Webdienste verwalten

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/system-admin/manage-web-services-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Webdienste verwalten . . . 1
- Übersicht zur Verwaltung von Webdiensten . . . 1
- Zugriff auf ONTAP Webdienste verwalten . . . 1
- Die Webprotokoll-Engine in ONTAP verwalten . . . 3
- ONTAP Befehle zur Verwaltung der Webprotokoll-Engine . . . 4
- Zugriff auf ONTAP Webdienste konfigurieren . . . 5
- ONTAP Befehle zur Verwaltung von Webdiensten . . . 7
- Befehle zur Verwaltung von Mountpunkten auf ONTAP Nodes . . . 7
- SSL in ONTAP verwalten . . . 8
  - Befehle zur Verwaltung von SSL . . . 8
- HSTS für ONTAP Webdienste verwenden . . . 9
  - HSTS-Konfiguration anzeigen . . . 9
  - HSTS aktivieren und das maximale Alter festlegen . . . 10
  - HSTS deaktivieren . . . 10
- Probleme beim Zugriff auf ONTAP Webdienste beheben . . . 10

Webdienste verwalten

Übersicht zur Verwaltung von Webdiensten

Sie können einen Webdienst für den Cluster oder eine Storage Virtual Machine (SVM) aktivieren oder deaktivieren, die Einstellungen für Webdienste anzeigen und steuern, ob Benutzer einer Rolle auf einen Webdienst zugreifen können.

Webdienste für den Cluster oder eine SVM lassen sich auf folgende Weise verwalten:

- Aktivieren oder Deaktivieren eines bestimmten Webdienstes
- Festlegung, ob der Zugriff auf einen Webdienst ausschließlich auf verschlüsseltes HTTP (SSL) beschränkt ist
- Anzeige der Verfügbarkeit von Webdiensten
- Benutzern einer Rolle den Zugriff auf einen Webservice erlauben oder verweigern
- Anzeigen der Rollen, die auf einen Webdienst zugreifen dürfen

Damit ein Benutzer auf einen Webdienst zugreifen kann, müssen alle folgenden Bedingungen erfüllt sein:

- Der Benutzer muss authentifiziert sein.

  Ein Webdienst könnte beispielsweise nach einem Benutzernamen und einem Passwort fragen. Die Antwort des Benutzers muss mit einem gültigen Konto übereinstimmen.

- Dem Benutzer muss die korrekte Zugriffsmethode zugewiesen werden.

  Die Authentifizierung ist nur für Benutzer mit der korrekten Zugriffsmethode für den jeweiligen Webdienst erfolgreich. Für den ONTAP API Webdienst `ontapi` müssen Benutzer die `ontapi` Zugriffsmethode haben. Für alle anderen Webdienste müssen Benutzer die `http` Zugriffsmethode haben.

  > Die `security login`Befehle werden verwendet, um die Zugriffsmethoden und Authentifizierungsmethoden von Benutzern zu verwalten.

- Der Webdienst muss so konfiguriert sein, dass die Zugriffskontrollrolle des Benutzers zulässig ist.

  > Sie verwenden die `vserver services web access`Befehle, um den Zugriff einer Rolle auf einen Webdienst zu steuern.

Wenn eine Firewall aktiviert ist, muss die Firewall-Richtlinie für die LIF, die für Webdienste verwendet werden soll, so eingerichtet sein, dass HTTP oder HTTPS zulässig ist.

Wenn Sie HTTPS für den Zugriff auf Webdienste verwenden, muss SSL für den Cluster oder die SVM, die den Webdienst anbietet, ebenfalls aktiviert sein, und Sie müssen ein digitales Zertifikat für den Cluster oder die SVM bereitstellen.

Zugriff auf ONTAP Webdienste verwalten

Ein Webdienst ist eine Anwendung, auf die Benutzer über HTTP oder HTTPS zugreifen können. Der Clusteradministrator kann die Webprotokoll-Engine einrichten, SSL

konfigurieren, einen Webdienst aktivieren und Benutzern einer Rolle den Zugriff auf einen Webdienst ermöglichen.

Ab ONTAP 9.6 werden die folgenden Webdienste unterstützt:

- Service Processor-Infrastruktur (`spi`)

  Dieser Dienst stellt die Protokoll-, Core-Dump- und MIB-Dateien eines Knotens für den HTTP- oder HTTPS-Zugriff über die Cluster-Management-LIF oder eine Knoten-Management-LIF zur Verfügung. Die Standardeinstellung ist `enabled`.

  Bei einer Anfrage zum Zugriff auf die Protokolldateien oder Core-Dump-Dateien eines Knotens erstellt der `spi` Webdienst automatisch einen Mountpunkt von einem Knoten zum Root-Volume eines anderen Knotens, auf dem sich die Dateien befinden. Es ist nicht erforderlich, den Mountpunkt manuell zu erstellen.

- ONTAP APIs (`ontapi`)

  Dieser Dienst ermöglicht das Ausführen von ONTAP-APIs, um administrative Funktionen mit einem Remote-Programm durchzuführen. Die Standardeinstellung ist `enabled`.

  Dieser Dienst wird möglicherweise für einige externe Verwaltungstools benötigt. Wenn beispielsweise der System Manager verwendet wird, sollte dieser Dienst aktiviert bleiben.

- Data ONTAP Erkennung (`disco`)

  Dieser Dienst ermöglicht es externen Verwaltungsanwendungen, den Cluster im Netzwerk zu erkennen. Die Standardeinstellung ist `enabled`.

- Support-Diagnose (`supdiag`)

  Dieser Dienst steuert den Zugriff auf eine privilegierte Umgebung auf dem System, um die Problemanalyse und -behebung zu unterstützen. Die Standardeinstellung ist `disabled`. Dieser Dienst sollte nur auf Anweisung des technischen Supports aktiviert werden.

- System Manager (`sysmgr`)

  Dieser Dienst steuert die Verfügbarkeit des System Manager, der in ONTAP enthalten ist. Die Standardeinstellung ist `enabled`. Dieser Dienst wird nur auf dem Cluster unterstützt.

- Firmware-Update Baseboard Management Controller (BMC) (`FW_BMC`)

  Dieser Dienst ermöglicht Ihnen das Herunterladen von BMC-Firmware-Dateien. Die Standardeinstellung ist `enabled`.

- ONTAP Dokumentation (`docs`)

  Dieser Dienst ermöglicht den Zugriff auf die ONTAP Dokumentation. Die Standardeinstellung ist `enabled`.

- ONTAP RESTful APIs (`docs_api`)

  Dieser Dienst ermöglicht den Zugriff auf die ONTAP RESTful API-Dokumentation. Die Standardeinstellung ist `enabled`.

- Datei-Upload und Download (`fud`)

  Dieser Dienst bietet das Hoch- und Herunterladen von Dateien. Die Standardeinstellung ist `enabled`.

- ONTAP Messaging (`ontapmsg`)

  Dieser Dienst unterstützt eine Publish- und Subscribe-Schnittstelle, mit der Sie Ereignisse abonnieren können. Die Standardeinstellung ist `enabled`.

- ONTAP Portal (`portal`)

  Dieser Dienst implementiert das Gateway in einen virtuellen Server. Die Standardeinstellung ist `enabled`.

- ONTAP RESTful-Schnittstelle (`rest`)

  Dieser Dienst unterstützt eine RESTful-Schnittstelle, die zur Fernverwaltung aller Elemente der Clusterinfrastruktur verwendet wird. Die Standardeinstellung ist `enabled`.

- Support für Security Assertion Markup Language (SAML) Service Provider (`saml`)

  Dieser Dienst stellt Ressourcen zur Unterstützung des SAML-Dienstanbieters bereit. Die Standardeinstellung ist `enabled`.

- SAML Service Provider (`saml-sp`)

  Dieser Dienst bietet Dienste wie SP-Metadaten und den Assertion Consumer Service für den Service Provider an. Die Standardeinstellung ist `enabled`.

Ab ONTAP 9.7 werden die folgenden zusätzlichen Dienste unterstützt:

- Konfigurationssicherungsdateien (`backups`)

  Dieser Dienst ermöglicht Ihnen das Herunterladen von Konfigurationssicherungsdateien. Die Standardeinstellung ist `enabled`.

- ONTAP Sicherheit (`security`)

  Dieser Dienst unterstützt die Verwaltung von CSRF-Tokens für eine verbesserte Authentifizierung. Die Standardeinstellung ist `enabled`.

Die Webprotokoll-Engine in ONTAP verwalten

Sie können die Webprotokoll-Engine im Cluster konfigurieren, um festzulegen, ob der Webzugriff zulässig ist und welche SSL-Versionen verwendet werden dürfen. Sie können außerdem die Konfigurationseinstellungen der Webprotokoll-Engine anzeigen.

Die Webprotokoll-Engine kann auf Clusterebene auf folgende Weise verwaltet werden:

- Sie können festlegen, ob Remote-Clients HTTP oder HTTPS für den Zugriff auf Webdienstinhalte verwenden dürfen, indem Sie den `system services web modify` Befehl mit dem `-external` Parameter verwenden.

- Sie können festlegen, ob SSLv3 für den sicheren Webzugriff verwendet werden soll, indem Sie den `security config modify` Befehl mit dem `-supported-protocol` Parameter verwenden. Standardmäßig ist SSLv3 deaktiviert. Transport Layer Security 1.0 (TLSv1.0) ist aktiviert und kann bei Bedarf deaktiviert werden.

  Weitere Informationen zu `security config modify` finden sich in der "ONTAP-Befehlsreferenz".

- Der Federal Information Processing Standard (FIPS) 140-2-Konformitätsmodus kann für clusterweite Web-Service-Schnittstellen der Steuerungsebene aktiviert werden.

  Standardmäßig ist der FIPS 140-2 Compliance-Modus deaktiviert.

  - **Wenn der FIPS 140-2-Konformitätsmodus deaktiviert ist** Der FIPS 140-2-Konformitätsmodus kann aktiviert werden, indem der `is-fips-enabled` Parameter auf `true` für den `security config modify` Befehl gesetzt wird und anschließend der `security config show` Befehl zur Bestätigung des Online-Status verwendet wird.
  - **Wenn der FIPS 140-2 Konformitätsmodus aktiviert ist**
    - Ab ONTAP 9.11.1 sind TLSv1, TLSv1.1 und SSLv3 deaktiviert, und nur TLSv1.2 und TLSv1.3 bleiben aktiviert. Dies betrifft andere Systeme und Kommunikationswege, die intern und extern zu ONTAP 9 sind. Wenn der FIPS 140-2-Konformitätsmodus aktiviert und anschließend wieder deaktiviert wird, bleiben TLSv1, TLSv1.1 und SSLv3 deaktiviert. Je nach vorheriger Konfiguration bleibt entweder TLSv1.2 oder TLSv1.3 aktiviert.
    - Bei Versionen von ONTAP vor 9.11.1 sind sowohl TLSv1 als auch SSLv3 deaktiviert und nur TLSv1.1 und TLSv1.2 bleiben aktiviert. ONTAP verhindert, dass sowohl TLSv1 als auch SSLv3 aktiviert werden, wenn der FIPS 140-2-Konformitätsmodus aktiviert ist. Wenn der FIPS 140-2-Konformitätsmodus aktiviert und anschließend wieder deaktiviert wird, bleiben TLSv1 und SSLv3 deaktiviert, aber entweder TLSv1.2 oder sowohl TLSv1.1 als auch TLSv1.2 sind aktiviert, abhängig von der vorherigen Konfiguration.

- Die Konfiguration der clusterweiten Sicherheit lässt sich mit dem `system security config show` Befehl anzeigen.

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

Wenn die Firewall aktiviert ist, muss die Firewall-Richtlinie für die logische Schnittstelle (LIF), die für Webdienste verwendet werden soll, so konfiguriert werden, dass HTTP- oder HTTPS-Zugriff erlaubt ist.

Wenn Sie HTTPS für den Zugriff auf Webdienste verwenden, muss SSL auch für den Cluster oder die Storage Virtual Machine (SVM) aktiviert sein, die den Webdienst anbietet, und es ist ein digitales Zertifikat für den Cluster oder die SVM bereitzustellen.

In MetroCluster Konfigurationen werden die Einstellungsänderungen, die Sie für die Webprotokoll-Engine auf einem Cluster vornehmen, nicht auf den Partnercluster repliziert.

Verwandte Informationen

- "TLS-Hardware-Offload konfigurieren"

ONTAP Befehle zur Verwaltung der Webprotokoll-Engine

Sie verwenden die `system services web` Befehle zur Verwaltung der Webprotokoll-Engine. Sie verwenden die `system services firewall policy create` und

`network interface modify` Befehle, um Webzugriffsanfragen das Passieren der Firewall zu ermöglichen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Die Webprotokoll-Engine wird auf Clusterebene konfiguriert: • Die Webprotokoll-Engine für den Cluster kann aktiviert oder deaktiviert werden. • SSLv3 für den Cluster aktivieren oder deaktivieren • FIPS 140-2-Konformität für sichere Webdienste (HTTPS) aktivieren oder deaktivieren	`system services web modify`
Die Konfiguration der Webprotokoll-Engine auf Clusterebene anzeigen, feststellen, ob die Webprotokolle im gesamten Cluster funktionsfähig sind, und anzeigen, ob die FIPS 140-2-Konformität aktiviert und online ist.	`system services web show`
Die Konfiguration der Webprotokoll-Engine auf Knotenebene sowie die Aktivität der Webdienstverarbeitung für die Knoten im Cluster aufzeigen	`system services web node show`
Eine Firewall-Richtlinie erstellen oder einer bestehenden Firewall-Richtlinie den HTTP- oder HTTPS-Protokolldienst hinzufügen, damit Webzugriffsanfragen durch die Firewall geleitet werden können	`system services firewall policy create` Das Setzen des `-service` Parameters auf `http` oder `https` ermöglicht, dass Webzugriffsanfragen durch die Firewall geleitet werden.
Einer Firewall-Richtlinie einem LIF zuordnen	`network interface modify` Der `-firewall-policy`Parameter kann verwendet werden, um die Firewall-Richtlinie eines LIF zu ändern.

Verwandte Informationen

- "Netzwerkschnittstelle ändern"

Zugriff auf ONTAP Webdienste konfigurieren

Die Konfiguration des Zugriffs auf Webdienste ermöglicht es autorisierten Benutzern, über HTTP oder HTTPS auf die Dienstinhalte im Cluster oder einer Storage Virtual Machine (SVM) zuzugreifen.

Schritte

1. Wenn eine Firewall aktiviert ist, muss in der Firewall-Richtlinie für die LIF, die für Webdienste verwendet wird, HTTP- oder HTTPS-Zugriff eingerichtet sein:

   Ob eine Firewall aktiviert ist, lässt sich mit dem `system services firewall show`

Befehl überprüfen.

a. Zur Überprüfung, ob HTTP oder HTTPS in der Firewall-Richtlinie eingerichtet ist, kann der `system services firewall policy show` Befehl verwendet werden.

   Der `-service`Parameter des `system services firewall policy create`Befehls wird auf `http`oder `https`gesetzt, damit die Richtlinie den Webzugriff unterstützt.

b. Zur Überprüfung, ob die Firewall-Richtlinie, die HTTP oder HTTPS unterstützt, dem LIF zugeordnet ist, das Webdienste bereitstellt, kann der `network interface show` Befehl mit dem `-firewall -policy` Parameter verwendet werden.

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

   Sie verwenden den `network interface modify` Befehl mit dem `-firewall-policy` Parameter, um die Firewall-Richtlinie für eine LIF in Kraft zu setzen.

Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Um die Webprotokoll-Engine auf Clusterebene zu konfigurieren und Webdienstinhalte zugänglich zu machen, wird der `system services web modify` Befehl verwendet.
3. Wenn die Nutzung sicherer Webdienste (HTTPS) vorgesehen ist, sollte SSL aktiviert und digitale Zertifikatsinformationen für den Cluster oder die SVM mit dem `security ssl modify` Befehl bereitgestellt werden.

   Weitere Informationen zu `security ssl modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Um einen Webdienst für den Cluster oder die SVM zu aktivieren, wird der `vserver services web modify` Befehl verwendet.

   Dieser Schritt ist für jeden Dienst zu wiederholen, der für den Cluster oder die SVM aktiviert werden soll.

5. Um einer Rolle den Zugriff auf Webdienste auf dem Cluster oder der SVM zu autorisieren, wird der `vserver services web access create` Befehl verwendet.

   Die Rolle, der Sie Zugriff gewähren, muss bereits existieren. Vorhandene Rollen können mit dem `security login role show` Befehl angezeigt oder neue Rollen mit dem `security login role create` Befehl erstellt werden.

   Weitere Informationen zu `security login role show` und `security login role create` finden sich in der "ONTAP-Befehlsreferenz".

6. Für eine Rolle, die zum Zugriff auf einen Webdienst autorisiert wurde, sollte sichergestellt werden, dass ihre Benutzer ebenfalls mit der richtigen Zugriffsmethode konfiguriert sind, indem die Ausgabe des `security login show` Befehls überprüft wird.

   Um auf den ONTAP API Webdienst `ontapi` zuzugreifen, muss ein Benutzer mit der `ontapi` Zugriffsmethode konfiguriert sein. Um auf alle anderen Webdienste zuzugreifen, muss ein Benutzer mit der `http` Zugriffsmethode konfiguriert sein.

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

Mit dem `security login create` Befehl wird eine Zugriffsmethode für einen Benutzer hinzugefügt. Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von Webdiensten

Sie verwenden die `vserver services web` Befehle, um die Verfügbarkeit von Webdiensten für den Cluster oder eine Storage Virtual Machine (SVM) zu verwalten. Sie verwenden die `vserver services web access`Befehle, um den Zugriff einer Rolle auf einen Webdienst zu steuern.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Ein Webdienst für den Cluster oder eine SVM kann konfiguriert werden: • Einen Webservice aktivieren oder deaktivieren • Geben Sie an, ob für den Zugriff auf einen Webdienst ausschließlich HTTPS verwendet werden kann.	`vserver services web modify`
Anzeige der Konfiguration und Verfügbarkeit von Webdiensten für den Cluster oder eine SVM	`vserver services web show`
Eine Rolle für den Zugriff auf einen Webdienst im Cluster oder einer SVM autorisieren	`vserver services web access create`
Die Rollen, die zum Zugriff auf Webdienste im Cluster oder anSVM berechtigt sind, werden angezeigt.	`vserver services web access show`
Verhindern, dass eine Rolle auf einen Webdienst im Cluster oder einer SVM zugreift	`vserver services web access delete`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

Befehle zur Verwaltung von Mountpunkten auf ONTAP Nodes

Der `spi` Webdienst erstellt automatisch einen Mountpunkt von einem Knoten zum Root-Volume eines anderen Knotens, sobald eine Anfrage zum Zugriff auf die Logdateien oder Core-Dateien eines Knotens eingeht. Obwohl Sie Mountpunkte nicht manuell verwalten müssen, kann dies mithilfe der `system node root-mount` Befehle erfolgen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Einen Mountpunkt manuell von einem Knoten zum Root-Volume eines anderen Knotens erstellen	`system node root-mount create`Von einem Knoten zu einem anderen kann nur ein einziger Mountpunkt existieren.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Vorhandene Mountpunkte auf den Knoten im Cluster werden angezeigt, einschließlich des Zeitpunkts ihrer Erstellung und ihres aktuellen Status.	`system node root-mount show`
Einen Mountpunkt von einem Knoten zum Root-Volume eines anderen Knotens löschen und Verbindungen zu diesem Mountpunkt zwangsweise schließen	`system node root-mount delete`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

SSL in ONTAP verwalten

Die `security ssl` Befehle dienen zur Verwaltung des SSL-Protokolls für den Cluster oder eine Storage Virtual Machine (SVM). Das SSL-Protokoll verbessert die Sicherheit des Webzugriffs, indem ein digitales Zertifikat verwendet wird, um eine verschlüsselte Verbindung zwischen einem Webserver und einem Browser herzustellen.

Sie können SSL für den Cluster oder eine Storage Virtual Machine (SVM) auf folgende Weise verwalten:

- SSL-Aktivierung
- Generieren und Installieren eines digitalen Zertifikats und dessen Zuordnung zum Cluster oder zur SVM
- Anzeigen der SSL-Konfiguration, um festzustellen, ob SSL aktiviert ist und, falls verfügbar, der Name des SSL-Zertifikats
- Einrichten von Firewall-Richtlinien für den Cluster oder die SVM, sodass Webzugriffsanfragen durchgelassen werden können
- Festlegen, welche SSL-Versionen verwendet werden können
- Beschränkung des Zugriffs auf einen Webdienst auf HTTPS-Anfragen

Befehle zur Verwaltung von SSL

Sie verwenden die `security ssl` Befehle, um das SSL-Protokoll für den Cluster oder eine Storage Virtual Machine (SVM) zu verwalten.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
SSL für den Cluster oder eine SVM aktivieren und ein digitales Zertifikat zuordnen	`security ssl modify`
Die SSL-Konfiguration und den Zertifikatsnamen für den Cluster oder eine SVM anzeigen	`security ssl show`

Weitere Informationen zu `security ssl modify` und `security ssl show` finden sich in der "ONTAP-Befehlsreferenz".

HSTS für ONTAP Webdienste verwenden

HTTP Strict Transport Security (HSTS) ist ein Sicherheitsmechanismus für Webseiten, der diese vor Man-in-the-Middle-Angriffen wie Protokoll-Downgrade-Angriffen und Cookie-Hijacking schützt. Durch die Erzwingung von HTTPS stellt HSTS sicher, dass die gesamte Kommunikation zwischen dem Browser des Nutzers und dem Server verschlüsselt ist. Ab ONTAP 9.17.1 kann ONTAP HTTPS-Verbindungen für ONTAP Webdienste erzwingen.

> HSTS wird vom Webbrowser erst durchgesetzt, nachdem eine erste sichere HTTPS-Verbindung mit ONTAP hergestellt wurde. Wenn der Browser keine erste sichere Verbindung herstellt, wird HSTS nicht durchgesetzt. Weitere Informationen zur Verwaltung von HSTS enthält die Dokumentation des Browsers.

Über diese Aufgabe

- Ab Version 9.17.1 ist HSTS für neu installierte ONTAP Cluster standardmäßig aktiviert. Beim Upgrade auf 9.17.1 ist HSTS nicht standardmäßig aktiviert. HSTS muss nach dem Upgrade aktiviert werden.
- HSTS wird für alle "ONTAP-Webdienste" unterstützt.

Bevor Sie beginnen

- Für die folgenden Aufgaben sind erweiterte Berechtigungen erforderlich.

HSTS-Konfiguration anzeigen

Sie können die aktuelle HSTS-Konfiguration anzeigen, um zu prüfen, ob sie aktiviert ist, und die Einstellung für das maximale Alter einsehen.

Schritte

1. Mit dem `system services web show`Befehl wird die aktuelle Webdienstkonfiguration einschließlich der HSTS-Einstellungen angezeigt:

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                        Per Address Limit: 80
                      Wait Queue Capacity: 192
                             HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
           Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                            HSTS Enabled: true
```

```
                    HSTS max age (Seconds): 63072000
```

HSTS aktivieren und das maximale Alter festlegen

Ab ONTAP 9.17.1 ist HSTS auf neuen ONTAP Clustern standardmäßig aktiviert. Wenn ein bestehender Cluster auf Version 9.17.1 oder höher aktualisiert wird, muss HSTS manuell auf dem Cluster aktiviert werden, um die Verwendung von HTTPS zu erzwingen. HSTS kann aktiviert und das maximale Alter festgelegt werden. Das maximale Alter kann jederzeit geändert werden, wenn HSTS aktiviert ist. Sobald HSTS aktiviert ist, erzwingen Browser sichere Verbindungen erst, nachdem eine erste sichere Verbindung hergestellt wurde.

Schritte

1. Mit dem `system services web modify`Befehl lässt sich HSTS aktivieren oder das maximale Alter anpassen:

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

   `-hsts-max-age` Gibt die Dauer in Sekunden an, für die der Browser die Durchsetzung von HTTPS beibehält. Der Standardwert beträgt 63072000 Sekunden (zwei Jahre).

HSTS deaktivieren

Browser speichern die Einstellung für die maximale Gültigkeitsdauer von HSTS bei jeder Verbindung und erzwingen HSTS für die gesamte Dauer, selbst wenn HSTS auf ONTAP deaktiviert ist. Nach der Deaktivierung von HSTS dauert es bis zum Ablauf der konfigurierten maximalen Gültigkeitsdauer, bis der Browser die Erzwingung von HSTS beendet. Sollte in diesem Zeitraum keine sichere Verbindung möglich sein, verweigern Browser, die HSTS erzwingen, den Zugriff auf ONTAP Webdienste, bis das Problem behoben ist oder die maximale Gültigkeitsdauer des Browsers abgelaufen ist.

Schritte

1. HSTS mit dem Befehl `system services web modify` deaktivieren:

```
system services web modify -hsts-enabled false
```

Verwandte Informationen

"RFC 6797 – HTTP Strict Transport Security (HSTS)"

Probleme beim Zugriff auf ONTAP Webdienste beheben

Konfigurationsfehler führen zu Problemen beim Zugriff auf Webdienste. Die Fehler lassen sich beheben, wenn LIF, Firewall-Richtlinie, Webprotokoll-Engine, Webdienste, digitale Zertifikate und die Benutzerzugriffsberechtigung korrekt konfiguriert sind.

Die folgende Tabelle unterstützt bei der Identifizierung und Behebung von Konfigurationsfehlern bei Webdiensten:

Dieses Zugriffsproblem…	Tritt aufgrund dieses Konfigurationsfehlers auf…	Um den Fehler zu beheben…
Ihr Webbrowser gibt eine `unable to connect` oder `failure to establish a connection` Fehlermeldung zurück, wenn Sie versuchen, auf einen Webdienst zuzugreifen.	Ihre LIF ist möglicherweise nicht korrekt konfiguriert.	Stellen Sie sicher, dass Sie den LIF anpingen können, der den Webdienst bereitstellt. Sie verwenden den `network ping` Befehl, um einen LIF anzupingen.
Ihre Firewall ist möglicherweise falsch konfiguriert.	Es muss sichergestellt sein, dass eine Firewall-Richtlinie eingerichtet ist, die HTTP oder HTTPS unterstützt, und dass diese Richtlinie dem LIF zugewiesen ist, der den Webdienst bereitstellt. Sie verwenden die `system services firewall policy` Befehle, um Firewall-Richtlinien zu verwalten. Sie verwenden den `network interface modify` Befehl mit dem `-firewall -policy` Parameter, um eine Richtlinie mit einem LIF zu verknüpfen.	Ihre Webprotokoll-Engine ist möglicherweise deaktiviert.
Stellen Sie sicher, dass die Webprotokoll-Engine aktiviert ist, damit Webdienste zugänglich sind. Sie verwenden die `system services web` Befehle, um die Webprotokoll-Engine für den Cluster zu verwalten.	Ihr Webbrowser gibt eine `not found` Fehlermeldung zurück, wenn Sie versuchen, auf einen Webdienst zuzugreifen.	Der Webdienst ist möglicherweise deaktiviert.

Dieses Zugriffsproblem…	Tritt aufgrund dieses Konfigurationsfehlers auf…	Um den Fehler zu beheben…
Stellen Sie sicher, dass jeder Webdienst, auf den Zugriff gewährt werden soll, einzeln aktiviert ist. Der `vserver services web modify`Befehl wird verwendet, um einen Webdienst für den Zugriff zu aktivieren.	Der Webbrowser kann sich mit dem Benutzernamen und dem Passwort nicht bei einem Webdienst anmelden.	Der Benutzer kann nicht authentifiziert werden, das Zugriffsverfahren ist nicht korrekt oder der Benutzer ist nicht berechtigt, auf den Webdienst zuzugreifen.
Stellen Sie sicher, dass das Benutzerkonto existiert und mit dem korrekten Zugriffsverfahren und Authentifizierungsverfahren konfiguriert ist. Außerdem muss die Rolle des Benutzers zum Zugriff auf den Webdienst berechtigt sein. Sie verwenden die `security login` Befehle, um Benutzerkonten sowie deren Zugriffs- und Authentifizierungsverfahren zu verwalten. Für den Zugriff auf den ONTAP API-Webdienst ist die `ontapi` Zugriffsmethode erforderlich. Für den Zugriff auf alle anderen Webdienste ist die `http` Zugriffsmethode erforderlich. Sie verwenden die `vserver services web access` Befehle, um den Zugriff einer Rolle auf einen Webdienst zu verwalten.	Sie stellen über HTTPS eine Verbindung zu Ihrem Webdienst her und Ihr Webbrowser zeigt an, dass Ihre Verbindung unterbrochen ist.	Möglicherweise ist SSL auf dem Cluster oder der Storage Virtual Machine (SVM), die den Webdienst bereitstellt, nicht aktiviert.

Dieses Zugriffsproblem…	Tritt aufgrund dieses Konfigurationsfehlers auf…	Um den Fehler zu beheben…
Es muss sichergestellt sein, dass SSL auf dem Cluster oder der SVM aktiviert ist und dass das digitale Zertifikat gültig ist. Sie verwenden die `security ssl` Befehle zur Verwaltung der SSL-Konfiguration für HTTP-Server und den `security certificate show` Befehl zur Anzeige von Informationen zu digitalen Zertifikaten.	Sie stellen eine Verbindung zu Ihrem Webdienst über HTTPS her, und Ihr Webbrowser zeigt an, dass die Verbindung nicht vertrauenswürdig ist.	Möglicherweise verwenden Sie ein selbstsigniertes digitales Zertifikat.

Verwandte Informationen

- "Was sind Best Practices für die Netzwerkkonfiguration für ONTAP?"
- "Netzwerk-Ping"
- "Netzwerkschnittstelle ändern"
- "security certificate generate-csr"
- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "security ssl"

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.