Gestire le impostazioni di sicurezza del server SMB

ONTAP 9

NetApp
April 24, 2024

Sommario

Gestire le impostazioni di sicurezza del server SMB

In che modo ONTAP gestisce l'autenticazione dei client SMB

Prima che gli utenti possano creare connessioni SMB per accedere ai dati contenuti nella SVM, devono essere autenticati dal dominio a cui appartiene il server SMB. Il server SMB supporta due metodi di autenticazione, Kerberos e NTLM (NTLMv1 o NTLMv2). Kerberos è il metodo predefinito utilizzato per autenticare gli utenti del dominio.

Autenticazione Kerberos

ONTAP supporta l'autenticazione Kerberos durante la creazione di sessioni SMB autenticate.

Kerberos è il servizio di autenticazione principale di Active Directory. Il server Kerberos o il servizio KDC (Kerberos Key Distribution Center) memorizza e recupera informazioni sui principi di sicurezza in Active Directory. A differenza del modello NTLM, i client Active Directory che desiderano stabilire una sessione con un altro computer, ad esempio il server SMB, contattano direttamente un KDC per ottenere le proprie credenziali di sessione.

Autenticazione NTLM

L'autenticazione del client NTLM viene eseguita utilizzando un protocollo di risposta alle sfide basato sulla conoscenza condivisa di un segreto specifico dell'utente basato su una password.

Se un utente crea una connessione SMB utilizzando un account utente Windows locale, l'autenticazione viene eseguita localmente dal server SMB utilizzando NTLMv2.

Linee guida per le impostazioni di sicurezza del server SMB in una configurazione di disaster recovery SVM

Prima di creare una SVM configurata come destinazione di disaster recovery in cui l'identità non viene preservata (la `-identity-preserve` l'opzione è impostata su `false` Nella configurazione di SnapMirror), è necessario conoscere il modo in cui le impostazioni di sicurezza del server SMB vengono gestite sulla SVM di destinazione.

- Le impostazioni di sicurezza del server SMB non predefinite non vengono replicate nella destinazione.

  Quando si crea un server SMB sulla SVM di destinazione, tutte le impostazioni di sicurezza del server SMB vengono impostate sui valori predefiniti. Quando la destinazione di disaster recovery SVM viene inizializzata, aggiornata o risincronizzata, le impostazioni di sicurezza del server SMB sull'origine non vengono replicate nella destinazione.

- È necessario configurare manualmente le impostazioni di sicurezza del server SMB non predefinite.

  Se sono state configurate impostazioni di sicurezza del server SMB non predefinite sulla SVM di origine, è necessario configurare manualmente queste stesse impostazioni sulla SVM di destinazione dopo che la

destinazione diventa di lettura/scrittura (dopo che la relazione SnapMirror è stata interrotta).

Visualizza informazioni sulle impostazioni di sicurezza del server SMB

È possibile visualizzare informazioni sulle impostazioni di sicurezza dei server SMB sulle macchine virtuali dello storage (SVM). È possibile utilizzare queste informazioni per verificare che le impostazioni di protezione siano corrette.

A proposito di questa attività

Un'impostazione di protezione visualizzata può essere il valore predefinito per quell'oggetto o un valore non predefinito configurato utilizzando l'interfaccia CLI di ONTAP o gli oggetti Criteri di gruppo di Active Directory.

Non utilizzare `vserver cifs security show` Comando per i server SMB in modalità workgroup, perché alcune opzioni non sono valide.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su…	Immettere il comando…
Tutte le impostazioni di sicurezza su una SVM specificata	`vserver cifs security show -vserver` *`vserver_name`*
Una o più impostazioni di sicurezza specifiche sulla SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` È possibile immettere `-fields ?` per determinare quali campi è possibile utilizzare.

Esempio

L'esempio seguente mostra tutte le impostazioni di sicurezza per 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
```

Le impostazioni visualizzate dipendono dalla versione di ONTAP in esecuzione.

L'esempio seguente mostra l'inclinazione del clock Kerberos per SVM vs1:

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

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

Informazioni correlate

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Attiva o disattiva la complessità della password richiesta per gli utenti SMB locali

La complessità richiesta delle password offre una maggiore sicurezza per gli utenti SMB locali sulle vostre macchine virtuali di storage (SVM). La funzione di complessità della password richiesta è attivata per impostazione predefinita. Puoi disattivarlo e riattivarlo in qualsiasi momento.

Prima di iniziare

Gli utenti locali, i gruppi locali e l'autenticazione dell'utente locale devono essere abilitati sul server CIFS.

> **A proposito di questa attività**
>
> Non utilizzare `vserver cifs security modify` Comando per un server CIFS in modalità gruppo di lavoro perché alcune opzioni non sono valide.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera che la complessità della password richiesta per gli utenti SMB locali sia…	Immettere il comando…
Attivato	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Disattivato	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Verificare l'impostazione di sicurezza per la complessità della password richiesta: `vserver cifs security show -vserver` *`vserver_name`*

Esempio

L'esempio seguente mostra che la complessità della password richiesta è abilitata per gli utenti SMB locali per SVM vs1:

```
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
```

Informazioni correlate

Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS

Utilizzo di utenti e gruppi locali per l'autenticazione e l'autorizzazione

Requisiti per le password dell'utente locale

Modifica delle password degli account utente locali

Modificare le impostazioni di sicurezza Kerberos del server CIFS

È possibile modificare alcune impostazioni di sicurezza Kerberos del server CIFS, tra cui il tempo massimo consentito di disallineamento del clock Kerberos, la durata del ticket Kerberos e il numero massimo di giorni di rinnovo del ticket.

A proposito di questa attività

Modifica delle impostazioni Kerberos del server CIFS mediante `vserver cifs security modify` Il comando modifica le impostazioni solo sulla singola SVM (Storage Virtual Machine) specificata con `-vserver` parametro. È possibile gestire centralmente le impostazioni di sicurezza Kerberos per tutte le SVM del cluster appartenenti allo stesso dominio Active Directory utilizzando gli oggetti Criteri di gruppo (GPO) di Active Directory.

Fasi

1. Eseguire una o più delle seguenti operazioni:

Se si desidera…	Inserisci…
Specificare il tempo massimo consentito di inclinazione dell'orologio Kerberos in minuti (9.13.1 e successivi) o secondi (9.12.1 o precedenti).	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* L'impostazione predefinita è 5 minuti.
Specificare la durata del ticket Kerberos in ore.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` L'impostazione predefinita è 10 ore.
Specificare il numero massimo di giorni di rinnovo del ticket.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* L'impostazione predefinita è 7 giorni.
Specificare il timeout per i socket sui KDC dopo il quale tutti i KDC sono contrassegnati come irraggiungibili.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* L'impostazione predefinita è 3 secondi.

2. Verificare le impostazioni di sicurezza Kerberos:

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

Esempio

Nell'esempio seguente vengono apportate le seguenti modifiche alla sicurezza Kerberos: "Kerberos Clock

Skew” (inclinazione clock Kerberos) è impostato su 3 minuti e “Kerberos Ticket Age” (durata ticket Kerberos) è impostato su 8 ore per SVM vs1:

```
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
```

Informazioni correlate

"Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS"

"GPO supportati"

"Applicazione di oggetti Criteri di gruppo ai server CIFS"

Impostare il livello minimo di sicurezza per l’autenticazione del server SMB

È possibile impostare il livello di sicurezza minimo del server SMB, noto anche come *LMCompatibilityLevel*, sul server SMB per soddisfare i requisiti di sicurezza aziendali per l’accesso al client SMB. Il livello di sicurezza minimo è il livello minimo dei token di sicurezza che il server SMB accetta dai client SMB.

A proposito di questa attività

- I server SMB in modalità workgroup supportano solo l’autenticazione NTLM. L’autenticazione Kerberos non è supportata.
- LMCompatibilityLevel si applica solo all’autenticazione del client SMB, non all’autenticazione dell’amministratore.

È possibile impostare il livello di sicurezza minimo per l’autenticazione su uno dei quattro livelli di sicurezza supportati.

Valore	Descrizione
`lm-ntlm-ntlmv2-krb` (impostazione predefinita)	La macchina virtuale per lo storage (SVM) accetta la protezione con autenticazione LM, NTLM, NTLMv2 e Kerberos.
`ntlm-ntlmv2-krb`	SVM accetta la sicurezza di autenticazione NTLM, NTLMv2 e Kerberos. SVM nega l'autenticazione LM.
`ntlmv2-krb`	SVM accetta la sicurezza di autenticazione NTLMv2 e Kerberos. SVM nega l'autenticazione LM e NTLM.
`krb`	SVM accetta solo la sicurezza con autenticazione Kerberos. SVM nega l'autenticazione LM, NTLM e NTLMv2.

Fasi

1. Impostare il livello minimo di protezione per l'autenticazione: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verificare che il livello di protezione per l'autenticazione sia impostato sul livello desiderato: `vserver cifs security show -vserver vserver_name`

Informazioni correlate

Attivazione o disattivazione della crittografia AES per le comunicazioni basate su Kerberos

Configurare una protezione avanzata per le comunicazioni basate su Kerberos utilizzando la crittografia AES

Per una maggiore sicurezza con la comunicazione basata su Kerberos, è possibile attivare la crittografia AES-256 e AES-128 sul server SMB. Per impostazione predefinita, quando si crea un server SMB su SVM, la crittografia AES (Advanced Encryption Standard) viene disattivata. È necessario abilitarlo per sfruttare la protezione avanzata fornita dalla crittografia AES.

La comunicazione relativa a Kerberos per SMB viene utilizzata durante la creazione del server SMB sulla SVM e durante la fase di configurazione della sessione SMB. Il server SMB supporta i seguenti tipi di crittografia per le comunicazioni Kerberos:

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

Se si desidera utilizzare il tipo di crittografia con la massima protezione per le comunicazioni Kerberos, è necessario attivare la crittografia AES per le comunicazioni Kerberos su SVM.

Quando viene creato il server SMB, il controller di dominio crea un account computer in Active Directory. A questo punto, il KDC viene a conoscenza delle funzionalità di crittografia di un determinato account di computer. Successivamente, viene selezionato un particolare tipo di crittografia per crittografare il ticket di servizio che il client presenta al server durante l'autenticazione.

A partire da ONTAP 9.12.1, è possibile specificare i tipi di crittografia da segnalare al KDC di Active Directory (ad). È possibile utilizzare `-advertised-enc-types` opzione per attivare i tipi di crittografia consigliati ed è possibile utilizzarla per disattivare i tipi di crittografia più deboli. Scopri come "Attiva e disattiva i tipi di crittografia per le comunicazioni basate su Kerberos".

> Intel AES New Instructions (Intel AES NI) è disponibile in SMB 3.0, migliorando l'algoritmo AES e accelerando la crittografia dei dati con le famiglie di processori supportate.a partire da SMB 3.1.1, AES-128-GCM sostituisce AES-128-CCM come algoritmo hash utilizzato dalla crittografia SMB.

Informazioni correlate

Modifica delle impostazioni di sicurezza Kerberos del server CIFS

Attiva o disattiva la crittografia AES per le comunicazioni basate su Kerberos

Per sfruttare al massimo la protezione della comunicazione basata su Kerberos, è necessario utilizzare la crittografia AES-256 e AES-128 sul server SMB. A partire da ONTAP 9.13.1, la crittografia AES è attivata per impostazione predefinita. Se non si desidera che il server SMB selezioni i tipi di crittografia AES per la comunicazione basata su Kerberos con Active Directory (ad) KDC, è possibile disattivare la crittografia AES.

Se la crittografia AES è attivata per impostazione predefinita e se si dispone dell'opzione per specificare i tipi di crittografia, dipende dalla versione di ONTAP in uso.

Versione di ONTAP	La crittografia AES è abilitata …	È possibile specificare i tipi di crittografia?
9.13.1 e versioni successive	Per impostazione predefinita	Sì
9.12.1	Manualmente	Sì
9.11.1 e precedenti	Manualmente	No

A partire da ONTAP 9.12.1, la crittografia AES viene attivata e disattivata tramite `-advertised-enc-types` Che consente di specificare i tipi di crittografia annunciati a ad KDC. L'impostazione predefinita è `rc4` e. `des`, Ma quando viene specificato un tipo AES, viene attivata la crittografia AES. È inoltre possibile utilizzare l'opzione per disattivare esplicitamente i tipi di crittografia RC4 e DES più deboli. In ONTAP 9.11.1 e versioni precedenti, è necessario utilizzare `-is-aes-encryption-enabled` Opzione per attivare e disattivare la crittografia AES e i tipi di crittografia non possono essere specificati.

Per migliorare la sicurezza, la macchina virtuale di storage (SVM) modifica la password dell'account della macchina in ad ogni volta che viene modificata l'opzione di sicurezza AES. La modifica della password potrebbe richiedere credenziali amministrative ad per l'unità organizzativa (OU) che contiene l'account del computer.

Se una SVM è configurata come destinazione di disaster recovery in cui l'identità non viene preservata (la

`-identity-preserve` l'opzione è impostata su `false` Nella configurazione di SnapMirror), le impostazioni di sicurezza del server SMB non predefinite non vengono replicate nella destinazione. Se è stata attivata la crittografia AES sulla SVM di origine, è necessario abilitarla manualmente.

Esempio 1. Fasi

ONTAP 9.12.1 e versioni successive

1. Eseguire una delle seguenti operazioni:

Se si desidera che i tipi di crittografia AES per la comunicazione Kerberos siano…	Immettere il comando…
Attivato	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Disattivato	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Nota: la `-is-aes-encryption-enabled` L'opzione è obsoleta in ONTAP 9.12.1 e potrebbe essere rimossa in una release successiva.

2. Verificare che la crittografia AES sia attivata o disattivata come desiderato: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Esempi

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su 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
```

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs2. All'amministratore viene richiesto di inserire le credenziali amministrative ad per l'unità organizzativa contenente il server SMB.

```
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 e versioni precedenti

1. Eseguire una delle seguenti operazioni:

Se si desidera che i tipi di crittografia AES per la comunicazione Kerberos siano…	Immettere il comando…
Attivato	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Disattivato	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Verificare che la crittografia AES sia attivata o disattivata come desiderato: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Il `is-aes-encryption-enabled` viene visualizzato il campo `true` Se la crittografia AES è attivata e. `false` se è disattivato.

Esempi

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su 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
```

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs2. All'amministratore viene richiesto di inserire le credenziali amministrative ad per l'unità organizzativa contenente il server SMB.

```
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
```

Utilizza la firma SMB per migliorare la sicurezza di rete

Utilizza la firma SMB per migliorare la panoramica sulla sicurezza di rete

La firma SMB aiuta a garantire che il traffico di rete tra il server SMB e il client non venga compromesso, evitando attacchi di replay. Per impostazione predefinita, ONTAP supporta la firma SMB quando richiesto dal client. Facoltativamente, l'amministratore dello storage può configurare il server SMB in modo che richieda la firma SMB.

In che modo i criteri di firma SMB influiscono sulla comunicazione con un server CIFS

Oltre alle impostazioni di sicurezza della firma SMB del server CIFS, due criteri di firma SMB sui client Windows controllano la firma digitale delle comunicazioni tra i client e il server CIFS. È possibile configurare l'impostazione che soddisfa i requisiti di business.

I criteri SMB dei client sono controllati tramite le impostazioni dei criteri di protezione locali di Windows, che vengono configurate utilizzando Microsoft Management Console (MMC) o gli oggetti Criteri di gruppo di Active Directory. Per ulteriori informazioni sulla firma SMB del client e sui problemi di sicurezza, consultare la documentazione di Microsoft Windows.

Di seguito sono riportate le descrizioni dei due criteri di firma SMB sui client Microsoft:

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

  Questa impostazione controlla se la funzionalità di firma SMB del client è attivata. È attivato per impostazione predefinita. Quando questa impostazione è disattivata sul client, le comunicazioni del client con il server CIFS dipendono dall'impostazione della firma SMB sul server CIFS.

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

  Questa impostazione specifica se il client richiede la firma SMB per comunicare con un server. È disattivato per impostazione predefinita. Quando questa impostazione è disattivata sul client, il comportamento della firma SMB si basa sull'impostazione del criterio per `Microsoft network client: Digitally sign communications (if server agrees)` E l'impostazione sul server CIFS.

> Se l'ambiente include client Windows configurati per richiedere la firma SMB, è necessario attivare la firma SMB sul server CIFS. In caso contrario, il server CIFS non può fornire dati a questi sistemi.

I risultati effettivi delle impostazioni di firma SMB del client e del server CIFS dipendono dal fatto che le sessioni SMB utilizzino SMB 1.0 o SMB 2.x e versioni successive.

La seguente tabella riassume il comportamento effettivo della firma SMB se la sessione utilizza SMB 1.0:

Client	ONTAP - Firma non richiesta	ONTAP—Firma obbligatoria
Firma disattivata e non richiesta	Non firmato	Firmato
Firma abilitata e non richiesta	Non firmato	Firmato
Firma disattivata e obbligatoria	Firmato	Firmato
Firma abilitata e obbligatoria	Firmato	Firmato

> I client SMB 1 di Windows meno recenti e alcuni client SMB 1 non Windows potrebbero non riuscire a connettersi se la firma è disattivata sul client ma richiesta sul server CIFS.

La seguente tabella riassume il comportamento effettivo della firma SMB se la sessione utilizza SMB 2.x o SMB 3.0:

> Per i client SMB 2.x e SMB 3.0, la firma SMB è sempre abilitata. Non può essere disattivato.

Client	ONTAP - Firma non richiesta	ONTAP—Firma obbligatoria
Firma non richiesta	Non firmato	Firmato
Firma obbligatoria	Firmato	Firmato

La seguente tabella riassume il comportamento predefinito della firma SMB del client e del server Microsoft:

Protocollo	Algoritmo hash	Può attivare/disattivare	Può richiedere/non richiedere	Impostazione predefinita del client	Server predefinito	DC predefinito
SMB 1.0	MD5	Sì	Sì	Abilitato (non richiesto)	Disattivato (non richiesto)	Obbligatorio
SMB 2.x	HMAC SHA-256	No	Sì	Non richiesto	Non richiesto	Obbligatorio
SMB 3.0	AES-CMAC.	No	Sì	Non richiesto	Non richiesto	Obbligatorio

> Microsoft sconsiglia di utilizzare `Digitally sign communications (if client agrees)` oppure `Digitally sign communications (if server agrees)` Impostazioni di Criteri di gruppo. Microsoft non consiglia più di utilizzare `EnableSecuritySignature` impostazioni del registro di sistema. Queste opzioni influiscono solo sul comportamento di SMB 1 e possono essere sostituite da `Digitally sign communications (always)` Impostazione di Criteri di gruppo o l' `RequireSecuritySignature` impostazione del registro di sistema. È inoltre possibile ottenere ulteriori informazioni dal Microsoft Blog.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Basics of SMB Signing (informazioni di base sulla firma SMB) (che riguardano sia SMB1 che SMB2)]

Impatto delle performance della firma SMB

Quando le sessioni SMB utilizzano la firma SMB, tutte le comunicazioni SMB da e verso i client Windows hanno un impatto sulle performance, che influisce sia sui client che sul server (ovvero sui nodi del cluster che eseguono la SVM contenente il server SMB).

L'impatto delle performance si presenta come un aumento dell'utilizzo della CPU sia sui client che sul server, anche se la quantità di traffico di rete non cambia.

L'entità dell'impatto delle performance dipende dalla versione di ONTAP 9 in esecuzione. A partire da ONTAP 9.7, un nuovo algoritmo di crittografia off-load può consentire migliori performance nel traffico SMB firmato. L'offload della firma SMB è attivato per impostazione predefinita quando è attivata la firma SMB.

Le migliori performance di firma SMB richiedono la funzionalità di offload AES-NI. Consultare Hardware

Universe (HWU) per verificare che l'offload AES-NI sia supportato per la piattaforma.

Ulteriori miglioramenti delle prestazioni sono possibili anche se si è in grado di utilizzare SMB versione 3,11 che supporta l'algoritmo GCM molto più veloce.

A seconda della rete, della versione di ONTAP 9, della versione SMB e dell'implementazione di SVM, l'impatto delle performance della firma SMB può variare notevolmente; è possibile verificarlo solo tramite test nell'ambiente di rete.

La maggior parte dei client Windows negozia la firma SMB per impostazione predefinita, se attivata sul server. Se si richiede la protezione SMB per alcuni client Windows e se la firma SMB causa problemi di performance, è possibile disattivare la firma SMB su qualsiasi client Windows che non richieda protezione contro gli attacchi di replay. Per informazioni sulla disattivazione della firma SMB sui client Windows, consultare la documentazione di Microsoft Windows.

Consigli per la configurazione della firma SMB

È possibile configurare il comportamento della firma SMB tra i client SMB e il server CIFS per soddisfare i requisiti di sicurezza. Le impostazioni scelte durante la configurazione della firma SMB sul server CIFS dipendono dai requisiti di sicurezza.

È possibile configurare la firma SMB sul client o sul server CIFS. Durante la configurazione della firma SMB, prendere in considerazione i seguenti consigli:

Se…	Consiglio…
Si desidera aumentare la sicurezza della comunicazione tra il client e il server	Rendere necessaria la firma SMB sul client abilitando il `Require Option (Sign always)` impostazione di sicurezza sul client.
Si desidera che tutto il traffico SMB verso una determinata macchina virtuale di storage (SVM) sia firmato	Rendere necessaria la firma SMB sul server CIFS configurando le impostazioni di sicurezza in modo che richiedano la firma SMB.

Per ulteriori informazioni sulla configurazione delle impostazioni di sicurezza del client Windows, consultare la documentazione Microsoft.

Linee guida per la firma SMB quando sono configurati LIFS di dati multipli

Se si attiva o disattiva la firma SMB richiesta sul server SMB, è necessario conoscere le linee guida per le configurazioni LIFS di dati multipli per una SVM.

Quando si configura un server SMB, potrebbero essere configurate più LIF di dati. In tal caso, il server DNS contiene più server `A` Registrare le voci per il server CIFS, utilizzando tutti lo stesso nome host del server SMB, ma ciascuna con un indirizzo IP univoco. Ad esempio, un server SMB con due LIF dati configurati potrebbe avere il seguente DNS `A` voci di record:

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

Il comportamento normale è che, quando si modifica l'impostazione richiesta per la firma SMB, solo le nuove connessioni dai client vengono influenzate dalla modifica dell'impostazione della firma SMB. Tuttavia, esiste un'eccezione a questo comportamento. Esiste un caso in cui un client dispone di una connessione esistente a una condivisione e il client crea una nuova connessione alla stessa condivisione dopo la modifica dell'impostazione, mantenendo la connessione originale. In questo caso, sia la connessione SMB nuova che quella esistente adottano i nuovi requisiti per la firma SMB.

Si consideri il seguente esempio:

1. Client1 si connette a una condivisione senza la firma SMB richiesta utilizzando il percorso `O:\`.
2. L'amministratore dello storage modifica la configurazione del server SMB per richiedere la firma SMB.
3. Client1 si connette alla stessa condivisione con la firma SMB richiesta utilizzando il percorso `S:\` (mantenendo la connessione utilizzando il percorso `O:\`).
4. Il risultato è che la firma SMB viene utilizzata quando si accede ai dati su entrambi `O:\` e. `S:\` dischi.

Attiva o disattiva la firma SMB richiesta per il traffico SMB in entrata

È possibile applicare il requisito per i client di firmare i messaggi SMB attivando la firma SMB richiesta. Se attivato, ONTAP accetta i messaggi SMB solo se dispongono di firme valide. Se si desidera consentire la firma SMB, ma non la si desidera, è possibile disattivare la firma SMB richiesta.

A proposito di questa attività

Per impostazione predefinita, la firma SMB richiesta è disattivata. È possibile attivare o disattivare la firma SMB richiesta in qualsiasi momento.

> La firma SMB non viene disattivata per impostazione predefinita nei seguenti casi:
>
> 1. La firma SMB richiesta è attivata e il cluster viene reinstallato su una versione di ONTAP che non supporta la firma SMB.
> 2. Il cluster viene successivamente aggiornato a una versione di ONTAP che supporta la firma SMB.
>
> In queste circostanze, la configurazione della firma SMB originariamente configurata su una versione supportata di ONTAP viene mantenuta attraverso la reversione e il successivo aggiornamento.

Quando si imposta una relazione di disaster recovery SVM (Storage Virtual Machine), il valore selezionato per `-identity-preserve` opzione di `snapmirror create` Determina i dettagli di configurazione replicati nella SVM di destinazione.

Se si imposta `-identity-preserve` opzione a. `true` (ID-Preserve), l'impostazione di protezione della firma SMB viene replicata nella destinazione.

Se si imposta `-identity-preserve` opzione a. `false` (Non-ID-Preserve), l'impostazione di protezione della firma SMB non viene replicata nella destinazione. In questo caso, le impostazioni di sicurezza del server CIFS sulla destinazione vengono impostate sui valori predefiniti. Se è stata attivata la firma SMB richiesta sulla SVM di origine, è necessario attivare manualmente la firma SMB richiesta sulla SVM di destinazione.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera che la firma SMB richiesta sia…	Immettere il comando…
Attivato	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Disattivato	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Verificare che la firma SMB richiesta sia attivata o disattivata determinando se il valore in `Is Signing Required` nell'output del seguente comando viene impostato il valore desiderato: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Esempio

L'esempio seguente abilita la firma SMB richiesta per 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
```

Le modifiche alle impostazioni di crittografia sono valide per le nuove connessioni. Le connessioni esistenti non sono interessate.

Determinare se le sessioni SMB sono firmate

È possibile visualizzare le informazioni sulle sessioni SMB connesse sul server CIFS. È possibile utilizzare queste informazioni per determinare se le sessioni SMB sono firmate. Questo può essere utile per determinare se le sessioni del client SMB si connettono con le impostazioni di sicurezza desiderate.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su…	Immettere il comando…
Tutte le sessioni firmate su una specifica macchina virtuale di storage (SVM)	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`

Se si desidera visualizzare informazioni su…	Immettere il comando…
Dettagli di una sessione firmata con un ID di sessione specifico sulla SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Esempi

Il seguente comando visualizza le informazioni sulla sessione relative alle sessioni firmate su SVM vs1. L'output di riepilogo predefinito non visualizza il campo di output "is Session Signed":

```
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
```

Il seguente comando visualizza informazioni dettagliate sulla sessione, incluso se la sessione è firmata, in una sessione SMB con un ID sessione 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
```

Informazioni correlate

Monitorare le statistiche delle sessioni firmate SMB

È possibile monitorare le statistiche delle sessioni SMB e determinare quali sessioni stabilite sono firmate e quali no.

A proposito di questa attività

Il `statistics` il comando al livello di privilegio avanzato fornisce `signed_sessions` Contatore che è possibile utilizzare per monitorare il numero di sessioni SMB firmate. Il `signed_sessions` il contatore è disponibile con i seguenti oggetti di statistiche:

- `cifs` Consente di monitorare la firma SMB per tutte le sessioni SMB.
- `smb1` Consente di monitorare la firma SMB per le sessioni SMB 1.0.
- `smb2` Consente di monitorare la firma SMB per le sessioni SMB 2.x e SMB 3.0.

  Le statistiche SMB 3.0 sono incluse nell'output di `smb2` oggetto.

Se si desidera confrontare il numero di sessioni firmate con il numero totale di sessioni, è possibile confrontare l'output per `signed_sessions` contatore con l'output per `established_sessions` contatore.

È necessario avviare una raccolta di campioni di statistiche prima di poter visualizzare i dati risultanti. Se non si interrompe la raccolta dei dati, è possibile visualizzare i dati del campione. L'interruzione della raccolta dei dati fornisce un campione fisso. La mancata interruzione della raccolta dei dati consente di ottenere dati aggiornati da utilizzare per il confronto con le query precedenti. Il confronto può aiutarti a identificare le tendenze.

Fasi

1. Impostare il livello di privilegio su Advanced:
   `set -privilege advanced`
2. Avviare una raccolta di dati:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se non si specifica `-sample-id` Il comando genera un identificatore di esempio e definisce questo campione come campione predefinito per la sessione CLI. Il valore per `-sample-id` è una stringa di testo. Se si esegue questo comando durante la stessa sessione CLI e non si specifica `-sample-id` il comando sovrascrive il campione predefinito precedente.

   È possibile specificare il nodo su cui si desidera raccogliere le statistiche. Se non si specifica il nodo, l'esempio raccoglie le statistiche per tutti i nodi nel cluster.
3. Utilizzare `statistics stop` comando per interrompere la raccolta dei dati per il campione.
4. Visualizzare le statistiche della firma SMB:

Se si desidera visualizzare informazioni per…	Inserisci…
Sessioni firmate	`show -sample-id sample_ID -counter signed_sessions

Se si desidera visualizzare informazioni per…	Inserisci…
node_name [-node *node_name*]`	Sessioni firmate e sessioni stabilite
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

Se si desidera visualizzare le informazioni solo per un singolo nodo, specificare l'opzione `-node` parametro.

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

Esempi

L'esempio seguente mostra come monitorare le statistiche di firma SMB 2.x e SMB 3.0 su Storage Virtual Machine (SVM) vs1.

Il seguente comando passa al livello di privilegio avanzato:

```
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
```

Il seguente comando avvia la raccolta dati per un nuovo campione:

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

Il seguente comando interrompe la raccolta di dati per l'esempio:

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

Il seguente comando mostra le sessioni SMB firmate e le sessioni SMB stabilite per nodo dell'esempio:

```
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
```

Il seguente comando mostra le sessioni SMB firmate per node2 dell'esempio:

```
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
```

Il seguente comando torna al livello di privilegio admin:

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

Informazioni correlate

Determinare se le sessioni SMB sono firmate

"Panoramica sulla gestione e sul monitoraggio delle performance"

Configurare la crittografia SMB richiesta sui server SMB per il trasferimento dei dati su SMB

Panoramica sulla crittografia SMB

La crittografia SMB per i trasferimenti di dati su SMB è un miglioramento della sicurezza che è possibile attivare o disattivare sui server SMB. È inoltre possibile configurare l'impostazione di crittografia SMB desiderata in base alla condivisione mediante un'impostazione di proprietà di condivisione.

Per impostazione predefinita, quando si crea un server SMB sulla Storage Virtual Machine (SVM), la crittografia SMB viene disattivata. È necessario abilitarlo per sfruttare la sicurezza avanzata fornita dalla crittografia SMB.

Per creare una sessione SMB crittografata, il client SMB deve supportare la crittografia SMB. I client Windows che iniziano con Windows Server 2012 e Windows 8 supportano la crittografia SMB.

La crittografia SMB sulla SVM è controllata da due impostazioni:

- Un'opzione di sicurezza per server SMB che attiva la funzionalità sulla SVM
- Una proprietà di condivisione SMB che configura l'impostazione di crittografia SMB in base alla condivisione

È possibile decidere se richiedere la crittografia per l'accesso a tutti i dati sulla SVM o se richiedere la crittografia SMB per accedere ai dati solo nelle condivisioni selezionate. Le impostazioni a livello di SVM sostituiscono quelle a livello di condivisione.

La configurazione effettiva della crittografia SMB dipende dalla combinazione delle due impostazioni ed è descritta nella tabella seguente:

Crittografia SMB server abilitata	Share encoded data Setting Enabled (Condividi dati crittografati	Comportamento della crittografia lato server
Vero	Falso	La crittografia a livello di server è attivata per tutte le condivisioni di SVM. Con questa configurazione, la crittografia viene eseguita per l'intera sessione SMB.

Crittografia SMB server abilitata	Share encoded data Setting Enabled (Condividi dati crittografati	Comportamento della crittografia lato server
Vero	Vero	La crittografia a livello di server è attivata per tutte le condivisioni di SVM, indipendentemente dalla crittografia a livello di condivisione. Con questa configurazione, la crittografia viene eseguita per l'intera sessione SMB.
Falso	Vero	La crittografia a livello di condivisione è attivata per le condivisioni specifiche. Con questa configurazione, la crittografia viene eseguita dalla connessione ad albero.
Falso	Falso	Nessuna crittografia abilitata.

I client SMB che non supportano la crittografia non possono connettersi a un server SMB o a una condivisione che richiede la crittografia.

Le modifiche alle impostazioni di crittografia sono valide per le nuove connessioni. Le connessioni esistenti non sono interessate.

Impatto delle performance della crittografia SMB

Quando le sessioni SMB utilizzano la crittografia SMB, tutte le comunicazioni SMB da e verso i client Windows hanno un impatto sulle performance, che influisce sia sui client che sul server (ovvero sui nodi del cluster che eseguono la SVM che contiene il server SMB).

L'impatto delle performance si presenta come un aumento dell'utilizzo della CPU sia sui client che sul server, anche se la quantità di traffico di rete non cambia.

L'entità dell'impatto delle performance dipende dalla versione di ONTAP 9 in esecuzione. A partire da ONTAP 9.7, un nuovo algoritmo di crittografia off-load può consentire migliori performance nel traffico SMB crittografato. L'offload della crittografia SMB è attivato per impostazione predefinita quando la crittografia SMB è attivata.

Le performance di crittografia SMB avanzate richiedono la funzionalità di offload AES-NI. Consultare Hardware Universe (HWU) per verificare che l'offload AES-NI sia supportato per la piattaforma.

Ulteriori miglioramenti delle prestazioni sono possibili anche se si è in grado di utilizzare SMB versione 3,11 che supporta l'algoritmo GCM molto più veloce.

A seconda della rete, della versione di ONTAP 9, della versione SMB e dell'implementazione di SVM, l'impatto delle performance della crittografia SMB può variare notevolmente; è possibile verificarlo solo tramite test nell'ambiente di rete.

La crittografia SMB è disattivata per impostazione predefinita sul server SMB. È necessario attivare la crittografia SMB solo sulle condivisioni SMB o sui server SMB che richiedono la crittografia. Con la crittografia SMB, ONTAP esegue un'ulteriore elaborazione della decifratura delle richieste e della crittografia delle risposte per ogni richiesta. La crittografia SMB deve quindi essere attivata solo quando necessario.

Attiva o disattiva la crittografia SMB richiesta per il traffico SMB in entrata

Se si desidera richiedere la crittografia SMB per il traffico SMB in entrata, è possibile attivarla sul server CIFS o a livello di condivisione. Per impostazione predefinita, la crittografia SMB non è richiesta.

A proposito di questa attività

È possibile attivare la crittografia SMB sul server CIFS, che si applica a tutte le condivisioni sul server CIFS. Se non si desidera la crittografia SMB richiesta per tutte le condivisioni sul server CIFS o se si desidera attivare la crittografia SMB richiesta per il traffico SMB in entrata su base share-by-share, è possibile disattivare la crittografia SMB richiesta sul server CIFS.

Quando si imposta una relazione di disaster recovery SVM (Storage Virtual Machine), il valore selezionato per `-identity-preserve` opzione di `snapmirror create` Determina i dettagli di configurazione replicati nella SVM di destinazione.

Se si imposta `-identity-preserve` opzione a. `true` (ID-Preserve), l'impostazione di sicurezza della crittografia SMB viene replicata nella destinazione.

Se si imposta `-identity-preserve` opzione a. `false` (Non-ID-Preserve), l'impostazione di sicurezza della crittografia SMB non viene replicata nella destinazione. In questo caso, le impostazioni di sicurezza del server CIFS sulla destinazione vengono impostate sui valori predefiniti. Se è stata attivata la crittografia SMB sulla SVM di origine, è necessario attivare manualmente la crittografia SMB del server CIFS sulla destinazione.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera che la crittografia SMB richiesta per il traffico SMB in entrata sul server CIFS sia…	Immettere il comando…
Attivato	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Disattivato	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Verificare che la crittografia SMB richiesta sul server CIFS sia attivata o disattivata come desiderato: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   Il `is-smb-encryption-required` viene visualizzato il campo `true` Se necessario, la crittografia SMB è attivata sul server CIFS e. `false` se è disattivato.

Esempio

Nell'esempio seguente viene attivata la crittografia SMB richiesta per il traffico SMB in entrata per il server CIFS su 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
```

Determinare se i client sono connessi utilizzando sessioni SMB crittografate

È possibile visualizzare informazioni sulle sessioni SMB connesse per determinare se i client utilizzano connessioni SMB crittografate. Questo può essere utile per determinare se le sessioni del client SMB si connettono con le impostazioni di sicurezza desiderate.

A proposito di questa attività

Le sessioni dei client SMB possono avere uno dei tre livelli di crittografia seguenti:

- `unencrypted`

  La sessione SMB non è crittografata. Non è stata configurata la crittografia a livello di SVM (Storage Virtual Machine) o a livello di condivisione.

- `partially-encrypted`

  La crittografia viene avviata quando si verifica la connessione ad albero. La crittografia a livello di condivisione è configurata. La crittografia a livello di SVM non è attivata.

- `encrypted`

  La sessione SMB è completamente crittografata. La crittografia a livello di SVM è attivata. La crittografia a livello di condivisione potrebbe non essere attivata. L'impostazione di crittografia a livello di SVM sostituisce l'impostazione di crittografia a livello di condivisione.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su…	Immettere il comando…
Sessioni con un'impostazione di crittografia specificata per le sessioni su una SVM specificata	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`

Se si desidera visualizzare informazioni su…	Immettere il comando…
L'impostazione di crittografia per un ID sessione specifico su una SVM specificata	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Esempi

Il seguente comando visualizza informazioni dettagliate sulla sessione, inclusa l'impostazione di crittografia, in una sessione SMB con ID sessione 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
```

Monitorare le statistiche di crittografia SMB

È possibile monitorare le statistiche di crittografia SMB e determinare quali sessioni stabilite e quali connessioni di condivisione sono crittografate e quali no.

A proposito di questa attività

Il `statistics` Command al livello di privilegio avanzato fornisce i seguenti contatori, che è possibile utilizzare per monitorare il numero di sessioni SMB crittografate e condividere le connessioni:

Nome del contatore	Descrizioni
`encrypted_sessions`	Indica il numero di sessioni SMB 3.0 crittografate

Nome del contatore	Descrizioni
`encrypted_share_connections`	Indica il numero di condivisioni crittografate su cui è avvenuta una connessione ad albero
`rejected_unencrypted_sessions`	Indica il numero di configurazioni di sessione rifiutate a causa della mancanza di funzionalità di crittografia del client
`rejected_unencrypted_shares`	Indica il numero di mappature di condivisione rifiutate a causa della mancanza di funzionalità di crittografia del client

Questi contatori sono disponibili con i seguenti oggetti di statistiche:

- `cifs` Consente di monitorare la crittografia SMB per tutte le sessioni SMB 3.0.

  Le statistiche SMB 3.0 sono incluse nell'output di `cifs` oggetto. Se si desidera confrontare il numero di sessioni crittografate con il numero totale di sessioni, è possibile confrontare l'output per `encrypted_sessions` contatore con l'output per `established_sessions` contatore.

  Se si desidera confrontare il numero di connessioni di condivisione crittografate con il numero totale di connessioni di condivisione, è possibile confrontare l'output per `encrypted_share_connections` contatore con l'output per `connected_shares` contatore.

- `rejected_unencrypted_sessions` Fornisce il numero di tentativi di stabilire una sessione SMB che richiede la crittografia da parte di un client che non supporta la crittografia SMB.
- `rejected_unencrypted_shares` Fornisce il numero di tentativi di connessione a una condivisione SMB che richiede la crittografia da parte di un client che non supporta la crittografia SMB.

È necessario avviare una raccolta di campioni di statistiche prima di poter visualizzare i dati risultanti. Se non si interrompe la raccolta dati, è possibile visualizzare i dati del campione. L'interruzione della raccolta dei dati fornisce un campione fisso. La mancata interruzione della raccolta dei dati consente di ottenere dati aggiornati da utilizzare per il confronto con le query precedenti. Il confronto può aiutarti a identificare le tendenze.

Fasi

1. Impostare il livello di privilegio su Advanced:
   `set -privilege advanced`
2. Avviare una raccolta di dati:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se non si specifica `-sample-id` Il comando genera un identificatore di esempio e definisce questo campione come campione predefinito per la sessione CLI. Il valore per `-sample-id` è una stringa di testo. Se si esegue questo comando durante la stessa sessione CLI e non si specifica `-sample-id` il comando sovrascrive il campione predefinito precedente.

   È possibile specificare il nodo su cui si desidera raccogliere le statistiche. Se non si specifica il nodo, l'esempio raccoglie le statistiche per tutti i nodi nel cluster.

3. Utilizzare `statistics stop` comando per interrompere la raccolta dei dati per il campione.

4. Visualizza le statistiche di crittografia SMB:

Se si desidera visualizzare informazioni per…	Inserisci…
Sessioni crittografate	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Sessioni crittografate e sessioni stabilite
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Connessioni di condivisione crittografate
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Connessioni di condivisione crittografate e condivisioni connesse	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Sessioni non crittografate rifiutate	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Connessioni di condivisione non crittografate rifiutate
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

Se si desidera visualizzare le informazioni solo per un singolo nodo, specificare l'opzione `-node` parametro.

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

Esempi

L'esempio seguente mostra come monitorare le statistiche di crittografia SMB 3.0 su storage virtual machine (SVM) vs1.

Il seguente comando passa al livello di privilegio avanzato:

```
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
```

Il seguente comando avvia la raccolta dati per un nuovo campione:

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

Il seguente comando interrompe la raccolta dei dati per quell'esempio:

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

Il seguente comando mostra le sessioni SMB crittografate e le sessioni SMB stabilite dal nodo dell'esempio:

```
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
```

Il comando seguente mostra il numero di sessioni SMB non crittografate rifiutate dal nodo dell'esempio:

```
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.
```

Il comando seguente mostra il numero di condivisioni SMB connesse e di condivisioni SMB crittografate dal nodo dell'esempio:

```
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.
```

Il comando seguente mostra il numero di connessioni di condivisione SMB non crittografate rifiutate dal nodo dell'esempio:

```
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.
```

Informazioni correlate

Determinazione degli oggetti e dei contatori delle statistiche disponibili

"Panoramica sulla gestione e sul monitoraggio delle performance"

Comunicazione sicura della sessione LDAP

Concetti relativi alla firma e al sealing LDAP

A partire da ONTAP 9, è possibile configurare la firma e il sealing per abilitare la

sicurezza della sessione LDAP sulle query a un server Active Directory (ad). È necessario configurare le impostazioni di sicurezza del server CIFS sulla macchina virtuale di storage (SVM) in modo che corrispondano a quelle del server LDAP.

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

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

Abilitare la firma e il sealing LDAP sul server CIFS

Prima che il server CIFS possa utilizzare la firma e il sealing per una comunicazione sicura con un server LDAP di Active Directory, è necessario modificare le impostazioni di sicurezza del server CIFS per abilitare la firma e il sealing LDAP.

Prima di iniziare

Per determinare i valori di configurazione della protezione appropriati, rivolgersi all'amministratore del server ad.

Fasi

1. Configurare l'impostazione di sicurezza del server CIFS che abilita il traffico firmato e sigillato con i server LDAP di Active Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-session -security-for-ad-ldap {none|sign|seal}`

   È possibile attivare la firma (`sign`, integrità dei dati), firma e sigillatura (`seal`, integrità dei dati e crittografia), o nessuna delle due `none`, nessuna firma o sigillatura). Il valore predefinito è `none`.

2. Verificare che l'impostazione di protezione per la firma e il sealing LDAP sia impostata correttamente: `vserver cifs security show -vserver` *`vserver_name`*

> Se SVM utilizza lo stesso server LDAP per eseguire query di mappatura dei nomi o altre informazioni UNIX, ad esempio utenti, gruppi e netgroup, è necessario attivare l'impostazione corrispondente con `-session-security` opzione di `vserver services name-service ldap client modify` comando.

Configurare LDAP su TLS

Esportare una copia del certificato della CA principale autofirmato

Per utilizzare LDAP su SSL/TLS per la protezione delle comunicazioni Active Directory, è necessario prima esportare una copia del certificato CA principale autofirmato di Active Directory Certificate Service in un file di certificato e convertirla in un file di testo ASCII. Questo file di testo viene utilizzato da ONTAP per installare il certificato sulla macchina virtuale di storage (SVM).

Prima di iniziare

Active Directory Certificate Service deve essere già installato e configurato per il dominio a cui appartiene il server CIFS. Per informazioni sull'installazione e la configurazione di Active Director Certificate Services, consultare la Microsoft TechNet Library.

"Microsoft TechNet Library: technet.microsoft.com"

Fase

1. Ottenere un certificato CA principale del controller di dominio presente in `.pem` formato del testo.

   "Microsoft TechNet Library: technet.microsoft.com"

Al termine

Installare il certificato sulla SVM.

Informazioni correlate

"Microsoft TechNet Library"

Installare il certificato della CA principale autofirmato su SVM

Se è richiesta l'autenticazione LDAP con TLS durante l'associazione ai server LDAP, è necessario installare prima il certificato della CA principale autofirmato su SVM.

A proposito di questa attività

Quando LDAP su TLS è attivato, il client LDAP di ONTAP su SVM non supporta i certificati revocati in ONTAP 9.0 e 9.1.

A partire da ONTAP 9.2, tutte le applicazioni di ONTAP che utilizzano le comunicazioni TLS possono controllare lo stato dei certificati digitali utilizzando il protocollo OCSP (Online Certificate Status Protocol). Se OCSP è abilitato per LDAP su TLS, i certificati revocati vengono rifiutati e la connessione non riesce.

Fasi

1. Installare il certificato della CA principale autofirmato:

   a. Avviare l'installazione del certificato: `security certificate install -vserver vserver_name -type server-ca`

      L'output della console visualizza il seguente messaggio: `Please enter Certificate: Press <Enter> when done`

   b. Aprire il certificato `.pem` copiare il certificato con un editor di testo, incluse le righe che iniziano con `-----BEGIN CERTIFICATE-----` e terminando con `-----END CERTIFICATE-----`, quindi incollare il certificato dopo il prompt dei comandi.

   c. Verificare che il certificato sia visualizzato correttamente.

   d. Completare l'installazione premendo Invio.

2. Verificare che il certificato sia installato: `security certificate show -vserver` *`vserver_name`*

Attivare LDAP su TLS sul server

Prima che il server SMB possa utilizzare TLS per una comunicazione sicura con un server LDAP Active Directory, è necessario modificare le impostazioni di sicurezza del server SMB per attivare LDAP su TLS.

A partire da ONTAP 9.10.1, il binding del canale LDAP è supportato per impostazione predefinita sia per le connessioni LDAP Active Directory (ad) che per i servizi di nomi. ONTAP proverà l'associazione del canale con connessioni LDAP solo se Start-TLS o LDAPS è attivato insieme alla sicurezza della sessione impostata su Sign o Seal. Per disattivare o riabilitare l'associazione del canale LDAP con i server ad, utilizzare `-try-channel-binding-for-ad-ldap` con il `vserver cifs security modify` comando.

Per ulteriori informazioni, consulta:

- "Panoramica LDAP"
- "2020 requisiti di binding del canale LDAP e firma LDAP per Windows".

Fasi

1. Configurare l'impostazione di sicurezza del server SMB che consente la comunicazione LDAP sicura con i server LDAP di Active Directory: `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Verificare che l'impostazione di protezione LDAP su TLS sia impostata su `true`: `vserver cifs security show -vserver vserver_name`

> Se SVM utilizza lo stesso server LDAP per eseguire query di mappatura dei nomi o altre informazioni UNIX (ad esempio utenti, gruppi e netgroup), è necessario modificare anche `-use-start-tls` utilizzando l'opzione `vserver services name-service ldap client modify` comando.