設定
ONTAP 9

NetApp
April 13, 2024

目錄

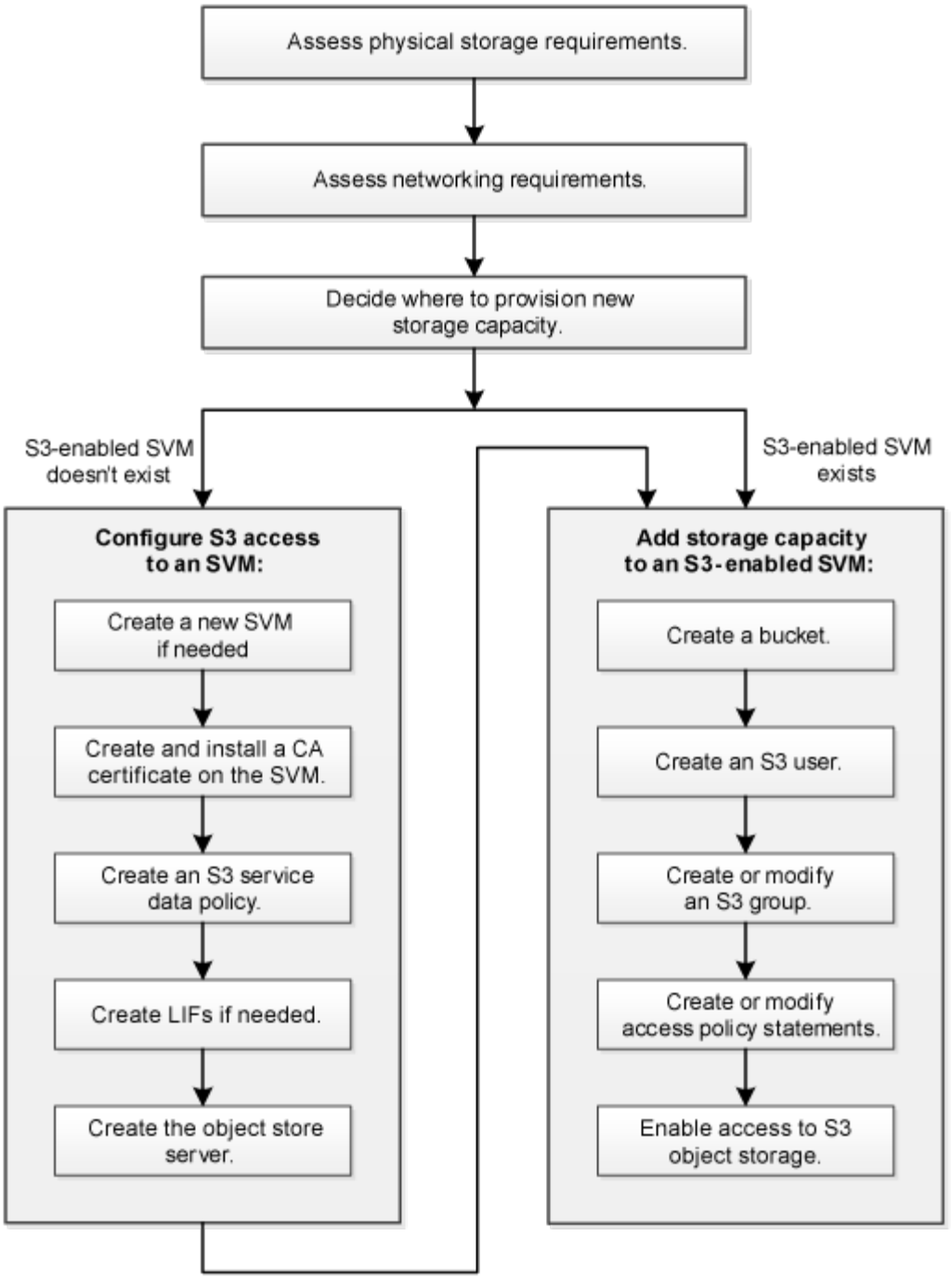
設定

關於**S3**組態程序

S3組態工作流程

設定S3需要評估實體儲存設備和網路需求、然後選擇專屬於您目標的工作流程、包括設定S3存取新的或現有的SVM、或是將儲存庫和使用者新增至已完全設定為S3存取的現有SVM。

當您使用System Manager設定S3存取新儲存VM時、系統會提示您輸入憑證和網路資訊、儲存VM和S3物件儲存伺服器會在單一作業中建立。



評估實體儲存需求

在為用戶端配置S3儲存設備之前、您必須確保現有集合體中有足夠空間可用於新的物件存放區。如果沒有、您可以將磁碟新增至現有的Aggregate、或建立所需類型和位置的新Aggregate。

關於這項工作

當您在啟用S3的SVM中建立S3儲存區時、FlexGroup 會自動建立一個支援儲存區的功能。您可以ONTAP Select自動讓底層的Aggregate和FlexGroup 架構元件（預設值）使用、也可以FlexGroup 自行選擇底層的Aggregate和架構元件。

如果您決定指定Aggregate和FlexGroup 等元件（例如、如果您對基礎磁碟有特定的效能要求）、您應該確定您的Aggregate組態符合配置FlexGroup 一個可靠的實務做法準則。深入瞭解：

- "資料區管理FlexGroup"
- "NetApp技術報告4571-A：NetApp ONTAP FlexGroup 《關於NetApp的最新資訊》最佳實務做法"

如果您是供應Cloud Volumes ONTAP 來自於整個過程的貯體、強烈建議您手動選取基礎Aggregate、以確保它們僅使用一個節點。使用兩個節點的集合體可能會影響效能、因為節點將位於不同地理位置的可用度區域、因此容易受到延遲問題的影響。 深入瞭解 "打造庫位以供Cloud Volumes ONTAP 使用"。

您可以使用ONTAP VMware S3伺服器來建立本機FabricPool 的功能性分層、也就是在效能層所在的同一個叢集內。舉例來說、如果您將SSD磁碟連接至一個HA配對、而且想要將_Cold資料分層至另一個HA配對中的HDD磁碟、這項功能就很實用。在此使用案例中、S3伺服器和包含本機容量層的儲存區應該與效能層位於不同的HA配對中。單節點和雙節點叢集不支援本機分層。

步驟

1. 顯示現有Aggregate中的可用空間：

   ```
   storage aggregate show
   ```

   如果有一個具有足夠空間或必要節點位置的集合體、請記錄其S3組態名稱。

   ```
   cluster-1::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. 如果沒有具有足夠空間或必要節點位置的集合體、請使用將磁碟新增至現有的集合體 `storage aggregate add-disks` 或使用建立新的 Aggregate `storage aggregate create` 命令。

評估網路需求

將S3儲存設備提供給用戶端之前、您必須確認網路設定正確、以符合S3資源配置需求。

開始之前

必須設定下列叢集網路物件：

- 實體與邏輯連接埠
- 廣播網域
- 子網路（如有需要）
- IPspaces（視需要而定、除了預設IPspace）
- 容錯移轉群組（視需要、以及每個廣播網域的預設容錯移轉群組）
- 外部防火牆

關於這項工作

若要使用遠端FabricPool 的支援能力（雲端）階層和遠端S3用戶端、您必須使用資料SVM並設定資料生命量。對於架構雲端層、您也必須設定叢集間的生命體、不需要叢集對等。FabricPool

對於本機FabricPool 的功能區階層、您必須使用系統SVM（稱為「叢集」）、但LIF組態有兩種選項：

- 您可以使用叢集LIF。

  在此選項中、不需要進一步的LIF組態、但叢集生命期的流量會增加。此外、其他叢集也無法存取本機層級。

- 您可以使用資料和叢集間的LIF。

  此選項需要額外的組態、包括啟用S3傳輸協定的LIF、但也可將本機層作為遠端FabricPool 的異地雲端層存取至其他叢集。

步驟

1. 顯示可用的實體和虛擬連接埠：

   ```
   network port show
   ```

   - 如果可能、您應該使用資料網路速度最高的連接埠。
   - 資料網路中的所有元件必須具有相同的MTU設定、才能獲得最佳效能。

2. 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、請確認該子網路存在且有足夠的可用位址：

   ```
   network subnet show
   ```

   子網路包含屬於同一第3層子網路的IP位址集區。子網路是使用建立的 `network subnet create` 命令。

3. 顯示可用的IPspaces：

   ```
   network ipspace show
   ```

   您可以使用預設IPspace或自訂IPspace。

4. 如果您要使用IPv6位址、請確認叢集上已啟用IPv6：

   ```
   network options ipv6 show
   ```

如有需要、您可以使用啟用 IPv6 `network options ipv6 modify` 命令。

決定新**S3**儲存容量的配置位置

在建立新的S3儲存區之前、您必須先決定要將它放在新的或現有的SVM中。此決定決定決定您的工作流程。

選擇

- 如果您想要在未啟用S3的新SVM或SVM中配置儲存區、請完成下列主題中的步驟。

  "為S3建立SVM"

  "為S3建立儲存庫"

  雖然S3可以與NFS和SMB共存於SVM中、但如果符合下列其中一項條件、您可以選擇建立新的SVM：

  - 您是第一次在叢集上啟用S3。
  - 您在不想啟用S3支援的叢集中有現有的SVM。
  - 叢集中有一個或多個啟用S3的SVM、您想要另一個具有不同效能特性的S3伺服器。 在SVM上啟用S3之後、請繼續配置儲存區。
- 如果您想要在現有的S3型SVM上配置初始儲存區或其他儲存區、請完成下列主題中的步驟。

  "為S3建立儲存庫"

設定**S3**對**SVM**的存取

為**S3**建立**SVM**

雖然S3可以與SVM中的其他傳輸協定共存、但您可能想要建立新的SVM來隔離命名空間和工作負載。

關於這項工作

如果您僅從SVM提供S3物件儲存設備、則S3伺服器不需要任何DNS組態。不過、如果使用其他通訊協定、您可能會想要在SVM上設定DNS。

當您使用System Manager設定S3存取新儲存VM時、系統會提示您輸入憑證和網路資訊、儲存VM和S3物件儲存伺服器會在單一作業中建立。

範例 **1.** 步驟

系統管理員

您應準備好將S3伺服器名稱輸入為完整網域名稱（FQDN）、用戶端將使用此名稱來存取S3。S3伺服器FQDN不得以儲存區名稱開頭。

您應準備好輸入介面角色資料的IP位址。

如果您使用的是外部CA簽署的憑證、系統會在此程序期間提示您輸入；您也可以選擇使用系統產生的憑證。

1. 在儲存VM上啟用S3。

   a. 新增儲存VM：按一下「儲存設備>儲存**VM**」、然後按一下「新增」。

      如果這是沒有現有儲存VM的新系統：請按一下*儀表板>設定傳輸協定*。

   如果您要將S3伺服器新增至現有的儲存VM：請按一下「儲存設備>儲存**VM**」、選取儲存VM、按一下「設定」、然後按一下 ⚙ 低於* S3 *。

   a. 按一下「啟用**S2**」、然後輸入「S3伺服器名稱」。
   b. 選取憑證類型。

      無論您是選擇系統產生的憑證、或是自己的憑證、用戶端存取都必須使用此憑證。

   c. 輸入網路介面。
2. 如果您選取系統產生的憑證、則在確認建立新的儲存VM時、會看到憑證資訊。按一下「下載」並儲存以供用戶端存取。
   - 不會再顯示秘密金鑰。
   - 如果您再次需要憑證資訊：按一下*儲存設備>儲存設備VM*、選取儲存設備VM、然後按一下*設定*。

CLI

1. 確認叢集上的S3已獲得授權：

   ```
   system license show -package s3
   ```

   如果沒有、請聯絡您的銷售代表。

2. 建立SVM：

   ```
   vserver create -vserver <svm_name> -subtype default -rootvolume
   <root_volume_name> -aggregate <aggregate_name> -rootvolume-security
   -style unix -language C.UTF-8 -data-services <data-s3-server>
   -ipspace <ipspace_name>
   ```

- 使用的 UNIX 設定 `-rootvolume-security-style` 選項。
- 使用預設的 C.UTF-8 `-language` 選項。
- 。 `ipspace` 設定為選用項目。

3. 驗證新建立的SVM的組態和狀態：

```
vserver show -vserver <svm_name>
```

。 `Vserver Operational State` 欄位必須顯示 `running` 州/省。如果顯示 `initializing` 狀態、表示有些中繼作業（例如建立根磁碟區）失敗、您必須刪除 SVM 並重新建立它。

範例

下列命令會在IPspace ipspaceA中建立SVM以供資料存取：

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services _data-s3-server_ -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

下列命令顯示 SVM 是以 1 GB 的根磁碟區所建立、而且是自動啟動且位於中 `running` 州/省。根磁碟區具有預設的匯出原則、不含任何規則、因此根磁碟區在建立時不會匯出。根據預設、會建立 vsadmin 使用者帳戶、並位於中 `locked` 州/省。vsadmin角色會指派給預設的vsadmin使用者帳戶。

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                       Vserver Admin State: running
                 Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

在SVM上建立並安裝CA憑證

需要憑證授權單位（CA）憑證、才能啟用從S3用戶端到啟用S3的SVM的HTTPS流量。

關於這項工作

雖然可以將S3伺服器設定為僅使用HTTP、而且雖然可以設定不需CA憑證的用戶端、但最佳做法是使用ONTAP CA憑證來保護HTTPS流量。

本機分層使用案例不需要CA憑證、因為IP流量只會流經叢集生命體。

本程序中的指示將建立並安裝ONTAP 一個自我簽署的驗證書。也支援協力廠商提供的CA憑證；如需詳細資訊、請參閱系統管理員驗證文件。

"系統管理員驗證與RBAC"

請參閱 `security certificate` 手冊頁以瞭解其他組態選項。

步驟

1. 建立自我簽署的數位憑證：

`security certificate create -vserver svm_name -type root-ca -common-name ca_cert_name`

。 `-type root-ca` 選項會建立及安裝自我簽署的數位憑證、以作為憑證授權單位（ CA ）來簽署其他憑證。

。 `-common-name` 選項會建立 SVM 的憑證授權單位（ CA ）名稱、並在產生憑證的完整名稱時使用。

預設的憑證大小為2048位元。

範例

```
cluster-1::> security certificate create -vserver svm1.example.com -type
root-ca -common-name svm1_ca

The certificate's generated name for reference:
svm1_ca_159D1587CE21E9D4_svm1_ca
```

顯示憑證產生的名稱時、請務必儲存以供此程序的後續步驟使用。

2. 產生憑證簽署要求：

`security certificate generate-csr -common-name s3_server_name [additional_options]`

。 `-common-name` 簽署要求的參數必須是 S3 伺服器名稱（ FQDN ）。

如有需要、您可以提供SVM的位置和其他詳細資訊。

系統會提示您保留一份憑證要求和私密金鑰、以供日後參考。

3. 使用SVM_CA簽署CSR以產生S3伺服器的憑證：

`security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial ca_cert_serial_number [additional_options]`

輸入您在先前步驟中使用的命令選項：

- `-ca` — 您在步驟 1 中輸入的 CA 的一般名稱。
- `-ca-serial` — 步驟 1 中的 CA 序號。例如、如果CA憑證名稱為svm1_ca _159D1587CE21E9D4_svm1_ca、序號為159D1587CE21E9D4。

  根據預設、簽署的憑證將於365天內到期。您可以選取其他值、並指定其他簽署詳細資料。

  出現提示時、複製並輸入您在步驟2中儲存的憑證要求字串。

隨即顯示已簽署的憑證、請儲存以供日後使用。

4. 在啟用S3的SVM上安裝簽署的憑證：

`security certificate install -type server -vserver svm_name`

出現提示時、請輸入憑證和私密金鑰。

如果需要憑證鏈結、您可以選擇輸入中繼憑證。

顯示私密金鑰和CA簽署的數位憑證時、請將其儲存以供日後參考。

5. 取得公開金鑰憑證：

`security certificate show -vserver svm_name -common-name ca_cert_name -type root-ca -instance`

儲存公開金鑰憑證以供稍後的用戶端組態使用。

範例

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
           FQDN or Custom Common Name: svm1_ca
          Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                  Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
               Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
                Certificate Start Date: Thu May 09 10:58:39 2020
           Certificate Expiration Date: Fri May 08 10:58:39 2021
                Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
                State or Province Name:
                         Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                              Protocol: SSL
                      Hashing Function: SHA256
                Self-Signed Certificate: true
       Is System Internal Certificate: false
```

建立S3服務資料原則

您可以為S3資料和管理服務建立服務原則。需要S3服務資料原則、才能在LIF上啟用S3資料流量。

關於這項工作

如果您使用資料生命體和叢集間生命體、則需要S3服務資料原則。如果您使用叢集生命體來處理本機分層使用案例、則不需要使用此功能。

當為LIF指定服務原則時、該原則會用來建構LIF的預設角色、容錯移轉原則和資料傳輸協定清單。

雖然可針對SVM和LIF設定多種傳輸協定、但在處理物件資料時、S3是唯一的傳輸協定、是最佳實務做法。

步驟

1. 將權限設定變更為進階：

   ```
   set -privilege advanced
   ```

2. 建立服務資料原則：

   ```
   network interface service-policy create -vserver svm_name -policy policy_name
   -services data-core,data-s3-server
   ```

   。 `data-core` 和 `data-s3-server` 雖然可視需要納入其他服務、但啟用 ONTAP S3 只需要服務。

建立資料生命量

如果您建立新的SVM、您為S3存取所建立的專屬lifs應該是資料lifs。

開始之前

- 基礎實體或邏輯網路連接埠必須已設定為系統管理 `up` 狀態。
- 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、則該子網路必須已經存在。

  子網路包含屬於同一第3層子網路的IP位址集區。它們是使用建立的 `network subnet create` 命令。

- LIF服務原則必須已經存在。

關於這項工作

- 您可以在同一個網路連接埠上同時建立IPV4和IPv6 LIF。
- 如果叢集中有大量的生命、您可以使用來驗證叢集上支援的 LIF 容量 `network interface capacity show` 命令和 LIF 容量、可透過使用在每個節點上支援 `network interface capacity details show` 命令（進階權限層級）。
- 如果您要啟用遠端FabricPool 的靜態容量（雲端）分層、則也必須設定叢集間的LIF。

步驟

1. 建立LIF：

   ```
   network interface create -vserver svm_name -lif lif_name -service-policy
   ```

service_policy_names -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address* | -subnet-name *subnet_name*} -firewall-policy data -auto-revert {true|false}

- -home-node 是 LIF 在返回時返回的節點 network interface revert 命令會在LIF上執行。

  您也可以指定 LIF 是否應該使用自動還原至主節點和主連接埠 -auto-revert 選項。

- -home-port 是 LIF 在時傳回的實體或邏輯連接埠 network interface revert 命令會在LIF上執行。
- 您可以使用指定 IP 位址 -address 和 -netmask 或是您可以使用從子網路進行分配 -subnet_name 選項。
- 使用子網路提供IP位址和網路遮罩時、如果子網路是使用閘道定義、則使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。
- 如果您手動指派IP位址（不使用子網路）、則在不同IP子網路上有用戶端或網域控制器時、可能需要設定通往閘道的預設路由。。 network route create 手冊頁包含在 SVM 中建立靜態路由的相關資訊。
- 適用於 -firewall-policy 選項、請使用相同的預設值 data 成為 LIF 角色。

  如果需要、您可以稍後建立並新增自訂防火牆原則。

  從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

- -auto-revert 可讓您指定資料 LIF 是否在啟動、管理資料庫狀態變更或建立網路連線等情況下自動還原至其主節點。預設設定為 false`但您可以將其設定為 `false 視環境中的網路管理原則而定。
- 。 -service-policy 選項會指定您建立的資料和管理服務原則、以及您需要的任何其他原則。

2. 如果您要在中指派 IPv6 位址 -address 選項：

   a. 使用 network ndp prefix show 用於查看在各種接口上學習的 RA 前綴列表的命令。

      。 network ndp prefix show 命令可在進階權限層級使用。

   b. 使用格式 prefix:id 手動建構 IPv6 位址。

      prefix 是在各種介面上學習的首碼。

   用於導出 id，選擇隨機 64 位元十六進位數字。

3. 使用確認 LIF 已成功建立 network interface show 命令。
4. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	network ping
IPv6位址	network ping6

範例

下列命令顯示如何建立指派給的 S3 資料 LIF `my-S3-policy` 服務原則：

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

下列命令顯示叢集1中的所有LIF。資料生命週期1和資料傳輸3均設定為使用IPv4位址、而資料傳輸4則設定為使用IPv6位址：

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

建立叢集間的生命體、以進行遠端**FabricPool** 分層

如果FabricPool 您使用ONTAP 支援使用支援的物件S3來啟用遠端的功能（雲端）分層、則必須設定叢集間的生命體。您可以在與資料網路共用的連接埠上設定叢集間的LIF。如此可減少叢集間網路所需的連接埠數量。

開始之前

- 基礎實體或邏輯網路連接埠必須已設定為系統管理 `up` 狀態。
- LIF服務原則必須已經存在。

關於這項工作

本機Fabric集區分層或外部S3應用程式不需要叢集間生命體。

步驟

1. 列出叢集中的連接埠：

   ```
   network port show
   ```

   下列範例顯示中的網路連接埠 `cluster01`：

   ```
   cluster01::> network port show
                                                                 Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

2. 在系統SVM上建立叢集間LIF：

   ```
   network interface create -vserver Cluster -lif LIF_name -service-policy
   default-intercluster -home-node node -home-port port -address port_IP -netmask
   netmask
   ```

   以下範例建立叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02`：

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. 驗證是否已建立叢集間的LIF：

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. 驗證叢集間的LIF是否為備援：

   `network interface show –service-policy default-intercluster -failover`

   以下範例顯示叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02` 在上 `e0c` 連接埠將容錯移轉至 `e0d` 連接埠。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

建立**S3**物件存放區伺服器

與由NAS和SAN伺服器提供的檔案或區塊儲存設備相比、物件儲存伺服ONTAP 器可將資料管理為S3物件ONTAP 。

開始之前

您應準備好將S3伺服器名稱輸入為完整網域名稱（FQDN）、用戶端將使用此名稱來存取S3。FQDN不得以儲存區名稱開頭。

您應該擁有自我簽署的CA憑證（在先前步驟中建立）或由外部CA廠商簽署的憑證。本機分層使用案例不需要CA憑證、因為IP流量只會流經叢集生命體。

關於這項工作

建立物件存放區伺服器時、會建立一個具有UID 0的root使用者。不會為此root使用者產生存取金鑰或秘密金鑰。ONTAP 管理員必須執行 `object-store-server users regenerate-keys` 命令來設定此使用者的存取金鑰和秘密金鑰。

NetApp最佳實務做法是、請勿使用此root使用者。任何使用root使用者存取金鑰或秘密金鑰的用戶端應用程式、都能完整存取物件存放區中的所有儲存區和物件。

請參閱 `vserver object-store-server` 手冊頁、瞭解其他組態和顯示選項。

範例 **2.** 步驟

系統管理員

如果您要將S3伺服器新增至現有的儲存VM、請使用此程序。若要將S3伺服器新增至新的儲存VM、請參閱"為S3建立儲存SVM"。

您應準備好輸入介面角色資料的IP位址。

1. 在現有的儲存VM上啟用S3。
   a. 選取儲存VM：按一下*儲存設備>儲存VM*、選取儲存VM、按一下*設定*、然後按一下 低於* S3 *。
   b. 按一下「啟用**S2**」、然後輸入「S3伺服器名稱」。
   c. 選取憑證類型。

      無論您是選擇系統產生的憑證、或是自己的憑證、用戶端存取都必須使用此憑證。

   d. 輸入網路介面。
2. 如果您選取系統產生的憑證、則在確認建立新的儲存VM時、會看到憑證資訊。按一下「下載」並儲存以供用戶端存取。
   - 不會再顯示秘密金鑰。
   - 如果您再次需要憑證資訊：按一下*儲存設備>儲存設備VM*、選取儲存設備VM、然後按一下*設定*。

CLI

1. 建立S3伺服器：

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   您可以在建立S3伺服器時或稍後隨時指定其他選項。

   - 如果您正在設定本機分層、 SVM 名稱可以是資料 SVM 或系統 SVM （叢集）名稱。
   - 憑證名稱應為伺服器憑證的名稱（終端使用者或葉憑證）、而非伺服器 CA 憑證（中繼或根 CA 憑證）。
   - 預設會在連接埠443上啟用HTTPS。您可以使用變更連接埠號碼 `-secure-listener-port` 選項。

     啟用 HTTPS 時、必須有 CA 憑證才能與 SSL/TLS 正確整合。

   - HTTP 預設為停用。啟用時、伺服器會在連接埠 80 上接聽。您可以使用啟用 `-is-http-enabled` 或使用變更連接埠編號 `-listener-port` 選項。

     啟用 HTTP 時、要求和回應會以純文字透過網路傳送。

2. 確認 S3 已設定：

   ```
   vserver object-store-server show
   ```

範例

此命令可驗證所有物件儲存伺服器的組態值：

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                   Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

將儲存容量新增至啟用S3的SVM

建立儲存庫

S3 物件保留在 _buckets 中。它們不是嵌套在其他目錄內的目錄內的檔案。

開始之前

包含 S3 伺服器的儲存 VM 必須已經存在。

關於這項工作

- 從 ONTAP 9.14.1 開始、在 S3 FlexGroup 磁碟區上建立貯體時、已啟用自動調整大小功能。如此可避免在現有和新的 FlexGroup 磁碟區上建立貯體時過度分配容量。根據下列準則、 FlexGroup 磁碟區的大小會調整為所需的最小大小。所需的最小大小是 FlexGroup Volume 中所有 S3 儲存區的總大小。
  - 從 ONTAP 9.14.1 開始、如果在建立新的儲存區時建立 S3 FlexGroup Volume 、則會以所需的最小大小建立 FlexGroup Volume 。
  - 如果在 ONTAP 9.14.1 之前建立 S3 FlexGroup Volume 、則在 ONTAP 9.14.1 之後建立或刪除的第一個儲存區、會將 FlexGroup 磁碟區調整為所需的最小大小。
  - 如果 S3 FlexGroup Volume 是在 ONTAP 9.14.1 之前建立的、而且已有最低需求大小、則在 ONTAP 9.14.1 之後建立或刪除儲存區、會維持 S3 FlexGroup 磁碟區的大小。
- 儲存服務層級是預先定義的調適性服務品質（QoS）原則群組、具有_value_、_Performance _和_Extreme _預設層級。您也可以定義自訂QoS原則群組、並將其套用至儲存區、而非預設的儲存服務層級之一。如需儲存服務定義的詳細資訊、請參閱 "儲存服務定義"。如需效能管理的詳細資訊、請參閱 "效能管理"。從ONTAP 供應儲存設備開始、預設會啟用QoS。您可以在資源配置程序期間或稍後停用QoS或選擇自訂QoS原則。
- 如果您正在設定本機容量分層、您可以在資料儲存 VM 中建立貯體和使用者、而不是在 S3 伺服器所在的系統儲存 VM 中建立。
- 若要進行遠端用戶端存取、您必須在啟用S3的儲存VM中設定儲存區。如果您在未啟用S3的儲存VM中建立

儲存貯體、則只能用於本機分層。

- 從 ONTAP 9.14.1 開始、您就可以了 "在 MetroCluster 組態中的鏡射或無鏡射 Aggregate 上建立貯體"。
- 在CLI中、當您建立儲存庫時、有兩種資源配置選項：
  - 讓ONTAP Select 底層的集合體和FlexGroup 元件不再存在（預設）
    - 透過自動選取集合體、即可為第一個儲存區建立及設定一個等量磁碟區。ONTAP FlexGroup它會自動選取適用於您平台的最高服務層級、或是您可以指定儲存服務層級。您稍後在儲存 VM 中新增的任何其他貯體、都會有相同的基礎 FlexGroup Volume 。
    - 或者、您也可以指定是否要使用儲存區進行分層、在這種情況ONTAP 下、VMware會嘗試選擇低成本的媒體、為階層式資料提供最佳效能。
  - 您可以選取基礎 Aggregate 和 FlexGroup 元件（需要進階權限命令選項）：您可以選擇手動選取必須建立儲存區和包含 FlexGroup 磁碟區的集合體、然後指定每個集合體的組成數量。新增其他庫位時：
    - 如果您為新的貯體指定集合體和成員、FlexGroup 將會為新的貯體建立新的功能區。
    - 如果您未指定新儲存區的集合體和成員、則新儲存區將會新增至現有FlexGroup 的版本資訊區。 請參閱 資料區管理FlexGroup 以取得更多資訊。

      當您在建立貯體時指定集合體和成員時、不會套用預設或自訂的QoS原則群組。您可以稍後使用來執行 `vserver object-store-server bucket modify` 命令。

    請參閱 "修改Vserver物件存放區伺服器儲存區" 以取得更多資訊。

*附註：*如果您是供應Cloud Volumes ONTAP 來自支援對象的鏟斗、則應使用CLI程序。強烈建議您手動選取基礎Aggregate、以確保它們僅使用一個節點。使用兩個節點的集合體可能會影響效能、因為節點將位於不同地理位置的可用度區域、因此容易受到延遲問題的影響。

使用 **ONTAP CLI** 建立 **S3** 儲存區

1. 如果您打算自行選取集合體和 FlexGroup 元件、請將權限等級設為進階（否則管理權限等級就足夠了）：`set -privilege advanced`
2. 建立儲存庫：

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

   儲存 VM 名稱可以是資料儲存 VM 、也可以是 `Cluster` （系統儲存 VM 名稱）（如果您正在設定本機分層）。

   如果您未指定任何選項、 ONTAP 會建立一個 800GB 儲存庫、並將服務層級設為系統可用的最高層級。

   如果您想ONTAP 要根據效能或使用量來建立儲存庫、請使用下列其中一個選項：

   - 服務層級

     包括 `-storage-service-level` 具有下列其中一個值的選項： `value`、 `performance`或 `extreme`。

   - 分層

包括 `-used-as-capacity-tier true` 選項。

如果您要指定要在其上建立基礎FlexGroup 的流通量的集合體、請使用下列選項：

- `-aggr-list` 參數指定用於 FlexGroup Volume 組成的集合體清單。

  清單中的每個項目都會在指定的Aggregate上建立一個組成項目。您可以多次指定集合體、以便在集合上建立多個成員。

為了在FlexGroup 整個Singfuse Volume中提供一致的效能、所有的集合體都必須使用相同的磁碟類型和RAID群組組組態。

- `-aggr-list-multiplier` 參數會指定在所列的集合體上重複的次數 `-aggr-list` 建立 FlexGroup Volume 時的參數。

  的預設值 `-aggr-list-multiplier` 參數為 4 。

3. 視需要新增QoS原則群組：

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   -group qos_policy_group
   ```

4. 確認儲存庫建立：

   ```
   vserver object-store-server bucket show [-instance]
   ```

範例

以下範例為儲存 VM 建立儲存區 `vs1` 大小 `1TB` 並指定 Aggregate ：

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

使用 **System Manager** 建立 **S3** 儲存區

1. 在啟用S3的儲存VM上新增儲存區。
   a. 按一下「儲存設備>桶」、然後按一下「新增」。
   b. 輸入名稱、選取儲存VM、然後輸入大小。
      - 如果您此時按一下*「儲存*」、就會以下列預設設定建立儲存區：
        - 除非任何群組原則已經生效、否則不會授予使用者桶的存取權。

          您不應該使用S3 root使用者來管理ONTAP 物件儲存設備並分享其權限、因為它對物件儲存區的存取權限不受限制。而是使用您指派的管理權限來建立使用者或群組。

        - 服務品質（效能）等級、是您系統可用的最高等級。
      - 按一下 * 儲存 * 以建立具有這些預設值的貯體。

設定其他權限和限制

您可以按一下「 * 更多選項 * 」來設定物件鎖定、使用者權限和效能層級的設定、或是稍後修改這些設定。

如果您打算使用S3物件存放區FabricPool 來進行分層、請考慮選擇*用於分層*（使用低成本媒體、為階層式資料提供最佳效能）、而非效能服務層級。

如果您想要啟用物件的版本設定以供稍後恢復、請選取 * 啟用版本管理 * 。如果您啟用貯體上的物件鎖定、預設會啟用版本設定。如需物件版本設定的相關資訊、請參閱 "在適用於 Amazon 的 S3 儲存區中使用版本設定"。

從 9.14.1 開始、 S3 儲存區支援物件鎖定。S3 物件鎖定需要標準 SnapLock 授權。本授權隨附於 "ONTAP One"。 在 ONTAP One 之前、 SnapLock 授權已包含在安全性與法規遵循套件中。安全性與法規遵循套件已不再提供、但仍有效。雖然目前並不需要、但現有客戶可以選擇 "升級至 ONTAP One"。 如果您要啟用貯體上的物件鎖定、您應該 "確認已安裝 SnapLock 授權"。如果未安裝 SnapLock 授權、您必須 "安裝" 您可以先啟用物件鎖定。 當您確認已安裝 SnapLock 授權時、若要保護您的儲存區中的物件、避免遭到刪除或覆寫、請選取 * 啟用物件鎖定 * 。鎖定功能可在所有或特定版本的物件上啟用、而且只有在叢集節點初始化 SnapLock 規範時鐘時才會啟用。請遵循下列步驟：

1. 如果未在叢集的任何節點上初始化 SnapLock 規範時鐘、則會出現 * 初始化 SnapLock 規範時鐘 * 按鈕。按一下 * 初始化 SnapLock Compliance Clock* 、初始化叢集節點上的 SnapLock 規範時鐘。
2. 選取 * Governance * 模式以啟動時間鎖定、允許對物件執行寫入一次、讀取多（ WORM ）權限。即使在 _Governance 模式中、具有特定權限的系統管理員使用者也可以刪除物件。
3. 如果您想要指派更嚴格的物件刪除和更新規則、請選取 * 符合性 * 模式。在此物件鎖定模式中、只有在指定的保留期間完成時、物件才能過期。除非指定保留期間、否則物件會無限期地保持鎖定。
4. 如果您希望鎖定在特定期間內生效、請指定鎖定的保留期限（以天或年為單位）。

鎖定適用於版本控制和非版本控制的 S3 貯體。物件鎖定不適用於 NAS 物件。

您可以為貯體設定保護和權限設定、以及效能服務層級。

您必須先建立使用者和群組、才能設定權限。

如需相關資訊、請參閱 "為新的儲存貯體建立鏡射"。

確認可存取貯體

在 S3 用戶端應用程式（無論是 ONTAP S3 或外部第三方應用程式）上、您可以輸入下列命令來驗證您對新建立的儲存區的存取：

- S3伺服器CA憑證。
- 使用者的存取金鑰和秘密金鑰。
- S3伺服器FQDN名稱和儲存區名稱。

在 **MetroCluster** 組態中的鏡射或無鏡射 **Aggregate** 上建立貯體

從 ONTAP 9.14.1 開始、您可以在 MetroCluster FC 和 IP 組態中的鏡射或無鏡射集合體上配置貯體。

關於這項工作

- 根據預設、儲存區會配置在鏡射的集合體上。
- 中所述的相同資源配置準則 "建立儲存庫" 適用於在 MetroCluster 環境中建立貯體。
- MetroCluster 環境 * 不 * 支援下列 S3 物件儲存功能：
  - S3 SnapMirror
  - S3 貯體生命週期管理
  - S3 物件鎖定在 * 符合性 * 模式

    支援 * Governance * 模式中的 S3 物件鎖定。

  - 本機 FabricPool 分層

開始之前

包含S3伺服器的SVM必須已經存在。

建立貯體的程序

CLI

1. 如果您打算自行選取集合體和 FlexGroup 元件、請將權限等級設為進階（否則管理權限等級就足夠了）：`set -privilege advanced`
2. 建立儲存庫：

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   設定 `-use-mirrored-aggregates` 選項 `true` 或 `false` 視您要使用鏡射或無鏡射的 Aggregate 而定。

   依預設 `-use-mirrored-aggregates` 選項設定為 `true`。

   - SVM 名稱必須是資料 SVM 。
   - 如果您未指定任何選項、 ONTAP 會建立一個 800GB 儲存庫、並將服務層級設為系統可用的最高層級。
   - 如果您想ONTAP 要根據效能或使用量來建立儲存庫、請使用下列其中一個選項：
     - 服務層級

       包括 `-storage-service-level` 具有下列其中一個值的選項： `value`、 `performance`或 `extreme`。

     - 分層

       包括 `-used-as-capacity-tier true` 選項。
   - 如果您要指定要在其上建立基礎FlexGroup 的流通量的集合體、請使用下列選項：
     - 。 `-aggr-list` 參數指定用於 FlexGroup Volume 組成的集合體清單。

       清單中的每個項目都會在指定的Aggregate上建立一個組成項目。您可以多次指定集合體、以便在集合上建立多個成員。

   為了在FlexGroup 整個Singfuse Volume中提供一致的效能、所有的集合體都必須使用相同的磁碟類型和RAID群組組態。

   - 。 `-aggr-list-multiplier` 參數會指定在所列的集合體上重複的次數 `-aggr-list` 建立 FlexGroup Volume 時的參數。

     的預設值 `-aggr-list-multiplier` 參數為 4 。
3. 視需要新增QoS原則群組：

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   -group qos_policy_group
   ```
4. 確認儲存庫建立：

```
vserver object-store-server bucket show [-instance]
```

範例

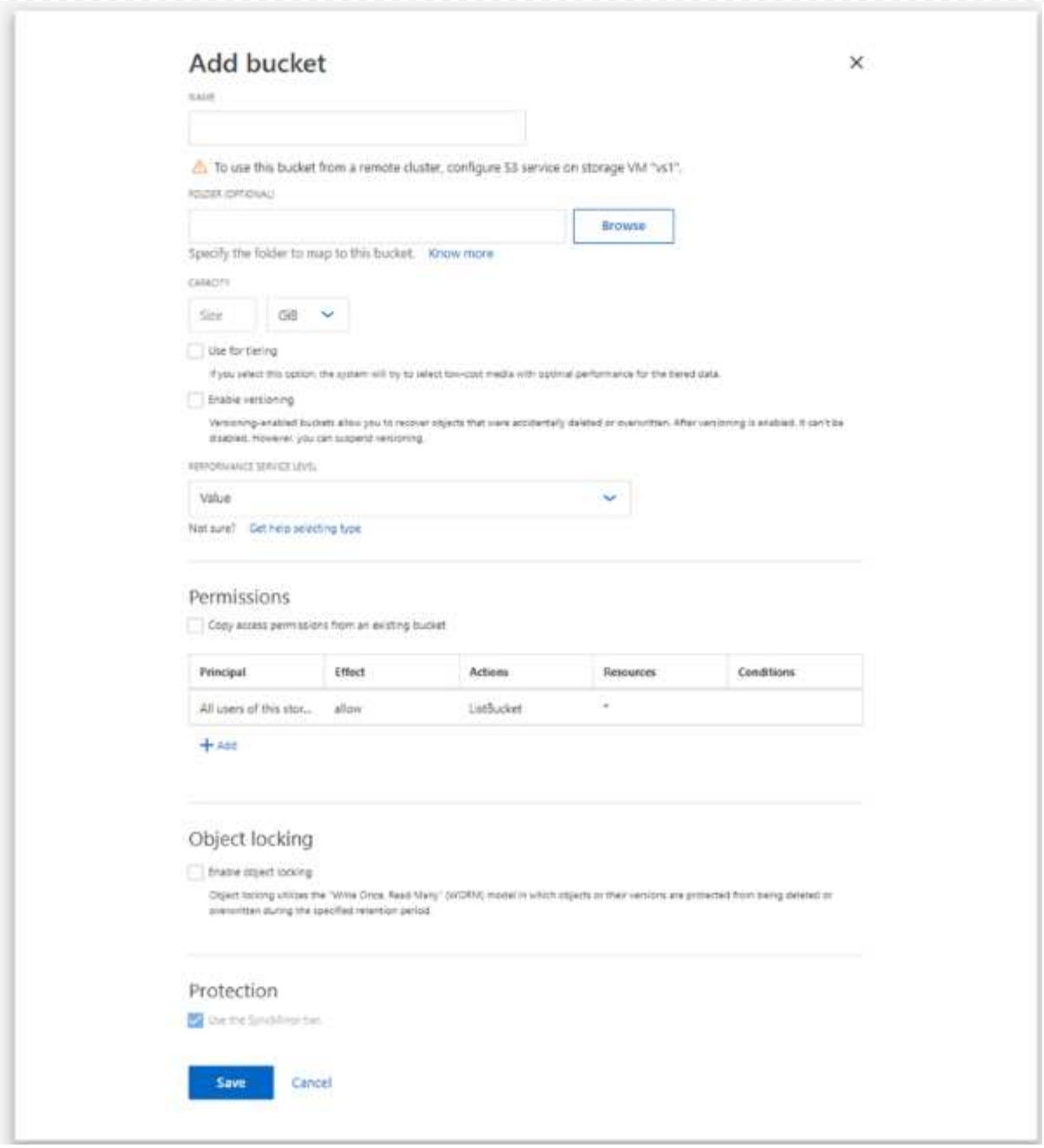
以下範例為鏡射集合體上大小為 1TB 的 SVM VS1 建立貯體：

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

系統管理員

1. 在啟用S3的儲存VM上新增儲存區。
   a. 按一下「儲存設備>桶」、然後按一下「新增」。
   b. 輸入名稱、選取儲存VM、然後輸入大小。

      根據預設、儲存區會配置在鏡射的 Aggregate 上。如果您想要在未鏡射的 Aggregate 上建立貯體、請選取 * 更多選項 * 、然後取消核取 * 保護 * 下的 * 使用 SyncMirror 垛層 * 方塊、如下圖所示：



- 如果您此時按一下*「儲存*」、就會以下列預設設定建立儲存區：
  - 除非任何群組原則已經生效、否則不會授予使用者桶的存取權。

> 您不應該使用S3 root使用者來管理ONTAP 物件儲存設備並分享其權限、因為它對物件儲存區的存取權限不受限制。而是使用您指派的管理權限來建立使用者或群組。

  - 服務品質（效能）等級、是您系統可用的最高等級。
- 您可以按一下*更多選項*來設定使用者權限和效能層級、或是稍後再修改這些設定。
  - 您必須先建立使用者和群組、才能使用*其他選項*來設定其權限。
  - 如果您打算使用S3物件存放區FabricPool 來進行分層、請考慮選擇*用於分層*（使用低成本媒體、為階層式資料提供最佳效能）、而非效能服務層級。

2. 在S3用戶端應用程式（另一個ONTAP 支援系統或外部協力廠商應用程式）上、輸入下列命令來驗證新儲存庫的存取：
   - S3伺服器CA憑證。
   - 使用者的存取金鑰和秘密金鑰。
   - S3伺服器FQDN名稱和儲存區名稱。

建立貯體生命週期管理規則

從 ONTAP 9.13.1 開始、您可以建立生命週期管理規則、以管理 S3 儲存區的物件生命週期。您可以定義貯體中特定物件的刪除規則、並透過這些規則將這些貯體物件過期。如此一來、您就能符合保留要求、並有效管理整個 S3 物件儲存。

如果您的貯體物件啟用物件鎖定、則物件到期的生命週期管理規則將不會套用至鎖定的物件。如需物件鎖定的相關資訊、請參閱 "建立儲存庫"。

開始之前

已啟用S3的SVM必須已存在S3伺服器和儲存區。請參閱 "為S3建立SVM" 以取得更多資訊。

關於這項工作

建立生命週期管理規則時、您可以將下列刪除動作套用至貯體物件：

- 刪除目前版本：此動作會使規則所識別的物件過期。如果在貯體上啟用版本設定、 S3 會使所有過期的物件無法使用。如果未啟用版本設定、則此規則會永久刪除物件。CLI 操作是 `Expiration`。
- 刪除非目前版本：此動作指定 S3 何時可永久移除非目前物件。CLI 操作是 `NoncurrentVersionExpiration`。
- 刪除過期的刪除標記 - 此動作會刪除過期的物件刪除標記。 在啟用版本設定的儲存區中、具有刪除標記的物件會成為物件的目前版本。物件不會被刪除、也無法對其執行任何動作。當沒有與這些物件相關的目前版本時、這些物件就會過期。CLI 操作是 `Expiration`。
- 刪除不完整的多部分上傳：此動作會設定允許多部分上傳保持進行中的最長時間（以天為單位）。之後將被刪除。CLI 操作是 `AbortIncompleteMultipartUpload`。

您遵循的程序取決於您使用的介面。使用 ONTAP 9.13 、 1 、您需要使用 CLI 。從 ONTAP 9.14.1 開始、您也可以使用系統管理員。

使用 **CLI** 管理生命週期管理規則

從 ONTAP 9.13.1 開始、您可以使用 ONTAP CLI 建立生命週期管理規則、使 S3 儲存區中的物件過期。

開始之前

對於 CLI 、您需要在建立貯體生命週期管理規則時、定義每個到期動作類型的必填欄位。這些欄位可在初始建立後修改。下表顯示每種行動類型的唯一欄位。

行動類型	唯一欄位

NonCurrentVersionExpiration	• `-non-curr-days` 刪除非目前版本的天數 • `-new-non-curr-versions` - 要保留的最新非最新版本數
過期	• `-obj-age-days` - 建立後的天數、之後可刪除物件的目前版本 • `-obj-exp-date` 物件到期的特定日期 • `-expired-obj-del-markers` - 清理物件刪除標記
AbortIncompleteMultiPart上 傳	• `-after-initiation-days` - 初始化的天數、之後可中止上傳

若要將貯體生命週期管理規則僅套用至特定物件子集、管理員必須在建立規則時設定每個篩選。如果在建立規則時未設定這些篩選條件、則規則會套用至貯體內的所有物件。

所有篩選器都可以在初始建立後修改、但下列項目除外：

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

步驟

1. 使用 `vserver object-store-server bucket lifecycle-management-rule create` 命令及到期動作類型的必填欄位、以建立您的貯體生命週期管理規則。

範例

下列命令會建立 NonCurrentVersionExpiration Bucket 生命週期管理規則：

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

範例

下列命令會建立到期庫位生命週期管理規則：

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

範例

下列命令會建立一個 AbortIncompleteMultpartUpload 貯體生命週期管理規則：

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

使用 **System Manager** 管理生命週期管理規則

從 ONTAP 9.14.1 開始、您可以使用系統管理員來過期 S3 物件。您可以新增、編輯及刪除 S3 物件的生命週期管理規則。此外、您可以匯入為一個貯體建立的生命週期規則、並將其用於其他貯體中的物件。您可以停用作用中規則、稍後再啟用。

新增生命週期管理規則

1. 按一下 * 儲存 > 鏟斗 * 。
2. 選取您要指定到期規則的貯體。
3. 按一下 ⋮ 圖示並選取 * 管理生命週期規則 * 。
4. 按一下 * 新增 > 生命週期規則 * 。
5. 在「新增生命週期規則」頁面上、新增規則名稱。
6. 定義規則的範圍、無論您想要規則套用至貯體中的所有物件、或是特定物件。如果您想要指定物件、請至少新增下列其中一個篩選條件：
   a. 字首：指定規則應套用的物件金鑰名稱前置字元。通常是物件的路徑或資料夾。您可以為每個規則輸入一個前置碼。除非提供有效的前置詞、否則規則會套用至貯體中的所有物件。
   b. 標籤：針對規則應套用的物件、指定最多三個金鑰和值配對（標籤）。只有有效的金鑰可用於篩選。此值為選用項目。不過、如果您新增值、請務必僅新增對應金鑰的有效值。
   c. 大小：您可以將範圍限制在物件的最小和最大大小之間。您可以輸入其中一個或兩個值。預設單位為 MIB 。
7. 指定動作：
   a. * 使物件的目前版本過期 * ：設定規則、使所有目前物件在建立後的特定天數或特定日期永遠無法使用。如果選取 * 刪除過期的物件刪除標記 * 選項、則無法使用此選項。

b. * 永久刪除非目前版本 * ：指定版本成為非目前版本的天數、之後可刪除的天數、以及要保留的版本數。

c. * 刪除過期的物件刪除標記 * ：選取此動作可刪除具有過期刪除標記的物件、亦即刪除沒有關聯目前物件的標記。

> 當您選取「 * 使物件的目前版本過期 * 」選項、並在保留期間之後自動刪除所有物件時、此選項將無法使用。使用物件標籤進行篩選時、也無法使用此選項。

d. * 刪除不完整的多部份上傳 * ：設定要刪除不完整多部份上傳的天數。如果在指定保留期間內進行中的多個部分上傳失敗、您可以刪除不完整的多個部分上傳。使用物件標籤進行篩選時、此選項將無法使用。

e. 按一下「 * 儲存 * 」。

匯入生命週期規則

1. 按一下 * 儲存 > 鏟斗 * 。
2. 選取您要匯入到期規則的貯體。
3. 按一下 ⋮ 圖示並選取 * 管理生命週期規則 * 。
4. 按一下 * 新增 > 匯入規則 * 。
5. 選取您要從中匯入規則的貯體。將顯示為所選儲存庫所定義的生命週期管理規則。
6. 選取您要匯入的規則。您可以選擇一次選取一個規則、預設選擇是第一個規則。
7. 按一下*匯入*。

編輯、刪除或停用規則

您只能編輯與規則相關的生命週期管理動作。如果使用物件標籤篩選規則、則無法使用 * 刪除過期物件刪除標記 * 和 * 刪除不完整的多部分上傳 * 選項。

當您刪除規則時、該規則將不再套用至先前關聯的物件。

1. 按一下 * 儲存 > 鏟斗 * 。
2. 選取您要編輯、刪除或停用生命週期管理規則的儲存區。
3. 按一下 ⋮ 圖示並選取 * 管理生命週期規則 * 。
4. 選取所需規則。您可以一次編輯及停用一個規則。您可以一次刪除多個規則。
5. 選取 * 編輯 * 、 * 刪除 * 或 * 停用 * 、然後完成程序。

建立**S3**使用者

所有 ONTAP 物件存放區都需要使用者授權、才能限制連線至授權用戶端。

開始之前。

啟用 S3 的儲存 VM 必須已經存在。

關於這項工作

S3 使用者可以存取儲存 VM 中的任何儲存區。當您建立 S3 使用者時、也會為使用者產生存取金鑰和秘密金鑰。應與使用者共用這些資源、以及物件存放區的 FQDN 和貯體名稱。S3 使用者的金鑰可以使用檢視

`vserver object-store-server user show` 命令。

您可以在儲存區原則或物件伺服器原則中、將特定的存取權限授予S3使用者。

> 當您建立新的物件存放區伺服器時、 ONTAP 會建立 root 使用者（ UID 0 ）、這是具有存取所有儲存區權限的使用者。NetApp 不建議以 root 使用者身分管理 ONTAP S3 、而是建議以特定權限建立管理員使用者角色。

CLI

1. 建立S3使用者：
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - 新增註解是選擇性的。
   - 從 ONTAP 9.14.1 開始、您可以定義金鑰在中有效的時間週期 `-key-time-to-live` 參數。您可以使用此格式新增保留期間、以指出存取金鑰過期的期間：
     `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
     例如、如果您想要輸入一天、兩小時、三分鐘和四秒的保留期間、請將值輸入為 `P1DT2H3M4S`。除非另有說明、金鑰的有效時間不限。

     以下範例建立名稱為的使用者 `sm_user1` 在儲存 VM 上 `vs0`，關鍵保留期為一週。

```
vserver object-store-server user create -vserver vs0 -user sm_user1
-key-time-to-live P1W
```

2. 請務必儲存存取金鑰和秘密金鑰。從 S3 用戶端進行存取時、需要使用這些資料。

系統管理員

1. 按一下「儲存設備>儲存設備**VM**」。選取您需要新增使用者的儲存 VM 、選取 * 設定 * 、然後按一下 在S3下。
2. 若要新增使用者、請按一下 * 使用者 > 新增 * 。
3. 輸入使用者名稱。
4. 從 ONTAP 9.14.1 開始、您可以指定為使用者建立之存取金鑰的保留期間。您可以指定金鑰自動過期的保留期間（以天、小時、分鐘或秒為單位）。依預設、此值設為 `0` 這表示金鑰無限期有效。
5. 按一下「 * 儲存 * 」。系統會建立使用者、並為使用者產生存取金鑰和秘密金鑰。
6. 下載或儲存存取金鑰和秘密金鑰。從 S3 用戶端進行存取時、需要使用這些資料。

後續步驟

- 建立或修改S3群組

建立或修改**S3**群組

您可以建立具有適當存取授權的使用者群組、以簡化儲存庫存取。

開始之前

啟用S3的SVM中的S3使用者必須已經存在。

關於這項工作

S3群組中的使用者可以被授予SVM中任何儲存區的存取權、但不能在多個SVM中存取。群組存取權限可透過兩種方式進行設定：

- 在鏟斗層級

  建立S3使用者群組之後、您可以在Bucket原則聲明中指定群組權限、這些權限只會套用至該儲存區。

- 在SVM層級

  建立S3使用者群組之後、您可以在群組定義中指定物件伺服器原則名稱。這些原則會決定群組成員的儲存區和存取權。

系統管理員

1. 編輯儲存虛擬機器：按一下*儲存設備>儲存虛擬機器*、按一下儲存虛擬機器、按一下*設定*、然後按一下 在S3下。
2. 新增群組：選取*群組*、然後選取*新增*。
3. 輸入群組名稱、然後從使用者清單中選取。
4. 您可以選取現有的群組原則或立即新增原則、也可以稍後新增原則。

CLI

1. 建立S3群組：
   `vserver object-store-server group create -vserver` *`svm_name`* `-name` *`group_name`* `-users` *`user_name\(s\)`* `[-policies` *`policy_names`*`] [-comment` *`text`*`\]`
   。 `-policies` 在物件存放區中只有一個儲存區的組態中、可以省略選項；群組名稱可以新增至儲存區原則。
   。 `-policies` 選項可在稍後隨一起新增 `vserver object-store-server group modify` 建立物件儲存伺服器原則之後的命令。

重新產生金鑰並修改其保留期間

使用者建立期間會自動產生存取金鑰和秘密金鑰、以啟用 S3 用戶端存取。如果金鑰過期或洩漏、您可以重新產生使用者的金鑰。

如需建立存取金鑰的相關資訊、請參閱 "建立S3使用者"。

CLI

1. 執行以重新產生使用者的存取和秘密金鑰 `vserver object-store-server user regenerate-keys` 命令。
2. 根據預設、產生的金鑰會無限期有效。從 9.14.1 開始、您可以修改金鑰的保留期間、之後金鑰會自動過期。您可以使用以下格式新增保留期間：
   `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
   例如、如果您想要輸入一天、兩小時、三分鐘和四秒的保留期間、請將值輸入為 `P1DT2H3M4S`。

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-time-to-live 0
   ```

3. 儲存存取和秘密金鑰。從 S3 用戶端進行存取時、需要使用這些資料。

系統管理員

1. 按一下「儲存設備>儲存設備**VM**」、然後選取儲存設備VM。
2. 在*設定*索引標籤中、按一下 在「* S3 *」方塊中。
3. 在 * 使用者 * 索引標籤中、確認沒有存取金鑰、或金鑰已過期。
4. 如果您需要重新產生金鑰、請按一下 按一下使用者旁邊的 * 重新產生 Key* 。
5. 根據預設、產生的金鑰在不確定的時間內有效。從 9.14.1 開始、您可以修改金鑰的保留期間、之後金鑰會自動過期。以天、小時、分鐘或秒為單位輸入保留期間。
6. 按一下「 * 儲存 * 」。金鑰即會重新產生。金鑰保留期間的任何變更都會立即生效。
7. 下載或儲存存取金鑰和秘密金鑰。從 S3 用戶端進行存取時、需要使用這些資料。

建立或修改存取原則聲明

關於儲存區和物件存放區伺服器原則

使用者和群組對S3資源的存取權是由儲存區和物件存放區伺服器原則所控制。如果您的使用者或群組數量不多、在庫位層級控制存取可能就足夠了、但如果您有許多使用者和群組、則更容易控制物件庫伺服器層級的存取。

修改庫位原則

您可以將存取規則新增至預設的儲存區原則。其存取控制的範圍是包含貯體的範圍、因此當有單一貯體時、最適合使用此功能。

開始之前

已啟用 S3 的儲存 VM 必須已存在、其中包含 S3 伺服器和儲存區。

在授予權限之前、您必須先建立使用者或群組。

關於這項工作

您可以為新使用者和群組新增聲明、也可以修改現有聲明的屬性。如需更多選項、請參閱 `vserver object-store-server bucket policy` 手冊頁。

使用者和群組權限可在建立儲存區時或稍後視需要授予。您也可以修改儲存區容量和QoS原則群組指派。

從 ONTAP 9.9.1 開始、如果您計畫在 ONTAP S3 伺服器上支援 AWS 用戶端物件標記功能、就會執行這些動作 `GetObjectTagging`、 `PutObjectTagging`和 `DeleteObjectTagging` 需要使用貯體或群組原則來允許。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

步驟

1. 編輯儲存桶：按一下「儲存設備>儲存桶」、按一下所需的儲存桶、然後按一下「編輯」。
新增或修改權限時、您可以指定下列參數：
   - 主要：授予存取權的使用者或群組。
   - * effect*：允許或拒絕存取使用者或群組。
   - 動作：特定使用者或群組的儲存庫允許動作。
   - 資源：儲存區內已授予或拒絕存取的物件路徑和名稱。

     預設值*_bucketname_*和*_bucketname/_會授予儲存區中所有物件的存取權。您也可以授與單一物件的存取權、例如***_Bucketname/_** readme.txt*。
   - 條件（選用）：嘗試存取時會評估的運算式。例如、您可以指定允許或拒絕存取的IP位址清單。

> 從 ONTAP 9.14.1 開始、您可以在 * 資源 * 欄位中指定貯體原則的變數。這些變數是預留位置、在評估原則時會以關聯式值取代。例如、 If `${aws:username}` 會指定為原則的變數、然後此變數會以要求內容使用者名稱取代、並可依照該使用者的設定來執行原則動作。

CLI

步驟

1. 在庫位政策中加入聲明：

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

下列參數定義存取權限：

`-effect`	此聲明可能允許或拒絕存取
`-action`	您可以指定 `*` 表示所有動作、或是下列一或多個動作清單： `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`,`GetObjectAcl`, `ListBucketMultipartUploads`, 和 `ListMultipartUploadParts`。
`-principal`	一或多個S3使用者或群組的清單。 • 最多可指定10個使用者或群組。 • 如果已指定 S3 群組、則該群組必須採用格式 `group/group_name`. • `*` 可以指定為公開存取、也就是說、無需存取金鑰和秘密金鑰即可存取。 • 如果未指定主體、則會授予儲存 VM 中的所有 S3 使用者存取權。

-resource	儲存區及其所包含的任何物件。萬用字元 * 和 ？可用於形成用於指定資源的規則運算式。對於資源、您可以在原則中指定變數。這些原則變數是預留位置、在評估原則時會以關聯式值取代。

您可以選擇性地指定文字字串做為的註解 -sid 選項。

範例

以下範例為儲存 VM svm1.example.com 和 Bucket1 建立物件儲存區伺服器貯體原則聲明、指定允許存取物件儲存區伺服器使用者使用者 1 的讀我資料夾。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

以下範例為儲存 VM svm1.example.com 和 Bucket1 建立物件儲存區伺服器貯體原則聲明、指定物件儲存區伺服器群組群組 1 的所有物件存取權。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

從 ONTAP 9.14.1 開始、您可以指定貯體原則的變數。以下範例為儲存 VM 建立伺服器儲存區原則聲明 svm1 和 bucket1`和指定 `${aws:username} 做為原則資源的變數。評估原則時、原則變數會以要求內容使用者名稱取代、並可依照該使用者的設定來執行原則動作。例如、評估下列原則陳述時、${aws:username} 替換為執行 S3 作業的使用者。如果是使用者 user1 執行作業時、會授予該使用者存取權 bucket1 做為 bucket1/user1/*。

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

建立或修改物件存放區伺服器原則

您可以建立可套用至物件存放區中一或多個儲存區的原則。物件存放區伺服器原則可附加至使用者群組、因此可簡化跨多個資源區的資源存取管理。

開始之前

已啟用S3的SVM必須已存在S3伺服器和儲存區。

關於這項工作

您可以在物件儲存伺服器群組中指定預設或自訂原則、以在SVM層級啟用存取原則。原則只有在群組定義中指定之後才會生效。

使用物件儲存伺服器原則時、您可以在群組定義中指定主體（即使用者和群組）、而非在原則本身中指定主體。

有三種唯讀的預設原則可供存取ONTAP 不完整的S3資源：

- FullAccess
- NoS3 存取
- ReadOnlyAccess

您也可以建立新的自訂原則、然後為新使用者和群組新增陳述式、或是修改現有陳述式的屬性。如需更多選項、請參閱 `vserver object-store-server policy` "命令參考資料"。

從 ONTAP 9.9.1 開始、如果您計畫在 ONTAP S3 伺服器上支援 AWS 用戶端物件標記功能、就會執行這些動作 `GetObjectTagging`、 `PutObjectTagging`和 `DeleteObjectTagging` 需要使用貯體或群組原則來允許。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**建立或修改物件存放區伺服器原則

步驟

1. 編輯儲存虛擬機器：按一下*儲存設備>儲存虛擬機器*、按一下儲存虛擬機器、按一下*設定*、然後按一下 在S3下。
2. 新增使用者：按一下*原則*、然後按一下*新增*。
   a. 輸入原則名稱、然後從群組清單中選取。
   b. 選取現有的預設原則或新增原則。

      新增或修改群組原則時、您可以指定下列參數：

      - 群組：授予存取權的群組。
      - 效果：允許或拒絕存取一或多個群組。
      - 行動：特定群組的一個或多個儲存桶中允許的行動。
      - 資源：一或多個儲存區內的物件路徑和名稱、這些儲存區已授予或拒絕存取權限。例如：
        - ***授予對儲存VM中所有儲存區的存取權。
        - * Bucketname*與* Bucketname/*可授予特定儲存區中所有物件的存取權。
        - * Bucketname/readme.txt*可讓您存取特定儲存區中的物件。
   c. 如有需要、請在現有原則中新增陳述式。

CLI

使用**CLI**建立或修改物件存放區伺服器原則

步驟

1. 建立物件儲存伺服器原則：

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. 建立原則聲明：

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   下列參數定義存取權限：

`-effect`	此聲明可能允許或拒絕存取

`-action`	您可以指定 * 表示所有動作、或是下列一或多個動作清單： `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads`，和 `ListMultipartUploadParts`。
`-resource`	儲存區及其所包含的任何物件。萬用字元 * 和 ？可用於形成用於指定資源的規則運算式。

您可以選擇性地指定文字字串做為的註解 `-sid` 選項。

根據預設、新的對帳單會新增至對帳單清單的結尾、並依順序處理。稍後新增或修改說明時、您可以選擇修改說明 `-index` 設定以變更處理順序。

設定外部目錄服務的 S3 存取

從 ONTAP 9.14.1 開始、外部目錄的服務已與 ONTAP S3 物件儲存設備整合。這項整合可透過外部目錄服務簡化使用者和存取管理。

您可以為屬於外部目錄服務的使用者群組提供存取 ONTAP 物件儲存環境的權限。輕量型目錄存取傳輸協定（ LDAP ）是與 Active Directory 等目錄服務進行通訊的介面、可為身分識別與存取管理（ IAM ）提供資料庫和服務。若要提供存取權、您必須在 ONTAP S3 環境中設定 LDAP 群組。設定存取權限之後、群組成員就擁有 ONTAP S3 工作區的權限。如需 LDAP 的相關資訊、請參閱 "使用LDAP的總覽"。

您也可以將 Active Directory 使用者群組設定為快速繫結模式、以便驗證使用者認證、並透過 LDAP 連線驗證協力廠商和開放原始碼 S3 應用程式。

開始之前

在設定 LDAP 群組及啟用群組存取的快速繫結模式之前、請先確認下列事項：

1. 已建立啟用 S3 的儲存 VM 、其中包含 S3 伺服器。請參閱 "為S3建立SVM"。
2. 該儲存 VM 中已建立一個儲存區。請參閱 "建立儲存庫"。
3. 在儲存 VM 上設定 DNS 。請參閱 "設定DNS服務"。
4. 儲存 VM 上會安裝 LDAP 伺服器的自我簽署根憑證授權單位（ CA ）憑證。請參閱 "在SVM上安裝自我簽署的根CA憑證"。
5. LDAP 用戶端在 SVM 上設定為啟用 TLS 。請參閱 "建立LDAP用戶端組態" 和 "將 LDAP 用戶端組態與 SVM 建立關聯以取得資訊"。

設定外部目錄服務的 S3 存取

1. 將 LDAP 指定為 SVM 的名稱服務資料庫 _ 、以用於群組、並將密碼指定為 LDAP ：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

如需此命令的詳細資訊、請參閱 "Vserver服務名稱服務ns交換器修改" 命令。

2. 使用建立物件儲存庫貯體原則聲明 `principal` 設定為您要授與存取權的 LDAP 群組：

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

範例：下列範例建立的 Bucket 原則陳述式 `buck1`。原則允許 LDAP 群組存取 `group1` 至資源（貯體及其物件） `buck1`。

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. 驗證 LDAP 群組中的使用者 `group1` 能夠從 S3 用戶端執行 S3 作業。

使用 **LDAP** 快速繫結模式進行驗證

1. 將 LDAP 指定為 SVM 的名稱服務資料庫 _ 、以用於群組、並將密碼指定為 LDAP ：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

如需此命令的詳細資訊、請參閱 "Vserver服務名稱服務ns交換器修改" 命令。

2. 確保存取 S3 儲存貯體的 LDAP 使用者具有在儲存庫原則中定義的權限。如需詳細資訊、請參閱 "修改庫位原則"。

3. 確認 LDAP 群組中的使用者可以執行下列作業：

   a. 以下列格式設定 S3 用戶端上的存取金鑰：
   `"NTAPFASTBIND" + base64-encode(user-name:password)`

範例： "NTAPFASTBIND" + base64 編碼（ LDAP 使用者：密碼）、結果是 NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=

> S3 用戶端可能會提示輸入秘密金鑰。如果沒有秘密金鑰、則可以輸入至少 16 個字元的任何密碼。

b. 從使用者具有權限的 S3 用戶端執行基本 S3 作業。

讓 LDAP 或網域使用者產生自己的 S3 存取金鑰

從 ONTAP 9.14.1 開始、身為 ONTAP 管理員、您可以建立自訂角色、並將其授予本機或網域群組或輕量型目錄存取傳輸協定（ LDAP ）群組、讓屬於這些群組的使用者能夠產生自己的存取權和機密金鑰、以供 S3 用戶端存取。

您必須在儲存 VM 上執行幾個組態步驟、才能建立自訂角色、並將其指派給啟動 API 以產生存取金鑰的使用者。

開始之前

請確認下列事項：

1. 已建立啟用 S3 的儲存 VM 、其中包含 S3 伺服器。請參閱 "為S3建立SVM"。
2. 該儲存 VM 中已建立一個儲存區。請參閱 "建立儲存庫"。
3. 在儲存 VM 上設定 DNS 。請參閱 "設定DNS服務"。
4. 儲存 VM 上會安裝 LDAP 伺服器的自我簽署根憑證授權單位（ CA ）憑證。請參閱 "在SVM上安裝自我簽署的根CA憑證"。
5. LDAP 用戶端在儲存 VM 上設定為啟用 TLS 。請參閱 "建立LDAP用戶端組態" 和。
6. 將用戶端組態與虛擬伺服器建立關聯。請參閱 "將LDAP用戶端組態與SVM建立關聯" 和 "Vserver服務名稱服務LDAP建立"。
7. 如果您使用的是資料儲存 VM 、請在 VM 上建立管理網路介面（ LIF ）、以及 LIF 的服務原則。請參閱 "建立網路介面" 和 "建立網路介面服務原則" 命令。

設定使用者以產生存取金鑰

1. 將 LDAP 指定為儲存 VM 的名稱服務資料庫 _ 、以用於群組和 LDAP 密碼：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

如需此命令的詳細資訊、請參閱 "Vserver服務名稱服務ns交換器修改" 命令。

2. 建立可存取 S3 使用者 REST API 端點的自訂角色：
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
在此範例中 `s3-role` 角色是針對儲存 VM 上的使用者所產生 `svm-1`，授予所有存取權限、讀取、建立及更

新。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

如需此命令的詳細資訊、請參閱 "建立安全登入REST角色" 命令。

3. 使用安全登入命令建立 LDAP 使用者群組、並新增新的自訂角色以存取 S3 使用者 REST API 端點。如需此命令的詳細資訊、請參閱 "建立安全登入" 命令。

```
security login create -user-or-group-name <ldap-group-name> -application
http -authentication-method nsswitch -role <custom-role-name> -is-ns
-switch-group yes
```

在此範例中、是 LDAP 群組 `ldap-group-1` 是在中建立的 `svm-1`以及自訂角色 `s3role` 新增至 IT 以存取 API 端點、並在快速繫結模式中啟用 LDAP 存取。

```
security login create -user-or-group-name ldap-group-1 -application http
-authentication-method nsswitch -role s3role -is-ns-switch-group yes
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

如需詳細資訊、請參閱 "使用LDAP快速連結進行Nsswitch驗證"。

將自訂角色新增至網域或 LDAP 群組、可讓該群組中的使用者有限存取 ONTAP `/api/protocols/s3/services/{svm.uuid}/users` 端點：透過叫用 API 、網域或 LDAP 群組使用者可以產生自己的存取權和秘密金鑰、以存取 S3 用戶端。他們只能為自己產生金鑰、而不能為其他使用者產生金鑰。

做為 **S3** 或 **LDAP** 使用者、產生您自己的存取金鑰

從 ONTAP 9.14.1 開始、如果您的系統管理員已授予您自行產生金鑰的角色、您就可以產生自己的存取權和秘密金鑰、以供存取 S3 用戶端。您只能使用下列 ONTAP REST API 端點自行產生金鑰。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。如需此端點其他方法的相關資訊、請參閱參考資料 "API 文件"。

HTTP方法	路徑
貼文	/api/protocols / s3/services / ｛ SVM.uuid ｝ / 使用者

Curl範例

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"_name_"}'
```

Json輸出範例

```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```

允許用戶端存取**S3**物件儲存設備

啟用**ONTAP** 對遠端**FabricPool** 分層的支援功能、以存取**S3**

若要將S3用作遠端的不同步容量（雲端）層、則必須由S3管理員向遠端的不同步叢集管理員提供S3伺服器組態的相關資訊。ONTAP FabricPool ONTAP ONTAP

關於這項工作

若要設定FabricPool SURE Cloud階層、必須提供下列S3伺服器資訊：

- 伺服器名稱（FQDN）
- 儲存區名稱
- CA憑證
- 存取金鑰
- 密碼（秘密存取金鑰）

此外、還需要下列網路組態：

- DNS ONTAP 伺服器中必須有一個遠端不完整的S3伺服器主機名稱項目、該伺服器是針對管理SVM設定的、包括S3伺服器的FQDN名稱及其lifs上的IP位址。
- 雖然不需要叢集對等、但必須在本機叢集上設定叢集間生命量。

請參閱FabricPool 《關於將ONTAP S3設定為雲端層的支援文件》。

"使用FabricPool 不實的功能來管理儲存設備層"

啟用**ONTAP** 對本地**FabricPool** 資訊的「支援」功能、以存取「**S3**」

若要將S3用作本地的「不支援能力」層、您必須根據建立的儲存區來定義物件存放區、然後將物件存放區附加至效能層集合體、以建立一個「不支援功能」ONTAP FabricPool FabricPool 。

開始之前

您必須擁有 ONTAP S3 伺服器名稱和貯體名稱、而且 S3 伺服器必須使用叢集生命體（搭配使用）建立 `-vserver Cluster` 參數）。

關於這項工作

物件存放區組態包含有關本機容量層的資訊、包括S3伺服器、儲存區名稱和驗證需求。

建立後的物件存放區組態不得重新關聯至不同的物件存放區或儲存區。您可以為本機層建立多個儲存區、但無法在單一儲存區中建立多個物件存放區。

本地容量層不需要使用此功能的證書。FabricPool

步驟

1. 建立本機容量層的物件存放區：

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - `-container-name` 是您建立的 S3 儲存區。
   - `-access-key` 參數會將要求授權給 ONTAP S3 伺服器。
   - `-secret-password` 參數（秘密存取金鑰）會驗證對 ONTAP S3 伺服器的要求。
   - 您可以設定 `-is-certificate-validation-enabled` 參數至 `false` 停用 ONTAP S3 的憑證檢查。

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipspace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

2. 顯示並驗證物件存放區組態資訊：

   `storage aggregate object-store config show`

3. 選用：若要查看磁碟區中有多少資料處於非使用中狀態、請依照中的步驟進行 "使用非作用中資料報告來判斷Volume中有多少資料處於非作用中狀態"。

   查看磁碟區中有多少資料處於非作用中狀態、有助於決定哪些Aggregate用於FabricPool 本地分層。

4. 將物件存放區附加至Aggregate：

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   您可以使用 `allow-flexgroup` **`true`** 可附加包含 FlexGroup Volume 成分的集合體。

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. 顯示物件存放區資訊、並驗證附加的物件存放區是否可用：

   `storage aggregate object-store show`

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
aggr1        MyLocalObjStore      available
```

從**S3**應用程式啟用用戶端存取

若要讓S3用戶端應用程式存取ONTAP S3伺服器、ONTAP 則該管理員必須向S3使用者提供組態資訊。

開始之前

S3用戶端應用程式必須能夠使用ONTAP 下列AWS簽名版本、使用支援驗證的功能：

- 簽名版本4 ONTAP 、更新版本
- 簽名版本2 ONTAP 、更新版本

其他的簽名版本不受ONTAP 支援。

此S3管理員必須已建立S3使用者、並在儲存區原則或物件儲存伺服器原則中、以個別使用者或群組成員的身分授予他們存取權限。ONTAP

S3用戶端應用程式必須能夠解析ONTAP 不支援的S3伺服器名稱、ONTAP 因為該名稱需要由S3管理員提供S3伺服器的正式作業的S3伺服器名稱（FQDN）和IP位址。

關於這項工作

若要存取ONTAP S3儲存區、S3用戶端應用程式的使用者會輸入ONTAP 由S3管理員提供的資訊。

從S9.9開始ONTAP 、ONTAP 支援下列AWS用戶端功能的不支援SS3伺服器：

- 使用者定義的物件中繼資料

  使用PUT（或POST）建立物件時、可將一組金鑰值配對指派給物件做為中繼資料。在物件上執行取得/取得作業時、會傳回使用者定義的中繼資料以及系統中繼資料。

- 物件標記

  您可以指派一組個別的金鑰值配對作為標籤、以便將物件分類。與中繼資料不同的是、標記是以物件的REST API獨立建立和讀取、而且會在物件建立或之後的任何時間執行。

> 若要讓用戶端取得及放置標記資訊、請採取行動 `GetObjectTagging`、`PutObjectTagging`和 `DeleteObjectTagging` 需要使用貯體或群組原則來允許。

如需詳細資訊、請參閱AWS S3文件。

步驟

1. 輸入S3伺服器名稱和CA憑證、以ONTAP 驗證S3用戶端應用程式與S3伺服器。
2. 輸入下列資訊、在S3用戶端應用程式上驗證使用者：
   - S3伺服器名稱（FQDN）和儲存區名稱
   - 使用者的存取金鑰和秘密金鑰

儲存服務定義

包含預先定義的儲存服務、這些服務會對應到對應的最低效能因素。ONTAP

叢集或SVM中可用的實際儲存服務集、取決於SVM中組成集合體的儲存設備類型。

下表顯示如何將最低效能因素對應至預先定義的儲存服務：

儲存服務	預期**IOPS**（**SLA**）	尖峰**IOPS**（**SLO**）	最小**Volume IOPS**	預估延遲	預期的**IOPS**是否強制執行？
價值	每 TB 128 個	每 TB 512 個	75	17 毫秒	在本網站上：是的AFF 否則：不會
效能	每TB 2048個	每 TB 4096 個	500	2 毫秒	是的
極致	每 TB 6144 個	每 TB 12288 個	1000	1 毫秒	是的

下表定義每種媒體或節點類型的可用儲存服務層級：

媒體或節點	可用的儲存服務層級
磁碟	價值
虛擬機器磁碟	價值
LUN FlexArray	價值
混合式	價值
容量最佳化的Flash	價值
固態硬碟（SSD）-非AFF	價值
效能最佳化的Flash - SSD（AFF VMware）	極致、效能、價值