瞭解基礎知識
Setup and administration

NetApp
February 20, 2026

目錄

瞭解基礎知識

了解NetApp Workload Factory

NetApp Workload Factory 是一個強大的生命週期管理平台，旨在幫助您使用Amazon FSx for NetApp ONTAP檔案系統優化工作負載。可以使用 Workload Factory 和 FSx for ONTAP簡化的工作負載包括資料庫、VMware 遷移到 VMware Cloud on AWS、AI 聊天機器人等。

工作負載是指資源、程式碼、服務或應用程式的組合，旨在服務業務目標。這可以是任何內容，從面向客戶的應用程式到後端流程。工作負載可能涉及單一 AWS 帳戶中的部分資源，也可能跨越多個帳戶。

Amazon FSx for NetApp ONTAP為關鍵任務應用程式、資料庫、容器、VMware Cloud 資料儲存和使用者檔案提供完全託管的 AWS 原生 NFS、SMB/CIFS 和 iSCSI 儲存磁碟區。您可以透過 Workload Factory 和使用原生 AWS 管理工具來管理 FSx for ONTAP 。

功能

Workload Factory平台提供以下主要功能。

靈活且低成本的儲存設備

探索、部署及管理適用於雲端 NetApp ONTAP 檔案系統的 Amazon FSX 。適用於 ONTAP 的 FSX 將 ONTAP 的完整功能帶給原生 AWS 託管服務、提供一致的混合雲體驗。

將內部部署 **vSphere** 環境移轉至 **AWS** 上的 **VMware Cloud**

VMware Cloud on AWS 移轉顧問可讓您分析內部部署 vSphere 環境中目前的虛擬機器組態、產生將建議的 VM 配置部署至 AWS 上的 VMware Cloud 的計畫、並將 NetApp ONTAP 檔案系統的自訂 Amazon FSX 做為外部資料存放區。

資料庫生命週期管理

利用 Amazon FSX for NetApp ONTAP 探索資料庫工作負載並分析成本節約效益；將 SQL Server 資料庫移轉至適用於 ONTAP 儲存設備的 FSX 時，善用儲存與應用程式的效益；部署 SQL 伺服器，資料庫及資料庫複本以實作廠商最佳實務做法；使用基礎架構做為程式碼聯合試驗以自動化作業；持續監控及最佳化 SQL 伺服器環境，以改善效能，可用度，保護及成本效益。

AI chatbot 開發

利用您的 FSX for ONTAP 檔案系統來儲存組織的 chatbot 來源和 AI Engine 資料庫。這可讓您將組織的非結構化資料內嵌到企業級聊天機器人應用程式中。

節省計算機以節省成本

分析您目前使用 Amazon Elastic Block Store （ EBS ）或 Elastic File System （ EFS ）儲存設備或 Amazon FSX for Windows File Server 的部署、瞭解移轉至 Amazon FSX for NetApp ONTAP 可節省多少成本。您也可以使用計算機來執行「假設」案例、以供您規劃未來的部署作業使用。

服務帳戶可促進自動化

使用服務帳戶安全可靠地自動化NetApp Workload Factory 操作。服務帳戶提供可靠、持久的自動化，不受任何用戶管理限制，並且由於它們僅提供 API 訪問，因此更加安全。

問我人工智慧助手

向 AI 助理詢問有關管理和操作 FSx for ONTAP檔案系統的問題。使用模型上下文協定 (MCP)，Ask Me 可以安全地與外部環境互動並查詢 API 工具，以提供適合您特定儲存環境的回應。

支援的雲端供應商

Workload Factory 可讓您管理雲端儲存並使用 Amazon Web Services 中的工作負載功能。

安全性

NetApp Workload Factory的安全性是NetApp的首要任務。Workload Factory 中的所有工作負載均運作在Amazon FSx for NetApp ONTAP之上。除此之外，還有所有 "AWS 安全功能"NetApp Workload Factory已收到 "SOC2 Type 1 合規性、SOC2 Type 2 合規性和 HIPAA 合規性"。

Amazon FSx for NetApp ONTAP for NetApp Workload Factory 是一款"用於部署企業應用程式的 AWS 解決方案"它是在充分考慮了架構良好的最佳實踐的基礎上創建的。

成本

Workload Factory 可以免費使用。您向 Amazon Web Services (AWS) 支付的費用取決於您計劃部署的儲存和工作負載服務。這包括Amazon FSx for NetApp ONTAP 、AWS 基礎架構上的 VMware Cloud、AWS 服務等的成本。

工作負載工廠的工作原理

Workload Factory 包括透過 SaaS 層提供的基於 Web 的控制台、帳戶、控制對雲端資產的存取的操作模式、提供 Workload Factory 和 AWS 帳戶之間隔離連接的連結等。

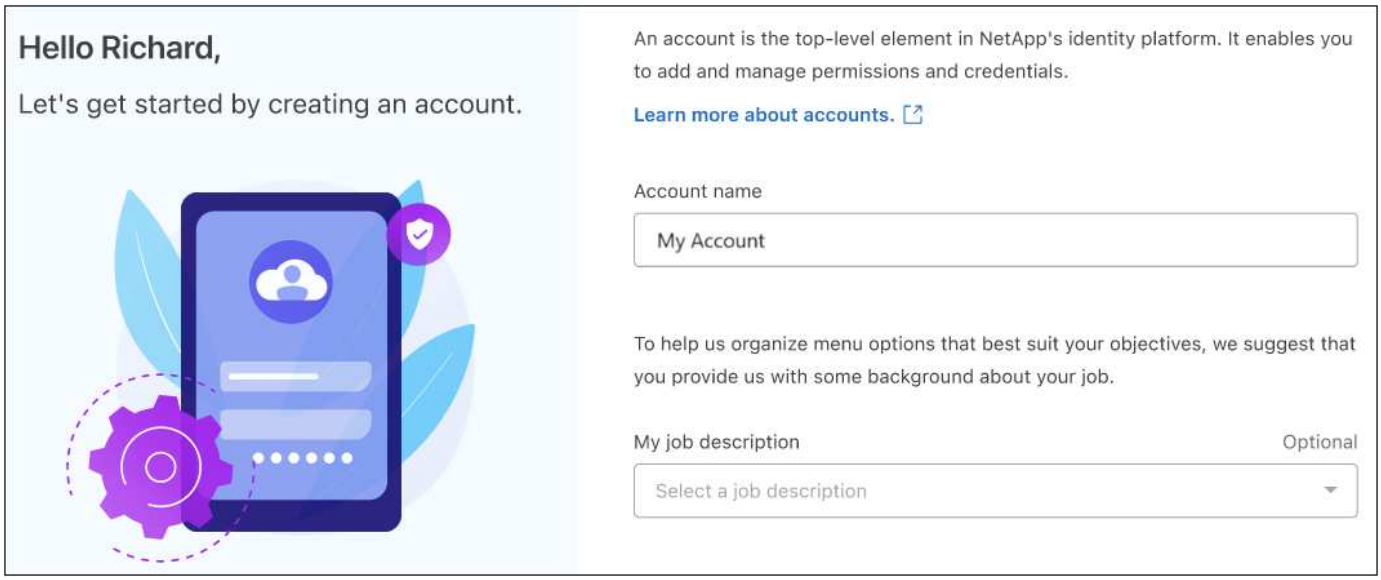
軟體即服務

可透過以下方式存取 Workload Factory"NetApp Workload Factory 控制台"以及"NetApp控制台"。這些 SaaS 體驗使您能夠在最新功能發佈時自動存取它們，並輕鬆地在 Workload Factory 帳戶和連結之間切換。

"了解更多關於不同遊戲主機體驗的信息"

帳戶

當您第一次登入 Workload Factory 時，系統會提示您建立帳戶。此帳戶可讓您使用憑證為您的組織組織資源、工作負載和工作負載存取權限。



建立帳戶時，您是該帳戶的單一 *account admin* 使用者。

如果您的組織需要額外的帳戶或使用者管理、請使用產品內的聊天室與我們聯絡。

如果您使用NetApp控制台，那麼您已經屬於一個帳戶，因為 Workload Factory 利用NetApp帳戶。

服務帳戶

服務帳戶可作為“使用者”，可以對NetApp Workload Factory 進行授權 API 呼叫以實現自動化目的。這使得管理自動化變得更加容易，因為您不需要基於可以隨時離開公司的真實人員的使用者帳戶來建立自動化腳本。Workload Factory 中的所有帳戶持有者都被視為帳戶管理員。帳戶管理員可以建立和刪除多個服務帳戶。

"瞭解如何管理服務帳戶"

權限

Workload Factory 提供靈活的權限策略，使您能夠仔細控制對雲端環境的訪問，並根據您的 IT 策略為 Workload Factory 分配遞增的信任。

"了解更多關於工作負載工廠權限策略的信息"

連線連結

Workload Factory 連結在 Workload Factory 與一個或多個 FSx for ONTAP檔案系統之間建立信任關係和連線。這使您能夠直接從ONTAP REST API 呼叫監控和管理某些檔案系統功能，而這些功能無法透過Amazon FSx for ONTAP API 取得。

您不需要連結即可開始使用 Workload Factory，但在某些情況下，您需要建立連結來解鎖所有 Workload Factory 功能和工作負載能力。

連結目前使用 AWS Lambda 。

"深入瞭解連結"

CodeBox 自動化

Codebox 是一個基礎架構即代碼 (IaC) 副駕駛，可協助開發人員和 DevOps 工程師產生執行 Workload Factory 支援的任何操作所需的程式碼。程式碼格式包括 Workload Factory REST API、AWS CLI 和 AWS CloudFormation。

Codebox 與 Workload Factory 操作模式（*basic*、*read-only* 和 *read/write*）保持一致，並為執行準備設定了清晰的路徑以及自動化目錄，以便將來快速重複使用。

Codebox 窗格會顯示由特定工作流程作業所產生的 IAC 、並由圖形化精靈或交談式聊天介面進行比對。雖然 Codebox 支援色彩編碼、並可搜尋簡單的導覽和分析、但不允許編輯。您只能複製或儲存到自動化目錄。

"深入瞭解 CodeBox"

節省計算機

Workload Factory 提供節省計算器，以便您可以將儲存環境、資料庫或 VMware 工作負載在 FSx for ONTAP檔案系統上的成本與其他 Amazon 服務進行比較。根據您的儲存需求，您可能會發現 FSx for ONTAP檔案系統是最具成本效益的選擇。

- "瞭解如何探索儲存環境的節約效益"
- "瞭解如何探索資料庫工作負載的節約效益"
- "了解如何為您的 VMware 工作負載節省成本"

架構良好的工作負載

Workload Factory 可協助您維護和執行符合 AWS 良好架構框架的可靠、安全、高效且經濟的儲存和資料庫配置。Workload Factory 每天掃描 FSx 中的ONTAP檔案系統、SQL Server 和 Oracle 資料庫部署情況，以提供有關潛在錯誤配置的見解，並建議手動或自動操作來修復問題。

"了解更多關於架構良好的工作負載的信息"

使用NetApp Workload Factory 的工具

您可以將NetApp Workload Factory 與以下工具一起使用：

- **Workload Factory** 控制台：Workload Factory 控制台提供您的應用程式和專案的視覺化、整體視圖。
- * NetApp控制台*： NetApp控制台提供混合介面體驗，以便您可以將 Workload Factory 與其他NetApp資料服務一起使用。
- 問我：使用問我 AI 助理來提問並了解有關 Workload Factory 的更多信息，而無需離開 Workload Factory 控制台。從 Workload Factory 幫助選單中存取「問我」。
- **CloudShell CLI**：Workload Factory 包含 CloudShell CLI，可透過基於瀏覽器的單一 CLI 跨帳號管理和操作 AWS 和NetApp環境。從 Workload Factory 控制台頂部欄存取 CloudShell。
- **REST API**：使用 Workload Factory REST API 部署和管理您的 FSx for ONTAP檔案系統和其他 AWS 資源。
- **CloudFormation**：使用 AWS CloudFormation 程式碼執行您在 Workload Factory 控制台中定義的操作，以從您的 AWS 帳戶中的 CloudFormation 堆疊對 AWS 和第三方資源進行建模、配置和管理。
- **Terraform NetApp Workload Factory** 提供者：使用 Terraform 建置和管理在 Workload Factory 控制台中

產生的基礎架構工作流程。

REST API

Workload Factory 讓您能夠針對特定工作負載最佳化、自動化和操作 FSx for ONTAP檔案系統。每個工作負載都公開一個相關的 REST API。總的來說，這些工作負載和 API 構成了一個靈活且可擴展的開發平台，您可以使用它來管理 FSx for ONTAP檔案系統。

使用 Workload Factory REST API 有幾個好處：

- API 的設計是以 REST 技術和目前最佳實務為基礎。核心技術包括 HTTP 和 JSON 。
- Workload Factory 驗證是基於 OAuth2 標準。 NetApp依賴 Auth0 服務實作。
- Workload Factory 基於 Web 的控制台使用相同的核心 REST API，因此兩個存取路徑之間具有一致性。

"查看 Workload Factory REST API 文檔"

主控台體驗

NetApp Workload Factory 可透過兩個基於 Web 的控制台存取。了解如何使用 Workload Factory 控制台和NetApp控制台存取 Workload Factory。

- * NetApp控制台*：提供混合體驗，您可以在相同位置管理 FSx for ONTAP檔案系統和在Amazon FSx for NetApp ONTAP上執行的工作負載。
- **Workload Factory** 控制台：提供專用的 Workload Factory 體驗，專注於在Amazon FSx for NetApp ONTAP上執行的工作負載。

在NetApp控制台中存取 Workload Factory

您可以從NetApp Console存取 Workload Factory。除了使用 Workload Factory 來取得 AWS 儲存和工作負載功能外，您還可以存取其他資料服務，例如NetApp Copy and Sync等。

步驟

1. 登入"NetApp控制台"。
2. 從NetApp控制台選單中，選擇 **Workloads**，然後選擇 **Overview**。

在 Workload Factory 控制台中造訪 Workload Factory

您可以從 Workload Factory 控制台存取 Workload Factory。

步驟

1. 登入"工作負載工廠控制台"。

NetApp Workload Factory 的權限

若要使用NetApp Workload Factory 功能和服務，您需要提供權限，以便 Workload Factory 可以在您的雲端環境中執行操作。

為何要使用權限

當您提供權限時，Workload Factory 會將政策附加到實例，該策略具有管理該 AWS 帳戶中資源和進程的權限。這使得 Workload Factory 能夠執行各種操作，從發現您的儲存環境到部署 AWS 資源，例如儲存管理中的檔案系統或 GenAI 工作負載的知識庫。

例如，對於資料庫工作負載，當 Workload Factory 被授予所需的權限時，它會掃描給定帳戶和區域中的所有 EC2 實例，並過濾所有基於 Windows 的機器。如果主機上安裝並執行了 AWS Systems Manager (SSM) Agent，且 System Manager 網路配置正確，則 Workload Factory 可以存取 Windows 機器並驗證是否安裝了 SQL Server 軟體。

依工作負載的權限

每個工作負載都使用權限在工作負載工廠中執行特定任務。權限被打包成一系列權限策略。捲動到您使用的工作負載，了解權限策略、權限策略的可複製 JSON 以及列出所有權限、其用途、使用位置以及支援它們的權限策略的表格。

儲存設備的權限

儲存可用的 IAM 策略為 Workload Factory 提供了管理公有雲環境中的資源和進程所需的權限。

儲存功能提供以下權限策略供您選擇：

- 檢視、規劃與分析：檢視 FSx for ONTAP檔案系統，了解系統運作狀況，取得系統架構完善的分析，並探索節省成本的方法。
- 操作與修復：執行操作任務，例如調整檔案系統容量和修復檔案系統設定問題。
- 檔案系統建立和刪除：建立和刪除ONTAP檔案系統和儲存虛擬機器的 FSx。

查看所需的身分識別和存取管理 (IAM) 策略：

視圖、規劃與分析

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeSharedVpcConfiguration",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "ce:GetCostAndUsage",
        "ce:GetTags",
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

營運和補救

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateVolume",
        "fsx:DeleteVolume",
        "fsx:UpdateFileSystem",
```

```
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:DetachAndDeleteS3AccessPoint",
        "s3:CreateAccessPoint",
        "s3:DeleteAccessPoint",
        "s3:GetObjectTagging",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListInferenceProfiles",
        "bedrock:GetInferenceProfile",
        "s3tables:CreateTableBucket",
        "s3tables:ListTables",
        "s3tables:GetTable",
        "s3tables:GetTableMetadataLocation",
        "s3tables:CreateTable",
        "s3tables:GetNamespace",
        "s3tables:PutTableData",
        "s3tables:CreateNamespace",
        "s3tables:GetTableData",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:GetTableBucket",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:ListTagsForResource",
        "s3tables:TagResource",
        "s3:GetObjectTagging",
        "s3:ListBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

檔案系統的建立和刪除

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DeleteFileSystem",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:TagResource",
        "fsx:UntagResource",
        "kms:CreateGrant",
        "iam:CreateServiceLinkedRole",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumeStatus",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/AppCreator": "NetappFSxWF"
        }
      }
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

下表顯示儲存設備的權限。

儲存設備權限表

目的	行動	使用處	權限政策
為 ONTAP 檔案系統建立 FSX	fsx:CreateFileSystem	部署	檔案系統的建立和刪除
為 ONTAP 檔案系統的 FSX 建立安全群組	EC2：建立安全性群組	部署	檔案系統的建立和刪除
將標籤新增至適用於 ONTAP 檔案系統的 FSX 安全性群組	EC2：建立標記	部署	檔案系統的建立和刪除
授權 ONTAP 檔案系統的 FSX 安全性群組外傳和進入	EC2：授權安全性群組出口	部署	檔案系統的建立和刪除
	EC2：授權安全性群組入口	部署	檔案系統的建立和刪除
授與角色可在適用於 ONTAP 的 FSX 與其他 AWS 服務之間提供通訊	IAM ： CreateServiceLinkedIn 角色	部署	檔案系統的建立和刪除
取得詳細資料以填寫適用於 ONTAP 檔案系統部署的 FSX 表單	EC2：取消功能Vpcs	• 部署 • 探索節約效益	檔案系統的建立和刪除
	EC2：無資料子網路	• 部署 • 探索節約效益	檔案系統的建立和刪除
	EC2：取消安全性群組	• 部署 • 探索節約效益	檔案系統的建立和刪除
	EC2：取消功能表	• 部署 • 探索節約效益	檔案系統的建立和刪除
	EC2：網路介面	• 部署 • 探索節約效益	檔案系統的建立和刪除
	EC2 ： DescribeVolume 狀態	• 部署 • 探索節約效益	檔案系統的建立和刪除

目的	行動	使用處	權限政策
取得 KMS 金鑰詳細資料，並使用適用於 ONTAP 加密的 FSX	公里：建立授予	部署	檔案系統的建立和刪除
	KMS ： DescribeKey	部署	檔案系統的建立和刪除
	kms ： ListKeys	部署	檔案系統的建立和刪除
	kms：清單別名	部署	檔案系統的建立和刪除
取得 EC2 執行個體的 Volume 詳細資料	EC2：減量磁碟區	• 庫存 • 探索節約效益	視圖、規劃與分析
取得 EC2 執行個體的詳細資料	EC2：資料說明	探索節約效益	視圖、規劃與分析
在節約計算機中說明彈性檔案系統	Elasticfilesystem：描述檔案系統	探索節約效益	視圖、規劃與分析
列出適用於 ONTAP 資源的 FSX 標籤	FSX ： ListTagsForResource	庫存	視圖、規劃與分析
管理適用於 ONTAP 檔案系統的 FSX 的安全性群組外傳和進入	EC2：RevokeSecurity GroupIngress	管理作業	檔案系統的建立和刪除
	ec2：撤銷安全群組出口	管理作業	檔案系統的建立和刪除
	EC2：刪除安全性群組	管理作業	檔案系統的建立和刪除

目的	行動	使用處	權限政策
建立，檢視及管理 ONTAP 檔案系統資源的 FSX	fsx:CreateVolume	管理作業	營運和補救
	FSX ： TagResource	管理作業	營運和補救
	fsx:CreateStorageVirtualMachine	管理作業	檔案系統的建立和刪除
	fsx：刪除檔案系統	管理作業	檔案系統的建立和刪除
	fsx：刪除儲存虛擬機	管理作業	視圖、規劃與分析
	fsx:DescribeFileSystems	庫存	視圖、規劃與分析
	FSX ： DescrubeStorageVirtualMachines	庫存	視圖、規劃與分析
	fsx：描述共享虛擬PC配置	庫存	視圖、規劃與分析
	fsx：更新檔案系統	管理作業	營運和補救
	fsx：更新儲存虛擬機	管理作業	營運和補救
	FSX ： DescribeVolumes	庫存	視圖、規劃與分析
	fsx:UpdateVolume	管理作業	營運和補救
	fsx：刪除卷	管理作業	營運和補救
	FSX ： UntagResource	管理作業	營運和補救
	FSX ： DescrubeBackups	管理作業	視圖、規劃與分析
	fsx:建立備份	管理作業	營運和補救
	fsx：從備份建立磁碟區	管理作業	營運和補救
	fsx：刪除備份	管理作業	營運和補救
取得檔案系統和 Volume 度量	cloudswatch ： GetMetricData	管理作業	視圖、規劃與分析
	cloudwatch：GetMetricStatistics	管理作業	視圖、規劃與分析
模擬工作負載作業，以驗證可用權限，並與所需的 AWS 帳戶權限進行比較	IAM ： SimulatePrincipalPolicy	部署	全部

目的	行動	使用處	權限政策
為ONTAP EMS 事件的 FSx 提供基於人工智慧的洞察	Bedrock ： ListInferenceProfiles	FSx 用於ONTAP EMS 分析	營運和補救
	基岩：取得推理配置文件	FSx 用於ONTAP EMS 分析	營運和補救
	基岩：呼叫模型及其反應流	FSx 用於ONTAP EMS 分析	營運和補救
	Bedrock ： InvokeModel	FSx 用於ONTAP EMS 分析	營運和補救
從 AWS Cost Explorer 取得 FSx for ONTAP檔案系統的成本和使用量資料。	ce:獲取成本和使用情況	成本和使用分析	視圖、規劃與分析
	ce:GetTags	成本和使用分析	視圖、規劃與分析
建立 S3 存取點並將其連接到 Amazon FSx for NetApp ONTAP 檔案系統	fsx:CreateAndAttachS3AccessPoint	S3 存取點管理	營運和補救
從 FSx for ONTAP 檔案系統中分離 S3 存取點並將其刪除	fsx:DetachAndDeleteS3AccessPoint	S3 存取點管理	營運和補救
建立 S3 存取點，以簡化儲存區存取管理	s3：CreateAccessPoint	S3 存取點管理	營運和補救
刪除 S3 存取點	s3：DeleteAccessPoint	S3 存取點管理	營運和補救
在 S3 存取點新增標籤	s3：TagResource	S3 存取點管理	營運和補救
在 S3 存取點上列出並檢視標籤	s3：ListTagsForResource	S3 存取點管理	營運和補救
從 S3 存取點移除標籤	s3：UntagResource	S3 存取點管理	營運和補救
在 S3 存取點儲存貯體中探索物件	s3：ListBucket	S3 儲存貯體作業	營運和補救
列出、建立和描述 S3 表儲存貯體	s3tables：ListTableBuckets s3tables：CreateTableBucket s3tables：GetTableBucket	S3 表儲存貯體管理	營運和補救
列出、建立和擷取 S3 表	s3tables：ListTables s3tables ：CreateTable s3tables ：GetTable	S3 表格操作	營運和補救
讀取表格中繼資料位置	s3tables ：GetTableMetadataLocation	S3 表格中繼資料操作	營運和補救
更新表中繼資料位置	s3tables ：UpdateTableMetadataLocation	S3 表格中繼資料操作	營運和補救
列出、建立和擷取表命名空間	s3tables：ListNamespaces s3tables：CreateNamespace s3tables：GetNamespace	S3 命名空間作業	營運和補救

目的	行動	使用處	權限政策
讀取表格資料（select、scan）	s3tables：GetTableData	S3 表格資料操作	營運和補救
寫入表格資料（插入）	s3tables：PutTableData	S3 表格資料操作	營運和補救
列出庫存表中的標籤（取得 FSx for ONTAP、儲存 VM、磁碟區 ID）	s3tables：ListTagsForResource	S3 表格標籤操作	營運和補救
為 Workload Factory 查詢標記庫存表	s3tables：TagResource	S3 表格標籤操作	營運和補救
透過存取點擷取物件標記	s3：GetObjectTagging	S3 物件操作	營運和補救

資料庫工作負載的權限

資料庫工作負載可用的 IAM 策略提供了 Workload Factory 管理公有雲環境中的資源和進程所需的權限。

資料庫提供以下權限策略供您選擇：

- 檢視、規劃與分析：檢視資料庫資源清單，了解資源的運作狀況，檢視資料庫配置的良好架構分析，探索節省成本的方法，取得錯誤日誌分析，並探索節省成本的方法。
- 操作與修復：對資料庫資源執行操作任務，並修復資料庫配置和底層 FSx for ONTAP檔案系統儲存的問題。
- 資料庫主機建立：根據最佳實務部署資料庫主機和底層 FSx for ONTAP檔案系統儲存。

選取您的作業模式以檢視所需的 IAM 原則：

資料庫工作負載的 **IAM** 策略

視圖、規劃與分析

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CommonGroup",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:GetMetricData",
                "sns:ListTopics",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeRegions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "kms:ListAliases",
                "kms:ListKeys",
                "kms:DescribeKey",
                "cloudformation:ListStacks",
                "cloudformation:DescribeAccountLimits",
                "ds:DescribeDirectories",
                "fsx:DescribeVolumes",
                "fsx:DescribeBackups",
                "fsx:DescribeStorageVirtualMachines",
                "fsx:DescribeFileSystems",
                "servicequotas:ListServiceQuotas",
                "ssm:GetParametersByPath",
                "ssm:GetCommandInvocation",
                "ssm:SendCommand",
                "ssm:GetConnectionStatus",
                "ssm:DescribePatchBaselines",
                "ssm:DescribeInstancePatchStates",
                "ssm:ListCommands",
```

```
                "ssm:DescribeInstanceInformation",
                "fsx:ListTagsForResource",
                "logs:DescribeLogGroups",
                "bedrock:GetFoundationModelAvailability",
                "bedrock:ListInferenceProfiles"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "SSMParameterStore",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:GetParameters",
                "ssm:PutParameter",
                "ssm:DeleteParameters"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmdb/*"
        },
        {
            "Sid": "SSMResponseCloudWatch",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:netapp/wlmdb/*"
        }
    ]
}
```

營運和補救

```
[
    {
        "Sid": "FSxRemediation",
        "Effect": "Allow",
        "Action": [
            "fsx:UpdateFileSystem",
            "fsx:UpdateVolume"
        ],
        "Resource": "*"
    },
    {
        "Sid": "EC2Remediation",
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:StopInstances"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/aws:cloudformation:stack-name":
"WLMDB*"
            }
        }
    }
]
```

建立資料庫主機

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2TagGroup",
            "Effect": "Allow",
            "Action": [
                "ec2:AllocateAddress",
                "ec2:AllocateHosts",
                "ec2:AssignPrivateIpAddresses",
                "ec2:AssociateAddress",
                "ec2:AssociateRouteTable",
                "ec2:AssociateSubnetCidrBlock",
                "ec2:AssociateVpcCidrBlock",
                "ec2:AttachInternetGateway",
```

```
                "ec2:AttachNetworkInterface",
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateVolume",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DetachNetworkInterface",
                "ec2:DetachVolume",
                "ec2:DisassociateAddress",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DisassociateRouteTable",
                "ec2:DisassociateSubnetCidrBlock",
                "ec2:DisassociateVpcCidrBlock",
                "ec2:ModifyInstancePlacement",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVolume",
                "ec2:ModifyVolumeAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRoute",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
                }
            }
        },
        {
            "Sid": "FSxNGroup",
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
```

```
                }
            }
        },
        {
            "Sid": "CreationGroup",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStacks",
                "cloudformation:ValidateTemplate",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateLaunchTemplateVersion",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVpcEndpoint",
                "ec2:RunInstances",
                "ec2:DescribeTags",
                "ec2:DescribeLaunchTemplates",
                "ec2:ModifyVpcAttribute",
                "fsx:CreateFileSystem",
                "fsx:CreateStorageVirtualMachine",
                "fsx:CreateVolume",
                "fsx:DescribeFileSystemAliases",
                "kms:CreateGrant",
                "kms:DescribeCustomKeyStores",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:GetLogGroupFields",
                "logs:GetLogRecord",
                "logs:ListLogDeliveries",
                "logs:PutLogEvents",
                "logs:TagResource",
                "sns:Publish",
                "ssm:PutComplianceItems",
                "ssm:PutConfigurePackageResult",
                "ssm:PutInventory",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateInstanceAssociationStatus",
                "ssm:UpdateInstanceInformation",
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
```

```
                "ssmmessages:OpenDataChannel",
                "compute-optimizer:GetEnrollmentStatus",
                "compute-optimizer:PutRecommendationPreferences",
                "compute-
optimizer:GetEffectiveRecommendationPreferences",
                "compute-optimizer:GetEC2InstanceRecommendations",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeAutoScalingInstances",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ArnGroup",
            "Effect": "Allow",
            "Action": [
                "cloudformation:SignalResource"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/WLMDB*",
                "arn:aws:logs:*:*:log-group:WLMDB*"
            ]
        },
        {
            "Sid": "IAMGroup1",
            "Effect": "Allow",
            "Action": [
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:PutRolePolicy",
                "iam:RemoveRoleFromInstanceProfile"
            ],
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ]
        },
        {
            "Sid": "IAMGroup2",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "ec2.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMGroup3",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ec2.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMGroup4",
            "Effect": "Allow",
            "Action": "iam:CreateRole",
            "Resource": "arn:aws:iam::*:role/WLMDB*"
        }
    ]
}
```

下表顯示資料庫工作負載的權限。

資料庫工作負載的權限表

目的	行動	使用處	權限政策
取得 FSx for ONTAP、EBS 和 FSx for Windows File Server 的指標統計資料以及計算最佳化建議	cloudwatch：GetMetricStatistics	• 庫存 • 探索節約效益	視圖、規劃與分析
從已註冊的 SQL 節點收集已儲存至 Amazon CloudWatch 的效能指標。資料將在已註冊 SQL 實例的管理實例畫面上產生效能趨勢圖。	cloudswatch ： GetMetricData	庫存	視圖、規劃與分析
取得 EC2 執行個體的詳細資料	EC2：資料說明	• 庫存 • 探索節約效益	視圖、規劃與分析
	EC2：評量會議	部署	視圖、規劃與分析
	EC2：網路介面	部署	視圖、規劃與分析
	EC2 ： DescribeInstanceTypes	• 部署 • 探索節約效益	視圖、規劃與分析
取得詳細資料以填寫適用於 ONTAP 部署的 FSX 表單	EC2：取消功能Vpcs	• 部署 • 庫存	視圖、規劃與分析
	EC2：無資料子網路	• 部署 • 庫存	視圖、規劃與分析
	EC2：取消安全性群組	部署	視圖、規劃與分析
	EC2：取消影像	部署	視圖、規劃與分析
	EC2：取消註冊	部署	視圖、規劃與分析
	EC2：取消功能表	• 部署 • 庫存	視圖、規劃與分析
取得任何現有的 VPC 端點，判斷是否需要在部署之前建立新的端點	EC2：取消資料VpcEndpoints	• 部署 • 庫存	視圖、規劃與分析

目的	行動	使用處	權限政策
如果在 EC2 執行個體上的公用網路連線不存在所需服務的 VPC 端點，請建立這些端點	EC2 ： CreateVpcEndpoint	部署	建立資料庫主機
取得適用於驗證節點的區域執行個體類型（ T2.micro/T3.micro ）	EC2 ： DescrubeInstanceTypeOffing	部署	視圖、規劃與分析
取得每個附加 EBS 磁碟區的快照詳細資料，以瞭解價格與成本預估	EC2：取消快照	探索節約效益	視圖、規劃與分析
取得每個附加 EBS 磁碟區的詳細資料，以瞭解價格與預估節約效益	EC2：減量磁碟區	• 庫存 • 探索節約效益	視圖、規劃與分析
取得適用於 ONTAP 檔案系統加密之 FSX 的 KMS 金鑰詳細資料	kms：清單別名	部署	視圖、規劃與分析
	kms ： ListKeys	部署	視圖、規劃與分析
	KMS ： DescribeKey	部署	視圖、規劃與分析
取得在環境中執行的 CloudForgation 堆疊清單，以檢查配額限制	雲端：清單堆疊	部署	視圖、規劃與分析
在觸發部署之前，請先檢查資源的帳戶限制	雲端： DescrubeAccountLimits	部署	視圖、規劃與分析
取得區域中 AWS 管理的 Active Directory 清單	DS:DescrubeDirectories	部署	視圖、規劃與分析

目的	行動	使用處	權限政策
取得適用於 ONTAP 檔案系統的磁碟區，備份， SVM ， AZs 檔案系統和 FSX 標籤的清單和詳細資料	FSX ： DescribeVolumes	• 庫存 • 探索節約效益	視圖、規劃與分析
	FSX ： DescrubeBackups	• 庫存 • 探索節約效益	視圖、規劃與分析
	FSX ： DescrubeStorageVirtualMachines	• 部署 • 管理作業 • 庫存	視圖、規劃與分析
	fsx:DescribeFileSystems	• 部署 • 管理作業 • 庫存 • 探索節約效益	視圖、規劃與分析
	FSX ： ListTagsForResource	管理作業	視圖、規劃與分析
取得 CloudFormation 和 VPC 的服務配額限制 / 在使用者帳戶中為提供的 SQL、網域和 FSx for ONTAP憑證建立金鑰	serviceEquotas ： ListServiceQuotas	部署	視圖、規劃與分析
使用 SSM) 查詢取得適用於 ONTAP 支援區域的 FSX 更新清單	SSM) ： GetParametersByPath	部署	視圖、規劃與分析
部署後發送管理操作命令後，輪詢 SSM 回應	SSM) ： GetCommandInvocation	• 管理作業 • 庫存 • 探索節約效益 • 最佳化	視圖、規劃與分析
透過 SSM 向 EC2 執行個體傳送命令以進行發現和管理	S10:SendCommand	• 管理作業 • 庫存 • 探索節約效益 • 最佳化	視圖、規劃與分析

目的	行動	使用處	權限政策
取得部署後執行個體的 SSM 連線狀態	SSM) ： GetConnectionStatus	• 管理作業 • 庫存 • 最佳化	視圖、規劃與分析
擷取一組受管理 EC2 執行個體（ SQL 節點）的 SSM 關聯狀態	SSM) ： DescrubeInstanceInformation	庫存	視圖、規劃與分析
取得作業系統修補程式評估可用的修補程式基準清單	SSM) ： DescrubePatchBasines	最佳化	視圖、規劃與分析
取得 Windows EC2 執行個體的修補狀態，以進行作業系統修補程式評估	SSM) ： DescribeInstancePatchStates	最佳化	視圖、規劃與分析
列出 AWS Patch Manager 在 EC2 執行個體上執行的命令，以進行作業系統修補程式管理	SSM/ListCommands	最佳化	視圖、規劃與分析
檢查帳戶是否已註冊 AWS 運算最佳化工具	運算最佳化工具： GetEnrollmentStatus	• 探索節約效益 • 最佳化	建立資料庫主機
更新 AWS 運算最佳化工具中現有的建議偏好選項，針對 SQL Server 工作負載量提供量身打造的建議	運算最佳化工具：推桿建議偏好設定	• 探索節約效益 • 最佳化	建立資料庫主機
從 AWS 運算最佳化工具取得對指定資源有效的建議偏好選項	運算最佳化工具： GetEffectiveRecompendationPreferences	• 探索節約效益 • 最佳化	建立資料庫主機
取得 AWS 運算最佳化工具為 Amazon Elastic Compute Cloud （ Amazon EC2 ） 執行個體所產生的建議	運算最佳化工具： GetEC2InstanceRecompendations	• 探索節約效益 • 最佳化	建立資料庫主機
檢查執行個體與自動縮放群組的關聯	自動縮放：去除自動縮放群組	• 探索節約效益 • 最佳化	建立資料庫主機
	自動縮放：去除自動縮放的實例	• 探索節約效益 • 最佳化	建立資料庫主機

目的	行動	使用處	權限政策
取得，列出，建立及刪除 AD 的 SSM 參數， ONTAP 的 FSX 參數，以及在 AWS 帳戶中部署或管理時所使用的 SQL 使用者認證	SSM) ： GetParameter [1]	• 部署 • 管理作業 • 庫存	視圖、規劃與分析
	S10:GetParameters [1]	• 部署 • 管理作業 • 庫存	視圖、規劃與分析
	SSM) ：推桿參數 [1]	• 部署 • 管理作業	視圖、規劃與分析
	S10:DeleteParameters [1]	• 部署 • 管理作業	視圖、規劃與分析
將網路資源與 SQL 節點和驗證節點建立關聯，並將其他次要 IP 新增至 SQL 節點	EC2 ： AllocateAddress [1]	部署	建立資料庫主機
	EC2 ： AllocateHos[1]	部署	建立資料庫主機
	EC2 ： AssignPrivate IpAddresses [1]	部署	建立資料庫主機
	EC2 ： AssociateAddress [1]	部署	建立資料庫主機
	EC2 ： AssociateRouteTable [1]	部署	建立資料庫主機
	EC2 ： AssociateSubnetCidrBlock [1]	部署	建立資料庫主機
	EC2 ： AssociateVpcCidrBlock [1]	部署	建立資料庫主機
	EC2 ： AttachInternetGateway [1]	部署	建立資料庫主機
	EC2 ： AttachNetworkInterface [1]	部署	建立資料庫主機
將部署所需的 EBS 磁碟區附加至 SQL 節點	EC2：AttachVolume	部署	建立資料庫主機
將安全性群組附加到已配置的 EC2 執行個體並修改規則	EC2：授權安全性群組出口	部署	建立資料庫主機
	EC2：授權安全性群組入口	部署	建立資料庫主機
建立部署 SQL 節點所需的 EBS 磁碟區	EC2：建立磁碟區	部署	建立資料庫主機

目的	行動	使用處	權限政策
移除以 T2.micro 類型建立的暫存驗證節點，以及用於復原或重試失敗的 EC2 SQL 節點	EC2：刪除網路介面	部署	建立資料庫主機
	EC2：刪除安全性群組	部署	建立資料庫主機
	EC2：刪除標記	部署	建立資料庫主機
	EC2：刪除Volume	部署	建立資料庫主機
	EC2 ： DetachNetwork Interface	部署	建立資料庫主機
	EC2：分離Volume	部署	建立資料庫主機
	EC2 ： DiscassociateAddress	部署	建立資料庫主機
	EC2：中斷IamInstanceProfile	部署	建立資料庫主機
	EC2 ： DiscassociateRouteTable	部署	建立資料庫主機
	EC2 ： DiscassociateSubnetCidrBlock	部署	建立資料庫主機
	EC2 ： DiscassociateVpcCidrBlock	部署	建立資料庫主機
修改已建立 SQL 執行個體的屬性。僅適用於以 WLMDB 開頭的名稱。	EC2：修改實例屬性	部署	營運和補救
	EC2 ： ModifyInstancePlacement	部署	建立資料庫主機
	EC2：修改網路互連屬性	部署	建立資料庫主機
	EC2 ： ModifySubnetAttribute.	部署	建立資料庫主機
	EC2：修改Volume	部署	建立資料庫主機
	EC2：修改Volume屬性	部署	建立資料庫主機
	EC2 ： ModifyVpcAttribute	部署	建立資料庫主機
解除關聯並銷毀驗證執行個體	EC2 ： ReleaseAddress	部署	建立資料庫主機
	EC2 ：安慰劑 Route	部署	建立資料庫主機
	EC2 ： ReplaceRouteTableAssociation	部署	建立資料庫主機
	EC2：RevokeSecurity GroupEgress	部署	建立資料庫主機
	EC2：RevokeSecurity GroupIngress	部署	建立資料庫主機
啟動部署的執行個體	EC2：啟動安裝	部署	營運和補救
停止部署的執行個體	EC2：停止執行	部署	營運和補救
為 NetApp ONTAP 資源標記 Amazon FSX 的自訂值，以在資源管理期間取得帳單詳細資料	fsx:TagResource [1]	• 部署 • 管理作業	建立資料庫主機

目的	行動	使用處	權限政策
建立並驗證 CloudForgation 範本以進行部署	雲端：建立堆疊	部署	建立資料庫主機
	雲端：取消功能堆疊事件	部署	建立資料庫主機
	雲端：無標準堆疊	部署	建立資料庫主機
	雲端：清單堆疊	部署	視圖、規劃與分析
	cloudformation：驗證範本	部署	建立資料庫主機
建立巢狀堆疊範本以重試及復原	EC2 ： CreateLaunchTemplate	部署	建立資料庫主機
	EC2 ： CreateLaunchTemplateVersion	部署	建立資料庫主機
管理已建立執行個體的標記和網路安全性	EC2：建立網路介面	部署	建立資料庫主機
	EC2：建立安全性群組	部署	建立資料庫主機
	EC2：建立標記	部署	建立資料庫主機
取得資源配置的執行個體詳細資料	ec2:描述地址	部署	視圖、規劃與分析
	ec2:描述啟動模板	部署	視圖、規劃與分析
啟動建立的執行個體	EC2：RunInstances	部署	建立資料庫主機
為佈建所需的 ONTAP 資源建立 FSX 。對於現有的適用於 ONTAP 系統的 FSX ，系統會建立新的 SVM 來裝載 SQL Volume 。	fsx:CreateFileSystem	部署	建立資料庫主機
	fsx:CreateStorageVirtualMachine	部署	建立資料庫主機
	fsx:CreateVolume	• 部署 • 管理作業	建立資料庫主機
取得 ONTAP 詳細資料的 FSX	fsx:描述檔案系統別名	部署	建立資料庫主機
調整 ONTAP 檔案系統的 FSX 大小，以修正檔案系統保留空間	fsx:UpdateFilesystem	最佳化	營運和補救
調整磁碟區大小以修正記錄和 TempDB 磁碟機大小	fsx:UpdateVolume	最佳化	營運和補救
取得 KMS 金鑰詳細資料，並使用適用於 ONTAP 加密的 FSX	公里：建立授予	部署	建立資料庫主機
	kms:描述自訂密鑰存儲	部署	建立資料庫主機
	KMS ： GenerateDataKey	部署	建立資料庫主機

目的	行動	使用處	權限政策
建立 CloudWatch 記錄檔，用於在 EC2 執行個體上執行驗證和資源配置指令碼	記錄檔： CreateLogGroup	部署	建立資料庫主機
	記錄： CreateLogStream	部署	建立資料庫主機
	日誌：取得日誌群組字段	部署	建立資料庫主機
	日誌：取得日誌記錄	部署	建立資料庫主機
	記錄： ListLogDeliverys	部署	建立資料庫主機
	記錄： PutLogEvents	• 部署 • 管理作業	建立資料庫主機
	記錄： TagResource	部署	建立資料庫主機
遇到 SSM 輸出截斷時，Workload Factory 會切換到 SQL 執行個體的 Amazon CloudWatch 日誌	記錄檔： GetLogEvents	• 儲存評估（最佳化） • 庫存	視圖、規劃與分析
允許 Workload Factory 取得目前日誌組並檢查 Workload Factory 建立的日誌組是否設定了保留	記錄： DescribeLogGroups	• 儲存評估（最佳化） • 庫存	視圖、規劃與分析
允許 Workload Factory 為其建立的日誌組設定一天的保留策略，以避免 SSM 指令輸出的日誌流不必要地積累	記錄： PutRetentionPolicy	• 儲存評估（最佳化） • 庫存	視圖、規劃與分析
列出客戶 SNS 主題，並在選取時發佈至 WLMDB 後端 SNS 和客戶 SNS	SnS:ListTopics	部署	視圖、規劃與分析
	SnS ：發佈	部署	建立資料庫主機
必要的 SSM 權限，可在已佈建的 SQL 執行個體上執行探索指令碼，並擷取 ONTAP 支援的 AWS 區域的最新 FSX 清單。	SSM) ： PuttinianceItem	部署	建立資料庫主機
	S10:PutConfigurePackageResult	部署	建立資料庫主機
	SSM) ： PuttInventory	部署	建立資料庫主機
	SSM) ：更新關聯狀態	部署	建立資料庫主機
	SSM) ： UpdateInstanceAssociationStatus	部署	建立資料庫主機
	SSM) ： UpdateInstanceInformation	部署	建立資料庫主機
	ssmmessages：建立控制通道	部署	建立資料庫主機
	ssmmessages：建立資料通道	部署	建立資料庫主機
	ssmmessages：開啟控制通道	部署	建立資料庫主機
	ssmmessages：開放式資料通道	部署	建立資料庫主機

目的	行動	使用處	權限政策
在成功或失敗時發出 CloudForgation 堆疊訊號。	雲端： SignalResource [1]	部署	建立資料庫主機
將範本建立的 EC2 角色新增至 EC2 的執行個體設定檔，以允許 EC2 上的指令碼存取部署所需的資源。	IAM：AddRoleToInstanceProfile	部署	建立資料庫主機
為 EC2 建立執行個體設定檔，並附加建立的 EC2 角色。	IAM：CreatanceProfile	部署	建立資料庫主機
透過下列權限範本建立 EC2 角色	IAM：建立角色	部署	建立資料庫主機
建立連結至 EC2 服務的角色	IAM ： CreateServiceLinkedIn 角色 [2]	部署	建立資料庫主機
刪除部署期間為驗證節點所建立的執行個體設定檔	IAM：刪除InstanceProfile	部署	建立資料庫主機
取得角色和原則詳細資料，以判斷權限的任何落差，並驗證部署	IAM ： GetPolicy	部署	建立資料庫主機
	IAM ： GetPolicyVersion	部署	建立資料庫主機
	IAM：GetRole	部署	建立資料庫主機
	IAM ： GetRolePolicy	部署	建立資料庫主機
	IAM ： GetUser	部署	建立資料庫主機
將建立的角色傳遞給 EC2 執行個體	IAM ： PassRole [3]	部署	建立資料庫主機
將具有必要權限的原則新增至所建立的 EC2 角色	IAM：Putt角色 原則	部署	建立資料庫主機
從已配置的 EC2 執行個體設定檔中分離角色	IAM ：RemoveRoleFromInstanceProfile	部署	建立資料庫主機
模擬工作負載作業，以驗證可用權限，並與所需的 AWS 帳戶權限進行比較	IAM ： SimulatePrincipalPolicy	部署	全部
取得可用於錯誤日誌分析的基礎模型	Bedrock:GetFoundationModelAvailability	錯誤日誌分析	視圖、規劃與分析
列出 Amazon Bedrock 中可用於錯誤日誌分析的介面設定檔	Bedrock ： ListInferenceProfiles	錯誤日誌分析	視圖、規劃與分析

1. 權限僅限於從 WLMDB 開始的資源。
2. "IAM:CreateServiceLinkedIn Role" 受 "iam:AWSServiceName" 限制： "ec2.amazonaws.com"*
3. "IAM:PassRole" 受 "iAM:PassedToService" 限制： "ec2.amazonaws.com"*

GenAI 工作負載的權限

VMware 工作負載的 IAM 策略會根據您所處的運作模式，提供 Workload Factory for VMware 管理公有雲環境中的資源和流程所需的權限。

GenAI IAM 策略僅支援讀取/寫入權限：

- 讀取/寫入：使用指派的憑證代表您在 AWS 中執行和自動執行操作，這些憑證具有執行所需的已驗證權限。

GenAI 工作負載的 IAM 原則

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudformationGroup",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/wlmai*/*"
    },
    {
      "Sid": "EC2Group",
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/aws:cloudformation:stack-name": "wlmai*"
        }
      }
    },
    {
      "Sid": "EC2DescribeGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
```

```
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:PutRolePolicy",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup2",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid": "FSXNGroup",
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeVolumes",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FSXNGroup2",
      "Effect": "Allow",
      "Action": [
```

```
        "fsx:UntagResource",
        "fsx:TagResource"
      ],
      "Resource": [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ]
    },
    {
      "Sid": "SSMParameterStore",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmai/*"
    },
    {
      "Sid": "SSM",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/aws/service/*"
    },
    {
      "Sid": "SSMMessages",
      "Effect": "Allow",
      "Action": [
        "ssm:GetCommandInvocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSMCommandDocument",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/AWS-RunShellScript"
      ]
    },
    {
      "Sid": "SSMCommandInstance",
```

```
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:GetConnectionStatus"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/aws:cloudformation:stack-name": "wlmai-*"
        }
      }
    },
    {
      "Sid": "KMS",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SNS",
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatch",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchAiEngine",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
```

```
        "logs:DescribeLogStreams"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*"
    },
    {
      "Sid": "CloudWatchAiEngineLogStream",
      "Effect": "Allow",
      "Action": [
        "logs:GetLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*:*"
    },
    {
      "Sid": "BedrockGroup",
      "Effect": "Allow",
      "Action": [
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:PutModelInvocationLoggingConfiguration",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchBedrock",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/bedrock*"
    },
    {
      "Sid": "BedrockLoggingAttachRole",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::*:role/NetApp_AI_Bedrock*"
    },
    {
```

```
      "Sid": "BedrockLoggingIamOperations",
      "Effect": "Allow",
      "Action": [
        "iam:CreatePolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QBusiness",
      "Effect": "Allow",
      "Action": [
        "qbusiness:ListApplications"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

下表提供 GenAI 工作負載權限的詳細資料。

GenAI 工作負載的權限表

目的	行動	使用處	權限政策
在部署和重建作業期間建立 AI 引擎雲端堆疊	雲端：建立堆疊	部署	讀取/寫入
建立 AI 引擎雲端堆疊	雲端：無標準堆疊	部署	讀取/寫入
列出 AI 引擎部署精靈的區域	EC2：取消註冊	部署	讀取/寫入
顯示 AI 引擎標籤	EC2：取消標示	部署	讀取/寫入
列出 S3 儲存桶	S3：ListAllMyb桶	部署	讀取/寫入
在建立 AI 引擎堆疊之前列出 VPC 端點	EC2 ： CreateVpcEndpoint	部署	讀取/寫入
在部署和重建作業期間，在 AI 引擎堆疊建立期間建立 AI 引擎安全性群組	EC2：建立安全性群組	部署	讀取/寫入
在部署和重建作業期間，標記由 AI 引擎堆疊建立所建立的資源	EC2：建立標記	部署	讀取/寫入
從 AI 引擎堆疊將加密事件發佈至 WLMAI 後端	KMS ： GenerateDataKey	部署	讀取/寫入
	kms ：解密	部署	讀取/寫入
將事件和自訂資源從 AI 引擎堆疊發佈至 WLMAI 後端	SnS ：發佈	部署	讀取/寫入
在 AI 引擎部署精靈期間列出 VPC	EC2：取消功能Vpcs	部署	讀取/寫入
在「 AI 引擎部署精靈」中列出子網路	EC2：無資料子網路	部署	讀取/寫入
在 AI 引擎部署和重建期間取得路由表	EC2：取消功能表	部署	讀取/寫入
在 AI 引擎部署精靈期間列出金鑰配對	EC2：評量會議	部署	讀取/寫入
在 AI 引擎堆疊建立期間列出安全性群組（以在私有端點上尋找安全性群組）	EC2：取消安全性群組	部署	讀取/寫入
取得 VPC 端點，判斷是否應在 AI 引擎部署期間建立任何端點	EC2：取消資料VpcEndpoints	部署	讀取/寫入
列出 Amazon Q Business 應用程式	qbusiness ： ListApplications	部署	讀取/寫入
列出執行個體以瞭解 AI 引擎狀態	EC2：資料說明	疑難排解	讀取/寫入
在部署和重建作業期間，列出 AI 引擎堆疊建立期間的映像	EC2：取消影像	部署	讀取/寫入

目的	行動	使用處	權限政策
在部署和重建作業期間建立 AI 執行個體堆疊期間，建立並更新 AI 執行個體和私有端點安全群組	EC2：RevokeSecurity GroupEgress	部署	讀取/寫入
	EC2：RevokeSecurity GroupIngress	部署	讀取/寫入
在部署和重建作業期間，在雲端堆疊建立期間執行 AI 引擎	EC2：RunInstances	部署	讀取/寫入
在部署和重建作業期間，在堆疊建立期間附加安全群組並修改 AI 引擎的規則	EC2：授權安全性群組出口	部署	讀取/寫入
	EC2：授權安全性群組入口	部署	讀取/寫入
向其中一個基礎模式提出聊天要求	Bedrock ： InvokeModelWithResponseStream	部署	讀取/寫入
開始對基礎模型進行聊天 / 嵌入要求	Bedrock ： InvokeModel	部署	讀取/寫入
顯示區域中可用的基礎模型	Bedrock:ListFoundationModels	部署	讀取/寫入
取得基礎模型的相關資訊	Bedrock:GetFoundationModel	部署	讀取/寫入
驗證對基礎模型的存取	Bedrock:GetFoundationModelAvailability	部署	讀取/寫入
確認在部署和重建作業期間需要建立 Amazon CloudWatch 記錄群組	記錄： DescribeLogGroups	部署	讀取/寫入
在 AI 引擎精靈期間取得支援 FSX 和 Amazon bedrock 的區域	SSM) ： GetParametersByPath	部署	讀取/寫入
在部署和重建作業期間，取得 AI 引擎部署的最新 Amazon Linux 映像	S10:GetParameters	部署	讀取/寫入
從傳送至 AI 引擎的命令取得 SSM 回應	SSM) ： GetCommandInvocation	部署	讀取/寫入
檢查與 AI 引擎的 SSM 連線	S10:SendCommand	部署	讀取/寫入
	SSM) ： GetConnectionStatus	部署	讀取/寫入
在部署和重建作業期間，於堆疊建立期間建立 AI 引擎執行個體設定檔	IAM：建立角色	部署	讀取/寫入
	IAM：CreatanceProfile	部署	讀取/寫入
	IAM：AddRoleToInstanceProfile	部署	讀取/寫入
	IAM：Putt角色 原則	部署	讀取/寫入
	IAM ： GetRolePolicy	部署	讀取/寫入
	IAM：GetRole	部署	讀取/寫入
	IAM ： TagRole	部署	讀取/寫入
	IAM：密碼	部署	讀取/寫入

目的	行動	使用處	權限政策
模擬工作負載作業，以驗證可用權限，並與所需的 AWS 帳戶權限進行比較	IAM ： SimulatePrincipalPolicy	部署	讀取/寫入
在「建立知識庫」精靈中列出 ONTAP 檔案系統的 FSX	FSX ： DescribeVolumes	知識庫建立	讀取/寫入
在「建立知識庫」精靈中列出 ONTAP 檔案系統磁碟區的 FSX	fsx:DescribeFileSystems	知識庫建立	讀取/寫入
在重建作業期間，管理 AI 引擎上的知識庫	FSX ： ListTagsForResource	疑難排解	讀取/寫入
在「建立知識庫」精靈中，列出適用於 ONTAP 檔案系統儲存虛擬機器的 FSX	FSX ： DescrubeStorageVirtualMachines	部署	讀取/寫入
將知識庫移至新執行個體	FSX ： UntagResource	疑難排解	讀取/寫入
在重建期間管理 AI 引擎上的知識庫	FSX ： TagResource	疑難排解	讀取/寫入
以安全的方式儲存 SSM 機密（ ECR 權杖， CIFS 認證，租賃服務帳戶金鑰）	SSM) ： GetParameter	部署	讀取/寫入
	SSM) ： Puttarameter	部署	讀取/寫入
在部署和重建作業期間，將 AI 引擎記錄傳送至 Amazon CloudWatch 記錄群組	記錄檔： CreateLogGroup	部署	讀取/寫入
	記錄： PutRetentionPolicy	部署	讀取/寫入
將 AI 引擎記錄傳送至 Amazon CloudWatch 記錄群組	記錄： TagResource	疑難排解	讀取/寫入
從 Amazon CloudWatch 取得 SSM 回應（回應時間過長時）	記錄： DescribeLogStreams	疑難排解	讀取/寫入
取得 Amazon CloudWatch 的 SSM 回應	記錄檔： GetLogEvents	疑難排解	讀取/寫入
在部署和重建作業期間建立堆疊時，為 Amazon 基礎記錄建立 Amazon CloudWatch 記錄群組	記錄檔： CreateLogGroup	部署	讀取/寫入
	記錄： PutRetentionPolicy	部署	讀取/寫入
	記錄： TagResource	部署	讀取/寫入
列出模型的推斷輪廓	Bedrock ： ListInferenceProfiles	疑難排解	讀取/寫入

VMware 工作負載的權限

VMware 工作負載有以下權限策略可供選擇：

- 檢視、規劃與分析：檢視 EVS 虛擬化環境的清單，取得系統架構完善的分析，並探索節省成本的方法。
- 資料儲存部署與連線：將建議的 VM 版面配置部署至 Amazon EVS、Amazon EC2 或 VMware Cloud on AWS vSphere 叢集，並使用自訂的Amazon FSx for NetApp ONTAP檔案系統作為外部資料儲存。

選擇權限策略以查看所需的 IAM 策略：

適用於 **VMware** 工作負載的 **IAM** 原則

視圖、規劃與分析

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeDhcpOptions",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "secretsmanager:ListSecrets",
        "evs:ListEnvironments",
        "evs:GetEnvironment",
        "evs:ListEnvironmentVlans"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

資料儲存部署和連接

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:DescribeFileSystems",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:CreateVolume",
        "fsx:DescribeVolumes",
        "fsx:TagResource",
        "sns:Publish",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:CreateGrant"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

下表提供 VMware 工作負載權限的詳細資料。

VMware 工作負載的權限表

目的	行動	使用處	權限政策
附加安全性群組並修改已佈建節點的規則	EC2：授權安全性群組入口	部署	資料儲存部署和連接
建立 EBS 磁碟區	fsx:CreateVolume	部署	資料儲存部署和連接
為 VMware 工作負載所建立的 NetApp ONTAP 資源標記 FSX 的自訂值	FSX ： TagResource	部署	資料儲存部署和連接
建立並驗證 CloudForgation 範本	雲端：建立堆疊	部署	資料儲存部署和連接
管理已建立執行個體的標記和網路安全性	EC2：建立安全性群組	部署	資料儲存部署和連接
啟動建立的執行個體	EC2：RunInstances	部署	資料儲存部署和連接
取得 EC2 執行個體詳細資料	EC2：資料說明	庫存	資料儲存部署和連接
在部署和重建作業期間，列出堆疊建立期間的映像	EC2：取消影像	庫存	資料儲存部署和連接
查看與 VPC 關聯的 DHCP 選項集的配置詳情	ec2:描述DHCP選項	庫存	視圖、規劃與分析
取得所選環境中的 VPC 以完成部署表單	EC2：取消功能Vpcs	• 部署 • 庫存	視圖、規劃與分析
取得所選環境中的子網路以完成部署表單	EC2：無資料子網路	• 部署 • 庫存	視圖、規劃與分析
取得所選環境中的安全性群組，以完成部署表單	EC2：取消安全性群組	部署	視圖、規劃與分析
取得所選環境中的可用性區域	EC2 ：去除可用性區域	• 部署 • 庫存	視圖、規劃與分析
透過 Amazon FSX for NetApp ONTAP 支援取得地區資訊	EC2：取消註冊	部署	視圖、規劃與分析
取得 KMS 金鑰的別名，以用於 Amazon FSX 進行 NetApp ONTAP 加密	kms：清單別名	部署	視圖、規劃與分析
取得 KMS 金鑰以用於 Amazon FSX 的 NetApp ONTAP 加密	kms ： ListKeys	部署	視圖、規劃與分析

目的	行動	使用處	權限政策
取得 KMS 金鑰到期詳細資料，以用於 Amazon FSX 進行 NetApp ONTAP 加密	KMS ： DescribeKey	部署	視圖、規劃與分析
列出 AWS Secrets Manager 中的金鑰	secretsmanager:列出秘密	庫存	視圖、規劃與分析
從 Amazon EVS 取得環境列表	evs:列出環境	庫存	視圖、規劃與分析
獲取有關特定 Amazon EVS 環境的詳細信息	evs:GetEnvironment	庫存	視圖、規劃與分析
列出與 Amazon EVS 環境關聯的 VLAN	evs:列出環境VLAN	庫存	視圖、規劃與分析
為資源配置所需的 NetApp ONTAP 資源建立 Amazon FSX	fsx:CreateFileSystem	部署	資料儲存部署和連接
	fsx:CreateStorageVirtualMachine	部署	資料儲存部署和連接
	fsx:CreateVolume	• 部署 • 管理作業	資料儲存部署和連接
取得 Amazon FSX 以取得 NetApp ONTAP 詳細資料	FSX：說明*	• 部署 • 庫存 • 管理作業 • 探索節約效益	資料儲存部署和連接
取得 KMS 金鑰詳細資料，並使用 Amazon FSX 進行 NetApp ONTAP 加密	公里：建立授予	部署	資料儲存部署和連接
	公里：描述*	部署	視圖、規劃與分析
	公里：清單*	部署	視圖、規劃與分析
	kms ：解密	部署	資料儲存部署和連接
	KMS ： GenerateDataKey	部署	資料儲存部署和連接
列出客戶 SNS 主題，並在選取的情況下發佈至 WLMVMC 後端 SNS 和客戶 SNS	SnS ：發佈	部署	資料儲存部署和連接

目的	行動	使用處	權限政策
模擬工作負載作業，以驗證可用權限，並與所需的 AWS 帳戶權限進行比較	IAM ： SimulatePrincipalPolicy	部署	• 資料儲存部署和連接 • 視圖、規劃與分析

變更記錄

新增和移除權限時、我們會在下方各節中加以註記。

2025 年 2 月 1 日

以下權限已新增至儲存工作負載：

- `s3:TagResource`
- `s3:ListTagsForResource`
- `s3:UntagResource`
- `s3tables:CreateTableBucket`
- `s3tables:ListTables`
- `s3tables:GetTable`
- `s3tables:GetTableMetadataLocation`
- `s3tables:CreateTable`
- `s3tables:GetNamespace`
- `s3tables:PutTableData`
- `s3tables:CreateNamespace`
- `s3tables:GetTableData`
- `s3tables:ListNamespaces`
- `s3tables:ListTableBuckets`
- `s3tables:GetTableBucket`
- `s3tables:UpdateTableMetadataLocation`
- `s3tables:ListTagsForResource`
- `s3tables:TagResource`
- `s3:GetObjectTagging`
- `s3:ListBucket`

2025 年 12 月 4 日

以下權限已新增至儲存工作負載：

- `fsx:CreateAndAttachS3AccessPoint`
- `fsx:DetachAndDeleteS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:DeleteAccessPoint`

2025年11月27日

以下權限已新增至儲存工作負載：

- `bedrock:ListInferenceProfiles`
- `bedrock:GetInferenceProfile`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:InvokeModel`

2025年11月2日

儲存、資料庫工作負載和 VMware 工作負載中的「唯讀」和「讀取/寫入」權限策略已被替換，以便在分配權限時提供更精細的粒度和更大的靈活性。

2025年10月5日

以下權限已從 GenAI 中刪除，現在由 GenAI 引擎處理：

- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:CreatePolicy`

2025 年 6 月 29 日

現在，資料庫在唯讀模式下具有以下權限： `cloudwatch:GetMetricData` 。

2025 年 6 月 3 日

現在，GenAI 在讀取/寫入模式下具有以下權限： `s3:ListAllMyBuckets` 。

2025 年 4 月 5 日

現在，GenAI 在讀取/寫入模式下具有以下權限： `qbusiness:ListApplications` 。

現在，資料庫在唯讀模式下具有以下權限：

- `logs:GetLogEvents`
- `logs:DescribeLogGroups`

現在，資料庫在讀取/寫入模式下具有以下權限：
`logs:PutRetentionPolicy` 。

2025 年 **4** 月 **2** 日

現在，資料庫在唯讀模式下具有以下權限： `ssm:DescribeInstanceInformation` 。

2025 年 **3** 月 **30** 日

GenAI 工作負載權限更新

GenAI 的「讀取/寫入模式」下現在提供以下權限：

- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:createPolicy`
- `bedrock:ListInferenceProfiles`

已從 GenAI 的「讀取/寫入模式」中刪除以下權限： `Bedrock:GetFoundationModel` 。

IAM ： **SimulatePrincipalPolicy** 權限更新

這 `iam:SimulatePrincipalPolicy`如果您在新增其他 AWS 帳戶憑證或從 Workload Factory 控制台新增新的工作負載功能時啟用自動權限檢查，則權限是所有工作負載權限原則的一部分。此權限模擬工作負載操作，並在從工作負載工廠部署資源之前檢查您是否具有所需的 AWS 帳戶權限。啟用此檢查可減少清理失敗操作的資源和新增缺少的權限所需的時間和精力。

2025 年 **3** 月 **2** 日

現在，GenAI 在讀取/寫入模式下具有以下權限： `bedrock:GetFoundationModel` 。

2025 年 **3** 月 **2** 日

現在，資料庫在唯讀模式下具有以下權限： `iam:SimulatePrincipalPolicy` 。