



Management der Administratorauthentifizierung und RBAC mit der CLI

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

- Management der Administratorauthentifizierung und RBAC mit der CLI 1
 - Administratorauthentifizierung und RBAC – Übersicht mit der CLI 1
 - Administratorauthentifizierung und RBAC-Workflow 1
- Arbeitsblätter für die Administratorauthentifizierung und die RBAC-Konfiguration 3
- Erstellen von Anmeldekonten 14
- Management von Zugriffssteuerungsrollen 24
- Verwalten von Administratorkonten 30
- Management der Verifizierung von mehreren Administratoren 44

Management der Administratorauthentifizierung und RBAC mit der CLI

Administratorauthentifizierung und RBAC – Übersicht mit der CLI

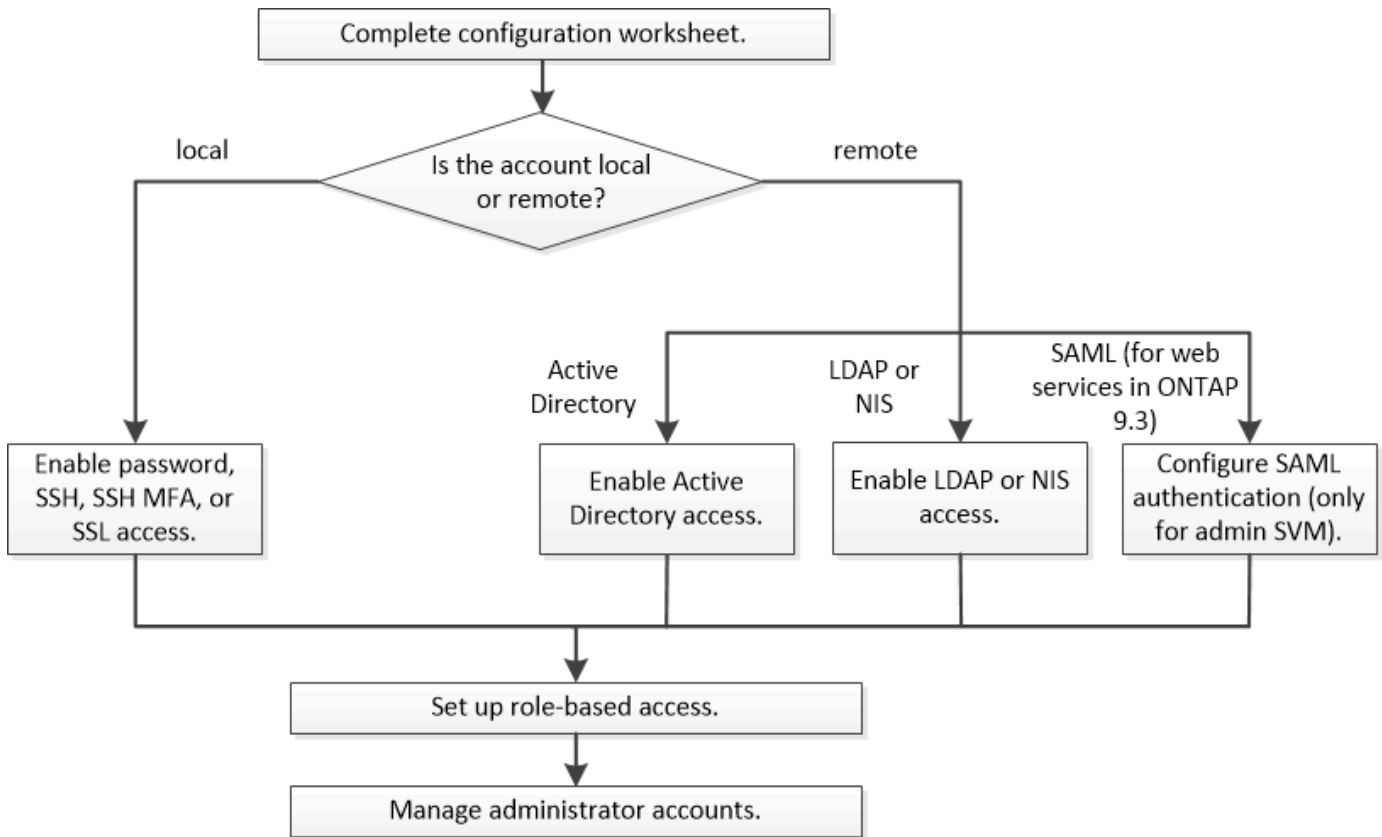
Sie können Anmeldekonto für ONTAP Cluster-Administratoren und SVM-Administratoren (Storage Virtual Machine) aktivieren. Zudem können Sie mithilfe der rollenbasierten Zugriffssteuerung (RBAC) die Funktionen von Administratoren definieren.

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 aktivieren, um auf eine Storage Virtual Machine (SVM) zuzugreifen. Sie stellen dieselben Werte mit `security login modify` Befehl Wenn Sie ändern, wie ein Konto auf eine SVM zugreift.

Feld	Beschreibung	Ihr Wert
<code>-vserver</code>	Der Name der SVM, auf die das Konto zugreift. Der Standardwert ist der Name der Admin-SVM für das Cluster.	
<code>-user-or-group-name</code>	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.	
<code>-application</code>	Die Applikation für den Zugriff auf die SVM: <ul style="list-style-type: none">• <code>http</code>• <code>ontapi</code>• <code>snmp</code>• <code>ssh</code>	

-authmethod	<p>Die Methode, die zur Authentifizierung des Kontos verwendet wird:</p> <ul style="list-style-type: none"> • <code>cert</code> Für die SSL-Zertifikatauthentifizierung • <code>domain</code> Für die Active Directory-Authentifizierung • <code>nsswitch</code> Für LDAP- oder NIS-Authentifizierung • <code>password</code> Für die Authentifizierung von Benutzerpasswörtern • <code>publickey</code> Für die Authentifizierung eines öffentlichen Schlüssels • <code>community</code> Für SNMP-Community-Strings • <code>usm</code> Für SNMP-Sicherheitsmodell • <code>saml</code> Für die SAML-Authentifizierung (Security Assertion Markup Language) 	
-remote-switch-ipaddress	<p>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 handeln, der von der MetroCluster-Systemzustandsüberwachung (MCC-HM) überwacht wird. Diese Option ist nur anwendbar, wenn die Anwendung ist <code>snmp</code> Und die Authentifizierungsmethode lautet <code>usm</code>.</p>	
-role	<p>Die Zugriffskontrollrolle, die dem Konto zugewiesen ist:</p> <ul style="list-style-type: none"> • Für das Cluster (die Admin-SVM) lautet der Standardwert <code>admin</code>. • Für eine Daten-SVM ist der Standardwert <code>vsadmin</code>. 	

-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	<p>Zweite Authentifizierungsmethode bei Multi-Faktor-Authentifizierung in ONTAP 9.3:</p> <ul style="list-style-type: none"> • <code>none</code> Bei Nichtnutzen der Multi-Faktor-Authentifizierung ist der Standardwert • <code>publickey</code> Für die Authentifizierung eines öffentlichen Schlüssels, wenn der aktiviert ist <code>authmethod</code> Ist Passwort oder <code>nswitch</code> • <code>password</code> Für die Authentifizierung von Benutzerpasswörtern, wenn der verwendet wird <code>authmethod</code> Ist ein öffentlicher Schlüssel • <code>nswitch</code> Für die Authentifizierung von Benutzerpasswörtern, wenn die <code>authmethod</code> <code>Publickey</code> ist <div style="border-left: 1px solid black; padding-left: 10px; margin-left: 20px;">  <p>Ab ONTAP 9.4 ist auch Unterstützung für <code>nswitch</code> verfügbar.</p> </div> <p>Die Reihenfolge der Authentifizierung ist immer der öffentliche Schlüssel gefolgt vom Passwort.</p>	

-is-ldap-fastbind	<p>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 nswitch. "Erfahren Sie mehr über LDAP fastbind für nswitch Authentifizierung."</p>	
-------------------	---	--

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 SVM, die der Rolle zugeordnet 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.	

<p>-access</p>	<p>(Optional) der Zugriffsebene für die Rolle. Für Befehlsverzeichnisse:</p> <ul style="list-style-type: none"> • 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 <p>Für <i>nonintrinsic</i> Befehle (Befehle, die nicht enden create, modify, delete, Oder show):</p> <ul style="list-style-type: none"> • none (Der Standardwert für benutzerdefinierte Rollen) verweigert den Zugriff auf den Befehl • readonly Ist nicht zutreffend • all Gewährt Zugriff auf den Befehl <p>Um den Zugriff auf intrinsische Befehle zu gewähren oder zu verweigern, müssen Sie das Befehlsverzeichnis angeben.</p>	
<p>-query</p>	<p>(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.</p>	

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
<code>-vserver</code>	(Optional) der Name der SVM, auf die das Konto zugreift.	
<code>-username</code>	Der Benutzername des Kontos. Der Standardwert, <code>admin</code> , Dies ist der Standardname des Cluster-Administrators.	
<code>-index</code>	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.	
<code>-publickey</code>	Der öffentliche OpenSSH-Schlüssel. Sie sollten den Schlüssel in doppelte Anführungszeichen (") setzen.	
<code>-role</code>	Die Zugriffskontrollrolle, die dem Konto zugewiesen ist.	
<code>-comment</code>	(Optional) Beschreibungstext für den öffentlichen Schlüssel. Sie sollten den Text in doppelte Anführungszeichen (") einschließen.	

Installieren Sie ein digitales Zertifikat für einen CA-signierten Server

Sie stellen diese Werte dem zur Verfügung `security certificate generate-csr` Befehl beim Generieren einer CSR (Digital Certificate Signing Request) zur Verwendung bei der Authentifizierung einer SVM als SSL-Server.

Feld	Beschreibung	Ihr Wert
------	--------------	----------

<code>-common-name</code>	Der Name des Zertifikats, bei dem es sich um einen vollständig qualifizierten Domänennamen (FQDN) oder einen benutzerdefinierten gemeinsamen Namen handelt.	
<code>-size</code>	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.	
<code>-country</code>	Das Land der SVM in einem Code, der aus zwei Buchstaben besteht. Der Standardwert ist <code>us</code> . Eine Liste der Codes finden Sie auf den man-Pages.	
<code>-state</code>	Bundesstaat oder Provinz der SVM	
<code>-locality</code>	Der Lokalität der SVM.	
<code>-organization</code>	Der Organisation der SVM.	
<code>-unit</code>	Der Einheit, die in der Organisation der SVM enthalten ist.	
<code>-email-addr</code>	Die E-Mail-Adresse des Ansprechpartners für die SVM.	
<code>-hash-function</code>	Die kryptografische Hashing-Funktion zum Signieren des Zertifikats. Der Standardwert ist <code>SHA256</code> . Mögliche Werte sind <code>SHA1</code> , <code>SHA256</code> , und <code>MD5</code> .	

Sie stellen diese Werte dem zur Verfügung `security certificate install` Befehl bei der Installation eines digitalen CA-signierten Zertifikats zur Authentifizierung des Clusters oder der SVM als SSL-Server. In der folgenden Tabelle sind nur die Optionen aufgeführt, die für die Kontenkonfiguration relevant sind.

Feld	Beschreibung	Ihr Wert
<code>-vserver</code>	Der Name der SVM, auf der das Zertifikat installiert werden soll.	

-type	<p>Der Zertifikatstyp:</p> <ul style="list-style-type: none"> • <code>server</code> Für Serverzertifikate und Zwischenzertifikate • <code>client-ca</code> Für das öffentliche Schlüsselzertifikat der Root-CA des SSL-Clients • <code>server-ca</code> Für das öffentliche Schlüsselzertifikat der Root-CA des SSL-Servers, von dem ONTAP ein Client ist • <code>client</code> 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 Daten-SVM konfiguriert haben und Sie die SVM als Gateway oder „*Tunnel*“ für den Zugriff des Active Directory-Domänencontrollers auf das Cluster konfigurieren möchten.

Feld	Beschreibung	Ihr Wert
-vserver	Der Name der SVM, 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 SVM-Computerkonto in der Active Directory-Domäne erstellen möchten.

Feld	Beschreibung	Ihr Wert
-vserver	Der Name der SVM, 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 Domännennamen 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 beim Erstellen einer LDAP-Client-Konfiguration für die SVM.



Ab ONTAP 9.2 beginnt der `-ldap-servers` Feld ersetzt das `-servers` Feld. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse als Wert für den LDAP-Server verwenden.

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

Feld	Beschreibung	Ihr Wert
<code>-vserver</code>	Der Name der SVM für die Client-Konfiguration.	
<code>-client-config</code>	Der Name der Client-Konfiguration.	
<code>-servers</code>	ONTAP 9.0, 9.1: Eine kommagetrennte Liste von IP-Adressen für die LDAP-Server, mit denen der Client verbunden wird.	
<code>-ldap-servers</code>	ONTAP 9.2: Eine kommagetrennte Liste von IP-Adressen und Hostnamen für die LDAP-Server, mit denen der Client verbunden ist.	
<code>-schema</code>	Das Schema, das der Client zum Erstellen von LDAP-Abfragen verwendet.	

-use-start-tls	<p>Gibt an, ob der Client die Kommunikation mit dem LDAP-Server über Start TLS verschlüsselt (<code>true</code> Oder <code>false</code>).</p>	
	<p> Start TLS wird nur für den Zugriff auf Data SVMs unterstützt. Der Zugriff auf Admin-SVMs wird nicht unterstützt.</p>	

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

Feld	Beschreibung	Ihr Wert
-vserver	Der Name der SVM, der die Client-Konfiguration zugeordnet werden soll.	
-client-config	Der Name der Client-Konfiguration.	
-client-enabled	Gibt an, ob die SVM die LDAP-Client-Konfiguration verwenden kann (<code>true</code> Oder <code>false</code>).	

Sie stellen diese Werte dem zur Verfügung `vserver services name-service nis-domain create` Befehl beim Erstellen einer NIS-Domänenkonfiguration auf einer SVM.



Ab ONTAP 9.2 beginnt der `-nis-servers` Feld ersetzt das `-servers` Feld. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse als Wert für den NIS-Server verwenden.

Feld	Beschreibung	Ihr Wert
-vserver	Der Name der SVM, auf der die Domänenkonfiguration erstellt werden soll.	
-domain	Der Name der Domäne.	
-active	Gibt an, ob die Domäne aktiv ist (<code>true</code> Oder <code>false</code>).	

<code>-servers</code>	ONTAP 9.0, 9.1: Eine kommagetrennte Liste von IP-Adressen für die NIS-Server, die von der Domänenkonfiguration verwendet werden.	
<code>-nis-servers</code>	ONTAP 9.2: Eine kommagetrennte 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
<code>-vserver</code>	Der Name der SVM, auf der der Name Service-Look-Up-Auftrag konfiguriert werden soll.	
<code>-database</code>	Die Namensdienstdatenbank: <ul style="list-style-type: none"> • <code>hosts</code> Für Dateien und DNS-Namensdienste • <code>group</code> Für Dateien, LDAP und NIS-Name-Services • <code>passwd</code> Für Dateien, LDAP und NIS-Name-Services • <code>netgroup</code> Für Dateien, LDAP und NIS-Name-Services • <code>namemap</code> Für Dateien und LDAP-Namensdienste 	
<code>-sources</code>	Die Reihenfolge, in der Sie Namensdienstquellen suchen (in einer kommagetrennten Liste): <ul style="list-style-type: none"> • <code>files</code> • <code>dns</code> • <code>ldap</code> • <code>nis</code> 	

Konfigurieren Sie den SAML-Zugriff

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

Feld	Beschreibung	Ihr Wert
<code>-idp-uri</code>	Die FTP-Adresse oder HTTP-Adresse des IdP-Hosts (Identity Provider), von dem aus die IdP-Metadaten heruntergeladen werden können.	
<code>-sp-host</code>	Der Hostname oder die IP-Adresse des Host des SAML-Service-Providers (ONTAP-System). Standardmäßig wird die IP-Adresse der Cluster-Management-LIF verwendet.	
<code>-cert-ca</code> Und <code>-cert-serial</code> , Oder <code>-cert-common-name</code>	Die Serverzertifikatdetails des Host des Service-Providers (ONTAP-System). Sie können entweder die Zertifizierungsstelle des Diensteanbieters und die Seriennummer des Zertifikats oder den allgemeinen Serverzertifikats eingeben.	
<code>-verify-metadata-server</code>	Gibt an, ob die Identität des IdP-Metadatenservers validiert werden muss (<code>true</code> Oder <code>false</code>). Die Best Practice besteht darin, diesen Wert immer auf festzulegen <code>true</code> .	

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.



Die folgenden allgemeinen Namen können nicht für Remote-Cluster- und SVM-Administratorkonten verwendet werden: „adm“, „bin“, „cli“, „Daemon“, „ftp“, „Spiele“, „Halt“, „lp“, „Mail“, „man“, „Naroot“, „netapp“, „Nachrichten“, „niemand“, „Betreiber“, „Root“, „Shutdown“, „sshd“, „Sync“, „sys“, „uucp“ und „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.

Was Sie benötigen

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

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.

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-SVMengCluster 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

Was Sie benötigen

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

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 ssh-ed25519 Host Key Algorithmus wurde in 9.11.1 entfernt

Weitere Informationen finden Sie unter ["Konfiguration der Netzwerksicherheit mit FIPS"](#).

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 SVMengData1 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](#)

Multi-Faktor-SSH-Authentifizierung (MFA) aktivieren

Ab ONTAP 9.3 können Sie den verwenden `security login create` Um die Sicherheit zu verbessern, müssen sich Administratoren bei einem Administrator oder einer Daten-SVM sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem Benutzerpasswort einloggen.

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.

Weitere Informationen zu ["Mehrstufige Authentifizierung in ONTAP 9 \(TR-4647\)"](#).

Bevor Sie beginnen

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

Über diese Aufgabe

- Sie müssen 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.

- 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 Benutzer wird immer mit Authentifizierung des öffentlichen Schlüssels und der Kennwortauthentifizierung authentifiziert.

Schritt

1. Lokale Administratorkonten erforderlich, um über SSH MFA auf eine SVM zuzugreifen:

```
security login create -vserver SVM -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 `SVMengData1` 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".
```

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 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

Was Sie benötigen

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

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](#)



Für Cluster-Administratorkonten wird die Zertifikatauthentifizierung nur mit unterstützt `http` Und `ontapi` Applikationen unterstützt. Bei SVM-Administratorkonten wird die Zertifikatauthentifizierung nur von unterstützt `ontapi` Applikation.

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 Befehlsyntax 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 `SVMengData2` 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.

Was Sie benötigen

- 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.

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 9.11.1 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 Und `ontapi` Applikationen unterstützt.

Schritt

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

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod domain -role role -comment comment [-is-  
ldap-fastbind true]
```

Eine vollständige Befehlsyntax finden Sie im "[Arbeitsblatt](#)".

["Erstellen oder Ändern von Anmeldekonten"](#)

Mit dem folgenden Befehl wird das AD-Cluster-Administratorkonto aktiviert `DOMAIN1\guest1` Mit dem vordefinierten `backup` Rolle für den Zugriff auf die Administrator-SVMengCluster.

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

Mit dem folgenden Befehl werden die SVM-Administratorkonten im AD-Gruppenkonto aktiviert `DOMAIN1\adgroup` Mit dem vordefinierten `vsadmin-volume` Rolle für den Zugriff auf die SVMengData.

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

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.

Was Sie benötigen

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

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.

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 Befehlsyntax finden Sie im "[Arbeitsblatt](#)".

"Erstellen oder Ändern von Anmeldekonto"

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

```
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](#)

Konfigurieren Sie die SAML-Authentifizierung

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

Was Sie benötigen

- Sie müssen das IdP für SAML-Authentifizierung konfiguriert haben.
- Sie müssen über die IdP-URI verfügen.

Über diese Aufgabe

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

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

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

Schritte

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

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

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

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

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


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

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

will be disrupted.

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

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

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

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

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

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

3. SAML-Konfiguration aktivieren:

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

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

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

- a. Anmeldemethode für neue Benutzer mit SAML-Authentifizierung erstellen: `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. Überprüfen Sie, ob 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**

```

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.

Was Sie benötigen

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.

Was Sie benötigen

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

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.

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	<ul style="list-style-type: none"> • Alle Befehlsverzeichnisse (DEFAULT) • security login rest-role • security login role
Schreibgeschützt	<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • set • system node autosupport 	Keine	Alle anderen Befehlsverzeichnisse (DEFAULT)
Backup	Alle	vserver services ndmp

readonly	volume	Keine
Alle anderen Befehlsverzeichnisse (DEFAULT)	readonly	Alle
<ul style="list-style-type: none"> • security login password <p>Nur zur Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 der Protokolle NFS, SMB, iSCSI und FC Einschließlich FCoE • Dienste konfigurieren: DNS, LDAP und NIS • Überwachen von Jobs • Monitoring von Netzwerkverbindungen und Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
Vsadmin-Volume	<ul style="list-style-type: none"> • 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 und FC, einschließlich FCoE • Dienste konfigurieren: DNS, LDAP und NIS • Monitoring der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
Vsadmin-Protokoll	<ul style="list-style-type: none"> • Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Konfiguration von Protokollen NFS, SMB, iSCSI und FC, einschließlich FCoE • Dienste konfigurieren: DNS, LDAP und NIS • Verwalten von LUNs • Monitoring der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM

Vsadmin-Backup	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

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.

Bevor Sie beginnen

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

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.

Schritt

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 Befehlsyntax finden Sie im ["Arbeitsblatt"](#).

["Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto"](#)

Der folgende Befehl ordnet dem SVM-Administratorkonto einen öffentlichen Schlüssel zu `svmin1` Für die SVM `engData1`. Dem öffentlichen Schlüssel wird die Indexnummer 5 zugewiesen.

```
cluster1::>security login publickey create -vserver engData1 -username
svmin1 -index 5 -publickey
"ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J
/vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIza
FciDy7hgnmdj9eNGedGr/JNrftQbLD1hZybX+72DpQB0tYWBhe6eDJ1oPLob
ZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

Erstellen und Installieren eines CA-signierten Serverzertifikats

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.

Was Sie benötigen

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 A erstellt 2048-Bit privater Schlüssel generiert durch die SHA256 Hashing-Funktion für den Einsatz durch Software Gruppe in der IT Abteilung eines Unternehmens, dessen eigener gemeinsamer Name ist `server1.companyname.com`, Befindet sich in Sunnyvale, California, 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
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEWAxCTAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
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.

Was Sie benötigen

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 Befehlsyntax 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 wird das CA-signierte installiert `server` Zertifikat und Zwischenzertifikate auf der `SVMengData2`.

```
cluster1::>security certificate install -vserver engData2 -type server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRhc
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBGNV
BAoTAAEJMAcGA1UECXMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBGNVBAoTAAEJMAcGA1UECzMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C61X2G32Sx8VEalth94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrFYC8KwE9k7A0y1RzBLdUwK9
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+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwbG90b3R5bGUuY29yYXZl
bG1DZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmfSaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDEwhodHRwOi8vd3d3LnZhbG1kYXRpb24gIDAE
```

```
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECmMoR28gRGFkZHZkgQ2xhc3MgMiBDZXJ0
-----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-----
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBACtG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACtG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEzhodHRw
-----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.

Konfigurieren Sie den Active Directory-Domänencontroller-Zugriff

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 in...
HMAC-SHA256, basierend auf dem Advanced Encryption Standard (AES)	ONTAP 9.10.1 und höher
DES und HMAC-MD5 (bei festem Schlüssel)	Alle ONTAP 9 Versionen

Wenn Sie AES-Sitzungsschlüssel während der Einrichtung des sicheren Netzwerklogon-Kanals in ONTAP 9.10.1 und höher verwenden möchten, müssen Sie diese mit dem folgenden Befehl aktivieren:

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

Die Standardeinstellung lautet `false`.

In ONTAP-Versionen vor 9.10.1, wenn der Domain-Controller AES für sichere Netlogon-Dienste erzwingt, schlägt die Verbindung fehl. Der Domain-Controller muss so konfiguriert sein, dass er in diesen Versionen starke Schlüsselverbindungen mit ONTAP akzeptiert.

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.

Was Sie benötigen

- 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.

HINWEIS

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 Befehlsyntax finden Sie im "[Arbeitsblatt](#)".



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

Die SMB-fähige Daten-SVM wird mit dem folgenden Befehl konfiguriert `engData` Als Authentifizierungstunnel.

```
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.

Was Sie benötigen

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

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.

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 Befehlsyntax finden Sie im ["Arbeitsblatt"](#).

Mit dem folgenden Befehl wird ein Computerkonto mit dem Namen erstellt `ADSERVER1` In der Domäne `example.com` Für die SVM `engData`. 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 den LDAP- oder NIS-Serverzugriff

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.

Was Sie benötigen

- 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.

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 (Windows 2008, Windows 2012 und höher AD-Server)
- 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 in den folgenden Dokumenten:

- ["NFS-Konfiguration"](#)
- ["Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP"](#)

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 Befehlsyntax finden Sie im ["Arbeitsblatt"](#).

Mit dem folgenden Befehl wird eine LDAP-Client-Konfiguration mit dem Namen erstellt `corp` Auf der SVM `engData`. Der Client macht anonyme Bindungen mit den LDAP-Servern mit den IP-Adressen `172.160.0.100` Und `172.16.0.101`. Der Client verwendet das `RFC-2307` Schema zum Erstellen von LDAP-Abfragen. 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.

Was Sie benötigen

- 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.

Über diese Aufgabe

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

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 der SVM erstellt `engData`. 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.

Was Sie benötigen

- 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"](#).

Mit dem folgenden Befehl wird die Suchreihenfolge der LDAP- und NIS-Namensdienstquellen für die festgelegt `passwd` Datenbank auf dem `engDataSVM`:

```
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.

Was Sie benötigen

- 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.

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 auf der man-Page `security login role config modify`

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 `SVMvs1.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.

Was Sie benötigen

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 vorgehackte SHA-2-Passwörter nur mithilfe des NetApp Manageability SDK (Security-Login-create und Security-Login-modify-password).

"Bessere Managebarkeit"

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 vserver_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.

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](#)."

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*`

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.

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
volume snaplock modify	vserver peer delete

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. Antragsteller, 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-Warmmeldungen 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	<code>security login show</code>
Ändern der Anmeldeinformationen aktueller Administratoren	<code>security login modify <parameters></code>
Erstellen neuer Administratorkonten	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

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	<code>security multi-admin-verify approval-group modify [parameters]</code>
Mitglieder hinzufügen oder entfernen	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[, approver2...]] [-approvers-to-remove approver1[, approver2...]]</code>
Gruppe löschen	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

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.

Erforderliche Genehmiger

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

Hinweis: die erforderliche Anzahl an Genehmigern muss kleiner als die Gesamtzahl der eindeutigen Genehmiger in den Standardgenehmigungsgruppen sein.

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	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn] -enabled true [-execution-expiry [nnh][nmm][nns]] [-approval-expiry [nnh][nmm][nns]]</pre> <p>Beispiel : mit dem folgenden Befehl wird MAV mit 1 Genehmigungsgruppe, 2 erforderlichen Genehmigern und Standard-Ablauffristen aktiviert.</p> <pre>cluster-1::> security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>Führen Sie die Erstkonfiguration durch Hinzufügen von mindestens einer Konfiguration durch "Betriebsregel."</p>
Änderung einer MAV-Konfiguration (erfordert MAV-Genehmigung)	<pre>security multi-admin-verify approval- group modify [-approval-groups group1 [,group2...]] [-required-approvers nn] [-execution-expiry [nnh][nmm][nns]] [-approval-expiry [nnh][nmm][nns]]</pre>
Überprüfung der MAV-Funktionalität	<pre>security multi-admin-verify show</pre> <p>Beispiel:</p> <pre>cluster-1::> security multi-admin- verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- true 2 1h 1h mav-grp1</pre>
MAV-Funktionalität deaktivieren (MAV-Genehmigung erforderlich)	<pre>security multi-admin-verify modify -enabled false</pre>

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.

In ONTAP 9.11.1 können Sie Regeln für die folgenden Befehle erstellen.

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

Darüber hinaus sind die folgenden Befehle standardmäßig geschützt, wenn MAV aktiviert ist. Sie können jedoch die Regeln ändern, um den Schutz für diese Befehle zu entfernen.

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

Die Regeln für MAV-System-default-Befehle – das `security multi-admin-verify` Befehle – kann nicht geändert werden.

Beim Erstellen einer Regel können Sie optional die angeben `-query` Option, um die Anforderung auf einen Teil der Befehlsfunktion zu beschränken. Beispiel: Im Befehl „Default set“ `-query` ist auf festgelegt `-privilege diag`, Das bedeutet, dass eine Anfrage nur dann für den Befehl `set` generiert wird, wenn `-Privilege diag` angegeben ist.


```

smci-vs1m20::> security multi-admin-verify rule show
                                     Required Approval
Vserver Operation                    Approvers Groups
-----
vs01      set                         -           -
          Query: -privilege diagnostic

```

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.



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

- Erforderliche Anzahl der Genehmiger
- Genehmigungsgruppen
- Ablaufrist der Genehmigung
- Ablaufrist 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. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie Auf  Neben **Multi-Admin-Genehmigung** im Abschnitt **Sicherheit**.
3. Klicken Sie Auf  **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 Befehloptionen 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	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>
Ändern der Anmeldeinformationen aktueller Administratoren	<code>security login modify <parameters></code> Beispiel: Die folgende Regel erfordert die Genehmigung, um das Root-Volume zu löschen. <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code>
Regel ändern	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
Löschen Sie eine Regel	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
Regeln anzeigen	<code>security multi-admin-verify rule show</code>

Details zur Befehlsyntax 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 voll1 -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 voll1
    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 voll1 -vserver vs0
```

```
Info: Volume "voll1" 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 voll_*" 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 "voll1" in Vserver
"vs0" ?
{y|n}: y
```

- b. Wenn der Antrag gegen ein Vetos gestellt wird oder die Ablaufrist 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 voll1
        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 voll1 -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 Operationsregel 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	<code>security multi-admin-verify request approve nn</code>
Veto auf eine Anfrage	<code>security multi-admin-verify request veto nn</code>

Wenn Sie... wollen	Geben Sie diesen Befehl ein
Zeigt alle Anfragen, ausstehende Anfragen oder eine einzelne Anforderung an	<code>`security multi-admin-verify request { show</code>
<code>show-pending } [nn] { -fields field1[,field2...]</code>	<code>[-instance]}`</code> 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 <code>-fields</code> Parameter) oder über alle Felder (mit dem <code>-instance</code> Parameter).
Löschen Sie eine Anfrage	<code>security multi-admin-verify request delete nn</code>

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: -

```

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.