



管理 **S3** 存取點

Workload Factory for NetApp Console

NetApp
October 07, 2026

目錄

管理 S3 存取點	1
在 NetApp Workload Factory 中為一個 volume 建立 S3 存取端點	1
在 NetApp Workload Factory 中管理 Volume 的 S3 存取點	2
編輯 Volume 的 S3 存取點	2
檢視 Volume 的 S3 存取點詳細資料	2
在 NetApp Workload Factory 中刪除某個 volume 的 S3 存取端點	3
為 NetApp Workload Factory 設定 Journal 資料表基礎架構	3
關於此任務	3
開始之前	4
設定日誌表基礎架構	6
疑難排解日誌表的基礎架構設定	7
日誌表設定的權限參考	10

管理 S3 存取點

在 NetApp Workload Factory 中為一個 volume 建立 S3 存取端點

在 NetApp Workload Factory 中為磁碟區建立並附加 S3 存取點。

關於此任務

Amazon FSx for NetApp ONTAP 允許 NFS 和 SMB 檔案系統存取 S3 資料，並連接到 Amazon Bedrock、SageMaker、Athena、AWS Glue 等 AWS 服務。您可以將 AWS 服務連接到所有物件儲存資料。

將 S3 存取點附加到 FSx for ONTAP 檔案系統中的 NFS 和 SMB Volume，以便 AWS 服務可以像存取 S3 儲存貯體中的檔案一樣存取它們。附加存取點時，請定義一個唯一 ID，選擇檔案存取類型（UNIX 或 Windows），並新增用於存取授權的使用者名稱。

附加 S3 存取點後，它會出現在 AWS Management Console 中，並附有一個唯一的別名。使用此別名作為 AWS 服務（例如 Amazon Bedrock）的 S3 儲存貯體名稱，即可存取 Amazon FSx for NetApp ONTAP 磁碟區中的檔案。

您可以將多個 S3 存取點連接到單一 FSx for ONTAP 磁碟區，每個存取點都有唯一的存取層級，以連接到多個 AWS 服務。

開始之前

開始之前、請先完成下列需求。

- 您必須擁有一個已存在的包含 S3 存取點的磁碟區。["使用 S3 存取點建立磁碟區"](#)
- 您必須在 Workload Factory 中["使用 operations and remediation 權限原則授予認證"](#)完成此任務。

步驟

1. 登入 ["NetApp Console"](#)。
2. 選擇選單 ，工作負載 > **Volume** 資源管理器。
3. 選擇要使用的 Volume 的動作選單，然後選擇 進階動作，再選擇 管理 **S3** 存取點。
4. 在「管理 S3 存取點」頁面上、選取 * 建立並附加 S3 存取點 *。
5. 在「建立並連接 S3 存取點」頁面上，提供以下資訊：
 - **S3 存取點名稱**：輸入 S3 存取點的名稱。
 - **User**：選擇具有磁碟區存取權限的現有使用者或建立新使用者。
 - **使用者類型**：選取 **UNIX** 或 **Windows** 作為使用者類型。
 - **網路組態**：選取 **Internet** 或 **Virtual private cloud (VPC)**。您選擇的網路類型決定了存取點是可從網際網路存取、還是僅限於特定 VPC。若要使用 Journal 表格功能、您必須選取 **Internet** 作為網路組態。
 - **清單表**：選用。需要 getObject 權限。在磁碟區上啟用清單表，即可為所有可透過 S3 存取點存取的物件產生中繼資料，並產生 AWS S3 請求成本。如需詳細資訊，請參閱 ["Amazon S3 定價文件"](#)。表格每 24 小時更新一次。
 - **S3 存取點標籤**：您可以選擇新增最多 50 個標籤或移除標籤。

6. 選擇 **Create**。

相關資訊

您可以選擇在 Workload Factory 中使用 S3 存取點的日誌表功能。日誌表基礎架構會擷取並儲存 Amazon FSx for ONTAP 磁碟區存取點上的使用者存取事件和物件操作的稽核日誌。若要啟用日誌表功能、您必須設定必要的 AWS 基礎架構、包括 AWS CloudTrail、AWS CloudWatch、AWS S3 儲存桶、AWS CloudWatch 日誌群組、以及 AWS Identity and Access Management (IAM) 角色和政策。["為 NetApp Workload Factory 設定日誌表格基礎架構"](#)。

其他相關主題：

["在 NetApp Workload Factory 中編輯或刪除 Volume 的 S3 存取點"](#)

在 NetApp Workload Factory 中管理 Volume 的 S3 存取點

在 NetApp Workload Factory 中更新 Volume 的 S3 存取點詳細資訊或刪除 S3 存取點。

您也可以啟用或停用存取點的 **Inventory table**。Inventory table 會為所有可透過 S3 存取點存取的物件產生中繼資料，並產生 AWS S3 請求費用。如需詳細資訊，請參閱 ["Amazon S3 定價文件"](#)。

編輯 Volume 的 S3 存取點

在 NetApp Workload Factory 中編輯磁碟區的 S3 存取點。

步驟

1. 登入 ["NetApp Console"](#)。
2. 選擇選單 ，工作負載 > 儲存設備 > **Volume** 資源管理器。
3. 選擇要編輯 S3 存取點的 Volume 的動作選單，然後選取 進階動作，然後選取 管理 **S3** 存取點。
4. 從 **Manage S3 access points** 畫面中，選擇操作選單，然後選擇 **Edit access point**。
5. 進行更新，然後選取 **Apply**。

若要設定 journal table 功能的基礎架構，您必須選擇 **Internet** 作為 S3 存取點的網路設定。["瞭解如何為 NetApp Workload Factory 設定 Journal 資料表基礎架構"](#)。

檢視 Volume 的 S3 存取點詳細資料

查看 S3 存取點詳細資訊，例如別名、ARN 和 S3 URI。啟用清單和日誌表後，您可以查看跨 S3 存取點的使用者存取事件和物件操作的中繼資料和稽核記錄。

關於此任務

啟用磁碟區的清單表後，您可以查看連接到該磁碟區的現有 S3 存取點的存取點、清單表和表儲存桶詳細資料。系統也會在 AWS Management Console 中提供指向清單表的連結。

啟用日誌表後，Workload Factory 會在表格中產生存取點の日誌供您參考。此表格包含 CloudTrail 事件、追蹤 (AWS 活動記錄)、CloudTrail 篩選器、CloudWatch 日誌群組等資訊。

您可以複製存取點詳細資訊以供其他應用程式使用。

步驟

1. 登入 ["NetApp Console"](#)。
2. 選擇選單 ，工作負載 > 儲存設備 > **Volume** 資源管理器。
3. 選擇要檢視詳細資料的 Volume 的操作選單，然後選擇 進階操作，接著選擇 檢視詳細資料。

詳細資訊顯示在四個標籤下：`* Access point`、`Inventory table`、`Journal table` 和 `* Table bucket *`。

4. 如果庫存表或日記帳表的狀態已啟用，但您缺少 `get:Object` 權限，請依照對話方塊中的指示新增所需的權限。
5. 當日誌表狀態為「待處理」時，您必須提供 CloudTrail ARN 才能將日誌表連接到已建立的基礎架構。請依照說明使用 AWS CLI 或 AWS 管理控制台部署 CloudFormation 堆疊，然後返回 Workload Factory 控制台輸入 CloudTrail ARN。

在 NetApp Workload Factory 中刪除某個 volume 的 S3 存取端點

從 NetApp Workload Factory 的一個磁碟區中刪除現有的 S3 存取端點。

步驟

1. 登入 ["NetApp Console"](#)。
2. 選擇選單 ，工作負載 > 儲存設備 > **Volume** 資源管理器。
3. 選擇要管理 S3 存取點的 Volume 的動作選單，然後選取 進階動作，然後選取 管理 **S3** 存取點。
4. 選擇要刪除的 S3 存取點的動作功能表，然後選取 **Delete**。
5. 在*刪除 S3 存取點*對話方塊中、選取*刪除*以從磁碟區刪除 S3 存取點。

Workload Factory 不會刪除清單表或日誌表、但您可以從 AWS Management Console 手動移除它們。

相關資訊

- ["設定日誌表基礎架構"](#)

為 NetApp Workload Factory 設定 Journal 資料表基礎架構

設定日誌表基礎架構，以擷取和儲存 Amazon FSx for ONTAP 磁碟區存取點的使用者存取事件和物件操作的稽核日誌。需要執行多個步驟來設定 AWS 服務的基礎架構，例如 AWS CloudTrail、AWS CloudWatch、AWS S3 儲存桶、AWS CloudWatch 日誌群組、AWS Identity and Access Management (IAM) 和 AWS S3 表，以便日誌事件能夠正確地在管道中傳輸並被 Workload Factory 讀取。

關於此任務

Journal 表功能可擷取受監控 FSx for ONTAP S3 存取點的 S3 資料平面事件（PutObject、GetObject、DeleteObject 等）。它使用部署到您 AWS 帳戶中的一系列 AWS 服務。正確設定基礎架構後，它會連接到 FSx for ONTAP Volume 存取點，並建立管道，將使用者存取和物件操作稽核事件擷取到 Journal 表中。

下表列出構成基礎架構一部分的 AWS 服務、其各自的資源名稱模式，以及該服務在管道中的用途。

AWS 服務	資源名稱模式	目的
AWS CloudFormation	netapp-metadata-*	將所有基礎架構部署為堆疊
AWS S3 儲存貯體	netapp-metadata-cloudtrail-events-logs-{uuid}	儲存原始 CloudTrail 日誌檔案
AWS CloudTrail	netapp-metadata-journal-資料-事件-追蹤-{uuid}	擷取特定存取點的 S3 資料事件
AWS CloudWatch 日誌群組	netapp-metadata-journal-資料-事件-{uuid}	以結構化日誌項目的形式接收 CloudTrail 事件
IAM 角色	- netapp-metadata-cloudtrail-cw-role-{uuid} - netapp-metadata-s3table-integration-role-{uuid}	主動整合
ObservabilityAdmin	S3TableIntegration	將 CloudWatch 日誌橋接至 S3 Tables 表格
S3 資料表	aws-cloudwatch 儲存貯體 → logs.aws_cloudtrail__data	以 Iceberg 格式儲存結構化、可查詢的 CloudTrail 事件

{uuid} 是在建立範本時產生的隨機 8 個字元識別碼。

開始之前

若要啟用 Journal 表功能，請完成下列步驟：

- 已存在一個有 S3 存取點的磁碟區。["使用 S3 存取點建立磁碟區"](#)
- 將網路設定設為 **Internet** 以用於 S3 存取端點。["編輯 S3 存取點的網路組態"](#)。
- ["授予 *operations and remediation* 權限"](#) 至您的 Workload Factory 認證資料。
- 將下列 IAM 政策權限新增至用於執行 CloudFormation 部署以設定 Journal 表的 AWS 帳戶。

▼ 日誌表設定的 IAM 原則權限

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CFNStack",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/netapp-
metadata-*/*"
    },
  ],
}
```

```

{
  "Sid": "StarResources",
  "Effect": "Allow",
  "Action": [
    "cloudformation:GetTemplateSummary",
    "cloudtrail:DescribeTrails",
    "logs:DescribeLogGroups",
    "logs:ListSourcesForS3TableIntegration",
    "observabilityadmin:CreateS3TableIntegration",
    "observabilityadmin:GetS3TableIntegration",
    "observabilityadmin:TagResource",
    "observabilityadmin:ListTagsForResource"
  ],
  "Resource": "*"
},
{
  "Sid": "S3Bucket",
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:PutBucketPolicy",
    "s3:PutBucketTagging"
  ],
  "Resource": "arn:aws:s3:::netapp-metadata-*"
},
{
  "Sid": "IAMRoles",
  "Effect": "Allow",
  "Action": [
    "iam:CreateRole",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:GetRole"
  ],
  "Resource": "arn:aws:iam::*:role/netapp-metadata-*"
},
{
  "Sid": "PassRole",
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::*:role/netapp-metadata-*",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": [
        "cloudtrail.amazonaws.com",
        "logs.amazonaws.com"
      ]
    }
  }
}

```

```

    ]
  }
},
{
  "Sid": "CloudTrail",
  "Effect": "Allow",
  "Action": [
    "cloudtrail:CreateTrail",
    "cloudtrail:StartLogging",
    "cloudtrail:AddTags",
    "cloudtrail:PutEventSelectors"
  ],
  "Resource": "arn:aws:cloudtrail:*:*:trail/netapp-metadata-
* "
},
{
  "Sid": "CWLogGroup",
  "Effect": "Allow",
  "Action": [
    "logs:CreateLogGroup",
    "logs>DeleteLogGroup",
    "logs:PutRetentionPolicy",
    "logs:TagResource",
    "logs:AssociateSourceToS3TableIntegration"
  ],
  "Resource": "arn:aws:logs:*:*:log-group/netapp-metadata-*"
},
{
  "Sid": "S3Table",
  "Effect": "Allow",
  "Action": [
    "s3tables>CreateTableBucket",
    "s3tables:PutTableBucketEncryption",
    "s3tables:PutTableBucketPolicy"
  ],
  "Resource": "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
}
]
}

```

設定日誌表基礎架構

設定基礎架構，以從 S3 存取點擷取 AWS 服務事件到日誌表中。

步驟

1. 登入 "NetApp Console"。
2. 選擇選單 ，工作負載 > 儲存設備 > **FSx for ONTAP**。
3. 從 **FSx for ONTAP** 中，選擇包含要更新的 Volume 的檔案系統的操作選單，然後選擇 管理。
4. 從檔案系統總覽中，選擇 **Volume** 標籤。
5. 在「磁碟區」標籤中，選擇要管理 S3 存取點的磁碟區的操作選單，然後選擇 進階操作，再選擇 管理 **S3** 存取點。
6. 從 **Manage S3 access points** 畫面中，選擇操作選單，然後選擇 **Edit access point**。
7. 在「編輯 S3 存取點」對話方塊中、確保網路組態設定為「Internet」。
8. 依照對話方塊中的說明設定日誌表功能的基礎架構。
9. 下載 CloudFormation 範本。
10. 在您的 AWS 帳戶中部署 CloudFormation 堆疊。
 - a. 將範本 JSON 儲存至檔案。
 - b. 使用 AWS CLI 或 AWS Management Console 部署範本。
 - c. 等待堆疊達到 `CREATE_COMPLETE` 狀態。
 - d. 從堆疊輸出中取得 CloudTrail ARN。
11. 返回 Workload Factory 主控台，然後回到要管理 S3 存取點的磁碟區。
12. 從磁碟區動作功能表中選取 **View details**。
13. 在 **Journal table** 標籤中，輸入 CloudTrail ARN。
14. 選擇 **Apply**。

如果任何步驟失敗，[疑難排解日誌表的基礎架構設定](#) 或聯絡 NetApp 支援以尋求協助。

疑難排解日誌表的基礎架構設定

您可以使用 AWS Management Console 或 AWS CLI 來疑難排解 CloudFormation 堆疊部署及其建立的資源期間發生的故障。

解決問題後，請再次提交 CloudTrail ARN 以重新啟動日誌表設定。

常見的 CloudFormation 部署故障

IAM 權限不足

部署角色 / 使用者需要一組特定的權限。請參閱 [開始之前](#) 以取得完整原則。

如果堆疊失敗並出現 `AccessDenied` 或 `InsufficientPermission` 錯誤，請檢查堆疊事件並尋找 `ResourceStatusReason` 欄位中缺少的權限。

CloudTrail 限制

AWS 預設每個區域最多只能建立 5 條軌跡。如果帳戶已建立 5 條軌跡，`the FsxDataEventTrail` 資源將失敗，並顯示：超出最大軌跡數 (5)。您可以使用以下命令檢查區域層級的軌跡數：

```
aws cloudtrail describe-trails \
  --no-include-shadow-trails \
  --region <region> \
  --query "length(trailList)"
```

解決選項

- 選項 1：刪除該區域中未使用的追蹤以騰出空間。
- 選項 2：使用現有追蹤。在重新部署 CloudFormation 堆疊之前，請從範本中移除 `FsxDataEventTrail`、`CloudTrailBucket`、`CloudTrailBucketPolicy` 和 `CloudTrailToCloudWatchRole` 資源。然後在初始化步驟中傳遞現有追蹤的 ARN。現有追蹤必須配置 CloudWatch Log Group、將 S3TableIntegration 與該 Log Group 建立關聯，並且正在記錄資料事件。

S3 Table 整合已存在

如果帳戶中已經存在 `aws_cloudtrail` 資料來源的 S3TableIntegration，則 `LogsToS3TableIntegration` 資源將會失敗。

解決方案

在重新部署 CloudFormation 堆疊之前，請從範本中移除 `LogsToS3TableIntegration` 和 `S3TableIntegrationRole` 資源。只要您為 `aws_cloudtrail` 資料事件進行設定，系統就會自動使用現有的整合。

檢查現有整合：

```
aws observabilityadmin list-s3-table-integrations --region <your-region>
```

S3 儲存貯體名稱已存在

儲存桶名稱 `netapp-metadata-cloudtrail-events-logs-{uuid}` 是全域唯一的。如果發生衝突，請重新要求範本以取得新的 UUID。

IAM 角色已存在

如果先前的部分部署遺留了 `netapp-metadata-*` 名稱模式相同的 IAM 角色，則在建立角色時堆疊將失敗。請先刪除這些孤立的角色：

```
aws iam delete-role-policy \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid> \
  --policy-name <policy-name>
aws iam delete-role \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid>
```

啟用日誌表後發生的故障

提交 CloudTrail ARN 後，Workload Factory 會自動發送 *seed*（或測試）事件來驗證整個資源管道。如果驗證成功，種子事件將到達 S3 Tables 表中。此測試大約需要 10 分鐘。

如果測試驗證失敗、您可能會收到下列其中一則錯誤訊息：

錯誤訊息	意義
表 <code>aws_cloudtrail__data</code> 未在 <code>{bucket}</code> 中建立。請驗證 <code>s3table</code> 權限。	<code>S3TableIntegration</code> 未建立 CloudWatch 管理的表格。CloudWatch Logs 與 S3 Tables 之間的管道已中斷。
表格存在，但日誌種子事件未顯示。請檢查 CloudTrail 和 CloudWatch 權限。	表格存在，但特定的種子事件從未到達。CloudTrail 與 S3 Tables 表格之間的管道中斷。
無法啟動日誌設定。.....	背景種子 / 輪詢流程期間發生錯誤。請檢查後續訊息以取得詳細資料。

解決步驟

當日誌達到 FAILED 時，請透過管道階段向前追蹤種子事件，以確定其確切停止位置。每個步驟都對應至範本建立的特定 AWS 資源。

1. 檢查 CloudTrail S3 儲存桶。

此追蹤程式會將原始事件日誌寫入 S3 儲存貯體 `netapp-metadata-cloudtrail-events-logs`。請尋找最近的日誌檔案。

如果沒有日誌檔案，則表示 CloudTrail 沒有捕獲到事件。請檢查以下內容：

- 追蹤記錄正在記錄 (`IsLogging: true`)
- 進階事件選取器包含正確的存取點 ARN
- 進階事件選擇器包括 ``eventCategory = Data`` 和 ``resources.type = AWS::S3::AccessPoint`` 的篩選器

2. 檢查 CloudWatch 日誌群組。

該路徑也會向 CloudWatch Log Group 傳送事件。Log Group 名稱以 ``netapp-metadata-journal-data-events-<uuid>`` 開頭。

- 如果日誌組為空，則 CloudTrail 不會將事件傳遞到 CloudWatch。請檢查 `CloudTrailToCloudWatchRole` IAM 角色是否存在並具有 ``logs:CreateLogStream`` 和 ``logs:PutLogEvents`` 權限，並確保追蹤已使用正確的 ``CloudWatchLogsLogGroupArn`` 和 ``CloudWatchLogsRoleArn`` 進行設定。
- 如果種子事件出現在日誌群組中，則問題出在下游 — 繼續執行步驟 3。

3. 請查看 S3 Tables 表格(`aws-cloudwatch`)。

`S3TableIntegration` 會自動建立一個名為 `aws-cloudwatch` 的表格儲存桶，並在 `logs.aws_cloudtrail__data` 中填入一個表格。此表格僅在第一個事件流過後才會建立。

- 如果 `aws-cloudwatch` 表格儲存桶不存在，則 `S3TableIntegrationRole` 缺少權限。它需要 ``s3tables:CreateTableBucket``、``s3tables:PutTableBucketEncryption`` 和 ``s3tables:PutTableBucketPolicy`` — 所有這些權限都限定在 ``arn:aws:s3tables:*:*:bucket/aws-cloudwatch`` 範圍內。
- 如果表格儲存桶存在但 ``logs.aws_cloudtrail__data`` 未顯示，則整合未路由事件。整合必須顯示 ``Status: ACTIVE`` 並將 ``aws_cloudtrail`` 作為日誌來源。
- 如果表存在但種子事件不在其中，則該事件可能仍在傳輸中。S3 Tables 資料導入有一定的延遲。請稍等

幾分鐘。如果 15-20 分鐘後仍未出現，則整合可能已中斷。

4. 直接查詢種子事件。

- 在 AWS Management Console 中開啟 S3 Tables。
- 導覽至 aws-cloudwatch 表格儲存桶 → aws_cloudtrail__data 表格，然後使用 **Preview** 按鈕直接在瀏覽器中執行快速查詢。
- 如果事件已存在於表中，但日誌仍顯示 `FAILED`，則可能是輪詢視窗在事件到達之前已過期。

解決問題後，返回 Workload Factory 主控台。再次提交 Trail ARN 以重試 [啟動日誌表設定](#)。

- 如果設定仍然失敗，請聯絡 NetApp 支援以尋求協助。

日誌表設定的權限參考

用於部署 CloudFormation 堆疊以啟用 Journal 表功能的 IAM 角色需要下列權限。請參閱 [開始之前](#) 以取得包含所需權限的可複製 JSON 策略。

堆疊操作

權限	資源	為什麼
cloudformation : CreateStack	arn:aws:cloudformation:*:*:stack/netapp-metadata-/*	建立堆疊
cloudformation : DescribeStacks	arn:aws:cloudformation:*:*:stack/netapp-metadata-/*	監控堆疊狀態
cloudformation : DescribeStackEvents	arn:aws:cloudformation:*:*:stack/netapp-metadata-/*	診斷資源層級故障 cloudformation:GetTemplateSummary * 預檢範本驗證

CloudTrail

權限	資源	為什麼
cloudtrail : CreateTrail	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	建立追蹤
cloudtrail : StartLogging	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	啟用記錄
cloudtrail : AddTags	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	套用識別標籤
cloudtrail : PutEventSelectors	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	設定資料事件擷取
cloudtrail : DescribeTrails	*	解析堆疊輸出的追蹤 ARN

S3

權限	資源	為什麼
s3 : CreateBucket	arn:aws:s3:::netapp-metadata-*	建立 CloudTrail 日誌儲存貯體

權限	資源	為什麼
s3 : PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	允許 CloudTrail 寫入日誌
s3 : PutBucketTagging	arn:aws:s3:::netapp-metadata-*	套用識別標籤

IAM

權限	資源	為什麼
iam : CreateRole	arn:aws:iam::*:role/netapp-metadata-*	建立兩個 IAM 角色
iam : PutRolePolicy	arn:aws:iam::*:role/netapp-metadata-*	附加內嵌原則
iam : TagRole	arn:aws:iam::*:role/netapp-metadata-*	套用識別標籤
iam : GetRole	arn:aws:iam::*:role/netapp-metadata-*	確認角色處於作用中狀態
iam : PassRole	arn:aws:iam::*:role/netapp-metadata-* (條件 : PassedToService = cloudtrail.amazonaws.com 、 logs.amazonaws.com)	傳遞角色至 CloudTrail 和 CloudWatch Logs

CloudWatch 日誌

權限	資源	為什麼
日誌 : CreateLogGroup	arn:aws:logs::*:log-group:netapp-metadata-*	建立日誌群組
日誌:DeleteLogGroup	arn:aws:logs::*:log-group:netapp-metadata-*	如果建立失敗，請清理日誌群組
日誌 : PutRetentionPolicy	arn:aws:logs::*:log-group:netapp-metadata-*	設定 30 天保留期
日誌 : TagResource	arn:aws:logs::*:log-group:netapp-metadata-*	套用識別標籤
logs:AssociateSourceToS3TableIntegration	arn:aws:logs::*:log-group:netapp-metadata-*	將 CloudTrail 來源連結至 S3 Tables
日誌 : DescribeLogGroups	*	檢查日誌群組是否存在
logs:ListSourcesForS3TableIntegration	*	確認整合關聯

ObservabilityAdmin

權限	資源	為什麼
observabilityadmin:CreateS3TableIntegration	*	建立 CloudWatch → S3 Tables 橋接器

權限	資源	為什麼
observabilityadmin:GetS3TableIntegration	*	確認整合已啟動
observabilityadmin : TagResource	*	套用識別標籤
observabilityadmin : ListTagsForResource	*	漂移偵測

S3 資料表

權限	資源	為什麼
s3tables : CreateTableBucket	arn:aws:s3tables:*.:.bucket/aws-cloudwatch	建立 S3 Tables 儲存貯體 (透過整合角色)
s3tables : PutTableBucketEncryption	arn:aws:s3tables:*.:.bucket/aws-cloudwatch	設定 AES256 加密
s3tables : PutTableBucketPolicy	arn:aws:s3tables:*.:.bucket/aws-cloudwatch	允許 CloudWatch Logs 存取

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。