在 上保護半導體開發環境的策略 AWS

AWS 方案指引

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 方案指引: 在 上保護半導體開發環境的策略 AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

簡介 1
Semiconductor 產業概觀 1
Semiconductor 公司需要最新的技術功能 1
使用規模經濟、彈性和自動化 1
安全和合規 3
減少合規工作 3
使用參考架構 3
保護半導體資料 4
防止未經授權的存取和資料外洩 4
設定許可 4
驗證使用者 5
傳輸資料 5
加密資料 6
管理傳出網路流量 6
符合資料落地要求 6
保護遠端體驗 8
最佳化遠端桌面體驗 8
保護與第三方的協同合作 9
AWS 安全服務 11
防止勒索軟體 12
AWS 雲端 差異化器 13
結論 14
文件歷史紀錄 15
..... xvi

在 上保護半導體開發環境的策略 AWS

Mike Virgilio、Allan Carter 和 Nikhil Marrapu，Amazon Web Services (AWS)

2023 年 6 月 (文件歷史記錄)

本文件提供策略指引，協助您保護並符合在 中操作之半導體工作負載的合規要求 AWS 雲端。其中包括 AWS 服務 和 功能的範例架構和概觀，您可以用來實作本指南，並協助保護敏感資料免於安全風險。

Semiconductor 產業概觀

根據 Semiconductor Industry Association，該半導體業務是 USD5734.4 億美金的全球產業。為了保護智慧財產權 (IP)，安全性是業界的首要任務。半導體公司需要開發環境，以便其工程師可以設計晶片、電腦系統、電路板和其他產品。安全開發環境必須嚴格控制誰可以存取其中的 IP。

公司開發自己的 IP，但他們通常也會使用來自第三方供應商的 IP，例如處理器核心、標準介面、來自半導體代工廠的程序設計套件 (PDKs)，以及來自電子設計自動化 (EDA) 公司的授權工具。開發程序的高度協作性質意味著內部工程師和來自這些第三方公司的工程師需要存取開發環境。關鍵的安全要求是防止未經授權的資料從安全開發環境外洩。

Semiconductor 公司需要最新的技術功能

Semiconductor 公司在競爭激烈的產業中營運，其中speed-to-market和創新對於成功至關重要。隨著晶片設計和製造需求變得越來越複雜，半導體公司需要存取最新的技術，以滿足並超越業界的需求。的可擴展性和容量可以滿足運算和儲存需求的指數增長 AWS 雲端。透過全方位的基礎設施和強大的運算、網路和儲存解決方案， AWS 可讓半導體公司利用機器學習、高效能運算和自動化等尖端技術。使用這些技術可以加速研究和開發工作、最佳化製造程序，並提供最新技術的存取權。有價值的 IP 是複雜攻擊的吸引人目標，使安全性成為安全開發環境的首要任務。

使用規模經濟、彈性和自動化

AWS 為公司提供規模經濟、資源彈性和自動化功能，這些功能對成功至關重要。由於 AWS 已與數十萬家公司合作，因此可以實現大規模的規模經濟，這可降低所有 的成本。 AWS 基礎設施彈性可讓公司輕鬆擴展以滿足最嚴苛的工作負載，然後縮減規模以最佳化成本。此外， AWS 自動化功能可協助公司建立可重複的程序，將未區分的手動任務降至最低。 AWS 提供各式各樣的安全服務和功能，協助半導體公司透過強大的安全控制來保護工作負載，包括網路分割、資料加密和法規合規。透過在 中建

置 AWS 雲端，半導體公司可以專注於創新和成長，同時確保其資料和操作具有應對潛在安全風險的彈性。

在 上實現半導體開發環境的安全性和合規性 AWS

AWS 已制定最佳實務指引，以實作安全控制和發佈的參考架構，以滿足半導體產業需求。本節討論如何使用 AWS 建議的設計和參考架構，協助實現任務關鍵工作負載的安全性和合規性 AWS。

使用 減少合規工作 AWS

AWS 共同責任模型描述 AWS 和 客戶之間如何共同承擔安全與合規的責任。 AWS 負責雲端的安全，而客戶負責雲端的安全。這有助於公司透過承擔雲端基礎設施的責任，減少實現企業和法規要求所需的工作量 AWS。

以下 AWS 服務 可協助半導體公司證明符合公司和法規要求：

- AWS Artifact 為各種合規架構提供可下載的合規報告，包括國際標準化組織 (ISO)、國家標準技術研究所 (NIST) 和聯邦風險與授權管理計劃 (FedRAMP)。您可以結合 AWS Artifact 報告與企業雲端資源評估，以證明稽核人員的合規性，並協助減少符合美國國際武器運輸法規 (ITAR) 等法規所需的時間和精力。
- AWS Audit Manager 可以使用預先建置的自訂架構和自動化證據收集，將您的合規要求映射至 AWS 用量資料。

透過使用這些服務和功能，公司可以更有效地實現企業和法規要求的合規。如需 是否 AWS 服務 在 AWS 保證計劃範圍內的詳細資訊，請參閱AWS 服務 合規計劃範圍內的 。

使用提供的參考架構

AWS 根據各種產業的數千個部署，制定方案指引和最佳實務。這些建議包含在 AWS Well-Architected 架構、AWS 雲端採用架構 (AWS CAF) 和AWS 安全參考架構 (AWS SRA) 中。

在架構和設計安全開發環境時， AWS 提供以上述架構為基礎的半導體和電子參考架構。這些參考架構旨在保護資料和工作負載。

您可以使用AWS 安全成熟度模型，以分階段方式引導您完成安全控制的待處理項目。

透過使用這些架構、模型和參考架構，您可以在雲端中建立強大的安全狀態，並協助保護關鍵資產。

在 上保護半導體資料 AWS

透過 AWS，您可以管理資料的隱私權控制，並控制資料的使用方式、誰可以存取資料，以及資料加密的方式。這些功能是以彈性且安全的雲端運算環境為基礎。本節會檢閱 AWS 功能，以協助半導體公司實作資料存取控制並解決資料駐留需求。

本節包含下列主題：

- 防止未經授權的存取和資料外洩
- 在 上滿足資料駐留要求 AWS

防止未經授權的存取和資料外洩

根據 2022 年資料外洩成本報告 (Ponemon Institute 報告），2022 年資料外洩的平均成本為 USD4。對於半導體公司而言，保護智慧財產權 (IP) 至關重要。因未經授權的存取而遺失 IP 可能會導致財務損失、聲譽受損，甚至是法規後果。這些潛在後果會導致控制對資料和資料流程的存取，而資料是架構良好的設計的關鍵層面。

保護資料安全的重要考量包括：

- 存取安全開發環境的使用者身分驗證
- 在安全開發環境中存取資料的使用者授權
- 記錄所有進出安全開發環境的傳輸
- 架構環境之間的安全資料流程
- 傳輸中和靜態資料的加密
- 限制和記錄傳出網路流量

設定許可

AWS Identity and Access Management (IAM) 透過控制已驗證並獲授權使用的人員，協助您安全地管理對 AWS 資源的存取。根據預設，除非明確允許，否則 中的任何動作 AWS 都會隱含拒絕。您可以透過建立 政策 AWS 來管理 中的存取。您可以使用政策來定義哪些使用者可以存取哪些資源，以及他們可以對這些資源執行哪些動作。 AWS 最佳實務是套用最低權限許可，這表示您只授予使用者執行任務所需的許可。如需詳細資訊，請參閱 IAM 文件中的下列內容：

- IAM 中的政策和許可

- Policy 評估邏輯
- IAM 中的安全最佳實務

驗證使用者

AWS 最佳實務是要求人類使用者使用聯合身分提供者 AWS ，以使用臨時憑證來存取 。集中使用者人力資源存取的建議服務是 AWS IAM Identity Center。此服務可協助您安全地建立或連線您的人力資源身分，並集中管理其跨 AWS 帳戶 和應用程式的存取。IAM Identity Center 可以使用 SAML 2.0、Open ID Connect (OIDC) 或 OAuth 2.0 與外部身分提供者 (IdPs) 聯合，以提供無縫整合和使用者管理。如需詳細資訊，請參閱 (AWS 行銷） 中的聯合身分 AWS和聯合身分提供者和聯合身分 (IAM 文件）。

您也可以使用 驗證和授權使用者AWS Directory Service，以管理 目錄中定義的使用者和群組，例如 Active Directory。在安全開發環境中，您可以使用 Linux 檔案許可來授權和限制虛擬私有雲端 (VPC) 內的資料存取。使用 VPC 端點提供對 的存取， AWS 服務 而不周遊公有網際網路。使用端點政策來限制哪些 AWS 主體可以使用端點，並使用身分型政策來限制對 的存取 AWS 服務。

傳輸資料

AWS 提供多種方式將內部部署資料遷移至雲端。最初將資料存放在 Amazon Simple Storage Service (Amazon S3) 中很常見。Amazon S3 是一種雲端型物件儲存服務，可協助您存放、保護和擷取任意數量的資料。在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體之間傳輸資料時，可提供高達 25 Gbps 的頻寬。它還提供跨區域資料複寫和資料分層。存放在 Amazon S3 中的資料可作為複寫來源。您可以使用它來建立新的檔案系統，或將資料傳輸到 EC2 執行個體。您可以使用 Amazon S3 做為 AWS 受管、可攜式作業系統界面 (POSIX) 相容檔案系統的後端，以用於半導體工具和流程。

另一個 AWS 儲存服務是 Amazon FSx，它提供支援業界標準連線通訊協定的檔案系統，並提供跨 的高可用性和複寫 AWS 區域。半導體產業的常見選擇包括 Amazon FSx for NetApp ONTAP、Amazon FSx for Lustre 和 Amazon FSx for OpenZFS。Amazon FSx 中可擴展的高效能檔案系統非常適合在本機安全開發環境中存放資料。

AWS 建議您先在 上 AWS 定義半導體工作負載的儲存需求，然後識別適當的資料傳輸機制。 AWS 建議使用 AWS DataSync將資料從現場部署傳輸到 AWS。DataSync 是一種線上資料傳輸和探索服務，可協助您在 AWS 儲存服務之間來回移動檔案或物件資料。視您使用的是自我管理儲存系統或 NetApp 等儲存提供者而定，您可以設定 DataSync 來加速透過網際網路或透過 將資料移動和複寫至安全開發環境 AWS Direct Connect。DataSync 可以傳輸檔案系統資料和中繼資料，例如擁有權、時間戳記和存取許可。如果您要在 FSx for ONTAP 和 NetApp ONTAP 之間傳輸檔案， AWS 建議使用 NetApp SnapMirror。Amazon FSx 支援靜態和傳輸中的加密。使用 AWS CloudTrail和其他服務特定的記錄功

能來記錄所有 API 呼叫和相關的資料傳輸。將日誌集中在專用帳戶中，並套用不可變歷史記錄的精細存取政策。

AWS 提供額外的 服務，以協助控制資料流程，包括應用程式感知的網路防火牆，例如 AWS Network Firewall、Amazon Route 53 Resolver DNS 防火牆AWS WAF、 和 Web 代理。使用 Amazon Virtual Private Cloud (Amazon VPC)、Network Firewall、傳輸閘道路由表和服務控制政策 (SCPs) 中的安全群組、網路存取控制清單和 VPC 端點強制執行網路分段，以控制環境中的資料流程 AWS Organizations。使用 VPC 流程日誌和 VPC 流程日誌第 2-5 版中的可用欄位，集中記錄所有網路流量。

加密資料

使用 AWS Key Management Service (AWS KMS) 客戶受管金鑰或 加密所有靜態資料AWS CloudHSM。建立和維護精細的金鑰資源政策。如需詳細資訊，請參閱為靜態資料建立企業加密策略。

使用業界標準的 256 位元進階加密標準 (AES-256) 密碼強制執行至少 TLS 1.2，以加密傳輸中的資料。

管理傳出網路流量

如果安全開發環境需要網際網路存取，則應透過網路層級強制執行點記錄和限制所有傳出網際網路流量，例如透過 Network Firewall 或 Squid，這是開放原始碼代理。VPC 端點和網際網路代理有助於防止使用者未經授權洩露資料。這對於允許存取安全開發環境和只在 VPC 內的資料至關重要。

最後，您可以使用 Amazon VPC 的一項功能 Network Access Analyzer 來執行網路分段驗證，並識別不符合指定需求的潛在網路路徑。

透過分層安全控制，您可以建立和強制執行強大的資料周邊。如需詳細資訊，請參閱在 上建置資料周邊 AWS。

在 上滿足資料駐留要求 AWS

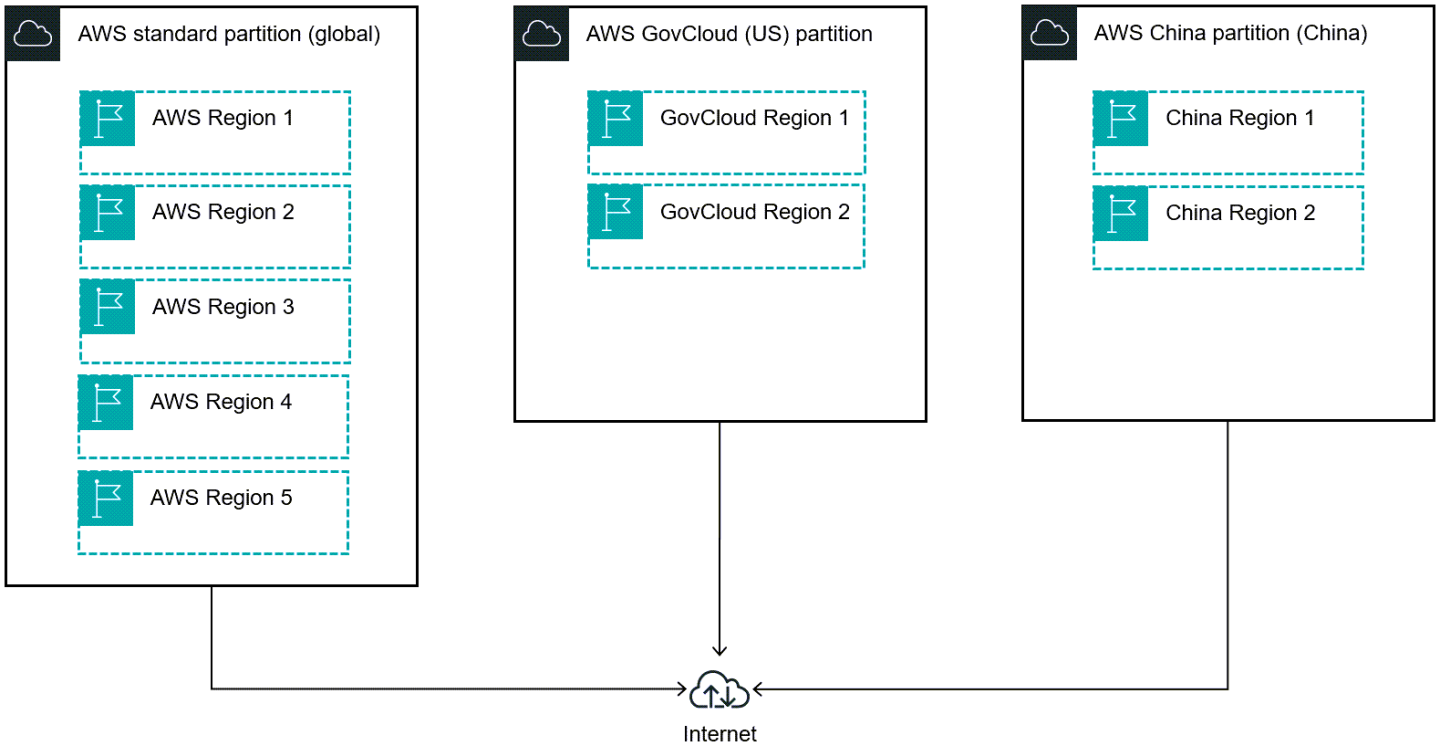
可用的分割區 AWS 區域、可用區域和本機區域可讓公司根據其唯一需求，為其資料和工作負載選擇最佳位置：

- 分割區是 AWS 區域. AWS commercial 區域的邏輯群組位於`aws`分割區中，而中國的區域位於`aws-cn`分割區中，且 AWS GovCloud (US) Regions 位於`aws-us-gov`分割區中。
- AWS 區域 是 AWS 叢集資料中心所在的個別地理區域。
- 每個 AWS 區域 都有多個隔離的位置，稱為可用區域。

- Local Zone 是地理位置接近您使用者的 區域延伸。

如需目前可用區域、可用區域和本機區域的詳細資訊，請參閱 AWS 全球基礎設施。

分割區提供與其他分割區中區域的資料、網路和機器隔離。 AWS 分割區會在不同分割區中的區域之間建立具有個別登入存取權的邏輯網路隔離。分割區包含一或多個區域，但 只 AWS 區域 存在於一個分割區中； AWS 區域 不能是兩個分割區的一部分。



您可以根據是否需要美國政府安全分類，在分割區之間進行選擇。處理未分類或官方資料的工作負載可以使用 AWS GovCloud (US) 或標準分割區。 AWS 也提供經認可的其他分割區，可在 Secret 和 Top-Secret 美國安全分類層級操作工作負載，但這些分割區超出本指南的範圍。如需這些分類層級操作工作負載的詳細資訊，請參閱美國國防雲端運算和美國智慧社群雲端運算。

我們建議在單一分割區中部署多區域工作負載，以減少任何合規、操作和技術挑戰。不過，使用案例有限，例如使用 AWS Direct Connect或 Amazon CloudFront，您可以在其中跨多個 整合服務以滿足特定目標。如需詳細資訊，請聯絡您的 AWS 解決方案架構師。

為工程師提供安全的遠端體驗

遠端視覺化是半導體設計中的關鍵元件。工具工程師使用遠端驗證，晶片設計人員則使用它來提交任務並檢視其狀態。本節提供強大的解決方案，可在不同的網路條件下表現良好。其設計為雲端原生，以便與 AWS 安全服務無縫整合。

本節包含下列主題：

- 最佳化遠端桌面體驗
- 保護與第三方的工程協作

最佳化遠端桌面體驗

設計人員通常會使用終端機型 SSH 工作階段或圖形化遠端桌面來提交和視覺化工作流程。遠端桌面提供 GUI 驅動的互動式工具（例如配置、位置和路由），讓工具工程師和晶片設計人員提交任務。AWS 提供 Amazon DCV，這是一種高效能遠端顯示通訊協定，可為工程和實體設計團隊提供強大的使用者介面。Amazon DCV 在不同的網路條件下表現良好。

Amazon DCV 會串流像素而非幾何，以協助保護資料隱私權。此外，Amazon DCV 使用 TLS 來保護像素和最終使用者輸入。

使用連線檔案，使用者可以立即連線至 Amazon DCV 工作階段。不過，請注意，連線檔案參數使用 `password`和 `proxypassword` 欄位而不加密。如需詳細資訊，請參閱使用連線檔案。Amazon DCV 會在伺服器和用戶端之間建立 TLS 連線。連線檔案中的驗證政策會決定當憑證無法驗證為可信時，用戶端如何回應。如需詳細資訊，請參閱設定憑證驗證政策。

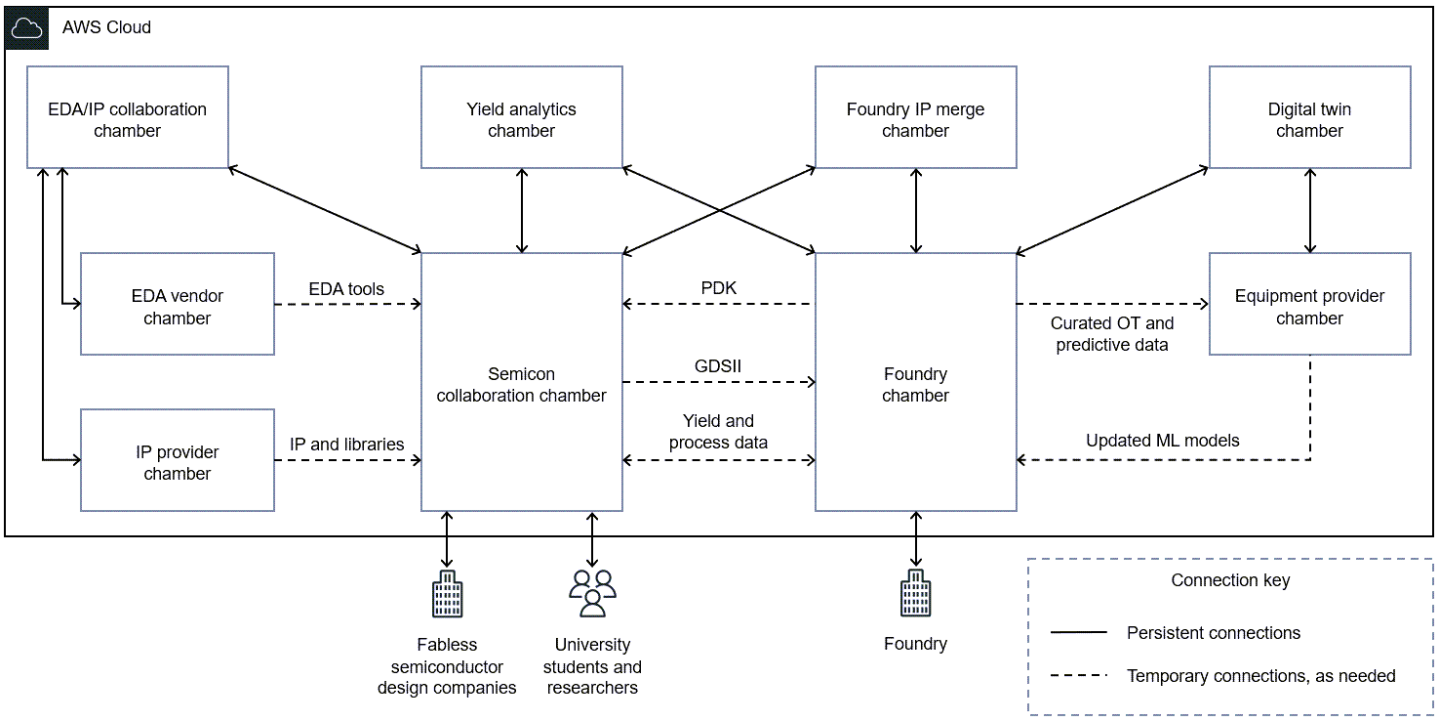
提供遠端桌面功能的其他內部部署商業解決方案包括 NoMachine 或 OpenText Exceed TurboX。

透過任何遠端桌面解決方案，基礎基礎設施由 Amazon Elastic Compute Cloud (Amazon EC2) 提供支援。根據共同的責任模型，您的責任包括以下領域，以協助保護遠端桌面執行個體的安全：

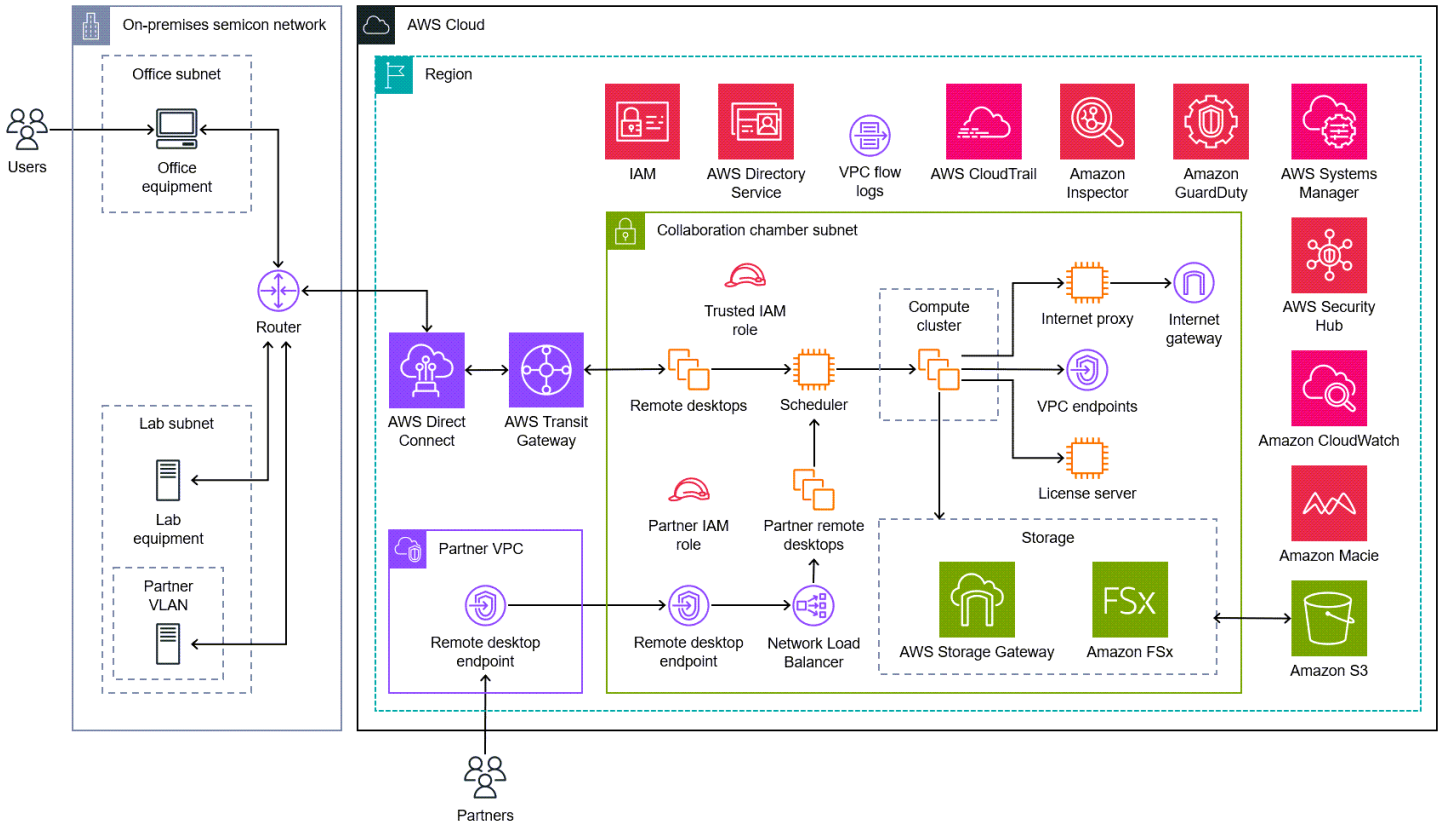
- 控制執行個體的網路存取，例如透過設定 VPC 和安全群組。如需詳細資訊，請參閱控制網路流量。
- 管理用於連線到執行個體的登入資料。
- 管理部署至訪客作業系統的訪客作業系統和軟體，包括更新和安全性修補程式。如需詳細資訊，請參閱在 Amazon EC2 中更新管理。
- 設定連接至執行個體的 IAM 角色以及與這些角色相關聯的許可。如需詳細資訊，請參閱 Amazon EC2 的 IAM 角色。

保護與第三方的工程協作

在開發期間與第三方的協作對於偵錯工具問題、取得設計 IP 整合的協助，以及引進具備專業技能的外部承包商至關重要。從內部部署基礎設施向第三方提供安全存取可能很困難。透過使用 AWS 基礎設施做為程式碼 (IaC)，您可以建立主要安全開發環境的副本，稱為協同合作室。為了協助防止資料外洩，請透過不允許存取網際網路來加強協同合作室的安全狀態。協同合作室具有協同合作者的帳戶，您可以整理室內的資料、工具和基礎設施，只包含協同合作所需的內容。協同合作完成後，請刪除協同合作室，以降低成本並移除對資料的任何潛在存取。下圖顯示設計和製造過程中的不同參與者如何使用各種類型的協同合作室。



下圖是協同合作室的參考架構。此架構可在設計和建置協同合作室時做為參考 AWS。圖表中的 AWS 安全、管理和監控服務有助於保護儲水盒，以保護 IP。如需這些服務的詳細資訊，請參閱本指南AWS 適用於半導體開發環境的安全服務中的 。


On-premises semicon network
Office subnet
Users
Office equipment
Router
Lab subnet
Lab equipment
Partner VLAN
AWS Cloud
Region
IAM
AWS Directory Service
VPC flow logs
AWS CloudTrail
Amazon Inspector
Amazon GuardDuty
AWS Systems Manager
Collaboration chamber subnet
Trusted IAM role
Compute cluster
Internet proxy
Internet gateway
AWS Security Hub
AWS Direct Connect
AWS Transit Gateway
Remote desktops
Scheduler
VPC endpoints
Amazon CloudWatch
License server
Partner IAM role
Partner remote desktops
Amazon Macie
Partner VPC
Storage
Remote desktop endpoint
Remote desktop endpoint
Network Load Balancer
AWS Storage Gateway
Amazon FSx
Amazon S3
Partners

AWS 適用於半導體開發環境的安全服務

AWS 已開發安全服務，旨在保護 中的工作負載和應用程式 AWS 雲端。這些服務可協助保護在雲端中操作的任何類型的工作負載，而不只是半導體工作負載。透過使用這些功能 AWS 服務，公司可以建立強大的預防性和偵測性控制、近乎即時地監控其安全狀態，並在出現安全風險和事件時快速修復。這些服務能夠隨著環境的成長而自動擴展，以維持涵蓋範圍和已建立的安全狀態。此外，雖然這些服務可能專注於特定功能，但它們支援稱為 Amazon EventBridge 的常見訊息匯流排，因此您可以整合服務並自動回應安全風險。

下列 AWS 服務 和 功能可協助您管理存取和政策、偵測和回應安全風險和事件，以及在環境中 AWS 實作監控和記錄：

- AWS CloudTrail 可協助您稽核 的控管、合規和營運風險 AWS 帳戶。
- Amazon GuardDuty 是一種持續的安全監控服務，可分析和處理日誌，以識別您 AWS 環境中非預期和可能未經授權的活動。
- Amazon Inspector 是一種漏洞管理服務，可持續掃描 AWS 工作負載是否有軟體漏洞和意外的網路暴露。
- AWS Security Hub CSPM 提供 中安全狀態的完整檢視 AWS。它還可協助您根據安全產業標準和最佳實務來檢查 AWS 環境。
- Amazon Security Lake 會自動將來自雲端、內部部署和自訂來源的安全資料集中到存放在您 中的專用資料湖 AWS 帳戶。您可以查詢和分析此安全資料，以探索趨勢和異常。
- 服務控制政策 SCPs) 是 中的一種政策類型 AWS Organizations ，可協助您集中管理 AWS 服務 跨多個帳戶的 使用。
- VPC 流程日誌是 Amazon Virtual Private Cloud (Amazon VPC) 的一項功能，可擷取進出 VPC 中網路介面之 IP 流量的相關資訊。您可以使用此資料來疑難排解和回應事件。

保護半導體工作負載和資料免受勒索軟體攻擊

勒索軟體是一種惡意軟體，旨在封鎖對電腦系統或資料的存取，直到完成付款為止。不幸的是，這種類型的攻擊在網際網路中普遍存在，並可能影響任何規模的企業。除了財務損失和聲譽受損之外，半導體公司還必須防止營運中斷，因為中斷可能會導致整個商業生態系統的大規模層疊供應鏈影響。它也可能導致寶貴的智慧財產權遺失。

為了協助防範勒索軟體，半導體公司必須保持警惕，以保護其內部部署和雲端環境的所有層面，尤其是存放、處理或傳輸資料的系統。 AWS 提供許多架構設計和控制項，可協助防範這類事件。除了本指南中提到的控制項之外，請參閱下列有關保護雲端工作負載免受勒索軟體攻擊 AWS 的資源：

- AWS 雲端 安全性 - 防範勒索軟體 (AWS 雲端 安全性）
- AWS 勒索軟體防禦藍圖 (AWS 安全部落格文章）
- 保護您的 AWS 環境免受勒索軟體攻擊 (AWS 網路研討會）
- eBook：保護您的 AWS 環境免受勒索軟體攻擊 (AWS eBook)
- 以 Amazon S3 中的資料為目標的勒索軟體事件剖析 (AWS 安全部落格文章）
- AWS 使用 NIST 網路安全架構 (CSF) 的勒索軟體風險管理 (AWS 白皮書）

半導體產業的差異 AWS 雲端 點

從現場部署環境遷移到 的商業案例 AWS ，對於半導體公司來說可能具有高度吸引力。內部部署基礎設施可能需要昂貴的管理成本、需要大量的前期投資、需要大量精力來維持和保持最新技術，以及需要從各種獨立廠商取得安全工具。透過 AWS，您只需支付使用的資源，這可協助您最佳化工作負載的成本。 AWS 也可讓您立即存取最新的高效能運算 (HPC) 和雲端儲存服務和功能。例如，Amazon FSx for NetApp ONTAP 是常用的儲存服務。您可以使用它將資料從內部部署 NetApp 儲存無縫遷移到 AWS 雲端，並提供網路隔離、資源層級許可、身分型身分驗證、加密、記錄和稽核。

AWS 也可以提升為半導體公司佈建和管理安全解決方案的效率。您可以在 中使用進階安全功能和服務 AWS，實作強大的安全狀態，協助保護您的資料和工作負載免於安全風險。透過使用 AWS Organizations和整合的安全服務，您可以自動在整個 AWS 帳戶 組織內部署安全控制。自動化功能可協助您自動回應風險並簡化安全操作，減少管理全方位安全架構所需的時間和資源。例如， AWS 提供工具和服務，以在整個環境中進行自動化安全管理、持續合規監控，以及風險偵測和回應。透過使用這些解決方案，半導體公司可以改善其安全狀態，同時降低成本並提高效率。整體而言，遷移到 AWS 有助於半導體公司在可擴展性、靈活性和安全性方面實現顯著優勢。

結論

AWS 提供廣泛且安全的平台，可支援半導體公司的需求。透過使用最新技術和利用擴展經濟、彈性擴展功能和各種安全服務，半導體公司可以在 中轉換其業務 AWS 雲端。這些解決 AWS 雲端 複雜挑戰的優勢，同時最佳化創新和持續成長。 AWS 全球基礎設施已準備好支援最複雜的需求，例如資料駐留和安全分類需求。 AWS 可協助您降低成本、提高敏捷性、更快創新，以及保護雲端中的智慧財產權。如需在 中設定半導體開發環境的協助 AWS 雲端，請聯絡您的 AWS 帳戶 團隊或使用聯絡 AWS表單。如需半導體產業 AWS 的其他資訊和資源，請參閱 Semiconductor & Hi-Tech Electronics。

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	—	2023 年 6 月 20 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。