



Configurare i name service

ONTAP 9

NetApp
January 08, 2026

Sommario

Configurare i name service	1
Scopri di più sui servizi di denominazione NFS ONTAP	1
Configurare la tabella di commutazione del servizio nomi NFS ONTAP	1
Configurare utenti e gruppi UNIX locali	2
Informazioni sugli utenti e i gruppi UNIX locali per le SVM NFS ONTAP	2
Creare utenti UNIX locali su SVM NFS ONTAP	2
Carica gli elenchi degli utenti UNIX locali su ONTAP NFS SVM	3
Creare gruppi UNIX locali su SVM NFS ONTAP	4
Aggiungere utenti al gruppo UNIX locale su ONTAP NFS SVM	4
Carica gruppi UNIX locali dagli URI su SVM NFS ONTAP	5
Lavorare con i netgroup	6
Informazioni sui netgroup sulle SVM NFS ONTAP	6
Carica netgroup dagli URI su SVM NFS ONTAP	6
Verifica le definizioni del netgroup SVM NFS ONTAP	8
Creare configurazioni di dominio NIS per SVM NFS ONTAP	9
Utilizzare LDAP	10
Scopri come utilizzare i servizi di denominazione LDAP su SVM NFS ONTAP	10
Creare nuovi schemi client LDAP per SVM NFS ONTAP	12
Creare configurazioni client LDAP per l'accesso ONTAP NFS	13
Associare le configurazioni client LDAP con ONTAP NFS SVM	17
Verificare le origini LDAP per gli SVM NFS ONTAP	17

Configurare i name service

Scopri di più sui servizi di denominazione NFS ONTAP

A seconda della configurazione del sistema storage, ONTAP deve essere in grado di cercare informazioni su host, utenti, gruppi o netgroup per fornire un accesso appropriato ai client. Per ottenere queste informazioni, è necessario configurare i name service per consentire a ONTAP di accedere ai name service locali o esterni.

È necessario utilizzare un servizio di nomi come NIS o LDAP per facilitare la ricerca dei nomi durante l'autenticazione del client. Si consiglia di utilizzare LDAP quando possibile per una maggiore sicurezza, in particolare durante l'implementazione di NFSv4 o versioni successive. È inoltre necessario configurare utenti e gruppi locali nel caso in cui i server dei nomi esterni non siano disponibili.

Le informazioni del servizio di nome devono essere mantenute sincronizzate su tutte le origini.

Configurare la tabella di commutazione del servizio nomi NFS ONTAP

È necessario configurare correttamente la tabella dello switch del name service per consentire a ONTAP di consultare i name service locali o esterni per recuperare le informazioni di mappatura di host, utenti, gruppi, netgroup o nomi.

Prima di iniziare

È necessario decidere quali servizi di nomi utilizzare per la mappatura di host, utenti, gruppi, netgroup o nomi, in base all'ambiente in uso.

Se si intende utilizzare netgroup, tutti gli indirizzi IPv6 specificati nei netgroup devono essere abbreviati e compressi come specificato in RFC 5952.

A proposito di questa attività

Non includere fonti di informazioni che non vengono utilizzate. Ad esempio, se NIS non viene utilizzato nell'ambiente, non specificare `-sources nis` opzione.

Fasi

1. Aggiungere le voci necessarie alla tabella dei name service switch:

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

2. Verificare che la tabella name service switch contenga le voci previste nell'ordine desiderato:

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

Se si desidera apportare delle correzioni, è necessario utilizzare `vserver services name-service ns-switch modify` oppure `vserver services name-service ns-switch delete` comandi.

Esempio

Nell'esempio riportato di seguito viene creata una nuova voce nella tabella name service switch per SVM vs1

che utilizza il file netgroup locale e un server NIS esterno per cercare le informazioni del netgroup in tale ordine:

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

Al termine

- Per consentire l'accesso ai dati, è necessario configurare i name service specificati per SVM.
- Se si elimina un servizio di nomi per SVM, è necessario rimuoverlo anche dalla tabella di switch del servizio di nomi.

L'accesso del client al sistema di storage potrebbe non funzionare come previsto, se non si riesce a eliminare il name service dalla tabella di switch del name service.

Configurare utenti e gruppi UNIX locali

Informazioni sugli utenti e i gruppi UNIX locali per le SVM NFS ONTAP

È possibile utilizzare utenti e gruppi UNIX locali su SVM per l'autenticazione e la mappatura dei nomi. È possibile creare manualmente utenti e gruppi UNIX oppure caricare un file contenente utenti o gruppi UNIX da un URI (Uniform Resource Identifier).

Per impostazione predefinita, è previsto un limite massimo di 32,768 gruppi di utenti UNIX locali e membri del gruppo combinati nel cluster. L'amministratore del cluster può modificare questo limite.

Creare utenti UNIX locali su SVM NFS ONTAP

È possibile utilizzare `vserver services name-service unix-user create` Per creare utenti UNIX locali. Un utente UNIX locale è un utente UNIX creato sull'opzione SVM as a UNIX name service da utilizzare nell'elaborazione delle mappature dei nomi.

Fase

1. Creare un utente UNIX locale:

```
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` specifica il nome utente. La lunghezza del nome utente deve essere pari o inferiore a 64 caratteri.

`-id integer` Specifica l'ID utente assegnato.

`-primary-gid integer` Specifica l'ID del gruppo primario. In questo modo l'utente viene aggiunto al gruppo primario. Dopo aver creato l'utente, è possibile aggiungerlo manualmente a qualsiasi altro gruppo desiderato.

Esempio

Il seguente comando crea un utente UNIX locale denominato johnm (nome completo "John Miller") sulla SVM

denominata vs1. L'utente ha l'ID 123 e l'ID del gruppo primario 100.

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

Carica gli elenchi degli utenti UNIX locali su ONTAP NFS SVM

In alternativa alla creazione manuale di singoli utenti UNIX locali in SVM, è possibile semplificare l'attività caricando un elenco di utenti UNIX locali in SVM da un URI (Uniform Resource Identifier) (`vserver services name-service unix-user load-from-uri`).

Fasi

1. Creare un file contenente l'elenco degli utenti UNIX locali che si desidera caricare.

Il file deve contenere informazioni sull'utente in UNIX `/etc/passwd` formato:

```
user_name: password: user_ID: group_ID: full_name
```

Il comando elimina il valore di `password` e i valori dei campi dopo `full_name` campo (`home_directory` e `shell`).

Le dimensioni massime supportate dei file sono 2.5 MB.

2. Verificare che l'elenco non contenga informazioni duplicate.

Se l'elenco contiene voci duplicate, il caricamento dell'elenco non riesce e viene visualizzato un messaggio di errore.

3. Copiare il file su un server.

Il server deve essere raggiungibile dal sistema di storage su HTTP, HTTPS, FTP o FTPS.

4. Determinare l'URI del file.

L'URI è l'indirizzo fornito al sistema di storage per indicare la posizione del file.

5. Caricare il file contenente l'elenco degli utenti UNIX locali nelle SVM dall'URI:

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

`-overwrite {true|false}` specifica se sovrascrivere le voci. L'impostazione predefinita è `false`.

Esempio

Il seguente comando carica un elenco di utenti UNIX locali dall'URI `ftp://ftp.example.com/passwd` Nella SVM denominata vs1. Gli utenti esistenti sulla SVM non vengono sovrascritti dalle informazioni dell'URI.

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

Creare gruppi UNIX locali su SVM NFS ONTAP

È possibile utilizzare `vserver services name-service unix-group create` Per creare gruppi UNIX locali per SVM. I gruppi UNIX locali vengono utilizzati con gli utenti UNIX locali.

Fase

1. Creare un gruppo UNIX locale:

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

`-name group_name` specifica il nome del gruppo. La lunghezza del nome del gruppo non deve superare i 64 caratteri.

`-id integer` Specifica l'ID del gruppo assegnato.

Esempio

Il seguente comando crea un gruppo locale denominato eng sulla SVM denominata vs1. Il gruppo ha l'ID 101.

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

Aggiungere utenti al gruppo UNIX locale su ONTAP NFS SVM

È possibile utilizzare `vserver services name-service unix-group adduser` Comando per aggiungere un utente a un gruppo UNIX supplementare locale a SVM.

Fase

1. Aggiunta di un utente a un gruppo UNIX locale:

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

`-name group_name` Specifica il nome del gruppo UNIX a cui aggiungere l'utente oltre al gruppo primario dell'utente.

Esempio

Il seguente comando aggiunge un utente denominato max a un gruppo UNIX locale denominato eng sulla SVM denominata vs1:

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

Carica gruppi UNIX locali dagli URI su SVM NFS ONTAP

In alternativa alla creazione manuale di singoli gruppi UNIX locali, è possibile caricare un elenco di gruppi UNIX locali nelle SVM da un URI (Uniform Resource Identifier) utilizzando `vserver services name-service unix-group load-from-uri` comando.

Fasi

1. Creare un file contenente l'elenco dei gruppi UNIX locali che si desidera caricare.

Il file deve contenere informazioni di gruppo in UNIX `/etc/group` formato:

`group_name: password: group_ID: comma_separated_list_of_users`

Il comando elimina il valore di `password` campo.

La dimensione massima supportata del file è di 1 MB.

La lunghezza massima di ciascuna riga del file di gruppo è di 32,768 caratteri.

2. Verificare che l'elenco non contenga informazioni duplicate.

L'elenco non deve contenere voci duplicate, altrimenti il caricamento dell'elenco non riesce. Se sono già presenti voci in SVM, è necessario impostare `-overwrite` parametro a. `true` per sovrascrivere tutte le voci esistenti con il nuovo file o assicurarsi che il nuovo file non contenga voci che duplicano le voci esistenti.

3. Copiare il file su un server.

Il server deve essere raggiungibile dal sistema di storage su HTTP, HTTPS, FTP o FTPS.

4. Determinare l'URI del file.

L'URI è l'indirizzo fornito al sistema di storage per indicare la posizione del file.

5. Caricare il file contenente l'elenco dei gruppi UNIX locali nella SVM dall'URI:

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

`-overwrite true false`} specifica se sovrascrivere le voci. L'impostazione predefinita è `false`. Se si specifica questo parametro come `true`, ONTAP sostituisce l'intero database locale dei gruppi UNIX della SVM specificata con le voci del file che si sta caricando.

Esempio

Il seguente comando carica un elenco di gruppi UNIX locali dall'URI `ftp://ftp.example.com/group` Nella

SVM denominata vs1. I gruppi esistenti sulla SVM non vengono sovrascritti dalle informazioni dell'URI.

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

Lavorare con i netgroup

Informazioni sui netgroup sulle SVM NFS ONTAP

È possibile utilizzare netgroup per l'autenticazione degli utenti e per associare i client nelle regole dei criteri di esportazione. È possibile fornire l'accesso ai netgroup da server di nomi esterni (LDAP o NIS) oppure caricare netgroup da un URI (Uniform Resource Identifier) nelle SVM utilizzando `vserver services name-service netgroup load` comando.

Prima di iniziare

Prima di lavorare con i netgroup, è necessario verificare che siano soddisfatte le seguenti condizioni:

- Tutti gli host nei netgroup, indipendentemente dall'origine (NIS, LDAP o file locali), devono disporre di record DNS sia in avanti (A) che in retromarcia (PTR) per fornire ricerche DNS coerenti in avanti e indietro. Inoltre, se un indirizzo IP di un client ha più record PTR, tutti questi nomi host devono essere membri del netgroup e avere record A corrispondenti.
- I nomi di tutti gli host nei netgroup, indipendentemente dalla loro origine (NIS, LDAP o file locali), devono essere scritti correttamente e utilizzare il maiuscolo/minuscolo corretto. Le incongruenze dei casi nei nomi host utilizzati nei netgroup possono causare comportamenti imprevisti, come i controlli di esportazione non riusciti.
- Tutti gli indirizzi IPv6 specificati nei netgroup devono essere abbreviati e compresi come specificato in RFC 5952.

Ad esempio, 2011:hu9:0:0:0:0:3:1 deve essere ridotto a 2011:hu9::3:1.

A proposito di questa attività

Quando si lavora con netgroup, è possibile eseguire le seguenti operazioni:

- È possibile utilizzare `vserver export-policy netgroup check-membership` Per determinare se un IP client è membro di un determinato netgroup.
- È possibile utilizzare `vserver services name-service getxxbyyy netgrp` per verificare se un client fa parte di un netgroup.

Il servizio sottostante per la ricerca viene selezionato in base all'ordine di switch name service configurato.

Carica netgroup dagli URI su SVM NFS ONTAP

Uno dei metodi che è possibile utilizzare per associare i client nelle regole dei criteri di esportazione consiste nell'utilizzare gli host elencati in netgroup. È possibile caricare

netgroup da un URI (Uniform Resource Identifier) in SVM in alternativa all'utilizzo di netgroup memorizzati in server di nomi esterni (`vserver services name-service netgroup load`).

Prima di iniziare

I file netgroup devono soddisfare i seguenti requisiti prima di essere caricati in una SVM:

- Il file deve utilizzare lo stesso formato di file di testo netgroup utilizzato per popolare NIS.

ONTAP controlla il formato del file di testo del netgroup prima di caricarlo. Se il file contiene errori, non viene caricato e viene visualizzato un messaggio che indica le correzioni da eseguire nel file. Dopo aver corretto gli errori, è possibile ricaricare il file netgroup nella SVM specificata.

- I caratteri alfabetici nei nomi host nel file netgroup devono essere minuscoli.
- La dimensione massima supportata del file è di 5 MB.
- Il livello massimo supportato per i netgroup di nidificazione è 1000.
- È possibile utilizzare solo i nomi host DNS primari quando si definiscono i nomi host nel file netgroup.

Per evitare problemi di accesso all'esportazione, i nomi host non devono essere definiti utilizzando i record CNAME DNS o round robin.

- Le porzioni di triplice utente e di dominio nel file netgroup devono essere mantenute vuote perché ONTAP non le supporta.

È supportata solo la parte host/IP.

A proposito di questa attività

ONTAP supporta le ricerche netgroup-by-host per il file netgroup locale. Dopo aver caricato il file netgroup, ONTAP crea automaticamente una mappa netgroup.byhost per abilitare le ricerche netgroup-by-host. In questo modo è possibile accelerare notevolmente le ricerche dei netgroup locali durante l'elaborazione delle regole dei criteri di esportazione per valutare l'accesso al client.

Fase

1. Caricare i netgroup nelle SVM da un URI:

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

Il caricamento del file netgroup e la creazione della mappa netgroup.byhost possono richiedere alcuni minuti.

Se si desidera aggiornare i netgroup, è possibile modificare il file e caricare il file netgroup aggiornato nella SVM.

Esempio

Il seguente comando carica le definizioni di netgroup nella SVM denominata vs1 dall'URL HTTP `http://intranet/downloads/corp-netgroup`:

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

Verifica le definizioni del netgroup SVM NFS ONTAP

Dopo aver caricato i netgroup nella SVM, è possibile utilizzare `vserver services name-service netgroup status` per verificare lo stato delle definizioni dei netgroup. In questo modo è possibile determinare se le definizioni dei netgroup sono coerenti su tutti i nodi che eseguono la SVM.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Verificare lo stato delle definizioni dei netgroup:

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

È possibile visualizzare ulteriori informazioni in una vista più dettagliata.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Esempio

Una volta impostato il livello di privilegio, il seguente comando visualizza lo stato del netgroup per tutte le SVM:

```

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

```

Creare configurazioni di dominio NIS per SVM NFS ONTAP

Se nel proprio ambiente viene utilizzato un NIS (Network Information Service) per i name service, è necessario creare una configurazione di dominio NIS per SVM utilizzando `vserver services name-service nis-domain create` comando.

Prima di iniziare

Tutti i server NIS configurati devono essere disponibili e raggiungibili prima di configurare il dominio NIS sulla SVM.

Se si intende utilizzare NIS per le ricerche nelle directory, le mappe nei server NIS non possono contenere più di 1,024 caratteri per ciascuna voce. Non specificare il server NIS non conforme a questo limite. In caso contrario, l'accesso client dipendente dalle voci NIS potrebbe non riuscire.

A proposito di questa attività

Se il database NIS contiene un `netgroup.byhost` map, ONTAP può utilizzarlo per ricerche più rapide. Il `netgroup.byhost` e `netgroup` le mappe nella directory devono essere sempre sincronizzate per evitare problemi di accesso al client. A partire da ONTAP 9.7, NIS `netgroup.byhost` le voci possono essere memorizzate nella cache utilizzando `vserver services name-service nis-domain netgroup-database` comandi.

L'utilizzo di NIS per la risoluzione dei nomi host non è supportato.

Fasi

1. Creare una configurazione di dominio NIS:

```
vserver services name-service nis-domain create -vserver vs1 -domain <domain_name> -nis-servers <IP_addresses>
```

È possibile specificare fino a 10 server NIS.



IL -nis-servers il campo sostituisce il -servers campo. Puoi usare il -nis-servers campo per specificare un nome host o un indirizzo IP per il server NIS.

2. Verificare che il dominio sia stato creato:

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

Esempio

Il seguente comando crea una configurazione di dominio NIS per un dominio NIS chiamato nisdomain sulla SVM denominata vs1 con un server NIS all'indirizzo IP 192.0.2.180 :

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

Utilizzare LDAP

Scopri come utilizzare i servizi di denominazione LDAP su SVM NFS ONTAP

Se nel proprio ambiente viene utilizzato LDAP per i name service, è necessario collaborare con l'amministratore LDAP per determinare i requisiti e le configurazioni appropriate del sistema di storage, quindi attivare SVM come client LDAP.

A partire da ONTAP 9.10.1, l'associazione del canale LDAP è supportata per impostazione predefinita sia per le connessioni LDAP di Active Directory che per quelle di servizi nome. ONTAP proverà l'associazione del canale con connessioni LDAP solo se Start-TLS o LDAPS è attivato insieme alla sicurezza della sessione impostata su Sign o Seal. Per disattivare o riabilitare l'associazione dei canali LDAP con i server dei nomi, utilizzare -try-channel-binding con il ldap client modify comando.

Per ulteriori informazioni, vedere "[2020 requisiti di binding del canale LDAP e firma LDAP per Windows](#)".

- Prima di configurare LDAP per ONTAP, verificare che l'implementazione del sito soddisfi le Best practice per la configurazione del server e del client LDAP. In particolare, devono essere soddisfatte le seguenti condizioni:
 - Il nome di dominio del server LDAP deve corrispondere alla voce del client LDAP.
 - I tipi di hash della password utente LDAP supportati dal server LDAP devono includere quelli supportati da ONTAP:
 - CRYPT (tutti i tipi) e SHA-1 (SHA, SSHA).
 - A partire da ONTAP 9.8, hash SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, Sono supportati anche SSHA-384 e SSHA-512).

- Se il server LDAP richiede misure di protezione della sessione, è necessario configurarle nel client LDAP.

Sono disponibili le seguenti opzioni di sicurezza della sessione:

- Firma LDAP (verifica dell'integrità dei dati) e firma e sigillatura LDAP (verifica e crittografia dell'integrità dei dati)
- AVVIARE TLS
- LDAPS (LDAP su TLS o SSL)
- Per abilitare le query LDAP firmate e sealed, è necessario configurare i seguenti servizi:
 - I server LDAP devono supportare il meccanismo GSSAPI (Kerberos) SASL.
 - I server LDAP devono disporre di record DNS A/AAAA e di record PTR impostati sul server DNS.
 - I server Kerberos devono avere record SRV presenti sul server DNS.
- Per abilitare L'AVVIO di TLS o LDAPS, tenere in considerazione i seguenti punti.
 - L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.
 - Se si utilizza LDAPS, il server LDAP deve essere abilitato per TLS o per SSL in ONTAP 9.5 e versioni successive. SSL non è supportato in ONTAP 9.0-9.4.
 - Nel dominio deve essere già configurato un server dei certificati.
- Per abilitare la funzione LDAP referral chasing (in ONTAP 9.5 e versioni successive), devono essere soddisfatte le seguenti condizioni:
 - Entrambi i domini devono essere configurati con una delle seguenti relazioni di trust:
 - Bidirezionale
 - Unidirezionale, in cui il primario si affida al dominio di riferimento
 - Genitore-figlio
 - Il DNS deve essere configurato in modo da risolvere tutti i nomi dei server indicati.
 - Le password di dominio devono essere le stesse per autenticare quando --bind-as-cifs-server è impostato su true.

Le seguenti configurazioni non sono supportate con la funzione LDAP referral chasing.



- Per tutte le versioni di ONTAP:
 - Client LDAP su una SVM amministrativa
- Per ONTAP 9.8 e versioni precedenti (sono supportati nella versione 9.9.1 e successive):
 - Firma e sigillatura LDAP (il -session-security opzionale)
 - Connessioni TLS crittografate (il -use-start-tls opzionale)
 - Comunicazioni tramite la porta LDAPS 636 (la -use-ldaps-for-ad-ldap opzionale)

- È necessario inserire uno schema LDAP durante la configurazione del client LDAP su SVM.

Nella maggior parte dei casi, uno degli schemi ONTAP predefiniti sarà appropriato. Tuttavia, se lo schema LDAP nel proprio ambiente differisce da questi, è necessario creare un nuovo schema client LDAP per ONTAP prima di creare il client LDAP. Rivolgersi all'amministratore LDAP per informazioni sui requisiti

dell'ambiente in uso.

- L'utilizzo di LDAP per la risoluzione dei nomi host non è supportato.

Per ulteriori informazioni

- "[Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP](#)"
- "[Installare certificati CA root autofirmati sulla SVM SMB di ONTAP](#)"

Creare nuovi schemi client LDAP per SVM NFS ONTAP

Se lo schema LDAP nell'ambiente in uso differisce dai valori predefiniti di ONTAP, è necessario creare un nuovo schema del client LDAP per ONTAP prima di creare la configurazione del client LDAP.

A proposito di questa attività

La maggior parte dei server LDAP può utilizzare gli schemi predefiniti forniti da ONTAP:

- MS-ad-BIS (lo schema preferito per la maggior parte dei server ad Windows 2012 e successivi)
- AD-IDMU (server ad Windows 2008, Windows 2012 e versioni successive)
- AD-SFU (server ad Windows 2003 e precedenti)
- RFC-2307 (SERVER LDAP UNIX)

Se è necessario utilizzare uno schema LDAP non predefinito, è necessario crearlo prima di creare la configurazione del client LDAP. Consultare l'amministratore LDAP prima di creare un nuovo schema.

Gli schemi LDAP predefiniti forniti da ONTAP non possono essere modificati. Per creare un nuovo schema, creare una copia e modificarla di conseguenza.

Fasi

1. Visualizzare i modelli di schema del client LDAP esistenti per identificare quello che si desidera copiare:

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

2. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

3. Creare una copia dello schema di un client LDAP esistente:

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

4. Modificare il nuovo schema e personalizzarlo in base all'ambiente:

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

5. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Creare configurazioni client LDAP per l'accesso ONTAP NFS

Se si desidera che ONTAP acceda ai servizi LDAP o Active Directory esterni del proprio ambiente, è necessario prima configurare un client LDAP sul sistema di archiviazione.

Prima di iniziare

Uno dei primi tre server nell'elenco dei domini risolti di Active Directory deve essere attivo e fornire i dati. In caso contrario, questa attività non riesce.



Vi sono più server, tra cui più di due server inattivi in qualsiasi momento.

Fasi

1. Rivolgersi all'amministratore LDAP per determinare i valori di configurazione appropriati per `vserver services name-service ldap client create` comando:
 - a. Specificare una connessione basata su dominio o su indirizzo ai server LDAP.

Il `-ad-domain` e `-servers` le opzioni si escludono a vicenda.

 - Utilizzare `-ad-domain` Opzione per attivare la ricerca del server LDAP nel dominio Active Directory.
 - È possibile utilizzare `-restrict-discovery-to-site` Opzione per limitare il rilevamento del server LDAP al sito predefinito CIFS per il dominio specificato. Se si utilizza questa opzione, è necessario specificare anche il sito predefinito CIFS con `-default-site`.
 - È possibile utilizzare `-preferred-ad-servers` Opzione per specificare uno o più server Active Directory preferiti in base all'indirizzo IP in un elenco delimitato da virgole. Una volta creato il client, è possibile modificare questo elenco utilizzando `vserver services name-service ldap client modify` comando.
 - Utilizzare `-servers` Opzione per specificare uno o più server LDAP (Active Directory o UNIX) per indirizzo IP in un elenco delimitato da virgole.



IL `-servers` l'opzione è deprecata. L' `-ldap-servers` il campo sostituisce il `-servers` campo. Questo campo può contenere un nome host o un indirizzo IP per il server LDAP.

- b. Specificare uno schema LDAP predefinito o personalizzato.

La maggior parte dei server LDAP può utilizzare gli schemi di sola lettura predefiniti forniti da ONTAP. Si consiglia di utilizzare questi schemi predefiniti, a meno che non sia necessario fare diversamente. In tal caso, è possibile creare uno schema personalizzato copiando uno schema predefinito (di sola lettura) e modificando la copia.

Schemi predefiniti:

- MS-AD-BIS

Basato su RFC-2307bis, questo è lo schema LDAP preferito per la maggior parte delle implementazioni LDAP standard di Windows 2012 e versioni successive.

- AD-IDMU

Basato su Active Directory Identity Management per UNIX, questo schema è appropriato per la maggior parte dei server ad Windows 2008, Windows 2012 e versioni successive.

- AD-SFU

Basato su Active Directory Services per UNIX, questo schema è appropriato per la maggior parte dei server ad Windows 2003 e precedenti.

- RFC-2307

In base a RFC-2307 (*un approccio per l'utilizzo di LDAP come Network Information Service*), questo schema è appropriato per la maggior parte dei server UNIX ad.

c. Selezionare valori di binding.

- `-min-bind-level {anonymous|simple|sasl}` specifica il livello minimo di autenticazione bind.

Il valore predefinito è **anonymous**.

- `-bind-dn LDAP_DN` specifica l'utente di binding.

Per i server Active Directory, è necessario specificare l'utente nel modulo account (DOMINIO/utente) o principale (user@domain.com). In caso contrario, è necessario specificare l'utente nel formato nome distinto (CN=user,DC=domain,DC=com).

- `-bind-password password` specifica la password di bind.

d. Selezionare le opzioni di sicurezza della sessione, se necessario.

È possibile attivare la firma e il sealing LDAP o LDAP su TLS, se richiesto dal server LDAP.

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

È possibile attivare la firma (sign, integrità dei dati), firma e sigillatura (seal, integrità dei dati e crittografia), o nessuna delle due none, nessuna firma o sigillatura). Il valore predefinito è none.

Dovresti anche impostare `-min-bind-level {sasl}` a meno che non si desideri che l'autenticazione bind venga meno a. **anonymous** oppure **simple** se la sign e il sealing non vengono a buon fine.

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

Se impostato su **true** E il server LDAP lo supporta, il client LDAP utilizza una connessione TLS crittografata al server. Il valore predefinito è **false**. Per utilizzare questa opzione, è necessario installare un certificato CA principale autofirmato del server LDAP.



Se nella VM di storage è stato aggiunto un server SMB a un dominio e il server LDAP è uno dei controller di dominio del dominio principale del server SMB, è possibile modificare l' `-session-security-for-ad-ldap` utilizzando l'opzione `vserver cifs security modify` comando.

e. Selezionare i valori di porta, query e base.

I valori predefiniti sono consigliati, ma è necessario verificare con l'amministratore LDAP che siano appropriati per l'ambiente in uso.

- `-port port` Specifica la porta del server LDAP.

Il valore predefinito è 389.

Se si intende utilizzare Start TLS per proteggere la connessione LDAP, è necessario utilizzare la porta predefinita 389. Start TLS (Avvia TLS) inizia come una connessione non crittografata sulla porta predefinita LDAP 389 e la connessione viene quindi aggiornata a TLS. Se si modifica la porta, l'avvio TLS non riesce.

- `-query-timeout integer` specifica il timeout della query in secondi.

L'intervallo consentito va da 1 a 10 secondi. Il valore predefinito è 3 secondi.

- `-base-dn LDAP_DN` Specifica il DN di base.

Se necessario, è possibile inserire più valori (ad esempio, se è attivata la funzione LDAP referral chasing). Il valore predefinito è "" (root).

- `-base-scope {base|onelevel|subtree}` specifica l'ambito di ricerca di base.

Il valore predefinito è subtree.

- `-referral-enabled {true|false}` Specifica se è attivata la funzione LDAP referral chasing.

A partire da ONTAP 9.5, questo consente al client LDAP di indirizzare le richieste di ricerca ad altri server ONTAP se il server LDAP primario restituisce una risposta di riferimento LDAP che indica la presenza dei record desiderati sui server LDAP citati. Il valore predefinito è **false**.

Per cercare i record presenti nei server LDAP indicati, è necessario aggiungere la base dn dei record indicati alla base-dn come parte della configurazione del client LDAP.

2. Creazione di una configurazione del client LDAP sulla VM di storage:

```
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}]
```



È necessario fornire il nome della VM di archiviazione quando si crea una configurazione client LDAP.

3. Verificare che la configurazione del client LDAP sia stata creata correttamente:

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

Esempi

Il seguente comando crea una nuova configurazione del client LDAP denominata ldap1 per la Storage VM VS1 da utilizzare con un server Active Directory per LDAP:

```
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
```

Il seguente comando crea una nuova configurazione del client LDAP denominata ldap1 per la VM di storage VS1 in modo che funzioni con un server Active Directory per LDAP su cui è richiesta la firma e la sigillatura e il rilevamento del server LDAP è limitato a un sito specifico per il dominio specificato:

```
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
```

Il seguente comando crea una nuova configurazione del client LDAP denominata ldap1 per la VM di storage VS1 in modo che funzioni con un server Active Directory per LDAP in cui è richiesta la ricerca del riferimento LDAP:

```
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
```

Il seguente comando modifica la configurazione del client LDAP denominata ldap1 per la macchina virtuale di storage VS1 specificando il DN di base:

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

Il seguente comando modifica la configurazione del client LDAP denominata ldap1 per la VM di storage VS1 abilitando la ricerca del riferimento:

```
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
```

Associare le configurazioni client LDAP con ONTAP NFS SVM

Per attivare LDAP su una SVM, è necessario utilizzare `vserver services name-service ldap create` Comando per associare una configurazione del client LDAP a SVM.

Prima di iniziare

- Un dominio LDAP deve già esistere all'interno della rete e deve essere accessibile al cluster su cui si trova la SVM.
- Una configurazione del client LDAP deve esistere su SVM.

Fasi

1. Abilitare LDAP su SVM:

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



Il `vserver services name-service ldap create` comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non riesce a contattare il server dei nomi.

Il seguente comando abilita LDAP su "vs1" SVM e lo configura per utilizzare la configurazione del client LDAP "ldap1":

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

2. Convalidare lo stato dei server dei nomi utilizzando il comando di controllo `ldap name-service` dei servizi vserver.

Il seguente comando convalida i server LDAP su SVM vs1.

```
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". |
```

Verificare le origini LDAP per gli SVM NFS ONTAP

È necessario verificare che le origini LDAP per i servizi nome siano elencate correttamente nella tabella di switch del servizio nome per SVM.

Fasi

- Visualizza il contenuto della tabella corrente dello switch name service:

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

Il comando seguente mostra i risultati per SVM My_SVM:

```
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 specifica le origini per la ricerca delle informazioni di mappatura dei nomi e in quale ordine. In un ambiente UNIX, questa voce non è necessaria. La mappatura dei nomi è necessaria solo in un ambiente misto che utilizza sia UNIX che Windows.

- Aggiornare ns-switch voce appropriata:

Se si desidera aggiornare la voce ns-switch per...	Immettere il comando...
Informazioni sull'utente	<pre>vserver services name-service ns- switch modify -vserver <i>vserver_name</i> -database passwd -sources ldap,files</pre>
Informazioni sul gruppo	<pre>vserver services name-service ns- switch modify -vserver <i>vserver_name</i> -database group -sources ldap,files</pre>
Informazioni sul netgroup	<pre>vserver services name-service ns- switch modify -vserver <i>vserver_name</i> -database netgroup -sources ldap,files</pre>

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.