瞭解NAS檔案存取

ONTAP 9

NetApp
April 24, 2024

目錄

瞭解NAS檔案存取

命名空間和交會點

命名空間與交會點總覽

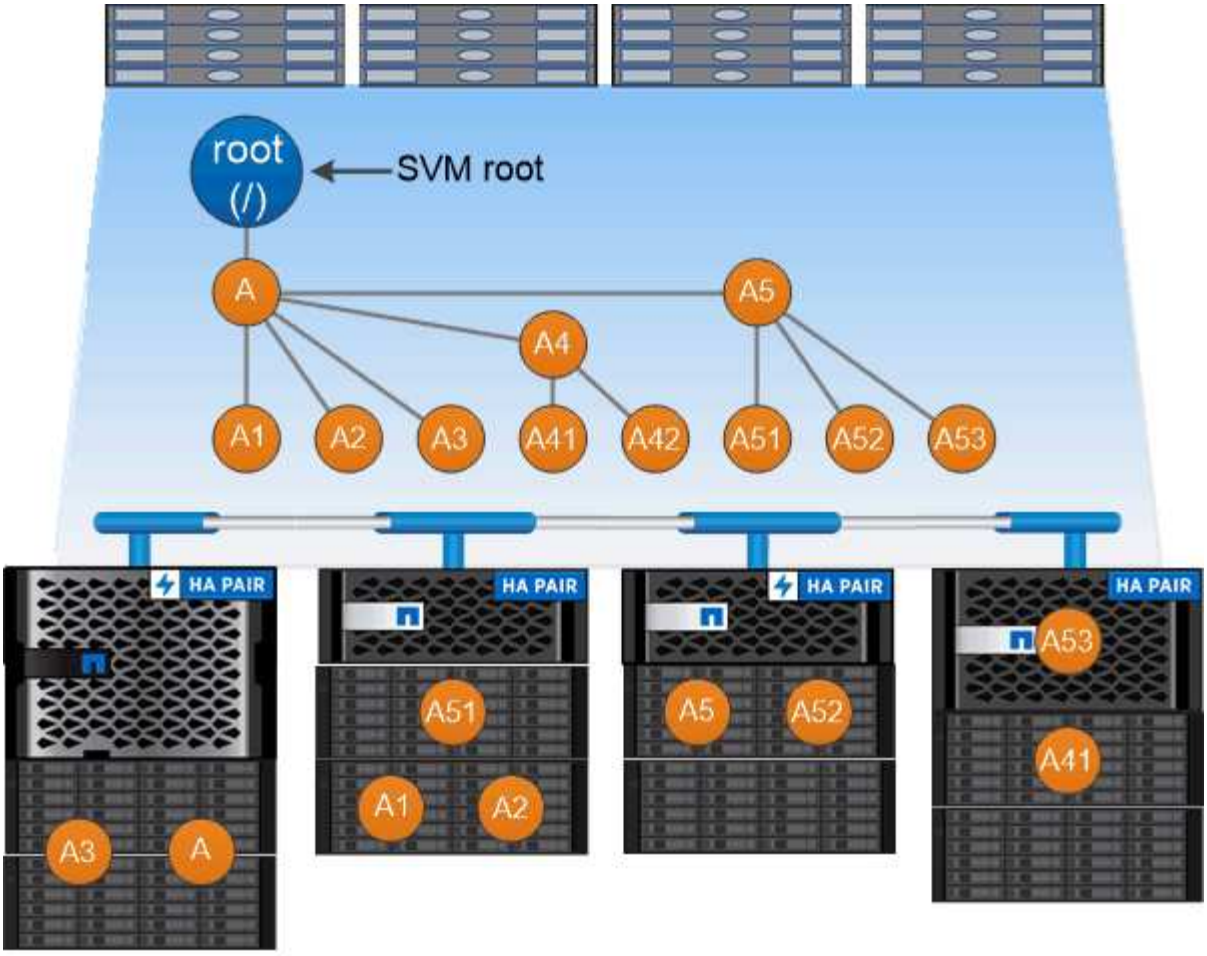
NAS *namespacity*_是一個邏輯群組、集合在_交會點、以建立單一檔案系統階層架構。具有足夠權限的用戶端可存取命名空間中的檔案、而無需指定檔案在儲存設備中的位置。未分段的磁碟區可位於叢集中的任何位置。

NAS用戶端不會掛載每個包含感興趣檔案的磁碟區、而是掛載NFS _EX出口_或存取SMB共享區。_匯出或共用區代表整個命名空間或命名空間內的中繼位置。用戶端只會存取裝載於其存取點下方的磁碟區。

您可以視需要將磁碟區新增至命名空間。您可以直接在父磁碟區交會下方或磁碟區內的目錄上建立交會點。名稱為「 'vol3' 」的 Volume 交會路徑可能是 `/vol1/vol2/vol3`或 `/vol1/dir2/vol3`或甚至 `/dir1/dir2/vol3`。路徑稱為_junction路徑。_

每個SVM都有一個獨特的命名空間。SVM根磁碟區是命名空間階層架構的起點。

> 為了確保資料在節點中斷或容錯移轉的情況下仍然可用、您應該為SVM根磁碟區建立_load-sharing mirror _複本。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

範例

以下範例建立一個名為「 'home4' 」的 Volume 、該 Volume 位於 SVM VS1 上、且具有交會路徑 `/eng/home` ：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

典型的NAS命名空間架構是什麼

您可以在建立SVM名稱空間時、使用幾種典型的NAS命名空間架構。您可以選擇符合業務和工作流程需求的命名空間架構。

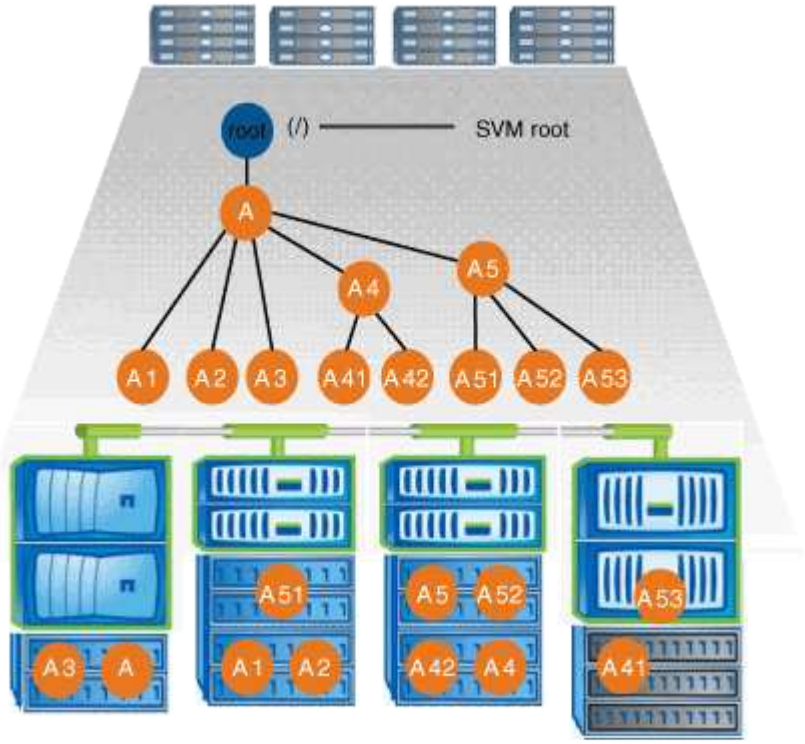
命名空間的頂端永遠是根磁碟區、以斜槓（/）表示。根目錄下的命名空間架構可分為三個基本類別：

- 單一分支樹狀結構、只有一個連接點可連接至命名空間的根
- 多個分支樹狀結構、並有多個交會點指向命名空間的根目錄

- 多個獨立磁碟區、每個磁碟區都有一個指向名稱空間根的獨立交會點

具有單一分支樹狀結構的命名空間

具有單一分支樹狀結構的架構具有單一插入點、可插入SVM命名空間的根目錄。單一插入點可以是輔助磁碟區、也可以是根目錄下的目錄。所有其他磁碟區都會安裝在單一插入點下方的交會點（可以是磁碟區或目錄）。

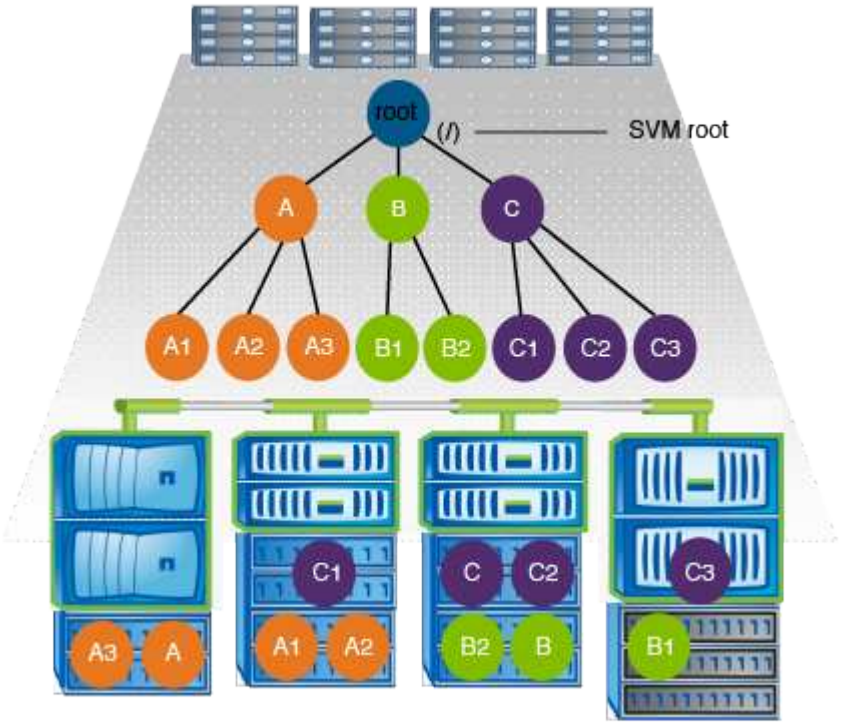


例如、具有上述命名空間架構的典型Volume交會組態可能類似下列組態、其中所有磁碟區都會連結到單一插入點下方、亦即名為「data'」的目錄：

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- --------------------     -----------
vs1     corp1        true     /data/dir1/corp1         RW_volume
vs1     corp2        true     /data/dir1/corp2         RW_volume
vs1     data1        true     /data/data1              RW_volume
vs1     eng1         true     /data/data1/eng1         RW_volume
vs1     eng2         true     /data/data1/eng2         RW_volume
vs1     sales        true     /data/data1/sales        RW_volume
vs1     vol1         true     /data/vol1               RW_volume
vs1     vol2         true     /data/vol2               RW_volume
vs1     vol3         true     /data/vol3               RW_volume
vs1     vs1_root     -        /                        -
```

具有多個分支樹狀結構的命名空間

具有多個分支樹狀結構的架構具有多個插入點、可插入到SVM命名空間的根目錄。插入點可以是輔助磁碟區、也可以是根目錄下的目錄。所有其他磁碟區都會安裝在插入點下方的交會點（可以是磁碟區或目錄）。

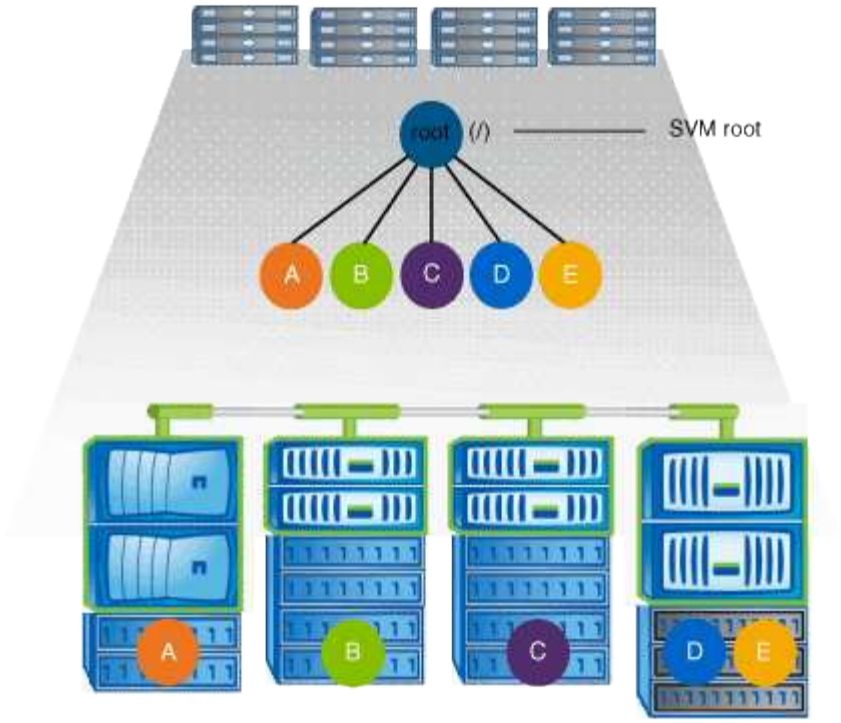


例如、具有上述命名空間架構的典型Volume交會組態可能類似下列組態、其中有三個插入點可插入SVM的根Volume。兩個插入點是名為「dATA」和「專案」的目錄。其中一個插入點是名為「稽核」的輔助磁碟區：

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- --------------------     -----------
vs1     audit         true     /audit                   RW_volume
vs1     audit_logs1   true     /audit/logs1             RW_volume
vs1     audit_logs2   true     /audit/logs2             RW_volume
vs1     audit_logs3   true     /audit/logs3             RW_volume
vs1     eng           true     /data/eng                RW_volume
vs1     mktg1         true     /data/mktg1              RW_volume
vs1     mktg2         true     /data/mktg2              RW_volume
vs1     project1      true     /projects/project1       RW_volume
vs1     project2      true     /projects/project2       RW_volume
vs1     vs1_root      -        /                        -
```

具有多個獨立磁碟區的命名空間

在具有獨立磁碟區的架構中、每個磁碟區都有一個插入點、指向SVM命名空間的根目錄、但是該磁碟區並未與另一個磁碟區連結。每個磁碟區都有一個獨特的路徑、可以直接連接到根目錄下方、也可以連接到根目錄下方的目錄下。



例如、具有上述命名空間架構的典型Volume交會組態可能類似下列組態、其中有五個插入點指向SVM的根Volume、每個插入點代表一個Volume的路徑。

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- --------------------     -----------
vs1     eng           true     /eng                     RW_volume
vs1     mktg          true     /vol/mktg                RW_volume
vs1     project1      true     /project1                RW_volume
vs1     project2      true     /project2                RW_volume
vs1     sales         true     /sales                   RW_volume
vs1     vs1_root      -        /                        -
```

如何控制對檔案的存取ONTAP

如何控制對檔案的存取總覽ONTAP

根據您指定的驗證型和檔案型限制、支援對檔案的存取。ONTAP

當用戶端連線至儲存系統以存取檔案時ONTAP 、必須執行兩項工作：

- 驗證

  透過驗證信任來源的身分識別、即可驗證用戶端。ONTAP此外、用戶端的驗證類型是一種方法、可用來判斷用戶端在設定匯出原則時是否能存取資料（CIFS為選用）。

- 授權

  透過比較使用者的認證資料與檔案或目錄上設定的權限、以及決定要提供的存取類型（如果有）、即可授權使用者。ONTAP

為了妥善管理檔案存取控制、ONTAP 必須與外部服務（例如NIS、LDAP和Active Directory伺服器）通訊。若要使用CIFS或NFS設定檔案存取的儲存系統、必須視ONTAP 您的環境而定、設定適當的服務。

驗證型限制

有了驗證型限制、您可以指定哪些用戶端機器、以及哪些使用者可以連線至儲存虛擬機器（SVM）。

支援UNIX和Windows伺服器的Kerberos驗證。ONTAP

檔案型限制

此功能可評估三種安全層級、以判斷實體是否有權針對位於SVM上的檔案和目錄執行要求的動作。ONTAP存取權取決於評估三種安全層級後的有效權限。

任何儲存物件最多可包含三種類型的安全層：

- 匯出（NFS）和共用（SMB）安全性

  匯出及共用安全性適用於用戶端存取特定NFS匯出或SMB共用區。具有管理權限的使用者可以從SMB和NFS用戶端管理匯出和共用層級的安全性。

- 儲存層級的存取保護檔案和目錄安全性

  儲存層級的存取保護安全性適用於存取SVM磁碟區的SMB和NFS用戶端。僅支援NTFS存取權限。為了對UNIX使用者執行安全性檢查、以存取已套用Storage Level Access Guard的磁碟區上的資料、UNIX使用者必須對應至擁有該磁碟區的SVM上的Windows使用者。ONTAP

  > 如果您從NFS或SMB用戶端檢視檔案或目錄的安全性設定、就不會看到儲存層級的存取保護安全性。即使是系統（Windows或UNIX）管理員、也無法從用戶端撤銷儲存層級的存取保護安全性。

- NTFS、UNIX及NFSv4原生檔案層級安全性

  代表儲存物件的檔案或目錄中存在原生檔案層級安全性。您可以從用戶端設定檔案層級的安全性。無論使用SMB或NFS存取資料、檔案權限都有效。

ONTAP 如何處理 NFS 用戶端驗證

如何處理NFS用戶端驗證總覽ONTAP

NFS用戶端必須經過適當驗證、才能存取SVM上的資料。利用您所設定的名稱服務來檢查UNIX認證、藉此驗證用戶端。ONTAP

當NFS用戶端連線至SVM時、ONTAP 根據SVM的名稱服務組態、透過檢查不同的名稱服務來取得使用者的UNIX認證。可檢查本機UNIX帳戶、NIS網域及LDAP網域的認證資料。ONTAP至少必須設定其中一項、ONTAP 才能讓支援中心成功驗證使用者。您可以指定多個名稱服務及ONTAP 其搜尋順序。

在純NFS環境中使用UNIX Volume安全性樣式、此組態足以驗證並為從NFS用戶端連線的使用者提供適當的檔案存取。

如果您使用混合、NTFS或統一磁碟區安全樣式、ONTAP 則必須為UNIX使用者取得SMB使用者名稱、才能使用Windows網域控制器進行驗證。這可能是因為使用本機UNIX帳戶或LDAP網域來對應個別使用者、或改用預設的SMB使用者。您可以指定ONTAP 名稱服務以何種順序搜尋、或指定預設的SMB使用者。

如何使用名稱服務ONTAP

使用名稱服務取得使用者和用戶端的相關資訊。ONTAP使用此資訊驗證使用者存取或管理儲存系統上的資料、並在混合式環境中對應使用者認證資料。ONTAP

當您設定儲存系統時、必須指定ONTAP 要使用哪些名稱服務來取得使用者認證以進行驗證。支援下列名稱服務：ONTAP

- 本機使用者（檔案）
- 外部NIS網域（NIS）
- 外部 LDAP 網域（ LDAP ）

您可以使用 `vserver services name-service ns-switch` 命令系列可將 SVM 設定為使用來源來搜尋網路資訊、以及搜尋這些資訊的順序。這些命令可提供的等效功能 `/etc/nsswitch.conf` UNIX 系統上的檔案。

當NFS用戶端連線至SVM時、ONTAP 此功能會檢查指定的名稱服務、以取得使用者的UNIX認證資料。如果名稱服務設定正確、ONTAP 而且能夠取得UNIX認證資料、ONTAP 則無法成功驗證使用者。

在混合式安全型態的環境中ONTAP 、可能必須對應使用者認證資料。您必須針對環境適當設定名稱服務、以便ONTAP 讓支援功能能夠正確對應使用者認證資料。

此外、還會使用名稱服務來驗證SVM系統管理員帳戶。ONTAP在設定或修改名稱服務交換器時、您必須謹記此點、以免意外停用SVM系統管理員帳戶的驗證。如需SVM管理使用者的詳細資訊、請參閱 "系統管理員驗證與RBAC"。

如何使用此功能、從NFS用戶端授予SMB檔案存取權限ONTAP

使用Windows NT檔案系統（NTFS）安全性語意、判斷UNIX使用者是否能在NFS用戶端上存取具有NTFS權限的檔案。ONTAP

為達成此目的、可將使用者的UNIX使用者ID（UID）轉換成SMB認證、然後使用SMB認證來驗證使用者是否擁有檔案的存取權限。ONTAPSMB認證包含主要安全性識別碼（SID）、通常是使用者的Windows使用者名稱、以及對應於使用者所屬Windows群組的一或多個群組SID。

將UNIX UID轉換為SMB認證所需的時間ONTAP 可從數十毫秒轉換為數百毫秒、因為此程序涉及連絡網域控制器。此功能可將UID對應至SMB認證、並在認證快取中輸入對應、以縮短轉換所造成的驗證時間。ONTAP

NFS認證快取的運作方式

當NFS使用者要求存取儲存系統上的NFS匯出時、ONTAP 必須從外部名稱伺服器或從本機檔案擷取使用者認證資料、才能驗證使用者。然後將這些認證資料儲存在內部認證快取中、以供日後參考。ONTAP瞭解NFS認證快取的運作方式、可讓您處理潛在的效能和存取問題。

如果沒有認證快取、ONTAP 每當NFS使用者要求存取時、就必須查詢名稱服務。在許多使用者存取的忙碌儲存系統上、這很快就會導致嚴重的效能問題、造成不必要的延遲、甚至使NFS用戶端存取遭到拒絕。

利用認證快取功能、ONTAP 當NFS用戶端傳送另一個要求時、將會擷取使用者認證資料、然後儲存預先決定的時間量、以便快速輕鬆地存取。此方法具有下列優點：

- 它可處理較少的外部名稱伺服器（例如NIS或LDAP）要求、進而減輕儲存系統的負載。
- 它能減少傳送要求給外部名稱伺服器的次數、進而減輕其負載。
- 它可免除從外部來源取得認證的等待時間、以便驗證使用者、進而加速使用者存取。

支援將正面和負面的認證資料儲存在認證快取中。ONTAP正向認證表示使用者已通過驗證並獲得存取權。負面認證表示使用者未通過驗證、因此被拒絕存取。

根據預設、ONTAP 將正向認證資料儲存24小時；也就是ONTAP 在初始驗證使用者之後、將快取認證資料用於該使用者24小時內的任何存取要求。如果使用者在24小時後要求存取、週期就會開始：ONTAP 由下列項目開始：循環捨棄快取的認證資料、並從適當的名稱服務來源再次取得認證資料。如果在過去24小時內、名稱伺服器上的認證有所變更、ONTAP 則會快取更新的認證資料、以供未來24小時使用。

根據預設、ONTAP 功能不正常的情況下、將負面認證資料儲存兩小時；也就是ONTAP 在一開始拒絕使用者存取之後、該使用者在兩小時內仍拒絕任何存取要求。如果使用者在2小時後要求存取、則週期將從下列項目開始：ONTAP 再次從適當的名稱服務來源取得認證。如果在過去兩小時內、名稱伺服器上的認證資料有所變更、ONTAP 則會快取更新的認證資料、以供未來兩小時使用。