Konfigurieren Sie Name Services

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

Konfigurieren Sie Name Services

Funktionsweise der Switch-Konfiguration für den ONTAP Name Service

ONTAP speichert Informationen zur Service-Konfiguration in einer Tabelle, die dem Äquivalent von entspricht `/etc/nsswitch.conf` File auf UNIX Systemen. Sie müssen die Funktion der Tabelle und deren Verwendung durch ONTAP kennen, damit Sie sie für Ihre Umgebung entsprechend konfigurieren können.

Die Switch-Tabelle für den ONTAP-Namensdienst legt fest, welche Namensdienstquellen ONTAP konsultiert, um Informationen für bestimmte Arten von Namensdienstinformationen abzurufen. Für jede SVM verwaltet ONTAP eine separate Name-Service-Switch-Tabelle.

Datenbanktypen

Die Tabelle enthält eine separate Namensdienstliste für jeden der folgenden Datenbanktypen:

Datenbanktyp	Definiert Namensdienstquellen für…	Gültige Quellen sind…
Hosts	Hostnamen in IP-Adressen werden konvertiert	Dateien, dns
Gruppieren	Benutzergruppeninformationen werden gesucht	Dateien, nis, ldap
Passwd	Benutzerinformationen werden gesucht	Dateien, nis, ldap
Netzgruppe	Netzgruppeninformationen werden gesucht	Dateien, nis, ldap
Namemap	Zuordnen von Benutzernamen	Dateien, ldap

Quelltypen

Die Quellen geben an, welche Namensdienstquelle zum Abrufen der entsprechenden Informationen verwendet werden soll.

Typ der Quelle angeben…	Um Informationen zu suchen in…	Verwaltet durch die Befehlsfamilien…

Dateien	Lokale Quelldateien	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Externe NIS-Server, wie in der NIS-Domain-Konfiguration der SVM angegeben	`vserver services name-service nis-domain`
ldap	Externe LDAP-Server, wie in der LDAP-Client-Konfiguration der SVM angegeben	`vserver services name-service ldap`
dns	Externe DNS-Server, die in der DNS-Konfiguration der SVM angegeben sind	`vserver services name-service dns`

Selbst wenn Sie NIS oder LDAP sowohl für den Datenzugriff als auch zur SVM-Administration-Authentifizierung verwenden möchten, sollten Sie weiterhin einschließen `files` Und konfigurieren Sie lokale Benutzer als Fallback, falls die NIS- oder LDAP-Authentifizierung fehlschlägt.

Protokolle für den Zugriff auf externe Quellen

Für den Zugriff auf die Server für externe Quellen verwendet ONTAP die folgenden Protokolle:

Externe Servicequelle	Für den Zugriff verwendetes Protokoll
NIS	UDP
DNS	UDP
LDAP	TCP

Beispiel

Im folgenden Beispiel wird die Switch-Konfiguration für den Namensservice für die SVM svm_1 angezeigt:

```
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
```

Um IP-Adressen für Hosts zu suchen, konsultiert ONTAP First lokale Quelldateien. Wenn die Abfrage keine Ergebnisse liefert, werden DNS-Server als nächstes überprüft.

Um Benutzer- oder Gruppeninformationen zu suchen, konsultiert ONTAP nur lokale Quelldateien. Wenn die Abfrage keine Ergebnisse liefert, schlägt die Suche fehl.

Um Informationen zu Netzgruppen zu suchen, konsultiert ONTAP First externe NIS-Server. Wenn die Abfrage keine Ergebnisse liefert, wird die lokale Netzgruppedatei als nächstes geprüft.

In der Tabelle für svm_1 sind keine Namensdiensteinträge für die Namenszuweisung vorhanden. Daher konsultiert ONTAP standardmäßig nur lokale Quelldateien.

Verwandte Informationen

"NetApp Technical Report 4668: Name Services Best Practices Guide"

LDAP verwenden

LDAP – Übersicht

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.
- Bei Verwendung von LDAPS muss der LDAP-Server für TLS oder für SSL in ONTAP 9.5 und höher aktiviert sein. SSL wird in ONTAP 9.0-9.4 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 sollten für die Authentifizierung identisch sein, wenn `--bind-as-cifs-server` Auf „true“ setzen.

> 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 (das `-session-security` Option)
> ◦ Verschlüsselte TLS-Verbindungen (das `-use-start-tls` Option)
> ◦ Kommunikation über LDAPS-Port 636 (der `-use-ldaps-for-ad-ldap` Option)

- Ab ONTAP 9.11.1 können Sie dies nutzen "LDAP fast bind für nsswitch-Authentifizierung."
- 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 Hostnamens wird nicht unterstützt.

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

LDAP-Signing- und Sealing-Konzepte

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 lautet `none`. Test

Das LDAP-Signing and Sealing für SMB-Datenverkehr wird auf der SVM mit dem aktiviert `-session -security-for-ad-ldap` Option für die `vserver cifs security modify` Befehl.

LDAPS-Konzepte

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. Es wurde zugunsten von TLS abgelehnt. SSL wird in ONTAP 9.0-9.4 nicht unterstützt.

- **TLS**

  (Transport Layer Security) ein IETF-Standards-Protokoll, das auf den früheren SSL-Spezifikationen basiert. Es ist der Nachfolger von SSL.

- **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; TLS wird von ONTAP 9 und höher unterstützt, SSL wird von ONTAP 9.5 und höher unterstützt.

  - In ONTAP 9.5-9.8 kann LDAPS nur auf Port 636 aktiviert werden. Verwenden Sie dazu den `-use -ldaps-for-ad-ldap` Parameter mit `vserver cifs security modify` Befehl.
  - Ab ONTAP 9.9 kann LDAPS auf jedem Port aktiviert werden, obwohl Port 636 weiterhin der Standard bleibt. Stellen Sie dazu den ein `-ldaps-enabled` Parameter an `true` Und geben Sie die gewünschte an `-port` Parameter. Weitere Informationen finden Sie im `vserver services name-service ldap client create` Man-Page

  > 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

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.

Was Sie benötigen

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
```

Konfigurationsoptionen für LDAP-Verzeichnissuches

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 die Standardeinstellung `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 Basisbereich angeben, wird der Standardwert verwendet `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-Suchebei Bedarf können mehrere Werte eingegeben werden (z. B. wenn LDAP-Weiterleitung in ONTAP 9.5 und späteren Versionen aktiviert ist).
`-base-scope`	Basisumfang für alle LDAP-Suchvorgänge
`-user-dn`	Basis-DNS für alle LDAP-BenutzersucheDieser Parameter gilt auch für die Suche nach Benutzernamen.
`-user-scope`	Basisumfang für alle LDAP-Benutzersuchen dieser Parameter gilt auch für die Suche nach dem User Name-Mapping.
`-group-dn`	Basis-DNS für alle LDAP-Gruppensuchen
`-group-scope`	Basisumfang für alle LDAP-Gruppensuchen
`-netgroup-dn`	Basis-DNS für alle LDAP-Netzgruppentsuche
`-netgroup-scope`	Basisumfang für alle LDAP-Netzgruppentsuche

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. Referenzobjekte werden jedoch nur dann gesucht, wenn die Verweisungsjagd aktiviert ist (mit dem `-referral-enabled true` Option) während der Erstellung oder Änderung von LDAP-Clients.

Verbesserung der Performance von LDAP-Verzeichnis Netzgroup-by-Host-Suchen

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.

Was Sie benötigen

Ihr LDAP-Verzeichnis muss ein enthalten `netgroup.byhost` Zuordnen:

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 Netzwerkgruppeninformationen in drei separaten, so genannten Zuordnungen `netgroup`, `netgroup.byuser`, und `netgroup.byhost`. Der Zweck des `netgroup.byuser` Und `netgroup.byhost` Karten sollen die Suche in Netzgruppen beschleunigen. ONTAP führt Netgroup-by-Host-Suchen auf NIS Servern durch und verbessert so die Mount-Reaktionszeiten.

LDAP-Verzeichnisse verfügen standardmäßig nicht über eine solche `netgroup.byhost` Zuordnung wie NIS-Server Es ist jedoch möglich, mit Hilfe von Drittanbieter-Tools einen NIS zu importieren `netgroup.byhost` In LDAP-Verzeichnissen zuordnen, um schnelle netzgruppenspezifische Suche zu ermöglichen. Wenn Sie Ihre LDAP-Umgebung so konfiguriert haben, dass sie Netgroup-by-Host-Suchen zulässt, können Sie den ONTAP LDAP-Client mit dem konfigurieren `netgroup.byhost` Kartenname, DN und Suchumfang für schnellere Suche nach Netzgruppen nach Host.

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 des 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 von netgroup-by-Host-Suchen 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 netgroup-by-Host-Suche nach LDAP-Verzeichnissen. Die Standardeinstellung lautet `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` Gibt den Distinguished Name des an `netgroup.byhost` Zuordnung im LDAP-Verzeichnis 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 Suchumfang für Netgroup-by-Host-Suchen an. Wenn Sie diesen Parameter nicht angeben, wird der Standardwert verwendet `subtree`.

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

> Ab ONTAP 9.2 Field Portal `-ldap-servers` Ersetzt das Feld `-servers`. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server verwenden.

4. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Mit dem folgenden Befehl wird die vorhandene LDAP-Client-Konfiguration „`ldap_corp`“ geändert, um netgroup-by-Host-Suchen mit dem zu aktivieren `netgroup.byhost` Zuordnung mit dem Namen „`nisMapName=„netgroup.byhost“,dc=corp,dc=example,dc=com`“ und Standardsuchumfang `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
```

Nachdem Sie fertig sind

Der `netgroup.byhost` Und `netgroup` Karten im Verzeichnis müssen stets synchron gehalten werden, um Clientzugriffsprobleme zu vermeiden.

Verwandte Informationen

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

Verwenden Sie LDAP fast bind für die nswitch-Authentifizierung

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 das zu bestätigen `ldap` Ist eine der konfigurierten Quellen für den nswitch `passwd` Datenbank, geben Sie 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 für bestehende Benutzer ein `security login modify` Und überprüfen Sie die folgenden Parametereinstellungen:

      `-authentication-method nsswitch`

   `-is-ldap-fastbind true`

   ◦ Informationen zu neuen Admin-Benutzern finden Sie unter "Aktivieren Sie den LDAP- oder NIS-Kontozugriff."

Zeigt LDAP-Statistiken an

Ab ONTAP 9.2 können Sie LDAP-Statistiken für Storage Virtual Machines (SVMs) auf einem Storage-System anzeigen, um die Performance zu überwachen und Probleme zu

diagnostizieren.

Was Sie benötigen

- 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

Das folgende Beispiel zeigt die Performance-Daten für das Objekt `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
```

Copyright-Informationen

Markeninformationen