Authentifizierung und Zugriffssteuerung

ONTAP 9

NetApp
April 24, 2024

Inhalt

Authentifizierung und Zugriffssteuerung

Übersicht über Authentifizierung und Zugriffssteuerung

Sie können die ONTAP-Cluster-Authentifizierung und die Zugriffssteuerung für ONTAP Web Services verwalten.

Mit System Manager oder der CLI können Sie den Client- und Administratorzugriff auf das Cluster und den Storage steuern und sichern.

Wenn Sie den klassischen System-Manager verwenden (nur in ONTAP 9.7 und früher verfügbar), lesen Sie "System Manager Classic (ONTAP 9.0 bis 9.7)"

Client-Authentifizierung und -Autorisierung

ONTAP authentifiziert einen Client-Computer und einen Benutzer, indem die Identität mit einer vertrauenswürdigen Quelle überprüft wird. ONTAP autorisiert einen Benutzer für den Zugriff auf eine Datei oder ein Verzeichnis, indem die Anmeldeinformationen des Benutzers mit den für die Datei oder das Verzeichnis konfigurierten Berechtigungen verglichen werden.

Administratorauthentifizierung und RBAC

Administratoren authentifizieren sich mithilfe von lokalen oder Remote-Anmeldungskonten beim Cluster und bei der Storage-VM. Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) legt die Befehle fest, auf die ein Administrator zugreifen kann.

Managen Sie die Administratorauthentifizierung und RBAC

Administratorauthentifizierung und RBAC – Übersicht mit der CLI

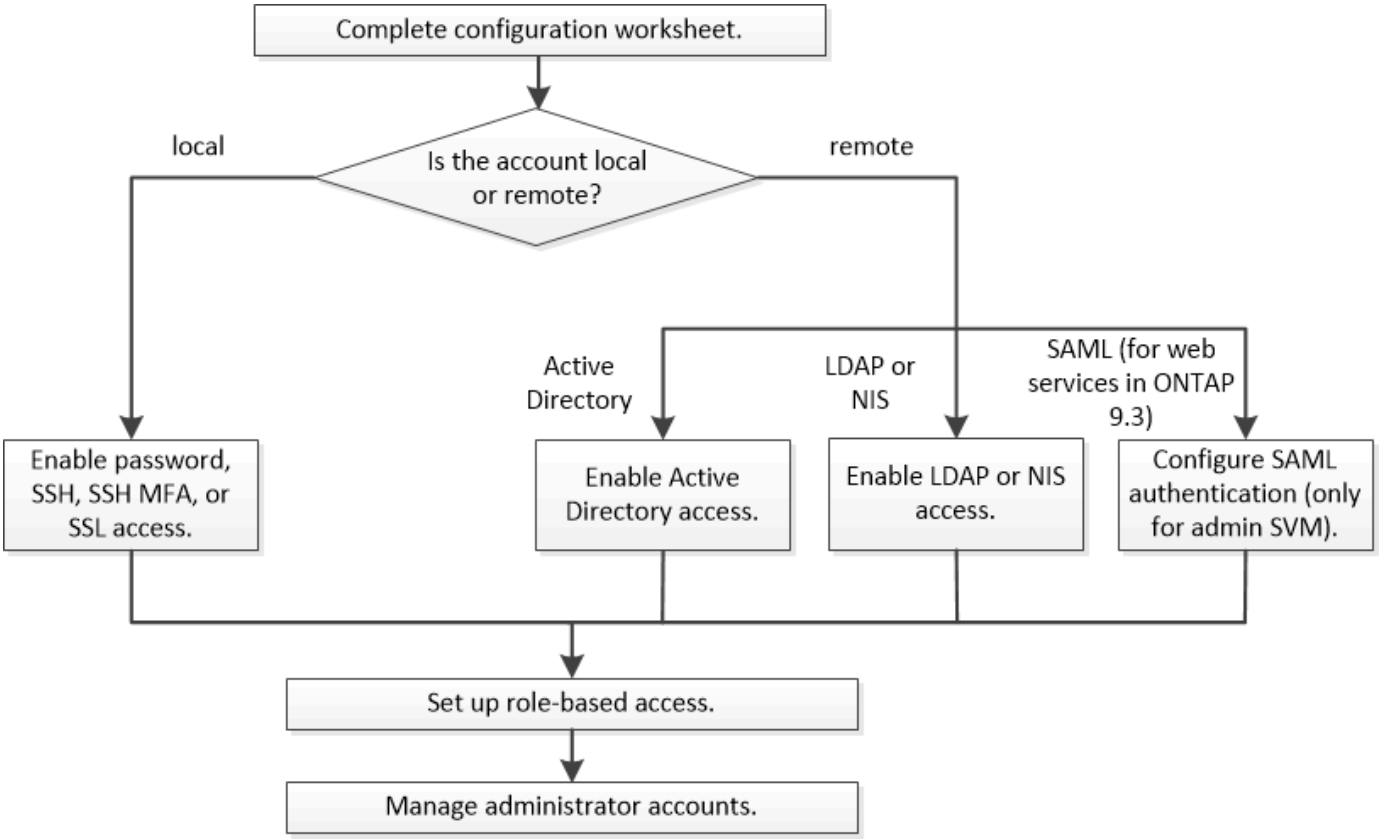
Sie können Anmeldekonten für ONTAP Cluster-Administratoren und SVM-Administratoren (Storage Virtual Machine) aktivieren. Zudem können Sie mithilfe der rollenbasierten Zugriffssteuerung (RBAC) die Funktionen von Administratoren definieren.

Sie bieten folgende Möglichkeiten für die Anmeldung bei Konten und RBAC:

- Sie möchten die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, nicht System Manager oder ein automatisiertes Scripting Tool.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie verwenden kein SNMP, um Informationen über das Cluster zu sammeln.

Administratorauthentifizierung und RBAC-Workflow

Sie können die Authentifizierung für lokale Administratorkonten oder Remote-Administratorkonten aktivieren. Die Kontoinformationen für ein lokales Konto befinden sich im Storage-System, und die Kontoinformationen für ein Remote-Konto befinden sich an anderer Stelle. Jedes Konto kann über eine vordefinierte Rolle oder eine benutzerdefinierte Rolle verfügen.



Sie können lokale Administratorkonten für den Zugriff auf eine Admin Storage Virtual Machine (SVM) oder auf eine Daten-SVM mit den folgenden Authentifizierungstypen aktivieren:

- Passwort
- Öffentlicher SSH-Schlüssel
- SSL-Zertifikat
- SSH-Multi-Faktor-Authentifizierung (MFA)

  Ab ONTAP 9.3 wird die Authentifizierung mit Passwort und öffentlichem Schlüssel unterstützt.

Sie können Remote-Administratorkonten für den Zugriff auf eine Admin-SVM oder eine Daten-SVM mit den folgenden Authentifizierungsarten aktivieren:

- Active Directory
- SAML-Authentifizierung (nur für Admin-SVM)

  Ab ONTAP 9.3 kann die SAML-Authentifizierung (Security Assertion Markup Language) über einen der folgenden Web-Services – Service-Prozessor-Infrastruktur, ONTAP-APIs oder System Manager – für den Zugriff auf die Admin-SVM verwendet werden.

- Ab ONTAP 9.4 kann SSH MFA für Remote-Benutzer auf LDAP- oder NIS-Servern verwendet werden. Die Authentifizierung mit nswitch und öffentlichem Schlüssel wird unterstützt.

Arbeitsblätter für die Administratorauthentifizierung und die RBAC-Konfiguration

Bevor Sie Login-Konten erstellen und die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) einrichten, sollten Sie Informationen für alle Elemente in den

Konfigurationsarbeitsblättern sammeln.

Erstellen oder Ändern von Anmeldekonten

Sie stellen diese Werte dem zur Verfügung `security login create` Befehl, wenn Sie Anmeldekonten für den Zugriff auf eine Storage-VM aktivieren. Sie stellen dieselben Werte mit bereit `security login modify` Befehl, wenn Sie ändern, wie ein Konto auf eine Storage-VM zugreift.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM, auf die das Konto zugreift. Der Standardwert ist der Name der Admin-Storage-VM für das Cluster.	
`-user-or-group-name`	Der Benutzername oder der Gruppenname des Kontos. Wenn Sie einen Gruppennamen angeben, können Sie auf jeden Benutzer in der Gruppe zugreifen. Sie können einem Benutzernamen oder Gruppennamen mehrere Anwendungen zuordnen.	
`-application`	Die Applikation, die für den Zugriff auf die Storage-VM verwendet wird: • `http` • `ontapi` • `snmp` • `ssh`	

`-authmethod`	Die Methode, die zur Authentifizierung des Kontos verwendet wird: • `cert` Für die SSL-Zertifikatauthentifizierung • `domain` Für die Active Directory-Authentifizierung • `nsswitch` Für LDAP- oder NIS-Authentifizierung • `password` Für die Authentifizierung von Benutzerpasswörtern • `publickey` Für die Authentifizierung eines öffentlichen Schlüssels • `community` Für SNMP-Community-Strings • `usm` Für SNMP-Sicherheitsmodell • `saml` Für die SAML-Authentifizierung (Security Assertion Markup Language)	
`-remote-switch-ipaddress`	Die IP-Adresse des Remote-Switch. Bei dem Remote-Switch kann es sich um einen Cluster-Switch-Switch-Health-Monitor (CSHM) oder einen Fibre Channel (FC)-Switch handelt, der von der MetroCluster-Systemzustandsüberwachung (MCC-HM) überwacht wird. Diese Option ist nur anwendbar, wenn die Anwendung ist `snmp` Und die Authentifizierungsmethode lautet `usm`.	
`-role`	Die Zugriffskontrollrolle, die dem Konto zugewiesen ist: • Für das Cluster (die Admin-Storage-VM) ist der Standardwert `admin`. • Für eine Storage-VM ist der Standardwert `vsadmin`.	

`-comment`	(Optional) Beschreibungstext des Kontos. Sie sollten den Text in doppelte Anführungszeichen (") einschließen.	
`-is-ns-switch-group`	Gibt an, ob es sich bei dem Konto um ein LDAP-Gruppenkonto oder ein NIS-Gruppenkonto handelt (`yes` Oder `no`).	
`-second-authentication -method`	Zweite Authentifizierungsmethode bei Multi-Faktor-Authentifizierung: • `none` Bei Nichtnutzen der Multi-Faktor-Authentifizierung ist der Standardwert • `publickey` Für die Authentifizierung eines öffentlichen Schlüssels, wenn der aktiviert ist `authmethod` Ist Passwort oder nsswitch • `password` Für die Authentifizierung von Benutzerpasswörtern, wenn der verwendet wird `authmethod` Ist ein öffentlicher Schlüssel • `nsswitch` Für die Authentifizierung von Benutzerpasswörtern, wenn die authmethod Publikkey ist Die Reihenfolge der Authentifizierung ist immer der öffentliche Schlüssel gefolgt vom Passwort.	
`-is-ldap-fastbind`	Beginnend mit ONTAP 9.11.1, wenn auf true gesetzt, aktiviert LDAP fast bind für nswitch Authentifizierung; der Standardwert ist false. Um LDAP fast Bind zu verwenden, wird der verwendet `-authentication-method` Wert muss auf gesetzt werden `nsswitch`. "Erfahren Sie mehr über LDAP fastbind für nswitch Authentifizierung."	

Konfigurieren Sie die Sicherheitsinformationen von Cisco Duo

Sie stellen diese Werte dem zur Verfügung `security login duo create` Befehl, wenn Sie die zwei-Faktor-Authentifizierung des Cisco Duo mit SSH-Anmeldungen für eine Storage-VM aktivieren.

Feld	Beschreibung	Ihr Wert
`-vserver`	Die Speicher-VM (in der ONTAP-CLI als vServer bezeichnet), auf die die Duo-Authentifizierungseinstellungen zutreffen.	
`-integration-key`	Ihr Integrationsschlüssel, den Sie erhalten, wenn Sie Ihre SSH-Anwendung bei Duo registrieren.	
`-secret-key`	Ihr Geheimschlüssel, den Sie erhalten, wenn Sie Ihre SSH-Anwendung bei Duo registrieren.	
`-api-host`	Der API-Hostname, der beim Registrieren Ihrer SSH-Anwendung bei Duo ermittelt wird. Beispiel: `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	Bei Service- oder Konfigurationsfehlern, die die Duo-Authentifizierung verhindern, schlägt fehl `safe` (Zugriff zulassen) oder `secure` (Zugriff verweigern). Die Standardeinstellung lautet `safe`, Was bedeutet, dass die Duo-Authentifizierung umgangen wird, wenn sie aufgrund von Fehlern wie dem Duo-API-Server nicht zugänglich ist.	

`-http-proxy`	Verwenden Sie den angegebenen HTTP-Proxy. Wenn der HTTP-Proxy eine Authentifizierung erfordert, geben Sie die Anmeldeinformationen in die Proxy-URL ein. Beispiel: `http-proxy=http://username:password@proxy.example.org:8080`	
`-autopush`	Entweder `true` Oder `false`. Standard ist `false`. Wenn `true`, Duo sendet automatisch eine Push-Login-Anfrage an das Telefon des Benutzers, um zu einem Anruf zurückkehren, wenn Push nicht verfügbar ist. Beachten Sie, dass dadurch die Kenncode-Authentifizierung effektiv deaktiviert wird. Wenn `false`, Der Benutzer wird aufgefordert, eine Authentifizierungsmethode auszuwählen. Bei Konfiguration mit `autopush = true`Wir empfehlen die Einstellung `max-prompts = 1`.	

`-max-prompts`	Wenn sich ein Benutzer nicht mit einem zweiten Faktor authentifizieren kann, fordert Duo den Benutzer auf, sich erneut zu authentifizieren. Mit dieser Option wird die maximale Anzahl von Eingabeaufforderungen festgelegt, die Duo vor dem verweigern des Zugriffs anzeigt. Muss sein `1`, `2`, Oder `3`. Der Standardwert ist `1`. Beispiel: Wann `max-prompts = 1`, Der Benutzer muss sich bei der ersten Eingabeaufforderung erfolgreich authentifizieren, während wenn `max-prompts = 2`Wenn der Benutzer bei der ersten Aufforderung falsche Informationen eingibt, wird er aufgefordert, sich erneut zu authentifizieren. Bei Konfiguration mit `autopush = true`Wir empfehlen die Einstellung `max-prompts = 1`. Für die beste Erfahrung wird ein Benutzer mit nur publickey Authentifizierung immer haben `max-prompts` Auf einstellen `1`.	
`-enabled`	Zwei-Faktor-Authentifizierung für Duo aktivieren. Auf einstellen `true` Standardmäßig. Wenn diese Option aktiviert ist, wird die Duo-zwei-Faktor-Authentifizierung während der SSH-Anmeldung gemäß den konfigurierten Parametern erzwungen. Wenn Duo deaktiviert ist (auf eingestellt `false`), Duo-Authentifizierung wird ignoriert.	

Definieren benutzerdefinierter Rollen

Sie stellen diese Werte dem zur Verfügung `security login role create` Befehl, wenn Sie eine benutzerdefinierte Rolle definieren.

Feld	Beschreibung	Ihr Wert

`-vserver`	(Optional) der Name der Storage-VM (in der ONTAP-CLI als vServer bezeichnet), die mit der Rolle verknüpft ist.	
`-role`	Der Name der Rolle.	
`-cmddirname`	Der Befehl oder das Befehlsverzeichnis, auf das die Rolle Zugriff erhält. Sie sollten Unterverzeichnisnamen in doppelte Anführungszeichen (") einschließen. Beispiel: `"volume snapshot"`. Eingabe ist erforderlich `DEFAULT` So geben Sie alle Befehlsverzeichnisse an.	
`-access`	(Optional) der Zugriffsebene für die Rolle. Für Befehlsverzeichnisse: • `none` (Der Standardwert für benutzerdefinierte Rollen) verweigert den Zugriff auf Befehle im Befehlsverzeichnis • `readonly` Gewährt Zugang zum `show` Befehle im Befehlsverzeichnis und seinen Unterverzeichnissen • `all` Gewährt Zugriff auf alle Befehle im Befehlsverzeichnis und seinen Unterverzeichnissen Für *nonintrinsische Befehle* (Befehle, die nicht enden `create`, `modify`, `delete`, Oder `show`): • `none` (Der Standardwert für benutzerdefinierte Rollen) verweigert den Zugriff auf den Befehl • `readonly` Ist nicht zutreffend • `all` Gewährt Zugriff auf den Befehl Um den Zugriff auf intrinsische Befehle zu gewähren oder zu verweigern, müssen Sie das Befehlsverzeichnis angeben.	

`-query`	(Optional) das Abfrageobjekt, das zum Filtern der Zugriffsebene verwendet wird, die in Form einer gültigen Option für den Befehl oder für einen Befehl im Befehlsverzeichnis angegeben ist. Sie sollten das Abfrageobjekt in doppelte Anführungszeichen (") einschließen. Beispiel: Wenn das Befehlsverzeichnis lautet `volume`, Das Abfrageobjekt `"-aggr aggr0"` Würde den Zugriff für den aktivieren `aggr0` Nur Aggregat.	

Einem Benutzerkonto einen öffentlichen Schlüssel zuordnen

Sie stellen diese Werte dem zur Verfügung `security login publickey create` Befehl, wenn Sie einen öffentlichen SSH-Schlüssel einem Benutzerkonto zuordnen.

Feld	Beschreibung	Ihr Wert
`-vserver`	(Optional) der Name der Speicher-VM, auf die das Konto zugreift.	
`-username`	Der Benutzername des Kontos. Der Standardwert, `admin`, Dies ist der Standardname des Cluster-Administrators.	
`-index`	Die Indexnummer des öffentlichen Schlüssels. Der Standardwert ist 0, wenn der Schlüssel der erste Schlüssel ist, der für das Konto erstellt wird. Andernfalls ist der Standardwert eine mehr als die höchste vorhandene Indexnummer für das Konto.	
`-publickey`	Der öffentliche OpenSSH-Schlüssel. Sie sollten den Schlüssel in doppelte Anführungszeichen (“) setzen.	
`-role`	Die Zugriffskontrollrolle, die dem Konto zugewiesen ist.	

`-comment`	(Optional) Beschreibungstext für den öffentlichen Schlüssel. Sie sollten den Text in doppelte Anführungszeichen (") einschließen.	
`-x509-certificate`	(Optional) ab ONTAP 9.13.1 können Sie die Zuordnung des X.509-Zertifikats zum öffentlichen SSH-Schlüssel verwalten. Wenn Sie ein X.509-Zertifikat mit dem öffentlichen SSH-Schlüssel verknüpfen, überprüft ONTAP bei der SSH-Anmeldung, ob dieses Zertifikat gültig ist. Wenn sie abgelaufen ist oder widerrufen wurde, ist die Anmeldung nicht zulässig und der zugehörige öffentliche SSH-Schlüssel ist deaktiviert. Mögliche Werte: • `install`: Installieren Sie das angegebene PEM-kodierte X.509-Zertifikat und verknüpfen Sie es mit dem öffentlichen SSH-Schlüssel. Fügen Sie den vollständigen Text für das Zertifikat ein, das Sie installieren möchten. • `modify`: Aktualisieren Sie das vorhandene PEM-kodierte X.509-Zertifikat mit dem angegebenen Zertifikat und verknüpfen Sie es mit dem öffentlichen SSH-Schlüssel. Fügen Sie den vollständigen Text für das neue Zertifikat ein. • `delete`: Entfernen Sie die vorhandene X.509-Zertifikatzuordnung mit dem öffentlichen SSH-Schlüssel.	

Installieren Sie ein digitales Zertifikat für einen CA-signierten Server

Sie stellen diese Werte dem zur Verfügung `security certificate generate-csr` Befehl, wenn Sie eine digitale Zertifikatsignierungsanforderung (CSR) für die Authentifizierung einer Speicher-VM als SSL-Server generieren.

Feld	Beschreibung	Ihr Wert

`-common-name`	Der Name des Zertifikats, bei dem es sich um einen vollständig qualifizierten Domänennamen (FQDN) oder einen benutzerdefinierten gemeinsamen Namen handelt.	
`-size`	Die Anzahl der Bits im privaten Schlüssel. Je höher der Wert, desto sicherer ist der Schlüssel. Der Standardwert ist `2048`. Mögliche Werte sind `512`, `1024`, `1536`, und `2048`.	
`-country`	Das Land der Storage VM in einem zweistelligen Code. Der Standardwert ist `US`. Eine Liste der Codes finden Sie auf den man-Pages.	
`-state`	Der Status oder die Provinz der Storage-VM	
`-locality`	Die Lokalität der Storage-VM.	
`-organization`	Die Organisation der Storage-VM.	
`-unit`	Die Einheit in der Organisation der Storage-VM.	
`-email-addr`	Die E-Mail-Adresse des Kontaktadministrators für die Storage-VM.	
`-hash-function`	Die kryptografische Hashing-Funktion zum Signieren des Zertifikats. Der Standardwert ist `SHA256`. Mögliche Werte sind `SHA1`, `SHA256`, und `MD5`.	

Sie stellen diese Werte dem zur Verfügung `security certificate install` Befehl, wenn Sie ein CA-signiertes digitales Zertifikat zur Verwendung bei der Authentifizierung des Clusters oder der Speicher-VM als SSL-Server installieren. In der folgenden Tabelle sind nur die Optionen aufgeführt, die für die Kontenkonfiguration relevant sind.

Feld	Beschreibung	Ihr Wert

`-vserver`	Der Name der Storage-VM, auf der das Zertifikat installiert werden soll.	
`-type`	Der Zertifikatstyp: • `server` Für Serverzertifikate und Zwischenzertifikate • `client-ca` Für das öffentliche Schlüsselzertifikat der Root-CA des SSL-Clients • `server-ca` Für das öffentliche Schlüsselzertifikat der Root-CA des SSL-Servers, von dem ONTAP ein Client ist • `client` Für ein selbstsigniertes oder CA-signiertes digitales Zertifikat und einen privaten Schlüssel für ONTAP als SSL-Client	

Konfigurieren Sie den Active Directory-Domänencontroller-Zugriff

Sie stellen diese Werte dem zur Verfügung `security login domain-tunnel create` Befehl, wenn Sie bereits einen SMB-Server für eine Datenspeicher-VM konfiguriert haben und die Storage-VM als Gateway oder *Tunnel* für den Active Directory Domain Controller-Zugriff auf das Cluster konfigurieren möchten.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Speicher-VM, für die der SMB-Server konfiguriert wurde.	

Sie stellen diese Werte dem zur Verfügung `vserver active-directory create` Befehl, wenn Sie keinen SMB-Server konfiguriert haben und ein Storage-VM-Computerkonto in der Active Directory-Domäne erstellen möchten.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM, für die Sie ein Active Directory-Computerkonto erstellen möchten.	
`-account-name`	Der NetBIOS-Name des Computerkontos.	
`-domain`	Der vollständig qualifizierte Domänenname (FQDN).	

`-ou`	Die Organisationseinheit in der Domäne. Der Standardwert ist `CN=Computers`. ONTAP fügt diesen Wert an den Domänennamen an, um den Distinguished Name von Active Directory zu erzeugen.	

Konfigurieren Sie den LDAP- oder NIS-Serverzugriff

Sie stellen diese Werte dem zur Verfügung `vserver services name-service ldap client create` Befehl, wenn Sie eine LDAP-Client-Konfiguration für die Storage-VM erstellen.

In der folgenden Tabelle sind nur die Optionen aufgeführt, die für die Account-Konfiguration relevant sind:

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM für die Client-Konfiguration.	
`-client-config`	Der Name der Client-Konfiguration.	
`-ldap-servers`	Eine kommagetrennte Liste von IP-Adressen und Hostnamen für die LDAP-Server, mit denen der Client verbunden ist.	
`-schema`	Das Schema, das der Client zum Erstellen von LDAP-Abfragen verwendet.	
`-use-start-tls`	Gibt an, ob der Client die Kommunikation mit dem LDAP-Server über Start TLS verschlüsselt (`true` Oder `false`). Start TLS wird nur für den Zugriff auf Datenspeicher-VMs unterstützt. Es wird für den Zugriff auf Admin-Storage-VMs nicht unterstützt.	

Sie stellen diese Werte dem zur Verfügung `vserver services name-service ldap create` Befehl, wenn Sie eine LDAP-Client-Konfiguration mit der Storage-VM verknüpfen.

Feld	Beschreibung	Ihr Wert

`-vserver`	Der Name der Storage-VM, mit der die Client-Konfiguration verknüpft werden soll.	
`-client-config`	Der Name der Client-Konfiguration.	
`-client-enabled`	Gibt an, ob die Storage-VM die LDAP-Client-Konfiguration verwenden kann (`true` Oder `false`).	

Sie stellen diese Werte dem zur Verfügung `vserver services name-service nis-domain create` Befehl, wenn Sie eine NIS-Domänenkonfiguration auf einer Storage-VM erstellen.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM, auf der die Domänenkonfiguration erstellt werden soll.	
`-domain`	Der Name der Domäne.	
`-active`	Gibt an, ob die Domäne aktiv ist (`true` Oder `false`).	
`-servers`	**ONTAP 9.0, 9.1**: Eine kommagetrennte Liste von IP-Adressen für die NIS-Server, die von der Domänenkonfiguration verwendet werden.	
`-nis-servers`	Eine durch Kommas getrennte Liste von IP-Adressen und Hostnamen für die NIS-Server, die von der Domänenkonfiguration verwendet werden.	

Sie stellen diese Werte dem zur Verfügung `vserver services name-service ns-switch create` Befehl, wenn Sie den Aufstellungsauftrag für Namensdienstquellen angeben.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage VM, auf der die Look-Up-Reihenfolge des Namensservice konfiguriert werden soll.	

`-database`	Die Namensdienstdatenbank: • `hosts` Für Dateien und DNS-Namensdienste • `group` Für Dateien, LDAP und NIS-Name-Services • `passwd` Für Dateien, LDAP und NIS-Name-Services • `netgroup` Für Dateien, LDAP und NIS-Name-Services • `namemap` Für Dateien und LDAP-Namensdienste	
`-sources`	Die Reihenfolge, in der Sie Namensdienstquellen suchen (in einer kommagetrennten Liste): • `files` • `dns` • `ldap` • `nis`	

Konfigurieren Sie den SAML-Zugriff

Ab ONTAP 9.3 liefern Sie diese Werte mit dem `security saml-sp create` Befehl zum Konfigurieren der SAML-Authentifizierung.

Feld	Beschreibung	Ihr Wert
`-idp-uri`	Die FTP-Adresse oder HTTP-Adresse des IdP-Hosts (Identity Provider), von dem aus die IdP-Metadaten heruntergeladen werden können.	
`-sp-host`	Der Hostname oder die IP-Adresse des Host des SAML-Service-Providers (ONTAP-System). Standardmäßig wird die IP-Adresse der Cluster-Management-LIF verwendet.	

`-cert-ca` Und `-cert-serial`, Oder `-cert-common-name`	Die Serverzertifikatdetails des Host des Service-Providers (ONTAP-System). Sie können entweder die Zertifizierungsstelle des Dienstanbieters und die Seriennummer des Zertifikats oder den allgemeinen Serverzertifikats eingeben.	
`-verify-metadata-server`	Gibt an, ob die Identität des IdP-Metadatenservers validiert werden muss `true` Oder `false`). Die Best Practice besteht darin, diesen Wert immer auf festzulegen `true`.	

Erstellen von Anmeldekonten

Erstellen Sie die Übersicht über Login-Konten

Sie können lokale oder Remote-Cluster und SVM-Administratorkonten aktivieren. Bei einem lokalen Konto handelt es sich um ein Konto, in dem die Kontoinformationen, der öffentliche Schlüssel oder das Sicherheitszertifikat im Speichersystem gespeichert sind. INFORMATIONEN zu ANZEIGENKONTOKONTEN werden auf einem Domänencontroller gespeichert. LDAP- und NIS-Konten befinden sich auf LDAP- und NIS-Servern.

Cluster- und SVM-Administratoren

Ein_Cluster-Administrator_ greift auf die Admin-SVM für das Cluster zu. Der Administrator-SVM und ein Cluster-Administrator mit dem reservierten Namen `admin` Werden automatisch erstellt, wenn das Cluster eingerichtet ist.

Ein Clusteradministrator mit dem Standardwert `admin` Rolle kann den gesamten Cluster und seine Ressourcen verwalten. Der Cluster-Administrator kann bei Bedarf weitere Cluster-Administratoren mit unterschiedlichen Rollen erstellen.

Ein *SVM-Administrator* greift auf eine Daten-SVM zu. Je nach Bedarf erstellt der Cluster-Administrator Daten-SVMs und SVM-Administratoren.

Den werden SVM-Administratoren zugewiesen `vsadmin` Rolle standardmäßig. Der Cluster-Administrator kann je nach Bedarf SVM-Administratoren verschiedene Rollen zuweisen.

Namenskonventionen

Die folgenden allgemeinen Namen können nicht für Remote-Cluster- und SVM-Administratorkonten verwendet werden:

- „adm“
- „Bin“
- „cli“

- „Daemon“
- „ftp“
- „Spiele“
- „Anhalten“
- „lp“
- „E-Mail“
- „Mann“
- „Naroot“
- NetApp
- „news“
- „Niemand“
- „Operator“
- „Root“
- „Herunterfahren“
- „Sshd“
- „Synchronisieren“
- „Sys“
- „uucp“
- „Www“

Zusammengeführte Rollen

Wenn Sie mehrere Remote-Konten für denselben Benutzer aktivieren, wird dem Benutzer die Zuordnung aller für die Konten angegebenen Rollen zugewiesen. Das heißt, wenn einem LDAP- oder NIS-Konto das zugewiesen ist `vsadmin` Rolle und das AD-Gruppenkonto für denselben Benutzer wird der zugewiesen `vsadmin-volume` Rolle, der AD-Benutzer meldet sich mit dem Inklusiveren an `vsadmin` Sorgen. Die Rollen sollen *fusioniert werden*.

Aktivieren Sie den Zugriff auf lokales Konto

Lokalen Kontozugriff aktivieren – Übersicht

Bei einem lokalen Konto handelt es sich um ein Konto, in dem die Kontoinformationen, der öffentliche Schlüssel oder das Sicherheitszertifikat im Speichersystem gespeichert sind. Sie können das verwenden `security login create` Befehl zum Aktivieren von lokalen Konten für den Zugriff auf einen Administrator oder eine Daten-SVM

Aktivieren Sie den Zugriff auf das Passwort-Konto

Sie können das verwenden `security login create` Befehl zum Aktivieren von Administratorkonten für den Zugriff auf einen Administrator oder Daten-SVM mit einem Passwort Nachdem Sie den Befehl eingegeben haben, werden Sie zur Eingabe des Passworts aufgefordert.

Über diese Aufgabe

Wenn Sie sich nicht sicher sind, welche Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Ermöglichen Sie lokalen Administratorkonten den Zugriff auf eine SVM über ein Passwort:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Mit dem folgenden Befehl wird das Cluster-Administratorkonto aktiviert `admin1` Mit dem vordefinierten `backup` Rolle für den Zugriff auf die Administrator-SVM`engCluster` Mit einem Passwort. Nachdem Sie den Befehl eingegeben haben, werden Sie zur Eingabe des Passworts aufgefordert.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

Aktivieren Sie SSH-Konten für öffentliche Schlüssel

Sie können das verwenden `security login create` Befehl zum Aktivieren von Administratorkonten für den Zugriff auf eine Admin- oder Daten-SVM mit einem öffentlichen SSH-Schlüssel

Über diese Aufgabe

- Sie müssen den öffentlichen Schlüssel dem Konto zuordnen, bevor das Konto auf die SVM zugreifen kann.

  Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Wenn Sie sich nicht sicher sind, welche Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

Wenn Sie den FIPS-Modus auf dem Cluster aktivieren möchten, müssen vorhandene öffentliche SSH-Schlüsselkonten ohne die unterstützten Schlüsselalgorithmen mit einem unterstützten Schlüsseltyp neu konfiguriert werden. Die Konten sollten neu konfiguriert werden, bevor Sie FIPS aktivieren, sonst schlägt die Administratorauthentifizierung fehl.

Die folgende Tabelle gibt Algorithmen des Host-Schlüsseltyps an, die für ONTAP-SSH-Verbindungen unterstützt werden. Diese Schlüsseltypen gelten nicht für die Konfiguration der öffentlichen SSH-Authentifizierung.

Version von ONTAP	Im FIPS-Modus unterstützte Schlüsseltypen	Im nicht-FIPS-Modus unterstützte Schlüsseltypen
9.11.1 und höher	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 und früher	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa

Die Unterstützung für den Host Key Algorithmus ssh-ed25519 wird ab ONTAP 9.11.1 entfernt.

Weitere Informationen finden Sie unter "Konfiguration der Netzwerksicherheit mit FIPS".

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Lokale Administratorkonten können mithilfe eines öffentlichen SSH-Schlüssels auf eine SVM zugreifen:

   security login create -vserver *SVM_name* -user-or-group-name user_or_group_name -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Mit dem folgenden Befehl wird das SVM-Administratorkonto aktiviert `svmadmin1` Mit dem vordefinierten `vsadmin-volume` Rolle für den Zugriff auf die SVM`engData1` Verwenden eines öffentlichen SSH-Schlüssels:

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

Nachdem Sie fertig sind

Falls Sie dem Administratorkonto keinen öffentlichen Schlüssel zugeordnet haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto

Aktivieren Sie Multi-Faktor-Authentifizierungskonten (MFA)

Übersicht über Multi-Faktor-Authentifizierung

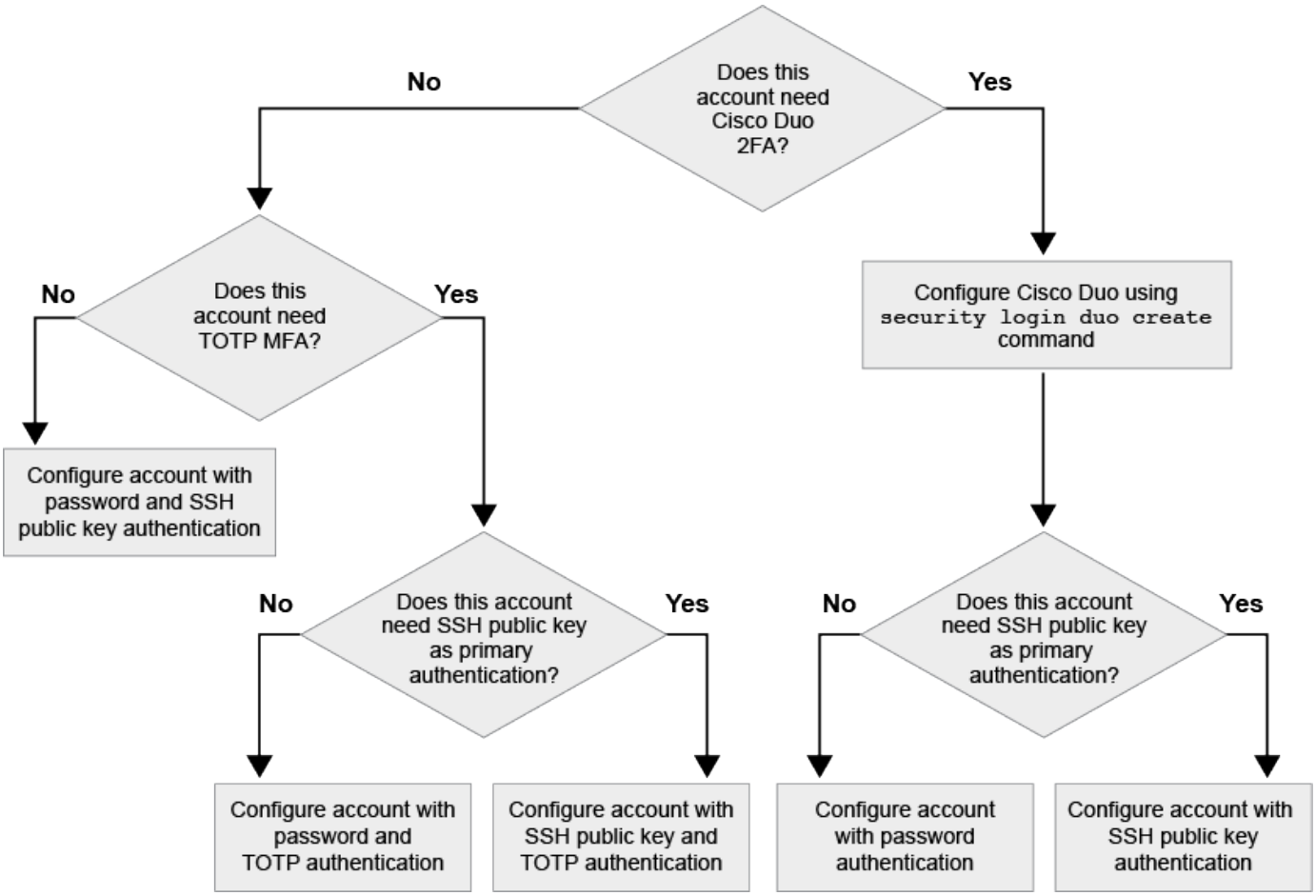
Dank der Multi-Faktor-Authentifizierung (MFA) können Sie die Sicherheit erhöhen, da Benutzer zur Anmeldung bei einem Administrator oder einer Storage-VM zwei Authentifizierungsmethoden bereitstellen müssen.

Je nach Ihrer Version von ONTAP können Sie eine Kombination aus einem öffentlichen SSH-Schlüssel, einem Benutzerpasswort und einem zeitbasierten Einmalpasswort (TOTP) zur mehrstufigen Authentifizierung

verwenden. Wenn Sie Cisco Duo (ONTAP 9.14.1 und höher) aktivieren und konfigurieren, dient es als zusätzliche Authentifizierungsmethode, die die bestehenden Methoden für alle Benutzer ergänzt.

Verfügbar ab…	Erste Authentifizierungsmethode	Zweite Authentifizierungsmethode
ONTAP 9.14.1	Öffentlicher SSH-Schlüssel	TOTP
	Benutzerkennwort	TOTP
	Öffentlicher SSH-Schlüssel	Cisco Duo
	Benutzerpasswort	Cisco Duo
ONTAP 9.13.1	Öffentlicher SSH-Schlüssel	TOTP
	Benutzerpasswort	TOTP
ONTAP 9.3	Öffentlicher SSH-Schlüssel	Benutzerpasswort

Wenn MFA konfiguriert ist, muss der Clusteradministrator zuerst das lokale Benutzerkonto aktivieren, dann muss das Konto vom lokalen Benutzer konfiguriert werden.



Aktivieren Sie Multi-Faktor-Authentifizierung

Dank der Multi-Faktor-Authentifizierung (MFA) können Sie die Sicherheit erhöhen, da Benutzer zur Anmeldung bei einem Administrator oder einer Daten-SVM zwei Authentifizierungsmethoden bereitstellen müssen.

Über diese Aufgabe

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Wenn Sie sich nicht sicher sind, welche Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

  "Ändern der Rolle, die einem Administrator zugewiesen ist"

- Wenn Sie einen öffentlichen Schlüssel für die Authentifizierung verwenden, müssen Sie den öffentlichen Schlüssel dem Konto zuordnen, bevor das Konto auf die SVM zugreifen kann.

  "Einem Benutzerkonto einen öffentlichen Schlüssel zuordnen"

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Ab ONTAP 9.12.1 können Sie Yubikey-Hardware-Authentifizierungsgeräte für SSH-Client MFA verwenden, indem Sie die Authentifizierungsstandards FIDO2 (Fast Identity Online) oder PIV (Personal Identity Verification) verwenden.

Aktivieren Sie MFA mit öffentlichem SSH-Schlüssel und Benutzerpasswort

Ab ONTAP 9.3 kann ein Cluster-Administrator lokale Benutzerkonten für die Anmeldung mit einem öffentlichen SSH-Schlüssel und einem Benutzerpasswort einrichten.

1. Aktivieren Sie MFA auf einem lokalen Benutzerkonto mit öffentlichem SSH-Schlüssel und Benutzerpasswort:

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   Der folgende Befehl erfordert das SVM-Administratorkonto `admin2` Mit dem vordefinierten `admin` Rolle zum Anmelden bei der SVM`engData1` Sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem Benutzerpasswort:

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

Aktivieren Sie MFA mit TOTP

Ab ONTAP 9.13.1 können Sie die Sicherheit erhöhen, indem Sie lokale Benutzer über einen öffentlichen SSH-Schlüssel oder ein Benutzerkennwort und ein zeitbasiertes Einmalpasswort (TOTP) bei einem Administrator

oder einer Daten-SVM einloggen müssen. Nachdem das Konto für MFA mit TOTP aktiviert wurde, muss sich der lokale Benutzer bei anmelden "Schließen Sie die Konfiguration ab".

TOTP ist ein Computeralgorithmus, der die aktuelle Zeit verwendet, um ein Einmalpasswort zu generieren. Wenn TOTP verwendet wird, ist es immer die zweite Form der Authentifizierung nach dem öffentlichen SSH-Schlüssel oder dem Benutzerpasswort.

Bevor Sie beginnen

Sie müssen ein Storage-Administrator sein, um diese Aufgaben auszuführen.

Schritte

Sie können MFA für mit einem Benutzerpasswort oder einem öffentlichen SSH-Schlüssel als erste Authentifizierungsmethode und TOTP als zweite Authentifizierungsmethode einrichten.

Aktivieren Sie MFA mit Benutzerpasswort und TOTP

1. Aktivieren Sie ein Benutzerkonto für Multi-Faktor-Authentifizierung mit einem Benutzerpasswort und einem TOTP.

   Für neue Benutzerkonten

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Für bestehende Benutzerkonten

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Vergewissern Sie sich, dass MFA mit TOTP aktiviert ist:

   ```
   security login show
   ```

Aktivieren Sie MFA mit öffentlichem SSH-Schlüssel und TOTP

1. Aktivieren Sie ein Benutzerkonto für Multi-Faktor-Authentifizierung mit einem öffentlichen SSH-Schlüssel und TOTP.

   Für neue Benutzerkonten

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Für bestehende Benutzerkonten

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Vergewissern Sie sich, dass MFA mit TOTP aktiviert ist:

```
security login show
```

Nachdem Sie fertig sind

- Falls Sie dem Administratorkonto keinen öffentlichen Schlüssel zugeordnet haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

  "Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto"

- Der lokale Benutzer muss sich anmelden, um die MFA-Konfiguration mit TOTP abzuschließen.

  "Konfigurieren Sie das lokale Benutzerkonto für MFA mit TOTP"

Verwandte Informationen

Weitere Informationen zu "Mehrstufige Authentifizierung in ONTAP 9 (TR-4647)".

Konfigurieren Sie das lokale Benutzerkonto für MFA mit TOTP

Ab ONTAP 9.13.1 können Benutzerkonten mit Multi-Faktor-Authentifizierung (MFA) unter Verwendung eines zeitbasierten Einmalpasswords (TOTP) konfiguriert werden.

Bevor Sie beginnen

- Der Storage-Administrator muss "Aktivieren Sie MFA mit TOTP" Als zweite Authentifizierungsmethode für Ihr Benutzerkonto.
- Die primäre Authentifizierungsmethode für das Benutzerkonto sollte ein Benutzerpasswort oder ein öffentlicher SSH-Schlüssel sein.
- Sie müssen Ihre TOTP-App so konfigurieren, dass sie mit Ihrem Smartphone funktioniert und Ihren TOTP-Schlüssel erstellt.

  TOTP wird von verschiedenen Authentifikator-Apps wie Google Authenticator unterstützt.

Schritte

1. Melden Sie sich mit Ihrer aktuellen Authentifizierungsmethode bei Ihrem Benutzerkonto an.

   Die aktuelle Authentifizierungsmethode sollte ein Benutzerpasswort oder ein öffentlicher SSH-Schlüssel sein.

2. Erstellen Sie die TOTP-Konfiguration für Ihr Konto:

   ```
   security login totp create -vserver "<svm_name>" -username
   "<account_username >"
   ```

3. Überprüfen Sie, ob die TOTP-Konfiguration für Ihr Konto aktiviert ist:

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

TOTP-Schlüssel zurücksetzen

Um die Sicherheit deines Kontos zu schützen, solltest du den TOTP-Schlüssel deaktivieren und einen neuen erstellen, wenn er kompromittiert oder verloren ist.

Setzen Sie TOTP zurück, wenn Ihr Schlüssel kompromittiert ist

Wenn Ihr TOTP-Schlüssel kompromittiert ist, Sie aber trotzdem Zugriff darauf haben, können Sie den kompromittierten Schlüssel entfernen und einen neuen erstellen.

1. Melden Sie sich mit Ihrem Benutzerkennwort oder dem öffentlichen SSH-Schlüssel und Ihrem kompromittierten TOTP-Schlüssel bei Ihrem Benutzerkonto an.
2. Entfernen Sie den kompromittierten TOTP-Schlüssel:

   ```
   security login totp delete -vserver <svm_name> -username
   <account_username>
   ```

3. Neuen TOTP-Schlüssel erstellen:

   ```
   security login totp create -vserver <svm_name> -username
   <account_username>
   ```

4. Überprüfen Sie, ob die TOTP-Konfiguration für Ihr Konto aktiviert ist:

   ```
   security login totp show -vserver <svm_name> -username
   <account_username>
   ```

Setzen Sie TOTP zurück, wenn Ihr Schlüssel verloren geht

Wenn Ihr TOTP-Geheimschlüssel verloren geht, wenden Sie sich an Ihren Speicheradministrator "Lassen Sie den Schlüssel deaktiviert". Nachdem der Schlüssel deaktiviert wurde, können Sie sich mit Ihrer ersten Authentifizierungsmethode anmelden und ein neues TOTP konfigurieren.

Bevor Sie beginnen

Der TOTP-Schlüssel muss von einem Speicheradministrator deaktiviert werden. Wenn Sie kein Storage-Administratorkonto haben, wenden Sie sich an Ihren Storage-Administrator, um den Schlüssel zu deaktivieren.

Schritte

1. Nachdem der TOTP-Schlüssel von einem Speicheradministrator deaktiviert wurde, melden Sie sich mit Ihrer primären Authentifizierungsmethode bei Ihrem lokalen Konto an.

2. Neuen TOTP-Schlüssel erstellen:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. Überprüfen Sie, ob die TOTP-Konfiguration für Ihr Konto aktiviert ist:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Deaktivieren Sie den geheimen TOTP-Schlüssel für das lokale Konto

Wenn der zeitbasierte TOTP-Schlüssel (One-Time Password) eines lokalen Benutzers verloren geht, muss der verlorene Schlüssel von einem Speicheradministrator deaktiviert werden, bevor der Benutzer einen neuen TOTP-Schlüssel erstellen kann.

Über diese Aufgabe

Diese Aufgabe kann nur über ein Cluster-Administratorkonto ausgeführt werden.

Schritt

1. Deaktivieren Sie den geheimen TOTP-Schlüssel:

```
security login totp delete -vserver "<svm_name>" -username
"<account_username>"
```

Aktivieren Sie SSL-Zertifikatkonten

Sie können das verwenden `security login create` Befehl zum Aktivieren von Administratorkonten für den Zugriff auf einen Administrator oder eine Daten-SVM mit einem SSL-Zertifikat

Über diese Aufgabe

- Sie müssen ein digitales Zertifikat für einen CA-signierten Server installieren, bevor das Konto auf die SVM zugreifen kann.

  Erstellen und Installieren eines CA-signierten Serverzertifikats

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Wenn Sie sich nicht sicher sind, welche Rolle die Zugriffskontrolle Sie dem Login-Konto zuweisen möchten, können Sie die Rolle später mit dem hinzufügen `security login modify` Befehl.

  Ändern der Rolle, die einem Administrator zugewiesen ist

Bei Clusteradministratorkonten wird die Zertifikatauthentifizierung mit unterstützt `http`, `ontapi`, und `rest` Applikationen unterstützt. Bei SVM-Administratorkonten wird die Zertifikatauthentifizierung nur von unterstützt `ontapi` Und `rest` Applikationen unterstützt.

Schritt

1. Aktivieren Sie lokale Administratorkonten für den Zugriff auf eine SVM mithilfe eines SSL-Zertifikats:

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   Eine vollständige Befehlssyntax finden Sie im "ONTAP-man-Pages nach Release".

   Mit dem folgenden Befehl wird das SVM-Administratorkonto aktiviert `svmadmin2` Mit der Standardeinstellung `vsadmin` Rolle für den Zugriff auf die SVM`engData2` Verwenden eines digitalen SSL-Zertifikats.

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

Nachdem Sie fertig sind

Wenn Sie kein digitales Zertifikat für einen CA-signierten Server installiert haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Erstellen und Installieren eines CA-signierten Serverzertifikats

Aktivieren Sie den Zugriff auf Active Directory-Konten

Sie können das verwenden `security login create` Befehl zum Aktivieren von Active Directory-Benutzer- oder Gruppenkonten für den Zugriff auf einen Administrator oder eine Daten-SVM Jeder Benutzer der AD-Gruppe kann mit der Rolle, die der Gruppe zugewiesen ist, auf die SVM zugreifen.

Über diese Aufgabe

- Sie müssen AD-Domänencontroller-Zugriff auf das Cluster oder SVM konfigurieren, bevor das Konto auf die SVM zugreifen kann.

  Active Directory-Domänencontroller-Zugriff wird konfiguriert

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Ab ONTAP 9.13.1 können Sie einen öffentlichen SSH-Schlüssel als primäre oder sekundäre Authentifizierungsmethode mit einem AD-Benutzerpasswort verwenden.

  Wenn Sie einen öffentlichen SSH-Schlüssel als primäre Authentifizierung verwenden, findet keine AD-Authentifizierung statt.

- Ab ONTAP 9.11.1 können Sie dies nutzen "LDAP fast bind für nsswitch-Authentifizierung" Wenn es vom AD LDAP-Server unterstützt wird.

- Wenn Sie sich nicht sicher sind, welche Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

  Ändern der Rolle, die einem Administrator zugewiesen ist

> Der Zugriff auf das Konto FÜR DIE ANZEIGENGRUPPE wird nur mit dem unterstützt `SSH`, `ontapi`, und `rest` Applikationen unterstützt. AD-Gruppen werden mit der SSH-Authentifizierung für öffentliche Schlüssel, die häufig für Multi-Faktor-Authentifizierung verwendet wird, nicht unterstützt.

Bevor Sie beginnen

- Die Cluster-Zeit muss innerhalb von fünf Minuten nach der Zeit auf dem AD Domain Controller synchronisiert werden.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Aktivieren Sie AD-Benutzer- oder Gruppenadministratorkonten für den Zugriff auf eine SVM:

   Für AD-Nutzer:

ONTAP-Version	Primäre Authentifizierung	Sekundäre Authentifizierung	Befehl
9.13.1 und höher	Öffentlicher Schlüssel	Keine	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

ONTAP-Version	Primäre Authentifizierung	Sekundäre Authentifizierung	Befehl

9.13.1 und höher	Domäne	Öffentlicher Schlüssel	**Für einen neuen Benutzer**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			Für einen bestehenden Benutzer
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 und höher	Domäne	Keine	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Für AD-Gruppen:

ONTAP-Version	Primäre Authentifizierung	Sekundäre Authentifizierung	Befehl
9.0 und höher	Domäne	Keine	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Eine vollständige Befehlssyntax finden Sie unter "Worksheets zur Administratorauthentifizierung und RBAC-Konfiguration"

Nachdem Sie fertig sind

Falls Sie keinen Zugriff von AD-Domänen-Controllern auf das Cluster oder SVM konfiguriert haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Active Directory-Domänencontroller-Zugriff wird konfiguriert

Aktivieren Sie den LDAP- oder NIS-Kontozugriff

Sie können das verwenden `security login create` Befehl zum Aktivieren von LDAP- oder NIS-Benutzerkonten für den Zugriff auf Admin oder Daten-SVMs. Wenn Sie keinen LDAP- oder NIS-Serverzugriff auf die SVM konfiguriert haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Über diese Aufgabe

- Gruppenkonten werden nicht unterstützt.
- Sie müssen LDAP- oder NIS-Serverzugriff auf die SVM konfigurieren, bevor das Konto auf die SVM zugreifen kann.

  Konfigurieren des LDAP- oder NIS-Serverzugriffs

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Wenn Sie sich nicht sicher sind, welche Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

  Ändern der Rolle, die einem Administrator zugewiesen ist

- Ab ONTAP 9.4 wird Multi-Faktor-Authentifizierung (MFA) für Remote-Benutzer über LDAP- oder NIS-Server unterstützt.
- Ab ONTAP 9.11.1 können Sie dies nutzen "LDAP fast bind für nsswitch-Authentifizierung" Wenn es vom LDAP-Server unterstützt wird.
- Aufgrund eines bekannten LDAP-Problems sollten Sie das nicht verwenden `':'` (Doppelpunkt) Zeichen in einem beliebigen Feld von LDAP-Benutzerkontoinformationen (z. B. `gecos`, `userPassword`, Und so weiter). Andernfalls schlägt die Suche für diesen Benutzer fehl.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Aktivieren Sie LDAP- oder NIS-Benutzer- oder Gruppenkonten für den Zugriff auf eine SVM:

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

"Erstellen oder Ändern von Anmeldekonten"

Mit dem folgenden Befehl wird das LDAP- oder NIS-Cluster-Administratorkonto aktiviert `guest2` Mit dem vordefinierten `backup` Rolle für den Zugriff auf die Administrator-SVM`engCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

2. MFA-Anmeldung für LDAP- oder NIS-Benutzer aktivieren:

   `security login modify -user-or-group-name rem_usr1 -application ssh -authentication-method nsswitch -role admin -is-ns-switch-group no -second -authentication-method publickey`

   Die Authentifizierungsmethode kann als angegeben werden `publickey` Und zweite Authentifizierungsmethode als `nsswitch`.

   Im folgenden Beispiel wird die MFA-Authentifizierung aktiviert:

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

Nachdem Sie fertig sind

Wenn Sie keinen LDAP- oder NIS-Serverzugriff auf die SVM konfiguriert haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Konfigurieren des LDAP- oder NIS-Serverzugriffs

Management von Zugriffssteuerungsrollen

Übersicht über Zugriffssteuerungsrollen verwalten

Die einem Administrator zugewiesene Rolle legt die Befehle fest, auf die der Administrator zugreifen kann. Sie weisen die Rolle beim Erstellen des Kontos für den Administrator zu. Sie können je nach Bedarf eine andere Rolle zuweisen oder benutzerdefinierte Rollen definieren.

Ändern Sie die einem Administrator zugewiesene Rolle

Sie können das verwenden `security login modify` Befehl zum Ändern der Rolle eines Cluster- oder SVM-Administratorkontos. Sie können eine vordefinierte oder benutzerdefinierte Rolle zuweisen.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Ändern Sie die Rolle eines Clusters oder SVM-Administrators:

   `security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment`

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   "Erstellen oder Ändern von Anmeldekonten"

   Mit dem folgenden Befehl wird die Rolle des AD-Cluster-Administratorkontos geändert `DOMAIN1\guest1` Für den vordefinierten `readonly` Rolle:

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   Mit dem folgenden Befehl wird die Rolle der SVM-Administratorkonten im AD-Gruppenkonto geändert `DOMAIN1\adgroup` Auf den Benutzer `vol_role` Rolle:

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

Definieren benutzerdefinierter Rollen

Sie können das verwenden `security login role create` Befehl zum Definieren einer benutzerdefinierten Rolle. Sie können den Befehl so oft wie nötig ausführen, um die genaue Kombination der Funktionen zu erreichen, die Sie mit der Rolle verknüpfen möchten.

Über diese Aufgabe

- Eine Rolle, ob vordefiniert oder benutzerdefiniert, gewährt oder verweigert den Zugriff auf ONTAP-Befehle oder Befehlsverzeichnisse.

  Ein Befehlsverzeichnis (`volume`, Zum Beispiel) ist eine Gruppe verwandter Befehle und Unterverzeichnisse. Sofern nicht wie in diesem Verfahren beschrieben, gewährt oder verweigert das Zulassen des Zugriffs auf ein Befehlsverzeichnis jedem Befehl im Verzeichnis und seinen Unterverzeichnissen den Zugriff.

- Bestimmter Befehlszugriff oder Unterverzeichnis-Zugriff überschreibt den Zugriff auf das übergeordnete Verzeichnis.

  Wenn eine Rolle mit einem Befehlsverzeichnis definiert ist und dann erneut mit einer anderen Zugriffsebene für einen bestimmten Befehl oder ein Unterverzeichnis des übergeordneten Verzeichnisses definiert wird, überschreibt die Zugriffsebene, die für den Befehl oder das Unterverzeichnis festgelegt ist, die des übergeordneten Verzeichnisses.

> Einem SVM-Administrator kann keine Rolle zugewiesen werden, die einem Befehl oder Befehlsverzeichnis Zugriff gibt, das nur dem zur Verfügung steht `admin` Cluster-Administrator – zum Beispiel der `security` Befehlsverzeichnis.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Definieren einer benutzerdefinierten Rolle:

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Die folgenden Befehle erteilen das `vol_role` Rollen vollständigen Zugriff auf die Befehle im `volume` Befehlsverzeichnis und schreibgeschützter Zugriff auf die Befehle im `volume snapshot` Unterverzeichnis.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   Die folgenden Befehle erteilen das `SVM_storage` Rolle nur-Lese-Zugriff auf die Befehle in der `storage` Befehlsverzeichnis, kein Zugriff auf die Befehle im `storage encryption` Unterverzeichnis und vollständigen Zugriff auf das `storage aggregate plex offline` Nicht-intrinsischer Befehl.

   ```
   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage" -access readonly

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage encryption" -access none

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage aggregate plex offline" -access all
   ```

Vordefinierte Rollen für Cluster-Administratoren

Die vordefinierten Rollen für Cluster-Administratoren sollten die meisten Ihrer Anforderungen erfüllen. Sie können bei Bedarf benutzerdefinierte Rollen erstellen. Standardmäßig wird einem Cluster-Administrator das vordefinierte zugewiesen `admin` Rolle:

In der folgenden Tabelle werden die vordefinierten Rollen für Cluster-Administratoren aufgeführt:

Diese Rolle…	Verfügt über diese Zugriffsebene…	Zu den folgenden Befehlen oder Befehlsverzeichnissen
Admin	Alle	Alle Befehlsverzeichnisse (`DEFAULT`)
Admin-no-fsa (ab ONTAP 9.12.1 verfügbar)	Lese-/Schreibzugriff	• Alle Befehlsverzeichnisse (`DEFAULT`) • `security login rest-role` • `security login role`
Schreibgeschützt	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Keine
`volume file show-disk-usage`	AutoSupport	Alle
• `set` • `system node autosupport`	Keine	Alle anderen Befehlsverzeichnisse (`DEFAULT`)
Backup	Alle	`vserver services ndmp`

readonly	`volume`	Keine
Alle anderen Befehlsverzeichnisse (`DEFAULT`)	readonly	Alle
• `security login password` Nur zur Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • `set`	Keine	`security`
readonly	Alle anderen Befehlsverzeichnisse (`DEFAULT`)	Keine

Der `autosupport` Rolle ist dem vordefinierten zugewiesen `autosupport` Konto, das von AutoSupport OnDemand verwendet wird. ONTAP verhindert, dass Sie den ändern oder löschen können `autosupport` Konto. ONTAP verhindert darüber hinaus, dass Sie das zuweisen `autosupport` Rolle für andere Benutzerkonten.

Vordefinierte Rollen für SVM-Administratoren

Die vordefinierten Rollen für SVM-Administratoren sollten die meisten Ihrer Anforderungen erfüllen. Sie können bei Bedarf benutzerdefinierte Rollen erstellen. Standardmäßig wird einem SVM-Administrator das vordefinierte zugewiesen `vsadmin` Rolle:

In der folgenden Tabelle sind die vordefinierten Rollen für SVM-Administratoren aufgeführt:

Rollenname	Sorgen

Vsadmin	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Verwalten von Volumes, außer Verschieben von Volumes • Verwalten von Quotas, qtrees, Snapshot Kopien und Dateien • Verwalten von LUNs • Durchführung von SnapLock-Vorgängen mit Ausnahme von privilegierten Löschen • Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Dienste konfigurieren: DNS, LDAP und NIS • Überwachen von Jobs • Monitoring von Netzwerkverbindungen und Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
Vsadmin-Volume	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Managen von Volumes, einschließlich Volume-Verschiebungen • Verwalten von Quotas, qtrees, Snapshot Kopien und Dateien • Verwalten von LUNs • Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Dienste konfigurieren: DNS, LDAP und NIS • Monitoring der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
Vsadmin-Protokoll	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Dienste konfigurieren: DNS, LDAP und NIS • Verwalten von LUNs • Monitoring der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM

Vsadmin-Backup	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Verwalten des NDMP-Betriebs • Erstellung eines wiederhergestellten Lese-/Schreibvorgangs eines Volumes • Verwalten von SnapMirror Beziehungen und Snapshot Kopien • Anzeigen von Volumes und Netzwerkinformationen
Vsadmin-snaplock	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Verwalten von Volumes, außer Verschieben von Volumes • Verwalten von Quotas, qtrees, Snapshot Kopien und Dateien • Durchführung von SnapLock-Vorgängen einschließlich privilegierter Löschung • Konfiguration von Protokollen: NFS und SMB • Dienste konfigurieren: DNS, LDAP und NIS • Überwachen von Jobs • Monitoring von Netzwerkverbindungen und Netzwerkschnittstelle
Vsadmin-Readonly	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Monitoring des Systemzustands der SVM • Monitoring der Netzwerkschnittstelle • Anzeigen von Volumes und LUNs • Anzeigen von Services und Protokollen

Kontrolle des Administratorzugriffs

Die einem Administrator zugewiesene Rolle bestimmt, welche Funktionen der Administrator mit dem System Manager ausführen kann. Vordefinierte Rollen für Cluster-Administratoren und Storage VM-Administratoren werden von System Manager bereitgestellt. Sie weisen die Rolle beim Erstellen des Administratorkontos zu, oder Sie können später eine andere Rolle zuweisen.

Je nachdem, wie Sie den Kontozugriff aktiviert haben, müssen Sie unter Umständen einen der folgenden Schritte ausführen:

- Einem lokalen Konto einen öffentlichen Schlüssel zuordnen.

- Installieren Sie ein digitales Zertifikat für einen CA-signierten Server.
- Konfiguration des AD-, LDAP- oder NIS-Zugriffs

Sie können diese Aufgaben vor oder nach dem Aktivieren des Kontozugriffs ausführen.

Zuweisen einer Rolle zu einem Administrator

Weisen Sie einem Administrator eine Rolle wie folgt zu:

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie → Neben **Benutzer und Rollen**.
3. Wählen Sie + Add Unter **Benutzer**.
4. Geben Sie einen Benutzernamen an, und wählen Sie im Dropdown-Menü für **Role** eine Rolle aus.
5. Geben Sie eine Anmeldemethode und ein Kennwort für den Benutzer an.

Ändern der Administratorrolle

Ändern Sie die Rolle für einen Administrator wie folgt:

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Wählen Sie den Namen des Benutzers aus, dessen Rolle Sie ändern möchten, und klicken Sie dann auf das ⋮ Das wird neben dem Benutzernamen angezeigt.
3. Klicken Sie Auf **Bearbeiten**.
4. Wählen Sie eine Rolle im Dropdown-Menü für die **Rolle** aus.

Verwalten von Administratorkonten

Administratorkonten verwalten – Übersicht

Je nachdem, wie Sie den Kontozugriff aktiviert haben, müssen Sie möglicherweise einen öffentlichen Schlüssel mit einem lokalen Konto verknüpfen, ein digitales Zertifikat für einen CA-signierten Server installieren oder AD-, LDAP- oder NIS-Zugriff konfigurieren. Sie können alle diese Aufgaben vor oder nach der Aktivierung des Kontozugriffs ausführen.

Einem Administratorkonto einen öffentlichen Schlüssel zuordnen

Bei der SSH-Authentifizierung für den öffentlichen Schlüssel müssen Sie den öffentlichen Schlüssel einem Administratorkonto zuweisen, bevor das Konto auf die SVM zugreifen kann. Sie können das verwenden `security login publickey create` Befehl zum Zuordnen eines Schlüssels zu einem Administratorkonto.

Über diese Aufgabe

Wenn Sie ein Konto über SSH sowohl mit einem Passwort als auch mit einem öffentlichen SSH-Schlüssel authentifizieren, wird das Konto zunächst mit dem öffentlichen Schlüssel authentifiziert.

Bevor Sie beginnen

- Sie müssen den SSH-Schlüssel generiert haben.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Einen öffentlichen Schlüssel einem Administratorkonto zuordnen:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-comment` *`comment`*

   Eine vollständige Befehlssyntax finden Sie in der Worksheet-Referenz für "Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto".

2. Überprüfen Sie die Änderung, indem Sie den öffentlichen Schlüssel anzeigen:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Beispiel

Der folgende Befehl ordnet dem SVM-Administratorkonto einen öffentlichen Schlüssel zu `svmadmin1` Für die SVM `engData1`. Dem öffentlichen Schlüssel wird die Indexnummer 5 zugewiesen.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

Verwalten von öffentlichen SSH-Schlüsseln und X.509-Zertifikaten für ein Administratorkonto

Um die SSH-Authentifizierungssicherheit mit Administratorkonten zu erhöhen, können Sie die verwenden `security login publickey` Satz von Befehlen zur Verwaltung des öffentlichen SSH-Schlüssels und seiner Verknüpfung mit X.509-Zertifikaten.

Verknüpfen Sie einen öffentlichen Schlüssel und ein X.509-Zertifikat mit einem Administratorkonto

Ab ONTAP 9.13.1 können Sie ein X.509-Zertifikat mit dem öffentlichen Schlüssel verknüpfen, den Sie mit dem Administratorkonto verknüpfen. Dadurch erhalten Sie die zusätzliche Sicherheit bei der Überprüfung des Zertifikatablaufs oder des Widerrufs bei der SSH-Anmeldung für dieses Konto.

Über diese Aufgabe

Wenn Sie ein Konto über SSH sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem X.509-Zertifikat authentifizieren, überprüft ONTAP die Gültigkeit des X.509-Zertifikats, bevor es sich mit dem öffentlichen SSH-Schlüssel authentifiziert. Die SSH-Anmeldung wird abgelehnt, wenn das Zertifikat abgelaufen ist oder widerrufen wurde, und der öffentliche Schlüssel wird automatisch deaktiviert.

Bevor Sie beginnen

- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Sie müssen den SSH-Schlüssel generiert haben.
- Wenn Sie nur das X.509-Zertifikat auf Gültigkeit prüfen müssen, können Sie ein selbstsigniertes Zertifikat verwenden.

- Wenn Sie das X.509-Zertifikat auf Ablaufdatum und Widerruf prüfen müssen:
  - Sie müssen das Zertifikat von einer Zertifizierungsstelle erhalten haben.
  - Sie müssen die Zertifikatskette (Zwischen- und Stammzertifizierungsstellen) mit installieren `security certificate install` Befehle.
  - Sie müssen OCSP für SSH aktivieren. Siehe "Überprüfen Sie, ob digitale Zertifikate mit OCSP gültig sind" Weitere Anweisungen.

Schritte

1. Einen öffentlichen Schlüssel und ein X.509-Zertifikat einem Administratorkonto zuordnen:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-x509-certificate install`

   Eine vollständige Befehlssyntax finden Sie in der Worksheet-Referenz für "Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto".

2. Überprüfen Sie die Änderung, indem Sie den öffentlichen Schlüssel anzeigen:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Beispiel

Mit dem folgenden Befehl werden ein öffentlicher Schlüssel und ein X.509-Zertifikat dem SVM-Administratorkonto zugeordnet `svmadmin2` Für die SVM `engData2`. Der öffentliche Schlüssel wird mit der Indexnummer 6 belegt.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Entfernen Sie die Zertifikatszuordnung aus dem öffentlichen SSH-Schlüssel für ein Administratorkonto

Sie können die aktuelle Zertifikatzuordnung aus dem öffentlichen SSH-Schlüssel des Kontos entfernen und dabei den öffentlichen Schlüssel beibehalten.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Entfernen Sie die X.509-Zertifikatszuordnung aus einem Administratorkonto, und behalten Sie den vorhandenen öffentlichen SSH-Schlüssel bei:

   `security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete`

2. Überprüfen Sie die Änderung, indem Sie den öffentlichen Schlüssel anzeigen:

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

Beispiel

Mit dem folgenden Befehl wird die X.509-Zertifikatzuordnung aus dem SVM-Administratorkonto entfernt `svmadmin2` Für die SVM `engData2` Bei Indexnummer 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

Entfernen Sie den öffentlichen Schlüssel und die Zertifikatzuordnung aus einem Administratorkonto

Sie können den aktuellen öffentlichen Schlüssel und die Zertifikatkonfiguration aus einem Konto entfernen.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Entfernen Sie den öffentlichen Schlüssel und eine X.509-Zertifikatzuordnung aus einem Administratorkonto:

   ```
   security login publickey delete -vserver SVM_name -username user_name -index
   index
   ```

2. Überprüfen Sie die Änderung, indem Sie den öffentlichen Schlüssel anzeigen:

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

Beispiel

Mit dem folgenden Befehl werden ein öffentlicher Schlüssel und ein X.509-Zertifikat aus dem SVM-Administratorkonto entfernt `svmadmin3` Für die SVM `engData3` Bei Indexnummer 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

Konfigurieren Sie Cisco Duo 2FA für SSH-Anmeldungen

Ab ONTAP 9.14.1 können Sie ONTAP während der SSH-Anmeldung für die zwei-Faktor-Authentifizierung (2FA) konfigurieren. Sie konfigurieren Duo auf Cluster-Ebene und dies gilt standardmäßig für alle Benutzerkonten. Alternativ können Sie Duo auf der Ebene der Storage-VM (früher als vServer bezeichnet) konfigurieren. In diesem Fall gilt dies nur für Benutzer dieser Storage-VM. Wenn Sie Duo aktivieren und konfigurieren, dient es als zusätzliche Authentifizierungsmethode, die die bestehenden Methoden für alle Benutzer ergänzt.

Wenn Sie die Duo-Authentifizierung für SSH-Anmeldungen aktivieren, müssen Benutzer ein Gerät registrieren,

wenn sie sich das nächste Mal über SSH anmelden. Informationen zur Registrierung finden Sie im Cisco Duo "Dokumentation der Anmeldung".

Über die ONTAP-Befehlszeilenschnittstelle können Sie mit Cisco Duo die folgenden Aufgaben ausführen:

- Konfigurieren Sie Cisco Duo
- Ändern Sie die Cisco Duo-Konfiguration
- Entfernen Sie die Cisco Duo-Konfiguration
- Cisco Duo-Konfiguration anzeigen
- Entfernen Sie eine Duo-Gruppe
- Zeigen Sie Duo-Gruppen an
- Umgehen Sie die Duo-Authentifizierung für Benutzer

Konfigurieren Sie Cisco Duo

Sie können eine Cisco Duo-Konfiguration für den gesamten Cluster oder für eine bestimmte Storage-VM (in der ONTAP-CLI als vServer bezeichnet) erstellen. Verwenden Sie dazu das `security login duo create` Befehl. Wenn Sie dies tun, ist Cisco Duo für SSH-Anmeldungen für dieses Cluster oder diese Storage-VM aktiviert.

Schritte

1. Melden Sie sich beim Cisco Duo-Administratorbereich an.
2. Gehen Sie zu **Anwendungen > UNIX-Anwendung**.
3. Notieren Sie den Integrationsschlüssel, den geheimen Schlüssel und den API-Hostnamen.
4. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
5. Aktivieren Sie die Cisco Duo-Authentifizierung für diese Storage-VM und ersetzen Sie die Informationen aus Ihrer Umgebung durch die Werte in Klammern:

   ```
   security login duo create \
   -vserver <STORAGE_VM_NAME> \
   -integration-key <INTEGRATION_KEY> \
   -secret-key <SECRET_KEY> \
   -apihost <API_HOSTNAME>
   ```

   Weitere Informationen zu den erforderlichen und optionalen Parametern für diesen Befehl finden Sie unter "Arbeitsblätter für die Administratorauthentifizierung und die RBAC-Konfiguration".

Ändern Sie die Cisco Duo-Konfiguration

Sie können die Art und Weise ändern, wie Cisco Duo Benutzer authentifiziert (z. B. wie viele Authentifizierungsaufforderungen angegeben werden oder welcher HTTP-Proxy verwendet wird). Wenn Sie die Cisco Duo-Konfiguration für eine Speicher-VM (in der ONTAP-CLI als vServer bezeichnet) ändern müssen, können Sie die verwenden `security login duo modify` Befehl.

Schritte

1. Melden Sie sich beim Cisco Duo-Administratorbereich an.

2. Gehen Sie zu **Anwendungen > UNIX-Anwendung**.
3. Notieren Sie den Integrationsschlüssel, den geheimen Schlüssel und den API-Hostnamen.
4. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
5. Ändern Sie die Cisco Duo-Konfiguration für diese Speicher-VM, indem Sie aktualisierte Informationen aus Ihrer Umgebung durch die Werte in Klammern ersetzen:

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-is-enabled true|false \
-fail-mode safe|secure
```

Entfernen Sie die Cisco Duo-Konfiguration

Sie können die Cisco Duo-Konfiguration entfernen, sodass SSH-Benutzer sich bei der Anmeldung nicht mehr mit Duo authentifizieren müssen. Um die Cisco Duo-Konfiguration für eine Speicher-VM zu entfernen (in der ONTAP-CLI als vServer bezeichnet), können Sie die verwenden `security login duo delete` Befehl.

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Entfernen Sie die Cisco Duo-Konfiguration für diese Speicher-VM, und ersetzen Sie Ihren Speicher-VM-Namen für `<STORAGE_VM_NAME>`:

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

Dadurch wird die Cisco Duo-Konfiguration für diese Speicher-VM endgültig gelöscht.

Cisco Duo-Konfiguration anzeigen

Sie können die bestehende Cisco Duo-Konfiguration für eine Storage-VM (in der ONTAP-CLI als vServer bezeichnet) mit dem anzeigen `security login duo show` Befehl.

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Zeigen Sie die Cisco Duo-Konfiguration für diese Storage-VM. Optional können Sie den verwenden `vserver` Parameter zum Angeben einer Storage-VM, durch den der Name der Storage-VM ersetzt wird `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Sie sollten eine Ausgabe wie die folgende sehen:

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Erstellen Sie eine Duo-Gruppe

Sie können Cisco Duo anweisen, nur die Benutzer in einem bestimmten Active Directory, LDAP oder einer lokalen Benutzergruppe in den Duo-Authentifizierungsprozess einzubeziehen. Wenn Sie eine Duo-Gruppe erstellen, werden nur die Benutzer dieser Gruppe zur Duo-Authentifizierung aufgefordert. Sie können eine Duo-Gruppe mit dem erstellen `security login duo group create` Befehl. Wenn Sie eine Gruppe erstellen, können Sie optional bestimmte Benutzer dieser Gruppe aus dem Duo-Authentifizierungsprozess ausschließen.

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Erstellen Sie die Duo-Gruppe, indem Sie Informationen aus Ihrer Umgebung durch die Werte in Klammern ersetzen. Wenn Sie den nicht angeben `-vserver` Parameter, wird die Gruppe auf Cluster-Ebene erstellt:

   ```
   security login duo group create -vserver <STORAGE_VM_NAME> -group-name
   <GROUP_NAME> -exclude-users <USER1, USER2>
   ```

   Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen. Benutzer, die Sie mit der Option angeben `-exclude-users` Parameter werden nicht in den Duo-Authentifizierungsprozess einbezogen.

Zeigen Sie Duo-Gruppen an

Sie können vorhandene Cisco Duo-Gruppeneinträge mit der anzeigen `security login duo group show` Befehl.

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Zeigen Sie die Gruppeneinträge der Duo-Gruppe an und ersetzen Sie die Informationen aus Ihrer Umgebung durch die Werte in Klammern. Wenn Sie den nicht angeben `-vserver` Parameter, wird die Gruppe auf Cluster-Ebene angezeigt:

   ```
   security login duo group show -vserver <STORAGE_VM_NAME> -group-name
   <GROUP_NAME> -exclude-users <USER1, USER2>
   ```

   Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen. Benutzer, die Sie mit der Option angeben `-exclude-users` Parameter wird nicht angezeigt.

Entfernen Sie eine Duo-Gruppe

Sie können einen Duo-Gruppeneintrag mit dem entfernen `security login duo group delete` Befehl. Wenn Sie eine Gruppe entfernen, werden die Benutzer dieser Gruppe nicht mehr in den Duo-Authentifizierungsprozess einbezogen.

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Entfernen Sie den Gruppeneintrag Duo, und ersetzen Sie die Informationen aus Ihrer Umgebung durch die Werte in Klammern. Wenn Sie den nicht angeben `-vserver` Parameter, wird die Gruppe auf Cluster-Ebene entfernt:

   ```
   security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
   <GROUP_NAME>
   ```

   Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen.

Umgehen Sie die Duo-Authentifizierung für Benutzer

Sie können alle Benutzer oder bestimmte Benutzer von der Duo SSH-Authentifizierung ausschließen.

Alle Duo-Benutzer ausschließen

Sie können die Cisco Duo SSH-Authentifizierung für alle Benutzer deaktivieren.

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Deaktivieren Sie die Cisco Duo-Authentifizierung für SSH-Benutzer, indem Sie den vServer-Namen durch ersetzen `<STORAGE_VM_NAME>`:

   ```
   security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled-false
   ```

Benutzer der Duo-Gruppe ausschließen

Sie können bestimmte Benutzer, die Teil einer Duo-Gruppe sind, aus dem Duo SSH-Authentifizierungsprozess ausschließen.

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Deaktivieren Sie die Cisco Duo-Authentifizierung für bestimmte Benutzer in einer Gruppe. Ersetzen Sie den Gruppennamen und die Liste der auszuschließenden Benutzer durch die Werte in Klammern:

   ```
   security login group modify -group-name <GROUP_NAME> -exclude-users
   <USER1, USER2>
   ```

   Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen. Benutzer, die Sie mit angeben `-exclude-users` Parameter werden nicht in den Duo-Authentifizierungsprozess einbezogen.

Lokale Duo-Benutzer ausschließen

Sie können bestimmte lokale Benutzer von der Duo-Authentifizierung ausschließen, indem Sie das Cisco Duo-Administratorfenster verwenden. Anweisungen hierzu finden Sie im "Cisco Duo-Dokumentation".

Erstellen und installieren Sie eine Übersicht über ein CA-signiertes Serverzertifikat

Auf Produktionssystemen ist es eine Best Practice, ein von CA signiertes digitales Zertifikat zur Authentifizierung des Clusters oder der SVM als SSL-Server zu installieren. Sie können das verwenden `security certificate generate-csr` Befehl zum Generieren einer Zertifikatsignierungsanforderung (CSR) und des `security certificate install` Befehl zum Installieren des Zertifikats, das Sie von der Zertifizierungsstelle erhalten.

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

Sie können das verwenden `security certificate generate-csr` Befehl zum Generieren einer Zertifikatsignierungsanforderung (CSR). Nach Bearbeitung Ihrer Anfrage sendet Ihnen die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. CSR erstellen:

   ```
   security certificate generate-csr -common-name FQDN_or_common_name -size
   512|1024|1536|2048 -country country -state state -locality locality
   -organization organization -unit unit -email-addr email_of_contact -hash
   -function SHA1|SHA256|MD5
   ```

   Mit dem folgenden Befehl wird eine CSR mit einem 2048-Bit privaten Schlüssel erstellt, der von der

Hashing-Funktion „`SHA256`“ generiert wird, um von der Gruppe „`Software`“ in der Abteilung „` IT s`“ eines Unternehmens mit dem benutzerdefinierten gemeinsamen Namen „`erver1.companyname.com`"“ in Sunnyvale, Kalifornien, USA verwendet zu werden. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet „`web@example.com`“. Das System zeigt den CSR und den privaten Schlüssel in der Ausgabe an.

Beispiel für das Erstellen einer CSR

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Kopieren Sie die Zertifikatsanforderung aus der CSR-Ausgabe, und senden Sie sie in elektronischer Form (z. B. E-Mail) an eine vertrauenswürdige Drittanbieter-CA zum Signieren.

   Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat. Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten digitalen Zertifikats aufbewahren.

Installieren Sie ein CA-signiertes Serverzertifikat

Sie können das verwenden `security certificate install` Befehl zum Installieren eines CA-signierten Serverzertifikats auf einer SVM. ONTAP fordert Sie auf, die Stammzertifikate und Zwischenzertifikate der Zertifizierungsstelle (CA) anzugeben, die die Zertifikatskette des Serverzertifikats bilden.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritt

1. Installieren eines CA-signierten Serverzertifikats:

   ```
   security certificate install -vserver SVM_name -type certificate_type
   ```

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   > ONTAP fordert Sie zur Eingabe der CA-Stammzertifikate und der Zwischenzertifikate auf, die die Zertifikatskette des Serverzertifikats bilden. Die Kette beginnt mit dem Zertifikat der Zertifizierungsstelle, die das Serverzertifikat ausgestellt hat, und kann bis zum Stammzertifikat der Zertifizierungsstelle reichen. Fehlende Zwischenzertifikate führen zum Ausfall der Serverzertifikatinstallation.

   Mit dem folgenden Befehl werden das CA-signierte Serverzertifikat und die Zwischenzertifikate auf der SVM „`engData2`“ installiert.

Beispiel für die Installation eines CA-signierten Server-Zertifikats für Zwischenzertifikate

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

Verwalten von Zertifikaten mit System Manager

Ab ONTAP 9.10.1 können Sie mit System Manager vertrauenswürdige Zertifizierungsstellen, Client-/Serverzertifikate und lokale (Onboard-)Zertifizierungsstellen verwalten.

Mit System Manager können Sie die von anderen Anwendungen erhaltenen Zertifikate verwalten, sodass Sie die Kommunikation von diesen Anwendungen authentifizieren können. Sie können auch Ihre eigenen Zertifikate verwalten, die Ihr System für andere Anwendungen identifizieren.

Zeigen Sie Zertifikatinformationen an

Mit System Manager können Sie vertrauenswürdige Zertifizierungsstellen, Client-/Serverzertifikate und lokale Zertifikatbehörden anzeigen, die auf dem Cluster gespeichert sind.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Blättern Sie zum Bereich **Sicherheit**. Im Abschnitt **Zertifikate** werden die folgenden Details angezeigt:
   - Die Anzahl der gespeicherten vertrauenswürdigen Zertifizierungsstellen.
   - Die Anzahl der gespeicherten Client/Server-Zertifikate.
   - Die Anzahl der gespeicherten lokalen Zertifikatbehörden.
3. Wählen Sie eine beliebige Nummer aus, um Details zu einer Zertifikatskategorie anzuzeigen, oder wählen Sie aus → Um die Seite **Zertifikate** zu öffnen, die Informationen zu allen Kategorien enthält.
   In der Liste werden die Informationen für den gesamten Cluster angezeigt. Wenn Sie Informationen nur für eine bestimmte Storage-VM anzeigen möchten, führen Sie die folgenden Schritte aus:
   a. Wählen Sie **Storage > Storage VMs**.
   b. Wählen Sie die Storage-VM aus.
   c. Wechseln Sie zur Registerkarte **Einstellungen**.

d. Wählen Sie eine Zahl aus, die im Abschnitt **Zertifikat** angezeigt wird.

Nächste Schritte

- Auf der Seite **Certificates** können Sie dies auch Generieren Sie eine Anforderung zum Signieren eines Zertifikats.
- Die Zertifikatinformation ist in drei Registerkarten unterteilt, eine für jede Kategorie. Sie können auf jeder Registerkarte die folgenden Aufgaben ausführen:

Auf dieser Registerkarte…	Sie können folgende Verfahren durchführen…
• Vertrauenswürdige Zertifizierungsstellen*	• [install-trusted-cert] • Löschen einer vertrauenswürdigen Zertifizierungsstelle • Eine vertrauenswürdige Zertifizierungsstelle erneuern
Client/Server-Zertifikate	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
Lokale Zertifikatbehörden	• Erstellen Sie eine neue lokale Zertifizierungsstelle • Unterzeichnen Sie ein Zertifikat mithilfe einer lokalen Zertifizierungsstelle • Lokale Zertifizierungsstelle löschen • Erneuern Sie eine lokale Zertifizierungsstelle

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

Sie können eine Zertifikatsignierungsanforderung (CSR) mit System Manager auf einer beliebigen Registerkarte der Seite **Certificates** generieren. Es werden ein privater Schlüssel und ein entsprechender CSR erzeugt, der mit einer Zertifizierungsstelle signiert werden kann, um ein öffentliches Zertifikat zu generieren.

Schritte

1. Öffnen Sie die Seite **Zertifikate**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie **+CSR erstellen**.
3. Geben Sie die Informationen für den Betreff ein:
   a. Geben Sie einen **gemeinsamen Namen** ein.
   b. Wählen Sie ein **Land** aus.
   c. Geben Sie eine **Organisation** ein.
   d. Geben Sie eine **Organisationseinheit** ein.
4. Wenn Sie die Standardeinstellungen überschreiben möchten, wählen Sie **Weitere Optionen** und geben Sie zusätzliche Informationen ein.

Installieren Sie eine vertrauenswürdige Zertifizierungsstelle (Hinzufügen)

Sie können weitere vertrauenswürdige Zertifizierungsstellen in System Manager installieren.

Schritte

1. Öffnen Sie die Registerkarte * Trusted Certificate Authorities*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie + Add .
3. Führen Sie im Fenster * Vertrauenswürdige Zertifizierungsstelle hinzufügen* folgende Schritte aus:
   - Geben Sie einen **Namen** ein.
   - Wählen Sie für den **Scope** eine Storage-VM aus.
   - Geben Sie einen **gemeinsamen Namen** ein.
   - Wählen Sie einen **Typ** aus.
   - Geben Sie **Zertifikatdetails** ein oder importieren Sie sie.

Löschen einer vertrauenswürdigen Zertifizierungsstelle

Mit System Manager können Sie eine vertrauenswürdige Zertifizierungsstelle löschen.

> Sie können keine vertrauenswürdigen Zertifizierungsstellen löschen, die mit ONTAP vorinstalliert sind.

Schritte

1. Öffnen Sie die Registerkarte * Trusted Certificate Authorities*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der vertrauenswürdigen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ Wählen Sie neben dem Namen **Löschen**.

Eine vertrauenswürdige Zertifizierungsstelle erneuern

Mit System Manager können Sie eine vertrauenswürdige Zertifizierungsstelle erneuern, die abgelaufen ist oder bald abläuft.

Schritte

1. Öffnen Sie die Registerkarte * Trusted Certificate Authorities*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der vertrauenswürdigen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ Neben dem Zertifikatnamen dann **renew**.

Installieren Sie ein Client-/Serverzertifikat (hinzufügen)

Mit System Manager können Sie zusätzliche Client-/Server-Zertifikate installieren.

Schritte

1. Öffnen Sie die Registerkarte **Client/Server Certificates**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie + Add .
3. Führen Sie im Fenster **Client/Server-Zertifikat hinzufügen** folgende Schritte aus:
   - Geben Sie einen **Zertifikatnamen** ein.

- Wählen Sie für den **Scope** eine Storage-VM aus.
- Geben Sie einen **gemeinsamen Namen** ein.
- Wählen Sie einen **Typ** aus.
- Geben Sie **Zertifikatdetails** ein oder importieren Sie sie. Sie können entweder aus einer Textdatei die Zertifikatdetails einschreiben oder kopieren und einfügen oder den Text aus einer Zertifikatdatei importieren, indem Sie auf **Import** klicken.
- Geben Sie den **privaten Schlüssel** ein.
  Sie können entweder aus einer Textdatei den privaten Schlüssel einschreiben oder kopieren und einfügen oder den Text aus einer privaten Schlüsseldatei importieren, indem Sie auf **Import** klicken.

Erstellen (Hinzufügen) eines selbstsignierten Client/Server-Zertifikats

Mit System Manager können Sie zusätzliche selbstsignierte Client-/Server-Zertifikate generieren.

Schritte

1. Öffnen Sie die Registerkarte **Client/Server Certificates**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie **+Selbstsigniertes Zertifikat erstellen**.
3. Führen Sie im Fenster **selbst signiertes Zertifikat generieren** folgende Schritte aus:
   - Geben Sie einen **Zertifikatnamen** ein.
   - Wählen Sie für den **Scope** eine Storage-VM aus.
   - Geben Sie einen **gemeinsamen Namen** ein.
   - Wählen Sie einen **Typ** aus.
   - Wählen Sie eine **Hash-Funktion** aus.
   - Wählen Sie eine * Tastengröße* aus.
   - Wählen Sie eine **Storage-VM** aus.

Löschen Sie ein Client-/Serverzertifikat

Mit System Manager können Sie Client-/Server-Zertifikate löschen.

Schritte

1. Öffnen Sie die Registerkarte **Client/Server Certificates**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen des Client/Server-Zertifikats aus.
3. Wählen Sie ⋮ Klicken Sie neben dem Namen auf **Löschen**.

Erneuern eines Client-/Serverzertifikats

Mit System Manager können Sie ein Client-/Serverzertifikat verlängern, das abgelaufen ist oder kurz vor Ablauf steht.

Schritte

1. Öffnen Sie die Registerkarte **Client/Server Certificates**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen des Client/Server-Zertifikats aus.
3. Wählen Sie ⋮ Klicken Sie neben dem Namen auf **verlängern**.

Erstellen Sie eine neue lokale Zertifizierungsstelle

Mit System Manager können Sie eine neue lokale Zertifizierungsstelle erstellen.

Schritte

1. Öffnen Sie die Registerkarte * Lokale Zertifikatbehörden*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie + Add .
3. Führen Sie im Fenster * Lokale Zertifizierungsstelle hinzufügen* folgende Schritte aus:
   - Geben Sie einen **Namen** ein.
   - Wählen Sie für den **Scope** eine Storage-VM aus.
   - Geben Sie einen **gemeinsamen Namen** ein.
4. Wenn Sie die Standardeinstellungen überschreiben möchten, wählen Sie **Weitere Optionen** und geben Sie zusätzliche Informationen ein.

Unterzeichnen Sie ein Zertifikat mithilfe einer lokalen Zertifizierungsstelle

In System Manager können Sie eine lokale Zertifizierungsstelle zum Signieren eines Zertifikats verwenden.

Schritte

1. Öffnen Sie die Registerkarte * Lokale Zertifikatbehörden*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der lokalen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ Neben dem Namen dann **Zertifikat** signieren.
4. Füllen Sie das Formular **Signieren einer Zertifikatsignierungsanforderung** aus.
   - Sie können entweder den Inhalt der Zertifikatsignierung einfügen oder eine Zertifikatsignierungsanfragedatei importieren, indem Sie auf **Import** klicken.
   - Geben Sie die Anzahl der Tage an, für die das Zertifikat gültig sein soll.

Lokale Zertifizierungsstelle löschen

Mit System Manager können Sie eine lokale Zertifizierungsstelle löschen.

Schritte

1. Öffnen Sie die Registerkarte * Local Certificate Authority*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der lokalen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ Neben dem Namen dann **Löschen**.

Erneuern Sie eine lokale Zertifizierungsstelle

Mit System Manager können Sie eine lokale Zertifizierungsstelle erneuern, die abgelaufen ist oder bald abläuft.

Schritte

1. Öffnen Sie die Registerkarte * Local Certificate Authority*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der lokalen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ Klicken Sie neben dem Namen auf **verlängern**.

Konfigurieren Sie die Active Directory-Domänencontroller-Zugriffsübersicht

Sie müssen AD-Domänencontroller-Zugriff auf das Cluster oder SVM konfigurieren, bevor ein AD-Konto auf die SVM zugreifen kann. Falls Sie bereits einen SMB-Server für eine Daten-SVM konfiguriert haben, können Sie die SVM für einen AD-Zugriff auf das Cluster als Gateway oder „*Tunnel*“ konfigurieren. Wenn Sie keinen SMB-Server konfiguriert haben, können Sie ein Computerkonto für die SVM in der AD-Domäne erstellen.

ONTAP unterstützt die folgenden Authentifizierungsservices für Domänencontroller:

- Kerberos
- LDAP
- Netzanmeldung
- Lokale Sicherheitsbehörde (LSA)

ONTAP unterstützt die folgenden Sitzungsschlüsselalgorithmen für sichere Netlogon-Verbindungen:

Sitzungsschlüsselalgorithmus	Verfügbar ab…
HMAC-SHA256, basierend auf dem Advanced Encryption Standard (AES) Wenn auf dem Cluster ONTAP 9.9.1 oder früher ausgeführt wird und der Domänencontroller AES für sichere Netlogon-Dienste erzwingt, schlägt die Verbindung fehl. In diesem Fall müssen Sie Ihren Domänencontroller neu konfigurieren, um stattdessen starke Schlüsselverbindungen mit ONTAP zu akzeptieren.	ONTAP 9.10.1
DES und HMAC-MD5 (bei festem Schlüssel)	Alle ONTAP 9 Versionen

Wenn Sie AES-Sitzungsschlüssel während der Einrichtung des sicheren Netlogon-Kanals verwenden möchten, müssen Sie überprüfen, ob AES auf Ihrer SVM aktiviert ist.

- Ab ONTAP 9.14.1 ist AES standardmäßig aktiviert, wenn Sie eine SVM erstellen, und Sie müssen die Sicherheitseinstellungen Ihrer SVM nicht ändern, um AES-Sitzungsschlüssel während der Einrichtung des sicheren Netlogon-Kanals zu verwenden.
- In ONTAP 9.10.1 bis 9.13.1 ist AES beim Erstellen einer SVM standardmäßig deaktiviert. Sie müssen AES mit dem folgenden Befehl aktivieren:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

> Beim Upgrade auf ONTAP 9.14.1 oder höher wird die AES-Einstellung für vorhandene SVMs, die mit älteren ONTAP Versionen erstellt wurden, nicht automatisch geändert. Sie müssen den Wert für diese Einstellung immer noch aktualisieren, um AES für diese SVMs zu aktivieren.

Konfigurieren Sie einen Authentifizierungstunnel

Falls Sie bereits einen SMB-Server für eine Daten-SVM konfiguriert haben, können Sie den verwenden `security login domain-tunnel create` Befehl zum Konfigurieren der SVM als Gateway, oder *Tunnel*, für AD-Zugriff auf das Cluster.

Bevor Sie beginnen

- Sie müssen einen SMB-Server für eine Daten-SVM konfiguriert haben.
- Sie müssen ein AD-Domänenbenutzerkonto aktiviert haben, um auf die Admin-SVM für das Cluster zuzugreifen.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Wenn Sie seit ONTAP 9.10.1 über ein SVM-Gateway (Domain-Tunnel) für AD-Zugriff verfügen, können Sie Kerberos für die Admin-Authentifizierung verwenden, wenn Sie NTLM in Ihrer AD-Domäne deaktiviert haben. In früheren Versionen wurde Kerberos mit der Admin-Authentifizierung für SVM Gateways nicht unterstützt. Diese Funktion ist standardmäßig verfügbar; keine Konfiguration erforderlich.

> Kerberos-Authentifizierung wird immer zuerst versucht. Bei einem Fehler wird dann versucht, die NTLM-Authentifizierung zu aktivieren.

Schritt

1. Konfigurieren Sie eine SMB-fähige Daten-SVM als Authentifizierungstunnel für AD-Domänencontroller-Zugriff auf das Cluster:

   `security login domain-tunnel create -vserver svm_name`

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   > Die SVM muss ausgeführt werden, damit der Benutzer authentifiziert werden kann.

   Mit dem folgenden Befehl wird die SMB-fähige Daten-SVM „`engData`“ als Authentifizierungstunnel konfiguriert.

   ```
   cluster1::>security login domain-tunnel create -vserver engData
   ```

Erstellen Sie ein SVM-Computerkonto in der Domäne

Falls Sie noch keinen SMB-Server für eine Daten-SVM konfiguriert haben, können Sie den verwenden `vserver active-directory create` Befehl zum Erstellen eines Computerkontos für die SVM in der Domäne.

Über diese Aufgabe

Nach der Eingabe des `vserver active-directory create` Befehl, Sie werden aufgefordert, die Anmeldeinformationen für ein AD-Benutzerkonto mit ausreichenden Berechtigungen bereitzustellen, um der angegebenen Organisationseinheit in der Domäne Computer hinzuzufügen. Das Passwort des Kontos darf nicht leer sein.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritt

1. Erstellen eines Computerkontos für eine SVM in der AD-Domäne:

   `vserver active-directory create -vserver` *`SVM_name`* `-account-name` *`NetBIOS_account_name`* `-domain` *`domain`* `-ou` *`organizational_unit`*

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Mit dem folgenden Befehl wird ein Computerkonto mit dem Namen „`ADSERVER1`“ in der Domäne „`example.com`" für SVM "`engData`“ erstellt. Sie werden nach Eingabe des Befehls zur Eingabe der Anmeldedaten für das AD-Benutzerkonto aufgefordert.

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

Konfigurieren Sie die Übersicht über den Zugriff auf LDAP- oder NIS-Server

Sie müssen den LDAP- oder NIS-Serverzugriff auf eine SVM konfigurieren, bevor LDAP- oder NIS-Konten auf die SVM zugreifen können. Mit der Switch-Funktion können Sie LDAP oder NIS als alternative Namensdienstquellen verwenden.

Konfigurieren Sie den LDAP-Serverzugriff

Sie müssen den LDAP-Serverzugriff auf eine SVM konfigurieren, bevor LDAP-Konten auf die SVM zugreifen können. Sie können das verwenden `vserver services name-service ldap client create` Befehl zum Erstellen einer LDAP-Client-Konfiguration auf der SVM. Anschließend können Sie die verwenden `vserver services name-service ldap create` Befehl zum Zuordnen der LDAP-Client-Konfiguration zur SVM.

Über diese Aufgabe

Die meisten LDAP-Server können die von ONTAP bereitgestellten Standardschemata verwenden:

- MS-AD-bis (das bevorzugte Schema für die meisten Windows 2012- und späteren AD-Server)
- AD-IDMU (AD-Server Windows 2008, Windows 2016 und höher)
- AD-SFU (Windows 2003 und frühere AD-Server)
- RFC-2307 (UNIX LDAP-SERVER)

Es empfiehlt sich, die Standardschemata zu verwenden, es sei denn, es ist eine andere Voraussetzung zu tun. In diesem Fall können Sie ein eigenes Schema erstellen, indem Sie ein Standardschema kopieren und die

Kopie ändern. Weitere Informationen finden Sie unter:

- "NFS-Konfiguration"
- "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP"

Bevor Sie beginnen

- Sie müssen ein installiert haben "DIGITALES Zertifikat für DEN CA-signierten Server" Auf der SVM.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. LDAP-Client-Konfiguration auf einer SVM erstellen:

   `vserver services name-service ldap client create -vserver` *`SVM_name`* `-client -config` *`client_configuration`* `-servers` *`LDAP_server_IPs`* `-schema` *`schema`* `-use -start-tls true|false`

   > Start TLS wird nur für den Zugriff auf Data SVMs unterstützt. Der Zugriff auf Admin-SVMs wird nicht unterstützt.

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Mit dem folgenden Befehl wird eine LDAP-Client-Konfiguration mit dem Namen „`corp`“ auf SVM „ `engData`“ erstellt. Der Client bindet mit den IP-Adressen 172.160.0.100 und 172.16.0.101 anonymisiert an die LDAP-Server. Der Client verwendet das RFC-2307-Schema, um LDAP-Abfragen zu erstellen. Die Kommunikation zwischen Client und Server wird über Start TLS verschlüsselt.

   ```
   cluster1::> vserver services name-service ldap client create
   -vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
   -schema RFC-2307 -use-start-tls true
   ```

   > Ab ONTAP 9.2 Field Portal `-ldap-servers` Ersetzt das Feld `-servers`. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server verwenden.

2. Verbinden Sie die LDAP-Client-Konfiguration mit der SVM: `vserver services name-service ldap create -vserver` *`SVM_name`* `-client-config` *`client_configuration`* `-client-enabled true|false`

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Mit dem folgenden Befehl wird die LDAP-Client-Konfiguration zugeordnet `corp` Mit der SVM `engData`, Und aktiviert den LDAP-Client auf der SVM.

   ```
   cluster1::>vserver services name-service ldap create -vserver engData
   -client-config corp -client-enabled true
   ```

> Ab ONTAP 9.2 beginnt der `vserver services name-service ldap create` Der Befehl führt eine automatische Konfigurationsvalidierung durch und meldet eine Fehlermeldung, wenn ONTAP den Namensserver nicht kontaktieren kann.

3. Überprüfen Sie den Status der Namensserver mithilfe des LDAP-Prüfbefehls vserver Services Name-Service.

   Mit dem folgenden Befehl werden LDAP-Server auf der SVM vs0 validiert.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

   Der Befehl Name Service Check ist ab ONTAP 9.2 verfügbar.

Konfigurieren Sie den NIS-Serverzugriff

Sie müssen den NIS-Serverzugriff auf eine SVM konfigurieren, bevor NIS-Konten auf die SVM zugreifen können. Sie können das verwenden `vserver services name-service nis-domain create` Befehl zum Erstellen einer NIS-Domänenkonfiguration auf einer SVM.

Über diese Aufgabe

Sie können mehrere NIS-Domänen erstellen. Es kann nur eine NIS-Domäne festgelegt werden `active` Zu einer Zeit.

Bevor Sie beginnen

- Alle konfigurierten Server müssen verfügbar und zugänglich sein, bevor Sie die NIS-Domäne auf der SVM konfigurieren.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritt

1. Erstellen einer NIS-Domänenkonfiguration auf einer SVM:

   `vserver services name-service nis-domain create -vserver` *`SVM_name`* `-domain client_configuration -active true|false -nis-servers` *`NIS_server_IPs`*

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   > Ab ONTAP 9.2 Field Portal `-nis-servers` Ersetzt das Feld `-servers`. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server enthalten.

   Mit dem folgenden Befehl wird eine NIS-Domänenkonfiguration auf SVM „`engData`“ erstellt. Die NIS-Domäne `nisdomain` Ist bei der Erstellung aktiv und kommuniziert mit einem NIS-Server mit der IP-Adresse 192.0.2.180.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

Erstellen Sie einen Namensdienstschalter

Mit der Namensdienst-Switch-Funktion können Sie LDAP oder NIS als alternative Namensdienstquellen verwenden. Sie können das verwenden `vserver services name-service ns-switch modify` Befehl zum Festlegen der Reihenfolge für Name-Service-Quellen.

Bevor Sie beginnen

- Sie müssen LDAP- und NIS-Serverzugriff konfiguriert haben.
- Um diese Aufgabe auszuführen, müssen Sie ein Cluster-Administrator oder SVM-Administrator sein.

Schritt

1. Geben Sie die Suchreihenfolge für Namensdienstquellen an:

   `vserver services name-service ns-switch modify -vserver` *`SVM_name`* `-database` *`name_service_switch_database`* `-sources` *`name_service_source_order`*

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Der folgende Befehl gibt die Suchreihenfolge der LDAP- und NIS-Namensservice-Quellen für die Datenbank „`passwd`“ auf SVM „`engData`“ an.

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

Ändern Sie ein Administratorpasswort

Sie sollten Ihr Anfangspasswort sofort nach der ersten Anmeldung am System ändern. Als SVM-Administrator können Sie die verwenden `security login password` Befehl zum Ändern Ihres eigenen Passworts. Als Cluster-Administrator können Sie das verwenden `security login password` Befehl zum Ändern des Administratorkennworts.

Über diese Aufgabe

Das neue Passwort muss folgende Bedingungen erfüllen:

- Er darf den Benutzernamen nicht enthalten
- Sie muss mindestens acht Zeichen lang sein
- Sie muss mindestens einen Buchstaben und eine Ziffer enthalten
- Es darf nicht mit den letzten sechs Kennwörtern identisch sein

Sie können das verwenden `security login role config modify` Befehl zum Ändern der Kennwortregeln für Konten, die einer bestimmten Rolle zugeordnet sind. Weitere Informationen finden Sie im "Befehlsreferenz".

Bevor Sie beginnen

- Zum Ändern des eigenen Passworts müssen Sie ein Cluster- oder SVM-Administrator sein.
- Sie müssen ein Cluster-Administrator sein, um das Passwort eines anderen Administrators zu ändern.

Schritt

1. Ändern eines Administratorkennworts: `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   Mit dem folgenden Befehl wird das Passwort des Administrators geändert `admin1` Für die SVM`vs1.example.com`. Sie werden aufgefordert, das aktuelle Passwort einzugeben, dann das neue Passwort einzugeben und erneut einzugeben.

   ```
   vs1.example.com::>security login password -vserver engData -username
   admin1
   Please enter your current password:
   Please enter a new password:
   Please enter it again:
   ```

Sperren und Entsperren eines Administratorkontos

Sie können das verwenden `security login lock` Befehl zum Sperren eines Administratorkontos und des `security login unlock` Befehl zum Entsperren des Kontos.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgaben auszuführen.

Schritte

1. Administratorkonto sperren:

   ```
   security login lock -vserver SVM_name -username user_name
   ```

   Mit dem folgenden Befehl wird das Administratorkonto gesperrt `admin1` Für die SVM `vs1.example.com`:

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```

2. Administratorkonto entsperren:

   ```
   security login unlock -vserver SVM_name -username user_name
   ```

   Mit dem folgenden Befehl wird das Administratorkonto freigeschaltet `admin1` Für die SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

Fehlgeschlagene Anmeldeversuche verwalten

Wiederholt fehlgeschlagene Anmeldeversuche weisen manchmal darauf hin, dass ein Eindringling versucht, auf das Speichersystem zuzugreifen. Sie können eine Reihe von Maßnahmen ergreifen, um sicherzustellen, dass kein Einbruch stattfindet.

Wie Sie wissen, dass Anmeldeversuche fehlgeschlagen sind

Das Event Management System (EMS) informiert Sie jede Stunde über fehlgeschlagene Anmeldeversuche. Im finden Sie eine Aufzeichnung fehlgeschlagener Anmeldeversuche `audit.log` Datei:

Was tun, wenn wiederholte Anmeldeversuche fehlschlagen

Kurzfristig können Sie eine Reihe von Maßnahmen ergreifen, um Einbrüche zu verhindern:

- Kennwörter müssen aus einer Mindestanzahl von Groß-/Kleinschreibung, Kleinbuchstaben, Sonderzeichen und/oder Ziffern bestehen
- Legen Sie nach einem fehlgeschlagenen Anmeldeversuch eine Verzögerung fest
- Begrenzen Sie die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche und sperren Sie Benutzer nach der angegebenen Anzahl fehlgeschlagener Versuche
- Verfallen und sperren Sie Konten, die für eine bestimmte Anzahl von Tagen inaktiv sind

Sie können das verwenden `security login role config modify` Befehl zum Ausführen dieser Aufgaben.

Langfristig können Sie die folgenden zusätzlichen Schritte einleiten:

- Verwenden Sie die `security ssh modify` Befehl, um die Anzahl fehlgeschlagener Anmeldeversuche für alle neu erstellten SVMs zu begrenzen.
- Migrieren Sie vorhandene MD5-Algorithmus-Konten in den sichereren SHA-512-Algorithmus, indem Sie Benutzer dazu auffordern, ihre Passwörter zu ändern.

SHA-2 für Passwörter für Administratorkonten erzwingen

Vor ONTAP 9.0 erstellte Administratorkonten verwenden nach dem Upgrade weiterhin MD5-Passwörter, bis die Passwörter manuell geändert werden. MD5 ist weniger sicher als SHA-2. Daher sollten Sie nach dem Upgrade Benutzer von MD5-Konten auffordern, ihre Passwörter zu ändern, um die Standard-SHA-512-Hash-Funktion zu verwenden.

Über diese Aufgabe

Mit der Passwort-Hash-Funktion können Sie Folgendes tun:

- Zeigt Benutzerkonten an, die mit der angegebenen Hash-Funktion übereinstimmen.
- Verfallen von Konten, die eine angegebene Hash-Funktion verwenden (z. B. MD5), sodass die Benutzer ihre Passwörter bei der nächsten Anmeldung ändern müssen.

- Konten sperren, deren Passwörter die angegebene Hash-Funktion verwenden.
- Wenn Sie auf eine Version vor ONTAP 9 zurücksetzen, setzen Sie das Kennwort des Clusteradministrators zurück, damit es mit der Hash-Funktion (MD5) kompatibel ist, die von der früheren Version unterstützt wird.

ONTAP akzeptiert vorgehashte SHA-2-Passwörter nur unter Verwendung des NetApp Manageability SDK (`security-login-create` Und `security-login-modify-password`).

Schritte

1. Migrieren Sie die MD5-Administratorkonten auf die SHA-512-Passwort-Hash-Funktion:
   a. Alle MD5-Administratorkonten verfallen: `security login expire-password -vserver * -username * -hash-function md5`

      Dadurch werden MD5-Kontobenutzer gezwungen, ihre Passwörter bei der nächsten Anmeldung zu ändern.

   b. Benutzer von MD5-Konten bitten, sich über eine Konsole oder SSH-Sitzung anzumelden.

      Das System erkennt, dass die Konten abgelaufen sind, und fordert Benutzer auf, ihre Passwörter zu ändern. SHA-512 wird standardmäßig für die geänderten Passwörter verwendet.

2. Bei MD5-Konten, deren Benutzer sich nicht anmelden, um ihre Passwörter innerhalb eines bestimmten Zeitraums zu ändern, erzwingen Sie die Kontomigration:
   a. Konten sperren, die weiterhin die MD5-Hash-Funktion verwenden (erweiterte Berechtigungsebene): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

      Nach der von angegebenen Anzahl von Tagen `-lock-after`, Benutzer können nicht auf ihre MD5-Konten zugreifen.

   b. Entsperren Sie die Konten, wenn die Benutzer bereit sind, ihre Passwörter zu ändern: `security login unlock -vserver` *`svm_name`* `-username` *`user_name`*
   c. Benutzer müssen sich über eine Konsole oder SSH-Sitzung bei ihren Konten anmelden und ihre Passwörter ändern, wenn das System sie dazu auffordert.

Diagnostizieren und korrigieren Sie Probleme mit dem Dateizugriff

Schritte

1. Wählen Sie in System Manager **Storage > Storage VMs** aus.
2. Wählen Sie die Speicher-VM aus, auf der Sie eine Ablaufverfolgung durchführen möchten.
3. Klicken Sie Auf ⋮ **Mehr**.
4. Klicken Sie Auf **Trace File Access**.
5. Geben Sie den Benutzernamen und die IP-Adresse des Clients an, und klicken Sie dann auf **Tracing starten**.

   Die Trace-Ergebnisse werden in einer Tabelle angezeigt. Die Spalte **Gründe** gibt den Grund, warum auf eine Datei nicht zugegriffen werden konnte.

6. Klicken Sie Auf ⌄ In der linken Spalte der Ergebnistabelle können Sie die Zugriffsrechte für den Dateizugriff anzeigen.

Management der Verifizierung von mehreren Administratoren

Übersicht über die Verifizierung mit mehreren Administratoren

Ab ONTAP 9.11.1 können Sie die Überprüfung durch mehrere Administratoren (Multi-Admin Verification, MAV) verwenden, um sicherzustellen, dass bestimmte Vorgänge, wie das Löschen von Volumes oder Snapshot Kopien, nur nach Genehmigung von zugewiesenen Administratoren ausgeführt werden können. So werden gefährdete, böswillige oder unerfahrene Administratoren daran gehindert, unerwünschte Änderungen vorzunehmen oder Daten zu löschen.

Die Konfiguration der Prüfung für mehrere Administratoren umfasst:

- "Erstellen einer oder mehrerer Genehmigungsgruppen für Administratoren"
- "Aktivieren der Überprüfungsfunktion für mehrere Administratoren"
- "Hinzufügen oder Ändern von Regeln"

Nach der Erstkonfiguration können diese Elemente nur von Administratoren in einer MAV-Genehmigungsgruppe (MAV-Administratoren) geändert werden.

Wenn die Überprüfung durch mehrere Administratoren aktiviert ist, sind für jeden geschützten Vorgang drei Schritte erforderlich:

- Wenn ein Benutzer den Vorgang initiiert, A "Die Anforderung wird generiert."
- Bevor es ausgeführt werden kann, mindestens eine "MAV-Administrator muss genehmigen."
- Nach der Genehmigung schließt der Benutzer den Vorgang ab.

Die Überprüfung durch mehrere Administratoren ist nicht für Volumes oder Workflows gedacht, die mit hoher Automatisierung arbeiten, da jede automatisierte Aufgabe vor Abschluss des Vorgangs eine Genehmigung erfordert. Wenn Sie Automation und MAV gemeinsam nutzen möchten, empfiehlt es sich, Abfragen für bestimmte MAV-Operationen zu verwenden. So können Sie sich beispielsweise bewerben `volume delete` MAV regiert nur zu Volumes, in denen keine Automatisierung beteiligt ist, und Sie können die Volumes mit einem bestimmten Benennungsschema benennen.

> Wenn Sie die Verifizierungsfunktion mehrerer Administratoren ohne Genehmigung eines MAV-Administrators deaktivieren müssen, wenden Sie sich an den NetApp Support und erwähnen Sie den folgenden Knowledge Base-Artikel: "So deaktivieren Sie die Multi-Admin-Überprüfung, wenn MAV-Admin nicht verfügbar ist".

Funktionsweise der Multiadmin-Überprüfung

Die Überprüfung durch mehrere Administratoren umfasst:

- Eine Gruppe von einem oder mehreren Administratoren mit Genehmigung und Veto-Befugnissen.
- Eine Reihe von geschützten Operationen oder Befehlen in einer Tabelle *rules*.
- Eine *rules Engine* zur Identifizierung und Steuerung der Ausführung geschützter Vorgänge.

MAV-Regeln werden nach rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) evaluiert. Daher müssen Administratoren, die einen geschützten Betrieb ausführen oder genehmigen, bereits die minimalen RBAC-Rechte für diese Vorgänge besitzen. "Erfahren Sie mehr über RBAC."

Systemdefinierte Regeln

Wenn die Multi-Admin-Überprüfung aktiviert ist, werden durch systemdefinierte Regeln (auch bekannt als *guard-Rail*-Regeln) eine Reihe von MAV-Operationen festgelegt, die das Risiko enthalten, den MAV-Prozess selbst zu umgehen. Diese Vorgänge können nicht aus der Regeltabelle entfernt werden. Wenn MAV aktiviert ist, müssen Operationen, die durch ein Sternchen (*) gekennzeichnet sind, vor der Ausführung von einem oder mehreren Administratoren genehmigt werden, mit Ausnahme von **show**-Befehlen.

- `security multi-admin-verify modify` Betrieb*

  Steuert die Konfiguration der Verifizierungsfunktion für mehrere Administratoren.

- `security multi-admin-verify approval-group` Betrieb*

  Steuern Sie die Mitgliedschaft im Administratorensatz mit Anmeldeinformationen für die Überprüfung mehrerer Administratoren.

- `security multi-admin-verify rule` Betrieb*

  Steuern Sie die Befehlssatz, für die eine Multi-Admin-Überprüfung erforderlich ist.

- `security multi-admin-verify request` Betrieb

  Kontrollieren Sie den Genehmigungsprozess.

Regelgeschützte Befehle

Zusätzlich zu den systemdefinierten Befehlen sind die folgenden Befehle standardmäßig geschützt, wenn die Multi-Admin-Überprüfung aktiviert ist. Sie können jedoch die Regeln ändern, um den Schutz für diese Befehle zu entfernen.

- `security login password`
- `security login unlock`
- `set`

Die folgenden Befehle können in ONTAP 9.11.1 und neueren Versionen gesichert werden.

`cluster peer delete`	`volume snapshot autodelete modify`
`event config modify`	`volume snapshot delete`
`security login create`	`volume snapshot policy add-schedule`
`security login delete`	`volume snapshot policy create`
`security login modify`	`volume snapshot policy delete`
`system node run`	`volume snapshot policy modify`
`system node systemshell`	`volume snapshot policy modify-schedule`
`volume delete`	`volume snapshot policy remove-schedule`
`volume flexcache delete`	`volume snapshot restore`
	`vserver peer delete`

Die folgenden Befehle können ab ONTAP 9.13.1 geschützt werden:

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

Die folgenden Befehle können ab ONTAP 9.14.1 geschützt werden:

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

Funktionsweise der Multi-Admin-Genehmigung

Jedes Mal, wenn ein geschützter Vorgang in einem MAV-geschützten Cluster eingegeben wird, wird eine Anfrage zur Ausführung des Vorgangs an die entsprechende MAV-Administratorgruppe gesendet.

Sie können Folgendes konfigurieren:

- Die Namen, Kontaktinformationen und die Anzahl der Administratoren in der MAV-Gruppe.

  Ein MAV-Administrator sollte über eine RBAC-Rolle mit Cluster-Administratorrechten verfügen.

- Die Anzahl der MAV-Administratorgruppen.
  - Für jede Schutzregel wird eine MAV-Gruppe zugewiesen.

    - Für mehrere MAV-Gruppen können Sie konfigurieren, welche MAV-Gruppe eine bestimmte Regel genehmigt.
- Die Anzahl der erforderlichen MAV-Genehmigungen für die Ausführung eines geschützten Vorgangs.
- Eine Ablauffrist *Genehmigung*, innerhalb derer ein MAV-Administrator auf eine Genehmigungsanfrage antworten muss.
- Eine Ablauffrist *Ausführung*, innerhalb derer der anfragende Administrator den Vorgang abschließen muss.

Sobald diese Parameter konfiguriert sind, muss die MAV-Genehmigung geändert werden.

MAV-Administratoren können ihre eigenen Anforderungen zur Ausführung von geschützten Vorgängen nicht genehmigen. Daher:

- MAV sollte nicht auf Clustern mit nur einem Administrator aktiviert werden.
- Wenn sich nur eine Person in der MAV-Gruppe befindet, kann der MAV-Administrator keine geschützten Vorgänge aufrufen. Regelmäßige Administratoren müssen diese eingeben und der MAV-Administrator kann nur genehmigen.
- Wenn Sie möchten, dass MAV-Administratoren geschützte Vorgänge ausführen können, muss die Anzahl der MAV-Administratoren größer sein als die Anzahl der erforderlichen Genehmigungen. Wenn zum Beispiel zwei Genehmigungen für einen geschützten Vorgang erforderlich sind und Sie möchten, dass MAV-Administratoren diese ausführen, müssen sich drei Personen in der Gruppe MAV-Administratoren befinden.

MAV-Administratoren können Genehmigungsanfragen in E-Mail-Benachrichtigungen (über EMS) erhalten oder die Anforderungswarteschlange abfragen. Wenn sie eine Anfrage erhalten, können sie eine von drei Aktionen durchführen:

- Genehmigen
- Ablehnen (Veto)
- Ignorieren (keine Aktion)

E-Mail-Benachrichtigungen werden an alle Genehmiger gesendet, die einer MAV-Regel zugeordnet sind, wenn:

- Eine Anfrage wird erstellt.
- Ein Antrag ist genehmigt oder ein Veto eingelegt.
- Eine genehmigte Anfrage wird ausgeführt.

Wenn sich der Anforderer in derselben Genehmigungsgruppe für den Vorgang befindet, wird er eine E-Mail erhalten, wenn seine Anfrage genehmigt wird.

Hinweis: ein Antragsteller kann seine eigenen Anfragen nicht genehmigen, auch wenn er sich in der Genehmigungsgruppe befindet. Aber sie können die E-Mail-Benachrichtigungen erhalten. Anfragesteller, die sich nicht in Genehmigungsgruppen befinden (d. h. nicht MAV-Administratoren), erhalten keine E-Mail-Benachrichtigungen.

Funktionsweise der geschützten Operation

Wenn die Ausführung für einen geschützten Vorgang genehmigt wird, wird der anfragende Benutzer mit der Operation fortgesetzt, wenn er dazu aufgefordert wird. Wenn der Vorgang ein Vetos hat, muss der anfordernde Benutzer die Anfrage löschen, bevor er fortfahren kann.

MAV-Regeln werden nach RBAC-Berechtigungen evaluiert. Dadurch kann ein Benutzer ohne ausreichende RBAC-Berechtigungen für die Ausführung des Vorgangs den MAV-Anforderungsprozess nicht initiieren.

Management von Genehmigungsgruppen für Administratoren

Bevor Sie die MAV (Multi-Administrator Verification) aktivieren, müssen Sie eine Admin-Genehmigungsgruppe erstellen, die einen oder mehrere Administratoren enthält, die eine Genehmigung oder Veto-Berechtigung erhalten. Sobald Sie die Überprüfung mehrerer Administratoren aktiviert haben, müssen alle Änderungen an der Mitgliedschaft in der Genehmigungsgruppe von einem der vorhandenen qualifizierten Administratoren genehmigt werden.

Über diese Aufgabe

Sie können vorhandene Administratoren einer MAV-Gruppe hinzufügen oder neue Administratoren erstellen.

Die MAV-Funktionalität berücksichtigt vorhandene rollenbasierte RBAC-Einstellungen (Access Control, RBAC). Potenzielle MAV-Administratoren müssen über ausreichende Berechtigungen verfügen, um geschützte Vorgänge auszuführen, bevor sie zu MAV-Administratorgruppen hinzugefügt werden. "Erfahren Sie mehr über RBAC."

Sie können MAV so konfigurieren, dass MAV-Administratoren darauf aufmerksam gemacht werden, dass Genehmigungsanforderungen ausstehen. Dazu müssen Sie E-Mail-Benachrichtigungen konfigurieren, insbesondere die `Mail From` Und `Mail Server` Parameter—oder Sie können diese Parameter löschen, um die Benachrichtigung zu deaktivieren. Ohne E-Mail-Warnmeldungen müssen MAV-Administratoren die Genehmigungswarteschlange manuell prüfen.

System Manager Verfahren

Wenn Sie zum ersten Mal eine MAV-Genehmigungsgruppe erstellen möchten, lesen Sie das Verfahren zu System Manager nach "Aktivieren Sie die Verifizierung für mehrere Administratoren."

So ändern Sie eine vorhandene Genehmigungsgruppe oder erstellen eine zusätzliche Genehmigungsgruppe:

1. Identifizieren Sie die Administratoren, die eine Überprüfung durch mehrere Administratoren erhalten.
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie Auf → Neben **Benutzer und Rollen.**
   c. Klicken Sie Auf + Add Unter **Benutzer.**
   d. Ändern Sie den Dienstplan nach Bedarf.

      Weitere Informationen finden Sie unter "Kontrolle des Administratorzugriffs"

2. Erstellen oder Ändern der MAV-Genehmigungsgruppe:
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie Auf → Neben **Multi-Admin-Genehmigung** im Abschnitt **Sicherheit**. (Sie sehen die ⚙ Symbol, wenn MAV noch nicht konfiguriert ist.)
      - Name: Geben Sie einen Gruppennamen ein.
      - Genehmiger: Wählen Sie Genehmiger aus einer Benutzerliste aus.
      - E-Mail-Adresse: E-Mail-Adresse(n) eingeben.

- Standardgruppe: Wählen Sie eine Gruppe aus.

Eine MAV-Genehmigung ist erforderlich, um eine vorhandene Konfiguration zu bearbeiten, sobald MAV aktiviert ist.

CLI-Verfahren

1. Überprüfen Sie, ob die Werte für die festgelegt wurden `Mail From` Und `Mail Server` Parameter. Geben Sie Ein:

   ```
   event config show
   ```

   Die Anzeige sollte wie folgt lauten:

   ```
   cluster01::> event config show
                              Mail From:  admin@localhost
                            Mail Server:  localhost
                              Proxy URL:  -
                             Proxy User:  -
    Publish/Subscribe Messaging Enabled:  true
   ```

   Um diese Parameter zu konfigurieren, geben Sie Folgendes ein:

   ```
   event config modify -mail-from email_address -mail-server server_name
   ```

2. Identifizieren Sie die Administratoren, die eine Überprüfung durch mehrere Administratoren erhalten

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Zeigen Sie aktuelle Administratoren an	`security login show`
Ändern der Anmeldeinformationen aktueller Administratoren	`security login modify <parameters>`
Erstellen neuer Administratorkonten	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

3. Erstellen Sie die MAV-Genehmigungsgruppe:

   ```
   security multi-admin-verify approval-group create [ -vserver svm_name] -name
   group_name -approvers approver1[,approver2…] [[-email address1], address1…]
   ```

   - `-vserver` - Nur die Administrator-SVM wird in diesem Release unterstützt.
   - `-name` - Der MAV-Gruppenname, bis zu 64 Zeichen.
   - `-approvers` - Die Liste eines oder mehrerer Genehmiger.
   - `-email` - Eine oder mehrere E-Mail-Adressen, die benachrichtigt werden, wenn eine Anfrage erstellt, genehmigt, ein Veto eingelegt oder ausgeführt wird.

Beispiel: mit dem folgenden Befehl wird eine MAV-Gruppe mit zwei Mitgliedern und zugehörigen E-Mail-Adressen erstellt.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. Gruppenerstellung und -Mitgliedschaft überprüfen:

   `security multi-admin-verify approval-group show`

   Beispiel:

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name        Approvers        Email
-------  ---------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      email
pavan@myfirm.com,julia@myfirm.com
```

Verwenden Sie diese Befehle, um Ihre ursprüngliche MAV-Gruppenkonfiguration zu ändern.

Hinweis: Alle erfordern eine Genehmigung des MAV-Administrators vor der Ausführung.

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Ändern Sie die Gruppeneigenschaften, oder ändern Sie vorhandene Mitgliedsinformationen	`security multi-admin-verify approval-group modify [`*`parameters`*`]`
Mitglieder hinzufügen oder entfernen	`security multi-admin-verify approval-group replace [-vserver` *`svm_name`*`] -name` *`group_name`* `[-approvers-to-add` *`approver1`*`[,`*`approver2`*`…]][-approvers-to-remove` *`approver1`*`[,`*`approver2`*`…]]`
Gruppe löschen	`security multi-admin-verify approval-group delete [-vserver` *`svm_name`*`] -name` *`group_name`*

Aktivieren und Deaktivieren der Verifizierung von mehreren Administratoren

Multi-Admin-Verifizierung (MAV) muss explizit aktiviert werden. Sobald Sie die Überprüfung durch mehrere Administratoren aktiviert haben, muss die Genehmigung durch Administratoren in einer MAV-Genehmigungsgruppe (MAV-Administratoren) gelöscht werden.

Über diese Aufgabe

Wenn MAV aktiviert ist, muss MAV durch Ändern oder Deaktivieren der MAV-Administratorfreigabe genehmigt werden.

> Wenn Sie die Verifizierungsfunktion mehrerer Administratoren ohne Genehmigung eines MAV-Administrators deaktivieren müssen, wenden Sie sich an den NetApp Support und erwähnen Sie den folgenden Knowledge Base-Artikel: "So deaktivieren Sie die Multi-Admin-Überprüfung, wenn MAV-Admin nicht verfügbar ist".

Wenn Sie MAV aktivieren, können Sie global die folgenden Parameter angeben.

Genehmigungsgruppen

Eine Liste globaler Genehmigungsgruppen. Um die MAV-Funktionalität zu aktivieren, ist mindestens eine Gruppe erforderlich.

> Wenn Sie MAV mit Autonomous Ransomware Protection (ARP) verwenden, definieren Sie eine neue oder vorhandene Genehmigungsgruppe, die für die Genehmigung von ARP-Pause, Deaktivierung und Löschen von verdächtigen Anforderungen verantwortlich ist.

Erforderliche Genehmiger

Die Anzahl der Genehmiger, die für die Ausführung eines geschützten Vorgangs erforderlich sind. Die Standard- und die Mindestzahl ist 1.

> Die erforderliche Anzahl von Genehmigern muss geringer sein als die Gesamtzahl der eindeutigen Genehmiger in den standardmäßigen Genehmigungsgruppen.

Ablauf der Genehmigung (Stunden, Minuten, Sekunden)

Der Zeitraum, innerhalb dessen ein MAV-Administrator auf eine Genehmigungsanforderung reagieren muss. Der Standardwert ist eine Stunde (1 h), der unterstützte Mindestwert beträgt eine Sekunde (1 s) und der maximal unterstützte Wert beträgt 14 Tage (14d).

Ausführungsablauf (Stunden, Minuten, Sekunden)

Der Zeitraum, in dem der anfragende Administrator den Vorgang: Abschließen muss. Der Standardwert ist eine Stunde (1 h), der unterstützte Mindestwert beträgt eine Sekunde (1 s) und der maximal unterstützte Wert beträgt 14 Tage (14d).

Sie können diese Parameter auch für bestimmte Parameter überschreiben "Betriebsregeln."

System Manager Verfahren

1. Identifizieren Sie die Administratoren, die eine Überprüfung durch mehrere Administratoren erhalten.
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie Auf → Neben **Benutzer und Rollen.**
   c. Klicken Sie Auf + Add Unter **Benutzer.**
   d. Ändern Sie den Dienstplan nach Bedarf.

      Weitere Informationen finden Sie unter "Kontrolle des Administratorzugriffs"

2. Aktivieren Sie die Überprüfung durch mehrere Administratoren, indem Sie mindestens eine Genehmigungsgruppe erstellen und mindestens eine Regel hinzufügen.
   a. Klicken Sie Auf **Cluster > Einstellungen.**

b. Klicken Sie Auf ⚙ Neben **Multi-Admin-Genehmigung** im Abschnitt **Sicherheit**.

c. Klicken Sie Auf + Add Um mindestens eine Genehmigungsgruppe hinzuzufügen.

   - Name – Geben Sie einen Gruppennamen ein.
   - Genehmiger – Wählen Sie Genehmiger aus einer Benutzerliste aus.
   - E-Mail-Adresse – Geben Sie die E-Mail-Adresse(n) ein.
   - Standardgruppe – Wählen Sie eine Gruppe aus.

d. Fügen Sie mindestens eine Regel hinzu.

   - Operation – Wählen Sie einen unterstützten Befehl aus der Liste aus.
   - Abfrage – Geben Sie alle gewünschten Befehlsoptionen und Werte ein.
   - Optionale Parameter; lassen Sie leer, um globale Einstellungen anzuwenden, oder weisen Sie einen anderen Wert für bestimmte Regeln zu, um die globalen Einstellungen zu überschreiben.
     - Erforderliche Anzahl an Genehmigern
     - Genehmigungsgruppen

e. Klicken Sie auf **Erweiterte Einstellungen**, um die Standardeinstellungen anzuzeigen oder zu ändern.

   - Erforderliche Anzahl an Genehmigern (Standard: 1)
   - Ablauf der Testsuite (Standard: 1 Stunde)
   - Ablauf der Genehmigungsanforderung (Standard: 1 Stunde)
   - E-Mail-Server*
   - Von E-Mail-Adresse*

   *Diese aktualisieren die unter "Benachrichtigungsverwaltung" verwalteten E-Mail-Einstellungen. Sie werden aufgefordert, sie einzustellen, wenn sie noch nicht konfiguriert wurden.

f. Klicken Sie auf **Aktivieren**, um die Erstkonfiguration von MAV abzuschließen.

Nach der Erstkonfiguration wird der aktuelle MAV-Status in der Kachel **Multi-Admin Approval** angezeigt.

- Status (aktiviert oder nicht)
- Aktive Vorgänge, für die Genehmigungen erforderlich sind
- Anzahl der offenen Anfragen im Status „ausstehend“

Sie können eine vorhandene Konfiguration anzeigen, indem Sie auf klicken →. Zum Bearbeiten einer vorhandenen Konfiguration ist eine MAV-Genehmigung erforderlich.

So deaktivieren Sie die Multi-Admin-Verifizierung:

1. Klicken Sie Auf **Cluster > Einstellungen.**
2. Klicken Sie Auf ⚙ Neben **Multi-Admin-Genehmigung** im Abschnitt **Sicherheit**.
3. Klicken Sie auf die Schaltfläche zum Wechseln aktiviert.

   Zum Abschluss dieses Vorgangs ist eine MAV-Genehmigung erforderlich.

CLI-Verfahren

Bevor Sie MAV-Funktionalität in der CLI aktivieren, ist mindestens eine davon "MAV-Administratorgruppe" Muss erstellt worden sein.

Wenn Sie… wollen	Geben Sie diesen Befehl ein

MAV-Funktionalität aktivieren	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`
	
	Beispiel : mit dem folgenden Befehl wird MAV mit 1 Genehmigungsgruppe, 2 erforderlichen Genehmigern und Standard-Ablauffristen aktiviert.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Führen Sie die Erstkonfiguration durch Hinzufügen von mindestens einer Konfiguration durch "Betriebsregel."

Änderung einer MAV-Konfiguration (erfordert MAV-Genehmigung)	`security multi-admin-verify approval-group modify [-approval-groups group1 [,group2…]] [-required-approvers nn ] [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`

Überprüfung der MAV-Funktionalität	`security multi-admin-verify show`
	
	Beispiel:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

Wenn Sie… wollen	Geben Sie diesen Befehl ein
MAV-Funktionalität deaktivieren (MAV-Genehmigung erforderlich)	`security multi-admin-verify modify -enabled false`

Verwalten von Regeln für geschützte Vorgänge

Sie erstellen MAV-Regeln (Multi-Admin Verification), um Vorgänge zu bestimmen, die genehmigt werden müssen. Sobald ein Vorgang initiiert wird, werden geschützte Vorgänge abgefangen und eine Anfrage zur Genehmigung generiert.

Regeln können erstellt werden, bevor sie MAV durch einen beliebigen Administrator mit entsprechenden RBAC-Funktionen aktivieren. Sobald MAV aktiviert ist, ist bei jeder Änderung der Regelsammlung die Genehmigung durch MAV erforderlich.

Pro Vorgang kann nur eine MAV-Regel erstellt werden, z. B. können Sie nicht mehrere erstellen `volume-snapshot-delete` Regeln. Alle gewünschten Regelbedingungen müssen in einer Regel enthalten sein.

Regelgeschützte Befehle

Ab ONTAP 9.11.1 können Sie Regeln zum Schutz der folgenden Befehle erstellen.

`cluster peer delete`	`volume snapshot autodelete modify`
`event config modify`	`volume snapshot delete`
`security login create`	`volume snapshot policy add-schedule`
`security login delete`	`volume snapshot policy create`
`security login modify`	`volume snapshot policy delete`
`system node run`	`volume snapshot policy modify`
`system node systemshell`	`volume snapshot policy modify-schedule`
`volume delete`	`volume snapshot policy remove-schedule`
`volume flexcache delete`	`volume snapshot restore`
	`vserver peer delete`

Sie können Regeln erstellen, um die folgenden Befehle ab ONTAP 9.13.1 zu schützen:

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

Sie können Regeln erstellen, um die folgenden Befehle ab ONTAP 9.14.1 zu schützen:

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

Die Regeln für MAV-System-default-Befehle, die `security multi-admin-verify` "Befehle", Kann nicht geändert werden.

Zusätzlich zu den systemdefinierten Befehlen sind die folgenden Befehle standardmäßig geschützt, wenn die Multi-Admin-Überprüfung aktiviert ist. Sie können jedoch die Regeln ändern, um den Schutz für diese Befehle zu entfernen.

- `security login password`
- `security login unlock`
- `set`

Regelbeschränkungen

Beim Erstellen einer Regel können Sie optional die angeben `-query` Option, um die Anforderung auf einen Teil der Befehlsfunktion zu beschränken. Der `-query` Zudem lassen sich Konfigurationselemente wie SVM, Volume und Snapshot Namen begrenzen.

Beispiel: In `volume snapshot delete` Befehl, `-query` Kann auf eingestellt werden `-snapshot !hourly*,!daily*,!weekly*`, Das bedeutet, dass Volume Snapshots mit stündlichen, täglichen oder wöchentlichen Attributen von MAV-Schutzmaßnahmen ausgeschlossen sind.

```
smci-vsim20::> security multi-admin-verify rule show
                                                Required  Approval
Vserver Operation                               Approvers Groups
------- ------------------------------------- --------- -------------
vs01    volume snapshot delete                  -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

> Alle ausgeschlossenen Konfigurationselemente werden nicht durch MAV geschützt, und jeder Administrator kann sie löschen oder umbenennen.

Standardmäßig wird durch Regeln ein entsprechendes festgelegt `security multi-admin-verify request create "protected_operation"` Der Befehl wird automatisch generiert, wenn ein geschützter Vorgang eingegeben wird. Sie können diese Standardeinstellung so ändern, dass sie den erfordert `request create` Befehl separat eingegeben werden.

Standardmäßig erben Regeln die folgenden globalen MAV-Einstellungen, obwohl regelspezifische Ausnahmen angegeben werden können:

- Erforderliche Anzahl der Genehmiger

- Genehmigungsgruppen
- Ablauffrist der Genehmigung
- Ablauffrist der Ausführung

System Manager Verfahren

Wenn Sie zum ersten Mal eine Regel für geschützte Vorgänge hinzufügen möchten, lesen Sie die Verfahren zu System Manager nach "Aktivieren Sie die Verifizierung für mehrere Administratoren."

So ändern Sie den vorhandenen Regelsatz:

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie ⚙ Neben **Multi-Admin-Genehmigung** im Abschnitt **Sicherheit**.
3. Wählen Sie + Add Zum Hinzufügen von mindestens einer Regel können Sie auch vorhandene Regeln ändern oder löschen.
   - Operation – Wählen Sie einen unterstützten Befehl aus der Liste aus.
   - Abfrage – Geben Sie alle gewünschten Befehlsoptionen und Werte ein.
   - Optionale Parameter: Lassen Sie das Feld leer, um globale Einstellungen anzuwenden, oder weisen Sie einen anderen Wert für bestimmte Regeln zu, um die globalen Einstellungen zu überschreiben.
     - Erforderliche Anzahl an Genehmigern
     - Genehmigungsgruppen

CLI-Verfahren

> Alle `security multi-admin-verify rule` Befehle erfordern vor der Ausführung eine Genehmigung des MAV-Administrators außer `security multi-admin-verify rule show`.

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Erstellen Sie eine Regel	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

Ändern der Anmeldeinformationen aktueller Administratoren	`security login modify <parameters>`
	
	Beispiel: Die folgende Regel erfordert die Genehmigung, um das Root-Volume zu löschen.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

Regel ändern	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Löschen Sie eine Regel	`security multi-admin-verify rule delete -operation "protected_operation"`
Regeln anzeigen	`security multi-admin-verify rule show`

Details zur Befehlssyntax finden Sie im `security multi-admin-verify rule` Man-Pages.

Anforderung einer Ausführung geschützter Vorgänge

Wenn Sie einen geschützten Vorgang oder einen geschützten Befehl für ein Cluster initiieren, das für die MAV-Überprüfung (Multi-Admin Verification) aktiviert ist, fängt ONTAP den Vorgang automatisch ab und fordert zur Generierung einer Anfrage auf, die von einem oder mehreren Administratoren in einer MAV Approval Group (MAV Administrators) genehmigt werden muss. Alternativ können Sie auch eine MAV-Anfrage ohne Dialog erstellen.

Wenn die Anfrage genehmigt ist, müssen Sie die Anfrage entsprechend beantworten, um den Vorgang innerhalb der Ablauffrist des Antrags abzuschließen. Wenn ein Veto eingelegt oder die Anfrage oder die Ablauffristen überschritten werden, müssen Sie die Anfrage löschen und erneut einreichen.

Die MAV-Funktionalität berücksichtigt vorhandene RBAC-Einstellungen. Das heißt, Ihre Administratorrolle muss über ausreichende Berechtigungen verfügen, um einen geschützten Vorgang auszuführen, ohne die MAV-Einstellungen zu berücksichtigen. "Erfahren Sie mehr über RBAC".

Wenn Sie ein MAV-Administrator sind, müssen Ihre Anfragen zur Ausführung von geschützten Vorgängen auch von einem MAV-Administrator genehmigt werden.

System Manager Verfahren

Wenn ein Benutzer auf einen Menüpunkt klickt, um einen Vorgang zu starten und der Vorgang zu schützen, wird eine Anfrage zur Genehmigung generiert und der Benutzer erhält eine Benachrichtigung wie folgt:

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

Das Fenster **Multi-Admin Requests** steht zur Verfügung, wenn MAV aktiviert ist und ausstehende Anfragen basierend auf der Anmelde-ID des Benutzers und der MAV-Rolle (Genehmiger oder nicht) angezeigt werden. Für jede ausstehende Anforderung werden die folgenden Felder angezeigt:

- Betrieb
- Index (Zahl)
- Status (ausstehend, genehmigt, abgelehnt, ausgeführt oder abgelaufen)

  Wird eine Anfrage von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.

- Abfrage (alle Parameter oder Werte für die angeforderte Operation)

- Benutzer Wird Angefordert
- Die Anfrage Läuft Ab Am
- (Anzahl der ausstehenden Genehmiger
- (Anzahl der möglichen Genehmiger

Wenn die Anfrage genehmigt wird, kann der anfragende Benutzer den Vorgang innerhalb des Ablaufzeitraums wiederholen.

Wenn der Benutzer den Vorgang ohne Genehmigung erneut versucht, wird eine Benachrichtigung wie folgt angezeigt:

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

CLI-Verfahren

1. Geben Sie den geschützten Vorgang direkt oder mit dem Befehl MAV Request ein.

   Beispiele – um ein Volume zu löschen, geben Sie einen der folgenden Befehle ein:

   - `volume delete`

     ```
     cluster-1::*> volume delete -volume vol1 -vserver vs0

     Warning: This operation requires multi-admin verification. To create
     a
              verification request use "security multi-admin-verify
     request
              create".

              Would you like to create a request for this operation?
               {y|n}: y

     Error: command failed: The security multi-admin-verify request (index
     3) is
            auto-generated and requires approval.
     ```

   - `security multi-admin-verify request create “volume delete”`

     ```
     Error: command failed: The security multi-admin-verify request (index
     3)
            requires approval.
     ```

2. Den Status der Anfrage überprüfen und auf die MAV-Benachrichtigung antworten.

a. Wenn der Antrag genehmigt wird, beantworten Sie die CLI-Meldung, um den Vorgang abzuschließen.

Beispiel:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. Wenn der Antrag gegen ein Vetos gestellt wird oder die Ablauffrist abgelaufen ist, löschen Sie die Anfrage, und senden Sie sie erneut oder wenden Sie sich an den MAV-Administrator.

Beispiel:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Managen Sie Anforderungen für geschützte Vorgänge

Wenn Administratoren einer MAV-Genehmigungsgruppe (MAV-Administratoren) über eine Anfrage zur Ausführung eines ausstehenden Vorgangs benachrichtigt werden, müssen sie innerhalb eines festgelegten Zeitraums mit einer Genehmigungs- oder Veto-Nachricht (Ablauf der Genehmigung) antworten. Wenn keine ausreichende Anzahl von Genehmigungen eingegangen ist, muss der Anfordernde die Anfrage löschen und eine andere erstellen.

Über diese Aufgabe

Genehmigungsanforderungen werden mit Indexnummern identifiziert, die in E-Mail-Nachrichten und Anzeigen der Anforderungswarteschlange enthalten sind.

Die folgenden Informationen aus der Anforderungswarteschlange können angezeigt werden:

Betrieb

Der geschützte Vorgang, für den die Anforderung erstellt wird.

Abfrage

Das Objekt (oder die Objekte), auf das der Benutzer die Operation anwenden möchte.

Bundesland

Der aktuelle Status der Anfrage; ausstehend, genehmigt, abgelehnt, abgelaufen, Ausgeführt. Wird eine Anfrage von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.

Erforderliche Genehmiger

Die Anzahl der MAV-Administratoren, die zur Genehmigung der Anfrage erforderlich sind. Ein Benutzer kann den Parameter erforderliche Genehmiger für die Operationssegel festlegen. Wenn ein Benutzer die erforderlichen Genehmiger nicht auf die Regel setzt, werden die erforderlichen Genehmiger aus der globalen Einstellung angewendet.

Ausstehende Genehmiger

Die Anzahl der MAV-Administratoren, die noch erforderlich sind, um die Anfrage zu genehmigen, die als genehmigt gekennzeichnet werden soll.

Ablauf der Genehmigung

Der Zeitraum, innerhalb dessen ein MAV-Administrator auf eine Genehmigungsanforderung reagieren muss. Jeder autorisierte Benutzer kann den Genehmigungssatz für eine Betriebsregel festlegen. Wenn für die Regel kein Genehmigungssatz festgelegt ist, wird der Genehmigungssatz aus der globalen Einstellung angewendet.

Ablauf der Ausführung

Der Zeitraum, in dem der anfordernde Administrator den Vorgang abschließen muss. Jeder autorisierte Benutzer kann das Ablaufdatum für eine Betriebsregel festlegen. Wenn für die Regel kein Ausführungs-Expiry festgelegt ist, wird das Ausführen-Expiry aus der globalen Einstellung angewendet.

Anwender genehmigt

Die MAV-Administratoren, die den Antrag genehmigt haben.

Vetoed durch den Benutzer

Die MAV-Administratoren, die den Antrag gegen das Vetos gestellt haben.

Storage-VM (vServer)

Der SVM, der die Anforderung zugeordnet ist. In dieser Version wird nur die Admin-SVM unterstützt.

Der Benutzer wurde angefordert

Der Benutzername des Benutzers, der die Anforderung erstellt hat.

Uhrzeit erstellt

Die Uhrzeit, zu der die Anfrage erstellt wurde.

Nach Genehmigung der Zeit

Die Zeit, zu der der Antragsstatus in „genehmigt“ geändert wurde.

Kommentar

Kommentare, die mit der Anfrage verknüpft sind.

Benutzer erlaubt

Die Liste der Benutzer, für die der geschützte Vorgang ausgeführt werden kann, für den die Anforderung genehmigt wird. Wenn `users-permitted` Ist leer, dann kann jeder Benutzer mit entsprechenden

Berechtigungen den Vorgang durchführen.

Alle abgelaufenen oder ausgeführten Anfragen werden gelöscht, wenn ein Limit von 1000 Anfragen erreicht wird oder wenn die abgelaufene Zeit länger als 8 Stunden für abgelaufene Anfragen ist. Vetos-Anträge werden gelöscht, sobald sie als abgelaufen markiert sind.

System Manager Verfahren

MAV-Administratoren erhalten E-Mail-Nachrichten mit Details der Genehmigungsanforderung, Ablauffrist anfordern und einen Link zum Genehmigen oder Ablehnen der Anfrage. Sie können über den Link in der E-Mail auf ein Genehmigungsdialogfeld zugreifen oder im System Manager zu **Events & Jobs>Requests** navigieren.

Das Fenster **Requests** steht zur Verfügung, wenn die Multi-Admin-Überprüfung aktiviert ist und ausstehende Anfragen basierend auf der Anmelde-ID und der MAV-Rolle des Benutzers (Genehmiger oder nicht) angezeigt werden.

- Betrieb
- Index (Zahl)
- Status (ausstehend, genehmigt, abgelehnt, ausgeführt oder abgelaufen)

  Wird eine Anfrage von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.

- Abfrage (alle Parameter oder Werte für die angeforderte Operation)
- Benutzer Wird Angefordert
- Die Anfrage Läuft Ab Am
- (Anzahl der ausstehenden Genehmiger
- (Anzahl der möglichen Genehmiger

MAV-Administratoren verfügen in diesem Fenster über zusätzliche Steuerelemente. Sie können einzelne Vorgänge oder ausgewählte Gruppen von Operationen genehmigen, ablehnen oder löschen. Wenn der MAV-Administrator jedoch der anfragende Benutzer ist, kann er seine eigenen Anforderungen nicht genehmigen, ablehnen oder löschen.

CLI-Verfahren

1. Wenn Sie über ausstehende Anfragen per E-Mail benachrichtigt werden, notieren Sie die Indexnummer der Anfrage und den Ablauf der Genehmigung. Die Indexnummer kann auch mit den unten genannten Optionen **show** oder **show-exwaring** angezeigt werden.
2. Genehmigen oder Vereinen der Anfrage.

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Genehmigen einer Anfrage	`security multi-admin-verify request approve` *`nn`*
Veto auf eine Anfrage	`security multi-admin-verify request veto` *`nn`*

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Zeigt alle Anfragen, ausstehende Anfragen oder eine einzelne Anforderung an	`security multi-admin-verify request { show
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  Sie können alle Anfragen in der Warteschlange oder nur ausstehende Anforderungen anzeigen. Wenn Sie die Indexnummer eingeben, werden nur die entsprechenden Informationen angezeigt. Sie können Informationen zu bestimmten Feldern anzeigen (mithilfe von `-fields` Parameter) oder über alle Felder (mit dem `-instance` Parameter).
Löschen Sie eine Anfrage	`security multi-admin-verify request delete` *`nn`*

Beispiel:

Die folgende Sequenz genehmigt einen Antrag, nachdem der MAV-Administrator die Anfrage-E-Mail mit der Indexnummer 3 erhalten hat, die bereits eine Genehmigung hat.

```
          cluster1::> security multi-admin-verify request show-pending
                                          Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

Beispiel:

Die folgende Sequenz vetoes einen Antrag, nachdem der MAV-Administrator die Anfrage-E-Mail mit der Nummer 3 erhalten hat, die bereits eine Genehmigung hat.

```
      cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

Authentifizierung und Autorisierung mit OAuth 2.0

Überblick über die Implementierung von ONTAP OAuth 2.0

Ab ONTAP 9.14 haben Sie die Möglichkeit, den Zugriff auf Ihre ONTAP-Cluster über das Open Authorization (OAuth 2.0)-Framework zu steuern. Sie können diese Funktion über jede der ONTAP-Administrationsschnittstellen konfigurieren, einschließlich der ONTAP-CLI, System Manager und REST-API. Die OAuth 2.0-Autorisierungs- und Zugriffskontrollentscheidungen können jedoch nur angewendet werden, wenn ein Client über die REST-API auf ONTAP zugreift.

> Die Unterstützung für OAuth 2.0 wurde erstmals mit ONTAP 9.14.0 eingeführt, sodass die Verfügbarkeit von der von Ihnen verwendeten ONTAP Version abhängt. Siehe "Versionshinweise zu ONTAP" Finden Sie weitere Informationen.

Funktionen und Vorteile

Die wichtigsten Merkmale und Vorteile der Verwendung von OAuth 2.0 mit ONTAP sind im Folgenden beschrieben.

Unterstützung für den Standard OAuth 2.0

OAuth 2.0 ist das Standard-Autorisierungsframework der Branche. Sie wird verwendet, um den Zugriff auf geschützte Ressourcen mit signierten Zugriffstoken zu beschränken und zu steuern. Die Verwendung von OAuth 2.0 bietet mehrere Vorteile:

- Viele Optionen für die Berechtigungskonfiguration
- Geben Sie niemals die Client-Anmeldeinformationen einschließlich Passwörter bekannt
- Token können basierend auf Ihrer Konfiguration auf „ablaufen lassen“ gesetzt werden
- Ideal geeignet für den Einsatz mit REST-APIs

Getestet mit mehreren gängigen Autorisierungsservern

Die ONTAP-Implementierung ist mit jedem OAuth 2.0-konformen Autorisierungsserver kompatibel. Es wurde mit den folgenden gängigen Servern oder Diensten getestet, darunter:

- Auth0
- Active Directory Federation Service (ADFS)
- Keycloak

Unterstützung für mehrere gleichzeitige Autorisierungsserver

Sie können bis zu acht Autorisierungsserver für einen einzelnen ONTAP-Cluster definieren. Dadurch erhalten Sie die Flexibilität, die Anforderungen Ihrer vielfältigen Sicherheitsumgebung zu erfüllen.

Integration in die REST-Rollen

Die ONTAP-Autorisierungsentscheidungen basieren letztlich auf den REST-Rollen, die Benutzern oder Gruppen zugewiesen sind. Diese Rollen werden entweder als eigenständige Bereiche im Zugriffstoken oder auf der Grundlage lokaler ONTAP-Definitionen zusammen mit Active Directory- oder LDAP-Gruppen übertragen.

Option zur Verwendung von Zugriffstoken mit Senderbeschränkungen

Sie können ONTAP und die Autorisierungsserver so konfigurieren, dass die gegenseitige Transportschicht-Sicherheit (MTLS) verwendet wird, wodurch die Clientauthentifizierung gestärkt wird. Sie garantiert, dass die OAuth 2.0-Zugriffstoken nur von den Clients verwendet werden, auf die sie ursprünglich ausgestellt wurden. Diese Funktion unterstützt und harmonisiert mit mehreren gängigen Sicherheitsempfehlungen, einschließlich der von FAPI und MITER festgelegten.

Implementierung und Konfiguration

Auf hoher Ebene gibt es mehrere Aspekte einer OAuth 2.0-Implementierung und -Konfiguration, die Sie bei der Inbetriebnahme berücksichtigen sollten.

OAuth 2.0 Einheiten innerhalb von ONTAP

Das OAuth 2.0-Autorisierungs-Framework definiert mehrere Einheiten, die realen oder virtuellen Elementen in Ihrem Rechenzentrum oder Netzwerk zugeordnet werden können. Die OAuth 2.0 Einheiten und ihre Anpassung an ONTAP sind in der folgenden Tabelle dargestellt.

OAuth 2.0-Einheit	Beschreibung
Ressource	Die REST-API-Endpunkte, die über interne ONTAP-Befehle Zugriff auf die ONTAP-Ressourcen bieten.
Ressourceneigentümer	Der ONTAP-Cluster-Benutzer, der die geschützte Ressource erstellt hat oder der sie standardmäßig besitzt.
Ressourcenserver	Der Host für die geschützten Ressourcen, die der ONTAP-Cluster ist.
Client	Eine Applikation, die den Zugriff auf einen REST-API-Endpunkt im Namen oder mit Genehmigung des Ressourceneigentümers anfordert.
Autorisierungsserver	In der Regel ein dedizierter Server, der für die Ausgabe von Zugriffstoken und die Durchsetzung von Verwaltungsrichtlinien verantwortlich ist.

ONTAP-Kernkonfiguration

Sie müssen den ONTAP-Cluster konfigurieren, um OAuth 2.0 zu aktivieren und zu verwenden. Dazu gehört die Einrichtung einer Verbindung zum Autorisierungsserver und die Definition der erforderlichen ONTAP-Autorisierungskonfiguration. Sie können diese Konfiguration über eine der Administrationsschnittstellen durchführen, einschließlich:

- ONTAP Befehlszeilenschnittstelle
- System Manager
- ONTAP REST API

Umwelt und unterstützende Dienstleistungen

Zusätzlich zu den ONTAP-Definitionen müssen Sie auch die Autorisierungsserver konfigurieren. Wenn Sie eine Gruppen-zu-Rollen-Zuordnung verwenden, müssen Sie auch die Active Directory-Gruppen oder das LDAP-Äquivalent konfigurieren.

Unterstützte ONTAP-Clients

Ab ONTAP 9.14 kann ein REST-API-Client über OAuth 2.0 auf ONTAP zugreifen. Bevor Sie einen REST-API-Aufruf ausgeben, müssen Sie ein Zugriffstoken vom Autorisierungsserver beziehen. Der Client leitet dieses Token dann über den Header der HTTP-Autorisierungsanforderung als *Bearer-Token* an den ONTAP-Cluster weiter. Je nach Sicherheitsstufe können Sie auch ein Zertifikat auf dem Client erstellen und installieren, um auf MTLS basierende Token mit Senderbeschränkungen zu verwenden.

Ausgewählte Terminologie

Wenn Sie sich mit einer OAuth 2.0-Bereitstellung mit ONTAP vertraut machen, ist es hilfreich, sich mit einigen Begriffen vertraut zu machen. Siehe "Weitere Ressourcen" Für Links zu weiteren Informationen über OAuth 2.0.

Access Token

Ein Token, das von einem Autorisierungsserver ausgegeben und von einer OAuth 2.0-Clientanwendung verwendet wird, um Anfragen für den Zugriff auf die geschützten Ressourcen zu stellen.

JSON-Webtoken

Der Standard, der zum Formatieren der Zugriffstoken verwendet wird. JSON wird verwendet, um die OAuth 2.0 Claims in einem kompakten Format darzustellen, wobei die Claims in drei Hauptabschnitten angeordnet sind.

Zugriffstoken, die durch den Absender eingeschränkt sind

Eine optionale Funktion, die auf dem Protokoll Mutual Transport Layer Security (MTLS) basiert. Durch die Verwendung eines zusätzlichen Bestätigungsanspruchs im Token wird sichergestellt, dass das Zugriffstoken nur von dem Client verwendet wird, auf den es ursprünglich ausgestellt wurde.

JSON-Webschlüsselsatz

Ein JWKS ist eine Sammlung öffentlicher Schlüssel, die von ONTAP zur Überprüfung der von den Clients präsentierten JWT-Token verwendet werden. Die Schlüsselsätze sind normalerweise über einen dedizierten URI am Autorisierungsserver verfügbar.

Umfang

Scopes bieten eine Möglichkeit, den Zugriff einer Applikation auf geschützte Ressourcen wie die REST-API von ONTAP zu beschränken oder zu steuern. Sie werden im Zugriffstoken als Strings dargestellt.

ONTAP-REST-Rolle

REST-Rollen wurden mit ONTAP 9.6 eingeführt und sind ein wichtiger Bestandteil des RBAC Framework von ONTAP. Diese Rollen unterscheiden sich von den früheren herkömmlichen Rollen, die immer noch von ONTAP unterstützt werden. Die OAuth 2.0-Implementierung in ONTAP unterstützt nur REST-Rollen.

HTTP-Autorisierungskopf

Eine Kopfzeile, die in der HTTP-Anforderung enthalten ist, um den Client und die zugehörigen Berechtigungen als Teil eines REST-API-Aufrufs zu identifizieren. Je nachdem, wie Authentifizierung und Autorisierung durchgeführt werden, stehen verschiedene Varianten oder Implementierungen zur Verfügung. Wenn ein OAuth 2.0-Zugriffstoken an ONTAP übergeben wird, wird das Token als *Bearer Token* identifiziert.

HTTP-Basisauthentifizierung

Eine frühe HTTP-Authentifizierungstechnik, die noch von ONTAP unterstützt wird. Die Klartext-Anmeldeinformationen (Benutzername und Passwort) werden mit einem Doppelpunkt verkettet und in base64 kodiert. Die Zeichenfolge wird in den Header der Autorisierungsanforderung eingefügt und an den Server gesendet.

FAPI

Eine Arbeitsgruppe der OpenID Foundation, die Protokolle, Datenschemas und Sicherheitsempfehlungen für die Finanzbranche bereitstellt. Die API wurde ursprünglich als Financial Grade API bekannt.

GEHRUNG

Ein privates gemeinnütziges Unternehmen, das technische und sicherheitstechnische Leitlinien für die US-Luftwaffe und die US-Regierung bereitstellt.

Weitere Ressourcen

Im Folgenden finden Sie einige zusätzliche Ressourcen. Sie sollten diese Seiten durchsehen, um weitere Informationen über OAuth 2.0 und die zugehörigen Standards zu erhalten.

Protokolle und Standards

- "RFC 6749: Das OAuth 2.0 Authorization Framework"
- "RFC 7519: JSON Web Tokens (JWT)"
- "RFC 7523: JSON Web Token (JWT) Profile für OAuth 2.0 Client Authentication and Authorization Grants"
- "RFC 7662: OAuth 2.0 Token-Introspektion"
- "RFC 7800: Proof-of-Possession Key für JWTs"

- "RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication und Certificate-bound Access Tokens"

Organisationen

- "OpenID Foundation"
- "FAPI-Arbeitsgruppe"
- "GEHRUNG"
- "IANA - JWT"

Produkte und Services

- "Auth0"
- "ADFS-Übersicht"
- "Keycloak"

Zusätzliche Tools und Dienstprogramme

- "JWT von Auth0"
- "OpenSSL"

NetApp Dokumentation und Ressourcen

- "ONTAP-Automatisierung" Dokumentation

Konzepte

Autorisierungsserver und Zugriffstoken

Autorisierungsserver führen als zentrale Komponente im OAuth 2.0-Autorisierungs-Framework mehrere wichtige Funktionen aus.

OAuth 2.0-Autorisierungsserver

Autorisierungsserver sind in erster Linie für das Erstellen und Signieren von Zugriffstoken verantwortlich. Diese Token enthalten Identitäts- und Autorisationsinformationen, die es einer Clientanwendung ermöglichen, selektiv auf geschützte Ressourcen zuzugreifen. Die Server sind in der Regel voneinander isoliert und können auf verschiedene Weise implementiert werden, beispielsweise als eigenständiger dedizierter Server oder als Teil eines größeren Identitäts- und Zugriffsverwaltungsprodukts.

> Für einen Autorisierungsserver kann manchmal eine andere Terminologie verwendet werden, insbesondere wenn die OAuth 2.0-Funktionalität in einem größeren Produkt oder einer größeren Lösung zur Identitäts- und Zugriffsverwaltung enthalten ist. Der Begriff **Identity Provider (IdP)** wird beispielsweise häufig mit **Authorization Server** synonym verwendet.

Administration

Zusätzlich zur Ausgabe von Zugriffstoken bieten Autorisierungsserver auch zugehörige Verwaltungsdienste, in der Regel über eine Web-Benutzeroberfläche. Sie können beispielsweise Folgendes definieren und verwalten:

- Benutzer- und Benutzerauthentifizierung
- Bereich
- Administrative Trennung durch Mandanten und Bereiche

- Richtlinienumsetzung
- Anbindung an verschiedene externe Dienste
- Unterstützung für andere Identitätsprotokolle (z. B. SAML)

ONTAP ist mit Autorisierungsservern kompatibel, die dem OAuth 2.0-Standard entsprechen.

Definieren auf ONTAP

Sie müssen einen oder mehrere Autorisierungsserver für ONTAP definieren. ONTAP kommuniziert sicher mit jedem Server, um Token zu überprüfen und andere damit verbundene Aufgaben zur Unterstützung der Client-Anwendungen auszuführen.

Die wichtigsten Aspekte der ONTAP-Konfiguration sind im Folgenden aufgeführt. Siehe auch "OAuth 2.0-Bereitstellungsszenarien" Finden Sie weitere Informationen.

Wie und wo die Zugriffstoken validiert werden

Es gibt zwei Optionen für die Validierung von Zugriffstoken.

- Lokale Validierung

  ONTAP kann Zugriffstoken lokal anhand der Informationen validieren, die vom Autorisierungsserver bereitgestellt werden, der das Token ausgestellt hat. Die vom Autorisierungsserver abgerufenen Informationen werden von ONTAP zwischengespeichert und in regelmäßigen Abständen aktualisiert.

- Fernintrospektion

  Sie können auch Remote-Introspektion verwenden, um Token auf dem Autorisierungsserver zu validieren. Introspektion ist ein Protokoll, das es autorisierten Parteien ermöglicht, einen Autorisierungsserver nach einem Zugriffstoken abzufragen. Es bietet ONTAP eine Möglichkeit, bestimmte Metadaten aus einem Zugriffstoken zu extrahieren und das Token zu validieren. ONTAP speichert einige Daten aus Gründen der Performance im Cache.

Netzwerkspeicherort

ONTAP befindet sich möglicherweise hinter einer Firewall. In diesem Fall müssen Sie einen Proxy als Teil der Konfiguration identifizieren.

Wie die Autorisierungsserver definiert werden

Sie können einen Autorisierungsserver für ONTAP über eine der Administrationsschnittstellen definieren, einschließlich CLI, System Manager oder REST-API. Beispielsweise verwenden Sie in der CLI den Befehl `security oauth2 client create`.

Anzahl der Autorisierungsserver

Sie können bis zu acht Autorisierungsserver für einen einzelnen ONTAP-Cluster definieren. Der gleiche Autorisierungsserver kann für denselben ONTAP-Cluster mehr als einmal definiert werden, solange die Ansprüche des Emittenten oder des Emittenten/der Zielgruppe eindeutig sind. Zum Beispiel, mit Keycloak wird dies immer der Fall sein, wenn verschiedene Bereiche.

Verwenden von OAuth 2.0-Zugriffstoken

Die von den Autorisierungsservern ausgegebenen OAuth 2.0-Zugriffstoken werden von ONTAP überprüft und für rollenbasierte Zugriffsentscheidungen für die REST-API-Clientanforderungen verwendet.

Abrufen eines Zugriffstoken

Sie müssen ein Zugriffstoken von einem Autorisierungsserver erwerben, der für das ONTAP-Cluster definiert ist, wo Sie die REST-API verwenden. Um ein Token zu erwerben, müssen Sie sich direkt an den Autorisierungsserver wenden.

> ONTAP gibt keine Zugriffstoken aus und leitet Anforderungen von Clients nicht an die Autorisierungsserver weiter.

Wie Sie ein Token anfordern, hängt von mehreren Faktoren ab, darunter:

- Autorisierungsserver und seine Konfigurationsoptionen
- OAuth 2.0 Zuschussart
- Client oder Softwaretool zur Ausgabe der Anforderung

Grant-Typen

Ein *Grant* ist ein gut definierter Prozess, einschließlich einer Reihe von Netzwerkflüssen, die zum anfordern und Empfangen eines OAuth 2.0-Zugriffstoken verwendet werden. Je nach Client-, Umgebungs- und Sicherheitsanforderungen können verschiedene Zuteilungsarten verwendet werden. Eine Liste der gängigen Fördertypen finden Sie in der folgenden Tabelle.

Zuteilungsart	Beschreibung
Client-Anmeldedaten	Ein beliebter Zuschusstyp, der nur auf der Verwendung von Anmeldeinformationen basiert (z. B. eine ID und ein gemeinsam genutzter Schlüssel). Es wird davon ausgegangen, dass der Client eine enge Vertrauensbeziehung zum Ressourcenbesitzer hat.
Passwort	Der Zuteilungstyp für die Kennwortanmeldeinformationen des Ressourceneigentümers kann in Fällen verwendet werden, in denen der Ressourceneigentümer über eine Vertrauensbeziehung zum Client verfügt. Sie kann auch bei der Migration älterer HTTP-Clients zu OAuth 2.0 nützlich sein.
Autorisierungscode	Dies ist eine ideale Zuteilungsart für vertrauliche Clients und basiert auf einem auf Umleitung basierenden Fluss. Es kann verwendet werden, um sowohl ein Zugriffstoken als auch ein Aktualisierungs-Token zu erhalten.

JWT-Inhalt

Ein OAuth 2.0-Zugriffstoken ist als JWT formatiert. Der Inhalt wird basierend auf Ihrer Konfiguration vom Autorisierungsserver erstellt. Die Token sind jedoch für die Client-Anwendungen undurchsichtig. Ein Kunde hat keinen Grund, ein Token zu prüfen oder sich des Inhalts bewusst zu sein.

Jedes JWT-Zugriffstoken enthält eine Reihe von Ansprüchen. Die Ansprüche beschreiben die Merkmale des Emittenten und die Autorisierung basierend auf administrativen Definitionen am Autorisierungsserver. Einige der mit dem Standard registrierten Ansprüche sind in der folgenden Tabelle beschrieben. Bei allen Strings wird zwischen Groß- und Kleinschreibung unterschieden.

Forderung	Stichwort	Beschreibung
Aussteller	ISS	Identifiziert den Prinzipal, der das Token ausgegeben hat. Die Antragsbearbeitung ist anwendungsspezifisch.

Forderung	Stichwort	Beschreibung
Betreff	Unterbereich	Der Betreff oder Benutzer des Tokens. Der Name ist global oder lokal eindeutig.
Zielgruppe	AUD	Die Empfänger, für die das Token bestimmt ist. Als Array von Strings implementiert.
Ablauf	exsp	Die Zeit, nach der das Token abläuft und zurückgewiesen werden muss.

Siehe "RFC 7519: JSON Web Tokens" Finden Sie weitere Informationen.

Optionen für die ONTAP-Clientautorisierung

Für die Anpassung Ihrer ONTAP-Clientautorisierung stehen verschiedene Optionen zur Verfügung. Die Autorisierungsentscheidungen basieren letztlich auf den ONTAP-REST-Rollen, die entweder in den Zugriffstoken enthalten sind oder von diesen abgeleitet wurden.

> Sie können nur verwenden "ONTAP REST-Rollen" Bei der Konfiguration der Autorisierung für OAuth 2.0. Die früheren herkömmlichen ONTAP Rollen werden nicht unterstützt.

Einführung

Die OAuth 2.0 Implementierung in ONTAP ist flexibel und robust und bietet Ihnen die Optionen, die Sie für die Sicherung der ONTAP Umgebung benötigen. Im Wesentlichen gibt es drei Hauptkonfigurationskategorien zur Definition der ONTAP-Clientautorisierung. Diese Konfigurationsoptionen schließen sich gegenseitig aus.

ONTAP wendet je nach Konfiguration die am besten geeignete Option an. Siehe "Wie ONTAP den Zugriff bestimmt" Finden Sie heraus, wie ONTAP Ihre Konfigurationsdefinitionen für Zugriffsentscheidungen verarbeitet.

OAuth 2.0 eigenständige Oszilloskope

Diese Bereiche enthalten eine oder mehrere benutzerdefinierte REST-Rollen, die jeweils in einer einzigen Zeichenfolge gekapselt sind. Sie sind unabhängig von den Rollendefinitionen von ONTAP. Sie müssen diese Bereichszeichenfolgen auf Ihrem Autorisierungsserver definieren.

Lokale ONTAP-spezifische REST-Rollen und Benutzer

Je nach Konfiguration können die lokalen ONTAP-Identitätsdefinitionen für Zugriffsentscheidungen verwendet werden. Folgende Optionen stehen zur Verfügung:

- Einzelne benannte REST-Rolle
- Übereinstimmung des Benutzernamens mit einem lokalen ONTAP-Benutzer

Die scope Syntax für eine benannte Rolle ist **ontap-role-**<URL-encoded-ONTAP-role-name>. Wenn die Rolle beispielsweise „admin“ lautet, lautet der Scope-String „ontap-role-admin“.

Active Directory oder LDAP-Gruppen

Wenn die lokalen ONTAP-Definitionen überprüft werden, aber keine Zugriffsentscheidung getroffen werden kann, werden die Active Directory („Domain“)- oder LDAP („nsswitch“)-Gruppen verwendet. Gruppeninformationen können auf zwei Arten angegeben werden:

- OAuth 2.0-Scope-String

  Unterstützt vertrauliche Anwendungen, die den Ablauf der Clientanmeldeinformationen verwenden, wenn kein Benutzer mit einer Gruppenmitgliedschaft vorhanden ist. Der Umfang sollte benannt werden **ontap-Group-**<URL-encoded-ONTAP-group-name>. Wenn die Gruppe beispielsweise „Entwicklung“ ist, lautet der Scope String „ontap-Group-Development“.

- In der „Gruppe“-Forderung

  Dies ist für Zugriffstoken vorgesehen, die von ADFS unter Verwendung des Ablaufs Resource Owner (Password Grant) ausgegeben werden.

Eigenständige Oszilloskope von OAuth 2.0

In sich geschlossene Bereiche sind Strings, die im Zugriffstoken enthalten sind. Jede dieser Rollen ist vollständig definiert und beinhaltet alles, was ONTAP für eine Zugriffsentscheidung benötigt. Der Umfang unterscheidet sich von jeder der REST-Rollen, die in ONTAP selbst definiert sind.

Format der Bereichszeichenfolge

Auf einer Basisebene wird der Umfang als zusammenhängende Zeichenfolge dargestellt und besteht aus sechs durch Doppelpunkte getrennten Werten. Die im Scope String verwendeten Parameter werden im Folgenden beschrieben.

ONTAP-Literal

Der Bereich muss mit dem Literalwert beginnen `ontap` In Kleinbuchstaben. Der ONTAP-spezifische Umfang wird angegeben.

Cluster

Dies definiert, auf welchen ONTAP Cluster sich der Umfang bezieht. Die Werte können Folgendes umfassen:

- Cluster-UUID

  Identifiziert ein einzelnes Cluster.

- Sternchen (*)

  Gibt an, dass der Umfang auf alle Cluster angewendet wird.

Sie können den ONTAP-CLI-Befehl verwenden `cluster identity show` Um die UUID des Clusters anzuzeigen. Falls nicht angegeben, gilt der Umfang für alle Cluster.

Rolle

Der Name der im eigenständigen Bereich enthaltenen REST-Rolle. Dieser Wert wird von ONTAP nicht untersucht oder auf vorhandene REST-Rollen abgestimmt, die für ONTAP definiert sind. Der Name wird für die Protokollierung verwendet.

Zugangsstufe

Dieser Wert gibt die Zugriffsebene an, die auf die Clientanwendung angewendet wird, wenn der API-Endpunkt im Umfang verwendet wird. Es gibt sechs mögliche Werte, wie in der Tabelle unten beschrieben.

Zugangsstufe	Beschreibung
Keine	Verweigert allen Zugriff auf den angegebenen Endpunkt.
readonly	Nur Lesezugriff mit GET ist möglich.
Read_create	Ermöglicht den Lesezugriff sowie die Erstellung neuer Ressourceninstanzen über POST.
Lesen_ändern	Ermöglicht den Lesezugriff sowie die Möglichkeit, vorhandene Ressourcen mithilfe von PATCHES zu aktualisieren.
Lesen_create_modify	Ermöglicht alle Zugriffe außer Löschen. Zu den zulässigen Operationen gehören GET (read), POST (create) und PATCH (Update).
Alle	Ermöglicht vollständigen Zugriff.

SVM

Der Name der SVM innerhalb des Clusters, für den der Umfang gilt. Verwenden Sie den *-Wert (Sternchen), um alle SVMs anzuzeigen.

> Diese Funktion wird von ONTAP 9.14.1 nicht vollständig unterstützt. Sie können den SVM-Parameter ignorieren und ein Sternchen als Platzhalter verwenden. Überprüfen Sie die "Versionshinweise zu ONTAP" Um auf zukünftige SVM-Unterstützung zu prüfen.

REST-API-URI

Der vollständige oder teilweise Pfad zu einer Ressource oder einem Satz zugehöriger Ressourcen. Der String muss mit beginnen `/api`. Wenn Sie keinen Wert angeben, gilt der Umfang für alle API-Endpunkte im ONTAP-Cluster.

Beispiele für den Umfang

Im Folgenden werden einige Beispiele für eigenständige Oszilloskope vorgestellt.

ontap:*:joes-role:read_create_modify:*:/API/Cluster

Bietet dem Benutzer, dem diese Rolle zugewiesen ist, den Zugriff auf das zu lesen, zu erstellen und zu ändern `/cluster` endpunkt:

CLI-Verwaltungstool

Um die Administration der eigenständigen Bereiche einfacher und weniger fehleranfällig zu machen, bietet ONTAP den CLI-Befehl `security oauth2 scope` So generieren Sie auf der Grundlage Ihrer Eingabeparameter Oszilloskop-Strings.

Der Befehl `security oauth2 scope` Basierend auf Ihren Angaben gibt es zwei Anwendungsfälle:

- CLI-Parameter für den Umfang einer Zeichenfolge

  Mit dieser Version des Befehls können Sie auf Grundlage der Eingabeparameter eine Bereichszeichenfolge generieren.

- Scope-String zu CLI-Parametern

Sie können diese Version des Befehls verwenden, um die Befehlsparameter basierend auf der Zeichenfolge für den Eingabebereich zu generieren.

Beispiel

Im folgenden Beispiel wird eine Scope-String mit der Ausgabe generiert, die nach dem unten stehenden Befehlsbeispiel enthalten ist. Die Definition gilt für alle Cluster.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Wie ONTAP den Zugriff bestimmt

Um OAuth 2.0 richtig zu entwickeln und zu implementieren, müssen Sie verstehen, wie Ihre Autorisierungskonfiguration von ONTAP verwendet wird, um Zugriffsentscheidungen für die Clients zu treffen.

Schritt 1: Eigenständige Bereiche

Wenn das Zugriffstoken eigenständige Bereiche enthält, untersucht ONTAP diese Bereiche zuerst. Wenn keine eigenständigen Bereiche vorhanden sind, mit Schritt 2 fortfahren.

Wenn ein oder mehrere eigenständige Bereiche vorhanden sind, wendet ONTAP jeden Bereich an, bis eine explizite **ALLOW**- oder **DENY**-Entscheidung getroffen werden kann. Wenn eine explizite Entscheidung getroffen wird, endet die Verarbeitung.

Wenn ONTAP keine explizite Zugriffsentscheidung treffen kann, fahren Sie mit Schritt 2 fort.

Schritt 2: Überprüfen Sie die lokale Rollenmarkierung

ONTAP überprüft den Wert des Flags `use-local-roles-if-present`. Der Wert dieses Flags wird für jeden Autorisierungsserver, der für ONTAP definiert ist, separat festgelegt.

- Wenn der Wert ist `true` Fahren Sie mit Schritt 3 fort.
- Wenn der Wert ist `false` Die Verarbeitung endet und der Zugriff wird verweigert.

Schritt 3: Benannte ONTAP REST-Rolle

Wenn das Zugriffstoken eine benannte REST-Rolle enthält, verwendet ONTAP die Rolle, um die Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine benannte REST-Rolle vorhanden ist oder die Rolle nicht gefunden wurde, fahren Sie mit Schritt 4 fort.

Schritt 4: Lokale ONTAP-Benutzer

Extrahieren Sie den Benutzernamen aus dem Zugriffstoken und versuchen Sie, ihn einem lokalen ONTAP-Benutzer zuzuordnen.

Wenn ein lokaler ONTAP-Benutzer abgeglichen wird, verwendet ONTAP die für den Benutzer definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn ein lokaler ONTAP-Benutzer nicht stimmt oder kein Benutzername im Zugriffstoken vorhanden ist,

fahren Sie mit Schritt 5 fort.

Schritt 5: Gruppen-zu-Rollen-Zuordnung

Extrahieren Sie die Gruppe aus dem Zugriffstoken, und versuchen Sie, sie einer Gruppe zuzuordnen. Die Gruppen werden über Active Directory oder einen gleichwertigen LDAP-Server definiert.

Wenn eine Gruppenübereinstimme vorhanden ist, verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine Gruppenübereinstimme vorhanden ist oder keine Gruppe im Zugriffstoken vorhanden ist, wird der Zugriff verweigert und die Verarbeitung wird beendet.

OAuth 2.0-Bereitstellungsszenarien

Beim Definieren eines Autorisierungsservers für ONTAP stehen verschiedene Konfigurationsoptionen zur Verfügung. Basierend auf diesen Optionen können Sie einen Autorisierungsserver erstellen, der für Ihre Bereitstellungsumgebung geeignet ist.

Zusammenfassung der Konfigurationsparameter

Beim Definieren eines Autorisierungsservers für ONTAP stehen mehrere Konfigurationsparameter zur Verfügung. Diese Parameter werden in der Regel in allen administrativen Schnittstellen unterstützt.

Die Parameternamen können je nach ONTAP-Administratorschnittstelle leicht variieren. Bei der Konfiguration der Remote-Introspektion wird der Endpunkt beispielsweise mit dem CLI-Befehlsparameter identifiziert `-introspection-endpoint`. Aber mit dem System Manager ist das äquivalente Feld *Authorization Server Token Introspection URI*. Um alle ONTAP-Verwaltungsschnittstellen aufzunehmen, wird eine allgemeine Beschreibung der Parameter bereitgestellt. Der genaue Parameter oder das Feld sollte je nach Kontext offensichtlich sein.

Parameter	Beschreibung
Name	Der Name des Autorisierungsservers, der ONTAP bekannt ist.
Applikation	Die ONTAP-interne Anwendung, für die die Definition gilt. Dies muss **http** sein.
Aussteller-URI	Der FQDN mit Pfad, der den Standort oder die Organisation identifiziert, der die Token ausgibt.
Provider-JWKS-URI	Der FQDN mit Pfad und Dateiname, bei dem ONTAP die JSON-Webschlüsselsätze erhält, die zur Validierung der Zugriffstoken verwendet werden.
JWKS-Aktualisierungsintervall	Das Zeitintervall, in dem festgelegt wird, wie oft ONTAP Zertifikatsinformationen vom Provider JWKS URI aktualisiert. Der Wert wird im ISO-8601-Format angegeben.
Introspektion Endpunkt	Der FQDN mit Pfad, den ONTAP zur Remote-Token-Validierung durch Introspektion verwendet.
Client-ID	Der Name des Clients, wie er auf dem Autorisierungsserver definiert ist. Wenn dieser Wert enthalten ist, müssen Sie auch den zugehörigen Client-Schlüssel basierend auf der Schnittstelle angeben.
Ausgehender Proxy	Damit wird der Zugriff auf den Autorisierungsserver ermöglicht, wenn sich ONTAP hinter einer Firewall befindet. Der URI muss im Curl-Format vorliegen.

Parameter	Beschreibung
Verwenden Sie ggf. lokale Rollen	Ein boolesches Flag, das bestimmt, ob die lokalen ONTAP-Definitionen verwendet werden, einschließlich einer benannten REST-Rolle und lokalen Benutzern.
Benutzeranspruch entfernen	Ein alternativer Name, den ONTAP für lokale Benutzer verwendet. Verwenden Sie die `sub` Feld im Zugriffstoken, das mit dem lokalen Benutzernamen übereinstimmt.

Bereitstellungsszenarien

Im Folgenden werden verschiedene gängige Bereitstellungsszenarien vorgestellt. Sie sind abhängig davon organisiert, ob die Token-Validierung lokal durch ONTAP oder Remote durch den Autorisierungsserver durchgeführt wird. Jedes Szenario enthält eine Liste der erforderlichen Konfigurationsoptionen. Siehe "Implementieren Sie OAuth 2.0 in ONTAP" Beispiele für Konfigurationsbefehle.

> Nachdem Sie einen Autorisierungsserver definiert haben, können Sie seine Konfiguration über die ONTAP-Verwaltungsschnittstelle anzeigen. Verwenden Sie beispielsweise den Befehl `security oauth2 client show` Mit der ONTAP CLI.

Lokale Validierung

Die folgenden Bereitstellungsszenarien basieren auf der lokalen Tokenvalidierung durch ONTAP.

Verwenden Sie eigenständige Bereiche ohne Proxy

Dies ist die einfachste Bereitstellung, bei der nur OAuth 2.0 eigenständige Bereiche verwendet werden. Keine der lokalen ONTAP-Identitätsdefinitionen werden verwendet. Sie müssen die folgenden Parameter angeben:

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Aussteller-URI

Sie müssen die Gültigkeitsbereiche auch auf dem Autorisierungsserver hinzufügen.

Verwenden Sie eigenständige Bereiche mit einem Proxy

In diesem Bereitstellungsszenario werden die eigenständigen Oszilloskope von OAuth 2.0 verwendet. Keine der lokalen ONTAP-Identitätsdefinitionen werden verwendet. Aber der Autorisierungsserver befindet sich hinter einer Firewall und Sie müssen daher einen Proxy konfigurieren. Sie müssen die folgenden Parameter angeben:

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Ausgehender Proxy
- Aussteller-URI
- Zielgruppe

Sie müssen die Gültigkeitsbereiche auch auf dem Autorisierungsserver hinzufügen.

Verwenden Sie lokale Benutzerrollen und die standardmäßige Zuweisung von Benutzernamen mit einem Proxy

Dieses Bereitstellungsszenario verwendet lokale Benutzerrollen mit Standardnamenszuordnung. Der Anspruch des Remotebenutzers verwendet den Standardwert `sub` Daher wird dieses Feld im Zugriffstoken verwendet, um mit dem lokalen Benutzernamen zu übereinstimmen. Der Benutzername darf maximal 40 Zeichen lang sein. Der Autorisierungsserver befindet sich hinter einer Firewall, Sie müssen also auch einen Proxy konfigurieren. Sie müssen die folgenden Parameter angeben:

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Verwenden Sie ggf. lokale Rollen (`true`)
- Ausgehender Proxy
- Aussteller

Sie müssen sicherstellen, dass der lokale Benutzer für ONTAP definiert ist.

Verwenden Sie lokale Benutzerrollen und alternative Benutzernamen-Zuordnungen mit einem Proxy

Dieses Bereitstellungsszenario verwendet lokale Benutzerrollen mit einem alternativen Benutzernamen, der für einen lokalen ONTAP-Benutzer verwendet wird. Der Autorisierungsserver befindet sich hinter einer Firewall, Sie müssen also einen Proxy konfigurieren. Sie müssen die folgenden Parameter angeben:

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Verwenden Sie ggf. lokale Rollen (`true`)
- Anspruch des Remote-Benutzers
- Ausgehender Proxy
- Aussteller-URI
- Zielgruppe

Sie müssen sicherstellen, dass der lokale Benutzer für ONTAP definiert ist.

Fernintrospektion

Die folgenden Bereitstellungskonfigurationen basieren auf ONTAP, die Token per Remote-Prüfung durch Introspektion validieren.

Verwenden Sie eigenständige Bereiche ohne Proxy

Dies ist eine einfache Bereitstellung, die auf der Verwendung der eigenständigen Oszilloskope von OAuth 2.0 basiert. Keine der ONTAP-Identitätsdefinitionen wird verwendet. Sie müssen die folgenden Parameter einschließen:

- Name
- Anwendung (http)
- Introspektion Endpunkt
- Client-ID

- Aussteller-URI

Sie müssen die Bereiche sowie den Client- und Client-Schlüssel auf dem Autorisierungsserver definieren.

Client-Authentifizierung mit gegenseitigem TLS

Je nach Ihren Sicherheitsanforderungen können Sie optional Mutual TLS (MTLS) zur Implementierung einer starken Clientauthentifizierung konfigurieren. Bei Verwendung mit ONTAP als Teil einer OAuth 2.0-Bereitstellung garantiert MTLS, dass die Zugriffstoken nur von den Clients verwendet werden, für die sie ursprünglich ausgegeben wurden.

Gegenseitiges TLS mit OAuth 2.0

Transport Layer Security (TLS) wird verwendet, um einen sicheren Kommunikationskanal zwischen zwei Anwendungen herzustellen, in der Regel zwischen einem Client-Browser und einem Webserver. Mutual TLS erweitert dies durch eine starke Identifizierung des Clients über ein Client-Zertifikat. Bei Verwendung in einem ONTAP-Cluster mit OAuth 2.0 wird die Basis-MTLS-Funktionalität durch das Erstellen und Verwenden von Sender-beschränkten Zugriffstoken erweitert.

Ein vom Absender beschränktem Zugriffstoken kann nur vom Client verwendet werden, an den es ursprünglich ausgegeben wurde. Um diese Funktion zu unterstützen, muss ein neuer Bestätigungsantrag gestellt werden (`cnf`) Wird in das Token eingefügt. Das Feld enthält die Eigenschaft `x5t#S256` Enthält einen Digest des Clientzertifikats, das bei der Anforderung des Zugriffstoken verwendet wird. Dieser Wert wird von ONTAP im Rahmen der Überprüfung des Tokens überprüft. Von Autorisierungsservern ausgegebene Zugriffstoken, die nicht durch den Absender eingeschränkt sind, enthalten keinen zusätzlichen Bestätigungsanspruch.

Sie müssen ONTAP so konfigurieren, dass MTLS für jeden Autorisierungsserver separat verwendet wird. Beispiel: Der CLI-Befehl `security oauth2 client` Enthält den Parameter `use-mutual-tls` Zur Steuerung der MTLS-Verarbeitung anhand von drei Werten, wie in der folgenden Tabelle dargestellt.

> In jeder Konfiguration hängen das Ergebnis und die von ONTAP ergriffenen Maßnahmen vom Wert des Konfigurationsparameters sowie vom Inhalt des Zugriffstoken und des Clientzertifikats ab. Die Parameter in der Tabelle sind vom kleinsten bis zum restriktivsten organisiert.

Parameter	Beschreibung
Keine	Die gegenseitige TLS-Authentifizierung OAuth 2.0 ist für den Autorisierungsserver vollständig deaktiviert. ONTAP führt keine MTLS-Clientzertifikatauthentifizierung durch, selbst wenn der Bestätigungsanspruch im Token vorhanden ist oder ein Clientzertifikat mit der TLS-Verbindung geliefert wird.
Anforderung	Die gegenseitige TLS-Authentifizierung von OAuth 2.0 wird erzwungen, wenn ein vom Absender beschränktes Zugriffstoken vom Client angezeigt wird. Das heißt, MTLS wird nur erzwungen, wenn die Bestätigung Anspruch (mit Eigentum `x5t#S256`) Ist im Access-Token vorhanden. Dies ist die Standardeinstellung.
Erforderlich	Die gegenseitige TLS-Authentifizierung OAuth 2.0 wird für alle Zugriffstoken durchgesetzt, die vom Autorisierungsserver ausgegeben werden. Daher müssen alle Zugriffstoken durch den Absender eingeschränkt sein. Die Authentifizierung und die REST-API-Anforderung schlagen fehl, wenn der Bestätigungsanspruch nicht im Zugriffstoken vorhanden ist oder wenn ein ungültiges Clientzertifikat vorliegt.

Grundlegende Implementierungsablaufs

Die typischen Schritte bei der Verwendung von MTLS mit OAuth 2.0 in einer ONTAP-Umgebung sind nachfolgend dargestellt. Siehe "RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication und Certificate-bound Access Tokens" Entnehmen.

Schritt 1: Erstellen und installieren Sie ein Client-Zertifikat

Die Ermittlung der Kundenidentität basiert auf dem Nachweis der Kenntnis eines privaten Kundenschlüssels. Der entsprechende öffentliche Schlüssel wird in ein signiertes X.509-Zertifikat gelegt, das vom Client vorgelegt wird. Auf einer übergeordneten Ebene umfassen die Schritte zur Erstellung des Clientzertifikats Folgendes:

1. Erzeugen Sie ein öffentliches und privates Schlüsselpaar
2. Erstellen Sie eine Zertifikatsignierungsanforderung
3. Senden Sie die CSR-Datei an eine bekannte Zertifizierungsstelle
4. CA überprüft die Anforderung und stellt das signierte Zertifikat aus

Sie können das Clientzertifikat normalerweise in Ihrem lokalen Betriebssystem installieren oder direkt mit einem gängigen Dienstprogramm wie Curl verwenden.

Schritt 2: Konfigurieren Sie ONTAP für die Verwendung von MTLS

Sie müssen ONTAP für die Verwendung von MTLS konfigurieren. Diese Konfiguration erfolgt für jeden Autorisierungsserver separat. Beispielsweise mit dem CLI-Befehl `security oauth2 client` Wird mit dem optionalen Parameter verwendet `use-mutual-tls`. Siehe "Implementieren Sie OAuth 2.0 in ONTAP" Finden Sie weitere Informationen.

Schritt 3: Client fordert ein Zugriffstoken an

Der Client muss ein Zugriffstoken vom Autorisierungsserver anfordern, der für ONTAP konfiguriert ist. Die Client-Anwendung muss MTLS mit dem in Schritt 1 erstellten und installierten Zertifikat verwenden.

Schritt 4: Der Autorisierungsserver generiert das Zugriffstoken

Der Autorisierungsserver überprüft die Clientanforderung und erstellt ein Zugriffstoken. Dazu wird ein Nachrichtendigest des Client-Zertifikats erstellt, das als Bestätigungsforderung im Token enthalten ist (Feld `cnf`).

Schritt 5: Client-Anwendung präsentiert das Zugriffstoken an ONTAP

Die Client-Anwendung führt einen REST-API-Aufruf zum ONTAP-Cluster durch und schließt das Zugriffstoken in den Header der Autorisierungsanforderung als **Bearer Token** ein. Der Client muss MTLS mit demselben Zertifikat verwenden, das für die Anforderung des Zugriffstoken verwendet wird.

Schritt 6: ONTAP überprüft Client und Token.

ONTAP erhält das Zugriffstoken in einer HTTP-Anfrage sowie das Clientzertifikat, das als Teil der MTLS-Verarbeitung verwendet wird. ONTAP validiert zuerst die Signatur im Zugriffstoken. Basierend auf der Konfiguration generiert ONTAP einen Nachrichtendigest des Client-Zertifikats und vergleicht ihn mit dem Bestätigungsanspruch **cnf** im Token. Wenn die beiden Werte übereinstimmen, hat ONTAP bestätigt, dass der Client, der die API-Anforderung erstellt, derselbe Client ist, für den das Zugriffstoken ursprünglich ausgegeben wurde.

Konfiguration und Implementierung

Bereiten Sie die Bereitstellung von OAuth 2.0 mit ONTAP vor

Bevor Sie OAuth 2.0 in einer ONTAP-Umgebung konfigurieren, sollten Sie die Bereitstellung vorbereiten. Im Folgenden finden Sie eine Zusammenfassung der wichtigsten Aufgaben und Entscheidungen. Die Anordnung der Abschnitte ist im Allgemeinen auf die Reihenfolge ausgerichtet, die Sie befolgen sollten. Dies gilt zwar für die meisten Implementierungen, Sie sollten es jedoch bei Bedarf an Ihre Umgebung anpassen. Sie sollten auch die Erstellung eines formellen Bereitstellungsplans in Betracht ziehen.

Je nach Umgebung können Sie die Konfiguration für die Autorisierungsserver auswählen, die für ONTAP definiert sind. Dazu gehören auch die Parameterwerte, die Sie für jeden Bereitstellungstyp spezifisch benötigen. Siehe "OAuth 2.0-Bereitstellungsszenarien" Finden Sie weitere Informationen.

Geschützte Ressourcen und Client-Applikationen

OAuth 2.0 ist ein Autorisierungs-Framework zur Kontrolle des Zugriffs auf geschützte Ressourcen. Aus diesem Grund besteht ein wichtiger erster Schritt bei jeder Bereitstellung darin zu bestimmen, welche Ressourcen verfügbar sind und welche Clients Zugriff darauf benötigen.

Identifizierung von Client-Applikationen

Sie müssen entscheiden, welche Clients OAuth 2.0 bei der Ausgabe von REST-API-Aufrufen verwenden und auf welche API-Endpunkte Zugriff benötigt wird.

Bestehende ONTAP REST-Rollen und lokale Benutzer prüfen

Sie sollten die vorhandenen ONTAP-Identitätsdefinitionen sowie die REST-Rollen und lokalen Benutzer überprüfen. Je nachdem, wie Sie OAuth 2.0 konfigurieren, können diese Definitionen für Zugriffsentscheidungen verwendet werden.

Globaler Übergang zu OAuth 2.0

Obwohl Sie die OAuth 2.0-Autorisierung schrittweise implementieren können, können Sie auch alle REST-API-Clients sofort nach OAuth 2.0 verschieben, indem Sie für jeden Autorisierungsserver ein globales Flag festlegen. Auf diese Weise können Sie basierend auf Ihrer bestehenden ONTAP-Konfiguration Zugriffsentscheidungen treffen, ohne dass Sie in sich geschlossene Bereiche erstellen müssen.

Autorisierungsserver

Die Autorisierungsserver spielen eine wichtige Rolle in Ihrer OAuth 2.0-Bereitstellung, indem sie Zugriffstoken ausgeben und die Verwaltungsrichtlinie durchsetzen.

Wählen Sie den Autorisierungsserver aus, und installieren Sie ihn

Sie müssen einen oder mehrere Autorisierungsserver auswählen und installieren. Es ist wichtig, sich mit den Konfigurationsoptionen und -Verfahren Ihrer Identitätsanbieter vertraut zu machen, einschließlich der Definition von Geltungsbereichen.

Stellen Sie fest, ob das Zertifikat der Autorisierungsstammzertifizierungsstelle installiert werden muss

ONTAP verwendet das Zertifikat des Autorisierungsservers, um die von den Clients präsentierten signierten Zugriffstoken zu validieren. Dazu benötigt ONTAP das Stammzertifizierungsstellenzertifikat und alle Zwischenzertifikate. Diese sind möglicherweise mit ONTAP vorinstalliert. Wenn nicht, müssen Sie sie installieren.

Bewerten Sie den Netzwerkstandort und die -Konfiguration

Wenn sich der Autorisierungsserver hinter einer Firewall befindet, muss ONTAP für die Verwendung eines Proxy-Servers konfiguriert werden.

Client-Authentifizierung und -Autorisierung

Es gibt mehrere Aspekte der Client-Authentifizierung und -Autorisierung, die Sie berücksichtigen müssen.

Eigenständige Bereiche oder lokale ONTAP-Identitätsdefinitionen

Sie können entweder eigenständige Bereiche definieren, die auf dem Autorisierungsserver definiert sind, oder auf die vorhandenen lokalen ONTAP-Identitätsdefinitionen, einschließlich Rollen und Benutzer, zurückgreifen.

Optionen mit lokaler ONTAP-Verarbeitung

Wenn Sie die ONTAP-Identitätsdefinitionen verwenden, müssen Sie entscheiden, welche Anwendung zutrifft. Dazu gehören:

- Benannte REST-Rolle
- Ordnen Sie lokale Benutzer zu
- Active Directory oder LDAP-Gruppen

Lokale Validierung oder Remote-Introspektion

Sie müssen entscheiden, ob die Zugriffstoken lokal durch ONTAP oder auf dem Autorisierungsserver durch Introspektion validiert werden. Es gibt auch mehrere verwandte Werte zu berücksichtigen, wie zum Beispiel das Aktualisierungsintervall.

Zugriffstoken, die durch den Absender eingeschränkt sind

Für Umgebungen, die ein hohes Maß an Sicherheit erfordern, können Sie auf Basis von MTLS sendende Zugriffstoken verwenden. Dies erfordert ein Zertifikat für jeden Client.

Administrationsschnittstelle

Sie können die Verwaltung von OAuth 2.0 über eine der ONTAP-Schnittstellen durchführen, einschließlich:

- Befehlszeilenschnittstelle
- System Manager
- REST API

Wie Clients Zugriffstoken anfordern

Die Client-Anwendungen müssen Zugriffstoken direkt vom Autorisierungsserver anfordern. Sie müssen entscheiden, wie dies geschehen wird, einschließlich der Zuschussart.

Konfigurieren Sie ONTAP

Es gibt mehrere ONTAP-Konfigurationsaufgaben, die Sie durchführen müssen.

Definieren Sie REST-Rollen und lokale Benutzer

Basierend auf Ihrer Autorisierungskonfiguration kann die lokale ONTAP-Identifizieren-Verarbeitung verwendet werden. In diesem Fall müssen Sie die REST-Rollen und Benutzerdefinitionen überprüfen und definieren.

Kernkonfiguration

Zur Durchführung der zentralen ONTAP-Konfiguration sind drei wichtige Schritte erforderlich:

- Installieren Sie optional das Stammzertifikat (und alle Zwischenzertifikate) für die Zertifizierungsstelle, die das Zertifikat des Autorisierungsservers signiert hat.
- Definieren Sie den Autorisierungsserver.
- Aktivieren Sie die OAuth 2.0-Verarbeitung für den Cluster.

Implementieren Sie OAuth 2.0 in ONTAP

Die Bereitstellung der zentralen OAuth 2.0-Funktionalität umfasst drei Hauptschritte.

Bevor Sie beginnen

Sie müssen die Bereitstellung von OAuth 2.0 vorbereiten, bevor Sie ONTAP konfigurieren. Sie müssen beispielsweise den Autorisierungsserver beurteilen, einschließlich der Art und Weise, wie das Zertifikat signiert wurde und ob es sich hinter einer Firewall befindet. Siehe "Bereiten Sie die Bereitstellung von OAuth 2.0 mit ONTAP vor" Finden Sie weitere Informationen.

Schritt 1: Installieren Sie das Zertifikat für den Authentifizierungsserver

ONTAP enthält eine große Anzahl vorinstallierter Stammzertifizierungsstellen-Zertifikate. So wird in vielen Fällen das Zertifikat für Ihren Autorisierungsserver von ONTAP ohne zusätzliche Konfiguration sofort erkannt. Je nachdem, wie das Zertifikat des Autorisierungsservers signiert wurde, müssen Sie möglicherweise ein Stammzertifizierungszertifikat und alle Zwischenzertifikate installieren.

Befolgen Sie die Anweisungen unten, um das Zertifikat zu installieren, falls es benötigt wird. Installieren Sie alle erforderlichen Zertifikate auf Cluster-Ebene.

Wählen Sie das richtige Verfahren, je nachdem, wie Sie auf ONTAP zugreifen.

Beispiel 1. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Klicken Sie neben **Certificates** auf →.
4. Klicken Sie auf der Registerkarte **Vertrauenswürdige Zertifizierungsstellen** auf **Hinzufügen**.
5. Klicken Sie auf **Import** und wählen Sie die Zertifikatdatei aus.
6. Vervollständigen Sie die Konfigurationsparameter für Ihre Umgebung.
7. Klicken Sie Auf **Hinzufügen**.

CLI

1. Starten Sie die Installation:

   ```
   security certificate install -type server-ca
   ```

2. Suchen Sie nach der folgenden Konsolenmeldung:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Öffnen Sie die Zertifikatdatei mit einem Texteditor.
4. Kopieren Sie das gesamte Zertifikat einschließlich der folgenden Zeilen:

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. Fügen Sie das Zertifikat nach der Eingabeaufforderung in das Terminal ein.
6. Drücken Sie **Enter**, um die Installation abzuschließen.
7. Vergewissern Sie sich, dass das Zertifikat installiert ist, indem Sie eine der folgenden Methoden verwenden:

   ```
   security certificate show-user-installed

   security certificate show
   ```

Schritt 2: Konfigurieren des Autorisierungsservers

Sie müssen mindestens einen Autorisierungsserver für ONTAP definieren. Sie sollten die Parameterwerte auf Grundlage Ihres Konfigurations- und Bereitstellungsplans auswählen. Prüfen "OAuth2-Bereitstellungsszenarien" Um die genauen Parameter zu bestimmen, die für Ihre Konfiguration erforderlich sind.

> Um eine Autorisierungsserverdefinition zu ändern, können Sie die vorhandene Definition löschen und eine neue erstellen.

Das folgende Beispiel basiert auf dem ersten einfachen Implementierungsszenario unter "Lokale Validierung".

Eigenständige Bereiche werden ohne Proxy verwendet.

Wählen Sie das richtige Verfahren, je nachdem, wie Sie auf ONTAP zugreifen. Das CLI-Verfahren verwendet symbolische Variablen, die Sie vor der Ausgabe des Befehls ersetzen müssen.

Beispiel 2. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Klicken Sie neben **OAuth 2.0 Authorization** auf **+**.
4. Wählen Sie **Weitere Optionen**.
5. Geben Sie die erforderlichen Werte für Ihre Bereitstellung an, z. B.:
   - Name
   - Anwendung (http)
   - Provider-JWKS-URI
   - Aussteller-URI
6. Klicken Sie Auf **Hinzufügen**.

CLI

1. Erstellen Sie die Definition erneut:

   ```
   security oauth2 client create -config-name <NAME> -provider-jwks-uri
   <URI_JWKS> -application http -issuer <URI_ISSUER>
   ```

   Beispiel:

   ```
   security oauth2 client create \
   -config-name auth0 \
   -provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
   realm/protocol/openid-connect/certs \
   -application http \
   -issuer https://superzap.dev.netapp.com:8443/realms/my-realm
   ```

Schritt 3: Aktivieren Sie OAuth 2.0

Der letzte Schritt ist die Aktivierung von OAuth 2.0. Dies ist eine globale Einstellung für das ONTAP Cluster.

> Aktivieren Sie die OAuth 2.0-Verarbeitung erst, wenn Sie bestätigen, dass ONTAP, die Autorisierungsserver und alle unterstützenden Dienste ordnungsgemäß konfiguriert wurden.

Wählen Sie das richtige Verfahren, je nachdem, wie Sie auf ONTAP zugreifen.

Beispiel 3. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Klicken Sie neben **OAuth 2.0 Authorization** auf →.
4. Aktivieren Sie **OAuth 2.0-Autorisierung**.

CLI

1. OAuth 2.0 aktivieren:

   ```
   security oauth2 modify -enabled true
   ```

2. Bestätigen Sie, dass OAuth 2.0 aktiviert ist:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Geben Sie einen REST-API-Aufruf mit OAuth 2.0 aus

Die OAuth 2.0-Implementierung in ONTAP unterstützt REST-API-Client-Applikationen. Sie können einen einfachen REST API-Aufruf mit Curl ausgeben, um mit OAuth 2.0 zu beginnen. Im folgenden Beispiel wird die ONTAP Cluster-Version abgerufen.

Bevor Sie beginnen

Sie müssen die Funktion OAuth 2.0 für Ihren ONTAP-Cluster konfigurieren und aktivieren. Dazu gehört auch die Definition eines Autorisierungsservers.

Schritt 1: Erwerben Sie ein Zugriffstoken

Sie müssen ein Zugriffstoken erwerben, um es mit dem REST-API-Aufruf zu verwenden. Die Token-Anforderung wird außerhalb von ONTAP ausgeführt, und die genaue Vorgehensweise hängt vom Autorisierungsserver und seiner Konfiguration ab. Sie können das Token über einen Webbrowser, mit einem Curl-Befehl oder mit einer Programmiersprache anfordern.

Zur Veranschaulichung wird unten ein Beispiel gezeigt, wie ein Zugriffstoken von Keycloak mit Curl angefordert werden kann.

Keycloak Beispiel

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

Sie sollten das zurückgegebene Token kopieren und speichern.

Schritt 2: Geben Sie den REST API-Aufruf aus

Nachdem Sie über ein gültiges Zugriffstoken verfügen, können Sie einen Curl-Befehl mit dem Zugriffstoken verwenden, um einen REST-API-Aufruf auszustellen.

Parameter und Variablen

Die beiden Variablen im Beispiel Curl sind in der folgenden Tabelle beschrieben.

Variabel	Beschreibung
FQDN_IP-DOLLAR	Der vollständig qualifizierte Domain-Name oder die IP-Adresse der ONTAP Management LIF.
ACCESS_TOKEN IN HÖHE VON USD	Das vom Autorisierungsserver ausgegebene Zugriffstoken OAuth 2.0.

Sie sollten diese Variablen zuerst in der Bash Shell-Umgebung festlegen, bevor Sie das Curl-Beispiel ausgeben. Geben Sie beispielsweise in der Linux CLI den folgenden Befehl ein, um die FQDN-Variable festzulegen und anzuzeigen:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

Nachdem beide Variablen in Ihrer lokalen Bash Shell definiert wurden, können Sie den Curl-Befehl kopieren und in die CLI einfügen. Drücken Sie **Enter**, um die Variablen zu ersetzen und den Befehl auszugeben.

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

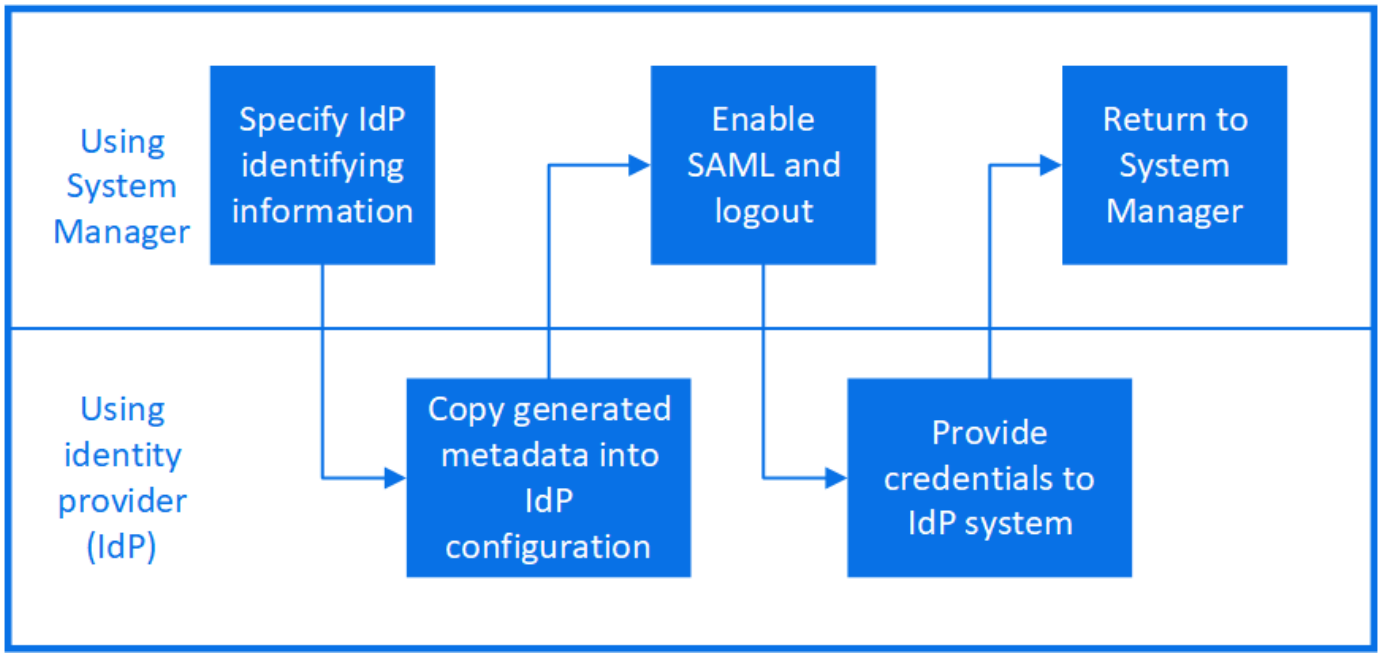
Konfigurieren Sie die SAML-Authentifizierung

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 Verzeichnisdienstanbietern wie Active Directory und LDAP authentifiziert.

Aktivieren Sie die SAML-Authentifizierung

Führen Sie die folgenden Schritte durch, um die SAML-Authentifizierung mit System Manager oder mit der CLI zu aktivieren. Wenn auf Ihrem Cluster ONTAP 9.7 oder eine frühere Version ausgeführt wird, sind die zu befolgenden Schritte in System Manager unterschiedlich. Weitere Informationen finden Sie in der System Manager Online-Hilfe, die auf Ihrem System verfügbar ist.

> Nach der Aktivierung der SAML-Authentifizierung können nur Remote-Benutzer auf die System Manager GUI zugreifen. Lokale Benutzer können nach Aktivierung der SAML-Authentifizierung nicht auf die System Manager-GUI zugreifen.



Bevor Sie beginnen

- Der IdP, den Sie für die Remote-Authentifizierung verwenden möchten, muss konfiguriert werden.

  > Lesen Sie die Dokumentation, die von der von Ihnen konfigurierten IdP bereitgestellt wird.

- Sie müssen die URI des IdP haben.

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.

Die folgenden IDPs wurden mit System Manager validiert:

- Active Directory Federation Services
- Cisco DUO (validiert mit den folgenden ONTAP-Versionen:)
  - 9.7P21 und neuere Versionen 9.7 (siehe "Dokumentation zu System Manager Classic")
  - 9.8P17 und höher 9.8
  - 9.9.1P13 und höher 9.9 Versionen
  - 9.10.1P9 und höher 9.10 Versionen
  - 9.11.1P4 und höher Version 9.11
  - 9.12.1 und höhere Versionen
- Shibboleth

Führen Sie je nach Umgebung die folgenden Schritte aus:

Beispiel 4. Schritte

System Manager

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie neben **SAML Authentication** auf ⚙.
3. Vergewissern Sie sich, dass das Kontrollkästchen **SAML-Authentifizierung aktivieren** aktiviert ist.
4. Geben Sie die URL der IdP-URI ein (einschließlich .
5. Ändern Sie die Host-System-Adresse, falls erforderlich.
6. Stellen Sie sicher, dass das richtige Zertifikat verwendet wird:
   - Wenn Ihr System nur mit einem Zertifikat mit dem Typ „Server“ zugeordnet war, wird dieses Zertifikat als Standard betrachtet und nicht angezeigt.
   - Wenn Ihr System mit mehreren Zertifikaten als Servertyp zugeordnet war, wird eines der Zertifikate angezeigt. Um ein anderes Zertifikat auszuwählen, klicken Sie auf **Ändern**.
7. Klicken Sie Auf **Speichern**. In einem Bestätigungsfenster werden die Metadateninformationen angezeigt, die automatisch in die Zwischenablage kopiert wurden.
8. Gehen Sie zum IdP-System, das Sie angegeben haben, und kopieren Sie die Metadaten aus der Zwischenablage, um die Systemmetadaten zu aktualisieren.
9. Kehren Sie zum Bestätigungsfenster (im System Manager) zurück und aktivieren Sie das Kontrollkästchen **Ich habe den IdP mit dem Host-URI oder Metadaten** konfiguriert.
10. Klicken Sie auf **Abmelden**, um SAML-basierte Authentifizierung zu aktivieren. Das IdP-System zeigt einen Authentifizierungsbildschirm an.
11. Geben Sie im IdP-System Ihre SAML-basierten Anmeldedaten ein. Nach der Überprüfung Ihrer Anmeldedaten werden Sie zur System Manager Startseite weitergeleitet.

CLI

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 Zertifikatinformationen des ONTAP-Webservers verwendet.

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

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://10.0.0.1/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

Second
User/Group                  Authentication                 Acct
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**
```

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.

Führen Sie je nach Umgebung die folgenden Schritte aus:

Beispiel 5. Schritte

System Manager

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie unter **SAML Authentication** auf die Schaltfläche **aktiviert**.
3. *Optional*: Sie können auch klicken ⚙ Neben **SAML Authentication** deaktivieren Sie dann das Kontrollkästchen **SAML Authentication** aktivieren.

CLI

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.
```

Verwandte Informationen

"ONTAP 9-Befehle"

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.

Ihr Ziel ist	Befehl
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

"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	`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

"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	`security ssl modify`
Zeigt den SSL-Konfigurations- und Zertifikatnamen für die Cluster-oranSVM 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*.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
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.
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.

Überprüfen Sie die Identität der Remoteserver mit Zertifikaten

Überprüfen Sie die Identität von Remote-Servern mithilfe der Zertifikatübersicht

ONTAP unterstützt die Funktionen für Sicherheitszertifikate zur Überprüfung der Identität von Remote-Servern.

Die ONTAP Software ermöglicht sichere Verbindungen unter Verwendung dieser digitalen Zertifikatfunktionen und -Protokolle:

- Online Certificate Status Protocol (OCSP) validiert den Status von digitalen Zertifikatsanforderungen von ONTAP-Diensten mithilfe von SSL- und TLS-Verbindungen (Transport Layer Security). Diese Funktion ist standardmäßig deaktiviert.
- Die ONTAP-Software enthält standardmäßig vertrauenswürdige Stammzertifikate.
- KMIP-Zertifikate (Key Management Interoperability Protocol) ermöglichen die gegenseitige Authentifizierung eines Clusters und eines KMIP-Servers.

Überprüfen Sie, ob digitale Zertifikate mit OCSP gültig sind

Ab ONTAP 9.2 ermöglicht OCSP (Online Certificate Status Protocol) ONTAP-Anwendungen, die TLS-Kommunikation (Transport Layer Security) nutzen, den digitalen Zertifikatsstatus zu erhalten, wenn OCSP aktiviert ist. Sie können OCSP-Zertifikatsprüfungen für bestimmte Anwendungen jederzeit aktivieren oder deaktivieren. Standardmäßig ist die Überprüfung des OCSP-Zertifikatsstatus deaktiviert.

Was Sie benötigen

Sie benötigen einen erweiterten Zugriff auf die Berechtigungsebene, um diese Aufgabe ausführen zu können.

Über diese Aufgabe

OCSP unterstützt folgende Anwendungen:

- AutoSupport
- Event Management System (EMS)
- LDAP über TLS
- Key Management Interoperability Protocol (KMIP)
- Audit-Protokollierung
- FabricPool
- SSH (ab ONTAP 9.13.1)

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`.
2. Um OCSP-Zertifikatsprüfungen für bestimmte ONTAP-Anwendungen zu aktivieren oder zu deaktivieren, verwenden Sie den entsprechenden Befehl.

Wenn Sie möchten, dass OCSP-Zertifikatsprüfungen für einige Anwendungen…	Verwenden Sie den Befehl…
Aktiviert	`security config ocsp enable -app` app name
Deaktiviert	`security config ocsp disable -app` app name

   Mit dem folgenden Befehl wird OCSP-Unterstützung für AutoSupport und EMS aktiviert.

```
cluster::*> security config ocsp enable -app asup,ems
```

   Wenn OCSP aktiviert ist, erhält die Anwendung eine der folgenden Antworten:

   - Gut - das Zertifikat ist gültig und die Kommunikation wird fortgesetzt.
   - Widerrufen: Das Zertifikat wird von der ausstellenden Zertifizierungsstelle dauerhaft als nicht vertrauenswürdig eingestuft und die Kommunikation kann nicht fortgesetzt werden.
   - Unbekannt – der Server verfügt über keine Statusinformationen zum Zertifikat und die Kommunikation kann nicht fortgesetzt werden.
   - OCSP-Serverinformationen fehlen im Zertifikat - der Server fungiert als deaktiviert und fährt mit der TLS-Kommunikation fort, aber es erfolgt keine Statusüberprüfung.
   - Keine Antwort vom OCSP-Server - die Anwendung schlägt fehl.
3. Verwenden Sie den entsprechenden Befehl, um OCSP-Zertifikatsprüfungen für alle Anwendungen mithilfe von TLS-Kommunikation zu aktivieren oder zu deaktivieren.

Wenn Sie möchten, dass OCSP-Zertifikatsprüfungen für alle Anwendungen durchgeführt werden…	Verwenden Sie den Befehl…

Aktiviert	`security config ocsp enable`
	
	`-app all`

Deaktiviert	`security config ocsp disable`
	
	`-app all`

Wenn alle Applikationen aktiviert sind, wird eine signierte Antwort empfangen, die angibt, dass das angegebene Zertifikat in Ordnung, annulliert oder unbekannt ist. Im Fall eines annulliert Zertifikats kann die Anwendung nicht fortgesetzt werden. Wenn die Anwendung keine Antwort vom OCSP-Server erhält oder der Server nicht erreichbar ist, wird die Anwendung nicht fortgesetzt.

4. Verwenden Sie die `security config ocsp show` Befehl zur Anzeige aller Applikationen, die OCSP unterstützen, und ihres Supportstatus.

```
cluster::*> security config ocsp show
         Application                        OCSP Enabled?
         --------------------               ---------------------
         autosupport                        false
         audit_log                          false
         fabricpool                         false
         ems                                false
         kmip                               false
         ldap_ad                            true
         ldap_nis_namemap                   true
         ssh                                true

         8 entries were displayed.
```

Anzeigen von Standardzertifikaten für TLS-basierte Anwendungen

Ab ONTAP 9.2 bietet ONTAP einen Standardsatz an vertrauenswürdigen Root-Zertifikaten für ONTAP-Anwendungen mithilfe von Transport Layer Security (TLS).

Was Sie benötigen

Die Standardzertifikate werden während der Erstellung oder beim Upgrade auf ONTAP 9.2 nur auf der Administrator-SVM installiert.

Über diese Aufgabe

Die aktuellen Applikationen, die als Client fungieren und eine Zertifikatvalidierung erfordern, sind AutoSupport, EMS, LDAP, Audit Logging, FabricPool, Und KMIP.

Wenn Zertifikate ablaufen, wird eine EMS-Nachricht aufgerufen, die den Benutzer zum Löschen der Zertifikate auffordert. Die Standardzertifikate können nur auf der erweiterten Berechtigungsebene gelöscht werden.

> Das Löschen der Standardzertifikate kann dazu führen, dass einige ONTAP-Anwendungen nicht wie erwartet funktionieren (z. B. AutoSupport- und Audit-Protokollierung).

Schritt

1. Sie können die Standardzertifikate, die auf der Admin-SVM installiert sind, anzeigen. Verwenden Sie dazu den Befehl „Security Certificate show“:

   `security certificate show -vserver –type server-ca`

   ```
   fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
   -type server-ca
   Vserver    Serial Number   Common Name                             Type
   ---------- --------------- ---------------------------------------
   ------------
   fas2552-2n-abc-3
              01              AAACertificateServices
   server-ca
       Certificate Authority: AAA Certificate Services
             Expiration Date: Sun Dec 31 18:59:59 2028
   ```

Cluster und KMIP-Server authentifizieren sich gegenseitig

Die Authentifizierung des Clusters und eine Übersicht über KMIP-Server wurden gegenseitig überprüft

Durch die gegenseitige Authentifizierung des Clusters und eines externen Schlüsselmanagers wie einem KMIP-Server (Key Management Interoperability Protocol) kann der Schlüsselmanager mithilfe von KMIP über SSL mit dem Cluster kommunizieren. Sie tun dies, wenn eine Applikation oder eine bestimmte Funktion (z. B. die Storage-Verschlüsselung) sicheren Datenzugriff mit sicheren Schlüsseln erfordert.

Generieren Sie eine Anforderung zum Signieren eines Zertifikats für das Cluster

Sie können das Sicherheitszertifikat verwenden `generate-csr` Befehl zum Generieren einer Zertifikatsignierungsanforderung (CSR). Nach Bearbeitung Ihrer Anfrage sendet Ihnen die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Was Sie benötigen

Um diese Aufgabe auszuführen, müssen Sie ein Cluster-Administrator oder SVM-Administrator sein.

Schritte

1. CSR erstellen:

security certificate generate-csr -common-name *FQDN_or_common_name* -size 512|1024|1536|2048 -country *country* -state *state* -locality *locality* -organization *organization* -unit *unit* -email-addr *email_of_contact* -hash -function SHA1|SHA256|MD5

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

Der folgende Befehl erzeugt einen CSR mit einem 2,048-bit privaten Schlüssel, der von der SHA256 Hashing-Funktion erzeugt wird, zur Verwendung durch die Software-Gruppe in der IT-Abteilung eines Unternehmens mit individuellem gemeinsamen Namen server1.companyname.com, mit Sitz in Sunnyvale, Kalifornien, USA. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet web@example.com. Das System zeigt den CSR und den privaten Schlüssel in der Ausgabe an.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Kopieren Sie die Zertifikatanforderung aus der CSR-Ausgabe, und senden Sie sie dann in elektronischer Form (z. B. E-Mail) an eine vertrauenswürdige Drittanbieter-CA zum Signieren.

   Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat. Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten digitalen Zertifikats aufbewahren.

Installieren Sie ein von einer Zertifizierungsstelle signiertes Serverzertifikat für das Cluster

Damit ein SSL-Server die Authentifizierung des Clusters oder der Storage Virtual Machine (SVM) als SSL-Client aktiviert, installieren Sie ein digitales Zertifikat mit dem Clienttyp auf dem Cluster oder der SVM. Anschließend stellen Sie dem SSL-Serveradministrator das Client-Ca-Zertifikat zur Installation auf dem Server zur Verfügung.

Was Sie benötigen

Sie müssen bereits das Stammzertifikat des SSL-Servers auf dem Cluster oder SVM mit dem installiert haben `server-ca` Zertifikatstyp.

Schritte

1. Um ein selbstsigniertes digitales Zertifikat für die Clientauthentifizierung zu verwenden, verwenden Sie das `security certificate create` Befehl mit dem `type client` Parameter.
2. Gehen Sie wie folgt vor, um ein von einer Zertifizierungsstelle signiertes digitales Zertifikat für die Clientauthentifizierung zu verwenden:

   a. Generieren Sie mithilfe des Sicherheitszertifikats eine digitale Zertifikatsignierungsanforderung (CSR) `generate-csr` Befehl.

      ONTAP zeigt die CSR-Ausgabe an, die eine Zertifikatanforderung und einen privaten Schlüssel enthält, und erinnert Sie daran, die Ausgabe in eine Datei zu kopieren, um sie später verwenden zu können.

   b. Senden Sie die Zertifikatsanforderung von der CSR-Ausgabe in einem elektronischen Formular (z. B. E-Mail) an eine vertrauenswürdige CA zum Signieren.

      Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten Zertifikats für zukünftige Referenz aufbewahren.

   Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat.

   a. Installieren Sie das CA-signierte Zertifikat mithilfe der `security certificate install` Befehl mit dem `-type client` Parameter.
   b. Geben Sie das Zertifikat und den privaten Schlüssel ein, wenn Sie dazu aufgefordert werden, und drücken Sie dann **Enter**.
   c. Geben Sie bei der Aufforderung zusätzliche Root- oder Zwischenzertifikate ein, und drücken Sie dann **Enter**.

      Sie installieren ein Zwischenzertifikat auf dem Cluster oder der SVM, wenn eine Zertifikatkette, die an der vertrauenswürdigen Stammzertifizierungsstelle beginnt und mit dem Ihnen ausgestellten SSL-Zertifikat endet, die Zwischenzertifikate fehlen. Ein Zwischenzertifikat ist ein vom vertrauenswürdigen Stammverzeichnis herausgegebenem untergeordneten Zertifikat, das speziell für die Ausgabe von Serverzertifikaten der Endeinheit ausgegeben wird. Das Ergebnis ist eine Zertifikatskette, die an der vertrauenswürdigen Stammzertifizierungsstelle beginnt, durch das Zwischenzertifikat geht und mit dem Ihnen ausgestellten SSL-Zertifikat endet.

3. Versorgen `client-ca` Zertifikat des Clusters oder der SVM an den Administrator des SSL-Servers zur Installation auf dem Server.

Der Befehl zum Anzeigen des Sicherheitszertifikats mit dem `-instance` Und `-type client-ca` Parameter zeigt das an `client-ca` Zertifikatsinformationen

Installieren Sie ein CA-signiertes Client-Zertifikat für den KMIP-Server

Der Zertifikatsubtyp des Key Management Interoperability Protocol (KMIP) (der Parameter -subtype kmip-cert) legt gemeinsam mit den Client- und Server-Ca-Typen fest, dass das Zertifikat für die wechselseitige Authentifizierung des Clusters und einen externen Schlüsselmanager, z. B. einen KMIP-Server, verwendet wird.

Über diese Aufgabe

Installieren Sie ein KMIP-Zertifikat, um einen KMIP-Server als SSL-Server für das Cluster zu authentifizieren.

Schritte

1. Verwenden Sie die `security certificate install` Befehl mit dem `-type server-ca` Und `-subtype kmip-cert` Parameter zur Installation eines KMIP-Zertifikats für den KMIP-Server.
2. Wenn Sie aufgefordert werden, geben Sie das Zertifikat ein, und drücken Sie anschließend die Eingabetaste.

   ONTAP erinnert Sie daran, dass Sie eine Kopie des Zertifikats zur späteren Verwendung aufbewahren.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```