Verwalten von Webservices

ONTAP 9

NetApp
September 12, 2024

Inhalt

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 der Zugriffsmethoden und Authentifizierungsmethoden von Benutzern.

- 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.

Management des Zugriffs auf Webservices

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 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 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: • 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` Einstellen des `-service` Parameter an `http` Oder `https` Ermöglicht das Durchgehen von Webzugriffsanfragen durch die Firewall.
Zuordnen einer Firewallrichtlinie zu einer logischen Schnittstelle	`network interface modify` Sie können das verwenden `-firewall-policy` Parameter zum Ändern der Firewall-Richtlinie einer LIF.

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 Webdienst autorisiert wurde, sicher, dass die Benutzer auch mit der richtigen Zugriffsmethode konfiguriert sind, indem Sie die Ausgabe des überprüfen `security login show` Befehl.

   Um auf den Webdienst 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.

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: • 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

"Befehlsreferenz für ONTAP"

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	`system node root-mount create` 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	`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

"Befehlsreferenz für ONTAP"

SSL verwalten

Verwenden Sie die `security ssl` Befehle zum Verwalten des SSL-Protokolls für das Cluster oder eine SVM (Storage Virtual Machine). 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

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

Ihr Ziel ist	Befehl
Aktivieren Sie SSL für den Cluster oder eine SVM, und verknüpfen Sie ein digitales Zertifikat mit diesem	`security ssl modify`
Zeigt die SSL-Konfiguration und den Zertifikatnamen für das Cluster oder eine SVM an	`security ssl show`

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 `unable to connect` Oder `failure to establish a connection` Fehler beim Zugriff auf einen Webdienst.	Ihr LIF ist möglicherweise falsch konfiguriert.	Stellen Sie sicher, dass Sie die LIF anpingen können, die den Webservice bereitstellt. Sie verwenden das `network ping` Befehl zum Ping eines LIF. Informationen zur Netzwerkkonfiguration finden Sie im *Network Management Guide*.
Ihre Firewall ist möglicherweise falsch konfiguriert.	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. Sie verwenden das `system services firewall policy` Befehle zum Management von Firewallrichtlinien Sie verwenden das `network interface modify` Befehl mit dem `-firewall -policy` Parameter zum Zuordnen einer Richtlinie zu einer LIF.	Ihre Web-Protokoll-Engine ist möglicherweise deaktiviert.
Stellen Sie sicher, dass die Web Protocol Engine aktiviert ist, damit Webservices verfügbar sind. Sie verwenden das `system services web` Befehle zum Verwalten der Web Protocol Engine für den Cluster.	Ihr Webbrowser gibt einen zurück `not found` Fehler beim Zugriff auf einen Webdienst.	Der Webdienst ist möglicherweise deaktiviert.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Stellen Sie sicher, dass jeder Webdienst, auf den Sie Zugriff zulassen möchten, individuell aktiviert ist. Sie verwenden das `vserver services web modify` Befehl zum Aktivieren eines Webservices für den Zugriff.	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 das `security login` Befehle zum Verwalten von Benutzerkonten und deren Zugriffsmethoden und Authentifizierungsmethoden. Für den Zugriff auf den Webdienst der ONTAP API ist das erforderlich `ontapi` Zugriffsmethode. Für den Zugriff auf alle anderen Webservices ist das erforderlich `http` Zugriffsmethode. Sie verwenden das `vserver services web access` Befehle zum Verwalten des Zugriffs einer Rolle auf einen Webdienst.	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 das `security ssl` Befehle zum Verwalten der SSL-Konfiguration für HTTP-Server und der `security certificate show` Befehl zum Anzeigen von digitalen Zertifikatinformationen.	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.