使用者指南

Red Hat OpenShift Service on AWS

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Red Hat OpenShift Service on AWS: 使用者指南

Copyright © 2024 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 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 Red Hat OpenShift Service on AWS？

Red Hat OpenShift Service on AWS (ROSA) 是一項受管理服務，您可以在 Red Hat OpenShift 企業 Kubernetes 平台上用來建置、擴充及部署容器化應用程式。 AWS ROSA 簡化將內部部署 Red Hat OpenShift 工作負載移至其他工作負載 AWS，並與其他 AWS 服務工作負載緊密

功能

ROSA 由和 Red Hat 共同支持 AWS 和運營。每個 ROSA 叢集都有 24 小時 Red Hat 站台可靠性工程師 (SRE) 支援叢集管理，並以 Red Hat 99.95% 的正常運作時間服務等級協定 (SLA) 為後盾。如需有關服務 Support 模式的詳細資訊，請參閱 ROSA.

ROSA 還提供以下功能：

- Red Hat SRE 支援叢集安裝、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、網路和行動裝置。
- 跨多個 AWS 可用區域執行和擴充 Kubernetes 控制平面，以確保高可用性。
- 使用 OpenShift API 和開發人員生產力工具 (包括服務網格、工作 CodeReady 區和無伺服器) 操作叢集。

ROSA 叢集部署模型

ROSA 提供兩種叢集部署模式：含託管控制平面的 ROSA (含有 HCP 的 ROSA) 和 ROSA 經典版。透過 ROSA 搭配 HCP，每個叢集都有一個專屬的控制平面，這個平面會隔離在 Red Hat 內， AWS 帳戶並由 Red Hat 管理。使用 ROSA 經典版，叢集控制平面基礎結構託管在客戶的 AWS 帳戶。

ROSA 搭配 HCP 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 基礎架構費用，ROSA 並加快叢集建立時間。如需 ROSA 搭配 HCP 和 ROSA 傳統版的相關資訊，請參閱部署選項。

> **Note**
>
> 含託管控制平面的 ROSA 目前不提供合規性認證或聯邦資訊處理標準 (FIPS)。如需詳細資訊，請參閱 Red Hat 文件中的合規性。

存取 ROSA

您可以使用下列介面定義和設定 ROSA 服務部署。

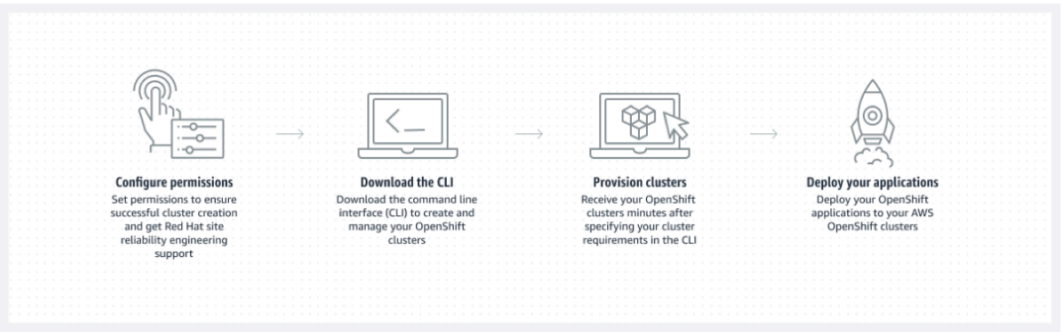
AWS

- ROSA 主控台 — 提供 Web 介面以啟用 ROSA 訂閱和購買 ROSA 軟體合約。
- AWS Command Line Interface (AWS CLI) — 提供多組指令， AWS 服務 並在視窗、macOS 和 Linux 上受到支援。如需詳細資訊，請參閱 AWS Command Line Interface。

紅帽 OpenShift

- Red Hat Hybrid Cloud 主控台 — 提供 Web 介面來建立、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 (Rosa) — 提供建立、更新和管理 ROSA 叢集的命令。
- OpenShift CLI (oc) — 提供用於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 無伺服器元件互動的命令，例如 KNative 服務和事件。
- 管道 CLI（ tkn ）-提供使用終端與 OpenShift 管道交互的命令。
- opm CLI-提供可協助操作員開發人員和叢集管理員從終端建立和維護 OpenShift 操作員目錄的命令。
- 操作員 SDK CLI-提供操作員開發人員可以用來構建，測試和部署 OpenShift 操作員的命令。

如何開始使用 ROSA



以下摘要說明的入門程序 ROSA。如需詳細的入門指示，請參閱開始使用 ROSA。

AWS Management Console/AWS CLI

1. 設定 ROSA 依賴 AWS 服務 於提供服務功能的權限。如需詳細資訊，請參閱先決條件。

2. 安裝並設定最新 AWS CLI 工具。如需詳細資訊，請參閱 AWS CLI 使用者指南 AWS CLI中的安裝最新版本的更新。
3. 在ROSA 主控台 ROSA中啟用。

紅帽混合雲主控台ROSA

1. 從 Red Hat 混合式雲端主控台下載最新版本的 ROSA OpenShift CLI 和 CLI。如需詳細資訊，請參閱 Red Hat 文件中的 ROSA CLI 入門。
2. 在 Red Hat 混合式雲端主控台或使用 ROSA CLI 建立 ROSA 叢集。
3. 當您的叢集準備就緒時，請設定身分識別提供者，以授與使用者對叢集的存取權。
4. 以與任何其他 OpenShift 環境相同的方式在 ROSA 叢集上部署和管理工作負載。

定價

的總成本 ROSA 由兩部分組成： ROSA 服務費和 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

依預設， ROSA 服務費用根據工作者節點使用的每 4 個 vCPU 按小時費率計算。所有支援的 AWS 標準區域的服務費用均一致。除了工作者節點服務費用外，含託管控制平面 (HCP) 叢集的 ROSA 還會產生每小時的叢集費用。

ROSA 提供 1 年期和 3 年的服務費合約，您可以購買這些合約，以節省工作者節點的隨需服務費用。如需詳細資訊，請參閱ROSA 合約。

AWS 基礎設施費

AWS 基礎架構費用適用於 AWS 全球基礎架構上託管的基礎工作者節點、基礎結構節點、控制平面節點、儲存和網路資源。 AWS 基礎設施費用因而異 AWS 區域。

下列項目的責任概述 Red Hat OpenShift Service on AWS

本文件概述了 Amazon Web Services (AWS)、Red Hat 以及 Red Hat OpenShift Service on AWS (ROSA) 受管理服務的客戶的責任。如需有關 ROSA 及其元件的詳細資訊，請參閱 Red Hat 文件中的政策與服務定義。

AWS 共同的責任模型定義了保護運行中提供的所有服務的基礎結構的 AWS 責任 AWS 雲端，包括 ROSA。 AWS 基礎架構包括硬體、軟體、網路和執行 AWS 雲端 服務的設施。這種 AWS 責任通常被稱為「雲的安全性」。 ROSA 為了以完全受控的服務形式運作，Red Hat 和客戶必須負責 AWS 責任模型定義為「雲端中的安全性」之服務元素。

Red Hat 負責持續管理 ROSA 叢集基礎架構、基礎應用程式平台及作業系統的安全性。雖然 ROSA 叢集託管在客戶的 AWS 資源上 AWS 帳戶，但是 ROSA 服務元件和 Red Hat 站台可靠性工程師 (SRE) 會透過客戶所建立的 IAM 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架構節點的部署與容量，並維護控制平面節點、基礎架構節點和 Worker 節點的版本。

Red Hat 與客戶共同負責 ROSA 網路管理、叢集記錄、叢集版本控制及容量管理。在 Red Hat 管理 ROSA 服務的同時，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。

概要

下表提供 Red Hat 以及的客戶責任的 AWS概觀 Red Hat OpenShift Service on AWS。

> **Note**
>
> 如果將`cluster-admin`角色新增至使用者，請參閱 Red Hat 企業合約附錄 4 (線上訂閱服務) 中的責任與排除注意事項。

Resource	事件與作業管理	變更管理	訪問和身份授權	安全性與法規遵循	災難復原
客戶資料	客戶	客戶	客戶	客戶	客戶
客戶應用	客戶	客戶	客戶	客戶	客戶
開發者服務	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	紅帽子, 以及, 顧客	紅帽子, 以及, 顧客	紅帽子, 以及, 顧客	Red Hat
應用網路	紅帽子, 以及, 顧客	紅帽子, 以及, 顧客	紅帽子, 以及, 顧客	Red Hat	Red Hat

Resource	事件與作業管理	變更管理	訪問和身份授權	安全性與法規遵循	災難復原
叢集網路	Red Hat	紅帽子, 以及, 顧客	紅帽子, 以及, 顧客	Red Hat	Red Hat
虛擬網路管理	紅帽子, 以及, 顧客	紅帽子, 以及, 顧客	紅帽子, 以及, 顧客	紅帽子, 以及, 顧客	紅帽子, 以及, 顧客
虛擬運算管理 (控制平面、基礎架構和工作者節點)	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
叢集版本	Red Hat	紅帽子, 以及, 顧客	Red Hat	Red Hat	Red Hat
容量管理	Red Hat	紅帽子, 以及, 顧客	Red Hat	Red Hat	Red Hat
虛擬儲存管理	Red Hat	Red Hat	Red Hat	Red Hat	Red Hat
AWS 軟件（公共 AWS 服務）	AWS	AWS	AWS	AWS	AWS
硬體/全球基礎設施AWS	AWS	AWS	AWS	AWS	AWS

按地區劃分的共同責任任務

AWS、Red Hat 與客戶共同負責監控與維護 ROSA 元件。本文件會依地區與作業來定義 ROSA 服務責任。

事件與作業管理

AWS 負責保護執行中提供之所有服務的硬體基礎結構 AWS 雲端。Red Hat 負責管理預設平台網路所需的服務元件。客戶必須負責客戶應用程式資料的事件與作業管理，以及客戶可能已設定的任何自訂網路。

Resource	服務責任	客戶責任
應用網路	紅帽 • 監視原生 OpenShift 路由器服務，並回應警示。	顧客 • 監控應用程式路由的健康狀態，以及其後面的端點。 • 向 AWS 和紅帽報告中斷。
虛擬網路管理	紅帽 • 監視預設平台 Amazon VPC 網路所需的 AWS 負載平衡器、子網路和 AWS 服務 元件。回應警示。	顧客 • 監視 AWS 負載平衡器端點的健全狀況。 • 監控透過 Amazon VPCVPC 對虛擬私人雲端連線、 AWS VPN 連線或潛在問題或安全威脅選擇性設定 AWS Direct Connect 的網路流量。
虛擬儲存管理	紅帽 • 監視用於叢集節點的 Amazon EBS 磁碟區，以及用於 ROSA 服務內建容器映像登錄的 Amazon S3 儲存貯體。回應警示。	顧客 • 監控應用程式資料的健康狀況 • 如果使用客戶管理 AWS KMS keys ，請建立並控制金鑰生命週期和金鑰原則以進行 Amazon EBS 加密。
AWS 軟件（公共 AWS 服務）	AWS • 如需 AWS 事件與作業管理的相關資訊，請參閱 AWS 白皮書中的營運彈性和服務 AWS 持續性。	顧客 • 監控客戶帳戶中 AWS 資源的健康狀況。 • 使用 IAM 工具將適當的權限套用至客戶帳戶中的 AWS 資源。
硬體/全球基礎設施AWS	AWS	顧客

Resource	服務責任	客戶責任
	• 如需 AWS 事件與作業管理的相關資訊，請參閱 AWS 白皮書中的營運彈性和服務 AWS 持續性。	• 設定、管理和監控客戶應用程式和資料，以確保適當執行應用程式和資料安全性控制。

變更管理

AWS 負責保護執行中提供之所有服務的硬體基礎結構 AWS 雲端。Red Hat 負責對客戶將控制的叢集基礎架構和服務進行變更，並維護控制平面節點、基礎架構節點和工作者節點的版本。客戶必須負責啟動基礎架構變更。客戶還負責安裝和維護選購服務、叢集上的網路組態，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	紅帽 • 集中彙總和監控平台稽核記錄。 • 提供並維護記錄操作員，讓客戶能夠為預設應用程式記錄部署記錄堆疊。 • 根據客戶要求提供審計日誌。	顧客 • 在叢集上安裝選用的預設應用程式記錄操作員。 • 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。 • 如果客戶應用程式正在影響記錄堆疊或叢集的穩定性，請調整應用程式記錄檔的大小和頻率。 • 透過支援案例要求平台稽核記錄，以研究特定事件。
應用網路	紅帽 • 設定公用負載平衡器。提供設定私有負載平衡器的功能，並在需要時最多設定一個額外的負載平衡器。	顧客 • 使用物件為專案和網繭網路、網繭輸入和網繭輸出設定非預設網繭網路權限。`NetworkPolicy`

Resource	服務責任	客戶責任
	• 設定原生 OpenShift 路由器服務。提供將路由器設置為私有路由器並添加最多一個額外的路由器碎片的功能。 • 安裝、設定和維護預設內部網繭流量的 OpenShift SDN 元件。 • 提供客戶管理NetworkPolicy 和 EgressNetworkPolicy (防火牆) 物件的能力。	• 使用 OpenShift 叢集管理員為預設應用程式路由要求私人負載平衡器。 • 使用 OpenShift 叢集管理員最多可設定一個額外的公用或私有路由器碎片，以及對應的負載平衡器。 • 針對特定服務要求和設定任何其他服務負載平衡器。 • 設定任何必要的 DNS 轉送規則。
叢集網路	紅帽 • 設定叢集管理元件，例如公用或私人服務端點，以及與 Amazon VPC元件的必要整合。 • 設定工作者、基礎結構和控制平面節點之間進行內部叢集通訊所需的內部網路元件。	顧客 • 佈建叢集時，透過 OpenShift 叢集管理員為機器 CIDR、服務 CIDR 和網繭 CIDR 提供選用的非預設 IP 位址範圍。 • 要求在叢集建立時或透過 OpenShift 過叢集管理員建立叢集後將 API 服務端點設為公開或私有。

Resource	服務責任	客戶責任
虛擬網路管理	紅帽 • 設定並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。 • 提供客戶管理與內部部署資源的 AWS VPN 連線能力、Amazon VPCVPC 連線，以及透過 OpenShift 叢集管理員 AWS Direct Connect 所需的能力。 • 讓客戶能夠建立和部署 AWS 負載平衡器，以搭配服務負載平衡器使用。	顧客 • 設定和維護選用 Amazon VPC 元件，例如 Amazon VPC至 VPC 連線、 AWS VPN 連線或。 AWS Direct Connect • 針對特定服務要求和設定任何其他負載平衡器。
虛擬運算管理	紅帽 • 設定並設定 ROSA 控制平面和資料平面，以使用 Amazon EC2 執行個體進行叢集運算。 • 監視和管理叢集上 Amazon EC2 控制平面和基礎架構節點的部署。	顧客 • 透過使用叢集管理 Amazon EC2 員或 ROSA CLI 建立機器 OpenShift 集區來監視和管理工作者節點。 • 管理客戶部署應用程式和應用程式資料的變更。

Resource	服務責任	客戶責任
叢集版本	紅帽 • 啟用升級排程程序。 • 監控升級進度並解決遇到的任何問題。 • 針對次要和維護升級發佈變更記錄檔和版本說明。	顧客 • 立即排定維護版本升級，以供將 future 使用，或自動升級。 • 確認並排程次要版本升級。 • 確定叢集版本保留在受支援的次要版本上。 • 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	紅帽 • 監控控制平面的使用情況。控制平面包括控制平面節點和基礎架構節點。 • 調整控制平面節點並調整大小，以維持服務品質。	顧客 • 監視工作者節點使用率，並在適當的情況下啟用 auto 擴展功能。 • 決定叢集的擴展策略。如需有關機器集區的詳細資訊，請參閱其他資源。 • 使用提供的 OpenShift 叢集管理員控制項，視需要新增或移除其他 Worker 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	紅帽 • 設定並配置 Amazon EBS 為叢集佈建本機節點儲存體和持續性磁碟區儲存體。 • 設定並設定內建映像登錄以使用 Amazon S3 值區儲存空間。 • 定期修剪中的映像登錄資源， Amazon S3 以最佳化 Amazon S3 使用率和叢集效能。	顧客 • 選擇性地設定 Amazon EBS CSI 驅動程式或 Amazon EFS CSI 驅動程式，以在叢集上佈建持續性磁碟區。

Resource	服務責任	客戶責任

AWS 軟件（公共 AWS 服務）	AWS
	
	運算
	
	• 提 Amazon EC2 供用於 ROSA 控制平面、基礎結構和工作者節點的服務。
	
	儲存
	
	• 提供 Amazon EBS 以允許 ROSA 服務為叢集佈建本機節點儲存區和持續性磁碟區儲存體。
	
	聯網
	
	• 提供下列 AWS 雲端 服務以滿足 ROSA 虛擬網路基礎架構的需求：
	  • Amazon VPC
	  • Elastic Load Balancing
	  • IAM
	• 提供下列選用 AWS 服務 整合 ROSA：
	  • AWS VPN
	  • AWS Direct Connect
	  • AWS PrivateLink
	  • AWS Transit Gateway
		顧客
		
		• 使用與 IAM 主體或 AWS STS 臨時安全登入資料相關聯的存取金鑰 ID 和秘密存取金鑰來簽署要求。
		• 指定叢集建立期間要使用的 VPC 子網路。
		• 選擇性地設定客戶管理的 VPC 以搭配叢集使用 ROSA 。

Resource	服務責任	客戶責任
硬體/全球基礎設施AWS	AWS • 如需資 AWS 料中心管理控制的相關資訊，請參閱 AWS 雲端 安全性頁面上的我們的控制項。 • 如需有關變更管理最佳實務的資訊，請參閱 AWS 解決方案庫 AWS中的變更管理指引。	顧客 • 針對客戶應用程式和託管於 AWS 雲端.

訪問和身份授權

存取和身分識別授權包括管理叢集、應用程式和基礎結構資源的授權存取權限的責任。這包括提供存取控制機制、驗證、授權和管理資源存取等工作。

Resource	服務責任	客戶責任
日誌	紅帽 • 遵守以業界標準為基礎的分層內部存取流程，以取得平台稽核記錄。 • 提供原生 OpenShift RBAC 功能。	顧客 • 將 OpenShift RBAC 設定為控制專案的存取，並透過擴充專案的應用程式記錄來控制。 • 對於協力廠商或自訂應用程式記錄解決方案，客戶需負責存取管理。
應用網路	紅帽 • 提供原生 OpenShift RBAC 和`dedicated-admin` 功能。	顧客 • 根據需要配置 OpenShift `dedicated-admin` 和 RBAC 以控制對路由配置的訪問。

Resource	服務責任	客戶責任
		• 管理 Red Hat 的 Red Hat 組織管理員，以授與 OpenShift 叢集管理員的存取權。叢集管理員可用來設定路由器選項，並提供服務負載平衡器配額。
叢集網路	紅帽 • 透過 OpenShift 叢集管理員提供客戶存取控制。提供原生 OpenShift RBAC 和`dedicated-admin` 功能。	顧客 • 根據需要配置 OpenShift `dedicated-admin` 和 RBAC 以控制對路由配置的訪問。 • 管理 Red Hat 組織的 Red Hat 帳號成員資格。 • 管理 Red Hat 的組織管理員，以授與 OpenShift 叢集管理員的存取權。
虛擬網路管理	紅帽 • 透過 OpenShift 叢集管理員提供客戶存取控制。	顧客 • 透過 OpenShift 叢集管理員管理 AWS 元件的選用使用者存取權。
虛擬運算管理	紅帽 • 透過 OpenShift 叢集管理員提供客戶存取控制。	顧客 • 透過 OpenShift 叢集管理員管理 AWS 元件的選用使用者存取權。 • 建立啟用 ROSA 服務存取所需的 IAM 角色和附加原則。

Resource	服務責任	客戶責任
虛擬儲存管理	紅帽 • 透過 OpenShift 叢集管理員提供客戶存取控制。	顧客 • 透過 OpenShift 叢集管理員管理 AWS 元件的選用使用者存取權。 • 建立啟用 ROSA 服務存取所需的 IAM 角色和附加原則。
AWS 軟件（公共 AWS 服務）	AWS 運算 • 提 Amazon EC2 供用於 ROSA 控制平面、基礎結構和工作者節點的服務。 儲存 • 提供 Amazon EBS，用於允許 ROSA 為叢集佈建本機節點儲存區和持續性磁碟區儲存體。 • 提供 Amazon S3，用於服務的內置映像註冊表。 聯網 • 提供 AWS Identity and Access Management (IAM)，由客戶用來控制對在客戶帳戶上執行之 ROSA 資源的存取。	顧客 • 建立啟用 ROSA 服務存取所需的 IAM 角色和附加原則。 • 使用 IAM 工具將適當的權限套用至客戶帳戶中的 AWS 資源。 • 若要 ROSA 在整個 AWS 組織中啟用，客戶必須負責管理 AWS Organizations 系統管理員。 • 若要 ROSA 在整個 AWS 組織中啟用，客戶必須負責使用分配 ROSA 軟體權利授權 AWS License Manager。

Resource	服務責任	客戶責任
硬體/全球基礎設施AWS	AWS • 如需資 AWS 料中心實體存取控制的相關資訊，請參閱 AWS 雲端 安全性頁面上的我們的控制項。	顧客 • 客戶對 AWS 全球基礎設施概不負責。

安全性與法規遵循

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	紅帽 • 將叢集稽核記錄傳送至 Red Hat SIEM 以分析安全性事件。保留稽核記錄一段定義的時間，以支援鑑識分析。	顧客 • 分析安全事件的應用程式記錄檔。 • 如果需要的保留時間超過預設記錄堆疊所提供的更長時間，請透過記錄附屬容器或協力廠商記錄應用程式，將應用程式記錄檔傳送至外部端點。
虛擬網路管理	紅帽 • 監控虛擬網路元件，找出潛在問題和安全威脅。 • 使用公用 AWS 工具進行額外的監控和保護。	顧客 • 監控選用的已設定虛擬網路元件，找出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防護。
虛擬運算管理	紅帽	顧客

Resource	服務責任	客戶責任
	• 監控虛擬運算元件，找出潛在問題和安全性威脅。 • 使用公用 AWS 工具進行額外的監控和保護。	• 監控選用的已設定虛擬網路元件，找出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防護。
虛擬儲存管理	紅帽 • 監控虛擬儲存元件，找出潛在問題和安全威脅。 • 使用公用 AWS 工具進行額外的監控和保護。 • 依預設，使用 Amazon EBS 提供的 AWS 受管理 KMS 金鑰，將 ROSA 服務設定為加密控制平面、基礎結構和背景工作者節點磁碟區資料。 • 將 ROSA 服務設定為使用預設儲存區類別的客戶持續性磁碟區與 Amazon EBS 提供的 AWS 受管 KMS 金鑰加密。 • 讓客戶能夠使用受管理的客戶 KMS key 來加密持續性磁碟區。 • 將容器映像登錄設定為使用具有 Amazon S3 受管理金鑰的伺服器端加密靜態映像登錄資料 (SSE-3)。 • 提供客戶建立公用或私人 Amazon S3 映像檔登錄的功能，以保護其容器映像不受未經授權的使用者存取。	顧客 • 佈建 Amazon EBS 磁碟區。 • 管理 Amazon EBS 磁碟區儲存空間，以確保有足夠的儲存空間可作為中的磁碟區掛接 ROSA。 • 建立持續性磁碟區宣告，並透過 OpenShift 叢集管理員產生持續性磁碟區。

Resource	服務責任	客戶責任
AWS 軟件（公共 AWS 服務）	AWS 運算 • 提供 Amazon EC2，用於 ROSA 控制平面，基礎結構和工作節點。如需詳細資訊，請參閱 Amazon EC2 使用指南Amazon EC2中的「基礎結構安全性」。 儲存 • 提供 Amazon EBS，用於 ROSA 控制平面、基礎結構和工作者節點磁碟區，以及 Kubernetes 持續性磁碟區。如需詳細資訊，請參閱《 Amazon EC2 使用指南》Amazon EC2中的〈資料保護〉。 • 提供 AWS KMS， ROSA 用於加密控制平面、基礎結構、背景工作節點磁碟區和持續性磁碟區。如需詳細資訊，請參閱《使用指南》中的 Amazon EC2 〈Amazon EBS 加密〉。 • 提供 Amazon S3，用於 ROSA 服務的內建容器映像登錄。若要取得更多資訊，請參閱 Amazon S3 使用指南中的Amazon S3 安全性。	顧客 • 確保遵循安全性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，請參閱中的基礎結構安全性 Amazon EC2和 Amazon EC2. • 監控選用的已設定虛擬網路元件，找出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防護。 • 建立選用的客戶受管 KMS 金鑰，並使用 KMS 金鑰加密 Amazon EBS 持續性磁碟區。 • 監控虛擬存儲中的客戶數據，以查找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，以增加隱私並控制 AWS 全球基礎設施上的網絡訪問，包括內置的網絡防火牆 Amazon VPC，私有或專用網絡連接，以及安全設施之間 AWS 的 AWS 全球和區域網絡上的所有流量自動加密。如需詳細資訊，請參閱安全性簡介白皮書中的AWS 共同責任模型與基礎結構 AWS 安全性。	
硬體/全球基礎設施AWS	AWS • 提供 ROSA 用於提供服務功能的 AWS 全球基礎架構。如需有關 AWS 安全性控制的詳細資訊，請參閱 AWS 白皮書中的 AWS 基礎結構安全性。 • AWS 使用和 Security Hub 等工具，為客戶提供文件以管理合規需求， AWS Artifact 並檢查其 AWS 安全狀態。	顧客 • 設定、管理和監控客戶應用程式和資料，以確保適當執行應用程式和資料安全性控制。 • 使用 IAM 工具將適當的權限套用至客戶帳戶中的 AWS 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製和組態，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	紅帽 • 還原或重新建立平台運作所需的受影響虛擬網路元件。	顧客 • 在可能的情況下，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	紅帽 • 監控叢集並取代故障的 Amazon EC2 控制平面或基礎架構節點。 • 提供客戶手動或自動取代失敗的 Worker 節點的能力。	顧客 • 透過 OpenShift 叢集管理員或 ROSA CLI 編輯機器集區組態，以取代失敗的 Amazon EC2 Worker 節點。
虛擬儲存管理	紅帽 • 對於 AWS IAM 使用使用者認證建立的 ROSA 叢集，請透過每小時、每日和每週的磁碟區快照來備份叢集上的所有 Kubernetes 物件。	顧客 • 備份客戶應用程式和應用程式資料。
AWS 軟件（公共 AWS 服務）	AWS 運算 • 提 Amazon EC2 供支援資料備援的功能，例如 Amazon EBS 快照和 Amazon EC2 Auto Scaling. 如需詳細資訊，請參閱《使用指南》Amazon EC2中的 Amazon EC2 〈復原性〉。	顧客 • 設定 ROSA 異地同步備份叢集以改善容錯能力和叢集可用性。 • 使用 Amazon EBS CSI 驅動程式佈建持續性磁碟區以啟用磁碟區快照。 • 建立持續性磁碟區的 CSI 磁 Amazon EBS 碟區快照。

Resource	服務責任	客戶責任
	儲存 • 提供 ROSA 服務和客戶透過磁碟區快照備份叢集上 Amazon EBS 磁 Amazon EBS 碟區的功能。 • 如需支援資料復原 Amazon S3 功能的相關資訊，請參閱. Amazon S3 聯網 • 如需支援資料復原 Amazon VPC 功能的相關資訊，請參閱《 Amazon VPC 使用指南》Amazon Virtual Private Cloud中的〈復原性〉。	
硬體/全球基礎設施AWS	AWS • 提供可跨可用區域擴充控制平面、基礎架構和工作者節點的 AWS 全球基礎架構。ROSA 此功能可 ROSA 協調區域之間的自動容錯移轉，而不會中斷。 • 如需災難復原最佳做法的詳細資訊，請參閱 AWS Well-Architected 的架構中雲端中的災難復原選項。	顧客 • 設定 ROSA 異地同步備份叢集以改善容錯能力和叢集可用性。

客戶對資料和應用程式的責任

客戶必須負責部署到的應用程式、工作負載和資料 Red Hat OpenShift Service on AWS。然 AWS 而，Red Hat 提供了各種工具來協助客戶管理平台上的資料和應用程式。

Resource	紅帽如何 AWS 幫助	客戶責任
客戶資料	紅帽 • 依照產業安全性與合規性標準所定義，維護資料加密的平台層級標準。 • 提供 OpenShift 元件以協助管理應用程式資料，例如機密。 • 啟用與資料服務整合，例 Amazon RDS 如儲存和管理叢集外部的資料和/或 AWS。 AWS • 提供 Amazon RDS 讓客戶能夠在叢集外部儲存和管理資料。	顧客 • 維護儲存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這些資料的責任。
客戶應用	紅帽 • 佈建已安裝 OpenShift 元件的叢集，讓客戶可以存取 OpenShift 和 Kubernetes API 來部署和管理容器化應用程式 • 使用映像提取密碼建立叢集，讓客戶部署可以從 Red Hat 容器目錄登錄中提取映像檔。 • 提供 OpenShift API 的存取權，讓客戶可以用來設定操作員，將社群 AWS、第三	顧客 • 維護客戶與協力廠商應用程式、資料及完整應用程式生命週期的責任。 • 如果客戶使用操作員或外部映像將 Red Hat、社群、第三方、他們自己的服務或其他服務新增至叢集，則客戶必須負責處理這些服務，並與適當的供應商 (包括 Red Hat) 合作來解決任何問題。 • 使用提供的工具和功能來設定和部署；保持最新狀態；設定資源要求和限制

Resource	紅帽如何 AWS 幫助	客戶責任
	方和 Red Hat 服務新增至叢集。 • 提供儲存類別和外掛程式，以支援用於客戶應用程式的持續性磁碟區。 • 提供容器映像登錄，讓客戶能夠將應用程式容器映像安全地儲存在叢集上，以部署和管理應用程式。 AWS • 提供 Amazon EBS 支援與客戶應用程式搭配使用的持續性磁碟區。 • 提供 Amazon S3 以支援 Red Hat 佈建容器映像檔登錄。	；調整叢集大小以擁有足夠的資源來執行應用程式；設定權限；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；以及管理其高可用性和彈性的工作負載。 • 維護監視執行應用程式的責任 Red Hat OpenShift Service on AWS，包括安裝和操作軟體以收集測量結果、建立警示及保護應用程式中的機密。

部署選項

ROSA 提供兩種叢集部署模式：含託管控制平面的 ROSA (含有 HCP 的 ROSA) 和 ROSA 經典版。透過 ROSA 搭配 HCP，每個叢集都有一個專屬的控制平面，這個平面會隔離在 Red Hat 內， AWS 帳戶並由 Red Hat 管理。使用 ROSA 經典版，叢集控制平面基礎結構託管在客戶的 AWS 帳戶。

ROSA 搭配 HCP 提供更有效率的控制平面架構，有助於減少執行時產生的 AWS 基礎架構費用， ROSA 並加快叢集建立時間。兩種叢集部署模型都可以在 AWS ROSA 主控台中啟用。您可以選擇在使用 ROSA CLI 佈建 ROSA 叢集時，選取要使用的部署模型。

> **Note**
>
> 含託管控制平面的 ROSA 目前不提供合規性認證或聯邦資訊處理標準 (FIPS)。如需詳細資訊，請參閱 Red Hat 文件中的合規性。

羅莎與 HCP 和羅莎經典之間的區別

ROSA 與 HCP 和 ROSA 經典之間存在幾個技術差異。

	羅莎與 HCP	羅莎經典
叢集基礎架構主	• 控制平面元件，例如 etcd、API 伺服器和 oauth，都是以紅帽擁有並受管理的方式託管。 AWS 帳戶背景工作者節點基礎結構託管在客戶的 AWS 帳戶。不使用專用基礎結構節點；平台元件會部署至 Worker 節點。	• 控制平面元件託管在客戶的 AWS 帳戶基礎架構和工作者節點旁邊。
佈建時間	• 大約 10 分鐘	• 所需時間約 40 分鐘。
架構	• 控制平面基礎架構由 Red Hat 完全管理。除了透過專用且明確公開的端點外，最終客戶無法直接使用控制平面基礎架構。 • 工作者節點託管在客戶的 AWS 帳戶。	• 控制平面基礎架構託管在客戶的 AWS 帳戶。 • 工作者節點託管在客戶的 AWS 帳戶。
AWS Identity and Access Management	• 使用 AWS 受管理的策略。	• 使用由服務定義的客戶管理策略。
最小 Amazon EC2 覆蓋區	• 一個叢集至少需要在客戶的兩個節點上託管 AWS 帳戶。	• 一個叢集至少需要在客戶的節點上託管七個節點 AWS 帳戶。
叢集佈建	• 使用 ROSA CLI 佈建叢集。 • 客戶佈建將控制平面元件部署到 Red Hat 的叢集 AWS 帳戶。	• 使用 ROSA CLI 或網頁使用者介面佈建叢集。 • 叢集控制平面、工作者節點和基礎結構節點會佈建到客戶的節點中 AWS 帳戶。

	羅莎與 HCP	羅莎經典
	• 客戶佈建機器集區，以將工作者節點部署到客戶的節點 AWS 帳戶。	
升級	• 分別升級控制平面和機器集區。	• 必須同時升級整個叢集。
AWS 區域	• 如需 AWS 區域 可用性的資訊，請參閱 AWS 一般參考指南中的Red Hat OpenShift Service on AWS 端點和配額。	• 如需 AWS 區域 可用性的資訊，請參閱 AWS 一般參考指南中的Red Hat OpenShift Service on AWS 端點和配額。
合規	• 如需符合性資訊，請參閱 Red Hat 文件中的合規性。	• 如需符合性資訊，請參閱 Red Hat 文件中的合規性。

開始使用 ROSA

Red Hat OpenShift Service on AWS (ROSA) 是一項受管理服務，您可以使用 Red Hat OpenShift 企業 Kubernetes 平台來建置、擴充及部署容器化應用程式。 AWS

ROSA 叢集部署模型

ROSA 支援兩種叢集部署模式：含託管控制平面的 ROSA (含 HCP 的 ROSA) 和 ROSA 經典版。ROSA 搭配 HCP 提供更有效率的控制平面架構，可降低 AWS 基礎架構成本， ROSA 並加快叢集建立時間。如需 ROSA 搭配 HCP 和 ROSA 傳統版的相關資訊，請參閱部署選項。

> **Note**
>
> 使用託管控制平面的 ROSA 目前不提供 FIPS。

入門指南

有四個入門指南可用於將應用程式部署到新建立的 ROSA 叢集。每個教學課程涵蓋以下內容：

- 啟用 ROSA 服務並設定 AWS 先決條件
- 建立必要的 IAM 角色和原則
- 建立 ROSA 叢集
- 建立叢集管理員以快速存取叢集
- 設定身分識別提供者
- 授與使用者對叢集的存取權
- 將應用程式部署到叢集
- 刪除叢集和叢集資源

透過 HCP 開始使用 ROSA 服務

透過 ROSA 搭配 HCP，您可以使用 AWS STS 和 ROSA CLI 建立具有必要 IAM 角色和原則的叢集。如需 ROSA 與 HCP 相關 IAM 原則的相關AWS 資 IAM訊，請參閱. ROSA

建立叢集之後，您可以使用 Red Hat 混合雲主控台或 OpenShift CLI 將公用應用程式工作負載部署到叢集。如需將應用程式部署到具有 HCP 叢集的新建 ROSA 的步驟，請參閱在 auto 模式下使用 ROSA CLI 使用 HCP 開始使用 ROSA。

開始使用 ROSA 經典版

使用 ROSA 典型，您可以使用 AWS STS 和 ROSA CLI 建立具有必要 IAM 角色和原則附加的叢集。建立叢集之後，您就可以使用 Red Hat 混合雲主控台或 OpenShift CLI 將公用應用程式工作負載部署到叢集。如需開始使用 ROSA CLI 自動叢集建立 (auto) 模式的步驟，請參閱在 auto 動模式下使用 ROSA CLI 開始使用 ROSA 傳統版。如需開始使用 ROSA CLI 手動叢集建立 (manual) 模式的步驟，請參閱在手動模式下使用 ROSA CLI 開始使用 ROSA 傳統版。

如果您需要將 ROSA 傳統叢集和應用程式工作負載設為私有，請參閱 ROSA 典型使用入門 AWS PrivateLink。

在 auto 模式下使用 ROSA CLI 開始使用 ROSA 搭配 HCP

下列各節說明如何使用AWS STS和 ROSA CLI 使用託管控制平面 (含有 HCP 的 ROSA) 開始使用 ROSA。如需 ROSA 搭配 HCP 的詳細資訊，請參閱部署選項。

ROSACLI 使用auto模manual式或模式來建立IAM資源，以及建立. ROSA 叢集 auto模式會自動建立必要的IAM角色和原則以及 OIDC 提供者。 manualmode 輸出手動創建IAM資源所需的AWS CLI命令。通過使用manual模式，您可以在手動運行之前檢閱生成的AWS CLI命令。使用manual模式，您也可以將命令傳遞給組織中的其他管理員或群組，以便他們可以建立資源。

本文件中的程序使用 ROSA CLI auto 模式，為含有 HCP 的 ROSA 建立必要的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
- 步驟 1：啟用ROSA並設定先決條件
- 步驟 2：使用 HCP 叢集為 ROSA 建立Amazon VPC架構
- 步驟 3：創建所需的IAM角色和 OpenID Connect 配置
- 步驟 4：使用和 ROSA CLI auto 模式建立含有 HCP 叢集AWS STS的 ROSA
- 步驟 5：設定身分識別提供者並授與叢集存取權
- 步驟 6：授與使用者存取 叢集

先決條件

開始之前，請確定您已完成下列動作：

- 安裝和配置最新的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 ROSACLI 入門。
- Service Quotas必須為、和設定必要的服務配額 Amazon EC2 Amazon VPCAmazon EBS，才 Elastic Load Balancing能建立和執行ROSA叢集。 AWS或 Red Hat 可能會根據問題解決的要求，代表您要求增加服務配額。若要檢視所需的配額，請參閱AWS一般參考中的Red Hat OpenShift Service on AWS端點和配額。
- 若要獲得的AWS支援ROSA，您必須啟用AWS商務、企業版加速或企業支援方案。Red Hat 可能會代表您要求AWS支援，以便解決問題。如需詳細資訊，請參 S upport ROSA。若要啟用AWS Support，請參閱AWS Support頁面。
- 如果您使用AWS Organizations來管理AWS 帳戶該主機ROSA服務，組織的服務控制原則 (SCP) 必須設定為允許 Red Hat 不受限制地執行 SCP 中列出的政策動作。如需詳細資訊，請參閱 ROSASCP 疑難排解說明文件。如需 SCP 的詳細資訊，請參閱服務控制原則 (SCP)。
- 如果AWS STS將ROSA叢集與部署到默認情況下禁用的啟用AWS 區域中，則必須使用以下命令將中所有區域的安全性權杖更新為版本 2。AWS 帳戶

```
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 AWS 一般參考AWS 區域中的管理。

步驟 1：啟用ROSA並設定先決條件

若要建立 ROSA叢集，您必須先在AWSROSA主控台中啟用ROSA服務。主AWSROSA控台會驗證您是否AWS 帳戶具有必要的AWS Marketplace權限、服務配額以及名為的 Elastic Load Balancing (ELB) 服務連結角色。`AWSServiceRoleForElasticLoadBalancing`如果缺少任何先決條件，主控台會提供如何設定帳戶以符合先決條件的指引。

1. 導覽至 ROSA 主控台。
2. 選擇 Get started (開始使用)。
3. 在 [驗證ROSA必要條件] 頁面上，選取 [我同意與 Red Hat 分享我的聯絡資訊]。
4. 選擇「啟用」ROSA。
5. 在頁面驗證您的服務配額符合ROSA先決條件並建立 ELB 服務連結角色後，請開啟新的終端機工作階段，以ROSA叢集使用 CLI 建立您的第一個終端機工作階段。ROSA

步驟 2：使用 HCP 叢集為 ROSA 建立Amazon VPC架構

若要使用 HCP 建立 ROSA叢集，您必須先設定自己的Amazon VPC架構，以將解決方案部署到。ROSA 搭配 HCP 時，客戶必須為每個用於建立叢集的可用區域設定至少一個公用和私有子網路。對於單一可用區叢集，僅使用可用區域。對於異地同步備份叢集，需要三個可用區域。

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

下列程序會使AWS CLI用在單一可用區叢集的單一可用區域中建立公用和私有子網路。所有叢集資源都位於私有子網路中。公用子網路會使用 NAT 閘道將輸出流量路由傳送至網際網路。

此範例使用的 CIDR 區塊`10.0.0.0/16`做為. 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。

1. 透過執行下列命令來設定叢集名稱的環境變數。

```
ROSA_CLUSTER_NAME=rosa-hcp
```

2. 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
```

   上述命令會傳回新 VPC 的 ID。以下為範例輸出。

```
vpc-0410832ee325aafea
```

3. 使用上一個步驟中的 VPC ID，使用變數標記 VPC。`ROSA_CLUSTER_NAME`

```
aws ec2 create-tags --resources <VPC_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

4. 在 VPC 上啟用 DNS 主機名稱支援。

```
aws ec2 modify-vpc-attribute --vpc-id <VPC_ID_VALUE> --enable-dns-hostnames
```

5. 使用 10.0.1.0/24 CIDR 區塊在 VPC 中建立公用子網路，並指定應在其中建立資源的可用區域。

> **Important**
>
> 建立子網路時，請確定子網路建立至具有可用ROSA執行個體類型的可用區域。如果您未選擇特定的可用區域，則會在您指定的任何一個可用區域中AWS 區域建立子網路。
> 若要指定特定的可用區域，請使用create-subnet命令中的--availability zone引數。您可以使用指rosa list instance-types令列出所有可用的ROSA例證類型。若要檢查指定的可用區域是否有執行個體類型可用，請使用下列命令。
>
> ```
> aws ec2 describe-instance-type-offerings --location-type availability-zone --
> filters Name=location,Values=<availability_zone> --region <region> --output
>  text | egrep "<instance_type>"
> ```

> **Important**
>
> ROSA 搭配 HCP 時，客戶必須為每個用於建立叢集的可用區域設定至少一個公用和私有子網路。對於單一可用區叢集，只需要一個可用區域。對於異地同步備份叢集，需要三個可用區域。如果不符合這些需求，叢集建立會失敗。

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.1.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

上述命令會傳回新子網路的 ID。以下為範例輸出。

```
subnet-0b6a7e8cbc8b75920
```

6. 使用上一個步驟中的子網路 ID，使用ROSA_CLUSTER_NAME-public變數標記子網路。

```
aws ec2 create-tags --resources <PUBLIC_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-public
```

7. 使用 10.0.0.0/24 CIDR 區塊在 VPC 中建立私有子網路，並指定部署公用子網路的相同可用區域。

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.0.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

上述命令會傳回新子網路的 ID。以下為範例輸出。

```
subnet-0b6a7e8cbc8b75920
```

8. 使用上一個步驟中的子網路 ID，使用ROSA_CLUSTER_NAME-private變數標記子網路。

```
aws ec2 create-tags --resources <PRIVATE_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

9. 為輸出流量建立網際網路閘道，並將其附加至 VPC。

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output
 text

aws ec2 attach-internet-gateway --vpc-id <VPC_ID_VALUE> --internet-gateway-id
 <IG_ID_VALUE>
```

10.使用ROSA_CLUSTER_NAME變數標記網際網路閘道。

```
aws ec2 create-tags --resources <IG_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

11.為輸出流量建立路由表，將其與公用子網路建立關聯，並設定要路由到網際網路閘道的流量。

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PUBLIC_SUBNET_ID> --route-table-id
 <PUBLIC_RT_ID>
```

```
aws ec2 create-route --route-table-id <PUBLIC_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <IG_ID_VALUE>
```

12.使用ROSA_CLUSTER_NAME變數標記公用路由表格，並驗證路由表是否已正確設定。

```
aws ec2 create-tags --resources <PUBLIC_RT_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME

aws ec2 describe-route-tables --route-table-id <PUBLIC_RT_ID>
```

13.使用彈性 IP 位址在公用子網路中建立 NAT 閘道，以啟用通往私有子網路的流量。

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text

aws ec2 create-nat-gateway --subnet-id <PUBLIC_SUBNET_ID> --allocation-id
 <EIP_ADDRESS>  --query NatGateway.NatGatewayId --output text
```

14.使用$ROSA_CLUSTER_NAME變數標記 NAT 閘道和彈性 IP 位址。

```
aws ec2 create-tags --resources <EIP_ADDRESS>  --resources <NAT_GATEWAY_ID> --tags
 Key=Name,Value=$ROSA_CLUSTER_NAME
```

15.為私有子網路流量建立路由表，將其與私有子網路建立關聯，並設定要路由至 NAT 閘道的流量。

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PRIVATE_SUBNET_ID> --route-table-id
 <PRIVATE_RT_ID>

aws ec2 create-route --route-table-id <PRIVATE_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <NAT_GATEWAY_ID>
```

16.使用$ROSA_CLUSTER_NAME-private變數標記私有路由表和彈性 IP 位址。

```
aws ec2 create-tags --resources <PRIVATE_RT_ID> <EIP_ADDRESS> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

步驟 3：創建所需的IAM角色和 OpenID Connect 配置

使用 HCP 叢集建立 ROSA 之前，您必須建立必要的IAM角色和原則，以及 OpenID Connect (OIDC) 設定。如需有關 ROSA 與 HCP 的IAM角色和原則的詳細AWS資IAM訊，請參閱. ROSA

此程序會使用 ROSA CLI 的auto模式，自動建立建立含 HCP 叢集之 ROSA 所需的 OIDC 組態。

1. 建立必要的IAM帳號角色和策略。

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

-force-policy-creation 參數會更新任何現有的角色和原則。如果沒有角色和策略存在，則命令會改為建立這些資源。

> **Note**
>
> 如果您的離線訪問令牌已過期，ROSACLI 將輸出一條錯誤消息，指出您的授權令牌需要更新。如需疑難排解的步驟，請參閱疑難排解 ROSA CLI 過期離線存取權杖。

2. 建立 OpenID Connect (OIDC) 組態，以啟用叢集的使用者驗證。此組態已註冊，以便與 OpenShift 叢集管理員 (OCM) 搭配使用。

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

3. 複製 ROSA CLI 輸出中提供的 OIDC 組態識別碼。稍後需要提供 OIDC 組態識別碼，以建立含有 HCP 叢集的 ROSA。
4. 若要確認與您的使用者組織相關聯之叢集可用的 OIDC 組態，請執行下列命令。

```
rosa list oidc-config
```

5. 建立必要的IAM操作員角色，並<OIDC_CONFIG_ID>以先前複製的 OIDC 組態 ID 取代。

   Example

> **Important**
>
> 建立「操作員」角色<PREFIX_NAME>時，您必須在中提供前置詞。如果不這樣做會產生錯誤。

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

6. 若要確認已建立IAM操作員角色，請執行下列命令：

```
rosa list operator-roles
```

步驟 4：使用和 ROSA CLI **auto** 模式建立含有 HCP 叢集AWS STS的 ROSA

您可以使叢集用 AWS Security Token Service (AWS STS) 和 ROSA CLI 中提供的auto模式建立含有 HCP 的 ROSA。您可以選擇使用公用 API 和輸入或私有 API 和輸入來建立叢集。

您可以叢集使用單一可用區域 (單一可用區域) 或多個可用區域 (異地同步備份) 建立。在任何一種情況下，您機器的 CIDR 值都必須符合 VPC 的 CIDR 值。

下列程序會使用指rosa create cluster --hosted-cp令來建立具有 H 叢集 CP 的單一可用區 ROSA。若要建立異地同步備份叢集，請multi-az在指令中指定您要部署的每個私有子網路的私有子網路 ID。

1. 使用下列其中一個命令建立含 HCP 叢集的 ROSA。
   - 使用公用 API 和輸入建立具有 HCP 叢集的 ROSA，並指定叢集名稱、操作員角色前置詞、OIDC 組態識別碼，以及公用和私有子網路 ID。

     ```
     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>
     ```

   - 使用私有 API 和輸入建立具有 HCP 叢集的 ROSA，並指定叢集名稱、操作員角色前置詞、OIDC 組態識別碼和私有子網路 ID。

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

2. 檢查您的叢集.

```
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，請參閱疑難排解ROSA叢集建立問題。
> 若要聯絡AWS Support或 Red Hat Support 人員尋求協助，請參閱支援ROSA。

3. 透過觀看 OpenShift 安裝程式記錄來追蹤叢集建立進度。

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

步驟 5：設定身分識別提供者並授與叢集存取權

ROSA包括一個內置的 OAuth 服務器。建立完成後叢集，您必須將 OAuth 設定為使用身分識別提供者。然後，您可以將使用者新增至已設定的身分識別提供者，以授與他們存取您的叢集. 您可以視需要授與這些使用者`cluster-admin`或`dedicated-admin`權限。

您可以為您的 ROSA叢集. 支援的類型包括 GitHub 企業 GitHub、 GitLab、谷歌、LDAP、OpenID Connect 和 HTPassWD 身份提供者。

> **Important**
>
> HTPasswd 身分提供者僅包含在內，以便建立單一靜態系統管理員使用者。HTPasswd 不支援做為的一般使用身分識別提供者。ROSA

下列程序會將 GitHub 身分識別提供者設定為範例。如需有關如何設定每個支援的身分識別提供者類型的指示，請參閱設定的身分識別提供者AWS STS。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 如果您沒有 GitHub 組織可用於您的身分識別佈建叢集，請建立一個組織。如需詳細資訊，請參閱 GitHub 文件中的步驟。
3. 使用 ROSA CLI 的互動模式，為您的叢集設定身分識別提供者。

```
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. 開啟輸出中的 URL，並<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] 以在 GitHub 組織中註冊新的 OAuth 應用程式。
7. 使用 GitHub OAuth 頁面中的資訊，透過執行下列命令來填入剩餘的`rosa create idp`互動式提示。取代 GitHub OAuth 應用程式中的認證，<GITHUB_CLIENT_ID>並加<GITHUB_CLIENT_SECRET>以取代。

```
...
? 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**
>
> 身分識別提供者組態可能需要大約兩分鐘的時間才會變成作用中狀態。如果您設定了`cluster-admin`使用者，則可以執行`oc get pods -n openshift-authentication --watch`以監視使用更新的組態重新部署 OAuth 網繭。

8. 確認身分識別提供者已正確設定。

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

步驟 6：授與使用者存取 叢集

您可以將使用者新增至已設定的叢集身分識別提供者，以授與使用者存取您的權限。

下列程序會將使用者新增至已設定為識別佈建的 GitHub 組織至叢集。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 邀請需要叢集存取您 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。

步驟 7：將管理員權限授與使用者

將使用者新增至設定的身分識別提供者後，您可以授與您的使用者`cluster-admin`或`dedicated-admin`權限叢集。

設定`cluster-admin`權限

1. 執行下列命令以授與`cluster-admin`權限。將`<IDP_USER_NAME>`和取代為您`<CLUSTER_NAME>`的使用者和叢集名稱。

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

2. 確認使用者是否列為`cluster-admins`群組的成員。

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

設定**dedicated-admin**權限

1. 使用以下命令授予dedicated-admin權限。執<IDP_USER_NAME>行<CLUSTER_NAME>下列命令，以您的使用者和叢集名稱取代和。

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

2. 確認使用者是否列為cluster-admins群組的成員。

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

步驟 8：透叢集過 Red Hat 混合雲端主控台存取

叢集透過 Red Hat 混合式雲端主控台登入您的帳戶。

1. 使用下列命令取得您叢集的主控台 URL。以您的 叢集 名稱取代 <CLUSTER_NAME>。

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

2. 導航到輸出中的控制台 URL 並登錄。

   在「使用... 登入」對話方塊中，選擇身分識別提供者名稱，並完成提供者提出的任何授權要求。

步驟 9：從開發人員目錄部署應用程式

您可以從 Red Hat 混合式雲端主控台部署開發人員目錄測試應用程式，並以路由公開。

1. 瀏覽至 Red Hat 混合式雲端主控台，然後選擇您要部署應用程式的叢集。
2. 在叢集頁面上，選擇 [開啟主控台]。
3. 在「管理員」觀點中，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」與「摘要」。
5. 選擇 [建立] 以建立專案。
6. 切換到開發人員視角，然後選擇 + 添加。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框中，選擇所有服務。
8. 在「開發人員目錄」頁面中，JavaScript從選單中選擇語言 >。
9. 選擇 Node.js，然後選擇建立應用程式，開啟「建立來源到影像的應用程式」頁面。

> **Note**
>
> 您可能需要選擇「清除所有篩選器」才能顯示 Node.js 選項。

10.在「Git」區段中，選擇「試用範例」。

11.在「名稱」欄位中，新增唯一名稱。

12.選擇 建立 。

> **Note**
>
> 新的應用程式需要幾分鐘的時間來部署。

13.部署完成時，請選擇應用程式的路由 URL。

瀏覽器中會開啟一個新標籤，其中包含類似下列內容的訊息。

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

14.(選擇性) 刪除應用程式並清理資源：

a. 在「管理員」觀點中，選擇「首頁 > 專案」。

b. 開啟專案的動作功能表，然後選擇 [刪除專案]。

步驟 10：刪除叢集和AWS STS資源

您可以使用 ROSA CLI 刪除使叢集用 AWS Security Token Service (AWS STS) 的。您也可以使用 ROSA CLI 刪除由建立的IAM角色和 OIDC 提供者。ROSA若要刪除由建立的IAM策略ROSA，您可以使用主IAM控台。

> **Important**
>
> IAM相同帳戶中的其他ROSA叢集ROSA可能會使用由建立的角色和原則。

1. 刪除叢集並觀看日誌。<CLUSTER_NAME>替換為您的名稱或 ID 叢集。

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

> **Important**
>
> 您必須等待完全刪除，才能移除IAM角色、原則和 OIDC 提供者。叢集需要帳戶 IAM 角色才能刪除安裝程式建立的資源。操作員 IAM 角色必須清理 OpenShift 操作員建立的資源。操作員使用 OIDC 提供者進行驗證。

2. 執行下列命令，刪除叢集操作員用來驗證的 OIDC 提供者。

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

3. 刪除叢集特定的操作員IAM角色。

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

4. 使用以下命令刪除帳戶 IAM 角色。以要刪除之帳戶 IAM 角色的前置詞取<PREFIX>代。如果您在建立帳戶 IAM 角色時指定了自訂首碼，請指定預設ManagedOpenShift前置詞。

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

5. 刪除由建立的IAM策略ROSA。
   a. 登入 IAM 主控台。
   b. 在 [存取管理] 下的左側功能表中，選擇 [原則]。
   c. 選取您要刪除的策略，然後選擇 [動作] > [刪除]。
   d. 輸入策略名稱，然後選擇「刪除」。
   e. 重複此步驟以刪除的每個 IAM 政策叢集。

在 auto 模式下使用 ROSA CLI 開始使用 ROSA 經典版

下列各節說明如何開始使用 ROSA 經典使用AWS STS和 ROSA CLI。如需 ROSA 傳統版的詳細資訊，請參閱部署選項。

ROSACLI 使用auto模manual式或模式來建立佈建 ROSA叢集. IAM auto模式立即創建所需的IAM角色和策略以及 OpenID Connect（OIDC）提供程序。 manualmode 輸出創建IAM資源所需的AWS CLI命令。透過使用manual模式，您可以先檢閱產生的AWS CLI指令，然後再手動執行它們。使用manual模式，您也可以將命令傳遞給組織中的其他管理員或群組，以便他們可以建立資源。

本文件中的程序使用 ROSA CLI 的auto模式來建立 ROSA 傳統版所需的IAM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

開始之前，請確定您已完成下列動作：

- 安裝和配置最新的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 ROSACLI 入門。
- Service Quotas必須為、和設定必要的服務配額 Amazon EC2 Amazon VPCAmazon EBS，才 Elastic Load Balancing能建立和執行ROSA叢集。 AWS或 Red Hat 可能會根據問題解決的要求，代表您要求增加服務配額。若要檢視所需的配額，請參閱AWS一般參考中的Red Hat OpenShift Service on AWS端點和配額。
- 若要獲得的AWS支援ROSA，您必須啟用AWS商業、企業版加速或企業支援方案。Red Hat 可能會代表您要求AWS支援，以便解決問題。如需詳細資訊，請參 S upport ROSA。若要啟用AWS Support，請參閱AWS Support頁面。
- 如果您使用AWS Organizations來管理AWS 帳戶該主機ROSA服務，組織的服務控制原則 (SCP) 必須設定為允許 Red Hat 不受限制地執行 SCP 中列出的政策動作。如需詳細資訊，請參閱 ROSASCP 疑難排解說明文件。如需 SCP 的詳細資訊，請參閱服務控制原則 (SCP)。
- 如果AWS STS將ROSA叢集與部署到默認情況下禁用的啟用AWS 區域中，則必須使用以下命令將中所有區域的安全性權杖更新為版本 2。AWS 帳戶

```
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 AWS 一般參考AWS 區域中的管理。

步驟 1：啟用ROSA並設定先決條件

若要建立 ROSA叢集，您必須先在AWSROSA主控台中啟用ROSA服務，並確認是否符合AWS先決條件。主AWSROSA控台會驗證您是否AWS 帳戶具有必要的AWS Marketplace權限、服務配額以及名為的 Elastic Load Balancing (ELB) 服務連結角色。`AWSServiceRoleForElasticLoadBalancing`如果缺少任何先決條件，主控台會提供如何設定帳戶以符合先決條件的指引。

1. 導覽至 ROSA 主控台。
2. 選擇 Get started (開始使用)。
3. 在 [驗證ROSA必要條件] 頁面上，選取 [我同意與 Red Hat 分享我的聯絡資訊]。
4. 選擇「啟用」ROSA。
5. 在頁面驗證您的服務配額符合ROSA先決條件並建立 ELB 服務連結角色後，請開啟新的終端機工作階段，以叢集使用 CLI 建立您的第一個 ROSA 傳統版。ROSA

步驟 2：使用AWS STS和 ROSA CLI **`auto`** 模式建立 ROSA 傳統叢集

您可以使叢集用 AWS Security Token Service (AWS STS) 和 ROSA CLI 中提供的`auto`模式來建立 ROSA 經典。

1. 建立必要的IAM帳號角色和策略。

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

> **Note**
>
> 如果您的離線訪問令牌已過期，ROSACLI 將輸出一條錯誤消息，指出您的授權令牌需要更新。如需疑難排解的步驟，請參閱疑難排解 ROSA CLI 過期離線存取權杖。

2. AWS STS使叢集用 ROSA CLI `auto` 模式下的預設值來建立一個。使用預設值時，會安裝最新的穩定 OpenShift 版本。

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

> **Note**
>
> 當您指定時`--mode auto`，此`rosa create cluster`命令會自動建立叢集特定的操作員IAM角色和 OIDC 提供者。操作員使用 OIDC 提供者進行驗證。

3. 檢查您的叢集.

```
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，請參閱疑難排解ROSA叢集佈建問題。
> 若要聯絡AWS Support或 Red Hat Support 人員尋求協助，請參閱支援ROSA。

4. 透過觀看 OpenShift 安裝程式記錄來追蹤叢集建立進度。

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

步驟 3：設定身分識別提供者並授與叢集存取權

ROSA包括一個內置的 OAuth 服務器。建立完成後叢集，您必須將 OAuth 設定為使用身分識別提供者。然後，您可以將使用者新增至已設定的身分識別提供者，以授與他們存取您的叢集. 您可以視需要授與這些使用者`cluster-admin`或`dedicated-admin`權限。

您可以為您的 ROSA叢集. 支援的類型包括 GitHub 企業 GitHub、 GitLab、谷歌、LDAP、OpenID Connect 和 HTPassWD 身份提供者。

> **Important**
>
> HTPasswd 身分提供者僅包含在內，以便建立單一靜態系統管理員使用者。HTPasswd 不支援做為的一般使用身分識別提供者。ROSA

下列程序會將 GitHub 身分識別提供者設定為範例。如需有關如何設定每個支援的身分識別提供者類型的指示，請參閱設定的身分識別提供者AWS STS。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 如果您沒有 GitHub 組織可用於您的身分識別佈建叢集，請建立一個組織。如需詳細資訊，請參閱 GitHub 文件中的步驟。
3. 使用 ROSA CLI 的互動模式，為您的叢集設定身分識別提供者。

```
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. 開啟輸出中的 URL，並<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] 以在 GitHub 組織中註冊新的 OAuth 應用程式。
7. 使用 GitHub OAuth 頁面中的資訊，透過執行下列命令來填入剩餘的`rosa create idp`互動式提示。取代 GitHub OAuth 應用程式中的認證，<GITHUB_CLIENT_ID>並加<GITHUB_CLIENT_SECRET>以取代。

```
...
? 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**
>
> 身分識別提供者組態可能需要大約兩分鐘的時間才會變成作用中狀態。如果您設定了`cluster-admin`使用者，則可以執行`oc get pods -n openshift-authentication --watch`以監視使用更新的組態重新部署 OAuth 網繭。

8. 確認身分識別提供者已正確設定。

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

步驟 4：授與使用者存取 叢集

您可以將使用者新增至已設定的叢集身分識別提供者，以授與使用者存取您的權限。

下列程序會將使用者新增至已設定為識別佈建的 GitHub 組織至叢集。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 邀請需要叢集存取您 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。

步驟 5：將管理員權限授與使用者

將使用者新增至設定的身分識別提供者後，您可以授與您的使用者`cluster-admin`或`dedicated-admin`權限叢集。

設定`cluster-admin`權限

1. 執行下列命令以授與`cluster-admin`權限。將`<IDP_USER_NAME>`和取代為您`<CLUSTER_NAME>`的使用者和叢集名稱。

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

2. 確認使用者是否列為cluster-admins群組的成員。

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

設定dedicated-admin權限

1. 使用以下命令授予dedicated-admin權限。執<IDP_USER_NAME>行<CLUSTER_NAME>下列命令，以您的使用者和叢集名稱取代和。

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

2. 確認使用者是否列為cluster-admins群組的成員。

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

步驟 6：透叢集過 Web 主控台存取

在您建立叢集系統管理員使用者或將使用者新增至您設定的身分識別提供者之後，您就可以叢集透過 Red Hat Hybrid Cloud 主控台登入您的。

1. 使用下列命令取得您叢集的主控台 URL。以您的 叢集 名稱取代 <CLUSTER_NAME>。

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

2. 導航到輸出中的控制台 URL 並登錄。
   - 如果您已建立使用cluster-admin者，請使用提供的認證登入。
   - 如果您已為您設定身分識別提供者叢集，請在 [使用... 登入] 對話方塊中選擇身分識別提供者名稱，並完成提供者提出的任何授權要求。

步驟 7：從開發人員目錄部署應用程式

您可以從 Red Hat 混合式雲端主控台部署開發人員目錄測試應用程式，並透過路由公開它。

1. 瀏覽至 Red Hat 混合式雲端主控台，然後選擇您要部署應用程式的叢集。

2. 在叢集頁面上，選擇 [開啟主控台]。
3. 在「管理員」觀點中，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」與「摘要」。
5. 選擇 [建立] 以建立專案。
6. 切換到開發人員視角，然後選擇 + 添加。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框中，選擇所有服務。
8. 在「開發人員目錄」頁面中，JavaScript從選單中選擇「語言」>。
9. 選擇 Node.js，然後選擇建立應用程式，開啟「建立來源到影像的應用程式」頁面。

> **Note**
>
> 您可能需要選擇「清除所有篩選器」才能顯示 Node.js 選項。

10.在「Git」區段中，選擇「試用範例」。
11.在「名稱」欄位中，新增唯一名稱。
12.選擇 建立 。

> **Note**
>
> 新的應用程式需要幾分鐘的時間來部署。

13.部署完成時，請選擇應用程式的路由 URL。

瀏覽器中會開啟一個新標籤，其中包含類似下列內容的訊息。

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

14.(選擇性) 刪除應用程式並清理資源：

a. 在「管理員」觀點中，選擇「首頁 > 專案」。
b. 開啟專案的動作功能表，然後選擇 [刪除專案]。

步驟 8：撤銷管理員權限和用戶訪問權限

您可以使`cluster-admin`用 ROSA CLI 撤銷使用者的`dedicated-admin`權限。

若要撤銷使用者的存取權，您必須從設定的身分識別提供者中移除該使用者。

撤銷使用者的**cluster-admin**權限

1. 使用下列命令撤銷cluster-admin權限。<CLUSTER_NAME>以您的使用者和叢集名稱取<IDP_USER_NAME>代和。

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

2. 確認使用者未列為cluster-admins群組成員。

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

撤銷使用者的**dedicated-admin**權限

1. 使用下列命令撤銷dedicated-admin權限。<CLUSTER_NAME>以您的使用者和叢集名稱取<IDP_USER_NAME>代和。

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

2. 確認使用者未列為dedicated-admins群組成員。

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

撤銷使用者存取 叢集

您可以從設定的身分識別提叢集供者中移除身分識別提供者使用者，以撤銷他們的存取。

您可以為您的叢集. 下列程序會撤銷 GitHub 組織成員的叢集存取權。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 從您的 GitHub 組織中移除使用者。如需詳細資訊，請參閱 GitHub 文件中的從組織移除成員。

步驟 9：刪除叢集和AWS STS資源

您可以使用 ROSA CLI 刪除使叢集用 AWS Security Token Service (AWS STS) 的。您也可以使用 ROSA CLI 刪除由建立的IAM角色和 OIDC 提供者。ROSA若要刪除由建立的IAM策略ROSA，您可以使用主IAM控台。

> **Important**
>
> IAM相同帳戶中的其他ROSA叢集ROSA可能會使用由建立的角色和原則。

1. 刪除叢集並觀看日誌。<CLUSTER_NAME>替換為您的名稱或 ID 叢集。

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

> **Important**
>
> 您必須等待完全刪除，才能移除IAM角色、原則和 OIDC 提供者。叢集需要帳戶 IAM 角色才能刪除安裝程式建立的資源。操作員 IAM 角色必須清理 OpenShift 操作員建立的資源。操作員使用 OIDC 提供者進行驗證。

2. 執行下列命令，刪除叢集操作員用來驗證的 OIDC 提供者。

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

3. 刪除叢集特定的操作員IAM角色。

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

4. 使用以下命令刪除帳戶 IAM 角色。以要刪除之帳戶 IAM 角色的前置詞取<PREFIX>代。如果您在建立帳戶 IAM 角色時指定了自訂前置詞，請指定預設ManagedOpenShift前置詞。

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

5. 刪除由建立的IAM策略ROSA。
   a. 登入 IAM 主控台。
   b. 在 [存取管理] 下的左側功能表中，選擇 [原則]。
   c. 選取您要刪除的策略，然後選擇 [動作] > [刪除]。
   d. 輸入策略名稱，然後選擇「刪除」。
   e. 重複此步驟以刪除的每個 IAM 政策叢集。

在手動模式下使用 ROSA CLI 開始使用 ROSA 經典版

下列各節說明如何開始使用 ROSA 經典使用AWS STS和 ROSA CLI。如需 ROSA 傳統版的詳細資訊，請參閱部署選項。

ROSACLI 使用auto模式或manual模式來建立佈建所需的IAM資源ROSA叢集。 auto模式立即創建所需的IAM角色和策略以及 OpenID Connect（OIDC）提供程序。 manualmode 輸出創建IAM資源所需的AWS CLI命令。透過使用manual模式，您可以先檢閱產生的AWS CLI指令，然後再手動執行它們。您也可以使用manual將命令傳遞給組織中的其他管理員或群組，以便他們可以建立資源。

本文件中的程序使用 ROSA CLI 的manual模式來建立 ROSA 傳統版所需的IAM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

開始之前，請確定您已完成下列動作：

- 安裝和配置最新的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 ROSACLI 入門。
- Service Quotas必須為、和設定必要的服務配額 Amazon EC2 Amazon VPCAmazon EBS，才 Elastic Load Balancing能建立和執行ROSA叢集。 AWS或 Red Hat 可能會根據問題解決的要求，代表您要求增加服務配額。若要檢視所需的配額，請參閱AWS一般參考中的Red Hat OpenShift Service on AWS端點和配額。

- 若要獲得的AWS支援ROSA，您必須啟用AWS商務、企業版加速或企業支援方案。Red Hat 可能會代表您要求AWS支援，以便解決問題。如需詳細資訊，請參 S upport ROSA。若要啟用AWS Support，請參閱AWS Support頁面。
- 如果您使用AWS Organizations來管理AWS 帳戶該主機ROSA服務，組織的服務控制原則 (SCP) 必須設定為允許 Red Hat 不受限制地執行 SCP 中列出的政策動作。如需詳細資訊，請參閱 ROSASCP 疑難排解說明文件。如需 SCP 的詳細資訊，請參閱服務控制原則 (SCP)。
- 如果AWS STS將ROSA叢集與部署到默認情況下禁用的啟用AWS 區域中，則必須使用以下命令將中所有區域的安全性權杖更新為版本 2。AWS 帳戶

```
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 AWS 一般參考AWS 區域中的管理。

步驟 1：啟用ROSA並設定先決條件

若要建立 ROSA叢集，您必須先在AWSROSA主控台中啟用該ROSA服務。主AWSROSA控台會驗證您是否AWS 帳戶具有必要的AWS Marketplace權限、服務配額以及名為的 Elastic Load Balancing (ELB) 服務連結角色。`AWSServiceRoleForElasticLoadBalancing`如果缺少任何先決條件，主控台會提供如何設定帳戶以符合先決條件的指引。

1. 導覽至 ROSA 主控台。
2. 選擇 Get started (開始使用)。
3. 在 [驗證ROSA必要條件] 頁面上，選取 [我同意與 Red Hat 分享我的聯絡資訊]。
4. 選擇「啟用」ROSA。
5. 在頁面驗證您的服務配額符合ROSA先決條件並建立 ELB 服務連結角色後，請開啟新的終端機工作階段，以ROSA叢集使用 CLI 建立您的第一個終端機工作階段。ROSA

步驟 2：使用AWS STS和 ROSA CLI `manual` 模式建立 ROSA 傳統叢集

您可以使叢集用 AWS Security Token Service (AWS STS) 和 ROSA CLI 中提供的`manual`模式來建立 ROSA 經典。

建立時叢集，您可以執行以使用一系列互動式提示`rosa create cluster --interactive`來自訂部署。如需詳細資訊，請參閱 Red Hat 文件中的互動式叢集建立模式參考。

佈建叢集之後，輸出中會提供單一命令。執行此命令以部署使用完全相同自訂組態的進一步叢集。

> **Note**
>
> AWS共用 VPC 目前不支援ROSA安裝。

1. 建立必要的IAM帳號角色和策略。

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

> **Note**
>
> 如果您的離線訪問令牌已過期，ROSACLI 將輸出一條錯誤消息，指出您的授權令牌需要更新。如需疑難排解的步驟，請參閱疑難排解 ROSA CLI 過期離線存取權杖。

2. 執行輸出中產生的AWS CLI命令，以建立角色和原則。
3. 建立叢集具有 AWS STS in `--interactive` 模式以指定任何自訂設定。

```
rosa create cluster --interactive --sts
```

> **Important**
>
> 在 etcd 中為金鑰值啟用 etcd 加密之後，會產生約 20% 的效能額外負荷。除了加密 etcd 磁碟區的預設加密之外，還引入了第二層Amazon EBS加密所造成的額外負荷。

4. 若要建立叢集特定的操作員IAM角色，請在目前的工作目錄中產生操作員原則 JSON 檔案，並輸出AWS CLI指令以供檢閱。

```
rosa create operator-roles --mode manual --cluster <CLUSTER_NAME|CLUSTER_ID>
```

5. 從輸出中運行AWS CLI命令。
6. 創建叢集操作員用於進行身份驗證的 OpenID Connect（OIDC）提供程序。

```
rosa create oidc-provider --mode auto --cluster <CLUSTER_NAME|CLUSTER_ID>
```

7. 檢查您的叢集.

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

> **Note**
>
> 如果建立程序失敗或State欄位在 40 分鐘後未變更為就緒狀態，請參閱疑難排解ROSA叢集建立問題。
> 若要聯絡AWS Support或 Red Hat Support 人員尋求協助，請參閱支援ROSA。

8. 透過觀看 OpenShift 安裝程式記錄來追蹤叢集建立進度。

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

步驟 3：設定身分識別提供者並授與叢集存取權

ROSA包括一個內置的 OAuth 服務器。建立完成後叢集，您必須將 OAuth 設定為使用身分識別提供者。然後，您可以將使用者新增至已設定的身分識別提供者，以授與他們存取您的叢集. 您可以視需要授與這些使用者cluster-admin或dedicated-admin權限。

您可以為您的叢集. 支援的類型包括： GitHub 企業版 GitHub GitLab、谷歌、LDAP、OpenID Connect 和 HTPassWD 身分識別提供者。

> **Important**
>
> HTPasswd 身分提供者僅包含在內，以便建立單一靜態系統管理員使用者。HTPasswd 不支援做為的一般使用身分識別提供者。ROSA

下列程序會將 GitHub 身分識別提供者設定為範例。如需有關如何設定每個支援的身分識別提供者類型的指示，請參閱設定的身分識別提供者AWS STS。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 如果您沒有 GitHub 組織可用於您的身分識別佈建 ROSA叢集，請建立一個組織。如需詳細資訊，請參閱 GitHub 文件中的步驟。
3. 使用 ROSA CLI 的互動模式，為您的叢集設定身分識別提供者。

```
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. 使用以下命令打開輸出中的 URL。<GITHUB_ORG_NAME>以您 GitHub 組織的名稱取代。

6. 在 GitHub 網頁上，選擇 [註冊應用程式] 以在 GitHub 組織中註冊新的 OAuth 應用程式。

7. 使用 GitHub OAuth 頁面中的資訊，使用下列命令填入剩餘的`rosa create idp`互動式提示。取代 GitHub OAuth 應用程式中的認證，<GITHUB_CLIENT_ID>並加<GITHUB_CLIENT_SECRET>以取代。

```
...
? 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**
>
> 身分識別提供者組態可能需要大約兩分鐘的時間才會變成作用中狀態。如果您設定了`cluster-admin`使用者，則可以執行命`oc get pods -n openshift-authentication --watch`令來監視 OAuth 網繭以更新的組態重新部署。

8. 使用下列命令確認身分識別提供者已正確設定。

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

步驟 4：授與使用者存取 叢集

您可以將使用者新增至已設定的叢集身分識別提供者，以授與使用者存取您的權限。

下列程序會將使用者新增至已設定為識別佈建的 GitHub 組織叢集。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 邀請需要叢集存取您 GitHub 組織的使用者。如需詳細資訊，請參閱 Github 上的文件中的邀請使用者加入您的組織。

步驟 5：將管理員權限授與使用者

將使用者新增至設定的身分識別提供者後，您可以授與您的使用者`cluster-admin`或`dedicated-admin`權限叢集。

設定`cluster-admin`權限

1. 使用以下命令授予`cluster-admin`權限。將`<IDP_USER_NAME>`和取代為您`<CLUSTER_NAME>`的使用者和叢集名稱。

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

2. 確認使用者是否列為`cluster-admins`群組的成員。

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

設定**dedicated-admin**權限

1. 使用以下命令授予dedicated-admin權限。<CLUSTER_NAME>以您的使用者和叢集名稱取<IDP_USER_NAME>代和。

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

2. 確認使用者是否列為cluster-admins群組的成員。

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

步驟 6：透叢集過 Web 主控台存取

在您建立叢集系統管理員使用者或將使用者新增至您設定的身分識別提供者之後，您就可以叢集透過 Red Hat Hybrid Cloud 主控台登入您的。

1. 使用下列命令取得您叢集的主控台 URL。以您的 叢集 名稱取代 <CLUSTER_NAME>。

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

2. 導航到輸出中的控制台 URL 並登錄。
   - 如果您建立使用cluster-admin者，請使用提供的認證登入。
   - 如果您為您的身分識別提供者設定叢集，請在 [使用... 登入] 對話方塊中選擇身分識別提供者名稱，並完成提供者提出的任何授權要求。

步驟 7：從開發人員目錄部署應用程式

您可以從 Red Hat 混合式雲端主控台部署開發人員目錄測試應用程式，並透過路由公開它。

1. 瀏覽至 Red Hat 混合式雲端主控台，然後選擇您要部署應用程式的叢集。
2. 在叢集頁面上，選擇 [開啟主控台]。
3. 在「管理員」觀點中，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」與「摘要」。
5. 選擇 [建立] 以建立專案。
6. 切換到開發人員視角，然後選擇 + 添加。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框中，選擇所有服務。

8. 在「開發人員目錄」頁面中，JavaScript從選單中選擇「語言」>。
9. 選擇 Node.js，然後選擇建立應用程式，開啟「建立來源到影像的應用程式」頁面。

> **Note**
> 您可能需要選擇「清除所有篩選器」才能顯示 Node.js 選項。

10.在「Git」區段中，選擇「試用範例」。
11.在「名稱」欄位中，新增唯一名稱。
12選擇 建立 。

> **Note**
> 新的應用程式需要幾分鐘的時間來部署。

13.部署完成時，請選擇應用程式的路由 URL。

瀏覽器中會開啟一個新標籤，其中包含類似下列內容的訊息。

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

14.(選擇性) 刪除應用程式並清理資源。
a. 在「管理員」觀點中，選擇「首頁 > 專案」。
b. 開啟專案的動作功能表，然後選擇 [刪除專案]。

步驟 8：撤銷管理員權限和用戶訪問權限

您可以使`cluster-admin`用 ROSA CLI 撤銷使用者的`dedicated-admin`權限。

若要撤銷使用者的存取權，您必須從設定的身分識別提供者中移除該使用者。

撤銷使用者的`cluster-admin`權限

1. 使用下列命令撤銷`cluster-admin`權限。`<CLUSTER_NAME>`以您的使用者和叢集名稱取`<IDP_USER_NAME>`代和。

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

2. 確認使用者未列為`cluster-admins`群組成員。

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

撤銷使用者的**dedicated-admin**權限

1. 使用以下命令撤銷dedicated-admin權限。<CLUSTER_NAME>以您的使用者和叢集名稱取<IDP_USER_NAME>代和。

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

2. 確認使用者未列為dedicated-admins群組成員。

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

撤銷使用者存取 叢集

您可以從設定的身分識別提叢集供者中移除身分識別提供者使用者，以撤銷他們的存取。

您可以為您的叢集. 下列程序會撤銷 GitHub 組織成員的叢集存取權。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 從您的 GitHub 組織中移除使用者。如需詳細資訊，請參閱 GitHub 文件中的從組織移除成員。

步驟 9：刪除叢集和AWS STS資源

您可以使用 ROSA CLI 刪除使叢集用 AWS Security Token Service (AWS STS) 的。您也可以使用 ROSA CLI 刪除由建立的IAM角色和 OIDC 提供者。ROSA若要刪除由建立的IAM策略ROSA，您可以使用主IAM控台。

> **Important**
>
> IAM相同帳戶中的其他ROSA叢集ROSA可能會使用由建立的角色和原則。

1. 刪除叢集並觀看日誌。<CLUSTER_NAME>替換為您的名稱或 ID 叢集。

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

> **Important**
>
> 您必須等待完全刪除，才能移除IAM角色、原則和 OIDC 提供者。叢集需要帳戶 IAM 角色才能刪除安裝程式建立的資源。操作員 IAM 角色必須清理 OpenShift 操作員建立的資源。操作員使用 OIDC 提供者進行驗證。

2. 執行下列命令，刪除叢集操作員用來驗證的 OIDC 提供者。

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

3. 刪除叢集特定的操作員IAM角色。

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

4. 使用以下命令刪除帳戶 IAM 角色。以要刪除之帳戶 IAM 角色的前置詞取<PREFIX>代。如果您在建立帳戶 IAM 角色時指定了自訂前置詞，請指定預設ManagedOpenShift前置詞。

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

5. 刪除由建立的IAM策略ROSA。
   a. 登入 IAM 主控台。
   b. 在 [存取管理] 下的左側功能表中，選擇 [原則]。
   c. 選取您要刪除的策略，然後選擇 [動作] > [刪除]。
   d. 輸入策略名稱，然後選擇「刪除」。
   e. 重複此步驟以刪除的每個 IAM 政策叢集。

開始使用 ROSA 經典使用 AWS PrivateLink

ROSA 傳統叢集可以透過幾種不同的方式部署：公用、私有或私有AWS PrivateLink. 如需 ROSA 傳統版的詳細資訊，請參閱部署選項。對於公共和私 OpenShift 叢集有叢集配置，都可以訪問 Internet，並且在應用程序層的應用程序工作負載上設置隱私。

如果您要求叢集和應用程式工作負載均為私有工作負載，則可以AWS PrivateLink使用 ROSA 典型進行設定。 AWS PrivateLink是一種高可用性、可擴充的技術，ROSA用於在AWS客戶帳戶中的ROSA服務與叢集資源之間建立私有連線。Red Hat 站台可靠性工程 (SRE) 團隊可以使用連線到叢集AWS PrivateLink端點的私有子網路AWS PrivateLink，存取叢集以進行支援和補救。

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

主題

先決條件

開始之前，請確定您已完成下列動作：

- 安裝和配置最新的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 ROSACLI 入門。
- Service Quotas必須為、和設定必要的服務配額 Amazon EC2 Amazon VPCAmazon EBS，才 Elastic Load Balancing能建立和執行ROSA叢集。 AWS或 Red Hat 可能會根據問題解決的要求，代表您要求增加服務配額。若要檢視所需的配額，請參閱AWS一般參考中的Red Hat OpenShift Service on AWS端點和配額。
- 若要獲得的AWS支援ROSA，您必須啟用AWS商務、企業版加速或企業支援方案。Red Hat 可能會代表您要求AWS支援，以便解決問題。如需詳細資訊，請參 S upport ROSA。若要啟用AWS Support，請參閱AWS Support頁面。
- 如果您使用AWS Organizations來管理AWS 帳戶該主機ROSA服務，組織的服務控制原則 (SCP) 必須設定為允許 Red Hat 不受限制地執行 SCP 中列出的政策動作。如需詳細資訊，請參閱 ROSASCP 疑難排解說明文件。如需 SCP 的詳細資訊，請參閱服務控制原則 (SCP)。
- 如果AWS STS將ROSA叢集與部署到默認情況下禁用的啟用AWS 區域中，則必須使用以下命令將中所有區域的安全性權杖更新為版本 2。AWS 帳戶

```
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 AWS 一般參考AWS 區域中的管理。

步驟 1：啟用ROSA並設定先決條件

若要建立 ROSA叢集，您必須先在AWSROSA主控台中啟用該ROSA服務。主AWSROSA控台會驗證您是否AWS 帳戶具有必要的AWS Marketplace權限、服務配額以及名為的 Elastic Load Balancing (ELB) 服務連結角色。`AWSServiceRoleForElasticLoadBalancing`如果缺少任何先決條件，主控台會提供如何設定帳戶以符合先決條件的指引。

1. 導覽至 ROSA 主控台。
2. 選擇 Get started (開始使用)。
3. 在 [驗證ROSA必要條件] 頁面上，選取 [我同意與 Red Hat 分享我的聯絡資訊]。
4. 選擇「啟用」ROSA。
5. 在頁面驗證您的服務配額符合ROSA先決條件並建立 ELB 服務連結角色後，請開啟新的終端機工作階段，以ROSA叢集使用 CLI 建立您的第一個終端機工作階段。ROSA

步驟 2：建立叢集的Amazon VPC架構

若要建立使用ROSA叢集的AWS PrivateLink，您必須先設定自己的Amazon VPC架構，以將解決方案部署到。 ROSA客戶要求每個用於建立叢集的可用區域至少設定一個公用和私有子網路。對於單一可用區叢集，僅使用可用區域。對於異地同步備份叢集，需要三個可用區域。

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

下列程序會使AWS CLI用在單一可用區叢集的單一可用區域中建立公用和私有子網路。所有叢集資源都位於私有子網路中。公用子網路會使用 NAT 閘道將輸出流量路由傳送至網際網路。

此範例使用的 CIDR 區塊`10.0.0.0/16`做為. 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。

1. 透過執行下列命令來設定叢集名稱的環境變數。

```
ROSA_CLUSTER_NAME=rosa-privatelink
```

2. 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
```

上述命令會傳回新 VPC 的 ID。以下為範例輸出。

```
vpc-0410832ee325aafea
```

3. 使用上一個步驟中的 VPC ID，使用變數標記 VPC。ROSA_CLUSTER_NAME

```
aws ec2 create-tags --resources <VPC_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

4. 在 VPC 上啟用 DNS 主機名稱支援。

```
aws ec2 modify-vpc-attribute --vpc-id <VPC_ID_VALUE> --enable-dns-hostnames
```

5. 使用 10.0.1.0/24 CIDR 區塊在 VPC 中建立公用子網路，並指定應在其中建立資源的可用區域。

> **Important**
>
> 建立子網路時，請確定子網路建立至具有可用ROSA執行個體類型的可用區域。如果您未選擇特定的可用區域，則會在您指定的任何一個可用區域中AWS 區域建立子網路。
> 若要指定特定的可用區域，請使用create-subnet命令中的--availability zone引數。您可以使用指rosa list instance-types令列出所有可用的ROSA例證類型。若要檢查指定的可用區域是否有執行個體類型可用，請使用下列命令。
>
> ```
> aws ec2 describe-instance-type-offerings --location-type availability-zone --
> filters Name=location,Values=<availability_zone> --region <region> --output
>  text | egrep "<instance_type>"
> ```

> **Important**
>
> ROSA客戶要求每個用於建立叢集的可用區域至少設定一個公用和私有子網路。對於單一可用區叢集，只需要一個可用區域。對於異地同步備份叢集，需要三個可用區域。如果不符合這些需求，叢集建立會失敗。

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.1.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

上述命令會傳回新子網路的 ID。以下為範例輸出。

```
subnet-0b6a7e8cbc8b75920
```

6. 使用上一個步驟中的子網路 ID，使用ROSA_CLUSTER_NAME-public變數標記子網路。

```
aws ec2 create-tags --resources <PUBLIC_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-public
```

7. 使用 10.0.0.0/24 CIDR 區塊在 VPC 中建立私有子網路，並指定部署公用子網路的相同可用區域。

```
aws ec2 create-subnet --vpc-id <VPC_ID_VALUE> --cidr-block 10.0.0.0/24 --
availability-zone <AZ_NAME> --query Subnet.SubnetId --output text
```

上述命令會傳回新子網路的 ID。以下為範例輸出。

```
subnet-0b6a7e8cbc8b75920
```

8. 使用上一個步驟中的子網路 ID，使用ROSA_CLUSTER_NAME-private變數標記子網路。

```
aws ec2 create-tags --resources <PRIVATE_SUBNET_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

9. 為輸出流量建立網際網路閘道，並將其附加至 VPC。

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output
 text
```

```
aws ec2 attach-internet-gateway --vpc-id <VPC_ID_VALUE> --internet-gateway-id
 <IG_ID_VALUE>
```

10.使用ROSA_CLUSTER_NAME變數標記網際網路閘道。

```
aws ec2 create-tags --resources <IG_ID_VALUE> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME
```

11.為輸出流量建立路由表，將其與公用子網路建立關聯，並設定要路由到網際網路閘道的流量。

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text

aws ec2 associate-route-table --subnet-id <PUBLIC_SUBNET_ID> --route-table-id
 <PUBLIC_RT_ID>

aws ec2 create-route --route-table-id <PUBLIC_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <IG_ID_VALUE>
```

12.使用ROSA_CLUSTER_NAME變數標記公用路由表格，並驗證路由表是否已正確設定。

```
aws ec2 create-tags --resources <PUBLIC_RT_ID> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME

aws ec2 describe-route-tables --route-table-id <PUBLIC_RT_ID>
```

13.使用彈性 IP 位址在公用子網路中建立 NAT 閘道，以啟用通往私有子網路的流量。

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text

aws ec2 create-nat-gateway --subnet-id <PUBLIC_SUBNET_ID> --allocation-id
 <EIP_ADDRESS>  --query NatGateway.NatGatewayId --output text
```

14.使用$ROSA_CLUSTER_NAME變數標記 NAT 閘道和彈性 IP 位址。

```
aws ec2 create-tags --resources <EIP_ADDRESS>  --resources <NAT_GATEWAY_ID> --tags
 Key=Name,Value=$ROSA_CLUSTER_NAME
```

15.為私有子網路流量建立路由表，將其與私有子網路建立關聯，並設定要路由至 NAT 閘道的流量。

```
aws ec2 create-route-table --vpc-id <VPC_ID_VALUE> --query RouteTable.RouteTableId --
output text
```

```
aws ec2 associate-route-table --subnet-id <PRIVATE_SUBNET_ID> --route-table-id
 <PRIVATE_RT_ID>

aws ec2 create-route --route-table-id <PRIVATE_RT_ID> --destination-cidr-block
 0.0.0.0/0 --gateway-id <NAT_GATEWAY_ID>
```

16.使用$ROSA_CLUSTER_NAME-private變數標記私有路由表和彈性 IP 位址。

```
aws ec2 create-tags --resources <PRIVATE_RT_ID> <EIP_ADDRESS> --tags Key=Name,Value=
$ROSA_CLUSTER_NAME-private
```

第 3 步：創建一個集群 AWS PrivateLink

您可以使用AWS PrivateLink和 ROSA CLI 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 (異地同步備份)。在任何一種情況下，您機器的 CIDR 值都必須符合 VPC 的 CIDR 值。

下列程序會使用指`rosa create cluster`令來建立單一可用區ROSA叢集。若要建立異地同步備份叢集，請`multi-az`在指令中指定您要部署的每個私有子網路的私有子網路 ID。

> **Note**
>
> 如果您使用防火牆，則必須對其進行設定，才ROSA能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防火牆必要條件。

1. 叢集透過執行下列命令建立單一可用區。

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

> **Note**
>
> 若要建立使AWS PrivateLink用 and AWS Security Token Service (AWS STS) 短期認證的叢集，請附`--sts --mode manual`加`--sts --mode auto`或`rosa create cluster`指令結尾。

2. 依照互動式提示建立叢集操作員IAM角色。

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

3. 創建叢集操作員用於進行身份驗證的 OpenID Connect（OIDC）提供程序。

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

4. 檢查您的叢集.

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

Example

> **Note**
>
> 叢集State欄位最多可能需要 40 分鐘才能顯示ready狀態。如果佈建失敗或ready在 40 分鐘後未顯示，請參閱疑難排解ROSA叢集佈建問題。

若要聯絡AWS Support或 Red Hat Support 人員尋求協助，請參閱支援ROSA。

5. 透過觀看 OpenShift 安裝程式記錄來追蹤叢集建立進度。

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

步驟 4：設定 AWS PrivateLink DNS 轉送

使用在中AWS PrivateLink建立公用託管區域和私有託管區域的Route 53叢集 Route 53私有託管區域內的記錄只能從其指派給的 VPC 內解析。

讓我們加密 DNS-01 驗證需要一個公共區域，以便為域發行有效和公開信任的證書。驗證記錄會在「讓我們加密」驗證完成後刪除。發行和續訂這些憑證仍需要該區域，通常每 60 天需要一次。雖然這些區域通常顯示為空白，但公用區域在驗證程序中扮演重要角色。

如需AWS私有託管區域的詳細資訊，請參閱使用私有區域。如需有關公用託管區域的詳細資訊，請參閱使用公有託管區域。

設定輸Route 53 Resolver入端點

若要允許記錄 (例如`api.<cluster_domain>`和`*.apps.<cluster_domain>`在 VPC 外部解析)，請設定Route 53 Resolver輸入端點。

1. 開啟 Route 53 主控台。
2. 在 [解析程式] 下的導覽窗格中，選擇 [輸入端點]。
3. 選擇「設定端點」。
4. 在右上角，使用選擇AWS 區域器選擇包AWS 區域含用於叢集的 VPC。
5. 在 [基本組態] 下，選擇 [僅輸入]，然後選擇 [下一步
6. 在 [設定輸入端點] 頁面上，完成輸入端點的 [一般設定] 區段。在此端點的 [安全性群組] 下，選擇一個安全群組，該群組允許來自目的地連接埠 53 上遠端網路的輸入 UDP 和 TCP 流量。
7. 在 [IP 位址] 區段中，選擇建立叢集時使用的可用區域和專用子網路，然後選擇下一步。
8. (選擇性) 完成「標籤」區段。
9. 選擇 Submit (提交)。

設定叢集的 DNS 轉送

關聯內Route 53 Resolver部端點並可操作之後，請設定 DNS 轉送，以便您網路上的指定伺服器可以處理 DNS 查詢。

1. 將您的公司網路設定為將 DNS 查詢轉寄至頂層網域的 IP 位址，例如`drow-pl-01.htno.p1.openshiftapps.com`。
2. 如果您要將 DNS 查詢從一個 VPC 轉寄到另一個 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，請參閱特定的 DNS 伺服器文件，以針對已安裝的叢集網域設定選擇性 DNS 轉送。

步驟 5：設定身分識別提供者並授與叢集存取權

ROSA包括一個內置的 OAuth 服務器。建立完成後 ROSA叢集，您必須將 OAuth 設定為使用身分識別提供者。然後，您可以將使用者新增至已設定的身分識別提供者，以授與他們存取您的叢集. 您可以視需要授與這些使用者`cluster-admin`或`dedicated-admin`權限。

您可以為您的叢集. 支持的類型包括 GitHub 企業 GitHub，谷歌 GitLab，LDAP，OpenID Connect 和 HTPassWD 身份提供商。

> **Important**
>
> HTPasswd 身分提供者僅包含在內，以便建立單一靜態系統管理員使用者。HTPasswd 不支援做為的一般使用身分識別提供者。ROSA

下列程序會將 GitHub 身分識別提供者設定為範例。如需有關如何設定每個支援的身分識別提供者類型的指示，請參閱設定的身分識別提供者AWS STS。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 如果您沒有 GitHub 組織可用於您的身分識別佈建 ROSA叢集，請建立一個組織。如需詳細資訊，請參閱 GitHub 文件中的步驟。
3. 使用 ROSA CLI 的互動模式，透過執行下列命令來設定叢集的身分識別提供者。

```
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. 開啟輸出中的 URL，並<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] 以在 GitHub 組織中註冊新的 OAuth 應用程式。
7. 使用 GitHub OAuth 頁面中的資訊填入剩餘的`rosa create idp`互動式提示，<GITHUB_CLIENT_ID>並取代 GitHub OAuth 應<GITHUB_CLIENT_SECRET>用程式中的認證。

```
...
? 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

身分識別提供者組態可能需要大約兩分鐘的時間才會變成作用中狀態。如果您設定了`cluster-admin`使用者，則可以執行命`oc get pods -n openshift-authentication --watch`令來監視 OAuth 網繭以更新的組態重新部署。

8. 確認身分識別提供者已正確設定。

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

步驟 6：授與使用者存取 叢集

您可以將使用者新增至已設定的叢集身分識別提供者，以授與使用者存取您的權限。

下列程序會將使用者新增至已設定為識別佈建的 GitHub 組織至叢集。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 邀請需要叢集存取您 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。

步驟 7：將管理員權限授與使用者

將使用者新增至設定的身分識別提供者之後，您可以授與您的使用者`cluster-admin`或`dedicated-admin`權限叢集。

設定**cluster-admin**權限

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

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

2. 確認使用者是否列為cluster-admins群組的成員。

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

設定**dedicated-admin**權限

1. 使用以下命令授予dedicated-admin權限。<CLUSTER_NAME>以您的使用者和叢集名稱取<IDP_USER_NAME>代和。

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

2. 確認使用者是否列為cluster-admins群組的成員。

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

步驟 8：透叢集過 Web 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識別提供者之後，您就可以叢集透過 Red Hat Hybrid Cloud 主控台登入您的。

1. 使用下列命令取得您叢集的主控台 URL。以您的 叢集 名稱取代 <CLUSTER_NAME>。

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

2. 導航到輸出中的控制台 URL 並登錄。
   - 如果您已建立使用cluster-admin者，請使用提供的認證登入。
   - 如果您已為您設定身分識別提供者叢集，請在 [使用... 登入] 對話方塊中選擇身分識別提供者名稱，並完成提供者提出的任何授權要求。

步驟 9：從開發人員目錄部署應用程式

您可以從 Red Hat 混合式雲端主控台部署開發人員目錄測試應用程式，並透過路由公開它。

1. 瀏覽至 Red Hat 混合式雲端主控台，然後選擇您要部署應用程式的叢集。
2. 在叢集頁面上，選擇 [開啟主控台]。
3. 在「管理員」觀點中，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」與「摘要」。
5. 選擇 [建立] 以建立專案。
6. 切換到開發人員視角，然後選擇 + 添加。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框中，選擇所有服務。
8. 在「開發人員目錄」頁面中，JavaScript從選單中選擇「語言」>。
9. 選擇 Node.js，然後選擇建立應用程式，開啟「建立來源到影像的應用程式」頁面。

> **Note**
> 您可能需要選擇「清除所有篩選器」才能顯示 Node.js 選項。

10.在「Git」區段中，選擇「試用範例」。

11.在「名稱」欄位中，新增唯一名稱。

12.選擇 建立 。

> **Note**
> 新的應用程式需要幾分鐘的時間來部署。

13.部署完成時，請選擇應用程式的路由 URL。

瀏覽器中會開啟一個新標籤，其中包含類似下列內容的訊息。

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

14.(選擇性) 刪除應用程式並清理資源。

a. 在「管理員」觀點中，選擇「首頁 > 專案」。

b. 開啟專案的動作功能表，然後選擇 [刪除專案]。

步驟 10：撤銷管理員權限和用戶訪問權限

您可以使cluster-admin用 ROSA CLI 撤銷使用者的dedicated-admin權限。

若要撤銷使用者的存取權，您必須從設定的身分識別提供者中移除該使用者。

撤銷使用者的**cluster-admin**權限

1. 使用下列命令撤銷cluster-admin權限。<CLUSTER_NAME>以您的使用者和叢集名稱取<IDP_USER_NAME>代和。

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

2. 確認使用者未列為cluster-admins群組成員。

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

撤銷使用者的**dedicated-admin**權限

1. 使用下列命令撤銷dedicated-admin權限。<CLUSTER_NAME>以您的使用者和叢集名稱取<IDP_USER_NAME>代和。

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

2. 確認使用者未列為dedicated-admins群組成員。

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

撤銷使用者對 叢集

您可以從設定的身分識別提叢集供者中移除身分識別提供者使用者，以撤銷他們的存取。

您可以為您的叢集. 下列程序會撤銷 GitHub 組織成員的叢集存取權。

1. 導航到網站並登錄到您的帳戶。 GitHub
2. 從您的 GitHub 組織中移除使用者。如需詳細資訊，請參閱 GitHub 文件中的從組織移除成員。

步驟 11：刪除叢集和AWS STS資源

您可以使用 ROSA CLI 刪除使叢集用 AWS Security Token Service (AWS STS) 的。您也可以使用 ROSA CLI 刪除由建立的IAM角色和 OIDC 提供者。ROSA若要刪除由建立的IAM策略ROSA，您可以使用主IAM控台。

> **Important**
>
> IAM相同帳戶中的其他ROSA叢集ROSA可能會使用由建立的角色和原則。

1. 刪除叢集並觀看日誌。<CLUSTER_NAME>替換為您的名稱或 ID 叢集。

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

> **Important**
>
> 您必須等待完全刪除，才能移除IAM角色、原則和 OIDC 提供者。叢集需要帳戶 IAM 角色才能刪除安裝程式建立的資源。操作員 IAM 角色必須清理 OpenShift 操作員建立的資源。操作員使用 OIDC 提供者進行驗證。

2. 執行下列命令，刪除叢集操作員用來驗證的 OIDC 提供者。

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

3. 刪除叢集特定的操作員IAM角色。

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

4. 使用以下命令刪除帳戶 IAM 角色。以要刪除之帳戶 IAM 角色的前置詞取<PREFIX>代。如果您在建立帳戶 IAM 角色時指定了自訂前置詞，請指定預設ManagedOpenShift前置詞。

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

5. 刪除由建立的IAM策略ROSA。
   a. 登入 IAM 主控台。
   b. 在 [存取管理] 下的左側功能表中，選擇 [原則]。
   c. 選取您要刪除的策略，然後選擇 [動作] > [刪除]。

d. 輸入策略名稱，然後選擇「刪除」。

e. 重複此步驟以刪除的每個 IAM 政策叢集。

中的安全性 ROSA

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同的責任。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：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。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。若要瞭解適用的規範遵循方案 ROSA，請參閱合規計劃範圍AWS 服務 中的。
- 雲端中的安全性 — 您的責任取決於您使用的資料。 AWS 服務 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。

本文件可協助您瞭解如何在使用時套用共同責任模型 ROSA。它會說明如何設定 ROSA 以符合安全性和合規性目標。您還將學習如何使用其 AWS 服務 他幫助您監控和保護 ROSA 資源的其他方法。

目錄

資料保護 ROSA

ROSA文件與AWS 共用責任模型的責任概觀定義了中的資料保護 ROSA。 AWS 負責保護運行所有 AWS 雲端. Red Hat 負責保護叢集基礎架構和基礎服務平台。客戶必須負責維持對此基礎架構上託管之內容的控制權。此內容包括您使用的安全性組態和管理工作。 AWS 服務 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 AWS 安全部落格上的AWS 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 認證並設定個別使用者。如此一來，每個使用者都只會獲得授予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 資源進行通訊。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默認安全控制 AWS 服務。
- 使用進階受管理的安全性服務 Amazon Macie，例如，有助於探索和保護儲存在中的敏感資料 Amazon S3。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，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。這包括當您使用主控台、API ROSA 或 AWS SDK 時 AWS 服務 使用或其他使用時。 AWS CLI您輸入的任何資料 ROSA 或其他服務都可能會被拾取，以便包含在診斷記錄中。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
- 網際網路流量隱私權

使用加密保護資料

資料保護是指在傳輸中（往返 ROSA）和靜態（儲存在 AWS 資料中心的磁碟上）時保護資料。

Red Hat OpenShift Service on AWS 提供對連接至 ROSA 控制平面、基礎架構和工作者節點 Amazon EC2 執行個體的 Amazon Elastic Block Store (Amazon EBS) 儲存磁碟區的安全存取權，以及用於持續性儲存的 Kubernetes 持續性磁碟區。 ROSA 加密靜態和傳輸中的磁碟區資料，並使用 AWS Key Management Service (AWS KMS) 來協助保護您的加密資料。該服務用 Amazon S3 於容器映像註冊表存儲，默認情況下，靜態加密。

> **Important**
>
> 因為這 ROSA 是一項受管理的服務， AWS 而 Red Hat 會管理所 ROSA 使用的基礎架構。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支援的儲存磁碟區的資料加密

Red Hat OpenShift Service on AWS 使用 Kubernetes 持續性磁碟區 (PV) 架構，允許叢集管理員佈建具有持續性儲存區的叢集。持續性磁碟區以及控制平面、基礎結構和背景工作者節點均由連接至 Amazon EC2 執行個體的 Amazon Elastic Block Store (Amazon EBS) 儲存磁碟區提供支援。

對於受支援的 ROSA 持續性磁碟區和節點 Amazon EBS，會在託管 EC2 執行個體的伺服器上進行加密作業，以確保執行個體及其附加儲存之間靜態資料和傳輸中資料的安全性。如需詳細資訊，請參閱《使用指南》中的 Amazon EC2 〈Amazon EBS 加密〉。

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

ROSA 預設為使用 Amazon EBS CSI 驅動程式來佈建 Amazon EBS 儲存區。依預設， Amazon EBS CSI 驅動程式和 Amazon EBS CSI 驅動程式操作員會安裝在`openshift-cluster-csi-drivers`命名空間中的叢集上。 Amazon EBS CSI 驅動程式和操作員可讓您動態佈建持續性磁碟區並建立磁碟區快照。

ROSA 也能夠使用 CSI 驅動程式和 Amazon EFS Amazon EFS CSI 驅動程式操作員來佈建持續性磁碟區。 Amazon EFS 驅動程式和操作員也可讓您在網繭之間或與 Kubernetes 內部或外部的其他應用程式共用檔案系統資料。

CSI 駕駛員和 Amazon EBS Amazon EFS CSI 驅動程序在傳輸過程中都可以保護磁碟區數據。如需詳細資訊，請參閱 Red Hat 文件中的使用容器儲存介面 (CSI)。

> **Important**
>
> 使用 Amazon EFS CSI 驅動程式動態佈建 ROSA 持續性磁碟區時，在評估檔案系統權限時，請 Amazon EFS 考量存取點的使用者 ID、群組 ID (GID) 和次要群組識別碼。 Amazon EFS 以存取點上的使用者和群組識別碼取代檔案上的使用者和群組識別碼，並忽略 NFS 用戶端 ID。因此， Amazon EFS 無訊息地忽略`fsGroup`設定。 ROSA 無法通過使用替換文件的 GID `fsGroup`。任何可存取已掛接存 Amazon EFS 取點的網繭都可以存取磁碟區上的任何檔案。若要取得更多資訊，請參閱《使用指南》中的〈 Amazon EFS 使用 Amazon EFS 存取點〉。

電子光碟加密

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，並新增額外的加密層。`etcd`一旦加密，您將產生大約 20% 的額外效能額外負荷。我們建議您僅在使用案例特別需要時才啟用`etcd`加密。如需詳細資訊，請參閱 ROSA 服務定義中的 etcd 加密。

金鑰管理

ROSA 用 KMS keys 於安全地管理客戶應用程式的控制平面、基礎架構和工作者資料磁碟區和持續性磁碟區。在建立叢集期間，您可以選擇使用由 KMS key 提供的預設 AWS 管理 Amazon EBS，或指定您自己的客戶管理金鑰。如需詳細資訊，請參閱使用 KMS 進行資料加密。

內建影像登錄的資料加密

ROSA 提供內建容器映像登錄，以透過儲存 Amazon S3 貯體儲存區儲存、擷取和共用容器映像檔。登錄由 OpenShift 映像登錄操作員設定及管理。它為使用者提供了一個 out-of-the-box 解決方案，以管理執行其工作負載並在現有叢集基礎結構之上執行的映像檔。如需詳細資訊，請參閱 Red Hat 文件中的登錄。

ROSA 提供公共和私人映像註冊表。對於企業應用程式，我們建議使用私人登錄來保護您的映像檔，避免未經授權的使用者使用。若要保護登錄的靜態資料，預設 ROSA 會使用含 Amazon S3 受管理金鑰的伺服器端加密 (SSE-S3)。這不需要您採取任何行動，並且不收取額外費用。如需詳細資訊，請參閱《使用指南》中的使用 Amazon S3 受管理加密金鑰使用伺服器端加密來保護資料 (SSE-S3)。Amazon S3

ROSA 使用傳輸層安全性 (TLS) 通訊協定來保護往返映像登錄的資料。如需詳細資訊，請參閱 Red Hat 文件中的登錄。

使用 KMS 的資料加密

ROSA 用 AWS KMS 於安全地管理加密資料的金鑰。根據預設，會使用由所 KMS key 提供的 AWS 管理來加密控制平面、基礎架構和背景工作者節點磁碟區 Amazon EBS。這 KMS key 有別名`aws/ebs`。依預設，使用預設 gp3 儲存類別的持續性磁碟區也會使用此 KMS key加密。

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

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續性磁碟區，或指定您自己的客戶管理對稱 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。

您也可以透過定義一個來加密叢集中個別容器的持續性磁碟區 KMS key。當您在部署到時具有明確的符合性和安全性準則時，這非常有用 AWS。如需詳細資訊，請參閱 Red Hat 文件 KMS key中的 AWS 使用加密容器持續性磁碟區。

使用您自 KMS keys己的磁碟區加密持續性磁碟區時，應考慮以下幾點：

- 當您使用自己的 KMS 加密時 KMS key，金鑰必須存在 AWS 區域 於叢集中。
- 創建和使用您自己的費用是相關的 KMS keys。如需詳細資訊，請參閱 AWS Key Management Service 定價。

網際網路流量隱私權

Red Hat OpenShift Service on AWS 使用 Amazon Virtual Private Cloud (Amazon VPC) 在 ROSA 叢集中的資源之間建立界限，並控制它們、內部部署網路和網際網路之間的流量。如需有關 Amazon VPC 安全性的詳細資訊，請參閱《 Amazon VPC 使用指南》中 Amazon VPC的「網路間流量隱私權」。

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存取網際網路。如果您是叢集管理員，也可以在網繭層級定義網路原則，以限制 ROSA 叢集中網繭的網繭間流量。如需詳細資訊，請參閱 ROSA.

的身分識別與存取管理 ROSA

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制誰可以驗證（登錄）和授權（有權限）使用 ROSA 資源。 IAM 是您 AWS 服務可以免費使用的。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- ROSA 以識別為基礎的原則範例
- AWS 受管理的 IAM 政策 ROSA
- 疑難排解 ROSA 身分和存取

物件

你如何使用 AWS Identity and Access Management （ IAM ）不同，具體取決於你在做的工作 ROSA。

服務使用者-如果您使用 ROSA 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 ROSA 功能來完成工作時，您可能需要其他權限。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，請參閱疑難排解 ROSA 身分與存取權限。

服務管理員-如果您負責公司的 ROSA 資源，您可能擁有完整的存取權 ROSA。決定您的服務使用者應該存取哪些 ROSA 功能和資源是您的工作。然後，您必須向 IAM 管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念 IAM。

IAM 管理員-如果您是 IAM 系統管理員，您可能想要瞭解用來管理存取權的原則的詳細資訊 ROSA。若要檢視可在中使用的以 ROSA 身分識別為基礎的原則範例 IAM，請參閱以ROSA 身分識別為基礎的原則範例。

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 AWS 帳戶 root 使用者、或假設 IAM 角色的 IAM 使用者身分驗證 (登入 AWS)。

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM Identity Center) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用 IAM 角色設定聯合身分識別。當您使 AWS 用同盟存取時，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 AWS 帳戶中的如何登入

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以便使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 AWS 一般參考中的簽名版本 4 簽署程序。

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) 來增加帳戶的安全性。若要進一步了解，請參閱 IAM 身份中心 (AWS 單一登入的後續任務) 使用者指南中的多因素身份驗證和 IAM 使用者指南中的使用多因素身份 AWS驗證 (MFA)。

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，該身分可以完整存取帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 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 root 使用者身分登入的完整工作清單，請參閱《帳戶管理參考指南》中的需要 root 使用者認證的工作。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時登入資料進行存取 AWS 服務 。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identity Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

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，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM 身分中心的相關資訊，請參閱什麼是 IAM 身分中心？ 在 AWS IAM 身分中心 (AWS Single Sign-On 的後續任務) 使用者指南中。

IAM 使用者 和群組

A IAM 使用者是您的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不 IAM 使用者 要建立具有密碼和存取金鑰等長期認證的使用者。不過，如果您有需要長期認證的特定使用案例 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 群組是指定集合的識別 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，您可以擁有一個名為 IamAdmins 的群組，並授與該群組管理資源的權限。 IAM

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，但角色僅提供暫時憑證。若要深入了解，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 角色是您 AWS 帳戶 中具有特定權限的身份。它類似於一個 IAM 使用者，但與特定的人沒有關聯。您可以 AWS Management Console 透過切換角色來暫時擔任中的角色。 IAM 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需有關使用角色的方法的詳細資訊，請參閱 IAM IAM 使用者指南中的使用角色。

IAM 具有臨時認證的角色在下列情況下很有用：

- 同盟使用者存取-若要將權限指派給同盟身分，您可以建立角色並定義角色的權限。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。如需許可集的相關資訊，請參閱 AWS IAM 身分中心中的許可集 (AWS Single Sign-On 的後續任務) 使用者指南。
- 臨時 IAM 使用者 權限- IAM 使用者 可以假定 IAM 角色暫時承擔特定任務的不同權限。
- 跨帳戶存取-您可以使用 IAM 角色允許不同帳戶中的某個人 (受信任的主體) 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。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與以資源為基礎的政策有何不同。
- 跨服務訪問-某些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在中執行應用程式 Amazon EC2 或將物件儲存在中 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。
  - 轉寄存取工作階段 (FAS)-當您使用 IAM 使用者 或角色執行中的動作時 AWS，您會被視為主參與者。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 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 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-服務角色是指服務代表您執行動作的 IAM 角色。 IAM 管理員可以從中建立、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. 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 IAM 帳戶中，且屬於服務所有。 IAM 管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 執行於的應用程式 Amazon EC2 -您可以使用 IAM 角色來管理在執行個體上 Amazon EC2 執行並提出 AWS CLI 或 AWS API 要求的應用程式的臨時登入資料。這比在 Amazon EC2 實例中存儲訪問密鑰更好。若要將 AWS 角色指派給 Amazon EC2 執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上 Amazon EC2 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》中的使用 IAM 角色將許可授與在 Amazon EC2 執行個體上執行的應用程式。

若要了解是否使用 IAM 角色或使用 IAM 者，請參閱 IAM 使用者指南中的何時建立 IAM 角色 (而非使用者)。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。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哪些內容。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。若要授與使用者對所需資源執行動作的權限， IAM 管理員可以建立 IAM 策略。然後，系統管理員可以將 IAM 原則新增至角色，使用者可以擔任這些角色。

IAM 原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

以身分識別為基礎的原則是 JSON 權限原則文件，您可以附加至身分識別 (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政 IAM 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。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略 IAM 中使用 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 ACL 的服務範例。如需進一步瞭解 ACL，請參閱《Amazon Simple Storage Service 開發人員指南》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原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限-權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給 IAM 實體 (IAM 使用者 或角色) 的最大權限。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。如需有關許可界限的詳細資訊，請參閱《IAM 使用者指南》中的IAM 實體權限界限。
- 服務控制策略（SCP）-SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。 AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。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權限，包括每個 AWS 帳戶 root 使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱 AWS Organizations 使用者指南中的 SCP 如何運作。
- 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。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

ROSA 以識別為基礎的原則範例

依預設， IAM 使用者 和角色沒有建立或修改 AWS 資源的權限。他們也無法使用 AWS Management Console AWS CLI、或 AWS API 執行工作。 IAM 系統管理員必須建立授與使用者和角色權限的 IAM 政策，才能在所需的指定資源上執行特定 API 作業。然後，系統管理員必須將這些原則附加至需要這些權限的 IAM 使用者 或群組。

若要了解如何使用這些 JSON 政策文件範例建立以 IAM 身分識別為基礎的政策，請參閱 IAM 使用者指南中的 JSON 索引標籤上建立政策。

使用控 ROSA 制台

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。權限可讓主參與者訂閱及取消訂閱中的 ROSA 產品清單，以 AWS Marketplace 及檢視 AWS Marketplace 訂閱。若要新增必要的許可，請前往主ROSA 控台並將受 AWS 管政策附加ROSAManageSubscription到 IAM 主體。如需有關的詳細資訊ROSAManageSubscription，請參閱AWS 受管理的原則:ROSA ManageSubscription。

AWS 適用於 ROSA 與醫護機構的管理政策

含託管控制平面 (HCP) 的 ROSA 會使用具有服務作業和支援所需權限的 AWS 受管理原則。您可以使用 ROSA IAM CLI 或主控台將這些原則附加至 AWS 帳戶.

如需詳細資訊，請參閱 ROSA的AWS 受管政策。

ROSA 經典版的客戶管理政策

ROSA 典型使用具有服務預先定義的許可的客戶受管 IAM 政策。您可以使用 ROSA CLI 建立這些原則，並將它們附加到 AWS 帳戶. ROSA 要求根據服務定義配置這些策略，以確保持續的操作和服務支持。

> **Note**
>
> 您不應該在未先諮詢 Red Hat 的情況下更改 ROSA 傳統政策。這樣做可能會使 Red Hat 的 99.95% 叢集正常運作時間服務等級協定失效。含託管控制平面的 ROSA 會使用 AWS 受管理的原則，其權限集較為有限。如需詳細資訊，請參閱 ROSA的AWS 受管政策。

客戶管理政策有兩種類型 ROSA：帳戶策略和操作員政策。帳號原則會附加至服務用來與 Red Hat 建立信任關係的 IAM 角色，以提供網站可靠性工程師 (SRE) 支援、叢集建立及運算功能。操作員原則會附加至操作員用於與輸入、儲存、映像登錄和節點管理相關之叢集作業的 IAM 角色。 OpenShift 每個帳戶策略都會建立一次 AWS 帳戶，而每個叢集建立一次運算子策略。

如需詳細資訊，請參閱 ROSA 傳統帳戶原則和 ROSA 傳統操作員原則。

允許使用者檢視他們自己的許可

此範例顯示如何建立原則，IAM 使用者 以便檢視附加至其使用者身分識別的內嵌和受管理原則。此原則包含在主控台上完成此動作或以程式設計方式使用 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": "*"
        }
    ]
}
```

羅莎經典帳戶政策

本節提供 ROSA 傳統所需帳號策略的詳細資訊。ROSA 傳統版需要這些權限才能管理叢集執行的 AWS 資源，並啟用 Red Hat 站台可靠性工程師對叢集的支援。您可以為策略名稱指派自訂前置詞，但這些策略應按照此頁面上的定義命名 (例如`ManagedOpenShift-Installer-Role-Policy`)。

帳號策略特定於 OpenShift 次要發行版本，並且具有向後相容性。在建立或升級叢集之前，您應該執行以確認原則版本和叢集版本是否相同`rosa list account-roles`。如果原則版本小於叢集版本，請執行`rosa upgrade account-roles`以升級角色和附加的原則。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原則和角色。

[前綴]-安裝程序角色策略

您可以將 `[Prefix]-Installer-Role-Policy` 連接到 IAM 實體。您必須先將此政策附加到名為的 IAM 角色，才能建立 ROSA 傳統叢集`[Prefix]-Installer-Role`。此原則會授與必要的權限，讓 ROSA 安裝程式管理叢集建立所需的 AWS 資源。

許可政策

本政策文件中定義的權限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:PassRole",
                "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"
                }
            }
        }
    ]
}
```

[前綴]-角ControlPlane色策略

您可以將 [Prefix]-ControlPlane-Role-Policy 連接到 IAM 實體。您必須先將此政策附加到名為的 IAM 角色，才能建立 ROSA 傳統叢集[Prefix]-ControlPlane-Role。此原則會將必要的權限授與 ROSA 傳統版，以管理控制平面 Amazon EC2 和讀取的 Elastic Load Balancing 資源，以及託管 ROSA 控制平面的資源 KMS keys。

許可政策

本政策文件中定義的權限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": "*"
        }
    ]
}
```

[前綴]-工人角色政策

您可以將 [Prefix]-Worker-Role-Policy 連接到 IAM 實體。您必須先將此政策附加到名為的 IAM 角色，才能建立 ROSA 傳統叢集[Prefix]-Worker-Role。此政策將所需的許可授予 ROSA 傳統版，以描述作為工作者節點執行的 EC2 執行個體。

許可政策

本政策文件中定義的權限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": "*"
        }
    ]
}
```

[前綴]-Support 角色政策

您可以將 [Prefix]-Support-Role-Policy 連接到 IAM 實體。您必須先將此政策附加到名為的 IAM 角色，才能建立 ROSA 傳統叢集[Prefix]-Support-Role。此原則會將必要的權限授與 Red Hat 站台可靠性工程，以觀察、診斷及支援 ROSA 傳統叢集所使用的 AWS 資源，包括變更叢集節點狀態的能力。

許可政策

本政策文件中定義的權限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*"
            ]
        }
    ]
}
```

羅莎經典運營商政策

此段落提供 ROSA 傳統所需之運算子原則的詳細資訊。您必須先將這些原則附加至相關的操作員角色，才能建立 ROSA 傳統叢集。每個叢集都需要一組唯一的操作員角色。

需要這些權限才能允許 OpenShift 操作員管理 ROSA 傳統叢集節點。您可以為原則名稱指派自訂前置詞，以簡化原則管理 (例如`ManagedOpenShift-openshift-ingress-operator-cloud-credentials`)。

[前綴]-openshift-ingress-operator-cloud-證書

您可以將 `[Prefix]-openshift-ingress-operator-cloud-credentials` 連接到 IAM 實體。此原則會將必要的權限授與 Ingress 操作員，以佈建和管理外部叢集存取的負載平衡器和 DNS 組態。此原則也允許 Ingress 操作員讀取和篩選 Route 53 資源標籤值，以探索託管區域。如需有關操作員的詳細資訊，請參閱 OpenShift GitHub 文件中的OpenShift 入口操作員。

許可政策

本政策文件中定義的權限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": "*"
        }
    ]
}
```

[前綴]-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。此原則會授與 Amazon EBS CSI 驅動程式操作員所需的權限，以便在 ROSA 傳統叢集上安裝和維護 Amazon EBS CSI 驅動程式。如需有關運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的 aws-ebs-csi-driver-operator。

許可政策

本政策文件中定義的權限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": "*"
        }
    ]
}
```

[前綴]-雲憑openshift-machine-api-aws據

您可以將 `[Prefix]-openshift-machine-api-aws-cloud-credentials` 連接到 IAM 實體。此原則會將必要的權限授與機器 Config 操作員，以描述、執行及終止以背景工作節點管理的 Amazon EC2 執行個體。此原則也會授與允許使用的 Worker 節點根磁碟區磁碟區進行磁碟加密的權限 AWS KMS keys。如需有關運算子的詳細資訊，請參閱 OpenShift GitHub 文件machine-config-operator中的。

許可政策

本政策文件中定義的權限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:PassRole",
                "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
                }
            }
        }
    ]
}
```

[前綴]-雲憑openshift-cloud-credential-operator據

您可以將 [Prefix]-openshift-cloud-credential-operator-cloud-credentials 連接到 IAM 實體。此政策授予雲端登入資料操作員所需的權限，以擷取 IAM 使用者 詳細資料，包括存取金鑰

ID、附加的內嵌政策文件、使用者的建立日期、路徑、使用者 ID 和 Amazon 資源名稱 (ARN)。如需有關運算子的詳細資訊，請參閱 OpenShift GitHub 文件cloud-credential-operator中的。

許可政策

本政策文件中定義的權限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": "*"
        }
    ]
}
```

[前綴]-雲憑openshift-image-registry-installer據

您可以將 `[Prefix]-openshift-image-registry-installer-cloud-credentials` 連接到 IAM 實體。此原則會授與映像登錄操作員所需的權限，以佈建及管理 ROSA Classic 叢集內映像登錄和相依服務的資源，包括 Amazon S3. 這是必要的，以便操作員可以安裝和維護 ROSA 傳統叢集的內部登錄。如需有關運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的映像登錄操作員。

許可政策

本政策文件中定義的權限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": "*"
        }
    ]
}
```

[前綴]-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。此原則會將必要的權限授與雲端網路 Config 控制器操作員，以佈建和管理網路資源，以供 ROSA 傳統叢集網路覆蓋使用。操作員會使用這些權限來管理 Amazon EC2 執行個體的私有 IP 位址，做為 ROSA 傳統叢集的一部分。如需有關運算子的詳細資訊，請參閱 OpenShift GitHub 文件loud-network-config-controller中的 C。

許可政策

本政策文件中定義的權限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 受管理的 IAM 政策 ROSA

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 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。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱 IAM 使用指南中的AWS 受管理策略。

AWS 管理策略：羅莎 ManageSubscription

您可以將`ROSAManageSubscription`原則附加至您的 IAM 實體。在 AWS ROSA 主控台 ROSA 中啟用之前，必須先將此原則附加到主控台角色。

此原則會授予您管理 ROSA 訂閱所需的 AWS Marketplace 權限。

許可詳細資訊

此政策包含以下許可。

- `aws-marketplace:Subscribe`-授予訂閱 AWS Marketplace 產品的權限 ROSA。
- `aws-marketplace:Unsubscribe`-允許主參與者移除 AWS Marketplace 產品的訂閱。
- `aws-marketplace:ViewSubscriptions`-允許主參與者從中 AWS Marketplace檢視訂閱。這是必要的， IAM 主體才能檢視可用的 AWS Marketplace 訂閱。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理原則參考指南》ManageSubscription中的 ROSA。

AWS 具有 HCP 帳戶角色之 ROSA 的受管理原則

您可以將這些 AWS 受管政策附加到搭配託管控制平面 (HCP) 使用 ROSA 所需的帳戶角色。Red Hat 網站可靠性工程 (SRE) 支援叢集、叢集建立和運算功能都需要這些權限。

需要下列受管理的策略：

- ROSA WorkerInstancePolicy — 允許 ROSA 服務管理叢集中的 Amazon EC2 執行個 ROSA 體生命週期。
- ROSSRE SupportPolicy — 授予 Red Hat 站台可靠性工程師 (SRE) 所需的權限，以直接觀察、診斷及支援叢集相關 AWS 資源，包括變更 ROSA 叢集節點狀態的能力。 ROSA
- ROSA InstallerPolicy — 授予安裝程式所需的權限，以管理支援叢集安裝的 AWS 資源。

AWS 具有 HCP 操作員角色的 ROSA 管理政策

您可以將這些 AWS 受管政策附加到搭配託管控制平面 (HCP) 使用 ROSA 所需的操作員角色。需要權限才能允許 OpenShift 操作員透過 HCP 叢集節點管理 ROSA。

需要下列受管理的策略：

- RosaAmazoneBSCSI DriverOperatorPolicy — 授予 Amazon EBS CSI 驅動程式操作員所需的權限，以便在叢集上安裝和維護 CSI 驅動程式。 Amazon EBS ROSA
- ROSA IngressOperatorPolicy — 授與入口操作員所需的權限，以佈建和管理叢集的負載平衡器和 DNS 組態。 ROSA 該策略允許對標籤值的讀取存取權。然後，操作員會篩選 Route 53 資源的標籤值，以探索託管區域。
- ROSA ImageRegistryOperatorPolicy — 授與映像登錄操作員所需的權限，以佈建和管理 ROSA 叢集內映像登錄和相依服務 (包括 S3) 的資源。
- ROSA CloudNetworkConfigOperatorPolicy — 授予雲端網路 Config 控制器操作員所需的權限，以佈建和管理 ROSA 叢集網路覆蓋的網路資源。
- ROSA KubeControllerPolicy — 授予 kube 控制器所需的權限 Amazon EC2 Elastic Load Balancing，以便管理和託管控制平面集群的 AWS KMS 資源。 ROSA
- ROSA NodePoolManagementPolicy — 將必要權限授與 NodePool 控制器，以描述、執行和終止以背景工作節點管理的 Amazon EC2 執行個體。此原則也會使用金鑰啟用 Worker 節點根磁碟區的磁碟加 AWS KMS 密。

- ROSAKMS ProviderPolicy — 授予內建 AWS 加密提供者所需的權限，以管理支援 etcd 資料加密的 AWS KMS 金鑰。此原則允許 Amazon EC2 使用加密提供者提供的 KMS 金鑰來加密和解 AWS 密`etcd`資料。
- ROSA ControlPlaneOperatorPolicy — 授予控制平面操作員所需的權限，以便管理 Amazon EC2 託管控制平面叢集的 Route 53 資源。 ROSA

若要檢視受管理的策略權限，請參閱AWS 受管理的策略參考指南中的 AWS 受管理策略

ROSAAWS 受管理策略的更新

檢視 ROSA 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱ROSA 文件記錄頁面上的 RSS 摘要。

變更	描述	日期
羅莎 NodePoolManagement Policy -政策更新	ROSA 已更新原則，以允許 ROSA 節點集區管理員描述 DHCP 選項集，以便設定適當的私人 DNS 名稱。若要深入瞭解，請參閱 ROSA NodePoolManagementPolicy。	2024年5月2日
羅莎 InstallerPolicy -政策更新	ROSA 已更新原則，允許 ROSA 安裝程式使用標籤金鑰比對`"kubernetes.io/cluster/*"` 將標籤新增至子網路。若要深入瞭解，請參閱 ROSA InstallerPolicy。	2024年4月24日
羅薩瑞 SupportPolicy — 政策更新	ROSA 已更新原則，以允許 SRE 角色擷取已標記 ROSA 為`red-hat-managed` 的執行個體設定檔相關資訊。要了解更多信息，請參閱 ROSSRE SupportPolicy。	2024年4月10日
羅莎 InstallerPolicy -政策更新	ROSA 已更新原則，以允許 ROSA 安裝程式驗證的 AWS	2024年4月10日

變更	描述	日期
	受管理原則 ROSA 是否已附加至使用的 IAM 角色 ROSA。此更新也可讓安裝程式識別是否已將客戶管理的政策附加至 ROSA 角色。若要深入瞭解，請參閱 ROSA InstallerPolicy。	
羅莎 InstallerPolicy -政策更新	ROSA 已更新原則，以允許服務在因缺少客戶指定的叢集 OIDC 提供者而導致叢集安裝失敗時提供安裝程式警示訊息。此更新也可讓服務擷取現有的 DNS 名稱伺服器，以便叢集佈建作業具有冪等性。若要深入瞭解，請參閱 ROSA InstallerPolicy。	2024年1月26日
羅薩瑞 SupportPolicy — 政策更新	ROSA 已更新原則，以允許服務使用 DescribeSecurityGroups API 對安全群組執行讀取作業。要了解更多信息，請參閱 ROSSRE SupportPolicy。	2024年1月22日
羅莎 ImageRegistryOperatorPolicy -政策更新	ROSA 已更新原則，以允許映像登錄操作員對具有 14 個字元名稱的區域中的 Amazon S3 值區採取動作。若要深入瞭解，請參閱 ROSA ImageRegistryOperatorPolicy。	2023 年 12 月 12 日

變更	描述	日期
羅莎 KubeControllerPolicy -政策更新	ROSA 已更新原則，以允許說明可用區域、 Amazon EC2 執行個體、路由表、安全群組、VPC 和子網路。 kube-controller-manager 若要深入瞭解，請參閱 ROSA KubeControllerPolicy。	2023 年 10 月 16 日
羅莎 ManageSubscription -政策更新	ROSA 更新原則以使用託管控制平面新增 ROSA ProductId。若要深入瞭解，請參閱 ROSA ManageSubscription。	2023 年 8 月 1 日
羅莎 KubeControllerPolicy -政策更新	ROSA 已更新原則，以允許將網路負載平衡器建立為 Kubernetes 服務負載平衡器。kube-controller-manager 網路負載平衡器提供更強大的處理揮發性工作負載的能力，並支援負載平衡器的靜態 IP 位址。若要深入瞭解，請參閱 ROSA KubeControllerPolicy。	2023 年 7 月 13 日
羅莎 NodePoolManagementPolicy -添加了新的政策	ROSA 新增了一個新的政策，允許 NodePool 控制器描述、執行和終止作為工作節點管理的 Amazon EC2 執行個體。此原則也會使用金鑰啟用 Worker 節點根磁碟區的磁碟加 AWS KMS 密。若要深入瞭解，請參閱 ROSA NodePoolManagementPolicy。	2023 年 6 月 8 日

變更	描述	日期
羅莎 InstallerPolicy -添加了新的政策	ROSA 增加了一個新的策略，以允許安裝程序管理支持集群安裝的 AWS 資源。若要深入瞭解，請參閱 ROSA Installer Policy。	2023 年 6 月 6 日
羅薩瑞 SupportPolicy -添加了新政策	ROSA 新增了一項新政策，讓 Red Hat SRE 能夠直接觀察、診斷並支援與 ROSA 叢集相關的 AWS 資源，包括變更 ROSA 叢集節點狀態的能力。要了解更多信息，請參閱 ROSSRE SupportPolicy。	2023 年 6 月 1 日
羅薩克姆斯 ProviderPolicy -添加了新的策略	ROSA 已新增新原則，以允許內建的 AWS 加密提供者管理 AWS KMS 金鑰以支援 etcd 資料加密。要了解更多信息，請參閱 ROSAKMS ProviderPolicy。	2023 年 4 月 27 日
羅莎 KubeControllerPolicy -添加了新的政策	ROSA 增加了一個新的策略，允許 kube 控制器管理 Amazon EC2 Elastic Load Balancing，並 ROSA 與託管控制平面集群的 AWS KMS 資源。若要深入瞭解，請參閱 ROSA KubeControllerPolicy。	2023 年 4 月 27 日
羅莎 ImageRegistryOperatorPolicy -添加了新的政策	ROSA 新增政策以允許映像登錄操作員佈建和管理 ROSA 叢集內映像登錄和相依服務 (包括 S3) 的資源。若要深入瞭解，請參閱 ROSA ImageRegistryOperatorPolicy。	2023 年 4 月 27 日

變更	描述	日期
羅莎 ControlPlaneOperatorPolicy -添加了新的政策	ROSA 已新增新原則，以允許控制平面操作員管 Amazon EC2 理託管控制平面叢集的 Route 53 資源。 ROSA 若要深入瞭解，請參閱 ROSA ControlPlaneOperatorPolicy。	2023 年 4 月 24 日
羅莎 CloudNetworkConfigOperatorPolicy -添加了新的政策	ROSA 新增政策，允許雲端網路 Config 控制器操作員為 ROSA 叢集網路覆蓋佈建和管理網路資源。若要深入瞭解，請參閱 ROSA CloudNetworkConfigOperatorPolicy。	2023 年 4 月 20 日
羅莎 IngressOperatorPolicy -添加了新的政策	ROSA 已新增新原則，以允許 Ingress 操作員佈建和管理叢集的負載平衡器和 DNS 組態。 ROSA 若要深入瞭解，請參閱 ROSA IngressOperatorPolicy。	2023 年 4 月 20 日
羅莎亞馬遜 BSCSI — 添加了新DriverOperatorPolicy 政策	ROSA 增加了一個新的策略，以允許 Amazon EBS CSI 驅動程序操作員在 ROSA 集群上安裝和維護 Amazon EBS CSI 驅動程序。若要深入瞭解，請參閱羅莎亞馬遜 BSCSI DriverOperatorPolicy。	2023 年 4 月 20 日
羅莎 WorkerInstancePolicy -添加了新的政策	ROSA 新增政策以允許服務管理叢集資源。若要深入瞭解，請參閱 ROSA WorkerInstancePolicy。	2023 年 4 月 20 日

變更	描述	日期
羅莎 ManageSubscription -添加了新的政策	ROSA 已新增政策，以授與管理 ROSA 訂閱所需的 AWS Marketplace 權限。若要深入瞭解，請參閱 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 開始追蹤其 AWS 受管理策略的變更。	2022 年 3 月 2 日

AWS 具有 HCP 帳戶角色之 ROSA 的受管理原則

> **Note**
>
> 這些 AWS 受管理的原則適用於 ROSA 與託管控制平面 (HCP) 搭配使用。ROSA 傳統叢集使用客戶受管 IAM 政策。如需 ROSA 傳統原則的詳細資訊，請參閱 ROSA 傳統帳戶原則和 ROSA 傳統運算子原則。

這些 AWS 受管政策會新增 ROSA 與託管控制平面 (HCP) IAM 角色搭配使用的許可。Red Hat 網站可靠性工程 (SRE) 技術支援、叢集安裝、控制平面與運算功能都需要這些權限。

主題

- AWS 管理策略：羅莎 WorkerInstancePolicy
- AWS 管理策略：俄羅斯 SupportPolicy
- AWS 管理策略：羅莎 InstallerPolicy

AWS 管理策略：羅莎 WorkerInstancePolicy

您可以附加`ROSAWorkerInstancePolicy`到您的 IAM 實體。建立含託管控制平面叢集的 ROSA 之前，您必須先將此政策附加到背景工作者 IAM 角色。

許可詳細資訊

此原則包含下列權限，可讓 ROSA 服務完成下列工作：

- `ec2`— 作為 ROSA 叢集中工作者節點生命週期管理的一部分，檢閱 AWS 區域 和 Amazon EC2 執行個體詳細資料。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理原則參考指南》WorkerInstancePolicy中的 ROSA。

AWS 管理策略：俄羅斯 SupportPolicy

您可以將 `ROSASRESupportPolicy` 連接到 IAM 實體。

建立含託管控制平面叢集的 ROSA 之前，您必須先將此政策附加至支援 IAM 角色。此原則會授予 Red Hat 網站可靠性工程師 (SRE) 所需的權限，以便直接觀察、診斷及支援與 ROSA 叢集相關的 AWS 資源，包括變更 ROSA 叢集節點狀態的能力。

許可詳細資訊

此原則包含下列權限，可讓 Red Hat SRE 完成下列工作：

- `cloudtrail`— 讀取與叢集相關的 AWS CloudTrail 事件和追蹤。
- `cloudwatch`— 讀取與叢 Amazon CloudWatch 集相關的指標。
- `ec2`— 讀取、描述和檢閱與叢集健全狀況相關的 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、描述和檢閱叢集健康狀態相關的 Elastic Load Balancing 參數。
- `iam`— 評估與叢集健全狀況相關的 IAM 角色。
- `route53`— 檢閱與叢集健康狀態相關的 DNS 設定。
- `sts`— `DecodeAuthorizationMessage` — 讀取 IAM 消息以進行調試。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理策略參考指南》SupportPolicy中的 ROASRE。

AWS 管理策略：羅莎 InstallerPolicy

您可以附加`ROSAInstallerPolicy`到您的 IAM 實體。

建立含託管控制平面叢集的 ROSA 之前，您必須先將此政策附加到名為的 IAM 角色`[Prefix]-ROSA-Worker-Role`。此原則可讓實體將遵循`[Prefix]-ROSA-Worker-Role`模式的任何角色新增至執行個體設定檔。此原則會授與必要的權限給安裝程式，以管理支援 ROSA 叢集安裝的 AWS 資源。

許可詳細資訊

此原則包含下列權限，可讓安裝程式完成下列工作：

- ec2— 使用 Red Hat AWS 帳戶 所擁有及管理的 AMI Amazon EC2 執行執行個體。說明與 Amazon EC2 節點相關聯的 Amazon EC2 執行個體、磁碟區和網路資源。這是必要的，如此 Kubernetes 控制平面才能將執行個體加入叢集。這也是必要的，以便叢集可以評估其內部的存在 Amazon VPC。使用標籤索引鍵比對"kubernetes.io/cluster/*"來標記子網路。若要確保叢集輸入所使用的負載平衡器僅在適用的子網路中建立，則必須執行此動作。
- 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。需要此權限，Kubernetes 控制平面才能動態佈建 Kubernetes 服務和應用程式服務所要求的負載平衡器。 OpenShift
- kms— 讀取 AWS KMS 金鑰、建立和管理授權 Amazon EC2，以及傳回唯一的對稱資料金鑰以供外部 AWS KMS使用。當建立叢集時啟用加密時，使用etcd加密etcd資料是必要的。
- iam— 驗證 IAM 角色和政策。動態佈建和管理叢集相關的 Amazon EC2 執行個體設定檔。使用iam:TagInstanceProfile權限將標籤新增至 IAM 執行個體設定檔。當叢集安裝因缺少客戶指定的叢集 OIDC 提供者而失敗時，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 認證。假設用於建立叢集的認證。
- secretsmanager— 讀取秘密值，以安全地允許客戶管理的 OIDC 配置作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 受管理原則參考指南》InstallerPolicy中的 ROSA。

AWS 具有 HCP 操作員角色的 ROSA 管理政策

> **Note**
>
> 這些 AWS 受管理的原則適用於 ROSA 與託管控制平面 (HCP) 搭配使用。ROSA 傳統叢集使用客戶受管 IAM 政策。如需 ROSA 傳統原則的詳細資訊，請參閱 ROSA 傳統帳戶原則和 ROSA 傳統運算子原則。

這些 AWS 受管政策會新增 ROSA 與託管控制平面 (HCP) IAM 角色搭配使用的許可。具有 HCP 叢集的 ROSA 上的 OpenShift 操作員需要這些權限才能管理叢集節點。

主題

- AWS 管理策略:羅莎亞馬遜 DriverOperatorPolicy
- AWS 管理策略：羅莎 IngressOperatorPolicy
- AWS 管理策略：羅莎 ImageRegistryOperatorPolicy
- AWS 管理策略：羅莎 CloudNetworkConfigOperatorPolicy
- AWS 管理策略：羅莎 KubeControllerPolicy
- AWS 管理策略：羅莎 NodePoolManagementPolicy
- AWS 受管理的策略：俄羅斯 ProviderPolicy
- AWS 管理策略：羅莎 ControlPlaneOperatorPolicy

AWS 管理策略:羅莎亞馬遜 DriverOperatorPolicy

您可以附加ROSAAmazonEBSCSIDriverOperatorPolicy到您的 IAM 實體。您必須將此政策附加到操作員 IAM 角色，以允許具有託管控制平面叢集的 ROSA 與其他人進行呼叫 AWS 服務。每個叢集都需要一組唯一的操作員角色。

此原則授予 Amazon EBS CSI 驅動程式操作員必要的權限，以便在 ROSA 叢集上安裝和維護 Amazon EBS CSI 驅動程式。如需有關運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的aws-ebs-csi-driver 運算子。

許可詳細資訊

此原則包含下列權限，可讓 Amazon EBS 驅動程式操作員完成下列工作：

- ec2— 建立、修改、連接、卸離和刪除連接至 Amazon EC2 執行個體的 Amazon EBS 磁碟區。建立和刪除磁 Amazon EBS 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《管理策略參考指南》DriverOperatorPolicy中的《RosaAmazoneBSCSI》。 AWS

AWS 管理策略：羅莎 IngressOperatorPolicy

您可以附加ROSAIngressOperatorPolicy到您的 IAM 實體。您必須將此政策附加到操作員 IAM 角色，以允許具有託管控制平面叢集的 ROSA 與其他人進行呼叫 AWS 服務。每個叢集都需要一組唯一的操作員角色。

此原則會將必要的權限授與 Ingress 操作員，以佈建和管理叢集的負載平衡器和 DNS 組態。 ROSA 該策略允許對標籤值的讀取存取權。然後，操作員會篩選 Route 53 資源的標籤值，以探索託管區域。如需有關操作員的詳細資訊，請參閱 OpenShift GitHub 文件中的OpenShift 入口操作員。

許可詳細資訊

此原則包含下列權限，可讓 Ingress 操作員完成下列工作：

- `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 叢集控制的 DNS 的記錄。
- `tag`— 使用權限管理已標記的`tag:GetResources`資源。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理原則參考指南》IngressOperatorPolicy中的 ROSA。

AWS 管理策略：羅莎 ImageRegistryOperatorPolicy

您可以附加`ROSAImageRegistryOperatorPolicy`到您的 IAM 實體。您必須將此政策附加到操作員 IAM 角色，以允許具有託管控制平面叢集的 ROSA 與其他人進行呼叫 AWS 服務。每個叢集都需要一組唯一的操作員角色。

此政策授予映像登錄操作員所需的權限，以佈建和管理 ROSA 叢集內映像登錄和相依服務 (包括 S3) 的資源。這是必要的，以便操作員可以安裝和維護 ROSA 叢集的內部登錄。如需有關運算子的詳細資訊，請參閱 OpenShift GitHub 文件中的映像登錄操作員。

許可詳細資訊

此原則包含下列權限，可讓映像登錄操作員完成下列動作：

- `s3`— 將 Amazon S3 值區管理並評估為容器映像內容和叢集中繼資料的持續性儲存區。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理原則參考指南》ImageRegistryOperatorPolicy中的 ROSA。

AWS 管理策略：羅莎 CloudNetworkConfigOperatorPolicy

您可以附加`ROSACloudNetworkConfigOperatorPolicy`到您的 IAM 實體。您必須將此政策附加到操作員 IAM 角色，以允許具有託管控制平面叢集的 ROSA 與其他人進行呼叫 AWS 服務。每個叢集都需要一組唯一的操作員角色。

此原則會授予雲端網路 Config 控制器操作員所需的權限，以佈建及管理 ROSA 叢集網路覆蓋的網路資源。操作員會使用這些權限來管理 ROSA 叢集中 Amazon EC2 執行個體的私有 IP 位址。如需有關運算子的詳細資訊，請參閱 OpenShift GitHub 文件loud-network-config-controller中的 C。

許可詳細資訊

此原則包含下列權限，可讓 Cloud 網路 Config 控制器操作員完成下列工作：

- ec2— 讀取、指派和說明叢集中連線 Amazon EC2 執行個體、 Amazon VPC 子網路和彈性網路介面的 ROSA 組態。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理原則參考指南》CloudNetworkConfigOperatorPolicy中的 ROSA。

AWS 管理策略：羅莎 KubeControllerPolicy

您可以附加ROSAKubeControllerPolicy到您的 IAM 實體。您必須將此政策附加到操作員 IAM 角色，以允許具有託管控制平面叢集的 ROSA 與其他人進行呼叫 AWS 服務。每個叢集都需要一組唯一的操作員角色。

此原則會授與 kube 控制器所需的權限 Amazon EC2 Elastic Load Balancing，以便管理具有託管控制平面叢集之 ROSA 的 AWS KMS 資源。如需有關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

此原則包含下列權限，可讓 kube 控制器完成下列工作：

- ec2— 建立、刪除和新增標籤至 Amazon EC2 執行個體安全群組。將輸入規則新增至安全群組。說明可用區域、 Amazon EC2 執行個體、路由表、安全群組、VPC 和子網路。
- elasticloadbalancing— 建立和管理負載平衡器及其原則、建立和管理負載平衡器接聽程式、向目標群組註冊目標，以及管理目標群組、使用負載平衡器註冊和取消註冊 Amazon EC2 執行個體，以及將標籤新增至負載平衡器。
- kms-檢索有關 AWS KMS 密鑰的詳細信息。當建立叢集時啟用加密時，使用etcd加密etcd資料是必要的。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理原則參考指南》KubeControllerPolicy中的 ROSA。

AWS 管理策略：羅莎 NodePoolManagementPolicy

您可以附加ROSANodePoolManagementPolicy到您的 IAM 實體。您必須將此政策附加到操作員 IAM 角色，以允許具有託管控制平面叢集的 ROSA 對其他 AWS 服務進行呼叫。每個叢集都需要一組唯一的操作員角色。

此原則會將必要的權限授與 NodePool 控制器，以描述、執行和終止以 Worker 節點形式管理的 Amazon EC2 執行個體。此原則也授與允許使用 AWS KMS 金鑰對 Worker 節點根磁碟區進行磁碟加密的權限。如需有關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

此原則包含下列權限，可讓 NodePool 控制器完成下列工作：

- ec2— 使用 Red Hat AWS 帳戶 所擁有及管理的 AMI Amazon EC2 執行執行個體。管理叢集中的 ROSA EC2 生命週期。使用 Elastic Load Balancing、 Amazon VPC、和動態建立和整合工作者節點 Amazon EC2。 Route 53 Amazon EBS
- iam— 透 Elastic Load Balancing 過名為AWSServiceRoleForElasticLoadBalancing的服務連結角色使用。指派角色給 Amazon EC2 執行個體設定檔。
- kms— 讀取 AWS KMS 金鑰、建立和管理授權 Amazon EC2，以及傳回唯一的對稱資料金鑰以供外部 AWS KMS使用。若要允許 Worker 節點根磁碟區進行磁碟加密，這是必要的。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理原則參考指南》NodePoolManagementPolicy中的 ROSA。

AWS 受管理的策略：俄羅斯 ProviderPolicy

您可以附加ROSAKMSProviderPolicy到您的 IAM 實體。您必須將此政策附加到操作員 IAM 角色，以允許具有託管控制平面叢集的 ROSA 與其他人進行呼叫 AWS 服務。每個叢集都需要一組唯一的操作員角色。

此原則會將必要權限授與內建的 AWS 加密提供者，以管理支援資etcd料加密的 AWS KMS 金鑰。此原則允許 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。如需有關此提供者的詳細資訊，請參閱 Kubernetes 文 GitHub 件中的AWS 加密提供者。

許可詳細資訊

此原則包含下列權限，可讓加 AWS 密提供者完成下列工作：

- kms— 加密, 解密, 和檢索密 AWS KMS 鑰. 當建立叢集時啟用加密時，使用etcd加密etcd資料是必要的。

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理策略參考指南》ProviderPolicy中的 ROSAKMS。

AWS 管理策略：羅莎 ControlPlaneOperatorPolicy

您可以附加ROSAControlPlaneOperatorPolicy到您的 IAM 實體。您必須將此政策附加到操作員 IAM 角色，以允許具有託管控制平面叢集的 ROSA 與其他人進行呼叫 AWS 服務。每個叢集都需要一組唯一的操作員角色。

此原則會授與控制平面操作員所需的權限，以管理 Amazon EC2 ROSA 與託管控制平面叢集的 Route 53 資源。如需有關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

此原則包含下列權限，可讓控制平面操作員完成下列工作：

- ec2— 建立和管理 Amazon VPC 端點。
- route53— 列出和更改 Route 53 記錄集和列出託管區域.

若要檢視完整的 JSON 政策文件，請參閱《 AWS 受管理原則參考指南》ControlPlaneOperatorPolicy中的 ROSA。

疑難排解 ROSA 身分和存取

使用下列資訊可協助您診斷及修正使用和時可能會遇到的 ROSA 常見問題 IAM。

AWS Organizations 服務控制策略拒絕所需 AWS Marketplace 的權限

如果您嘗試啟用時，您的 AWS Organizations 服務控制原則 (SCP) 不允許所需的 AWS Marketplace 訂閱權限 ROSA，則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，則必須聯絡您的系統管理員以尋求協助。您的管理員是管理組織帳戶的人員。要求該人執行下列動作：

1. 將 SCP 設定為允許aws-marketplace:Subscribeaws-marketplace:Unsubscribe、和aws-marketplace:ViewSubscriptions權限。如需詳細資訊，請參閱《 AWS Organizations 使用指南》中的〈更新 SCP〉。
2. ROSA 在組織的管理帳戶中啟用。

3. 將 ROSA 訂閱共用至需要在組織內存取權的成員帳戶。如需詳細資訊，請參閱《AWS Marketplace 購買指南》中的「在組織中共用訂閱」。

使用者或角色沒有必要的 AWS Marketplace 權限

如果您的 IAM 主體在嘗試啟用時沒有必要的 AWS Marketplace 訂閱權限 ROSA，就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 受管政策附加ROSAManageSubscription到您的 IAM 身分。如需詳細資訊，請參閱《AWS 受管理原則參考指南》ManageSubscription中的 ROSA。
2. 遵循步驟 1：啟用 ROSA 並設定要啟用的必要條件中的程序 ROSA。

如果您沒有檢視或更新中權限集的權限， IAM 或者收到錯誤訊息，則必須聯絡系統管理員以尋求協助。要求該人員附加ROSAManageSubscription至您的 IAM 身分，並遵循步驟 1：啟用 ROSA 並設定必要條件中的程序。當管理員執行此動作時，它會透 ROSA 過更新中所有 IAM 身分識別的權限集來啟用 AWS 帳戶。

系統管理員封鎖的必要 AWS Marketplace 權限

如果您的帳戶管理員封鎖了必要的 AWS Marketplace 訂閱權限，當您嘗試啟用時，就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，則必須聯絡您的系統管理員以尋求協助。要求該人執行下列動作：

1. 前往ROSA 主控台並將 AWS 受管政策附加ROSAManageSubscription到您的 IAM 身分。如需詳細資訊，請參閱《AWS 受管理原則參考指南》ManageSubscription中的 ROSA。
2. 遵循步驟 1：啟用 ROSA 並設定要啟用的必要條件中的程序 ROSA。此程序可透 ROSA 過更新中所有 IAM 身分識別的權限集來啟用 AWS 帳戶。

建立負載平衡器時出錯： AccessDenied

如果您尚未建立負載平衡器，則AWSServiceRoleForElasticLoadBalacing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 ROSA 叢集 沒有該角色的AWSServiceRoleForElasticLoadBalacing角色，就會發生下列錯誤：

```
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該AWSServiceRoleForElasticLoadBalancing角色。

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

2. 如果您沒有此角色，請依照使用者指南中的「建立服務連結角色」中的 Elastic Load Balancing 指示建立角色。

韌性 ROSA

AWS 全球基礎設施韌

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分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的網路進行連接。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 為客戶提供在單一可用區域或跨多個 AWS 可用區域執行 Kubernetes 控制平面和資料平面的選項。雖然單一可用區叢集對於實驗很有用，但建議客戶在多個可用區域中執行工作負載。這確保了應用程序甚至可以承受完整的可用區域故障-本身是一個非常罕見的事件。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

ROSA 叢集彈性

ROSA 控制平面至少由三個 OpenShift 控制平面節點組成。每個控制平面節點都是由 API 伺服器執行個體、執行個etcd體和控制器所組成。如果控制平面節點故障，所有 API 請求都會自動路由到其他可用節點，以確保叢集可用性。

ROSA 資料平面至少由兩個 OpenShift 基礎結構節點和兩個 OpenShift 工作者節點組成。基礎結構節點會執行支援 OpenShift 叢集基礎結構元件的網繭，例如預設路由器、內建 OpenShift 登錄，以及用於叢集度量和監視的元件。 OpenShift 工作者節點會執行使用者應用程式

Red Hat 網站可靠性工程師 (SRE) 可全面管理控制平面和基礎架構節點。Red Hat SRE 會主動監控 ROSA 叢集，並負責更換任何故障的控制平面節點和基礎架構節點。如需詳細資訊，請參閱的職責概觀 ROSA。

> **Important**
>
> 因為這 ROSA 是一項受管理的服務，Red Hat 負責管理所 ROSA 使用的基 AWS 礎架構。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。

如果工作者節點在資料平面上發生故障，控制平面會將未排定的網繭重新定位到運作中的 Worker 節點，直到復原或取代失敗的節點為止。透過啟用叢集中的機器自動調整規模，可以手動或自動取代失敗的 Worker 節點。如需詳細資訊，請參閱 Red Hat 文件中的叢集自動調度資源。

客戶部署的應用程式

雖然 ROSA 提供許多保護來確保服務的高可用性，但客戶還是有責任建置其部署的應用程式，以取得高可用性，以保護工作負載免於停機時間。如需詳細資訊，請參閱 Red Hat 文件 ROSA中的關於可用性。

基礎結構安全 ROSA

作為託管服務， Red Hat OpenShift Service on AWS 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全支柱中的基礎結構保護 — AWS Well-Architected 的架構。

您可以使用 AWS 已發佈的 API 呼叫透 ROSA 過 AWS 網路進行存取。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 (SRE) 負責管理叢集與基礎應用程式平台的持續管理與網路安全。如需有關 Red Hat 職責的詳細資訊 ROSA，請參閱的責任概觀 ROSA。

當您建立新叢集時， ROSA 提供建立公用 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。此連線可用來與叢集通訊 (使用 OpenShift 管理工具，例如 ROSA CLI 和 OpenShift CLI)。私有連接允許節點和 API 服務器之間的所有通信保留在 VPC 中。如果您啟用 API 伺服器和應用程式路由的私人存取，則必須使用現有的 VPC 並 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) 的組合來保護。如需有關 Kubernetes RBAC 的詳細資訊，請參閱 Kubernetes 說明文件中的使用 RB AC 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 VPC 中建立 ROSA 叢集，請指定要使用的 VPC 子網路和可用區域。您也可以定義要使用的叢集網路的 CIDR 範圍，並將這些 CIDR 範圍與 VPC 子網路相符。如需詳細資訊，請參閱 Red Hat 文件中的 CIDR 範圍定義。

對於使用公用 API 端點的叢集， ROSA 需要針對您要將叢集部署到的每個可用區域，為您的 VPC 設定公用和私有子網路。對於使用私有 API 端點的叢集，只需要私有子網路。

如果您使用現有的 VPC，則可以將叢集設定 ROSA 為在建立叢集期間或之後使用 HTTP 或 HTTPS Proxy 伺服器來加密叢集 Web 流量，從而為資料增加另一層安全性。當您啟用 Proxy 時，會拒絕核心叢集元件直接存取網際網路。Proxy 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 說明文件中的設定叢集範圍的代理伺服器。

網繭網路隔離

如果您是叢集管理員，則可以在網繭層級定義網路原則，以限制 ROSA 叢集中網繭的流量。如需詳細資訊，請參閱 Red Hat 文件中的網路政策。

ROSA Service Quotas

Red Hat OpenShift Service on AWS(ROSA) 使用、() Amazon EC2、Amazon Virtual Private Cloud (Amazon VPC) 和 Amazon Elastic Block Store Elastic Load Balancing (ELBAmazon EBS) 的服務配額來佈建叢集。

所需的最低配額 ROSA

對於下列Amazon EBS配額Amazon EC2和配額，ROSA需要比預設服務提供的配額更高。若要使用ROSA，您可能需對這些配額請求提高配額。如需詳細資訊，請參閱《Service Quotas使用者指南》中的請求提高配額。

Important

對於隨需的標準 (A、C、D、H、I、M、R、T、Z) Amazon EC2 執行個體不足以建立ROSA叢集。 ROSA叢集建立需要 100 個或更高的 vCPUs。若要增加此配額，請開啟Service Quotas主控台並要求增加配額。

Note

您可以使用 SDK 檢查配額，但 SDK 計算不包括現有ROSA資源。AWSSDK 中的配額檢查可能會通過，且ROSA叢集建立可能會失敗。若要修正此問題，請開啟Service Quotas主控台並要求提高配額。

名稱	服務代碼	預設	最低要求	可調整	Description (描述)
執行中隨需的標準 (A、C、D、H、I、M、R、T、Z) 執行個體	ec2	5	100	是	指派給執行中隨需的標準 (A、C、D、H、I、M、R、T、Z) 執行個體。 5 個 vCPUs 的預設值不足

名稱	服務代碼	預設	最低要求	可調整	Description (描述)
					以建立ROSA叢集。 ROSA需要 100 個 vCPUs 才能建立叢集。
適用於一般用途 SSD (gp3) 磁碟區的儲存 (TiB)	ebs	50	300	是	可在此區域的一般用途 SSD (gp3) 磁碟區佈建的最大彙總儲存容量 (TiB)。 需要 300 TiB 的儲存裝置才能達到最佳效能。
gp2 磁碟區的儲存 (TiB) 磁碟區	ebs	50	300	是	此區域中可在一般用途 SSD (gp2) 磁碟區佈建的最大彙總儲存容量 (TiB)。 需要 300 TiB 的儲存裝置才能達到最佳效能。

名稱	服務代碼	預設	最低要求	可調整	Description (描述)
io1 磁碟區的儲存 (TiB) 佈建 IOPS SSD (io1) 磁碟區	ebs	50	300	是	可在此區域中佈建的 IOPS SSD (io1) 磁碟區之間佈建的最大彙總儲存容量 (TiB)。 需要 300 TiB 的儲存裝置才能達到最佳效能。

> **Note**
>
> 預設值是由 AWS 設定的初始配額，與實際套用的配額值和可能的服務配額上限不同。如需詳細資訊，請參閱《使用指南》Service Quotas中的Service Quotas〈術語〉。

的預設配額 ROSA

ROSA使用Amazon EC2、Amazon VPC、和的下列預設配額Elastic Load Balancing。Amazon EBS如需增加配額的相關資訊，請參閱Service Quotas使用者指南中的要求增加配額。

Amazon EC2

- EC2-VPC 彈性 IP

Amazon VPC

- 每個區域的 VPC 數
- 每個區域的網路介面
- 每個區域的 Internet 閘道數

Amazon EBS

- 每個區域的快照

- io1 磁碟區適用於佈建 IOPS SSD (io1) 磁碟區

Elastic Load Balancing

- Application Load Balancers每個地區
- Classic Load Balancers每個地區

與 ROSA 整合的 AWS 服務

ROSA與其他AWS 服務公司合作，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 ROSA 用來執行任務的服務。

主題

- 如何 ROSA 使用 AWS Marketplace

如何 ROSA 使用 AWS Marketplace

AWS Marketplace 是精心策劃的數位目錄，您可以使用它來尋找、購買、部署和管理建置解決方案和經營業務所需的第三方軟體、資料和服務。 AWS Marketplace 透過彈性的定價選項和多種部署方式，簡化軟體授權和採購。

ROSA 用 AWS Marketplace 於服務計量和計費。ROSA 經典版是透過 AWS Marketplace Amazon 機器映像 (AMI) 產品計量和計費，而含託管控制平面 (HCP) 的 ROSA 則是透過 AWS Marketplace 軟體即服務 (SaaS) 產品計量和計費。

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

術語

此頁面在討論 ROSA 與之整合時使用下列術語 AWS Marketplace。

Amazon Machine Image (AMI)

伺服器的影像，包括作業系統和其他軟體，在上執行 AWS。

AMI 訂閱

在中 AWS Marketplace，基於 AMI 的軟件產品（例如 ROSA 經典）使用每小時的年度訂閱定價模式。每小時定價是預設定價模式，但您可以選擇預先為一種 Amazon EC2 執行個體類型購買一年的用量。

SaaS 訂閱

在中 AWS Marketplace， software-as-a-service （SaaS）產品（例如 ROSA 與 HCP）採用基於使用量的訂閱模式。軟件銷售商會跟踪您的使用情況，您只需為您使用的內容付費。

公開發售

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

私人優惠

私人優惠是一種購買計劃，允許賣家和買家協商自定義價格和最終用戶許可協議（EULA）條款，以便在中 AWS Marketplace進行購買。

ROSA 服務費

Red Hat 網站可靠性工程師 (SRE) 對 OpenShift 軟體和叢集管理所 ROSA 收取的費用。 ROSA 服務費用通過計量 AWS Marketplace 並顯示在您的帳 AWS 單上。

AWS 基礎設施費

針對 AWS 服務 基礎 ROSA 叢集 AWS 收費的標準費用 Amazon EC2，包括 Amazon EBS Amazon S3、、和 Elastic Load Balancing。費用是通過使用中計算 AWS 服務 的，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 ROSA 服務費的計量和計費。 ROSA 服務費用包括 Red Hat 網站可靠性工程師 (SRE) 存取 OpenShift 軟體和叢集管理。 ROSA 所有支援的 AWS 標準區域的服務費用均一致。根據預設，根據這些叢集中執行的叢集和工作者節點 vCPUs 數目，ROSA 與 HCP 服務費用依預設會以固定的小時費率計算。ROSA 傳統服務費用會根據工作者節點 vCPUs 數量的需求計算。ROSA 典型不會針對控制平面或所需基礎結構節點收取服務費用。

ROSA 客戶也會為 AWS 服務 基 AWS 礎 ROSA 叢集支付標準基礎架構費用 Amazon EC2 Amazon EBS，包括 Amazon S3、和 Elastic Load Balancing。 AWS 基礎設施費用與通 AWS Marketplace過計量的 ROSA 服務費用是單獨的計費項目。 AWS 基礎架構費用依預設 AWS 區域 而有所不同，並以每小時使用量為基礎。為了節省額外的 AWS 基礎架構成本，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 Plan s 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 控制台中查看 ROSA 服務費和 AWS 基礎設施費用並管理付款。您還可以使用 AWS Cost Explorer Service 界面免費查看成本並監控使用情況。如需詳細資訊，請參閱《 AWS Billing

and Cost Management 使用指南》中的「檢視帳單」和「 AWS 成本管理系統使用者指南」 AWS Cost Explorer Service中的「分析成本」。

透過主控台訂閱 ROSA Marketplace 清單

當您在ROSA 主控台 ROSA中啟用時，您 AWS 帳戶 已訂閱 ROSA 經典版和 ROSA，並且已開啟 HCP 清單。 AWS Marketplace啟用 ROSA 訂閱不收取任何費用。

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 購買指南》中的「在組織中共用訂閱」。

ROSA 合同

ROSA 用 AWS Marketplace 於為 ROSA 與 HCP 和 ROSA 經典版提供可選合同。合同可節省 ROSA 工作人員節點服務費。 ROSA 合同不影響 AWS 基礎設施收取的費用。

12 個月合約

您可以透過主控台透過 HCP 購買為期 12 個月的 ROSA 經典版和 ROSA 公開發售合約。 ROSA

> **Note**
>
> 您必須先在您的帳戶啟用 ROSA 傳統版，才能從主機購買 12 個月的合約。

> **Note**
>
> 12 個月的合約不能轉移至私人優惠。

購買 ROSA 經典 12 個月合約

當您購買 ROSA 經典 12 個月合約時，您需要支付年期預付款，並針對承保的執行個體在接下來的 12 個月內無需支付小時服務費。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目而定。該合同不包括對所使用的基 AWS 礎設施 ROSA 收取 AWS 服務 的基礎設施費用。如需詳細資訊，請參閱 Red Hat OpenShift Service on AWS 定價。

合約僅涵蓋您在合約建立期間指定的執行個體類型 (例如 m5.xlarge)。您可以購買額外 12 個月的合約，以節省多個 Amazon EC2 執行個體類型的成本。在 12 個月合約以外的使用量會產生隨需費率的 ROSA 服務費用。

> **Note**
>
> ROSA 經典 12 個月合約不會 auto 續約。

購買為期 12 個月的 ROSA 經典版合約

> **Note**
>
> 如果您在尚未支援 HCP 的 ROSA 的區域中使用 ROSA 主控台，則此工作流程尚不可用。如需支援 ROSA 與 HCP 的區域清單，請參閱 ROSA 與 HCP 和 ROSA 經典版之間的差異。
> 若要在沒有提供 HCP 支援的 ROSA 區域購買 ROSA 傳統合約，請前往ROSA 主控台並選擇 [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. 為 ROSA 經典選擇合約。
4. 選擇「購買合約」。
5. 選取所需的 EC2 執行個體類型和執行個體數量。
6. 選擇「複查合約」。
7. 檢閱合約明細，然後選擇「購買合約」。

> **Note**
>
> ROSA 使用主控台建立後，12 個月的合約將無法降級或取消。如果您需要在有效合約期間內降級或取消合約，請前往AWS Support 中心並開啟支援案例。

向醫護機構購買 ROSA 12 個月合約

當您在主控台中透過 HCP 啟用 ROSA 時，最初會在您的帳戶上建立免費的 12 個月 ROSA 與 HCP 合約，以方便隨需計費。如果您選擇購買含 HCP 的 ROSA 合約以節省工作者節點服務費用，則會修改初始合約，以涵蓋您指定的工作者節點 vCPUs 和控制平面的使用成本。

當您透過 HCP 12 個月購買 ROSA 合約時，您需要支付年期的預付款項，並針對涵蓋的工作者節點 vCPUs 和控制平面支付未來 12 個月的小時使用費。合約成本是根據您選取的背景工作節點 vCPUs 和

控制平面的數目而定。合約僅涵蓋您在合約建立期間指定的工作節點 vCPUs 和控制平面。該合同不包括對所使用的基 AWS 礎設施 ROSA 收取 AWS 服務 的基礎設施費用。如需詳細資訊，請參閱 Red Hat OpenShift Service on AWS 定價。

每月使用配額

購買後，您的預付 vCPUs 和控制平面會轉換為每月用量配額。每小時隨需使用率適用於超過每月配額的 vCPU 和控制平面使用量。ROSA 與醫護機構使用以下公式來計算與合約相關的每月配額：

- 工作者節點 vCPUs 數量：vCPUs 數量 x 24 小時 x 365 天/12 個月
- 控制飛機：控制飛機數量 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 個控制平面時，可轉換成每月 2,920,000 個工作者節點 vCPU 小時的配額，以及每月可消耗 5,840 小時的控制平面小時。

向醫護機構購買 ROSA 12 個月合約

> **Note**
>
> 如果您使用的區域中的 Red Hat OpenShift Service on AWS 主控台尚未透過託管控制平面支援 ROSA，則此工作流程尚不可用。如需支援 ROSA 與 HCP 的區域清單，請參閱 ROSA 與 HCP 和 ROSA 經典版之間的差異。

1. 前往 ROSA 主控台。
2. 在左側導覽窗格中，選擇 [合約]。
3. 選擇與醫護機構合作的 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「複查合約」。
8. 檢閱合約明細，然後選擇「購買合約」。

> **Note**
>
> ROSA 使用主控台建立後，12 個月的合約將無法降級或取消。如果您需要在有效合約期間內降級或取消合約，請前往AWS Support 中心並開啟支援案例。

透過醫護機構升級 ROSA 12 個月合約

您可以使用額外的工作者節點 vCPUs 和控制平面，隨時透過 HCP 12 個月合約升級作用中的 ROSA。當您透過 HCP 12 個月的合約升級 ROSA 時，您需要為增加的資源支付預付款。按比例分攤的金額是根據合約剩餘天數來計算。合約僅涵蓋您在合約建立期間指定的工作節點 vCPUs 和控制平面。合約升級不會影響 AWS 基礎設施收取的費用。

升級後，新增的 vCPUs 和控制平面會使用與原始合約購買相同的公式，轉換為每月使用配額。每小時隨需使用率適用於超過每月配額的 vCPU 和控制平面使用量。如需詳細資訊，請參閱每月使用量配額。

向醫護機構升級 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. 選擇與醫護機構合作的 ROSA 合約。
4. 選擇 Upgrade (升級)。
5. 輸入要新增的 vCPUs 數目。以 4 的倍數指定。
6. 輸入要加入至合約的控制平面數目。
7. 選擇 [檢閱升級]。
8. 檢閱合約詳細資料並選擇 [購買升級]。

> **Note**
>
> ROSA 12 個月經典版合約無法升級。您可以隨時使用 ROSA 主控台購買額外 12 個月的 ROSA 經典合約。

獲得私人報價

您可以要求 ROSA 與 HCP 或 ROSA 經典版相關的 AWS Marketplace 私人優惠，以獲得與 Red Hat 協商的產品定價和終端使用者授權合約 (EULA) 條款。如需更多資訊，請參閱「AWS Marketplace 買家指南」中的「私人優惠」。

要獲得 ROSA 私人報價

> **Note**
>
> 如果您是 AWS Organizations 使用者，且收到已發給付款人和成員帳戶的私人優惠，請依照下列程序 ROSA 直接訂閱組織中的每個帳戶。
> 如果您收到僅發放給 AWS Organizations 付款人帳戶的 ROSA 傳統私人優惠，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 購買指南》中的「在組織中共用訂閱」。

1. 一旦發出私人優惠，請登入主AWS Marketplace 控台。
2. 開啟含有 ROSA 私人優惠連結的電子郵件。
3. 點擊鏈接直接訪問私人報價。

> **Note**
>
> 在登錄到正確的帳戶之前按照此鏈接將導致發現頁面註釋（404）錯誤。

4. 查看條款和條件。
5. 選擇「接受條款」。

> **Note**
>
> 如果不接受 AWS Marketplace 私人優惠，則起的 ROSA 服務費用 AWS Marketplace 將繼續按每小時公開費率計費。

6. 若要驗證優惠詳細資料，請選取 [在產品清單中顯示詳細資料]。
7. 若要開始使用 ROSA，請選擇 [繼續設定]。您將被重定向到控 ROSA 制台。

私人 Marketplace

私人 Marketplace 可讓管理員建立已核准產品的自訂數位目錄 AWS Marketplace。管理員可以 AWS Marketplace 針對 AWS 組織單位或其組織 AWS 帳戶 內的其他單位建立一組獨特的經過審核的軟體集合，供其購買。

如果您的組織使用私人市集，系統管理員必須先將的 AWS Marketplace 清單新增 ROSA 至私人市集，使用者才能啟用服務。如需詳細資訊，請參閱 AWS Marketplace 購買指南中的私人市集入門。

故障診斷

下列文件說明如何疑難排解啟用 ROSA 和佈建 ROSA 叢集時可能發生的問題。

主題

Support ROSA

您可以使用 ROSA Red Hat 支援團隊獲得疑難排解支援。 AWS Support 您可以向任何一個組織開啟 Support 案例，並轉送至正確的團隊以解決您的問題。

AWS Support

開啟 ROSA 技術案例需要開 AWS 發人員 Support 計劃，但建議您使用 AWS 商業或企業隨機 Support 方案，才能持續存取 ROSA 技術支援和架構指引。在必要時，Red Hat 會使用 AWS Support API 為客戶開啟案例。 AWS 商業 Support 和 AWS 企業上網服務可讓支援工程師持續存取電話、網路和聊天。如需 AWS Support 計劃的詳細資訊，請參閱AWS Support。

如需啟用 AWS Support 方案的步驟，請參閱如何註冊方 AWS Support 案？

AWS Support 如需建立案例的相關資訊，請參閱建立支援案例和案例管理。

紅帽 Support

ROSA 包括紅帽高級 Support。若要獲得 Red Hat 進階 Support，請瀏覽至 Red Hat 客戶入口網站，並使用支援案例工具建立支援票證。如需詳細資訊，請參閱如何使用 Red Hat 支援服務。

排解 ROSA 叢集建立問題

本節包含建立 ROSA 叢集時可能遇到的問題的解決方案。

您也可以透 ROSA過 Red Hat 支援團隊獲得疑難排解支援。 AWS Support 如需詳細資訊，請參 S upport ROSA。

主題

存取 ROSA 叢集偵錯記錄

若要開始疑難排解應用程式的問題，請先檢閱偵錯記錄檔。 ROSA CLI 偵錯記錄檔會提供建立 叢集 失敗時所產生的錯誤訊息的詳細資料。

若要顯示 叢集 偵錯資訊，請執行下列 ROSA CLI 命令。在命令中，<cluster_name>替換為您的 叢集.

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

ROSA 叢集在 叢集 建立期間無法檢查 AWS 服務配額

描述

若要使用 ROSA，您帳戶的服務配額可能需要增加。如需更多相關資訊，請參閱 ROSA Service Quotas。

解決方案

1. 執行下列命令以識別您帳戶的配額。

```
rosa verify quota
```

> **Note**
>
> 配額是不同的 AWS 區域。請務必確認您區域的每個配額。

2. 如果您需要增加配額，請瀏覽至主Service Quotas 控台。
3. 在功能窗格中，選擇 [AWS 服務]。
4. 選擇需要增加配額的服務。
5. 選取需要增加的配額，然後選擇 [要求增加配額]。

6. 在 [要求增加配額] 中，輸入您希望配額設為的總金額，然後選擇 [要求]。

疑難排解 ROSA CLI 過期離線存取權杖

描述

如果您使用 ROSA CLI 且您的 api.openshift.com 離線存取權杖過期，則會出現錯誤訊息。當 sso.redhat.com 使令牌無效時會發生這種情況。

解決方案

1. 瀏覽至「OpenShift 叢集管理員 API 權杖」頁面，然後選擇「載入權杖」。
2. 在終端中複製並粘貼以下身份驗證命令。

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

疑難排解非 STSROSA 叢集問題

本節說明如何疑難排解佈建非 STSROSA 叢集時可能遇到的問題。

建議您使用AWS Security Token Service (STS) 短期登入資料佈建ROSA叢集，以獲得更好的安全性保護。如需佈建ROSA STS 叢集的相關資訊，請參閱AWS STS在 auto 模式下開始ROSA使用。

您也可以透ROSA過 Red Hat 支援團隊獲得疑難排解支援。AWS Support如需詳細資訊，請參 SupportROSA。

無法創建一叢集個錯 osdCcsAdmin 誤

> **Note**
>
> 只有當您使用佈建ROSA叢集的非 STS 方法時，才會發生此錯誤。若要避免此問題，請ROSA使用AWS STS. 如需詳細資訊，請參閱AWS STS在ROSA自 auto 模式中。

描述

如叢集果不建立，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.
```

解決方案

1. 刪除堆疊

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

2. 重新初始化您的帳戶

```
rosa init
```

ROSA 使用者指南的文件歷史記錄

下表涵蓋的所有文件更新 ROSA。

變更	描述	日期
ROSA 與 HCP 擴 AWS 區域展	含託管控制平面 (HCP) 的 ROSA 現已在中東 (阿拉伯聯合大公國) AWS 區域推出。	2024年5月13日
ROSA 與 HCP 擴 AWS 區域展	ROSA 與託管控制平面 (HCP) 現已在歐洲 (巴黎) AWS 區域推出。	2024年5月6日
更新羅莎 NodePoolManagementPolicy	更新了 AWS 受管政策羅莎NodePoolManagementPolicy。	2024年5月2日
ROSA 與 HCP 擴 AWS 區域展	含託管控制平面 (HCP) 的 ROSA 現已在歐洲 (西班牙) AWS 區域推出。	2024年4月29 日
更新羅莎 InstallerPolicy	更新了 AWS 受管政策羅莎InstallerPolicy。	2024年4月24日
ROSA 與 HCP 擴 AWS 區域展	含託管控制平面 (HCP) 的 ROSA 現已在歐洲 (蘇黎世) AWS 區域推出。	2024年4月19 日
ROSA 與 HCP 擴 AWS 區域展	含託管控制平面 (HCP) 的 ROSA 現已在亞太區域 (大阪) AWS 區域推出。	2024年4月17日
更新羅莎InstallerPolicy 和羅薩爾 SupportPolicy	更新了 AWS 受管政策羅莎InstallerPolicy 和羅薩斯SupportPolicy。	2024年4月10日

ROSA 與 HCP 擴 AWS 區域展	ROSA 與託管控制平面（HCP）現已在亞太地區（香港）AWS 區域上市。	2024年4月8日
ROSA 與 HCP 擴 AWS 區域展	含託管控制平面 (HCP) 的 ROSA 現已在南美洲 (聖保羅) AWS 區域推出。	2024年4月1日
ROSA 與 HCP 擴 AWS 區域展	含託管控制平面 (HCP) 的 ROSA 現已在中東 (巴林) AWS 區域推出。	2024年3月25日
ROSA 與 HCP 擴 AWS 區域展	含託管控制平面 (HCP) 的 ROSA 現已在亞太區域 (首爾) AWS 區域推出。	2024年3月14日
ROSA 與 HCP 擴 AWS 區域展	含託管控制平面 (HCP) 的 ROSA 現已在非洲 (開普敦) AWS 區域推出。	2024年3月5日
更新羅莎 InstallerPolicy	更新了 AWS 受管政策羅莎InstallerPolicy。	2024年1月26日
更新羅薩瑞 SupportPolicy	更新了 AWS 受管政策 SupportPolicy	2024年1月22日
更新羅莎 ImageRegistryOperatorPolicy	更新了 AWS 受管政策羅莎ImageRegistryOperatorPolicy。	2023 年 12 月 12 日
更新羅莎 KubeControllerPolicy	更新了 AWS 受管政策羅莎KubeControllerPolicy。	2023 年 10 月 16 日
更新羅莎 ManageSubscription	更新了 AWS 受管政策羅莎 ManageSubscription。	2023 年 8 月 1 日
更新羅莎 KubeControllerPolicy	更新了 AWS 受管政策羅莎KubeControllerPolicy。	2023 年 7 月 13 日

新增羅莎安全頁面	新增 ROSA 的彈性、ROSA 中的基礎架構安全性，以及 ROSA 頁面中的資料保護。	2023 年 6 月 30 日
添加了部署選項頁面	添加了部署選項頁面。	2023 年 6 月 9 日
添加了新的 AWS 受管政策 ROSA NodePoolManagement Policy	已新增 AWS 受管政策 ROSA NodePoolManagement Policy 。	2023 年 6 月 8 日
添加了新的 AWS 受管政策 ROSA InstallerPolicy	已新增 AWS 受管政策 ROSA InstallerPolicy 。	2023 年 6 月 6 日
增加了新的 AWS 受管政策 SupportPolicy	新增SupportPolicy 了新的 AWS 受管政策。	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
更新了什麼是 AWS 上的紅帽 OpenShift 服務？	更新了 AWS 上的「什麼是 Red Hat OpenShift 服務」頁面。	2023 年 5 月 24 日
為 ROSA 操作員角色新增 AWS 受管政策	新增ProviderPolicy 了新的 AWS 受管政策羅莎ImageRegistryOperatorPolicyKubeControllerPolicy、羅莎和羅薩克姆。	2023 年 4 月 27 日
添加了新的 AWS 受管政策 ROSA ControlPlaneOperatorPolicy	已新增 AWS 受管政策 ROSA ControlPlaneOperatorPolicy 。	2023 年 4 月 24 日
針對 ROSA 帳戶角色新增 AWS 受管政策	已新增 ROSA 帳戶和操作員角色頁面的 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
新增疑難排解頁	已新增疑難排解頁面。	2022 年 11 月 1 日

新增入門頁面	新增入門頁面。	2022 年 8 月 12 日
添加了新的 AWS 受管政策 ROSA ManageSubscription	已新增 AWS 受管政策 ROSA ManageSubscription 。	2022 年 4 月 11 日
初始版本	AWS 使用者指南上的 Red Hat OpenShift 服務初始發行版本。	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。