使用者指南

Red Hat OpenShift Service on AWS

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

Red Hat OpenShift Service on AWS: 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、任從何貶低或使 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 擁有的商標都是其各自擁有者的資產，這些擁有者不一定與 Amazon.s 相關聯、連線或贊助。

Table of Contents

什麼是 Red Hat OpenShift Service on AWS？ ... 1
功能 ... 1
存取 ROSA ... 1
如何開始使用 ROSA ... 2
定價 ... 3
ROSA 服務費用 ... 3
AWS 基礎設施費用 ... 3
責任 ... 3
概觀 ... 4
按區域劃分的共同責任任務 ... 5
資料和應用程式的客戶責任 ... 21
架構 ... 24
比較 ROSA 與 HCP 和 ROSA classic ... 24
開始使用 ROSA ... 26
設定 ... 26
先決條件 ... 26
啟用 ROSA 和設定 AWS 先決條件 ... 27
建立 ROSA HCP 叢集 - CLI ... 27
先決條件 ... 28
建立 Amazon VPC 架構 ... 28
建立必要的 IAM 角色和 OpenID Connect 組態 ... 34
使用 CLI 和 建立具有 HCP ROSA 叢集的 ROSA AWS STS ... 36
設定身分提供者並授予 叢集 存取權 ... 37
授予使用者對 的存取權 叢集 ... 38
設定`cluster-admin`許可 ... 39
設定`dedicated-admin`許可 ... 39
叢集 透過 Red Hat 混合雲端主控台存取 ... 39
從 Developer Catalog 部署應用程式 ... 40
從使用者撤銷`cluster-admin`許可 ... 41
從使用者撤銷`dedicated-admin`許可 ... 41
撤銷使用者對 的存取權 叢集 ... 41
刪除叢集 AWS STS 和資源 ... 41
建立 ROSA 傳統叢集 - CLI ... 43
先決條件 ... 43

使用 CLI ROSA 和 建立 ROSA 傳統叢集 AWS STS 43
設定身分提供者並授予 叢集 存取權 45
授予使用者對 的存取權 叢集 47
設定cluster-admin許可 47
設定dedicated-admin許可 48
叢集 透過 Red Hat 混合雲端主控台存取 48
從 Developer Catalog 部署應用程式 48
從使用者撤銷cluster-admin許可 49
從使用者撤銷dedicated-admin許可 50
撤銷使用者對 的存取權 叢集 50
刪除叢集 AWS STS 和資源 50
建立 ROSA 傳統叢集 - AWS PrivateLink 51
先決條件 52
建立 Amazon VPC 架構 52
使用 CLI ROSA 和 建立 ROSA 傳統叢集 AWS PrivateLink 57
設定 AWS PrivateLink DNS 轉送 59
設定身分提供者並授予 叢集 存取權 60
授予使用者對 的存取權 叢集 61
設定cluster-admin許可 62
設定dedicated-admin許可 62
叢集 透過 Red Hat 混合雲端主控台存取 62
從 Developer Catalog 部署應用程式 63
從使用者撤銷cluster-admin許可 64
從使用者撤銷dedicated-admin許可 64
撤銷使用者對 的存取權 叢集 64
刪除叢集 AWS STS 和資源 65
安全 67
資料保護 67
資料加密 68
身分與存取管理 71
目標對象 71
使用身分驗證 72
使用政策管理存取權 74
ROSA 身分型政策範例 76
AWS 受管政策 95
故障診斷 112

恢復能力 114
AWS 全球基礎設施彈性 114
ROSA 叢集彈性 114
客戶部署的應用程式彈性 115
基礎架構安全 115
叢集網路隔離 116
Pod 網路隔離 116
Service Quotas 117
使用其他 服務 118
ROSA 而且 AWS Marketplace 118
術語 118
ROSA 付款和帳單 119
透過主控台訂閱 ROSA Marketplace 清單 120
購買 ROSA 合約 120
私有市場 125
故障診斷 126
存取 ROSA 叢集偵錯日誌 126
ROSA 叢集在 叢集 建立期間服務 AWS 配額檢查失敗 126
對 CLI ROSA 過期的離線存取權杖進行故障診斷 127
無法建立 叢集 具有 osdCcsAdmin 錯誤的 127
後續步驟 128
取得支援 128
開啟 支援 案例 128
開啟 Red Hat Support 案例 128
文件歷史紀錄 129
..... cxxxiii

什麼是 Red Hat OpenShift Service on AWS？

Red Hat OpenShift Service on AWS (ROSA) 是一項受管服務，您可以使用 Red Hat OpenShift 企業 Kubernetes 平台在 上建置、擴展和部署容器化應用程式 AWS。 可 ROSA 簡化將內部部署 Red Hat OpenShift 工作負載移至其中的流程 AWS，並提供與其他 的緊密整合 AWS 服務。

功能

ROSA 由 AWS 和 Red Hat 共同支援和操作。每個 ROSA 叢集都具有 24 小時 Red Hat 網站可靠性工程師 (SRE) 對叢集管理的支援，並以 Red Hat 的 99.95% 運作時間服務層級協議 (SLA) 為後盾。如需服務支援模型的詳細資訊，請參閱the section called “取得支援”。

ROSA 也提供下列功能：

- Red Hat SRE 支援的叢集安裝、叢集維護和叢集升級。
- AWS 服務 整合包括 AWS 運算、資料庫、分析、機器學習、聯網和行動。
- 跨多個 AWS 可用區域執行和擴展 Kubernetes 控制平面，以確保高可用性。
- 使用 OpenShift APIs 和開發人員生產力工具操作叢集，包括 Service Mesh、CodeReady Workspaces 和 Serverless。

存取 ROSA

您可以使用下列界面來定義和設定您的 ROSA 服務部署。

AWS

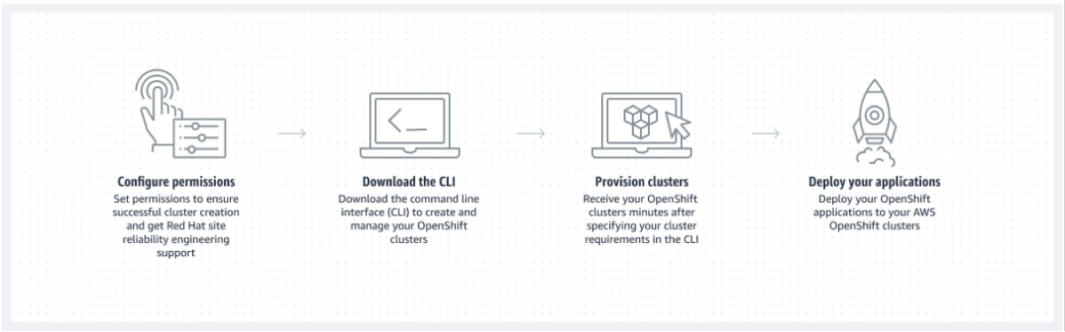
- ROSA 主控台 — 提供 Web 界面，以啟用 ROSA 訂閱並購買 ROSA 軟體合約。
- AWS Command Line Interface (AWS CLI) — 為 Windows、macOS AWS 服務 和 Linux 支援廣泛的和 命令集。如需詳細資訊，請參閱AWS Command Line Interface。

Red Hat OpenShift

- Red Hat 混合雲端主控台 — 提供 Web 界面來建立、更新和管理 ROSA 叢集、安裝叢集附加元件，以及建立和部署應用程式至 ROSA 叢集。
- ROSA CLI （玫瑰） — 提供建立、更新和管理 ROSA 叢集的命令。

- OpenShift CLI (oc) — 提供建立應用程式和管理 OpenShift 容器平台專案的命令。
- Knative CLI (kn) - 提供可用於與 OpenShift Serverless 元件互動的命令，例如 Knative Serving 和 Eventing。
- Pipelines CLI (tkn) - 提供使用終端機與 OpenShift Pipelines 互動的命令。
- opm CLI - 提供命令，協助運算子開發人員和叢集管理員從終端機建立和維護 OpenShift 運算子目錄。
- 運算子 SDK CLI - 提供運算子開發人員可用來建置、測試和部署 OpenShift 運算子的命令。

如何開始使用 ROSA



以下摘要說明 的入門程序 ROSA。如需詳細入門說明，請參閱 開始使用 ROSA 。

AWS Management Console/AWS CLI

1. 設定 AWS 服務 ROSA 的許可，以交付服務功能。如需詳細資訊，請參閱the section called “先決條件”。
2. 安裝和設定最新的 AWS CLI 工具。如需詳細資訊，請參閱 AWS CLI 《 使用者指南》中的安裝我們更新最新版本的 AWS CLI。
3. 在 ROSA 主控台 ROSA 中啟用 。

Red Hat 混合雲端主控台/ROSA CLI

1. 從 Red Hat ROSA 混合雲端主控台下載最新版本的 CLI 和 OpenShift CLI。 https://console.redhat.com/openshift如需詳細資訊，請參閱 Red Hat 文件中的 ROSA CLI 入門。
2. 在 Red Hat 混合雲端主控台或使用 CLI ROSA 建立 ROSA 叢集。
3. 當您的叢集準備就緒時，請設定身分提供者以授予使用者對叢集的存取權。
4. 在 ROSA 叢集上部署和管理工作負載的方式與使用任何其他 OpenShift 環境的方式相同。

定價

的總成本 ROSA 包含兩個元件： ROSA 服務費用和 AWS 基礎設施費用。如需定價的詳細資訊，請參閱Red Hat OpenShift Service on AWS 定價。

ROSA 服務費用

根據預設， ROSA 工作者節點使用之每 4 個 vCPU 按小時費率隨需產生服務費用。所有支援 AWS 的標準區域中的服務費用都是一致的。除了工作者節點服務費用之外，具有託管控制平面 (HCP) 叢集的 ROSA 會產生每小時叢集費用。

ROSA 提供 1 年和 3 年服務費合約，您可以購買該合約，以節省工作者節點的隨需服務費用。如需詳細資訊，請參閱the section called “購買 ROSA 合約”。

AWS 基礎設施費用

AWS 基礎設施費用適用於託管於 AWS 全球基礎設施的基礎工作者節點、基礎設施節點、控制平面節點、儲存體和網路資源。 AWS 基礎設施費用因而異 AWS 區域。

的責任概觀 ROSA

本文件概述 Amazon Web Services (AWS) 受管服務的 Red Hat OpenShift Service on AWS (ROSA)、Red Hat 和 客戶的責任。如需 ROSA 及其元件的詳細資訊，請參閱 Red Hat 文件中的政策和服務定義。

AWS 共同責任模型定義了保護執行 中所有服務的基礎設施 AWS 的責任 AWS 雲端，包括執行 AWS 雲端 服務的 AWS 硬體、軟體、聯網和設施 ROSA。此 AWS 責任通常稱為「雲端安全性」。若要以全受管服務 ROSA 的形式運作，Red Hat 和客戶需負責 AWS 責任模型定義為「雲端安全性」的服務元素。

Red Hat 負責 ROSA 叢集基礎設施、基礎應用程式平台和作業系統的持續管理和安全性。當 ROSA 叢集託管在客戶 AWS 的資源上時 AWS 帳戶，服務 ROSA 元件和 Red Hat 網站可靠性工程師 (SREs) 會透過客戶建立 IAM 的角色從遠端存取叢集。Red Hat 使用此存取權來管理叢集上所有控制平面和基礎設施節點的部署和容量，並維護控制平面節點、基礎設施節點和工作者節點的版本。

Red Hat 和客戶共同負責 ROSA 網路管理、叢集記錄、叢集版本控制和容量管理。雖然 Red Hat 會管理 ROSA 服務，但客戶必須全權負責管理和保護部署到的任何應用程式、工作負載和資料 ROSA。

概觀

下表提供 AWS、 Red Hat 和 客戶責任的概觀 Red Hat OpenShift Service on AWS。

> **Note**
>
> 如果`cluster-admin`角色已新增至使用者，請參閱 Red Hat Enterprise Agreement 附錄 4（線上訂閱服務）中的責任和排除備註。

Resource	事件和操作管理	變更管理	存取和身分授權	安全與法規合規	災難復原
客戶資料	客戶	客戶	客戶	客戶	客戶
客戶應用程式	客戶	客戶	客戶	客戶	客戶
開發人員服務	客戶	客戶	客戶	客戶	客戶
平台監控	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
日誌	Red Hat	Red Hat 和客戶	Red Hat 和客戶	Red Hat 和客戶	Red Hat
應用程式聯網	Red Hat 和客戶	Red Hat 和客戶	Red Hat 和客戶	Red Hat	Red Hat
叢集聯網	Red Hat	Red Hat 和客戶	Red Hat 和客戶	Red Hat	Red Hat
虛擬網路管理	Red Hat 和客戶	Red Hat 和客戶	Red Hat 和客戶	Red Hat 和客戶	Red Hat 和客戶
虛擬運算管理（控制平面、基礎設施和工作者節點）	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat

Resource	事件和操作管理	變更管理	存取和身分授權	安全與法規合規	災難復原
叢集版本	Red Hat	Red Hat 和客戶	Red Hat	Red Hat	Red Hat
容量管理	Red Hat	Red Hat 和客戶	Red Hat	Red Hat	Red Hat
虛擬儲存管理	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS 軟體（公有 AWS 服務)	AWS	AWS	AWS	AWS	AWS
硬體/AWS 全球基礎設施	AWS	AWS	AWS	AWS	AWS

按區域劃分的共同責任任務

AWS、Red Hat 和客戶共同負責監控和維護 ROSA 元件。本文件依區域和任務定義 ROSA 服務責任。

事件和操作管理

AWS 負責保護執行 中提供之所有服務的硬體基礎設施 AWS 雲端。Red Hat 負責管理預設平台聯網所需的服務元件。客戶負責客戶應用程式資料和客戶可能設定的任何自訂聯網的事件和操作管理。

Resource	服務責任	客戶責任
應用程式聯網	Red Hat • 監控原生 OpenShift 路由器服務，並回應提醒。	客戶 • 監控應用程式路由的運作狀態，以及其背後的端點。 • 向 AWS 和 Red Hat 報告中斷。
虛擬聯網管理	Red Hat	客戶

Resource	服務責任	客戶責任
	• 監控預設平台聯網所需的 AWS 負載平衡器、 Amazon VPC 子網路和 AWS 服務 元件。回應提醒。	• 監控 AWS 負載平衡器端點的運作狀態。 • 監控可選擇透過 Amazon VPC至 VPC 連線、 AWS VPN 連線或 AWS Direct Connect 潛在問題或安全威脅設定的網路流量。
虛擬儲存管理	Red Hat • 監控用於叢集節點的 Amazon EBS 磁碟區，以及用於 ROSA 服務內建容器映像登錄檔的 Amazon S3 儲存貯體。回應提醒。	客戶 • 監控應用程式資料的運作狀態。 • 如果 AWS KMS keys 使用客戶受管，請建立和控制金鑰生命週期和金鑰政策以進行 Amazon EBS 加密。
AWS 軟體 （公有 AWS 服務)	AWS • 如需有關 AWS 事件和操作管理的資訊，請參閱 AWS 白皮書中的如何 AWS 維持操作彈性和服務持續性。	客戶 • 監控客戶帳戶中 AWS 資源的運作狀態。 • 使用 IAM 工具將適當的許可套用至客戶帳戶中 AWS 的資源。
硬體/AWS 全球基礎設施	AWS • 如需 AWS 事件和操作管理的相關資訊，請參閱 AWS 白皮書中的如何 AWS 維護操作彈性和服務持續性。	客戶 • 設定、管理和監控客戶應用程式和資料，以確保應用程式和資料安全控制得到適當的強制執行。

變更管理

AWS 負責保護執行 中提供之所有服務的硬體基礎設施 AWS 雲端。Red Hat 負責啟用客戶將控制的叢集基礎設施和服務的變更，以及維護控制平面節點、基礎設施節點和工作者節點的版本。客戶負責啟動

基礎設施變更。客戶也負責安裝和維護選用服務、叢集上的聯網組態，以及客戶資料和應用程式的變更。

Resource	服務責任	客戶責任
日誌	Red Hat • 集中彙總和監控平台稽核日誌。 • 提供和維護記錄運算子，讓客戶能夠部署記錄堆疊以進行預設應用程式記錄。 • 應客戶要求提供稽核日誌。	客戶 • 在叢集上安裝選用的預設應用程式記錄運算子。 • 安裝、設定和維護任何選用的應用程式記錄解決方案，例如記錄附屬容器或第三方記錄應用程式。 • 如果應用程式影響記錄堆疊或叢集的穩定性，請調校客戶應用程式產生之應用程式日誌的大小和頻率。 • 透過支援案例請求平台稽核日誌，以研究特定事件。
應用程式聯網	Red Hat • 設定公有負載平衡器。提供設定私有負載平衡器和最多一個額外負載平衡器的能力。 • 設定原生 OpenShift 路由器服務。提供將路由器設定為私有，並新增最多一個額外的路由器碎片的功能。 • 為預設的內部 Pod 流量安裝、設定和維護 OpenShift SDN 元件。 • 讓客戶能夠管理和 `NetworkPolicy` `EgressNet`	客戶 • 使用 `NetworkPolicy` 物件設定專案和 Pod 網路、Pod 輸入和 Pod 輸出的非預設 Pod 網路許可。 • 使用 OpenShift Cluster Manager 請求預設應用程式路由的私有負載平衡器。 • 使用 OpenShift Cluster Manager 設定最多一個額外的公有或私有路由器碎片和對應的負載平衡器。 • 請求和設定特定 服務的任何其他服務負載平衡器。

Resource	服務責任	客戶責任
	`workPolicy` （防火牆）物件。	• 設定任何必要的 DNS 轉送規則。
叢集聯網	Red Hat • 設定叢集管理元件，例如公有或私有服務端點，以及與 Amazon VPC元件的必要整合。 • 設定工作者、基礎設施和控制平面節點之間內部叢集通訊所需的內部網路元件。	客戶 • 佈建叢集時，視需要透過 OpenShift Cluster Manager 提供機器 CIDR、服務 CIDR 和 Pod CIDR 的選用非預設 IP 地址範圍。 • 請求 API 服務端點在叢集建立時或透過 OpenShift Cluster Manager 建立叢集之後成為公有或私有。
虛擬網路管理	Red Hat • 設定佈建叢集所需的 Amazon VPC 元件，例如子網路、負載平衡器、網際網路閘道和 NAT 閘道。 • 讓客戶能夠透過 OpenShift Cluster Manager 管理與內部部署資源、 Amazon VPC 對 VPC AWS VPN 連線的連線能力，以及 AWS Direct Connect 視需要進行管理。 • 讓客戶能夠建立和部署 AWS 負載平衡器，以便與服務負載平衡器搭配使用。	客戶 • 設定和維護選用 Amazon VPC 元件，例如 Amazon VPC至 VPC 的連線、 AWS VPN 連線或 AWS Direct Connect。 • 請求和設定特定 服務的任何其他負載平衡器。

Resource	服務責任	客戶責任
虛擬運算管理	Red Hat • 設定控制 ROSA 平面和資料平面，以使用 Amazon EC2 執行個體進行叢集運算。 • 監控和管理叢集上 Amazon EC2 控制平面和基礎設施節點的部署。	客戶 • 使用 OpenShift Cluster Manager ROSA 或 CLI 建立機器集區來監控和管理 Amazon EC2 工作者節點。 • 管理客戶部署的應用程式和應用程式資料的變更。
叢集版本	Red Hat • 啟用升級排程程序。 • 監控升級進度，並修正遇到的任何問題。 • 發佈次要和維護升級的變更日誌和版本備註。	客戶 • 排程維護版本立即升級，以供未來使用，或進行自動升級。 • 確認並排程次要版本升級。 • 確保叢集版本保持在支援的次要版本上。 • 在次要和維護版本上測試客戶應用程式，以確保相容性。
容量管理	Red Hat • 監控控制平面的使用。控制平面包括控制平面節點和基礎設施節點。 • 擴展和調整控制平面節點的大小，以維持服務品質。	客戶 • 監控工作者節點使用率，並在適當時啟用自動擴展功能。 • 判斷叢集的擴展策略。 • 使用提供的 OpenShift Cluster Manager 控制項，視需要新增或移除其他工作者節點。 • 回應有關叢集資源需求的 Red Hat 通知。

Resource	服務責任	客戶責任
虛擬儲存管理	Red Hat • 設定和設定 Amazon EBS 來佈建叢集的本機節點儲存體和持久性磁碟區儲存體。 • 設定並設定內建映像登錄檔以使用儲存 Amazon S3 貯體儲存。 • 在 中定期刪除映像登錄資源 Amazon S3 ，以最佳化 Amazon S3 用量和叢集效能。	客戶 • 選擇性地設定 Amazon EBS CSI 驅動程式或 Amazon EFS CSI 驅動程式，以在叢集上佈建持久性磁碟區。

Resource	服務責任	客戶責任

AWS 軟體（公有 AWS 服務）	AWS
	
	運算
	
	• 提供服務 Amazon EC2 ，用於 ROSA 控制平面、基礎設施和工作者節點。
	
	儲存
	
	• Amazon EBS 提供 以允許 ROSA 服務為叢集佈建本機節點儲存體和持久性磁碟區儲存體。
	
	聯網
	
	• 提供下列 AWS 雲端 服務以滿足 ROSA 虛擬聯網基礎設施需求：
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• 為 提供下列選用 AWS 服務整合 ROSA：
	  • AWS VPN
	  • AWS Direct Connect
	  • AWS PrivateLink
	  • AWS Transit Gateway
		客戶
		
		• 使用與 IAM 委託人或 AWS STS 臨時安全登入資料相關聯的存取金鑰 ID 和私密存取金鑰來簽署請求。
		• 為叢集指定要在叢集建立期間使用的 VPC 子網路。
		• 選擇性地設定客戶管理的 VPC 以搭配 ROSA 叢集使用。

Resource	服務責任	客戶責任
硬體/AWS 全球基礎設施	AWS • 如需 AWS 資料中心管理控制的相關資訊，請參閱 AWS 雲端 安全頁面上的我們的控制。 • 如需有關變更管理最佳實務的資訊，請參閱 AWS 解決方案程式庫中的變更管理指南 AWS。	客戶 • 針對託管在 上的客戶應用程式和資料實作變更管理最佳實務 AWS 雲端。

存取和身分授權

存取和身分授權包括管理授權存取叢集、應用程式和基礎設施資源的責任。這包括提供存取控制機制、身分驗證、授權和管理資源存取等任務。

Resource	服務責任	客戶責任
日誌	Red Hat • 遵守適用於平台稽核日誌的產業標準型分層內部存取程序。 • 提供原生 OpenShift RBAC 功能。	客戶 • 設定 OpenShift RBAC 來控制對專案的存取，以及延伸專案的應用程式日誌。 • 對於第三方或自訂應用程式記錄解決方案，客戶負責存取管理。
應用程式聯網	Red Hat • 提供原生 OpenShift RBAC 和`dedicated-admin` 功能。	客戶 • 設定 OpenShift `dedicated-admin` 和 RBAC 以控制視需要路由組態的存取。 • 管理 Red Hat 的 Red Hat 組織管理員，以授予 OpenShift Cluster Manager

Resource	服務責任	客戶責任
		的存取權。叢集管理員用於設定路由器選項，並提供服務負載平衡器配額。
叢集聯網	Red Hat • 透過 OpenShift Cluster Manager 提供客戶存取控制。提供原生 OpenShift RBAC 和`dedicated-admin`功能。	客戶 • 設定 OpenShift `dedicated-admin` 和 RBAC 以控制視需要路由組態的存取。 • 管理 Red Hat 帳戶的 Red Hat 組織成員資格。 • 管理 Red Hat 的組織管理員，以授予 OpenShift Cluster Manager 的存取權。
虛擬網路管理	Red Hat • 透過 OpenShift Cluster Manager 提供客戶存取控制。	客戶 • 透過 OpenShift Cluster Manager 管理選用使用者對 AWS 元件的存取。
虛擬運算管理	Red Hat • 透過 OpenShift Cluster Manager 提供客戶存取控制。	客戶 • 透過 OpenShift Cluster Manager 管理選用使用者對 AWS 元件的存取。 • 建立啟用 ROSA 服務存取所需的 IAM 角色和連接政策。
虛擬儲存管理	Red Hat • 透過 OpenShift Cluster Manager 提供客戶存取控制。	客戶 • 透過 OpenShift Cluster Manager 管理選用使用者對 AWS 元件的存取。 • 建立啟用 ROSA 服務存取所需的 IAM 角色和連接政策。

Resource	服務責任	客戶責任
AWS 軟體（公有 AWS 服務）	AWS 運算 • 提供服務 Amazon EC2 ，用於 ROSA 控制平面、基礎設施和工作者節點。 儲存 • 提供 Amazon EBS，用於允許 為叢集 ROSA 佈建本機節點儲存體和持久性磁碟區儲存體。 • 提供 Amazon S3，用於服務的內建映像登錄檔。 聯網 • Provide AWS Identity and Access Management (IAM)，供客戶用來控制對客戶帳戶上執行 ROSA 之資源的存取。	客戶 • 建立啟用 ROSA 服務存取所需的 IAM 角色和連接政策。 • 使用 IAM 工具將適當的許可套用至客戶帳戶中 AWS 的資源。 • 若要 ROSA 在整個 AWS 組織中啟用 ，客戶需負責管理 AWS Organizations 管理員。 • 若要 ROSA 在您的 AWS 組織中啟用 ，客戶需負責使用 來分配 ROSA 授予權利 AWS License Manager。
硬體/AWS 全球基礎設施	AWS • 如需 AWS 資料中心實體存取控制的相關資訊，請參閱 AWS 雲端 安全頁面上的「我們的控制項」。	客戶 • 客戶不負責 AWS 全球基礎設施。

安全與法規合規

以下是與合規相關的責任和控制：

Resource	服務責任	客戶責任
日誌	Red Hat • 將叢集稽核日誌傳送至 Red Hat SIEM 以分析安全事件。將稽核日誌保留一段時間，以支援鑑識分析。	客戶 • 分析安全事件的應用程式日誌。 • 如果需要比預設記錄堆疊提供的保留時間更長，請透過記錄附屬容器或第三方記錄應用程式，將應用程式日誌傳送至外部端點。
虛擬聯網管理	Red Hat • 監控虛擬網路元件是否有潛在問題和安全威脅。 • 使用公有 AWS 工具進行額外的監控和保護。	客戶 • 監控選用設定的虛擬網路元件是否有潛在問題和安全威脅。 • 視需要設定任何必要的防火牆規則或客戶資料中心保護。
虛擬運算管理	Red Hat • 監控虛擬運算元件是否有潛在問題和安全威脅。 • 使用公有 AWS 工具進行額外的監控和保護。	客戶 • 監控選用設定的虛擬網路元件是否有潛在問題和安全威脅。 • 視需要設定任何必要的防火牆規則或客戶資料中心保護。
虛擬儲存管理	Red Hat • 監控虛擬儲存元件是否有潛在問題和安全威脅。 • 使用公有 AWS 工具進行額外的監控和保護。	客戶 • 佈建磁碟 Amazon EBS 區。 • 管理 Amazon EBS 磁碟區儲存，以確保有足夠的儲存體可供掛載為磁碟區 ROSA。

Resource	服務責任	客戶責任
	• 根據預設，使用 Amazon EBS 提供的 AWS 受管 KMS 金鑰，設定 ROSA 服務來加密控制平面、基礎設施和工作者節點磁碟區資料。 • 設定 ROSA 服務，以加密使用預設儲存體方案的客戶持久性磁碟區，以及 Amazon EBS 提供的 AWS 受管 KMS 金鑰。 • 讓客戶能夠使用受管客戶 KMS key 來加密持久性磁碟區。 • 設定容器映像登錄檔，使用伺服器端加密搭配 Amazon S3 受管金鑰 (SSE-3) 加密靜態映像登錄檔資料。 • 讓客戶能夠建立公有或私有 Amazon S3 映像登錄檔，以保護其容器映像免於未經授權的使用者存取。	• 建立持久性磁碟區宣告，並透過 OpenShift Cluster Manager 產生持久性磁碟區。

Resource	服務責任	客戶責任
AWS 軟體（公有 AWS 服務）	AWS 運算 • 提供 Amazon EC2、用於 ROSA 控制平面、基礎設施和工作者節點。如需詳細資訊，請參閱 Amazon EC2《使用者指南》中的基礎設施安全 Amazon EC2。 儲存 • 提供 Amazon EBS、用於 ROSA 控制平面、基礎設施和工作者節點磁碟區，以及 Kubernetes 持久性磁碟區。如需詳細資訊，請參閱 Amazon EC2《使用者指南》中的資料保護 Amazon EC2。 • 提供 AWS KMS，其 ROSA 使用 來加密控制平面、基礎設施和工作者節點磁碟區和持久性磁碟區。如需詳細資訊，請參閱 Amazon EC2《使用者指南》中的Amazon EBS 加密。 • 提供 Amazon S3，用於 ROSA 服務的內建容器映像登錄檔。如需詳細資訊，請參閱 Amazon S3《使用者指南》中的Amazon S3 安全性。	客戶 • 確保遵循安全最佳實務和最低權限原則，以保護 Amazon EC2 執行個體上的資料。如需詳細資訊，請參閱 中的基礎設施安全性 Amazon EC2和 中的資料保護 Amazon EC2。 • 監控選用設定的虛擬網路元件是否有潛在問題和安全威脅。 • 視需要設定任何必要的防火牆規則或客戶資料中心保護。 • 建立選用的客戶受管 KMS 金鑰，並使用 KMS 金鑰加密 Amazon EBS 持久性磁碟區。 • 監控虛擬儲存體中的客戶資料是否有潛在問題和安全威脅。如需詳細資訊，請參閱 AWS 共同責任模型。

Resource	服務責任	客戶責任
	聯網 • 提供安全功能和服務，以提高 AWS 全球基礎設施的隱私權和控制網路存取，包括內建的網路防火牆 Amazon VPC、私有或專用網路連線，以及 AWS 安全設施之間 AWS 全球和區域網路上所有流量的自動加密。如需詳細資訊，請參閱安全簡介白皮書中的AWS 共同責任模型和基礎設施 AWS 安全。	
硬體/AWS 全球基礎設施	AWS • 提供 ROSA 用於交付服務功能的 AWS 全域基礎設施。如需 AWS 安全控制的詳細資訊，請參閱 AWS 白皮書中的AWS 基礎設施安全。 • 提供文件給客戶，以 AWS 使用 AWS Artifact 和 AWS Security Hub 等工具來管理合規需求並檢查其在 中的安全狀態。	客戶 • 設定、管理和監控客戶應用程式和資料，以確保應用程式和資料安全控制得到適當的強制執行。 • 使用 IAM 工具將適當的許可套用至客戶帳戶中 AWS 的資源。

災難復原

災難復原包括資料和組態備份、災難復原環境的資料複寫和組態，以及災難事件的容錯移轉。

Resource	服務責任	客戶責任
虛擬網路管理	Red Hat	客戶

Resource	服務責任	客戶責任
	• 還原或重新建立平台運作所需的受影響虛擬網路元件。	• 盡可能使用多個通道設定虛擬網路連線，以防止中斷。 • 如果使用具有多個叢集的全域負載平衡器，請維護容錯移轉 DNS 和負載平衡。
虛擬運算管理	Red Hat • 監控叢集並取代失敗的 Amazon EC2 控制平面或基礎設施節點。 • 讓客戶能夠手動或自動取代失敗的工作者節點。	客戶 • 透過 OpenShift Cluster Manager 或 ROSA CLI 編輯機器集區組態來取代失敗的 Amazon EC2 工作者節點。
虛擬儲存管理	Red Hat • 對於使用 AWS IAM 使用者登入資料建立的 ROSA 叢集，請透過每小時、每日和每週磁碟區快照來備份叢集上的所有 Kubernetes 物件。	客戶 • 備份客戶應用程式和應用程式資料。

Resource	服務責任	客戶責任
AWS 軟體（公有 AWS 服務）	AWS 運算 • 提供支援資料彈性 Amazon EC2 的功能，例如 Amazon EBS 快照和 Amazon EC2 Auto Scaling。如需詳細資訊，請參閱 Amazon EC2 《使用者指南》中的復原功能 Amazon EC2。 儲存 • 提供 ROSA 服務和客戶透過 Amazon EBS 磁碟區快照備份叢集上的 Amazon EBS 磁碟區的能力。 • 如需支援資料彈性 Amazon S3 的功能相關資訊，請參閱中的彈性 Amazon S3。 聯網 • 如需支援資料復原 Amazon VPC 功能的詳細資訊，請參閱 Amazon VPC 《使用者指南》中的復原功能 Amazon Virtual Private Cloud。	客戶 • 設定 ROSA 多可用區域叢集以改善容錯能力和叢集可用性。 • 使用 Amazon EBS CSI 驅動程式佈建持久性磁碟區以啟用磁碟區快照。 • 建立 Amazon EBS 持久性磁碟區的 CSI 磁碟區快照。

Resource	服務責任	客戶責任
硬體/AWS 全球基礎設施	AWS • 提供 AWS 全域基礎設施，允許 ROSA 跨可用區域擴展控制平面、基礎設施和工作者節點。此功能 ROSA 可讓協調區域之間的自動容錯移轉，而不會中斷。 • 如需災難復原最佳實務的詳細資訊，請參閱 AWS Well-Architected Framework 中的雲端災難復原選項。	客戶 • 設定 ROSA 多可用區域叢集以改善容錯能力和叢集可用性。

資料和應用程式的客戶責任

客戶必須對其部署的應用程式、工作負載和資料負責 Red Hat OpenShift Service on AWS。不過，AWS Red Hat 提供各種工具，協助客戶管理平台上的資料和應用程式。

Resource	AWS 和 Red Hat 如何提供協助	客戶責任
客戶資料	Red Hat • 維護 平台層級的資料加密標準，如產業安全和合規標準所定義。 • 提供 OpenShift 元件以協助管理應用程式資料，例如秘密。 • 啟用與資料服務的整合 Amazon RDS ，例如將資料存放和管理在叢集和/或外部 AWS。	客戶 • 對存放在 平台上的所有客戶資料，以及客戶應用程式如何使用和公開此資料，保持責任。

Resource	AWS 和 Red Hat 如何提供協助	客戶責任
	AWS • 提供 Amazon RDS 以允許客戶在叢集外部存放和管理資料。	

Resource	AWS 和 Red Hat 如何提供協助	客戶責任
客戶應用程式	Red Hat • 佈建已安裝 OpenShift 元件的叢集，讓客戶可存取 OpenShift 和 Kubernetes APIs 來部署和管理容器化應用程式。 • 建立具有映像的叢集會提取秘密，以便客戶部署可以從 Red Hat Container Catalog 登錄檔提取映像。 • 提供 OpenShift APIs的存取權，客戶可以用它來設定運算子，將社群 AWS、第三方和 Red Hat 服務新增至叢集。 • 提供儲存類別和外掛程式，以支援持久性磁碟區，以便與客戶應用程式搭配使用。 • 提供容器映像登錄檔，讓客戶可以在叢集上安全地存放應用程式容器映像，以部署和管理應用程式。 AWS • 提供 Amazon EBS 以支援持久性磁碟區，以搭配客戶應用程式使用。 • 提供 Amazon S3 以支援容器映像登錄檔的 Red Hat 佈建。	客戶 • 對客戶和第三方應用程式、資料和完整的應用程式生命週期負責。 • 如果客戶使用運算子或外部映像將 Red Hat、社群、第三方、自己的或其他服務新增至叢集，則客戶需負責這些服務，並與適當的提供者（包括 Red Hat) 合作，以排除任何問題。 • 使用提供的工具和功能來設定和部署；保持最新狀態；設定資源請求和限制；將叢集大小調整為具有足夠的資源來執行應用程式；設定許可；與其他 服務整合；管理客戶部署的任何映像串流或範本；外部服務；儲存、備份和還原資料；以及以其他方式管理其高可用性和彈性工作負載。 • 維護監控應用程式執行的責任 Red Hat OpenShift Service on AWS，包括安裝和操作軟體以收集指標、建立提醒，以及保護應用程式中的秘密。

ROSA 架構

Red Hat OpenShift Service on AWS (ROSA) 具有下列叢集拓撲：

- 託管控制平面 (HCP) - 控制平面託管在 Red Hat 的 內 AWS 帳戶 ，並由 Red Hat 管理。工作者節點會部署在客戶的 中 AWS 帳戶。
- 傳統 – 控制平面和工作者節點會部署在客戶的 中 AWS 帳戶。

與 HCP 合作的 ROSA 提供更有效率的控制平面架構，有助於降低執行時產生的 AWS 基礎設施費用， ROSA 並縮短叢集建立時間。您可以在 ROSA 主控台中 AWS 啟用具有 HCP 的 ROSA 和 ROSA classic。當您使用 CLI ROSA 佈建 ROSA 叢集時，您可以選擇要使用的架構。

> **Note**
> 具有託管控制平面 (HCP) 的 ROSA 不提供 FedRAMP High 和 HIPAA 合格合規認證。如需詳細資訊，請參閱 Red Hat 文件中的合規。

> **Note**
> 具有託管控制平面 (HCP) 的 ROSA 不提供聯邦資訊處理標準 (FIPS) 端點。

比較 ROSA 與 HCP 和 ROSA classic

下表比較 ROSA 與 HCP 和 ROSA 傳統架構模型。

	與 HCP 合作的 ROSA	ROSA 傳統
叢集基礎設施託管	控制平面元件，例如 etcd、API 伺服器和 oauth，託管在 Red Hat 擁有的 中 AWS 帳戶。	控制平面元件，例如 etcd、API 伺服器和 oauth，託管在客戶擁有的 中 AWS 帳戶。
Amazon VPC	工作者節點會透過 與控制平面通訊AWS PrivateLink。	工作者節點和控制平面節點部署在客戶的 VPC 中。

	與 HCP 合作的 ROSA	ROSA 傳統
AWS Identity and Access Management	使用 AWS 受管政策。	使用 服務定義的客戶受管政策。
多區域部署	控制平面部署在多個可用區域 (AZs) 之間。	控制平面可以部署在單一可用區域或多個可用AZs。
基礎設施節點	不使用專用基礎設施節點。平台元件會部署到工作者節點。	使用兩個單一可用區或三個多可用區專用節點來託管平台元件。
OpenShift 功能	平台監控、映像登錄檔和輸入控制器會部署在工作者節點中。	平台監控、映像登錄檔和輸入控制器部署在專用基礎設施節點中。
叢集升級	控制平面和每個機器集區都可以個別升級。	整個叢集必須同時升級。
最小 Amazon EC2 佔用空間	建立叢集需要兩個 Amazon EC2 執行個體。	建立叢集需要七個單一可用區或九個多可用區 Amazon EC2 執行個體。
AWS 區域	如需 AWS 區域 可用性，請參閱 AWS 一般參考指南中的Red Hat OpenShift Service on AWS 端點和配額。	如需 AWS 區域 可用性，請參閱 AWS 一般參考指南中的Red Hat OpenShift Service on AWS 端點和配額。

開始使用 ROSA

Red Hat OpenShift Service on AWS (ROSA) 是一種受管服務，您可以使用 Red Hat OpenShift 企業 Kubernetes 平台來建置、擴展和部署容器化應用程式 AWS。

您可以使用下列指南來建立第一個 ROSA 叢集、授予使用者存取權、部署第一個應用程式，以及了解如何撤銷使用者存取權和刪除叢集。

- the section called “建立 ROSA HCP 叢集 - CLI” - 使用 AWS STS 和 CLI 使用 HCP ROSA 叢集建立您的第一個 ROSA。
- the section called “建立 ROSA 傳統叢集 - AWS PrivateLink ” - 使用 建立您的第一個 ROSA 傳統叢集 AWS PrivateLink。
- the section called “建立 ROSA 傳統叢集 - CLI” - 使用 AWS STS 和 CLI ROSA 建立您的第一個 ROSA 傳統叢集。

設定 以使用 ROSA

若要準備您的環境以建立 ROSA 叢集，您需要完成下列動作。

先決條件

必須符合下列先決條件才能啟用 ROSA 叢集建立。

- 安裝和設定最新的 AWS CLI。如需詳細資訊，請參閱安裝或更新最新版本的 AWS CLI。
- 安裝和設定最新的 ROSA CLI 和 OpenShift 容器平台 CLI。如需詳細資訊，請參閱 CLI ROSA 入門。
- 您必須為 設定必要的服務配額 Amazon EC2 Amazon VPC Amazon EBS，且 Elastic Load Balancing AWS Red Hat 可以視需要代表您請求增加服務配額，以解決問題。若要檢視 所需的服務配額 ROSA，請參閱 AWS 一般參考中的Red Hat OpenShift Service on AWS 端點和配額。
- 若要取得 的 AWS 支援 ROSA，您必須啟用 AWS Business、Enterprise On-Ramp 或 Enterprise Support 計劃。Red Hat 可能會視需要代表您請求 AWS 支援以解決問題。如需詳細資訊，請參閱the section called “取得支援”。若要啟用 支援，請參閱 支援 頁面。
- 如果您使用 AWS Organizations 來管理 AWS 帳戶 託管 ROSA 服務的 ，則必須設定組織的服務控制政策 (SCP)，以允許 Red Hat 執行 SCP 中列出的政策動作，不受限制。如需詳細資訊，請參閱 the section called “AWS Organizations 服務控制政策拒絕必要的 AWS Marketplace 許可”。如需 SCPs的詳細資訊，請參閱服務控制政策 SCPs)。

- 如果將 叢集 ROSA 與 部署 AWS STS 到預設停用 AWS 區域 的 ，您必須 AWS 帳戶 使用下列命令，將 中所有區域的安全字符更新至版本 2。

```
aws iam set-security-token-service-preferences --global-endpoint-token-version
 v2Token
```

如需啟用區域的詳細資訊，請參閱 link：accounts/latest/reference/manage

啟用 ROSA 和設定 AWS 先決條件

若要建立 ROSA 叢集，您必須在 ROSA 主控台中 AWS 啟用 ROSA 服務。 AWS ROSA 主控台會驗證您的 是否 AWS 帳戶 具有必要的 AWS Marketplace 許可、服務配額，以及名為 的 Elastic Load Balancing (ELB) 服務連結角色`AWSServiceRoleForElasticLoadBalancing`。如果缺少任何這些先決條件，主控台會提供如何設定您的帳戶以符合先決條件的指導。

1. 導覽至 ROSA 主控台。
2. 選擇開始使用。
3. 在驗證 ROSA 先決條件頁面上，選取我同意與 Red Hat 共用我的聯絡資訊。
4. 選擇啟用 ROSA 。
5. 一旦頁面驗證您的服務配額符合 ROSA 先決條件並建立 ELB 服務連結角色，請開啟新的終端機工作階段， 叢集 以使用 CLI ROSA 建立您的第一個 ROSA 。

使用 CLI 建立具有 HCP ROSA 叢集的 ROSA

下列各節說明如何使用 AWS STS 和 CLI 來開始使用 ROSA 搭配託管控制平面 ROSA (ROSA 搭配 HCP)。如需使用 Terraform 建立含 HCP 叢集的 ROSA 的步驟，請參閱 Red Hat 文件。若要進一步了解建立 ROSA 叢集的 Terraform 提供者，請參閱 Terraform 文件。

ROSA CLI 使用 `auto` 模式或 `manual` 模式來建立建立 所需的 IAM ROSA 資源和 OpenID Connect (OIDC) 組態 叢集。 `auto` 模式會自動建立所需的 IAM 角色和政策和 OIDC 供應商。 `manual` 模式會輸出手動建立 IAM 資源所需的 AWS CLI 命令。透過使用 `manual` 模式，您可以在手動執行命令之前檢閱產生的 AWS CLI 命令。透過 `manual` 模式，您也可以將命令傳遞給組織中的另一個管理員或群組，讓他們可以建立資源。

本文件中的程序使用 ROSA CLI `auto` 模式，透過 HCP 建立 ROSA 所需的 IAM 資源和 OIDC 組態。如需更多開始使用的選項，請參閱 開始使用 ROSA 。

主題

- 先決條件
- 建立 Amazon VPC 架構
- 建立必要的 IAM 角色和 OpenID Connect 組態
- 使用 CLI 和 建立具有 HCP ROSA 叢集的 ROSA AWS STS
- 設定身分提供者並授予 叢集 存取權
- 授予使用者對 的存取權 叢集
- 設定cluster-admin許可
- 設定dedicated-admin許可
- 叢集 透過 Red Hat 混合雲端主控台存取
- 從 Developer Catalog 部署應用程式
- 從使用者撤銷cluster-admin許可
- 從使用者撤銷dedicated-admin許可
- 撤銷使用者對 的存取權 叢集
- 刪除叢集 AWS STS 和資源

先決條件

完成 中列出的先決條件動作the section called “設定”。

建立 Amazon VPC 架構

下列程序會建立可用於託管叢集的 Amazon VPC 架構。所有 叢集 資源都託管在私有子網路中。公有子網路會透過 NAT 閘道，將來自私有子網路的傳出流量路由至公有網際網路。此範例使用 `10.0.0.0/16` 的 CIDR 區塊 Amazon VPC。不過，您可以選擇不同的 CIDR 區塊。如需詳細資訊，請參閱調整 VPC 大小。

> **Important**
> 如果不符合 Amazon VPC 要求，叢集建立會失敗。

Example

Terraform

1. 安裝 Terraform CLI。如需詳細資訊，請參閱 Terraform 文件中的安裝說明。
2. 開啟終端機工作階段並複製 Terraform VPC 儲存庫。

```
git clone https://github.com/openshift-cs/terraform-vpc-example
```

3. 導覽至建立的目錄。

```
cd terraform-vpc-example
```

4. 啟動 Terraform 檔案。

```
terraform init
```

完成後，CLI 會傳回訊息，指出 Terraform 已成功初始化。

5. 若要根據現有範本建置 Terraform 計劃，請執行下列命令。 AWS 區域 必須指定 。或者，您可以選擇指定叢集名稱。

```
terraform plan -out rosa.tfplan -var region=<region>
```

命令執行後，就會將`rosa.tfplan`檔案新增至 `hypershift-tf` 目錄。如需更詳細的選項，請參閱 Terraform VPC 儲存庫的 README 檔案。

6. 套用計劃檔案來建置 VPC。

```
terraform apply rosa.tfplan
```

完成後，CLI 會傳回成功訊息，以驗證新增的資源。

a. （選用）為 Terraform 佈建的私有、公有和機器集區子網路 IDs 建立環境變數，以便在使用 HCP 叢集建立 ROSA 時使用。

```
export SUBNET_IDS=$(terraform output -raw cluster-subnets-string)
```

b. （選用）確認環境變數已正確設定。

```
echo $SUBNET_IDS
```

Amazon VPC console

1. 開啟 Amazon VPC 主控台。
2. 在 VPC 儀表板上，選擇 Create VPC (建立 VPC)。
3. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
4. 保持選取自動產生名稱標籤以建立 VPC 資源的「名稱」標籤，或將其清除以提供您自己的 VPC 資源「名稱」標籤。
5. 在IPv4 CIDR 區塊，輸入 VPC 的 IPv4 地址範圍。VPC 必須具有 IPv4 地址範圍。
6. （選用）若要支援 IPv6 流量，請選擇 IPv6 CIDR 區塊、Amazon 提供的 IPv6 CIDR 區塊。
7. 將租用保留為 `Default`。
8. 針對可用區域 (AZs) 的數量，選擇您需要的數目。對於異地同步備份部署， ROSA 需要三個可用區域。若要選擇子網路的 AZ，請展開自訂 AZ。

> **Note**
>
> 某些 ROSA 執行個體類型僅適用於特定可用區域。您可以使用 ROSA CLI 命令`rosa list instance-types`來列出所有可用的 ROSA 執行個體類型。若要檢查執行個體類型是否可用於指定的可用區域，請使用 AWS CLI 命令 `aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`。

9. 若要設定您的子網路，請選擇公有子網路數目和私有子網路數目的值。若要選擇子網路的 IP 地址範圍，請展開自訂子網路 CIDR 區塊。

> **Note**
>
> 與 HCP 合作的 ROSA 要求客戶為每個用於建立叢集的可用區域設定至少一個公有和私有子網路。

10. 若要透過 IPv4 授予私有子網路中公有網際網路的資源存取權，請針對 NAT 閘道選擇要在其中建立 NAT 閘道AZs 數量。在生產環境中，建議您在每個 AZ 中部署一個 NAT 閘道，並包含需要存取公有網際網路的資源。
11. （選用）如果您需要 Amazon S3 直接從 VPC 存取，請選擇 VPC 端點 S3 Gateway。
12. 保持選取預設 DNS 選項。 ROSA 需要 VPC 上的 DNS 主機名稱支援。

13展開其他標籤，選擇新增標籤，然後新增下列標籤鍵。 ROSA 會使用自動飛行前檢查來驗證是否使用這些標籤。

- 索引鍵：`kubernetes.io/role/elb`
- 索引鍵：`kubernetes.io/role/internal-elb`

14選擇建立 VPC。

AWS CLI

1. 使用 `10.0.0.0/16` CIDR 區塊建立 VPC。

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

上述命令會傳回 VPC ID。以下為範例輸出。

```
vpc-1234567890abcdef0
```

2. 將 VPC ID 存放在環境變數中。

```
export VPC_ID=vpc-1234567890abcdef0
```

3. 使用`VPC_ID`環境變數為 VPC 建立`Name`標籤。

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. 在 VPC 上啟用 DNS 主機名稱支援。

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. 在 VPC 中建立公有和私有子網路，指定應建立資源的可用區域。

> **Important**
>
> 與 HCP 合作的 ROSA 要求客戶為每個用於建立叢集的可用區域設定至少一個公有和私有子網路。對於異地同步備份部署，需要三個可用區域。如果不符合這些要求，叢集建立會失敗。

> **Note**
>
> 某些 ROSA 執行個體類型僅適用於特定可用區域。您可以使用 ROSA CLI 命令`rosa list instance-types`來列出所有可用的 ROSA 執行個體類型。若要檢查執行個體類型是否可用於指定的可用區域，請使用 AWS CLI 命令 `aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`。

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. 將公有和私有子網路 IDs存放在環境變數中。

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. 為您的 VPC 子網路建立下列標籤。 ROSA 會使用自動飛行前檢查來驗證是否使用這些標籤。

> **Note**
>
> 您必須至少標記一個私有子網路，如果適用，則必須標記一個公有子網路。

```
aws ec2 create-tags --resources $PUBLIC_SUB --tags Key=kubernetes.io/role/
elb,Value=1
aws ec2 create-tags --resources $PRIVATE_SUB --tags Key=kubernetes.io/role/
internal-elb,Value=1
```

8. 建立網際網路閘道和傳出流量的路由表。為私有流量建立路由表和彈性 IP 地址。

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

9. 將 IDs存放在環境變數中。

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

10將網際網路閘道連接至 VPC。

```
aws ec2 attach-internet-gateway \
    --vpc-id $VPC_ID \
    --internet-gateway-id $IGW
```

11將公有路由表與公有子網路建立關聯，並設定流量以路由至網際網路閘道。

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

12建立 NAT 閘道並將其與彈性 IP 地址建立關聯，以啟用私有子網路的流量。

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

13將私有路由表與私有子網路建立關聯，並設定流量以路由至 NAT 閘道。

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

14. (選用) 對於多可用區域部署，重複上述步驟，以設定具有公有和私有子網路的兩個其他可用區域。

建立必要的 IAM 角色和 OpenID Connect 組態

使用 HCP 叢集建立 ROSA 之前，您必須建立必要的 IAM 角色和政策，以及 OpenID Connect (OIDC) 組態。如需使用 HCP 的 ROSA IAM 角色和政策的詳細資訊，請參閱 the section called “ AWS 受管政策”。

此程序使用 `auto` ROSA CLI 模式自動建立使用 HCP 叢集建立 ROSA 所需的 OIDC 組態。

1. 建立必要的 IAM 帳戶角色和政策。`--force-policy-creation` 參數會更新任何現有的角色和政策。如果沒有角色和政策，命令會改為建立這些資源。

```
rosa create account-roles --force-policy-creation
```

> **Note**
>
> 如果您的離線存取字符已過期，CLI ROSA 會輸出錯誤訊息，指出您的授權字符需要更新。如需疑難排解的步驟，請參閱 the section called “對 CLI ROSA 過期的離線存取權杖進行故障診斷”。

2. 建立 OpenID Connect (OIDC) 組態，以啟用對叢集的使用者身分驗證。此組態已註冊為與 OpenShift Cluster Manager (OCM) 搭配使用。

```
rosa create oidc-config --mode=auto
```

3. 複製 CLI 輸出中提供的 OIDC ROSA 組態 ID。稍後需要提供 OIDC 組態 ID，才能使用 HCP 叢集建立 ROSA。
4. 若要驗證與使用者組織相關聯的叢集可用的 OIDC 組態，請執行下列命令。

```
rosa list oidc-config
```

5. 建立所需的 IAM 運算子角色，`<OIDC_CONFIG_ID>`以先前複製的 OIDC 組態 ID 取代 。

   Example

> **Important**
>
> 建立運算子角色`<PREFIX_NAME>`時，您必須在 中提供字首。否則會產生錯誤。

```
rosa create operator-roles --prefix <PREFIX_NAME> --oidc-config-id <OIDC_CONFIG_ID>
 --hosted-cp
```

6. 若要確認已建立 IAM 運算子角色，請執行下列命令：

```
rosa list operator-roles
```

使用 CLI 和 建立具有 HCP ROSA 叢集的 ROSA AWS STS

您可以使用 CLI 中提供的 叢集 AWS Security Token Service (AWS STS) 和 `auto` 模式，與 HCP ROSA 建立 ROSA。您可以選擇使用公有 API 和輸入或私有 API 和輸入建立叢集。

您可以使用 叢集 單一可用區域（單一可用區域）或多個可用區域（多可用區域）建立 。無論哪種情況，機器的 CIDR 值都必須符合您 VPC 的 CIDR 值。

下列程序使用 `rosa create cluster --hosted-cp`命令來建立具有 HCP 的單一可用區域 ROSA 叢集。若要建立異地同步備份 叢集，請在命令`multi-az`中指定 ，以及您要部署的每個私有子網路的私有子網路 IDs。

1. 使用下列其中一個命令建立具有 HCP 叢集的 ROSA。
   - 使用具有公有 API 和輸入之 HCP 叢集建立 ROSA，指定叢集名稱、運算子角色字首、OIDC 組態 ID，以及公有和私有子網路 IDs。

     ```
     rosa create cluster --cluster-name=<CLUSTER_NAME> --sts --mode=auto --hosted-cp --
     operator-roles-prefix <OPERATOR_ROLE_PREFIX> --oidc-config-id <OIDC_CONFIG_ID> --
     subnet-ids=<PUBLIC_SUBNET_ID>,<PRIVATE_SUBNET_ID>
     ```

   - 使用具有私有 API 和輸入之 HCP 叢集建立 ROSA，指定叢集名稱、運算子角色字首、OIDC 組態 ID 和私有子網路 IDs。

     ```
     rosa create cluster --private --cluster-name=<CLUSTER_NAME> --sts --mode=auto --
     hosted-cp --subnet-ids=<PRIVATE_SUBNET_ID>
     ```

2. 檢查 的狀態 叢集。

   ```
   rosa describe cluster -c <CLUSTER_NAME>
   ```

   > **Note**
   > 如果建立程序失敗，或 `State` 欄位在 10 分鐘後未變更為就緒狀態，請參閱 故障診斷。若要聯絡 支援 或 Red Hat 支援以取得協助，請參閱the section called “取得支援”。

3. 觀看 OpenShift 安裝程式日誌，追蹤 叢集 建立進度。

   ```
   rosa logs install -c <CLUSTER_NAME> --watch
   ```

設定身分提供者並授予 叢集 存取權

ROSA 包含內建的 OAuth 伺服器。 叢集 建立 之後，您必須設定 OAuth 以使用身分提供者。然後，您可以將使用者新增至您設定的身分提供者，以授予他們存取您的 的權限 叢集。您可以視需要授予這些使用者`cluster-admin`或`dedicated-admin`許可。

您可以為 ROSA 設定不同的身分提供者類型 叢集。支援的類型包括 GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect 和 HTPasswd 身分提供者。

> **Important**
>
> HTPasswd 身分提供者僅包含用於建立單一靜態管理員使用者。HTPasswd 不支援做為 的一般用途身分提供者 ROSA。

下列程序會將 GitHub 身分提供者設定為範例。如需如何設定每個支援身分提供者類型的指示，請參閱設定身分提供者 AWS STS。

1. 導覽至 github.com：// GitHub 帳戶。
2. 如果您沒有可用於您身分佈建的 GitHub 組織 叢集，請建立一個。如需詳細資訊，請參閱 GitHub 文件中的步驟。
3. 使用 CLI ROSA 的互動式模式，為您的叢集設定身分提供者。

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 遵循輸出中的組態提示，限制對 GitHub 組織成員的 叢集 存取。

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
```

```
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 在輸出中開啟 URL，<GITHUB_ORG_NAME>以 GitHub 組織的名稱取代 。
6. 在 GitHub 網頁上，選擇註冊應用程式，在您的 GitHub 組織中註冊新的 OAuth 應用程式。
7. 執行下列命令，使用 GitHub OAuth 頁面中的資訊填入剩餘的`rosa create idp`互動式提示。將<GITHUB_CLIENT_ID>和 <GITHUB_CLIENT_SECRET>取代為 GitHub OAuth 應用程式的登入資料。

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> 可能需要大約兩分鐘的時間，身分提供者組態才會變成作用中。如果您設定了`cluster-admin`使用者，您可以執行 `oc get pods -n openshift-authentication --watch` 以使用更新的組態來監看 OAuth Pod 重新部署。

8. 確認身分提供者已正確設定。

```
rosa list idps --cluster=<CLUSTER_NAME>
```

授予使用者對 的存取權 叢集

您可以將使用者新增至已設定的身分提供者， 叢集 以授予使用者對 的存取權。

下列程序會將使用者新增至設定為將身分佈建至叢集的 GitHub 組織。

1. 導覽至 github.com 並登入您的 GitHub 帳戶。
2. 邀請需要 叢集 存取 GitHub 組織的使用者。如需詳細資訊，請參閱 GitHub 文件中的邀請使用者加入您的組織。

設定cluster-admin許可

1. 執行下列命令來授予cluster-admin許可。將 <IDP_USER_NAME> 和 取代<CLUSTER_NAME>為您的使用者和叢集名稱。

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者已列為cluster-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

設定dedicated-admin許可

1. 使用以下命令授予dedicated-admin許可。執行下列命令，將 <IDP_USER_NAME>和 <CLUSTER_NAME>取代為您的使用者和 叢集 名稱。

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者已列為cluster-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

叢集 透過 Red Hat 混合雲端主控台存取

叢集 透過 Red Hat 混合雲端主控台登入您的 。

1. 叢集 使用下列命令取得 的主控台 URL。<CLUSTER_NAME> 將 取代為 的名稱 叢集。

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 導覽至輸出中的主控台 URL 並登入。

   在使用...登入對話方塊中，選擇身分提供者名稱，並完成提供者提出的任何授權請求。

從 Developer Catalog 部署應用程式

從 Red Hat 混合雲端主控台，您可以部署 Developer Catalog 測試應用程式，並使用路由公開。

1. 導覽至 Red Hat 混合雲端主控台，然後選擇您要部署應用程式的叢集。
2. 在叢集的頁面上，選擇開啟主控台。
3. 在管理員角度中，選擇首頁 > 專案 > 建立專案。
4. 輸入專案的名稱，並選擇性地新增顯示名稱和描述。
5. 選擇建立以建立專案。
6. 切換到開發人員觀點，然後選擇 +Add。請確定選取的專案是剛建立的專案。
7. 在 Developer Catalog 對話方塊中，選擇所有 服務。
8. 在開發人員目錄頁面中，從功能表中選擇語言 > JavaScript。
9. 選擇 Node.js，然後選擇建立應用程式以開啟建立Source-to-Image應用程式頁面。

> **Note**
> 您可能需要選擇清除所有篩選條件以顯示 Node.js 選項。

10. 在 Git 區段中，選擇嘗試範例。
11. 在名稱欄位中，新增唯一名稱。
12. 選擇 Create (建立)。

> **Note**
> 新應用程式部署需要幾分鐘的時間。

13. 部署完成時，請選擇應用程式的路由 URL。

    瀏覽器中的新索引標籤會開啟，並顯示類似以下的訊息。

```
Welcome to your Node.js application on OpenShift
```

14. (選用) 刪除應用程式並清除資源：
    a. 在管理員角度中，選擇首頁 > 專案。
    b. 開啟專案的動作選單，然後選擇刪除專案。

從使用者撤銷cluster-admin許可

1. 使用下列命令撤銷cluster-admin許可。將 <IDP_USER_NAME> 和 取代<CLUSTER_NAME>為您的使用者和 叢集 名稱。

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者未列為cluster-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

從使用者撤銷dedicated-admin許可

1. 使用以下命令撤銷dedicated-admin許可。將 <IDP_USER_NAME> 和 取代<CLUSTER_NAME>為您的使用者和 叢集 名稱。

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者未列為dedicated-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

撤銷使用者對 的存取權 叢集

您可以將身分提供者使用者從設定的身分提供者中移除，以撤銷其 叢集 存取權。

您可以為 設定不同類型的身分提供者 叢集。下列程序會撤銷 GitHub 組織成員的 叢集 存取權。

1. 導覽至 github.com：// GitHub 帳戶。
2. 從 GitHub 組織中移除使用者。如需詳細資訊，請參閱 GitHub 文件中的從您的組織移除成員。

刪除叢集 AWS STS 和資源

您可以使用 ROSA CLI 來刪除使用 AWS Security Token Service () 叢集 的AWS STS。您也可以使用 ROSA CLI 來刪除由 建立 IAM 的角色和 OIDC 提供者 ROSA。若要刪除 建立 IAM 的政策 ROSA，您可以使用 IAM 主控台。

> **Note**
> IAM 建立的 角色和政策 ROSA 可能由相同帳戶中的其他 ROSA 叢集使用。

1. 刪除 叢集 並監看日誌。<CLUSTER_NAME> 將 取代為 的名稱或 ID 叢集。

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
> 您必須等待 完全 叢集 刪除，才能移除 IAM 角色、政策和 OIDC 供應商。刪除安裝程式建立的資源需要帳戶 IAM 角色。需要操作員 IAM 角色才能清除 OpenShift 操作員建立的資源。運算子使用 OIDC 提供者進行身分驗證。

2. 執行下列命令，刪除 叢集 運算子用來驗證的 OIDC 提供者。

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. 刪除叢集特定的運算子 IAM 角色。

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 使用下列命令刪除帳戶 IAM 角色。<PREFIX> 將 取代為要刪除的帳戶 IAM 角色的字首。如果您在建立帳戶 IAM 角色時指定了自訂字首，請指定預設`ManagedOpenShift`字首。

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. 刪除 建立 IAM 的政策 ROSA。
   a. 登入 IAM 主控台。
   b. 在存取管理下的左側選單中，選擇政策。
   c. 選取您要刪除的政策，然後選擇動作 > 刪除。
   d. 輸入政策名稱，然後選擇刪除。
   e. 重複此步驟來刪除 的每個 IAM 政策 叢集。

使用 CLI ROSA 建立 ROSA 傳統叢集

下列各節說明如何使用 AWS STS 和 CLI ROSA 開始使用 ROSA Classic。如需使用 Terraform 建立 ROSA 傳統叢集的步驟，請參閱 Red Hat 文件。若要進一步了解建立 ROSA 叢集的 Terraform 提供者，請參閱 Terraform 文件。

ROSA CLI 使用 `auto` 模式或 `manual` 模式來建立佈建 ROSA 所需的 IAM 資源 叢集。 `auto` 模式會立即建立所需的 IAM 角色和政策和 OpenID Connect (OIDC) 供應商。 `manual` 模式會輸出建立 IAM 資源所需的 AWS CLI 命令。透過使用 `manual` 模式，您可以在手動執行命令之前檢閱產生的 AWS CLI 命令。透過 `manual` 模式，您也可以將命令傳遞給組織中的另一個管理員或群組，讓他們可以建立資源。

如需更多開始使用的選項，請參閱開始使用 ROSA 。

主題

- 先決條件
- 使用 CLI ROSA 和 建立 ROSA 傳統叢集 AWS STS
- 設定身分提供者並授予 叢集 存取權
- 授予使用者對 的存取權 叢集
- 設定cluster-admin許可
- 設定dedicated-admin許可
- 叢集 透過 Red Hat 混合雲端主控台存取
- 從 Developer Catalog 部署應用程式
- 從使用者撤銷cluster-admin許可
- 從使用者撤銷dedicated-admin許可
- 撤銷使用者對 的存取權 叢集
- 刪除叢集 AWS STS 和資源

先決條件

完成 中列出的先決條件動作the section called “設定”。

使用 CLI ROSA 和 建立 ROSA 傳統叢集 AWS STS

您可以使用 CLI 叢集 ROSA 和 建立 ROSA 傳統 AWS STS。

1. 使用 `--mode auto`或 建立所需的 IAM 帳戶角色和政策`--mode manual`。

   -
     ```
     rosa create account-roles --classic --mode auto
     ```

   -
     ```
     rosa create account-roles --classic --mode manual
     ```

     > **Note**
     > 如果您的離線存取字符已過期，CLI ROSA 會輸出錯誤訊息，指出您的授權字符需要更新。如需疑難排解的步驟，請參閱 the section called “對 CLI ROSA 過期的離線存取權杖進行故障診斷”。

2. 叢集 使用 `--mode auto`或 建立 `--mode manual`。 `auto` 模式可讓您更快速地建立叢集。`manual` 模式會提示您指定叢集的自訂設定。

   -
     ```
     rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode auto
     ```

     > **Note**
     > 當您指定 時`--mode auto`，`rosa create cluster`命令會自動建立叢集特定的運算子 IAM 角色和 OIDC 供應商。運算子使用 OIDC 提供者進行身分驗證。

     > **Note**
     > 使用`--mode auto`預設值時，已安裝最新的穩定 OpenShift 版本。

   -
     ```
     rosa create cluster --cluster-name <CLUSTER_NAME> --sts --mode manual
     ```

     > **Important**
     > 如果您在 `manual` 模式中啟用 加密，則會產生大約 20% 的效能額外負荷。額外負荷是引進第二層加密的結果，以及加密已加密磁碟區的預設 Amazon EBS 加密。

> **Note**
> 在執行`manual`模式來建立叢集之後，您需要手動建立叢集特定的運算子 IAM 角色，以及叢集運算子用來驗證的 OpenID Connect 提供者。

3. 檢查 的狀態 叢集。

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
> 如果佈建程序失敗，或 `State` 欄位在 40 分鐘後未變更為就緒狀態，請參閱 故障診斷。若要聯絡 支援 或 Red Hat 支援以取得協助，請參閱 the section called “取得支援”。

4. 觀看 OpenShift 安裝程式日誌，追蹤 叢集 建立進度。

```
rosa logs install -c <CLUSTER_NAME> --watch
```

設定身分提供者並授予 叢集 存取權

ROSA 包含內建的 OAuth 伺服器。 叢集 建立 之後，您必須設定 OAuth 以使用身分提供者。然後，您可以將使用者新增至您設定的身分提供者，以授予他們存取您的 的權限 叢集。您可以視需要授予這些使用者`cluster-admin`或`dedicated-admin`許可。

您可以為 ROSA 設定不同的身分提供者類型 叢集。支援的類型包括 GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect 和 HTPasswd 身分提供者。

> **Important**
> HTPasswd 身分提供者僅包含用於建立單一靜態管理員使用者。HTPasswd 不支援做為 的一般用途身分提供者 ROSA。

下列程序會將 GitHub 身分提供者設定為範例。如需如何設定每個支援身分提供者類型的指示，請參閱設定身分提供者 AWS STS。

1. 導覽至 github.com：// GitHub 帳戶。
2. 如果您沒有可用於您身分佈建的 GitHub 組織 叢集，請建立一個。如需詳細資訊，請參閱 GitHub 文件中的步驟。
3. 使用 CLI ROSA 的互動式模式，為您的叢集設定身分提供者。

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 遵循輸出中的組態提示，限制對 GitHub 組織成員的 叢集 存取。

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 在輸出中開啟 URL，`<GITHUB_ORG_NAME>`以 GitHub 組織的名稱取代 。
6. 在 GitHub 網頁上，選擇註冊應用程式，在您的 GitHub 組織中註冊新的 OAuth 應用程式。
7. 執行下列命令，使用 GitHub OAuth 頁面中的資訊填入剩餘的`rosa create idp`互動式提示。將`<GITHUB_CLIENT_ID>`和 `<GITHUB_CLIENT_SECRET>`取代為 GitHub OAuth 應用程式的登入資料。

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
```

```
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> 可能需要大約兩分鐘的時間，身分提供者組態才會變成作用中。如果您設定了`cluster-admin`使用者，您可以執行 `oc get pods -n openshift-authentication --watch` 以使用更新的組態來監看 OAuth Pod 重新部署。

8. 確認身分提供者已正確設定。

```
rosa list idps --cluster=<CLUSTER_NAME>
```

授予使用者對 的存取權 叢集

您可以將使用者新增至已設定的身分提供者， 叢集 以授予使用者對 的存取權。

下列程序會將使用者新增至設定為將身分佈建至叢集的 GitHub 組織。

1. 導覽至 github.com 並登入您的 GitHub 帳戶。
2. 邀請需要 叢集 存取 GitHub 組織的使用者。如需詳細資訊，請參閱 GitHub 文件中的邀請使用者加入您的組織。

設定`cluster-admin`許可

1. 執行下列命令來授予`cluster-admin`許可。將 `<IDP_USER_NAME>` 和 取代`<CLUSTER_NAME>`為您的使用者和叢集名稱。

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者已列為`cluster-admins`群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

設定dedicated-admin許可

1. 使用以下命令授予dedicated-admin許可。執行下列命令，將 <IDP_USER_NAME>和 <CLUSTER_NAME>取代為您的使用者和 叢集 名稱。

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者已列為cluster-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

叢集 透過 Red Hat 混合雲端主控台存取

建立 叢集 管理員使用者或將使用者新增至您設定的身分提供者後，您可以透過 叢集 Red Hat 混合雲端主控台登入您的 。

1. 叢集 使用下列命令取得 的主控台 URL。<CLUSTER_NAME> 將 取代為 的名稱 叢集。

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 導覽至輸出中的主控台 URL 並登入。
   - 如果您建立了cluster-admin使用者，請使用提供的登入資料登入。
   - 如果您已為 設定身分提供者 叢集，請在使用...登入對話方塊中選擇身分提供者名稱，並完成提供者提出的任何授權請求。

從 Developer Catalog 部署應用程式

從 Red Hat 混合雲端主控台，您可以部署 Developer Catalog 測試應用程式，並使用路由公開。

1. 導覽至 Red Hat 混合雲端主控台，然後選擇您要部署應用程式的叢集。
2. 在叢集的頁面上，選擇開啟主控台。
3. 在管理員角度中，選擇首頁 > 專案 > 建立專案。
4. 輸入專案的名稱，並選擇性地新增顯示名稱和描述。
5. 選擇建立以建立專案。
6. 切換到開發人員觀點，然後選擇 + 新增。請確定選取的專案是剛建立的專案。

7. 在開發人員目錄對話方塊中，選擇所有 服務。
8. 在開發人員目錄頁面中，從功能表中選擇語言 > JavaScript。
9. 選擇 Node.js，然後選擇建立應用程式以開啟建立Source-to-Image應用程式頁面。

> **Note**
> 您可能需要選擇清除所有篩選條件以顯示 Node.js 選項。

10. 在 Git 區段中，選擇嘗試範例。
11. 在名稱欄位中，新增唯一名稱。
12. 選擇 Create (建立)。

> **Note**
> 新應用程式部署需要幾分鐘的時間。

13. 部署完成時，請選擇應用程式的路由 URL。

    瀏覽器中的新索引標籤會開啟，並顯示類似以下的訊息。

```
Welcome to your Node.js application on OpenShift
```

14. (選用) 刪除應用程式並清除資源：
    a. 在管理員角度中，選擇首頁 > 專案。
    b. 開啟專案的動作選單，然後選擇刪除專案。

從使用者撤銷cluster-admin許可

1. 使用下列命令撤銷cluster-admin許可。將 <IDP_USER_NAME> 和 取代<CLUSTER_NAME>為您的使用者和 叢集 名稱。

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者未列為cluster-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

從使用者撤銷dedicated-admin許可

1. 使用以下命令撤銷dedicated-admin許可。將 <IDP_USER_NAME> 和 取代<CLUSTER_NAME>為您的使用者和 叢集 名稱。

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者未列為dedicated-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

撤銷使用者對 的存取權 叢集

您可以將身分提供者使用者從設定的身分提供者中移除，以撤銷其 叢集 存取權。

您可以為 設定不同類型的身分提供者 叢集。下列程序會撤銷 GitHub 組織成員的 叢集 存取權。

1. 導覽至 github.com 並登入您的 GitHub 帳戶。
2. 從 GitHub 組織移除使用者。如需詳細資訊，請參閱 GitHub 文件中的從您的組織移除成員。

刪除叢集 AWS STS 和資源

您可以使用 ROSA CLI 來刪除使用 AWS Security Token Service () 叢集 的AWS STS。您也可以使用 ROSA CLI 來刪除由 建立 IAM 的角色和 OIDC 提供者 ROSA。若要刪除 建立 IAM 的政策 ROSA，您可以使用 IAM 主控台。

> **Important**
> IAM 建立的 角色和政策 ROSA 可能由相同帳戶中的其他 ROSA 叢集使用。

1. 刪除 叢集 並監看日誌。<CLUSTER_NAME> 將 取代為 的名稱或 ID 叢集。

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
>
> 您必須等待 完全 叢集 刪除，才能移除 IAM 角色、政策和 OIDC 提供者。刪除安裝程式建立的資源需要帳戶 IAM 角色。需要操作員 IAM 角色才能清除 OpenShift 操作員建立的資源。運算子使用 OIDC 提供者進行身分驗證。

2. 執行下列命令，刪除 叢集 運算子用來驗證的 OIDC 提供者。

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. 刪除叢集特定的運算子 IAM 角色。

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 使用下列命令刪除帳戶 IAM 角色。`<PREFIX>` 將 取代為要刪除的帳戶 IAM 角色字首。如果您在建立帳戶 IAM 角色時指定了自訂字首，請指定預設`ManagedOpenShift`字首。

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. 刪除 建立 IAM 的政策 ROSA。
   a. 登入 IAM 主控台。
   b. 在存取管理下的左側選單中，選擇政策。
   c. 選取您要刪除的政策，然後選擇動作 > 刪除。
   d. 輸入政策名稱，然後選擇刪除。
   e. 重複此步驟來刪除 的每個 IAM 政策 叢集。

建立使用 的 ROSA 傳統叢集 AWS PrivateLink

ROSA 傳統叢集可以透過幾種不同方式部署：公有、私有或私有 AWS PrivateLink。如需 ROSA Classic 的詳細資訊，請參閱 the section called “架構”。對於公有和私有 叢集 組態，OpenShift 叢集 可以存取網際網路，並在應用程式層的應用程式工作負載上設定隱私權。

如果您需要將 叢集 和應用程式工作負載都設為私有，您可以使用 AWS PrivateLink ROSA classic 進行設定。 AWS PrivateLink 是一種高可用性、可擴展的技術， ROSA 可用來在 AWS 客戶帳戶中 ROSA 的服務和叢集資源之間建立私有連線。透過 AWS PrivateLink，Red Hat 網站可靠性工程 (SRE) 團隊可以使用連線至叢集 AWS PrivateLink 端點的私有子網路來存取叢集，以取得支援和修復目的。

如需詳細資訊 AWS PrivateLink，請參閱什麼是 AWS PrivateLink？

主題

- 先決條件
- 建立 Amazon VPC 架構
- 使用 CLI ROSA 和 建立 ROSA 傳統叢集 AWS PrivateLink
- 設定 AWS PrivateLink DNS 轉送
- 設定身分提供者並授予 叢集 存取權
- 授予使用者對 的存取權 叢集
- 設定cluster-admin許可
- 設定dedicated-admin許可
- 叢集 透過 Red Hat 混合雲端主控台存取
- 從 Developer Catalog 部署應用程式
- 從使用者撤銷cluster-admin許可
- 從使用者撤銷dedicated-admin許可
- 撤銷使用者對 的存取權 叢集
- 刪除叢集 AWS STS 和資源

先決條件

完成 中列出的先決條件動作the section called “設定”。

建立 Amazon VPC 架構

下列程序會建立可用於託管叢集的 Amazon VPC 架構。所有 叢集 資源都託管在私有子網路中。公有子網路會透過 NAT 閘道，將來自私有子網路的傳出流量路由至公有網際網路。此範例使用 `10.0.0.0/16` 的 CIDR 區塊 Amazon VPC。不過，您可以選擇不同的 CIDR 區塊。如需詳細資訊，請參閱調整 VPC 大小。

> **Important**
>
> 如果不符合 Amazon VPC 要求，叢集建立會失敗。

Example

Amazon VPC console

1. 開啟 Amazon VPC 主控台。
2. 在 VPC 儀表板上，選擇 Create VPC (建立 VPC)。
3. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
4. 保持選取自動產生名稱標籤以建立 VPC 資源的「名稱」標籤，或將其清除以提供您自己的 VPC 資源「名稱」標籤。
5. 在IPv4 CIDR 區塊，輸入 VPC 的 IPv4 地址範圍。VPC 必須具有 IPv4 地址範圍。
6. （選用） 若要支援 IPv6 流量，請選擇 IPv6 CIDR 區塊、Amazon 提供的 IPv6 CIDR 區塊。
7. 將租用保留為 `Default`。
8. 針對可用區域 (AZs) 的數量，選擇您需要的數目。對於異地同步備份部署， ROSA 需要三個可用區域。若要選擇子網路的 AZ，請展開自訂 AZ。

   > **Note**
   > 某些 ROSA 執行個體類型僅適用於特定可用區域。您可以使用 ROSA CLI 命令`rosa list instance-types`來列出所有可用的 ROSA 執行個體類型。若要檢查執行個體類型是否可用於指定的可用區域，請使用 AWS CLI 命令 `aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`。

9. 若要設定您的子網路，請選擇公有子網路數目和私有子網路數目的值。若要選擇子網路的 IP 地址範圍，請展開自訂子網路 CIDR 區塊。

   > **Note**
   > ROSA 要求客戶在每個用來建立叢集的可用區域設定至少一個私有子網路。

10. 若要透過 IPv4 授予私有子網路中公有網際網路的資源存取權，請針對 NAT 閘道選擇要在其中建立 NAT 閘道AZs 數量。在生產環境中，建議您在每個 AZ 中部署一個 NAT 閘道，並包含需要存取公有網際網路的資源。
11. （選用） 如果您需要 Amazon S3 直接從 VPC 存取，請選擇 VPC 端點 S3 Gateway。
12. 保持選取預設 DNS 選項。 ROSA 需要 VPC 上的 DNS 主機名稱支援。

13選擇建立 VPC。

AWS CLI

1. 使用 `10.0.0.0/16` CIDR 區塊建立 VPC。

```
aws ec2 create-vpc \
    --cidr-block 10.0.0.0/16 \
    --query Vpc.VpcId \
    --output text
```

上述命令會傳回 VPC ID。以下為範例輸出。

```
vpc-1234567890abcdef0
```

2. 將 VPC ID 存放在環境變數中。

```
export VPC_ID=vpc-1234567890abcdef0
```

3. 使用`VPC_ID`環境變數為 VPC 建立`Name`標籤。

```
aws ec2 create-tags --resources $VPC_ID --tags Key=Name,Value=MyVPC
```

4. 在 VPC 上啟用 DNS 主機名稱支援。

```
aws ec2 modify-vpc-attribute \
    --vpc-id $VPC_ID \
    --enable-dns-hostnames
```

5. 在 VPC 中建立公有和私有子網路，指定應建立資源的可用區域。

> **Important**
>
> ROSA 要求客戶在每個用來建立叢集的可用區域設定至少一個私有子網路。對於異地同步備份部署，需要三個可用區域。如果不符合這些要求，叢集建立會失敗。

> **Note**
>
> 某些 ROSA 執行個體類型僅適用於特定可用區域。您可以使用 ROSA CLI 命令`rosa list instance-types`來列出所有可用的 ROSA 執行個體類型。若要檢查執行個體類型是否可用於指定的可用區域，請使用 AWS CLI 命令 `aws ec2 describe-instance-type-offerings --location-type availability-zone --filters Name=location,Values=<availability_zone> --region <region> --output text | egrep "<instance_type>"`。

```
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.1.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
aws ec2 create-subnet \
    --vpc-id $VPC_ID \
    --cidr-block 10.0.0.0/24 \
    --availability-zone us-east-1a \
    --query Subnet.SubnetId \
    --output text
```

6. 將公有和私有子網路 IDs存放在環境變數中。

```
export PUBLIC_SUB=subnet-1234567890abcdef0
export PRIVATE_SUB=subnet-0987654321fedcba0
```

7. 建立網際網路閘道和傳出流量的路由表。為私有流量建立路由表和彈性 IP 地址。

```
aws ec2 create-internet-gateway \
    --query InternetGateway.InternetGatewayId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
aws ec2 allocate-address \
    --domain vpc \
```

```
    --query AllocationId \
    --output text
aws ec2 create-route-table \
    --vpc-id $VPC_ID \
    --query RouteTable.RouteTableId \
    --output text
```

8. 將 IDs存放在環境變數中。

```
export IGW=igw-1234567890abcdef0
export PUBLIC_RT=rtb-0987654321fedcba0
export EIP=eipalloc-0be6ecac95EXAMPLE
export PRIVATE_RT=rtb-1234567890abcdef0
```

9. 將網際網路閘道連接至 VPC。

```
aws ec2 attach-internet-gateway \
    --vpc-id $VPC_ID \
    --internet-gateway-id $IGW
```

10將公有路由表與公有子網路建立關聯，並設定流量以路由至網際網路閘道。

```
aws ec2 associate-route-table \
    --subnet-id $PUBLIC_SUB \
    --route-table-id $PUBLIC_RT
aws ec2 create-route \
    --route-table-id $PUBLIC_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $IGW
```

11建立 NAT 閘道並將其與彈性 IP 地址建立關聯，以啟用私有子網路的流量。

```
aws ec2 create-nat-gateway \
    --subnet-id $PUBLIC_SUB \
    --allocation-id $EIP \
    --query NatGateway.NatGatewayId \
    --output text
```

12將私有路由表與私有子網路建立關聯，並設定流量以路由至 NAT 閘道。

```
aws ec2 associate-route-table \
    --subnet-id $PRIVATE_SUB \
    --route-table-id $PRIVATE_RT
```

```
aws ec2 create-route \
    --route-table-id $PRIVATE_RT \
    --destination-cidr-block 0.0.0.0/0 \
    --gateway-id $NATGW
```

13. （選用） 對於多可用區域部署，重複上述步驟，以設定具有公有和私有子網路的兩個其他可用區域。

使用 CLI ROSA 和 建立 ROSA 傳統叢集 AWS PrivateLink

您可以使用 ROSA CLI 和 AWS PrivateLink 建立 叢集 具有單一可用區域 （單一可用區域） 或多個可用區域 （多可用區域） 的 。無論哪種情況，機器的 CIDR 值都必須符合您 VPC 的 CIDR 值。

下列程序使用 `rosa create cluster`命令來建立 ROSA 傳統 叢集。若要建立異地同步備份 叢集，請在 命令`--multi-az`中指定 ，然後選取出現提示時要使用的私有子網路 IDs。

> **Note**
> 如果您使用防火牆，則必須將其設定為 ，讓 ROSA 可以存取其運作所需的網站。
> 如需詳細資訊，請參閱 Red Hat OpenShift 文件中的AWS 防火牆先決條件。

1. 使用 `--mode auto`或 建立所需的 IAM 帳戶角色和政策`--mode manual`。

   -
     ```
     rosa create account-roles --classic --mode auto
     ```
   -
     ```
     rosa create account-roles --classic --mode manual
     ```

     > **Note**
     > 如果您的離線存取字符已過期，CLI ROSA 會輸出錯誤訊息，指出您的授權字符需要更新。如需疑難排解的步驟，請參閱 the section called “對 CLI ROSA 過期的離線存取權杖進行故障診斷”。

2. 執行下列其中一個命令 叢集 來建立 。

   - 單一可用區

```
rosa create cluster --private-link --cluster-name=<CLUSTER_NAME> --machine-
cidr=10.0.0.0/16 --subnet-ids=<PRIVATE_SUBNET_ID>
```

- Multi-AZ

```
rosa create cluster --private-link --multi-az --cluster-name=<CLUSTER_NAME> --
machine-cidr=10.0.0.0/16
```

> **Note**
>
> 若要建立使用 AWS PrivateLink 搭配 AWS Security Token Service (AWS STS) 短期登入資料的叢集，請附加 `--sts --mode auto`或 `--sts --mode manual`至 `rosa create cluster` 命令的結尾。

3. 依照互動式提示建立 叢集 運算子 IAM 角色。

```
rosa create operator-roles --interactive -c <CLUSTER_NAME>
```

4. 建立 叢集 運算子用來驗證的 OpenID Connect (OIDC) 提供者。

```
rosa create oidc-provider --interactive -c <CLUSTER_NAME>
```

5. 檢查 的狀態 叢集。

```
rosa describe cluster -c <CLUSTER_NAME>
```

> **Note**
>
> `State` 欄位最多可能需要 40 分鐘 叢集 才能顯示`ready`狀態。如果佈建失敗或 40 分鐘後未顯示為 `ready` ，請參閱故障診斷。若要聯絡 支援 或 Red Hat 支援以取得協助，請參閱the section called “取得支援”。

6. 觀看 OpenShift 安裝程式日誌，追蹤 叢集 建立進度。

```
rosa logs install -c <CLUSTER_NAME> --watch
```

設定 AWS PrivateLink DNS 轉送

使用 AWS PrivateLink 建立公有託管區域和私有託管區域的叢集 Route 53。 Route 53 私有託管區域內的記錄只能從指派給它的 VPC 內解析。

Let's Encrypt DNS-01 驗證需要公有區域，才能為網域發出有效且公有信任的憑證。驗證記錄會在 Let's Encrypt 驗證完成後刪除。核發和續約這些憑證時，仍然需要該區域，通常每 60 天需要一次。雖然這些區域通常顯示為空白，但公有區域在驗證程序中扮演關鍵角色。

如需 AWS 私有託管區域的詳細資訊，請參閱使用私有區域。如需公有託管區域的詳細資訊，請參閱使用公有託管區域。

設定 Route 53 Resolver 傳入端點

1. 若要允許 `api.<cluster_domain>`和 等記錄`*.apps.<cluster_domain>`在 VPC 外部解析，請設定 Route 53 Resolver 傳入端點。

> **Note**
>
> 當您設定傳入端點時，至少需要指定兩個 IP 地址以進行備援。建議您至少在兩個可用區域中指定 IP 地址。您可以在那些或其他可用區域選擇性指定其他 IP 地址。

2. 當您設定傳入端點時，請選取您建立叢集時所使用的 VPC 和私有子網路。

設定叢集的 DNS 轉送

建立 Route 53 Resolver 內部端點關聯並運作後，請設定 DNS 轉送，以便 DNS 查詢可由您網路上的指定伺服器處理。

1. 設定您的公司網路，將 DNS 查詢轉送至頂層網域的 IP 地址，例如 `drow-pl-01.htno.p1.openshiftapps.com`。
2. 如果您要將 DNS 查詢從一個 VPC 轉送到另一個 VPC，請遵循管理轉送規則中的指示。
3. 如果您要設定遠端網路 DNS 伺服器，請參閱您的特定 DNS 伺服器文件，以設定已安裝叢集網域的選擇性 DNS 轉送。

設定身分提供者並授予 叢集 存取權

ROSA 包含內建的 OAuth 伺服器。建立 叢集 ROSA 之後，您必須設定 OAuth 以使用身分提供者。然後，您可以將使用者新增至您設定的身分提供者，以授予他們存取您的 的權限 叢集。您可以視需要授予這些使用者`cluster-admin`或`dedicated-admin`許可。

您可以為 設定不同的身分提供者類型 叢集。支援的類型包括 GitHub、GitHub Enterprise、GitLab、Google、LDAP、OpenID Connect 和 HTPasswd 身分提供者。

> **Important**
>
> HTPasswd 身分提供者僅包含用於建立單一靜態管理員使用者。HTPasswd 不支援做為 的一般用途身分提供者 ROSA。

下列程序會將 GitHub 身分提供者設定為範例。如需如何設定每個支援身分提供者類型的說明，請參閱設定身分提供者 AWS STS。

1. 導覽至 github.com：// GitHub 帳戶。
2. 如果您沒有可用於 ROSA 身分佈建的 GitHub 組織 叢集，請建立一個。如需詳細資訊，請參閱 GitHub 文件中的步驟。
3. 使用 CLI ROSA 的互動式模式，執行下列命令來設定叢集的身分提供者。

```
rosa create idp --cluster=<CLUSTER_NAME> --interactive
```

4. 遵循輸出中的組態提示，限制對 GitHub 組織成員的 叢集 存取。

```
I: Interactive mode enabled.
Any optional fields can be left empty and a default will be selected.
? Type of identity provider: github
? Identity provider name: github-1
? Restrict to members of: organizations
? GitHub organizations: <GITHUB_ORG_NAME>
? To use GitHub as an identity provider, you must first register the application:
  - Open the following URL:
    https://github.com/organizations/<GITHUB_ORG_NAME>/settings/
applications/new?oauth_application%5Bcallback_url%5D=https%3A%2F%2Foauth-
openshift.apps.<CLUSTER_NAME>/<RANDOM_STRING>.p1.openshiftapps.com%2Foauth2callback
%2Fgithub-1&oauth_application%5Bname%5D=<CLUSTER_NAME>&oauth_application
```

```
%5Burl%5D=https%3A%2F%2Fconsole-openshift-console.apps.<CLUSTER_NAME>/
<RANDOM_STRING>.p1.openshiftapps.com
  - Click on 'Register application'
...
```

5. 在輸出中開啟 URL，<GITHUB_ORG_NAME>以 GitHub 組織的名稱取代 。
6. 在 GitHub 網頁上，選擇註冊應用程式，在您的 GitHub 組織中註冊新的 OAuth 應用程式。
7. 使用 GitHub OAuth 頁面中的資訊來填入剩餘的`rosa create idp`互動式提示，將<GITHUB_CLIENT_ID>和 <GITHUB_CLIENT_SECRET>取代為 GitHub OAuth 應用程式的登入資料。

```
...
? Client ID: <GITHUB_CLIENT_ID>
? Client Secret: [? for help] <GITHUB_CLIENT_SECRET>
? GitHub Enterprise Hostname (optional):
? Mapping method: claim
I: Configuring IDP for cluster '<CLUSTER_NAME>'
I: Identity Provider 'github-1' has been created.
   It will take up to 1 minute for this configuration to be enabled.
   To add cluster administrators, see 'rosa grant user --help'.
   To login into the console, open https://console-openshift-
console.apps.<CLUSTER_NAME>.<RANDOM_STRING>.p1.openshiftapps.com and click on
 github-1.
```

> **Note**
>
> 可能需要約兩分鐘的時間，身分提供者組態才會變成作用中。如果您已設定`cluster-admin`使用者，您可以執行 `oc get pods -n openshift-authentication --watch`命令，以使用更新的組態來監看 OAuth Pod 重新部署。

8. 確認身分提供者已正確設定。

```
rosa list idps --cluster=<CLUSTER_NAME>
```

授予使用者對 的存取權 叢集

您可以將使用者新增至已設定的身分提供者， 叢集 以授予使用者對 的存取權。

下列程序會將使用者新增至設定為將身分佈建至叢集的 GitHub 組織。

1. 導覽至 github.com 並登入您的 GitHub 帳戶。
2. 邀請需要 叢集 存取 GitHub 組織的使用者。如需詳細資訊，請參閱 GitHub 文件中的邀請使用者加入您的組織。

設定cluster-admin許可

1. 使用以下命令授予cluster-admin許可。將 <IDP_USER_NAME> 和 取代<CLUSTER_NAME>為您的使用者和叢集名稱。

```
rosa grant user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者列為cluster-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

設定dedicated-admin許可

1. 使用下列命令授予dedicated-admin許可。將 <IDP_USER_NAME> 和 取代<CLUSTER_NAME>為您的使用者和 叢集 名稱。

```
rosa grant user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者列為cluster-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

叢集 透過 Red Hat 混合雲端主控台存取

在您建立 叢集 管理員使用者或將使用者新增至您設定的身分提供者之後，您可以透過 叢集 Red Hat 混合雲端主控台登入您的 。

1. 叢集 使用下列命令取得 的主控台 URL。<CLUSTER_NAME> 將 取代為 的名稱 叢集。

```
rosa describe cluster -c <CLUSTER_NAME> | grep Console
```

2. 導覽至輸出中的主控台 URL 並登入。

- 如果您建立了`cluster-admin`使用者，請使用提供的登入資料登入。
- 如果您已為 設定身分提供者 叢集，請在使用...登入對話方塊中選擇身分提供者名稱，並完成提供者提出的任何授權請求。

從 Developer Catalog 部署應用程式

從 Red Hat 混合雲端主控台，您可以部署 Developer Catalog 測試應用程式，並使用路由公開。

1. 導覽至 Red Hat 混合雲端主控台，然後選擇您要部署應用程式的叢集。
2. 在叢集的頁面上，選擇開啟主控台。
3. 在管理員角度中，選擇首頁 > 專案 > 建立專案。
4. 輸入專案的名稱，並選擇性地新增顯示名稱和描述。
5. 選擇建立以建立專案。
6. 切換到 Developer 觀點，然後選擇 +Add。請確定選取的專案是剛建立的專案。
7. 在開發人員目錄對話方塊中，選擇所有 服務。
8. 在開發人員目錄頁面中，從功能表中選擇語言 > JavaScript。
9. 選擇 Node.js，然後選擇建立應用程式以開啟建立Source-to-Image應用程式頁面。

> **Note**
> 您可能需要選擇清除所有篩選條件以顯示 Node.js 選項。

10. 在 Git 區段中，選擇嘗試範例。
11. 在名稱欄位中，新增唯一名稱。
12. 選擇 Create (建立)。

> **Note**
> 新應用程式部署需要幾分鐘的時間。

13. 部署完成時，請選擇應用程式的路由 URL。

    瀏覽器中的新索引標籤會開啟，並顯示類似以下的訊息。

```
Welcome to your Node.js application on OpenShift
```

14. (選用) 刪除應用程式並清除資源。
    a. 在管理員角度中，選擇首頁 > 專案。
    b. 開啟專案的動作選單，然後選擇刪除專案。

從使用者撤銷cluster-admin許可

1. 使用以下命令撤銷cluster-admin許可。將 <IDP_USER_NAME> 和 取代<CLUSTER_NAME>為您的使用者和 叢集 名稱。

```
rosa revoke user cluster-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者未列為cluster-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

從使用者撤銷dedicated-admin許可

1. 使用以下命令撤銷dedicated-admin許可。將 <IDP_USER_NAME> 和 取代<CLUSTER_NAME>為您的使用者和 叢集 名稱。

```
rosa revoke user dedicated-admin --user=<IDP_USER_NAME> --cluster=<CLUSTER_NAME>
```

2. 確認使用者未列為dedicated-admins群組的成員。

```
rosa list users --cluster=<CLUSTER_NAME>
```

撤銷使用者對 的存取權 叢集

您可以將身分提供者使用者從設定的身分提供者中移除，以撤銷其 叢集 存取權。

您可以為 設定不同類型的身分提供者 叢集。下列程序會撤銷 GitHub 組織成員的 叢集 存取權。

1. 導覽至 github.com 並登入您的 GitHub 帳戶。
2. 從您的 GitHub 組織移除使用者。如需詳細資訊，請參閱 GitHub 文件中的從您的組織移除成員。

刪除叢集 AWS STS 和資源

您可以使用 ROSA CLI 來刪除使用 AWS Security Token Service () 叢集 的AWS STS。您也可以使用 ROSA CLI 來刪除 建立 IAM 的角色和 OIDC 供應商 ROSA。若要刪除 建立 IAM 的政策 ROSA，您可以使用 IAM 主控台。

> **Important**
> IAM 建立的 角色和政策 ROSA 可能由相同帳戶中的其他 ROSA 叢集使用。

1. 刪除 叢集 並監看日誌。<CLUSTER_NAME> 將 取代為 的名稱或 ID 叢集。

```
rosa delete cluster --cluster=<CLUSTER_NAME> --watch
```

> **Important**
> 您必須等待 完全 叢集 刪除，才能移除 IAM 角色、政策和 OIDC 提供者。刪除安裝程式建立的資源需要帳戶 IAM 角色。需要操作員 IAM 角色才能清除 OpenShift 操作員建立的資源。運算子會使用 OIDC 提供者進行身分驗證。

2. 執行下列命令，刪除 叢集 運算子用來驗證的 OIDC 提供者。

```
rosa delete oidc-provider -c <CLUSTER_ID> --mode auto
```

3. 刪除叢集特定的運算子 IAM 角色。

```
rosa delete operator-roles -c <CLUSTER_ID> --mode auto
```

4. 使用下列命令刪除帳戶 IAM 角色。<PREFIX> 將 取代為要刪除的帳戶 IAM 角色的字首。如果您在建立帳戶 IAM 角色時指定了自訂字首，請指定預設`ManagedOpenShift`字首。

```
rosa delete account-roles --prefix <PREFIX> --mode auto
```

5. 刪除 建立 IAM 的政策 ROSA。
   a. 登入 IAM 主控台。
   b. 在存取管理下的左側選單中，選擇政策。
   c. 選取您要刪除的政策，然後選擇動作 > 刪除。

d. 輸入政策名稱，然後選擇刪除。

e. 重複此步驟來刪除 的每個 IAM 政策 叢集。

中的安全性 ROSA

的雲端安全性 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，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模型將此描述為雲端本身的安全和雲端內部的安全：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用的合規計劃 ROSA，請參閱AWS 服務 合規計劃範圍中的 。
- 雲端的安全性 – 您的責任取決於您使用 AWS 服務 的 。您也必須對其他因素負責，包括資料的機密性、您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 ROSA。它說明如何設定 ROSA 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 ROSA 資源。

目錄

- 中的資料保護 ROSA
- 的身分和存取管理 ROSA
- 中的彈性 ROSA
- 中的基礎設施安全 ROSA

中的資料保護 ROSA

the section called “責任” 文件和AWS 共同責任模型定義 中的資料保護 ROSA。 AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。Red Hat 負責保護叢集基礎設施和基礎服務平台。客戶負責控制在此基礎設施上託管的內容。此內容包含 AWS 服務 您使用之 的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需歐洲資料保護的相關資訊，請參閱安全部落格上的AWS 共同責任模型和 GDPR 部落格文章。 AWS

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 Identity and Access Management () 設定個別使用者IAM。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。
- 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。
- 使用進階受管安全服務 Amazon Macie，例如 ，協助探索和保護存放在其中的敏感資料 Amazon S3。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-2 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) 140-2 概觀。

我們強烈建議您絕對不要將客戶帳戶號碼等敏感的識別資訊，放在自由格式的欄位中，例如名稱欄位。這包括當您 AWS 服務 使用 ROSA 或使用主控台、API AWS CLI或其他 AWS SDKs 時。您輸入的任何資料 ROSA 或其他 服務都可能被選入診斷日誌中。當您提供外部伺服器的 URL 時，請勿在驗證您對該伺服器請求的 URL 中包含登入資料資訊。

主題

- 使用加密保護資料

使用加密保護資料

資料保護是指在傳輸中 （進出時 ROSA) 和靜態 （存放在 AWS 資料中心的磁碟上） 時保護資料。

Red Hat OpenShift Service on AWS 為 ROSA 控制平面、基礎設施和工作者節點提供連接至 Amazon EC2 執行個體的 Amazon Elastic Block Store (Amazon EBS) 儲存磁碟區安全存取，以及為持久性儲存提供 Kubernetes 持久性磁碟區。 ROSA 會加密靜態和傳輸中的磁碟區資料，並使用 AWS Key Management Service (AWS KMS) 協助保護您的加密資料。服務會使用 Amazon S3 來儲存容器映像登錄檔，依預設會進行靜態加密。

> **Important**
>
> 因為 ROSA 是受管服務， AWS 而 Red Hat 會管理 ROSA 使用的基礎設施。客戶不應嘗試從 AWS 主控台或 CLI 手動關閉 ROSA 使用的 Amazon EC2 執行個體。此動作可能會導致客戶資料遺失。

Amazon EBS後端儲存磁碟區的資料加密

Red Hat OpenShift Service on AWS 使用 Kubernetes 持久性磁碟區 (PV) 架構，允許叢集管理員佈建具有持久性儲存的叢集。持久性磁碟區，以及控制平面、基礎設施和工作者節點，都由連接至 Amazon EC2 執行個體的 Amazon Elastic Block Store (Amazon EBS) 儲存磁碟區提供支援。

對於 支援的 ROSA 持久性磁碟區和節點 Amazon EBS，加密操作會在託管 EC2 執行個體的伺服器上進行，以確保靜態資料和執行個體與其連接儲存體之間傳輸中資料的安全性。如需詳細資訊，請參閱 Amazon EC2 《 使用者指南》中的Amazon EBS 加密。

Amazon EBS CSI 驅動程式和 Amazon EFS CSI 驅動程式的資料加密

ROSA 預設為使用 Amazon EBS CSI 驅動程式佈建 Amazon EBS 儲存。根據預設， Amazon EBS CSI 驅動程式和 Amazon EBS CSI 驅動程式運算子會安裝在 `openshift-cluster-csi-drivers` 命名空間中的叢集上。 Amazon EBS CSI 驅動程式和運算子可讓您動態佈建持久性磁碟區並建立磁碟區快照。

ROSA 也能夠使用 Amazon EFS CSI 驅動程式和 Amazon EFS CSI 驅動程式運算子佈建持久性磁碟區。 Amazon EFS 驅動程式和運算子也可讓您在 Pod 之間或與 Kubernetes 內外的其他應用程式共用檔案系統資料。

CSI 驅動程式和 Amazon EBS Amazon EFS CSI 驅動程式的磁碟區資料在傳輸中都會受到保護。如需詳細資訊，請參閱 Red Hat 文件中的使用容器儲存界面 (CSI)。

> **Important**
>
> 使用 Amazon EFS CSI 驅動程式動態佈建 ROSA 持久性磁碟區時，評估檔案系統許可時，Amazon EFS 請考慮存取點的使用者 ID、群組 ID (GID) 和次要群組 IDs。 會將使用者和群組 IDs Amazon EFS 取代為存取點上具有使用者和群組 IDs的檔案，並忽略 NFS 用戶端 IDs。因此， 會無 Amazon EFS 提示地忽略`fsGroup`設定。 ROSA 無法使用 取代檔案 GID`fsGroup`。任何可以存取掛載 Amazon EFS 存取點的 Pod 都可以存取磁碟區上的任何檔案。如需詳細資訊，請參閱 Amazon EFS 《 使用者指南》中的使用 Amazon EFS 存取點。

etcd 加密

ROSA 提供在叢集建立期間啟用`etcd`磁碟區內`etcd`金鑰值加密的選項，新增額外的加密層。`etcd` 加密後，您將產生大約 20% 的額外效能額外負荷。建議您只有在使用案例特別需要加密時，才啟用`etcd`加密。如需詳細資訊，請參閱 ROSA 服務定義中的加密。

金鑰管理

ROSA 使用 KMS keys 為客戶應用程式安全地管理控制平面、基礎設施和工作者資料磁碟區和持久性磁碟區。在叢集建立期間，您可以選擇使用 KMS key 提供的預設 AWS 受管金鑰 Amazon EBS，或指定您自己的客戶受管金鑰。如需詳細資訊，請參閱the section called “金鑰管理”。

內建映像登錄檔的資料加密

ROSA 提供內建的容器映像登錄檔，透過儲存 Amazon S3 貯體儲存來存放、擷取和共用容器映像。登錄檔是由 OpenShift Image Registry Operator 設定和管理。它提供out-of-the-box解決方案，讓使用者管理執行工作負載的映像，並在現有的叢集基礎設施上執行。如需詳細資訊，請參閱 Red Hat 文件中的登錄檔。

ROSA 提供公有和私有映像登錄檔。對於企業應用程式，我們建議您使用私有登錄檔來保護映像不受未經授權的使用者使用。為了保護登錄檔的靜態資料， 預設 ROSA 會使用伺服器端加密搭配 Amazon S3 受管金鑰 (SSE-S3)。這不需要您採取任何動作，且不收取額外費用。如需詳細資訊，請參閱 Amazon S3 《 使用者指南》中的使用伺服器端加密搭配 Amazon S3 受管加密金鑰 (SSE-S3) 保護資料。

ROSA 使用 Transport Layer Security (TLS) 通訊協定來保護傳入和傳出映像登錄檔的資料。如需詳細資訊，請參閱 Red Hat 文件中的登錄檔。

網際網路流量隱私權

Red Hat OpenShift Service on AWS use Amazon Virtual Private Cloud (Amazon VPC) 在 ROSA 叢集中的資源之間建立邊界，並控制它們、內部部署網路和網際網路之間的流量。如需 Amazon VPC 安全性的詳細資訊，請參閱 Amazon VPC 《 使用者指南》中的 中的網際網路流量隱私權 Amazon VPC。

在 VPC 中，您可以將 ROSA 叢集設定為使用 HTTP 或 HTTPS 代理伺服器來拒絕直接網際網路存取。如果您是叢集管理員，也可以在 Pod 層級定義網路政策，將網際網路流量限制為 ROSA 叢集中的 Pod。如需詳細資訊，請參閱the section called “基礎架構安全”。

使用 KMS 的資料加密

ROSA 使用 AWS KMS 安全地管理加密資料的金鑰。根據預設，控制平面、基礎設施和工作者節點磁碟區會使用 KMS key 提供的 AWS 受管 進行加密 Amazon EBS。這 KMS key 具有別名 `aws/ebs`。使用預設 gp3 儲存類別的持久性磁碟區也會預設使用此項目加密 KMS key。

新建立的 ROSA 叢集設定為使用預設 gp3 儲存類別來加密持久性磁碟區。只有在儲存類別設定為加密時，才能使用任何其他儲存類別建立的持久性磁碟區才會加密。如需 ROSA 預先建置儲存類別的詳細資訊，請參閱 Red Hat 文件中的設定持久性儲存。

在叢集建立期間，您可以選擇使用預設 Amazon EBS提供的金鑰來加密叢集中的持久性磁碟區，或指定您自己的客戶受管對稱 KMS key。如需建立金鑰的詳細資訊，請參閱《 AWS KMS 開發人員指南》中的建立對稱加密 KMS 金鑰。

您也可以透過定義 來加密叢集內個別容器的持久性磁碟區 KMS key。當您在部署到 時有明確的合規和安全指導方針時，這很有用 AWS。如需詳細資訊，請參閱 Red Hat 文件中的AWS 使用 在 上加密容器持久性磁碟區 KMS key。

使用您自己的 加密持久性磁碟區時，應考慮下列事項 KMS keys：

- 當您搭配自己的 KMS 加密時 KMS key，金鑰必須與 AWS 區域 叢集位於相同的 中。
- 建立和使用您自己的 會產生相關費用 KMS keys。如需詳細資訊，請參閱 AWS Key Management Service 定價。

的身分和存取管理 ROSA

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。 IAM 管理員可控制誰可以經過身分驗證 （ 登入 ） 和授權 （ 具有許可 ） 來使用 ROSA 資源。 IAM 是 AWS 服務 您可以免費使用的 。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- ROSA 身分型政策範例
- AWS 的 受管政策 ROSA
- 對 ROSA 身分和存取進行故障診斷

目標對象

您的使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您所做的工作 ROSA。

服務使用者 - 如果您使用 ROSA 服務來執行任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多 ROSA 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 中的功能 ROSA，請參閱 the section called “故障診斷”。

服務管理員 - 如果您負責公司 ROSA 的資源，您可能擁有 的完整存取權 ROSA。您的任務是判斷服務使用者應存取哪些 ROSA 功能和資源。然後，您必須向 IAM 管理員提交請求，以變更服務使用者的許可。檢閱此頁面上的資訊，以了解 的基本概念 IAM。

IAM 管理員 - 如果您是 IAM 管理員，建議您了解用於管理 存取的政策詳細資訊 ROSA。若要檢視您可以在 中使用的以 ROSA 身分為基礎的政策範例 IAM，請參閱 the section called “ ROSA 身分型政策範例”。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須擔任 IAM 角色，以 AWS 帳戶 根使用者 IAM 使用者、 或 身分進行身分驗證 （ 登入 AWS)。

您可以使用透過身分來源提供的登入資料，以聯合身分 AWS 的形式登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。當您以聯合身分身分登入時，您的管理員先前會使用 IAM 角色設定聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 AWS 《 登入使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法來自行簽署請求的詳細資訊，請參閱 IAM 《 使用者指南》中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能還需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來提高帳戶的安全性。若要進一步了解，請參閱《 AWS IAM Identity Center (AWS 單一登入的後繼者） 使用者指南》中的多重要素驗證，以及《IAM 使用者指南》中的在 中使用多重要素驗證 (MFA) AWS。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從單一登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 根使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常作業。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以根使用者身分登入的任務完整清單，請參閱 IAM 《 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用 聯合身分提供者 AWS 服務 來使用臨時憑證來存取 。

聯合身分是您企業使用者目錄、Web 身分提供者、 AWS Directory Service、Identity Center 目錄或任何使用透過身分來源提供的登入資料 AWS 服務 存取的使用者。當聯合身分存取時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時登入資料。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需有關 IAM Identity Center 的資訊，請參閱《IAM Identity Center （單一登入的後繼者） 使用者指南》中的什麼是 AWS IAM Identity Center AWS ？。

IAM 使用者 和 群組

IAM 使用者 是您 中的身分 AWS 帳戶 ，具有單一人員或應用程式的特定許可。如果可能，我們建議依賴臨時登入資料，而不是建立擁有密碼和存取金鑰等長期登入資料 IAM 使用者 的人員。不過，如果您有特定的使用案例需要使用長期憑證 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是指定 集合的身分 IAM 使用者。您無法以群組身分登入。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有名為 IAMAdmins 的群組，並授予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。若要進一步了解，請參閱《IAM 使用者指南》中的何時建立 IAM 使用者 （而非角色）。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似於 IAM 使用者，但不與特定人員相關聯。您可以 AWS Management Console 切換 IAM 角色，暫時在 中擔任 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色方法的詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色。

IAM 具有臨時登入資料的 角色在下列情況下非常有用：

- 聯合身分使用者存取 - 若要將許可指派給聯合身分，您可以建立角色並定義角色的許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM中的角色相關聯。如需有關許可集的資訊，請參閱《 AWS IAM Identity Center (AWS 單一登入的後續） 使用者指南》中的許可集。

- 暫時 IAM 使用者 許可 - IAM 使用者 可以擔任 IAM 角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 - 您可以使用 IAM 角色，允許不同帳戶中的某人（信任的委託人）存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。若要了解跨帳戶存取的角色和資源型政策之間的差異，請參閱《IAM 使用者指南》中的IAM 角色與資源型政策的差異。
- 跨服務存取 - 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中呼叫 時，該服務通常會在 中執行應用程式 Amazon EC2 或將物件存放在其中 Amazon S3。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 (FAS) - 當您使用 IAM 使用者 或 角色在其中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。
  - 服務角色 - 服務角色是服務擔任以代表您執行動作 IAM 的角色。 IAM 管理員可以從內部建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。
  - 服務連結角色 - 服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的帳戶中 IAM ，並由服務擁有。 IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 上執行 Amazon EC2 的應用程式 - 您可以使用 IAM 角色來管理在 Amazon EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這較適合將存取金鑰存放在 Amazon EC2 執行個體中。若要將 AWS 角色指派給 Amazon EC2 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體描述檔包含 角色，並可讓在 Amazon EC2 執行個體上執行的程式取得臨時登入資料。如需詳細資訊，請參閱《IAM 使用者指南Amazon EC2 》中的使用 IAM 角色將許可授予執行個體上執行的應用程式。

若要了解如何使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的建立 IAM 角色（而非使用者）的時機。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件，當與身分或資源建立關聯時， AWS 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對所需資源執行動作的許可， IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者可以擔任角色。

IAM 無論您用來執行操作的方法為何， 政策都會定義動作的許可。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 AWS API 取得角色資訊。

身分型政策

身分型政策是您可以連接到身分的 JSON 許可政策文件，例如 IAM 使用者、 角色或 群組。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。以資源為基礎的政策的範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策 IAM 中使用來自 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF、 和 Amazon VPC 是支援 ACLs的服務範例。若要進一步了解 ACLs，請參閱《Amazon Simple Storage Service 使用者指南》中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 - 許可界限是一種進階功能，您可以在其中設定身分型政策可授予 IAM 實體 (IAM 使用者或角色） 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱《IAM 使用者指南》中的IAM 實體的許可界限。
- 服務控制政策 (SCPs) - SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 之多個 的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個 AWS 帳戶 根使用者。如需 Organizations 和 SCPs的詳細資訊，請參閱 AWS Organizations 《 使用者指南》中的服務控制政策 (SCPs)。
- 工作階段政策 - 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合身分使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

ROSA 身分型政策範例

根據預設， IAM 使用者 和 角色沒有建立或修改 AWS 資源的許可。他們也無法使用 AWS Management Console AWS CLI或 AWS API 執行任務。 IAM 管理員必須建立 IAM 政策，授予使用者和角色對所需指定資源執行特定 API 操作的許可。然後，管理員必須將這些政策連接到需要這些許可的 IAM 使用者 或 群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的在 JSON 標籤上建立政策。

使用 ROSA 主控台

若要 ROSA 從 主控台訂閱 ，您的 IAM 主體必須具有必要的 AWS Marketplace 許可。許可允許委託人訂閱和取消訂閱 中的 ROSA 產品清單 AWS Marketplace ，並檢視 AWS Marketplace 訂閱。若要新增必要的許可，請前往 ROSA 主控台，並將 AWS 受管政策連接至`ROSAManageSubscription`您的 IAM 主體。如需 `ROSAManageSubscription` 的相關資訊，請參閱 the section called “AWS 受管政策：ROSAManageSubscription”。

授權 ROSA 與 HCP 管理 AWS 資源

具有託管控制平面 (HCP) 的 ROSA 使用具有服務操作和支援所需許可的 AWS 受管政策。您可以使用 ROSA CLI 或 IAM 主控台將這些政策連接到 中的服務角色 AWS 帳戶。

如需詳細資訊，請參閱the section called “ AWS 受管政策”。

授權 ROSA classic 來管理 AWS 資源

ROSA classic 使用客戶受管 IAM 政策，具有 服務預先定義的許可。您可以使用 ROSA CLI 來建立這些政策，並將其連接到您 中的服務角色 AWS 帳戶。 ROSA 需要這些政策按照服務的定義進行設定，以確保持續操作和服務支援。

> **Note**
>
> 若未先諮詢 Red Hat，您不應更改 ROSA 傳統政策。這樣做可能會使 Red Hat 的 99.95% 叢集運作時間服務層級協議失效。具有託管控制平面的 ROSA 使用具有更有限許可集的 AWS 受管政策。如需詳細資訊，請參閱the section called “ AWS 受管政策”。

有兩種類型的客戶受管政策 ROSA：帳戶政策和運算子政策。帳戶政策會連接到 服務用來與 Red Hat 建立信任關係 IAM 的角色，以進行網站可靠性工程師 (SRE) 支援、叢集建立和運算功能。運算子政策會連接到 OpenShift 運算子用於與輸入、儲存、映像登錄檔和節點管理相關的叢集操作 IAM 的角色。每個帳戶政策建立一次 AWS 帳戶，而每個叢集建立一次運算子政策。

如需詳細資訊，請參閱the section called “ROSA 傳統帳戶政策”及the section called “ROSA 傳統運算子政策”。

允許使用者檢視他們自己的許可

此範例示範如何建立政策， IAM 使用者 允許 檢視連接至其使用者身分的內嵌和受管政策。此政策包含在主控台或使用 以程式設計方式完成此動作的許可 AWS CLI。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

ROSA 傳統帳戶政策

本節提供 ROSA classic 所需的帳戶政策詳細資訊。ROSA classic 需要這些許可，才能管理叢集執行的資源 AWS ，並啟用叢集的 Red Hat 網站可靠性工程師支援。您可以指派自訂字首給政策名稱，但這些政策應如此頁面所定義命名（例如 `ManagedOpenShift-Installer-Role-Policy`)。

帳戶政策專屬於 OpenShift 次要發行版本，且可回溯相容。在建立或升級叢集之前，您應該執行 來驗證政策版本和叢集版本是否相同`rosa list account-roles`。如果政策版本低於叢集版本，請執行 `rosa upgrade account-roles` 來升級角色和連接的政策。您可以針對相同次要發行版本的多個叢集使用相同的帳戶政策和角色。

【字首】-Installer-Role-Policy

您可以將 `[Prefix]-Installer-Role-Policy` 連接到 IAM 實體。您必須先將此政策連接至名為的 IAM 角色，才能建立 ROSA 傳統叢集`[Prefix]-Installer-Role`。此政策會授予必要的許可，讓 ROSA 安裝程式管理建立叢集所需的 AWS 資源。

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:AssociateDhcpOptions",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CopyImage",
                "ec2:CreateDhcpOptions",
                "ec2:CreateInternetGateway",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteDhcpOptions",
                "ec2:DeleteInternetGateway",
                "ec2:DeleteNatGateway",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteSubnet",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeleteVpc",
                "ec2:DeleteVpcEndpoints",
```

```
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:DetachInternetGateway",
                "ec2:DisassociateRouteTable",
                "ec2:GetConsoleOutput",
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVpcAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RunInstances",
```

```
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:GetInstanceProfile",
                "iam:TagInstanceProfile",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:ListInstanceProfiles",
                "iam:ListInstanceProfilesForRole",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:ListUserPolicies",
```

```
                "iam:ListUsers",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:SimulatePrincipalPolicy",
                "iam:TagRole",
                "iam:UntagRole",
                "route53:ChangeResourceRecordSets",
                "route53:ChangeTagsForResource",
                "route53:CreateHostedZone",
                "route53:DeleteHostedZone",
                "route53:GetAccountLimit",
                "route53:GetChange",
                "route53:GetHostedZone",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53:ListTagsForResource",
                "route53:UpdateHostedZoneComment",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketAcl",
                "s3:GetBucketCORS",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketReplication",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
```

```
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListAWSDefaultServiceQuotas",
                "sts:AssumeRole",
                "sts:AssumeRoleWithWebIdentity",
                "sts:GetCallerIdentity",
                "tag:GetResources",
                "tag:UntagResources",
                "ec2:CreateVpcEndpointServiceConfiguration",
                "ec2:DeleteVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:ModifyVpcEndpointServicePermissions",
                "kms:DescribeKey",
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/red-hat-managed": "true"
                }
            }
        }
    ]
}
```

【字首】-ControlPlane-Role-Policy

您可以將 `[Prefix]-ControlPlane-Role-Policy` 連接到 IAM 實體。您必須先將此政策連接至名為 的 IAM 角色，才能建立 ROSA 傳統叢集`[Prefix]-ControlPlane-Role`。此政策會將必要的許

可授予 ROSA classic，以管理託管 ROSA 控制平面的 Amazon EC2 和 Elastic Load Balancing 資源，以及讀取 KMS keys。

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteVolume",
                "ec2:Describe*",
                "ec2:DetachVolume",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifyVolume",
                "ec2:RevokeSecurityGroupIngress",
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:AttachLoadBalancerToSubnets",
                "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerPolicy",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateTargetGroup",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteLoadBalancer",
                "elasticloadbalancing:DeleteLoadBalancerListeners",
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:Describe*",
                "elasticloadbalancing:DetachLoadBalancerFromSubnets",
                "elasticloadbalancing:ModifyListener",
                "elasticloadbalancing:ModifyLoadBalancerAttributes",
                "elasticloadbalancing:ModifyTargetGroup",
```

```
                "elasticloadbalancing:ModifyTargetGroupAttributes",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
                "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

【字首】-Worker-Role-Policy

您可以將 `[Prefix]-Worker-Role-Policy` 連接到 IAM 實體。您必須先將此政策連接至名為 的 IAM 角色，才能建立 ROSA 傳統叢集`[Prefix]-Worker-Role`。此政策會將必要的許可授予 ROSA classic，以描述做為工作者節點執行的 EC2 執行個體。

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

【字首】-Support-Role-Policy

您可以將 `[Prefix]-Support-Role-Policy` 連接到 IAM 實體。您必須先將此政策連接至名為 的 IAM 角色，才能建立 ROSA 傳統叢集`[Prefix]-Support-Role`。此政策授予 Red Hat 網站可靠性工程所需的許可，以觀察、診斷和支援 ROSA 傳統叢集使用 AWS 的資源，包括變更叢集節點狀態的能力。

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:LookupEvents",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:CopySnapshot",
                "ec2:CreateNetworkInsightsPath",
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:CreateTags",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:DeleteTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAddressesAttribute",
                "ec2:DescribeAggregateIdFormat",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeByoipCidrs",
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeCarrierGateways",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeCoipPools",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeIdentityIdFormat",
                "ec2:DescribeIdFormat",
```

```
                "ec2:DescribeImageAttribute",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeIpv6Pools",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLocalGatewayRouteTables",
                "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
                "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
                "ec2:DescribeLocalGateways",
                "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
                "ec2:DescribeLocalGatewayVirtualInterfaces",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInsightsAnalyses",
                "ec2:DescribeNetworkInsightsPaths",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePlacementGroups",
                "ec2:DescribePrefixLists",
                "ec2:DescribePrincipalIdFormat",
                "ec2:DescribePublicIpv4Pools",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeRouteTables",
                "ec2:DescribeScheduledInstances",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshotAttribute",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGatewayAttachments",
                "ec2:DescribeTransitGatewayConnectPeers",
                "ec2:DescribeTransitGatewayConnects",
                "ec2:DescribeTransitGatewayMulticastDomains",
```

```
                "ec2:DescribeTransitGatewayPeeringAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeVolumeAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetAssociatedIpv6PoolCidrs",
                "ec2:GetConsoleOutput",
                "ec2:GetManagedPrefixListEntries",
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:GetTransitGatewayAttachmentPropagations",
                "ec2:GetTransitGatewayMulticastDomainAssociations",
                "ec2:GetTransitGatewayPrefixListReferences",
                "ec2:GetTransitGatewayRouteTableAssociations",
                "ec2:GetTransitGatewayRouteTablePropagations",
                "ec2:ModifyInstanceAttribute",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:SearchLocalGatewayRoutes",
                "ec2:SearchTransitGatewayMulticastGroups",
                "ec2:SearchTransitGatewayRoutes",
                "ec2:StartInstances",
                "ec2:StartNetworkInsightsAnalysis",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:ConfigureHealthCheck",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListenerCertificates",
```

```
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeRules",
                "elasticloadbalancing:DescribeSSLPolicies",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroupAttributes",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GetRole",
                "iam:ListRoles",
                "kms:CreateGrant",
                "route53:GetHostedZone",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "s3:GetBucketTagging",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListAllMyBuckets",
                "sts:DecodeAuthorizationMessage",
                "tiros:CreateQuery",
                "tiros:GetQueryAnswer",
                "tiros:GetQueryExplanation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::managed-velero*",
                "arn:aws:s3:::*image-registry*"
            ]
        }
    ]
}
```

ROSA 傳統運算子政策

本節提供 ROSA 傳統所需的運算子政策詳細資訊。您必須先將這些政策連接到相關的運算子角色，才能建立 ROSA 傳統叢集。每個叢集都需要一組唯一的運算子角色。

需要這些許可才能允許 OpenShift 運算子管理 ROSA 傳統叢集節點。您可以將自訂字首指派給政策名稱，以簡化政策管理（例如 `ManagedOpenShift-openshift-ingress-operator-cloud-credentials`)。

【字首】-openshift-ingress-operator-cloud-credentials

您可以將 `[Prefix]-openshift-ingress-operator-cloud-credentials` 連接到 IAM 實體。此政策會將必要的許可授予輸入運算子，以佈建和管理負載平衡器和 DNS 組態以進行外部叢集存取。此政策也允許輸入運算子讀取和篩選 Route 53 資源標籤值，以探索託管區域。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的 OpenShift 傳入運算子。 OpenShift GitHub

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "elasticloadbalancing:DescribeLoadBalancers",
                "route53:ListHostedZones",
                "route53:ListTagsForResources",
                "route53:ChangeResourceRecordSets",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

【字首】-openshift-cluster-csi-drivers-ebs-cloud-credentials

您可以將 `[Prefix]-openshift-cluster-csi-drivers-ebs-cloud-credentials` 連接到 IAM 實體。此政策授予 Amazon EBS CSI Driver Operator 在 ROSA 傳統叢集上安裝和維護 Amazon

EBS CSI 驅動程式所需的許可。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的 aws-ebs-csi-driver-operator。

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateSnapshot",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeSnapshots",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumesModifications",
                "ec2:DetachVolume",
                "ec2:EnableFastSnapshotRestores",
                "ec2:ModifyVolume"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

【字首】-openshift-machine-api-aws-cloud-credentials

您可以將 `[Prefix]-openshift-machine-api-aws-cloud-credentials` 連接到 IAM 實體。此政策會將必要的許可授予 Machine Config Operator，以描述、執行和終止以工作者節點管理的 Amazon EC2 執行個體。此政策也授予許可，允許使用 對工作者節點根磁碟區進行磁碟加密 AWS KMS keys。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的 machine-config-operator。

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:DescribeKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
```

```
        {
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

【字首】-openshift-cloud-credential-operator-cloud-credentials

您可以將 `[Prefix]-openshift-cloud-credential-operator-cloud-credentials` 連接到 IAM 實體。此政策授予 Cloud Credential Operator 擷取 IAM 使用者 詳細資訊的必要許可，包括存取金鑰 IDs、連接的內嵌政策文件、使用者的建立日期、路徑、使用者 ID 和 Amazon Resource Name (ARN)。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的 cloud-credential-operator。

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetUser",
                "iam:GetUserPolicy",
                "iam:ListAccessKeys"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

【字首】-openshift-image-registry-installer-cloud-credentials

您可以將 `[Prefix]-openshift-image-registry-installer-cloud-credentials` 連接到 IAM 實體。此政策會將必要的許可授予映像登錄運算子，以佈建和管理 ROSA Classic 叢集內映像登錄檔和相依服務的資源，包括 Amazon S3。這是必要的，以便運算子可以安裝和維護 ROSA 傳統叢集的內部登錄檔。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的映像登錄運算子。

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketTagging",
                "s3:GetBucketTagging",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucketMultipartUploads",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

【字首】-openshift-cloud-network-config-controller-cloud-cr

您可以將 `[Prefix]-openshift-cloud-network-config-controller-cloud-cr` 連接到 IAM 實體。此政策會將必要的許可授予 Cloud Network Config Controller Operator，以佈建和管理供 ROSA 傳統叢集聯網浮水印使用的聯網資源。運算子使用這些許可來管理 Amazon EC2 執行個體的私有 IP 地址，做為 ROSA 傳統叢集的一部分。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的 Cloud-network-config-controller。

許可政策

此政策文件中定義的許可會指定允許或拒絕哪些動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignIpv6Addresses",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 的 受管政策 ROSA

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可供現有 服務使用時， AWS 最有可能更新 AWS 受管政策。如需詳細資訊，請參閱 IAM 《使用者指南》中的 AWS 受管政策。

AWS 受管政策：ROSAManageSubscription

您可以將`ROSAManageSubscription`政策連接至 IAM 實體。在 ROSA 主控台 ROSA 中 AWS 啟用之前，您必須先將此政策連接至主控台角色。

此政策會授予您管理 ROSA 訂閱所需的 AWS Marketplace 許可。

許可詳細資訊

此政策包含以下許可。

- `aws-marketplace:Subscribe` - 准許訂閱 AWS Marketplace 產品 ROSA。
- `aws-marketplace:Unsubscribe` - 允許主體移除 AWS Marketplace 產品的訂閱。
- `aws-marketplace:ViewSubscriptions` - 允許主體從中檢視訂閱 AWS Marketplace。這是必要的，以便 IAM 委託人可以檢視可用的 AWS Marketplace 訂閱。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSAManageSubscription。

具有 HCP 帳戶政策的 ROSA

本節提供具有託管控制平面 (HCP) 的 ROSA 所需的帳戶政策詳細資訊。這些 AWS 受管政策會新增 ROSA 搭配 HCP IAM 角色使用的許可。Red Hat 網站可靠性工程 (SRE) 技術支援、叢集安裝以及控制平面和運算功能需要 許可。

> **Note**
>
> AWS 受管政策旨在供 ROSA 搭配託管控制平面 (HCP) 使用。ROSA 傳統叢集使用客戶受管 IAM 政策。如需 ROSA 傳統政策的詳細資訊，請參閱 the section called “ROSA 傳統帳戶政策”和 the section called “ROSA 傳統運算子政策”。

AWS 受管政策：ROSAWorkerInstancePolicy

您可以將 `ROSAWorkerInstancePolicy`連接到您的 IAM 實體。建立叢集之前，您必須連接具有此政策的 ROSA 工作者 IAM 角色。ROSA 服務 AWS 服務 會代表您呼叫其他 。他們會這樣做來管理您用於每個叢集的資源。

許可詳細資訊

此政策包含下列許可，允許 ROSA 工作者節點完成下列任務：

- `ec2` — 在 ROSA 叢集工作者節點生命週期管理中評估 AWS 區域 和 Amazon EC2 執行個體詳細資訊。
- `ecr` - 評估並從 ROSA 管理的 ECR 儲存庫取得叢集安裝和工作者節點生命週期管理所需的映像。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSAWorkerInstancePolicy。

AWS 受管政策：ROSASRESupportPolicy

您可以將 `ROSASRESupportPolicy` 連接到 IAM 實體。

使用託管控制平面叢集建立 ROSA 之前，您必須先將此政策連接至支援 IAM 角色。此政策會將必要的許可授予 Red Hat 網站可靠性工程師 (SREs)，以直接觀察、診斷和支援與 ROSA 叢集相關聯的 AWS 資源，包括變更 ROSA 叢集節點狀態的能力。

許可詳細資訊

此政策包含下列許可，允許 Red Hat SREs完成下列任務：

- `cloudtrail` — 讀取與叢集相關的 AWS CloudTrail 事件和線索。
- `cloudwatch` — 讀取與叢集相關的 Amazon CloudWatch 指標。
- `ec2` — 讀取、描述和檢閱與叢集運作狀態相關的 Amazon EC2 元件，例如安全群組、VPC 端點連線和磁碟區狀態。啟動、停止、重新啟動和終止 Amazon EC2 執行個體。
- `elasticloadbalancing` — 讀取、描述和檢閱與叢集運作狀態相關的 Elastic Load Balancing 參數。
- `iam` — 評估與叢集運作狀態相關的 IAM 角色。
- `route53` — 檢閱與叢集運作狀態相關的 DNS 設定。

- `sts` — `DecodeAuthorizationMessage` — 讀取 IAM 訊息以進行除錯。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSASRESupportPolicy。

AWS 受管政策：ROSAInstallerPolicy

您可以將 `ROSAInstallerPolicy`連接到您的 IAM 實體。

使用託管控制平面叢集建立 ROSA 之前，您必須先將此政策連接至名為 的 IAM 角色`[Prefix]-ROSA-Worker-Role`。此政策允許實體將遵循 `[Prefix]-ROSA-Worker-Role` 模式的任何角色新增至執行個體描述檔。此政策會將必要的許可授予安裝程式，以管理支援 ROSA 叢集安裝 AWS 的資源。

許可詳細資訊

此政策包含下列許可，允許安裝程式完成下列任務：

- `ec2` — 使用 Red Hat AWS 帳戶 擁有和管理之 中託管AMIs 執行 Amazon EC2 執行個體。描述與 Amazon EC2 節點相關聯的 Amazon EC2 執行個體、磁碟區和網路資源。需要此許可，Kubernetes 控制平面才能將執行個體加入叢集，而叢集可以評估其在其中的存在 Amazon VPC。使用符合 的標籤索引鍵來標記子網路`"kubernetes.io/cluster/*"`。這是必要的，以確保用於叢集傳入的負載平衡器僅在適用的子網路中建立。
- `elasticloadbalancing` — 將負載平衡器新增至叢集上的目標節點。從叢集上的目標節點移除負載平衡器。需要此許可，以便 Kubernetes 控制平面可以動態佈建 Kubernetes 服務和 OpenShift 應用程式服務請求的負載平衡器。
- `kms` — 讀取 AWS KMS 金鑰、建立和管理授予 Amazon EC2，並傳回唯一的對稱資料金鑰以供 外部使用 AWS KMS。在叢集建立時啟用加密時，這是使用`etcd`加密`etcd`資料的必要項目。
- `iam` — 驗證 IAM 角色和政策。動態佈建和管理與叢集相關的 Amazon EC2 執行個體描述檔。使用`iam:TagInstanceProfile`許可將標籤新增至 IAM 執行個體描述檔。當叢集安裝因缺少客戶指定的叢集 OIDC 供應商而失敗時，提供安裝程式錯誤訊息。
- `route53` — 管理建立叢集所需的 Route 53 資源。
- `servicequotas` — 評估建立叢集所需的服務配額。
- `sts` — 建立 ROSA 元件的臨時 AWS STS 登入資料。擔任用於建立叢集的登入資料。
- `secretsmanager` — 讀取秘密值，以安全地允許客戶受管的 OIDC 組態做為叢集佈建的一部分。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSAInstallerPolicy。

具有 HCP 運算子政策的 ROSA

本節提供有關具有託管控制平面 (HCP) 的 ROSA 所需的運算子政策的詳細資訊。您可以將這些 AWS 受管政策連接到搭配 HCP 使用 ROSA 所需的運算子角色。需要許可才能允許 OpenShift 運算子使用 HCP 叢集節點管理 ROSA。

> **Note**
>
> AWS 受管政策旨在供 ROSA 搭配託管控制平面 (HCP) 使用。ROSA 傳統叢集使用客戶受管 IAM 政策。如需 ROSA 傳統政策的詳細資訊，請參閱 the section called “ROSA 傳統帳戶政策”和 the section called “ROSA 傳統運算子政策”。

AWS 受管政策：ROSAAmazonEBSCSIDriverOperatorPolicy

您可以將 `ROSAAmazonEBSCSIDriverOperatorPolicy`連接到您的 IAM 實體。您必須將此政策連接至運算子 IAM 角色，以允許具有託管控制平面叢集的 ROSA 呼叫其他 AWS 服務。每個叢集都需要一組唯一的運算子角色。

此政策會將必要的許可授予 Amazon EBS CSI Driver Operator，以在 ROSA 叢集上安裝和維護 Amazon EBS CSI 驅動程式。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的 aws-ebs-csi-driver 運算子。

許可詳細資訊

此政策包含下列許可，允許 Amazon EBS Driver Operator 完成下列任務：

- `ec2` — 建立、修改、連接、分離和刪除連接到 Amazon EC2 執行個體的 Amazon EBS 磁碟區。建立和刪除 Amazon EBS 磁碟區快照，並列出 Amazon EC2 執行個體、磁碟區和快照。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSAAmazonEBSCSIDriverOperatorPolicy。

AWS 受管政策：ROSAIngressOperatorPolicy

您可以將 `ROSAIngressOperatorPolicy`連接到您的 IAM 實體。您必須將此政策連接至運算子 IAM 角色，以允許具有託管控制平面叢集的 ROSA 呼叫其他 AWS 服務。每個叢集都需要一組唯一的運算子角色。

此政策會將必要的許可授予輸入運算子，以佈建和管理 ROSA 叢集的負載平衡器和 DNS 組態。此政策允許讀取標籤值。然後，運算子會篩選 Route 53 資源的標籤值，以探索託管區域。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的 OpenShift 傳入運算子。 OpenShift GitHub

許可詳細資訊

此政策包含下列許可，允許輸入運算子完成下列任務：

- `elasticloadbalancing` — 描述佈建負載平衡器的狀態。
- `route53` — 列出 Route 53 託管區域，並編輯管理由 ROSA 叢集控制之 DNS 的記錄。
- `tag` — 使用 `tag:GetResources`許可管理標記的資源。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSAIngressOperatorPolicy。

AWS 受管政策：ROSAImageRegistryOperatorPolicy

您可以將 `ROSAImageRegistryOperatorPolicy`連接到您的 IAM 實體。您必須將此政策連接至運算子 IAM 角色，以允許具有託管控制平面叢集的 ROSA 呼叫其他 AWS 服務。每個叢集都需要一組唯一的運算子角色。

此政策會將必要的許可授予映像登錄運算子，以佈建和管理叢集 ROSA 內映像登錄檔和相依服務的資源，包括 S3。這是必要的，以便運算子可以安裝和維護 ROSA 叢集的內部登錄檔。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的映像登錄運算子。

許可詳細資訊

此政策包含下列許可，允許 Image Registry Operator 完成下列動作：

- `s3` — 管理和評估 Amazon S3 儲存貯體作為容器映像內容和叢集中繼資料的持久性儲存。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSAImageRegistryOperatorPolicy。

AWS 受管政策：ROSACloudNetworkConfigOperatorPolicy

您可以將 `ROSACloudNetworkConfigOperatorPolicy`連接到您的 IAM 實體。您必須將此政策連接至運算子 IAM 角色，以允許具有託管控制平面叢集的 ROSA 呼叫其他 AWS 服務。每個叢集都需要一組唯一的運算子角色。

此政策會將必要的許可授予 Cloud Network Config Controller Operator，以佈建和管理 ROSA 叢集聯網浮水印的聯網資源。運算子使用這些許可來管理 Amazon EC2 執行個體的私有 IP 地址，做為 ROSA 叢集的一部分。如需 運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的 Cloud-network-config-controller。

許可詳細資訊

此政策包含下列許可，允許 Cloud Network Config Controller Operator 完成下列任務：

- `ec2` — 讀取、指派和描述用於連接 ROSA 叢集中 Amazon EC2 執行個體、 Amazon VPC 子網路和彈性網路介面的組態。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSACloudNetworkConfigOperatorPolicy。

AWS 受管政策：ROSAKubeControllerPolicy

您可以將 `ROSAKubeControllerPolicy`連接到您的 IAM 實體。您必須將此政策連接至運算子 IAM 角色，以允許具有託管控制平面叢集的 ROSA 呼叫其他 AWS 服務。每個叢集都需要一組唯一的運算子角色。

此政策會授予 kube 控制器管理所需的許可 Amazon EC2 Elastic Load Balancing，以及具有託管控制平面叢集之 ROSA AWS KMS 的資源。如需此控制器的詳細資訊，請參閱 OpenShift 文件中的控制器架構。

許可詳細資訊

此政策包含下列許可，允許 kube 控制器完成下列任務：

- `ec2` — 建立、刪除標籤，並將標籤新增至 Amazon EC2 執行個體安全群組。將傳入規則新增至安全群組。描述可用區域、 Amazon EC2 執行個體、路由表、安全群組、VPCs和子網路。
- `elasticloadbalancing` — 建立和管理負載平衡器及其政策。建立和管理負載平衡器接聽程式。向目標群組註冊目標，並管理目標群組。向負載平衡器註冊和取消註冊 Amazon EC2 執行個體，並將標籤新增至負載平衡器。
- `kms` — 擷取 AWS KMS 金鑰的詳細資訊。在叢集建立時啟用加密時，這是使用`etcd`加密`etcd`資料的必要項目。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSAKubeControllerPolicy。

AWS 受管政策：ROSANodePoolManagementPolicy

您可以將 `ROSANodePoolManagementPolicy`連接到您的 IAM 實體。您必須將此政策連接至運算子 IAM 角色，以允許具有託管控制平面叢集的 ROSA 呼叫其他 AWS 服務。每個叢集都需要一組唯一的運算子角色。

此政策會將必要的許可授予 NodePool 控制器，以描述、執行和終止以工作者節點身分管理的 Amazon EC2 執行個體。此政策也授予許可，以允許使用 AWS KMS 金鑰對工作者節點根磁碟區進行磁碟加密，並標記連接至工作者節點的彈性網路界面。如需此控制器的詳細資訊，請參閱 OpenShift 文件中的控制器架構。

許可詳細資訊

此政策包含下列許可，允許 NodePool 控制器完成下列任務：

- `ec2` — 使用 Red Hat AWS 帳戶 擁有和管理的 中託管AMIs 執行 Amazon EC2 執行個體。在 ROSA 叢集中管理 EC2 生命週期。動態建立並整合工作者節點與 Elastic Load Balancing、 Amazon VPC Route 53 Amazon EBS、 和 Amazon EC2。
- `iam` — Elastic Load Balancing 透過名為 的服務連結角色使用 `AWSServiceRoleForElasticLoadBalancing`。將角色指派給 Amazon EC2 執行個體描述檔。
- `kms` — 讀取 AWS KMS 金鑰、建立和管理授予 Amazon EC2，並傳回唯一的對稱資料金鑰以供 外部使用 AWS KMS。這是允許工作者節點根磁碟區的磁碟加密的必要項目。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSANodePoolManagementPolicy。

AWS 受管政策：ROSAKMSProviderPolicy

您可以將 `ROSAKMSProviderPolicy`連接到您的 IAM 實體。您必須將此政策連接至運算子 IAM 角色，以允許具有託管控制平面叢集的 ROSA 呼叫其他 AWS 服務。每個叢集都需要一組唯一的運算子角色。

此政策會將必要的許可授予內建 AWS 加密提供者，以管理支援`etcd`資料加密的 AWS KMS 金鑰。此政策允許 Amazon EC2 使用 AWS 加密提供者提供的 KMS 金鑰來加密和解密`etcd`資料。如需此提供者的詳細資訊，請參閱 Kubernetes GitHub 文件中的AWS 加密提供者。

許可詳細資訊

此政策包含下列許可，允許 AWS 加密提供者完成下列任務：

- `kms` — 加密、解密和擷取 AWS KMS 金鑰。在叢集建立時啟用加密時，這是使用`etcd`加密`etcd`資料的必要項目。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSAKMSProviderPolicy。

AWS 受管政策：ROSAControlPlaneOperatorPolicy

您可以將 `ROSAControlPlaneOperatorPolicy`連接到您的 IAM 實體。您必須將此政策連接至運算子 IAM 角色，以允許具有託管控制平面叢集的 ROSA 呼叫其他 AWS 服務。每個叢集都需要一組唯一的運算子角色。

此政策會授予控制平面運算子所需的許可，以使用託管控制平面叢集來管理 ROSA 的 Route 53 Amazon EC2 和資源。如需此運算子的詳細資訊，請參閱 OpenShift 文件中的控制器架構。

許可詳細資訊

此政策包含下列許可，允許控制平面運算子完成下列任務：

- `ec2` — 建立和管理 Amazon VPC 端點。
- `route53` — 列出和變更 Route 53 記錄集，並列出託管區域。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ROSAControlPlaneOperatorPolicy。

ROSAAWS 受管政策的更新

檢視自此服務開始追蹤這些變更 ROSA 以來， AWS 受管政策更新的詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 文件歷史紀錄 頁面的 RSS 摘要。

變更	描述	日期
ROSAImageRegistryOperatorPolicy — 已更新政策	ROSA 已更新政策，將許可範圍縮小至 S3 儲存貯體資源層級。此變更同時符合 AWS 商業和 GovCloud 區域的 ROSA 儲存需求。如需詳細資訊，請參閱 the section called “AWS	2025 年 5 月 19 日

變更	描述	日期
	受管政策：ROSAImageRegistryOperatorPolicy”。	
ROSANodePoolManagementPolicy — 政策已更新	ROSA 已更新政策，以允許標記連接到工作者節點的彈性網路界面。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSANodePoolManagementPolicy”。	2025 年 5 月 5 日
ROSAImageRegistryOperatorPolicy — 已更新政策	ROSA 已更新政策，以允許 Red Hat OpenShift Image Registry Operator 在 AWS GovCloud 區域中佈建和管理 Amazon S3 儲存貯體和物件，以供 ROSA 叢集內映像登錄使用。此變更符合 AWS GovCloud 區域的 ROSA 儲存需求。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAImageRegistryOperatorPolicy”。	2025 年 4 月 16 日
ROSAWorkerInstancePolicy — 政策已更新	ROSA 已更新政策，允許工作者節點評估並從 ROSA 管理的 ECR 儲存庫取得叢集安裝和工作者節點生命週期管理所需的映像。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAWorkerInstancePolicy”。	2025 年 3 月 3 日

變更	描述	日期
ROSANodePoolManagementPolicy — 政策已更新	ROSA 已更新政策，允許僅在請求包含標籤 時，才在 ec2：RunInstances 呼叫期間類似 EC2 執行個體地標記彈性網路介面`red-hat-managed: true`。這些許可是使用 HCP 4.17 叢集支援 ROSA 的必要許可。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSANodePoolManagementPolicy”。	2025 年 2 月 24 日
ROSAAmazonEBSCSIDriverOperatorPolicy — 政策已更新	ROSA 已更新政策以支援新的 Amazon EBS 快照授權 API。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAAmazonEBSCSIDriverOperatorPolicy”。	2025 年 1 月 17 日
ROSANodePoolManagementPolicy — 政策已更新	ROSA 已更新政策，允許 ROSA 節點集區管理員描述 DHCP 選項集，以設定適當的私有 DNS 名稱。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSANodePoolManagementPolicy”。	2024 年 5 月 2 日

變更	描述	日期
ROSAInstallerPolicy — 政策已更新	ROSA 已更新政策，以允許 ROSA 安裝程式使用符合的標籤金鑰將標籤新增至子網路`"kubernetes.io/cluster/*"` 。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSA InstallerPolicy”。	2024 年 4 月 24 日
ROSASRESupportPolicy — 政策已更新	ROSA 已更新政策，以允許 SRE 角色擷取已標記為 ROSA 之執行個體描述檔的相關資訊`red-hat-managed` 。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSA SRESupportPolicy”。	2024 年 4 月 10 日
ROSAInstallerPolicy — 政策已更新	ROSA 已更新政策，以允許 ROSA 安裝程式驗證 的 AWS 受管政策 ROSA 是否連接到使用 IAM 的角色 ROSA。此更新還允許安裝程式識別客戶受管政策是否已連接到 ROSA 角色。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAInstallerPolicy”。	2024 年 4 月 10 日

變更	描述	日期
ROSAInstallerPolicy — 政策已更新	ROSA 已更新政策，允許服務在叢集安裝因缺少客戶指定的叢集 OIDC 供應商而失敗時提供安裝程式提醒訊息。此更新也允許服務擷取現有的 DNS 名稱伺服器，讓叢集佈建操作具有等冪性。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSA InstallerPolicy”。	2024 年 1 月 26 日
ROSASRESupportPolicy — 政策已更新	ROSA 已更新政策，以允許服務使用 DescribeSecurityGroups API 在安全群組上執行讀取操作。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSASRESupportPolicy”。	2024 年 1 月 22 日
ROSAImageRegistryOperatorPolicy — 已更新政策	ROSA 已更新政策，以允許映像登錄運算子對 14 個字元名稱區域中的 Amazon S3 儲存貯體採取動作。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSA ImageRegistryOperatorPolicy”。	2023 年 12 月 12 日

變更	描述	日期
ROSAKubeControllerPolicy — 政策已更新	ROSA 已更新政策，以允許 kube-controller-manager 描述可用區域、 Amazon EC2 執行個體、路由表、安全群組、VPCs和子網路。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSA KubeControllerPolicy”。	2023 年 10 月 16 日
ROSAManageSubscription — 已更新政策	ROSA 已更新政策，新增具有託管控制平面 ProductId 的 ROSA。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAManageSubscription”。	2023 年 8 月 1 日
ROSAKubeControllerPolicy — 政策已更新	ROSA 已更新政策，以允許 kube-controller-manager 將 Network Load Balancer 建立為 Kubernetes 服務負載平衡器。Network Load Balancer 提供更大的能力來處理揮發性工作負載，並支援負載平衡器的靜態 IP 地址。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSA KubeControllerPolicy”。	2023 年 7 月 13 日

變更	描述	日期
ROSANodePoolManagementPolicy — 新增的政策	ROSA 新增了新的政策，以允許 NodePool 控制器描述、執行和終止以工作者節點管理的 Amazon EC2 執行個體。此政策也會使用 AWS KMS 金鑰啟用工作者節點根磁碟區的磁碟加密。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSANodePoolManagementPolicy”。	2023 年 6 月 8 日
ROSAInstallerPolicy — 新增的政策	ROSA 新增了新的政策，以允許安裝程式管理支援叢集安裝 AWS 的資源。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAInstallerPolicy”。	2023 年 6 月 6 日
ROSASRESupportPolicy — 新增的政策	ROSA 新增了新的政策，以允許 Red Hat SREs直接觀察、診斷和支援與 ROSA 叢集相關聯的 AWS 資源，包括變更 ROSA 叢集節點狀態的能力。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSASRESupportPolicy”。	2023 年 6 月 1 日
ROSAKMSProviderPolicy — 新增政策	ROSA 新增了新的政策，以允許內建 AWS 加密提供者管理 AWS KMS 金鑰以支援加密的資料加密。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAKMSProviderPolicy”。	2023 年 4 月 27 日

變更	描述	日期
ROSAKubeControllerPolicy — 新增政策	ROSA 新增了新的政策，以允許 kube 控制器管理 Elastic Load Balancing Amazon EC2，以及 ROSA 具有託管控制平面叢集之 的 AWS KMS 資源。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAKubeControllerPolicy”。	2023 年 4 月 27 日
ROSAImageRegistryOperatorPolicy — 新增了新政策	ROSA 新增了新的政策，以允許映像登錄運算子佈建和管理叢集 ROSA 內映像登錄和相依服務的資源，包括 S3。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAImageRegistryOperatorPolicy”。	2023 年 4 月 27 日
ROSAControlPlaneOperatorPolicy — 新增政策	ROSA 新增了新的政策，以允許控制平面運算子 ROSA 使用託管控制平面叢集管理 的 Route 53 Amazon EC2 和資源。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAControlPlaneOperatorPolicy”。	2023 年 4 月 24 日

變更	描述	日期
ROSACloudNetworkConfigOperatorPolicy — 新增了新政策	ROSA 新增了新的政策，以允許 Cloud Network Config Controller Operator 佈建和管理 ROSA 叢集聯網浮水印的聯網資源。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSACloudNetworkConfigOperatorPolicy”。	2023 年 4 月 20 日
ROSAIngressOperatorPolicy — 新增政策	ROSA 新增了新的政策，以允許輸入運算子佈建和管理 ROSA 叢集的負載平衡器和 DNS 組態。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAIngressOperatorPolicy”。	2023 年 4 月 20 日
ROSAAmazonEBSCSIDriverOperatorPolicy — 新增政策	ROSA 新增了新的政策，以允許 Amazon EBS CSI Driver Operator 在 ROSA 叢集上安裝和維護 Amazon EBS CSI 驅動程式。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAAmazonEBSCSIDriverOperatorPolicy”。	2023 年 4 月 20 日
ROSAWorkerInstancePolicy — 新增政策	ROSA 新增了新的政策，以允許服務管理叢集資源。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSAWorkerInstancePolicy”。	2023 年 4 月 20 日

變更	描述	日期
ROSAManageSubscription — 新增的政策	ROSA 新增了新的政策，以授予管理 ROSA 訂閱所需的 AWS Marketplace 許可。如需詳細資訊，請參閱 the section called “AWS 受管政策：ROSA ManageSubscription”。	2022 年 4 月 11 日
Red Hat OpenShift Service on AWS 開始追蹤變更	Red Hat OpenShift Service on AWS 已開始追蹤其 AWS 受管政策的變更。	2022 年 3 月 2 日

對 ROSA 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 ROSA 和 時可能遇到的常見問題 IAM。

AWS Organizations 服務控制政策拒絕必要的 AWS Marketplace 許可

如果您的 AWS Organizations 服務控制政策 (SCP) 在嘗試啟用時不允許必要的 AWS Marketplace 訂閱許可 ROSA，會發生下列主控台錯誤。

```
An error occurred while enabling ROSA, because a service control policy (SCP) is
 denying required permissions. Contact your management account administrator, and
 consult the documentation for troubleshooting.
```

如果您收到此錯誤，則必須聯絡管理員尋求協助。您的管理員是管理您組織帳戶的人員。請該人員執行下列動作：

1. 設定 SCP 以允許 `aws-marketplace:Subscribe`、 `aws-marketplace:Unsubscribe`和 `aws-marketplace:ViewSubscriptions`許可。如需詳細資訊，請參閱 AWS Organizations《 使用者指南》中的更新 SCP。
2. ROSA 在組織的管理帳戶中啟用 。
3. 將 ROSA 訂閱分享給組織內需要存取的成員帳戶。如需詳細資訊，請參閱《 AWS Marketplace 買方指南》中的在組織中共用訂閱。

使用者或角色沒有必要的 AWS Marketplace 許可

如果您的 IAM 委託人在您嘗試啟用 時沒有必要的 AWS Marketplace 訂閱許可 ROSA，會發生下列主控台錯誤。

```
An error occurred while enabling ROSA, because your user or role does not have the
 required permissions.
```

若要解決此問題，請遵循這些步驟：

1. 前往 IAM 主控台，並將 AWS 受`ROSAManageSubscription`管政策連接至您的 IAM 身分。如需詳細資訊，請參閱《 AWS 受管政策參考指南》中的 ROSAManageSubscription。
2. 請遵循 the section called “啟用 ROSA 和設定 AWS 先決條件” 中的程序。

如果您沒有在 中檢視或更新許可集的許可， IAM 或您收到錯誤，則必須聯絡您的管理員尋求協助。要求該人員`ROSAManageSubscription`連接到 IAM 您的身分，並遵循 中的程序the section called “啟用 ROSA 和設定 AWS 先決條件”。當管理員執行此動作時，它會 ROSA 更新 下所有身分的許可集，以啟用 IAM AWS 帳戶。

管理員封鎖的必要 AWS Marketplace 許可

如果您的帳戶管理員封鎖必要的 AWS Marketplace 訂閱許可，當您嘗試啟用 時，會發生下列主控台錯誤 ROSA。

```
An error occurred while enabling ROSA because required permissions have been blocked by
 an administrator. ROSAManageSubscription includes the permissions required to enable
 ROSA. Consult the documentation and try again.
```

如果您收到此錯誤，則必須聯絡管理員尋求協助。請該人員執行下列動作：

1. 前往 ROSA 主控台，並將 AWS 受`ROSAManageSubscription`管政策連接至您的 IAM 身分。如需詳細資訊，請參閱《 AWS 受管政策參考指南》中的 ROSAManageSubscription。
2. 遵循 中的程序the section called “啟用 ROSA 和設定 AWS 先決條件”來啟用 ROSA。此程序 ROSA 會透過更新 下所有身分的許可集來啟用 IAM AWS 帳戶。

建立負載平衡器時發生錯誤：AccessDenied

如果您尚未建立負載平衡器，`AWSServiceRoleForElasticLoadBalacing`則服務連結角色可能不存在於您的帳戶中。如果您嘗試在帳戶中建立 叢集 沒有`AWSServiceRoleForElasticLoadBalacing`角色的 ， ROSA 會發生下列錯誤。

```
Error creating network Load Balancer: AccessDenied
```

若要解決此問題，請遵循這些步驟：

1. 檢查您的帳戶是否具有 `AWSServiceRoleForElasticLoadBalancing`角色。

   ```
   aws iam get-role --role-name "AWSServiceRoleForElasticLoadBalancing"
   ```

2. 如果您沒有此角色，請遵循 Elastic Load Balancing 《 使用者指南》中的建立服務連結角色中的指示來建立角色。

中的彈性 ROSA

AWS 全球基礎設施彈性

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些區域透過低延遲、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。

ROSA 為客戶提供在單一 AWS 可用區域中或跨多個可用區域執行 Kubernetes 控制平面和資料平面的選項。雖然單一可用區域叢集對於實驗很有用，但我們鼓勵客戶在多個可用區域中執行工作負載。這可確保應用程式甚至可以承受完整的可用區域故障，這是非常罕見的事件。

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。

ROSA 叢集彈性

ROSA 控制平面包含至少三個 OpenShift 控制平面節點。每個控制平面節點都由 API 伺服器執行個體、`etcd`執行個體和控制器組成。如果發生控制平面節點故障，所有 API 請求都會自動路由到其他可用的節點，以確保叢集可用性。

ROSA 資料平面至少包含兩個 OpenShift 基礎設施節點和兩個 OpenShift 工作者節點。基礎設施節點會執行支援 OpenShift 叢集基礎設施元件的 Pod，例如預設路由器、內建 OpenShift 登錄檔，以及叢集指標和監控的元件。OpenShift 工作者節點會執行最終使用者應用程式 Pod。

Red Hat 網站可靠性工程師 (SREs) 可完整管理控制平面和基礎設施節點。Red Hat SREs會主動監控 ROSA 叢集，並負責取代任何失敗的控制平面節點和基礎設施節點。如需詳細資訊，請參閱the section called “責任”。

> **Important**
>
> 由於 ROSA 是受管服務，Red Hat 負責管理 ROSA 所使用的基礎 AWS 基礎設施。客戶不應嘗試從 AWS 主控台或 手動關閉 ROSA 使用 的 Amazon EC2 執行個體 AWS CLI。此動作可能會導致客戶資料遺失。

如果資料平面上的工作者節點故障，控制平面會將未排程的 Pod 重新定位至正常運作的工作者節點（直到復原或取代故障的節點為止）。可以透過啟用叢集中機器的自動擴展來手動或自動取代失敗的工作者節點。如需詳細資訊，請參閱 Red Hat 文件中的叢集自動調整規模。

客戶部署的應用程式彈性

雖然 ROSA 提供許多保護以確保服務的高可用性，但客戶仍需負責建置其部署的應用程式以獲得高可用性，以保護工作負載免於停機。如需詳細資訊，請參閱 Red Hat 文件中的關於 的可用性 ROSA。

中的基礎設施安全 ROSA

作為受管服務， Red Hat OpenShift Service on AWS 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱AWS 雲端安全。若要使用基礎設施安全性的最佳實務設計您的 AWS 環境，請參閱安全支柱中的基礎設施保護：Well-Architected Framework。 AWS

您可以使用 AWS 發佈的 API 呼叫， ROSA 透過 AWS 網路存取 。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

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。

叢集網路隔離

Red Hat 網站可靠性工程師 (SREs) 負責叢集和基礎應用程式平台的持續管理和網路安全。如需 之 Red Hat 責任的詳細資訊 ROSA，請參閱 the section called “責任”。

當您建立新的叢集時， ROSA 會提供建立公有 Kubernetes API 伺服器端點和應用程式路由或私有 Kubernetes API 端點和應用程式路由的選項。此連線用於與您的叢集通訊 （使用 OpenShift 管理工具，例如 ROSA CLI 和 OpenShift CLI)。私有連線可讓節點與 API 伺服器之間的所有通訊保持在 VPC 內。如果您啟用 API 伺服器和應用程式路由的私有存取，您必須使用現有的 VPC 和 AWS PrivateLink ，將 VPC 連線至 OpenShift 後端服務。

Kubernetes API 伺服器存取是使用 AWS Identity and Access Management (IAM) 和原生 Kubernetes 角色型存取控制 (RBAC) 的組合進行保護。如需 Kubernetes RBAC 的詳細資訊，請參閱 Kubernetes 文件中的使用 RBAC 授權。

ROSA 可讓您使用多種類型的 TLS 終止來建立安全的應用程式路由，以將憑證提供給用戶端。如需詳細資訊，請參閱 Red Hat 文件中的安全路由。

如果您在現有的 VPC 中建立 ROSA 叢集，您可以指定叢集要使用的 VPC 子網路和可用區域。您也可以定義叢集網路要使用的 CIDR 範圍，並將這些 CIDR 範圍與 VPC 子網路配對。如需詳細資訊，請參閱 Red Hat 文件中的 CIDR 範圍定義。

對於使用公有 API 端點的叢集， ROSA 需要您的 VPC 針對您要部署叢集的每個可用區域設定公有和私有子網路。對於使用私有 API 端點的叢集，只需要私有子網路。

如果您使用的是現有的 VPC，您可以將 ROSA 叢集設定為在叢集建立期間或之後使用 HTTP 或 HTTPS 代理伺服器來加密叢集 Web 流量，為您的資料新增另一層安全性。當您啟用代理時，會拒絕核心叢集元件直接存取網際網路。代理不會拒絕使用者工作負載的網際網路存取。如需詳細資訊，請參閱 Red Hat 文件中的設定整個叢集的代理。

Pod 網路隔離

如果您是叢集管理員，您可以在 Pod 層級定義網路政策，將流量限制為 ROSA 叢集中的 Pod。

ROSA 服務配額

Red Hat OpenShift Service on AWS (ROSA) 使用 Amazon EC2 Amazon Virtual Private Cloud、Amazon Elastic Block Store和 的服務配額 Elastic Load Balancing 來佈建叢集。如需詳細資訊，請參閱 AWS 一般參考指南中的Red Hat OpenShift Service on AWS 端點和配額。

AWS 與 整合的 服務 ROSA

ROSA 與其他 合作 AWS 服務 ，為您的業務挑戰提供額外的解決方案。本主題識別使用 ROSA 來新增功能的 服務，或使用 ROSA 來執行任務的 服務。

主題

- ROSA 如何使用 AWS Marketplace

ROSA 如何使用 AWS Marketplace

AWS Marketplace 是精選的數位目錄，可用來尋找、購買、部署和管理第三方軟體、資料和服務，這些軟體、資料和服務是建置解決方案和執行業務時所需要的。 使用靈活的定價選項和多種部署方法，AWS Marketplace 簡化軟體授權和採購。

ROSA 使用 AWS Marketplace 進行服務計量和計費。ROSA Classic 是透過 AWS Marketplace 以 Amazon Machine Image (AMI) 為基礎的產品來計量和計費，而 ROSA 搭配託管控制平面 (HCP) 則是透過 AWS Marketplace 軟體即服務 (SaaS) 為基礎的產品來計量和計費。

此頁面說明如何 ROSA 使用 AWS Marketplace 處理付款、帳單、訂閱和合約購買。

術語

此頁面在討論 ROSA 與 的整合時，使用以下術語 AWS Marketplace。

Amazon Machine Image (AMI)

執行於 的伺服器映像，包括作業系統和其他軟體 AWS。

AMI 訂閱

在 中 AWS Marketplace，ROSA Classic 等以 AMI 為基礎的軟體產品會搭配年度訂閱定價模型，每小時使用 。每小時定價是預設定價模式，但您可以選擇預先購買一年的某個 Amazon EC2 執行個體類型的用量。

SaaS 訂閱

在 中 AWS Marketplace，ROSA 和 HCP 等software-as-a-service(SaaS) 產品採用以用量為基礎的訂閱模式。軟體賣方會追蹤您的用量，您只需為使用量付費。

公開優惠

公開優惠可讓您直接從 購買 AWS Marketplace 軟體和服務 AWS Management Console。

私有優惠

私有優惠是一種購買計劃，可讓賣方和買方協商自訂價格和最終使用者授權合約 (EULA) 條款，以用於購買 AWS Marketplace。

ROSA 服務費用

Red Hat 網站可靠性工程師 (SREs) ROSA 收取的 OpenShift 軟體和叢集管理費用。 ROSA 服務費用會計量並 AWS Marketplace 顯示在您的 AWS 帳單上。

AWS 基礎設施費用

AWS 服務 基礎 ROSA 叢集 AWS 的標準費用 Amazon EC2，包括 Amazon EBS Amazon S3和 Elastic Load Balancing。費用會透過 AWS 服務 正在使用的 計量，並顯示在您的 AWS 帳單上。

ROSA 付款和帳單

ROSA 與 整合 AWS Marketplace ，以啟用測量和計費 ROSA 服務費用。 ROSA 服務費用涵蓋 Red Hat 網站可靠性工程師 (SREs) 對 OpenShift 軟體和叢集管理的存取。 ROSA 所有支援 AWS 的標準區域中的服務費用都一致。根據在這些叢集中執行的叢集和工作者節點 vCPUs 數目，具有 HCP 服務費的 ROSA 預設會按固定小時費率隨需累積。ROSA 傳統服務費用會根據工作者節點 vCPUs 的數量隨需產生。ROSA Classic 不會針對控制平面或必要的基礎設施節點收取服務費用。

ROSA 客戶也會為 AWS 服務 基礎 ROSA 叢集支付標準 AWS 基礎設施費用 Amazon EC2 Amazon EBS，包括 Amazon S3和 Elastic Load Balancing AWS 基礎設施費用，是與透過 計費 ROSA 的服務費用不同的帳單項目 AWS Marketplace。 AWS 基礎設施費用依預設會因 而異 AWS 區域 ，且以每小時用量為基礎。若要節省額外的 AWS 基礎設施成本，您可以購買 Amazon EC2 節省計劃或預留執行個體。如需詳細資訊，請參閱 Amazon EC2 《 使用者指南》中的Compute Savings Plans 和預留執行個體。

ROSA 在您建立 ROSA 叢集或購買 ROSA 合約之前， 不會收取費用。如需詳細資訊，請參閱 Red Hat OpenShift Service on AWS 定價。

您可以在 AWS Billing 主控台中檢視 ROSA 服務費用和 AWS 基礎設施費用，並管理付款。您也可以使用 AWS Cost Explorer Service 界面免費檢視成本並監控用量。如需詳細資訊，請參閱 AWS 帳單與成本管理 《 使用者指南》中的檢視您的帳單，以及》 成本管理使用者指南》中的使用 分析您的 AWS Cost Explorer Service AWS 成本。

透過主控台訂閱 ROSA Marketplace 清單

當您在ROSA 主控台 ROSA 中啟用 時，您的 AWS 帳戶 會訂閱 ROSA 傳統和 ROSA，並開啟 HCP 清單 AWS Marketplace。啟用 ROSA 訂閱無需付費。

對於 AWS Organizations 使用者， ROSA 可讓您與組織中的其他帳戶共用 ROSA 傳統訂閱。如需詳細資訊，請參閱《 AWS Marketplace 買方指南》中的在組織中共用訂閱。

購買 ROSA 合約

ROSA 使用 AWS Marketplace 來提供選用的 ROSA 合約與 HCP 和 ROSA classic。合約可節省 ROSA 工作者節點服務費用。 ROSA 合約不會影響 AWS 基礎設施的費用。

12 個月合約

您可以從 ROSA 主控台向 HCP 購買 12 個月的 ROSA 傳統和 ROSA 公開優惠合約。

> **Note**
> 您必須先在帳戶中啟用 ROSA classic，才能從主控台購買 12 個月的合約。

> **Note**
> 12 個月合約無法轉移至私有優惠。

購買 ROSA 傳統 12 個月合約

當您購買 ROSA 傳統 12 個月合約時，您需預付每年期限的費用，並在接下來的 12 個月內為涵蓋的執行個體支付每小時服務費。合約成本是根據您選取的 Amazon EC2 執行個體類型和執行個體數量而定。合約不涵蓋使用基礎 所 ROSA 收取 AWS 服務 的 AWS 基礎設施費用。如需詳細資訊，請參閱 Red Hat OpenShift Service on AWS 定價。

合約僅涵蓋您在建立合約期間指定的執行個體類型 （例如 m5.xlarge)。您可以購買額外的 12 個月合約，以節省多個 Amazon EC2 執行個體類型的成本。在 12 個月合約外的使用會產生按需費率計費的 ROSA 服務費用。

> **Note**
> ROSA 傳統 12 個月合約不會自動續約。

購買 ROSA classic 的 12 個月合約

> **Note**
> 如果您在尚未向 HCP 支援 ROSA 的區域中使用 ROSA 主控台，則此工作流程尚無法使用。如需使用 HCP 支援 ROSA 的區域清單，請參閱 the section called “比較 ROSA 與 HCP 和 ROSA classic”。
> 若要在無 ROSA 且沒有 HCP 支援的區域中購買 ROSA 傳統合約，請前往 ROSA 主控台，然後選擇購買軟體合約並檢視現有合約。

1. 前往 ROSA 主控台。
2. 在左側導覽窗格中，選擇合約。
3. 選擇 ROSA 傳統合約。
4. 選擇購買合約。
5. 選取您需要的 EC2 執行個體類型和執行個體數量。
6. 選擇檢閱合約。
7. 檢閱合約詳細資訊，然後選擇購買合約。

> **Note**
> ROSA 使用主控台建立 12 個月合約後，無法降級或取消。如果您需要在有效合約期間降級或取消合約，請前往 支援 中心並開啟支援案例。

購買與 HCP 簽訂 12 個月合約的 ROSA

當您在主控台中啟用具有 HCP 的 ROSA 時，最初會在您的帳戶上建立具有 HCP 合約的 12 個月免費 ROSA，以方便隨需計費。如果您選擇使用 HCP 合約購買 ROSA 以節省工作者節點服務費用，則初始合約會修改為涵蓋您指定的工作者節點 vCPUs和控制平面的使用成本。

當您購買與 HCP 簽訂的 ROSA 12 個月合約時，您需預付每年期限的費用，並針對涵蓋的工作者節點 vCPUs和控制平面支付未來 12 個月的每小時使用費。合約成本是根據您選擇的工作者節點 vCPUs 和控制平面數量。合約僅涵蓋您在合約建立期間指定的工作者節點 vCPUs和控制平面。合約不涵蓋使用基礎 所 ROSA 收取 AWS 服務 的 AWS 基礎設施費用。如需詳細資訊，請參閱 Red Hat OpenShift Service on AWS 定價。

每月用量配額

購買時，預付vCPUs 和控制平面會轉換為每月用量配額。每小時隨需用量費率適用於 vCPU 和控制超過每月配額的平面用量。與 HCP 合作的 ROSA 使用以下公式來計算與合約相關聯的每月配額：

- 工作者節點 vCPUs：vCPUs數目 x 24 小時 x 365 天/12 個月
- 控制平面：控制平面數量 x 24 小時 x 365 天/12 個月

例如，購買 4，000 個工作者節點 vCPUs 和 8 個控制平面將轉換為每月 2，920，000 個工作者節點 vCPU 小時和每月 5，840 個控制平面小時消耗品的每月配額。

購買與 HCP 簽訂 12 個月合約的 ROSA

> **Note**
> 如果您在尚未支援具有託管控制平面的 ROSA 的區域中使用 Red Hat OpenShift Service on AWS 主控台，則此工作流程尚無法使用。如需使用 HCP 支援 ROSA 的區域清單，請參閱 the section called “比較 ROSA 與 HCP 和 ROSA classic”。

1. 前往 ROSA 主控台。
2. 在左側導覽窗格中，選擇合約。
3. 選擇與 HCP 簽訂的 ROSA 合約。
4. 選擇購買合約。
5. 輸入要購買的 vCPUs數量。以 4 的倍數指定 。
6. 輸入要購買的控制平面數量。
7. 選擇檢閱合約。
8. 檢閱合約詳細資訊，然後選擇購買合約。

> **Note**
>
> ROSA 使用主控台建立 12 個月合約後，無法降級或取消。如果您需要在有效合約期間降級或取消合約，請前往 支援 中心並開啟支援案例。

使用 HCP 12 個月合約升級 ROSA

您可以隨時使用 HCP 升級作用中的 ROSA 與額外工作者節點 vCPUs和控制平面的 12 個月合約。當您使用 HCP 12 個月合約升級 ROSA 時，您會為新增的資源預先按比例支付款項。按比例分配的金額是根據合約剩餘的天數來計算。合約僅涵蓋您在合約建立期間指定的工作者節點 vCPUs和控制平面。合約升級不會影響 AWS 基礎設施的費用。

升級時，新增vCPUs 和控制平面會使用與原始合約購買相同的公式轉換為每月用量配額。每小時隨需用量費率適用於 vCPU 和控制超過每月配額的平面用量。如需詳細資訊，請參閱the section called “每月用量配額”。

使用 HCP 升級 ROSA 12 個月合約

1. 前往 ROSA 主控台。
2. 在左側導覽窗格中，選擇合約。
3. 與 HCP 選擇 ROSA 的合約。
4. 選擇 Upgrade (升級)。
5. 輸入要新增vCPUs 數量。以 4 的倍數指定 。
6. 輸入要新增至合約的控制平面數量。
7. 選擇檢閱升級。
8. 檢閱合約詳細資訊，然後選擇購買升級。

> **Note**
>
> ROSA 傳統 12 個月合約無法升級。您可以隨時使用 ROSA 主控台購買額外的 12 個月 ROSA 傳統合約。

取得私有優惠

您可以向 HCP 或 ROSA classic 請求 ROSA 的 AWS Marketplace 私有優惠，以接收與 Red Hat 協商的產品定價和最終使用者授權合約 (EULA) 條款。如需詳細資訊，請參閱《 AWS Marketplace 買方指南》中的私有優惠。

取得 ROSA 私有優惠

> **Note**
>
> 如果您是 AWS Organizations 使用者，並收到核發給您付款人和成員帳戶的私有優惠，請遵循下列程序 ROSA 直接在您的組織中的每個帳戶訂閱 。
> 如果您收到僅向 AWS Organizations 付款人帳戶發出的 ROSA 傳統私有優惠，您將需要與組織中的成員帳戶共用訂閱。如需詳細資訊，請參閱 AWS Marketplace 買方指南中的在組織中共用訂閱。

1. 發出私有優惠後，請登入 AWS Marketplace 主控台。
2. 使用 ROSA 私有優惠連結開啟電子郵件。
3. 依照連結直接存取私有優惠。

> **Note**
>
> 在登入正確的帳戶之前，遵循此連結將導致找到頁面備註 (404) 錯誤。

4. 檢閱條款與條件。
5. 選擇接受術語。

> **Note**
>
> 如果不接受 AWS Marketplace 私有優惠，則 的 ROSA 服務費用 AWS Marketplace 將繼續以公有小時費率計費。

6. 若要驗證優惠詳細資訊，請在產品清單中選取顯示詳細資訊。
7. 若要開始使用 ROSA，請選擇繼續設定。系統會將您重新導向至 ROSA 主控台。

私有市場

Private Marketplace 可讓管理員從中建置已核准產品的自訂數位目錄 AWS Marketplace。管理員可以在 中為 AWS Marketplace AWS 組織單位或 AWS 帳戶 組織內的不同單位建立唯一一組可用的已審核軟體。

如果您的組織使用私有市集，管理員必須先 ROSA 將 的 AWS Marketplace 清單新增至私有市集，使用者才能啟用服務。如需詳細資訊，請參閱 AWS Marketplace 買方指南中的私有市集入門。

故障診斷

下頁詳細說明在建立或管理 ROSA 叢集時遇到的一些常見問題。

主題

- 存取 ROSA 叢集偵錯日誌
- ROSA 叢集在 叢集 建立期間服務 AWS 配額檢查失敗
- 對 CLI ROSA 過期的離線存取權杖進行故障診斷
- 無法建立 叢集 具有 osdCcsAdmin 錯誤的
- 後續步驟
- 取得 ROSA 支援

存取 ROSA 叢集偵錯日誌

若要開始疑難排解應用程式的問題，請先檢閱偵錯日誌。CLI ROSA 偵錯日誌提供當 叢集 無法建立時所產生錯誤訊息的詳細資訊。

若要顯示 叢集 偵錯資訊，請執行下列 ROSA CLI 命令。在 命令中，將 取代`<cluster_name>`為 的名稱 叢集。

```
rosa describe cluster -c <cluster_name> --debug
```

ROSA 叢集在 叢集 建立期間服務 AWS 配額檢查失敗

若要使用 ROSA，您帳戶的 服務配額可能需要增加。如需詳細資訊，請參閱 Red Hat OpenShift Service on AWS 端點和配額。

1. 執行下列命令來識別您帳戶的配額。

```
rosa verify quota
```

> **Note**
> 配額不同 AWS 區域。請務必驗證您區域的每個配額。

2. 如果您需要增加配額，請導覽至 Service Quotas 主控台。
3. 在導覽窗格中，選擇 AWS 服務。
4. 選擇需要提高配額的服務。
5. 選取需要增加的配額，然後選擇請求增加配額。
6. 對於增加請求配額，輸入您希望配額的總數量，然後選擇請求。

對 CLI ROSA 過期的離線存取權杖進行故障診斷

如果您使用 ROSA CLI 且 api.openshift.com 離線存取字符過期，則會顯示錯誤訊息。當 sso.redhat.com 使字符失效時，就會發生這種情況。

1. 導覽至 OpenShift Cluster Manager API 權杖頁面，然後選擇載入權杖。
2. 在終端機中複製並貼上下列身分驗證命令。

```
rosa login --token="<api_token>"
```

無法建立 叢集 具有 osdCcsAdmin 錯誤的

> **Note**
> 只有在您使用非 STS 方法來佈建 ROSA 叢集時，才會發生此錯誤。若要避免此問題，請使用佈建 ROSA 叢集 AWS STS。如需詳細資訊，請參閱the section called “建立 ROSA 傳統叢集 - CLI”。

如果您的 叢集 無法建立，您可能會收到下列錯誤訊息：

```
Failed to create cluster: Unable to create cluster spec: Failed to get access keys for
 user 'osdCcsAdmin': NoSuchEntity: The user with name osdCcsAdmin cannot be found.
```

1. 刪除堆疊

```
rosa init --delete-stack
```

2. 重新初始化您的帳戶。

```
rosa init
```

後續步驟

- 請造訪 OpenShift 文件。
- 開啟支援 案例或 Red Hat Support 案例。
- 尋找常見問題 Red Hat OpenShift Service on AWS的答案。
- 如需 ROSA 支援模型的詳細資訊，請參閱the section called “取得支援”。

取得 ROSA 支援

使用 ROSA，您可以從 支援 和 Red Hat 支援團隊獲得支援。任何一個組織都可以開啟支援案例，並路由至正確的團隊來解決您的問題。

開啟 支援 案例

AWS 需要開發人員支援計劃才能開啟 ROSA 技術案例，但建議使用 AWS 企業、企業或企業駐場支援計劃，才能持續存取 ROSA 技術支援和架構指導。Red Hat 會視需要使用 支援 API 為客戶開啟案例。AWS Business、Enterprise 和 Enterprise On-Ramp 支援計畫可讓支援工程師持續存取電話、Web 和聊天。如需 支援 計劃的詳細資訊，請參閱 支援。

如需啟用 支援 計劃的步驟，請參閱如何註冊 支援 計劃？

如需建立 支援 案例的相關資訊，請參閱建立支援案例和案例管理。

開啟 Red Hat Support 案例

ROSA 包含 Red Hat Premium Support。若要接收 Red Hat Premium Support，請導覽至 Red Hat 客戶入口網站，並使用支援案例工具來建立支援票證。如需詳細資訊，請參閱如何與 Red Hat 支援互動。

文件歷史記錄

下表說明 文件的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

變更	描述	日期
已更新 ROSAImageRegistryOperatorPolicy	已更新 AWS 受管政策 ROSAImageRegistryOperatorPolicy。	2025 年 5 月 19 日
已更新 ROSANodePoolManagementPolicy	已更新 AWS 受管政策 ROSANodePoolManagementPolicy。	2025 年 5 月 5 日
已更新 ROSAImageRegistryOperatorPolicy	已更新 AWS 受管政策 ROSAImageRegistryOperatorPolicy。	2025 年 4 月 16 日
已更新 ROSAWorkerInstancePolicy	已更新 AWS 受管政策 ROSAWorkerInstancePolicy。	2025 年 3 月 3 日
已更新 ROSANodePoolManagementPolicy	已更新 AWS 受管政策 ROSANodePoolManagementPolicy。	2025 年 2 月 24 日
已更新 ROSAAmazonEBSCSIDriverOperatorPolicy	已更新 AWS 受管政策 ROSAAmazonEBSCSIDriverOperatorPolicy。	2025 年 1 月 17 日
具有 HCP AWS 區域 擴展的 ROSA	具有託管控制平面 (HCP) 的 ROSA 現在可在中東（阿拉伯聯合大公國）使用 AWS 區域。	2024 年 5 月 13 日
具有 HCP AWS 區域 擴展的 ROSA	具有託管控制平面 (HCP) 的 ROSA 現已在歐洲（巴黎）提供 AWS 區域。	2024 年 5 月 6 日

已更新 ROSANodePoolManagementPolicy	已更新 AWS 受管政策 ROSANodePoolManagementPolicy。	2024 年 5 月 2 日
具有 HCP AWS 區域 擴展的 ROSA	具有託管控制平面 (HCP) 的 ROSA 現已在歐洲（西班牙）提供 AWS 區域。	2024 年 4 月 29 日
已更新 ROSAInstallerPolicy	已更新 AWS 受管政策 ROSAInstallerPolicy。	2024 年 4 月 24 日
具有 HCP AWS 區域 擴展的 ROSA	具有託管控制平面 (HCP) 的 ROSA 現已在歐洲（蘇黎世）提供 AWS 區域。	2024 年 4 月 19 日
具有 HCP AWS 區域 擴展的 ROSA	具有託管控制平面 (HCP) 的 ROSA 現在可在亞太區域（大阪）使用 AWS 區域。	2024 年 4 月 17 日
已更新 ROSAInstallerPolicy 和 ROSASRESupportPolicy	已更新 AWS 受管政策 ROSAInstallerPolicy 和 ROSASRESupportPolicy。	2024 年 4 月 10 日
具有 HCP AWS 區域 擴展的 ROSA	具有託管控制平面 (HCP) 的 ROSA 現在可在亞太區域（香港）使用 AWS 區域。	2024 年 4 月 8 日
具有 HCP AWS 區域 擴展的 ROSA	具有託管控制平面 (HCP) 的 ROSA 現已在南美洲（聖保羅）提供 AWS 區域。	2024 年 4 月 1 日
具有 HCP AWS 區域 擴展的 ROSA	具有託管控制平面 (HCP) 的 ROSA 現已在中東（巴林）提供 AWS 區域。	2024 年 3 月 25 日
具有 HCP AWS 區域 擴展的 ROSA	具有託管控制平面 (HCP) 的 ROSA 現在可在亞太區域（首爾）使用 AWS 區域。	2024 年 3 月 14 日

具有 HCP AWS 區域 擴展的 ROSA	非洲（開普敦）現在提供具有託管控制平面 (HCP) 的 ROSA AWS 區域。	2024 年 3 月 5 日
已更新 ROSAInstallerPolicy	已更新 AWS 受管政策 ROSAInstallerPolicy。	2024 年 1 月 26 日
已更新 ROSASRESupportPolicy	已更新 AWS 受管政策 ROSASRESupportPolicy。	2024 年 1 月 22 日
已更新 ROSAImageRegistryOperatorPolicy	已更新 AWS 受管政策 ROSAImageRegistryOperatorPolicy。	2023 年 12 月 12 日
已更新 ROSAKubeControllerPolicy	已更新 AWS 受管政策 ROSAKubeControllerPolicy。	2023 年 10 月 16 日
更新的 ROSAManageSubscription	已更新 AWS 受管政策 ROSAManageSubscription。	2023 年 8 月 1 日
已更新 ROSAKubeControllerPolicy	已更新 AWS 受管政策 ROSAKubeControllerPolicy。	2023 年 7 月 13 日
新增 ROSA 安全性頁面	已新增 ROSA 中的彈性、ROSA 中的基礎設施安全性，以及 ROSA 頁面中的資料保護。	2023 年 6 月 30 日
新增部署選項頁面	已新增部署選項頁面。	2023 年 6 月 9 日
新增了新的 AWS 受管政策 ROSANodePoolManagementPolicy	已新增新的 AWS 受管政策 ROSANodePoolManagementPolicy。	2023 年 6 月 8 日
新增了新的 AWS 受管政策 ROSAInstallerPolicy	已新增新的 AWS 受管政策 ROSAInstallerPolicy。	2023 年 6 月 6 日
新增了新的 AWS 受管政策 ROSASRESupportPolicy	已新增新的 AWS 受管政策 ROSASRESupportPolicy。	2023 年 6 月 1 日

新增 ROSA 的責任概觀	新增 ROSA 頁面的責任概觀。	2023 年 5 月 26 日
已更新什麼是 Red Hat OpenShift Service on AWS？	已更新什麼是 Red Hat OpenShift Service on AWS 頁面。	2023 年 5 月 24 日
新增 ROSA 運算子角色的新 AWS 受管政策	已新增新的 AWS 受管政策 ROSAImageRegistryOperatorPolicy、ROSA KubeControllerPolicy 和 ROSAKMSProviderPolicy。	2023 年 4 月 27 日
新增了新的 AWS 受管政策 ROSAControlPlaneOperatorPolicy	已新增新的 AWS 受管政策 ROSAControlPlaneOperatorPolicy。	2023 年 4 月 24 日
新增 ROSA 帳戶角色的新 AWS 受管政策	已新增 ROSA 帳戶和運算子角色頁面的新 AWS 受管政策頁面。	2023 年 4 月 20 日
新增 ROSA 服務配額頁面	已新增 ROSA 服務配額頁面。	2022 年 12 月 22 日
新增故障診斷頁面	已新增故障診斷頁面。	2022 年 11 月 1 日
新增入門頁面	已新增入門頁面。	2022 年 8 月 12 日
新增了新的 AWS 受管政策 ROSAManageSubscription	已新增新的 AWS 受管政策 ROSAManageSubscription。	2022 年 4 月 11 日
初始版本	Red Hat OpenShift Service on AWS 使用者指南的初始版本。	2021 年 3 月 24 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。