Verwalten der Sicherheitseinstellungen für SMB-Server

ONTAP 9

NetApp
April 24, 2024

Inhalt

Verwalten der Sicherheitseinstellungen für SMB-Server

Wie ONTAP mit der SMB-Client-Authentifizierung umgeht

Bevor Benutzer SMB-Verbindungen für den Zugriff auf Daten in der SVM erstellen können, müssen sie von der Domäne authentifiziert werden, zu der der SMB-Server gehört. Der SMB-Server unterstützt zwei Authentifizierungsmethoden: Kerberos und NTLM (NTLMv1 oder NTLMv2). Kerberos ist die Standardmethode zur Authentifizierung von Domänenbenutzern.

Kerberos Authentifizierung

ONTAP unterstützt Kerberos-Authentifizierung bei der Erstellung authentifizierter SMB-Sessions.

Kerberos ist der primäre Authentifizierungsservice für Active Directory. Der Kerberos-Server oder der Kerberos Key Distribution Center-Service (KDC) speichert und ruft Informationen über Sicherheitsprinzipien im Active Directory ab. Im Gegensatz zum NTLM-Modell wenden sich Active Directory-Clients, die eine Sitzung mit einem anderen Computer, wie dem SMB-Server, herstellen möchten, direkt an ein KDC, um ihre Sitzungsanmeldeinformationen zu erhalten.

NTLM-Authentifizierung

Die NTLM-Client-Authentifizierung erfolgt mithilfe eines Protokolls für die Sicherheitsantwort, das auf einem gemeinsam genutzten Wissen über ein benutzerspezifisches Geheimnis basiert.

Wenn ein Benutzer eine SMB-Verbindung unter Verwendung eines lokalen Windows-Benutzerkontos erstellt, wird die Authentifizierung lokal vom SMB-Server mithilfe von NTLMv2 durchgeführt.

Richtlinien für die Sicherheitseinstellungen von SMB-Servern in einer SVM-Disaster-Recovery-Konfiguration

Vor dem Erstellen einer SVM, die als Disaster-Recovery-Ziel konfiguriert ist und wo die Identität nicht erhalten wird (des `-identity-preserve` Die Option ist auf festgelegt `false` In der SnapMirror Konfiguration) ist zu wissen, wie SMB-Server-Sicherheitseinstellungen auf der Ziel-SVM verwaltet werden.

- Nicht standardmäßige SMB-Server-Sicherheitseinstellungen werden nicht auf das Ziel repliziert.

  Wenn Sie einen SMB-Server auf der Ziel-SVM erstellen, sind alle SMB-Server-Sicherheitseinstellungen auf die Standardwerte festgelegt. Wenn das SVM Disaster-Recovery-Ziel initialisiert, aktualisiert oder neu synchronisiert wird, werden die SMB-Server-Sicherheitseinstellungen auf der Quelle nicht zum Ziel repliziert.

- Sie müssen die Sicherheitseinstellungen für nicht standardmäßige SMB-Server manuell konfigurieren.

  Wenn Sie auf der Quell-SVM nicht standardmäßige SMB-Server-Sicherheitseinstellungen konfiguriert haben, müssen Sie diese Einstellungen nach Lese-/Schreibzugriff des Ziels manuell auf der Ziel-SVM konfigurieren (nachdem die SnapMirror Beziehung unterbrochen wurde).

Zeigt Informationen zu SMB-Serversicherheitseinstellungen an

Sie können Informationen über die Sicherheitseinstellungen von SMB-Servern auf Ihren Storage Virtual Machines (SVMs) anzeigen. Mit diesen Informationen können Sie überprüfen, ob die Sicherheitseinstellungen korrekt sind.

Über diese Aufgabe

Eine angezeigte Sicherheitseinstellung kann der Standardwert für dieses Objekt oder ein nicht-Standardwert sein, der entweder über die ONTAP-CLI oder über Active Directory-Gruppenrichtlinienobjekte konfiguriert wird.

Verwenden Sie das nicht `vserver cifs security show` Befehl für SMB-Server im Workgroup-Modus, da einige der Optionen nicht gültig sind.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Alle Sicherheitseinstellungen auf einer angegebenen SVM	`vserver cifs security show -vserver` *`vserver_name`*
Eine bestimmte Sicherheitseinstellungen oder -Einstellungen für die SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` Sie können eingeben `-fields ?` Um zu bestimmen, welche Felder Sie verwenden können.

Beispiel

Im folgenden Beispiel werden alle Sicherheitseinstellungen für SVM vs1 dargestellt:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
              Is Password Complexity Required:        true
         Use start_tls For AD LDAP connection:        false
                    Is AES Encryption Enabled:        false
                       LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                   Is SMB Encryption Required:        false
                      Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Beachten Sie, dass die angezeigten Einstellungen von der ausgeführten ONTAP-Version abhängig sind.

Das folgende Beispiel zeigt den Kerberos-Clock-Skew für SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Verwandte Informationen

Anzeigen von Informationen zu GPO-Konfigurationen

Aktivieren oder Deaktivieren der erforderlichen Passwortkomplexität für lokale SMB-Benutzer

Die erforderliche Komplexität von Passwörtern erhöht die Sicherheit von lokalen SMB-Benutzern auf Ihren Storage Virtual Machines (SVMs). Die Funktion für die erforderliche Passwortkomplexität ist standardmäßig aktiviert. Sie können sie jederzeit deaktivieren und erneut aktivieren.

Bevor Sie beginnen

Lokale Benutzer, lokale Gruppen und lokale Benutzerauthentifizierung müssen auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Sie dürfen das nicht verwenden `vserver cifs security modify` Befehl für einen CIFS-Server im Workgroup-Modus, da einige der Optionen nicht gültig sind.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die erforderliche Passwortkomplexität für lokale SMB-Benutzer…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Deaktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Überprüfen Sie die Sicherheitseinstellung für die erforderliche Passwortkomplexität: `vserver cifs security show -vserver` *`vserver_name`*

Beispiel

Das folgende Beispiel zeigt, dass die erforderliche Komplexität des Passworts für lokale SMB-Benutzer in SVM vs1 aktiviert wird:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Verwandte Informationen

Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers

Verwendung lokaler Benutzer und Gruppen zur Authentifizierung und Autorisierung

Anforderungen für lokale Benutzerpasswörter

Ändern der Passwörter für lokales Benutzerkonto

Ändern Sie die Kerberos-Sicherheitseinstellungen des CIFS-Servers

Sie können bestimmte Kerberos-Sicherheitseinstellungen des CIFS-Servers ändern, einschließlich der maximal zulässigen Skew-Zeit für Kerberos-Uhren, der Lebensdauer des Kerberos-Tickets und der maximalen Anzahl an Tagen für die Ticketverlängerung.

Über diese Aufgabe

Ändern der Kerberos-Einstellungen des CIFS-Servers mit `vserver cifs security modify` Befehl ändert die Einstellungen nur auf der einzelnen Storage Virtual Machine (SVM), die Sie mit angeben `-vserver` Parameter. Kerberos-Sicherheitseinstellungen für alle SVMs im Cluster, die zur selben Active Directory-Domäne gehören, lassen sich mithilfe von Gruppenrichtlinienobjekten (Active Directory Group Policy Objects, GPOs) zentral managen.

Schritte

1. Führen Sie eine oder mehrere der folgenden Aktionen aus:

Ihr Ziel ist	Eingeben…
Geben Sie die maximal zulässige Kerberos-Zeitversatz in Minuten (9.13.1 und höher) oder Sekunden (9.12.1 oder früher) an.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* Die Standardeinstellung ist 5 Minuten.
Geben Sie die Lebensdauer des Kerberos-Tickets in Stunden an.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` Die Standardeinstellung ist 10 Stunden.
Geben Sie die maximale Anzahl an Tagen für die Ticketverlängerung an.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* Die Standardeinstellung ist 7 Tage.
Geben Sie die Zeitüberschreitung für Sockets auf KDCs an, nach der alle KDCs als nicht erreichbar markiert sind.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* Die Standardeinstellung ist 3 Sekunden.

2. Überprüfen Sie die Kerberos-Sicherheitseinstellungen:

   `vserver cifs security show -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden die folgenden Änderungen an der Kerberos-Sicherheit vorgenommen:

„`Kerberos Clock Skew`“ ist auf 3 Minuten eingestellt und „`Kerberos Ticket Age`“ ist für SVM vs1 auf 8 Stunden eingestellt:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                   Kerberos Renewal Age:                    7 days
                   Kerberos KDC Timeout:                    3 seconds
                    Is Signing Required:               false
        Is Password Complexity Required:                true
   Use start_tls For AD LDAP connection:               false
             Is AES Encryption Enabled:                false
                LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:               false
```

Verwandte Informationen

"Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers"

"Unterstützte Gruppenrichtlinienobjekte"

"Werden Gruppenrichtlinienobjekte auf CIFS-Server angewendet"

Legen Sie die Mindestsicherheitsstufe für die Authentifizierung des SMB-Servers fest

Sie können die minimale Sicherheitsstufe für SMB-Server, auch bekannt als *LMKompatibilitätLevel*, auf Ihrem SMB-Server festlegen, um Ihre geschäftlichen Sicherheitsanforderungen für SMB-Client-Zugriff zu erfüllen. Die Mindestsicherheitsstufe ist die Mindeststufe der Sicherheitstoken, die der SMB-Server von SMB-Clients akzeptiert.

Über diese Aufgabe

- SMB-Server im Workgroup-Modus unterstützen nur NTLM-Authentifizierung. Kerberos-Authentifizierung wird nicht unterstützt.
- LmKompatibilitätLevel gilt nur für die SMB-Client-Authentifizierung, nicht für die Administratorauthentifizierung.

Sie können die Mindestsicherheitsstufe für die Authentifizierung auf eine von vier unterstützten Sicherheitsstufen festlegen.

Wert	Beschreibung
`lm-ntlm-ntlmv2-krb` (Standard)	Die Storage Virtual Machine (SVM) akzeptiert die Sicherheit der LM-, NTLM-, NTLMv2- und Kerberos-Authentifizierung.
`ntlm-ntlmv2-krb`	Die SVM akzeptiert die Authentifizierungssicherheit von NTLM, NTLMv2 und Kerberos. Die SVM bestreitet die LM-Authentifizierung.
`ntlmv2-krb`	Die SVM akzeptiert die Sicherheit der NTLMv2- und Kerberos-Authentifizierung. Die SVM leugnet die LM- und NTLM-Authentifizierung.
`krb`	Die SVM akzeptiert nur die Kerberos-Authentifizierungssicherheit. Die SVM leugnet die LM-, NTLM- und NTLMv2-Authentifizierung.

Schritte

1. Legen Sie die Mindestsicherheitsstufe für die Authentifizierung fest: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Vergewissern Sie sich, dass die Sicherheitsstufe für die Authentifizierung auf die gewünschte Stufe eingestellt ist: `vserver cifs security show -vserver vserver_name`

Verwandte Informationen

Aktivieren oder Deaktivieren der AES-Verschlüsselung für Kerberos-basierte Kommunikation

Konfigurieren Sie starke Sicherheit für Kerberos-basierte Kommunikation mithilfe von AES-Verschlüsselung

Für höchste Sicherheit mit Kerberos-basierter Kommunikation können Sie AES-256- und AES-128-Verschlüsselung auf dem SMB-Server aktivieren. Wenn Sie einen SMB-Server auf der SVM erstellen, ist die Verschlüsselung für Advanced Encryption Standard (AES) deaktiviert. Sie müssen es aktivieren, um die Vorteile der hohen Sicherheit durch AES-Verschlüsselung zu nutzen.

Die Kommunikation mit Kerberos für SMB wird während der Erstellung von SMB-Servern auf der SVM sowie während der Setup-Phase der SMB-Session verwendet. Der SMB-Server unterstützt die folgenden Verschlüsselungstypen für die Kerberos-Kommunikation:

- AES 256
- AES 128
- DES
- RC4-HMAC

Wenn Sie den höchsten Verschlüsselungstyp für Kerberos-Kommunikation nutzen möchten, sollten Sie die

AES-Verschlüsselung für Kerberos-Kommunikation auf der SVM aktivieren.

Wenn der SMB-Server erstellt wird, erstellt der Domänencontroller ein Computermaschinenkonto in Active Directory. Zu diesem Zeitpunkt wird der KDC die Verschlüsselungsfähigkeiten des jeweiligen Maschinenkontos bewusst. Anschließend wird ein bestimmter Verschlüsselungstyp für die Verschlüsselung des Service-Tickets ausgewählt, das der Client dem Server während der Authentifizierung bereitstellt.

Ab ONTAP 9.12.1 können Sie angeben, welche Verschlüsselungstypen für das Active Directory (AD) KDC angekündigt werden sollen. Sie können das verwenden `-advertised-enc-types` Option zum Aktivieren empfohlener Verschlüsselungstypen, und Sie können es verwenden, um schwächere Verschlüsselungstypen zu deaktivieren. Erfahren Sie, wie Sie "Aktiviert und deaktiviert Verschlüsselungstypen für Kerberos-basierte Kommunikation".

> Intel AES New Instructions (Intel AES NI) ist in SMB 3.0 128 verfügbar, verbessert den AES-Algorithmus und beschleunigt die Datenverschlüsselung mit unterstützten Prozessorfamilien.ab SMB 3.1.1 ersetzt AES-128-GCM als Hash-Algorithmus, der von der SMB-Verschlüsselung verwendet wird.

Verwandte Informationen

Ändern der Kerberos-Sicherheitseinstellungen des CIFS-Servers

Aktiviert oder deaktiviert die AES-Verschlüsselung für Kerberos-basierte Kommunikation

Um die höchste Sicherheit mit Kerberos-basierter Kommunikation zu nutzen, sollten Sie AES-256- und AES-128-Verschlüsselung auf dem SMB-Server verwenden. Ab ONTAP 9.13.1 ist die AES-Verschlüsselung standardmäßig aktiviert. Wenn Sie nicht möchten, dass der SMB-Server die AES-Verschlüsselungstypen für Kerberos-basierte Kommunikation mit dem Active Directory (AD) KDC wählt, können Sie die AES-Verschlüsselung deaktivieren.

Ob die AES-Verschlüsselung standardmäßig aktiviert ist und ob Sie die Möglichkeit haben, Verschlüsselungstypen anzugeben, hängt von Ihrer ONTAP-Version ab.

ONTAP-Version	AES-Verschlüsselung ist aktiviert …	Sie können Verschlüsselungstypen angeben?
9.13.1 und höher	Standardmäßig	Ja.
9.12.1	Manuell	Ja.
9.11.1 und früher	Manuell	Nein

Ab ONTAP 9.12.1 wird die AES-Verschlüsselung mit dem aktiviert und deaktiviert `-advertised-enc-types` Option, mit der Sie die Verschlüsselungstypen angeben können, die für das AD KDC angekündigt werden. Die Standardeinstellung ist `rc4` Und `des`, Wenn aber ein AES-Typ angegeben wird, ist AES-Verschlüsselung aktiviert. Sie können auch die Option verwenden, um die schwächeren RC4- und DES-Verschlüsselungstypen explizit zu deaktivieren. In ONTAP 9.11.1 und früheren Versionen müssen Sie den verwenden `-is-aes-encryption-enabled` Option zum Aktivieren und Deaktivieren von AES-Verschlüsselung, und Verschlüsselungstypen können nicht angegeben werden.

Zur Verbesserung der Sicherheit ändert die Storage Virtual Machine (SVM) bei jeder Änderung der AES-Sicherheitsoption ihr Passwort für das Computerkonto in der AD. Wenn Sie das Passwort ändern, sind möglicherweise administrative AD-Anmeldeinformationen für die Organisationseinheit (Organisationseinheit, OU) erforderlich, die das Computerkonto enthält.

Wenn eine SVM als Disaster-Recovery-Ziel konfiguriert ist, wo sie nicht erhalten wird (das `-identity -preserve` Die Option ist auf festgelegt `false` In der SnapMirror-Konfiguration) werden die nicht standardmäßigen SMB-Server-Sicherheitseinstellungen nicht auf das Ziel repliziert. Wenn Sie die AES-Verschlüsselung auf der Quell-SVM aktiviert haben, müssen Sie sie manuell aktivieren.

Beispiel 1. Schritte

ONTAP 9.12.1 und höher

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die AES-Verschlüsselungstypen für Kerberos Kommunikation…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Hinweis: Das `-is-aes-encryption-enabled` Die Option ist veraltet in ONTAP 9.12.1 und kann in einer späteren Version entfernt werden.

2. Vergewissern Sie sich, dass die AES-Verschlüsselung nach Bedarf aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Beispiele

Im folgenden Beispiel werden die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1 aktiviert:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

Im folgenden Beispiel werden die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2 aktiviert. Der Administrator wird aufgefordert, die Administrator-AD-Anmeldedaten für die Organisationseinheit einzugeben, die den SMB-Server enthält.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 und früher

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die AES-Verschlüsselungstypen für Kerberos Kommunikation…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Vergewissern Sie sich, dass die AES-Verschlüsselung nach Bedarf aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Der `is-aes-encryption-enabled` Feld wird angezeigt `true` Bei Aktivierung der AES-Verschlüsselung und `false` Wenn sie deaktiviert ist.

Beispiele

Im folgenden Beispiel werden die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1 aktiviert:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

Im folgenden Beispiel werden die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2 aktiviert. Der Administrator wird aufgefordert, die Administrator-AD-Anmeldedaten für die Organisationseinheit einzugeben, die den SMB-Server enthält.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Verwenden Sie SMB-Signing, um die Netzwerksicherheit zu erhöhen

Verwenden Sie SMB Signing, um die Übersicht über die Netzwerksicherheit zu verbessern

SMB-Signaturen tragen dazu bei, dass der Netzwerkverkehr zwischen dem SMB Server und dem Client nicht beeinträchtigt wird. Dies wird durch die Vermeidung von Wiederholungsangriffen verhindert. Standardmäßig unterstützt ONTAP SMB-Signaturen, wenn vom Client angefordert wird. Optional kann der Storage-Administrator den SMB-

Server so konfigurieren, dass SMB-Signaturen erforderlich sind.

Wie sich SMB-Signing-Richtlinien auf die Kommunikation mit einem CIFS-Server auswirken

Zusätzlich zu den SMB-Sicherheitseinstellungen des CIFS-Servers steuern zwei SMB-Signaturrichtlinien auf Windows-Clients das digitale Signieren der Kommunikation zwischen Clients und dem CIFS-Server. Sie können die Einstellung konfigurieren, die Ihren geschäftlichen Anforderungen entspricht.

Die SMB-Richtlinien für Clients werden über lokale Einstellungen für Windows-Sicherheitsrichtlinien gesteuert, die mithilfe der Microsoft Management Console (MMC) oder Active Directory-Gruppenrichtlinienobjekte konfiguriert wurden. Weitere Informationen zu SMB-Signing- und Sicherheitsproblemen des Clients finden Sie in der Microsoft Windows-Dokumentation.

Die folgenden Beschreibungen der beiden SMB-Signaturrichtlinien für Microsoft-Clients:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Diese Einstellung steuert, ob die SMB-Signing-Funktion des Clients aktiviert ist. Standardmäßig ist sie aktiviert. Wenn diese Einstellung auf dem Client deaktiviert ist, hängt die Client-Kommunikation mit dem CIFS-Server von der SMB-Signing-Einstellung auf dem CIFS-Server ab.

- `Microsoft network client: Digitally sign communications (always)`

  Diese Einstellung steuert, ob der Client SMB-Signaturen für die Kommunikation mit einem Server benötigt. Sie ist standardmäßig deaktiviert. Wenn diese Einstellung für den Client deaktiviert ist, basiert das Verhalten der SMB-Signatur auf der Richtlinieneinstellung für `Microsoft network client: Digitally sign communications (if server agrees)` Und die Einstellung auf dem CIFS-Server.

> Wenn in Ihrer Umgebung Windows Clients enthalten sind, die für SMB-Signaturen konfiguriert sind, müssen Sie SMB-Signaturen auf dem CIFS-Server aktivieren. Wenn nicht, kann der CIFS-Server diesen Systemen keine Daten bereitstellen.

Die effektiven Ergebnisse von SMB-Signing-Einstellungen für Clients und CIFS-Server hängen davon ab, ob in den SMB-Sitzungen SMB 1.0 oder SMB 2.x und höher verwendet werden.

Die folgende Tabelle fasst das effektive Verhalten von SMB-Signaturen zusammen, wenn die Sitzung SMB 1.0 verwendet:

Client	ONTAP- Signatur nicht erforderlich	ONTAP- Signatur erforderlich
Die Signatur ist deaktiviert und nicht erforderlich	Nicht signiert	Unterschrift
Das Signieren ist aktiviert und nicht erforderlich	Nicht signiert	Unterschrift

Client	ONTAP- Signatur nicht erforderlich	ONTAP- Signatur erforderlich
Die Signatur ist deaktiviert und erforderlich	Unterschrift	Unterschrift
Das Signieren ist aktiviert und erforderlich	Unterschrift	Unterschrift

Ältere Windows SMB 1-Clients und einige nicht-Windows SMB 1-Clients können möglicherweise keine Verbindung herstellen, wenn das Signieren auf dem Client deaktiviert ist, aber auf dem CIFS-Server erforderlich ist.

Die folgende Tabelle fasst das effektive Verhalten von SMB-Signaturen zusammen, wenn die Sitzung SMB 2.x oder SMB 3.0 verwendet:

Für SMB 2.x- und SMB 3.0-Clients ist SMB-Signatur immer aktiviert. Sie kann nicht deaktiviert werden.

Client	ONTAP- Signatur nicht erforderlich	ONTAP- Signatur erforderlich
Das Signieren ist nicht erforderlich	Nicht signiert	Unterschrift
Signieren erforderlich	Unterschrift	Unterschrift

Die folgende Tabelle bietet einen Überblick über das Standardverhalten der SMB-Signatur von Microsoft Client und Server:

Protokoll	Hash-Algorithmus	Kann aktiviert/deaktiviert werden	Bedarf möglich/nicht erforderlich	Client-Standard	Server-Standard	DC-Standard
SMB 1.0	MD5	Ja.	Ja.	Aktiviert (nicht erforderlich)	Deaktiviert (nicht erforderlich)	Erforderlich
SMB 2.x	HMAC SHA-256	Nein	Ja.	Nicht erforderlich	Nicht erforderlich	Erforderlich
SMB 3.0	AES-CMAC:	Nein	Ja.	Nicht erforderlich	Nicht erforderlich	Erforderlich

Microsoft empfiehlt die Verwendung nicht mehr `Digitally sign communications (if client agrees)` Oder `Digitally sign communications (if server agrees)` Einstellungen für Gruppenrichtlinien Microsoft empfiehlt auch nicht mehr die Verwendung des `EnableSecuritySignature` Registrierungseinstellungen: Diese Optionen wirken sich nur auf das Verhalten von SMB 1 aus und können durch das ersetzt werden `Digitally sign communications (always)` Einstellung für Gruppenrichtlinien oder der `RequireSecuritySignature` Registrierungseinstellung. Weitere Informationen erhalten Sie auch im Microsoft Blog.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Grundlagen der SMB-Signatur (sowohl für SMB1 als auch für SMB2)]

Auswirkungen der SMB-Signatur auf die Performance

Wenn SMB-Sitzungen SMB-Signing verwenden, wirkt sich die gesamte SMB-Kommunikation zwischen und und von Windows Clients auf die Performance aus. Dies wirkt sich sowohl auf die Clients als auch auf den Server aus (d. h. auf den Nodes auf dem Cluster, auf denen die SVM mit dem SMB-Server ausgeführt wird).

Die Auswirkungen auf die Performance zeigen sich in der erhöhten CPU-Auslastung sowohl auf Clients als auch auf dem Server, obwohl sich die Menge des Netzwerkdatenverkehrs nicht ändert.

Das Ausmaß der Performance-Auswirkungen hängt von der Version von ONTAP 9 ab, die Sie ausführen. Ab ONTAP 9.7 kann ein neuer Algorithmus zur Auslagerung der Verschlüsselung eine bessere Performance im signierten SMB-Datenverkehr ermöglichen. SMB Signing Offload ist standardmäßig aktiviert, wenn SMB Signing aktiviert ist.

Für eine verbesserte Performance von SMB-Signaturen ist die AES-NI-Offload-Funktion erforderlich. Überprüfen Sie im Hardware Universe (HWU), ob die AES-NI-Entlastung für Ihre Plattform unterstützt wird.

Weitere Leistungsverbesserungen sind auch möglich, wenn Sie die SMB-Version 3.11 verwenden können, die den wesentlich schnelleren GCM-Algorithmus unterstützt.

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung können die Performance-Auswirkungen von SMB-Signing stark variieren. Sie können das System nur bei Tests in Ihrer Netzwerkumgebung verifizieren.

Die meisten Windows-Clients verhandeln die SMB-Signatur standardmäßig, wenn sie auf dem Server aktiviert ist. Wenn Sie für einige Ihrer Windows Clients SMB-Schutz benötigen und wenn das SMB-Signing Performance-Probleme verursacht, können Sie das SMB-Signieren auf einem Ihrer Windows-Clients deaktivieren, die keinen Schutz vor Replay-Angriffen benötigen. Informationen zum Deaktivieren der SMB-Anmeldung auf Windows-Clients finden Sie in der Microsoft Windows-Dokumentation.

Empfehlungen für die Konfiguration von SMB-Signaturen

Sie können das SMB-Signing-Verhalten zwischen SMB-Clients und dem CIFS-Server so konfigurieren, dass die Sicherheitsanforderungen erfüllt werden. Die Einstellungen, die Sie beim Konfigurieren von SMB-Signing auf Ihrem CIFS-Server auswählen, hängen von den Sicherheitsanforderungen ab.

Sie können die SMB-Signatur entweder auf dem Client oder auf dem CIFS-Server konfigurieren. Beim Konfigurieren von SMB-Signing sind folgende Empfehlungen zu berücksichtigen:

Wenn…	Empfehlung…
Sie möchten die Sicherheit der Kommunikation zwischen dem Client und dem Server erhöhen	Geben Sie beim Client SMB-Signaturen an, indem Sie den aktivieren `Require Option (Sign always)` Sicherheitseinstellung auf dem Client.
Sie möchten den gesamten SMB-Datenverkehr an eine bestimmte Storage Virtual Machine (SVM) signiert haben	SMB-Signaturen werden auf dem CIFS-Server benötigt, indem die Sicherheitseinstellungen konfiguriert werden, die SMB-Signatur erfordern.

Weitere Informationen zum Konfigurieren der Windows-Client-Sicherheitseinstellungen finden Sie in der Microsoft-Dokumentation.

Richtlinien für das SMB-Signing beim Konfigurieren mehrerer Daten-LIFS

Wenn Sie die erforderliche SMB-Signatur auf dem SMB-Server aktivieren bzw. deaktivieren, sollten Sie die Richtlinien für mehrere Daten-LIFS-Konfigurationen für eine SVM kennen.

Wenn Sie einen SMB Server konfigurieren, sind möglicherweise mehrere Daten-LIFs konfiguriert. Wenn dies der Fall ist, enthält der DNS-Server mehrere `A` Notieren Sie Einträge für den CIFS-Server, die alle denselben SMB-Serverhostnamen verwenden, jedoch jeweils über eine eindeutige IP-Adresse verfügen. Ein SMB-Server mit zwei konfigurierten Daten-LIFs hat beispielsweise den folgenden DNS `A` Eintragseinträge:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

Das normale Verhalten besteht darin, dass beim Ändern der erforderlichen SMB-Signing-Einstellung nur neue Verbindungen von Clients von der Änderung der SMB-Signing-Einstellung betroffen sind. Allerdings gibt es eine Ausnahme von diesem Verhalten. Es gibt einen Fall, in dem ein Client eine bestehende Verbindung zu einer Freigabe hat, und der Client erstellt eine neue Verbindung zu derselben Freigabe, nachdem die Einstellung geändert wurde, während die ursprüngliche Verbindung beibehalten wird. In diesem Fall übernehmen sowohl die neue als auch die bestehende SMB-Verbindung die neuen SMB-Signaturanforderungen.

Beispiel:

1. Client1 stellt eine Verbindung zu einem Share ohne die erforderliche SMB-Signatur über den Pfad her `O:\`.
2. Der Storage-Administrator ändert die SMB Server-Konfiguration, für die SMB-Signaturen erforderlich sind.
3. Client1 verbindet sich mit demselben Share mit der erforderlichen SMB-Signatur über den Pfad `S:\` (Während die Verbindung über den Pfad aufrechterhalten wird `O:\`).
4. Infolgedessen wird SMB Signing verwendet, wenn der Zugriff auf Daten über beide erfolgt `O:\` Und `S:\` Laufwerke.

Aktivieren oder Deaktivieren der erforderlichen SMB-Signatur für eingehenden SMB-Datenverkehr

Sie können die Anforderung für Clients durchsetzen, SMB-Nachrichten zu signieren, indem Sie das erforderliche SMB-Signieren aktivieren. Wenn aktiviert, akzeptiert ONTAP nur SMB-Nachrichten, wenn sie über gültige Signaturen verfügen. Wenn Sie SMB-Signaturen zulassen möchten, aber nicht benötigen, können Sie das erforderliche SMB-Signieren deaktivieren.

Über diese Aufgabe

Standardmäßig ist das erforderliche SMB-Signing deaktiviert. Sie können erforderliche SMB-Signaturen jederzeit aktivieren oder deaktivieren.

> SMB-Signaturen sind unter den folgenden Umständen standardmäßig nicht deaktiviert:
>
> 1. Das erforderliche SMB-Signing ist aktiviert und das Cluster wird auf eine Version von ONTAP zurückgesetzt, die keine SMB-Signatur unterstützt.
> 2. Anschließend wird das Cluster auf eine Version von ONTAP aktualisiert, die SMB-Signaturen unterstützt.
>
> Unter diesen Bedingungen wird die Konfiguration der SMB-Signaturen, die ursprünglich auf einer unterstützten Version von ONTAP konfiguriert wurde, durch Reversion und anschließendes Upgrade beibehalten.

Wenn Sie eine Disaster-Recovery-Beziehung (SVM) für Storage Virtual Machine (SVM) einrichten, wählen Sie den entsprechenden Wert für die `-identity-preserve` Option des `snapmirror create` Der Befehl bestimmt die Konfigurationsdetails, die in der Ziel-SVM repliziert werden.

Wenn Sie die einstellen `-identity-preserve` Option auf `true` (ID-Preserve) wird die Sicherheitseinstellung für SMB-Signaturen zum Ziel repliziert.

Wenn Sie die einstellen `-identity-preserve` Option auf `false` (Nicht-ID-Preserve) wird die SMB-Sicherheitseinstellung für das Signieren nicht auf das Ziel repliziert. In diesem Fall sind die Sicherheitseinstellungen des CIFS-Servers auf dem Ziel auf die Standardwerte festgelegt. Wenn Sie die erforderliche SMB-Signatur auf der Quell-SVM aktiviert haben, müssen Sie die erforderliche SMB-Signatur manuell auf der Ziel-SVM aktivieren.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn SMB-Signatur erforderlich sein soll…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Deaktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Vergewissern Sie sich, dass die erforderliche SMB-Signatur aktiviert oder deaktiviert ist, indem Sie

bestimmen, ob der Wert im verwendet wird `Is Signing Required` Feld in der Ausgabe des folgenden Befehls wird auf den gewünschten Wert gesetzt: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Beispiel

Im folgenden Beispiel werden die erforderlichen SMB-Signaturen für SVM vs1 ermöglicht:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- -------------------
vs1      true
```

> Änderungen an den Verschlüsselungseinstellungen werden für neue Verbindungen wirksam. Bestehende Verbindungen sind davon nicht betroffen.

Bestimmen Sie, ob SMB-Sitzungen signiert sind

Sie können Informationen zu verbundenen SMB-Sitzungen auf dem CIFS-Server anzeigen. Anhand dieser Informationen können Sie bestimmen, ob SMB-Sitzungen signiert sind. Dies kann hilfreich sein, um zu ermitteln, ob SMB-Client-Sessions eine Verbindung zu den gewünschten Sicherheitseinstellungen herstellen.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Alle signierten Sitzungen auf einer angegebenen Storage Virtual Machine (SVM)	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Details für eine signierte Sitzung mit einer spezifischen Session-ID auf der SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Beispiele

Mit dem folgenden Befehl werden Sitzungsinformationen über unterzeichnete Sitzungen in SVM vs1 angezeigt. Das Ausgabefeld „`is Session Signed`“ wird in der Standardausgabe der Zusammenfassung nicht angezeigt:

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                      Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279  1       10.1.1.1         DOMAIN\joe          2          23s
```

Mit dem folgenden Befehl werden detaillierte Sitzungsinformationen angezeigt, einschließlich des Signals der Sitzung für eine SMB-Sitzung mit einer Session-ID von 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                  Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                 Windows User: DOMAIN\joe
                    UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Verwandte Informationen

Überwachen der Statistiken von SMB-signierten Sitzungen

Überwachen Sie die Statistiken von SMB-signierten Sitzungen

Sie können die Statistiken von SMB-Sitzungen überwachen und feststellen, welche festgelegten Sitzungen signiert sind und welche nicht.

Über diese Aufgabe

Der `statistics` Mit dem Befehl auf der erweiterten Berechtigungsebene werden die angezeigt `signed_sessions` Zähler, mit dem Sie die Anzahl der signierten SMB-Sitzungen überwachen können. Der `signed_sessions` Der Zähler ist mit den folgenden Statistikobjekten verfügbar:

- `cifs` Ermöglicht Ihnen das Monitoring der SMB-Signatur für alle SMB-Sitzungen.
- `smb1` Ermöglicht Ihnen das Monitoring der SMB-Signatur für SMB 1.0-Sitzungen.
- `smb2` Ermöglicht Ihnen das Monitoring von SMB-Signaturen für SMB 2.x- und SMB 3.0-Sitzungen.

  Die SMB 3.0-Statistiken sind in der Ausgabe für das enthalten `smb2` Objekt:

Wenn Sie die Anzahl der signierten Sitzungen mit der Gesamtanzahl der Sitzungen vergleichen möchten, können Sie die Ausgabe für den vergleichen `signed_sessions` Gegenhalten mit der Ausgabe für das `established_sessions` Zähler.

Sie müssen eine Statistik-Probensammlung starten, bevor Sie die resultierenden Daten anzeigen können. Sie können Daten aus der Probe anzeigen, wenn Sie die Datenerfassung nicht beenden. Wenn Sie die Datenerfassung anhalten, erhalten Sie eine feste Probe. Wenn Sie die Datenerfassung nicht stoppen, können Sie aktualisierte Daten abrufen, die Sie zum Vergleich mit früheren Abfragen verwenden können. Der Vergleich kann Ihnen dabei helfen, Trends zu erkennen.

Schritte

1. Stellen Sie die Berechtigungsebene auf Erweiteriert: + ein `set -privilege advanced`
2. Datensammlung starten:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Wenn Sie den nicht angeben `-sample-id` Parameter: Der Befehl generiert eine Proben-ID für Sie und definiert diese Probe als Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` Ist eine Textzeichenfolge. Wenn Sie diesen Befehl während derselben CLI-Sitzung ausführen und den nicht angeben `-sample-id` Parameter: Der Befehl überschreibt das vorherige Standardbeispiel.

   Optional können Sie den Node angeben, auf dem Sie Statistiken sammeln möchten. Wenn Sie den Node nicht angeben, sammelt der Probe Statistiken für alle Nodes im Cluster.
3. Verwenden Sie die `statistics stop` Befehl zum Beenden des Datensammelns für die Probe.
4. SMB-Signaturstatistiken anzeigen:

Wenn Sie Informationen anzeigen möchten für…	Eingeben…
Signierte Sitzungen	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Signierte Sitzungen und etablierte Sessions
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   Wenn Sie Informationen nur für einen einzelnen Node anzeigen möchten, geben Sie die Option an `-node` Parameter.
5. Zurück zur Administrator-Berechtigungsebene:
   `set -privilege admin`

Beispiele

Das folgende Beispiel zeigt, wie Sie Statistiken von SMB 2.x und SMB 3.0 auf Storage Virtual Machine (SVM) vs1 überwachen können.

Der folgende Befehl bewegt sich auf die erweiterte Berechtigungsebene:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

Mit dem folgenden Befehl wird die Datenerfassung für einen neuen Probe gestartet:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

Mit dem folgenden Befehl wird die Datenerfassung für die Probe angehalten:

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

Mit dem folgenden Befehl werden aus dem Beispiel signierte SMB-Sitzungen und etablierte SMB-Sitzungen pro Node angezeigt:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- -------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

Mit dem folgenden Befehl werden signierte SMB-Sitzungen für node2 im Beispiel angezeigt:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- -------------------------
    node_name                                                node2
    signed_sessions                                              1
```

Der folgende Befehl kehrt zurück zur Administrator-Berechtigungsebene:

```
cluster1::*> set -privilege admin
```

Verwandte Informationen

Bestimmen, ob SMB-Sitzungen signiert sind

"Performance Monitoring und Management – Überblick"

Die erforderliche SMB-Verschlüsselung auf SMB-Servern für Datentransfers über SMB konfigurieren

Übersicht über die SMB-Verschlüsselung

Die SMB-Verschlüsselung für Datentransfers über SMB ist eine Verbesserung der Sicherheit, die auf SMB-Servern aktiviert bzw. deaktiviert werden kann. Sie können die gewünschte SMB-Verschlüsselungseinstellung auch auf Share-by-Share-Basis über eine Einstellung für Share-Eigenschaften konfigurieren.

Wenn Sie einen SMB-Server auf der SVM (Storage Virtual Machine) erstellen, ist die SMB-Verschlüsselung standardmäßig deaktiviert. Sie müssen die erweiterte Sicherheit durch SMB-Verschlüsselung aktivieren.

Zum Erstellen einer verschlüsselten SMB-Sitzung muss der SMB-Client SMB-Verschlüsselung unterstützen. Windows Clients ab Windows Server 2012 und Windows 8 unterstützen die SMB-Verschlüsselung.

Die SMB-Verschlüsselung auf der SVM wird über zwei Einstellungen gesteuert:

- Eine Sicherheitsoption für SMB-Server zur Aktivierung der Funktionen auf der SVM
- Eine SMB-Share-Eigenschaft, die die SMB-Verschlüsselungseinstellung auf Share-by-Share-Basis konfiguriert

Sie haben die Wahl, ob eine Verschlüsselung für den Zugriff auf alle Daten der SVM erforderlich ist oder ob eine SMB-Verschlüsselung erforderlich ist, um nur Daten in ausgewählten Freigaben zuzugreifen. Einstellungen auf SVM-Ebene ersetzen die Einstellungen auf Share-Ebene.

Die effektive SMB-Verschlüsselungskonfiguration hängt von der Kombination der beiden Einstellungen ab. Diese werden in der folgenden Tabelle beschrieben:

SMB-Server-Verschlüsselung aktiviert	Einstellung für die Verschlüsselung freigeben aktiviert	Verschlüsselungsverhalten auf Server-Seite
Richtig	Falsch	Die Verschlüsselung auf Server-Ebene ist für alle Shares in der SVM aktiviert. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.

SMB-Server-Verschlüsselung aktiviert	Einstellung für die Verschlüsselung freigeben aktiviert	Verschlüsselungsverhalten auf Server-Seite
Richtig	Richtig	Die Verschlüsselung auf Server-Ebene ist für alle Freigaben der SVM unabhängig von der Verschlüsselung auf Share-Ebene aktiviert. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.
Falsch	Richtig	Die Verschlüsselung auf Share-Ebene ist für die spezifischen Freigaben aktiviert. Mit dieser Konfiguration erfolgt die Verschlüsselung über die Baumverbindung.
Falsch	Falsch	Es ist keine Verschlüsselung aktiviert.

SMB-Clients, die keine Verschlüsselung unterstützen, können keine Verbindung zu einem SMB-Server oder einer Freigabe herstellen, für die eine Verschlüsselung erforderlich ist.

Änderungen an den Verschlüsselungseinstellungen werden für neue Verbindungen wirksam. Bestehende Verbindungen sind davon nicht betroffen.

Performance-Einbußen der SMB-Verschlüsselung

Wenn SMB-Sessions SMB-Verschlüsselung verwenden, wirkt sich die gesamte SMB-Kommunikation zwischen und von Windows Clients auf die Performance aus. Dies wirkt sich sowohl auf die Clients als auch auf den Server aus (d. h. auf den Nodes auf dem Cluster, auf dem die SVM mit dem SMB-Server ausgeführt wird).

Die Auswirkungen auf die Performance zeigen sich in der erhöhten CPU-Auslastung sowohl auf Clients als auch auf dem Server, obwohl sich die Menge des Netzwerkdatenverkehrs nicht ändert.

Das Ausmaß der Performance-Auswirkungen hängt von der Version von ONTAP 9 ab, die Sie ausführen. Ab ONTAP 9.7 kann ein neuer Algorithmus zur Auslagerung von Verschlüsselung eine bessere Performance im verschlüsselten SMB-Datenverkehr ermöglichen. Bei aktivierter SMB-Verschlüsselung ist die SMB-Verschlüsselung standardmäßig aktiviert.

Für eine verbesserte Performance der SMB-Verschlüsselung ist die AES-NI-Offload-Funktion erforderlich. Überprüfen Sie im Hardware Universe (HWU), ob die AES-NI-Entlastung für Ihre Plattform unterstützt wird.

Weitere Leistungsverbesserungen sind auch möglich, wenn Sie die SMB-Version 3.11 verwenden können, die den wesentlich schnelleren GCM-Algorithmus unterstützt.

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung variieren die Performance-Auswirkungen der SMB-Verschlüsselung erheblich. Sie können die Verschlüsselung nur bei Tests in Ihrer Netzwerkumgebung verifizieren.

Die SMB-Verschlüsselung ist auf dem SMB-Server standardmäßig deaktiviert. Die SMB-Verschlüsselung sollte nur auf den SMB-Freigaben oder SMB-Servern aktiviert werden, die eine Verschlüsselung erfordern. Bei der SMB-Verschlüsselung führt ONTAP eine zusätzliche Verarbeitung der Entschlüsselung der Anforderungen durch und verschlüsselt die Antworten für jede Anforderung. Die SMB-Verschlüsselung sollte daher nur bei Bedarf aktiviert werden.

Aktivieren oder Deaktivieren der erforderlichen SMB-Verschlüsselung für eingehenden SMB-Datenverkehr

Wenn Sie eine SMB-Verschlüsselung für eingehenden SMB-Datenverkehr benötigen, können Sie diese auf dem CIFS-Server oder auf Share-Ebene aktivieren. Standardmäßig ist keine SMB-Verschlüsselung erforderlich.

Über diese Aufgabe

Sie können die SMB-Verschlüsselung auf dem CIFS-Server aktivieren, der für alle Freigaben auf dem CIFS-Server gilt. Wenn Sie keine erforderliche SMB-Verschlüsselung für alle Freigaben auf dem CIFS-Server wünschen oder die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr auf Share-Basis aktivieren möchten, können Sie die erforderliche SMB-Verschlüsselung auf dem CIFS-Server deaktivieren.

Wenn Sie eine Disaster-Recovery-Beziehung (SVM) für Storage Virtual Machines einrichten, wählen Sie den entsprechenden Wert für das aus `-identity-preserve` Option des `snapmirror create` Der Befehl bestimmt die Konfigurationsdetails, die in der Ziel-SVM repliziert werden.

Wenn Sie die einstellen `-identity-preserve` Option auf `true` (ID-Preserve), die Sicherheitseinstellung für SMB-Verschlüsselung wird zum Ziel repliziert.

Wenn Sie die einstellen `-identity-preserve` Option auf `false` (Nicht-ID-Erhalt), die SMB-Verschlüsselungseinstellung wird nicht auf das Ziel repliziert. In diesem Fall sind die Sicherheitseinstellungen des CIFS-Servers auf dem Ziel auf die Standardwerte festgelegt. Wenn Sie die SMB-Verschlüsselung auf der Quell-SVM aktiviert haben, müssen Sie die SMB-Verschlüsselung für CIFS-Server auf dem Zielsystem manuell aktivieren.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr auf dem CIFS-Server benötigen…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Deaktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Vergewissern Sie sich, dass die erforderliche SMB-Verschlüsselung auf dem CIFS-Server nach Bedarf aktiviert oder deaktiviert ist: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

Der `is-smb-encryption-required` Feld wird angezeigt `true` Bei Bedarf ist die SMB-Verschlüsselung auf dem CIFS-Server und aktiviert `false` Wenn sie deaktiviert ist.

Beispiel

Das folgende Beispiel ermöglicht die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr für den CIFS-Server auf SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Bestimmen Sie, ob Clients über verschlüsselte SMB-Sessions verbunden sind

Sie können Informationen zu verbundenen SMB-Sitzungen anzeigen, um zu bestimmen, ob Clients verschlüsselte SMB-Verbindungen verwenden. Dies kann hilfreich sein, um zu ermitteln, ob SMB-Client-Sessions eine Verbindung zu den gewünschten Sicherheitseinstellungen herstellen.

Über diese Aufgabe

SMB-Client-Sessions können eine von drei Verschlüsselungsebenen aufweisen:

- `unencrypted`

  Die SMB-Sitzung ist nicht verschlüsselt. Die Verschlüsselung auf Storage Virtual Machine (SVM)- oder Share-Level-Ebene ist nicht konfiguriert.

- `partially-encrypted`

  Die Verschlüsselung wird gestartet, wenn die Baumverbindung auftritt. Die Verschlüsselung auf Share-Ebene wird konfiguriert. Verschlüsselung auf SVM-Ebene ist nicht aktiviert.

- `encrypted`

  Die SMB-Sitzung ist vollständig verschlüsselt. Verschlüsselung auf SVM-Ebene ist aktiviert. Verschlüsselung auf Share-Ebene ist möglicherweise aktiviert oder nicht. Die Verschlüsselungseinstellung auf SVM-Ebene ersetzt die Verschlüsselungseinstellung auf Share-Ebene.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Sitzungen mit einer bestimmten Verschlüsselungseinstellung für Sitzungen auf einer bestimmten SVM	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
Die Verschlüsselungseinstellung für eine bestimmte Session-ID auf einer bestimmten SVM	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

Beispiele

Mit dem folgenden Befehl werden ausführliche Sitzungsinformationen, einschließlich der Verschlüsselungseinstellung, für eine SMB-Sitzung mit einer Session-ID von 2 angezeigt:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                  Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                 Windows User: DOMAIN\joe
                    UNIX User: pcuser
                  Open Shares: 1
                   Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Überwachen Sie die SMB-Verschlüsselungsstatistiken

Sie können die SMB-Verschlüsselungsstatistiken überwachen und festlegen, welche festgelegten Sitzungen und Verbindungen verschlüsselt sind und welche nicht.

Über diese Aufgabe

Der `statistics` Mit dem Befehl auf der erweiterten Berechtigungsebene werden die folgenden Zähler

angezeigt, mit denen Sie die Anzahl der verschlüsselten SMB-Sessions überwachen und Verbindungen gemeinsam nutzen können:

Zählername	Beschreibungen
`encrypted_sessions`	Zeigt die Anzahl der verschlüsselten SMB 3.0-Sitzungen an
`encrypted_share_connections`	Gibt die Anzahl der verschlüsselten Freigaben an, auf denen eine Baumverbindung stattgefunden hat
`rejected_unencrypted_sessions`	Gibt die Anzahl der aufgrund fehlender Client-Verschlüsselungsfunktion abgelehnten Sitzungseinstellungen an
`rejected_unencrypted_shares`	Gibt die Anzahl der zurückgewiesenen Freigaberattierungen an, da die Client-Verschlüsselungsfunktion nicht verfügbar ist

Diese Zähler sind mit den folgenden Statistikobjekten verfügbar:

- `cifs` Ermöglicht Ihnen das Monitoring der SMB-Verschlüsselung für alle SMB 3.0-Sitzungen.

  Die SMB 3.0-Statistiken sind in der Ausgabe für das enthalten `cifs` Objekt: Wenn Sie die Anzahl der verschlüsselten Sitzungen mit der Gesamtanzahl der Sitzungen vergleichen möchten, können Sie die Ausgabe für den vergleichen `encrypted_sessions` Gegenhalten mit der Ausgabe für das `established_sessions` Zähler.

  Wenn Sie die Anzahl der verschlüsselten Share-Verbindungen mit der Gesamtanzahl der Share-Verbindungen vergleichen möchten, können Sie die Ausgabe für den vergleichen `encrypted_share_connections` Gegenhalten mit der Ausgabe für das `connected_shares` Zähler.

- `rejected_unencrypted_sessions` Gibt die Anzahl an Fällen an, in denen versucht wurde, eine SMB-Sitzung einzurichten, für die Verschlüsselung von einem Client erforderlich ist, der keine SMB-Verschlüsselung unterstützt.
- `rejected_unencrypted_shares` Bietet die Anzahl der Versuche, eine Verbindung zu einer SMB-Freigabe herzustellen, die Verschlüsselung von einem Client erfordert, der keine SMB-Verschlüsselung unterstützt.

Sie müssen eine Statistik-Probensammlung starten, bevor Sie die resultierenden Daten anzeigen können. Sie können Daten aus der Probe anzeigen, wenn Sie die Datenerfassung nicht beenden. Wenn Sie die Datenerfassung anhalten, erhalten Sie eine feste Probe. Wenn Sie die Datenerfassung nicht stoppen, können Sie aktualisierte Daten abrufen, die Sie zum Vergleich mit früheren Abfragen verwenden können. Der Vergleich kann Ihnen dabei helfen, Trends zu erkennen.

Schritte

1. Stellen Sie die Berechtigungsebene auf Erweiteriert: + ein `set -privilege advanced`
2. Datensammlung starten:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

Wenn Sie den nicht angeben `-sample-id` Parameter: Der Befehl generiert eine Proben-ID für Sie und definiert diese Probe als Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` Ist eine Textzeichenfolge. Wenn Sie diesen Befehl während derselben CLI-Sitzung ausführen und den nicht angeben `-sample-id` Parameter: Der Befehl überschreibt das vorherige Standardbeispiel.

Optional können Sie den Node angeben, auf dem Sie Statistiken sammeln möchten. Wenn Sie den Node nicht angeben, sammelt der Probe Statistiken für alle Nodes im Cluster.

3. Verwenden Sie die `statistics stop` Befehl zum Beenden des Datensammelns für die Probe.
4. SMB-Verschlüsselungsstatistiken anzeigen:

Wenn Sie Informationen anzeigen möchten für…	Eingeben…
Verschlüsselte Sitzungen	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Verschlüsselte Sitzungen und etablierte Sitzungen
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Verschlüsselte Verbindungen für Freigaben
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Verschlüsselte Verbindungen für Freigaben und verbundene Freigaben	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Abgelehnte unverschlüsselte Sitzungen	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Abgelehnte unverschlüsselte Verbindungen für die Freigabe
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

Wenn Sie nur Informationen für einen einzelnen Node anzeigen möchten, geben Sie die Option an `-node` Parameter.

5. Zurück zur Administrator-Berechtigungsebene:
   `set -privilege admin`

Beispiele

Das folgende Beispiel zeigt, wie Sie die Verschlüsselungsstatistiken von SMB 3.0 auf Storage Virtual Machine (SVM) vs1 überwachen können.

Der folgende Befehl bewegt sich auf die erweiterte Berechtigungsebene:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

Mit dem folgenden Befehl wird die Datenerfassung für einen neuen Probe gestartet:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

Mit dem folgenden Befehl wird die Datenerfassung für diesen Probe angehalten:

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

Mit dem folgenden Befehl werden verschlüsselte SMB-Sitzungen und etablierte SMB-Sessions nach Node aus dem Beispiel angezeigt:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                Value
    ----------------------------  ----------------------
    established_sessions                      1
    encrypted_sessions                        1

2 entries were displayed
```

Mit dem folgenden Befehl wird die Anzahl der abgelehnten nicht verschlüsselten SMB-Sessions des Node aus dem Beispiel angezeigt:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                    Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

Mit dem folgenden Befehl wird die Anzahl der verbundenen SMB-Freigaben und verschlüsselten SMB-Freigaben durch den Node im Beispiel angezeigt:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

Mit dem folgenden Befehl wird die Anzahl der abgelehnten nicht verschlüsselten SMB-Share-Verbindungen pro Node im Beispiel angezeigt:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Verwandte Informationen

Ermitteln, welche Statistikobjekte und Zähler verfügbar sind

"Performance Monitoring und Management – Überblick"

Sichere LDAP-Sitzungskommunikation

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 CIFS-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`.

Das LDAP-Signing and Sealing im CIFS-Verkehr ist auf der SVM mit dem aktiviert `-session-security-for-ad-ldap` Option für die `vserver cifs security modify` Befehl.

Aktivieren Sie das LDAP-Signing und Sealing auf dem CIFS-Server

Bevor Ihr CIFS-Server Signing and Sealing für eine sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, müssen Sie die CIFS-Server-Sicherheitseinstellungen ändern, um das LDAP-Signing und das Sealing zu aktivieren.

Bevor Sie beginnen

Sie müssen sich mit Ihrem AD-Serveradministrator in Verbindung setzen, um die entsprechenden Werte für die Sicherheitskonfiguration zu ermitteln.

Schritte

1. Konfigurieren Sie die CIFS-Serversicherheitseinstellung, die den signierten und versiegelten Datenverkehr mit Active Directory LDAP-Servern ermöglicht: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   Sie können das Signieren aktivieren (`sign`, Datenintegrität), Signing und Sealing (`seal`, Datenintegrität und Verschlüsselung) oder keines von beiden `none`, Kein Signing oder Sealing). Der Standardwert ist `none`.

2. Vergewissern Sie sich, dass die LDAP-Einstellung zum Signieren und Versiegeln richtig eingestellt ist: `vserver cifs security show -vserver` *`vserver_name`*

   > Wenn die SVM denselben LDAP-Server zum Abfragen der Name-Mapping oder anderer UNIX-Informationen wie Benutzer, Gruppen und Netzgruppen verwendet, müssen Sie die entsprechende Einstellung mit dem aktivieren `-session-security` Option des `vserver services name-service ldap client modify` Befehl.

Konfigurieren Sie LDAP über TLS

Exportieren Sie eine Kopie des selbstsignierten Root-CA-Zertifikats

Um LDAP über SSL/TLS zu verwenden, um die Active Directory-Kommunikation zu sichern, müssen Sie zuerst eine Kopie des selbstsignierten Stammzertifikats des Active Directory-Zertifikatdienstes in eine Zertifikatdatei exportieren und in eine ASCII-Textdatei konvertieren. Diese Textdatei wird von ONTAP verwendet, um das Zertifikat auf der Storage Virtual Machine (SVM) zu installieren.

Bevor Sie beginnen

Der Active Directory Certificate Service muss bereits für die Domäne installiert und konfiguriert sein, zu der der CIFS-Server gehört. Informationen zum Installieren und Konfigurieren von Active Director Certificate Services finden Sie in der Microsoft TechNet Library.

"Microsoft TechNet Bibliothek: technet.microsoft.com"

Schritt

1. Erhalten Sie ein Root-CA-Zertifikat des Domain-Controllers im `.pem` Textformat

   "Microsoft TechNet Bibliothek: technet.microsoft.com"

Nachdem Sie fertig sind

Installieren Sie das Zertifikat auf der SVM.

Verwandte Informationen

"Microsoft TechNet-Bibliothek"

Installieren Sie das selbstsignierte Root-CA-Zertifikat auf der SVM

Wenn bei der Anbindung an LDAP-Server eine LDAP-Authentifizierung mit TLS erforderlich ist, müssen Sie zuerst das selbstsignierte Root-CA-Zertifikat auf der SVM installieren.

Über diese Aufgabe

Wenn LDAP über TLS aktiviert ist, unterstützt der ONTAP-LDAP-Client der SVM nicht widerrief Zertifikate in ONTAP 9.0 und 9.1.

Ab ONTAP 9.2 können alle Anwendungen innerhalb von ONTAP, die TLS-Kommunikation verwenden, den digitalen Zertifikatsstatus mithilfe des Online Certificate Status Protocol (OCSP) überprüfen. Wenn OCSP für LDAP über TLS aktiviert ist, werden zurückgeworfene Zertifikate abgelehnt und die Verbindung schlägt fehl.

Schritte

1. Installieren Sie das selbstsignierte Root-CA-Zertifikat:

   a. Starten Sie die Zertifikatinstallation: `security certificate install -vserver vserver_name -type server-ca`

      Über die Konsolenausgabe wird die folgende Meldung angezeigt: `Please enter Certificate: Press <Enter> when done`

   b. Öffnen Sie das Zertifikat `.pem` Datei mit einem Texteditor, kopieren Sie das Zertifikat, einschließlich der Zeilen beginnend mit `-----BEGIN CERTIFICATE-----` Und endet mit `-----END CERTIFICATE-----`, Und fügen Sie dann das Zertifikat nach der Eingabeaufforderung ein.

   c. Vergewissern Sie sich, dass das Zertifikat ordnungsgemäß angezeigt wird.

   d. Schließen Sie die Installation durch Drücken der Eingabetaste ab.

2. Vergewissern Sie sich, dass das Zertifikat installiert ist: `security certificate show -vserver vserver_name`

Aktivieren Sie LDAP über TLS auf dem Server

Bevor Ihr SMB-Server TLS für eine sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, müssen Sie die SMB-Serversicherheitseinstellungen ändern, um LDAP über TLS zu aktivieren.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für Active Directory (AD)- als auch für Name-Services-LDAP-Verbindungen unterstützt. ONTAP versucht die Channel-Bindung mit LDAP-Verbindungen nur dann, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Seal gesetzt ist. Um die LDAP-Kanalbindung mit AD-Servern zu deaktivieren oder erneut zu aktivieren, verwenden Sie das `-try-channel-binding-for-ad-ldap` Parameter mit `vserver cifs security modify` Befehl.

Weitere Informationen finden Sie unter:

- "LDAP-Übersicht"
- "2020 LDAP-Channel-Binding und LDAP-Signing-Anforderungen für Windows".

Schritte

1. Konfigurieren Sie die SMB-Server-Sicherheitseinstellung, die eine sichere LDAP-Kommunikation mit Active Directory LDAP-Servern ermöglicht: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Vergewissern Sie sich, dass die Sicherheitseinstellung LDAP über TLS auf festgelegt ist `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Wenn die SVM denselben LDAP-Server zum Abfragen der Name-Zuordnung oder anderer UNIX-Informationen (z. B. Benutzer, Gruppen und Netgroups) verwendet, müssen Sie auch das ändern `-use-start-tls` Mit der Option `vserver services name-service ldap client modify` Befehl.