設定名稱服務
ONTAP 9

NetApp
April 24, 2024

目錄

設定名稱服務

設定名稱服務總覽

根據儲存系統的組態、ONTAP 支援功能需要能夠查詢主機、使用者、群組或網路群組資訊、才能正確存取用戶端。您必須設定名稱服務、才能讓ONTAP 支援功能支援使用本機或外部名稱服務來取得此資訊。

您應該使用名稱服務（例如NIS或LDAP）、以便在用戶端驗證期間進行名稱查詢。最好盡可能使用LDAP來提高安全性、尤其是在部署NFSv4或更新版本時。如果外部名稱伺服器無法使用、您也應該設定本機使用者和群組。

名稱服務資訊必須在所有來源上保持同步。

設定名稱服務交換器表

您必須正確設定名稱服務交換器表、才能讓ONTAP 支援功能支援使用者參考本機或外部名稱服務、以擷取主機、使用者、群組、網路群組或名稱對應資訊。

您需要的產品

您必須決定要用於主機、使用者、群組、netgroup或名稱對應的名稱服務、以符合您的環境需求。

如果您打算使用netGroups、則必須依照RFC 5952中的指定、縮短及壓縮netGroups中指定的所有IPv6位址。

關於這項工作

請勿包含未使用的資訊來源。例如、如果您的環境中未使用 NIS 、請勿指定 `-sources nis` 選項。

步驟

1. 將必要的項目新增至名稱服務交換器表：

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. 驗證名稱服務交換器表格是否包含所需順序的預期項目：

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   如果您想要進行任何修正、您必須使用 `vserver services name-service ns-switch modify` 或 `vserver services name-service ns-switch delete` 命令。

範例

下列範例會在名稱服務交換器表中建立新項目、讓SVM VS1使用本機netgroup檔案和外部NIS伺服器、以該順序查詢netgroup資訊：

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

完成後

- 您必須設定您為SVM指定的名稱服務、才能提供資料存取。
- 如果您刪除SVM的任何名稱服務、也必須將其從名稱服務交換器表格中移除。

  如果您無法從名稱服務交換器表格中刪除名稱服務、用戶端對儲存系統的存取可能無法如預期般運作。

設定本機UNIX使用者和群組

設定本機UNIX使用者和群組總覽

您可以使用SVM上的本機UNIX使用者和群組進行驗證和名稱對應。您可以手動建立UNIX使用者和群組、也可以從統一資源識別元（URI）載入包含UNIX使用者或群組的檔案。

叢集中的本機UNIX使用者群組和群組成員、預設上限為32、768。叢集管理員可以修改此限制。

建立本機UNIX使用者

您可以使用 `vserver services name-service unix-user create` 建立本機UNIX 使用者的命令。本機UNIX使用者是您在SVM上建立的UNIX使用者、是UNIX名稱服務選項、用於處理名稱對應。

步驟

1. 建立本機UNIX使用者：

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* 指定使用者名稱。使用者名稱長度必須少於64個字元。

   `-id` *`integer`* 指定您指派的使用者 ID 。

   `-primary-gid` *`integer`* 指定主要群組 ID 。這會將使用者新增至主要群組。建立使用者之後、您可以手動將使用者新增至任何想要的其他群組。

範例

下列命令會在名為VS1的SVM上建立名為johnm（全名「John Miller」）的本機UNIX使用者。使用者的 ID 為 123 、主要群組 ID 為 100 。

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

從URI載入本機UNIX使用者

除了在 SVM 中手動建立個別的本機 UNIX 使用者之外、您也可以從統一的資源識別元（

URI）將本機 UNIX 使用者清單載入 SVM 、以簡化工作。（`vserver services name-service unix-user load-from-uri`）。

步驟

1. 建立包含您要載入之本機UNIX使用者清單的檔案。

   檔案必須包含 UNIX 中的使用者資訊 `/etc/passwd` 格式：

   `user_name: password: user_ID: group_ID: full_name`

   命令會捨棄的值 *`password`* 欄位和之後欄位的值 *`full_name`* 欄位（*`home_directory`* 和 *`shell`*）。

   支援的檔案大小上限為2.5 MB。

2. 確認清單中沒有任何重複資訊。

   如果清單包含重複的項目、則載入清單時會失敗並顯示錯誤訊息。

3. 將檔案複製到伺服器。

   儲存系統必須透過HTTP、HTTPS、FTP或FTPS連線至伺服器。

4. 判斷檔案的URI是什麼。

   URI是您提供給儲存系統的位址、用以指出檔案所在位置。

5. 從URI將包含本機UNIX使用者清單的檔案載入SVM：

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite {true false}` 指定是否覆寫項目。預設值為 `false`。

範例

下列命令會從 URI 載入本機 UNIX 使用者清單 `ftp://ftp.example.com/passwd` 進入名為 VS1 的 SVM 。SVM上的現有使用者不會被URI的資訊覆寫。

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

建立本機**UNIX**群組

您可以使用 `vserver services name-service unix-group create` 建立 SVM 本機 UNIX 群組的命令。本機UNIX群組適用於本機UNIX使用者。

步驟

1. 建立本機UNIX群組：

`vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

`-name` *`group_name`* 指定群組名稱。群組名稱長度必須少於64個字元。

`-id` *`integer`* 指定您指派的群組 ID 。

範例

下列命令會在名為VS1的SVM上建立名為eng的本機群組。群組的ID為101。

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

新增使用者至本機**UNIX**群組

您可以使用 `vserver services name-service unix-group adduser` 命令、將使用者新增至 SVM 本機的輔助 UNIX 群組。

步驟

1. 新增使用者至本機UNIX群組：

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* 指定要新增使用者的 UNIX 群組名稱、以及使用者的主要群組。

範例

下列命令會將名為max的使用者新增至名為VS1的SVM上名為eng的本機UNIX群組：

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

從**URI**載入本機**UNIX**群組

除了手動建立個別的本機 UNIX 群組之外、您也可以使用、從統一的資源識別元（URI）將本機 UNIX 群組清單載入 SVM `vserver services name-service unix-group load-from-uri` 命令。

步驟

1. 建立包含您要載入之本機UNIX群組清單的檔案。

   檔案必須包含 UNIX 中的群組資訊 `/etc/group` 格式：

   `group_name: password: group_ID: comma_separated_list_of_users`

命令會捨棄的值 *password* 欄位。

支援的檔案大小上限為 1 MB 。

群組檔案中每一行的長度上限為32、768個字元。

2. 確認清單中沒有任何重複資訊。

   清單不得包含重複的項目、否則載入清單將會失敗。如果 SVM 中已有項目、您必須設定 `-overwrite` 參數至 `true` 以新檔案覆寫所有現有項目、或確保新檔案不包含任何重複現有項目的項目。

3. 將檔案複製到伺服器。

   儲存系統必須透過HTTP、HTTPS、FTP或FTPS連線至伺服器。

4. 判斷檔案的URI是什麼。

   URI是您提供給儲存系統的位址、用以指出檔案所在位置。

5. 從URI將包含本機UNIX群組清單的檔案載入SVM：

   ```
   vserver services name-service unix-group load-from-uri -vserver vserver_name
   -uri {ftp|http|ftps|https}://uri -overwrite {true|false}
   ```

   `-overwrite true false}` 指定是否覆寫項目。預設值為 `false`。如果您將此參數指定為 `true`， ONTAP 會將指定 SVM 的整個現有本機 UNIX 群組資料庫，取代為您所載入檔案的項目。

範例

下列命令會從 URI 載入本機 UNIX 群組清單 `ftp://ftp.example.com/group` 進入名為 VS1 的 SVM 。SVM上的現有群組不會被URI的資訊覆寫。

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

使用netGroups

使用網路群組總覽

您可以使用netGroups進行使用者驗證、並在匯出原則規則中比對用戶端。您可以從外部名稱伺服器（ LDAP 或 NIS ）提供網路群組的存取權、也可以使用將網路群組從統一的資源識別碼（ URI ）載入 SVM `vserver services name-service netgroup load` 命令。

您需要的產品

在使用netGroups之前、您必須確保符合下列條件：

- 不論來源（NIS、LDAP或本機檔案）為何、網路群組中的所有主機都必須同時擁有轉送（A）和反向（PTr）DNS記錄、才能提供一致的轉送和反向DNS查詢。

此外、如果用戶端的IP位址有多筆PTr記錄、則所有這些主機名稱都必須是netgroup的成員、並具有對應的A記錄。

- 不論來源（NIS、LDAP或本機檔案）為何、netGroups中所有主機的名稱都必須正確拼寫、並使用正確的大小寫。在netGroups中使用的主機名稱若不一致、可能會導致非預期的行為、例如匯出檢查失敗。
- 在netGroups中指定的所有IPv6位址都必須依照RFC 5952中的指定來縮短和壓縮。

  例如、2011：hu9：0：0：0：0：3：1必須縮短為2011：hu9：3：1。

關於這項工作

使用netGroups時、您可以執行下列作業：

- 您可以使用 `vserver export-policy netgroup check-membership` 用於確定客戶端 IP 是否是某個 netgroup 的成員的命令。
- 您可以使用 `vserver services name-service getxxbyyy netgrp` 用於檢查用戶端是否為 netgroup 的一部分的命令。

  執行查詢的基礎服務是根據設定的名稱服務交換器順序來選取。

將網路群組載入SVM

您可以在匯出原則規則中使用符合用戶端的方法之一、就是使用netGroups中列出的主機。您可以將網路群組從統一的資源識別碼（URI）載入 SVM 、以取代使用儲存在外部名稱伺服器中的網路群組 (`vserver services name-service netgroup load`）。

您需要的產品

Netgroup檔案在載入SVM之前、必須符合下列要求：

- 檔案必須使用與NIS相同的適當netgroup文字檔格式。

  此功能可在載入netgroup文字檔格式之前檢查其內容。ONTAP如果檔案包含錯誤、則不會載入、並會顯示訊息、指出您必須在檔案中執行的修正。更正錯誤後、您可以將netgroup檔案重新載入指定的SVM。

- netgroup檔案中主機名稱中的任何字母字元都應為小寫。
- 支援的檔案大小上限為 5 MB 。
- 巢狀網路群組支援的最大層級為1000。
- 在netgroup檔案中定義主機名稱時、只能使用主要DNS主機名稱。

  為了避免匯出存取問題、不應使用DNS CNAME/或循環配置資源記錄來定義主機名稱。

- netgroup檔案中三個群組的使用者和網域部分應保持空白、因為ONTAP 無法支援它們。

  僅支援主機/IP部分。

關於這項工作

支援各主機的netgroup搜尋本機netgroup檔案。ONTAP載入netgroup檔案後ONTAP 、Syname會自動建立netgroup .byhost對應、以啟用逐主機的netgroup搜尋。這可大幅加速本機netgroup搜尋、以處理匯出原則規

則來評估用戶端存取。

步驟

1. 從URI將網路群組載入SVM：

   ```
   vserver services name-service netgroup load -vserver vserver_name -source
   {ftp|http|ftps|https}://uri
   ```

   載入netgroup檔案並建置netgroup。byhost對應可能需要數分鐘的時間。

   如果要更新netgroup、您可以編輯該檔案、然後將更新的netgroup檔案載入SVM。

範例

下列命令會從 HTTP URL 將 netgroup 定義載入名為 VS1 的 SVM `http://intranet/downloads/corp-netgroup`：

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

驗證netgroup定義的狀態

將網路群組載入 SVM 後、您可以使用 `vserver services name-service netgroup status` 用於驗證 netgroup 定義狀態的命令。這可讓您判斷支援SVM的所有節點上的netgroup定義是否一致。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 驗證netgroup定義的狀態：

   ```
   vserver services name-service netgroup status
   ```

   您可以在更詳細的檢視畫面中顯示其他資訊。

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

範例

設定權限層級後、下列命令會顯示所有SVM的netgroup狀態：

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

建立NIS網域組態

如果您的環境中使用網路資訊服務（NIS）來提供名稱服務、則必須使用為 SVM 建立 NIS 網域組態 `vserver services name-service nis-domain create` 命令。

您需要的產品

在SVM上設定NIS網域之前、所有已設定的NIS伺服器都必須可供使用且可連線。

如果您打算使用NIS進行目錄搜尋、則NIS伺服器中的對應每個項目不得超過1,024個字元。請勿指定不符合此限制的NIS伺服器。否則、用戶端存取相依於NIS項目可能會失敗。

關於這項工作

您可以建立多個NIS網域。不過、您只能使用設為的項目 `active`。

如果您的 NIS 資料庫包含 `netgroup.byhost` MAP 、 ONTAP 可以使用它來加快搜尋速度。。`netgroup.byhost` 和 `netgroup` 目錄中的地圖必須隨時保持同步、以避免用戶端存取問題。從 ONTAP 9.7 開始、 NIS `netgroup.byhost` 您可以使用快取項目 `vserver services name-service nis-domain netgroup-database` 命令。

不支援使用 NIS 進行主機名稱解析。

步驟

1. 建立NIS網域組態：

```
vserver services name-service nis-domain create -vserver vs1 -domain
domain_name -active true -servers IP_addresses
```

您最多可以指定10部NIS伺服器。

> 從 ONTAP 9.2 開始 `-nis-servers` 取代欄位 `-servers`。此新欄位可取得 NIS 伺服器的主機名稱或 IP 位址。

2. 確認網域已建立：

```
vserver services name-service nis-domain show
```

範例

下列命令會在SVM上建立名為nisDomain的NIS網域、並將其設為作用中NIS網域組態、該SVM名稱為VS1、其中NIS伺服器的IP位址為192.0.2.180：

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -active true -nis-servers 192.0.2.180
```

使用LDAP

使用LDAP的總覽

如果您的環境中使用LDAP來提供名稱服務、您必須與LDAP管理員合作、以判斷需求和適當的儲存系統組態、然後將SVM啟用為LDAP用戶端。

從ONTAP 功能支援的版本為：從功能支援的版本為：LDAP通道繫結、依預設會同時支援Active Directory和名稱服務LDAP連線。僅當啟用Start-TLS或LDAPS並將工作階段安全性設定為簽署或密封時、才能嘗試透過LDAP連線進行通道繫結。ONTAP若要停用或重新啟用與名稱伺服器的 LDAP 通道繫結、請使用 `-try-channel-binding` 參數 `ldap client modify` 命令。

如需詳細資訊、請參閱 "2020 LDAP通道繫結和LDAP簽署要求、適用於Windows"。

- 在設定LDAP ONTAP 以供使用之前、您應確認您的站台部署符合LDAP伺服器和用戶端組態的最佳實務做法。尤其必須符合下列條件：
  - LDAP伺服器的網域名稱必須符合LDAP用戶端上的項目。
  - LDAP伺服器支援的LDAP使用者密碼雜湊類型必須包含ONTAP 下列項目：
    - 加密（所有類型）和SHA-1（SHa、SSHA）。
    - 從ONTAP 《Sf9.8》、《SHA-2雜湊》（SHA-256、SSH-384、SHA-512、SSHA-256、 也支援SSHA-384和SSHA-512）。
  - 如果LDAP伺服器需要工作階段安全性措施、您必須在LDAP用戶端中進行設定。

    下列工作階段安全性選項可供使用：

    - LDAP簽署（提供資料完整性檢查）及LDAP簽署與密封（提供資料完整性檢查與加密）

        - 啟動TLS
        - LDAPS（LDAP over TLS或SSL）
    - 若要啟用已簽署和密封的LDAP查詢、必須設定下列服務：
        - LDAP伺服器必須支援GSPI（Kerberos）SASL機制。
        - LDAP伺服器必須在DNS伺服器上設定DNS A/AAAA記錄和PTr記錄。
        - Kerberos伺服器必須在DNS伺服器上存在SRV.記錄。
    - 若要啟用Start TLS或LDAPS、應考慮下列事項。
        - 使用Start TLS而非LDAPS是NetApp最佳實務做法。
        - 如果使用LDAPS、則LDAP伺服器必須在ONTAP 支援TLS或支援SSL的情況下、於支援更新版本的支援更新版本中啟用。不支援SSL。ONTAP
        - 必須已在網域中設定憑證伺服器。
    - 若要啟用LDAP參照追蹤（ONTAP 在更新版本的版本中）、必須滿足下列條件：
        - 這兩個網域都應設定下列其中一個信任關係：
            - 雙向
            - 單向、主要信任參照網域
            - 父-子
        - DNS必須設定為解析所有參照的伺服器名稱。
        - 網域密碼在-bind-as CIFS伺服器設定為true時、應相同進行驗證。

> LDAP參照追蹤不支援下列組態。
>
> - 所有ONTAP 版本：
> - 管理SVM上的LDAP用戶端
> - 適用於更新版本的支援功能（9.9.1及更新版本均支援）ONTAP ：
> - LDAP 簽署與密封（ `-session-security` 選項）
> - 加密 TLS 連線（ `-use-start-tls` 選項）
> - 透過 LDAPS 連接埠 636 （ `-use-ldaps-for-ad-ldap` 選項）

- 在SVM上設定LDAP用戶端時、您必須輸入LDAP架構。

  在大多數情況下、預設ONTAP 的架構之一將是適當的。不過、如果您環境中的LDAP架構與這些架構不同、則必須先建立新的LDAP用戶端架構ONTAP 以供使用、才能建立LDAP用戶端。請洽詢您的LDAP管理員、瞭解您環境的需求。

- 不支援使用LDAP進行主機名稱解析。

以取得更多資訊

- "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"
- "在SVM上安裝自我簽署的根CA憑證"

建立新的**LDAP**用戶端架構

如果您環境中的LDAP架構不同於ONTAP 支援功能的預設值、您必須先建立新的LDAP用戶端架構ONTAP 以供使用、才能建立LDAP用戶端組態。

關於這項工作

大多數LDAP伺服器都可以使用ONTAP 由下列功能提供的預設架構：

- ms-AD-BIS（大多數Windows 2012及更新版本AD伺服器的偏好架構）
- AD-IDMU（Windows 2008、Windows 2012及更新版本的AD伺服器）
- AD-SFU（Windows 2003和舊版AD伺服器）
- RFC-2307（UNIX LDAP伺服器）

如果您需要使用非預設LDAP架構、則必須先建立該架構、再建立LDAP用戶端組態。在建立新架構之前、請先諮詢您的LDAP管理員。

無法修改由功能提供的預設LDAP架構ONTAP 。若要建立新架構、請建立複本、然後據此修改複本。

步驟

1. 顯示現有的LDAP用戶端架構範本、以識別您要複製的範本：

   ```
   vserver services name-service ldap client schema show
   ```

2. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

3. 複製現有的LDAP用戶端架構：

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. 修改新的架構並針對您的環境自訂：

   ```
   vserver services name-service ldap client schema modify
   ```

5. 返回管理權限層級：

   ```
   set -privilege admin
   ```

建立**LDAP**用戶端組態

如果您想要 ONTAP 存取環境中的外部 LDAP 或 Active Directory 服務、則必須先在儲存系統上設定 LDAP 用戶端。

您需要的產品

Active Directory 網域解析清單中前三部伺服器之一必須為正常運作並提供資料。否則、此工作將會失敗。

有多部伺服器、其中有兩部以上的伺服器在任何時間點停機。

步驟

1. 請洽詢您的 LDAP 管理員、以決定的適當組態值 `vserver services name-service ldap client create` 命令：

   a. 指定與LDAP伺服器的網域型或位址型連線。

      - `-ad-domain` 和 `-servers` 選項是互斥的。

        - 使用 `-ad-domain` 在 Active Directory 網域中啟用 LDAP 伺服器探索的選項。

          - 您可以使用 `-restrict-discovery-to-site` 將 LDAP 伺服器探索限制在指定網域的 CIFS 預設網站的選項。如果使用此選項、您也需要使用指定 CIFS 預設站台 `-default-site`。

        - 您可以使用 `-preferred-ad-servers` 選項可依以逗號分隔的清單中的 IP 位址來指定一或多個偏好的 Active Directory 伺服器。建立用戶端之後、您可以使用修改此清單 `vserver services name-service ldap client modify` 命令。

        - 使用 `-servers` 選項可依以逗號分隔的清單中的 IP 位址來指定一或多個 LDAP 伺服器（Active Directory 或 UNIX）。

          - `-servers` ONTAP 9.2 中的選項已過時。從 ONTAP 9.2 開始 `-ldap-servers` 欄位會取代 `-servers` 欄位。此欄位可取得 LDAP 伺服器的主機名稱或 IP 位址。

   b. 指定預設或自訂LDAP架構。

      大多數LDAP伺服器都可以使用ONTAP 由功能介紹的預設唯讀架構。除非有其他需求、否則最好使用這些預設架構。如果是、您可以複製預設架構（它們是唯讀的）、然後修改複本、藉此建立自己的架構。

      預設架構：

      - MS-AD-BIS

        根據RFC-2307bis、這是大多數標準Windows 2012及更新版本LDAP部署的慣用LDAP架構。

      - `AD-IDMU`

        根據Active Directory Identity Management for UNIX、此架構適用於大多數Windows 2008、Windows 2012及更新的AD伺服器。

      - `AD-SFU`

        此架構以Active Directory Services for UNIX為基礎、適用於大多數Windows 2003和舊版AD伺服器。

      - `RFC-2307`

        根據RFC-2307（*an*方法使用*LDAP*做為網路資訊服務）、此架構適用於大多數UNIX AD伺服器。

   c. 選取「連結值」。

      - `-min-bind-level {anonymous|simple|sasl}` 指定最小繫結驗證層級。

預設值為 **anonymous**。

- `-bind-dn` *`LDAP_DN`* 指定綁定用戶。

  對於Active Directory伺服器、您必須在帳戶（網域\使用者）或主體（user@domain.com）表單中指定使用者。否則、您必須以辨別名稱（CN=user,DC=domain,DC=com）格式指定使用者。

- `-bind-password` *`password`* 指定綁定密碼。

d. 如有需要、請選取工作階段安全選項。

如果LDAP伺服器需要、您可以啟用LDAP簽署和密封、或透過TLS啟用LDAP。

- `--session-security {none|sign|seal}`

  您可以啟用簽署 (`sign`、資料完整性）、簽署及密封 (`seal``或兩者皆非 `none`、無簽署或密封）。預設值為 `none`。

  您也應該設定 `-min-bind-level {sasl}` 除非您想讓繫結驗證回復為 **anonymous** 或 **simple** 如果簽署和密封綁定失敗。

- `-use-start-tls {true|false}`

  如果設為 **true** LDAP 伺服器也支援此功能、 LDAP 用戶端會使用加密的 TLS 連線連線至伺服器。預設值為 **false**。您必須安裝LDAP伺服器的自我簽署根CA憑證、才能使用此選項。

> ⓘ 如果儲存 VM 已將 SMB 伺服器新增至網域、而 LDAP 伺服器是 SMB 伺服器主網域的其中一個網域控制器、則您可以修改 `-session-security-for-ad-ldap` 選項：使用 `vserver cifs security modify` 命令。

e. 選取連接埠、查詢和基礎值。

建議使用預設值、但您必須向LDAP管理員確認這些值是否適合您的環境。

- `-port` *`port`* 指定 LDAP 伺服器連接埠。

  預設值為 `389`。

如果您打算使用Start TLS來保護LDAP連線、則必須使用預設連接埠389。啟動TLS會以純文字連線的形式透過LDAP預設連接埠389開始、然後將該連線升級為TLS。如果您變更連接埠、啟動TLS就會失敗。

- `-query-timeout` *`integer`* 指定查詢逾時（以秒為單位）。

  允許的範圍為1到10秒。預設值為 `3` 秒。

- `-base-dn` *`LDAP_DN`* 指定基礎 DN 。

  如有需要、可輸入多個值（例如啟用LDAP參照追蹤）。預設值為 `""` （根目錄）。

- `-base-scope {base|onelevel|subtree}` 指定基本搜尋範圍。

  預設值為 `subtree`。

- `-referral-enabled {true|false}` 指定是否啟用 LDAP 參照追蹤。

  從ONTAP 功能介紹9.5開始、ONTAP 如果主要LDAP伺服器傳回LDAP參照回應、表示所需記錄存在於參照的LDAP伺服器上、即可讓功能介紹LDAP用戶端將查詢要求參照到其他LDAP伺服器。預設值為 **false**。

若要搜尋所參照LDAP伺服器中的記錄、必須將所參照記錄的基礎DN新增至基礎DN、做為LDAP用戶端組態的一部分。

2. 在儲存 VM 上建立 LDAP 用戶端組態：

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

   建立 LDAP 用戶端組態時、您必須提供儲存 VM 名稱。

3. 確認LDAP用戶端組態已成功建立：

```
vserver services name-service ldap client show -client-config
client_config_name
```

範例

下列命令會建立名為 ldap1 的新 LDAP 用戶端組態、讓儲存 VM VS1 與 Active Directory 伺服器 for LDAP 搭配使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

下列命令會建立名為 ldap1 的新 LDAP 用戶端組態、讓儲存 VM VS1 與需要簽署和密封的 Active Directory 伺服器搭配使用、而 LDAP 伺服器探索則僅限於指定網域的特定站台：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

下列命令會建立名為 ldap1 的新 LDAP 用戶端組態、讓儲存 VM VS1 與需要 LDAP 參照追蹤的 Active Directory

伺服器搭配使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

下列命令會指定基礎 DN 、以修改儲存 VM VS1 的 LDAP 用戶端組態 ldap1 ：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

下列命令可啟用參照追蹤功能、修改儲存 VM VS1 的 LDAP 用戶端組態 ldap1 ：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

將LDAP用戶端組態與SVM建立關聯

若要在 SVM 上啟用 LDAP 、您必須使用 `vserver services name-service ldap create` 用於將 LDAP 用戶端組態與 SVM 建立關聯的命令。

您需要的產品

- LDAP網域必須已存在於網路中、且SVM所在的叢集必須能夠存取。
- SVM上必須存在LDAP用戶端組態。

步驟

1. 在 SVM 上啟用 LDAP ：

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > 從 ONTAP 9.2 開始 `vserver services name-service ldap create` 如果 ONTAP 無法連絡名稱伺服器、命令會執行自動組態驗證、並回報錯誤訊息。

   下列命令可在「VS1」SVM上啟用LDAP、並將其設定為使用「LDAP1」LDAP用戶端組態：

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. 使用vserver services name-service LDAP檢查命令來驗證名稱伺服器的狀態。

   下列命令可驗證SVM VS1上的LDAP伺服器。

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

   名稱服務檢查命令可從ONTAP 版本號不含資訊的9.2開始使用。

驗證名稱服務交換器表中的**LDAP**來源

您必須驗證SVM的名稱服務交換器表中是否正確列出名稱服務的LDAP來源。

步驟

1. 顯示目前名稱服務交換器表格內容：

   `vserver services name-service ns-switch show -vserver` *`svm_name`*

   下列命令顯示SVM My_SVM的結果：

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
My_SVM          hosts            files,
                                 dns
My_SVM          group            files,ldap
My_SVM          passwd           files,ldap
My_SVM          netgroup         files
My_SVM          namemap          files
5 entries were displayed.
```

   `namemap` 指定要搜尋名稱對應資訊的來源、以及搜尋順序。在純UNIX環境中、不需要輸入此項目。只有在同時使用UNIX和Windows的混合環境中才需要名稱對應。

2. 更新 `ns-switch` 視情況輸入：

如果您想要更新下列項目的**ns**交換器項目...	輸入命令...
使用者資訊	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database passwd -sources ldap,files`
群組資訊	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database group -sources ldap,files`
網路群組資訊	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database netgroup -sources ldap,files`