SMB Server-Sicherheitseinstellungen verwalten

ONTAP 9

NetApp
September 30, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/authentication-access-security-concept.html on September 30, 2026. Always check docs.netapp.com for the latest.

Inhalt

SMB Server-Sicherheitseinstellungen verwalten . . . 1
Informationen zur Handhabung der ONTAP SMB Client-Authentifizierung . . . 1
Kerberos-Authentifizierung . . . 1
NTLM-Authentifizierung . . . 1
Informationen zu den SMB-Server-Sicherheitseinstellungen für die ONTAP SVM-Disaster Recovery Konfiguration . . . 1
Informationen zu den Sicherheitseinstellungen des ONTAP SMB-Servers anzeigen . . . 2
ONTAP Passwortkomplexität für lokale SMB-Benutzer konfigurieren . . . 3
Die Kerberos-Sicherheitseinstellungen des ONTAP SMB-Servers ändern . . . 4
Das minimale Sicherheit bei der Authentifizierung Niveau des ONTAP SMB-Servers festlegen . . . 6
Starke ONTAP SMB-Sicherheit für Kerberos-basierte Kommunikation mit AES-Verschlüsselung konfigurieren . . . 7
AES-Verschlüsselung für die Kerberos-basierte Kommunikation von ONTAP SMB konfigurieren . . . 8
SMB-Signierung zur Erhöhung der Netzwerksicherheit verwenden . . . 11
Informationen zur Verwendung von ONTAP SMB-Signaturen zur Verbesserung der Netzwerksicherheit . . . 11
Wie sich Signaturrichtlinien auf die Kommunikation mit ONTAP SMB-Servern auswirken . . . 11
Informationen zu den Auswirkungen der ONTAP SMB-Signatur auf die Leistung . . . 13
ONTAP SMB Signaturkonfigurationsempfehlungen . . . 14
Informationen zur ONTAP SMB-Signaturkonfiguration für mehrere Daten-LIFS . . . 14
ONTAP-Signierung für eingehenden SMB-Datenverkehr konfigurieren . . . 15
Feststellen, ob ONTAP SMB-Sitzungen signiert sind . . . 16
ONTAP SMB-signierte Sitzungsstatistiken überwachen . . . 18
Erforderliche SMB-Verschlüsselung auf SMB-Servern für Datenübertragungen über SMB konfigurieren . . . 21
Informationen zur ONTAP SMB-Verschlüsselung . . . 21
Informationen zu den Auswirkungen der ONTAP SMB-Verschlüsselung auf die Performance . . . 23
ONTAP SMB-Verschlüsselung für eingehenden Datenverkehr aktivieren oder deaktivieren . . . 23
Ermitteln, ob Clients über verschlüsselte ONTAP SMB-Sitzungen verbunden sind. . . . 24
ONTAP SMB-Verschlüsselungsstatistiken überwachen . . . 26
Sichere LDAP-Sitzungskommunikation . . . 30
Informationen zu ONTAP SMB LDAP-Signierung und -Versiegelung . . . 30
LDAP-Signierung und -Versiegelung auf ONTAP SMB-Servern aktivieren . . . 30
LDAP über TLS für ONTAP SMB-Server konfigurieren . . . 31

SMB Server-Sicherheitseinstellungen verwalten

Informationen zur Handhabung der ONTAP SMB Client-Authentifizierung

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

Kerberos-Authentifizierung

ONTAP unterstützt die Kerberos-Authentifizierung beim Erstellen authentifizierter SMB-Sitzungen.

Kerberos ist der primäre Authentifizierungsdienst für Active Directory. Der Kerberos-Server oder Kerberos Key Distribution Center (KDC) Dienst speichert und ruft Informationen über Sicherheitsprinzipale im Active Directory ab. Im Gegensatz zum NTLM-Modell kontaktieren Active Directory Clients, die eine Sitzung mit einem anderen Computer wie dem SMB Server herstellen möchten, direkt einen KDC, um ihre Sitzungsberechtigungen zu erhalten.

NTLM-Authentifizierung

Die NTLM Client-Authentifizierung erfolgt mittels eines Challenge-Response-Protokolls, das auf dem gemeinsamen Wissen über ein benutzerspezifisches Geheimnis basiert, welches wiederum auf einem Passwort beruht.

Wenn ein Benutzer eine SMB-Verbindung mit einem lokalen Windows-Benutzerkonto herstellt, erfolgt die Authentifizierung lokal durch den SMB-Server mittels NTLMv2.

Informationen zu den SMB-Server-Sicherheitseinstellungen für die ONTAP SVM-Disaster Recovery Konfiguration

Bevor eine SVM erstellt wird, die als Disaster Recovery-Ziel konfiguriert ist, bei dem die Identität nicht erhalten bleibt (die `-identity-preserve` Option ist auf `false` in der SnapMirror-Konfiguration gesetzt), ist es wichtig, Informationen darüber zu haben, wie die SMB-Server-Sicherheitseinstellungen auf der Ziel-SVM verwaltet werden.

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

  Beim Erstellen eines SMB-Servers auf der Ziel-SVM werden alle Sicherheitseinstellungen des SMB-Servers auf die Standardwerte gesetzt. Bei der Initialisierung, Aktualisierung oder Resynchronisierung der SVM für die Notfallwiederherstellung werden die Sicherheitseinstellungen des SMB-Servers auf der Quelle nicht auf das Ziel repliziert.

- Die von den Standardeinstellungen abweichenden Sicherheitseinstellungen des SMB-Servers sind manuell zu konfigurieren.

  Wenn auf der Quell-SVM nicht standardmäßige SMB-Server-Sicherheitseinstellungen konfiguriert sind,

müssen diese Einstellungen auf der Ziel-SVM manuell konfiguriert werden, nachdem die Ziel-SVM Lese- und Schreibzugriff erhält (nachdem die SnapMirror Beziehung aufgehoben wurde).

Informationen zu den Sicherheitseinstellungen des ONTAP SMB-Servers anzeigen

Informationen zu den Sicherheitseinstellungen des SMB-Servers auf den Storage Virtual Machines (SVMs) können angezeigt werden. Diese Informationen ermöglichen die Überprüfung, ob die Sicherheitseinstellungen korrekt sind.

Über diese Aufgabe

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

Der `vserver cifs security show` Befehl sollte für SMB-Server im Arbeitsgruppenmodus nicht verwendet werden, da einige Optionen ungültig sind.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	Geben Sie den Befehl ein…
Alle Sicherheitseinstellungen auf einer bestimmten SVM	`vserver cifs security show -vserver` *`vserver_name`*
Eine oder mehrere spezifische Sicherheitseinstellungen auf dem SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]`Sie können `-fields ?` eingeben, um festzustellen, welche Felder Sie verwenden können.

Beispiel

Das folgende Beispiel zeigt alle Sicherheitseinstellungen für SVM vs1:

```
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 abhängen.

Das folgende Beispiel zeigt die Kerberos-Taktabweichung für SVM vs1:

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

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

Verwandte Informationen

Informationen zu GPO-Konfigurationen anzeigen

ONTAP Passwortkomplexität für lokale SMB-Benutzer konfigurieren

Die erforderliche Passwortkomplexität bietet erhöhte Sicherheit für lokale SMB-Benutzer auf Ihren Storage Virtual Machines (SVMs). Die Funktion für erforderliche Passwortkomplexität ist standardmäßig aktiviert. Sie kann jederzeit deaktiviert und wieder aktiviert werden.

Bevor Sie beginnen

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

Über diese Aufgabe

Der `vserver cifs security modify` Befehl sollte für einen CIFS-Server im Arbeitsgruppenmodus nicht verwendet werden, da einige Optionen ungültig sind.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn eine erforderliche Passwortkomplexität für lokale SMB-Benutzer gelten soll…	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. Die Sicherheitseinstellung für die erforderliche Passwortkomplexität überprüfen: `vserver cifs security show -vserver vserver_name`

Beispiel

Das folgende Beispiel zeigt, dass die erforderliche Kennwortkomplexität für lokale SMB-Benutzer für SVM vs1 aktiviert ist:

```
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

- Informationen zu den Server-Sicherheitseinstellungen
- Informationen zu lokalen Benutzern und Gruppen
- Anforderungen an lokale Benutzerpasswörter
- Passwörter lokaler Benutzerkonten ändern

Die Kerberos-Sicherheitseinstellungen des ONTAP SMB-Servers ändern

Sie können bestimmte Kerberos-Sicherheitseinstellungen des CIFS-Servers ändern, darunter die maximal zulässige Kerberos-Uhrzeitabweichung, die Lebensdauer des Kerberos-Tickets und die maximale Anzahl der Ticketverlängerungstage.

Über diese Aufgabe

Die Änderung der Kerberos-Einstellungen eines CIFS-Servers mittels des `vserver cifs security modify` Befehls ändert die Einstellungen nur auf der einzelnen Storage Virtual Machine (SVM), die Sie mit dem `-vserver` Parameter angeben. Die Kerberos-Sicherheitseinstellungen für alle SVMs im Cluster, die zur selben Active Directory Domäne gehören, können zentral über Active Directory Gruppe Policy Objects (GPOs) verwaltet werden.

Schritte

1. Eine oder mehrere der folgenden Aktionen können durchgeführt werden:

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

2. Die Kerberos-Sicherheitseinstellungen überprüfen:

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

Beispiel

Das folgende Beispiel nimmt die folgenden Änderungen an der Kerberos-Sicherheit vor: “Kerberos Clock Skew” wird auf 3 Minuten und “Kerberos Ticket Age” auf 8 Stunden für SVM vs1 gesetzt:

```
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

"Informationen zu den Server-Sicherheitseinstellungen"

"Unterstützte Gruppenrichtlinienobjekte"

"Anwenden von Gruppenrichtlinienobjekten auf CIFS-Server"

Das minimale Sicherheit bei der Authentifizierung Niveau des ONTAP SMB-Servers festlegen

Sie können die minimale Sicherheitsstufe des SMB-Servers, auch bekannt als *LMCompatibilityLevel*, auf Ihrem SMB-Server festlegen, um die Sicherheitsanforderungen Ihres Unternehmens für den SMB-Clientzugriff zu erfüllen. Die minimale Sicherheitsstufe ist die Mindeststufe der Sicherheitstoken, die der SMB-Server von SMB-Clients akzeptiert.

Über diese Aufgabe

- SMB-Server im Arbeitsgruppenmodus unterstützen ausschließlich NTLM-Authentifizierung. Kerberos-Authentifizierung wird nicht unterstützt.
- LMCompatibilityLevel gilt nur für die SMB-Client-Authentifizierung, nicht für die Administrator-Authentifizierung.

Das minimale Sicherheit bei der Authentifizierung kann auf eines von vier unterstützten Sicherheitsniveaus festgelegt werden.

Wert	Beschreibung
`lm-ntlm-ntlmv2-krb` (Standard)	Die Storage Virtual Machine (SVM) akzeptiert LM-, NTLM-, NTLMv2- und Kerberos-Sicherheit bei der Authentifizierung.
`ntlm-ntlmv2-krb`	Die SVM akzeptiert NTLM-, NTLMv2- und Kerberos-Sicherheit bei der Authentifizierung. Die SVM lehnt LM-Authentifizierung ab.
`ntlmv2-krb`	Die SVM akzeptiert NTLMv2 und Kerberos Sicherheit bei der Authentifizierung. Die SVM lehnt LM und NTLM Authentifizierung ab.
`krb`	Die SVM akzeptiert ausschließlich Kerberos-Sicherheit bei der Authentifizierung. Die SVM verweigert LM-, NTLM- und NTLMv2-Authentifizierung.

Schritte

1. Minimales Sicherheitsniveau bei der Authentifizierung festlegen: `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`

2. Es sollte sichergestellt sein, dass die Sicherheit bei der Authentifizierung auf das gewünschte Niveau eingestellt ist: `vserver cifs security show -vserver vserver_name`

Verwandte Informationen

AES-Verschlüsselung für Kerberos-basierte Kommunikation konfigurieren

Starke ONTAP SMB-Sicherheit für Kerberos-basierte Kommunikation mit AES-Verschlüsselung konfigurieren

Für maximale Sicherheit bei Kerberos-basierter Kommunikation kann die AES-256- und AES-128-Verschlüsselung auf dem SMB-Server aktiviert werden. Standardmäßig ist beim Erstellen eines SMB-Servers auf der SVM die Advanced Encryption Standard (AES)-Verschlüsselung deaktiviert. Eine Aktivierung ist erforderlich, um von der starken Sicherheit der AES-Verschlüsselung zu profitieren.

Die Kerberos-bezogene Kommunikation für SMB wird sowohl bei der Erstellung des SMB-Servers auf der SVM als auch während der Einrichtung der SMB-Sitzung verwendet. Der SMB-Server unterstützt die folgenden Verschlüsselungstypen für die Kerberos-Kommunikation:

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

Wenn die höchste Sicherheitsverschlüsselungsart für die Kerberos-Kommunikation verwendet werden soll, sollte die AES-Verschlüsselung für die Kerberos-Kommunikation auf der SVM aktiviert werden.

Bei der Erstellung des SMB-Servers legt der Domänencontroller ein Computerkonto in Active Directory an. Zu diesem Zeitpunkt erkennt der KDC die Verschlüsselungsfunktionen dieses Computerkontos. Anschließend wird ein bestimmter Verschlüsselungstyp für die Verschlüsselung des Diensttickets ausgewählt, das der Client dem Server während der Authentifizierung vorlegt.

Ab ONTAP 9.12.1 kann festgelegt werden, welche Verschlüsselungstypen dem Active Directory (AD) KDC bekanntgegeben werden. Die `-advertised-enc-types` Option kann verwendet werden, um empfohlene Verschlüsselungstypen zu aktivieren und schwächere Verschlüsselungstypen zu deaktivieren. Informationen dazu, wie "AES-Verschlüsselung für Kerberos-basierte Kommunikation konfigurieren".

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

Verwandte Informationen

Die Server-Sicherheitseinstellungen anpassen

AES-Verschlüsselung für die Kerberos-basierte Kommunikation von ONTAP SMB konfigurieren

Um die maximale Sicherheit bei der Kerberos-basierten Kommunikation zu gewährleisten, sollte auf dem SMB-Server die AES-256- und AES-128-Verschlüsselung verwendet werden. Ab ONTAP 9.13.1 ist die AES-Verschlüsselung standardmäßig aktiviert. Wenn nicht gewünscht ist, dass der SMB-Server die AES-Verschlüsselungstypen für die Kerberos-basierte Kommunikation mit dem Active Directory (AD) KDC auswählt, kann die AES-Verschlüsselung deaktiviert werden.

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 …	Es können Verschlüsselungstypen angegeben werden.
9.13.1 und später	Standardmäßig	Ja
9.12.1	Manuell	Ja
9.11.1 und früher	Manuell	Nein

Ab ONTAP 9.12.1 wird die AES-Verschlüsselung mit der `-advertised-enc-types` Option aktiviert und deaktiviert, wodurch die an den AD KDC gemeldeten Verschlüsselungstypen festgelegt werden können. Die Standardeinstellung ist `rc4` und `des`, aber wenn ein AES-Typ angegeben wird, ist die AES-Verschlüsselung aktiviert. Mit der Option kann außerdem explizit das Deaktivieren der schwächeren Verschlüsselungstypen RC4 und DES erfolgen. In ONTAP 9.11.1 und früher muss die `-is-aes-encryption-enabled` Option verwendet werden, um die AES-Verschlüsselung zu aktivieren und zu deaktivieren; die Verschlüsselungstypen können dabei nicht angegeben werden.

Wenn der `-advertised-enc-types` Parameter geändert wird, ersetzen die angegebenen Verschlüsselungstypen alle zuvor konfigurierten Typen. Alle vorherigen Einstellungen für Verschlüsselungstypen werden entfernt.

Zur Erhöhung der Sicherheit ändert die Storage Virtual Machine (SVM) ihr Maschinenkontokennwort im AD jedes Mal, wenn die AES-Sicherheitsoption geändert wird. Für die Kennwortänderung sind möglicherweise administrative AD-Anmeldeinformationen für die Organisationseinheit (OU) erforderlich, die das Maschinenkonto enthält. Eine Anmeldeaufforderung erscheint nur, wenn ONTAP das Maschinenkontokennwort im Active Directory zurücksetzen muss und Ihre AD-Konfiguration administrative Anmeldeinformationen für die Organisationseinheit erfordert, die das Maschinenkonto enthält. Wenn Ihr AD synchronisiert ist und die automatische Zurücksetzung aktiviert ist, erscheint keine Aufforderung.

Wenn eine SVM als Disaster-Recovery-Ziel konfiguriert ist, bei dem die Identität nicht erhalten bleibt (die `-identity-preserve` Option ist auf `false` in der SnapMirror-Konfiguration gesetzt), werden die nicht standardmäßigen SMB-Server-Sicherheitseinstellungen nicht auf das Ziel repliziert. Ist die AES-Verschlüsselung auf der Quell-SVM aktiviert, muss sie manuell aktiviert werden.

Beispiel 1. Schritte

ONTAP 9.12.1 und höher

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die AES-Verschlüsselungstypen für die Kerberos-Kommunikation verwendet werden sollen…	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: Die `-is-aes-encryption-enabled` Option ist in ONTAP 9.12.1 veraltet und könnte in einer späteren Version entfernt werden.

2. Es kann überprüft werden, ob die AES-Verschlüsselung wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Beispiele

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1:

```
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
```

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2. Der Administrator wird aufgefordert, die administrativen AD-Anmeldeinformationen für die OU 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 die AES-Verschlüsselungstypen für die Kerberos-Kommunikation verwendet werden sollen…	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. Es kann überprüft werden, ob die AES-Verschlüsselung wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Das `is-aes-encryption-enabled` Feld zeigt `true` an, wenn die AES-Verschlüsselung aktiviert ist, und `false` wenn sie deaktiviert ist.

Beispiele

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1:

```
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
```

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2. Der Administrator wird aufgefordert, die administrativen AD-Anmeldeinformationen für die OU 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
```

Verwandte Informationen

"Domänenbenutzer kann sich nicht im Cluster mit Domain-Tunnel anmelden"

SMB-Signierung zur Erhöhung der Netzwerksicherheit verwenden

Informationen zur Verwendung von ONTAP SMB-Signaturen zur Verbesserung der Netzwerksicherheit

Die SMB-Signierung trägt dazu bei, sicherzustellen, dass der Netzwerkverkehr zwischen dem SMB-Server und dem Client nicht kompromittiert wird; dies geschieht durch die Verhinderung von Replay-Angriffen. Standardmäßig unterstützt ONTAP die SMB-Signierung, wenn sie vom Client angefordert wird. Optional kann der Speicheradministrator den SMB-Server so konfigurieren, dass die SMB-Signierung erforderlich ist.

Wie sich Signaturrichtlinien auf die Kommunikation mit ONTAP SMB-Servern auswirken

Zusätzlich zu den SMB-Signatur-Sicherheitseinstellungen des CIFS-Servers steuern zwei SMB-Signaturrichtlinien auf Windows-Clients die digitale Signatur der Kommunikation zwischen Clients und dem CIFS-Server. Es kann die Einstellung konfiguriert werden, die den Geschäftsanforderungen entspricht.

Die SMB-Clientrichtlinien werden über die lokalen Sicherheitsrichtlinieneinstellungen von Windows gesteuert, die mithilfe der Microsoft Management Console (MMC) oder Active Directory GPOs konfiguriert werden. Weitere Informationen zur SMB-Clientsignierung und zu Sicherheitsproblemen enthält die Microsoft Windows-Dokumentation.

Hier sind Beschreibungen der beiden SMB-Signaturrichtlinien auf Microsoft Clients:

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

  Diese Einstellung steuert, ob die SMB-Signaturfunktion des Clients aktiviert ist. Sie ist standardmäßig aktiviert. Wenn diese Einstellung auf dem Client deaktiviert ist, hängt die Kommunikation des Clients mit dem CIFS-Server von der SMB-Signatureinstellung auf dem CIFS-Server ab.

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

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

> Wenn Ihre Umgebung Windows-Clients umfasst, die so konfiguriert sind, dass sie SMB-Signierung erfordern, muss die SMB-Signierung auf dem CIFS-Server aktiviert werden. Andernfalls kann der CIFS-Server diesen Systemen keine Daten bereitstellen.

Die effektiven Ergebnisse der SMB-Signatureinstellungen von Client und CIFS-Server hängen davon ab, ob die SMB-Sitzungen SMB 1.0 oder SMB 2.x und höher verwenden.

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

Client	ONTAP Unterschrift nicht erforderlich	ONTAP Unterschrift erforderlich
Signieren deaktiviert und nicht erforderlich	Nicht unterschrieben	Unterzeichnet
Signierung aktiviert und nicht erforderlich	Nicht unterschrieben	Unterzeichnet
Signieren deaktiviert und erforderlich	Unterzeichnet	Unterzeichnet
Signierung aktiviert und erforderlich	Unterzeichnet	Unterzeichnet

> Ältere Windows SMB 1 Clients und einige Nicht-Windows SMB 1 Clients können möglicherweise keine Verbindung herstellen, wenn die Signierung auf dem Client deaktiviert ist, aber auf dem CIFS-Server erforderlich ist.

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

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

Client	ONTAP Unterschrift nicht erforderlich	ONTAP Unterschrift erforderlich
Unterschrift nicht erforderlich	Nicht unterschrieben	Unterzeichnet

Client	ONTAP Unterschrift nicht erforderlich	ONTAP Unterschrift erforderlich
Unterschrift erforderlich	Unterzeichnet	Unterzeichnet

Die folgende Tabelle fasst das Standardverhalten von Microsoft-Client und -Server bei der SMB-Signierung zusammen:

Protokoll	Hash-Algorithmus	Kann aktiviert/deaktiviert werden	Kann erforderlich sein/nicht erforderlich sein	Client-Standard	Serverstandard	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 nicht mehr, `Digitally sign communications (if client agrees)` oder `Digitally sign communications (if server agrees)` Gruppenrichtlinieneinstellungen zu verwenden. Microsoft empfiehlt außerdem nicht mehr, die `EnableSecuritySignature` Registrierungseinstellungen zu verwenden. Diese Optionen betreffen nur das SMB 1 Verhalten und können durch die `Digitally sign communications (always)` Gruppenrichtlinieneinstellung oder die `RequireSecuritySignature` Registrierungseinstellung ersetzt werden.

Informationen zu den Auswirkungen der ONTAP SMB-Signatur auf die Leistung

Wenn SMB-Sitzungen SMB-Signatur verwenden, kommt es zu Leistungseinbußen bei der gesamten SMB-Kommunikation mit Windows-Clients, was sowohl die Clients als auch den Server betrifft (also die Knoten im Cluster, auf denen die SVM mit dem SMB-Server ausgeführt wird).

Die Auswirkungen auf die Leistung zeigen sich in einer erhöhten CPU-Auslastung sowohl auf den Clients als auch auf dem Server, obwohl sich das Netzwerkverkehr nicht ändert.

Das Ausmaß der Leistungseinbußen hängt von der Version von ONTAP 9 ab, die Sie verwenden. Ab ONTAP 9.7 kann ein neuer Verschlüsselungs-Offload-Algorithmus eine bessere Performance bei signiertem SMB-Datenverkehr ermöglichen. SMB-Signatur-Offload ist standardmäßig aktiviert, wenn die SMB-Signierung aktiviert ist.

Für eine verbesserte SMB-Signaturleistung ist die AES-NI-Offload-Funktion erforderlich. Im Hardware Universe (HWU) kann überprüft werden, ob für Ihre Plattform AES-NI-Offload unterstützt wird.

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

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung kann der Einfluss der SMB-

Signierung auf die Leistung stark variieren; dies lässt sich nur durch Tests in Ihrer Netzwerkumgebung überprüfen.

Die meisten Windows-Clients verhandeln standardmäßig die SMB-Signierung, sofern diese auf dem Server aktiviert ist. Wenn für einige Ihrer Windows-Clients SMB-Schutz erforderlich ist und die SMB-Signierung Leistungsprobleme verursacht, kann die SMB-Signierung auf allen Windows-Clients deaktiviert werden, die keinen Schutz vor Replay-Angriffen benötigen. Weitere Informationen zum Deaktivieren der SMB-Signierung auf Windows-Clients enthält die Microsoft Windows-Dokumentation.

ONTAP SMB Signaturkonfigurationsempfehlungen

Sie können das SMB-Signaturverhalten zwischen SMB-Clients und dem CIFS-Server an Ihre Sicherheitsanforderungen anpassen. Die Einstellungen, die bei der Konfiguration der SMB-Signatur auf dem CIFS-Server gewählt werden, hängen von den jeweiligen Sicherheitsanforderungen ab.

Sie können die SMB-Signatur entweder auf dem Client oder auf dem CIFS-Server konfigurieren. Bei der Konfiguration der SMB-Signatur sind die folgenden Empfehlungen zu berücksichtigen:

Wenn…	Empfehlung…
Die Sicherheit der Kommunikation zwischen Client und Server soll erhöht werden.	Die SMB-Signatur wird auf dem Client erforderlich gemacht, indem die `Require Option (Sign always)` Sicherheitseinstellung auf dem Client aktiviert wird.
Es wird gewünscht, dass der gesamte SMB-Datenverkehr zu einer bestimmten Storage Virtual Machine (SVM) signiert ist.	SMB-Signatur auf dem CIFS-Server erforderlich machen, indem die Sicherheitseinstellungen so konfiguriert werden, dass SMB-Signatur erforderlich ist.

Weitere Informationen zur Konfiguration der Windows Client-Sicherheitseinstellungen bietet die Microsoft-Dokumentation.

Informationen zur ONTAP SMB-Signaturkonfiguration für mehrere Daten-LIFS

Wenn Sie die erforderliche SMB-Signierung auf dem SMB-Server aktivieren oder deaktivieren, sollten die Richtlinien für mehrere Daten-LIFS-Konfigurationen für eine SVM bekannt sein.

Bei der Konfiguration eines SMB-Servers können mehrere Daten-LIFs eingerichtet sein. In diesem Fall enthält der DNS-Server mehrere `A` Einträge für den CIFS-Server, die alle denselben Hostnamen des SMB-Servers verwenden, aber jeweils eine eindeutige IP-Adresse besitzen. Beispielsweise könnte ein SMB-Server mit zwei konfigurierten Daten-LIFs die folgenden DNS `A` Einträge aufweisen:

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

Normalerweise werden bei einer Änderung der erforderlichen SMB-Signatur-Einstellung nur neue Verbindungen von Clients von der Änderung der SMB-Signatur-Einstellung betroffen. Es gibt jedoch eine Ausnahme von diesem Verhalten. Es gibt einen Fall, in dem ein Client bereits eine Verbindung zu einer

Freigabe hat und nach der Änderung der Einstellung eine neue Verbindung zur selben Freigabe herstellt, während die ursprüngliche Verbindung bestehen bleibt. In diesem Fall übernehmen sowohl die neue als auch die bestehende SMB-Verbindung die neuen SMB-Signatur-Anforderungen.

Das folgende Beispiel ist zu berücksichtigen:

1. Client1 stellt eine Verbindung zu einer Freigabe ohne erforderliche SMB-Signierung über den Pfad `O:\` her.
2. Der Speicheradministrator ändert die SMB-Server Konfiguration, sodass die SMB-Signierung erforderlich ist.
3. Client1 stellt eine Verbindung zur selben Freigabe mit der erforderlichen SMB-Signatur unter Verwendung des Pfads `S:\` (wobei die Verbindung unter Verwendung des Pfads `O:\` aufrechterhalten wird).
4. Das Ergebnis ist, dass die SMB-Signatur beim Zugriff auf Daten sowohl über das `O:\` als auch das `S:\` Laufwerk verwendet wird.

ONTAP-Signierung für eingehenden SMB-Datenverkehr konfigurieren

Sie können die Anforderung, dass Clients SMB-Nachrichten signieren, durch Aktivieren der erforderlichen SMB-Signierung durchsetzen. Wenn diese Option aktiviert ist, akzeptiert ONTAP SMB-Nachrichten nur, wenn sie gültige Signaturen aufweisen. Wenn die SMB-Signierung zugelassen, aber nicht vorgeschrieben werden soll, kann die erforderliche SMB-Signierung deaktiviert werden.

Über diese Aufgabe

Die erforderliche SMB-Signatur ist standardmäßig deaktiviert. Sie können die erforderliche SMB-Signatur jederzeit aktivieren oder deaktivieren.

Die SMB-Signierung ist unter den folgenden Umständen nicht standardmäßig deaktiviert:

1. Die erforderliche SMB-Signierung ist aktiviert, und der Cluster wird auf eine Version von ONTAP zurückgesetzt, die die SMB-Signierung nicht unterstützt.
2. Anschließend erfolgt ein Upgrade des Clusters auf eine Version von ONTAP, die SMB-Signierung unterstützt.

   Unter diesen Umständen bleibt die SMB-Signaturkonfiguration, die ursprünglich auf einer unterstützten Version von ONTAP konfiguriert wurde, auch bei einem Downgrade und einem anschließenden Upgrade erhalten.

Wenn eine Disaster-Recovery-Beziehung für eine Storage Virtual Machine (SVM) eingerichtet wird, bestimmt der Wert, der für die `-identity-preserve` Option des `snapmirror create` Befehls ausgewählt wird, welche Konfigurationsdetails in die Ziel-SVM repliziert werden.

Wenn die `-identity-preserve` Option auf `true` (ID-preserve) gesetzt ist, wird die SMB-Signatur-Sicherheitseinstellung auf das Ziel repliziert.

Wenn Sie die `-identity-preserve` Option auf `false` (non-ID-preserve) setzen, wird die SMB-Signatur-Sicherheitseinstellung nicht an das Ziel repliziert. In diesem Fall werden die CIFS-Server-Sicherheitseinstellungen auf dem Ziel auf die Standardwerte gesetzt. Wenn auf der Quell-SVM die erforderliche SMB-Signatur aktiviert ist, muss die erforderliche SMB-Signatur auf der Ziel-SVM manuell aktiviert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die erforderliche SMB-Signierung aktiviert werden 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. Überprüfen Sie, ob die erforderliche SMB-Signierung aktiviert oder deaktiviert ist, indem festgestellt wird, ob der Wert im `Is Signing Required` Feld in der Ausgabe des folgenden Befehls auf den gewünschten Wert gesetzt ist: `vserver cifs security show -vserver vserver_name -fields is-signing-required`

Beispiel

Das folgende Beispiel aktiviert die erforderliche SMB-Signierung für SVM vs1:

```
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.

Verwandte Informationen

- "snapmirror create"

Feststellen, ob ONTAP SMB-Sitzungen signiert sind

Informationen über verbundene SMB-Sitzungen auf dem CIFS-Server können angezeigt werden. Diese Informationen ermöglichen die Feststellung, ob SMB-Sitzungen signiert sind. Dies kann hilfreich sein, um zu bestimmen, ob SMB-Client-Sitzungen mit den gewünschten Sicherheitseinstellungen verbunden sind.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	Geben Sie den Befehl ein…
Alle signierten Sitzungen auf einer bestimmten Storage Virtual Machine (SVM)	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Details zu einer signierten Sitzung mit einer bestimmten Sitzungs-ID auf der SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Beispiele

Der folgende Befehl zeigt Sitzungsinformationen zu signierten Sitzungen auf SVM vs1 an. Die Standard-Zusammenfassungsausgabe zeigt das Ausgabefeld „`Ist Sitzung signiert`“ nicht an:

```
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
```

Der folgende Befehl zeigt detaillierte Sitzungsinformationen an, einschließlich der Information, ob die Sitzung signiert ist, für eine SMB-Sitzung mit der Sitzungs-ID 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

Überwachung von SMB-signierten Sitzungsstatistiken

ONTAP SMB-signierte Sitzungsstatistiken überwachen

Sie können SMB-Sitzungsstatistiken überwachen und feststellen, welche bestehenden Sitzungen signiert sind und welche nicht.

Über diese Aufgabe

Der `statistics`Befehl auf der erweiterten Berechtigungsstufe stellt den `signed_sessions`Zähler bereit, mit dem die Anzahl der signierten SMB-Sitzungen überwacht werden kann. Der `signed_sessions`Zähler ist mit den folgenden Statistiken-Objekten verfügbar:

- `cifs`ermöglicht die Überwachung der SMB-Signierung für alle SMB-Sitzungen.
- `smb1` Ermöglicht die Überwachung der SMB-Signatur für SMB 1.0-Sitzungen.
- `smb2`ermöglicht die Überwachung der SMB-Signierung für SMB 2.x und SMB 3.0 Sitzungen.

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

Wenn Sie die Anzahl der signierten Sitzungen mit der Gesamtzahl der Sitzungen vergleichen möchten, kann die Ausgabe für den `signed_sessions` Counter mit der Ausgabe für den `established_sessions` Counter verglichen werden.

Sie müssen eine Statistiken Stichprobenerfassung starten, bevor Sie die resultierenden Daten anzeigen können. Daten aus der Stichprobe können angezeigt werden, wenn die Datenerfassung nicht gestoppt wird. Das Stoppen der Datenerfassung ergibt eine feste Stichprobe. Wenn die Datenerfassung nicht gestoppt wird, besteht die Möglichkeit, aktualisierte Daten zu erhalten, die zum Vergleich mit früheren Abfragen verwendet werden können. Der Vergleich kann dabei helfen, Trends zu erkennen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt:
   `set -privilege advanced`
2. Datenerfassung starten:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Wenn der `-sample-id` Parameter nicht angegeben wird, generiert der Befehl eine Beispielkennung für Sie und definiert dieses Beispiel als das Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` ist ein Text-String. Wenn dieser Befehl während derselben CLI-Sitzung ausgeführt wird und der `-sample -id` Parameter nicht angegeben wird, überschreibt der Befehl das vorherige Standardbeispiel.

   Sie können optional den Knoten angeben, auf dem Sie Statistiken erfassen möchten. Wenn Sie keinen Knoten angeben, erfasst das Beispiel Statistiken für alle Knoten im Cluster.

   Weitere Informationen zu `statistics start` finden sich in der "ONTAP-Befehlsreferenz".
3. Mit dem `statistics stop` Befehl wird das Sammeln von Daten für die Probe gestoppt.

   Weitere Informationen zu `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

4. SMB-Signaturstatistiken anzeigen:

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

Wenn Informationen nur für einen einzelnen Knoten angezeigt werden sollen, kann der optionale `-node`Parameter angegeben werden.

Weitere Informationen zu `statistics show` finden sich in der "ONTAP-Befehlsreferenz".

5. Zurück zur Administratorrechteebene:
`set -privilege admin`

▼ **Beispiele**

Das folgende Beispiel zeigt, wie die Signaturstatistiken von SMB 2.x und SMB 3.0 auf der Storage Virtual Machine (SVM) vs1 überwacht werden können.

Der folgende Befehl wechselt zur erweiterten Berechtigungsstufe:

```
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
```

Der folgende Befehl startet die Datenerfassung für eine neue Probe:

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

Der folgende Befehl beendet die Datenerfassung für das Beispiel:

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

Der folgende Befehl zeigt signierte SMB-Sitzungen und aufgebaute SMB-Sitzungen pro Knoten aus dem Beispiel:

```
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
```

Der folgende Befehl zeigt signierte SMB-Sitzungen für node2 aus dem Beispiel an:

```
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 wechselt zurück auf die Administratorrechteebene:

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

Verwandte Informationen

- Feststellen, ob SMB-Sitzungen signiert sind
- "Überblick über Leistungsüberwachung und Management"

Erforderliche SMB-Verschlüsselung auf SMB-Servern für Datenübertragungen über SMB konfigurieren

Informationen zur ONTAP SMB-Verschlüsselung

Die SMB-Verschlüsselung für Datenübertragungen über SMB ist eine Sicherheitsverbesserung, die auf SMB-Servern aktiviert oder deaktiviert werden kann. Die gewünschte SMB-Verschlüsselungseinstellung kann auch für jede einzelne Freigabe über eine Freigabeeigenschaft konfiguriert werden.

Standardmäßig ist die SMB-Verschlüsselung deaktiviert, wenn ein SMB-Server auf der Storage Virtual Machine (SVM) erstellt wird. Sie muss aktiviert werden, um von der erhöhten Sicherheit durch die SMB-Verschlüsselung zu profitieren.

Um eine verschlüsselte SMB-Sitzung zu erstellen, muss der SMB-Client die SMB-Verschlüsselung unterstützen. Windows Clients ab Windows Server 2012 und Windows 8 unterstützen die SMB-Verschlüsselung.

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

- Eine SMB-Server-Sicherheitsoption, die die Funktionalität auf der SVM ermöglicht
- Eine SMB-Freigabeeigenschaft, die die SMB-Verschlüsselungseinstellung für jede einzelne Freigabe konfiguriert

Sie können entscheiden, ob für den Zugriff auf alle Daten auf der SVM eine Verschlüsselung erforderlich sein soll oder ob für den Zugriff auf Daten nur in ausgewählten Freigaben SMB-Verschlüsselung erforderlich sein soll. Die `encrypt-data` Freigabeeigenschaft erfordert SMB-Verschlüsselung für den Zugriff auf eine Freigabe. Ab ONTAP 9.11.1 ermöglicht die `allow-unencrypted-access` Freigabeeigenschaft SMB2-Clients den Zugriff auf eine Freigabe ohne Verschlüsselung, während SMB3-Clients weiterhin Verschlüsselung verwenden, wenn `encrypt-data` aktiviert ist.

SVM-Einstellungen haben Vorrang vor Freigabeeinstellungen.

Die effektive SMB-Verschlüsselungskonfiguration hängt von der Kombination der beiden Einstellungen ab und ist in der folgenden Tabelle beschrieben:

SMB-Server mit aktivierter SMB-Verschlüsselung	Einstellung „Daten verschlüsseln“ für die Freigabe aktiviert	Einstellung „Unverschlüsselten Zugriff zulassen“ aktiviert	Server-seitiges Verschlüsselungsverhalten
True	Falsch	Falsch	Die serverseitige Verschlüsselung ist für alle Freigaben in der SVM aktiviert. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.

SMB-Server mit aktivierter SMB-Verschlüsselung	Einstellung „Daten verschlüsseln“ für die Freigabe aktiviert	Einstellung „Unverschlüsselten Zugriff zulassen“ aktiviert	Server-seitiges Verschlüsselungsverhalten
True	True	Falsch	Die serverseitige Verschlüsselung ist für alle Freigaben in der SVM aktiviert, unabhängig von der Freigabeverschlüsselung. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.
Falsch	True	Falsch	Die Freigabeverschlüsselung ist für die betreffenden Freigaben aktiviert. SMB3 Clients verwenden Verschlüsselung, SMB2 Clients können jedoch unverschlüsselt auf die Freigabe zugreifen, da die `allow-unencrypted-access`Eigenschaft aktiviert ist.
Falsch	Falsch	Falsch	Es ist keine Verschlüsselung aktiviert.
Falsch	Falsch	True	Es ist keine Verschlüsselung aktiviert. Die `allow-unencrypted-access` Eigenschaft hat keine Auswirkung, sofern `encrypt-data` nicht aktiviert ist.

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

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

Die `allow-unencrypted-access` Eigenschaft wird ab ONTAP 9.11.1 unterstützt.

Die SMB-Verschlüsselung auf SVM-Ebene überschreibt die Einstellungen auf Freigabeebene.

Informationen zu den Auswirkungen der ONTAP SMB-Verschlüsselung auf die Performance

Wenn SMB-Sitzungen SMB-Verschlüsselung verwenden, kommt es bei der gesamten SMB-Kommunikation mit Windows-Clients zu Leistungseinbußen, die sowohl die Clients als auch den Server betreffen (das heißt, die Knoten im Cluster, auf denen die SVM ausgeführt wird, die den SMB-Server enthält).

Die Auswirkungen auf die Leistung zeigen sich in einer erhöhten CPU-Auslastung sowohl auf den Clients als auch auf dem Server, obwohl sich das Netzwerkverkehr nicht ändert.

Das Ausmaß der Leistungseinbußen hängt von der Version von ONTAP 9 ab, die Sie verwenden. Ab ONTAP 9.7 kann ein neuer Verschlüsselungs-Offload-Algorithmus eine bessere Performance im verschlüsselten SMB-Datenverkehr ermöglichen. Die SMB-Verschlüsselungsauslagerung ist standardmäßig aktiviert, wenn die SMB-Verschlüsselung aktiviert ist.

Für eine verbesserte SMB-Verschlüsselungsleistung ist die AES-NI-Offload-Funktion erforderlich. Im Hardware Universe (HWU) kann überprüft werden, ob für Ihre Plattform AES-NI-Offload unterstützt wird.

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

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung kann der Einfluss der SMB-Verschlüsselung auf die Leistung stark variieren; dies lässt sich nur durch Tests in Ihrer Netzwerkumgebung überprüfen.

Die SMB-Verschlüsselung ist auf dem SMB-Server standardmäßig deaktiviert. Die SMB-Verschlüsselung sollte nur für diejenigen SMB-Freigaben oder SMB-Server aktiviert werden, die eine Verschlüsselung benötigen. Mit SMB-Verschlüsselung führt ONTAP für jede Anfrage eine zusätzliche Verarbeitung durch, indem die Anfragen entschlüsselt und die Antworten verschlüsselt werden. Die SMB-Verschlüsselung sollte daher nur bei Bedarf aktiviert werden.

ONTAP SMB-Verschlüsselung für eingehenden Datenverkehr aktivieren oder deaktivieren

Wenn die SMB-Verschlüsselung für eingehenden SMB-Datenverkehr erforderlich sein soll, kann sie auf dem CIFS-Server oder auf Freigabeebene aktiviert werden. Standardmäßig ist die SMB-Verschlüsselung nicht erforderlich.

Über diese Aufgabe

Sie können die SMB-Verschlüsselung auf dem CIFS-Server aktivieren, wodurch sie für alle Freigaben auf dem CIFS-Server gilt. Wenn für alle Freigaben auf dem CIFS-Server keine verpflichtende SMB-Verschlüsselung erforderlich sein soll oder wenn verpflichtende SMB-Verschlüsselung für eingehenden SMB-Datenverkehr nur für einzelne Freigaben aktiviert werden soll, kann die verpflichtende SMB-Verschlüsselung auf dem CIFS-Server deaktiviert werden.

Wenn Sie eine Storage Virtual Machine (SVM) Notfallwiederherstellungsbeziehung einrichten, bestimmt der Wert, den Sie für die `-identity-preserve` Option des `snapmirror create` Befehls auswählen, die Konfigurationsdetails, die in die Ziel-SVM repliziert werden.

Wenn die `-identity-preserve` Option auf `true` (ID-preserve) gesetzt ist, wird die SMB-Verschlüsselungssicherheitseinstellung auf das Ziel repliziert.

Wenn die `-identity-preserve` Option auf `false` (non-ID-preserve) gesetzt ist, wird die SMB-Verschlüsselungssicherheitseinstellung nicht auf das Ziel repliziert. In diesem Fall werden die CIFS-Server-Sicherheitseinstellungen auf dem Ziel auf die Standardwerte gesetzt. Wenn auf der Quell-SVM die SMB-Verschlüsselung aktiviert ist, muss die CIFS-Server-SMB-Verschlüsselung auf dem Ziel manuell aktiviert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr auf dem CIFS-Server benötigt wird…	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. Es sollte überprüft werden, ob die erforderliche SMB-Verschlüsselung auf dem CIFS-Server wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   Das `is-smb-encryption-required` Feld zeigt `true` an, wenn die erforderliche SMB-Verschlüsselung auf dem CIFS-Server aktiviert ist, und `false` wenn sie deaktiviert ist.

Beispiel

Das folgende Beispiel aktiviert 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
```

Verwandte Informationen

- "snapmirror create"

Ermitteln, ob Clients über verschlüsselte ONTAP SMB-Sitzungen verbunden sind.

Sie können Informationen über verbundene SMB-Sitzungen anzeigen, um festzustellen, ob Clients verschlüsselte SMB-Verbindungen verwenden. Dies kann hilfreich sein, um zu bestimmen, ob SMB-Client-Sitzungen mit den gewünschten Sicherheitseinstellungen

verbunden sind.

Über diese Aufgabe

Die Sitzungen von SMB-Clients können eine von drei Verschlüsselungsstufen aufweisen:

- `unencrypted`

  Die SMB-Sitzung ist nicht verschlüsselt. Weder auf Storage Virtual Machine (SVM)-Ebene noch auf Freigabeebene ist eine Verschlüsselung konfiguriert.

- `partially-encrypted`

  Die Verschlüsselung wird beim Tree-Connect initiiert. Die Verschlüsselung auf Freigabeebene ist konfiguriert. Die Verschlüsselung auf SVM-Ebene ist nicht aktiviert.

- `encrypted`

  Die SMB-Sitzung ist vollständig verschlüsselt. Die SVM-Verschlüsselung ist aktiviert. Die Freigabeverschlüsselung kann aktiviert sein oder nicht. Die Einstellung für die SVM-Verschlüsselung hat Vorrang vor der Einstellung für die Freigabeverschlüsselung.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

Beispiele

Der folgende Befehl zeigt detaillierte Sitzungsinformationen, einschließlich der Verschlüsselungseinstellung, zu einer SMB-Sitzung mit der Sitzungs-ID 2 an:

```
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
```

ONTAP SMB-Verschlüsselungsstatistiken überwachen

Sie können die SMB-Verschlüsselungsstatistiken überwachen und feststellen, welche hergestellten Sitzungen und Freigabeverbindungen verschlüsselt sind und welche nicht.

Über diese Aufgabe

Der `statistics` Befehl auf der Ebene mit erweiterten Berechtigungen stellt die folgenden Zähler bereit, mit denen Sie die Anzahl der verschlüsselten SMB-Sitzungen und Freigabeverbindungen überwachen können:

Zählername	Beschreibungen
`encrypted_sessions`	Gibt die Anzahl der verschlüsselten SMB 3.0 Sitzungen an.
`encrypted_share_connections`	Gibt die Anzahl der verschlüsselten Anteile an, auf denen eine Baumverbindung stattgefunden hat
`rejected_unencrypted_sessions`	Gibt die Anzahl der abgelehnten Sitzungsaufbauten aufgrund fehlender Client-Verschlüsselungsfunktionen an
`rejected_unencrypted_shares`	Gibt die Anzahl der aufgrund fehlender Client-Verschlüsselungsfunktionen abgelehnten Freigabezuordnungen an

Diese Zähler sind mit den folgenden Statistiken-Objekten verfügbar:

- `cifs`ermöglicht die Überwachung der SMB-Verschlüsselung für alle SMB 3.0-Sitzungen.

  Die SMB 3.0 Statistiken sind in der Ausgabe für das `cifs` Objekt enthalten. Wenn die Anzahl der verschlüsselten Sitzungen mit der Gesamtzahl der Sitzungen verglichen werden soll, kann die Ausgabe für den `encrypted_sessions` Counter mit der Ausgabe für den `established_sessions` Counter verglichen werden.

  Wenn Sie die Anzahl der verschlüsselten Freigabeverbindungen mit der Gesamtzahl der Freigabeverbindungen vergleichen möchten, kann die Ausgabe für den `encrypted_share_connections` Counter mit der Ausgabe für den `connected_shares` Counter verglichen werden.

- `rejected_unencrypted_sessions`Gibt die Anzahl der Versuche an, eine SMB-Sitzung herzustellen, die eine Verschlüsselung erfordert, von einem Client, der SMB-Verschlüsselung nicht unterstützt.

- `rejected_unencrypted_shares`Gibt die Anzahl der Versuche an, eine Verbindung zu einer SMB-Freigabe herzustellen, die eine Verschlüsselung erfordert, von einem Client, der SMB-Verschlüsselung nicht unterstützt.

Sie müssen eine Statistiken Stichprobenerfassung starten, bevor Sie die resultierenden Daten anzeigen können. Sie können Daten aus der Stichprobe anzeigen, wenn Sie die Datenerfassung nicht beenden. Das Stoppen der Datenerfassung ergibt eine feste Stichprobe. Wenn die Datenerfassung nicht gestoppt wird, besteht die Möglichkeit, aktualisierte Daten zu erhalten, die zum Vergleich mit früheren Abfragen verwendet werden können. Der Vergleich kann dabei helfen, Trends zu erkennen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt:
   `set -privilege advanced`
2. Datenerfassung starten:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Wenn der `-sample-id` Parameter nicht angegeben wird, generiert der Befehl eine Beispielkennung für Sie und definiert dieses Beispiel als das Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` ist ein Text-String. Wenn dieser Befehl während derselben CLI-Sitzung ausgeführt wird und der `-sample-id` Parameter nicht angegeben wird, überschreibt der Befehl das vorherige Standardbeispiel.

   Sie können optional den Knoten angeben, auf dem Sie Statistiken erfassen möchten. Wenn Sie keinen Knoten angeben, erfasst das Beispiel Statistiken für alle Knoten im Cluster.

   Weitere Informationen zu `statistics start` finden sich in der "ONTAP-Befehlsreferenz".
3. Mit dem `statistics stop` Befehl wird das Sammeln von Daten für die Probe gestoppt.

   Weitere Informationen zu `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".
4. SMB-Verschlüsselungsstatistiken:

Wenn Sie Informationen zu … anzeigen möchten	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 Freigabeverbindungen
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Verschlüsselte Freigabeverbindungen 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 Freigabeverbindungen

Wenn Sie Informationen zu … anzeigen möchten	Eingeben…
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

Wenn Informationen nur für einen einzelnen Knoten angezeigt werden sollen, kann der optionale `-node`Parameter angegeben werden.

Weitere Informationen zu `statistics show` finden sich in der "ONTAP-Befehlsreferenz".

5. Zurück zur Administratorrechteebene:
`set -privilege admin`

▼ **Beispiele**

Das folgende Beispiel zeigt, wie die SMB 3.0 Verschlüsselungsstatistiken auf einer Storage Virtual Machine (SVM) vs1 überwacht werden können.

Der folgende Befehl wechselt zur erweiterten Berechtigungsstufe:

```
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
```

Der folgende Befehl startet die Datenerfassung für eine neue Probe:

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

Der folgende Befehl beendet die Datenerfassung für diese Stichprobe:

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

Der folgende Befehl zeigt verschlüsselte SMB-Sitzungen und aufgebaute SMB-Sitzungen des Knotens aus dem Beispiel an:

```
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
```

Der folgende Befehl zeigt die Anzahl der vom Knoten aus dem Beispiel abgelehnten unverschlüsselten SMB-Sitzungen an:

```
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.
```

Der folgende Befehl zeigt die Anzahl der verbundenen SMB-Freigaben und der verschlüsselten SMB-Freigaben nach dem Knoten aus dem Beispiel:

```
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.
```

Der folgende Befehl zeigt die Anzahl der vom Knoten aus dem Beispiel abgelehnten unverschlüsselten SMB-Freigabeverbindungen:

```
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

- Welche Statistiken, Objekte und Zähler auf den Servern verfügbar sind, lässt sich feststellen.
- "Überblick über Leistungsüberwachung und Management"

Sichere LDAP-Sitzungskommunikation

Informationen zu ONTAP SMB LDAP-Signierung und -Versiegelung

Ab ONTAP 9 können Sie die Signierung und Versiegelung konfigurieren, um die LDAP-Sitzungssicherheit bei Abfragen an einen Active Directory (AD)-Server zu aktivieren. Die CIFS-Server-Sicherheitseinstellungen auf der Storage Virtual Machine (SVM) müssen so konfiguriert werden, dass sie mit denen des LDAP-Servers übereinstimmen.

Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe einer geheimen Schlüsseltechnologie. Versiegeln verschlüsselt die LDAP-Nutzlastdaten, um die Übertragung sensibler Informationen im Klartext zu vermeiden. Eine Option für den *LDAP Security Level* gibt an, ob der LDAP-Datenverkehr signiert, signiert und versiegelt oder keines von beidem sein muss. Der Standardwert ist `none`.

Die LDAP-Signierung und -Versiegelung des CIFS-Datenverkehrs ist auf der SVM mit der `-session -security-for-ad-ldap` Option zum `vserver cifs security modify` Befehl aktiviert.

LDAP-Signierung und -Versiegelung auf ONTAP SMB-Servern aktivieren

Bevor Ihr CIFS-Server die Signierung und Versiegelung für die sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, sind die

Sicherheitseinstellungen des CIFS-Servers so zu ändern, dass LDAP-Signierung und -Versiegelung aktiviert werden.

Bevor Sie beginnen

Es ist erforderlich, sich mit Ihrem AD-Serveradministrator abzustimmen, um die geeigneten Sicherheitskonfigurationswerte zu ermitteln.

Schritte

1. Die CIFS-Server-Sicherheitseinstellung konfigurieren, die 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 Signieren (`sign`, Datenintegrität, Signieren und Versiegeln (`seal`, Datenintegrität und Verschlüsselung oder keines von beidem `none`, keine Signierung oder Versiegelung, aktivieren. Der Standardwert ist `none`.

2. Überprüfen, ob die LDAP-Signatur- und Versiegelungssicherheitseinstellung korrekt konfiguriert ist: `vserver cifs security show -vserver vserver_name`

> Wenn die SVM denselben LDAP-Server für die Abfrage von Namenszuordnungen oder anderen UNIX-Informationen wie Benutzern, Gruppen und Netzgruppen verwendet, muss die entsprechende Einstellung mit der `-session-security` Option des `vserver services name-service ldap client modify` Befehls aktiviert werden.

LDAP über TLS für ONTAP SMB-Server konfigurieren

Konfigurieren Sie LDAP über TLS für ONTAP SMB-Server, um die Kommunikation zwischen dem SMB-Server und Active Directory LDAP-Servern zu sichern.

Schritt 1: Selbstsignierte Stammzertifizierungsstellenzertifikate für ONTAP SMB SVMs exportieren

Um LDAP über SSL/TLS zur Sicherung der Active Directory-Kommunikation zu verwenden, muss zunächst eine Kopie des selbstsignierten Stammzertifikats des Active Directory Certificate Service in eine Zertifikatsdatei exportiert und in eine ASCII-Textdatei konvertiert werden. Diese Textdatei wird von ONTAP verwendet, um das Zertifikat auf der Storage Virtual Machine (SVM) zu installieren.

Der Active Directory-Zertifikatdienst muss für die Domäne, zu der der CIFS-Server gehört, bereits installiert und konfiguriert sein. Informationen zur Installation und Konfiguration von Active Directory Certificate Services finden Sie in der Dokumentation "Microsoft TechNet Bibliothek: technet.microsoft.com"

> Ab ONTAP 9.13.1 ist, wenn `-use-start-tls-for-ad-ldap` oder `-use-ldaps-for-ad-ldap` für den SMB-Server aktiviert ist, sicherzustellen, dass die erforderlichen CA-Zertifikate für vertrauenswürdige Domänen sowie für die Heimatdomäne installiert sind. ONTAP muss TLS- oder LDAPS-Verbindungen zu Domänencontrollern vertrauenswürdiger Domänen herstellen können, um deren Standortinformationen zu ermitteln.

Schritt

1. Ein Root-CA-Zertifikat des Domänencontrollers im `.pem` Textformat erhalten.

   "Microsoft TechNet Bibliothek: technet.microsoft.com"

Was kommt als Nächstes

Das Zertifikat auf der SVM installieren.

Schritt 2: Installieren Sie selbstsignierte Stammzertifikate der Zertifizierungsstelle auf der ONTAP SMB SVM

Wenn bei der Anbindung an LDAP-Server eine LDAP-Authentifizierung mit TLS erforderlich ist, muss zunächst das selbstsignierte Root-CA-Zertifikat auf der SVM installiert werden.

Über diese Aufgabe

Alle Anwendungen innerhalb von ONTAP, die TLS-Kommunikation nutzen, können den Status digitaler Zertifikate mithilfe des Online Certificate Status Protocol (OCSP) überprüfen. Wenn OCSP für LDAP über TLS aktiviert ist, werden widerrufene Zertifikate zurückgewiesen und die Verbindung schlägt fehl.

Schritte

1. Das selbstsignierte Stammzertifikat der Zertifizierungsstelle installieren:
   a. Beginnen Sie die Zertifikatsinstallation:

      ```
      security certificate install -vserver <SVM_name> -type server-ca
      ```

      Die Konsolenausgabe zeigt folgende Meldung an: `Please enter Certificate: Press <Enter> when done`

   b. Öffnen Sie die `.pem` Zertifikatsdatei mit einem Texteditor, das Zertifikat einschließlich der Zeilen kopieren, die mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----` enden, und das Zertifikat anschließend nach der Eingabeaufforderung einfügen.
   c. Es wird überprüft, ob das Zertifikat korrekt angezeigt wird.
   d. Die Installation wird durch Drücken der Eingabetaste abgeschlossen.
2. Überprüfen Sie, ob das Zertifikat installiert ist:

   ```
   security certificate show -vserver <SVM_name>
   ```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"

Schritt 3: LDAP über TLS auf dem ONTAP SMB-Server aktivieren

Bevor Ihr SMB-Server TLS für die sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, müssen die Sicherheitseinstellungen des SMB-Servers geändert werden, damit LDAP über TLS genutzt werden kann.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für Active Directory (AD) als auch für Namensdienst-LDAP-Verbindungen unterstützt. ONTAP versucht die Kanalbindung mit LDAP-Verbindungen nur, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Versiegeln eingestellt ist. Um die LDAP-Kanalbindung mit AD-Servern zu deaktivieren oder wieder zu aktivieren, kann der `-try-channel-binding-for-ad-ldap` Parameter mit dem `vserver cifs`

`security modify` Befehl verwendet werden.

Weitere Informationen sind unter folgendem Link verfügbar:

- "Informationen zu LDAP für ONTAP NFS SVMs"
- "LDAP-Kanalbindungs- und LDAP-Signaturanforderungen für Windows 2020".

Schritte

1. Konfigurieren Sie die SMB-Server-Sicherheitseinstellung, die eine sichere LDAP-Kommunikation mit Active Directory LDAP-Servern ermöglicht:

```
vserver cifs security modify -vserver <SVM_name> -use-start-tls-for-ad
-ldap true
```

> Ab ONTAP 9.13.1 verwendet ONTAP, wenn die sichere LDAP-Kommunikation für Active Directory-Verbindungen aktiviert ist, diese sicheren Verbindungen auch für die Kontaktaufnahme mit Domänencontrollern vertrauenswürdiger Domänen. Wenn die erforderlichen Zertifikate für Domänencontroller vertrauenswürdiger Domänen nicht installiert sind, kann ONTAP möglicherweise keine Standortinformationen zu vertrauenswürdigen Domänen ermitteln.

2. Überprüfen Sie, ob die LDAP-über-TLS-Sicherheitseinstellung auf `true` gesetzt ist:

```
vserver cifs security show -vserver <SVM_name>
```

> Wenn die SVM denselben LDAP-Server für die Abfrage von Namenszuordnungen oder anderen UNIX-Informationen (wie Benutzern, Gruppen und Netzgruppen) verwendet, muss auch die Option `-use-start-tls` mit dem Befehl `vserver services name-service ldap client modify` geändert werden.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.