Configurare i name service

ONTAP 9

NetApp
April 24, 2024

Sommario

Configurare i name service

Funzionamento della configurazione dello switch ONTAP name service

ONTAP memorizza le informazioni di configurazione del name service in una tabella equivalente a `/etc/nsswitch.conf` File su sistemi UNIX. È necessario comprendere la funzione della tabella e il modo in cui ONTAP la utilizza in modo da poterla configurare in modo appropriato per l'ambiente in uso.

La tabella ONTAP name service switch determina le origini del servizio di nomi che ONTAP consulta per recuperare le informazioni relative a un determinato tipo di informazioni sul servizio di nomi. ONTAP gestisce una tabella di switch del name service separata per ogni SVM.

Tipi di database

La tabella memorizza un elenco di name service separato per ciascuno dei seguenti tipi di database:

Tipo di database	Definisce le origini del servizio nome per…	Le origini valide sono…
host	Conversione dei nomi host in indirizzi IP	file, dns
gruppo	Ricerca di informazioni sul gruppo di utenti	file, nis, ldap
password	Ricerca delle informazioni dell'utente	file, nis, ldap
netgroup	Ricerca di informazioni sul netgroup	file, nis, ldap
mappa dei nomi	Mappatura dei nomi utente	file, ldap

Tipi di origine

Le origini specificano quale nome di origine del servizio utilizzare per recuperare le informazioni appropriate.

Specifica tipo di origine…	Per cercare informazioni in…	Gestito dalle famiglie di comandi…

file	File di origine locali	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Server NIS esterni come specificato nella configurazione del dominio NIS di SVM	`vserver services name-service nis-domain`
ldap	Server LDAP esterni come specificato nella configurazione del client LDAP di SVM	`vserver services name-service ldap`
dns	Server DNS esterni come specificato nella configurazione DNS di SVM	`vserver services name-service dns`

Anche se si prevede di utilizzare NIS o LDAP per l'accesso ai dati e l'autenticazione dell'amministrazione SVM, è comunque necessario includere `files` E configurare gli utenti locali come fallback nel caso in cui l'autenticazione NIS o LDAP non riesca.

Protocolli utilizzati per accedere a fonti esterne

Per accedere ai server per le origini esterne, ONTAP utilizza i seguenti protocolli:

Origine esterna del name service	Protocollo utilizzato per l'accesso
NIS	UDP
DNS	UDP
LDAP	TCP

Esempio

Nell'esempio seguente viene visualizzata la configurazione dello switch name service per SVM svm_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Per cercare gli indirizzi IP degli host, ONTAP consulta innanzitutto i file di origine locali. Se la query non restituisce alcun risultato, i server DNS vengono controllati in seguito.

Per cercare informazioni su utenti o gruppi, ONTAP consulta solo i file di origine locali. Se la query non restituisce alcun risultato, la ricerca non riesce.

Per cercare informazioni sui netgroup, ONTAP consulta prima i server NIS esterni. Se la query non restituisce alcun risultato, viene selezionato il file netgroup locale.

Non sono presenti voci di name service per la mappatura dei nomi nella tabella per SVM svm_1. Pertanto, ONTAP consulta solo i file di origine locali per impostazione predefinita.

Informazioni correlate

"Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"

Utilizzare LDAP

Panoramica LDAP

Un server LDAP (Lightweight Directory Access Protocol) consente di gestire centralmente le informazioni dell'utente. Se si memorizza il database utente su un server LDAP nell'ambiente in uso, è possibile configurare il sistema di storage in modo che cerchi le informazioni utente nel database LDAP esistente.

- 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` impostare 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)

- A partire da ONTAP 9.11.1, è possibile utilizzare "LDAP fast bind per l'autenticazione nsswitch."
- 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, vedere "Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP".

Concetti relativi alla firma e al sealing LDAP

A partire da ONTAP 9, è possibile configurare la firma e il sealing per abilitare la sicurezza della sessione LDAP sulle query a un server Active Directory (ad). È necessario configurare le impostazioni di sicurezza del server NFS sulla macchina virtuale di storage (SVM) in modo che corrispondano a quelle del server LDAP.

La firma conferma l'integrità dei dati del payload LDAP utilizzando la tecnologia a chiave segreta. Il sealing crittografa i dati del payload LDAP per evitare la trasmissione di informazioni sensibili in testo non crittografato. Un'opzione *LDAP Security Level* indica se il traffico LDAP deve essere firmato, firmato e sigillato o no. L'impostazione predefinita è `none`. test

La firma LDAP e il sealing sul traffico SMB sono attivati sulla SVM con `-session-security-for-ad-ldap` al `vserver cifs security modify` comando.

Concetti LDAPS

È necessario comprendere alcuni termini e concetti relativi al modo in cui ONTAP protegge le comunicazioni LDAP. ONTAP può utilizzare TLS O LDAPS DI AVVIO per impostare sessioni autenticate tra server LDAP integrati in Active Directory o server LDAP basati su UNIX.

Terminologia

È necessario comprendere alcuni termini relativi all'utilizzo di LDAPS da parte di ONTAP per proteggere le comunicazioni LDAP.

- **LDAP**

  (Lightweight Directory Access Protocol) protocollo per l'accesso e la gestione delle directory di informazioni. LDAP viene utilizzato come directory di informazioni per la memorizzazione di oggetti come utenti, gruppi e netgroup. LDAP fornisce inoltre servizi di directory che gestiscono questi oggetti e soddisfano le richieste LDAP dai client LDAP.

- **SSL**

  (Secure Sockets Layer) protocollo sviluppato per l'invio sicuro di informazioni su Internet. SSL è supportato da ONTAP 9 e versioni successive, ma è stato deprecato a favore di TLS.

- **TLS**

  (Transport Layer Security) un protocollo di tracciamento degli standard IETF basato sulle specifiche SSL precedenti. È il successore di SSL. TLS è supportato da ONTAP 9,5 e versioni successive.

- **LDAPS (LDAP su SSL o TLS)**

  Protocollo che utilizza TLS o SSL per proteggere le comunicazioni tra client LDAP e server LDAP. I termini *LDAP su SSL* e *LDAP su TLS* vengono talvolta utilizzati in modo intercambiabile. LDAPS è supportato da

ONTAP 9,5 e versioni successive.

- In ONTAP 9.5-9.8, LDAPS può essere attivato solo sulla porta 636. A tale scopo, utilizzare `-use -ldaps-for-ad-ldap` con il `vserver cifs security modify` comando.
- A partire da ONTAP 9.9.1, LDAPS può essere attivato su qualsiasi porta, anche se la porta 636 rimane quella predefinita. A tale scopo, impostare `-ldaps-enabled` parametro a. `true` e specificare il desiderato `-port` parametro. Per ulteriori informazioni, consultare `vserver services name-service ldap client create` pagina man

> L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.

- **Avvia TLS**

  (Noto anche come *start_tls*, *STARTTLS* e *STARTTLS*) un meccanismo per fornire comunicazioni sicure utilizzando i protocolli TLS.

  ONTAP utilizza STARTTLS per proteggere la comunicazione LDAP e la porta LDAP predefinita (389) per comunicare con il server LDAP. Il server LDAP deve essere configurato in modo da consentire le connessioni sulla porta LDAP 389; in caso contrario, le connessioni LDAP TLS dalla SVM al server LDAP non funzionano.

Utilizzo di LDAPS da parte di ONTAP

ONTAP supporta l'autenticazione del server TLS, che consente al client LDAP SVM di confermare l'identità del server LDAP durante l'operazione di binding. I client LDAP abilitati per TLS possono utilizzare tecniche standard di crittografia a chiave pubblica per verificare che il certificato e l'ID pubblico di un server siano validi e siano stati emessi da un'autorità di certificazione (CA) elencata nell'elenco delle CA attendibili del client.

LDAP supporta STARTTLS per crittografare le comunicazioni utilizzando TLS. STARTTLS inizia come connessione non crittografata sulla porta LDAP standard (389) e la connessione viene quindi aggiornata a TLS.

ONTAP supporta:

- LDAPS per il traffico SMB tra i server LDAP integrati in Active Directory e SVM
- LDAPS per il traffico LDAP per la mappatura dei nomi e altre informazioni UNIX

  I server LDAP integrati in Active Directory o i server LDAP basati su UNIX possono essere utilizzati per memorizzare informazioni per la mappatura dei nomi LDAP e altre informazioni UNIX, come utenti, gruppi e netgroup.

- Certificati della CA principale autofirmati

  Quando si utilizza un LDAP integrato in Active-Directory, il certificato root autofirmato viene generato quando il servizio certificati di Windows Server viene installato nel dominio. Quando si utilizza un server LDAP basato su UNIX per la mappatura dei nomi LDAP, il certificato root autofirmato viene generato e salvato utilizzando i mezzi appropriati per l'applicazione LDAP.

Per impostazione predefinita, LDAPS è disattivato.

Attiva il supporto LDAP RFC2307bis

Se si desidera utilizzare LDAP e si desidera utilizzare le appartenenze a gruppi nidificati, è possibile configurare ONTAP per abilitare il supporto di LDAP RFC2307bis.

Di cosa hai bisogno

È necessario aver creato una copia di uno degli schemi client LDAP predefiniti che si desidera utilizzare.

A proposito di questa attività

Negli schemi client LDAP, gli oggetti di gruppo utilizzano l'attributo memberUid. Questo attributo può contenere più valori ed elenca i nomi degli utenti che appartengono a quel gruppo. Negli schemi client LDAP abilitati per RFC2307bis, gli oggetti di gruppo utilizzano l'attributo uniqueMember. Questo attributo può contenere il nome distinto completo (DN) di un altro oggetto nella directory LDAP. In questo modo è possibile utilizzare gruppi nidificati poiché i gruppi possono avere altri gruppi come membri.

L'utente non deve essere membro di più di 256 gruppi, inclusi i gruppi nidificati. ONTAP ignora tutti i gruppi che superano il limite di 256 gruppi.

Per impostazione predefinita, il supporto RFC2307bis è disattivato.

> Il supporto RFC2307bis viene attivato automaticamente in ONTAP quando viene creato un client LDAP con lo schema MS-ad-BIS.

Per ulteriori informazioni, vedere "Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP".

Fasi

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

   ```
   set -privilege advanced
   ```

2. Modificare lo schema del client LDAP RFC2307 copiato per abilitare il supporto RFC2307bis:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modificare lo schema in modo che corrisponda alla classe di oggetti supportata nel server LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modificare lo schema in modo che corrisponda al nome dell'attributo supportato nel server LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Opzioni di configurazione per le ricerche nelle directory LDAP

È possibile ottimizzare le ricerche nelle directory LDAP, incluse le informazioni relative a

utenti, gruppi e netgroup, configurando il client LDAP di ONTAP per la connessione ai server LDAP nel modo più appropriato per il proprio ambiente. È necessario capire quando sono sufficienti i valori di ricerca predefiniti di base e ambito LDAP e quali parametri specificare quando i valori personalizzati sono più appropriati.

Le opzioni di ricerca del client LDAP per le informazioni relative a utenti, gruppi e netgroup possono aiutare a evitare query LDAP non riuscite e, di conseguenza, l'accesso del client ai sistemi di storage non riuscito. Inoltre, contribuiscono a garantire che le ricerche siano il più efficienti possibile per evitare problemi di performance del client.

Valori di base e di ricerca dell'ambito predefiniti

La base LDAP è il DN di base predefinito utilizzato dal client LDAP per eseguire query LDAP. Tutte le ricerche, incluse quelle relative a utenti, gruppi e netgroup, vengono eseguite utilizzando il DN di base. Questa opzione è appropriata quando la directory LDAP è relativamente piccola e tutte le voci pertinenti si trovano nello stesso DN.

Se non si specifica un DN di base personalizzato, il valore predefinito è `root`. Ciò significa che ogni query esegue la ricerca nell'intera directory. Sebbene questo massimizzi le possibilità di successo della query LDAP, può essere inefficiente e causare una riduzione significativa delle prestazioni con directory LDAP di grandi dimensioni.

L'ambito di base LDAP è l'ambito di ricerca predefinito utilizzato dal client LDAP per eseguire query LDAP. Tutte le ricerche, incluse quelle relative a utenti, gruppi e netgroup, vengono eseguite utilizzando l'ambito di base. Determina se la query LDAP ricerca solo la voce denominata, le voci di un livello al di sotto del DN o l'intera sottostruttura al di sotto del DN.

Se non si specifica un ambito di base personalizzato, il valore predefinito è `subtree`. Ciò significa che ogni query esegue la ricerca nell'intero sottostruttura sotto il DN. Sebbene questo massimizzi le possibilità di successo della query LDAP, può essere inefficiente e causare una riduzione significativa delle prestazioni con directory LDAP di grandi dimensioni.

Valori di ricerca di base e ambito personalizzati

In alternativa, è possibile specificare valori di base e di ambito separati per le ricerche di utenti, gruppi e netgroup. La limitazione della base di ricerca e dell'ambito delle query in questo modo può migliorare significativamente le prestazioni, poiché limita la ricerca a una sottosezione più piccola della directory LDAP.

Se si specificano valori di base e ambito personalizzati, questi sovrascrivono la base di ricerca predefinita generale e l'ambito per le ricerche di utenti, gruppi e netgroup. I parametri per specificare i valori di base e ambito personalizzati sono disponibili a livello di privilegio avanzato.

Parametro client LDAP…	Specifica custom…
`-base-dn`	DN di base per tutte le ricerche LDAP è possibile inserire più valori, se necessario (ad esempio, se la funzione LDAP referral chasing è attivata in ONTAP 9.5 e versioni successive).
`-base-scope`	Ambito di base per tutte le ricerche LDAP
`-user-dn`	DNS di base per tutte le ricerche degli utenti LDAP questo parametro si applica anche alle ricerche di mappatura dei nomi utente.

`-user-scope`	Ambito di base per tutte le ricerche degli utenti LDAP questo parametro si applica anche alle ricerche di associazione dei nomi utente.
`-group-dn`	DNS di base per tutte le ricerche di gruppi LDAP
`-group-scope`	Ambito di base per tutte le ricerche di gruppi LDAP
`-netgroup-dn`	DNS di base per tutte le ricerche dei netgroup LDAP
`-netgroup-scope`	Ambito di base per tutte le ricerche dei netgroup LDAP

Più valori DN di base personalizzati

Se la struttura della directory LDAP è più complessa, potrebbe essere necessario specificare più DNS di base per cercare determinate informazioni in più parti della directory LDAP. È possibile specificare più DNS per i parametri DN dell'utente, del gruppo e del netgroup separandoli con un punto e virgola (;) e racchiudendo l'intero elenco di ricerca DN con virgolette doppie ("). Se un DN contiene un punto e virgola, è necessario aggiungere un carattere di escape () immediatamente prima del punto e virgola nel DN.

Si noti che l'ambito si applica all'intero elenco di DNS specificato per il parametro corrispondente. Ad esempio, se si specifica un elenco di tre diversi DNS utente e sottostruttura per l'ambito utente, l'utente LDAP ricerca nell'intera sottostruttura ciascuno dei tre DNS specificati.

A partire da ONTAP 9.5, è anche possibile specificare LDAP *referral chasing*, che consente al client LDAP di indirizzare le richieste di ricerca ad altri server ONTAP se il server LDAP primario non restituisce una risposta di riferimento LDAP. Il client utilizza i dati di riferimento per recuperare l'oggetto di destinazione dal server descritto nei dati di riferimento. Per cercare oggetti presenti nei server LDAP indicati, è possibile aggiungere la base-dn degli oggetti indicati alla base-dn come parte della configurazione del client LDAP. Tuttavia, gli oggetti referrati vengono ricercati solo quando è attivata la funzione di referral chasing (ricerca riferimenti), utilizzando il `-referral-enabled true` Durante la creazione o la modifica del client LDAP.

Migliorare le performance delle ricerche di directory LDAP netgroup-by-host

Se l'ambiente LDAP è configurato per consentire ricerche netgroup-by-host, è possibile configurare ONTAP in modo che ne tragga vantaggio ed eseguire ricerche netgroup-by-host. In questo modo è possibile accelerare notevolmente le ricerche dei netgroup e ridurre i possibili problemi di accesso al client NFS dovuti alla latenza durante le ricerche dei netgroup.

Di cosa hai bisogno

La directory LDAP deve contenere un `netgroup.byhost` mappa.

I server DNS devono contenere record di ricerca sia in avanti (A) che in retromarcia (PTR) per i client NFS.

Quando si specificano gli indirizzi IPv6 nei netgroup, è sempre necessario accorciare e comprimere ciascun indirizzo come specificato in RFC 5952.

A proposito di questa attività

I server NIS memorizzano le informazioni del netgroup in tre mappe distinte denominate `netgroup`, `netgroup.byuser`, e. `netgroup.byhost`. Lo scopo di `netgroup.byuser` e. `netgroup.byhost` maps consente di velocizzare le ricerche di netgroup. ONTAP può eseguire ricerche netgroup-by-host sui server NIS per migliorare i tempi di risposta del montaggio.

Per impostazione predefinita, le directory LDAP non dispongono di tale opzione `netgroup.byhost` mappare come i server NIS. Tuttavia, con l'aiuto di strumenti di terze parti, è possibile importare un NIS `netgroup.byhost` eseguire la mappatura nelle directory LDAP per consentire ricerche rapide netgroup-by-host. Se l'ambiente LDAP è stato configurato per consentire ricerche netgroup-by-host, è possibile configurare il client LDAP ONTAP con `netgroup.byhost` nome mappa, DN e ambito di ricerca per ricerche più rapide tra netgroup e host.

La ricezione più rapida dei risultati per le ricerche netgroup-by-host consente a ONTAP di elaborare più rapidamente le regole di esportazione quando i client NFS richiedono l'accesso alle esportazioni. In questo modo si riduce la possibilità di ritardi di accesso dovuti a problemi di latenza della ricerca nel netgroup.

Fasi

1. Ottenere l'esatto nome completo del NIS `netgroup.byhost` mappatura importata nella directory LDAP.

   Il DN della mappa può variare a seconda dello strumento di terze parti utilizzato per l'importazione. Per ottenere prestazioni ottimali, specificare il DN esatto della mappa.

2. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
3. Abilitare le ricerche netgroup-by-host nella configurazione client LDAP della macchina virtuale di storage (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`} Attiva o disattiva la ricerca netgroup-by-host delle directory LDAP. L'impostazione predefinita è `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` specifica il nome distinto di `netgroup.byhost` mappare la directory LDAP. Sovrascrive il DN di base per le ricerche netgroup-by-host. Se non si specifica questo parametro, ONTAP utilizza invece il DN di base.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} specifica l'ambito di ricerca per le ricerche netgroup-by-host. Se non si specifica questo parametro, l'impostazione predefinita è `subtree`.

   Se la configurazione del client LDAP non esiste ancora, è possibile attivare le ricerche netgroup-by-host specificando questi parametri quando si crea una nuova configurazione del client LDAP utilizzando `vserver services name-service ldap client create` comando.

   > A partire da ONTAP 9.2, il campo `-ldap-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server LDAP.

4. Tornare al livello di privilegio admin: `set -privilege admin`

Esempio

Il seguente comando modifica la configurazione del client LDAP esistente denominata "ldap_corp" per abilitare le ricerche netgroup-by-host utilizzando `netgroup.byhost` mappa denominata "nisMapName="netgroup.byhost",DC=corp,DC=example,DC=com" e l'ambito di ricerca predefinito `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Al termine

Il `netgroup.byhost` e. `netgroup` le mappe nella directory devono essere sempre sincronizzate per evitare problemi di accesso al client.

Informazioni correlate

"IETF RFC 5952: Una raccomandazione per la rappresentazione del testo dell'indirizzo IPv6"

Utilizza il binding rapido LDAP per l'autenticazione nsswitch

A partire da ONTAP 9.11.1, è possibile sfruttare la funzionalità LDAP *fast bind* (nota anche come *Concurrent BIND*) per richieste di autenticazione client più semplici e veloci. Per utilizzare questa funzionalità, il server LDAP deve supportare la funzionalità di associazione rapida.

A proposito di questa attività

Senza il binding rapido, ONTAP utilizza il binding semplice LDAP per autenticare gli utenti amministratori con il server LDAP. Con questo metodo di autenticazione, ONTAP invia un nome utente o di gruppo al server LDAP, riceve la password hash memorizzata e confronta il codice hash del server con il codice hash generato localmente dalla password utente. Se sono identici, ONTAP concede l'autorizzazione di accesso.

Grazie alla funzionalità di associazione rapida, ONTAP invia solo le credenziali utente (nome utente e password) al server LDAP tramite una connessione sicura. Il server LDAP convalida quindi queste credenziali e richiede a ONTAP di concedere le autorizzazioni di accesso.

Uno dei vantaggi di fast bind è che non è necessario che ONTAP supporti ogni nuovo algoritmo di hashing supportato dai server LDAP, perché l'hashing delle password viene eseguito dal server LDAP.

"Scopri come utilizzare fast bind."

È possibile utilizzare le configurazioni client LDAP esistenti per l'associazione rapida LDAP. Tuttavia, si consiglia vivamente di configurare il client LDAP per TLS o LDAPS; in caso contrario, la password viene inviata via cavo in testo normale.

Per abilitare il binding rapido LDAP in un ambiente ONTAP, è necessario soddisfare i seguenti requisiti:

- Gli utenti admin di ONTAP devono essere configurati su un server LDAP che supporti il fast bind.
- ONTAP SVM deve essere configurato per LDAP nel database name Services switch (nsswitch).
- Gli account di gruppo e utente amministratore di ONTAP devono essere configurati per l'autenticazione nsswitch utilizzando il collegamento rapido.

Fasi

1. Verificare con l'amministratore LDAP che il collegamento rapido LDAP sia supportato sul server LDAP.
2. Assicurarsi che le credenziali dell'utente amministratore di ONTAP siano configurate sul server LDAP.
3. Verificare che l'amministratore o l'SVM dei dati sia configurato correttamente per il binding rapido LDAP.

a. Per confermare che il server fast bind LDAP è elencato nella configurazione del client LDAP, immettere:

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

"Informazioni sulla configurazione del client LDAP."

b. Per confermare `ldap` è una delle sorgenti configurate per nsswitch `passwd` database, inserire:

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

"Scopri di più sulla configurazione di nsswitch."

4. Assicurarsi che gli utenti admin stiano autenticando con nsswitch e che l'autenticazione LDAP fast bind sia attivata nei propri account.

   - Per gli utenti esistenti, immettere `security login modify` e verificare le seguenti impostazioni dei parametri:

     `-authentication-method nsswitch`

   `-is-ldap-fastbind true`

   - Per i nuovi utenti admin, vedere "Abilitare l'accesso all'account LDAP o NIS."

Visualizzare le statistiche LDAP

A partire da ONTAP 9.2, è possibile visualizzare le statistiche LDAP per le macchine virtuali di storage (SVM) su un sistema storage per monitorare le performance e diagnosticare i problemi.

Di cosa hai bisogno

- È necessario aver configurato un client LDAP su SVM.
- Gli oggetti LDAP da cui è possibile visualizzare i dati devono essere stati identificati.

Fase

1. Visualizzare i dati delle performance per gli oggetti del contatore:

   ```
   statistics show
   ```

Esempi

Nell'esempio riportato di seguito vengono illustrati i dati relativi alle prestazioni per l'oggetto `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```