Verwenden Sie SMB-Signing, um die Netzwerksicherheit zu erhöhen

ONTAP 9

NetApp
September 12, 2024

Inhalt

Verwenden Sie SMB-Signing, um die Netzwerksicherheit zu erhöhen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Protokoll	Hash-Algorithmus	Kann aktiviert/deaktiviert werden	Bedarf möglich/nicht erforderlich	Client-Standard	Server-Standard	DC-Standard
SMB 3.0	AES-CMAC:	Nein	Ja.	Nicht erforderlich	Nicht erforderlich	Erforderlich

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

Auswirkungen der SMB-Signatur auf die Performance

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

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

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

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

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

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

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

Empfehlungen für die Konfiguration von SMB-Signaturen

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

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

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

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

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

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

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

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

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

Beispiel:

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

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

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

Über diese Aufgabe

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

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

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

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

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

2. Vergewissern Sie sich, dass die erforderliche SMB-Signatur aktiviert oder deaktiviert ist, indem Sie bestimmen, ob der Wert im verwendet wird `Is Signing Required` Feld in der Ausgabe des folgenden Befehls wird auf den gewünschten Wert gesetzt: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Beispiel

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

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

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

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

Bestimmen Sie, ob SMB-Sitzungen signiert sind

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Alle signierten Sitzungen auf einer angegebenen Storage Virtual Machine (SVM)	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Details für eine signierte Sitzung mit einer spezifischen Session-ID auf der SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Beispiele

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

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

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

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

Verwandte Informationen

Überwachen der Statistiken von SMB-signierten Sitzungen

Überwachen Sie die Statistiken von SMB-signierten Sitzungen

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

Über diese Aufgabe

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

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

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

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

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

Schritte

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

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

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

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

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

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

Beispiele

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

Der folgende Befehl bewegt sich auf die erweiterte Berechtigungsebene:

```
cluster1::> set -privilege advanced

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

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

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

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

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

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

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

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

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

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

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

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

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

Der folgende Befehl kehrt zurück zur Administrator-Berechtigungsebene:

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

Verwandte Informationen

Bestimmen, ob SMB-Sitzungen signiert sind

"Performance Monitoring und Management – Überblick"