Verwalten von Webservices

ONTAP 9

NetApp
February 12, 2026

Inhalt

Verwalten von Webservices . . . 1
- Web Services-Übersicht verwalten . . . 1
- Verwalten des Zugriffs auf ONTAP -Webdienste . . . 1
- Verwalten Sie die Webprotokollengine in ONTAP . . . 3
- ONTAP -Befehle zur Verwaltung der Webprotokoll-Engine . . . 4
- Konfigurieren des Zugriffs auf ONTAP Webdienste . . . 5
- ONTAP -Befehle zur Verwaltung von Webdiensten . . . 7
- Befehle zum Verwalten von Mount-Punkten auf ONTAP -Knoten . . . 7
- SSL in ONTAP verwalten . . . 8
  - Befehle zum Verwalten von SSL . . . 8
- Verwenden Sie HSTS für ONTAP Webdienste . . . 9
  - HSTS-Konfiguration anzeigen . . . 9
  - Aktivieren Sie HSTS und legen Sie das Höchstalter fest . . . 10
  - HSTS deaktivieren . . . 10
- Beheben von Problemen beim Zugriff auf ONTAP Webdienste . . . 11

Verwalten von Webservices

Web Services-Übersicht verwalten

Sie können einen Webdienst für das Cluster oder eine Storage Virtual Machine (SVM) aktivieren bzw. deaktivieren, die Einstellungen für Webservices anzeigen und festlegen, ob Benutzer einer Rolle auf einen Webservice zugreifen können.

Es gibt folgende Möglichkeiten, Web-Services für das Cluster oder eine SVM zu managen:

- Aktivieren oder Deaktivieren eines bestimmten Webservice
- Festlegen, ob der Zugriff auf einen Webdienst nur auf verschlüsseltes HTTP (SSL) beschränkt ist
- Anzeigen der Verfügbarkeit von Webservices
- Benutzern einer Rolle den Zugriff auf einen Webservice zu ermöglichen oder zu verdrängen
- 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.

  Beispielsweise kann ein Webdienst einen Benutzernamen und ein Kennwort anfordern. Die Antwort des Benutzers muss mit einem gültigen Konto übereinstimmen.

- Der Benutzer muss mit der richtigen Zugriffsmethode eingerichtet sein.

  Authentifizierung ist nur für Benutzer mit der richtigen Zugriffsmethode für den angegebenen Webdienst erfolgreich. Für den Webservice der ONTAP-API (`ontapi`) müssen Benutzer über die `ontapi` Zugriffsmethode verfügen. Für alle anderen Webdienste müssen Benutzer über die `http` Zugriffsmethode verfügen.

  > Sie verwenden die `security login` Befehle, um die Zugriffsmethoden und Authentifizierungsmethoden von Benutzern zu verwalten.

- Der Webdienst muss so konfiguriert sein, dass die Zugriffskontrollrolle des Benutzers zugelassen wird.

  > 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 Firewallrichtlinie für die Nutzung von LIF für Web-Services so eingerichtet sein, dass HTTP oder HTTPS möglich sind.

Wenn Sie HTTPS für den Webservice-Zugriff verwenden, muss auch die SSL für das Cluster oder die SVM mit dem Webservice aktiviert sein. Des Weiteren müssen Sie ein digitales Zertifikat für das Cluster oder die SVM vorlegen.

Verwalten des Zugriffs auf ONTAP -Webdienste

Ein Webservice ist eine Anwendung, auf die Benutzer über HTTP oder HTTPS zugreifen

können. Der Clusteradministrator kann die Web-Protokoll-Engine einrichten, SSL konfigurieren, einen Webdienst aktivieren und Benutzern einer Rolle den Zugriff auf einen Webdienst ermöglichen.

Ab ONTAP 9.6 werden die folgenden Webservices unterstützt:

- Service-Prozessor-Infrastruktur (`spi`)

  Dieser Service stellt Protokoll, Core Dump und MIB-Dateien für HTTP- oder HTTPS-Zugriff über die Cluster-Management-LIF oder Node-Management-LIF bereit. Die Standardeinstellung ist `enabled`.

  Bei einer Anfrage zum Zugriff auf die Protokolldateien oder Core-Dump-Dateien eines Knotens wird der `spi` Der Webdienst erstellt automatisch einen Einhängepunkt von einem Knoten zum Stammvolume eines anderen Knotens, auf dem sich die Dateien befinden. Sie müssen den Einhängepunkt nicht manuell erstellen.

- ONTAP-APIs (`ontapi`)

  Mit diesem Service können Sie ONTAP APIs ausführen und administrative Funktionen mit einem Remote-Programm ausführen. Die Standardeinstellung ist `enabled`.

  Dieser Service ist möglicherweise für einige externe Verwaltungstools erforderlich. Wenn Sie beispielsweise System Manager verwenden, sollten Sie diesen Service aktiviert lassen.

- Data ONTAP-Ermittlung(`disco`)

  Dieser Service ermöglicht Off-Box-Managementapplikationen, den Cluster im Netzwerk zu erkennen. Die Standardeinstellung ist `enabled`.

- Support-Diagnose (`supdiag`)

  Dieser Service steuert den Zugriff auf eine privilegierte Umgebung des Systems, um die Problemanalyse und -Behebung zu unterstützen. Die Standardeinstellung ist `disabled`. Sie sollten diesen Service nur aktivieren, wenn Sie sich unter Anleitung durch den technischen Support richten.

- System Manager (`sysmgr`)

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

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

  Mit diesem Service können Sie BMC-Firmware-Dateien herunterladen. Die Standardeinstellung ist `enabled`.

- ONTAP Dokumentation (`docs`)

  Dieser Service bietet Zugriff auf die ONTAP-Dokumentation. Die Standardeinstellung ist `enabled`.

- ONTAP RESTful APIs(`docs_api`

  Dieser Service bietet Zugriff auf die Dokumentation der ONTAP RESTful API. Die Standardeinstellung ist `enabled`.

- Datei hochladen und herunterladen (`fud`)

  Dieser Service bietet Datei-Upload und Download. Die Standardeinstellung ist `enabled`.

- ONTAP-Nachrichten (`ontapmsg`)

  Dieser Service unterstützt eine Schnittstelle für Veröffentlichung und Abonnements, über die Sie Ereignisse abonnieren können. Die Standardeinstellung ist `enabled`.

- ONTAP-Portal (`portal`)

  Dieser Service implementiert das Gateway auf einem virtuellen Server. Die Standardeinstellung ist `enabled`.

- ONTAP RESTful-Schnittstelle (`rest`)

  Dieser Service unterstützt eine RESTful Schnittstelle, über die alle Elemente der Cluster-Infrastruktur per Remote-Zugriff gemanagt werden. Die Standardeinstellung ist `enabled`.

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

  Dieser Service bietet Ressourcen zur Unterstützung des SAML-Service-Providers. Die Standardeinstellung ist `enabled`.

- SAML-Dienstanbieter (`saml-sp`)

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

Ab ONTAP 9.7 werden die folgenden zusätzlichen Services unterstützt:

- Sicherungsdateien Für Die Konfiguration (`backups`)

  Dieser Service ermöglicht Ihnen das Herunterladen von Backup-Konfigurationsdateien. Die Standardeinstellung ist `enabled`.

- ONTAP-Sicherheit(`security`)

  Dieser Service unterstützt das CSRF-Token-Management für eine erweiterte Authentifizierung. Die Standardeinstellung ist `enabled`.

Verwalten Sie die Webprotokollengine in ONTAP

Sie können die Web Protocol Engine auf dem Cluster so konfigurieren, dass festgelegt wird, ob Webzugriff zulässig ist und welche SSL-Versionen verwendet werden können. Sie können auch die Konfigurationseinstellungen für die Web-Protokoll-Engine anzeigen.

Sie haben folgende Möglichkeiten, die Web-Protokoll-Engine auf Cluster-Ebene zu verwalten:

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

Parameter verwenden.

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

  Erfahren Sie mehr über `security config modify` in der "ONTAP-Befehlsreferenz".

- Sie können den Compliance-Modus des Federal Information Processing Standard (FIPS) 140-2 für Cluster-weite Webservice-Schnittstellen auf Kontrollebene aktivieren.

  Der FIPS 140-2-2-Compliance-Modus ist standardmäßig deaktiviert.

  - **Wenn der FIPS 140-2-Compliance-Modus deaktiviert ist** können Sie den FIPS 140-2-Compliance-Modus aktivieren `is-fips-enabled true` `security config modify`, indem Sie den Parameter für den `security config show` Befehl auf setzen und dann den Online-Status mit dem Befehl bestätigen.
  - **Wenn der FIPS 140-2-Konformitätsmodus aktiviert ist**
    - Ab ONTAP 9.11.1 sind TLSv1, TLSv1.1 und SSLv3 deaktiviert, und nur TSLv1.2 und TSLv1.3 bleiben aktiviert. Sie wirkt sich auf andere interne und externe Systeme und Kommunikation mit ONTAP 9 aus. Wenn Sie den FIPS 140-2 Compliance-Modus aktivieren und anschließend deaktivieren, bleiben TLSv1, TLSv1.1 und SSLv3 deaktiviert. Je nach vorheriger Konfiguration bleibt entweder TLSv1.2 oder TLSv1.3 aktiviert.
    - Für Versionen von ONTAP vor 9.11.1 sind TLSv1 und SSLv3 deaktiviert, und nur TLSv1.1 und TLSv1.2 bleiben aktiviert. ONTAP verhindert, dass Sie TLSv1 und SSLv3 aktivieren, wenn der Compliance-Modus nach FIPS 140-2 aktiviert ist. Wenn Sie den FIPS 140-2-Compliance-Modus aktivieren und anschließend deaktivieren, bleiben TLSv1 und SSLv3 deaktiviert, jedoch sind je nach vorheriger Konfiguration entweder TLSv1.2 oder TLSv1.1 und TLSv1.2 aktiviert.

- Sie können die Konfiguration der Sicherheit für das gesamte Cluster mit dem `system security config show` Befehl anzeigen.

  Erfahren Sie mehr über `security config show` in der "ONTAP-Befehlsreferenz".

Wenn die Firewall aktiviert ist, muss die Firewallrichtlinie für die logische Schnittstelle (LIF) eingerichtet werden, die für Webservices verwendet werden soll, damit HTTP- oder HTTPS-Zugriff möglich ist.

Wenn Sie HTTPS für den Webservice-Zugriff verwenden, muss auch die SSL für das Cluster oder die Storage Virtual Machine (SVM) mit dem Web-Service aktiviert sein. Des Weiteren müssen Sie ein digitales Zertifikat für das Cluster oder die SVM angeben.

In MetroCluster Konfigurationen werden die von Ihnen vorgenommenen Änderungen an der Web Protocol Engine eines Clusters nicht im Partner-Cluster repliziert.

ONTAP -Befehle zur Verwaltung der Webprotokoll-Engine

Sie verwenden die `system services web` Befehle, um die Web-Protokoll-Engine zu verwalten. Mit den `system services firewall policy create` `network interface modify` Befehlen und können Sie zulassen, dass Webzugriffsanfragen durch die Firewall geleitet werden.

Ihr Ziel ist	Befehl
Konfigurieren Sie die Web Protocol Engine auf Cluster-Ebene: • Aktiviert oder deaktiviert die Web Protocol Engine für das Cluster • Aktivieren oder deaktivieren Sie SSLv3 für das Cluster • Aktivieren oder Deaktivieren der Compliance nach FIPS 140-2 für sichere Web-Services (HTTPS)	`system services web modify`
Anzeige der Konfiguration der Web Protocol Engine auf Cluster-Ebene, Ermittlung der Funktionsfähigkeit der Webprotokolle im gesamten Cluster und Anzeige der online-aktivierten FIPS 140-2-Compliance-Funktionen	`system services web show`
Zeigt die Konfiguration der Web-Protokoll-Engine auf Node-Ebene und die Aktivitäten der Webservice-Handhabung für die Knoten im Cluster an	`system services web node show`
Erstellen Sie eine Firewallrichtlinie oder fügen Sie einem vorhandenen Firewallrichtlinie HTTP- oder HTTPS-Protokollservice hinzu, um Webzugriffsanfragen durch die Firewall zu durchlaufen	`system services firewall policy create` Wenn Sie den `-service` Parameter auf `http` oder `https` setzen, können Webzugriffsanfragen über die Firewall geleitet werden.
Zuordnen einer Firewallrichtlinie zu einer logischen Schnittstelle	`network interface modify` Sie können den `-firewall-policy` Parameter verwenden, um die Firewallrichtlinie einer logischen Schnittstelle zu ändern.

Verwandte Informationen

- "Änderung der Netzwerkschnittstelle"

Konfigurieren des Zugriffs auf ONTAP Webdienste

Durch die Konfiguration des Zugriffs auf Webservices können autorisierte Benutzer HTTP oder HTTPS verwenden, um auf den Service-Inhalt des Clusters oder eine Storage Virtual Machine (SVM) zuzugreifen.

Schritte

1. Wenn eine Firewall aktiviert ist, stellen Sie sicher, dass in der Firewallrichtlinie für die LIF HTTP- oder HTTPS-Zugriffe eingerichtet sind, die für Web-Services verwendet werden:

Mit dem `system services firewall show` Befehl können Sie überprüfen, ob eine Firewall aktiviert ist.

a. Um zu überprüfen, ob HTTP oder HTTPS in der Firewallrichtlinie eingerichtet `system services firewall policy show` sind, verwenden Sie den Befehl.

   Sie setzen den `-service` Parameter des `system services firewall policy create` Befehls auf `http` oder `https`, um die Richtlinie für den Webzugriff zu aktivieren.

b. Um zu überprüfen, ob die Firewallrichtlinie, die HTTP oder HTTPS unterstützt, mit der logischen Schnittstelle verknüpft ist, die Webservices bereitstellt, verwenden Sie den `network interface show` Befehl mit dem `-firewall-policy` Parameter.

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

   Sie verwenden den `network interface modify` Befehl mit dem `-firewall-policy` Parameter, um die Firewallrichtlinie für eine LIF anzuwenden.

Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

2. Um die Web-Protokoll-Engine auf Cluster-Ebene zu konfigurieren und den Zugriff auf Web-Service-Inhalte `system services web modify` zu ermöglichen, verwenden Sie den Befehl.
3. Wenn Sie planen, sichere Webservices (HTTPS) zu verwenden, aktivieren Sie SSL und stellen Sie mit dem `security ssl modify` Befehl digitale Zertifikatinformationen für den Cluster oder die SVM bereit.

   Erfahren Sie mehr über `security ssl modify` in der "ONTAP-Befehlsreferenz".

4. Um einen Web Service für das Cluster oder die SVM zu aktivieren, verwenden Sie den `vserver services web modify` Befehl.

   Sie müssen diesen Schritt für jeden Service wiederholen, den Sie für das Cluster oder die SVM aktivieren möchten.

5. Um eine Rolle für den Zugriff auf Webservices im Cluster oder der SVM `vserver services web access create` zu autorisieren, verwenden Sie den Befehl.

   Die Rolle, die Sie Zugriff gewähren, muss bereits vorhanden sein. Sie können vorhandene Rollen mit dem `security login role show` Befehl anzeigen oder mit dem `security login role create` Befehl neue Rollen erstellen.

   Erfahren Sie mehr über `security login role show` und `security login role create` in der "ONTAP-Befehlsreferenz".

6. Für eine Rolle, die für den Zugriff auf einen Webdienst autorisiert wurde, stellen Sie sicher `security login show`, dass die Benutzer auch mit der richtigen Zugriffsmethode konfiguriert sind, indem Sie die Ausgabe des Befehls überprüfen.

   Um auf den Webservice der ONTAP API zuzugreifen `ontapi`, muss ein Benutzer mit der `ontapi` Zugriffsmethode konfiguriert werden. Um auf alle anderen Webservices zugreifen `http` zu können, muss ein Benutzer mit der Zugriffsmethode konfiguriert sein.

   Erfahren Sie mehr über `security login show` in der "ONTAP-Befehlsreferenz".

Sie verwenden den `security login create` Befehl, um eine Zugriffsmethode für einen Benutzer hinzuzufügen. Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

ONTAP -Befehle zur Verwaltung von Webdiensten

Mit den `vserver services web` Befehlen managen Sie die Verfügbarkeit von Web-Services für das Cluster oder eine Storage Virtual Machine (SVM). Sie verwenden die `vserver services web access` Befehle, um den Zugriff einer Rolle auf einen Webdienst zu steuern.

Ihr Ziel ist	Befehl
Konfigurieren eines Webservice für das Cluster oder anSVM: • Aktivieren oder Deaktivieren eines Webservice • Geben Sie an, ob nur HTTPS für den Zugriff auf einen Webdienst verwendet werden kann	`vserver services web modify`
Anzeigen der Konfiguration und Verfügbarkeit von Webservices für das Cluster oder eine anSVM	`vserver services web show`
Autorisieren eine Rolle für den Zugriff auf einen Web-Service auf dem Cluster oder einer anSVM	`vserver services web access create`
Zeigen Sie die Rollen an, die für den Zugriff auf Webservices im Cluster oder auf anSVM autorisiert sind	`vserver services web access show`
Verhindern Sie, dass eine Rolle auf einen Webservice auf dem Cluster oder einer anSVM zugreift	`vserver services web access delete`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

Befehle zum Verwalten von Mount-Punkten auf ONTAP -Knoten

Der `spi` Webdienst erstellt automatisch einen Bereitstellungspunkt von einem Node zum Root-Volume eines anderen Node, wenn auf die Protokolldateien oder Kerndateien des Node zugegriffen werden soll. Obwohl Sie Mount-Punkte nicht manuell verwalten müssen, können Sie dies mithilfe der `system node root-mount` Befehle tun.

Ihr Ziel ist	Befehl
Erstellen Sie manuell einen Mount-Punkt von einem Node zum Root-Volume eines anderen Nodes	`system node root-mount create` Von einem Node zum anderen kann nur ein einzelner Bereitstellungspunkt vorhanden sein.
Zeigen Sie vorhandene Mount-Punkte auf den Nodes im Cluster an, einschließlich der Zeit, die ein Mount-Punkt erstellt wurde, und des aktuellen Status	`system node root-mount show`
Löschen Sie einen Bereitstellungspunkt von einem Node zum Root-Volume eines anderen Node, und erzwingen Sie die Verbindungen zum Mount-Punkt zum Schließen	`system node root-mount delete`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

SSL in ONTAP verwalten

Verwenden Sie die `security ssl` Befehle, um das SSL-Protokoll für das Cluster oder eine SVM (Storage Virtual Machine) zu managen. Das SSL-Protokoll verbessert die Sicherheit des Webzugriffs, indem es ein digitales Zertifikat verwendet, um eine verschlüsselte Verbindung zwischen einem Webserver und einem Browser herzustellen.

Sie haben folgende Möglichkeiten, SSL für das Cluster oder eine Storage Virtual Machine (SVM) zu verwalten:

- Aktivieren von SSL
- Generieren und Installieren eines digitalen Zertifikats und Verknüpfen eines Zertifikats mit dem Cluster oder der SVM
- Anzeigen der SSL-Konfiguration zur Bestätigung, ob SSL aktiviert wurde, und, falls verfügbar, der Name des SSL-Zertifikats
- Einrichtung von Firewallrichtlinien für das Cluster oder SVM, um Webzugriffsanfragen durchzuführen
- Definieren, welche SSL-Versionen verwendet werden können
- Beschränkung des Zugriffs auf nur HTTPS-Anforderungen für einen Webdienst

Befehle zum Verwalten von SSL

Mit den `security ssl` Befehlen managen Sie das SSL-Protokoll für den Cluster oder eine Storage Virtual Machine (SVM).

Ihr Ziel ist	Befehl
Aktivieren Sie SSL für den Cluster oder eine SVM, und verknüpfen Sie ein digitales Zertifikat mit diesem	`security ssl modify`

Ihr Ziel ist	Befehl
Zeigt die SSL-Konfiguration und den Zertifikatnamen für das Cluster oder eine SVM an	`security ssl show`

Erfahren Sie mehr über `security ssl modify` und `security ssl show` in der "ONTAP-Befehlsreferenz".

Verwenden Sie HSTS für ONTAP Webdienste

HTTP Strict Transport Security (HSTS) ist ein Mechanismus für Websicherheitsrichtlinien, der Websites vor Man-in-the-Middle-Angriffen wie Protokoll-Downgrades und Cookie-Hijacking schützt. Durch die erzwungene Verwendung von HTTPS stellt HSTS sicher, dass die gesamte Kommunikation zwischen dem Browser des Benutzers und dem Server verschlüsselt ist. Ab ONTAP 9.17.1 kann ONTAP HTTPS-Verbindungen für ONTAP Webdienste erzwingen.

HSTS wird vom Webbrowser erst erzwungen, nachdem eine erste sichere HTTPS-Verbindung mit ONTAP hergestellt wurde. Wenn der Browser keine erste sichere Verbindung herstellt, wird HSTS nicht erzwungen. Informationen zur HSTS-Verwaltung finden Sie in der Dokumentation Ihres 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 standardmäßig deaktiviert. Sie müssen HSTS nach dem Upgrade aktivieren.
- HSTS wird für alle unterstützt "ONTAP -Webdienste" .

Bevor Sie beginnen

- Für die folgenden Aufgaben sind erweiterte Berechtigungen erforderlich.

HSTS-Konfiguration anzeigen

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

Schritte

1. Verwenden Sie die `system services web show` Befehl zum Anzeigen der aktuellen Webdienstkonfiguration, einschließlich der HSTS-Einstellungen:

```
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
```

Aktivieren Sie HSTS und legen Sie das Höchstalter fest

Ab ONTAP 9.17.1 ist HSTS auf neuen ONTAP Clustern standardmäßig aktiviert. Wenn Sie einen vorhandenen Cluster auf 9.17.1 oder höher aktualisieren, müssen Sie HSTS manuell aktivieren, um die Verwendung von HTTPS zu erzwingen. Sie können HSTS aktivieren und das maximale Alter festlegen. Sie können das maximale Alter jederzeit ändern, wenn HSTS aktiviert ist. Sobald HSTS aktiviert ist, erzwingen Browser sichere Verbindungen erst, nachdem eine erste sichere Verbindung hergestellt wurde.

Schritte

1. Verwenden Sie die `system services web modify` Befehl zum Aktivieren von HSTS oder Ändern des Höchstalters:

```
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 HTTPS-Erzwingung speichert. Der Standardwert beträgt 63072000 Sekunden (zwei Jahre).

HSTS deaktivieren

Browser speichern die Einstellung für das maximale HSTS-Alter bei jeder Verbindung und setzen HSTS während der gesamten Dauer durch, selbst wenn HSTS auf ONTAP deaktiviert ist. Nach der Deaktivierung dauert es bis zur konfigurierten maximalen Altersdauer, bis der Browser die HSTS-Durchsetzung beendet. Sollte während dieser Zeit keine sichere Verbindung möglich sein, erlauben Browser, die HSTS erzwingen, keinen Zugriff auf ONTAP Webdienste, bis das Problem behoben ist oder die maximale Altersgrenze des Browsers abgelaufen ist.

Schritte

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

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

Verwandte Informationen

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

Beheben von Problemen beim Zugriff auf ONTAP Webdienste

Konfigurationsfehler führen zu Problemen mit dem Webservice-Zugriff. Sie können die Fehler beheben, indem Sie sicherstellen, dass LIF, Firewall-Richtlinie, Web-Protokoll-Engine, Web-Services, digitale Zertifikate, Und die Benutzerzugriffsautorisierung sind alle richtig konfiguriert.

Die folgende Tabelle hilft Ihnen bei der Identifizierung und Behebung von Fehlern bei der Webservice-Konfiguration:

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Ihr Webbrowser gibt einen `unable to connect failure to establish a connection` Fehler oder zurück, wenn Sie versuchen, auf einen Webdienst zuzugreifen.	Ihr LIF ist möglicherweise falsch konfiguriert.	Stellen Sie sicher, dass Sie die LIF anpingen können, die den Webservice bereitstellt. Sie verwenden den `network ping` Befehl, um eine LIF zu pingen.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Ihre Firewall ist möglicherweise falsch konfiguriert. Sie verwenden die `system services firewall policy` Befehle zum Verwalten von Firewallrichtlinien. Sie verwenden den `network interface modify` Befehl mit dem `-firewall -policy` Parameter, um eine Richtlinie einer LIF zuzuordnen.	Vergewissern Sie sich, dass eine Firewallrichtlinie eingerichtet ist, um HTTP oder HTTPS zu unterstützen und die Richtlinie der logischen Schnittstelle, die den Webservice bereitstellt, zugewiesen ist.	Ihre Web-Protokoll-Engine ist möglicherweise deaktiviert.
Stellen Sie sicher, dass die Web Protocol Engine aktiviert ist, damit Webservices verfügbar sind. Sie verwenden die `system services web` Befehle, um die Web-Protokoll-Engine für den Cluster zu verwalten.	Ihr Webbrowser gibt einen `not found` Fehler zurück, wenn Sie versuchen, auf einen Webdienst zuzugreifen.	Der Webdienst ist möglicherweise deaktiviert.
Stellen Sie sicher, dass jeder Webdienst, auf den Sie Zugriff zulassen möchten, individuell aktiviert ist. Sie verwenden den `vserver services web modify` Befehl, um einen Webdienst für den Zugriff zu aktivieren.	Der Webbrowser meldet sich nicht bei einem Webdienst mit dem Kontonamen und Passwort eines Benutzers an.	Der Benutzer kann nicht authentifiziert werden, die Zugriffsmethode ist nicht korrekt oder der Benutzer ist nicht berechtigt, auf den Webdienst zuzugreifen.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Stellen Sie sicher, dass das Benutzerkonto vorhanden ist und mit der richtigen Zugriffsmethode und Authentifizierungsmethode konfiguriert ist. Stellen Sie außerdem sicher, dass die Rolle des Benutzers für den Zugriff auf den Webdienst autorisiert ist. Sie verwenden die `security login` Befehle, um Benutzerkonten und ihre Zugriffsmethoden und Authentifizierungsmethoden zu verwalten. Für den Zugriff auf den Webservice der ONTAP-API ist die `ontapi` Zugriffsmethode erforderlich. Für den Zugriff auf alle anderen Webdienste `http` ist die Zugriffsmethode erforderlich. Sie verwenden die `vserver services web access` Befehle, um den Zugriff einer Rolle auf einen Webdienst zu verwalten.	Sie stellen eine Verbindung zu Ihrem Webdienst über HTTPS her, und Ihr Webbrowser zeigt an, dass die Verbindung unterbrochen wird.	Möglicherweise ist SSL nicht auf dem Cluster oder der Storage Virtual Machine (SVM) aktiviert, die den Webservice bereitstellt.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Vergewissern Sie sich, dass für den Cluster oder die SVM SSL aktiviert ist und das digitale Zertifikat gültig ist. Sie verwenden die `security ssl` Befehle, um die SSL-Konfiguration für HTTP-Server `security certificate show` zu verwalten, und den Befehl, um digitale Zertifikatinformation en anzuzeigen.	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"
- "Änderung der Netzwerkschnittstelle"
- "Sicherheitszertifikat generieren-csr"
- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "Sicherheit SSL"