，驗證或變更顯示的登入資料。然後選擇下一步。
13. 對於 Role Services (角色服務)，選取 Certification Authority (憑證授權單位)。然後選擇下一步。
14. 對於 Setup Type (設定類型)，選取 Standalone CA (獨立 CA)。然後選擇下一步。

15. 對於 CA Type (CA 類型)，選取 Root CA (根 CA)。然後選擇下一步。

 Note

您可以根據公有金鑰基礎設施和組織安全政策的設計，選擇建立根 CA 或次級 CA。本教學課程說明如何建立根 CA 以簡化程序。

16. 對於 Private Key (私有金鑰)，選取 Create a new private key (建立新的私有金鑰)。然後選擇下一步。

17. 對於 Cryptography (加密法)，執行下列動作：

- a. 對於選取密碼編譯提供者，從功能表中選擇其中一個 CloudHSM 金鑰儲存提供者選項。這些是 AWS CloudHSM 金鑰儲存供應商。例如，您可以選擇 RSA#CloudHSM 金鑰儲存提供者。
- b. 對於 Key length (金鑰長度)，選擇其中一個金鑰長度選項。
- c. 對於 Select the hash algorithm for signing certificates issued by this CA (選取用於簽署這個 CA 發出之憑證的雜湊演算法)，請選擇其中一個雜湊演算法選項。

選擇下一步。

18. 對於 CA Name (CA 名稱)，執行下列動作：

- a. (選用) 編輯常用的名稱。
- b. (選用) 輸入辨別名稱尾碼。

選擇下一步。

19. 對於 Validity Period (有效期間)，以年、月、週或天指定時段。然後選擇下一步。

20. 對於 Certificate Database (憑證資料庫)，您可以接受預設值，或選擇變更資料庫和資料庫日誌的位置。然後選擇下一步。

21. 對於 Confirmation (確認)，檢閱您的 CA 的相關資訊，然後選擇 Configure (設定)。

22. 選擇 Close (關閉)，然後再次選擇 Close (關閉)。

您現在具有 Windows Server CA AWS CloudHSM。若要了解如何使用您的 CA 來簽署憑證簽署要求 (CSR)，請移至[簽署 CSR](#)。

### 步驟 3：使用 Windows Server CA 簽署憑證簽署請求 (CSR) AWS CloudHSM

您可以使用 Windows Server CA 搭配 AWS CloudHSM 簽署憑證簽署請求 (CSR)。若要完成以下步驟，您需要有效的 CSR。有幾種方式可建立 CSR，包括：

- 使用 OpenSSL
- 使用 Windows Server Internet Information Services (IIS) Manager
- 在 Microsoft Management Console 中使用憑證嵌入式管理單元
- 在 Windows 上使用 certreq 命令列公用程式

建立 CSR 的步驟已超出本教學課程的範圍。當您有 CSR 時，您可以向 Windows Server CA 簽署此 CSR。

#### 向 Windows Server CA 簽署 CSR

1. 如果您尚未這麼做，請連接至您的 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 在 Windows 伺服器上，啟動 Server Manager (伺服器管理員)。
3. 在伺服器管理員儀表板右上角，選擇 Tools (工具)、Certification Authority (憑證授權單位)。
4. 在 Certification Authority (憑證授權單位) 視窗中，選擇您的電腦名稱。
5. 從 Action (執行) 功能表中，選擇 All Tasks (所有工作)、Submit new request (提交新要求)。
6. 選取您的 CSR 檔案，然後選擇 Open (開啟)。
7. 在 Certification Authority (憑證授權單位) 視窗中，按兩下 Pending Requests (擱置要求)。
8. 選取擱置要求。然後，從 Action (執行) 功能表中，選擇 All Tasks (所有工作)、Issue (發行)。
9. 在 Certification Authority (憑證授權單位) 視窗中，按兩下 Issued Requests (已發出的要求)，以檢視已簽署的憑證。
10. (選用) 若要將已簽署的憑證匯出到檔案，請完成以下步驟：
  - a. 在 Certification Authority (憑證授權單位) 視窗中，按兩下憑證。
  - b. 選擇 Details (詳細資料) 標籤，然後選擇 Copy to File (複製到檔案)。
  - c. 依照憑證匯出精靈中的指示進行。

您現在擁有 Windows Server CA AWS CloudHSM，以及 Windows Server CA 簽署的有效憑證。

## 使用用戶端 SDK 3 將 Windows Server 設定為憑證授權機構 (CA)

在公有金鑰基礎設施 (PKI) 中，憑證授權單位 (CA) 是發行數位憑證的受信任實體。這些數位憑證透過公有金鑰加密和數位簽章，將公有金鑰繫結至身分識別 (個人或組織)。若要操作 CA，您必須保護簽署 CA 所發行憑證的私有金鑰，以維護信任。您可以將私有金鑰儲存在 AWS CloudHSM 叢集中的 HSM 中，並使用 HSM 執行密碼編譯簽署作業。

在本教學課程中，您會使用 Windows Server 和 AWS CloudHSM 來設定 CA。您會在 Windows 伺服器上安裝適用於 Windows 的 AWS CloudHSM 用戶端軟體，然後將 Active Directory Certificate Services (AD CS) 角色新增到您的 Windows Server。設定此角色時，您可以使用 AWS CloudHSM 金鑰儲存提供者 (KSP) 在您的 AWS CloudHSM 叢集上建立和存放 CA 的私有金鑰。KSP 是將 Windows 伺服器連接到 AWS CloudHSM 叢集的橋接器。在最後一個步驟，您會使用 Windows Server CA 來簽署憑證簽署要求 (CSR)。

如需詳細資訊，請參閱下列主題：

### 主題

- [步驟 1：設定先決條件](#)
- [步驟 2：使用 建立 Windows Server CA AWS CloudHSM](#)
- [步驟 3：使用 Windows Server CA 簽署憑證簽署請求 \(CSR\) AWS CloudHSM](#)

### 步驟 1：設定先決條件

若要使用 將 Windows Server 設定為憑證授權機構 (CA) AWS CloudHSM，您需要下列項目：

- 具有至少一個 HSM 的作用中 AWS CloudHSM 叢集。
- 執行 Windows Server 作業系統並安裝 Windows AWS CloudHSM 用戶端軟體的 Amazon EC2 執行個體。本教學課程使用 Microsoft Windows Server 2016。
- 一位密碼編譯使用者 (CU)，擁有及管理 HSM 上的 CA 私有金鑰。

### 使用 設定 Windows Server CA 的先決條件 AWS CloudHSM

1. 完成「[開始使用](#)」中的步驟。當您啟動 Amazon EC2 用戶端時，請選擇 Windows Server AMI。本教學課程使用 Microsoft Windows Server 2016。當您完成這些步驟，便擁有至少包含一個 HSM 的作用中叢集。您也有執行 Windows Server 的 Amazon EC2 用戶端執行個體，其中已安裝 Windows 用戶端 AWS CloudHSM 軟體。

2. (選用) 在您的叢集中新增更多 HSM。如需詳細資訊，請參閱[將 HSM 新增至 AWS CloudHSM 叢集](#)。
3. 連接至您的用戶端執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
4. 使用[透過 CloudHSM CLI 管理 HSM 使用者](#)或使用 [CloudHSM Management Utility \(CMU\) 管理 HSM 使用者來建立加密使用者 \(CU\)](#)。保持追蹤 CU 使用者名稱和密碼。您需要它們來完成下一個步驟。
5. 使用您在先前步驟中建立的 CU 使用者名稱和密碼，[設定 HSM 的登入資料](#)。
6. 在步驟 5 中，如果您使用 Windows 認證管理員來設定 HSM 登入資料，請從 SysInternals 下載 [psexec.exe](#)，以 NT Authority\SYSTEM 的身分執行下列命令：

```
psexec.exe -s "C:\Program Files\Amazon\CloudHsm\tools\nset_cloudhsm_credentials.exe" --username <USERNAME> --password <PASSWORD>
```

以 HSM 憑證取代 <#####> 和 <##>。

若要使用 建立 Windows Server CA AWS CloudHSM，請前往 [建立 Windows Server CA](#)。

## 步驟 2：使用 建立 Windows Server CA AWS CloudHSM

若要建立 Windows Server CA，您可以將 Active Directory Certificate Services (AD CS) 角色新增到您的 Windows Server。新增此角色時，您可以使用 AWS CloudHSM 金鑰儲存提供者 (KSP) 在您的 AWS CloudHSM 叢集上建立和存放 CA 的私有金鑰。

### Note

建立您的 Windows Server CA 時，您可以選擇建立根 CA 或次級 CA。您一般會根據組織的公有金鑰基礎設施和安全政策的設計進行此決策。本教學課程說明如何建立根 CA 以簡化程序。

將 AD CS 角色新增至您的 Windows Server 和建立 CA 的私有金鑰

1. 如果您尚未這麼做，請連接至您的 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 在 Windows 伺服器上，啟動 Server Manager (伺服器管理員)。
3. 在 Server Manager (伺服器管理員) 儀表板中，選擇 Add roles and features (新增角色和功能)。



4. 閱讀 Before you begin (開始之前) 資訊，然後選擇 Next (下一步)。
5. 對於 Installation Type (安裝類型)，選擇 Role-based or feature-based installation (角色型或功能型安裝)。然後選擇下一步。
6. 對於 Server Selection (伺服器選項)，選擇 Select a server from the server pool (從伺服器集區選取伺服器)。然後選擇下一步。
7. 對於 Server Roles (伺服器角色)，執行下列動作：
  - a. 選取 Active Directory Certificate Services (Active Directory Certificate Services)。
  - b. 對於 Add features that are required for Active Directory Certificate Services (新增 Active Directory Certificate Services 需要的功能，選擇 Add Features (新增功能)。
  - c. 選擇 Next (下一步) 來完成伺服器角色的選取。
8. 對於 Features (功能)，接受預設值，然後選擇 Next (下一步)。
9. 對於 AD CS (AD CS)，執行下列動作：
  - a. 選擇下一步。
  - b. 選取 Certification Authority (憑證授權單位)，然後選擇 Next (下一步)。
10. 對於 Confirmation (確認)，閱讀確認資訊，然後選擇 Install (安裝)。請勿關閉視窗。
11. 選擇反白顯示的 Configure Active Directory Certificate Services on the destination server (在目的地伺服器上設定 Active Directory Certificate Services) 連結。
12. 對於 Credentials (登入資料)，驗證或變更顯示的登入資料。然後選擇下一步。
13. 對於 Role Services (角色服務)，選取 Certification Authority (憑證授權單位)。然後選擇下一步。
14. 對於 Setup Type (設定類型)，選取 Standalone CA (獨立 CA)。然後選擇下一步。
15. 對於 CA Type (CA 類型)，選取 Root CA (根 CA)。然後選擇下一步。

 Note

您可以根據公有金鑰基礎設施和組織安全政策的設計，選擇建立根 CA 或次級 CA。本教學課程說明如何建立根 CA 以簡化程序。

16. 對於 Private Key (私有金鑰)，選取 Create a new private key (建立新的私有金鑰)。然後選擇下一步。
17. 對於 Cryptography (加密法)，執行下列動作：
  - a. 對於 Select a cryptographic provider (選取密碼編譯供應商)，從功能表選擇其中一個 Cavium Key Storage Provider (Cavium 金鑰儲存供應商) 選項。這些是 AWS CloudHSM 金鑰儲存供

應商。例如，您可以選擇 RSA#Cavium Key Storage Provider (RSA#Cavium 金鑰儲存供應商)。

- b. 對於 Key length (金鑰長度)，選擇其中一個金鑰長度選項。
- c. 對於 Select the hash algorithm for signing certificates issued by this CA (選取用於簽署這個 CA 發出之憑證的雜湊演算法)，請選擇其中一個雜湊演算法選項。

選擇下一步。

18. 對於 CA Name (CA 名稱)，執行下列動作：

- a. (選用) 編輯常用的名稱。
- b. (選用) 輸入辨別名稱尾碼。

選擇下一步。

19. 對於 Validity Period (有效期間)，以年、月、週或天指定時段。然後選擇下一步。
20. 對於 Certificate Database (憑證資料庫)，您可以接受預設值，或選擇變更資料庫和資料庫日誌的位置。然後選擇下一步。
21. 對於 Confirmation (確認)，檢閱您的 CA 的相關資訊，然後選擇 Configure (設定)。
22. 選擇 Close (關閉)，然後再次選擇 Close (關閉)。

您現在具有 Windows Server CA AWS CloudHSM。若要了解如何使用您的 CA 來簽署憑證簽署要求 (CSR)，請移至[簽署 CSR](#)。

### 步驟 3：使用 Windows Server CA 簽署憑證簽署請求 (CSR) AWS CloudHSM

您可以使用 Windows Server CA 搭配 AWS CloudHSM 簽署憑證簽署請求 (CSR)。若要完成以下步驟，您需要有效的 CSR。有幾種方式可建立 CSR，包括：

- 使用 OpenSSL
- 使用 Windows Server Internet Information Services (IIS) Manager
- 在 Microsoft Management Console 中使用憑證嵌入式管理單元
- 在 Windows 上使用 certreq 命令列公用程式

建立 CSR 的步驟已超出本教學課程的範圍。當您有 CSR 時，您可以向 Windows Server CA 簽署此 CSR。



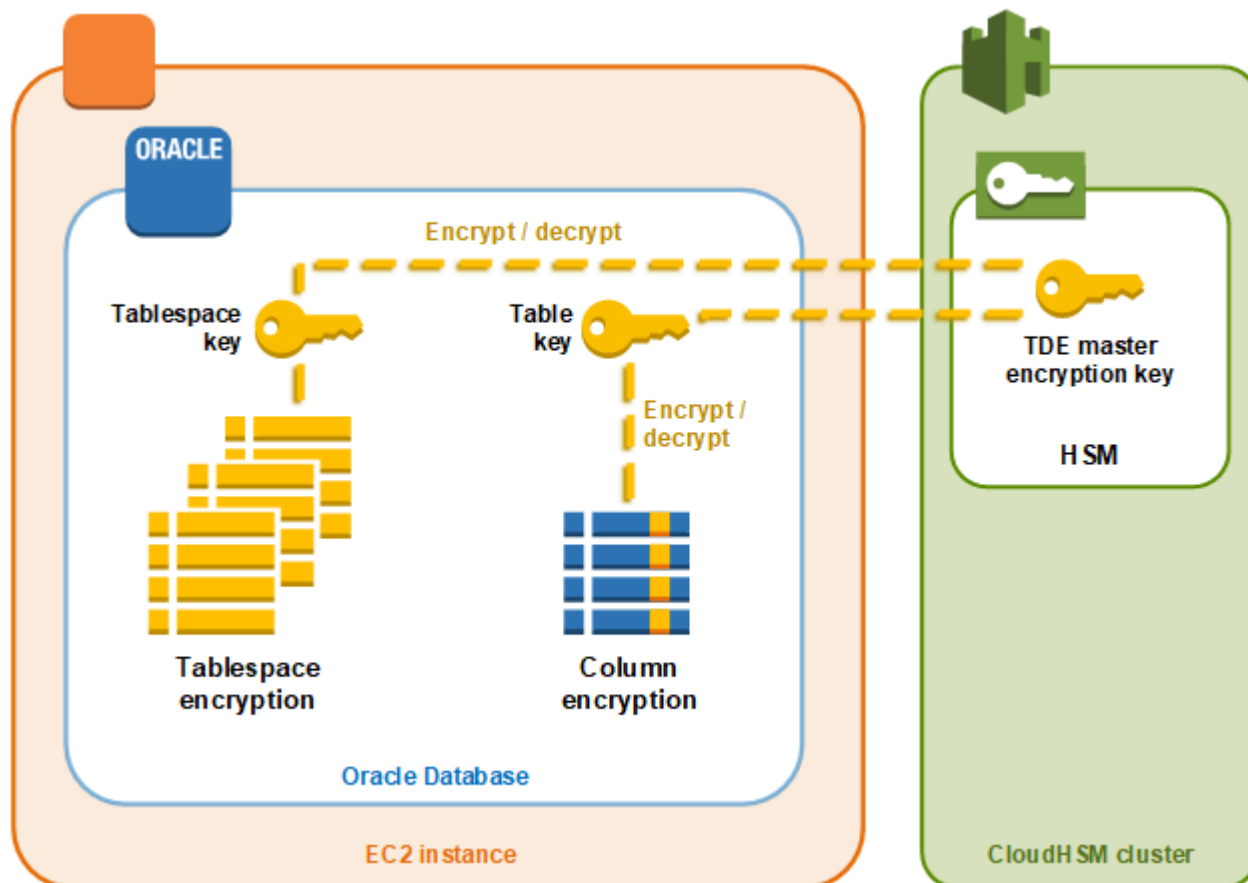
## 向 Windows Server CA 簽署 CSR

1. 如果您尚未這麼做，請連接至您的 Windows 伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 在 Windows 伺服器上，啟動 Server Manager (伺服器管理員)。
3. 在伺服器管理員儀表板右上角，選擇 Tools (工具)、Certification Authority (憑證授權單位)。
4. 在 Certification Authority (憑證授權單位) 視窗中，選擇您的電腦名稱。
5. 從 Action (執行) 功能表中，選擇 All Tasks (所有工作)、Submit new request (提交新要求)。
6. 選取您的 CSR 檔案，然後選擇 Open (開啟)。
7. 在 Certification Authority (憑證授權單位) 視窗中，按兩下 Pending Requests (擱置要求)。
8. 選取擱置要求。然後，從 Action (執行) 功能表中，選擇 All Tasks (所有工作)、Issue (發行)。
9. 在 Certification Authority (憑證授權單位) 視窗中，按兩下 Issued Requests (已發出的要求)，以檢視已簽署的憑證。
10. (選用) 若要將已簽署的憑證匯出到檔案，請完成以下步驟：
  - a. 在 Certification Authority (憑證授權單位) 視窗中，按兩下憑證。
  - b. 選擇 Details (詳細資料) 標籤，然後選擇 Copy to File (複製到檔案)。
  - c. 依照憑證匯出精靈中的指示進行。

您現在擁有 Windows Server CA AWS CloudHSM，以及 Windows Server CA 簽署的有效憑證。

## Oracle 資料庫的透明資料加密 (TDE) 搭配 AWS CloudHSM

透明資料加密 (TDE) 可用來加密資料庫檔案。使用 TDE，資料庫軟體將資料存儲在磁盤上之前對其進行加密。資料庫資料表資料欄或資料表空間中的資料會使用資料表金鑰或資料表空間金鑰加密。Oracle 的資料庫軟體的某些版本提供 TDE。在 Oracle TDE 中，這些金鑰會使用 TDE 主加密金鑰加密。您可以將 TDE 主加密金鑰存放在 AWS CloudHSM 叢集的 HSMs 中，以達到更高的安全性。



在這個解決方案中，您使用在 Amazon EC2 執行個體上安裝的 Oracle 資料庫。Oracle 資料庫會與[適用於 PKCS #11 的 AWS CloudHSM 軟體程式庫](#)整合，可將 TDE 主金鑰存放在您叢集中的 HSM。

#### ⚠ Important

- 建議在 Amazon EC2 執行個體上安裝 Oracle 資料庫。

執行下列步驟以完成 Oracle TDE 與 AWS CloudHSM 的整合。

#### 主題

- [步驟 1. 設定先決條件](#)
- [步驟 3：產生 Oracle TDE 主加密金鑰](#)

## 步驟 1. 設定先決條件

若要完成 Oracle TDE 與 的整合 AWS CloudHSM，您需要下列項目：

- 具有至少一個 HSM 的作用中 AWS CloudHSM 叢集。
- 執行 Amazon Linux 作業系統的 Amazon EC2 執行個體，其中已安裝下列軟體：
  - AWS CloudHSM 用戶端和命令列工具。
  - PKCS #11 AWS CloudHSM 的軟體程式庫。
  - Oracle Database. AWS CloudHSM support Oracle TDE 整合。用戶端 SDK 5.6 及更高版本支援適用於 Oracle 資料庫 19c 的 Oracle TDE。客戶端 SDK 3 支援適用於 Oracle 資料庫 11g 和 12c 版的 Oracle TDE。
- 加密使用者 (CU)，擁有及管理叢集中 HSM 上的 TDE 主加密金鑰。

完成以下步驟來設定所有先決條件。

#### 設定 Oracle TDE 與 整合的先決條件 AWS CloudHSM

1. 完成「[開始使用](#)」中的步驟。完成之後，您將擁有一個作用中叢集，且其中有一個 HSM。您也會有一個執行 Amazon Linux 作業系統的 Amazon EC2 執行個體。AWS CloudHSM 用戶端和命令列工具也會進行安裝和設定。
2. (選用) 在您的叢集中新增更多 HSM。如需詳細資訊，請參閱[將 HSM 新增至 AWS CloudHSM 叢集](#)。
3. 連接到 Amazon EC2 用戶端執行個體，並執行下列動作：
  - a. [安裝 PKCS #11 AWS CloudHSM 的軟體程式庫](#)。
  - b. 安裝 Oracle 資料庫。如需詳細資訊，請參閱 [Oracle 資料庫文件](#)。用戶端 SDK 5.6 及更高版本支援適用於 Oracle 資料庫 19c 的 Oracle TDE。客戶端 SDK 3 支援適用於 Oracle 資料庫 11g 和 12c 版的 Oracle TDE。
  - c. 使用 cloudhsm\_mgmt\_util 命令列工具來在您的叢集上建立加密使用者 (CU)。如需關於建立 CU 的詳細資訊，請參閱[如何使用 CMU 管理 HSM 使用者](#)和 [HSM 使用者](#)。

## 步驟 3：產生 Oracle TDE 主加密金鑰

若要在叢集中 HSM 上產生 Oracle TDE 主金鑰，請完成以下程序中的步驟。

#### 產生主金鑰

1. 使用下列命令開啟 Oracle SQL\*Plus。當系統提示時，請輸入您安裝 Oracle 資料庫時所設定的系統密碼。

```
sqlplus / as sysdba
```

**Note**

對於用戶端 SDK 3，每次產生主金鑰時，都必須設定 `CLOUDHSM_IGNORE_CKA_MODIFIABLE_FALSE` 環境變數。此變數僅用於產生主金鑰。如需詳細資訊，請參閱[整合第三方應用程式的已知問題](#)中的「問題：Oracle 在產生主金鑰期間設定 PKCS #11 屬性 `CKA_MODIFIABLE`，但 HSM 不支援此屬性」。

- 執行 SQL 陳述式來建立主加密金鑰，如下列範例所示。請使用與 Oracle 資料庫版本對應的陳述式。以加密使用者 (CU) 的使用者名稱取代 `<CU #####>`。以 CU 密碼取代 `<##>`。

**Important**

只執行一次下列命令。每次執行此命令都會建立新的主加密金鑰。

- 若為 Oracle 資料庫第 11 版，請執行下列 SQL 陳述式。

```
SQL> alter system set encryption key identified by "<CU user name>:<password>";
```

- 若為 Oracle 資料庫第 12 版和第 19c 版，請執行下列 SQL 陳述式。

```
SQL> administer key management set key identified by "<CU user name>:<password>";
```

如果回應是 `System altered` 或 `keystore altered`，則表示您已成功產生和設定 Oracle TDE 的主金鑰。

- (選用) 執行以下命令來驗證 Oracle 錢包的狀態。

```
SQL> select * from v$encryption_wallet;
```

如果錢包未開啟，請使用下列其中一個命令來開啟。以加密使用者 (CU) 的名稱取代 `<CU #####>`。以 CU 密碼取代 `<##>`。

- 若為 Oracle 11，請執行下列命令來開啟錢包。

```
SQL> alter system set encryption wallet open identified by "<CU user
name>:<password>";
```

若要手動關閉錢包，請執行下列命令。

```
SQL> alter system set encryption wallet close identified by "<CU user
name>:<password>";
```

- 若為 Oracle 12 和 Oracle 19c，請執行下列命令來開啟錢包。

```
SQL> administer key management set keystore open identified by "<CU user
name>:<password>";
```

若要手動關閉錢包，請執行下列命令。

```
SQL> administer key management set keystore close identified by "<CU user
name>:<password>";
```

## 搭配使用 Microsoft SignTool AWS CloudHSM 來簽署檔案

AWS CloudHSM 支援透過用戶端 SDK 3 和用戶端 SDK 5 使用 Microsoft Signtool 簽署檔案。使用這些工具的步驟會因您目前下載的用戶端 SDK 版本而異。下列各節提供每個 SDK 的資訊。

### 主題

- [使用 Microsoft SignTool 搭配用戶端 SDK 5 來簽署檔案](#)
- [使用 Microsoft SignTool 搭配用戶端 SDK 3 來簽署檔案](#)

## 使用 Microsoft SignTool 搭配用戶端 SDK 5 來簽署檔案

在加密和公開金鑰基礎設施 (PKI) 中，數位簽章是用來確認資料已由可信任的實體傳送。此簽章也代表傳輸中的資料未經過篡改。簽章是一種由寄件者的私有金鑰產生的加密雜湊。接收者可以使用寄件者的公有金鑰解密其雜湊簽章，以驗證資料完整性。因此，應該由寄件者負責維護數位憑證。數位憑證代表寄件者的私有金鑰擁有權，並可將解密所需的公有金鑰提供給接收者。只要私有金鑰由寄件者擁有，就可以信任簽章。AWS CloudHSM 提供安全的 FIPS 140-2 第 3 級驗證硬體，讓您使用獨佔的單一租用戶存取來保護這些金鑰。

許多組織使用 Microsoft SignTool，這是一種命令列工具，可簽署、驗證檔案，並加入時間戳記，以簡化程式碼簽署程序。您可以使用 AWS CloudHSM 安全地存放您的金鑰對，直到 SignTool 需要這些金鑰對為止，從而為簽署資料建立易於自動化的工作流程。

下列主題提供如何使用 SignTool 搭配的概觀 AWS CloudHSM。

## 主題

- [步驟 1：設定先決條件](#)
- [步驟 2：建立簽署憑證](#)
- [步驟 3：簽署檔案](#)

## 步驟 1：設定先決條件

若要搭配使用 Microsoft SignTool AWS CloudHSM，您需要下列項目：

- 執行 Windows 作業系統的 Amazon EC2 用戶端執行個體。
- 憑證授權單位 (CA)；不論是自己維護，或由第三方供應商建立。
- 與 EC2 執行個體位於相同虛擬公有雲端 (VPC) 中的作用中 AWS CloudHSM 叢集。叢集必須至少包含一個 HSM。
- 在 AWS CloudHSM 叢集中擁有和管理金鑰的加密使用者 (CU)。
- 未簽署的檔案或可執行檔。
- Microsoft Windows 軟體開發套件 (SDK)。

設定 AWS CloudHSM 搭配 Windows SignTool 使用的先決條件

1. 請依照本指南中[入門](#)一節的說明，來啟動 Windows EC2 執行個體與 AWS CloudHSM 叢集。
2. 如果您想要託管自己的 Windows Server CA，請遵循將 [Windows Server 設定為憑證授權單位 AWS CloudHSM](#) 中的步驟 1 和 2。否則，請繼續使用您公開信任的第三方 CA。
3. 在您的 Windows EC2 執行個體上，下載並安裝下列其中一個版本的 Microsoft Windows 軟體開發套件：
  - [Microsoft Windows SDK 10](#)
  - [Microsoft Windows SDK 8.1](#)
  - [Microsoft Windows SDK 7](#)

SignTool 可執行檔是 Windows SDK Signing Tools for Desktop Apps 安裝功能的一部分。如果您不需要其他功能，可以省略其安裝。預設安裝位置為：

```
C:\Program Files (x86)\Windows Kits\<SDK version>\bin\<version number>\<CPU architecture>\signtool.exe
```

您現在可以使用 Microsoft Windows SDK、AWS CloudHSM 叢集和 CA 來[建立簽署憑證](#)。

## 步驟 2：建立簽署憑證

現在您已將 Windows SDK 下載到您的 EC2 執行個體上，即可使用它來產生憑證簽署請求 (CSR)。CSR 是未簽署的憑證，最終會傳遞到您的 CA 以進行簽署。在這個範例中，我們使用 Windows SDK 隨附的 certreq 可執行檔，來產生 CSR。

使用 **certreq** 可執行檔來產生 CSR

1. 如果您尚未連線至 Windows EC2 執行個體，請先進行連線。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 建立名為 request.inf 的檔案，其中包含以下各行。將 Subject 資訊取代為您組織的相關資訊。如需每個參數的說明，請參閱 [Microsoft 文件](#)。

```
[Version]
Signature= $Windows NT$
[NewRequest]
Subject = "C=<Country>,CN=<www.website.com>,O=<Organization>,OU=<Organizational-Unit>,L=<City>,S=<State>"
RequestType=PKCS10
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "CloudHSM Key Storage Provider"
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE"
MachineKeySet = True
Exportable = False
```

3. 執行 certreq.exe。在此範例中，我們將 CSR 儲存為 request.csr。

```
certreq.exe -new request.inf request.csr
```

在內部，會在您的 AWS CloudHSM 叢集上產生新的金鑰對，並使用該對的私有金鑰來建立 CSR。

4. 將 CSR 提交給您的 CA。如果您使用的是 Windows Server CA，請依照下列步驟進行：
  - a. 輸入下列命令以開啟 CA 工具：

```
certsrv.msc
```

- b. 在新的視窗中，以滑鼠右鍵按一下 CA 伺服器的名稱。選擇 All Tasks (所有任務)，然後選擇 Submit new request (提交新請求)。
  - c. 導覽至 request.csr 的位置，然後選擇 Open (開啟)。
  - d. 展開伺服器 CA 功能表，導覽至待處理的請求資料夾。用滑鼠右鍵按一下您剛建立的請求，並在 All Tasks (所有任務) 下方選擇 Issue (發行)。
  - e. 現在，導覽至 Issued Certificates (發行的憑證) 資料夾 (位於 Pending Requests (待處理的請求) 資料夾上方)。
  - f. 選擇 Open (開啟) 以檢視憑證，然後選擇 Details (詳細資訊) 標籤。
  - g. 選擇 Copy to File (複製到檔案) 來啟動 [憑證匯出精靈]。將 DER 編碼的 X.509 檔案以 signedCertificate.cer 名稱儲存到安全的位置。
  - h. 結束 CA 工具，並使用下列命令，將憑證檔案移至 Windows 的個人憑證存放區中。其他應用程式即可使用此憑證。

```
certreq.exe -accept signedCertificate.cer
```

您現在可以使用匯入的憑證來[簽署檔案](#)。

### 步驟 3：簽署檔案

您現在可以開始使用 SignTool 和匯入的憑證，來簽署您的範例檔案。若要執行此作業，您需要知道憑證的 SHA-1 雜湊或「指紋」。指紋是用來確保 SignTool 只使用經過 AWS CloudHSM 驗證的憑證。在這個範例中，我們使用 PowerShell 取得憑證的雜湊。您也可以使用 CA 的 GUI 或 Windows 軟體開發套件的 certutil 可執行檔。

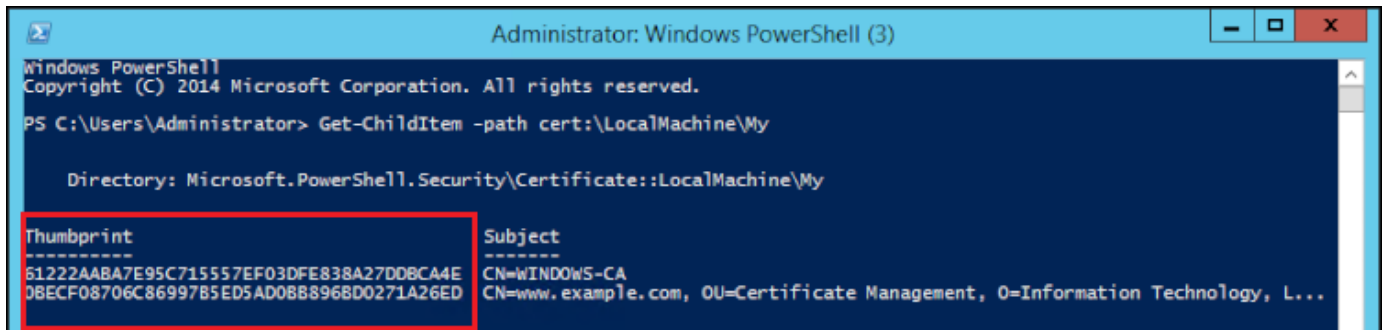
取得憑證的指紋，並使用它來簽署檔案

1. 以管理員身分開啟 PowerShell，並執行下列命令：



```
Get-ChildItem -path cert:\LocalMachine\My
```

複製傳回的 Thumbprint。



```

Administrator: Windows PowerShell (3)
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ChildItem -path cert:\LocalMachine\My

Directory: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

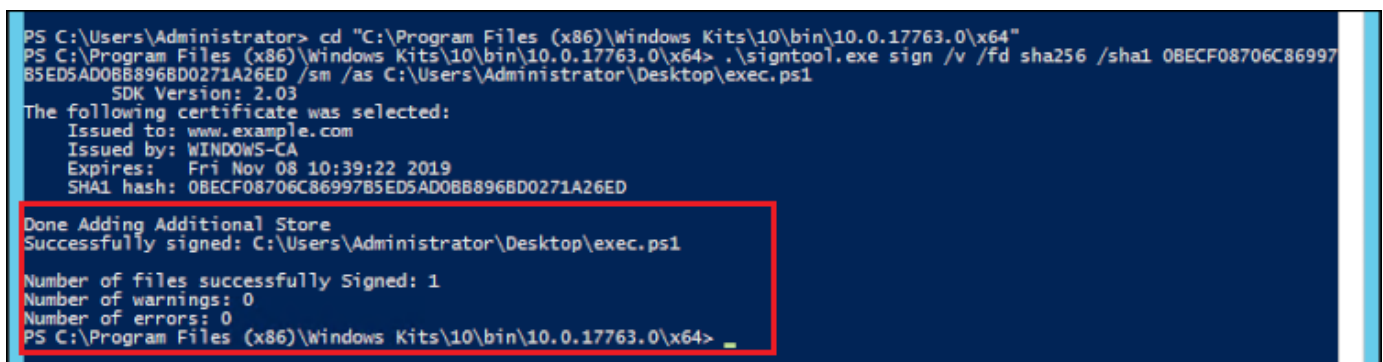
Thumbprint Subject

61222AABA7E95C715557EF03DFE838A27D08CA4E CN=WINDOWS-CA
0BECF08706C86997B5ED5AD0B88968D0271A26ED CN=www.example.com, OU=Certificate Management, O=Information Technology, L...

```

2. 導覽至 PowerShell 中包含 SignTool.exe 的目錄。預設位置為 C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64。
3. 最後，執行以下命令簽署您的檔案。如果命令成功，PowerShell 會傳回成功訊息。

```
signtool.exe sign /v /fd sha256 /sha1 <thumbprint> /sm C:\Users\Administrator\
\Desktop\<test>.ps1
```



```

PS C:\Users\Administrator> cd "C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64"
PS C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64> .\signtool.exe sign /v /fd sha256 /sha1 0BECF08706C86997
B5ED5AD0B88968D0271A26ED /sm /as C:\Users\Administrator\Desktop\exec.ps1
 SDK Version: 2.03
The following certificate was selected:
 Issued to: www.example.com
 Issued by: WINDOWS-CA
 Expires: Fri Nov 08 10:39:22 2019
 SHA1 hash: 0BECF08706C86997B5ED5AD0B88968D0271A26ED

Done Adding Additional Store
Successfully signed: C:\Users\Administrator\Desktop\exec.ps1

Number of files successfully Signed: 1
Number of warnings: 0
Number of errors: 0
PS C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64>

```

4. (選用) 若要驗證檔案上的簽章，請使用下列命令：

```
signtool.exe verify /v /pa C:\Users\Administrator\Desktop\<test>.ps1
```

## 使用 Microsoft SignTool 搭配用戶端 SDK 3 來簽署檔案

在加密和公開金鑰基礎設施 (PKI) 中，數位簽章是用來確認資料已由可信任的實體傳送。此簽章也代表傳輸中的資料未經過篡改。簽章是一種由寄件者的私有金鑰產生的加密雜湊。接收者可以使用寄件者的公有金鑰解密其雜湊簽章，以驗證資料完整性。因此，應該由寄件者負責維護數位憑證。數位憑證代表

寄件者的私有金鑰擁有權，並可將解密所需的公有金鑰提供給接收者。只要私有金鑰由寄件者擁有，就可以信任簽章。AWS CloudHSM 提供安全的 FIPS 140-2 第 3 級驗證硬體，讓您使用獨佔的單一租用戶存取來保護這些金鑰。

許多組織使用 Microsoft SignTool，這是一種命令列工具，可簽署、驗證檔案，並加入時間戳記，以簡化程式碼簽署程序。您可以使用 AWS CloudHSM 安全地存放您的金鑰對，直到 SignTool 需要這些金鑰對為止，從而為簽署資料建立易於自動化的工作流程。

下列主題提供如何使用 SignTool 搭配的概觀 AWS CloudHSM。

## 主題

- [步驟 1：設定先決條件](#)
- [步驟 2：建立簽署憑證](#)
- [步驟 3：簽署檔案](#)

## 步驟 1：設定先決條件

若要搭配使用 Microsoft SignTool AWS CloudHSM，您需要下列項目：

- 執行 Windows 作業系統的 Amazon EC2 用戶端執行個體。
- 憑證授權單位 (CA)；不論是自己維護，或由第三方供應商建立。
- 與 EC2 執行個體位於相同虛擬公有雲端 (VPC) 中的作用中 AWS CloudHSM 叢集。叢集必須至少包含一個 HSM。
- 在 AWS CloudHSM 叢集中擁有和管理金鑰的加密使用者 (CU)。
- 未簽署的檔案或可執行檔。
- Microsoft Windows 軟體開發套件 (SDK)。

設定 AWS CloudHSM 搭配 Windows SignTool 使用的先決條件

1. 請依照本指南中[入門](#)一節的說明，來啟動 Windows EC2 執行個體與 AWS CloudHSM 叢集。
2. 如果您想要託管自己的 Windows Server CA，請遵循將 [Windows Server 設定為憑證授權單位 AWS CloudHSM](#) 中的步驟 1 和 2。否則，請繼續使用您公開信任的第三方 CA。
3. 在您的 Windows EC2 執行個體上，下載並安裝下列其中一個版本的 Microsoft Windows 軟體開發套件：
  - [Microsoft Windows SDK 10](#)

- [Microsoft Windows SDK 8.1](#)
- [Microsoft Windows SDK 7](#)

SignTool 可執行檔是 Windows SDK Signing Tools for Desktop Apps 安裝功能的一部分。如果您不需要其他功能，可以省略其安裝。預設安裝位置為：

```
C:\Program Files (x86)\Windows Kits\<SDK version>\bin\<version number>\<CPU architecture>\signtool.exe
```

您現在可以使用 Microsoft Windows SDK、AWS CloudHSM 叢集和 CA 來[建立簽署憑證](#)。

## 步驟 2：建立簽署憑證

現在您已將 Windows SDK 下載到您的 EC2 執行個體上，即可使用它來產生憑證簽署請求 (CSR)。CSR 是未簽署的憑證，最終會傳遞到您的 CA 以進行簽署。在這個範例中，我們使用 Windows SDK 隨附的 certreq 可執行檔，來產生 CSR。

使用 **certreq** 可執行檔來產生 CSR

1. 如果您尚未連線至 Windows EC2 執行個體，請先進行連線。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 建立名為 request.inf 的檔案，其中包含以下各行。將 Subject 資訊取代為您組織的相關資訊。如需每個參數的說明，請參閱 [Microsoft 文件](#)。

```
[Version]
Signature= $Windows NT$
[NewRequest]
Subject = "C=<Country>,CN=<www.website.com>,O=<Organization>,OU=<Organizational-Unit>,L=<City>,S=<State>"
RequestType=PKCS10
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "Cavium Key Storage Provider"
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE"
MachineKeySet = True
Exportable = False
```

3. 執行 certreq.exe。在此範例中，我們將 CSR 儲存為 request.csr。

```
certreq.exe -new request.inf request.csr
```

在內部，會在您的 AWS CloudHSM 叢集上產生新的金鑰對，並使用該對的私有金鑰來建立 CSR。

4. 將 CSR 提交給您的 CA。如果您使用的是 Windows Server CA，請依照下列步驟進行：

a. 輸入下列命令以開啟 CA 工具：

```
certsrv.msc
```

- b. 在新的視窗中，以滑鼠右鍵按一下 CA 伺服器的名稱。選擇 All Tasks (所有任務)，然後選擇 Submit new request (提交新請求)。
- c. 導覽至 request.csr 的位置，然後選擇 Open (開啟)。
- d. 展開伺服器 CA 功能表，導覽至待處理的請求資料夾。用滑鼠右鍵按一下您剛建立的請求，並在 All Tasks (所有任務) 下方選擇 Issue (發行)。
- e. 現在，導覽至 Issued Certificates (發行的憑證) 資料夾 (位於 Pending Requests (待處理的請求) 資料夾上方)。
- f. 選擇 Open (開啟) 以檢視憑證，然後選擇 Details (詳細資訊) 標籤。
- g. 選擇 Copy to File (複製到檔案) 來啟動 [憑證匯出精靈]。將 DER 編碼的 X.509 檔案以 signedCertificate.cer 名稱儲存到安全的位置。
- h. 結束 CA 工具，並使用下列命令，將憑證檔案移至 Windows 的個人憑證存放區中。其他應用程式即可使用此憑證。

```
certreq.exe -accept signedCertificate.cer
```

您現在可以使用匯入的憑證來[簽署檔案](#)。

### 步驟 3：簽署檔案

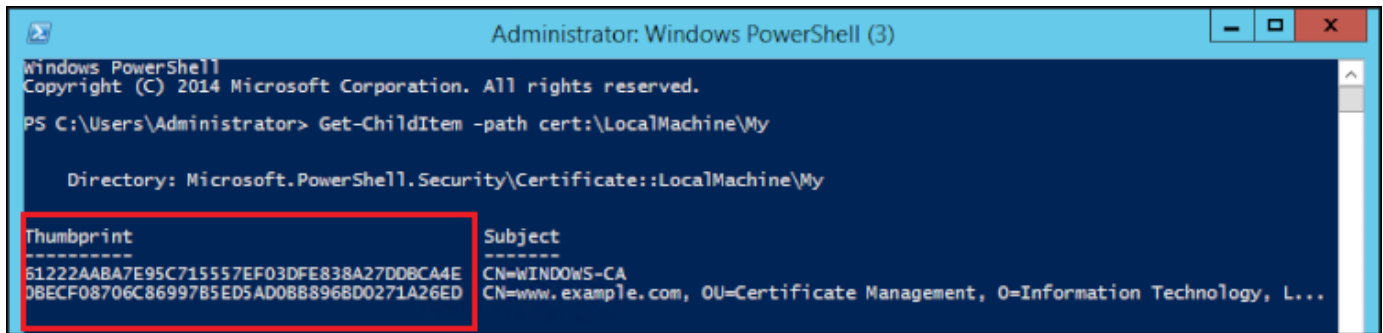
您現在可以開始使用 SignTool 和匯入的憑證，來簽署您的範例檔案。若要執行此作業，您需要知道憑證的 SHA-1 雜湊或「指紋」。指紋是用來確保 SignTool 只使用經過 AWS CloudHSM 驗證的憑證。在這個範例中，我們使用 PowerShell 取得憑證的雜湊。您也可以使用 CA 的 GUI 或 Windows 軟體開發套件的 certutil 可執行檔。

取得憑證的指紋，並使用它來簽署檔案

1. 以管理員身分開啟 PowerShell，並執行下列命令：

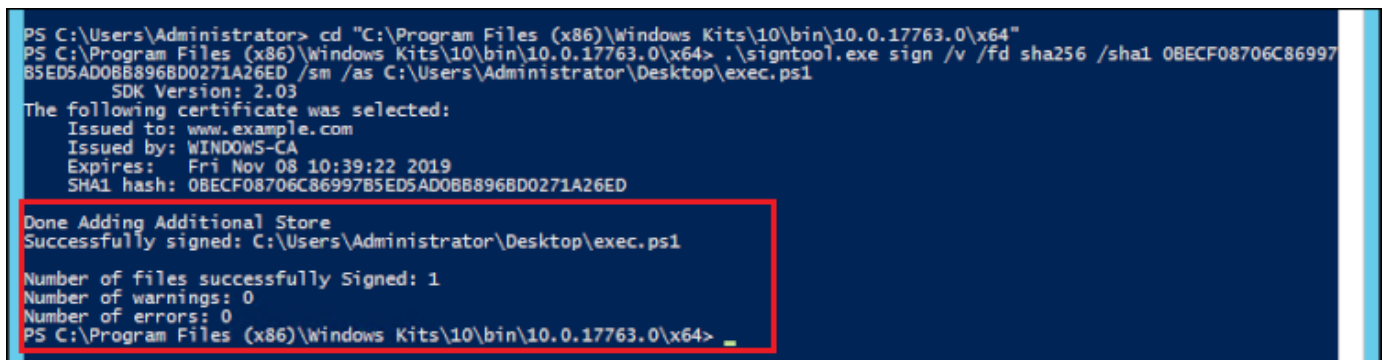
```
Get-ChildItem -path cert:\LocalMachine\My
```

複製傳回的 Thumbprint。



2. 導覽至 PowerShell 中包含 SignTool.exe 的目錄。預設位置為 C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64。
3. 最後，執行以下命令簽署您的檔案。如果命令成功，PowerShell 會傳回成功訊息。

```
signtool.exe sign /v /fd sha256 /sha1 <thumbprint> /sm C:\Users\Administrator\
\Desktop\<test>.ps1
```



4. (選用) 若要驗證檔案上的簽章，請使用下列命令：

```
signtool.exe verify /v /pa C:\Users\Administrator\Desktop\<test>.ps1
```

# Java Keytool 和 Jarsigner 與 整合 AWS CloudHSM

AWS CloudHSM 透過用戶端 SDK 3 和用戶端 SDK 5 提供與 Java Keytool 和 Jarsigner 公用程式的整合。使用這些工具的步驟會因您目前下載的用戶端 SDK 版本而異。下列各節提供每個 SDK 的資訊。

## 主題

- [使用用戶端 SDK 5 AWS CloudHSM 與 Java Keytool 和 Jarsigner 整合](#)
- [使用用戶端 SDK 3 AWS CloudHSM 與 Java Keytool 和 Jarsigner 整合](#)

## 使用用戶端 SDK 5 AWS CloudHSM 與 Java Keytool 和 Jarsigner 整合

AWS CloudHSM 金鑰存放區是特殊用途的 JCE 金鑰存放區，透過 keytool 和等第三方工具，利用與硬體安全模組 (HSM) 上金鑰相關聯的憑證 jarsigner。AWS CloudHSM 不會在 HSM 上存放憑證，因為憑證是公有、非機密資料。AWS CloudHSM 金鑰存放區會將憑證存放在本機檔案中，並將憑證映射至 HSM 上的對應金鑰。

當您使用 AWS CloudHSM 金鑰存放區產生新的金鑰時，本機金鑰存放區檔案中不會產生任何項目 – 金鑰會在 HSM 上建立。同樣的，當您使用 AWS CloudHSM 金鑰存放區搜尋金鑰時，搜尋會傳遞至 HSM。當您將憑證存放在 AWS CloudHSM 金鑰存放區時，提供者會驗證 HSM 上是否存在具有對應別名的金鑰對，然後建立與對應金鑰對一起提供的憑證的關聯。

## 主題

- [使用用戶端 SDK 5 AWS CloudHSM 與 Java Keytool 和 Jarsigner 整合的先決條件](#)
- [使用用戶端 SDK 5 搭配 keytool 使用 AWS CloudHSM 金鑰存放區](#)
- [使用用戶端 SDK 5 搭配 Jarsigner 使用 AWS CloudHSM 金鑰存放區](#)
- [使用用戶端 SDK 5 AWS CloudHSM 整合 Java Keytool 和 Jarsigner 的已知問題](#)

## 使用用戶端 SDK 5 AWS CloudHSM 與 Java Keytool 和 Jarsigner 整合的先決條件

若要使用 AWS CloudHSM 金鑰存放區，您必須先初始化和設定 AWS CloudHSM JCE 開發套件。請使用下列步驟來執行此操作。

### 步驟 1：安裝 JCE

若要安裝 JCE，包括 AWS CloudHSM 用戶端先決條件，請遵循[安裝 Java 程式庫](#)的步驟。

## 步驟 2：將 HSM 登入憑證新增至環境變數

設定環境變數以包含您的 HSM 登入憑證。

### Linux

```
$ export HSM_USER=<HSM user name>
```

```
$ export HSM_PASSWORD=<HSM password>
```

### Windows

```
PS C:\> $Env:HSM_USER=<HSM user name>
```

```
PS C:\> $Env:HSM_PASSWORD=<HSM password>
```

#### Note

AWS CloudHSM JCE 提供各種登入選項。若要搭配第三方應用程式使用 AWS CloudHSM 金鑰存放區，您必須搭配環境變數使用隱含登入。如果您想要透過應用程式碼使用明確登入，您必須使用 AWS CloudHSM 金鑰存放區建置自己的應用程式。如需詳細資訊，請參閱有關[使用 AWS CloudHSM 金鑰存放區](#)的文章。

## 步驟 3：註冊 JCE 提供者

如要在 Java CloudProvider 組態中註冊 JCE 提供者，請執行下列步驟：

1. 在 Java 安裝中開啟 `java.security` 組態檔案進行編輯。
2. 在 `java.security` 組態檔案中，新增 `com.amazonaws.cloudhsm.jce.provider.CloudHsmProvider` 為最後一個提供者。例如，如果 `java.security` 檔案中有九個供應商，請將下列提供者新增為區段中的最後一個供應商。  
  
`security.provider.10=com.amazonaws.cloudhsm.jce.provider.CloudHsmProvider`



**Note**

將 AWS CloudHSM 提供者新增為較高的優先順序可能會對系統效能造成負面影響，因為 AWS CloudHSM 供應商將優先處理可能安全地卸載至軟體的操作。最佳實務是，一律指定您希望用於操作的提供者，無論是 AWS CloudHSM 還是軟體型提供者。

**Note**

keytool 搭配 AWS CloudHSM -providerName 金鑰存放區使用產生金鑰時，指定 -providerclass、和 -providerpath 命令列選項可能會導致錯誤。

## 使用用戶端 SDK 5 搭配 keytool 使用 AWS CloudHSM 金鑰存放區

[Keytool](#) 是常見的金鑰和憑證任務的常用命令列公用程式。完整的 Keytool 教學並不在 AWS CloudHSM 文件範圍之內。本文說明透過金鑰存放區使用 AWS CloudHSM 做為信任根時，應搭配各種 AWS CloudHSM keytool 函數使用的特定參數。

搭配 AWS CloudHSM 金鑰存放區使用 keytool 時，請為任何 keytool 命令指定下列引數：

### Linux

```
-storetype CLOUDHSM -J-classpath< '-J/opt/cloudhsm/java/*'>
```

### Windows

```
-storetype CLOUDHSM -J-classpath<' -J"C:\Program Files\Amazon\CloudHSM\java*" '>
```

如果您想要使用金鑰存放區建立新的 AWS CloudHSM 金鑰存放區檔案，請參閱 [使用用戶端 SDK 3 的 AWS CloudHSM AWS CloudHSM KeyStore](#)。若要使用現有的金鑰存放區，請使用金鑰存放區引數指定其名稱 (包含路徑) 至 Keytool。如果您在 keytool 命令中指定不存在的金鑰存放區檔案，AWS CloudHSM 金鑰存放區會建立新的金鑰存放區檔案。

### 使用 keytool 建立新的 AWS CloudHSM 金鑰

您可以使用 keytool 來產生 AWS CloudHSM JCE SDK 支援的 RSA、AES 和 DESede 類型金鑰。



 Important

透過 `keytool` 產生的金鑰會在軟體中產生，然後匯入 AWS CloudHSM 做為可擷取的持久性金鑰。

我們強烈建議您不要在 `Keytool` 中產生不可匯出的金鑰，然後又匯入相對應的憑證至金鑰存放區。如果您透過 `keytool` 和 `Jarsigner` 使用可擷取的 RSA 或 EC 金鑰，提供者會從匯出金鑰，AWS CloudHSM 然後在本機使用金鑰進行簽署操作。

如果您有多個用戶端執行個體連接到 AWS CloudHSM 叢集，請注意，在一個用戶端執行個體的金鑰存放區上匯入憑證不會自動在其他用戶端執行個體上提供憑證。若要在每個用戶端執行個體上註冊金鑰和相關憑證，您必須執行 Java 應用程式，如 [the section called “使用 Keytool 產生 CSR”](#) 所述。或者，您可以在一個用戶端上進行必要的變更，並將產生的金鑰存放區檔案複製到其他每個用戶端執行個體。

範例 1：產生對稱 AES-256 金鑰，並將其儲存在工作目錄中名為 `"example_keystore.store"` 的金鑰存放區檔案中。將 `<secret label>` 取代為唯一的標籤。

## Linux

```
$ keytool -genseckey -alias <secret label> -keyalg aes \
-keysize 256 -keystore example_keystore.store \
-storetype CloudHSM -J-classpath '-J/opt/cloudhsm/java/*' \
```

## Windows

```
PS C:\> keytool -genseckey -alias <secret label> -keyalg aes `
-keysize 256 -keystore example_keystore.store `
-storetype CloudHSM -J-classpath '-J"C:\Program Files\Amazon\CloudHSM\java*"'
```

範例 2：產生 RSA 2048 金鑰對，並將其儲存在工作目錄中名為 `"example_keystore.store"` 的金鑰存放區檔案中。將 `<RSA key pair label>` 取代為唯一的標籤。

## Linux

```
$ keytool -genkeypair -alias <RSA key pair label> \
-keyalg rsa -keysize 2048 \
-sigalg sha512withrsa \
-keystore example_keystore.store \
```

```
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*'
```

## Windows

```
PS C:\> keytool -genkeypair -alias <RSA key pair label> `
-keyalg rsa -keysize 2048 `
-sigalg sha512withrsa `
-keystore example_keystore.store `
-storetype CLOUDHSM `
-J-classpath '-J"C:\Program Files\Amazon\CloudHSM\java*"'
```

您可以在 Java 程式庫中找到[支援的簽章演算法](#)清單。

使用 AWS CloudHSM keytool 刪除金鑰

AWS CloudHSM 金鑰存放區不支援刪除金鑰。您可以使用[可銷毀介面](#)的銷毀方法刪除金鑰。

```
((Destroyable) key).destroy();
```

使用 keytool 產生 AWS CloudHSM CSR

如果您使用[適用於 AWS CloudHSM 用戶端 SDK 5 的 OpenSSL 動態引擎](#)，您可以在產生憑證簽署要求 (CSR) 時獲得最大的彈性。以下命令使用 Keytool 來產生具有別名 example-key-pair 的金鑰對適用 CSR。

## Linux

```
$ keytool -certreq -alias <key pair label> \
-file my_csr.csr \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*'
```

## Windows

```
PS C:\> keytool -certreq -alias <key pair label> `
-file my_csr.csr `
-keystore example_keystore.store `
-storetype CLOUDHSM `
```

```
-J-classpath '-J"C:\Program Files\Amazon\CloudHSM\java*"'
```

### Note

若要使用 Keytool 的金鑰對，該金鑰對必須再指定的金鑰存放區檔案中有項目。如果您要使用非 Keytool 產生的金鑰對，則必須將金鑰和憑證中繼資料匯入至金鑰存放區。如需匯入金鑰存放區資料的說明，請參閱 [the section called “使用 keytool 將憑證匯入金鑰存放區”](#)。

## 使用 keytool 將中繼憑證和根憑證匯入 AWS CloudHSM 金鑰存放區

若要在中匯入 CA 憑證 AWS CloudHSM，您必須在新匯入的憑證上啟用完整憑證鏈的驗證。以下為命令的範例。

### Linux

```
$ keytool -import -trustcacerts -alias rootCAcert \
-file rootCAcert.cert -keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*'
```

### Windows

```
PS C:\> keytool -import -trustcacerts -alias rootCAcert \
-file rootCAcert.cert -keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J"C:\Program Files\Amazon\CloudHSM\java*"'
```

如果您將多個用戶端執行個體連接到 AWS CloudHSM 叢集，在某個用戶端執行個體的金鑰存放區上匯入憑證不會自動在其他用戶端執行個體上提供憑證。您必須在每個用戶端執行個體上匯入憑證。

## 使用 keytool 從 AWS CloudHSM 金鑰存放區刪除憑證

下列命令顯示如何從 Java keytool 金鑰存放區刪除 AWS CloudHSM 憑證的範例。

### Linux

```
$ keytool -delete -alias mydomain \
-keystore example_keystore.store
```

```
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*'
```

## Windows

```
PS C:\> keytool -delete -alias mydomain \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J"C:\Program Files\Amazon\CloudHSM\java*"'
```

如果您將多個用戶端執行個體連接到 AWS CloudHSM 叢集，刪除某個用戶端執行個體金鑰存放區上的憑證不會自動從其他用戶端執行個體移除憑證。您必須在每個用戶端執行個體上刪除憑證。

使用 AWS CloudHSM keytool 將工作憑證匯入金鑰存放區

憑證簽署要求 (CSR) 簽署後，您就可以將其匯入 AWS CloudHSM 金鑰存放區，並與適當的金鑰對建立關聯。以下是命令範例。

## Linux

```
$ keytool -importcert -noprompt -alias <key pair label> \
-file my_certificate.crt \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*'
```

## Windows

```
PS C:\> keytool -importcert -noprompt -alias <key pair label> \
-file my_certificate.crt \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J"C:\Program Files\Amazon\CloudHSM\java*"'
```

別名應為金鑰存放區中具有關聯憑證的金鑰對。如果金鑰是非 Keytool 產生，或是在不同的用戶端執行個體上產生，您就必須先將金鑰和憑證中繼資料匯入金鑰存放區。

憑證鏈必須是可驗證的。如果您無法驗證憑證，則可能需要將簽署 (憑證授權單位) 憑證匯入金鑰存放區，以便驗證該鏈結。

## AWS CloudHSM 使用 keytool 從 匯出憑證

下列範例會產生二進位 X.509 格式的憑證。若要從 匯出人類可讀憑證 AWS CloudHSM，請將 `-rfc` 新增至 `-exportcert` 命令。

### Linux

```
$ keytool -exportcert -alias <key pair label> \
-file my_exported_certificate.crt \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*'
```

### Windows

```
PS C:\> keytool -exportcert -alias <key pair label> \
-file my_exported_certificate.crt \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J"C:\Program Files\Amazon\CloudHSM\java*"'
```

## 使用用戶端 SDK 5 搭配 Jarsigner 使用 AWS CloudHSM 金鑰存放區

Jarsigner 是常用的命令列公用程式，用於使用安全地存放在硬體安全模組 (HSM) 上的金鑰簽署 JAR 檔案。Jarsigner 的完整教學課程超出 AWS CloudHSM 文件的範圍。本節說明您應該用來簽署和驗證簽章的 Jarsigner 參數，並以 AWS CloudHSM 做為透過 AWS CloudHSM 金鑰存放區的信任根。

### 使用 Jarsigner 設定 AWS CloudHSM 金鑰和憑證

在使用 Jarsigner 簽署 AWS CloudHSM JAR 檔案之前，請確定您已設定或完成下列步驟：

1. 遵循 [AWS CloudHSM 金鑰存放區必要條件](#) 中的指引。
2. 設定您的簽署金鑰以及關聯的憑證和憑證鏈，這些憑證和憑證鏈應存放在目前伺服器或用戶端執行個體的 AWS CloudHSM 金鑰存放區中。在上建立金鑰，AWS CloudHSM 然後將相關聯的中繼資料匯入至您的 AWS CloudHSM 金鑰存放區。如果您要使用 Keytool 設定金鑰和憑證，請參閱 [the section called “使用 Keytool 建立新金鑰”](#)。如果您使用多個用戶端執行個體來簽署 JAR，請建立金鑰並匯入憑證鏈。然後將生成的金鑰存放區文件複製到每個用戶端執行個體。如果您經常產生新的金鑰，您可能會發現將憑證個別匯入至每個用戶端執行個體更容易。
3. 整個憑證鏈必須是可驗證的。若要驗證憑證鏈，您可能需要將 CA 憑證和中繼憑證新增至 AWS CloudHSM 金鑰存放區。有關使用 Java 程式碼驗證憑證鏈的說明，請參閱 [the section called “簽署](#)

[JAR 檔案](#)”中的程式碼片段。如果需要，您也可以使用 Keytool 匯入憑證。如需使用 Keytool 的說明，請參閱 [the section called “使用 keytool 將憑證匯入金鑰存放區”](#)。

## 使用 AWS CloudHSM 和 Jarsigner 簽署 JAR 檔案

使用以下命令，使用 AWS CloudHSM 和 Jarsigner 簽署 JAR 檔案：

Linux;

### 對於 OpenJDK 8

```
jarsigner -keystore example_keystore.store \
-signedjar signthisclass_signed.jar \
-sigalg sha512withrsa \
-storetype CloudHSM \
-J-classpath '-J/opt/cloudhsm/java/*:/usr/lib/jvm/java-1.8.0/lib/tools.jar' \
-J-Djava.library.path=/opt/cloudhsm/lib \
signthisclass.jar <key pair label>
```

### 對於 OpenJDK 11、OpenJDK 17 和 OpenJDK 21

```
jarsigner -keystore example_keystore.store \
-signedjar signthisclass_signed.jar \
-sigalg sha512withrsa \
-storetype CloudHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib \
signthisclass.jar <key pair label>
```

## Windows

### 對於 OpenJDK8

```
jarsigner -keystore example_keystore.store \
-signedjar signthisclass_signed.jar \
-sigalg sha512withrsa \
-storetype CloudHSM \
-J-classpath '-JC:\Program Files\Amazon\CloudHSM\java*;C:\Program Files\Java\
\jdk1.8.0_331\lib\tools.jar' \

```

```
"-J-Djava.library.path='C:\Program Files\Amazon\CloudHSM\lib\' " `
signthisclass.jar <key pair label>
```

對於 OpenJDK 11、OpenJDK 17 和 OpenJDK 21

```
jarsigner -keystore example_keystore.store `
-signedjar signthisclass_signed.jar `
-sialg sha512withrsa `
-storetype CloudHSM `
-J-classpath '-JC:\Program Files\Amazon\CloudHSM\java*' `
"-J-Djava.library.path='C:\Program Files\Amazon\CloudHSM\lib\' " `
signthisclass.jar <key pair label>
```

使用以下命令來驗證已簽署的 JAR：

Linux

對於 OpenJDK8

```
jarsigner -verify \
-keystore example_keystore.store \
-sialg sha512withrsa \
-storetype CloudHSM \
-J-classpath '-J/opt/cloudhsm/java/*:/usr/lib/jvm/java-1.8.0/lib/tools.jar' \
-J-Djava.library.path=/opt/cloudhsm/lib \
signthisclass_signed.jar <key pair label>
```

對於 OpenJDK 11、OpenJDK 17 和 OpenJDK 21

```
jarsigner -verify \
-keystore example_keystore.store \
-sialg sha512withrsa \
-storetype CloudHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib \
signthisclass_signed.jar <key pair label>
```

## Windows

### 對於 OpenJDK 8

```
jarsigner -verify `
-keystore example_keystore.store `
-sigalg sha512withrsa `
-storetype CloudHSM `
-J-classpath '-JC:\Program Files\Amazon\CloudHSM\java*;C:\Program Files\Java\jdk1.8.0_331\lib\tools.jar' `
"-J-Djava.library.path='C:\Program Files\Amazon\CloudHSM\lib\'" `
signthisclass_signed.jar <key pair label>
```

### 對於 OpenJDK 11、OpenJDK 17 和 OpenJDK 21

```
jarsigner -verify `
-keystore example_keystore.store `
-sigalg sha512withrsa `
-storetype CloudHSM `
-J-classpath '-JC:\Program Files\Amazon\CloudHSM\java*' `
"-J-Djava.library.path='C:\Program Files\Amazon\CloudHSM\lib\'" `
signthisclass_signed.jar <key pair label>
```

## 使用用戶端 SDK 5 AWS CloudHSM 整合 Java Keytool 和 Jarsigner 的已知問題

下列清單提供使用用戶端 SDK 5 與 AWS CloudHSM 和 Java Keytool 和 Jarsigner 整合的目前已知問題清單。

1. 不支持使用 Keytool 和 Jarsigner 的 EC 金鑰。

## 使用用戶端 SDK 3 AWS CloudHSM 與 Java Keytool 和 Jarsigner 整合

AWS CloudHSM 金鑰存放區是特殊用途的 JCE 金鑰存放區，透過 keytool 和 等第三方工具，利用與硬體安全模組 (HSM) 上金鑰相關聯的憑證 jarsigner。AWS CloudHSM 不會在 HSM 上存放憑證，因為憑證是公有、非機密資料。AWS CloudHSM 金鑰存放區會將憑證存放在本機檔案中，並將憑證映射至 HSM 上的對應金鑰。



當您使用 AWS CloudHSM 金鑰存放區產生新的金鑰時，本機金鑰存放區檔案中不會產生任何項目 – 金鑰會在 HSM 上建立。同樣的，當您使用 AWS CloudHSM 金鑰存放區搜尋金鑰時，搜尋會傳遞至 HSM。當您將憑證存放在 AWS CloudHSM 金鑰存放區時，提供者會驗證 HSM 上是否存在具有對應別名的金鑰對，然後建立與對應金鑰對一起提供的憑證的關聯。

## 主題

- [使用用戶端 SDK 3 AWS CloudHSM 與 Java Keytool 和 Jarsigner 整合的先決條件](#)
- [使用用戶端 SDK 3 搭配 keytool 使用 AWS CloudHSM 金鑰存放區](#)
- [使用用戶端 SDK 3 搭配 Jarsigner 使用 AWS CloudHSM 金鑰存放區](#)
- [使用用戶端 SDK 3 AWS CloudHSM 整合 Java Keytool 和 Jarsigner 的已知問題](#)
- [向金鑰存放區註冊預先存在的 AWS CloudHSM 金鑰](#)

## 使用用戶端 SDK 3 AWS CloudHSM 與 Java Keytool 和 Jarsigner 整合的先決條件

若要使用 AWS CloudHSM 金鑰存放區，您必須先初始化和設定 AWS CloudHSM JCE 開發套件。請使用下列步驟來執行此操作。

### 步驟 1：安裝 JCE

若要安裝 JCE，包括 AWS CloudHSM 用戶端先決條件，請遵循[安裝 Java 程式庫](#)的步驟。

### 步驟 2：將 HSM 登入憑證新增至環境變數

設定環境變數以包含您的 HSM 登入憑證。

```
export HSM_PARTITION=PARTITION_1
export HSM_USER=<HSM user name>
export HSM_PASSWORD=<HSM password>
```

#### Note

CloudHSM JCE 提供多種登入選項。若要搭配第三方應用程式使用 AWS CloudHSM 金鑰存放區，您必須搭配環境變數使用隱含登入。如果您想要透過應用程式碼使用明確登入，您必須使用 AWS CloudHSM 金鑰存放區建置自己的應用程式。如需詳細資訊，請參閱有關[使用 AWS CloudHSM 金鑰存放區](#)的文章。

### 步驟 3：註冊 JCE 供應商

若要註冊 JCE 提供商，請前往 Java CloudProvider 組態。

1. 在 Java 安裝中開啟 java.security 組態檔案進行編輯。
2. 在 java.security 組態檔案中，新增 com.cavium.provider.CaviumProvider 為最後一個提供商。例如，如果 java.security 檔案中有九個供應商，請將下列提供商新增為區段中的最後一個供應商。如果將 Cavium 提供商新增為優先順序較高的提供商，可能會對您的系統效能帶來負面影響。

```
security.provider.10=com.cavium.provider.CaviumProvider
```

#### Note

進階使用者可能習慣在使用 keytool 時指定 -providerName、-providerclass 和 -providerpath 命令列選項，而不是更新安全性組態檔案。如果您在使用金鑰存放區產生 AWS CloudHSM 金鑰時嘗試指定命令列選項，則會導致錯誤。

### 使用用戶端 SDK 3 搭配 keytool 使用 AWS CloudHSM 金鑰存放區

[Keytool](#) 是 Linux 系統中常見的金鑰和憑證任務的常用命令列執行程序。完整的 Keytool 教學並不在 AWS CloudHSM 文件範圍之內。本文說明透過金鑰存放區使用 AWS CloudHSM 做為信任根時，應搭配各種 AWS CloudHSM keytool 函數使用的特定參數。

搭配 金鑰 AWS CloudHSM 存放區使用 keytool 時，請為任何 keytool 命令指定下列引數：

```
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib
```

如果您想要使用金鑰存放區建立新的 AWS CloudHSM 金鑰存放區檔案，請參閱 [使用用戶端 SDK 3 的 AWS CloudHSM AWS CloudHSM KeyStore](#)。若要使用現有的金鑰存放區，請使用金鑰存放區引數指定其名稱 (包含路徑) 至 Keytool。如果您在 keytool 命令中指定不存在的金鑰存放區檔案，AWS CloudHSM 金鑰存放區會建立新的金鑰存放區檔案。

### 使用 keytool 建立新的 AWS CloudHSM 金鑰

您可以使用 keytool 來產生 AWS CloudHSM JCE SDK 支援的任何類型的金鑰。請參閱 Java 程式庫的 [支援金鑰](#) 文章中金鑰和長度的完整清單。

 Important

透過 keytool 產生的金鑰會在軟體中產生，然後匯入 AWS CloudHSM 做為可擷取的持久性金鑰。

直接在硬體安全模組 (HSM) 上建立不可擷取金鑰，然後將其與 keytool 或 Jarsigner 搭配使用的指示，會顯示在[向 AWS CloudHSM Key Store 註冊既有金鑰](#)的程式碼範例中。我們強烈建議您不要在 Keytool 中產生不可匯出的金鑰，然後又匯入相對應的憑證至金鑰存放區。如果您透過 keytool 和 jarsigner 使用可擷取的 RSA 或 EC 金鑰，提供者會從 匯出金鑰，AWS CloudHSM 然後在本機使用金鑰進行簽署操作。

如果您有多個用戶端執行個體連接到 CloudHSM 叢集，請注意，在一個用戶端執行個體的金鑰存放區上匯入憑證不會自動讓憑證可於其他用戶端執行個體使用。若要在每個用戶端執行個體上註冊金鑰和相關憑證，您必須執行 Java 應用程式，如[使用 Keytool 產生 CSR](#)中所述。或者，您可以在一個用戶端上進行必要的變更，並將產生的金鑰存放區檔案複製到其他每個用戶端執行個體。

範例 1：產生對稱 AES-256 金鑰，並將其儲存在工作目錄中名為 "example\_keystore.store" 的金鑰存放區檔案中。將 *<secret label>* 取代為唯一的標籤。

```
keytool -genseckey -alias <secret label> -keyalg aes \
-keysize 256 -keystore example_keystore.store \
-storetype CloudHSM -J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib/
```

範例 2：產生 RSA 2048 金鑰對，並將其儲存在工作目錄中名為 "example\_keystore.store" 的金鑰存放區檔案中。將 *<RSA key pair label>* 取代為唯一的標籤。

```
keytool -genkeypair -alias <RSA key pair label> \
-keyalg rsa -keysize 2048 \
-sigalg sha512withrsa \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib/
```

範例 3：產生 p256 ED 金鑰並將其儲存在工作目錄中名為 "example\_keystore.store" 的金鑰存放區檔案中。將 *<ec key pair label>* 取代為唯一的標籤。

```
keytool -genkeypair -alias <ec key pair label> \
```

```
-keyalg ec -keysize 256 \
-sigalg SHA512withECDSA \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib/
```

您可以在 Java 程式庫中找到[支援的簽章演算法](#)清單。

### 使用 keytool 刪除 AWS CloudHSM 金鑰

AWS CloudHSM 金鑰存放區不支援刪除金鑰。若要刪除金鑰，您必須使用 AWS CloudHSM 命令列工具的 deleteKey 函數[使用 KMU 刪除 AWS CloudHSM 金鑰](#)。

### 使用 keytool 產生 AWS CloudHSM CSR

如果您使用 [適用於 AWS CloudHSM 用戶端 SDK 5 的 OpenSSL 動態引擎](#)，您可以在產生憑證簽署要求 (CSR) 時獲得最大的彈性。以下命令使用 Keytool 來產生具有別名 example-key-pair 的金鑰對適用 CSR。

```
keytool -certreq -alias <key pair label> \
-file example_csr.csr \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib/
```

#### Note

若要使用 Keytool 的金鑰對，該金鑰對必須再指定的金鑰存放區檔案中有項目。如果您要使用非 Keytool 產生的金鑰對，則必須將金鑰和憑證中繼資料匯入至金鑰存放區。如需匯入金鑰存放區資料的指示，請參閱[使用 AWS CloudHSM Keytool 將中繼憑證和根憑證匯入金鑰存放區](#)。

### 使用 keytool 將中繼憑證和根憑證匯入 AWS CloudHSM 金鑰存放區

若要將 CA 憑證匯入 AWS CloudHSM，您必須在新匯入的憑證上啟用完整憑證鏈的驗證。以下為命令的範例。

```
keytool -import -trustcacerts -alias rootCAcert \

```

```
-file rootCAcert.cert -keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib/
```

如果您將多個用戶端執行個體連接到 AWS CloudHSM 叢集，在某個用戶端執行個體的金鑰存放區上匯入憑證不會自動在其他用戶端執行個體上提供憑證。您必須在每個用戶端執行個體上匯入憑證。

使用 keytool 從 AWS CloudHSM 金鑰存放區刪除憑證

下列命令顯示如何從 Java keytool 金鑰存放區刪除 AWS CloudHSM 憑證的範例。

```
keytool -delete -alias mydomain -keystore \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib/
```

如果您將多個用戶端執行個體連接到 AWS CloudHSM 叢集，刪除某個用戶端執行個體金鑰存放區上的憑證不會自動從其他用戶端執行個體移除憑證。您必須在每個用戶端執行個體上刪除憑證。

使用 keytool 將 AWS CloudHSM 工作憑證匯入金鑰存放區

憑證簽署要求 (CSR) 簽署後，您就可以將其匯入 AWS CloudHSM 金鑰存放區，並與適當的金鑰對建立關聯。以下是命令範例。

```
keytool -importcert -noprompt -alias <key pair label> \
-file example_certificate.crt \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib/
```

別名應為金鑰存放區中具有關聯憑證的金鑰對。如果金鑰是非 Keytool 產生，或是在不同的用戶端執行個體上產生，您就必須先將金鑰和憑證中繼資料匯入金鑰存放區。如需匯入憑證中繼資料的指示，請參閱[使用金鑰存放區註冊既有 AWS CloudHSM 金鑰](#)中的程式碼範例。

憑證鏈必須是可驗證的。如果您無法驗證憑證，則可能需要將簽署 (憑證授權單位) 憑證匯入金鑰存放區，以便驗證該鏈結。

## AWS CloudHSM 使用 keytool 從 匯出憑證

下列範例會產生二進位 X.509 格式的憑證。若要從 匯出人類可讀憑證 AWS CloudHSM，請將 `-rfc` 新增至 `-exportcert` 命令。

```
keytool -exportcert -alias <key pair label> \
-file example_exported_certificate.crt \
-keystore example_keystore.store \
-storetype CLOUDHSM \
-J-classpath '-J/opt/cloudhsm/java/*' \
-J-Djava.library.path=/opt/cloudhsm/lib/
```

## 使用用戶端 SDK 3 搭配 Jarsigner 使用 AWS CloudHSM 金鑰存放區

Jarsigner 是常用的命令列公用程式，用於使用安全地存放在硬體安全模組 (HSM) 上的金鑰簽署 JAR 檔案。Jarsigner 的完整教學課程超出 AWS CloudHSM 文件的範圍。本節說明您應該用來簽署和驗證簽章的 Jarsigner 參數，並將 AWS CloudHSM 做為透過 AWS CloudHSM 金鑰存放區的信任根。

### 使用 Jarsigner 設定 AWS CloudHSM 金鑰和憑證

在使用 Jarsigner 簽署 AWS CloudHSM JAR 檔案之前，請確定您已設定或完成下列步驟：

1. 遵循 [AWS CloudHSM 金鑰存放區必要條件](#) 中的指引。
2. 設定您的簽署金鑰以及關聯的憑證和憑證鏈，這些憑證和憑證鏈應存放在目前伺服器或用戶端執行個體的 AWS CloudHSM 金鑰存放區中。在 上建立金鑰，AWS CloudHSM 然後將相關聯的中繼資料匯入至您的 AWS CloudHSM 金鑰存放區。使用 [向金鑰存放區註冊既有 AWS CloudHSM 金鑰](#) 中的程式碼範例，將中繼資料匯入金鑰存放區。如果您要使用 Keytool 設定金鑰和憑證，請參閱 [使用 keytool 建立新的 AWS CloudHSM 金鑰](#)。如果您使用多個用戶端執行個體來簽署 JAR，請建立金鑰並匯入憑證鏈。然後將生成的金鑰存放區文件複製到每個用戶端執行個體。如果您經常產生新的金鑰，您可能會發現將憑證個別匯入至每個用戶端執行個體更容易。
3. 整個憑證鏈必須是可驗證的。若要驗證憑證鏈，您可能需要將 CA 憑證和中繼憑證新增至 AWS CloudHSM 金鑰存放區。如需使用 Java 程式碼驗證憑證鏈的說明，[請參閱使用 AWS CloudHSM 和 Jarsigner 簽署 JAR 檔案](#) 中的程式碼片段。如果需要，您也可以使用 Keytool 匯入憑證。如需使用 keytool 的指示，請參閱 [使用 Keytool 將中繼憑證和根憑證匯入 AWS CloudHSM Key Store](#)。

### 使用 AWS CloudHSM 和 Jarsigner 簽署 JAR 檔案

使用以下命令，使用 AWS CloudHSM 和 jarsigner 簽署 JAR 檔案：

```
jarsigner -keystore example_keystore.store \
```



```
-signedjar signthisclass_signed.jar \
-sigalg sha512withrsa \
-storetype CloudHSM \
-J-classpath '-J/opt/cloudhsm/java/*:/usr/lib/jvm/java-1.8.0/lib/tools.jar' \
-J-Djava.library.path=/opt/cloudhsm/lib \
signthisclass.jar <key pair label>
```

使用以下命令來驗證已簽署的 JAR：

```
jarsigner -verify \
-keystore example_keystore.store \
-sigalg sha512withrsa \
-storetype CloudHSM \
-J-classpath '-J/opt/cloudhsm/java/*:/usr/lib/jvm/java-1.8.0/lib/tools.jar' \
-J-Djava.library.path=/opt/cloudhsm/lib \
signthisclass_signed.jar <key pair label>
```

## 使用用戶端 SDK 3 AWS CloudHSM 整合 Java Keytool 和 Jarsigner 的已知問題

下列清單提供使用用戶端 SDK 3 與 AWS CloudHSM 和 Java Keytool 和 Jarsigner 整合的目前已知問題清單。

- 使用 Keytool 產生金鑰時，提供商組態中的第一個提供商不能是 CaviumProvider。
- 使用 Keytool 產生金鑰時，系統會使用安全性組態檔案中的第一個 (受支援的) 提供商來產生金鑰。這通常是軟體提供商。產生的金鑰接著會獲得別名，並在金鑰新增程序期間以持久性（權杖）金鑰的形式匯入 AWS CloudHSM HSM。
- 搭配 AWS CloudHSM 金鑰存放區使用 keytool 時，請勿在命令列上指定 -providerclass、-providerName 或 -providerpath 選項。按照[金鑰存放區先決條件](#)中的說明，在安全提供商檔案中指定這些選項。
- 當透過 Keytool 和 Narsigner 使用不可擷取的 EC 金鑰時，SunEC 提供商必須從 java.security 檔案的提供商清單中移除/停用。如果您透過 keytool 和 Jarsigner 使用可擷取的 EC 金鑰，提供者會從 AWS CloudHSM HSM 匯出金鑰位元，並在本機使用金鑰進行簽署操作。我們不建議您搭配 Keytool 或 Jarsigner 使用可匯出的金鑰。

## 向金鑰存放區註冊預先存在的 AWS CloudHSM 金鑰

為了最大限度地提高屬性和標籤的安全性和靈活性，我們建議您使用 [key\\_mgmt\\_util](#) 產生 AWS CloudHSM 簽署金鑰。您也可以使用 Java 應用程式來產生 AWS CloudHSM 中的金鑰。

下一節提供程式碼範例，示範如何在 HSM 上產生新的金鑰對，並使用匯入至 AWS CloudHSM 金鑰存放區的現有金鑰進行註冊。匯入的金鑰可以與第三方工具 (如 Keytool 和 Jarsigner) 搭配使用。

若要使用既有的金鑰，請修改程式碼範例以依標籤查詢金鑰，而不是產生新金鑰。依標籤尋找金鑰的範例程式碼可在 GitHub 的 [KeyUtilitiesRunner.java 範例](#) 中取得。

#### Important

AWS CloudHSM 向本機金鑰存放區註冊存放在的金鑰不會匯出金鑰。註冊金鑰時，金鑰存放區會註冊金鑰的別名 (或標籤)，並建立本機儲存憑證物件與 AWS CloudHSM 金鑰對之間的關聯。只要金鑰對建立為不可匯出，金鑰位元就不會離開 HSM。

```
//
// Copyright 2018 Amazon.com, Inc. or its affiliates. All Rights Reserved.
//
// Permission is hereby granted, free of charge, to any person obtaining a copy of
// this
// software and associated documentation files (the "Software"), to deal in the
// Software
// without restriction, including without limitation the rights to use, copy, modify,
// merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
// permit persons to whom the Software is furnished to do so.
//
// THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
// INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
// PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
// HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
// OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
// SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
//

package com.amazonaws.cloudhsm.examples;

import com.cavium.key.CaviumKey;
import com.cavium.key.parameter.CaviumAESKeyGenParameterSpec;
import com.cavium.key.parameter.CaviumRSAKeyGenParameterSpec;
import com.cavium.asn1.Encoder;
import com.cavium.cfm2.Util;
```



```
import javax.crypto.KeyGenerator;

import java.io.ByteArrayInputStream;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.FileNotFoundException;

import java.math.BigInteger;

import java.security.*;
import java.security.cert.Certificate;
import java.security.cert.CertificateException;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import java.security.interfaces.RSAPrivateKey;
import java.security.interfaces.RSAPublicKey;
import java.security.KeyStore.PasswordProtection;
import java.security.KeyStore.PrivateKeyEntry;
import java.security.KeyStore.Entry;

import java.util.Calendar;
import java.util.Date;
import java.util.Enumuration;

//
// KeyStoreExampleRunner demonstrates how to load a keystore, and associate a
// certificate with a
// key in that keystore.
//
// This example relies on implicit credentials, so you must setup your environment
// correctly.
//
// https://docs.aws.amazon.com/cloudhsm/latest/userguide/java-library-
install.html#java-library-credentials
//

public class KeyStoreExampleRunner {

 private static byte[] COMMON_NAME_OID = new byte[] { (byte) 0x55, (byte) 0x04,
(byte) 0x03 };
 private static byte[] COUNTRY_NAME_OID = new byte[] { (byte) 0x55, (byte) 0x04,
(byte) 0x06 };
```

```

 private static byte[] LOCALITY_NAME_OID = new byte[] { (byte) 0x55, (byte) 0x04,
(byte) 0x07 };
 private static byte[] STATE_OR_PROVINCE_NAME_OID = new byte[] { (byte) 0x55,
(byte) 0x04, (byte) 0x08 };
 private static byte[] ORGANIZATION_NAME_OID = new byte[] { (byte) 0x55, (byte)
0x04, (byte) 0x0A };
 private static byte[] ORGANIZATION_UNIT_OID = new byte[] { (byte) 0x55, (byte)
0x04, (byte) 0x0B };

 private static String helpString = "KeyStoreExampleRunner%n" +
 "This sample demonstrates how to load and store keys using a keystore.%n%n"
+
 "Options%n" +
 "\t--help\t\t\tDisplay this message.%n" +
 "\t--store <filename>\t\tPath of the keystore.%n" +
 "\t--password <password>\t\tPassword for the keystore (not your CU
password).%n" +
 "\t--label <label>\t\t\tLabel to store the key and certificate under.%n" +
 "\t--list\t\t\tList all the keys in the keystore.%n%n";

 public static void main(String[] args) throws Exception {
 Security.addProvider(new com.cavium.provider.CaviumProvider());
 KeyStore keyStore = KeyStore.getInstance("CloudHSM");

 String keystoreFile = null;
 String password = null;
 String label = null;
 boolean list = false;
 for (int i = 0; i < args.length; i++) {
 String arg = args[i];
 switch (args[i]) {
 case "--store":
 keystoreFile = args[++i];
 break;
 case "--password":
 password = args[++i];
 break;
 case "--label":
 label = args[++i];
 break;
 case "--list":
 list = true;
 break;
 case "--help":

```

```

 help();
 return;
 }
}

if (null == keystoreFile || null == password) {
 help();
 return;
}

if (list) {
 listKeys(keystoreFile, password);
 return;
}

if (null == label) {
 label = "Keystore Example Keypair";
}

//
// This call to keyStore.load() will open the pkcs12 keystore with the supplied
// password and connect to the HSM. The CU credentials must be specified using
// standard CloudHSM login methods.
//
try {
 FileInputStream instream = new FileInputStream(keystoreFile);
 keyStore.load(instream, password.toCharArray());
} catch (FileNotFoundException ex) {
 System.err.println("Keystore not found, loading an empty store");
 keyStore.load(null, null);
}

PasswordProtection passwd = new PasswordProtection(password.toCharArray());
System.out.println("Searching for example key and certificate...");

PrivateKeyEntry keyEntry = (PrivateKeyEntry) keyStore.getEntry(label, passwd);
if (null == keyEntry) {
 //
 // No entry was found, so we need to create a key pair and associate a
certificate.
 // The private key will get the label passed on the command line. The
keystore alias
 // needs to be the same as the private key label. The public key will have
":public"

```

```

 // appended to it. The alias used in the keystore will We associate the
certificate
 // with the private key.
 //
 System.out.println("No entry found, creating...");
 KeyPair kp = generateRSAKeyPair(2048, label + ":public", label);
 System.out.printf("Created a key pair with the handles %d/%d\n",
((CaviumKey) kp.getPrivate()).getHandle(), ((CaviumKey) kp.getPublic()).getHandle());

 //
 // Generate a certificate and associate the chain with the private key.
 //
 Certificate self_signed_cert = generateCert(kp);
 Certificate[] chain = new Certificate[1];
 chain[0] = self_signed_cert;
 PrivateKeyEntry entry = new PrivateKeyEntry(kp.getPrivate(), chain);

 //
 // Set the entry using the label as the alias and save the store.
 // The alias must match the private key label.
 //
 keyStore.setEntry(label, entry, passwd);

 FileOutputStream outstream = new FileOutputStream(keystoreFile);
 keyStore.store(outstream, password.toCharArray());
 outstream.close();

 keyEntry = (PrivateKeyEntry) keyStore.getEntry(label, passwd);
 }

 long handle = ((CaviumKey) keyEntry.getPrivateKey()).getHandle();
 String name = keyEntry.getCertificate().toString();
 System.out.printf("Found private key %d with certificate %s\n", handle, name);
}

private static void help() {
 System.out.println(helpString);
}

//
// Generate a non-extractable / non-persistent RSA keypair.
// This method allows us to specify the public and private labels, which
// will make KeyStore aliases easier to understand.
//

```

```

 public static KeyPair generateRSAKeyPair(int keySizeInBits, String publicLabel,
String privateLabel)
 throws InvalidAlgorithmParameterException, NoSuchAlgorithmException,
NoSuchProviderException {

 boolean isExtractable = false;
 boolean isPersistent = false;
 KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("rsa", "Cavium");
 CaviumRSAKeyGenParameterSpec spec = new
CaviumRSAKeyGenParameterSpec(keySizeInBits, new BigInteger("65537"), publicLabel,
privateLabel, isExtractable, isPersistent);

 keyPairGen.initialize(spec);

 return keyPairGen.generateKeyPair();
 }

 //
 // Generate a certificate signed by a given keypair.
 //
 private static Certificate generateCert(KeyPair kp) throws CertificateException {
 CertificateFactory cf = CertificateFactory.getInstance("X509");
 PublicKey publicKey = kp.getPublic();
 PrivateKey privateKey = kp.getPrivate();
 byte[] version = Encoder.encodeConstructed((byte) 0,
Encoder.encodePositiveBigInteger(new BigInteger("2"))); // version 1
 byte[] serialNo = Encoder.encodePositiveBigInteger(new BigInteger(1,
Util.computeKCV(publicKey.getEncoded())));

 // Use the SHA512 OID and algorithm.
 byte[] signatureOid = new byte[] {
 (byte) 0x2A, (byte) 0x86, (byte) 0x48, (byte) 0x86, (byte) 0xF7, (byte)
0x0D, (byte) 0x01, (byte) 0x01, (byte) 0x0D };
 String sigAlgoName = "SHA512WithRSA";

 byte[] signatureId = Encoder.encodeSequence(
 Encoder.encodeOid(signatureOid),
 Encoder.encodeNull());

 byte[] issuer = Encoder.encodeSequence(
 encodeName(COUNTRY_NAME_OID, "<Country>"),
 encodeName(STATE_OR_PROVINCE_NAME_OID, "<State>"),
 encodeName(LOCALITY_NAME_OID, "<City>"),

```

```

 encodeName(ORGANIZATION_NAME_OID,
"<Organization>"),
 encodeName(ORGANIZATION_UNIT_OID, "<Unit>"),
 encodeName(COMMON_NAME_OID, "<CN>")
);

 Calendar c = Calendar.getInstance();
 c.add(Calendar.DAY_OF_YEAR, -1);
 Date notBefore = c.getTime();
 c.add(Calendar.YEAR, 1);
 Date notAfter = c.getTime();
 byte[] validity = Encoder.encodeSequence(
 Encoder.encodeUTCTime(notBefore),
 Encoder.encodeUTCTime(notAfter)
);
 byte[] key = publicKey.getEncoded();

 byte[] certificate = Encoder.encodeSequence(
 version,
 serialNo,
 signatureId,
 issuer,
 validity,
 issuer,
 key);

 Signature sig;
 byte[] signature = null;
 try {
 sig = Signature.getInstance(sigAlgoName, "Cavium");
 sig.initSign(privateKey);
 sig.update(certificate);
 signature = Encoder.encodeBitstring(sig.sign());

 } catch (Exception e) {
 System.err.println(e.getMessage());
 return null;
 }

 byte [] x509 = Encoder.encodeSequence(
 certificate,
 signatureId,
 signature
);

 return cf.generateCertificate(new ByteArrayInputStream(x509));

```

```

 }

 //
 // Simple OID encoder.
 // Encode a value with OID in ASN.1 format
 //
 private static byte[] encodeName(byte[] nameOid, String value) {
 byte[] name = null;
 name = Encoder.encodeSet(
 Encoder.encodeSequence(
 Encoder.encodeOid(nameOid),
 Encoder.encodePrintableString(value)
)
);
 return name;
 }

 //
 // List all the keys in the keystore.
 //
 private static void listKeys(String keystoreFile, String password) throws Exception
 {
 KeyStore keyStore = KeyStore.getInstance("CloudHSM");

 try {
 FileInputStream instream = new FileInputStream(keystoreFile);
 keyStore.load(instream, password.toCharArray());
 } catch (FileNotFoundException ex) {
 System.err.println("Keystore not found, loading an empty store");
 keyStore.load(null, null);
 }

 for(Enumeration<String> entry = keyStore.aliases(); entry.hasMoreElements();) {
 System.out.println(entry.nextElement());
 }
 }
}

```

# 搭配使用 Microsoft 資訊清單產生和編輯工具 (Mage.exe) AWS CloudHSM 來簽署檔案

## Note

AWS CloudHSM 僅支援 Windows SDK for .NET Framework 4.8.1 和更新版本中包含的 64 位元 Mage 工具。

下列主題提供如何使用 [Mage.exe](#) 的概觀 AWS CloudHSM。

### 主題

- [步驟 1：設定先決條件](#)
- [步驟 2：建立簽署憑證](#)
- [步驟 3：簽署檔案](#)

## 步驟 1：設定先決條件

若要搭配使用 Microsoft Mage.exe AWS CloudHSM，您需要下列項目：

- 執行 Windows 作業系統的 Amazon EC2 執行個體
- 憑證授權機構 (CA)，可以是自我維護或從第三方供應商取得
- 與 EC2 執行個體位於相同虛擬私有雲端 (VPC) 中的作用中 AWS CloudHSM 叢集，至少有一個 HSM
- 在 AWS CloudHSM 叢集中擁有和管理金鑰的加密使用者 (CU)
- 未簽署的檔案或可執行檔
- Microsoft Windows 軟體開發套件 (SDK)

設定 AWS CloudHSM 搭配 Mage.exe 使用的先決條件

1. 按照本指南[入門](#)一節中的指示啟動 Windows EC2 執行個體和 AWS CloudHSM 叢集。
2. 如果您想要託管自己的 Windows Server CA，請完成將 [Windows Server 設定為憑證授權單位 AWS CloudHSM](#) 中的步驟 1 和 2。否則，請使用您公開信任的第三方 CA。
3. 在 Windows EC2 執行個體上下載並安裝適用於 .NET Framework 4.8.1 或更新版本的 Microsoft Windows 開發套件：



- [Microsoft Windows SDK 10](#)

mage.exe 可執行檔是 Windows 開發套件工具的一部分。預設安裝位置為：

```
C:\Program Files (x86)\Windows Kits\<SDK version>\bin\<version number>\x64\Mage.exe
```

完成這些步驟後，您可以使用 Microsoft Windows 開發套件、AWS CloudHSM 叢集和 CA [來建立簽署憑證](#)。

## 步驟 2：建立簽署憑證

現在您已在 EC2 執行個體上安裝 Windows 開發套件，您可以使用它來產生憑證簽署請求 (CSR)。CSR 是您提交給 CA 簽署的未簽署憑證。在此範例中，我們使用 Windows certreq 開發套件隨附的可執行檔來產生 CSR。

使用 certreq 可執行檔產生 CSR

1. 連線至您的 Windows EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。
2. 建立名為 request.inf 且具有下列內容的檔案。將 Subject 資訊取代為您組織的詳細資訊：

```
[Version]
Signature= $Windows NT$
[NewRequest]
Subject = "C=<Country>,CN=<www.website.com>,O=<Organization>,OU=<Organizational-Unit>,L=<City>,S=<State>"
RequestType=PKCS10
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 2048
ProviderName = "CloudHSM Key Storage Provider"
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE"
MachineKeySet = True
Exportable = False
```

如需每個參數的說明，請參閱 [Microsoft 文件](#)。

3. 執行 certreq.exe 以產生 CSR：

```
certreq.exe -new request.inf request.csr
```

此命令會在您的 AWS CloudHSM 叢集上產生新的金鑰對，並使用私有金鑰來建立 CSR。

4. 將 CSR 提交給您的 CA。如果您使用的是 Windows Server CA，請遵循下列步驟：

a. 開啟 CA 工具：

```
certsrv.msc
```

- b. 在新的視窗中，以滑鼠右鍵按一下 CA 伺服器的名稱。選擇 All Tasks (所有任務)，然後選擇 Submit new request (提交新請求)。
- c. 導覽至 的位置 request.csr，然後選擇開啟。
- d. 展開伺服器 CA 選單，然後導覽至待定請求資料夾。在剛建立的請求上按一下滑鼠右鍵，選擇所有任務，然後選擇問題。
- e. 導覽至已發行憑證資料夾。
- f. 選擇 Open (開啟) 以檢視憑證，然後選擇 Details (詳細資訊) 標籤。
- g. 選擇 Copy to File (複製到檔案) 來啟動 [憑證匯出精靈]。將 DER 編碼的 X.509 檔案以 signedCertificate.cer 名稱儲存到安全的位置。
- h. 結束 CA 工具並執行下列命令，將憑證檔案移至 Windows 中的個人憑證存放區：

```
certreq.exe -accept signedCertificate.cer
```

您現在可以使用匯入的憑證來[簽署檔案](#)。

## 步驟 3：簽署檔案

現在您已擁有 Mage.exe 和匯入的憑證，您可以簽署 檔案。您需要知道憑證的 SHA-1 雜湊或指紋。指紋可確保 Mage.exe 僅使用由 驗證的憑證。AWS CloudHSM在這個範例中，我們使用 PowerShell 取得憑證的雜湊。

取得憑證的指紋，並使用它來簽署檔案

1. 導覽至包含 的目錄mage.exe。預設位置為：

```
C:\Program Files (x86)\Microsoft SDKs\Windows\v10.0A\bin\NETFX 4.8.1 Tools\x64
```

- 若要使用 Mage.exe 建立範例應用程式檔案，請執行下列命令：

```
mage.exe -New Application -ToFile C:\Users\Administrator\Desktop\sample.application
```

- 以管理員身分開啟 PowerShell，並執行下列命令：

```
Get-ChildItem -path cert:\LocalMachine\My
```

從輸出複製 Key Container、Thumbprint 和 Provider 值。

```
===== Certificate 1 =====
Serial Number: 7ad8df4f5bfaf5a3405d32aa4a01b85a
Issuer: CN=EC2AMAZ-0BVI3HH-CA
NotBefore: 2/4/2025 7:55 PM
NotAfter: 2/4/2030 8:05 PM
Subject: CN=EC2AMAZ-0BVI3HH-CA
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 08f295934325ee2c37ea01ab605ceeb81610d3be thumbprint
Key Container = EC2AMAZ-0BVI3HH-CA key container
Provider = CloudHSM Key Storage Provider provider
Signature test passed
CertUtil: -store command completed successfully.
```

- 執行下列命令來簽署您的 檔案：

```
mage.exe -Sign -CertHash <thumbprint> -KeyContainer <keycontainer> -
CryptoProvider <CloudHSM Key Storage Provider/Cavium Key Storage Provider> C:\Users
\Administrator\Desktop\<sample.application>
```

如果命令成功，PowerShell 會傳回成功訊息。

- 若要驗證 檔案上的簽章，請使用下列命令：

```
mage.exe -Verify -CryptoProvider <CloudHSM Key Storage Provider/Cavium Key Storage
Provider> C:\Users\Administrator\Desktop\<sample.application>
```

## 其他第三方廠商與 的整合 AWS CloudHSM

數個第三方供應商支援 AWS CloudHSM 做為信任根。這表示您可以在 CloudHSM 叢集建立和存放基礎金鑰時使用您選擇的軟體解決方案。因此，您在 中的工作負載 AWS 可以依賴 CloudHSM 的延遲、可用性、可靠性和彈性優勢。以下清單包含支援 CloudHSM 的第三方廠商。

 Note

AWS 不為任何第三方廠商背書或提供代金券。

- [Hashicorp Vault](#) 是一種秘密管理工具旨在提供組織之間的協作和控管。它支援 AWS Key Management Service 和 AWS CloudHSM 做為信任根，以提供額外的保護。
- [Thycotic Secrets Server](#) 可協助客戶管理特殊權限帳戶間的敏感登入資料。它支援 AWS CloudHSM 做為信任的根。
- [P6R 的 KMIP 轉接器](#) 可讓您透過標準 KMIP 介面來利用 AWS CloudHSM 執行個體。
- [PrimeKey EJBCA](#) 是一種適用於 PKI 的熱門開放原始碼解決方案。它可讓您安全地建立和存放金鑰對 AWS CloudHSM。
- [Box KeySafe](#) 為具有嚴格安全性、隱私權及法律合規要求的許多組織提供雲端內容的加密金鑰管理。客戶可以透過 AWS CloudHSM AWS KMS 自訂金鑰存放區，在 中直接 AWS Key Management Service 或間接保護 KeySafe 金鑰。
- [Insyde Software](#) 支援 AWS CloudHSM 做為韌體簽署的信任根。
- [F5 BIG-IP LTM](#) 支援 AWS CloudHSM 做為信任的根目錄。
- [Cloudera Navigator Key HSM](#) 可讓您使用 CloudHSM 叢集，來為 Cloudera Navigator Key Trustee 伺服器建立和存放金鑰。
- [Venafi 信任保護平台](#) 透過 AWS CloudHSM 金鑰產生和保護功能為 TLS、SSH 和程式碼簽署提供全面的機器身分管理。

# 監控 AWS CloudHSM

除了用戶端 SDK 內建的記錄功能之外，您也可以使用 AWS CloudTrail Amazon CloudWatch Logs 和 Amazon CloudWatch 進行監控 AWS CloudHSM。

## 用戶端 SDK 日誌

使用 Client SDK 記錄來監視您建立之應用程式的診斷和疑難排解資訊。

## CloudTrail

使用 CloudTrail 來監控您 AWS 帳戶中的所有 API 呼叫，包括您建立和刪除叢集、硬體安全模組 (HSM) 和資源標籤的呼叫。

## CloudWatch Logs

使用 CloudWatch Logs 監控 HSM 執行個體的日誌，其中包括建立和刪除 HSM 使用者的事件、變更使用者密碼、建立和刪除金鑰等。

## CloudWatch

使用 CloudWatch 即時監控您叢集的運作狀態。

## 主題

- [使用 AWS CloudHSM 用戶端 SDK 日誌](#)
- [使用 AWS CloudTrail 和 AWS CloudHSM](#)
- [使用 Amazon CloudWatch Logs 和 AWS CloudHSM Audit Logs](#)
- [取得的 CloudWatch 指標 AWS CloudHSM](#)

# 使用 AWS CloudHSM 用戶端 SDK 日誌

您可以擷取用戶端 SDK 產生的日誌。AWS CloudHSM 提供使用用戶端 SDK 3 和用戶端 SDK 5 記錄的實作。

## 主題

- [用戶端 SDK 5 記錄](#)
- [用戶端 SDK 3 記錄](#)

## 用戶端 SDK 5 記錄

用戶端 SDK 5 日誌包含以元件命名的檔案中每個元件的資訊。您可以使用用戶端 SDK 5 的設定工具來設定每個元件的記錄。

如果您沒有指定檔案的位置，系統會將日誌寫入預設位置：

### PKCS #11 library

- Linux

```
/opt/cloudhsm/run/cloudhsm-pkcs11.log
```

### Windows

```
C:\Program Files\Amazon\CloudHSM\cloudhsm-pkcs11.log
```

### OpenSSL Dynamic Engine

- Linux

```
stderr
```

### JCE provider

- Linux

```
/opt/cloudhsm/run/cloudhsm-jce.log
```

### Windows

```
C:\Program Files\Amazon\CloudHSM\cloudhsm-jce.log
```

如需關於如何設定用戶端 SDK 5 記錄的資訊，請參閱[用戶端 SDK 5 設定工具](#)

## 用戶端 SDK 3 記錄

用戶端 SDK 3 日誌包含來自 AWS CloudHSM 用戶端協助程式的詳細資訊。日誌的位置取決於您執行用戶端常駐程式的 Amazon EC2 用戶端執行個體的作業系統。

### Amazon Linux

在 Amazon Linux 中，AWS CloudHSM 用戶端日誌會寫入名為 `/opt/cloudhsm/run/cloudhsm_client.log` 的檔案。您可以使用 `logrotate` 或類似的工具來輪換和管理這些日誌。

### Amazon Linux 2

在 Amazon Linux 2 中，AWS CloudHSM 用戶端日誌會收集並存放在日誌中。您可以使用 `journalctl` 來檢視和管理這些日誌。例如，使用下列命令來檢視 AWS CloudHSM 用戶端日誌。

```
journalctl -f -u cloudhsm-client
```

### CentOS 7

在 CentOS 7 中，AWS CloudHSM 用戶端日誌會收集並存放在日誌中。您可以使用 `journalctl` 來檢視和管理這些日誌。例如，使用下列命令來檢視 AWS CloudHSM 用戶端日誌。

```
journalctl -f -u cloudhsm-client
```

### CentOS 8

在 CentOS 8 中，AWS CloudHSM 用戶端日誌會收集並存放在日誌中。您可以使用 `journalctl` 來檢視和管理這些日誌。例如，使用下列命令來檢視 AWS CloudHSM 用戶端日誌。

```
journalctl -f -u cloudhsm-client
```

### RHEL 7

在 Red Hat Enterprise Linux 7 中，AWS CloudHSM 用戶端日誌會收集並存放在日誌中。您可以使用 `journalctl` 來檢視和管理這些日誌。例如，使用下列命令來檢視 AWS CloudHSM 用戶端日誌。

```
journalctl -f -u cloudhsm-client
```

### RHEL 8

在 Red Hat Enterprise Linux 8 中，AWS CloudHSM 用戶端日誌會收集並存放在日誌中。您可以使用 `journalctl` 來檢視和管理這些日誌。例如，使用下列命令來檢視 AWS CloudHSM 用戶端日誌。

```
journalctl -f -u cloudhsm-client
```

## Ubuntu 16.04

在 Ubuntu 16.04 中，AWS CloudHSM 用戶端日誌會收集並存放在日誌中。您可以使用 `journalctl` 來檢視和管理這些日誌。例如，使用下列命令來檢視 AWS CloudHSM 用戶端日誌。

```
journalctl -f -u cloudhsm-client
```

## Ubuntu 18.04

在 Ubuntu 18.04 中，AWS CloudHSM 用戶端日誌會收集並存放在日誌中。您可以使用 `journalctl` 來檢視和管理這些日誌。例如，使用下列命令來檢視 AWS CloudHSM 用戶端日誌。

```
journalctl -f -u cloudhsm-client
```

## Windows

- 用於 Windows 用戶端 1.1.2+：

AWS CloudHSM 用戶端日誌會寫入程式 `cloudhsm.log` 檔案資料夾中的檔案 `AWS CloudHSM` (`C:\Program Files\Amazon\CloudHSM\`)。每個日誌檔案名稱都會加上時間戳記，指出 AWS CloudHSM 用戶端何時啟動。

- 用於 Windows 用戶端 1.1.1 和更早版本：

用戶端日誌不會被寫入檔案。日誌會顯示在命令提示字元或您啟動 AWS CloudHSM 用戶端的 PowerShell 視窗中。

## 使用 AWS CloudTrail 和 AWS CloudHSM

AWS CloudHSM 已與整合 AWS CloudTrail，此服務提供使用者、角色或服務在 AWS 中採取動作的記錄 AWS CloudHSM。CloudTrail 會將的所有 API 呼叫擷取 AWS CloudHSM 為事件。擷取的呼叫包括從 AWS CloudHSM 主控台呼叫，以及對 AWS CloudHSM API 操作的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括的事件 AWS CloudHSM。即使您未設定追蹤，依然可以透過 CloudTrail 主控台的事件歷史記錄檢視最新事件。使用 CloudTrail 所收集的資訊，您可以判斷提出的請求 AWS CloudHSM、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。



若要進一步了解 CloudTrail，請參閱「[AWS CloudTrail 使用者指南](#)」。如需 AWS CloudHSM API 操作的完整清單，請參閱 AWS CloudHSM API 參考中的[動作](#)。

## AWS CloudHSM CloudTrail 中的資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。當活動在 中發生時 AWS CloudHSM，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他服務 AWS 事件。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱[使用 CloudTrail 事件歷史記錄檢視事件](#)。

若要不持續記錄您 AWS 帳戶中的事件，包括 的事件 AWS CloudHSM，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有 AWS 區域。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [從多個區域接收 CloudTrail 日誌檔案](#)，以及[從多個帳戶接收 CloudTrail 日誌檔案](#)

CloudTrail 會記錄所有 AWS CloudHSM 操作，包括唯讀操作，例如 DescribeClusters 和 ListTags，以及管理操作，例如 InitializeCluster、CreatHsm 和 DeleteBackup。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 請求是否使用根還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

## 了解 AWS CloudHSM 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示示範 CreateHsm動作的 AWS CloudHSM CloudTrail 日誌項目。

```
{
 "eventVersion": "1.05",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "AR0AJZVM5NEGZSTCITAMM:ExampleSession",
 "arn": "arn:aws:sts::111122223333:assumed-role/AdminRole/ExampleSession",
 "accountId": "111122223333",
 "accessKeyId": "ASIAIY22AX6VRYNBJSA",
 "sessionContext": {
 "attributes": {
 "mfaAuthenticated": "false",
 "creationDate": "2017-07-11T03:48:44Z"
 },
 "sessionIssuer": {
 "type": "Role",
 "principalId": "AR0AJZVM5NEGZSTCITAMM",
 "arn": "arn:aws:iam::111122223333:role/AdminRole",
 "accountId": "111122223333",
 "userName": "AdminRole"
 }
 }
 },
 "eventTime": "2017-07-11T03:50:45Z",
 "eventSource": "cloudhsm.amazonaws.com",
 "eventName": "CreateHsm",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "205.251.233.179",
 "userAgent": "aws-internal/3",
 "requestParameters": {
 "availabilityZone": "us-west-2b",
 "clusterId": "cluster-fw7mh6mayb5"
 },
 "responseElements": {
 "hsm": {
 "eniId": "eni-65338b5a",
 "clusterId": "cluster-fw7mh6mayb5",
 "state": "CREATE_IN_PROGRESS",
 "eniIp": "10.0.2.7",
 "hsmId": "hsm-6lz2hfmnzbx",
 "subnetId": "subnet-02c28c4b",
 "availabilityZone": "us-west-2b"
 }
 }
}
```

```
},
"requestID": "1dae0370-65ec-11e7-a770-6578d63de907",
"eventID": "b73a5617-8508-4c3d-900d-aa8ac9b31d08",
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

## 使用 Amazon CloudWatch Logs 和 AWS CloudHSM Audit Logs

當您帳戶中的 HSM 從 AWS CloudHSM [命令列工具](#)或[軟體程式庫](#)收到命令時，它會以稽核日誌形式記錄命令的執行。HSM 稽核日誌包含所有用戶端啟動的[管理命令](#)，包含建立和刪除 HSM、登入和登出 HSM 以及管理使用者和金鑰的命令。這些日誌提供已變更 HSM 狀態的可靠動作記錄。

AWS CloudHSM 會收集您的 HSM 稽核日誌，並代表您將其傳送至 [Amazon CloudWatch Logs](#)。您可以使用 CloudWatch Logs 的功能來管理 AWS CloudHSM 稽核日誌，包括搜尋和篩選日誌，以及將日誌資料匯出至 Amazon S3。您可以在 [Amazon CloudWatch 主控台](#)中使用 HSM 稽核日誌，或在 [AWS CLI](#) 和 [CloudWatch Logs SDKs](#) 中使用 CloudWatch Logs 命令。

### 主題

- [HSM 稽核記錄的運作方式](#)
- [在 CloudWatch Logs 中檢視 AWS CloudHSM 稽核日誌](#)
- [解譯 AWS CloudHSM 稽核日誌](#)
- [AWS CloudHSM 稽核日誌參考](#)

## HSM 稽核記錄的運作方式

稽核記錄會在所有 AWS CloudHSM 叢集中自動啟用。它無法停用或關閉，而且任何設定都無法 AWS CloudHSM 阻止 將日誌匯出至 CloudWatch Logs。每個日誌事件都具有一個時間戳記和序列號碼，指出事件的順序並協助您偵測任何日誌竄改。

每個 HSM 執行個體都會產生自身的日誌。各種 HSM 的稽核日誌 (甚至是位於相同叢集中的 HSM) 都可能不同。例如，只有每個叢集中的第一個 HSM 會記錄 HSM 的初始化。初始化事件不會出現在從備份複製之 HSM 的日誌中。同樣地，當您建立金鑰時，產生金鑰的 HSM 會記錄金鑰產生事件。其他位於叢集中的 HSM 則會在透過同步接收到金鑰時記錄事件。

AWS CloudHSM 會收集日誌並將其發佈到您帳戶中的 CloudWatch Logs。若要代表您與 CloudWatch Logs 服務通訊，AWS CloudHSM 會使用[服務連結角色](#)。與該角色相關聯的 IAM 政策僅允許 AWS CloudHSM 執行將稽核日誌傳送至 CloudWatch Logs 所需的任務。

### ⚠ Important

若您在 2018 年 1 月 20 日前建立叢集，並且尚未建立連接的服務連結角色，您必須手動建立該角色。這是 CloudWatch 從 AWS CloudHSM 叢集接收稽核日誌的必要條件。如需有關服務連結角色建立的詳細資訊，請參閱[了解服務連接角色](#)，以及 IAM 使用者指南的[建立一個服務連接角色](#)。

## 在 CloudWatch Logs 中檢視 AWS CloudHSM 稽核日誌

Amazon CloudWatch Logs 會將稽核日誌組織到日誌群組，並在日誌群組內組織到日誌串流。每個日誌項目都是 event.createing。會為每個叢集 AWS CloudHSM 建立一個日誌群組，並為叢集中的每個 HSM 建立一個日誌串流。您不需要建立任何 CloudWatch Logs 元件或變更任何設定。

- 日誌群組名稱是 /aws/cloudhsm/<cluster ID>；例如 /aws/cloudhsm/cluster-likphkxygsn。當您在 AWS CLI 或 PowerShell 命令中使用日誌群組名稱時，請務必將它括上雙引號。
- 日誌串流名稱是 HSM ID；例如 hsm-nwbbiqbj4jk。

一般而言，每個 HSM 都有一個日誌串流。不過，任何變更 HSM ID 的動作 (例如 HSM 故障及更換時) 都會建立新的日誌串流。

如需 CloudWatch Logs 概念的詳細資訊，請參閱 Amazon CloudWatch Logs 使用者指南中的[概念](#)。

您可以從 中的 CloudWatch Logs 頁面 AWS Management Console、 中的 [CloudWatch Logs 命令](#) AWS CLI、[CloudWatch Logs PowerShell cmdlets](#) 或 [CloudWatch Logs SDKs](#) 檢視 HSM 的稽核日誌。如需詳細資訊，請參閱 Amazon CloudWatch Logs 使用者指南中的[檢視日誌資料](#)。

例如，下圖顯示 AWS Management Console 中 cluster-likphkxygsn 叢集の日誌群組。

CloudWatch > Log Groups

Create Metric Filter Actions

Filter: Log Group Name Prefix x

Log Groups 1-1

| Log Groups                                              | Expire Events After | Metric Filters | Subscriptions |
|---------------------------------------------------------|---------------------|----------------|---------------|
| <input type="radio"/> /aws/cloudhsm/cluster-likphkxygsn | Never Expire        | 0 filters      | None          |

當您選擇叢集日誌群組名稱時，可以檢視叢集中每個 HSM 的日誌串流。下圖顯示 cluster-likphkxygsn 叢集中 HSM 的日誌串流。

CloudWatch > Log Groups > Streams for /aws/cloudhsm/cluster-likphkxygsn

Search Log Group Create Log Stream Delete Log Stream

Filter: Log Stream Name Prefix x

Log Streams 1-2

| Log Streams                              | Last Event Time        |
|------------------------------------------|------------------------|
| <input type="checkbox"/> hsm-aht4p3sgs3c | 2017-12-28 06:12 UTC-8 |
| <input type="checkbox"/> hsm-xkvjp4wk5o3 | 2017-12-28 06:12 UTC-8 |

當您選擇 HSM 日誌串流名稱時，可以檢視稽核日誌中的事件。例如，此事件 (序號為 0x0 且 Opcode 為 CN\_INIT\_TOKEN) 一般是每個叢集中第一個 HSM 的第一個事件。它記錄叢集中 HSM 的初始化。

| Filter events     |                                                                                                                                                                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time (UTC +00:00) | Message                                                                                                                                                                                                                                                                   |
| 2017-12-19        | <pre>Time: 12/19/17 21:01:16.962174, usecs:1513717276962174 Sequence No : 0x0 Reboot counter : 0xe8 Command Type(hex) : CN_MGMT_CMD (0x0) Opcode : CN_INIT_TOKEN (0x1) Session Handle : 0x1004001 Response : 0:HSM Return: SUCCESS Log type : MINIMAL_LOG_ENTRY (0)</pre> |

您可以使用 CloudWatch Logs 中的所有許多功能來管理稽核日誌。例如，您可以使用篩選事件功能來尋找事件中的特定文字，例如 CN\_CREATE\_USER Opcode。

若要尋找所有未包含指定文字的事件，請在文字前面新增減號 (-)。例如，若要尋找未包含 CN\_CREATE\_USER 的事件，請輸入 -CN\_CREATE\_USER。

| CN_CREATE_USER                                                                                                                                                                                                                                                                                                                                      |                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| Time (UTC +00:00)                                                                                                                                                                                                                                                                                                                                   | Message                           |
| 2017-12-20                                                                                                                                                                                                                                                                                                                                          |                                   |
| No older events                                                                                                                                                                                                                                                                                                                                     |                                   |
| ▼ 00:04:53                                                                                                                                                                                                                                                                                                                                          | Time: 12/20/17 00:04:53.635826, u |
| Time: 12/20/17 00:04:53.635826, usecs:1513728293635826<br>Sequence No : 0x13a<br>Reboot counter : 0xe8<br>Command Type(hex) : CN_MGMT_CMD (0x0)<br>Opcode : CN_CREATE_USER (0x3)<br>Session Handle : 0x1014006<br>Response : 0:HSM Return: SUCCESS<br>Log type : MGMT_USER_DETAILS_LOG (2)<br>User Name : testuser<br>User Type : CN_CRYPT_USER (1) |                                   |

## 解譯 AWS CloudHSM 稽核日誌

HSM 稽核日誌中的事件具有標準欄位。有些事件類型具有額外的欄位，可擷取事件相關的實用資訊。例如，使用者登入和使用管理事件會包含使用者名稱和使用者的使用者類型。金鑰管理命令則包含金鑰控制點。

有數個欄位可提供特別重要的資訊。Opcode 會識別記錄的管理命令。Sequence No 則會識別日誌串流中的事件，指出記錄該事件的順序。

例如，下列範例事件為 HSM 日誌串流中的第二個事件 (Sequence No: 0x1)。它會顯示 HSM 產生密碼加密金鑰，即其啟動常式的一部分。

```
Time: 12/19/17 21:01:17.140812, usecs:1513717277140812
Sequence No : 0x1
Reboot counter : 0xe8
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_GEN_PSWD_ENC_KEY (0x1d)
Session Handle : 0x1004001
Response : 0:HSM Return: SUCCESS
```

```
Log type : MINIMAL_LOG_ENTRY (0)
```

下列欄位常見於稽核日誌中的每個 AWS CloudHSM 事件。

### 時間

事件發生的時間，其時區為 UTC 時區。時間會以可供人閱讀的時間格式，以及單位為微秒的 Unix 時間顯示。

### 重新開機計數器

32 位元的持久性序數計數器，會在 HSM 硬體重新開機時遞增。

日誌串流中的所有事件都具有相同的重新開機計數器值。但是，重新開機計數器對日誌串流來說可能並非唯一，因為相同叢集中不同 HSM 執行個體的計數都可能不同。

### 序號

64 位元的序數計數器，會在發生每個日誌事件時遞增。每個日誌串流中的第一個事件都具有 0x0 的序號。Sequence No 的值之間不應會有任何間隙。序號在日誌串流中是唯一的。

### 命令類型

代表命令種類的十六進位值。AWS CloudHSM 日誌串流中命令的命令類型為 CN\_MGMT\_CMD (0x0) 或 CN\_CERT\_AUTH\_CMD (0x9)。

### Opcode

識別執行的管理命令。如需 AWS CloudHSM 稽核日誌中的 Opcode 值清單，請參閱 [AWS CloudHSM 稽核日誌參考](#)。

### 工作階段控點

識別執行命令及記錄事件的工作階段。

### 回應

記錄針對管理命令的回應。您可以針對 SUCCESS 和 ERROR 值搜尋 Response 欄位。

### 日誌類型

指出記錄命令之日誌的 AWS CloudHSM 日誌類型。

- MINIMAL\_LOG\_ENTRY (0)
- MGMT\_KEY\_DETAILS\_LOG (1)
- MGMT\_USER\_DETAILS\_LOG (2)
- GENERIC\_LOG



## 稽核日誌事件的範例

日誌串流中的事件會記錄 HSM 從建立到刪除的歷史記錄。您可以使用日誌檢閱您 HSM 的生命週期，洞見其操作。當您解譯事件時，請注意表示管理命令或動作的 Opcode，以及指出事件順序的 Sequence No。

### 主題

- [範例：初始化叢集中的第一個 HSM](#)
- [登入及登出事件](#)
- [範例：建立和刪除使用者](#)
- [範例：建立和刪除金鑰對](#)
- [範例：產生及同步金鑰](#)
- [範例：匯出金鑰](#)
- [範例：匯入金鑰](#)
- [範例：共用和取消共用金鑰](#)

### 範例：初始化叢集中的第一個 HSM

每個叢集中第一個 HSM 的稽核日誌串流都與叢集中其他 HSM 的日誌串流有相當大的差異。每個叢集中第一個 HSM 的稽核日誌會記錄其建立和初始化。叢集中其他從備份產生之 HSM 的日誌會從登入事件開始。

#### Important

下列初始化項目不會出現在於 CloudHSM 稽核日誌功能釋出 (2018 年 8 月 30 日) 前初始化之叢集的 CloudWatch 日誌中。如需詳細資訊，請參閱[文件歷史記錄](#)。

下列範例事件會出現在叢集中第一個 HSM 的日誌串流內。日誌中的第一個事件 (帶有 Sequence No 0x0 的事件) 代表初始化 HSM 的命令 (CN\_INIT\_TOKEN)。回應表示命令成功 (Response : 0: HSM Return: SUCCESS)。

```
Time: 12/19/17 21:01:16.962174, usecs:1513717276962174
Sequence No : 0x0
Reboot counter : 0xe8
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_INIT_TOKEN (0x1)
```

```
Session Handle : 0x1004001
Response : 0:HSM Return: SUCCESS
Log type : MINIMAL_LOG_ENTRY (0)
```

此範例日誌串流中的第二個事件 (Sequence No 0x1) 會記錄建立 HSM 使用之密碼加密金鑰的命令 (CN\_GEN\_PSWD\_ENC\_KEY)。

這是每個叢集中第一個 HSM 很典型的過程。因為相同叢集中的後續 HSM 都是第一個 HSM 的複本，他們會使用相同的密碼加密金鑰。

```
Time: 12/19/17 21:01:17.140812, usecs:1513717277140812
Sequence No : 0x1
Reboot counter : 0xe8
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_GEN_PSWD_ENC_KEY (0x1d)
Session Handle : 0x1004001
Response : 0:HSM Return: SUCCESS
Log type : MINIMAL_LOG_ENTRY (0)
```

此範例日誌串流中的第三個事件 (Sequence No 0x2) 為建立「應用裝置使用者 (AU)」[???](#)，即 AWS CloudHSM 服務。涉及 HSM 使用者的事件會包含使用者名稱和使用者類型的額外欄位。

```
Time: 12/19/17 21:01:17.174902, usecs:1513717277174902
Sequence No : 0x2
Reboot counter : 0xe8
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_CREATE_APPLIANCE_USER (0xfc)
Session Handle : 0x1004001
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : app_user
User Type : CN_APPLIANCE_USER (5)
```

此範例日誌串流中的第四個事件 (Sequence No 0x3) 會記錄 CN\_INIT\_DONE 事件，即完成 HSM 初始化。

```
Time: 12/19/17 21:01:17.298914, usecs:1513717277298914
Sequence No : 0x3
Reboot counter : 0xe8
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_INIT_DONE (0x95)
```

```
Session Handle : 0x1004001
Response : 0:HSM Return: SUCCESS
Log type : MINIMAL_LOG_ENTRY (0)
```

您可以依循啟動過程中的剩餘事件。這些事件可能包含幾項登入和登出事件，以及金鑰加密金鑰 (KEK) 的產生。下列事件會記錄變更「前加密主管 (PRECO)」[???](#)密碼的命令。此命令會啟用叢集。

```
Time: 12/13/17 23:04:33.846554, usecs:1513206273846554
Sequence No: 0x1d
Reboot counter: 0xe8
Command Type(hex): CN_MGMT_CMD (0x0)
Opcode: CN_CHANGE_PSWD (0x9)
Session Handle: 0x2010003
Response: 0:HSM Return: SUCCESS
Log type: MGMT_USER_DETAILS_LOG (2)
User Name: admin
User Type: CN_CRYPT0_PRE_OFFICER (6)
```

## 登入及登出事件

當解譯您的稽核日誌時，請注意記錄使用者登入和登出 HSM 的事件。這些事件可協助您判斷從登入到登出命令之間，執行管理命令的使用者序列為何。

例如，此日誌項目會記錄名為 admin 之加密主管的登入。序號 (0x0) 指出這是此日誌串流中的第一個事件。

當使用者登入 HSM 時，叢集中的其他 HSM 也會記錄使用者的登入事件。初始登入事件之後不久，您便可以在叢集中其他 HSM 的日誌串流中找到相對應的登入事件。

```
Time: 01/16/18 01:48:49.824999, usecs:1516067329824999
Sequence No : 0x0
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_LOGIN (0xd)
Session Handle : 0x7014006
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : admin
User Type : CN_CRYPT0_OFFICER (2)
```

以下範例事件會記錄 admin 加密主管登出。序號 (0x2) 指出這是此日誌串流中的第三個事件。

若登入的使用者在沒有登出的情況下關閉工作階段，日誌串流便會包含一個 CN\_APP\_FINALIZE 或關閉工作階段事件 (CN\_SESSION\_CLOSE)，而非 CN\_LOGOUT 事件。與登入事件不同，此登出事件通常只會由執行命令的 HSM 記錄。

```
Time: 01/16/18 01:49:55.993404, usecs:1516067395993404
Sequence No : 0x2
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_LOGOUT (0xe)
Session Handle : 0x7014000
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : admin
User Type : CN_CRYPT0_OFFICER (2)
```

若登入嘗試因為使用者名稱無效而失敗，則 HSM 會記錄一項 CN\_LOGIN 事件，其中包含登入命令中提供的使用者名稱和類型。回應會顯示錯誤訊息 157，解釋使用者名稱不存在。

```
Time: 01/24/18 17:41:39.037255, usecs:1516815699037255
Sequence No : 0x4
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_LOGIN (0xd)
Session Handle : 0xc008002
Response : 157:HSM Error: user isn't initialized or user with this name doesn't exist
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : ExampleUser
User Type : CN_CRYPT0_USER (1)
```

若登入嘗試因為密碼無效而失敗，則 HSM 會記錄一項 CN\_LOGIN 事件，其中包含登入命令中提供的使用者名稱和類型。回應會顯示帶有 RET\_USER\_LOGIN\_FAILURE 錯誤碼的錯誤訊息。

```
Time: 01/24/18 17:44:25.013218, usecs:1516815865013218
Sequence No : 0x5
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_LOGIN (0xd)
Session Handle : 0xc008002
Response : 163:HSM Error: RET_USER_LOGIN_FAILURE
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : testuser
```

```
User Type : CN_CRYPT0_USER (1)
```

## 範例：建立和刪除使用者

此範例會顯示加密管理員 (CO) 建立和刪除使用者時記錄的日誌事件。

第一個事件記錄 CO (admin) 登入 HSM。序號為 0x0 表示此為日誌串流中的第一個事件。事件中也包含了登入使用者的名稱和類型。

```
Time: 01/16/18 01:48:49.824999, usecs:1516067329824999
Sequence No : 0x0
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_LOGIN (0xd)
Session Handle : 0x7014006
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : admin
User Type : CN_CRYPT0_OFFICER (2)
```

日誌串流中的下一個事件 (序號為 0x1) 則記錄了 CO 建立新的加密使用者 (CU)。事件中也包含了新使用者的名稱和類型。

```
Time: 01/16/18 01:49:39.437708, usecs:1516067379437708
Sequence No : 0x1
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_CREATE_USER (0x3)
Session Handle : 0x7014006
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : bob
User Type : CN_CRYPT0_USER (1)
```

然後，CO 會建立另一個加密管理員 (alice)。序號指出此動作是接續在前一個動作之後，期間沒有任何介入動作。

```
Time: 01/16/18 01:49:55.993404, usecs:1516067395993404
Sequence No : 0x2
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_CREATE_CO (0x4)
```

```
Session Handle : 0x7014007
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : alice
User Type : CN_CRYPT0_OFFICER (2)
```

稍後，名為 admin 的 CO 登入並刪除名為 alice 的加密管理員。HSM 記錄 CN\_DELETE\_USER 事件。事件中也包含了遭刪除之使用者的名稱和類型。

```
Time: 01/23/18 19:58:23.451420, usecs:1516737503451420
Sequence No : 0xb
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_DELETE_USER (0xa1)
Session Handle : 0x7014007
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : alice
User Type : CN_CRYPT0_OFFICER (2)
```

### 範例：建立和刪除金鑰對

此範例顯示您建立及刪除金鑰對時，於 HSM 稽核日誌中記錄的事件。

下列事件會記錄名為 crypto\_user 的加密使用者 (CU) 登入 HSM。

```
Time: 12/13/17 23:09:04.648952, usecs:1513206544648952
Sequence No: 0x28
Reboot counter: 0xe8
Command Type(hex): CN_MGMT_CMD (0x0)
Opcode: CN_LOGIN (0xd)
Session Handle: 0x2014005
Response: 0:HSM Return: SUCCESS
Log type: MGMT_USER_DETAILS_LOG (2)
User Name: crypto_user
User Type: CN_CRYPT0_USER (1)
```

接著，CU 會產生一組金鑰對 (CN\_GENERATE\_KEY\_PAIR)。私有金鑰具有金鑰控制代碼 131079。公有金鑰具有金鑰控制代碼 131078。

```
Time: 12/13/17 23:09:04.761594, usecs:1513206544761594
Sequence No: 0x29
```

```
Reboot counter: 0xe8
Command Type(hex): CN_MGMT_CMD (0x0)
Opcode: CN_GENERATE_KEY_PAIR (0x19)
Session Handle: 0x2014004
Response: 0:HSM Return: SUCCESS
Log type: MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle: 131079
Public Key Handle: 131078
```

CU 立即刪除了金鑰對。CN\_DESTROY\_OBJECT 事件會記錄公有金鑰的刪除 (131078)。

```
Time: 12/13/17 23:09:04.813977, usecs:1513206544813977
Sequence No: 0x2a
Reboot counter: 0xe8
Command Type(hex): CN_MGMT_CMD (0x0)
Opcode: CN_DESTROY_OBJECT (0x11)
Session Handle: 0x2014004
Response: 0:HSM Return: SUCCESS
Log type: MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle: 131078
Public Key Handle: 0
```

接著，第二個 CN\_DESTROY\_OBJECT 事件會記錄私有金鑰的刪除 (131079)。

```
Time: 12/13/17 23:09:04.815530, usecs:1513206544815530
Sequence No: 0x2b
Reboot counter: 0xe8
Command Type(hex): CN_MGMT_CMD (0x0)
Opcode: CN_DESTROY_OBJECT (0x11)
Session Handle: 0x2014004
Response: 0:HSM Return: SUCCESS
Log type: MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle: 131079
Public Key Handle: 0
```

最後，CU 登出。

```
Time: 12/13/17 23:09:04.817222, usecs:1513206544817222
Sequence No: 0x2c
Reboot counter: 0xe8
Command Type(hex): CN_MGMT_CMD (0x0)
Opcode: CN_LOGOUT (0xe)
```

```
Session Handle: 0x2014004
Response: 0:HSM Return: SUCCESS
Log type: MGMT_USER_DETAILS_LOG (2)
User Name: crypto_user
User Type: CN_CRYPT0_USER (1)
```

### 範例：產生及同步金鑰

此範例顯示在具有多個 HSM 的叢集中建立金鑰的效果。在其中一個 HSM 上產生的金鑰，會從 HSM 以遮罩物件擷取，然後以遮罩物件插入其他 HSM。

#### Note

用戶端工具可能會無法成功同步金鑰。或是命令可能會包含 `min_srv` 參數，限定將金鑰同步至指定數量的 HSM。無論哪種情況，AWS CloudHSM 服務都會將金鑰與叢集中的其他 HSMs 同步。由於 HSM 僅會在其日誌中記錄用戶端的管理命令，因此伺服器端的同步不會記錄在 HSM 的日誌中。

首先請考慮接收及執行命令的 HSM 日誌串流。日誌串流會針對 HSM ID `hsm-abcde123456` 予以命名，但 HSM ID 未出現在日誌事件中。

首先，`testuser` 加密使用者 (CU) 登入 `hsm-abcde123456` HSM。

```
Time: 01/24/18 00:39:23.172777, usecs:1516754363172777
Sequence No : 0x0
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_LOGIN (0xd)
Session Handle : 0xc008002
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : testuser
User Type : CN_CRYPT0_USER (1)
```

CU 會執行 [exSymKey](#) 命令來產生對稱金鑰。`hsm-abcde123456` HSM 會產生金鑰控點為 262152 的對稱金鑰。HSM 會在其日誌中記錄 `CN_GENERATE_KEY` 事件。

```
Time: 01/24/18 00:39:30.328334, usecs:1516754370328334
Sequence No : 0x1
Reboot counter : 0x107
```



```
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_GENERATE_KEY (0x17)
Session Handle : 0xc008004
Response : 0:HSM Return: SUCCESS
Log type : MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle : 262152
Public Key Handle : 0
```

hsm-abcde123456 之日誌串流中的下一個事件會記錄金鑰同步處理程序中的第一個步驟。從 HSM 將新的金鑰 (金鑰控點 262152) 擷取為遮罩物件。

```
Time: 01/24/18 00:39:30.330956, usecs:1516754370330956
Sequence No : 0x2
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_EXTRACT_MASKED_OBJECT_USER (0xf0)
Session Handle : 0xc008004
Response : 0:HSM Return: SUCCESS
Log type : MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle : 262152
Public Key Handle : 0
```

現在請考慮 HSM hsm-zyxwv987654 (相同叢集中的另一個 HSM) 之日誌串流。此日誌串流也包含 testuser CU 的登入事件。時間值會在使用者登入 hsm-abcde123456 HSM 之後短暫發生。

```
Time: 01/24/18 00:39:23.199740, usecs:1516754363199740
Sequence No : 0xd
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_LOGIN (0xd)
Session Handle : 0x7004004
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : testuser
User Type : CN_CRYPT0_USER (1)
```

此 HSM 的這個日誌串流沒有 CN\_GENERATE\_KEY 事件。但它的事件會記錄與此 HSM 的金鑰同步處理。CN\_INSERT\_MASKED\_OBJECT\_USER 事件會記錄將金鑰 262152 接收為遮罩物件。現在，金鑰 262152 存在於叢集的兩個 HSM 上。

```
Time: 01/24/18 00:39:30.408950, usecs:1516754370408950
Sequence No : 0xe
```

```
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_INSERT_MASKED_OBJECT_USER (0xf1)
Session Handle : 0x7004003
Response : 0:HSM Return: SUCCESS
Log type : MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle : 262152
Public Key Handle : 0
```

CU 使用者登出時，此 CN\_LOGOUT 事件只會顯示在收到命令之 HSM 的日誌串流中。

### 範例：匯出金鑰

此範例顯示加密使用者 (CU) 從含多個 HSM 的叢集匯出金鑰時所記錄的稽核日誌事件。

下列事件會記錄 CU (testuser) 登入 [key\\_mgmt\\_util](#)。

```
Time: 01/24/18 19:42:22.695884, usecs:1516822942695884
Sequence No : 0x26
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_LOGIN (0xd)
Session Handle : 0x7004004
Response : 0:HSM Return: SUCCESS
Log type : MGMT_USER_DETAILS_LOG (2)
User Name : testuser
User Type : CN_CRYPT0_USER (1)
```

CU 執行 [exSymKey](#) 命令來匯出金鑰 7 (256 位元 AES 金鑰)。此命令使用金鑰 6 (HSM 上的 256 位元 AES 金鑰) 做為包裝金鑰。

接收此命令的 HSM 會記錄金鑰 7 (即將匯出的金鑰) 的 CN\_WRAP\_KEY 事件。

```
Time: 01/24/18 19:51:12.860123, usecs:1516823472860123
Sequence No : 0x27
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_WRAP_KEY (0x1a)
Session Handle : 0x7004003
Response : 0:HSM Return: SUCCESS
Log type : MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle : 7
Public Key Handle : 0
```

然後，HSM 會記錄包裝金鑰 (金鑰 6) 的 CN\_NIST\_AES\_WRAP 事件。金鑰會予以包裝後立即予以解除包裝，但 HSM 只會記錄一個事件。

```
Time: 01/24/18 19:51:12.905257, usecs:1516823472905257
Sequence No : 0x28
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_NIST_AES_WRAP (0x1e)
Session Handle : 0x7004003
Response : 0:HSM Return: SUCCESS
Log type : MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle : 6
Public Key Handle : 0
```

exSymKey 命令會將匯出的金鑰寫入至檔案，但不會變更 HSM 上的金鑰。因此，叢集中其他 HSM 的日誌內沒有對應事件。

#### 範例：匯入金鑰

此範例顯示您將金鑰匯入至叢集中的 HSM 時所記錄的稽核日誌事件。在此範例中，加密使用者 (CU) 使用 [imSymKey](#) 命令將 AES 金鑰匯入至 HSM。此命令使用金鑰 6 做為包裝金鑰。

接收這些命令的 HSM 會先記錄金鑰 6 (包裝金鑰) 的 CN\_NIST\_AES\_WRAP 事件。

```
Time: 01/24/18 19:58:23.170518, usecs:1516823903170518
Sequence No : 0x29
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_NIST_AES_WRAP (0x1e)
Session Handle : 0x7004003
Response : 0:HSM Return: SUCCESS
Log type : MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle : 6
Public Key Handle : 0
```

接著，HSM 會記錄代表匯入操作的 CN\_UNWRAP\_KEY 事件。匯入的金鑰會獲指派金鑰控點 11。

```
Time: 01/24/18 19:58:23.200711, usecs:1516823903200711
Sequence No : 0x2a
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_UNWRAP_KEY (0x1b)
```

```
Session Handle : 0x7004003
Response : 0:HSM Return: SUCCESS
Log type : MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle : 11
Public Key Handle : 0
```

產生或匯入新的金鑰時，用戶端工具會自動嘗試同步處理新的金鑰與叢集中的其他 HSM。在此情況下，將金鑰 11 從 HSM 擷取為遮罩物件時，HSM 會記錄 CN\_EXTRACT\_MASKED\_OBJECT\_USER 事件。

```
Time: 01/24/18 19:58:23.203350, usecs:1516823903203350
Sequence No : 0x2b
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_EXTRACT_MASKED_OBJECT_USER (0xf0)
Session Handle : 0x7004003
Response : 0:HSM Return: SUCCESS
Log type : MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle : 11
Public Key Handle : 0
```

叢集中其他 HSM 的日誌串流會反映收到新匯入的金鑰。

例如，此事件會記錄在相同叢集中不同 HSM 的日誌串流內。此 CN\_INSERT\_MASKED\_OBJECT\_USER 事件會記錄收到代表金鑰 11 的遮罩物件。

```
Time: 01/24/18 19:58:23.286793, usecs:1516823903286793
Sequence No : 0xb
Reboot counter : 0x107
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_INSERT_MASKED_OBJECT_USER (0xf1)
Session Handle : 0xc008004
Response : 0:HSM Return: SUCCESS
Log type : MGMT_KEY_DETAILS_LOG (1)
Priv/Secret Key Handle : 11
Public Key Handle : 0
```

### 範例：共用和取消共用金鑰

此範例顯示當加密使用者 (CU) 與其他加密使用者共用或停止共用 ECC 私有金鑰所記錄的稽核日誌事件。CU 可使用 [shareKey](#) 命令，並提供金鑰控制代碼、使用者 ID，及 1 值以共用金鑰，或 0 值以停止共用金鑰。

在下列範例中，接收命令的 HSM 會記錄 CM\_SHARE\_OBJECT 事件，其表示共用操作。

```
Time: 02/08/19 19:35:39.480168, usecs:1549654539480168
Sequence No : 0x3f
Reboot counter : 0x38
Command Type(hex) : CN_MGMT_CMD (0x0)
Opcode : CN_SHARE_OBJECT (0x12)
Session Handle : 0x3014007
Response : 0:HSM Return: SUCCESS
Log type : UNKNOWN_LOG_TYPE (5)
```

## AWS CloudHSM 稽核日誌參考

AWS CloudHSM 在稽核日誌事件中記錄 HSM 管理命令。每個事件都有一個操作碼 (Opcode) 值，以識別發生的動作和其回應。您可以使用 Opcode 值來搜尋、排序和篩選日誌。

下表定義 AWS CloudHSM 稽核日誌中的 Opcode 值。

| 操作碼 (Opcode)             | 描述                                         |
|--------------------------|--------------------------------------------|
| 使用者登入：這些事件包含使用者名稱和使用者類型。 |                                            |
| CN_LOGIN (0xd)           | <a href="#">使用者登入</a>                      |
| CN_LOGOUT (0xe)          | <a href="#">使用者登出</a>                      |
| CN_APP_FINALIZE          | 與 HSM 的連線已關閉。已刪除此連線中的任何工作階段金鑰或規定人數權杖。      |
| CN_CLOSE_SESSION         | 具有 HSM 的工作階段已關閉。已刪除此工作階段中的任何工作階段金鑰或規定人數權杖。 |
| 使用者管理：這些事件包含使用者名稱和使用者類型。 |                                            |
| CN_CREATE_USER (0x3)     | <a href="#">建立加密使用者 (CU)</a>               |
| CN_CREATE_CO             | <a href="#">建立加密管理員 (CO)</a>               |
| CN_DELETE_USER           | <a href="#">刪除使用者</a>                      |
| CN_CHANGE_PSWD           | <a href="#">變更使用者密碼</a>                    |

| 操作碼 (Opcode)                  | 描述                                                                                          |
|-------------------------------|---------------------------------------------------------------------------------------------|
| CN_SET_M_VALUE                | Set <a href="#">規定人數身分驗證</a> (M of N) for a user action                                     |
| CN_APPROVE_TOKEN              | Approve a <a href="#">規定人數身分驗證</a> token for a user action                                  |
| CN_DELETE_TOKEN               | Delete one or more <a href="#">規定人數字符</a>                                                   |
| CN_GET_TOKEN                  | Request a signing token to initiate a <a href="#">規定人數操作</a>                                |
| 金鑰管理：這些事件包含金鑰控制代碼。            |                                                                                             |
| CN_GENERATE_KEY               | <a href="#">產生對稱金鑰</a>                                                                      |
| CN_GENERATE_KEY_PAIR (0x19)   | Generate an asymmetric key pair                                                             |
| CN_CREATE_OBJECT              | Import a public key (without wrapping)                                                      |
| CN_MODIFY_OBJECT              | Set a key attribute                                                                         |
| CN_DESTROY_OBJECT (0x11)      | Deletion of a <a href="#">工作階段金鑰</a>                                                        |
| CN_TOMBSTONE_OBJECT           | Deletion of a <a href="#">權杖金鑰</a>                                                          |
| CN_SHARE_OBJECT               | <a href="#">共用或取消共用金鑰</a>                                                                   |
| CN_WRAP_KEY                   | Export an encrypted copy of a key ( <a href="#">wrapKey</a> )                               |
| CN_UNWRAP_KEY                 | Import an encrypted copy of a key ( <a href="#">unwrapKey</a> )                             |
| CN_DERIVE_KEY                 | Derive a symmetric key from an existing key                                                 |
| CN_NIST_AES_WRAP              | 使用 AES 金鑰加密或解密金鑰                                                                            |
| CN_INSERT_MASKED_OBJECT_USER  | Insert an encrypted key with attributes from another HSM in the cluster.                    |
| CN_EXTRACT_MASKED_OBJECT_USER | Wraps/encrypts a key with attributes from the HSM to be sent to another HSM in the cluster. |

| 操作碼 (Opcode)                     | 描述                                              |
|----------------------------------|-------------------------------------------------|
| Back up HSMs                     |                                                 |
| CN_BACKUP_BEGIN                  | Begin the backup process                        |
| CN_BACKUP_END                    | Completed the backup process                    |
| CN_RESTORE_BEGIN                 | Begin restoring from a backup                   |
| CN_RESTORE_END                   | Completed the restoration process from a backup |
| Certificate-Based Authentication |                                                 |
| CN_CERT_AUTH_STORE_CERT          | Stores the cluster certificate                  |
| HSM Instance Commands            |                                                 |
| CN_INIT_TOKEN (0x1)              | Start the HSM initialization process            |
| CN_INIT_DONE                     | The HSM initialization process has finished     |
| CN_GEN_KEY_ENC_KEY               | Generate a key encryption key (KEK)             |
| CN_GEN_PSWD_ENC_KEY (0x1d)       | Generate a password encryption key (PEK)        |
| HSM crypto commands              |                                                 |
| CN_FIPS_RAND                     | Generate a FIPS-compliant random number         |

## 取得的 CloudWatch 指標 AWS CloudHSM

使用 CloudWatch 即時監控 AWS CloudHSM 叢集。指標可以按區域、叢集 ID 或叢集 ID 和 HSM ID 分類。

AWS/CloudHSM 命名空間包含下列指標：

| 指標                                     | 描述                                                                                                                                  |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| HsmUnhealthy                           | HSM 執行個體未正常運作。AWS CloudHSM 會自動為您取代運作狀態不佳的執行個體。在我們更換 HSM 同時，您可以選擇主動擴展叢集大小以降低效能影響。                                                    |
| HsmTemperature <sup>1</sup>            | 硬體處理器的結合溫度。溫度到達攝氏 110 度時系統會關閉。                                                                                                      |
| HsmKeysSessionOccupied                 | HSM 執行個體使用的工作階段金鑰數目。                                                                                                                |
| HsmKeysTokenOccupied                   | HSM 執行個體和叢集使用的權杖金鑰數目。                                                                                                               |
| HsmSslCtxsOccupied <sup>1</sup>        | HSM 執行個體目前建立的端對端加密通路數目。最多可達 2,048 個通路。                                                                                              |
| HsmSessionCount                        | HSM 執行個體的連線數目。最多可達 2,048 個。根據預設，用戶端常駐程式會設定為在 end-to-end 加密通道下開啟每個 HSM 執行個體的兩個工作階段。AWS CloudHSM 也可以使用 HSM 開啟最多 2 個連線，以監控 HSMs 的運作狀態。 |
| HsmUsersAvailable                      | 可以建立的額外使用者數目。這等於使用者數目上限 (如 HsmUsersMax 所列) 減去至今已建立的使用者。                                                                             |
| HsmUsersMax <sup>1</sup>               | 可以在 HSM 執行個體上建立的使用者數目上限。                                                                                                            |
| InterfaceEth2OctetsInput <sup>1</sup>  | 迄今為止累計傳入 HSM 的流量總和。                                                                                                                 |
| InterfaceEth2OctetsOutput <sup>1</sup> | 迄今為止累計傳出 HSM 的流量總和。                                                                                                                 |

- **【1】** 此指標不適用於 hsm2m.medium。



# AWS CloudHSM 效能資訊

對於生產 AWS CloudHSM 叢集，您應該至少有兩個分散在區域中不同可用區域的硬體安全模組 (HSM) 執行個體。我們建議您測試叢集的負載，以確定您應預期的尖峰負載，然後在叢集中再新增一個 HSM 以確保高可用性。若是需要新產生金鑰持久性的應用程式，建議您至少讓三個 HSM 執行個體分散在一個區域的不同可用區域中。

## 效能資料

AWS CloudHSM 叢集的效能會根據特定工作負載而有所不同。若要提高效能，您可以將其他 HSM 執行個體新增至叢集中。效能可能會因 EC2 執行個體上的組態、資料大小和其他應用程式負載而有所不同。我們鼓勵對您的應用程式進行負載測試，以判斷擴展需求。

下表顯示使用 hsm1.medium 執行個體在 EC2 執行個體上執行之常見密碼編譯演算法的近似效能。

hsm1.medium 的效能資料

| 作業            | 雙 HSM 叢集 <sup>1</sup> | 三個 HSM 叢集 <sup>2</sup> | 六個 HSM 叢集 <sup>3</sup> |
|---------------|-----------------------|------------------------|------------------------|
| RSA 2048 位元符號 | 每秒 2,000 次運算          | 每秒 3,000 次運算           | 每秒 5,000 次運算           |
| EC P256 符號    | 每秒 500 次運算            | 每秒 750 次運算             | 每秒 1,500 次運算           |

下表顯示使用 hsm2m.medium 在 EC2 執行個體上執行之常見密碼編譯演算法的近似效能。

hsm2m.medium 的效能資料

| 作業            | 雙 HSM 叢集 <sup>1</sup> | 三個 HSM 叢集 <sup>2</sup> | 六個 HSM 叢集 <sup>3</sup> |
|---------------|-----------------------|------------------------|------------------------|
| RSA 2048 位元符號 | 2000 操作/秒             | 3000 操作/秒              | 5000 操作/秒              |
| EC P256 符號    | 3000 操作/秒             | 4500 操作/秒              | 7000 操作/秒              |

- [1] 雙 HSM 叢集，其中 Java 多執行緒應用程式在一個 [c4.large EC2 執行個體](#) 上執行，其中一個 HSM 位於與 EC2 執行個體相同的 AZ 中。
- [2] 三個 HSM 叢集，其中 Java 多執行緒應用程式在一個 [c4.large EC2 執行個體](#) 上執行，其中一個 HSM 位於與 EC2 執行個體相同的 AZ 中。

- [3] 六個 HSM 叢集，其中 Java 多執行緒應用程式在一個 [c4.large EC2 執行個體](#) 上執行，其中兩個 HSM 位於與 EC2 執行個體相同的可用區域中。

## HSM 調節

當您的工作負載超過叢集的 HSM 容量時，您會收到錯誤訊息，指出 HSM 忙碌或得到調節。有關發生這種情況時該怎麼做的詳細信息，請參閱 [HSM 調節](#)

# 中的安全性 AWS CloudHSM

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模型](#)將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也為您提供可安全使用的服務。在[AWS 合規計畫](#)中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用的合規計劃 AWS CloudHSM，請參閱[合規計劃的 AWS 服務範圍](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規。

本文件可協助您了解如何在使用時套用共同責任模型 AWS CloudHSM。下列主題說明如何設定 AWS CloudHSM 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 AWS CloudHSM 資源。

## 目錄

- [使用 IAM 政策控制 API 存取](#)
- [中的資料保護 AWS CloudHSM](#)
- [的身分和存取管理 AWS CloudHSM](#)
- [合規](#)
- [中的彈性 AWS CloudHSM](#)
- [中的基礎設施安全 AWS CloudHSM](#)
- [AWS CloudHSM 和 VPC 端點](#)
- [在 中更新管理 AWS CloudHSM](#)

## 使用 IAM 政策控制 API 存取

### 將 IAM 政策升級至 IPv6

AWS CloudHSM 客戶使用 IAM 政策來控制對 AWS CloudHSM APIs 存取，並防止設定範圍以外的任何 IP 地址能夠存取 AWS CloudHSM APIs。

除了 IPv4 之外，託管 AWS CloudHSM APIs `cloudhsmv2.<region>.api.aws` 雙堆疊端點還支援 IPv46。IPv6

需要同時支援 IPv4 和 IPv6 的客戶必須更新其 IP 地址篩選政策來處理 IPv6 地址，否則會影響其 AWS CloudHSM 透過 IPv6 連線至 的能力。

## 誰應該升級？

使用雙定址搭配包含 `aws:sourceip` 的政策客戶會受到此升級的影響。雙定址表示網路同時支援 IPv4 和 IPv6。

如果您使用的是雙定址，則必須更新目前使用 IPv4 格式地址設定的 IAM 政策，以包含 IPv6 格式地址。

如需存取問題的協助，請聯絡 [支援](#)。

### Note

下列客戶不受此升級影響：

- 僅位於 IPv4 網路的客戶。

## 什麼是 IPv6？

IPv6 是新一代 IP 標準，旨在最終取代 IPv4。舊版 IPv4 使用 32 位元定址機制來支援 43 億部裝置。IPv6 改為使用 128 位元定址來支援大約 340 兆兆億（或 2 到第 128 個電源）的裝置。

如需詳細資訊，請參閱 [VPC IPv6 網頁](#)。

```
2001:cdba:0000:0000:0000:0000:3257:9652
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

## 更新 IPv6 的 IAM 政策

IAM 政策目前用於使用 `aws:SourceIp` 篩選條件設定允許的 IP 地址範圍。

雙定址支援 IPv4 和 IPv6 流量。如果您的網路使用雙定址，您必須更新用於 IP 地址篩選的任何 IAM 政策，以包含 IPv6 地址範圍。

例如，以下政策會識別 Condition 元素 `203.0.113.0.*` 中允許的 IPv4 地址範圍 `192.0.2.0.*` 和 。

```
https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
 "Version": "2012-10-17",
 "Statement": {
 "Effect": "Deny",
 "Action": "*",
 "Resource": "*",
 "Condition": {
 "NotIpAddress": {
 "aws:SourceIp": [
 "*192.0.2.0/24*",
 "*203.0.113.0/24*"
]
 },
 "Bool": {
 "aws:ViaAWSService": "false"
 }
 }
 }
}
```

若要更新此政策，請變更 Condition 元素以包含 IPv6 地址範圍 2001:DB8:1234:5678::/64 和 2001:cdba:3257:8593::/64。

#### Note

請勿移除現有的 IPv4 地址，因為需要它們才能回溯相容。

```
"Condition": {
 "NotIpAddress": {
 "aws:SourceIp": [
 "*192.0.2.0/24*", <<DO NOT REMOVE existing IPv4 address>>
 "*203.0.113.0/24*", <<DO NOT REMOVE existing IPv4 address>>
 "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
 "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
]
 },
 "Bool": {
 "aws:ViaAWSService": "false"
 }
}
```

```
}
```

## 確認您的用戶端支援 IPv6

建議使用 `cloudhsmv2.{region}.api.aws` 端點的客戶驗證他們是否可以連線到它。下列步驟說明如何執行驗證。

此範例使用 Linux 和 curl 8.6.0 版，並使用位於 `api.aws` 端點且已啟用 IPv6 的端點 [AWS CloudHSM 的服務端點](#)。

### Note

將 切換 AWS 區域 到用戶端所在的相同區域。在此範例中，我們使用美國東部（維吉尼亞北部） – `us-east-1` 端點。

1. 使用以下 `dig` 命令判斷端點是否以 IPv6 地址解析。

```
dig +short AAAA cloudhsmv2.us-east-1.api.aws
2600:1f18:e2f:4e05:1a8a:948e:7c08:c1c3
```

2. 使用以下 `curl` 命令判斷用戶端網路是否可以進行 IPv6 連線。404 回應代碼表示連線成功，而 0 回應代碼表示連線失敗。

```
curl --ipv6 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
%{response_code}\n" https://cloudhsmv2.us-east-1.api.aws

remote ip: 2600:1f18:e2f:4e05:1a8a:948e:7c08:c1c3
response code: 404
```

如果已識別遠端 IP，且回應代碼不是 0，則已成功使用 IPv6 與端點建立網路連線。遠端 IP 應該是 IPv6 地址，因為作業系統應該選取對用戶端有效的通訊協定。如果遠端 IP 不是 IPv6 地址，請使用下列命令 `curl` 強制使用 IPv4。

```
curl --ipv4 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
%{response_code}\n" https://cloudhsmv2.us-east-1.api.aws

remote ip: 3.123.154.250
response code: 404
```

如果遠端 IP 為空白或回應碼為 0，則用戶端網路或端點的網路路徑為IPv4-only。您可以使用下列curl命令來驗證此組態。

```
curl -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
%{response_code}\n" https://cloudhsmv2.us-east-1.api.aws

remote ip: 3.123.154.250
response code: 404
```

## 中的資料保護 AWS CloudHSM

AWS [共同責任模型](#)適用於 中的資料保護 AWS CloudHSM。如此模型所述，AWS 負責保護執行所有的 全球基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 AWS CloudHSM 或使用主控台、API AWS CLI或其他 AWS 服務 AWS SDKs 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

## 靜態加密

當從 HSM AWS CloudHSM 進行備份時，HSM 會先加密其資料，再將其傳送至 AWS CloudHSM。資料會使用唯一、短暫的加密金鑰進行加密。如需詳細資訊，請參閱[AWS CloudHSM 叢集備份](#)。

## 傳輸中加密

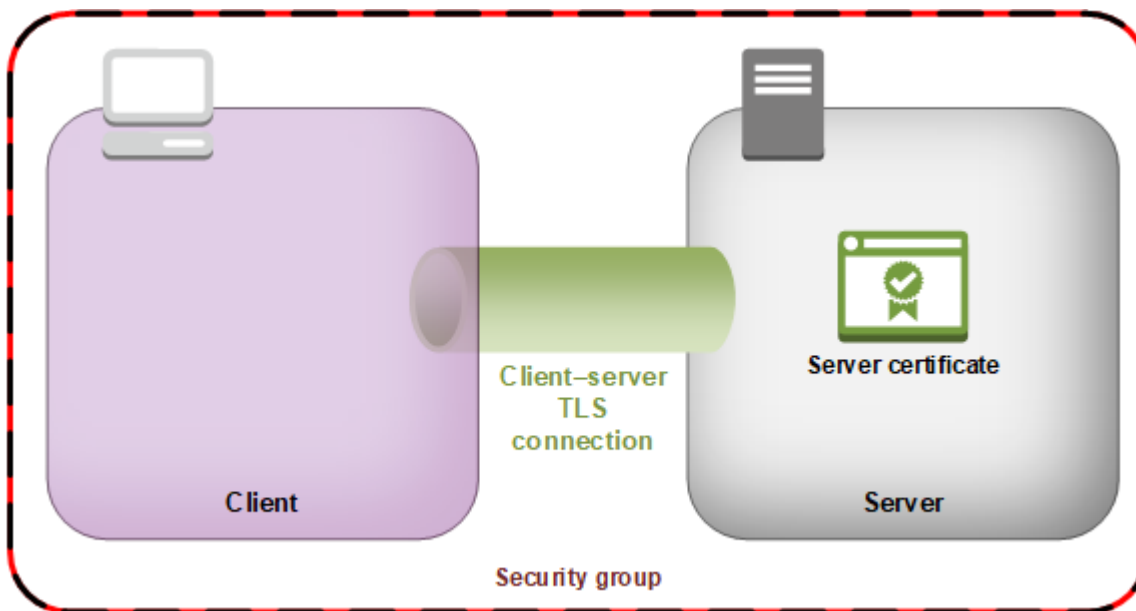
AWS CloudHSM 用戶端與叢集中的 HSM 之間的通訊會端對端加密。只有您的用戶端和 HSM 能解密此通訊。如需詳細資訊，請參閱[端對端加密](#)。

## AWS CloudHSM 用戶端end-to-end加密

會將用戶端執行個體與您叢集中 HSM 之間的通訊進行端對端加密。只有您的用戶端和 HSM 可以解密通訊。

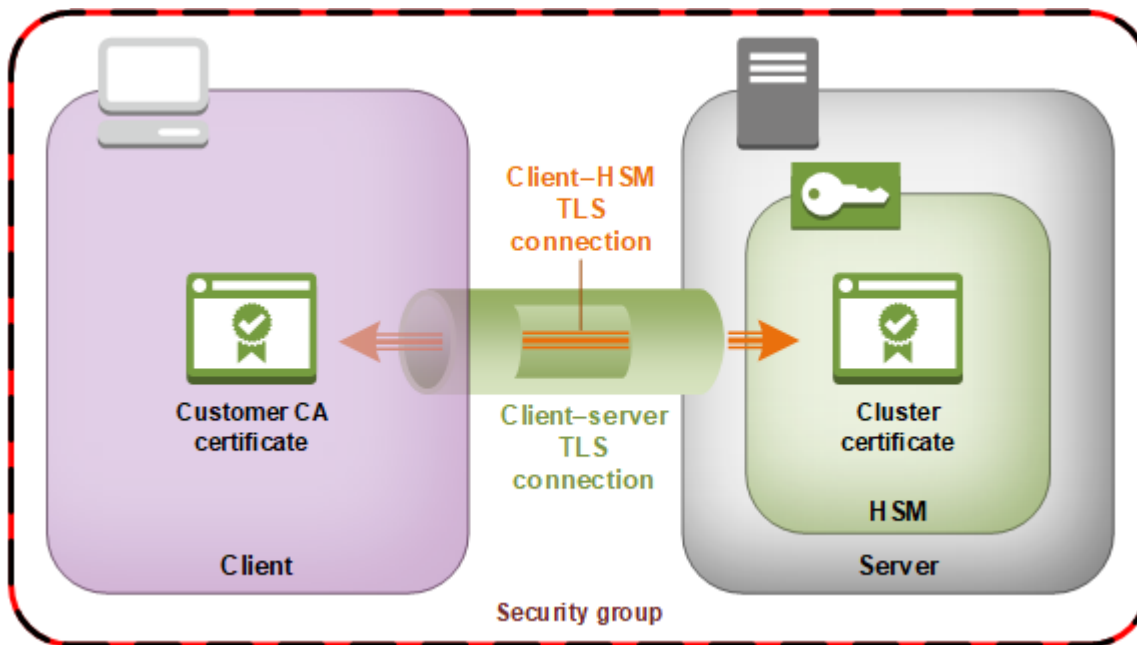
以下程序說明用戶端如何與 HSM 建立端對端加密的通訊。

1. 您的用戶端會與託管 HSM 硬體的伺服器建立 Transport Layer Security (TLS) 連線。您叢集的安全群組僅會允許來自安全群組中用戶端執行個體對伺服器的傳入流量。用戶端也會檢查伺服器的憑證，以確保它是受信任的伺服器。



2. 下一步，用戶端會與 HSM 硬體建立加密連接。HSM 擁有您使用自己的憑證授權單位 (CA) 簽署的叢集憑證，而用戶端會有 CA 的根憑證。在建立用戶端 HSM 的加密連線之前，用戶端會對其根憑證驗證 HSM 的叢集憑證。只有在用戶端成功驗證 HSM 受信任時，才會建立連接。





## 叢集備份的安全性

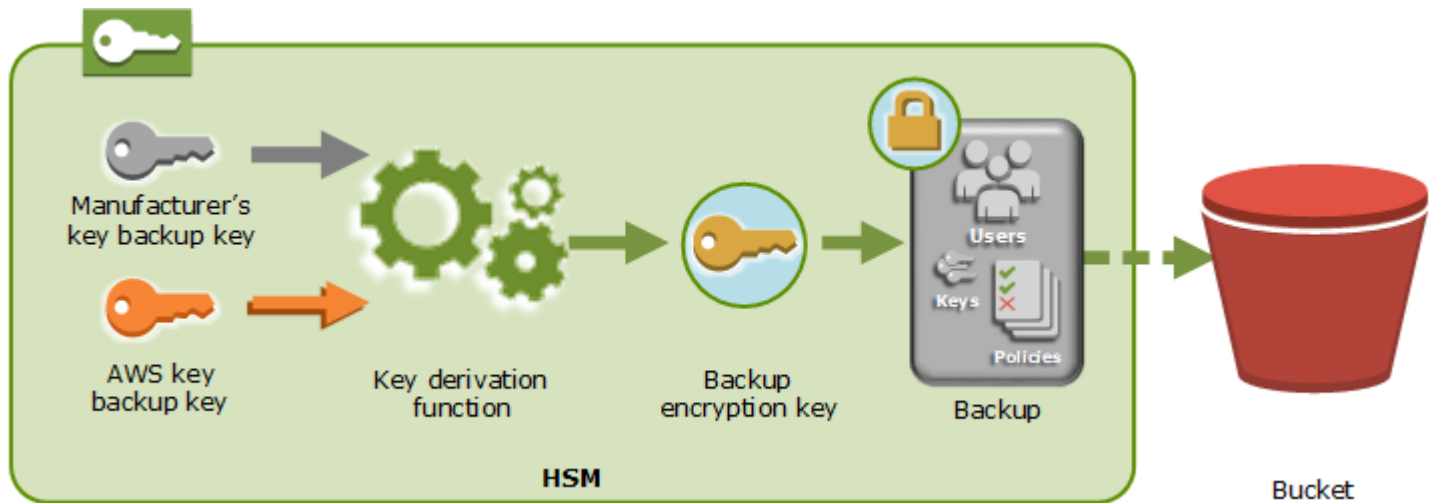
當從 HSM AWS CloudHSM 備份時，HSM 會先加密其所有資料，再將其傳送至 AWS CloudHSM。資料永遠不會以純文字格式離開 HSM。此外，備份無法由解密，AWS 因為 AWS 無法存取用來解密備份的金鑰。

為了加密其資料，HSM 使用唯一、暫時性的加密金鑰，也就是暫時性備份金鑰 (EBK)。EBK 是在 AWS CloudHSM 進行備份時，在 HSM 內產生的 AES 256 位元加密金鑰。HSM 會產生 EBK，然後用它來加密 HSM 的資料，使用符合 [NIST 特刊 800-38F](#)、經 FIPS 核准的 AES 金鑰包裝方法。然後，HSM 會將加密的資料提供給 AWS CloudHSM。加密的資料包含 EBK 加密的複本。

若要加密 EBK，HSM 會使用另一個加密金鑰，稱為持久性備份金鑰 (PBK)。PBK 也是 AES 256 位元加密金鑰。若要產生 PBK，HSM 會在符合 [NIST 特刊 800-108](#) 的計數器模式中使用經 FIPS 核准的金鑰衍生函數 (KDF)。此 KDF 的輸入包括下列項目：

- 製造商金鑰備份金鑰 (MKBK)，由硬體製造商永久內嵌在 HSM 硬體中。
- AWS 金鑰備份金鑰 (AKBK)，最初設定時可安全地安裝在 HSM 中 AWS CloudHSM。

下圖彙總加密程序。備份加密金鑰代表持久性備份金鑰 (PBK) 和暫時性備份金鑰 (EBK)。



AWS CloudHSM 可以將備份還原至相同製造商所建立的僅 AWS 擁有 HSMs。因為每個備份包含來自原始 HSM 的所有使用者、金鑰和組態，還原的 HSM 會包含與原始 HSM 相同的保護和存取控制。還原的資料會將還原之前已在 HSM 上的所有其他資料覆寫。

備份僅包含加密的資料。在服務將備份存放在 Amazon S3 之前，服務會使用 AWS Key Management Service (AWS KMS) 再次加密備份。

## 的身分和存取管理 AWS CloudHSM

AWS 使用安全登入資料來識別您並授予您對 AWS 資源的存取權。您可以使用 AWS Identity and Access Management (IAM) 的功能，允許其他使用者、服務和應用程式完整或有限地使用您的 AWS 資源。您可以在不共用您的安全登入資料的情況下執行這項操作。

預設情況下，IAM 使用者沒有可建立、檢視或修改 AWS 資源的許可。若要允許 IAM 使用者存取資源 (例如負載平衡器)，並執行工作，您可以：

1. 建立 IAM 政策以准許 IAM 使用者使用他們所需的特定資源和 API 動作。
2. 將政策連接到 IAM 使用者所屬的 IAM 使用者或群組。

將政策連接到使用者或使用者群組時，政策會允許或拒絕使用者在特定資源上執行特定任務的許可。

例如，您可以使用 IAM 在 AWS 帳戶下建立使用者與群組。IAM 使用者可以是個人、系統或應用程式。然後，您需要使用 IAM 政策，將許可授予使用者和群組在指定資源上執行特定動作。

## 使用 IAM 政策授予許可

將政策連接到使用者或使用者群組時，政策會允許或拒絕使用者在特定資源上執行特定任務的許可。

IAM 政策為包含一或多個陳述式的 JSON 文件。每個陳述式的結構，如下列範例所示。

```
{
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "<effect>",
 "Action": "<action>",
 "Resource": "<resource-arn>",
 "Condition": {
 "<condition>": {
 "<key>": "<value>"
 }
 }
 }]
}
```

- **Effect** : Effect 可以是 Allow 或 Deny。根據預設，IAM 使用者沒有使用資源和 API 動作的許可，因此所有請求均會遭到拒絕。明確允許覆寫預設值。明確拒絕覆寫任何允許。
- **Action** : Action 是您授予或拒絕許可的特定 API 動作。如需有關指定動作的詳細資訊，請參閱 [的 API 動作 AWS CloudHSM](#)。
- **資源** — 受動作影響的資源。AWS CloudHSM 不支援資源層級許可。您必須使用 \* 萬用字元來指定所有 AWS CloudHSM 資源。
- **Condition** : 您可以選擇性地使用條件來控制政策何時生效。如需詳細資訊，請參閱 [的條件索引鍵 AWS CloudHSM](#)。

如需詳細資訊，請參閱《IAM 使用者指南》<https://docs.aws.amazon.com/IAM/latest/UserGuide/>。

## 的 API 動作 AWS CloudHSM

在 IAM 政策陳述式的動作元素中，您可以指定 AWS CloudHSM 提供的任何 API 動作。您必須以小寫字串 cloudhsm: 做為動作名稱的字首，如下列範例所示。

```
"Action": "cloudhsm:DescribeClusters"
```

若要在單一陳述式中指定多個動作，請將它們括在方括號中，並以逗號分隔，如下列範例所示。

```
"Action": [
 "cloudhsm:DescribeClusters",
 "cloudhsm:DescribeHsm"
```

```
]
```

您也可以使用 \* 萬用字元指定多個動作。下列範例指定 AWS CloudHSM 以開頭的所有 API 動作名稱 List。

```
"Action": "cloudhsm:List"
```

若要指定 的所有 API 動作 AWS CloudHSM，請使用 \* 萬用字元，如下列範例所示。

```
"Action": "cloudhsm:"
```

如需的 API 動作清單 AWS CloudHSM，請參閱[AWS CloudHSM 動作](#)。

## 的條件索引鍵 AWS CloudHSM

在建立政策時，您可以指定控制政策生效時機的條件。每個條件都包含一或多個索引鍵/值對。有全球條件金鑰和服務特定的條件金鑰。

AWS CloudHSM 沒有服務特定的內容索引鍵。

如需有關全域條件金鑰的詳細資訊，請參閱《IAM 使用者指南》中的 [AWS 全域條件上下文金鑰](#)。

## 的預先定義 AWS 受管政策 AWS CloudHSM

AWS 建立的受管政策會針對常用案例授予必要的許可。您可以根據 IAM 使用者對於 AWS CloudHSM 需要的存取權，將這些政策連接到 IAM 使用者：

- `AWSCloudHSMFullAccess` — 授予使用 AWS CloudHSM 功能所需的完整存取權。
- `AWSCloudHSMReadOnlyAccess` — 授予 AWS CloudHSM 功能的唯讀存取權。

## 的客戶受管政策 AWS CloudHSM

建議您為 建立僅包含執行所需許可的 AWS CloudHSM IAM 管理員群組 AWS CloudHSM。將具有適當許可的政策連接至此群組。視需要將 IAM 使用者新增至群組。您新增的每個使用者都會繼承系統管理員群組的政策。

此外，我們建議您根據使用者需要的許可來建立其他使用者群組。這可確保只有受信任的使用者才能存取重要的 API 動作。例如，您可以建立一個使用者群組，用來授予叢集和 HSM 的唯讀存取權。由於此群組不允許使用者刪除叢集或 HSM，因此不受信任的使用者無法影響生產工作負載的可用性。

隨著隨時間增加新的 AWS CloudHSM 管理功能，您可以確保只有信任的使用者才能立即存取。透過在建立時指派有限的許可給政策，您可以稍後手動為其指派新的功能許可。

以下是的範例政策 AWS CloudHSM。如需有關如何建立政策並將其附于 IAM 使用者群組的資訊，請參閱《IAM 使用者指南》中在 [JSON 標籤上建立政策](#)。

### 範例

- [唯讀許可](#)
- [進階使用者許可](#)
- [管理許可](#)

#### Example 範例：唯讀許可

此政策允許存取 DescribeClusters 和 DescribeBackups API 動作。它也包含特定 Amazon EC2 API 動作的其他許可。不過，此政策不允許使用者刪除叢集或 HSM。

```
{
 "Version": "2012-10-17",
 "Statement": {
 "Effect": "Allow",
 "Action": [
 "cloudhsm:DescribeClusters",
 "cloudhsm:DescribeBackups",
 "cloudhsm:ListTags"
],
 "Resource": "*"
 }
}
```

#### Example 範例：進階使用者許可

此政策允許存取 API AWS CloudHSM 動作的子集。其中也包含特定 Amazon EC2 動作的其他許可。不過，此政策不允許使用者刪除叢集或 HSM。您必須包含 iam:CreateServiceLinkedRole 動作，AWS CloudHSM 以允許在帳戶中自動建立 AWSServiceRoleForCloudHSM 服務連結角色。此角色允許 AWS CloudHSM 記錄事件。如需詳細資訊，請參閱[的服務連結角色 AWS CloudHSM](#)。

**Note**

如需查看每個 API 的特定許可，請參閱《服務授權參考》中的[適用於 AWS CloudHSM 的操作、資源和條件金鑰](#)。

```
{
 "Version": "2012-10-17",
 "Statement": {
 "Effect": "Allow",
 "Action": [
 "cloudhsm:DescribeClusters",
 "cloudhsm:DescribeBackups",
 "cloudhsm:CreateCluster",
 "cloudhsm:CreateHsm",
 "cloudhsm:RestoreBackup",
 "cloudhsm:CopyBackupToRegion",
 "cloudhsm:InitializeCluster",
 "cloudhsm:ListTags",
 "cloudhsm:TagResource",
 "cloudhsm:UntagResource",
 "ec2:CreateNetworkInterface",
 "ec2:DescribeNetworkInterfaces",
 "ec2:DescribeNetworkInterfaceAttribute",
 "ec2:DetachNetworkInterface",
 "ec2>DeleteNetworkInterface",
 "ec2:CreateSecurityGroup",
 "ec2:AuthorizeSecurityGroupIngress",
 "ec2:AuthorizeSecurityGroupEgress",
 "ec2:RevokeSecurityGroupEgress",
 "ec2:DescribeSecurityGroups",
 "ec2>DeleteSecurityGroup",
 "ec2:CreateTags",
 "ec2:DescribeVpcs",
 "ec2:DescribeSubnets",
 "iam:CreateServiceLinkedRole"
],
 "Resource": "*"
 }
}
```

## Example 範例：管理許可

此政策允許存取所有 AWS CloudHSM API 動作，包括刪除 HSMs和叢集的動作。其中也包含特定 Amazon EC2 動作的其他許可。您必須包含 `iam:CreateServiceLinkedRole`動作，AWS CloudHSM 以允許在帳戶中自動建立 `AWSServiceRoleForCloudHSM` 服務連結角色。此角色允許 AWS CloudHSM 記錄事件。如需詳細資訊，請參閱[的服務連結角色 AWS CloudHSM](#)。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "cloudhsm:*",
 "ec2:CreateNetworkInterface",
 "ec2:DescribeNetworkInterfaces",
 "ec2:DescribeNetworkInterfaceAttribute",
 "ec2:DetachNetworkInterface",
 "ec2>DeleteNetworkInterface",
 "ec2:CreateSecurityGroup",
 "ec2:AuthorizeSecurityGroupIngress",
 "ec2:AuthorizeSecurityGroupEgress",
 "ec2:RevokeSecurityGroupEgress",
 "ec2:DescribeSecurityGroups",
 "ec2>DeleteSecurityGroup",
 "ec2:CreateTags",
 "ec2:DescribeVpcs",
 "ec2:DescribeSubnets",
 "iam:CreateServiceLinkedRole"
],
 "Resource": "*"
 }
]
}
```

## 的服務連結角色 AWS CloudHSM

您先前建立以[的客戶受管政策 AWS CloudHSM](#)包含 `iam:CreateServiceLinkedRole` action 的 IAM 政策。AWS CloudHSM 定義名為 `AWSServiceRoleForCloudHSM` [的服務連結角色](#)。角色由預先定義，AWS CloudHSM 並包含 AWS CloudHSM 需要代表您呼叫其他 AWS 服務的許可。此角色可讓您更輕鬆地設定服務，因為您不需要手動新增角色政策和信任政策許可。

角色政策允許代表您 AWS CloudHSM 建立 Amazon CloudWatch Logs 日誌群組和日誌串流，以及寫入日誌事件。您可以在下面和 IAM 主控台中檢視此角色政策。

```
{
 "Version": "2018-06-12",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "logs:CreateLogGroup",
 "logs:CreateLogStream",
 "logs:PutLogEvents",
 "logs:DescribeLogStreams"
],
 "Resource": [
 "arn:aws:logs:*:*:*"
]
 }
]
}
```

AWSServiceRoleForCloudHSM 角色的信任政策允許 AWS CloudHSM 擔任該角色。

```
{
 "Version": "2018-06-12",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "cloudhsm.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

## 建立服務連結角色 (自動)

AWS CloudHSM 如果您在建立 AWS CloudHSM 管理員群組時定義的許可中包含 `iam:CreateServiceLinkedRole` 動作，會在您建立叢集時建立 AWSServiceRoleForCloudHSM 角色。請參閱 [的客戶受管政策 AWS CloudHSM](#)。



如果您已經有一或多個叢集，而只想要新增 `AWSServiceRoleForCloudHSM` 角色，您可以使用主控台、[create-cluster](#) 命令或 [CreateCluster](#) API 操作來建立叢集。然後，使用主控台、[delete-cluster](#) 命令或 [DeleteCluster](#) API 操作來刪除叢集。建立新叢集會建立服務連結角色，並將此角色套用到您帳戶中的所有叢集。或者，您可以手動建立角色。如需詳細資訊，請參閱下一節。

#### Note

如果您只是為了新增 `AWSServiceRoleForCloudHSM` 角色而建立叢集，就不需要執行 [入門 AWS CloudHSM](#) 中描述的所有步驟來建立叢集。

## 建立服務連結角色 (手動)

您可以使用 IAM 主控台 AWS CLI 或 API 來建立 `AWSServiceRoleForCloudHSM` 角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立服務連結角色](#)。

## 編輯服務連結角色

AWS CloudHSM 不允許您編輯 `AWSServiceRoleForCloudHSM` 角色。例如，建立角色後，您無法變更其名稱，因為可能有各種實體依名稱來參考該角色。您也無法變更角色政策。但是，您可以使用 IAM 來編輯角色描述。如需更多資訊，請參閱《IAM 使用者指南》中的 [編輯服務連結角色](#)。

## 刪除 服務連結角色

只要已套用服務連結角色的叢集仍然存在，您就無法刪除此服務連結角色。若要刪除角色，您必須先刪除叢集中的每個 HSM，然後刪除叢集。您的帳戶中的每個叢集都必須刪除。然後，您可以使用 IAM 主控台 AWS CLI 或 API 來刪除角色。如需刪除叢集的詳細資訊，請參閱 [刪除 AWS CloudHSM 叢集](#)。如需詳細資訊，請參閱《IAM 使用者指南》中的 [刪除服務連結角色](#)。

## 合規

對於 FIPS 模式的叢集，AWS CloudHSM 提供符合 PCI-PIN、PCI-3DS 和 SOC2 合規要求的 FIPS 核准的 HSMs。AWS CloudHSM 也為客戶提供選擇非 FIPS 模式叢集的選項。如需適用於每個的認證和合規要求的詳細資訊，請參閱 [AWS CloudHSM 叢集模式](#)。

依賴 FIPS 驗證的 HSM 可協助您滿足 AWS 雲端中資料安全的企業、合約和法規合規要求。

## FIPS 140-2 合規

美國聯邦資訊處理標準 (FIPS) 第 140-2 號公報中，美國政府的安全標準具體說明密碼模組的安全要求，以保護敏感資訊。提供的 hsm1.medium HSMs 類型 AWS CloudHSM 已通過 FIPS 140-2 第 3 級認證 ([憑證 #4218](#))。如需詳細資訊，請參閱[硬體的 FIPS 驗證](#)。

## FIPS 140-3 合規

聯邦資訊處理標準 (FIPS) 出版物 140-3 是美國政府安全標準，可指定保護敏感資訊之密碼編譯模組的安全要求。提供的 hsm2m.medium HSMs 類型 AWS CloudHSM 已通過 FIPS 140-3 第 3 級認證 ([憑證 #4703](#))。如需詳細資訊，請參閱[硬體的 FIPS 驗證](#)。

## [PCI DSS 合規](#)

支付卡產業資料安全標準 (PCI DSS) 是一種由 [PCI 安全標準協會](#) 管理的專屬資訊安全標準。提供的 HSMs AWS CloudHSM 符合 PCI DSS。

## [PCI PIN 合規](#)

PCI PIN 針對傳輸、處理和管理個人識別號碼 (PIN) 資料、自動櫃員機和銷售點 (POS) 終端機進行交易時所使用的資訊，提供安全要求和評估標準。提供的 hsm1.medium 和 hsm2m.medium HSMs AWS CloudHSM 都符合 PCI PIN 規範。如需詳細資訊，請參閱文章《AWS CloudHSM 現已通過 PCI PIN 認證》<https://aws.amazon.com/blogs/security/aws-cloudhsm-is-now-pci-pin-certified/>。

## PCI-3DS 合規性

PCI 3DS (或三個網域安全、3-D 安全) 為 EMV 3D 安全電子商務支付提供數據的安全性。PCI 3DS 為線上購物提供了另一層安全性。提供的 hsm1.medium HSMs 類型 AWS CloudHSM 符合 PCI-3DS 規範。

## SOC2

SOC2 是協助服務組織展示其雲端和資料中心安全控制的架構。AWS CloudHSM 已在關鍵領域實作 SOC2 控制，以遵循可信任的服務原則。如需詳細資訊，請參閱 [《AWS SOC 常見問答集頁面》](#)。

## AWS CloudHSM PCI-PIN 合規FAQs

PCI PIN 針對傳輸、處理和管理個人識別號碼 (PIN) 資料、自動櫃員機和銷售點 (POS) 終端機進行交易時所使用的資訊，提供安全要求和評估標準。

客戶可透過 AWS Artifact (可隨選存取 AWS 合規報告的自助入口網站) 取得 PCI-PIN 合規聲明文件 (AOC) 和責任摘要。如需詳細資訊，請在 [AWS 管理主控台登入 AWS Artifact](#)，或在 [《AWS Artifact 入門指南》](#) 中進一步了解。

## 常見問答集

問：什麼是合規聲明文件和責任摘要？

合規證明 (AOC) 是由合格 PIN 評估者 (QPA) 所產生，證明 AWS CloudHSM 符合 PCI-PIN 標準中的適用控制項。責任摘要矩陣說明 AWS CloudHSM 及其客戶的個別責任控制。

問：如何取得合規 AWS CloudHSM 證明？

客戶可透過 AWS Artifact (自助入口網站) 取得 PCI-PIN 合規聲明文件 (AOC)。AWS Artifact 是一個可隨需存取 AWS 合規報告的自助入口網站。如需詳細資訊，請在 [AWS 管理主控台登入 AWS Artifact](#)，或在 [《AWS Artifact 入門指南》](#) 中進一步了解。

問：如何了解我負責哪些 PCI PIN 控制項？

如需詳細資訊，請參閱 AWS PCI PIN 合規套件中的「AWS CloudHSM PCI PIN 責任摘要」，該套件可透過 AWS Artifact 供客戶使用。AWS Artifact 是一種自助式入口網站，可讓您隨需存取 AWS 合規報告。如需詳細資訊，請在 [AWS 管理主控台登入 AWS Artifact](#)，或在 [《AWS Artifact 入門指南》](#) 中進一步了解。

問：身為 AWS CloudHSM 客戶，我可以依賴 PCI-PIN 合規證明 (AOC) 嗎？

客戶必須管理自己的 PCI-PIN 合規性。您需要透過合格的 PIN 評估員 (QPA) 進行正式的 PCI-PIN 證明程序，以驗證您的付款工作負載是否符合所有 PCI-PIN 控制項/需求。不過，對於 AWS 負責的控制項，您的 QPA 可以依賴合規證明 AWS CloudHSM (AOC)，而無需進一步測試。

問：AWS CloudHSM 是否負責與金鑰管理生命週期相關的 PCI-PIN 要求？

AWS CloudHSM 負責 HSMs 的實體裝置生命週期。客戶負責 PCI-PIN 標準中的金鑰管理生命週期需求。

問：哪些 AWS CloudHSM 控制項符合 PCI-PIN 規範？

AOC 摘要說明 QPA 評估的 AWS CloudHSM 控制項。客戶可透過 AWS Artifact 取得 PCI-PIN 責任摘要。AWS Artifact 是一個可隨需存取 AWS 合規報告的自助入口網站。

問：是否 AWS CloudHSM 支援 PIN 轉譯和 DUKPT 等付款函數？

否，AWS CloudHSM 提供一般用途 HSMs。隨著時間的推移，我們可能會提供付款功能。雖然服務不會直接執行付款功能，AWS CloudHSM 但 PCI PIN 合規證明可讓客戶為其執行的服務達成自己的 PCI 合規 AWS CloudHSM。如果您有興趣在工作負載中使用 AWS 付款加密服務，請參閱部落格「[使用 AWS 付款加密技術將付款處理移至雲端](#)」。

## 棄用通知

有時候，AWS CloudHSM 可能會棄用功能，以保持符合 FIPS 140、PCI-DSS、PCI-PIN、PCI-3DS, SOC2 的要求，或因為end-of-support硬體。此頁面會列出目前套用的變更。

### HSM1 棄用

hsm1.medium 執行個體類型將於 AWS CloudHSM 2025 年 12 月 1 日終止支援。為了確保持續服務，我們推出了下列變更：

- 從 2025 年 4 月開始，您將無法建立新的 hsm1.medium 叢集。
- 從 2025 年 4 月開始，我們將開始自動將現有的 hsm1.medium 叢集遷移至新的 hsm2m.medium 執行個體類型。

hsm2m.medium 執行個體類型與您目前的 AWS CloudHSM 執行個體類型相容，並提升效能。若要避免中斷應用程式，您必須升級至最新版本的用戶端 SDK。如需升級說明，請參閱 [???。](#)

您有兩種遷移選項：

1. 當您準備好時，選擇加入 CloudHSM 受管遷移。如需更多詳細資訊，[???。](#)
2. 從 hsm1 叢集的備份建立新的 hsm2m.medium 叢集，並將您的應用程式重新導向至新的叢集。建議您針對此方法使用藍/綠部署策略。如需詳細資訊，請參閱[???。](#)

### FIPS 140 合規性：2024 機制棄用

美國國家標準技術研究院 (NIST) <sup>1</sup> 建議，在 2023 年 12 月 31 日之後不允許對三重 DES (DESede、3DES、DES3) 加密以及 RSA 金鑰包裝和取消包裝 (採用 PKCS #1 v1.5 的填充方式) 的支援。因此，在我們的聯邦資訊處理標準 (FIPS) 模式叢集中，對這些的支援將於 2024 年 1 月 1 日結束。在非 FIPs 模式下，叢集仍支援這些項目。

本指南適用於下列密碼編譯操作：

- 三重 DES 金鑰產生

- CKM\_DES3\_KEY\_GEN 對於 PKCS #11 程式庫
- DESede JCE 提供商的註冊機
- genSymKey 與 -t=21 用於 KMU 中
- 使用三重 DES 金鑰進行加密 (注意：允許解密操作)
  - 對於 PKCS #11 程式庫：CKM\_DES3\_CBC 加密、CKM\_DES3\_CBC\_PAD 加密和 CKM\_DES3\_ECB 加密
  - 對於 JCE 提供商：DESede/CBC/PKCS5Padding 加密、DESede/CBC/NoPadding 加密、DESede/ECB/Padding 加密和 DESede/ECB/NoPadding 加密
- 使用 PKCS #1 v1.5 填充進行 RSA 金鑰包裝、取消包裝、加密和解密
  - CKM\_RSA\_PKCS 為 PKCS #11 SDK 進行包裝、取消包裝、加密和解密
  - RSA/ECB/PKCS1Padding 包裝、取消包裝、加密和解密 JCE SDK
  - wrapKey、unwrapKey 與 -m 12 用於 KMU (注意：12 是機制 RSA\_PKCS 的值)

[1] 有關此變更的詳細信息，請參閱 [《過渡使用加密算法和密鑰長度》](#) 中的表 1 和表 5。

## 中的彈性 AWS CloudHSM

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置的。AWS 區域提供多個實體隔離和隔離的可用區域，這些區域以低延遲、高輸送量和高度備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。如需支援彈性之 AWS CloudHSM 功能的詳細資訊，請參閱 [AWS CloudHSM 叢集高可用性和負載平衡](#)。

## 中的基礎設施安全 AWS CloudHSM

作為受管服務，AWS CloudHSM 受到 [Amazon Web Services：安全程序概觀](#) 白皮書中所述的 AWS 全球網路安全程序的保護。

您可以使用 AWS 發佈的 API 呼叫，AWS CloudHSM 透過網路存取。此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 [AWS Security Token Service](#) (AWS STS) 來產生暫時安全憑證來簽署請求。

## 網路隔離

虛擬私有雲端 (VPC) 是 AWS 雲端中您自己邏輯隔離區域中的虛擬網路。您可以在 VPC 的私有子網路中建立叢集。您可以在建立 VPC 時建立私有子網路。如需詳細資訊，請參閱[建立的虛擬私有雲端 \(VPC\) AWS CloudHSM](#)。

當您建立 HSM 時，請在子網路中 AWS CloudHSM 輸入彈性網路界面 (ENI)，以便與 HSMs 互動。如需詳細資訊，請參閱[AWS CloudHSM 叢集架構](#)。

AWS CloudHSM 會建立安全群組，允許叢集中的 HSMs 之間的傳入和傳出通訊。您可以使用此安全群組，讓 EC2 執行個體與叢集中的 HSM 通訊。如需詳細資訊，請參閱[設定的用戶端 Amazon EC2 執行個體安全群組 AWS CloudHSM](#)。

## 使用者的授權

使用時 AWS CloudHSM，在 HSM 上執行的操作需要已驗證 HSM 使用者的登入資料。如需詳細資訊，請參閱[the section called “使用者類型”](#)。

## AWS CloudHSM 和 VPC 端點

您可以在 VPC 和 之間建立私有連線，AWS CloudHSM 方法是建立介面 VPC 端點。介面端點採用[AWS PrivateLink](#)技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線的情況下私下存取 AWS CloudHSM APIs。VPC 中的執行個體不需要公有 IP 地址即可與 AWS CloudHSM APIs 通訊。您的 VPC 與 AWS CloudHSM 之間的網路流量都會在 Amazon 網路的範圍內。

每個介面端點都是由您子網路中的一或多個[彈性網路介面](#)表示。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的界面 [VPC 端點 \(AWS PrivateLink\)](#)。

## AWS CloudHSM VPC 端點的考量事項

設定介面 VPC 端點之前 AWS CloudHSM，請務必檢閱《Amazon VPC 使用者指南》中的[介面端點屬性和限制](#)。

- AWS CloudHSM 支援從您的 VPC 呼叫其所有 API 動作。

## 為 AWS CloudHSM 建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 來建立 AWS CloudHSM 服務的 VPC 端點 AWS CLI。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[建立介面端點](#)。



若要為 建立 VPC 端點 AWS CloudHSM，請使用下列服務名稱：

```
com.amazonaws.<region>.cloudhsmv2
```

例如，在美國西部 (奧勒岡) 區域 (us-west-2)，服務名稱為：

```
com.amazonaws.us-west-2.cloudhsmv2
```

若要更容易使用 VPC 端點，您可以為 VPC 端點啟用[私人 DNS 主機名稱](#)。如果您選取啟用私有 DNS 名稱選項，標準 AWS CloudHSM DNS 主機名稱 (https://cloudhsmv2.<region>.amazonaws.com 和 https://cloudhsmv2.<region>.api.aws) 會解析為您的 VPC 端點。

此選項可讓您更輕鬆使用 VPC 端點。根據預設，AWS SDKs 和 AWS CLI 會使用標準 AWS CloudHSM DNS 主機名稱，因此您不需要在應用程式和命令中指定 VPC 端點 URL。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[透過介面端點存取服務](#)。

## 為 建立 VPC 端點政策 AWS CloudHSM

您可以將端點政策連接至控制 AWS CloudHSM存取權限的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的[使用 VPC 端點控制對服務的存取](#)。

範例：AWS CloudHSM 動作的 VPC 端點政策

以下是 端點政策的範例 AWS CloudHSM。連接到端點時，此政策會授予所有資源上所有委託人的所列 AWS CloudHSM 動作的存取權。如需其他 AWS CloudHSM 動作及其對應的 IAM 許可[的身分和存取管理 AWS CloudHSM](#)，請參閱。

```
{
 "Statement": [
 {
 "Principal": "*",
 "Effect": "Allow",
```

```
 "Action":[
 "<cloudhsm>:<DescribeBackups>",
 "<cloudhsm>:<DescribeClusters>",
 "<cloudhsm>:<ListTags>",
],
 "Resource": "*"
}
]
```

## 在 中更新管理 AWS CloudHSM

AWS 會管理韌體。韌體由第三方維護，且 NIST 必須根據 hsm 類型評估 FIPS 140-2 第 3 級或 FIPS 140-3 第 3 級合規。只能安裝由 FIPS 金鑰 (AWS 沒有存取權) 以密碼編譯方式簽署的韌體。



# 故障診斷 AWS CloudHSM

如果您遇到 問題 AWS CloudHSM，下列主題可協助您解決這些問題。

## 主題

- [AWS CloudHSM 已知問題](#)
- [AWS CloudHSM 用戶端 SDK 3 金鑰同步失敗](#)
- [AWS CloudHSM 用戶端 SDK 3 使用 pkpspeed 工具驗證 HSM 效能](#)
- [AWS CloudHSM 用戶端 SDK 5 使用者包含不一致的值](#)
- [AWS CloudHSM 用戶端 SDK 5 使用者複寫失敗](#)
- [AWS CloudHSM 用戶端 SDK 5 金鑰複寫失敗](#)
- [AWS CloudHSM 在金鑰可用性檢查期間看到的錯誤](#)
- [AWS CloudHSM 使用 JCE 擷取金鑰](#)
- [HSM 調節](#)
- [讓 HSM 使用者在 AWS CloudHSM 叢集中的 HSMs 之間保持同步](#)
- [與叢集的 AWS CloudHSM 連線中斷](#)
- [CloudWatch 中缺少 AWS CloudHSM 稽核日誌](#)
- [中 AES 金鑰包裝長度不合規的自訂 IVs AWS CloudHSM](#)
- [解決 AWS CloudHSM 叢集建立失敗](#)
- [擷取 AWS CloudHSM 用戶端組態日誌](#)

## AWS CloudHSM 已知問題

AWS CloudHSM 有下列已知問題。選擇主題以進一步了解。

## 主題

- [所有 HSM 執行個體的已知問題](#)
- [hsm1.medium AWS CloudHSM 執行個體的已知問題](#)
- [hsm2m.medium AWS CloudHSM 執行個體的已知問題](#)
- [PKCS #11 程式庫的已知問題 AWS CloudHSM](#)

- [適用於的 JCE 開發套件的已知問題 AWS CloudHSM](#)
- [適用於的 OpenSSL 動態引擎的已知問題 AWS CloudHSM](#)
- [的金鑰儲存提供者 \(KSP\) 的已知問題 AWS CloudHSM](#)
- [使用執行 Amazon Linux 2 的 Amazon EC2 執行個體的已知問題 AWS CloudHSM](#)
- [整合第三方應用程式與的已知問題 AWS CloudHSM](#)
- [AWS CloudHSM 叢集修改的已知問題](#)
- [在 hsm2.medium 上使用 AWS CloudHSM 用戶端 5.12.0 版的已知操作失敗問題](#)

## 所有 HSM 執行個體的已知問題

下列問題會影響 AWS CloudHSM 所有使用者，無論他們是使用 key\_mgmt\_util 命令列工具、PKCS #11 SDK、JCE SDK 或 OpenSSL SDK。

### 主題

- [問題：AES 金鑰包裝使用 PKCS #5 填補，而不是使用零填補的金鑰包裝標準合規實作。](#)
- [問題：用戶端常駐程式的組態檔案中至少要有一個有效的 IP 地址，才能成功連接到叢集。](#)
- [問題：資料上限為 16 KB，可使用 AWS CloudHSM 用戶端 SDK 3 進行雜湊和簽署](#)
- [問題：匯入的金鑰無法指定為不可匯出](#)
- [問題：key\\_mgmt\\_util 中的 wrapKey 和 unWrapKey 命令預設機制已移除。](#)
- [問題：如果在您的叢集中有單一 HSM，HSM 容錯移轉無法正常運作。](#)
- [問題：如果您在短期內超過您叢集中 HSM 的金鑰容量，用戶端會進入未處理的錯誤狀態。](#)
- [問題：不支援使用 800 位元組以上的 HMAC 金鑰進行摘要操作。](#)
- [問題：隨用戶端 SDK 3 散發的 client\\_info 工具會刪除選用輸出引數所指定的路徑內容](#)
- [問題：在容器化環境中使用 --cluster-id 引數執行 SDK 5 設定工具時收到錯誤。](#)
- [問題：您收到錯誤「無法從提供的 pfx 檔案建立 cert/key。錯誤：NotPkcs8」](#)
- [問題：ECDSA 簽署失敗，並從 SDK 5.16 開始出現「無效的機制」錯誤](#)

問題：AES 金鑰包裝使用 PKCS #5 填補，而不是使用零填補的金鑰包裝標準合規實作。

此外，不支援無填補和零填補的金鑰包裝。

- **影響：**如果您使用此演算法在其中包裝和取消包裝，則不會有任何影響 AWS CloudHSM。不過，包裝的金鑰 AWS CloudHSM 無法在預期符合無填補規格的其他 HSMs 或軟體內取消包裝。這是因為在標準合規取消包裝期間，系統可能會在金鑰資料後加上 8 個位元組的資料填補。外部包裝的金鑰無法正確取消包裝到 AWS CloudHSM 執行個體中。
- **因應措施：**若要將在 AWS CloudHSM 執行個體上使用含 PKCS #5 填補的「AES 金鑰包裝」包裝的金鑰在外部取消包裝，在嘗試使用該金鑰前請先去除額外的填補。您可以在檔案編輯器裁剪額外的位元組，或是只將金鑰的位元組複製到程式碼中的新緩衝區。
- **解決方案狀態：**在 3.1.0 用戶端和軟體版本中，AWS CloudHSM 為 AES 金鑰包裝提供符合標準的選項。如需詳細資訊，請參閱[AES 金鑰包裝](#)。

**問題：**用戶端常駐程式的組態檔案中至少要有一個有效的 IP 地址，才能成功連接到叢集。

- **影響：**如果您刪除叢集中的每個 HSM，然後新增另一個 HSM，該 HSM 會得到新 IP 地址，而用戶端協助程式會繼續在原來的 IP 地址搜尋您的 HSM。
- **因應措施：**如果您執行不穩定的工作負載，建議您在 [CreateHsm](#) 函數中使用 `IpAddress` 參數，將彈性網絡介面 (ENI) 設定為其原始值。請注意，ENI 為可用區域 (AZ) 專用。另一個替代的做法是，刪除 `/opt/cloudhsm/daemon/1/cluster.info` 檔案，然後將用戶端組態重設為新 HSM 的 IP 地址。您也可以使用 `client -a <IP address>` 命令。如需詳細資訊，請參閱[安裝和設定用戶端 AWS CloudHSM \(Linux\)](#) 或[安裝和設定 AWS CloudHSM 用戶端 \(Windows\)](#)。

**問題：**資料上限為 16 KB，可使用 AWS CloudHSM 用戶端 SDK 3 進行雜湊和簽署

- **解決狀態：**會將小於 16KB 的資料繼續傳送至 HSM 進行雜湊處理。我們已新增可在本機、軟體、大小在 16KB 與 64KB 之間的資料進行雜湊處理的功能。如果資料緩衝區大於 64KB，用戶端 SDK 5 會明確失敗。您必須將用戶端和 SDK 更新至大於 5.0.0 或更新版本的版本，才能從修正中獲益。

**問題：**匯入的金鑰無法指定為不可匯出

- **解決狀態：**已修正此問題。您的部分無須採取任何動作，即可受益於修正。

**問題：**`key_mgmt_util` 中的 `wrapKey` 和 `unWrapKey` 命令預設機制已移除。

- **解決方法：**使用 `wrapKey` 或 `unWrapKey` 命令時，您必須使用 `-m` 選項來指定機制。如需詳細資訊，請參閱[wrapKey](#) 或 [unWrapKey](#) 文章中的範例。

**問題：**如果在您的叢集中有單一 HSM，HSM 容錯移轉無法正常運作。

- **影響：**如果您叢集中的單一 HSM 執行個體失去連線，即使之後還原 HSM 執行個體，用戶端也將不會與此執行個體連線。
- **因應措施：**我們建議至少在任一生產叢集中執行兩個 HSM 執行個體。如果您使用此組態，您將不會受到此問題影響。如果是單一 HSM 叢集，請退回用戶端協助程式，以還原連線。
- **解決狀態：**此狀態已在 AWS CloudHSM 用戶端 1.1.2 版本中解決。您必須升級到此用戶端，以受益於此修正。

**問題：**如果您在短期內超過您叢集中 HSM 的金鑰容量，用戶端會進入未處理的錯誤狀態。

- **影響：**用戶端遇到未處理的錯誤狀態時，用戶端會凍結且必須重新啟動。
- **因應措施：**請測試您的傳輸量，以確保您並非以用戶端無法處理的速率建立工作階段金鑰。您可以新增 HSM 至叢集，或減慢工作階段金鑰的建立速度，藉以降低速率。
- **解決狀態：**此狀態已在 AWS CloudHSM 用戶端 1.1.2 版本中解決。您必須升級到此用戶端，以受益於此修正。

**問題：**不支援使用 800 位元組以上的 HMAC 金鑰進行摘要操作。

- **影響：**800 位元組以上的 HMAC 金鑰可以在 HSM 上產生或匯入 HSM。然而，如果您透過 JCE 或 `key_mgmt_util` 在摘要操作中使用較大的金鑰，此次操作將會失敗。請注意，如果您使用 PKCS11，HMAC 金鑰的大小限制為 64 位元組。
- **因應措施：**如果您將 HMAC 金鑰用於 HSM 上的摘要操作，請大小小於 800 位元組。
- **解決狀態：**此時並無。

**問題：**隨用戶端 SDK 3 散發的 `client_info` 工具會刪除選用輸出引數所指定的路徑內容

- **影響：**指定輸出路徑下的所有現有檔案和子目錄可能永久遺失。
- **因應措施：**使用 `client_info` 工具時，請勿使用選用引數 `-output path`。
- **解決狀態：**此狀態已在[用戶端 3.3.2 版本](#)中解決。您必須升級到此用戶端，以受益於此修正。

問題：在容器化環境中使用 **--cluster-id** 引數執行 SDK 5 設定工具時收到錯誤。

使用 --叢集-id 引數搭配使用 [設定工具] 時，您會收到下列錯誤：

No credentials in the property bag

執行個體中繼資料服務版本 2 (IMDSv2) 的更新造成此錯誤。如需詳細資訊，請參閱 [IMDSv2](#) 文件。

- 影響：此問題會影響在容器化環境中在 SDK 5.5.0 及更新版本上執行設定工具的使用者，以及使用 EC2 執行個體中繼資料提供憑證。
- 解決方法：將 PUT 回應跳轉限制設定為至少兩個。如需如何執行此操作的指引，請參閱[設定執行個體中繼資料選項](#)。

問題：您收到錯誤「無法從提供的 pfx 檔案建立 cert/key。錯誤：NotPkcs8」

- 解決方法：您可以使用 openssl 命令將自訂 SSL 私有金鑰轉換為 PKCS8 格式：`openssl pkcs8 -topk8 -inform PEM -outform PEM -in ssl_private_key -out ssl_private_key_pkcs8`
- 解決狀態：此問題已在[用戶端 SDK 5.12.0 版本](#)中解決。您必須升級至此用戶端版本 或更新版本，才能從修正中獲益。

問題：ECDSA 簽署失敗，並從 SDK 5.16 開始出現「無效的機制」錯誤

- 影響：使用比金鑰強度更弱的雜湊函數時，ECDSA 簽署操作失敗。發生此失敗是因為 [FIPS 186-5](#) 要求雜湊函數至少與金鑰強度一樣強。

您可能會在用戶端日誌中看到類似這樣的錯誤：

```
[cloudhsm_provider::hsm1::session::ecdsa::sign::common][][] Digest security strength (80) is weaker than the key security strength (128)
```

- 解決方法：如果您無法更新雜湊函數，您可以遷移至非 FIPS 叢集，這不會強制執行雜湊強度要求。不過，我們建議您更新雜湊函數，以維持 FIPS 合規。

作為額外的解決方法，我們新增了組態選項來略過此要求。請注意，不建議使用此選項，因為使用具有較弱雜湊函數的 ECDSA 不會遵循安全最佳實務。若要使用此選項，請執行下列命令 (configure-cli 使用所使用 SDK 的設定工具取代 [the section called “語法”](#))：

```
sudo /opt/cloudhsm/bin/configure-cli --enable-ecdsa-with-weak-hash-function
```

- 解決方案：使用至少與您的 ECDSA 金鑰一樣強大的雜湊函數。如需雜湊函數和 ECDSA 金鑰強度的資訊，請參閱 [NIST SP 800-57 第 1 部分修訂版 5](#) 中的資料表 2 和 3。

## hsm1.medium AWS CloudHSM 執行個體的已知問題

下列問題會影響所有 AWS CloudHSM hsm1.medium 執行個體。

### 主題

- [問題：HSM 無法建立超過 250 個使用者](#)

### 問題：HSM 無法建立超過 250 個使用者

- 解決方法：此問題已在 AWS CloudHSM hsm2m.medium 執行個體類型上解決。
- 解決狀態：此時並無。

## hsm2m.medium AWS CloudHSM 執行個體的已知問題

下列問題會影響所有 AWS CloudHSM hsm2m.medium 執行個體。

### 主題

- [問題：hsm2m.medium 的登入延遲增加](#)
- [問題：使用 嘗試設定金鑰受信任屬性的 CO 會在用戶端 SDK 5.12.0 和更早版本中失敗](#)
- [問題：對於 FIPS 模式下的叢集，ECDSA 驗證將使用用戶端 SDK 5.12.0 和更早版本失敗](#)
- [問題：只有 PEM 格式的憑證可以向 CloudHSM CLI 註冊為 mtls 信任錨點](#)
- [問題：使用 mTLS 搭配密碼短語保護的用戶端私有金鑰時，客戶應用程式將停止處理所有請求。](#)
- [問題：使用 CloudHSM CLI 時，使用者複寫失敗](#)
- [問題：建立備份期間操作可能會失敗](#)
- [問題：在 hsm2m.medium 的某些案例中，用戶端 SDK 5.8 及更高版本不會對 HSM 限流操作執行自動重試](#)

## 問題：hsm2m.medium 的登入延遲增加

- 影響：hsm2m.medium 遵循最新的 FIPS 140-3 第 3 級要求。登入 hsm2m.medium 遵循增強的安全性和合規要求，這會導致延遲增加。
- 解決方法：如果可能，在相同的應用程式中序列化登入請求，以避免在登入期間延長延遲。並行的多個登入請求會導致延遲增加。

## 問題：使用 嘗試設定金鑰受信任屬性的 CO 會在用戶端 SDK 5.12.0 和更早版本中失敗

- 影響：任何嘗試設定金鑰信任屬性的 CO 使用者都會收到錯誤，指出 User type should be CO or CU。
- 解決方案：用戶端 SDK 的未來版本將解決此問題。更新將在使用者指南的 [中宣布文件歷史紀錄](#)。

## 問題：對於 FIPS 模式下的叢集，ECDSA 驗證將使用用戶端 SDK 5.12.0 和更早版本失敗

- 影響：ECDSA 驗證在 FIPS 模式下為 HSMs 執行的操作將會失敗。
- 解決狀態：此問題已在[用戶端 SDK 5.13.0 版本](#)中解決。您必須升級至此用戶端版本 或更新版本，才能從修正中獲益。

## 問題：只有 PEM 格式的憑證可以向 CloudHSM CLI 註冊為 mtls 信任錨點

- 影響：DER 格式的憑證無法向 CloudHSM CLI 註冊為 mTLS 信任錨點。
- 解決方法：您可以使用 openssl 命令，將 DER 格式的憑證轉換為 PEM 格式：`openssl x509 -inform DER -outform PEM -in certificate.der -out certificate.pem`

## 問題：使用 mTLS 搭配密碼短語保護的[用戶端私有金鑰](#)時，客戶應用程式將停止處理所有請求。

- 影響：應用程式執行的所有操作都將停止，並在整個應用程式生命週期內多次提示使用者輸入標準輸入的複雜密碼。如果未在操作逾時持續時間之前提供密碼短語，則操作會逾時並失敗。
- 解決方法：mTLS 不支援複雜密碼加密的私有金鑰。從用戶端私有金鑰移除複雜密碼加密



## 問題：使用 CloudHSM CLI 時，使用者複寫失敗

- 影響：使用 CloudHSM CLI 時，hsm2m.medium 執行個體上的使用者複寫失敗。user replicate 命令在 hsm1.medium 執行個體上如預期般運作。
- 解決方案：我們正在努力解決此問題。如需更新，請參閱《使用者指南[文件歷史紀錄](#)》中的。

## 問題：建立備份期間操作可能會失敗

- 影響：在 AWS CloudHSM 建立備份時，產生隨機數字之類的操作可能會在 hsm2m.medium 執行個體上失敗。
- 解決方案：為將服務中斷降至最低，請實作下列最佳實務：
  - 建立多 HSM 叢集
  - 設定您的應用程式以重試叢集操作

如需最佳實務的詳細資訊，請參閱「[的最佳實務 AWS CloudHSM](#)」。

## 問題：在 hsm2m.medium 的某些案例中，用戶端 SDK 5.8 及更高版本不會對 HSM 限流操作執行自動重試

- 影響：用戶端 SDK 5.8 及更高版本不會重試某些 HSM 限流操作
- 解決方法：遵循最佳實務來架構叢集，以處理負載並實作應用程式層級重試。我們目前正在進行修正。更新將在使用者指南的 中宣布[文件歷史紀錄](#)。

## PKCS #11 程式庫的已知問題 AWS CloudHSM

下列問題會影響 PKCS #11 程式庫 AWS CloudHSM。

### 主題

- [問題：PKCS #11 程式庫 3.0.0 版中的 AES 金鑰包裝不會在使用前驗證 IV。](#)
- [問題：PKCS #11 SDK 2.0.4 和先前的版本一律會針對 AES 金鑰包裝和取消包裝使用 0xA6A6A6A6A6A6A6A6 預設 IV。](#)
- [問題：既未支援也未處理 CKA\\_DERIVE 屬性。](#)
- [問題：既未支援也未處理 CKA\\_SENSITIVE 屬性。](#)
- [問題：不支援分段雜湊和簽署。](#)



- [問題：C\\_GenerateKeyPair 不是以符合標準的方式處理私有範本中的 CKA\\_MODULUS\\_BITS 或 CKA\\_PUBLIC\\_EXPONENT。](#)
- [問題：使用 CKM\\_AES\\_GCM 機制時，C\\_Encrypt 和 C\\_Decrypt API 操作的緩衝區不能超過 16 KB。](#)
- [問題：在 HSM 中橢圓曲線 Diffie-Hellman \(ECDH\) 金鑰衍生只會部分執行。](#)
- [問題：驗證 secp256k1 簽章在 EL6 平台上失敗，例如 CentOS6 和 RHEL 6](#)
- [問題：不正確的函數調用序列會給出未定義的結果而不是失敗](#)
- [問題：SDK 5 不支援唯讀工作階段](#)
- [問題：cryptoki.h 標頭檔案僅限 Windows](#)

問題：PKCS #11 程式庫 3.0.0 版中的 AES 金鑰包裝不會在使用前驗證 IV。

如果您指定的 IV 長度小於 8 個位元組，便會在使用之前利用無法預測的位元組進行填補。

 Note

這只會影響包含 CKM\_AES\_KEY\_WRAP 機制的 C\_WrapKey。

- 影響：如果您在 PKCS #11 程序庫 3.0.0 版中提供的 IV 長度小於 8 個位元組。您便可能無法取消包裝金鑰。
- 因應措施：
  - 我們強烈建議您升級到 PKCS #11 程式庫 3.0.1 或更新版本，這些新版本會在 AES 金鑰包裝期間強制要求 IV 長度。修改您的包裝程式碼以傳遞 NULL IV，或是指定預設 IV 0xA6A6A6A6A6A6A6A6。如需詳細資訊，請參閱 [AES 金鑰包裝的非合規長度自訂 IV](#)。
  - 如果您已搭配長度小於 8 個位元組的 IV 使用 PKCS #11 程式庫 3.0.0 包裝任何金鑰，請聯絡我們以取得[支援](#)。
- 解決狀態：此問題已在 PKCS #11 程式庫 3.0.1 中解決。如要使用 AES 金鑰包裝來包裝金鑰，請指定 NULL 或長度為 8 個位元組的 IV。

問題：PKCS #11 SDK 2.0.4 和先前的版本一律會針對 AES 金鑰包裝和取消包裝使用 **0xA6A6A6A6A6A6A6A6** 預設 IV。

使用者提供的 IV 會在無提示的情況下遭到忽略。

 Note

這只會影響包含 CKM\_AES\_KEY\_WRAP 機制的 C\_WrapKey。

- Impact: (影響：)
  - 如果您使用 PKCS #11 程式庫 2.0.4 或先前版本及使用者提供的 IV，您的金鑰會使用預設 IV 0xA6A6A6A6A6A6A6A6 進行包裝。
  - 如果您使用 PKCS #11 程式庫 3.0.0 或更新版本及使用者提供的 IV，您的金鑰則會使用使用者提供的 IV 進行包裝。
- Workarounds: (因應措施：)
  - 如要取消包裝使用 PKCS #11 程式庫 2.0.4 或先前版本包裝的金鑰，請使用預設 IV 0xA6A6A6A6A6A6A6A6。
  - 如要取消包裝使用 PKCS #11 程式庫 3.0.0 及更新版本包裝的金鑰，請使用使用者提供的 IV。
- Resolution status: (解決狀態：) 我們強烈建議您修改您的包裝和取消包裝程式碼，以傳遞 NULL IV，或是指定預設 IV 0xA6A6A6A6A6A6A6A6。

**問題：既未支援也未處理 CKA\_DERIVE 屬性。**

- 解決狀態：我們已實作修正接受金鑰 CKA\_DERIVE (如果設定為 FALSE)。在我們開始將金鑰衍生函數支援新增至 AWS CloudHSM 前，不支援將 CKA\_DERIVE 設定為 TRUE。您必須將用戶端和程式庫更新至 1.1.1 版或更高版本，才能受益於修正。

**問題：既未支援也未處理 CKA\_SENSITIVE 屬性。**

- 解決狀態：我們已實作可以接受和正確遵守 CKA\_SENSITIVE 屬性的修正。您必須將用戶端和程式庫更新至 1.1.1 版或更高版本，才能受益於修正。

**問題：不支援分段雜湊和簽署。**

- 影響：不會實作 C\_DigestUpdate 和 C\_DigestFinal。C\_SignFinal 也不會實作，非 NULL 緩衝區會失敗並發生 CKR\_ARGUMENTS\_BAD 錯誤。
- 解決方法：在應用程式中雜湊您的資料，並 AWS CloudHSM 僅用於簽署雜湊。

- 解決狀態：我們正在進行修復，讓用戶端和程式庫能夠正確實作分段雜湊。更新會公告於 AWS CloudHSM 論壇和版本歷史頁面中。

**問題：C\_GenerateKeyPair 不是以符合標準的方式處理私有範本中的 CKA\_MODULUS\_BITS 或 CKA\_PUBLIC\_EXPONENT。**

- 影響：當私有範本包含 CKA\_MODULUS\_BITS 或 CKA\_PUBLIC\_EXPONENT，C\_GenerateKeyPair 應該傳回 CKA\_TEMPLATE\_INCONSISTENT。但它反而產生私有金鑰，將所有使用欄位設為 FALSE。無法使用金鑰。
- 因應措施：建議您的應用程式除了錯誤碼，也檢查使用欄位值。
- 解決狀態：我們正在實作修正，讓系統在使用錯誤的私有金鑰範本時傳回適當的錯誤訊息。會在版本歷史頁面中公告更新的 PKCS #11 程式庫。

**問題：使用 CKM\_AES\_GCM 機制時，C\_Encrypt 和 C\_Decrypt API 操作的緩衝區不能超過 16 KB。**

AWS CloudHSM 不支援分段 AES-GCM 加密。

- 影響：您不能使用 CKM\_AES\_GCM 機制來加密大於 16 KB 的資料。
- 解決方法：您可以使用替代機制，例如 CKM\_AES\_CBC、CKM\_AES\_CBC\_PAD 或 ，您可以將資料分割為片段，並使用 AES\_GCM 個別方式加密每個片段。如果您使用的是 AES\_GCM，則必須管理資料的分割和後續加密。AWS CloudHSM 不會為您執行分段 AES-GCM 加密。請注意，FIPS 要求在 HSM 上 AES-GCM 產生的初始化向量 (IV)。因此，AES-GCM 加密資料之每個片段的 IV 都不同。
- 解決狀態：我們正在進行修復，讓程式庫在資料緩衝區過大時明確失敗。我們會針對 C\_EncryptUpdate 和 C\_DecryptUpdate API 操作傳回 CKR\_MECHANISM\_INVALID。我們正在評估支援較大緩衝區、而不需要仰賴分段加密的替代做法。更新將在 AWS CloudHSM 論壇和版本歷史記錄頁面上宣布。

**問題：在 HSM 中橢圓曲線 Diffie-Hellman (ECDH) 金鑰衍生只會部分執行。**

您的 EC 私有金鑰仍一律保留在 HSM 中，但金鑰衍生程序會分成多個步驟執行。因此，在用戶端會有每個步驟產生的中繼結果。

- 影響：在用戶端 SDK 3 中，使用 CKM\_ECDH1\_DERIVE 機制衍生的金鑰首先可在用戶端上使用，然後匯入 HSM。然後將金鑰控制代碼傳回給到您的應用程式。

- 因應措施：如果您在 AWS CloudHSM 中實作 SSL/TLS 卸載，此限制可能不是問題。如果您的應用程式要求金鑰需隨時符合 FIPS，請考慮使用其他不倚賴 ECDH 金鑰衍生的通訊協定。
- 解決狀態：SDK 5.16 現在支援具有金鑰衍生的 ECDH，完全在 HSM 內執行。

### 問題：驗證 secp256k1 簽章在 EL6 平台上失敗，例如 CentOS6 和 RHEL 6

這是因為 CloudHSM PKCS#11 程式庫會使用 OpenSSL 來驗證 EC 曲線資料，藉此避免在驗證操作初始化期間進行網路呼叫。由於 EL6 平台上的預設 OpenSSL 套件並不支援 Secp256k1，初始化作業會失敗。

- 影響：無法在 EL6 平台上進行 Secp256k1 簽章驗證，驗證呼叫會失敗並出現 CKR\_HOST\_MEMORY 錯誤。
- 因應措施：若 PKCS#11 應用程式需要驗證 secp256k1 簽章，則建議使用 Amazon Linux 1 或任何 EL7 平台。或者，您可將 OpenSSL 套件升級至支援 secp256k1 曲線的版本。
- 解決狀態：我們正在實作修正，以便在無法驗證本機曲線的情況下切換回 HSM。[版本歷史記錄](#)頁面中會公告更新的 PKCS#11 程式庫。

### 問題：不正確的函數調用序列會給出未定義的結果而不是失敗

- 影響：如果您調用不正確的函數序列，即使個別函數調用傳回成功，最終結果也不正確。例如，解密的資料可能與原始純文本不匹配，否則簽名可能無法驗證。此問題會影響單一和多部分作業。

函數序列不正確的範例：

- C\_EncryptInit/C\_EncryptUpdate 後跟 C\_Encrypt
- C\_DecryptInit/C\_DecryptUpdate 後跟 C\_Decrypt
- C\_SignInit/C\_SignUpdate 後跟 C\_Sign
- C\_VerifyInit/C\_VerifyUpdate 後跟 C\_Verify
- C\_FindObjectsInit 後跟 C\_FindObjectsInit
- 因應措施：您的應用程式應在符合 PKCS #11 規格的情況下，針對單一和多部分作業使用正確的函數調用順序。在此情況下，您的應用程式不應該依賴 CloudHSM PKCS #11 程式庫來傳回錯誤。

### 問題：SDK 5 不支援唯讀工作階段

- 問題：C\_OpenSession 的 SDK 5 不支援使用開啟唯讀工作階段。

- 影響：如果您嘗試在未提供的 CKF\_RW\_SESSION 情況下調用 C\_OpenSession，調用將失敗並顯示錯誤 CKR\_FUNCTION\_FAILED。
- 因應措施：開啟工作階段時，您必須將 CKF\_SERIAL\_SESSION | CKF\_RW\_SESSION 旗標傳遞至 C\_OpenSession 函數調用。

## 問題：cryptoki.h 標頭檔案僅限 Windows

- 問題：使用 Linux 上的 AWS CloudHSM 用戶端 SDK 5 版本 5.0.0 到 5.4.0，標頭檔案/opt/cloudhsm/include/pkcs11/cryptoki.h僅與 Windows 作業系統相容。
- 影響：嘗試在 Linux 作業系統的應用程式中包含此標頭檔案時，可能會遇到問題。
- 解決狀態：升級至 AWS CloudHSM 用戶端 SDK 5 5.4.1 版或更新版本，其中包含此標頭檔案的 Linux 相容版本。

## 適用於的 JCE 開發套件的已知問題 AWS CloudHSM

下列問題會影響的 JCE 開發套件 AWS CloudHSM。

### 主題

- [問題：使用非對稱金鑰對時，即使未明確建立或匯入金鑰，仍會看到已佔用的金鑰容量](#)
- [問題：JCE KeyStore 是唯讀的。](#)
- [問題：AES-GCM 加密的緩衝區不能超過 16,000 位元組。](#)
- [問題：在 HSM 中橢圓曲線 Diffie-Hellman \(ECDH\) 金鑰衍生只會部分執行。](#)
- [問題：KeyGenerator 和 KeyAttribute 錯誤地將金鑰大小參數解釋為位元組數而非位元數](#)
- [問題：用戶端 SDK 5 會發出警告「發生了非法的反射式存取作業」](#)
- [問題：JCE 工作階段集區已用盡](#)
- [問題：用戶端 SDK 5 記憶體流失搭配 getKey 操作](#)

## 問題：使用非對稱金鑰對時，即使未明確建立或匯入金鑰，仍會看到已佔用的金鑰容量

- 影響：此問題可能導致 HSM 意外用盡金鑰空間，並在您的應用程式使用標準 JCE 金鑰物件 (而非 CaviumKey 物件) 進行加密操作時發生。當您使用標準 JCE 金鑰物件時，CaviumProvider 會隱含地將該金鑰匯入 HSM 做為工作階段金鑰，且不會刪除此金鑰，直到應用程式結束為止。因此，金鑰會在應用程式執行時不斷累積，可能導致您的 HSM 用盡可用的金鑰空間，進而凍結您的應用程式。

- 因應措施：使用 `CaviumSignature` 類別、`CaviumCipher` 類別、`CaviumMac` 類別或 `CaviumKeyAgreement` 類別時，您應提供金鑰做為 `CaviumKey`，而非標準 JCE 金鑰物件。

您可以使用 [ImportKey](#) 類手動將普通金鑰轉換為 `CaviumKey`，然後在操作完成後手動刪除該金鑰。

- 解決狀態：我們正在更新 `CaviumProvider` 以正確管理隱含匯入。修正可供使用時即會在版本歷史頁面中公告。

**問題：**JCE KeyStore 是唯讀的。

- 影響：無法將 HSM 不支援的物件類型存放在 JCE 金鑰存放區中。特別是您無法在金鑰存放區中存放憑證。這會防止與 `jarsigner` 之類之工具 (其會預期在金鑰存放區中尋找憑證) 之間的互通性。
- 因應措施：您可以重新處理程式碼，從本機檔案或從 S3 儲存貯體位置 (而不是從金鑰存放區) 載入憑證。
- 解決狀態：您可以使用 AWS CloudHSM 金鑰存放區來存放憑證。

**問題：**AES-GCM 加密的緩衝區不能超過 16,000 位元組。

此外，也不支援分段的 AES-GCM 加密。

- 影響：您無法使用 AES-GCM 來加密大於 16,000 位元組的資料。
- 因應措施：您可以使用替代機制 (例如 AES-CBC)，或者可以將資料切分成數段，並個別加密每一個部分。如果切分資料，您必須管理切分後的加密文字及其解密。由於 FIPS 規定 AES-GCM 的初始向量 (IV) 要在 HSM 上產生，AES-GCM 加密之每個資料片段的 IV 都不同。
- 解決狀態：我們正在進行修復，讓程式庫在資料緩衝區過大時明確失敗。我們正在評估支援較大緩衝區、而不需要仰賴分段加密的替代做法。更新會公告於 AWS CloudHSM 論壇和版本歷史頁面中。

**問題：**在 HSM 中橢圓曲線 Diffie-Hellman (ECDH) 金鑰衍生只會部分執行。

您的 EC 私有金鑰仍一律保留在 HSM 中，但金鑰衍生程序會分成多個步驟執行。因此，在用戶端會有每個步驟產生的中繼結果。您可在 [Java 程式碼範例](#) 中查看 ECDH 金鑰衍生範例。

- 影響：用戶端 SDK 3 將 ECDH 功能新增至 JCE。當您使用 `KeyAgreement` 類別衍生 `SecretKey` 時，它首先可在用戶端上使用，然後匯入 HSM。然後將金鑰控制代碼傳回給到您的應用程式。
- 解決方法：如果您在中實作 SSL/TLS 卸載 AWS CloudHSM，則此限制可能不是問題。如果您的應用程式要求金鑰需隨時符合 FIPS，請考慮使用其他不倚賴 ECDH 金鑰衍生的通訊協定。



- 解決狀態：SDK 5.16 現在支援具有金鑰衍生的 ECDH，而金鑰衍生完全在 HSM 內執行。

**問題：**KeyGenerator 和 KeyAttribute 錯誤地將金鑰大小參數解釋為位元組數而非位元數

當使用 [KeyGenerator 類別](#) 的 init 函數或 [AWS CloudHSM KeyAttribute 列舉](#) 的 SIZE 屬性產生金鑰時，API 錯誤地預期引數是金鑰位元組的數目，但實際是金鑰位元的數目。

- 影響：用戶端 SDK 版本 5.4.0 至 5.4.2 錯誤地預期金鑰大小會以位元組形式提供給指定的 API。
- 解決方法：在使用用戶端 SDK 5.4.0 到 5.4.2 版 AWS CloudHSM 時，使用 KeyGenerator 類別或 KeyAttribute 列舉來產生金鑰之前，請先將金鑰大小從位元轉換為位元組。
- 解析狀態：升級您的用戶端 SDK 版本到 5.5.0 或更高版本，其中包括使用 KeyGenerator 類別或 KeyAttribute 列舉產生金鑰時正確期望金鑰大小的位元修正。

**問題：**用戶端 SDK 5 會發出警告「發生了非法的反射式存取作業」

當您將用戶端 SDK 5 與 Java 11 搭配使用時，CloudHSM 會擲回下列 Java 警告：

```
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by
 com.amazonaws.cloudhsm.jce.provider.CloudHsmKeyStore (file:/opt/cloudhsm/java/
cloudhsm-jce-5.6.0.jar) to field java.security .KeyStore.keyStoreSpi
WARNING: Please consider reporting this to the maintainers of
 com.amazonaws.cloudhsm.jce.provider.CloudHsmKeyStore
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective
access operations
WARNING: All illegal access operations will be denied in a future release
```

此問題已在用戶端 SDK 5.8 版及更新版本中修正。

**問題：**JCE 工作階段集區已用盡

**影響：**看到下列訊息後，您可能無法在 JCE 中執行作業：

```
com.amazonaws.cloudhsm.jce.jni.exception.InternalException: There are too many
operations
happening at the same time: Reached max number of sessions in session pool: 1000
```

**因應措施：**

- 如果您遇到影響，請重新啟動 JCE 應用程式。
- 執行作業時，您可能需要先完成 JCE 作業，才能遺失對作業的參照。

 Note

視作業而定，可能需要完成方法。

| 作業               | 完成方法                                                                                                        |
|------------------|-------------------------------------------------------------------------------------------------------------|
| 加密               | 在加密或解密模式下的 <code>doFinal()</code><br><br>在包裝模式下的 <code>wrap()</code><br><br>在取消包裝模式下的 <code>unwrap()</code> |
| KeyAgreement     | <code>generateSecret()</code> 或 <code>generateSecret(String)</code>                                         |
| KeyPairGenerator | <code>generateKeyPair()</code> 、 <code>genKeyPair()</code> 或 <code>reset()</code>                           |
| KeyStore         | 無需任何方法                                                                                                      |
| MAC              | <code>doFinal()</code> 或 <code>reset()</code>                                                               |
| MessageDigest    | <code>digest()</code> 或 <code>reset()</code>                                                                |
| SecretKeyFactory | 無需任何方法                                                                                                      |
| SecureRandom     | 無需任何方法                                                                                                      |
| 簽章               | 在簽署模式下的 <code>sign()</code><br><br>在驗證模式中下的 <code>verify()</code>                                           |

解決狀態：我們已在用戶端 SDK 5.9.0 及更新版本中解決此問題。若要修正此問題，請將用戶端 SDK 升級至其中一個版本。



## 問題：用戶端 SDK 5 記憶體流失搭配 getKey 操作

- 影響：API getKey操作在用戶端 SDK 5.10.0 版和更早版本中的 JCE 中存在記憶體流失。如果您在應用程式中多次使用 getKey API，這將導致記憶體成長增加，進而增加應用程式中的記憶體使用量。隨著時間的推移，這可能會導致限流錯誤或需要重新啟動應用程式。
- 解決方法：我們建議您升級至用戶端 SDK 5.11.0。如果無法這麼做，建議您不要在應用程式中多次呼叫 getKey API。相反地，請盡可能重複使用先前getKey操作中先前傳回的金鑰。
- 解決狀態：將您的用戶端 SDK 版本升級至 5.11.0 或更新版本，其中包含此問題的修正。

## 適用於的 OpenSSL 動態引擎的已知問題 AWS CloudHSM

這些是 OpenSSL 動態引擎的已知問題 AWS CloudHSM。

### 主題

- [問題：您無法在 RHEL 6 和 CentOS6 上安裝 AWS CloudHSM OpenSSL 動態引擎](#)
- [問題：預設僅支援將 RSA 卸載到 HSM。](#)
- [問題：在 HSM 上不支援使用金鑰進行內含 OAEP 填補的 RSA 加密和解密。](#)
- [問題：只會將 RSA 和 ECC 金鑰的私有金鑰產生卸載到 HSM。](#)
- [問題：你無法在 RHEL 8、CentOS 8 或 Ubuntu 18.04 LTS 上安裝用戶端 SDK 3 的 OpenSSL 動態引擎](#)
- [問題：SHA-1 在 RHEL 9 \(9.2+\) 上簽署並驗證棄用](#)
- [問題：AWS CloudHSM OpenSSL 動態引擎與 OpenSSL v3.x 的 FIPS 供應商不相容](#)
- [問題：從 SDK 5.16 開始，TLS 1.0 和 TLS 1.1 中的 ECDSA 密碼套件的 SSL/TLS 卸載失敗](#)

## 問題：您無法在 RHEL 6 和 CentOS6 上安裝 AWS CloudHSM OpenSSL 動態引擎

- 影響：OpenSSL 動態引擎僅[支援 OpenSSL 1.0.2\[f+\]](#)。在預設情況下，RHEL 6 和 CentOS 6 會隨附 OpenSSL 1.0.1。
- 因應措施：將 RHEL 6 和 CentOS 6 上的 OpenSSL 程式庫升級至 1.0.2[f+] 版。

## 問題：預設僅支援將 RSA 卸載到 HSM。

- 影響：為了發揮最大效能，並未將程式庫設定為卸載額外功能 (例如產生亂數或 EC-DH 操作)。
- 因應措施：如果您需要卸載額外操作，請透過支援案例聯絡我們。

- 解決狀態：我們正在新增對程式庫的支援，以透過組態檔案來設定卸載選項。更新可供使用時即會在版本歷史頁面中公告。

**問題：**在 HSM 上不支援使用金鑰進行內含 OAEP 填補的 RSA 加密和解密。

- 影響：含 OAEP 填補之對 RSA 加密和解密的任何呼叫會失敗，並發生除以零錯誤。這是因為 OpenSSL 動態引擎是在本機使用仿造的 PEM 檔案呼叫操作，而不是將操作卸載到 HSM 所造成。
- 因應措施：您可以使用 [AWS CloudHSM 用戶端 SDK 5 的 PKCS #11 程式庫](#) 或 [AWS CloudHSM 用戶端 SDK 5 的 JCE 提供者](#) 執行此程序。
- 解決狀態：我們正在新增對程式庫的支援，以讓您正確卸載此操作。更新可供使用時即會在版本歷史頁面中公告。

**問題：**只會將 RSA 和 ECC 金鑰的私有金鑰產生卸載到 HSM。

對於任何其他金鑰類型，OpenSSL AWS CloudHSM 引擎不會用於呼叫處理。而是改用本機 OpenSSL 引擎。這會在軟體中以本機的方式產生金鑰。

- 影響：容錯移轉並無提示，因此沒有任何跡象可告知您是否尚未收到在 HSM 上安全產生的金鑰。如果金鑰是由 OpenSSL 在本機的軟體中產生，您會看到包含 ".....+++++" 字串的輸出追蹤。將此操作卸載到 HSM 時，就不會有此追蹤。因為金鑰不是在 HSM 中產生或存放，將無法供日後使用。
- 因應措施：只針對 OpenSSL 引擎支援的金鑰類型使用 OpenSSL 引擎。對於所有其他金鑰類型，請在應用程式中使用 PKCS #11 或 JCE，或在 CLI `key_mgmt_util` 中使用。

**問題：**你無法在 RHEL 8、CentOS 8 或 Ubuntu 18.04 LTS 上安裝用戶端 SDK 3 的 OpenSSL 動態引擎

- 影響：在預設情況下，RHEL 8、CentOS 8 和 Ubuntu 18.04 LTS 所提供的 OpenSSL 版本不相容於用戶端 SDK 3 的 OpenSSL 動態引擎。
- 因應措施：使用提供 OpenSSL 動態引擎支援的 Linux 平台。如需關於支援的平台的詳細資訊，請參閱 [支援的平台](#)。
- 解決狀態：AWS CloudHSM 支援這些平台搭配適用於用戶端 SDK 5 的 OpenSSL 動態引擎。如需詳細資訊，請參閱 [支援的平台](#) 和 [OpenSSL 動態引擎](#)。

## 問題：SHA-1 在 RHEL 9 (9.2+) 上簽署並驗證棄用

- 影響：在 RHEL 9 (9.2+) 中已棄用用於密碼編譯目的的 SHA-1 訊息摘要。因此，使用 OpenSSL 動態引擎透過 SHA-1 簽署和驗證操作將會失敗。
- 解決方法：如果您的案例需要使用 SHA-1 來簽署/驗證現有或第三方密碼編譯簽章，請參閱[增強 RHEL 安全性：了解 RHEL 9 \(9.2+\) 和 RHEL 9 \(9.2+\) 上的 SHA-1 棄用](#)，以取得更多詳細資訊。  
[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9/html/9.0\\_release\\_notes/overview](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/9.0_release_notes/overview)

## 問題：AWS CloudHSM OpenSSL 動態引擎與 OpenSSL v3.x 的 FIPS 供應商不相容

- 影響：如果您在為 AWS CloudHSM OpenSSL 3.x 版啟用 FIPS 供應商時嘗試使用 OpenSSL 動態引擎，則會收到錯誤。
- 解決方法：若要將 AWS CloudHSM OpenSSL 動態引擎與 OpenSSL 3.x 版搭配使用，請確定已設定「預設」提供者。閱讀 [OpenSSL 網站上的](#)預設提供者詳細資訊。

## 問題：從 SDK 5.16 開始，TLS 1.0 和 TLS 1.1 中的 ECDSA 密碼套件的 SSL/TLS 卸載失敗

- 影響：使用 TLS 1.0 或 TLS 1.1 的連線嘗試失敗，因為這些版本使用 SHA-1 進行簽署，這不符合 [FIPS 186-5](#) 要求。
- 解決方法：如果您無法立即升級 TLS 版本，您可以遷移到非 FIPS 叢集，這不會強制執行雜湊強度要求。不過，我們建議您升級至 TLS 1.2 或 TLS 1.3，以維護 FIPS 合規和安全性最佳實務。
- 解決方案：升級您的實作以使用 TLS 1.2 或 TLS 1.3。由於安全問題，網際網路工程任務小組 (IETF) 已[棄用](#) TLS 1.0 和 TLS 1.1。

## 的金鑰儲存提供者 (KSP) 的已知問題 AWS CloudHSM

這些是 金鑰儲存提供者 (KSP) 的已知問題 AWS CloudHSM。

### 主題

- [問題：憑證存放區的驗證失敗](#)
- [問題：使用用戶端 SDK 5 的 SDK3 相容性模式時，憑證存放區中的容器名稱不一致](#)

## 問題：憑證存放區的驗證失敗

使用用戶端 SDK 5.14 和 5.15 版時，呼叫 `certutil -store my CERTIFICATE_SERIAL_NUMBER` 擲回下列錯誤：

```
ERROR: Could not verify certificate public key against private key
```

- 影響：您無法使用 `certutil` 驗證使用用戶端 SDK 5 建立的憑證存放區。
- 解決方法：使用私有金鑰簽署檔案並使用公有金鑰驗證簽章，以驗證與憑證相關聯的金鑰對。您可以依照[此處](#)提供的步驟，使用 Microsoft SignTool 來完成此操作。
- 解決狀態：我們正在努力新增使用 驗證憑證的支援 `certutil`。修正可供使用時即會在版本歷史頁面中公告。

## 問題：使用用戶端 SDK 5 的 SDK3 相容性模式時，憑證存放區中的容器名稱不一致

使用 `certutil -store my CERTIFICATE_SERIAL_NUMBER` 命令來檢視使用 [generate-file](#) 命令 in AWS CLI 5.16.0 產生金鑰參考檔案的憑證時，會發生下列錯誤：

```
ERROR: Container name inconsistent: CONTAINER_NAME
```

發生此錯誤是因為儲存在憑證中的容器名稱與 CloudHSM CLI 產生的金鑰參考檔案名稱不相符。

- 影響：儘管發生此錯誤，憑證及其相關聯的金鑰仍能正常運作。使用這些憑證的所有應用程式將繼續正常運作。
- 解決方法：若要解決此錯誤，請將金鑰參考檔案名稱重新命名為簡單或唯一容器名稱。請參閱 命令的下列範例輸出 `certutil -store my`

```
Subject: CN=www.website.com, OU=Organizational-Unit, O=Organization, L=City, S=State, C=US
Non-root Certificate
Cert Hash(sha1): 1add52
Key Container = 7e3c-b2f5
Simple container name: tq-3daacd89
Unique container name: tq-3daacd89
ERROR: Container name inconsistent: 7e3c-b2f5
```

根據預設，金鑰參考檔案會存放在 `C:\Users\Default\AppData\Roaming\Microsoft\Crypto\CaviumKSP\GlobalPartition`

1. 將金鑰參考檔案重新命名為簡單容器名稱。
  2. 使用新的金鑰容器名稱修復憑證存放區。如需詳細資訊，請參閱 [KSP Migration](#) 中的步驟 12 至 14。
- 解決狀態：此問題已在用戶端 SDK 5.16.1 版中修正。若要解決此問題，請將用戶端 SDK 升級至 5.16.1 版或更新版本。

## 使用執行 Amazon Linux 2 的 Amazon EC2 執行個體的已知問題 AWS CloudHSM

下列問題會影響 AWS CloudHSM 以及在 Amazon Linux 2 上執行的 Amazon EC2 執行個體。

問題：Amazon Linux 2 2018.07 版使用目前與 AWS CloudHSM SDKs 不相容的更新 **ncurses** 套件（第 6 版）

執行 the AWS CloudHSM [cloudhsm\\_mgmt\\_util](#) 或 [key\\_mgmt\\_util](#) 時，您看到下列錯誤：

```
/opt/cloudhsm/bin/cloudhsm_mgmt_util: error while loading shared libraries:
libncurses.so.5: cannot open shared object file: No such file or directory
```

- 影響：在 Amazon Linux 2 2018.07 版上執行的執行個體將無法使用所有 AWS CloudHSM 公用程式。
- 因應措施：在 Amazon Linux 2 EC2 執行個體上發出以下命令，安裝受支援的 ncurses 套件 (版本 5)：

```
sudo yum update && yum install ncurses-compat-libs
```

- 解決狀態：此狀態已在 AWS CloudHSM 用戶端 1.1.2 版本中解決。您必須升級到此用戶端，以受益於此修正。

## 整合第三方應用程式與的已知問題 AWS CloudHSM

與第三方應用程式整合 AWS CloudHSM 時，下列問題會影響。

## 問題：用戶端 SDK 3 不支援產生主金鑰時 Oracle 設定 PKCS #11 屬性 CKA\_MODIFIABLE。

此限制是在 PKCS #11 程式庫中定義的。如需詳細資訊，請參閱[支援的 PKCS #11 屬性](#)上的註釋 1。

- 影響：Oracle 主金鑰建立失敗。
- 因應措施：在建立新的主金鑰時，將特殊環境變數 CLOUDHSM\_IGNORE\_CKA\_MODIFIABLE\_FALSE 設定為 TRUE。只有在產生主金鑰時才需要此環境變數，您不需要將此環境變數用於其他任何用途。例如，您會將此變數用於您建立的第一個主金鑰，接著如果您想要輪換主金鑰版本，才會再次使用此環境變數。如需詳細資訊，請參閱[產生 Oracle TDE 主加密金鑰](#)。
- 解決狀態：我們正在改進 HSM 韌體，以完全支援 CKA\_MODIFIABLE 屬性。更新將在 AWS CloudHSM 論壇和版本歷史記錄頁面上宣布

## AWS CloudHSM 叢集修改的已知問題

下列問題會影響嘗試使用 modify-cluster API 變更叢集 HSM 類型的客戶。

### 主題

- [問題：由於 PBKDF2 反覆運算增加，登入延遲增加](#)
- [問題：由於權杖金鑰建立而無法修改 HSM 類型](#)

### 問題：由於 PBKDF2 反覆運算增加，登入延遲增加

- 影響：具有大量使用者的叢集將經歷較長的遷移期間。這是因為第一次將 hsm1.medium 備份還原至 hsm2m.medium 時，備份還原程序會對每個使用者執行 PBKDF2 操作的變更。
- 解決方法：設計您的應用程式以適應更長的遷移期。
- 解析狀態：無解析狀態。

### 問題：由於權杖金鑰建立而無法修改 HSM 類型

- 影響：執行字符金鑰型工作負載的客戶將無法開始遷移。這樣做是因為 HSM 將進入有限寫入模式，以防止在 HSM 類型修改期間發生資料遺失情況。
- 解決方法：停止建立和刪除權杖金鑰，然後等待 7 天。或者，如果您有
  - 無法處理封鎖字符金鑰遷移，也無法執行藍/綠部署。
  - 可以在遷移期間處理封鎖權杖金鑰操作，但無法等待整整 7 天。

- 解決狀態：此問題已解決。執行字符金鑰型工作負載的客戶現在可以開始遷移。遷移期間會封鎖權杖金鑰的建立和刪除。

## 在 hsm2.medium 上使用 AWS CloudHSM 用戶端 5.12.0 版的已知操作失敗問題

使用 AWS CloudHSM 用戶端 5.12.0 版 AWS CloudHSM 時，下列問題會受到影響

問題：get-attribute 操作期間發生錯誤

如果您要從 hsm1.medium 遷移至 hsm2m.medium 並使用 CloudHSM 用戶端 SDK 5.12.0，您可能會發現與屬性處理相關的錯誤。

您可能會在用戶端日誌中看到下列錯誤訊息：Error in deserialization of data: Invalid integer conversion

影響：以下操作將使用用戶端 5.12.0 版失敗

- 在 PKCS#11 SDK 中，呼叫 C\_GetAttributeValue 失敗
- 在 CloudHSM CLI 中，金鑰清單命令在輸出中沒有顯示屬性
- 在 CloudHSM CLI 中，使用 hsm1.medium 產生的金鑰的金鑰 generate-file 可能會失敗

解決方案：我們建議您升級至可解決此問題的最新版本 SDK。

## AWS CloudHSM 用戶端 SDK 3 金鑰同步失敗

在用戶端 SDK 3 中，如果用戶端同步失敗，AWS CloudHSM 會盡最大努力回應，以清除可能已建立的任何不需要的金鑰（現在是不需要的）。此程序包括立即移除不需要的金鑰材料，或標記不需要的材料以供日後移除。在這兩種情況下，解決方案都不需要您採取任何行動。在極少數情況下，AWS CloudHSM 如果無法移除且無法標記不需要的金鑰材料，您必須刪除金鑰材料。

問題：您嘗試產生符記金鑰、匯入或取消包裝作業，並看到 tombstone 失敗的錯誤。

```
2018-12-24T18:28:54Z liquidSecurity ERR: print_node_ts_status:
[create_object_min_nodes]Key: 264617 failed to tombstone on node:1
```

原因：移除和標記不需要 AWS CloudHSM 的金鑰材料失敗。



解決方案：叢集中的 HSM 包含未標示為不需要的不需要金鑰材料。您必須手動移除金鑰材料。若要手動刪除不想要的金鑰材料，請使用 `key_mgmt_util` (KMU) 或 PKCS #11 程式庫或 JCE 提供者中的 API。如需詳細資訊，請參閱 [deleteKey](#) 或 [用戶端 SDK](#)。

為了讓權杖金鑰更持久，AWS CloudHSM 會在用戶端同步設定中指定的 HSMs 數目下限上失敗金鑰建立操作。如需詳細資訊，請參閱 [AWS CloudHSM 中的金鑰同步](#)。

## AWS CloudHSM 用戶端 SDK 3 使用 pkpspeed 工具驗證 HSM 效能

本主題說明如何使用用戶端 SDK 3 驗證 AWS CloudHSM 硬體安全模組 (HSM) 效能。

若要驗證 AWS CloudHSM 叢集中 HSMs 的效能，您可以使用用戶端 SDK 3 隨附的 `pkpspeed` (Linux) 或 `pkpspeed_blocking` (Windows) 工具。`pkpspeed` 工具會在理想的條件下執行，並直接調用 HSM 來執行作業，而不需要透過 PKCS11 等的開發套件。建議您單獨對應用程式進行負載測試，以判斷擴展需求。不建議運行以下測試：隨機 (I)，ModExp (R) 和 EC 點乘法算法 (Y)。

如需有關在 Linux EC2 執行個體上安裝此用戶端的詳細資訊，請參閱[安裝和設定 CMU \(Linux\) 的 AWS CloudHSM 用戶端](#)。如需有關在 Windows 執行個體上安裝此用戶端的詳細資訊，請參閱[安裝和設定 CMU 的 AWS CloudHSM 用戶端 \(Windows\)](#)。

安裝並設定 AWS CloudHSM 用戶端之後，請執行下列命令來啟動用戶端。

### Amazon Linux

```
$ sudo start cloudhsm-client
```

### Amazon Linux 2

```
$ sudo service cloudhsm-client start
```

### CentOS 7

```
$ sudo service cloudhsm-client start
```

### CentOS 8

```
$ sudo service cloudhsm-client start
```



## RHEL 7

```
$ sudo service cloudhsm-client start
```

## RHEL 8

```
$ sudo service cloudhsm-client start
```

## Ubuntu 16.04 LTS

```
$ sudo service cloudhsm-client start
```

## Ubuntu 18.04 LTS

```
$ sudo service cloudhsm-client start
```

## Windows

- 用於 Windows 用戶端 1.1.2+ :

```
C:\Program Files\Amazon\CloudHSM>net.exe start AWSCloudHSMClient
```

- 用於 Windows 用戶端 1.1.1 和更早版本 :

```
C:\Program Files\Amazon\CloudHSM>start "cloudhsm_client" cloudhsm_client.exe C:
\ProgramData\Amazon\CloudHSM\data\cloudhsm_client.cfg
```

如果您已經安裝用戶端軟體，您可能需要下載並安裝最新版以取得 pkpspeed。您可以在 Linux 的 /opt/cloudhsm/bin/pkpspeed 或 Windows 的 C:\Program Files\Amazon\CloudHSM\ 中找到 pkpspeed 工具。

若要使用 pkpspeed，請執行 pkpspeed 命令或 pkpspeed\_blocking.exe，並指定 HSM 上加密使用者 (CU) 的使用者名稱和密碼。然後設定要使用的選項，同時考慮以下建議。

## 測試建議

- 若要測試 RSA 簽署的效能和驗證操作，請選擇 RSA\_CRT 加密 (在 Linux 中) 或選項 B (在 Windows 中)。不要選擇 RSA (Windows 中的選項 A)。加密的效果相同，但 RSA\_CRT 的效能最佳。

- 從少量的執行緒開始。若要測試 AES 效能，一個執行緒通常足以顯示最大的效能。若要測試 RSA 效能 (RSA\_CRT)，三個或四個執行緒通常足夠。

## pkpspeed 工具的可設定選項

- FIPS 模式：AWS CloudHSM 一律處於 FIPS 模式（如需詳細資訊，請參閱[AWS CloudHSM FAQs](#)）。這可以透過使用 AWS CloudHSM 使用者指南中記錄的 CLI 工具進行驗證，並執行指示 FIPS 模式狀態的 [使用 CMU 取得 AWS CloudHSM 叢集中每個 HSM 的硬體資訊](#) 命令。
- 測試類型 (封鎖與非封鎖)：這指定了如何以線程方式執行作業。您很可能會使用非封鎖獲得更好的數目。這是因為他們利用執行緒和並行。
- 執行緒數目：執行測試的執行緒數目。
- 執行測試的時間 (秒) (最大值 = 600)：pkpspeed 會產生以「作業/秒」為單位測量的結果，並針對執行測試的每秒報告此值。例如，如果測試執行 5 秒鐘，輸出可能會像下列範例值：
  - OPERATIONS/second 821/1
  - OPERATIONS/second 833/1
  - OPERATIONS/second 845/1
  - OPERATIONS/second 835/1
  - OPERATIONS/second 837/1

## 可以使用 pkpspeed 工具執行的測試

- AES GCM：測試 AES GCM 模式加密。
- 基本 3DES CBC：測試 3DES CBC 模式加密。請參閱下列備註 [1](#) 查看即將進行的變更。
- 基本 AES：測試 AES CBC/ECB 加密。
- 摘要：測試雜湊摘要。
- ECDSA 簽署：測試 ECDSA 簽署。
- ECDSA 驗證：測試 ECDSA 驗證。
- FIPS 隨機：測試 FIPS 相容隨機數的產生 (注意：這只能在封鎖模式中使用)。
- HMAC：測試 HMAC。
- 隨機：此測試不相關，因為我們使用的是 FIPS 140-2 HSM。
- RSA 非 CRT 與 RSA\_CRT：測試 RSA 簽署並驗證操作。
- RSA OAEP 加密：測試 RSA OAEP 加密。

- RSA OAEP 解密：測試 RSA OAEP 解密。
- RSA 私有解密非 CRT：測試 RSA 私有金鑰加密 (非優化)。
- RSA 私有金鑰解密 CRT：測試 RSA 私有金鑰加密 (優化)。
- RSA PSS 簽署：測試 RSA PSS 簽署。
- RSA PSS 驗證：測試 RSA PSS 驗證。
- RSA 公有金鑰加密：測試 RSA 公有金鑰加密。

RSA 公有金鑰加密，RSA 私有解密非 CRT 和 RSA 私有金鑰解密 CRT 還將提示使用者回答以下問題：

```
Do you want to use static key [y/n]
```

如果輸入 y，則會將預先計算的金鑰匯入 HSM。

如果輸入 n，則會產生新的金鑰。

**【1】** 根據 NIST 指引，在 2023 年之後，不允許在 FIPS 模式下使用叢集。對於處於非 FIPS 模式的叢集，在 2023 年之後仍然允許。如需詳細資訊，請參閱 [FIPS 140 合規性：2024 機制棄用](#)。

## 範例

以下範例示範在測試 HSM 的 RSA 和 AES 操作效能時，您在 pkpspeed (Linux) 或 pkpspeed\_blocking (Windows) 中可以選擇的選項。

Example：使用 pkpspeed 來測試 RSA 效能

您可以在 Windows、Linux 和相容的作業系統上執行這個範例。

### Linux

在 Linux 和相容的作業系統上，使用這些指示。

```
/opt/cloudhsm/bin/pkpspeed -s CU user name -p password
```

```
SDK Version: 2.03
```

```
 Available Ciphers:
```

```
 AES_128
```

```
 AES_256
```

```

3DES
RSA (non-CRT. modulus size can be 2048/3072)
RSA_CRT (same as RSA)
For RSA, Exponent will be 65537

Current FIPS mode is: 00002
Enter the number of thread [1-10]: 3
Enter the cipher: RSA_CRT
Enter modulus length: 2048
Enter time duration in Secs: 60
Starting non-blocking speed test using data length of 245 bytes...
[Test duration is 60 seconds]

Do you want to use static key[y/n] (Make sure that KEK is available)?n

```

## Windows

```

c:\Program Files\Amazon\CloudHSM>pkpspeed_blocking.exe -s CU user name -p password

Please select the test you want to run

RSA non-CRT----->A
RSA CRT----->B
Basic 3DES CBC----->C
Basic AES----->D
FIPS Random----->H
Random----->I
AES GCM ----->K

eXit----->X
B

Running 4 threads for 25 sec

Enter mod size(2048/3072):2048
Do you want to use Token key[y/n]n
Do you want to use static key[y/n] (Make sure that KEK is available)? n
OPERATIONS/second 821/1
OPERATIONS/second 833/1
OPERATIONS/second 845/1
OPERATIONS/second 835/1
OPERATIONS/second 837/1
OPERATIONS/second 836/1

```

```

OPERATIONS/second 837/1
OPERATIONS/second 849/1
OPERATIONS/second 841/1
OPERATIONS/second 856/1
OPERATIONS/second 841/1
OPERATIONS/second 847/1
OPERATIONS/second 838/1
OPERATIONS/second 843/1
OPERATIONS/second 852/1
OPERATIONS/second 837/

```

Example : 使用 pkpspeed 來測試 AES 效能

## Linux

在 Linux 和相容的作業系統上，使用這些指示。

```
/opt/cloudhsm/bin/pkpspeed -s <CU user name> -p <password>
```

```
SDK Version: 2.03
```

```
Available Ciphers:
```

```
AES_128
```

```
AES_256
```

```
3DES
```

```
RSA (non-CRT. modulus size can be 2048/3072)
```

```
RSA_CRT (same as RSA)
```

```
For RSA, Exponent will be 65537
```

```
Current FIPS mode is: 00000002
```

```
Enter the number of thread [1-10]: 1
```

```
Enter the cipher: AES_256
```

```
Enter the data size [1-16200]: 8192
```

```
Enter time duration in Secs: 60
```

```
Starting non-blocking speed test using data length of 8192 bytes...
```

## Windows

```

c:\Program Files\Amazon\CloudHSM>pkpspeed_blocking.exe -s CU user name -p password
login as USER
Initializing Cfm2 library
SDK Version: 2.03

```

```

Current FIPS mode is: 00000002
Please enter the number of threads [MAX=400] : 1
Please enter the time in seconds to run the test [MAX=600]: 20

Please select the test you want to run

RSA non-CRT----->A
RSA CRT----->B
Basic 3DES CBC----->C
Basic AES----->D
FIPS Random----->H
Random----->I
AES GCM ----->K

eXit----->X
D

Running 1 threads for 20 sec

Enter the key size(128/192/256):256
Enter the size of the packet in bytes[1-16200]:8192
OPERATIONS/second 9/1
OPERATIONS/second 10/1
OPERATIONS/second 11/1
OPERATIONS/second 10/1
OPERATIONS/second 10/1
OPERATIONS/second 10/1
OPERATIONS/second 10/...
```

## AWS CloudHSM 用戶端 SDK 5 使用者包含不一致的值

AWS CloudHSM 用戶端 SDK 5 中的 `user list` 命令會傳回叢集中所有使用者和使用者屬性的清單。如果任何使用者的屬性值為「不一致」，表示此使用者不會在您的叢集之間同步處理。這表示使用者在叢集中的不同 HSM 上具有不同的屬性。根據不一致屬性，可以採取不同的修復步驟。

以下資料表包含解決單一使用者不一致之處的步驟。如果單一使用者有多個不一致之處，請從上到下依照下列步驟來解決這些問題。如果有多個不一致的使用者，請為每個使用者瀏覽此清單，完全解決該使用者的不一致之處，然後再繼續下一個使用者。

**Note**

要執行這些步驟，您最好以管理員身份登錄。如果您的管理員帳戶不一致，請執行以下步驟使用管理員身分登錄並重複這些步驟，直到所有屬性都一致為止。管理員帳戶一致後，您可以繼續使用該管理員同步叢集中的其他使用者。

| 屬性不一致            | 使用者清單輸出範例                                                                                                                                          | 影響                                                                                                   | 復原方法                                                                                                                                                                                                                                                                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 使用者「角色」「不一致」     | <pre>{   "username":   "test_user",   "role":     "inconsistent ",    "locked":     "false",   "mfa": [],   "cluster-coverage":     "full" }</pre> | 此使用者是某些 HSM 上的加密使用者，也是其他 HSM 的管理員。如果兩個 SDK 同時嘗試使用不同角色建立相同的使用者，就可能會發生這種情況。您必須移除此使用者，然後以所需的角色重新建立該使用者。 | <ol style="list-style-type: none"> <li>以管理員身分登錄。</li> <li>刪除所有 HSM 上的使用者：           <pre>user delete --username &lt;user's name&gt; -- role admin  user delete --username &lt;user's name&gt; -- role crypto-user</pre> </li> <li>建立具有所需角色的使用者：           <pre>user create --username &lt;user's name&gt; --role &lt;desired role&gt;</pre> </li> </ol> |
| 使用者「叢集覆蓋範圍」「不一致」 | <pre>{   "username":   "test_user",</pre>                                                                                                          | 此使用者存在於叢集中的 HSM 子集上。如果 user create 部分成功或 user delete 部分                                              | 如果使用者不應該存在，請依照下列步驟執行：                                                                                                                                                                                                                                                                                                                                   |

| 屬性不一致 | 使用者清單輸出範例                                                                                                   | 影響                                                       | 復原方法                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <pre> "role": "crypto-user", "locked":   "false", "mfa": [], "cluster-coverage":   "inconsistent " } </pre> | <p>成功，就可能發生這種情況。</p> <p>您必須完成之前的作業，無論是建立或從叢集中移除此使用者。</p> | <ol style="list-style-type: none"> <li>1. 以管理員身分登錄。</li> <li>2. 執行此命令： <pre> user delete -- username&lt;user's name&gt; --role admin </pre> </li> <li>3. 現在，執行以下命令： <pre> user delete -- username&lt;user's name&gt; --role crypto-user </pre> <p>如果使用者應該存在，請依照下列步驟執行：</p> <ol style="list-style-type: none"> <li>1. 以管理員身分登錄。</li> <li>2. 執行以下命令： <pre> user create --username &lt;user's name&gt; --role &lt;desired role&gt; </pre> </li> </ol> </li> </ol> |



| 屬性不一致                      | 使用者清單輸出範例                                                                                                                                               | 影響                                                                                                      | 復原方法                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>使用者「鎖定」參數為「不一致」或「真」</p> | <pre>{   "username":   "test_user",   "role": "crypto-u ser",   "locked" :  <b>inconsistent</b> ,    "mfa": [],   "cluster- coverage":   "full" }</pre> | <p>此使用者在 HSM 的子集上遭到鎖定。</p> <p>如果使用者使用錯誤的密碼且只連線到叢集中的 HSM 子集，就會發生這種情況。</p> <p>您必須變更使用者的憑證，使其在叢集中保持一致。</p> | <p>如果使用者已啟用 MFA，請依照下列步驟執行：</p> <ol style="list-style-type: none"> <li>1. 以管理員身分登錄。</li> <li>2. 執行下列命令，以暫時停用 MFA：</li> </ol> <pre>user change- mfa token-sig n --username &lt;user's name&gt; --role &lt;desired role&gt; --disable</pre> <ol style="list-style-type: none"> <li>3. 變更使用者的密碼，以便他們可以登入所有 HSM：</li> </ol> <pre>user change-pa ssword --usernam e &lt;user's name&gt; --role &lt;desired role&gt;</pre> <p>如果應為使用者啟用 MFA，請依照下列步驟執行：</p> <ol style="list-style-type: none"> <li>1. 讓用戶登錄並重新啟用 MFA (這將要求他們簽署字符並在 PEM 檔案中提供其公有金鑰)：</li> </ol> |

| 屬性不一致 | 使用者清單輸出範例 | 影響 | 復原方法                                                                                                                                                  |
|-------|-----------|----|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |           |    | <pre>user change-<br/>mfa token-sig<br/>n --username<br/>  &lt;user's name&gt;<br/>  --role &lt;desired<br/>role&gt; --token<br/>  &lt;File&gt;</pre> |

| 屬性不一致        | 使用者清單輸出範例                                                                                                                                                                                                                                     | 影響                                                                                                              | 復原方法                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MFA 狀態為「不一致」 | <pre>{   "username":     "test_user",    "role": "crypto-user",   "locked":     "false",   "mfa": [     {       "strategy":         "token-sign",       "status":         "inconsistent "     }   ],   "cluster-coverage":     "full" }</pre> | <p>此使用者在叢集中的不同 HSM 上具有不同的 MFA 旗標。</p> <p>如果 MFA 作業只在 HSM 的子集上完成，就會發生這種情況。</p> <p>您必須重設使用者的密碼，並允許他們重新啟用 MFA。</p> | <p>如果使用者已啟用 MFA，請依照下列步驟執行：</p> <ol style="list-style-type: none"> <li>1. 以管理員身分登錄。</li> <li>2. 執行下列命令，以暫時停用 MFA：</li> </ol> <pre>user change-mfa token-sign --username &lt;user's name&gt; --role &lt;desired role&gt; --disable</pre> <ol style="list-style-type: none"> <li>3. 然後，您還需要變更使用者的密碼，以便他們可以登入所有 HSM：</li> </ol> <pre>user change-password --username &lt;user's name&gt; --role &lt;desired role&gt;</pre> <p>如果應為使用者啟用 MFA，請依照下列步驟執行：</p> <ol style="list-style-type: none"> <li>1. 讓用戶登錄並重新啟用 MFA (這將要求他們簽署字符並在 PEM 檔案中提供其公有金鑰)：</li> </ol> |

| 屬性不一致 | 使用者清單輸出範例 | 影響 | 復原方法                                                                                                                    |
|-------|-----------|----|-------------------------------------------------------------------------------------------------------------------------|
|       |           |    | <pre>user change- mfa token-sig n --username &lt;user's name&gt; --role &lt;desired role&gt; --token &lt;File&gt;</pre> |

## AWS CloudHSM 用戶端 SDK 5 使用者複寫失敗

CloudHSM CLI 中的 `user replicate` 命令會在複製的 AWS CloudHSM 叢集之間複寫使用者。本指南解決來源叢集內或來源與目的地叢集之間的使用者不一致所導致的失敗。使用者複寫會檢查下列屬性，以驗證使用者是否一致：

- 使用者角色
- 帳戶鎖定狀態
- Quorum 狀態
- Multi-Factor Authentication (MFA) 狀態

### 問題：所選使用者不會在整個叢集中同步

使用者複寫程序會檢查整個來源叢集的使用者同步。如果使用者的屬性具有「不一致」的值，這表示使用者不會跨叢集同步。使用者複寫失敗，並顯示下列錯誤訊息：

```
{
 "error_code": 1,
 "data": "Specified user is inconsistent across the cluster"
}
```

若要檢查來源叢集中的使用者非同步：

- 在 CloudHSM CLI 中執行 `user list` 命令。

```
aws-cloudhsm > user list
{
 "error_code": 0,
 "data": {
 "users": [
 {
 "username": "admin",
 "role": "admin",
 "locked": "false",
 "mfa": [],
 "quorum": [],
 "cluster-coverage": "full"
 },
 {
 "username": "example-inconsistent-user",
 "role": "admin",
 "locked": "false",
 "mfa": [],
 "quorum": [],
 "cluster-coverage": "inconsistent"
 },
 {
 "username": "app_user",
 "role": "internal(APPLIANCE_USER)",
 "locked": "false",
 "mfa": [],
 "quorum": [],
 "cluster-coverage": "full"
 }
]
 }
}
```

解決方案：同步整個來源叢集的使用者屬性

- 若要同步整個來源叢集的使用者資訊，請參閱下列各項：[AWS CloudHSM 用戶端 SDK 5 使用者包含不一致的值](#)。

## 問題：使用者存在於具有不同屬性的目的地叢集上

如果具有相同參考的使用者已存在於目的地叢集中的一或多個 HSMs 中，但具有不同的使用者屬性，則可能會發生下列錯誤：

```
{
 "error_code": 1,
 "data": "User replicate failed on 1 of 3 connections"
}
```

### Resolution

1. 決定應保留的使用者版本。
2. 執行 `user delete` 命令，刪除適當叢集中不需要的使用者。如需更多資訊，請參閱[使用 CloudHSM CLI 刪除 AWS CloudHSM 使用者](#)。
3. 執行 `user replicate` 命令來複寫使用者。

## AWS CloudHSM 用戶端 SDK 5 金鑰複寫失敗

CloudHSM CLI 中的 `key replicate` 命令會將金鑰從來源 AWS CloudHSM 叢集複寫到目的地 AWS CloudHSM 叢集。本指南解決來源叢集內或來源與目的地叢集之間的不一致所導致的故障。

### 問題：所選金鑰不會在整個叢集中同步

金鑰複寫程序會檢查整個來源叢集的金鑰同步。如果任何金鑰資訊或屬性具有「不一致」值，這表示金鑰不會跨叢集同步。金鑰複寫失敗，並顯示下列錯誤訊息：

```
{
 "error_code": 1,
 "data": "The selected key is not synchronized throughout the cluster"
}
```

若要檢查來源叢集中的金鑰非同步：

1. 在 CloudHSM CLI 中執行 `key list` 命令。
2. 使用 `--filter` 旗標指定金鑰。
3. 新增 `--verbose` 旗標，以查看包含金鑰涵蓋範圍資訊的完整輸出。

```
aws-cloudhsm > key list --filter attr.label=example-desynchronized-key-label --verbose
{
 "error_code": 0,
 "data": {
 "matched_keys": [
 {
 "key-reference": "0x0000000000048000f",
 "key-info": {
 "key-owners": [
 {
 "username": "cu1",
 "key-coverage": "full"
 }
],
 "shared-users": [],
 "key-quorum-values": {
 "manage-key-quorum-value": 0,
 "use-key-quorum-value": 0
 },
 "cluster-coverage": "full"
 },
 "attributes": {
 "key-type": "aes",
 "label": "example-desynchronized-key-label",
 "id": "0x",
 "check-value": "0xbe79db",
 "class": "secret-key",
 "encrypt": false,
 "decrypt": false,
 "token": true,
 "always-sensitive": true,
 "derive": false,
 "destroyable": true,
 "extractable": true,
 "local": true,
 "modifiable": true,
 "never-extractable": false,
 "private": true,
 "sensitive": true,
 "sign": "inconsistent",
 "trusted": false,
 "unwrap": false,
 "verify": true,
```

```
 "wrap": false,
 "wrap-with-trusted": false,
 "key-length-bytes": 16
 }
],
 "total_key_count": 1,
 "returned_key_count": 1
}
```

解決方案：同步整個來源叢集的金鑰資訊和屬性

若要同步整個來源叢集的金鑰資訊和屬性：

1. 對於不一致的金鑰屬性：使用 `key set-attribute` 命令來設定特定金鑰所需的屬性。
2. 對於不一致的共用使用者涵蓋範圍：使用 `key share` 或 `key unshare` 命令來調整與所需使用者的金鑰共用。

## 問題：具有不同資訊或屬性的目的地叢集中存在具有相同參考的金鑰

如果具有相同參考的金鑰存在於目的地叢集中，但具有不同的資訊或屬性，則可能會發生下列錯誤：

```
{
 "error_code": 1,
 "data": "Key replicate failed on 1 of 3 connections"
}
```

### Resolution

1. 決定應保留的金鑰版本。
2. 使用適當叢集中的 `key delete` 命令刪除不需要的金鑰版本。
3. 從具有正確版本的叢集複製金鑰。

## AWS CloudHSM 在金鑰可用性檢查期間看到的錯誤

問題：AWS CloudHSM 硬體安全模組 (HSM) 正在傳回下列錯誤：



Key **<KEY HANDLE>** does not meet the availability requirements - The key must be available on at least 2 HSMs before being used.

原因：金鑰可用性檢查會尋找在罕見但可能的情況下可能遺失的金鑰。此錯誤通常發生在僅具有一個 HSM 的叢集中，或在具有兩個 HSM 的叢集中，其中一個 HSM 正在取代的期間內發生。在這些情況下，以下客戶操作可能會導致上述錯誤：

- 使用類似 [CloudHSM CLI 中的產生對稱類別](#) 或 `aws hsm generate-asymmetric-pair` 的命令產生新的金鑰 [CloudHSM CLI 中的 generate-asymmetric-pair 類別](#)。
- [使用 CloudHSM CLI 列出使用者的金鑰](#) 作業已開始。
- 已啟動 SDK 的新執行個體。

 Note

OpenSSL 經常會放棄 SDK 的新執行個體。

解決方案/建議：從下列動作中進行選擇，以避免發生此錯誤：

- 在 [設定工具](#) 的設定檔案中，使用 `--disable-key-availability-check` 參數將金鑰可用性設定為 `false`。如需詳細資訊，請參閱設定工具之 [AWS CloudHSM 用戶端 SDK 5 組態參數](#) 區段。
- 如果使用具有兩個 HSM 的叢集，請避免使用提示錯誤的作業，但在初始化程式碼期間除外。
- 將叢集中的 HSM 數量增加到至少三個。

## AWS CloudHSM 使用 JCE 擷取金鑰

使用下列各節來疑難排解使用 JCE 擷取 AWS CloudHSM 金鑰的問題。

### getEncoded、getPrivateExponent 或 getS 傳回 Null

getEncoded、getPrivateExponent 和 getS 將傳回 null，因為它們預設為停用狀態。若要啟用它們，請參閱 [使用 JCE for 擷取金鑰 AWS CloudHSM](#)。

如果 getEncoded、getPrivateExponent 和 getS 在啟用後傳回 Null，金鑰不符合正確的先決條件。如需詳細資訊，請參閱 [使用 JCE for 擷取金鑰 AWS CloudHSM](#)。

## getEncoded、getPrivateExponent 或 getS 返回 HSM 之外的金鑰位元組

您或有權存取您系統的人已啟用清除金鑰擷取功能。如需詳細資訊，包括如何將此組態重設為預設停用狀態，請參閱下列頁面。

- [使用 JCE for 擷取金鑰 AWS CloudHSM](#)
- [保護金鑰並從 HSM 擷取金鑰](#)

## HSM 調節

當您的工作負載超過 AWS CloudHSM 叢集的硬體安全模組 (HSM) 容量時，您會收到錯誤訊息，指出 HSMs 忙碌或受到調節。發生這種情況時，您可能會看到 HSM 輸送量減少或拒絕請求的速率提高。此外，HSM 可能會傳送下列忙碌錯誤。

### 適用於用戶端 SDK 5

- 在 PKCS11 中，忙碌錯誤會映射至 CKR\_FUNCTION\_FAILED。發生此錯誤的原因有多種，但如果 HSM 限流造成此錯誤，則日誌中會出現下列日誌行：
  - `[cloudhsm_provider::hsm1::hsm_connection::e2e_encryption::error] Failed to prepare E2E response. Error: Received error response code from Server. Response Code: 187`
  - `[cloudhsm_pkcs11::decryption::aes_gcm] Received error from the server. Error: This operation is already in progress. Internal error code: 0x000000BB`
- 在 JCE 中，忙碌錯誤映射到 `com.amazonaws.cloudhsm.jce.jni.exception.InternalException: Unexpected error with the Provider: The HSM could not queue the request for processing.`
- 其他 SDK 的忙碌錯誤打印出以下消息：`Received error response code from Server. Response Code: 187.`

### 適用於用戶端 SDK 3

- 在 PKCS11 中，忙碌錯誤會映射到 CKR\_OPERATION\_ACTIVE 錯誤。
- 在 JCE 中，忙碌錯誤映射至 `CFM2Exception`，狀態為 `0xBB` (187)。應用程式可以使用 `CFM2Exception` 的 `getStatus()` 函數來檢查 HSM 傳回的狀態。

- 其他 SDK 忙碌錯誤將打印出以下消息：HSM Error: HSM is already busy generating the keys(or random bytes) for another request.

## Resolution

您可以完成下列其中一個或多個動作解決這些問題：

- 在應用程式層中針對已拒絕的 HSM 作業新增重試命令。在啟用重試命令之前，請確定叢集的大小已適當符合尖峰負載。

### Note

對於用戶端 SDK 5.8.0 及更新版本，預設會開啟重試命令。如需有關每個 SDK 重試命令設定的詳細資訊，請參閱 [用戶端 SDK 5 設定工具的進階組態](#)。

- 依照 [擴展 AWS CloudHSM 叢集中的 HSMs](#) 中的指示，將更多 HSM 新增至叢集。

### Important

我們建議您測試叢集的負載，以確定您應預期的尖峰負載，然後在叢集中再新增一個 HSM 以確保高可用性。

## 讓 HSM 使用者在 AWS CloudHSM 叢集中的 HSMs 之間保持同步

若要[管理 HSM 的使用者](#)，您可以使用稱為 cloudhsm\_mgmt\_util 的 AWS CloudHSM 命令列工具。它只會與在工具組態檔案中的 HSM 通訊。它不會注意到不在組態檔案之叢集中的其他 HSM。

AWS CloudHSM 會在叢集中的所有其他 HSMs 中同步 HSMs 上的金鑰，但不會同步 HSM 的使用者或政策。使用 cloudhsm\_mgmt\_util 來[管理 HSM 使用者](#)時，這些使用者變更可能只會影響一些叢集的 HSM，也就是 cloudhsm\_mgmt\_util 組態檔案中的 HSM。這可能會在叢集中跨 HSMs AWS CloudHSM 同步金鑰時造成問題，因為擁有金鑰的使用者可能不存在於叢集中的所有 HSMs。

為了避免這些問題，請在管理使用者之前，先編輯 cloudhsm\_mgmt\_util 組態檔案。如需詳細資訊，請參閱[???](#)。

## 與叢集的 AWS CloudHSM 連線中斷

當您[設定 AWS CloudHSM 用戶端](#)時，您提供了叢集中第一個 HSM 的 IP 地址。此 IP 地址會儲存在 AWS CloudHSM 用戶端的組態檔案中。用戶端啟動時，它會嘗試連接到這個 IP 地址。如果無法啟動 (例如，因為 HSM 故障或您已刪除 HSM)，您可能會看到如下錯誤：

```
LIQUIDSECURITY: Daemon socket connection error
```

```
LIQUIDSECURITY: Invalid Operation
```

若要解決這些錯誤，請將組態檔案中的 IP 地址，更新為叢集中作用中可存取 HSM 的 IP 地址。

更新 AWS CloudHSM 用戶端的組態檔案

1. 使用下列其中一種方法來尋找叢集中的作用中 HSM 的 IP 地址。
  - 在 [主控台中](#)，檢視叢集詳細資訊頁面上的 [AWS CloudHSM HSM](#) 標籤。
  - 使用 AWS Command Line Interface (AWS CLI) 發出 [describe-clusters](#) 命令。

您在後續步驟需要此 IP 地址。

2. 使用以下命令來停止用戶端。

Amazon Linux

```
$ sudo stop cloudhsm-client
```

Amazon Linux 2

```
$ sudo service cloudhsm-client stop
```

CentOS 7

```
$ sudo service cloudhsm-client stop
```

CentOS 8

```
$ sudo service cloudhsm-client stop
```

## RHEL 7

```
$ sudo service cloudhsm-client stop
```

## RHEL 8

```
$ sudo service cloudhsm-client stop
```

## Ubuntu 16.04 LTS

```
$ sudo service cloudhsm-client stop
```

## Ubuntu 18.04 LTS

```
$ sudo service cloudhsm-client stop
```

## Windows

- 用於 Windows 用戶端 1.1.2+ :

```
C:\Program Files\Amazon\CloudHSM>net.exe stop AWSCloudHSMClient
```

- 用於 Windows 用戶端 1.1.1 和更早版本 :

在您啟動 AWS CloudHSM 用戶端的命令視窗中使用 Ctrl + C。

3. 使用以下命令來更新用戶端的組態檔，以提供您在先前步驟找到的 IP 地址。

```
$ sudo /opt/cloudhsm/bin/configure -a <IP address>
```

4. 使用下列命令來啟動 用戶端。

## Amazon Linux

```
$ sudo start cloudhsm-client
```

## Amazon Linux 2

```
$ sudo service cloudhsm-client start
```

## CentOS 7

```
$ sudo service cloudhsm-client start
```

## CentOS 8

```
$ sudo service cloudhsm-client start
```

## RHEL 7

```
$ sudo service cloudhsm-client start
```

## RHEL 8

```
$ sudo service cloudhsm-client start
```

## Ubuntu 16.04 LTS

```
$ sudo service cloudhsm-client start
```

## Ubuntu 18.04 LTS

```
$ sudo service cloudhsm-client start
```

## Windows

- 用於 Windows 用戶端 1.1.2+ :

```
C:\Program Files\Amazon\CloudHSM>net.exe start AWSCloudHSMClient
```

- 用於 Windows 用戶端 1.1.1 和更早版本 :

```
C:\Program Files\Amazon\CloudHSM>start "cloudhsm_client" cloudhsm_client.exe
C:\ProgramData\Amazon\CloudHSM\data\cloudhsm_client.cfg
```

## CloudWatch 中缺少 AWS CloudHSM 稽核日誌

如果您在 2018 年 1 月 20 日之前建立 AWS CloudHSM 叢集，則需要手動設定[服務連結角色](#)，才能啟用該叢集的稽核日誌交付。如需如何在 HSM 叢集上啟用服務連結角色的指示，請參閱《IAM 使用者指南》中的[了解服務連結角色](#)以及[建立服務連結角色](#)。

## 中 AES 金鑰包裝長度不合規的自訂 IVs AWS CloudHSM

此故障診斷主題可協助您判斷應用程式是否產生無法復原的包裝金鑰。如果您受到此問題的影響，請使用本主題來解決問題。

### 主題

- [確定代碼是否生成不可復原的包裝金鑰。](#)
- [如果代碼生成不可復原的包裝金鑰，則必須採取的動作](#)

## 確定代碼是否生成不可復原的包裝金鑰。

只有當您符合以下所有條件時，您才會受到影響：

| 條件                               | 如何知道？                                                                                                                                                                                   |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 應用程式使用 PKCS #11 程式庫              | PKCS #11 程式庫會以 libpkcs11.so 檔案的形式安裝在 /opt/cloudhsm/lib 資料夾中。用 C 語言編寫的應用程序通常直接使用 PKCS #11 程式庫，而用 Java 編寫的應用程序可能通過 Java 抽象層間接使用程式庫。如果您使用的是 Windows，您不會受到影響，因為 PKCS #11 程式庫目前不適用於 Windows。 |
| 您的應用程式專門使用 3.0.0 版的 PKCS #11 程式庫 | <p>如果您收到來自 AWS CloudHSM 團隊的電子郵件，您可能會使用 PKCS #11 程式庫的 3.0.0 版。</p> <p>若要檢查應用程式執行個體上的軟體版本，請使用以下指令：</p>                                                                                    |

| 條件                                  | 如何知道？                                                                                                                                                                                                                                             |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | <pre>rpm -qa   grep ^cloudhsm</pre>                                                                                                                                                                                                               |
| 您可以使用 AES 金鑰包裝來包裝金鑰                 | <p>AES 金鑰包裝意味著您使用 AES 金鑰來包裝一些其他金鑰。對應的機制名稱為 CKM_AES_KEY_WRAP。它與函數 C_WrapKey 一起使用。其他使用初始化向量 (IV) 的 AES 包裝機制 (例如 CKM_AES_GCM 和 CKM_CLOUDHSM_AES_GCM) 不受此問題影響。<a href="#">進一步瞭解函數和機制</a>。</p>                                                         |
| 調用 AES 金鑰包裝時指定自定義 IV，並且此 IV 的長度小於 8 | <p>AES 金鑰包裝通常使用如下 CK_MECHANISM 結構初始化：</p> <pre>CK_MECHANISM mech = {CKM_AES_KEY_WRAP, IV_POINTER, IV_LENGTH};</pre> <p>只有在以下情況下此問題才適用於您：</p> <ul style="list-style-type: none"> <li>• IV_POINTER 為 NULL</li> <li>• IV_LENGTH 小於 8 個位元組</li> </ul> |

如果您不符合上述所有條件，則可以立即停止閱讀。您包裝的金鑰可以正確解開包裝，並且此問題不會影響您。否則，請參閱 [the section called “如果代碼生成不可復原的包裝金鑰，則必須採取的動作”](#)。

## 如果代碼生成不可復原的包裝金鑰，則必須採取的動作

您應該採取以下三個步驟：

1. 立即將 PKCS #11 程式庫升級到較新的版本
  - [適用於 Amazon Linux、CentOS 6 及 RHEL 6 的最新 PKCS #11 程式庫](#)
  - [適用於 Amazon Linux 2、CentOS 7 及 RHEL 7 的最新 PKCS #11 程式庫](#)
  - [適用於 Ubuntu 16.04 LTS 的最新 PKCS #11 程式庫](#)
2. 更新您的軟體以使用符合標準的 IV



強烈建議您遵循我們的範例程式碼，並直接指定 NULL IV，這會導致 HSM 使用符合標準的預設 IV。或者，您也可以明確指定 IV 與 0xA6A6A6A6A6A6A6A6 對應的 8 IV 長度。不建議使用任何其他 IV 進行 AES 金鑰包裝，並且會在未來版本的 PKCS #11 程式庫中明確禁用用於 AES 金鑰包裝的自定義 IV。

正確指定 IV 的範例程式碼會出現在 GitHub 上的 [aes\\_wrapping.c](#) 中。

### 3. 識別和恢復現有包裝的金鑰

您應該識別使用 3.0.0 版的 PKCS #11 程式庫包裝的任何金鑰，然後聯絡支援人員以尋求協助 (<https://aws.amazon.com/support>) 以復原這些金鑰。

#### Important

此問題只會影響以 3.0.0 版的 PKCS #11 程式庫包裝的金鑰。您可以使用舊版 PKCS #11 程式庫 (2.0.4 和較低編號的套件) 或更新版本 (3.0.1 和更高編號的套件) 來包裝金鑰。

## 解決 AWS CloudHSM 叢集建立失敗

當您建立叢集時，如果角色不存在，會 AWS CloudHSM 建立 AWSServiceRoleForCloudHSM 服務連結角色。如果 AWS CloudHSM 無法建立服務連結角色，則嘗試建立叢集可能會失敗。

此主題說明如何解決最常見的問題，使得您可以成功建立叢集。您只需要建立此角色一次。一旦在您的帳戶中建立服務連結角色，您可以使用任何支援的方法來建立額外的叢集和管理它們。

下列區段提供建議來對與服務連結角色相關的叢集建立錯誤進行故障排除。如果您嘗試這些建議，但仍無法建立叢集，請聯絡 [支援](#)。如需 AWSServiceRoleForCloudHSM 服務連結角色的詳細資訊，請參閱 [服務連結角色 AWS CloudHSM](#)。

#### 主題

- [新增遺失的許可](#)
- [手動建立服務連結角色](#)
- [使用非聯合身分使用者](#)

## 新增遺失的許可

若要建立服務連結角色，使用者必須具有 `iam:CreateServiceLinkedRole` 許可。如果建立叢集的 IAM 使用者沒有此許可，叢集建立程序會在嘗試在您的 AWS 帳戶中建立服務連結角色時失敗。

當許可遺失而造成失敗時，錯誤訊息會包含下列文字。

```
This operation requires that the caller have permission to call
iam:CreateServiceLinkedRole to create the CloudHSM Service Linked Role.
```

若要解決這個錯誤，請對要建立叢集 IAM 使用者授與 `AdministratorAccess` 許可，或將 `iam:CreateServiceLinkedRole` 許可新增至使用者的 IAM 政策。如需說明，請參閱[將許可新增至新的或現有的使用者](#)。

然後，再次嘗試[建立叢集](#)。

## 手動建立服務連結角色

您可以使用 IAM 主控台、CLI 或 API 來建立 `AWSServiceRoleForCloudHSM` 服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的[建立服務連結角色](#)。

## 使用非聯合身分使用者

登入資料源自 外部的聯合身分使用者 AWS，可以執行非聯合身分使用者的許多任務。不過，AWS 不會允許使用者從聯合端點發出 API 呼叫來建立服務連結角色。

若要解決這個問題，請使用 `iam:CreateServiceLinkedRole` 許可[建立一個非聯合身分使用者](#)，或是為現有的非聯合身分使用者授與 `iam:CreateServiceLinkedRole` 許可。然後，讓該使用者透過[???建立叢集 AWS CLI](#)。如此會在您的帳戶中建立服務連結角色。

建立服務連結角色後，您可以視需要刪除非聯合身分使用者建立的叢集。刪除叢集不會影響角色。之後，任何具有必要許可的使用者，包括聯合身分使用者，都可以在您的帳戶中建立 AWS CloudHSM 叢集。

若要驗證角色是否已建立，請在 <https://console.aws.amazon.com/iam/> 開啟 IAM 主控台，然後選擇角色。或是在 AWS CLI 中使用 IAM [獲取角色](#) 命令。

```
$ aws iam get-role --role-name AWSServiceRoleForCloudHSM
{
 "Role": {
```

```
"Description": "Role for CloudHSM service operations",
"AssumeRolePolicyDocument": {
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": "sts:AssumeRole",
 "Effect": "Allow",
 "Principal": {
 "Service": "cloudhsm.amazonaws.com"
 }
 }
]
},
"RoleId": "AR0AJ4I6WN5QVGG5G7CBY",
"CreateDate": "2017-12-19T20:53:12Z",
"RoleName": "AWSServiceRoleForCloudHSM",
"Path": "/aws-service-role/cloudhsm.amazonaws.com/",
"Arn": "arn:aws:iam::111122223333:role/aws-service-role/cloudhsm.amazonaws.com/AWSServiceRoleForCloudHSM"
}
```

## 擷取 AWS CloudHSM 用戶端組態日誌

AWS CloudHSM 為用戶端 SDK 3 和用戶端 SDK 5 提供工具，以收集您環境的相關資訊，供 AWS Support 疑難排解問題。

### 主題

- [AWS CloudHSM 用戶端 SDK 5 支援工具](#)
- [AWS CloudHSM 用戶端 SDK 3 支援工具](#)

## AWS CloudHSM 用戶端 SDK 5 支援工具

AWS CloudHSM 用戶端 SDK 5 的指令碼會擷取下列資訊：

- 用戶端 SDK 5 元件的組態檔案
- 可用日誌檔案
- 作業系統的目前版本
- 套件資訊

## 執行用戶端 SDK 5 的資訊工具

用戶端 SDK 5 包含每個元件的用戶端支援工具，但所有工具的功能都相同。執行工具來建立包含所有收集資訊的輸出檔案。

這些工具使用這樣的語法：

```
[pkcs11 | dyn | jce]_info
```

例如，若要從執行 PKCS #11 程式庫的 Linux 主機收集支援資訊，並讓系統寫入預設目錄，您可以執行下列命令：

```
/opt/cloudhsm/bin/pkcs11_info
```

該工具在 /tmp 目錄中創建輸出檔案。

### PKCS #11 library

在 Linux 上收集 PKCS #11 程式庫的支援資料

- 使用支援工具收集資料。

```
/opt/cloudhsm/bin/pkcs11_info
```

在 Windows 上收集 PKCS #11 程式庫的支援資料

- 使用支援工具收集資料。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\pkcs11_info.exe"
```

### OpenSSL Dynamic Engine

收集 Linux 上的 OpenSSL 動態引擎支援資料

- 使用支援工具收集資料。

```
/opt/cloudhsm/bin/dyn_info
```

## JCE provider

在 Linux 上收集 JCE 提供者的支援資料

- 使用支援工具收集資料。

```
/opt/cloudhsm/bin/jce_info
```

在 Windows 上收集 JCE 提供者的支援資料

- 使用支援工具收集資料。

```
PS C:\> & "C:\Program Files\Amazon\CloudHSM\bin\jce_info.exe"
```

## 從無伺服器環境擷取日誌

若要為 Fargate 或 Lambda 等無伺服器環境設定，建議您將 AWS CloudHSM 日誌類型設定為 term。一旦設定為 term，無伺服器環境就可以輸出到 CloudWatch。

若要從 CloudWatch 取得用戶端日誌，請參閱《Amazon CloudWatch Logs 使用者指南》中的[使用日誌群組和日誌串流](#)。

## AWS CloudHSM 用戶端 SDK 3 支援工具

AWS CloudHSM 用戶端 SDK 3 的指令碼會擷取下列資訊：

- 作業系統及其目前版本
- 來自 cloudhsm\_client.cfg、cloudhsm\_mgmt\_util.cfg 和 application.cfg 檔案的用戶端組態資訊
- 來自平台特定位置的用戶端記錄檔
- 使用 cloudhsm\_mgmt\_util 的叢集和 HSM 資訊
- OpenSSL 資訊
- 目前的用戶端和組建版本
- 安裝程式版本

## 執行用戶端 SDK 3 的資訊工具

指令碼會建立包含所有收集資訊的輸出檔案。指令碼會在 /tmp 目錄中建立輸出檔案。

Linux: /opt/cloudhsm/bin/client\_info

Windows: C:\Program Files\Amazon\CloudHSM\client\_info

### Warning

此指令碼存在用戶端 SDK 3 版本 3.1.0 到 3.3.1 的已知問題。強烈建議您升級至 3.3.2 版，其中包含此問題的修正程式。使用此工具之前，請參閱[已知問題](#)頁面以獲取更多資訊。

# AWS CloudHSM 配額

先前稱為限制的配額是 AWS 資源的指派值。下列配額適用於每個 AWS 區域和 AWS 帳戶 AWS CloudHSM 的資源。預設配額是套用的初始值 AWS，這些值列於下表中。可調整的配額可增加超過預設配額。

## Service Quotas

| 資源           | 預設配額 | 是否可調整？ |
|--------------|------|--------|
| 叢集           | 4    | 是      |
| HSM          | 6    | 是      |
| 每個叢集的 HSM 數目 | 28   | 否      |

建議的配額提高要求方式是開啟[服務配額主控台](#)。在主控台中，選擇您的服務和配額，然後提交您的要求。如需詳細資訊，請參閱[服務配額文件](#)。

以下「系統配額」表格中的配額無法調整。

## 系統配額

| 資源                            | hsm1.medium 配額 | hsm2m.medium 配額            |
|-------------------------------|----------------|----------------------------|
| 每個叢集的金鑰數目上限                   | 3,300          | 16,666 個金鑰，非對稱金鑰最多 3,333 個 |
| 每個叢集的使用者數目上限                  | 250            | 1,024                      |
| 使用者名稱的長度上限                    | 31 個字元         | 31 個字元                     |
| 必要密碼長度                        | 8 到 32 個字元     | 8 到 32 個字元                 |
| 每個叢集的同時用戶端連線數目上限 <sup>1</sup> | 900            | 900                        |
| 每個應用程式的 PKCS #11 工作階段數目上限     | 1,024          | 1,024                      |

[1] 用戶端 SDK 3 的用戶端連線是用戶端常駐程式。對於客戶端 SDK 5，用戶端連接是一個應用程式。



# AWS CloudHSM 用戶端 SDK 的下載

下列主題提供 AWS CloudHSM 用戶端 SDKs 的下載。

## Note

如需每個用戶端 SDK 支援哪些平台的資訊，請參閱 [AWS CloudHSM 用戶端 SDK 5 支援的平台](#) 和 [AWS CloudHSM 用戶端 SDK 3 支援的平台](#)。

## 主題

- [AWS CloudHSM 最新的用戶端 SDK 版本](#)
- [AWS CloudHSM 先前的用戶端 SDK 版本](#)
- [AWS CloudHSM 已取代的用戶端 SDK 版本](#)
- [AWS CloudHSM end-of-life 用戶端 SDK 版本](#)

## AWS CloudHSM 最新的用戶端 SDK 版本

2021 年 3 月，AWS CloudHSM 發行了用戶端 SDK 5.0.0 版，推出了具有不同需求、功能和平台支援的全新用戶端 SDK。

用戶端 SDK 5 完全支援生產環境，並提供與用戶端 SDK 3 相同的元件和支援層級。如需詳細資訊，請參閱 [比較 AWS CloudHSM 用戶端 SDK 元件支援](#)。

本節包含用戶端 SDK 的最新版本。

## 用戶端 SDK 5 版本：5.16.1 版

### Amazon Linux 2023

在 x86\_64 架構上下載適用於 Amazon Linux 2023 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 342e81846436708cfc1fb459a7ef1c7b065d8a68b50a5e63653c24918d0338a0)
- [OpenSSL 動態引擎](#) (SHA256 checksum 4e83bebcd20201c04629a03b70136df8d225d3056346789054c4e2ce8c9b3cba)
- [JCE 提供者](#) (SHA256 checksum 014e3c804a56087f8855ed30e480f9c193def0e1132a4769eae3ecd235d76c4f)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)

- [CloudHSM CLI](#) (SHA256 checksum 854c5c21f9fbef4f53a710340f213c272365c2bb1233106266eca5a5aa547e11)

在 ARM64 架構上下載適用於 Amazon Linux 2023 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum dbe9498d91e1e2e8f80fc870a4a6576b0dc801dc20cb7a82bfded79b3a362ac0)
- [OpenSSL 動態引擎](#) (SHA256 checksum 76cff941f36275163db146e05bf5fe64440248643ceb5dfcb3b64103f4f016a7)
- [JCE 提供者](#) (SHA256 checksum 8c38082797172b5630c74a8fc0c9e2652f0898bd2232b72911fbbaaa0260b5a6)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum 2a0640e32405a7db138afb2444a542eab11c0a7d9610d5406478c7ac4602a14b)

## Amazon Linux 2

在 x86\_64 架構上下載適用於 Amazon Linux 2 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum cfa59458ec239553c86ac55773bebc69a5dc7cdc08a3927917fd5918e10abe93)
- [OpenSSL 動態引擎](#) (SHA256 checksum 49e50bece7d73f3b7dc95eed1df856a6dee40e27f24f40f015c6a4a2e8dee839)
- [JCE 提供者](#) (SHA256 checksum 85c8853860aa36a6c54e75c94d607a334d64dd34683ba70430ff5be61eedcc56)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum 0efc3783e8429331aa446e45776fef46c7f9726a4768763ba4881dc2b05e090e)

在 ARM64 架構上下載適用於 Amazon Linux 2 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum dad60a0380ef0ea9c469cae4de10dc47124bbecedafb6956d009734cd49abceb)
- [OpenSSL 動態引擎](#) (SHA256 checksum 7ee303421d94544cbe9df03022c48af327833e631d8f1ec59a466673b6e9395d)
- [JCE 提供者](#) (SHA256 checksum 5ebe8157abb042ee92a7edfbfcb98bf79fc3a9907684565176fd28c387c08e88)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum 5e76b4a9021a3c92e59fc608c8263af731013835738977f376fb8ad9189add56)

## RHEL 9 (9.2+)

下載適用於 x86\_64 架構上 RHEL 9 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 696e58f74d89bd8e39f85bddc547f8c94fa2fbca498318a7bb94f22e8be7a668)
- [OpenSSL 動態引擎](#) (SHA256 checksum 86197cd8bdd70db91331bb8380ea094352b4087c95a04768d2cefc3bba18dffa)
- [JCE 提供者](#) (SHA256 checksum 37ccc2df3e8aadda74dc060f7f5bbe63e4769311f2ccbf313a8ab5d8831f206)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum 45a6db22db9ae64c239b49ea9281d29d2b4364dd63ee2408f463de17c4da1877)

在 ARM64 架構上下載適用於 RHEL 9 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum fd79bccf504f53a6e70497135fcea4e20982fca75b628124c7510dcbaddf56c)
- [OpenSSL 動態引擎](#) (SHA256 checksum 23fe7407be9c5f8da0ae64e560a9741887bc31936f0b88c8d1490e3c6893a8a8)
- [JCE 提供者](#) (SHA256 checksum bd1c43e3e28c2f71e78a41342c064ff873fd8e052f89f90227fe00eaa28f089e)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum 3e877a232303052b8a6b2b869dcf228edbb0da913d3d41393f622831f4455a27)

## RHEL 8 (8.3+)

在 x86\_64 架構上下載適用於 RHEL 8 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum d396c53c229b1eaa7cb30d4fcd17addc9170c7942795d1c82b23a157ec379686)
- [OpenSSL 動態引擎](#) (SHA256 checksum c01f2cb66a6c5be839906b25c6a7f7990507b1b8ec3da34c128c1a90838e48df)
- [JCE 提供者](#) (SHA256 checksum 1745ab78de0712111659e91301f80e771e1b7ebc2ff8c4cc5e37bce591058520)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum b3ca40ba66062856ef63848c71f6e9dfa0a46a2b18d44c2d96a798fc4a4fb9cf)

## Ubuntu 24.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum ade113ee72547cb6a8fe91a4f3ac403f462d0acd0a306f01d16ac90699f9b59c)
- [OpenSSL 動態引擎](#) (SHA256 checksum 9e00cb32b16fbb286a853f65c5c5154c3e805ad67820d829a0c5343f12cc9e00)
- [JCE 提供者](#) (SHA256 checksum 4fab322a138e14372aba394de29f444af640479dd338539be84e0cf659c8993b)

- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum f8c1e369885eb77ba4517388dab47c067a617e860fb67a028a1ebde0f96acaef)

在 ARM64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 5e15a69f8fb1429ed5c10429c91323fe82a63c0fe7bcc2f968820733d1737449)
- [OpenSSL 動態引擎](#) (SHA256 checksum f5136ee61bd34b74d59a01d37964b70a0f80ec5981f732b265af1c5466309e6f)
- [JCE 提供者](#) (SHA256 checksum acf5bebe7009461cdc1e31b95caadcbf80da09ec78d8f69142072da9baf61b79)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum 511376d2faf9f991f2193d08f80fc1edd53bf06daaa6fd8bd7a3fba0d6563ad1)

## Ubuntu 22.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum e1d787f10ee51d94732732811e4d2110f1b8e448e67fd47df8b53a2f7e56e3c8)
- [OpenSSL 動態引擎](#) (SHA256 checksum 29a9c41379754ce098a025feadc026f2f75a8638981f5b95ed07007d5b3d8510)
- [JCE 提供者](#) (SHA256 checksum 390d21e499ba181dc2774c3140433f6e60b49d9de3a892a89038c27e1aff157b)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum cadadafaa9464f944e5c2446df92fb1777a9e1e5116cab1b359a8aa101cf7ae8)

在 ARM64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 3b6a3d50b4a55c150f12308ee3914451897bc4cc4c8420accf1d2d706316fccf)
- [OpenSSL 動態引擎](#) (SHA256 checksum c366a3c5faf4de32a6dedc4613234ba3d331b0abac3241bed7d25e0109a44f64)
- [JCE 提供者](#) (SHA256 checksum 705416b47bc62781b5a6dfc78dd02dad4f18f842b569c3e210b9535813b9e70)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum 811b501615cf34665b70f103905094ca84ed7c126f72d91b040aacda99dbf22b)

## Ubuntu 20.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 20.04 LTS 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 6a2c33c78ada33fb435bbf8939b7cde3efe968e9f03250083dc6024b7ebd45b8)
- [OpenSSL 動態引擎](#) (SHA256 checksum 6ee178454e78d88e0ab92cd7c5b056d0c04cd6de192aea731d7ebcbd4c5ed761)
- [JCE 提供者](#) (SHA256 checksum 1e61ccd8d2b37c64467051d26e8d8bd592465ecef04282d6f4a9491707ba059d)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum 645693f2ede4fa0d7879eedaa41ae23120d902f24c9a637ba088f277e703cb96)

## Windows Server 2025

在 x86\_64 架構上下載適用於 Windows Server 2025 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 25beadaf28323412c60ed6695d89b6261d34da9cccf08869923b979854aa0329)
- [JCE 提供者](#) (SHA256 checksum 65f487f22c0786b80d81b387f5f4c8a6c9395c8d31a020c91fc0105829b8ec2c)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum d4dc9f5efd2b5e2eb07a59fb237f7f8dfd5476c859cdb9f91841354ce88783c4)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum 80f70eb3ba22d34e49b5b5da3fa183c86c751bff46229ae16fb83a5fc69a4d0c)

## Windows Server 2022

在 x86\_64 架構上下載適用於 Windows Server 2022 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 25beadaf28323412c60ed6695d89b6261d34da9cccf08869923b979854aa0329)
- [JCE 提供者](#) (SHA256 checksum 65f487f22c0786b80d81b387f5f4c8a6c9395c8d31a020c91fc0105829b8ec2c)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum d4dc9f5efd2b5e2eb07a59fb237f7f8dfd5476c859cdb9f91841354ce88783c4)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum 80f70eb3ba22d34e49b5b5da3fa183c86c751bff46229ae16fb83a5fc69a4d0c)

## Windows Server 2019

在 x86\_64 架構上下載適用於 Windows Server 2019 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 25beadaf28323412c60ed6695d89b6261d34da9cccf08869923b979854aa0329)
- [JCE 提供者](#) (SHA256 checksum 65f487f22c0786b80d81b387f5f4c8a6c9395c8d31a020c91fc0105829b8ec2c)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum d4dc9f5efd2b5e2eb07a59fb237f7f8dfd5476c859cdb9f91841354ce88783c4)
- [金鑰儲存供應商 \(KSP\)](#) (SHA256 checksum 80f70eb3ba22d34e49b5b5da3fa183c86c751bff46229ae16fb83a5fc69a4d0c)

## Windows Server 2016

在 x86\_64 架構上下載適用於 Windows Server 2016 的 5.16.1 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 25beadaf28323412c60ed6695d89b6261d34da9cccf08869923b979854aa0329)
- [JCE 提供者](#) (SHA256 checksum 65f487f22c0786b80d81b387f5f4c8a6c9395c8d31a020c91fc0105829b8ec2c)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 70320f9aee48a250f9384f626fc16db00ea35c32af4c29cd63e9c82065a0fe1b)
- [CloudHSM CLI](#) (SHA256 checksum d4dc9f5efd2b5e2eb07a59fb237f7f8dfd5476c859cdb9f91841354ce88783c4)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum 80f70eb3ba22d34e49b5b5da3fa183c86c751bff46229ae16fb83a5fc69a4d0c)

用戶端 SDK 5.16.1 新增在 CloudHSM CLI 中簽署和驗證預先建置資料的支援。

### 平台支援

- SDK 5.16.1 是提供 Ubuntu 20.04 LTS 平台支援的最後版本。如需詳細資訊，請參閱 [Ubuntu 網站](#)。

### CloudHSM CLI

- 新增在 CloudHSM CLI 中簽署和驗證預先雜湊資料的支援。如需詳細資訊，請參閱 [CloudHSM CLI 中的加密簽署類別](#)及 [CloudHSM CLI 中的加密驗證類別](#)。

## JCE 提供者

- 更新 AES/CBC/Pkcs5Padding Encryption 模式，以便在提供 null IV 時自動產生隨機初始化向量 (IV)。先前，null IV 會導致操作失敗。明確 IVs 仍然是解密操作的必要項目。

錯誤修正/效能改進：

- 減少 JCE 中重複摘要更新操作的延遲。
- 更新 `generate key-reference` 命令，以根據在 Windows Server 上執行時的屬性 ID 值正確命名 KSP 金鑰參考檔案。如需詳細資訊，請參閱[產生 KSP 金鑰參考 \(Windows\)](#)。

## AWS CloudHSM 先前的用戶端 SDK 版本

本節列出先前的用戶端 SDK 版本。

### 5.16.0 版

#### Amazon Linux 2023

在 x86\_64 架構上下載適用於 Amazon Linux 2023 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum d63271304f32f49838390a58d94a2140ae8a744ac64efcf0e6a65983c858d862)
- [OpenSSL 動態引擎](#) (SHA256 checksum 25d78c1df82355601ed6887bb47d64a06380d001da15a070cfa89dce65417fb6)
- [JCE 提供者](#) (SHA256 checksum fcd876813e5d114e2b042765ff98b256410e988a4e373ea1aae6f260aebdd554)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 7f1441eb08daa7ceab91161900d89974ee86e0a3c54d878a29e43db775bd04f5)

在 ARM64 架構上下載適用於 Amazon Linux 2023 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 0b42e4e89cddda10c5be5f295a52d7a541bba057a3a07d3d9b192cf9eb49c776)
- [OpenSSL 動態引擎](#) (SHA256 checksum e8ee949d44b9f9ba64ed36eb7944acacbd1d76d7cf09d5492deae5928a9953e9)
- [JCE 提供者](#) (SHA256 checksum 67a6fd8f7b5dfc60ec6d6d380c31035675373b542205ec7e5a687175191cd275)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 1e6c3053b19aded54045a3baa9fe2545f81a35332366cf2d77dca92ee888e654)



## Amazon Linux 2

在 x86\_64 架構上下載適用於 Amazon Linux 2 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 5a89ff9801f89f51e27e70869f2713cfe9bbd87d1198246cffaaf74aff9e809)
- [OpenSSL 動態引擎](#) (SHA256 checksum 991b6288289d07972915aa0be6dfd6b3c33c1d6312bc304225715e30832e688f)
- [JCE 提供者](#) (SHA256 checksum c5e673f79c2efd83195a288a5c8860c4bf74dba5bc8e422741dd5cc1be230fb3)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum b9021b0b348c08f433e7cce247ab1710e2a79f33a82ac36e1d6a4672171028db)

在 ARM64 架構上下載適用於 Amazon Linux 2 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 97677a7f9759637b548205d31c9a08a3e7b27dfa5a38e9a4e8e2398ae9869a5a)
- [OpenSSL 動態引擎](#) (SHA256 checksum dde369dc4efd9f59e5c9a5459a532ad5d273f87839fba6dd5dcde2c3a2b61517)
- [JCE 提供者](#) (SHA256 checksum b7d96e7453e26ff07ccd9437b102f4c21857c79daa6315054728fc7ac66150bc)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum c7386ac016b14ea8cb96a6ed655a67f46826cdb925bd87902277b5ce9b593d51)

## RHEL 9 (9.2+)

下載適用於 x86\_64 架構上 RHEL 9 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 178d3e1ff0ec8cdc7f8c8be9aab772b4195602bb1c48dea692b628689be5ea3d)
- [OpenSSL 動態引擎](#) (SHA256 checksum 0488ad66cd825fafee70d1a1ccb1c8045b089af7b7d6ccadbec75f535376048c)
- [JCE 提供者](#) (SHA256 checksum cc9a60fa981a46c674de1e715d92ec1b8cd5c801394bfb3f0d101880589d4202)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum cb7e3ce6704f015d5b9462f12e6ad5489366fb3e80f554a2bdf7f04e688be1a9)

下載 ARM64 架構上 RHEL 9 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 9567fb016b641821869919d4d6e9754ae08fd549381446640ff135a1e225b809)



- [OpenSSL 動態引擎](#) (SHA256 checksum 8c46a9dd908e77a0d8412e7050621d0c570e091845480815c230e26d1917227b)
- [JCE 提供者](#) (SHA256 checksum 78a7c714aedd068e5e2f12f5044a6ce1618e6dfacbccdd91b4a9b505842dcc6c9)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum d2340ef4092ca6c1fa1ac8b484550508a5d9d8670e663bef6e595a07f8151be3)

## RHEL 8 (8.3+)

下載適用於 x86\_64 架構上 RHEL 8 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 47bf628a4a2663b8e8c7207b43e5af1d05ed2247e85e1371773596c132c9a4ec)
- [OpenSSL 動態引擎](#) (SHA256 checksum 49dd44243863121f7781e0f4ac556828c746d85db723864ccf16ea5fb042846a)
- [JCE 提供者](#) (SHA256 checksum c5e8a6664e6a8e5338a98b3845bed029f5936b517e6043aeb65ad58c3364eed8)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 71f2cd6bd8892ccaea845bfe575cdf20016dd7176e5216b76290e499c822a2f2)

## Ubuntu 24.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum fd7e78050aba017b7dc859f0b1e6f354f56b22091cb262b328aad204064a2960)
- [OpenSSL 動態引擎](#) (SHA256 checksum 9d2a9e8049caa12c8027ad2963fa30f22e1032d4025e39a4e2d5985073c283f5)
- [JCE 提供者](#) (SHA256 checksum ae19c13f55e01538e989e8693aaf3a5d998c60f1ed71e721a34404a228947c20)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 7ebfdb3e8c4b8e01cc1e5dfe32ae18c9542d9c2940c77bd71ee102093aaf1d1c)

在 ARM64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum cfd9526cf495e81a2477b464ca3c124a89d07b1a366a14b39eeb27d6b5e2404b)
- [OpenSSL 動態引擎](#) (SHA256 checksum 02a5cc2cd9442b7bf982bb3ae44c9b134758b46e68e46fe4729b4adf1320d75c)
- [JCE 提供者](#) (SHA256 checksum 124d04f667a7222d624f528404a289405669f4e4a1983b8a7926758bf67e35ec)

- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum b874556b34ff5f0d082ca19f62822cf97d6e7074ce3861d7577090f99cba0cbd)

## Ubuntu 22.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum e36d9bf900e195e417db261034d820cb935bec5135a0aa332d46019c70257cac)
- [OpenSSL 動態引擎](#) (SHA256 checksum 2c39129a5acce96b8693ce8c4b4aa174d9c13bc8ea3c2652fa505b4e0a933842)
- [JCE 提供者](#) (SHA256 checksum 03b70d834985a2500b73eecd831bff4f30389eb67460bf1d799466e59a9f9cfd)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 3fc4fc662188ebbd430d9b5e01a57774567b926f3478d0a455fee4968c47460d)

在 ARM64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum c835d9bb604b5c47a702fd45267ffb9dfa37d68dd0734391f060835ea680a169)
- [OpenSSL 動態引擎](#) (SHA256 checksum 943213a0f14b50fbdf3a90286e7f7ab219ab77750698f5062013873419484a04)
- [JCE 提供者](#) (SHA256 checksum 0ecc3e65a3b94c2dd3913f44aba58764e5558a8bedd3b742a42e4769533f3734)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 8558328b224b850cf9e1b3c4f8773565a90e38ab43e2c9e90bc5b841f98898d2)

## Ubuntu 20.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 20.04 LTS 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 64a01e84d898aca3cd03f22022cf8dbbc806a1735a84df5f820ba5bfa3339b0e)
- [OpenSSL 動態引擎](#) (SHA256 checksum 53a73cfc60c3fddd3ad9173bf6e602faf289f20935b3c469a137847148442954)
- [JCE 提供者](#) (SHA256 checksum 09544cb8129af4d06a241e1fbc0b6e6c207e1a518e5cb202f7b6c9802507d1b8)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum e1fdf1e014541f57d3ba4688bad88e7557e32ba974e020b4da76f85f1fc6aa29)

## Windows Server 2025

在 x86\_64 架構上下載適用於 Windows Server 2025 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 6d3142d178127372de9ab40e7af5dc81fa7c627a18286dd521ad786d0947f17d)
- [JCE 提供者](#) (SHA256 checksum 9f5c28583b5127b90e753dd7ce6d081bbe4810c0c30c424192704efa6ad1be34)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 22cfed533f528e0975f452af51d334baa1b5c143e722182dca107622e703b1ca)
- [金鑰儲存供應商 \(KSP\)](#) (SHA256 checksum  
9045c4f3e81093c4b49b93f3ea3f5caf2a4e6980628e0db2d971c437dc203bfc)

## Windows Server 2022

在 x86\_64 架構上下載適用於 Windows Server 2022 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 6d3142d178127372de9ab40e7af5dc81fa7c627a18286dd521ad786d0947f17d)
- [JCE 提供者](#) (SHA256 checksum 9f5c28583b5127b90e753dd7ce6d081bbe4810c0c30c424192704efa6ad1be34)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 22cfed533f528e0975f452af51d334baa1b5c143e722182dca107622e703b1ca)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum  
9045c4f3e81093c4b49b93f3ea3f5caf2a4e6980628e0db2d971c437dc203bfc)

## Windows Server 2019

在 x86\_64 架構上下載適用於 Windows Server 2019 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 6d3142d178127372de9ab40e7af5dc81fa7c627a18286dd521ad786d0947f17d)
- [JCE 提供者](#) (SHA256 checksum 9f5c28583b5127b90e753dd7ce6d081bbe4810c0c30c424192704efa6ad1be34)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum  
bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 22cfed533f528e0975f452af51d334baa1b5c143e722182dca107622e703b1ca)
- [金鑰儲存供應商 \(KSP\)](#) (SHA256 checksum  
9045c4f3e81093c4b49b93f3ea3f5caf2a4e6980628e0db2d971c437dc203bfc)

## Windows Server 2016

在 x86\_64 架構上下載適用於 Windows Server 2016 的 5.16.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 6d3142d178127372de9ab40e7af5dc81fa7c627a18286dd521ad786d0947f17d)
- [JCE 提供者](#) (SHA256 checksum 9f5c28583b5127b90e753dd7ce6d081bbe4810c0c30c424192704efa6ad1be34)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum bbbbe99e427b7b4d51d7018a97c4d44372db020e44fdbb76fd3954fb104010e3)
- [CloudHSM CLI](#) (SHA256 checksum 22cfed533f528e0975f452af51d334baa1b5c143e722182dca107622e703b1ca)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum 9045c4f3e81093c4b49b93f3ea3f5caf2a4e6980628e0db2d971c437dc203bfc)

用戶端 SDK 5.16 為 JCE 提供者和 PKCS #11 程式庫在 hsm2m.medium 叢集類型上新增 ECDH 與 X963 KDF 支援。用戶端 SDK 5.16 也新增支援，可在 Windows Server 上使用 CloudHSM CLI 產生 KSP 金鑰參考檔案。

### CloudHSM CLI

- 新增在 Windows Server 上產生 KSP 金鑰參考檔案的支援，如需詳細資訊，請參閱 [產生 KSP 金鑰參考 \(Windows\)](#)。

### JCE 提供者

- 新增 ECDH 搭配 hsm2m.medium 叢集類型的 X963 KDF 支援，請參閱 [用戶端 SDK 5 AWS CloudHSM 的 JCE 提供者支援的機制](#)。

### PKCS #11 程式庫

- 新增 ECDH 搭配 hsm2m.medium 叢集類型的 X963 KDF 支援，請參閱 [用戶端 SDK AWS CloudHSM 5 的 PKCS #11 程式庫支援的機制](#)。

### 錯誤修正/效能改進：

- 已修正連線中斷期間工作階段金鑰未正確清除的錯誤。
- 修正 hsm2m.medium 上成功的 mTLS 登出操作錯誤傳回錯誤回應的問題。
- 修正 Windows 啟動期間連線失敗的問題。

- 修正 SDK 資訊工具在 Ubuntu 系統上顯示不正確輸出的問題。
- 修正先前在 FIPS 模式中允許具有較弱雜湊之 ECDSA 的問題。

## 5.15.0 版

### Amazon Linux 2023

在 x86\_64 架構上下載適用於 Amazon Linux 2023 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 41ef3178811df1dbb03b2cbac83fe0f4768bdc9b17005c409f1c0229f93ef11c)
- [OpenSSL 動態引擎](#) (SHA256 checksum afa1f9f8bd99f54866dea1b8928c00b951a6e492f5f36d0d6c7c38fff341d609)
- [JCE 提供者](#) (SHA256 checksum 6ea775e05570ef3497a4df5c35a6ec1c682aea73c48e7fecec3e541af995759e)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 78c10bb213dd14fcfc5836e358de6aedac61db05125fd61137b0082214fdecbe)

在 ARM64 架構上下載適用於 Amazon Linux 2023 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum cd0617d29b6d64c00c8e14fd9a92f604e14acda4746f4f0b86b9de42367192fb)
- [OpenSSL 動態引擎](#) (SHA256 checksum bc9acfd04eb1246eb3d5b0a8f3736ec017c0d1699d5395f85868d4a1722cd83)
- [JCE 提供者](#) (SHA256 checksum 96d05301486206577b7be05aac561649167b57272c9c06ff839fd8ff2b5d96d5)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum b870eadb27736a2cde98022d57e9704c67ae15878cf0b910738859cdabaa35a2)

### Amazon Linux 2

在 x86\_64 架構上下載適用於 Amazon Linux 2 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum c70ae4f0181a8187c9380481c51c1d03e12236dd86863ec818ed3f210b294c8e)
- [OpenSSL 動態引擎](#) (SHA256 checksum 08e9fd1dd80efa637f9a1727bb0de205ba124a3776b2e8bc21008ee458063a42)
- [JCE 提供者](#) (SHA256 checksum 7932ed060e72c53b2556f30694b0ffe5342b244b6628c7a9dc03966aa49c8fe6)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 0a939e4d5d0a2ff308c7a1d9e73ebc865e426214d556bde1bd29dbe807fbb583)

在 ARM64 架構上下載適用於 Amazon Linux 2 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum bcf907a8fb4722b09c54b8e5785fe2b8cffcedd6ee3fdda2d21879a012138077)
- [OpenSSL 動態引擎](#) (SHA256 checksum 8f70edc3a6a4a1bf0264c6567b1dda1ac69055f206753f88eeadbb8bf3bf9f38)
- [JCE 提供者](#) (SHA256 checksum 75dd67736bb08fe7e46e113af10803a255ba8edee3016ca963c1ee94fe59d43b)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 1c2ecf90c955281d99bcd8d1956d63debb15bbc8419744c83f88821ef8b78aee)

## RHEL 9 (9.2+)

下載適用於 x86\_64 架構上 RHEL 9 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 65bd0b815eebc806674a7bf7c54e9f884595881547f5fffd08ff6a38aabdcbe)
- [OpenSSL 動態引擎](#) (SHA256 checksum f2af9f5882ab2e5a11defecc660f8af5c4d9d6e2e2b89873e6833fc2976f44ac)
- [JCE 提供者](#) (SHA256 checksum 5124bace5d1544775c891f13a0e309b30dd73699116c46ecc9a77bba5f9cf633)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 1eec31fb2c0ab3c2839d9bdb37874cf8dbc74a383279068fce9e8613966d06e0)

下載 ARM64 架構上 RHEL 9 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum f498697519afa04b6b0362a4388a6a38e2cb6813b781d6ce3d97a7de89c5cbfe)
- [OpenSSL 動態引擎](#) (SHA256 checksum 5410da63108a1b209e567e9bccf8bd7e4035af88b0d58b9d78b10917be1b40c1)
- [JCE 提供者](#) (SHA256 checksum b46f233e6994d2c0ed505dc5c717ee3009daaeb2063d260aa78e06273770bffa)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum e9f93eaa58db2f7ea1174164ef96ab219700933d353243c3c6ab1aebac5ccffe)

## RHEL 8 (8.3+)

下載適用於 x86\_64 架構上 RHEL 8 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 87131e179d0e60ade302ec07b22803cfb39294bf060b786c41f154d95791ac94)
- [OpenSSL 動態引擎](#) (SHA256 checksum f412a2f5cd761db5940288bb252ce060d44735c6b436bb6d4fa7d3687a44a026)

- [JCE 提供者](#) (SHA256 checksum d0844f55c08f9ff9c393138a9041efe1b59dc3dce20c0b2c23406efe6acc43db)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 9fd8033e478ce6d7d640c063c4f007359cb04c19d519826a745ad0885f96a0f8)

## Ubuntu 24.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum ca5f2f80ae921cfebdc5c8bc35c39d2b19cfabfd5981932409eaf2e7c00a9097)
- [OpenSSL 動態引擎](#) (SHA256 checksum e44cd7b678a421957c84e4fc0f70280360fd4e1e66f4cabdd1b20b955ee5fcca)
- [JCE 提供者](#) (SHA256 checksum bc6382f12769c3d87c34522d0d616b7a8c108574c003814e1300938c386655ac)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum f786be86c204680e670f7817376ff376733ebd96b51c31e9c98213078596637f)

在 ARM64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 1ecf057d67137c0e9e1bb0dda57d581690c647b0360c3a617a8dc668919d08de)
- [OpenSSL 動態引擎](#) (SHA256 checksum 4f3d23e6b798f88be587108d8e6a225d796a3d080aef61ea384eb74a1270612a)
- [JCE 提供者](#) (SHA256 checksum b9fd16bdcc1fcf59fde0d3e0debee500b0b7edfdff69209e84d14393097fe9d2)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum a95922d9b44e64a64723db0c21ac89566515a5a6c87de990af4a9e1f40c7424f)

## Ubuntu 22.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 966be12eb32de813ca07e766abf7b5616c0d2e105e9296d920aadaca10e5afdf)
- [OpenSSL 動態引擎](#) (SHA256 checksum f2840151d87b7f9cbff68993c25397afd48a16f054abf0f2fd4624662d3087d6)
- [JCE 提供者](#) (SHA256 checksum 01aebdda05640e50a82cae04c5cb6d33ab909dadd917bd834957d4f75ad8c577)
- [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 2e5eba9409abc429828505779c512cd2424719766c0e488f50aee288966cf61d)



在 ARM64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 614f74f101c9c64fff515128c5a59fa23de5047494fe248e8aabdb441092b3e)
- [OpenSSL 動態引擎](#) (SHA256 checksum c15d6db77b76bce690749b73b947567eb5f2d76669887843116d0ce56c1f8ea7)
- [JCE 提供者](#) (SHA256 checksum bca8511d5c0a173b0fef326016ce5091b6e6829fa2b3cb45ed5621290ae3e42a)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 2f5b673148b682d7e34619c51b5e8799abe7dc7fd4f046158a0d05320ba24dc1)

## Ubuntu 20.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 20.04 LTS 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 86c8394b5ddff91a71194fb87c327efde36baa2380e559c04f9d543a6e74d61b)
- [OpenSSL 動態引擎](#) (SHA256 checksum 0a4227389fea61e6e7ac7cfa715eb341f7a4eeae9ed10e4c96da2c0dd4a18f9e)
- [JCE 提供者](#) (SHA256 checksum 65b2d926ff9dfbe6c7864bc3a41b3da2383bc731dd199bceff8805a0543fbe612)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 09c2e55bcf72f9e530717950d8c5dfdd48574ae6ccb09a049526ca5b2a3b8aa9)

## Windows Server 2025

在 x86\_64 架構上下載適用於 Windows Server 2025 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum a903b63fe286f15bf669c0555b1fa4d86b33592ed05af0809acac28c0d3ace16)
- [JCE 提供者](#) (SHA256 checksum fdef6251f06d77d51fddbc2184d3eec87ddec4fe35b3ac620343eb66c95ddf64)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 6cc9205fe1fc514ddd9774f824e512940d6b1bc4cc0e251265bc46ab99746c28)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum 52ed9b08cd0ce100b8dcd3d8e8f411b6201f9f1b27872b19d1136c0bf36a29b8)

## Windows Server 2022

在 x86\_64 架構上下載適用於 Windows Server 2022 的 5.15.0 版軟體：



- [PKCS #11 程式庫](#) (SHA256 checksum a903b63fe286f15bf669c0555b1fa4d86b33592ed05af0809acac28c0d3ace16)
- [JCE 提供者](#) (SHA256 checksum fdef6251f06d77d51fddbc2184d3eec87ddec4fe35b3ac620343eb66c95ddf64)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 6cc9205fe1fc514ddd9774f824e512940d6b1bc4cc0e251265bc46ab99746c28)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum 52ed9b08cd0ce100b8dcd3d8e8f411b6201f9f1b27872b19d1136c0bf36a29b8)

## Windows Server 2019

在 x86\_64 架構上下載適用於 Windows Server 2019 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum a903b63fe286f15bf669c0555b1fa4d86b33592ed05af0809acac28c0d3ace16)
- [JCE 提供者](#) (SHA256 checksum fdef6251f06d77d51fddbc2184d3eec87ddec4fe35b3ac620343eb66c95ddf64)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 6cc9205fe1fc514ddd9774f824e512940d6b1bc4cc0e251265bc46ab99746c28)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum 52ed9b08cd0ce100b8dcd3d8e8f411b6201f9f1b27872b19d1136c0bf36a29b8)

## Windows Server 2016

在 x86\_64 架構上下載適用於 Windows Server 2016 的 5.15.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum a903b63fe286f15bf669c0555b1fa4d86b33592ed05af0809acac28c0d3ace16)
- [JCE 提供者](#) (SHA256 checksum fdef6251f06d77d51fddbc2184d3eec87ddec4fe35b3ac620343eb66c95ddf64)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum ce5d92731f2a9c7f46c92bba92f3d0adff4ceb06b9d653597994100dfc352fbe)
- [CloudHSM CLI](#) (SHA256 checksum 6cc9205fe1fc514ddd9774f824e512940d6b1bc4cc0e251265bc46ab99746c28)
- [金鑰儲存供應商 \(KSP\)](#) (SHA256 checksum 52ed9b08cd0ce100b8dcd3d8e8f411b6201f9f1b27872b19d1136c0bf36a29b8)

用戶端 SDK 5.15 新增支援使用 CloudHSM CLI 在複製的叢集之間複寫使用者。用戶端 SDK 5.15 也為適用於 Windows Server 2025 的 PKCS #11 程式庫、JCE 提供者、CloudHSM CLI 和金鑰儲存提供者 (KSP) 新增安裝套件。

## 平台支援

- 新增對 PKCS #11 程式庫、JCE 提供者、CloudHSM CLI 和金鑰儲存提供者 (KSP) 的 Windows Server 2025 支援。

## CloudHSM CLI

- 新增下列命令：
  - 使用 CloudHSM CLI 複寫使用者

## 5.14.0 版

### Amazon Linux 2023

在 x86\_64 架構上下載適用於 Amazon Linux 2023 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 05e7a3882166c694a7a09bc735f08f91c8145a4215176665eacacdf3e509abe8)
- [OpenSSL 動態引擎](#) (SHA256 checksum f4dd9966988418e100c276dc0d521f91afdfc0e6c008dbf8eda446ebaca83c14)
- [JCE 提供者](#) (SHA256 checksum c4dee5c1173f6a1c7683aedb58e61d329c36933435c416f288d94bc9a68a6b31)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum 1fad069fde305450254287e43750d597db9af0cb8fd168300cd5eaed9e2af33a)

在 ARM64 架構上下載適用於 Amazon Linux 2023 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 9f34163d02bce26c1280e589310cda891d27995c50cec0a7fe083100ecff2b69)
- [OpenSSL 動態引擎](#) (SHA256 checksum 7444a4daad6e4715c82d6c39a7b03a07ee0201a13fe0f98da96acbf9d24abf6c)
- [JCE 提供者](#) (SHA256 checksum 3393fe3a0f5c3a9c92106d74b7de074c818e095f97d2cfd600dbd47779b90b37)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum d9a2edce48c5f6646d5a351cb431712f2d2fc62d21f8318e7bb1ce579819d7f4)

### Amazon Linux 2

在 x86\_64 架構上下載適用於 Amazon Linux 2 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 9c47b90bfa0ad51627cdb0dd8f148a56090fbdeb2490f1ab4009170c7b9c1120)
- [OpenSSL 動態引擎](#) (SHA256 checksum 215f9768331565085a317585b3dbe0514b251fdc428c96ed32491c4abb9fea56)
- [JCE 提供者](#) (SHA256 checksum a802f941e95fcbf0ef37775fc096c0d6ae4c916fa08330a9d56defc5f99ff2b7)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum ac10f23dd81264b1d10a0760f62b5006d2b2b66bf1c6378248ca9326afb65a83)

在 ARM64 架構上下載適用於 Amazon Linux 2 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum f2d1550f043c655ef5d51e2ca14a0416886d99902e0702bd7f30f93b2c563d4d)
- [OpenSSL 動態引擎](#) (SHA256 checksum 2c8e2c81af53ba3646d1f947894d84b9b54780bbca79b58f354125e4ac9427c0)
- [JCE 提供者](#) (SHA256 checksum 3f9c881056e6905d46358585db72143b59971958a708fa4ac75cb53994487213)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum 6d5985e44c9852409dd3d342239fbbf7d0f9ad43d445e0980153c9b9eafe2b6f)

## RHEL 9 (9.2+)

下載適用於 x86\_64 架構上 RHEL 9 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum c4812210421ff2fa5dac8477a2e6b10552aabd88b1f03d717e044e7293823158)
- [OpenSSL 動態引擎](#) (SHA256 checksum 3f6aeaa6ae1faae7d8bba1596f358cad1eec9e562cf08aaab9ded92cabe94719)
- [JCE 提供者](#) (SHA256 checksum bd8f120b08f738ad4d1534b0e32aad903758d5e75d3aba7cb9ff6a77dec533db)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum 84f13a9babd767edf90dabb0b14034ec5b2208898123a13966dd6b8519961c27)

下載 ARM64 架構上 RHEL 9 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 3faa1de563aa9773939cab7b39907dcb7b981ed7225019f9070a9dd52db7ae70)
- [OpenSSL 動態引擎](#) (SHA256 checksum 13b41ac47ef7ee7bf78f585b8347ca4da9ebc296e4fc1e6a0c2ff5b333354ca6)
- [JCE 提供者](#) (SHA256 checksum 06803655ebe54d59c180bb17ac6fe56337bdd58ad0f6fe87c50ff8df32f70258)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)

- [CloudHSM CLI](#) (SHA256 checksum e6b4e9688d0db9d72bbee3450fe19736d640c9931adbd4f4ef73cb7ac2a08cf4)

## RHEL 8 (8.3+)

在 x86\_64 架構上下載適用於 RHEL 8 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum e400aeea6dbf7721f97e71c643a0db4f5f1094fb197fc46dc0ab293de9d16f2d)
- [OpenSSL 動態引擎](#) (SHA256 checksum bfcc27d251e62f9eba0fd508e7d08dc62126642d4cdd0b5566183957768b8c54)
- [JCE 提供者](#) (SHA256 checksum b5500031b572c918a8df4a0347e01c8ea00a7366b865b310bd92427fa1ed53e3)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum 000712d0a691efc64a6c5d54bfeb1ab48b315ebb5dd6926b0502e326bf700291)

## Ubuntu 24.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum bbec70a198a4b173620b4018acc297ce6a6a80d372706e0101997d6bca35bca)
- [OpenSSL 動態引擎](#) (SHA256 checksum fcb77f75bd465b22401a09a20c410985833340295101263b7171cdcc4ac9f980)
- [JCE 提供者](#) (SHA256 checksum e1fa16aae2f6095c89a8bf392ef2cb9ca4db8853c858904ff90abf4bb491d74b)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum af32e0ac1c5f8c7f8cb40d255abe7c63ce9d981293187a3fb452562fa05756f4)

在 ARM64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 1232318b084347889f92136536537ca519373683ce39bce20f6ac3fa2f42d7c)
- [OpenSSL 動態引擎](#) (SHA256 checksum 1745ee3a33d8e6ea72644e903c55c6a206204cf0a8bea200bc4a7b15736ed801)
- [JCE 提供者](#) (SHA256 checksum 7a44acabbc90c996594ed53661937f9242850823347f7c386f02fc041a97471a)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum e6778bd12c55fd152b50033833531fe569472f4f2bd9927a345eb126e8305739)

## Ubuntu 22.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 6b4b1620e9a85267950633b171dd188b7ac7094e371e188abc1bef7a911a16f)
- [OpenSSL 動態引擎](#) (SHA256 checksum fee5f0a65fab0f46ad58689af5dc510721581f31364d3be5cbbf79f5d9a60db8)
- [JCE 提供者](#) (SHA256 checksum 5883a3d15e160d65f8e26f185e1ee30f68becad5f6fcd16abc1c4586689800b5)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum 7b1a8cd2962f4be7325154c080dabfb820beac5629e272c3a3ebc0e6cab11d27)

在 ARM64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 8680f63fd74272ea0e4d4c32dfb96b3eb9b60e03483c202d4e9b65ee101a178f)
- [OpenSSL 動態引擎](#) (SHA256 checksum c757304e8fc5f38be3bab7ac6d37a35dcb56d31e62f7194da62b3a176593d1d8)
- [JCE 提供者](#) (SHA256 checksum a78ee59341da56af315d126ec7ed9f0dafa6e99649f659db2436be3863cb035b)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum 18931bff869a0bd54846b3296d870fa19beba5652f979352be8fba6307e6d1aa)

## Ubuntu 20.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 20.04 LTS 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum f1461c16b135ebcc17deec46aab88bd113ea122b8942fc188d4f05cd03e919a8)
- [OpenSSL 動態引擎](#) (SHA256 checksum 89211a7a7ed50eda2dc385c31ea76f1fbabd389ca691204873531d983c3eb0f7)
- [JCE 提供者](#) (SHA256 checksum f098c32d61a53b073459a75d88b68e377a9b16335874fae060cb10df0da00df0)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum ff91fb930717c917344af2ba344dc6e02bd5abc004dcb6147e9412b67e2aa7ab)

## Windows Server 2022

在 x86\_64 架構上下載適用於 Windows Server 2022 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum ee5a8e8e85fff7acd0bbafa23740e3981f7dc52e708972b600c2b26603786838)

- [JCE 提供者](#) (SHA256 checksum 2ae0274f09f66981c03fd1e3c264e896ba7cd211168ea31369335db1b3ea2e77)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum 3938654f88ce010042e48909e23991e178e411e2bd9e3c9ec25fcb8157c0cd55)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum b026e4d8c11e9ff6f22a7b9e10b8bb29e7572665f0d7978a3cef7d2354b7693f)

## Windows Server 2019

在 x86\_64 架構上下載適用於 Windows Server 2019 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum ee5a8e8e85fff7acd0bbafa23740e3981f7dc52e708972b600c2b26603786838)
- [JCE 提供者](#) (SHA256 checksum 2ae0274f09f66981c03fd1e3c264e896ba7cd211168ea31369335db1b3ea2e77)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum 3938654f88ce010042e48909e23991e178e411e2bd9e3c9ec25fcb8157c0cd55)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum b026e4d8c11e9ff6f22a7b9e10b8bb29e7572665f0d7978a3cef7d2354b7693f)

## Windows Server 2016

在 x86\_64 架構上下載適用於 Windows Server 2016 的 5.14.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum ee5a8e8e85fff7acd0bbafa23740e3981f7dc52e708972b600c2b26603786838)
- [JCE 提供者](#) (SHA256 checksum 2ae0274f09f66981c03fd1e3c264e896ba7cd211168ea31369335db1b3ea2e77)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 173087a8f286dc4f88dc915ecc00aa515bec0ae2faf219654df9f3422d8e83bb)
- [CloudHSM CLI](#) (SHA256 checksum 3938654f88ce010042e48909e23991e178e411e2bd9e3c9ec25fcb8157c0cd55)
- [金鑰儲存提供者 \(KSP\)](#) (SHA256 checksum b026e4d8c11e9ff6f22a7b9e10b8bb29e7572665f0d7978a3cef7d2354b7693f)

用戶端 SDK 5.14 新增對使用 CloudHSM CLI 的規定人數控制金鑰用量和金鑰管理操作的支援。用戶端 SDK 5.14 也新增對 Windows 平台[AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 \(KSP\)](#)的支援。此外，用戶端 SDK 5.14 新增適用於 Windows Server 2022 的 PKCS #11 程式庫、JCE 提供者、CloudHSM CLI 和金鑰儲存提供者 (KSP) 的安裝套件。

## 平台支援

- 新增對 PKCS #11 程式庫、JCE 提供者、CloudHSM CLI 和金鑰儲存提供者 (KSP) 的 Windows Server 2022 支援。

## CloudHSM CLI

- 新增對規定人數控制金鑰用量和金鑰管理操作的支援。

## 金鑰儲存提供者 (KSP)

- 新增對金鑰儲存提供者 (KSP) 的支援，這是 Microsoft Windows 作業系統特有的密碼編譯 API。如需詳細資訊，請參閱[AWS CloudHSM 用戶端 SDK 5 的金鑰儲存提供者 \(KSP\)](#)

## 5.13.0 版

### Amazon Linux 2

在 x86\_64 架構上下載適用於 Amazon Linux 2 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum cefbcfe15f0bed09a2bc9b0c15824067dfede8ceb1ad6373659c7e583a604c95)
- [OpenSSL 動態引擎](#) (SHA256 checksum 7b384253f0a124b55092e6ab18e23d9c95067d55fa8167ef7817bd2ae1becd29)
- [JCE 提供者](#) (SHA256 checksum cfac14b593b027bdb8010d6019328e7129143be06ffe223d2d50c4b7e1ac747a)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum 6b762f0884368d2e234c5f6d45b4aeefb52d686105ec2c1affdbcdabb8dda7500)

在 ARM64 架構上下載適用於 Amazon Linux 2 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum ed0352cb33b4cb9fd3d2a00a8654f53e7290535474641a1714151b4190c1de07)
- [OpenSSL 動態引擎](#) (SHA256 checksum 5e55e24175167f38a7358178ba252cb7629def0de4c99eee8a25d44649ebe5ec)
- [JCE 提供者](#) (SHA256 checksum 4e19807e792f10ffd9819d381f02ad1485aaf45fee7f660054211b8f52224ed2)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum bf90dec12f39eb685df34d82fdf2dac1c87a86fbf8a03aabde2107113081a083)



## Amazon Linux 2023

在 x86\_64 架構上下載適用於 Amazon Linux 2023 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 7f95ca9dcdf19627333257d28b81d06cd5f10c70df1e2aa10a57af34213328eb)
- [OpenSSL 動態引擎](#) (SHA256 checksum 52de525d691b404b87c6381d4c71c9b5a51a80ada1c078d6433032bb4840ebe7)
- [JCE 提供者](#) (SHA256 checksum 98c69a66e353568e416a1daba161cf49e95e3196c82ae66628519aec82479787)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum 5b08e80ff26fef91c2693a8def394ec02d69ea36604c189885f9e1205aa83da0)

在 ARM64 架構上下載適用於 Amazon Linux 2023 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 3797803ceaea2ea2f495b7e08c9e344fad755b1919b93f341b5dc7246c484988)
- [OpenSSL 動態引擎](#) (SHA256 checksum 71bbd800adc024df13dd503268217530a6e85fae2ab0c07c75cd3f5905fd526a)
- [JCE 提供者](#) (SHA256 checksum 3d7213810899ebace2e6664fbd722edbf2a771f70d68a35885ed75007f3de2cb)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum 381420610beed60b7a402fb0f7c518b1b8df74690b6539f16c115342ef75cbee)

## RHEL 8 (8.3+)

下載適用於 x86\_64 架構上 RHEL 8 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 1a4d42b88f79f64ebc9fa55d091556cf04a16796014fa0488ade43cda62a0731)
- [OpenSSL 動態引擎](#) (SHA256 checksum d7658ea876c1a6209637fc4a4ef47e0421ea47e54d1d7d10eacc7eefabb86021)
- [JCE 提供者](#) (SHA256 checksum 54aae2a6e8b2a43e806c1320fff638345f88ade7e510a6b63c55573327ba160c)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum 587592eb395af73b33beadd67af5765354904d1cc92f83c0548a308af842a6c7)

## RHEL 9 (9.2+)

在 x86\_64 架構上下載適用於 RHEL 9 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 4e68cd8055300c40e8b4cb9a4303e84870c2b517a74c16f2bd6a10fcbab5f426)



- [OpenSSL 動態引擎](#) (SHA256 checksum a8ae26dc0eda9f143c4a44a3a7e399772039e238d8b5b0f36256cdd8ae6dc30b)
- [JCE 提供者](#) (SHA256 checksum 2948e6cec865f0934ac501a2d4724b1b8c4dc2d15b61155c41d60a0257e74110)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum 0f4b84b572722de119edbb35d50a00e3c390b019a88a9c3f279a9b76225b4520)

下載 ARM64 架構上 RHEL 9 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 0bea8d7e46bc7e9bd5fa36f64d43416ea400332602720f0ae162eb7b12eda312)
- [OpenSSL 動態引擎](#) (SHA256 checksum d96eddd33c5034357e8cc3c157ff1a03dafbaeb3f09b31ed324a2cbe9e424c01)
- [JCE 提供者](#) (SHA256 checksum 34bcabf11d0b7d34e6fc48c07ba9a383a4df26491e7c4c00cd7fcbf50cd30298)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum be7a22e5f64db4211f86eb361f79c5db93c237bd28ac0db5c274bba210cd431a)

## Ubuntu 20.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 20.04 LTS 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 97b3686b007c3d3a0d97f6774ad182d5702f6a233060522f4674fd233b3eafe9)
- [OpenSSL 動態引擎](#) (SHA256 checksum 3d453a428a920c2fccd40bb18fe11b7dba3194da6fb3e457ade77d1d2cfe2b35)
- [JCE 提供者](#) (SHA256 checksum 6e6e68d1ee6f14df9370bf6d37055328a49bf28e57de23152ddc9c51e8014508)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum 2515705e66e118deae9694a47fdb74ad64e66067a690545039dc2802e4e198f)

## Ubuntu 22.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 53ffd1d6353e6facb022631e4f258200a6efabeaf00ee9f4bf4418ec27633a39)
- [OpenSSL 動態引擎](#) (SHA256 checksum 4f49e0946ba376b3c2cef05c5ee63cd78202a08907ea0ac8027095e16e47eed1)
- [JCE 提供者](#) (SHA256 checksum 2840a8938c22de6a9e6130b250bc7dd7fc512d274d7a702e944db3d1396c0222)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)

- [CloudHSM CLI](#) (SHA256 checksum 9e8592967c330f50552249017695d116adbbc54321a35be33a48ca18d739beae)

在 ARM64 架構上下載適用於 Ubuntu 22.04 LTS 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 4ab4961eb97ec0cf8bd818176c99da763a416903e24855e0dd6b31f776a01f26)
- [OpenSSL 動態引擎](#) (SHA256 checksum f1a396bf9ac2d1e970e027e2ab7d388fc0f0634d3e9c16b91d6dd889698514ad)
- [JCE 提供者](#) (SHA256 checksum 4035bc68fe7bf978b83f4fd0eb99e49efe874c2e128f62e800b9ec95c8142ec0)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum 099137b934ec81d6bb87137f919d99a810f3149858ccdd69df51418f7e5485d9)

## Ubuntu 24.04 LTS

在 x86\_64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 7057ce0d74c50635eeede91edcf3ef2e7915bed6b1f73b7bca45ba3a44392b7e)
- [OpenSSL 動態引擎](#) (SHA256 checksum d76b59bf0ba1325adbb1ad3cea8050a38db1517e48c9d9bd1001a232df285904)
- [JCE 提供者](#) (SHA256 checksum e4296cef92f99e49d6ca6c0d07a82de5e1551a6ec550252c52329561533f4f6d)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum 47516fc88c8089edcd82e942f17351df7bfba8c7d640c9f909ad48ba4d980022)

在 ARM64 架構上下載適用於 Ubuntu 24.04 LTS 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum f2aefc6517ad4c6ef63124f380ae1f26fc2eb423d0a02e5b7ceda6769784a74f)
- [OpenSSL 動態引擎](#) (SHA256 checksum 6159f4eb648159d37f304982725e5ed0dc34e7fd0658a8dc8ccacf2b75a1f4d2)
- [JCE 提供者](#) (SHA256 checksum eeaf7e0345dcf78ae14595e4ab7967dd95fb6da06a42913423f76234f47ca3fc)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum 8656590f2caa5cd8c930b116ed12504caf99254f00c7563b90d799e6f69b2e77)

## Windows Server 2016

在 x86\_64 架構上下載適用於 Windows Server 2016 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 77e32ad8d28b1073286e95f8b350f99dd26c62ff32897fb86e9d79aef9c190fb)
- [JCE 提供者](#) (SHA256 checksum 191135271e912cf858d24ad4b07c7ff57c9c4a1b3635513cc6ab8dd5dc1a0e42)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum bb7960dd7bff73a1430cf2edc1bf36b0161309e5c354f0db44eaf086568507d5)

## Windows Server 2019

在 x86\_64 架構上下載適用於 Windows Server 2019 的 5.13.0 版軟體：

- [PKCS #11 程式庫](#) (SHA256 checksum 77e32ad8d28b1073286e95f8b350f99dd26c62ff32897fb86e9d79aef9c190fb)
- [JCE 提供者](#) (SHA256 checksum 191135271e912cf858d24ad4b07c7ff57c9c4a1b3635513cc6ab8dd5dc1a0e42)
  - [Javadocs 文檔 AWS CloudHSM](#) (SHA256 checksum 11b5de4a400861cc796b4b2ecaec706603e61ae7640bd0c4e2b090c7034d6318)
- [CloudHSM CLI](#) (SHA256 checksum bb7960dd7bff73a1430cf2edc1bf36b0161309e5c354f0db44eaf086568507d5)

用戶端 SDK 5.13 新增在 hsm2m.medium 叢集類型上設定交互 TLS 的支援。如需搭配 CloudHSM 使用交互 TLS 的資訊，請參閱 [在用戶端和 AWS CloudHSM 之間設定交互 TLS \(建議\)](#)。用戶端 SDK 5.13 也為 Ubuntu 24.04 LTS 新增安裝套件。

## 平台支援

- 新增對 x86\_64 上的 Ubuntu 24.04 LTS 和所有 SDKs 的 ARM64 架構的支援。

## CloudHSM CLI

- 新增管理使用者執行 [使用 CloudHSM CLI 複寫金鑰](#) 命令的支援。用戶端 SDK 5.12 推出金鑰複寫命令供加密使用者使用。
- 新增下列命令：
  - [CloudHSM CLI 中的叢集 mtls 類別](#)

## 錯誤修正/效能改進：

- 修正以下問題：減少用戶端偵測運作狀態不佳 HSM 連線所需的時間，這有助於防止 Lambda 暖啟動期間的連線中斷錯誤。

## 5.12.0 版

用戶端 SDK 5.12.0 將 ARM 支援新增至數個平台，並提升所有 SDKs 的效能。新功能已新增至 CloudHSM CLI 和 JCE 供應商。

### 平台支援

- 新增對所有 SDKs 的 ARM64 架構上的 Amazon Linux 2023 支援。
- 新增對所有 SDK 的 ARM64 架構上 Red Hat Enterprise Linux 9 (9.2+) 的支援。 SDKs
- 新增對所有 SDKs ARM64 架構上 Ubuntu 22.04 LTS 的支援。

### CloudHSM CLI

- 新增下列命令：
  - [使用 CloudHSM CLI 複寫金鑰](#)
- 新增連線至多個叢集的支援。如需詳細資訊，請參閱[使用 CloudHSM CLI 連線至多個叢集](#)。

### JCE 提供者

- 新增使用 KeyReferenceSpec 擷取金鑰 KeyStoreWithAttributes。
- 新增使用 一次 getKeys 擷取多個金鑰 KeyStoreWithAttributes。

### 效能改進

- 提升所有 SDKs 的 AES CBC NoPadding 操作效能。

## 5.11.0 版

用戶端 SDK 5.11.0 新增新功能、改善穩定性，並包含所有 SDKs 錯誤修正。

### 平台支援

- 新增對所有 SDKs 的 Amazon Linux 2023 和 RHEL 9 (9.2+) 支援。
- 由於 Ubuntu 18.04 LTS 的最近生命週期結束，已移除其支援。
- 由於 Amazon Linux 的最近生命週期結束，已移除對 Amazon Linux 的支援。

## CloudHSM CLI

- 新增下列命令：
  - [CloudHSM CLI 中的加密簽署類別](#)
  - [CloudHSM CLI 中的加密驗證類別](#)
  - [使用 CloudHSM CLI 匯入 PEM 格式金鑰](#)
  - [CloudHSM CLI 中的金鑰展開命令](#)
  - [CloudHSM CLI 中的金鑰包裝命令](#)
- [使用 CloudHSM CLI 匯出非對稱金鑰](#) 現在支援匯出公有金鑰。

## OpenSSL 動態引擎

- 現在安裝 AWS CloudHSM OpenSSL 程式庫版本 3.x 的平台支援 OpenSSL 動態引擎。這包括 Amazon Linux 2023、RHEL 9 (9.2+) 和 Ubuntu 22.04。

## JCE

- 新增對 JDK 17 和 JDK 21 的支援。
- 新增了對用於 HMAC 操作的 AES 金鑰的支援。
- 已新增金鑰屬性 ID。
- 引進了新的變 DataExceptionCause 體，用於金鑰耗盡：DataExceptionCause.KEY\_EXHAUSTED。

## 錯誤修正/效能改進：

- 將 label 屬性的長度上限從 126 個字元增加到 127 個字元。
- 已修正無法使用 RsaOaep 機制取消包裝 EC 金鑰的錯誤。
- 已解決 JCE 供應商中 getKey 操作的已知問題。請參閱 [問題：用戶端 SDK 5 記憶體流失搭配 getKey 操作](#) 以取得詳細資訊。
- 根據 FIPS 140-2，針對已達到最大加密區塊限制的三重 DES 金鑰，改善所有 SDKs 的記錄。
- 新增 OpenSSL 動態引擎的已知問題。如需詳細資訊，請參閱 [適用於的 OpenSSL 動態引擎的已知問題 AWS CloudHSM](#)。

## 5.10.0 版

用戶端 SDK 5.10.0 提升了穩定性，並修復了所有 SDK 的錯誤。

### CloudHSM CLI

- 新增了允許客戶使用 CloudHSM CLI 管理金鑰的新命令，包括：
  - 建立對稱金鑰和非對稱金鑰對
  - 共用和取消共用金鑰
  - 使用索引鍵屬性列出和篩選金鑰
  - 設定索引鍵屬性
  - 產生金鑰參考檔案
  - 刪除金鑰
- 已改善錯誤記錄。
- 新增了在互動式模式下對多行 unicode 命令的支持。

### 錯誤修正/效能改進：

- 提升了所有 SDK 在匯入、取消包裝、衍生和建立工作階段金鑰方面的性能。
- 修正了 JCE 提供者中無法在退出時移除暫存檔案的錯誤。
- 修正了因替換叢集中的 HSM 後造成特定情況下連線錯誤的錯誤。
- 修改了 JCE `getVersion` 輸出格式，以處理較大次要版本編號並包含修補程式編號。

### 平台支援

- 新增了 Ubuntu 22.04 對 JCE、PKCS #11 和 CloudHSM CLI 的支援 (該平台尚不支援 OpenSSL 動態引擎)。

## 5.9.0 版本

用戶端 SDK 5.9.0 提升了穩定性，並修復了所有 SDK 的錯誤。已對所有 SDK 進行了優化，以便在確定 HSM 無法使用時可立即通知應用程式操作失敗。此版本改善了 JCE 的效能。

### JCE 提供者

- 改善效能

- 修正工作階段集區耗盡的[已知問題](#)

## AWS CloudHSM 已取代的用戶端 SDK 版本

5.8.0 版及更早版本已棄用。建議在工作負載中不要使用已淘汰版本。後續不再對已淘汰版本提供相容更新，也不再託管已淘汰版本供下載。若您在使用已淘汰版本過程中，生產受到影響，則須升級版本進行軟體修復。

### 已棄用的用戶端 SDK 5 版本

本節列出已棄用的用戶端 SDK 5 版本。

#### 5.8.0 版本

5.8.0 版本新增了如下功能：使用 CloudHSM CLI 進行規定人數驗證、使用 JSSE 進行 SSL/TLS 卸載、提供 PKCS #11 多插槽支援、提供 JCE 多叢集/多使用者支援、使用 JCE 擷取金鑰、提供支援 JCE 的 KeyFactory、重新設定非終端傳回碼。該版本也提升了穩定性並修正了錯誤。

#### PKCS #11 程式庫

- 新增了對多插槽配置的支援功能。

#### JCE 提供者

- 新增了基於組態的金鑰擷取功能。
- 新增了對多叢集和多使用者組態的支援功能。
- 新增了使用 JSSE 進行 SSL 和 TLS 卸載的支援功能。
- 新增了 AES/CBC/NoPadding 取消包裝支援功能。
- 新增了金鑰工廠新類型：SecretKeyFactory 和 KeyFactory。

#### CloudHSM CLI

- 新增了對規定人數驗證的支援功能。

#### 5.7.0 版本

5.7.0 版本引入了 CloudHSM CLI 並包含一種全新加密式訊息驗證程式碼 (CMAC) 演算法。此版本在 Amazon Linux 2 上新增了 ARM 架構。JCE 提供者 Javadocs 現在可用於 AWS CloudHSM。

## PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。
- 目前 Amazon Linux 2 已支援 ARM 架构。
- 演算法
  - CKM\_AES\_CMAC (簽署及驗證)

## OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。
- 目前 Amazon Linux 2 已支援 ARM 架构。

## JCE 提供者

- 提升了穩定性並修正了錯誤。
- 演算法
  - AESCMAC

## 5.6.0 版本

5.6.0 版本包含 PKCS #11 程式庫和 JCE 提供者的新機制支援功能。5.6 版也支援 Ubuntu 20.04。

## PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。
- 機制
  - 適用於加密、解密、簽署及驗證模式的 CKM\_RSA\_X\_509

## OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

## JCE 提供者

- 提升了穩定性並修正了錯誤。
- 加密方式



- 適用於加密和解密模式的 RSA/ECB/NoPadding

## 支援的金鑰

- EC 曲線 secp224r1 和 secp521r1

## 平台支援

- 新增對 Ubuntu 20.04 的支援。

## 5.5.0 版本

5.5.0 版本新增了對 OpenJDK 11 的支援，整合了 Keytool 和 Jarsigner，同時也為 JCE 增加了其他機制。解決了關於 KeyGenerator 類別錯誤地將金鑰大小參數解釋為位元組而非位元的[已知問題](#)。

## PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。

## OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

## JCE 提供者

- 支援 Keytool 和 Jarsigner 公用程式
- 所有平台上均支援 OpenJDK 11
- 加密方式
  - AES/CBC/NoPadding 加密和解密模型
  - AES/ECB/PKCS5Padding 加密和解密模型
  - AES/CTR/NoPadding 加密和解密模型
  - AES/GCM/NoPadding 包裝和取消包裝模型
  - DESede/ECB/PKCS5Padding 加密和解密模型
  - DESede/CBC/NoPadding 加密和解密模型
  - AESWrap/ECB/NoPadding 包裝和取消包裝模型

- AESWrap/ECB/PKCS5Padding 包裝和取消包裝模型
- AESWrap/ECB/ZeroPadding 包裝和取消包裝模型
- RSA/ECB/PKCS1Padding 包裝和取消包裝模型
- RSA/ECB/OAEPPadding 包裝和取消包裝模型
- RSA/ECB/OAEPWithSHA-1ANDMGF1Padding 包裝和取消包裝模型
- RSA/ECB/OAEPWithSHA-224ANDMGF1Padding 包裝和取消包裝模型
- RSA/ECB/OAEPWithSHA-256ANDMGF1Padding 包裝和取消包裝模型
- RSA/ECB/OAEPWithSHA-384ANDMGF1Padding 包裝和取消包裝模型
- RSA/ECB/OAEPWithSHA-512ANDMGF1Padding 包裝和取消包裝模型
- RSAAESWrap/ECB/OAEPPadding 包裝和取消包裝模型
- RSAAESWrap/ECB/OAEPWithSHA-1ANDMGF1Padding 包裝和取消包裝模型
- RSAAESWrap/ECB/OAEPWithSHA-224ANDMGF1Padding 包裝和取消包裝模型
- RSAAESWrap/ECB/OAEPWithSHA-256ANDMGF1Padding 包裝和取消包裝模型
- RSAAESWrap/ECB/OAEPWithSHA-384ANDMGF1Padding 包裝和取消包裝模型
- RSAAESWrap/ECB/OAEPWithSHA-512ANDMGF1Padding 包裝和取消包裝模型
- KeyFactory 和 SecretKeyFactory
  - RSA : 2048 位元至 4096 位元 RSA 金鑰，以 256 位元為單位遞增
  - AES : 128 位元、192 位元和 256 位元 AES 金鑰
  - NIST 曲線 secp256r1 (P-256)、secp384r1 (P-384) 和 secp256k1 的 EC 金鑰對
  - DESede (3DES)
  - GenericSecret
  - HMAC : 支援 SHA1、SHA224、SHA256、SHA384 和 SHA512 雜湊
- 簽署/驗證
  - RSASSA-PSS
  - SHA1withRSA/PSS
  - SHA224withRSA/PSS
  - SHA256withRSA/PSS
  - SHA384withRSA/PSS
  - SHA512withRSA/PSS

- SHA224withRSAandMGF1
- SHA256withRSAandMGF1
- SHA384withRSAandMGF1
- SHA512withRSAandMGF1

#### 5.4.2 版本

5.4.2 版本提升了穩定性，並修復了所有 SDK 的錯誤。該版本也是 CentOS 8 平台的最後一個發行版本。如需詳細資訊，請參閱 [CentOS 網站](#)。

##### PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。

##### OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

##### JCE 提供者

- 提升了穩定性並修正了錯誤。

#### 5.4.1 版本

5.4.1 版本解決了 PKCS #11 程式庫的一個[已知問題](#)。該版本也是 CentOS 8 平台的最後一個發行版本。如需詳細資訊，請參閱 [CentOS 網站](#)。

##### PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。

##### OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

##### JCE 提供者

- 提升了穩定性並修正了錯誤。

## 5.4.0 版本

5.4.0 版本為所有平台新增了對 JCE 提供者的初始支援。JCE 提供者與 OpenJDK 8 相容。

### PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。

### OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

### JCE 提供者

- 金鑰類型
  - RSA : 2048 位元至 4096 位元 RSA 金鑰，以 256 位元為單位遞增。
  - AES : 128 位元、192 位元和 256 位元 AES 金鑰。
  - NIST 曲線 secp256r1 (P-256)、secp384r1 (P-384) 和 secp256k1 的 ECC 金鑰對。
  - DESede (3DES)
  - HMAC : 支援 SHA1、SHA224、SHA256、SHA384 和 SHA512 雜湊。
- 加密方式 (僅限加密和解密)
  - AES/GCM/NoPadding
  - AES/ECB/NoPadding
  - AES/CBC/PKCS5Padding
  - DESede/ECB/NoPadding
  - DESede/CBC/PKCS5Padding
  - AES/CTR/NoPadding
  - RSA/ECB/PKCS1Padding
  - RSA/ECB/OAEPPadding
  - RSA/ECB/OAEPWithSHA-1ANDMGF1Padding
  - RSA/ECB/OAEPWithSHA-224ANDMGF1Padding
  - RSA/ECB/OAEPWithSHA-256ANDMGF1Padding
  - RSA/ECB/OAEPWithSHA-384ANDMGF1Padding
  - RSA/ECB/OAEPWithSHA-512ANDMGF1Padding

- 摘要
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- 簽署/驗證
  - NONEwithRSA
  - SHA1withRSA
  - SHA224withRSA
  - SHA256withRSA
  - SHA384withRSA
  - SHA512withRSA
  - NONEwithECDSA
  - SHA1withECDSA
  - SHA224withECDSA
  - SHA256withECDSA
  - SHA384withECDSA
  - SHA512withECDSA
- 與 Java KeyStore 整合

### 5.3.0 版本

#### PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。

#### OpenSSL 動態引擎

- 新增了曲線 P-256、P-384 和 secp256k1 的 ECDSA 簽署/驗證支援。
- 新增對平台的支援：Amazon Linux、Amazon Linux 2、CentOS 7.8+、RHEL 7 (7.8+)。

已棄用的用戶端 SDK 5 版本

- 新增了對 OpenSSL 1.0.2 版本的支援。

- 提升了穩定性並修正了錯誤。

## JCE 提供者

- 金鑰類型
  - RSA : 2048 位元至 4096 位元 RSA 金鑰，以 256 位元為單位遞增。
  - AES : 128 位元、192 位元和 256 位元 AES 金鑰。
  - NIST 曲線 secp256r1 (P-256)、secp384r1 (P-384) 和 secp256k1 的 EC 金鑰對。
  - DESede (3DES)
  - HMAC : 支援 SHA1、SHA224、SHA256、SHA384 和 SHA512 雜湊。
- 加密方式 (僅限加密和解密)
  - AES/GCM/NoPadding
  - AES/ECB/NoPadding
  - AES/CBC/PKCS5Padding
  - DESede/ECB/NoPadding
  - DESede/CBC/PKCS5Padding
  - AES/CTR/NoPadding
  - RSA/ECB/PKCS1Padding
  - RSA/ECB/OAEPPadding
  - RSA/ECB/OAEPWithSHA-1ANDMGF1Padding
  - RSA/ECB/OAEPWithSHA-224ANDMGF1Padding
  - RSA/ECB/OAEPWithSHA-256ANDMGF1Padding
  - RSA/ECB/OAEPWithSHA-384ANDMGF1Padding
  - RSA/ECB/OAEPWithSHA-512ANDMGF1Padding
- 摘要
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384

- 簽署/驗證
  - NONEwithRSA
  - SHA1withRSA
  - SHA224withRSA
  - SHA256withRSA
  - SHA384withRSA
  - SHA512withRSA
  - NONEwithECDSA
  - SHA1withECDSA
  - SHA224withECDSA
  - SHA256withECDSA
  - SHA384withECDSA
  - SHA512withECDSA
- 與 Java KeyStore 整合

### 5.2.1 版本

#### PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。

#### OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

### 5.2.0 版本

5.2.0 版本新增了將其他金鑰類型和機制添加至 PKCS #11 程式庫的支援。

#### PKCS #11 程式庫

##### 金鑰類型

- ECDSA : P-224、P-256、P-384、P-521 和 secp256k1 曲線
- 三重 DES (3DES)

## 機制

- CKM\_EC\_KEY\_PAIR\_GEN
- CKM\_DES3\_KEY\_GEN
- CKM\_DES3\_CBC
- CKM\_DES3\_CBC\_PAD
- CKM\_DES3\_ECB
- CKM\_ECDSA
- CKM\_ECDSA\_SHA1
- CKM\_ECDSA\_SHA224
- CKM\_ECDSA\_SHA256
- CKM\_ECDSA\_SHA384
- CKM\_ECDSA\_SHA512
- 用於加密/解密的 CKM\_RSA\_PKCS

## OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

## 5.1.0 版本

5.1.0 版本新增了將其他機制添加至 PKCS #11 程式庫的支援。

## PKCS #11 程式庫

## 機制

- 用於包裝/取消包裝的 CKM\_RSA\_PKCS
- CKM\_RSA\_PKCS\_PSS
- CKM\_SHA1\_RSA\_PKCS\_PSS
- CKM\_SHA224\_RSA\_PKCS\_PSS
- CKM\_SHA256\_RSA\_PKCS\_PSS
- CKM\_SHA384\_RSA\_PKCS\_PSS
- CKM\_SHA512\_RSA\_PKCS\_PSS
- CKM\_AES\_ECB



- CKM\_AES\_CTR
- CKM\_AES\_CBC
- CKM\_AES\_CBC\_PAD
- CKM\_SP800\_108\_COUNTER\_KDF
- CKM\_GENERIC\_SECRET\_KEY\_GEN
- CKM\_SHA\_1\_HMAC
- CKM\_SHA224\_HMAC
- CKM\_SHA256\_HMAC
- CKM\_SHA384\_HMAC
- CKM\_SHA512\_HMAC
- 僅用於包裝/取消包裝的 CKM\_RSA\_PKCS\_OAEP
- CKM\_RSA\_AES\_KEY\_WRAP
- CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_NO\_PAD
- CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_PKCS5\_PAD
- CKM\_CLOUDHSM\_AES\_KEY\_WRAP\_ZERO\_PAD

## API 操作

- C\_CreateObject
- C\_DeriveKey
- C\_WrapKey
- C\_UnWrapKey

## OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

### 5.0.1 版本

5.0.1 版本新增了對 OpenSSL 動態引擎的初始支援。

## PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。

## OpenSSL 動態引擎

- OpenSSL 動態引擎的初始版本。
- 此版本為金鑰類型和 OpenSSL API 提供了介紹性支援：
  - 產生 2048 位元、3072 位元和 4096 位元金鑰的 RSA 金鑰
  - OpenSSL API：
    - 使用帶有 SHA1/224/256/384/512 和 RSA PSS 進行 [RSA 簽署](#)
    - [RSA 金鑰產生](#)

如需詳細資訊，請參閱 [OpenSSL 動態引擎](#)。

- 支援平台：CentOS 8.3+、Red Hat Enterprise Linux (RHEL) 8.3+ 和 Ubuntu 18.04 LTS
- 版本要求：OpenSSL 1.1.1

如需詳細資訊，請參閱 [支援平台](#)。

- CentOS 8.3+、Red Hat Enterprise Linux (RHEL) 8.3、Ubuntu 18.04 LTS、包括適用於特定加密套件的 NGINX 1.19 支持 SSL/TLS 卸載。

如需詳細資訊，請參閱 [使用 Tomcat 的 Linux 上的 SSL/TLS 卸載](#)，或使用 [NGINX 或 Apache 的 Linux 上的 SSL/TLS 卸載](#)。

## 5.0.0 版本

5.0.0 版本 為初始版本。

## PKCS #11 程式庫

- 此版本為初始版本。

## 用戶端 SDK 5.0.0 版本對 PKCS #11 程式庫的支援情況說明

本節詳細介紹了用戶端 SDK 5.0.0 版本在金鑰類型、機制、API 操作和屬性方面的支援情況。

### 金鑰類型：

- AES：128 位元、192 位元和 256 位元 AES 金鑰。
- RSA：2048 位元至 4096 位元 RSA 金鑰，以 256 位元為單位遞增

### 機制：

- CKM\_AES\_GCM
- CKM\_AES\_KEY\_GEN
- CKM\_CLOUDHSM\_AES\_GCM
- CKM\_RSA\_PKCS
- CKM\_RSA\_X9\_31\_KEY\_PAIR\_GEN
- CKM\_SHA1
- CKM\_SHA1\_RSA\_PKCS
- CKM\_SHA224
- CKM\_SHA224\_RSA\_PKCS
- CKM\_SHA256
- CKM\_SHA256\_RSA\_PKCS
- CKM\_SHA384
- CKM\_SHA384\_RSA\_PKCS
- CKM\_SHA512
- CKM\_SHA512\_RSA\_PKCS

#### API 操作：

- C\_CloseAllSessions
- C\_CloseSession
- C\_Decrypt
- C\_DecryptFinal
- C\_DecryptInit
- C\_DecryptUpdate
- C\_DestroyObject
- C\_Digest
- C\_DigestFinal
- C\_DigestInit
- C\_DigestUpdate
- C\_Encrypt
- C\_EncryptFinal

- C\_EncryptInit
- C\_EncryptUpdate
- C\_Finalize
- C\_FindObjects
- C\_FindObjectsFinal
- C\_FindObjectsInit
- C\_GenerateKey
- C\_GenerateKeyPair
- C\_GenerateRandom
- C\_GetAttributeValue
- C\_GetFunctionList
- C\_GetInfo
- C\_GetMechanismInfo
- C\_GetMechanismList
- C\_GetSessionInfo
- C\_GetSlotInfo
- C\_GetSlotList
- C\_GetTokenInfo
- C\_Initialize
- C\_Login
- C\_Logout
- C\_OpenSession
- C\_Sign
- C\_SignFinal
- C\_SignInit
- C\_SignUpdate
- C\_Verify
- C\_VerifyFinal
- C\_VerifyInit
- C\_VerifyUpdate

屬性：

- GenerateKeyPair
  - 所有 RSA 金鑰屬性
- GenerateKey
  - 所有 AES 金鑰屬性
- GetAttributeValue
  - 所有 RSA 金鑰屬性
  - 所有 AES 金鑰屬性

範例：

- [產生金鑰 \(AES、RSA、EC\)](#)
- [列出金鑰屬性](#)
- [使用 AES GCM 加密和解密資料](#)
- [使用 RSA 簽署和驗證資料](#)

## 已棄用的用戶端 SDK 3 版本

本節列出已棄用的用戶端 SDK 3 版本。

### 3.4.4 版

3.4.4 版本新增了對 JCE 提供者的更新。

#### AWS CloudHSM 用戶端軟體

- 更新版本的一致性。

#### PKCS #11 程式庫

- 更新版本的一致性。

#### OpenSSL 動態引擎

- 更新版本的一致性。

## JCE 提供者

- 將 log4j 更新至 2.17.1 版本。

## Windows (CNG 和 KSP 提供者)

- 更新版本的一致性。

### 3.4.3 版本

3.4.3 版本新增了對 JCE 提供者的更新。

## AWS CloudHSM 用戶端軟體

- 更新版本的一致性。

## PKCS #11 程式庫

- 更新版本的一致性。

## OpenSSL 動態引擎

- 更新版本的一致性。

## JCE 提供者

- 將 log4j 更新至 2.17.0 版本。

## Windows (CNG 和 KSP 提供者)

- 更新版本的一致性。

### 3.4.2 版本

3.4.2 版本新增了對 JCE 提供者的更新。

## AWS CloudHSM 用戶端軟體

- 更新版本的一致性。

## PKCS #11 程式庫

- 更新版本的一致性。

## OpenSSL 動態引擎

- 更新版本的一致性。

## JCE 提供者

- 將 log4j 更新至 2.16.0 版本。

## Windows (CNG 和 KSP 提供者)

- 更新版本的一致性。

## 3.4.1 版本

3.4.1 版本新增了對 JCE 提供者的更新。

## AWS CloudHSM 用戶端軟體

- 更新版本的一致性。

## PKCS #11 程式庫

- 更新版本的一致性。

## OpenSSL 動態引擎

- 更新版本的一致性。

## JCE 提供者

- 將 log4j 更新至 2.15.0 版本。

## Windows (CNG 和 KSP 提供者)

- 更新版本的一致性。

### 3.4.0 版本

3.4.0 版本新增了對所有元件的更新。

#### AWS CloudHSM 用戶端軟體

- 提升了穩定性並修正了錯誤。

#### PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。

#### OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

#### JCE 提供者

- 提升了穩定性並修正了錯誤。

#### Windows (CNG 和 KSP 提供者)

- 提升了穩定性並修正了錯誤。

### 3.3.2 版本

3.3.2 版解決 `client_info` 指令碼[的問題](#)。

#### AWS CloudHSM 用戶端軟體

- 更新版本的一致性。

#### PKCS #11 程式庫

- 更新版本的一致性。



## OpenSSL 動態引擎

- 更新版本的一致性。

## JCE 提供者

- 更新版本的一致性。

## Windows (CNG 和 KSP 提供者)

- 更新版本的一致性。

### 3.3.1 版本

3.3.1 版本新增了對所有元件的更新。

## AWS CloudHSM 用戶端軟體

- 提升了穩定性並修正了錯誤。

## PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。

## OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

## JCE 提供者

- 提升了穩定性並修正了錯誤。

## Windows (CNG 和 KSP 提供者)

- 提升了穩定性並修正了錯誤。

### 3.3.0 版本

3.3.0 版本新增了雙重要素驗證 (2FA) 和其他效能改進。

#### AWS CloudHSM 用戶端軟體

- 為加密管理員 (CO) 添加了 2FA 驗證。如需詳細資訊，請參閱[加密管理員雙重要素驗證管理](#)。
- 移除了對 RedHat Enterprise Linux 6 和 CentOS 6 的平台支援。如需詳細資訊，請參閱[Linux 支援](#)。
- 新增了 CMU 的獨立版本，可與用戶端 SDK 5 或用戶端 SDK 3 搭配使用。該版本與用戶端常駐程式 3.3.0 版本隨附的 CMU 版本相同。現在您可下載 CMU，無需下載用戶端常駐程式。

#### PKCS #11 程式庫

- 提升了穩定性並修正了錯誤。
- 移除了對 RedHat Enterprise Linux 6 和 CentOS 6 的平台支援。如需詳細資訊，請參閱[Linux 支援](#)。

#### OpenSSL 動態引擎

- 更新版本的一致性。
- 移除了對 RedHat Enterprise Linux 6 和 CentOS 6 的平台支援。如需詳細資訊，請參閱[Linux 支援](#)。

#### JCE 提供者

- 提升了穩定性並修正了錯誤。
- 移除了對 RedHat Enterprise Linux 6 和 CentOS 6 的平台支援。如需詳細資訊，請參閱[Linux 支援](#)。

#### Windows (CNG 和 KSP 提供者)

- 更新版本的一致性。

### 3.2.1 版本

3.2.1 版新增了 PKCS #11 程式庫 AWS CloudHSM 實作與 PKCS #11 標準、新平台和其他改進之間的合規分析。

#### AWS CloudHSM 用戶端軟體

- 新增對 CentOS 8、RHEL 8 和 Ubuntu 18.04 LTS 的平台支援。如需詳細資訊，請參閱 [???](#)。

#### PKCS #11 程式庫

- [用戶端 SDK 3.2.1 的 PKCS #11 程式庫合規性報告](#)
- 新增對 CentOS 8、RHEL 8 和 Ubuntu 18.04 LTS 的平台支援。如需詳細資訊，請參閱 [???](#)。

#### OpenSSL 動態引擎

- 不支援 CentOS 8、RHEL 8 和 Ubuntu 18.04 LTS。如需詳細資訊，請參閱 [???](#)。

#### JCE 提供者

- 新增對 CentOS 8、RHEL 8 和 Ubuntu 18.04 LTS 的平台支援。如需詳細資訊，請參閱 [???](#)。

#### Windows (CNG 和 KSP 提供者)

- 提升了穩定性並修正了錯誤。

### 3.2.0 版本

3.2.0 版本新增了對遮罩密碼和其他效能改進的支援。

#### AWS CloudHSM 用戶端軟體

- 新增了在使用命令行工具時隱藏密碼的支援。如需詳細資訊，請參閱 [loginHSM](#) 和 [logoutHSM](#) (cloudhsm\_mgmt\_util) 和 [loginHSM](#) 和 [logoutHSM](#) (key\_mgmt\_util)。

#### PKCS #11 程式庫

- 對於先前某些未受支援的 PKCS #11 機制，新增了對軟體中大型雜湊資料的支援。如需詳細資訊，請參閱[受支援的機制](#)。

### OpenSSL 動態引擎

- 提升了穩定性並修正了錯誤。

### JCE 提供者

- 更新版本的一致性。

### Windows (CNG 和 KSP 提供者)

- 提升了穩定性並修正了錯誤。

### 3.1.2 版本

3.1.2 版本新增了對 JCE 提供者的更新。

### AWS CloudHSM 用戶端軟體

- 更新版本的一致性。

### PKCS #11 程式庫

- 更新版本的一致性。

### OpenSSL 動態引擎

- 更新版本的一致性。

### JCE 提供者

- 將 log4j 更新至 2.13.3 版本

### Windows (CNG 和 KSP 提供者)

- 更新版本的一致性。

### 3.1.1 版本

#### AWS CloudHSM 用戶端軟體

- 更新版本的一致性。

#### PKCS #11 程式庫

- 更新版本的一致性。

#### OpenSSL 動態引擎

- 更新版本的一致性。

#### JCE 提供者

- 錯誤修正與效能改進。

#### Windows (CNG、KSP)

- 更新版本的一致性。

### 3.1.0 版本

3.1.0 版本新增[符合標準的 AES 金鑰包裝](#)。

#### AWS CloudHSM 用戶端軟體

- 升級新要求：您的用戶端版本須跟您正在使用的任何軟體程式庫版本相符。若要升級，您必須使用可同時升級用戶端和所有程式庫的批次命令。如需詳細資訊，請參閱[用戶端 SDK 3 升級](#)。
- Key\_mgmt\_util (KMU) 包含下列更新：
  - 新增了兩種新的 AES 金鑰包裝方法，即：符合標準的零填補 AES 金鑰包裝和無填補 AES 金鑰包裝。如需詳細資訊，請參閱 [wrapKey](#) 和 [unwrapKey](#)。
  - 使用 AES\_KEY\_WRAP\_PAD\_PKCS5 包裝金鑰時，無法使用自訂 IV 功能。如需詳細資訊，請參閱[AES 金鑰包裝](#)。

## PKCS #11 程式庫

- 新增了兩種新的 AES 金鑰包裝方法，即：符合標準的零填補 AES 金鑰包裝和無填補 AES 金鑰包裝。如需詳細資訊，請參閱[AES 金鑰包裝](#)。
- 您可以設定 RSA-PSS 簽章的 salt 長度。若要了解如何使用此功能，請參閱 GitHub 上的 [RSA-PSS 簽章的可設定 salt 長度](#)。

## OpenSSL 動態引擎

- 重大變更：使用 SHA1 的 TLS 1.0 和 1.2 加密套件不適應 OpenSSL 引擎 3.1.0。這個問題很快就會解決。
- 如果您想要在 RHEL 6 或 CentOS 6 上安裝 OpenSSL 動態引擎程式庫，請參閱有關這些作業系統上安裝之預設 OpenSSL 版本的[已知問題](#)。
- 已提升穩定性並修正錯誤

## JCE 提供者

- 重大變更：為解決 Java Cryptography Extension (JCE) 相容性問題，AES 包裝和取消包裝現在會正確使用 AesWrap 演算法，而不是 AES 演算法。這代表 Cipher.WRAP\_MODE 和 Cipher.UNWRAP\_MODE 不再適應 AES/ECB 和 AES/CBC 機制。

若要升級至用戶端 3.1.0 版本，您須更新程式碼。若您已有包裝金鑰，則須特別注意您用來取消包裝的機制以及 IV 預設值的變更方式。若您使用用戶端 3.0.0 版本或以下版本的包裝金鑰，則在 3.1.1 中，您須使用 AESWrap/ECB/PKCS5Padding 來取消包裝現有金鑰。如需詳細資訊，請參閱[AES 金鑰包裝](#)。

- 您可以從 JCE 提供者中列出具有相同標籤的多個金鑰。若要了解如何逐一查看所有可用金鑰，請參閱 GitHub 上的[尋找所有金鑰](#)。
- 您可在金鑰建立期間為屬性設定更多限制值，包括為公有金鑰和私有金鑰指定不同的標籤。如需詳細資訊，請參閱[支援的 Java 屬性](#)。

## Windows (CNG、KSP)

- 提升了穩定性並修正了錯誤。

## AWS CloudHSM end-of-life用戶端 SDK 版本

下列 AWS CloudHSM 用戶端版本已結束支援。這些 AWS CloudHSM 用戶端版本不再與 服務相容，也不會收到更新。為了維護應用程式的安全性，AWS CloudHSM 可能會拒絕來自己結束支援之版本的連線。

- SDK 3.4.4 版和更早版本已結束支援。
- SDK 5.8.0 版和更早版本已結束支援。

# 文件歷史紀錄

此主題說明 AWS CloudHSM 使用者指南的重大更新。

主題

- [最近更新](#)
- [舊版更新](#)

## 最近更新

下表說明此文件自 2018 年 4 月後的重大變更。除了這裡所列的主要變更外，我們也會經常更新文件以改進說明內容和範例，並且反映您傳送給我們的意見回饋。如要接收重大變更的通知，請使用右上角的連結來訂閱 RSS 摘要。

如需新版本的詳細資訊，請參閱 [AWS CloudHSM 用戶端 SDK 的下載](#)

| 變更                             | 描述                                   | 日期               |
|--------------------------------|--------------------------------------|------------------|
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.16.1 版。       | 2025 年 6 月 25 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.16.0 版。       | 2025 年 5 月 1 日   |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.15.0 版。       | 2025 年 2 月 3 日   |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.14.0 版。       | 2024 年 11 月 26 日 |
| <a href="#">新的 HSM 類型和叢集模式</a> | 新增在 FIPS 模式叢集中建立 (hsm2m.medium) 的支援。 | 2024 年 8 月 20 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.13.0 版。       | 2024 年 8 月 13 日  |



|                                |                                                  |                  |
|--------------------------------|--------------------------------------------------|------------------|
| <a href="#">新的 HSM 類型和叢集模式</a> | 啟動新的 HSM 類型 (hsm2m.medium) 和新的叢集模式 (非 FIPS)。     | 2024 年 6 月 10 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.12.0 版。                   | 2024 年 3 月 20 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.11.0 版。                   | 2024 年 1 月 17 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.10.0 版。                   | 2023 年 7 月 28 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.9.0 版。                    | 2023 年 5 月 23 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.8.0 版。                    | 2023 年 3 月 16 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.7.0 版。                    | 2022 年 11 月 16 日 |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.6.0 版。                    | 2022 年 9 月 1 日   |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.5.0 版。                    | 2022 年 5 月 13 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.4.2 版。                    | 2022 年 3 月 18 日  |
| <a href="#">新增版本</a>           | 已發行 AWS CloudHSM 用戶端 5.4.1 版。                    | 2022 年 2 月 10 日  |
| <a href="#">新增版本</a>           | 已發行適用於 Windows 平台的 AWS CloudHSM JCE 提供者 5.4.0 版。 | 2022 年 2 月 1 日   |

|                      |                                                               |                  |
|----------------------|---------------------------------------------------------------|------------------|
| <a href="#">新增版本</a> | 發行了 AWS CloudHSM 用戶端 5.4.0 版，該版本為所有 Linux 平台的 JCE 供應商新增了初始支援。 | 2022 年 1 月 28 日  |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 5.3.0 版。                                 | 2022 年 1 月 3 日   |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 3.4.4 版。                                 | 2022 年 1 月 3 日   |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 3.4.3 版。                                 | 2021 年 12 月 20 日 |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 3.4.2 版。                                 | 2021 年 12 月 15 日 |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 3.4.1 版。                                 | 2021 年 12 月 10 日 |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 5.2.1 版。                                 | 2021 年 10 月 4 日  |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 3.4.0 版。                                 | 2021 年 8 月 25 日  |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 5.2.0 版。                                 | 2021 年 8 月 3 日   |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 3.3.2 版。                                 | 2021 年 7 月 2 日   |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 5.1.0 版。                                 | 2021 年 6 月 1 日   |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 3.3.1 版。                                 | 2021 年 4 月 26 日  |
| <a href="#">新增版本</a> | 已發行 AWS CloudHSM 用戶端 5.0.1 版。                                 | 2021 年 4 月 8 日   |

|                        |                                                                                                            |                  |
|------------------------|------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">新增版本</a>   | 已發行 AWS CloudHSM 用戶端 5.0.0 版。                                                                              | 2021 年 3 月 12 日  |
| <a href="#">已新增的內容</a> | 新增界面 VPC 端點，這項 AWS 功能可讓您在 VPC 與之間建立私有連線，AWS CloudHSM 而不需要透過網際網路或 NAT 裝置、VPN 連線或 AWS Direct Connect 連線進行存取。 | 2021 年 2 月 10 日  |
| <a href="#">新增版本</a>   | 已發行 AWS CloudHSM 用戶端 3.3.0 版。                                                                              | 2021 年 2 月 3 日   |
| <a href="#">已新增的內容</a> | 新增管理備份保留功能，這項功能可自動刪除舊備份。                                                                                   | 2020 年 11 月 18 日 |
| <a href="#">已新增的內容</a> | 新增合規報告，以 PKCS #11 標準分析 PKCS #11 程式庫的 AWS CloudHSM 用戶端 SDK 3.2.1 實作。                                        | 2020 年 10 月 29 日 |
| <a href="#">新增版本</a>   | 已發行 AWS CloudHSM 用戶端 3.2.1 版。                                                                              | 2020 年 10 月 8 日  |
| <a href="#">已新增的內容</a> | 已新增說明 AWS CloudHSM 中金鑰同步處理設定的文件。                                                                           | 2020 年 9 月 1 日   |
| <a href="#">新增版本</a>   | 已發行 AWS CloudHSM 用戶端 3.2.0 版。                                                                              | 2020 年 8 月 31 日  |
| <a href="#">新增版本</a>   | 已發行 AWS CloudHSM 用戶端 3.1.2 版。                                                                              | 2020 年 7 月 30 日  |
| <a href="#">新增版本</a>   | 已發行 AWS CloudHSM 用戶端 3.1.1 版。                                                                              | 2020 年 6 月 3 日   |
| <a href="#">新增版本</a>   | 已發行 AWS CloudHSM 用戶端 3.1.0 版。                                                                              | 2020 年 5 月 21 日  |

|                          |                                                      |                  |
|--------------------------|------------------------------------------------------|------------------|
| <a href="#">新增版本</a>     | 已發行 AWS CloudHSM 用戶端 3.0.1 版。                        | 2020 年 4 月 20 日  |
| <a href="#">新增版本</a>     | 已發行適用於 Windows Server 平台的 AWS CloudHSM 用戶端 3.0.0 版。  | 2019 年 10 月 30 日 |
| <a href="#">新增版本</a>     | 已針對 Windows 以外的所有平台發行 AWS CloudHSM 用戶端 3.0.0 版。      | 2019 年 10 月 22 日 |
| <a href="#">新增版本</a>     | 已發行 AWS CloudHSM 用戶端 2.0.4 版。                        | 2019 年 8 月 26 日  |
| <a href="#">新增版本</a>     | 已發行 AWS CloudHSM 用戶端 2.0.3 版。                        | 2019 年 5 月 13 日  |
| <a href="#">新增版本</a>     | 已發行 AWS CloudHSM 用戶端 2.0.1 版。                        | 2019 年 3 月 21 日  |
| <a href="#">新增版本</a>     | 已發行 AWS CloudHSM 用戶端 2.0.0 版。                        | 2019 年 2 月 6 日   |
| <a href="#">已新增的區域支援</a> | 新增對歐洲（斯德哥爾摩）和 AWS GovCloud（美國東部）區域的 AWS CloudHSM 支援。 | 2018 年 12 月 19 日 |
| <a href="#">新增版本</a>     | 已發行適用於 Windows 的 AWS CloudHSM 用戶端 1.1.2 版。           | 2018 年 11 月 20 日 |
| <a href="#">更新已知問題</a>   | 將新內容新增至《故障診斷》指南。                                     | 2018 年 11 月 8 日  |
| <a href="#">新增版本</a>     | 已發行適用於 Linux 平台的 AWS CloudHSM 用戶端 1.1.2 版。           | 2018 年 11 月 8 日  |

|                          |                                                                                                                                                       |                  |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">已新增的區域支援</a> | 新增對歐洲（巴黎）和亞太區域（首爾）區域的 AWS CloudHSM 支援。                                                                                                                | 2018 年 10 月 24 日 |
| <a href="#">已新增的內容</a>   | 新增刪除和還原 AWS CloudHSM 備份的功能。                                                                                                                           | 2018 年 9 月 10 日  |
| <a href="#">已新增的內容</a>   | 已將自動稽核日誌傳送至 Amazon CloudWatch Logs。                                                                                                                   | 2018 年 8 月 13 日  |
| <a href="#">已新增的內容</a>   | 新增跨區域複製 AWS CloudHSM 叢集備份的功能。                                                                                                                         | 2018 年 7 月 30 日  |
| <a href="#">已新增的區域支援</a> | 新增對歐洲（倫敦）區域的 AWS CloudHSM 支援。                                                                                                                         | 2018 年 6 月 13 日  |
| <a href="#">已新增的內容</a>   | 新增對 Amazon Linux 2、Red Hat Enterprise Linux (RHEL) 6、Red Hat Enterprise Linux (RHEL) 7、CentOS 6、CentOS 7 和 Ubuntu 16.04 LTS 的 AWS CloudHSM 用戶端和程式庫支援。 | 2018 年 5 月 10 日  |
| <a href="#">新增版本</a>     | 新增 Windows AWS CloudHSM 用戶端。                                                                                                                          | 2018 年 4 月 30 日  |

## 舊版更新

下表說明 2018 年 AWS CloudHSM 之前的重要變更。

| 變更  | 描述                                                                             | 日期              |
|-----|--------------------------------------------------------------------------------|-----------------|
| 新內容 | 新增加密管理員 (CO) 的規定人數身分驗證 (M/N 存取控制)。如需詳細資訊，請參閱 <a href="#">使用 CloudHSM 管理公程式</a> | 2017 年 11 月 9 日 |

| 變更  | 描述                                                                                                   | 日期               |
|-----|------------------------------------------------------------------------------------------------------|------------------|
|     | <a href="#">(CMU) 管理規定人數身分驗證 (M/N 個存取控制)</a> 。                                                       |                  |
| 更新  | 新增有關使用 key_mgmt_util 命令列工具的文件。如需詳細資訊，請參閱 <a href="#">AWS CloudHSM Key Management Utility 命令的參考</a> 。 | 2017 年 11 月 9 日  |
| 新內容 | 新增 Oracle 透明資料加密。如需詳細資訊，請參閱 <a href="#">Oracle 資料庫加密</a> 。                                           | 2017 年 10 月 25 日 |
| 新內容 | 新增 SSL 卸載。如需詳細資訊，請參閱 <a href="#">SSL/TLS 卸載</a> 。                                                    | 2017 年 10 月 12 日 |
| 新指南 | 此版本推出 AWS CloudHSM                                                                                   | 2017 年 8 月 14 日  |

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。