



使用LDAP ONTAP 9

NetApp
January 08, 2026

目錄

使用LDAP	1
了解如何在 ONTAP NFS SVM 上使用 LDAP 名稱服務	1
以取得更多資訊	2
為 ONTAP NFS SVM 建立新的 LDAP 用戶端模式	2
為 ONTAP NFS 存取建立 LDAP 用戶端配置	3
將 LDAP 用戶端配置與 ONTAP NFS SVM 關聯	7
驗證 ONTAP NFS SVM 的 LDAP 來源	8

使用LDAP

了解如何在 ONTAP NFS SVM 上使用 LDAP 名稱服務

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 ONTAP SMB SVM 上安裝自我簽署的根 CA 憑證"](#)

為 ONTAP NFS SVM 建立新的 LDAP 用戶端模式

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
```

為 ONTAP NFS 存取建立 LDAP 用戶端配置

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。

開始之前

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) 。



已棄用。`-ldap-servers` 字段替換 `-servers` 場地。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::> vservers services name-service ldap client modify -vservers vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

將 LDAP 用戶端配置與 ONTAP NFS SVM 關聯

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

開始之前

- 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：

```
vservers services name-service ldap create -vservers vservers_name -client-config
client_config_name
```



這 `vservers services name-service ldap create` 如果 ONTAP 無法聯繫名稱伺服器，則該命令將執行自動設定驗證並報告錯誤訊息。

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

2. 使用 `vservers services name-service ldap check` 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::> vservers services name-service ldap check -vservers vs1

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

驗證 ONTAP NFS SVM 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
```

Vserver	Database	Source
-----	-----	-----
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	<pre>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</pre>
群組資訊	<pre>vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files</pre>
網路群組資訊	<pre>vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files</pre>

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。