LDAP verwenden

ONTAP 9

NetApp
January 08, 2026

Inhalt

LDAP verwenden

Erfahren Sie mehr über LDAP für ONTAP NFS SVMs

Ein LDAP-Server (Lightweight Directory Access Protocol) ermöglicht die zentrale Verwaltung von Benutzerinformationen. Wenn Sie Ihre Benutzerdatenbank auf einem LDAP-Server in Ihrer Umgebung speichern, können Sie Ihr Speichersystem so konfigurieren, dass Benutzerinformationen in Ihrer bestehenden LDAP-Datenbank angezeigt werden.

- Bevor Sie LDAP für ONTAP konfigurieren, sollten Sie überprüfen, ob die Standortbereitstellung die Best Practices für die LDAP-Server- und Client-Konfiguration erfüllt. Insbesondere sind folgende Voraussetzungen zu erfüllen:
  - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.
  - Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen die von ONTAP unterstützten LDAP-Benutzerpasswort-Typen enthalten:
    - CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
    - Beginnend mit ONTAP 9.8, SHA-2-Hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 und SSHA-512) werden ebenfalls unterstützt.
  - Wenn für den LDAP-Server Sitzungssicherheitsmaßnahmen erforderlich sind, müssen Sie diese im LDAP-Client konfigurieren.

    Folgende Sicherheitsoptionen sind verfügbar:

    - LDAP-Signatur (bietet Datenintegritätsprüfung) und LDAP-Signing and Sealing (bietet Datenintegritätsprüfung und -Verschlüsselung)
    - STARTEN SIE TLS
    - LDAPS (LDAP über TLS oder SSL)
  - Um signierte und versiegelte LDAP-Abfragen zu aktivieren, müssen die folgenden Dienste konfiguriert sein:
    - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
    - LDAP-Server müssen DNS-A/AAAA-Datensätze sowie PTR-Datensätze auf dem DNS-Server eingerichtet haben.
    - Kerberos-Server müssen über SRV-Datensätze auf dem DNS-Server verfügen.
  - Um TLS ODER LDAPS ZU STARTEN, sollten die folgenden Punkte berücksichtigt werden.
    - Es handelt sich hierbei um eine NetApp Best Practice, Start TLS statt LDAPS zu verwenden.
    - Wenn LDAPS verwendet wird, muss der LDAP-Server für TLS oder für SSL in ONTAP 9.5 und höher aktiviert sein. SSL wird in ONTAP 9.4 – 9.0 nicht unterstützt.
    - Ein Zertifikatsserver muss bereits in der Domäne konfiguriert sein.
  - Um LDAP-Verweisungsjagd zu ermöglichen (in ONTAP 9.5 und höher), müssen die folgenden Bedingungen erfüllt sein:
    - Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert werden:
      - Zwei-Wege

        - Eine Möglichkeit, bei der der primäre vertraut auf die Empfehlungsdomäne
        - Elternteil-Kind
    - DNS muss so konfiguriert sein, dass alle genannten Servernamen aufgelöst werden.
    - Domänenpasswörter müssen für die Authentifizierung identisch sein, wenn `--bind-as-cifs-server` sie auf true gesetzt sind.

> Die folgenden Konfigurationen werden mit LDAP-Referenznachverfolgungsjagd nicht unterstützt.
>
> - Für alle ONTAP-Versionen:
> - LDAP-Clients auf einer Administrator-SVM
> - Für ONTAP 9.8 und frühere Versionen (unterstützt ab 9.9.1):
> - LDAP-Signing and Sealing (`-session-security`optional)
> - Verschlüsselte TLS-Verbindungen (`-use-start-tls`Option)
> - Kommunikation über LDAPS-Port 636 (`-use-ldaps-for-ad-ldap`optional)

- Ab ONTAP 9.11.1 können Sie verwenden "Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs."
- Sie müssen beim Konfigurieren des LDAP-Clients auf der SVM ein LDAP-Schema eingeben.

  In den meisten Fällen ist eines der Standard-ONTAP-Schemas angemessen. Wenn sich das LDAP-Schema in Ihrer Umgebung jedoch von diesen unterscheidet, müssen Sie ein neues LDAP-Client-Schema für ONTAP erstellen, bevor Sie den LDAP-Client erstellen. Wenden Sie sich an Ihren LDAP-Administrator, um die Anforderungen Ihrer Umgebung zu besprechen.

- Die Verwendung von LDAP für die Auflösung des Host-Namens wird nicht unterstützt.

Weitere Informationen finden Sie unter "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP".

Erfahren Sie mehr über die LDAP-Signierung und -Versiegelung für ONTAP NFS SVMs

Ab ONTAP 9 können Sie Signing and Sealing konfigurieren, um die LDAP-Sitzungssicherheit bei Anfragen an einen Active Directory-Server (AD) zu aktivieren. Sie müssen die Sicherheitseinstellungen des NFS-Servers auf der Storage Virtual Machine (SVM) so konfigurieren, dass sie den auf dem LDAP-Server entsprechen.

Das Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe der Geheimschlüsseltechnologie. Das Sealing verschlüsselt die LDAP-Nutzlastdaten, um das Übertragen sensibler Informationen als unverschlüsselten Text zu vermeiden. Die Option *LDAP Security Level* gibt an, ob der LDAP-Datenverkehr signiert, signiert und versiegelt werden muss oder nicht. Die Standardeinstellung ist `none`. Test

LDAP-Signing und Sealing auf SMB-Traffic wird auf der SVM mit der `-session-security-for-ad-ldap` Option zum `vserver cifs security modify` Befehl aktiviert.

Erfahren Sie mehr über LDAPS für ONTAP NFS SVMs

Sie müssen bestimmte Begriffe und Konzepte verstehen, wie ONTAP die LDAP-Kommunikation sichert. ONTAP kann TLS ODER LDAPS STARTEN, um authentifizierte Sitzungen zwischen Active Directory-integrierten LDAP-Servern oder UNIX-basierten LDAP-Servern einzurichten.

Terminologie

Es gibt bestimmte Begriffe, die Sie verstehen sollten, wie ONTAP LDAPS verwendet, um LDAP-Kommunikation zu sichern.

- **LDAP**

  (Lightweight Directory Access Protocol) Ein Protokoll für den Zugriff auf und das Management von Informationsverzeichnissen. LDAP wird als Informationsverzeichnis zum Speichern von Objekten wie Benutzern, Gruppen und Netzwerkgruppen verwendet. LDAP bietet außerdem Verzeichnisdienste, die diese Objekte verwalten und LDAP-Anforderungen von LDAP-Clients erfüllen.

- * SSL*

  (Secure Sockets Layer) Ein Protokoll, das zum sicheren Versenden von Informationen über das Internet entwickelt wurde. SSL wird von ONTAP 9 und höher unterstützt, wurde jedoch zugunsten von TLS veraltet.

- **TLS**

  (Transport Layer Security) ein IETF-Standards-Protokoll, das auf den früheren SSL-Spezifikationen basiert. Es ist der Nachfolger von SSL. TLS wird von ONTAP 9.5 und höher unterstützt.

- **LDAPS (LDAP über SSL oder TLS)**

  Ein Protokoll, das TLS oder SSL zur sicheren Kommunikation zwischen LDAP-Clients und LDAP-Servern verwendet. Die Begriffe *LDAP über SSL* und *LDAP über TLS* werden manchmal synonym verwendet. LDAPS wird von ONTAP 9.5 und höher unterstützt.

  - In ONTAP 9.8-9.5 kann LDAPS nur auf Port 636 aktiviert werden. Verwenden Sie dazu die `-use -ldaps-for-ad-ldap` Parameter mit dem `vserver cifs security modify` Befehl.
  - Ab ONTAP 9.9 kann LDAPS auf jedem Port aktiviert werden, obwohl Port 636 weiterhin der Standard bleibt. Setzen Sie dazu den `-ldaps-enabled` Parameter auf `true` und geben Sie den gewünschten `-port` Parameter an. Erfahren Sie mehr über `vserver services name-service ldap client create` in der "ONTAP-Befehlsreferenz".

  > Es handelt sich hierbei um eine NetApp Best Practice, Start TLS statt LDAPS zu verwenden.

- **TLS starten**

  (Auch bekannt als *Start_tls*, *STARTTLS* und *StartTLS*) Ein Mechanismus zur sicheren Kommunikation mittels TLS-Protokollen.

  ONTAP verwendet STARTTLS zur Sicherung der LDAP-Kommunikation und verwendet den Standard-LDAP-Port (389) zur Kommunikation mit dem LDAP-Server. Der LDAP-Server muss so konfiguriert sein, dass Verbindungen über den LDAP-Port 389 zuzulassen. Andernfalls schlagen LDAP-TLS-Verbindungen

von der SVM zum LDAP-Server fehl.

So nutzt ONTAP LDAPS

ONTAP unterstützt die TLS-Serverauthentifizierung, sodass der SVM-LDAP-Client die Identität des LDAP-Servers während des Bindungsvorgangs bestätigen kann. TLS-fähige LDAP-Clients können mithilfe von Standardverfahren für Public-Key-Kryptografie überprüfen, ob das Zertifikat und die öffentliche ID eines Servers gültig sind und von einer Zertifizierungsstelle ausgestellt wurden, die in der Liste vertrauenswürdiger CAS des Clients aufgeführt ist.

LDAP unterstützt STARTTLS zur Verschlüsselung der Kommunikation mit TLS. STARTTLS beginnt als Klartext-Verbindung über den Standard-LDAP-Port (389) und wird dann auf TLS aktualisiert.

ONTAP unterstützt Folgendes:

- LDAPS für SMB-bezogenen Datenverkehr zwischen den durch Active Directory integrierten LDAP-Servern und der SVM
- LDAPS für LDAP-Datenverkehr für Namenszuweisung und andere UNIX-Informationen

  Entweder in Active Directory integrierte LDAP-Server oder UNIX-basierte LDAP-Server können zum Speichern von Informationen für die LDAP-Namenszuweisung und andere UNIX-Informationen verwendet werden, z. B. Benutzer, Gruppen und Netzwerkgruppen.

- Selbstsignierte Root-CA-Zertifikate

  Bei Verwendung eines in Active Directory integrierten LDAP wird das selbstsignierte Stammzertifikat generiert, wenn der Windows Server Certificate Service in der Domäne installiert wird. Bei Verwendung eines UNIX-basierten LDAP-Servers zur LDAP-Namenszuweisung wird das selbstsignierte Stammzertifikat generiert und unter Verwendung der für diese LDAP-Anwendung geeigneten Mittel gespeichert.

LDAPS ist standardmäßig deaktiviert.

Aktivieren Sie die LDAP RFC2307bis-Unterstützung für ONTAP NFS SVMs

Wenn Sie LDAP verwenden möchten und die zusätzliche Funktion benötigen, um geschachtelte Gruppenmitgliedschaften zu verwenden, können Sie ONTAP so konfigurieren, dass LDAP RFC2307bis Unterstützung aktiviert wird.

Bevor Sie beginnen

Sie müssen eine Kopie eines der Standard-LDAP-Client-Schemas erstellt haben, die Sie verwenden möchten.

Über diese Aufgabe

In LDAP-Client-Schemata verwenden Gruppenobjekte das Attribut memberUid. Dieses Attribut kann mehrere Werte enthalten und listet die Namen der Benutzer auf, die zu dieser Gruppe gehören. In RFC2307bis aktivierten LDAP-Client-Schemas verwenden Gruppenobjekte das Attribut uniqueMember. Dieses Attribut kann den vollständigen Distinguished Name (DN) eines anderen Objekts im LDAP-Verzeichnis enthalten. Damit können Sie verschachtelte Gruppen verwenden, da Gruppen andere Gruppen als Mitglieder haben können.

Der Benutzer darf nicht Mitglied von mehr als 256 Gruppen einschließlich verschachtelter Gruppen sein.

ONTAP ignoriert alle Gruppen über das 256 Gruppenlimit.

Standardmäßig ist die Unterstützung von RFC2307bis deaktiviert.

> Die Unterstützung von RFC2307bis wird in ONTAP automatisch aktiviert, wenn ein LDAP-Client mit dem MS-AD-bis-Schema erstellt wird.

Weitere Informationen finden Sie unter "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP".

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Ändern Sie das kopierte RFC2307 LDAP-Client-Schema, um die Unterstützung von RFC2307bis zu aktivieren:

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

3. Ändern Sie das Schema so, dass es mit der im LDAP-Server unterstützten Objektklasse übereinstimmt:

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

4. Ändern Sie das Schema so, dass es mit dem im LDAP-Server unterstützten Attributnamen übereinstimmt:

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

5. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

ONTAP NFS-Konfigurationsoptionen für LDAP-Verzeichnissuchen

Sie können LDAP-Verzeichnissuches, einschließlich Benutzer-, Gruppen- und Netzwerkgruppeninformationen, optimieren, indem Sie den ONTAP LDAP-Client so konfigurieren, dass eine Verbindung zu LDAP-Servern auf die für Ihre Umgebung am besten geeignete Weise hergestellt wird. Sie müssen wissen, wann die Standard-LDAP-Basis- und Bereichssuche ausreichen und welche Parameter angegeben werden sollen, wenn benutzerdefinierte Werte besser geeignet sind.

LDAP-Client-Suchoptionen für Benutzer-, Gruppen- und Netzwerkgruppeninformationen können dazu beitragen, fehlerhafte LDAP-Abfragen zu vermeiden, und damit einen fehlgeschlagenen Client-Zugriff auf Speichersysteme. Sie tragen außerdem dazu bei, dass die Suchvorgänge so effizient wie möglich sind, um Probleme mit der Client-Performance zu vermeiden.

Standardwerte für die Basis- und Bereichssuche

Die LDAP-Basis ist der Standard-Basis-DN, den der LDAP-Client zur Durchführung von LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netgroup-Suchen, werden mit dem Basis-DN durchgeführt. Diese Option ist geeignet, wenn Ihr LDAP-Verzeichnis relativ klein ist und alle relevanten Einträge im selben DN liegen.

Wenn Sie keinen benutzerdefinierten Basis-DN angeben, ist der Standardwert `root` . Das bedeutet, dass jede Abfrage das gesamte Verzeichnis durchsucht. Dies maximiert zwar die Erfolgsaussichten der LDAP-Abfrage, kann aber ineffizient sein und bei großen LDAP-Verzeichnissen zu einer deutlich geringeren Leistung führen.

Der Umfang der LDAP-Basis ist der Standard-Suchumfang, den der LDAP-Client zur Durchführung von LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netgroup-Suchen, werden mit dem Basisumfang durchgeführt. Es legt fest, ob die LDAP-Abfrage nur den benannten Eintrag durchsucht, eine Ebene unterhalb des DN eingibt oder die gesamte Unterstruktur unter dem DN.

Wenn Sie keinen benutzerdefinierten Basisumfang angeben, ist der Standardwert `subtree` . Das bedeutet, dass jede Abfrage die gesamte Unterstruktur unter dem DN durchsucht. Dies maximiert zwar die Erfolgsaussichten der LDAP-Abfrage, kann aber ineffizient sein und bei großen LDAP-Verzeichnissen zu einer deutlich geringeren Leistung führen.

Benutzerdefinierte Basis- und Bereichssuche

Optional können Sie separate Basis- und Bereichwerte für Benutzer-, Gruppen- und Netzgruppensuchen festlegen. Eine Begrenzung der Such-Basis und des Umfangs von Abfragen auf diese Weise kann die Leistung erheblich verbessern, da die Suche auf einen kleineren Unterabschnitt des LDAP-Verzeichnisses beschränkt wird.

Wenn Sie benutzerdefinierte Basis- und Bereichwerte angeben, überschreiben sie die allgemeine Standardsuchbasis und den Umfang für Benutzer-, Gruppen- und Netzgruppensuchen. Die Parameter zum Festlegen benutzerdefinierter Basis- und Bereichwerte sind auf der erweiterten Berechtigungsebene verfügbar.

LDAP-Client-Parameter…	Gibt Benutzerdefiniert an…
`-base-dn`	Basis-DN für alle LDAP-Suchen. Bei Bedarf können mehrere Werte eingegeben werden (z. B. wenn die LDAP-Referral-Chasing-Funktion in ONTAP 9.5 und späteren Versionen aktiviert ist).
`-base-scope`	Basisbereich für alle LDAP-Suchen.
`-user-dn`	Basis-DNs für alle LDAP-Benutzersuchen. Dieser Parameter gilt auch für die Suche nach Benutzernamenzuordnungen.
`-user-scope`	Basisbereich für alle LDAP-Benutzersuchen. Dieser Parameter gilt auch für die Suche nach Benutzernamenzuordnungen.
`-group-dn`	Basis-DNs für alle LDAP-Gruppensuchen.
`-group-scope`	Basisbereich für alle LDAP-Gruppensuchen.

`-netgroup-dn`	Basis-DNs für alle LDAP-Netzgruppensuchen.
`-netgroup-scope`	Basisbereich für alle LDAP-Netzgruppensuchen.

Mehrere benutzerdefinierte Basis-DN-Werte

Wenn Ihre LDAP-Verzeichnisstruktur komplexer ist, ist es möglicherweise erforderlich, dass Sie mehrere Basis-DNS angeben, um mehrere Teile Ihres LDAP-Verzeichnisses nach bestimmten Informationen zu durchsuchen. Sie können mehrere DNS für die DN-Parameter Benutzer, Gruppen und Netzwerkgruppen festlegen, indem Sie diese mit einem Semikolon (;) trennen und die gesamte DN-Suchliste mit doppelten Anführungszeichen (") schließen. Wenn ein DN ein Semikolon enthält, müssen Sie unmittelbar vor dem Semikolon im DN ein Escape-Zeichen (\) hinzufügen.

Der Umfang gilt für die gesamte für den entsprechenden Parameter angegebene DNS-Liste. Wenn Sie beispielsweise eine Liste mit drei verschiedenen Benutzer-DNS und Unterstrukturen für den Benutzerbereich angeben, sucht der LDAP-Benutzer die gesamte Unterstruktur für jedes der drei angegebenen DNS.

Ab ONTAP 9.5 können Sie auch LDAP *Referral Chasing* angeben, wodurch der ONTAP LDAP-Client Look-up-Anfragen an andere LDAP-Server weiterleiten kann, wenn keine LDAP-Referral-Antwort vom primären LDAP-Server zurückgegeben wird. Der Client verwendet diese Verweisdaten, um das Zielobjekt vom in den Empfehlungsdaten beschriebenen Server abzurufen. Um nach Objekten zu suchen, die in den genannten LDAP-Servern vorhanden sind, kann der Basis-dn der genannten Objekte im Rahmen der LDAP-Client-Konfiguration dem Basis-dn hinzugefügt werden. Referenzierten Objekten wird jedoch nur nachgesucht, wenn die Suche nach Empfehlungen aktiviert ist (mit der `-referral-enabled true` Option), während LDAP-Clienterstellung oder -Änderung.

Benutzerdefinierte LDAP-Suchfilter

Sie können den Parameter der LDAP-Konfigurationsoption verwenden, um einen benutzerdefinierten Suchfilter zu erstellen. Der `-group-membership-filter` Parameter gibt den Suchfilter an, der verwendet werden soll, wenn die Gruppenmitgliedschaft von einem LDAP-Server abgerufen wird.

Ein Beispiel für gültige Filter sind:

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

Erfahren Sie mehr über "So konfigurieren Sie LDAP in ONTAP".

Verbessern Sie die Leistung von LDAP-Verzeichnis-Netgroup-by-Host-Suchen für ONTAP NFS SVMs

Wenn Ihre LDAP-Umgebung so konfiguriert ist, dass sie Netgroup-by-Host-Suchen zuzulassen, können Sie ONTAP so konfigurieren, dass sie dies nutzt und Netgroup-by-Host-Suchen durchführen. Dies kann die Netgroup-Suche erheblich beschleunigen und mögliche Probleme beim NFS-Client-Zugriff aufgrund der Latenz bei der Suche in einer Netzgruppe verringern.

Bevor Sie beginnen

Ihr LDAP-Verzeichnis muss eine `netgroup.byhost` Zuordnung enthalten.

Ihre DNS-Server sollten sowohl vorwärts (A) als auch rückwärts (PTR) Suchdatensätze für NFS-Clients enthalten.

Wenn Sie IPv6-Adressen in Netzgruppen angeben, müssen Sie jede Adresse wie in RFC 5952 angegeben kürzen und komprimieren.

Über diese Aufgabe

NIS-Server speichern Netzgruppeninformationen in drei separaten Maps namens `netgroup`, `netgroup.byuser` und `netgroup.byhost`. Der Zweck der `netgroup.byuser` and `netgroup.byhost` Maps ist die Beschleunigung der Suche nach Netzgruppen. ONTAP führt Netgroup-by-Host-Suchen auf NIS Servern durch und verbessert so die Mount-Reaktionszeiten.

Standardmäßig verfügen LDAP-Verzeichnisse nicht über eine solche `netgroup.byhost` Zuordnung wie NIS-Server. Es ist jedoch möglich, mit Hilfe von Tools von Drittanbietern eine NIS- `netgroup.byhost`Map in LDAP-Verzeichnisse zu importieren, um eine schnelle Netzgruppensuche pro Host zu ermöglichen. Wenn Sie Ihre LDAP-Umgebung so konfiguriert haben, dass netgroup-by-Host-Suchen `netgroup.byhost` möglich sind, können Sie den ONTAP-LDAP-Client mit dem Zuordnungsnamen, DN und dem Suchbereich für schnellere Netzgruppen-by-Host-Suchen konfigurieren.

Wenn ONTAP die Ergebnisse für netzgruppenspezifische Host-Suchen schneller erhalten, kann Exportregeln schneller verarbeiten, wenn NFS-Clients Zugriff auf Exporte anfordern. Dies verringert die Wahrscheinlichkeit eines verzögerten Zugriffs aufgrund von Latenzproblemen bei der netgroup-Suche.

Schritte

1. Holen Sie sich den genauen vollständigen Distinguished Name der NIS- `netgroup.byhost`Zuordnung, die Sie in Ihr LDAP-Verzeichnis importiert haben.

   Der map-DN kann je nach dem Werkzeug eines Drittanbieters variieren, das Sie für den Import verwendet haben. Um eine optimale Leistung zu erzielen, sollten Sie den genauen MAP-DN angeben.

2. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
3. Aktivieren Sie die Suche von Netzgruppen pro Host in der LDAP-Client-Konfiguration der Storage Virtual Machine (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`} Aktiviert oder deaktiviert die Netzgruppensuche nach LDAP-Verzeichnissen pro Host. Der Standardwert ist `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` Gibt den Distinguished Name der `netgroup.byhost` Zuordnung im LDAP-Verzeichnis an. Es überschreibt den Basis-DN für Netgroup-by-Host-Suchen. Wenn Sie diesen Parameter nicht angeben, verwendet ONTAP stattdessen den Basis-DN.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} Gibt den Suchbereich für netzgruppenbasierte Suchvorgänge an. Wenn Sie diesen Parameter nicht angeben, ist die Standardeinstellung `subtree` .

   Wenn die LDAP-Client-Konfiguration noch nicht vorhanden ist, können Sie Netzgruppen-für-Host-Suchen aktivieren, indem Sie diese Parameter angeben, wenn `vserver services name-service ldap client create` Sie eine neue LDAP-Client-Konfiguration mit dem Befehl erstellen.

Der `-ldap-servers` Feld ersetzt das `-servers` Feld. Sie können das `-ldap-servers` , um entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server anzugeben.

4. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Beispiel

Mit dem folgenden Befehl wird die vorhandene LDAP-Client-Konfiguration mit dem Namen „`ldap_corp`“ geändert, um Netzgruppen-für-Host-Suchen unter Verwendung der `netgroup.byhost` Zuordnung „`nisMapName=„netgroup.byhost“,dc=corp,dc=example,dc=com`“ und des standardmäßigen Suchbereichs `subtree`zu ermöglichen:

```
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
```

Nachdem Sie fertig sind

Die `netgroup.byhost` und- `netgroup`Zuordnungen im Verzeichnis müssen jederzeit synchron gehalten werden, um Probleme mit dem Client-Zugriff zu vermeiden.

Verwandte Informationen

"IETF RFC 5952: Eine Empfehlung für die IPv6-Adresstext-Darstellung"

Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs

Ab ONTAP 9.11.1 können Sie die LDAP *fast BIND*-Funktionalität (auch bekannt als *Concurrent BIND*) für schnellere und einfachere Clientauthentifizierungsanforderungen nutzen. Um diese Funktion nutzen zu können, muss der LDAP-Server die Funktion für schnelles Binden unterstützen.

Über diese Aufgabe

Ohne schnelle Bindung verwendet ONTAP eine einfache LDAP-Bindung, um Administratorbenutzer mit dem LDAP-Server zu authentifizieren. Mit dieser Authentifizierungsmethode sendet ONTAP einen Benutzer- oder Gruppennamen an den LDAP-Server, empfängt das gespeicherte Hash-Passwort und vergleicht den Server-Hash-Code mit dem lokal aus dem Benutzerpasswort generierten Hash-Passcode. Sind sie identisch, gewährt ONTAP eine Anmeldegenehmigung.

Mit der F.A.S.T. BIND-Funktion sendet ONTAP über eine sichere Verbindung nur Benutzeranmeldeinformationen (Benutzername und Passwort) an den LDAP-Server. Der LDAP-Server validiert diese Anmeldedaten dann und weist ONTAP an, die Anmeldeberechtigungen zu erteilen.

Ein Vorteil von fast bind besteht darin, dass ONTAP nicht jeden neuen Hashing-Algorithmus unterstützt, der von LDAP-Servern unterstützt wird, unterstützen muss, da das Passwort-Hashing vom LDAP-Server durchgeführt wird.

"Erfahren Sie mehr über die Verwendung von fast Bind."

Vorhandene LDAP-Clientkonfigurationen können für LDAP fast Binding verwendet werden. Es wird jedoch dringend empfohlen, den LDAP-Client für TLS oder LDAPS zu konfigurieren; andernfalls wird das Passwort im

Klartext über das Kabel gesendet.

Zur Aktivierung der LDAP-F.A.S.T.-Bindung in einer ONTAP-Umgebung müssen Sie folgende Anforderungen erfüllen:

- ONTAP-Admin-Benutzer müssen auf einem LDAP-Server konfiguriert werden, der schnelle Bindungen unterstützt.
- Die ONTAP SVM muss für LDAP in der Name Services Switch (nsswitch)-Datenbank konfiguriert sein.
- ONTAP-Admin-Benutzer- und Gruppenkonten müssen für nswitch-Authentifizierung mit fast-BIND konfiguriert werden.

Schritte

1. Bestätigen Sie mit Ihrem LDAP-Administrator, dass LDAP fast BIND auf dem LDAP-Server unterstützt wird.
2. Stellen Sie sicher, dass die Anmeldedaten für ONTAP-Admin-Benutzer auf dem LDAP-Server konfiguriert sind.
3. Vergewissern Sie sich, dass der Administrator oder die Daten-SVM für LDAP fast bind richtig konfiguriert sind.

   a. Um zu bestätigen, dass der LDAP fast BIND-Server in der LDAP-Client-Konfiguration aufgeführt ist, geben Sie Folgendes ein:

      `vserver services name-service ldap client show`

      "Weitere Informationen zur LDAP-Client-Konfiguration."

   b. Um zu bestätigen, dass `ldap` es sich um eine der konfigurierten Quellen für die nsswitch `passwd` -Datenbank handelt, geben Sie Folgendes ein:

      `vserver services name-service ns-switch show`

   "Weitere Informationen zur nswitch-Konfiguration."

4. Stellen Sie sicher, dass Administratorbenutzer mit nswitch authentifizieren und die LDAP-Authentifizierung für die schnelle Bindung in ihren Konten aktiviert ist.

   ◦ Geben Sie bei vorhandenen Benutzern `security login modify` die folgenden Parametereinstellungen ein und überprüfen Sie sie:

      `-authentication-method nsswitch`

      `-is-ldap-fastbind true`

   Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

   ◦ Für neue Admin-Benutzer siehe "Aktivieren Sie den Zugriff auf das LDAP- oder NIS-ONTAP-Konto".

LDAP-Statistiken für ONTAP NFS SVMs anzeigen

Sie können LDAP-Statistiken für Storage Virtual Machines (SVMs) auf einem Speichersystem anzeigen, um die Leistung zu überwachen und Probleme zu

diagnostizieren.

Bevor Sie beginnen

- Sie müssen einen LDAP-Client auf der SVM konfiguriert haben.
- Sie müssen LDAP-Objekte identifiziert haben, von denen Sie Daten anzeigen können.

Schritt

1. Performance-Daten für Zählerobjekte anzeigen:

```
statistics show
```

Beispiele

Im folgenden Beispiel werden Statistiken für das Beispiel namens **smpl_1** für Zähler angezeigt: avg_Processor_busy und cpu_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Verwandte Informationen

- "Statistiken zeigen"
- "Statistikstart"
- "Statistikstopp"