



Management des Zugriffs auf Webservices

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

- Management des Zugriffs auf Webservices 1
 - Verwaltung des Zugriffs auf Webservices – Übersicht 1
 - Verwalten der Web Protocol Engine 2
 - Befehle zum Verwalten der Web Protocol Engine 3
 - Konfiguration der SAML-Authentifizierung für Webservices 4
 - Verwalten von Webservices 9
 - SSL verwalten 11
 - Befehle zum Verwalten von SSL 11
 - Konfigurieren Sie den Zugriff auf Webservices 12
 - Fehlerbehebung bei Problemen mit dem Webservice-Zugriff 13

Management des Zugriffs auf Webservices

Verwaltung des Zugriffs auf Webservices – Übersicht

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 Processor Infrastructure (*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 Anforderung für den Zugriff auf die Log-Dateien eines Node oder auf Core Dump-Dateien liefert das *spi* Web Service erstellt automatisch einen Bereitstellungspunkt von einem Node zum Root-Volume eines anderen Nodes, auf dem sich die Dateien befinden. Sie müssen den Bereitstellungspunkt 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 Discovery (*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.

- Aktualisierung des Firmware BaseBoard Management Controller (BMC) (*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 Messaging (`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-Unterstützung (`saml`)

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

- SAML-Service-Provider (`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:

- Backup-Dateien 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 der Web Protocol Engine

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 festlegen, ob Remote-Clients HTTP oder HTTPS für den Zugriff auf Web-Service-Inhalte verwenden können, indem Sie die verwenden `system services web modify` Befehl mit dem `-external` Parameter.
- Sie können angeben, ob SSLv3 für sicheren Webzugriff verwendet werden soll, indem Sie die verwenden `security config modify` Befehl mit dem `-supported-protocol` Parameter. SSLv3 ist standardmäßig deaktiviert. Transport Layer Security 1.0 (TLSv1.0) ist aktiviert und kann bei Bedarf deaktiviert werden.
- 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, indem Sie den einstellen `is-fips-enabled` Parameter an `true` Für das `security config modify` Befehl und dann mit `security config show` Befehl zum Bestätigen des Online-Status.
- **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. 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 der vorherigen Konfiguration bleiben entweder TLSV.1 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 Cluster-weiten Sicherheit mit anzeigen `system security config show` Befehl.

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.

Befehle zum Verwalten der Web Protocol Engine

Sie verwenden das `system services web` Befehle zum Verwalten der Web Protocol Engine. Sie verwenden das `system services firewall policy create` Und

network interface modify Befehle, mit denen Webzugriffsanfragen durch die Firewall gehen können.

Ihr Ziel ist	Befehl
Konfigurieren Sie die Web Protocol Engine auf Cluster-Ebene: <ul style="list-style-type: none"> • 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) 	<pre>system services web modify</pre>
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	<pre>system services web show</pre>
Zeigt die Konfiguration der Web-Protokoll-Engine auf Node-Ebene und die Aktivitäten der Webservice-Handhabung für die Knoten im Cluster an	<pre>system services web node show</pre>
Erstellen Sie eine Firewallrichtlinie oder fügen Sie einem vorhandenen Firewallrichtlinie HTTP- oder HTTPS-Protokollservice hinzu, um Webzugriffsanfragen durch die Firewall zu durchlaufen	<pre>system services firewall policy create</pre> <p>Einstellen des <code>-service</code> Parameter an <code>http</code> Oder <code>https</code> Ermöglicht das Durchgehen von Webzugriffsanfragen durch die Firewall.</p>
Zuordnen einer Firewallrichtlinie zu einer logischen Schnittstelle	<pre>network interface modify</pre> <p>Sie können das verwenden <code>-firewall-policy</code> Parameter zum Ändern der Firewall-Richtlinie einer LIF.</p>

Konfiguration der SAML-Authentifizierung für Webservices

Konfigurieren Sie die SAML-Authentifizierung

Ab ONTAP 9.3 können Sie die SAML-Authentifizierung (Security Assertion Markup Language) für Webservices konfigurieren. Wenn die SAML-Authentifizierung konfiguriert und aktiviert ist, werden Benutzer von einem externen Identitäts-Provider (IdP) anstelle von Verzeichnisdiensteanbietern wie Active Directory und LDAP authentifiziert.

Was Sie benötigen

- Sie müssen das IdP für SAML-Authentifizierung konfiguriert haben.

- Sie müssen über die IdP-URI verfügen.

Über diese Aufgabe

- SAML-Authentifizierung gilt nur für das `http` und `ontapi` Applikationen unterstützt.

Der `http` und `ontapi` Applikationen werden von folgenden Web-Services verwendet: Service Processor Infrastructure, ONTAP APIs oder System Manager.

- SAML-Authentifizierung ist nur für den Zugriff auf die Administrator-SVM anwendbar.

Schritte

1. SAML-Konfiguration für den Zugriff von ONTAP auf die IdP-Metadaten erstellen:

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` ist die FTP- oder HTTP-Adresse des IdP-Hosts, von dem die IdP-Metadaten heruntergeladen werden können.

`ontap_host_name` ist der Hostname oder die IP-Adresse des Host des SAML-Service-Providers, was in diesem Fall das ONTAP-System ist. Standardmäßig wird die IP-Adresse der Cluster-Management-LIF verwendet.

Optional können Sie die Zertifikatsinformationen für den ONTAP-Server angeben. Standardmäßig werden die Zertifikatsinformationen des ONTAP-Webservers verwendet.

```
cluster_12::> security saml-sp create -idp-uri
https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify
-metadata-server false
```

```
Warning: This restarts the web server. Any HTTP/S connections that are
active
```

```
will be disrupted.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.63.56.150/saml-sp/Metadata
```

```
Configure the IdP and Data ONTAP users for the same directory server
domain to ensure that users are the same for different authentication
methods. See the "security login show" command for the Data ONTAP user
configuration.
```

Die URL für den Zugriff auf die ONTAP-Hostmetadaten wird angezeigt.

2. Konfigurieren Sie vom IdP-Host aus das IdP mit den ONTAP-Host-Metadaten.

Weitere Informationen zum Konfigurieren des IdP finden Sie in der IdP-Dokumentation.

3. SAML-Konfiguration aktivieren:

```
security saml-sp modify -is-enabled true
```

Alle bestehenden Benutzer, die auf das zugreifen `http` Oder `ontapi` Die Applikation wird automatisch für die SAML-Authentifizierung konfiguriert.

4. Wenn Sie Benutzer für das erstellen möchten `http` Oder `ontapi` Anwendung, nachdem SAML konfiguriert wurde, geben Sie SAML als Authentifizierungsmethode für die neuen Benutzer an.

a. Erstellen Sie eine Anmeldemethode für neue Benutzer mit SAML-Authentifizierung:

```
security login create -user-or-group-name user_name -application [http | ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1  
-application http -authentication-method saml -vserver cluster_12
```

b. Vergewissern Sie sich, dass der Benutzereintrag erstellt wurde:

```
security login show
```

```
cluster_12::> security login show  
  
Vserver: cluster_12  
  
User/Group Authentication Acct Second  
Authentication  
Name Application Method Role Name Locked Method  
-----  
-----  
admin console password admin no none  
admin http password admin no none  
admin http saml admin - none  
admin ontapi password admin no none  
admin ontapi saml admin - none  
admin service-processor  
password admin no none  
admin ssh password admin no none  
admin1 http password backup no none  
**admin1 http saml backup -  
none**
```

Verwandte Informationen

["ONTAP 9-Befehle"](#)

Deaktivieren Sie die SAML-Authentifizierung

Sie können die SAML-Authentifizierung deaktivieren, wenn Sie die Authentifizierung von Webbenutzern mithilfe eines externen Identitätsanbieters (IdP) beenden möchten. Wenn

die SAML-Authentifizierung deaktiviert ist, werden die konfigurierten Verzeichnisdienstanbieter wie Active Directory und LDAP zur Authentifizierung verwendet.

Was Sie benötigen

Sie müssen über die Konsole angemeldet sein.

Schritte

1. SAML-Authentifizierung deaktivieren:

```
security saml-sp modify -is-enabled false
```

2. Wenn Sie die SAML-Authentifizierung nicht mehr verwenden möchten oder wenn Sie die IdP ändern möchten, löschen Sie die SAML-Konfiguration:

```
security saml-sp delete
```

Fehlerbehebung bei der SAML-Konfiguration

Wenn die Konfiguration der SAML-Authentifizierung (Security Assertion Markup Language) fehlschlägt, können Sie jeden Knoten, auf dem die SAML-Konfiguration fehlgeschlagen ist, manuell reparieren und nach dem Fehler wiederherstellen. Während der Reparatur wird der Webserver neu gestartet und alle aktiven HTTP-Verbindungen oder HTTPS-Verbindungen werden unterbrochen.

Über diese Aufgabe

Bei der Konfiguration der SAML-Authentifizierung wendet ONTAP pro Node die SAML-Konfiguration an. Wenn Sie die SAML-Authentifizierung aktivieren, versucht ONTAP automatisch, jeden Node bei Konfigurationsproblemen zu reparieren. Wenn Probleme mit der SAML-Konfiguration auf einem beliebigen Node auftreten, können Sie die SAML-Authentifizierung deaktivieren und dann die SAML-Authentifizierung erneut aktivieren. Es kann Situationen geben, in denen die SAML-Konfiguration auf einem oder mehreren Nodes nicht angewendet werden kann, selbst wenn Sie die SAML-Authentifizierung reaktivieren. Sie können den Node identifizieren, auf dem die SAML-Konfiguration ausgefallen ist, und diesen Node manuell reparieren.

Schritte

1. Melden Sie sich bei der erweiterten Berechtigungsebene an:

```
set -privilege advanced
```

2. Ermitteln des Knotens, auf dem die SAML-Konfiguration fehlgeschlagen ist:

```
security saml-sp status show -instance
```

```
cluster_12::~*> security saml-sp status show -instance

                Node: node1
                Update Status: config-success
                Database Epoch: 9
                Database Transaction Count: 997
                Error Text:
SAML Service Provider Enabled: false
                ID of SAML Config Job: 179

                Node: node2
                Update Status: config-failed
                Database Epoch: 9
                Database Transaction Count: 997
                Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
                ID of SAML Config Job: 180
2 entries were displayed.
```

3. Reparieren Sie die SAML-Konfiguration auf dem ausgefallenen Node:

security saml-sp repair -node *node_name*

```
cluster_12::~*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
        will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

Der Webserver wird neu gestartet und alle aktiven HTTP-Verbindungen oder HTTPS-Verbindungen werden unterbrochen.

4. Vergewissern Sie sich, dass SAML auf allen Knoten erfolgreich konfiguriert wurde:

security saml-sp status show -instance

```

cluster_12::*> security saml-sp status show -instance

                Node: node1
            Update Status: config-success
        Database Epoch: 9
    Database Transaction Count: 997
            Error Text:
SAML Service Provider Enabled: false
            ID of SAML Config Job: 179

                Node: node2
            Update Status: **config-success**
        Database Epoch: 9
    Database Transaction Count: 997
            Error Text:
SAML Service Provider Enabled: false
            ID of SAML Config Job: 180
2 entries were displayed.

```

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`), Benutzer müssen die haben `ontapi`

Zugriffsmethode. Für alle anderen Web-Dienste müssen die Benutzer über die verfügen `http` Zugriffsmethode.



Sie verwenden das `security login` Befehle zum Verwalten von Zugriffsmethoden und Authentifizierungsmethoden für Benutzer`.

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



Sie verwenden das `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.

Befehle zum Verwalten von Webservices

Sie verwenden das `vserver services web` Befehle zum Managen der Verfügbarkeit von Web-Services für das Cluster oder einer Storage Virtual Machine (SVM) Sie verwenden das `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: <ul style="list-style-type: none">• Aktivieren oder Deaktivieren eines Webservice• Geben Sie an, ob nur HTTPS für den Zugriff auf einen Webdienst verwendet werden kann	<code>vserver services web modify</code>
Anzeigen der Konfiguration und Verfügbarkeit von Webservices für das Cluster oder eine anSVM	<code>vserver services web show</code>
Autorisieren eine Rolle für den Zugriff auf einen Web-Service auf dem Cluster oder einer anSVM	<code>vserver services web access create</code>
Zeigen Sie die Rollen an, die für den Zugriff auf Webservices im Cluster oder auf anSVM autorisiert sind	<code>vserver services web access show</code>
Verhindern Sie, dass eine Rolle auf einen Webservice auf dem Cluster oder einer anSVM zugreift	<code>vserver services web access delete</code>

Verwandte Informationen

["ONTAP 9-Befehle"](#)

Befehle zum Verwalten von Mount-Punkten auf den Nodes

Der `spi` Webservice erstellt bei Anforderung einen Mount-Punkt automatisch von einem Node zum Root-Volume eines anderen Nodes, um auf die Log-Dateien oder Kerndateien des Node zuzugreifen. Obwohl Sie Mount-Punkte nicht manuell verwalten müssen, können Sie dies mit dem `tun system node root-mount` Befehle.

Ihr Ziel ist	Befehl
Erstellen Sie manuell einen Mount-Punkt von einem Node zum Root-Volume eines anderen Nodes	<code>system node root-mount create</code> Nur ein einzelner Mount-Punkt kann von einem Node zum anderen 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	<code>system node root-mount show</code>
Löschen Sie einen Bereitstellungspunkt von einem Node zum Root-Volume eines anderen Node, und erzwingen Sie die Verbindungen zum Mount-Punkt zum Schließen	<code>system node root-mount delete</code>

Verwandte Informationen

["ONTAP 9-Befehle"](#)

SSL verwalten

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 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

Sie verwenden das `security ssl` Befehle zum Managen des SSL-Protokolls für das Cluster ora Storage Virtual Machine (SVM).

Ihr Ziel ist	Befehl
Aktivieren Sie SSL für den Cluster oranSVM und verknüpfen Sie ein digitales Zertifikat mit ihm	<code>security ssl modify</code>
Zeigt den SSL-Konfigurations- und Zertifikatnamen für die Cluster-oranSVM an	<code>security ssl show</code>

Konfigurieren Sie den Zugriff auf Webservices

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:



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

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

Sie stellen die ein `-service` Parameter von `system services firewall policy create` Befehl an `http` Oder `https` Aktivieren der Richtlinie zur Unterstützung des Webzugriffs

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

Sie verwenden das `network interface modify` Befehl mit dem `-firewall-policy` Parameter, um die Firewall-Richtlinie für ein LIF zu nutzen

2. Verwenden Sie zum Konfigurieren der Webprotokoll-Engine auf Cluster-Ebene und für den Zugriff auf Webservice-Inhalte das `system services web modify` Befehl.
3. Wenn Sie Secure Web Services (HTTPS) verwenden möchten, aktivieren Sie SSL und stellen mithilfe von digitale Zertifikatinformationen für den Cluster oder die SVM zur Verfügung `security ssl modify` Befehl.
4. Um einen Webservice 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 Web-Services auf dem Cluster oder der SVM zu autorisieren, verwenden Sie den `vserver services web access create` Befehl.

Die Rolle, die Sie Zugriff gewähren, muss bereits vorhanden sein. Sie können vorhandene Rollen mit dem

anzeigen `security login role show` Führen Sie den Befehl aus, oder erstellen Sie neue Rollen mit `security login role create` Befehl.

6. Stellen Sie für eine Rolle, die für den Zugriff auf einen Webservice autorisiert wurde, sicher, dass die Benutzer auch mit der richtigen Zugriffsmethode konfiguriert sind, indem Sie die Ausgabe des `security login show` Befehl.

Um auf den Webservice der ONTAP API zuzugreifen (`ontapi`) Muss ein Benutzer mit dem konfiguriert werden `ontapi` Zugriffsmethode. Für den Zugriff auf alle anderen Webservices muss ein Benutzer mit dem konfiguriert werden `http` Zugriffsmethode.







Sie verwenden das `security login create` Befehl zum Hinzufügen einer Zugriffsmethode für einen Benutzer.

Fehlerbehebung bei Problemen mit dem Webservice-Zugriff

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 zurück <code>unable to connect</code> Oder <code>failure to establish a connection</code> Fehler beim Zugriff auf einen Webservice.	Ihr LIF ist möglicherweise falsch konfiguriert.	Stellen Sie sicher, dass Sie die LIF anpingen können, die den Webservice bereitstellt.  Sie verwenden das <code>network ping</code> Befehl zum Ping eines LIF. Informationen zur Netzwerkkonfiguration finden Sie im <i>Network Management Guide</i> .

Dieses Zugriffsproblem...	Tritt wegen dieses Konfigurationsfehlers auf...	So beheben Sie den Fehler:
<p>Ihre Firewall ist möglicherweise falsch konfiguriert.</p>	<p>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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> Sie verwenden das <code>system services firewall policy</code> Befehle zum Management von Firewallrichtlinien Sie verwenden das <code>network interface modify</code> Befehl mit dem <code>-firewall -policy</code> Parameter zum Zuordnen einer Richtlinie zu einer LIF.</p> </div>	<p>Ihre Web-Protokoll-Engine ist möglicherweise deaktiviert.</p>
<p>Stellen Sie sicher, dass die Web Protocol Engine aktiviert ist, damit Webservices verfügbar sind.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> Sie verwenden das <code>system services web</code> Befehle zum Verwalten der Web Protocol Engine für den Cluster.</p> </div>	<p>Ihr Webbrowser gibt einen zurück <code>not found</code> Fehler beim Zugriff auf einen Webdienst.</p>	<p>Der Webdienst ist möglicherweise deaktiviert.</p>
<p>Stellen Sie sicher, dass jeder Webdienst, auf den Sie Zugriff zulassen möchten, individuell aktiviert ist.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> Sie verwenden das <code>vserver services web modify</code> Befehl zum Aktivieren eines Webservices für den Zugriff.</p> </div>	<p>Der Webbrowser meldet sich nicht bei einem Webdienst mit dem Kontonamen und Passwort eines Benutzers an.</p>	<p>Der Benutzer kann nicht authentifiziert werden, die Zugriffsmethode ist nicht korrekt oder der Benutzer ist nicht berechtigt, auf den Webdienst zuzugreifen.</p>

Dieses Zugriffsproblem...	Tritt wegen dieses Konfigurationsfehlers auf...	So beheben Sie den Fehler:
<p>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.</p> <div style="border-left: 1px solid black; padding-left: 10px; margin-top: 20px;"> <p>Sie verwenden das <code>security login</code> Befehle zum Verwalten von Benutzerkonten und deren Zugriffsmethoden und Authentifizierungsmethoden. Für den Zugriff auf den Webdienst der ONTAP API ist das erforderlich <code>ontapi</code> Zugriffsmethode. Für den Zugriff auf alle anderen Webservices ist das erforderlich <code>http</code> Zugriffsmethode. Sie verwenden das <code>vserver services web access</code> Befehle zum Verwalten des Zugriffs einer Rolle auf einen Webdienst.</p> </div>	<p>Sie stellen eine Verbindung zu Ihrem Webdienst über HTTPS her, und Ihr Webbrowser zeigt an, dass die Verbindung unterbrochen wird.</p>	<p>Möglicherweise ist SSL nicht auf dem Cluster oder der Storage Virtual Machine (SVM) aktiviert, die den Webservice bereitstellt.</p>



Dieses Zugriffsproblem...	Tritt wegen dieses Konfigurationsfehlers auf...	So beheben Sie den Fehler:
<p>Vergewissern Sie sich, dass für den Cluster oder die SVM SSL aktiviert ist und das digitale Zertifikat gültig ist.</p> <div style="border-left: 1px solid black; padding-left: 10px; margin-left: 20px;"> <p> Sie verwenden das <code>security ssl</code> Befehle zum Verwalten der SSL-Konfiguration für HTTP-Server und der <code>security certificate show</code> Befehl zum Anzeigen von digitalen Zertifikatinformationen.</p> </div>	<p>Sie stellen eine Verbindung zu Ihrem Webdienst über HTTPS her, und Ihr Webbrowser zeigt an, dass die Verbindung nicht vertrauenswürdig ist.</p>	<p>Möglicherweise verwenden Sie ein selbstsigniertes digitales Zertifikat.</p>

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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 IRGEND EINER 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.