Authentifizierung und rollenbasierte Zugriffskontrolle für Administratoren verwalten

ONTAP 9

NetApp
November 16, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/authentication/index.html on November 16, 2026. Always check docs.netapp.com for the latest.

Inhalt

Authentifizierung und rollenbasierte Zugriffskontrolle für Administratoren verwalten . . . 1
Informationen zur ONTAP Administrator-Authentifizierung und RBAC (rollenbasierte Zugriffskontrolle) . . . 1
ONTAP Administrator-Authentifizierung und RBAC-Workflow . . . 1
Arbeitsblätter für die ONTAP Administratorauthentifizierung und die Einrichtung der rollenbasierten Zugriffssteuerung (RBAC) . . . 2
Anmeldekonten erstellen oder ändern . . . 3
Cisco Duo Sicherheitsinformationen konfigurieren . . . 5
Benutzerdefinierte Rollen definieren . . . 8
Einem Benutzerkonto wird ein öffentlicher Schlüssel zugeordnet. . . . 10
Globale Einstellungen für die dynamische Autorisierung konfigurieren . . . 11
Ein von einer Zertifizierungsstelle signiertes digitales Serverzertifikat installieren . . . 13
Konfiguration des Zugriffs auf den Active Directory Domänencontroller . . . 14
Zugriff auf LDAP- oder NIS-Server konfigurieren . . . 15
SAML-Zugriff konfigurieren . . . 17
Anmeldekonten erstellen . . . 18
Informationen zu ONTAP Administrator-Anmeldekonten . . . 18
Lokalen Kontozugriff aktivieren . . . 19
Multifaktor-Authentifizierung (MFA) Konten aktivieren . . . 22
Aktivierung des Active Directory-Zugriffs für ONTAP Administratorkonten . . . 29
LDAP- oder NIS-Zugriff für ONTAP Administratorkonten kann aktiviert werden. . . . 31
Zugriffskontrollrollen verwalten . . . 32
Informationen zu ONTAP Zugriffskontrollrollen . . . 33
Die einem ONTAP Administrator zugewiesene Rolle ändern . . . 33
Benutzerdefinierte Rollen für ONTAP Administratoren definieren . . . 33
Vordefinierte Rollen für ONTAP Clusteradministratoren . . . 35
Vordefinierte Rollen für ONTAP SVM Administratoren . . . 37
ONTAP Administratorzugriff mit System Manager verwalten . . . 39
Verwendung der JIT-Berechtigungserweiterung in ONTAP . . . 40
JIT-Zugangsstufenerhöhung in ONTAP konfigurieren . . . 41
Administratorkonten verwalten . . . 46
Informationen zu ONTAP Administratorkonten . . . 46
Einem ONTAP Administratorkonto einen öffentlichen Schlüssel zuordnen . . . 46
SSH Public Keys und X.509-Zertifikate für ONTAP Administratoren verwalten . . . 47
Cisco Duo 2FA für ONTAP SSH-Anmeldungen konfigurieren . . . 50
Ein von einer Zertifizierungsstelle signiertes Serverzertifikat in ONTAP generieren und installieren . . . 55
ONTAP Zertifikate mit System Manager verwalten . . . 58
Konfigurieren des Zugriffs auf Active Directory-Domänencontroller in ONTAP . . . 63
LDAP- oder NIS-Serverzugriff in ONTAP konfigurieren . . . 65
Ändern eines ONTAP Administratorpassworts . . . 69
Konfiguration von ONTAP Benachrichtigungen zum Ablauf von ONTAP Benutzerpasswörtern in System Manager . . . 70
Sperren und Entsperren eines ONTAP Administratorkontos . . . 71
Fehlgeschlagene Anmeldeversuche in ONTAP verwalten . . . 71

SHA-2 für Passwörter von ONTAP Administratorenkonten erzwingen . . . 72
Diagnose und Behebung von ONTAP Dateizugriffsproblemen mit System Manager . . . 73
Multi-Admin-Verifizierung verwalten . . . 73
Informationen zur ONTAP Multi-Admin-Verifizierung . . . 73
ONTAP Administrator-Genehmigungsgruppen für MAV verwalten . . . 99
Multi-Admin-Verifizierung in ONTAP aktivieren oder deaktivieren . . . 103
Multi-Admin-Verifizierungsregeln für geschützte Vorgänge in ONTAP verwalten . . . 107
Ausführung von MAV-geschützten Vorgängen in ONTAP anfordern . . . 110
Verwaltung von MAV geschützten Operationsanforderungen in ONTAP . . . 113
Dynamische Autorisierung verwalten . . . 118
Informationen zu ONTAP dynamischer Autorisierung . . . 118
Dynamische Autorisierung in ONTAP aktivieren oder deaktivieren . . . 119
Dynamische Autorisierung in ONTAP anpassen . . . 121

Authentifizierung und rollenbasierte Zugriffskontrolle für Administratoren verwalten

Informationen zur ONTAP Administrator-Authentifizierung und RBAC (rollenbasierte Zugriffskontrolle)

Sie können Anmeldekonten für ONTAP Clusteradministratoren und Administratoren von Storage Virtual Machines (SVM) aktivieren. Mit der rollenbasierten Zugriffssteuerung (RBAC) lassen sich die Berechtigungen der Administratoren definieren.

Lokale Administratorkonten können für den Zugriff auf eine Admin Storage Virtual Machine (SVM) oder eine Data SVM mit den folgenden Authentifizierungsverfahren aktiviert werden:

- "Passwort"
- "SSH öffentlicher Schlüssel"
- "SSL-Zertifikat"
- "SSH Multifaktor-Authentifizierung (MFA)"

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

Remote-Administratorkonten können Zugriff auf eine Admin-SVM oder eine Daten-SVM mit den folgenden Authentifizierungsverfahren erhalten:

- "Active Directory"

  Ab ONTAP 9.13.1 kann ein SSH Public Key entweder als primäres oder sekundäres Authentifizierungsverfahren für einen Active Directory Benutzer verwendet werden.

- "SAML-Authentifizierung (nur für Admin SVM)"

  Ab ONTAP 9.3 kann die Security Assertion Markup Language (SAML) Authentifizierung für den Zugriff auf die Admin-SVM über einen der folgenden Webdienste verwendet werden: Service Processor Infrastructure, ONTAP APIs oder System Manager.

- "LDAP oder NIS"

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

ONTAP Administrator-Authentifizierung und RBAC-Workflow

Sie können die Authentifizierung für lokale Administratorkonten oder Remote-Administratorkonten aktivieren. Die Kontoinformationen eines lokalen Kontos befinden sich auf dem Speichersystem und die Kontoinformationen eines Remote-Kontos befinden sich an einem anderen Ort. Jedem Konto kann eine vordefinierte Rolle oder eine benutzerdefinierte Rolle zugewiesen werden.

1 Vollständiges Konfigurationsarbeitsblatt

Vor dem Erstellen von Anmeldekonten und dem Einrichten der rollenbasierten Zugriffssteuerung (RBAC) sollten Informationen zu jedem Element in der "Konfigurationsarbeitsblätter" gesammelt werden.

2 Es wird festgestellt, ob das Administratorkonto lokal oder remote ist.

- **Bei lokaler Installation:** "Passwort", "SSH", "SSH MFA" oder "SSL" Zugriff aktivieren.
- **Bei Fernzugriff:** Die Art des Fernzugriffs bestimmen. Abhängig vom Zugriffstyp "Active Directory Zugriff aktivieren", "LDAP- oder NIS-Zugriff ermöglichen" oder "SAML-Authentifizierung (nur für Admin SVM) konfigurieren".

3 Rollenbasierte Zugriffssteuerung einrichten

Die einem Administrator zugewiesene Rolle bestimmt, auf welche Befehle der Administrator Zugriff hat. Die Rolle wird bei der Erstellung des Administratorkontos zugewiesen und kann "modifiziert" später geändert werden. Vordefinierte Rollen können für "Cluster" und "SVM" Administratoren verwendet werden oder "Benutzerdefinierte Rollen festlegen" nach Bedarf angepasst werden.

4 Administratorkonten verwalten

Je nachdem, wie Sie den Kontozugriff aktiviert haben, kann es erforderlich sein, einen "öffentlicher Schlüssel mit einem lokalen Konto" zuzuordnen, "öffentliche Schlüssel und X.509-Zertifikate" zu verwalten, "Cisco Duo 2FA für SSH Logins" zu konfigurieren, einen "CA-signiertes digitales Serverzertifikat" zu installieren oder "Active Directory" sowie "LDAP oder NIS" Zugriff zu konfigurieren. Jede dieser Aufgaben kann vor oder nach der Aktivierung des Kontozugriffs erfolgen.

5 Zusätzliche Sicherheitsfunktionen konfigurieren

- "Multi-Admin-Verifizierung verwalten"wenn sichergestellt werden soll, dass bestimmte Vorgänge die Genehmigung von festgelegten Administratoren erfordern.
- "Dynamische Autorisierung verwalten"wenn zusätzliche Autorisierungsprüfungen dynamisch basierend auf dem Vertrauensniveau eines Benutzers angewendet werden sollen.
- "Just-in-Time (JIT)-Berechtigungserweiterung konfigurieren"wenn Benutzern vorübergehend erhöhte Berechtigungen zum Ausführen bestimmter Aufgaben gewährt werden sollen.

Arbeitsblätter für die ONTAP Administratorauthentifizierung und die Einrichtung der rollenbasierten Zugriffssteuerung (RBAC)

Vor dem Erstellen von Anmeldekonten und dem Einrichten der rollenbasierten Zugriffssteuerung (RBAC) empfiehlt es sich, Informationen zu jedem Element in den Konfigurationsarbeitsblättern zusammenzustellen.

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Anmeldekonten erstellen oder ändern

Diese Werte werden mit dem `security login create` Befehl angegeben, wenn Anmeldekonten für den Zugriff auf eine Storage-VM aktiviert werden. Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

Sie geben dieselben Werte mit dem `security login modify` Befehl an, wenn Sie ändern, wie ein Konto auf eine Storage-VM zugreift. Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM, auf die das Konto zugreift. Der Standardwert ist der Name der administrativen Storage-VM für den Cluster.	
`-user-or-group-name`	Der Benutzername oder Gruppenname des Kontos. Die Angabe eines Gruppennamens ermöglicht den Zugriff für alle Benutzer in der Gruppe. Ein Benutzername oder Gruppenname kann mit mehreren Anwendungen verknüpft werden.	
`-application`	Die Anwendung, die für den Zugriff auf die Storage-VM verwendet wird: • `http` • `ontapi` • `snmp` • `ssh`	

`-authmethod`	Die Methode, die zur Authentifizierung des Kontos verwendet wird: • `cert` für die SSL-Authentifizierung • `domain` für die Active Directory Authentifizierung • `nsswitch`für LDAP oder NIS Authentifizierung • `password`zur Authentifizierung des Benutzerpassworts • `publickey` für die Public-Key-Authentifizierung • `community` für SNMP Community-Strings • `usm` für das SNMP Benutzersicherheitsmodell • `saml` für die Security Assertion Markup Language (SAML) Authentifizierung	
`-remote-switch-ipaddress`	Die IP-Adresse des Remote-Switches. Der Remote-Switch kann ein Cluster-Switch sein, der vom Cluster-Switch-Integritätsmonitor (CSHM) überwacht wird, oder ein Fibre Channel (FC) Switch, der vom MetroCluster Health Monitor (MCC-HM) überwacht wird. Diese Option ist nur anwendbar, wenn die Anwendung `snmp` ist und das Authentifizierungsverfahren `usm` ist.	
`-role`	Die dem Konto zugewiesene Zugriffskontrollrolle: • Für den Cluster (die Admin-Speicher-VM) ist der Standardwert `admin`. • Für eine Datenspeicher-VM ist der Standardwert `vsadmin`.	
`-comment`	(Optional) Beschreibender Text für das Konto. Der Text sollte in doppelte Anführungszeichen (") eingeschlossen werden.	

`-is-ns-switch-group`	Ob es sich bei dem Konto um ein LDAP-Gruppenkonto oder ein NIS-Gruppenkonto handelt (`yes` oder `no`).	
`-second-authentication -method`	Zweites Authentifizierungsverfahren im Falle einer Multifaktor-Authentifizierung: • `none`wenn keine Multifaktor-Authentifizierung verwendet wird, Standardwert • `publickey`für die Public-Key-Authentifizierung, wenn das `authmethod`Passwort oder nsswitch ist • `password`für die Benutzerpasswortauthentifizierung, wenn das `authmethod`Authentifizierungsverfahren der öffentliche Schlüssel ist • `nsswitch`zur Benutzerpasswort-Authentifizierung, wenn das Authentifizierungsverfahren publickey ist Die Reihenfolge der Authentifizierung ist immer der öffentliche Schlüssel, gefolgt vom Passwort.	
`-is-ldap-fastbind`	Ab ONTAP 9.11.1 aktiviert die Einstellung „true“ die LDAP-Schnellbindung für die nsswitch Authentifizierung; der Standardwert ist „false“. Um die LDAP-Schnellbindung zu nutzen, muss der `-authentication-method` Wert auf `nsswitch` gesetzt werden. "LDAP Fast Bind für die nsswitch-Authentifizierung für ONTAP NFS SVMs verwenden".	

Cisco Duo Sicherheitsinformationen konfigurieren

Diese Werte werden mit dem `security login duo create` Befehl bereitgestellt, wenn Cisco Duo Zwei-Faktor-Authentifizierung mit SSH-Anmeldungen für eine Storage-VM aktiviert wird. Weitere Informationen zu `security login duo create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert

`-vserver`	Die Storage-VM (in der ONTAP CLI als vserver bezeichnet), auf die die Duo Authentifizierungseinstellungen angewendet werden.	
`-integration-key`	Ihr Integrationsschlüssel, der bei der Registrierung Ihrer SSH-Anwendung bei Duo erhalten wurde.	
`-secret-key`	Ihr geheimer Schlüssel, der bei der Registrierung Ihrer SSH-Anwendung bei Duo erhalten wurde.	
`-api-host`	Der API-Hostname, der bei der Registrierung der SSH-Anwendung bei Duo erhalten wird. Beispiel: `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	Bei Service- oder Konfigurationsfehlern, die die Duo Authentifizierung verhindern, `safe` (Zugriff erlauben) oder `secure` (Zugriff verweigern). Standardmäßig ist `safe`, was bedeutet, dass die Duo Authentifizierung umgangen wird, wenn sie aufgrund von Fehlern wie einem nicht erreichbaren Duo API Server fehlschlägt.	
`-http-proxy`	Der angegebene HTTP-Proxy wird verwendet. Wenn der HTTP-Proxy eine Authentifizierung erfordert, sind die Anmeldeinformationen in die Proxy-URL aufzunehmen. Beispiel: `http-proxy=http://username:password@proxy.example.org:8080`	

`-autopush`	Entweder `true` oder `false`. Standardmäßig ist `false`. Wenn `true` aktiviert ist, sendet Duo automatisch eine Push-Anmeldeanfrage an das Telefon des Benutzers und wechselt zu einem Anruf, falls Push nicht verfügbar ist. Dabei wird die Passcode-Authentifizierung effektiv deaktiviert. Wenn `false` aktiviert ist, wird der Benutzer aufgefordert, ein Authentifizierungsverfahren auszuwählen. Bei Konfiguration mit `autopush = true` wird empfohlen, `max-prompts = 1` zu setzen.	
`-max-prompts`	Schlägt die Authentifizierung mit einem zweiten Faktor fehl, fordert Duo den Benutzer zur erneuten Authentifizierung auf. Diese Option legt die maximale Anzahl der Aufforderungen fest, die Duo anzeigt, bevor der Zugriff verweigert wird. Muss `1`, `2` oder `3` sein. Der Standardwert ist `1`. Wenn beispielsweise `max-prompts = 1`, muss sich der Benutzer beim ersten Prompt erfolgreich authentifizieren, während `max-prompts = 2`, wenn der Benutzer beim ersten Prompt falsche Informationen eingibt, er erneut zur Authentifizierung aufgefordert wird. Bei Konfiguration mit `autopush = true` wird empfohlen, `max-prompts = 1` zu setzen. Für das beste Benutzererlebnis wird bei einem Benutzer, der ausschließlich Publickey-Authentifizierung verwendet, immer `max-prompts` auf `1` gesetzt.	

`-enabled`	Duo-Zwei-Faktor-Authentifizierung aktivieren. Standardmäßig auf `true` gesetzt. Wenn aktiviert, wird die Duo-Zwei-Faktor-Authentifizierung beim SSH-Login gemäß den konfigurierten Parametern erzwungen. Wenn Duo deaktiviert ist (auf `false` gesetzt), wird die Duo-Authentifizierung ignoriert.	
`-pushinfo`	Diese Option liefert zusätzliche Informationen in der Push-Benachrichtigung, beispielsweise den Namen der Anwendung oder des Dienstes, auf den zugegriffen wird. Dies hilft Nutzern zu überprüfen, ob sie sich beim richtigen Dienst anmelden, und bietet eine zusätzliche Sicherheitsebene.	

Benutzerdefinierte Rollen definieren

Sie geben diese Werte mit dem `security login role create` Befehl an, wenn Sie eine benutzerdefinierte Rolle definieren. Weitere Informationen zu `security login role create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	(Optional) Der Name der Storage VM (in der ONTAP CLI als vserver bezeichnet), die der Rolle zugeordnet ist.	
`-role`	Die Bezeichnung der Rolle.	
`-cmddirname`	Der Befehl oder das Befehlsverzeichnis, auf das die Rolle Zugriff gewährt. Befehlsunterverzeichnisnamen sollten in doppelte Anführungszeichen (") gesetzt werden. Zum Beispiel `"volume snapshot"`. Es ist erforderlich, `DEFAULT` einzugeben, um alle Befehlsverzeichnisse anzugeben.	

`-access`	(Optional) Die Zugangsstufe für die Rolle. Für Befehlsverzeichnisse: • `none` (Der Standardwert für benutzerdefinierte Rollen) verweigert den Zugriff auf Befehle im Befehlsverzeichnis • `readonly` gewährt Zugriff auf die `show` Befehle im Befehlsverzeichnis und dessen Unterverzeichnissen • `all` gewährt Zugriff auf alle Befehle im Befehlsverzeichnis und dessen Unterverzeichnissen Für *nicht-intrinsische Befehle* (Befehle, die nicht mit `create`, `modify`, `delete` oder `show` enden): • `none` (Der Standardwert für benutzerdefinierte Rollen) verweigert den Zugriff auf den Befehl • `readonly` ist nicht anwendbar • `all` gewährt Zugriff auf den Befehl Um den Zugriff auf intrinsische Befehle zu gewähren oder zu verweigern, muss das Befehlsverzeichnis angegeben werden.	
`-query`	(Optional) Das Abfrageobjekt, das zum Filtern der Zugangsstufe verwendet wird, wird in Form einer gültigen Option für den Befehl oder für einen Befehl im Befehlsverzeichnis angegeben. Das Abfrageobjekt sollte in doppelte Anführungszeichen (") eingeschlossen werden. Wenn das Befehlsverzeichnis beispielsweise `volume` ist, würde das Abfrageobjekt `"-aggr aggr0"` den Zugriff nur für das `aggr0` Aggregat ermöglichen.	

Einem Benutzerkonto wird ein öffentlicher Schlüssel zugeordnet.

Diese Werte werden mit dem `security login publickey create` Befehl angegeben, wenn ein öffentlicher SSH-Schlüssel mit einem Benutzerkonto verknüpft wird. Weitere Informationen zu `security login publickey create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	(Optional) Der Name der Storage-VM, auf die das Konto zugreift.	
`-username`	Der Benutzername des Kontos. Der Standardwert, `admin`, was dem Standardnamen des Clusteradministrators entspricht.	
`-index`	Die Indexnummer des öffentlichen Schlüssels. Der Standardwert ist 0, wenn es sich um den ersten Schlüssel handelt, der für das Konto erstellt wurde; andernfalls ist der Standardwert um eins höher als die höchste bereits vorhandene Indexnummer des Kontos.	
`-publickey`	Der öffentliche OpenSSH-Schlüssel. Der Schlüssel sollte in doppelte Anführungszeichen (") gesetzt werden.	
`-role`	Die dem Konto zugewiesene Zugriffskontrollrolle.	
`-comment`	(Optional) Beschreibender Text für den öffentlichen Schlüssel. Der Text sollte in doppelte Anführungszeichen (") eingeschlossen werden.	

`-x509-certificate`	(Optional) Ab ONTAP 9.13.1 ist die Verwaltung der Zuordnung von X.509-Zertifikaten zum öffentlichen SSH-Schlüssel möglich. Wenn ein X.509-Zertifikat mit dem öffentlichen SSH-Schlüssel verknüpft wird, prüft ONTAP bei der SSH-Anmeldung, ob dieses Zertifikat gültig ist. Ist es abgelaufen oder widerrufen, wird die Anmeldung verweigert und der zugehörige öffentliche SSH-Schlüssel deaktiviert. Mögliche Werte: • `install`: Das angegebene PEM-kodierte X.509-Zertifikat wird installiert und mit dem öffentlichen SSH-Schlüssel verknüpft. Der vollständige Text des zu installierenden Zertifikats ist anzugeben. • `modify`: Das bestehende PEM-kodierte X.509-Zertifikat wird mit dem angegebenen Zertifikat aktualisiert und mit dem SSH-öffentlichen Schlüssel verknüpft. Der vollständige Text für das neue Zertifikat ist einzufügen. • `delete`: Die bestehende X.509-Zertifikatszuordnung mit dem öffentlichen SSH-Schlüssel wird entfernt.	

Globale Einstellungen für die dynamische Autorisierung konfigurieren

Ab ONTAP 9.15.1 werden diese Werte mit dem `security dynamic-authorization modify` Befehl angegeben. Weitere Informationen zu `security dynamic-authorization modify` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM, für die die Vertrauenswert-Einstellung geändert werden soll. Wird dieser Parameter ausgelassen, kommt die Einstellung auf Cluster-Ebene zur Anwendung.	

`-state`	Der dynamische Autorisierungsmodus. Mögliche Werte: • `disabled`: (Standard) Dynamische Autorisierung ist deaktiviert. • `visibility`: Dieser Modus ist nützlich zum Testen der dynamischen Autorisierung. In diesem Modus wird der Vertrauenswert bei jeder eingeschränkten Aktivität überprüft, aber nicht durchgesetzt. Allerdings wird jede Aktivität, die abgelehnt worden wäre oder zusätzlichen Authentifizierungsanforderungen unterliegen würde, protokolliert. • `enforced`Vorgesehen für die Verwendung nach Abschluss der Tests mit `visibility`-Modus. In diesem Modus wird der Vertrauenswert bei jeder eingeschränkten Aktivität geprüft, und Aktivitätseinschränkungen werden durchgesetzt, wenn die Einschränkungsbedingungen erfüllt sind. Das Unterdrückungsintervall wird ebenfalls durchgesetzt, wodurch zusätzliche Authentifizierungsaufforderungen innerhalb des angegebenen Intervalls verhindert werden.	
`-suppression-interval`	Verhindert zusätzliche Authentifizierungsabfragen innerhalb des angegebenen Intervalls. Das Intervall ist im ISO-8601-Format und akzeptiert Werte von 1 Minute bis einschließlich 1 Stunde. Wenn der Wert auf 0 gesetzt ist, ist das Unterdrückungsintervall deaktiviert und der Benutzer wird immer zu einer Authentifizierungsabfrage aufgefordert, wenn eine erforderlich ist.	

`-lower-challenge-boundary`	Die untere Grenze für die prozentuale Anzahl an Multifaktor-Authentifizierungs- (MFA) Herausforderungen. Der gültige Bereich liegt zwischen 0 und 99. Der Wert 100 ist ungültig, da dies dazu führt, dass alle Anfragen abgelehnt werden. Der Standardwert ist 0.	
`-upper-challenge-boundary`	Der obere Grenzwert für den Prozentsatz der MFA-Herausforderung. Der gültige Bereich liegt zwischen 0 und 100. Dieser Wert muss dem Wert des unteren Grenzwerts entsprechen oder größer sein. Ein Wert von 100 bedeutet, dass jede Anfrage entweder abgelehnt wird oder einer zusätzlichen Authentifizierung unterliegt; es gibt keine Anfragen, die ohne Herausforderung zugelassen werden. Der Standardwert ist 90.	

Ein von einer Zertifizierungsstelle signiertes digitales Serverzertifikat installieren

Diese Werte werden mit dem `security certificate generate-csr` Befehl angegeben, wenn eine digitale Zertifikatsignierungsanforderung (CSR) zur Verwendung bei der Authentifizierung einer Storage-VM als SSL-Server generiert wird. Weitere Informationen zu `security certificate generate-csr` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-common-name`	Der Name des Zertifikats, der entweder eine vollqualifizierte Domain (FQDN) oder ein benutzerdefinierter allgemeiner Name ist.	
`-size`	Die Anzahl der Bits im privaten Schlüssel. Je höher der Wert, desto sicherer der Schlüssel. Der Standardwert ist `2048`. Mögliche Werte sind `512`, `1024`, `1536` und `2048`.	
`-country`	Das Land der Storage-VM, als zweistelliger Code. Der Standardwert ist `US`. Eine Liste der Codes befindet sich unter "ONTAP-Befehlsreferenz".	
`-state`	Der Staat oder die Provinz der Storage-VM.	

`-locality`	Der Standort der Storage-VM.	
`-organization`	Die Organisation der Storage-VM.	
`-unit`	Die Einheit in der Organisation der Storage-VM.	
`-email-addr`	Die E-Mail-Adresse des Kontaktadministrators für die Storage-VM.	
`-hash-function`	Die kryptografische Hash-Funktion zum Signieren des Zertifikats. Der Standardwert ist `SHA256`. Mögliche Werte sind `SHA1`, `SHA256` und `MD5`.	

Diese Werte werden mit dem `security certificate install` Befehl bereitgestellt, wenn ein von einer Zertifizierungsstelle signiertes digitales Zertifikat zur Authentifizierung des Clusters oder der Storage-VM als SSL-Server installiert wird. Nur die für die Kontokonfiguration relevanten Optionen sind in der folgenden Tabelle aufgeführt. Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

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

Konfiguration des Zugriffs auf den Active Directory Domänencontroller

Sie geben diese Werte mit dem `security login domain-tunnel create` Befehl an, wenn bereits ein SMB-Server für eine Datenspeicher-VM konfiguriert wurde und die Storage-VM als Gateway oder Tunnel für den Zugriff des Active Directory Domain Controllers auf den Cluster konfiguriert werden soll. Weitere Informationen zu `security login domain-tunnel create` finden sich in der "ONTAP-Befehlsreferenz".

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

Sie geben diese Werte mit dem `vserver active-directory create` Befehl an, wenn kein SMB-Server konfiguriert ist und ein Storage VM-Computerkonto in der Active Directory-Domäne erstellt werden soll. Weitere Informationen zu `vserver active-directory create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM, für die ein Active Directory Computerkonto erstellt werden soll.	
`-account-name`	Der NetBIOS-Name des Computerkontos.	
`-domain`	Der vollqualifizierte Domainname (FQDN).	
`-ou`	Die Organisationseinheit in der Domäne. Der Standardwert ist `CN=Computers`. ONTAP hängt diesen Wert an den Domänennamen an, um den Active Directory individuellen Namen zu erzeugen.	

Zugriff auf LDAP- oder NIS-Server konfigurieren

Sie geben diese Werte mit dem `vserver services name-service ldap client create` Befehl an, wenn Sie eine LDAP-Client-Konfiguration für die Storage-VM erstellen. Weitere Informationen zu `vserver services name-service ldap client create` finden sich in der "ONTAP-Befehlsreferenz".

In der folgenden Tabelle sind nur die Optionen aufgeführt, die für die Kontokonfiguration relevant sind:

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM für die Clientkonfiguration.	
`-client-config`	Der Name der Client-Konfiguration.	
`-ldap-servers`	Eine durch Kommas getrennte Liste von IP-Adressen und Hostnamen der LDAP-Server, mit denen sich der Client verbindet.	
`-schema`	Das Schema, das der Client für LDAP-Abfragen verwendet.	

`-use-start-tls`	Ob der Client Start TLS zur Verschlüsselung der Kommunikation mit dem LDAP-Server verwendet (`true` oder `false`). Start TLS wird nur für den Zugriff auf Datenspeicher-VMs unterstützt. Für den Zugriff auf Admin-Speicher-VMs wird es nicht unterstützt.	

Diese Werte werden mit dem `vserver services name-service ldap create` Befehl angegeben, wenn eine LDAP-Client-Konfiguration mit der Storage-VM verknüpft wird. Weitere Informationen zu `vserver services name-service ldap create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM, mit der die Clientkonfiguration verknüpft werden soll.	
`-client-config`	Der Name der Client-Konfiguration.	
`-client-enabled`	Ob die Storage-VM die LDAP-Client-Konfiguration (`true` oder `false` verwenden kann).	

Diese Werte werden mit dem `vserver services name-service nis-domain create` Befehl angegeben, wenn eine NIS-Domänenkonfiguration auf einer Storage-VM erstellt wird. Weitere Informationen zu `vserver services name-service nis-domain create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM, auf der die Domänenkonfiguration erstellt werden soll.	
`-domain`	Der Name der Domain.	
`-nis-servers`	Eine durch Kommas getrennte Liste von IP-Adressen und Hostnamen für die NIS-Server, die von der Domänenkonfiguration verwendet werden.	

Sie geben diese Werte mit dem `vserver services name-service ns-switch create` Befehl an, wenn Sie die Suchreihenfolge für Namensdienstquellen angeben. Weitere Informationen zu `vserver services name-service ns-switch create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert

`-vserver`	Der Name der Storage-VM, auf der die Reihenfolge der Namensdienstabfrage konfiguriert werden soll.	
`-database`	Die Namensdienstdatenbank: • `hosts` für Dateien und DNS-Namensdienste • `group`für Dateien, LDAP und NIS Namensdienste • `passwd`für Dateien, LDAP und NIS Namensdienste • `netgroup`für Dateien, LDAP und NIS Namensdienste • `namemap` für Dateien und LDAP-Namensdienste	
`-sources`	Die Reihenfolge, in der die Namensdienstquellen in einer durch Kommas getrennten Liste durchsucht werden: • `files` • `dns` • `ldap` • `nis`	

SAML-Zugriff konfigurieren

Ab ONTAP 9.3 werden diese Werte mit dem `security saml-sp create` Befehl zur Konfiguration der SAML-Authentifizierung bereitgestellt. Weitere Informationen zu `security saml-sp create` finden sich in der "ONTAP-Befehlsreferenz".

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

`-cert-ca` und `-cert-serial`, oder `-cert-common-name`	Die Serverzertifikatdetails des Dienstanbieter-Hosts (ONTAP-System). Es kann entweder die ausstellende Zertifizierungsstelle (CA) des Dienstanbieters und die Seriennummer des Zertifikats oder der Common Name des Serverzertifikats eingegeben werden.	
`-verify-metadata-server`	Ob die Identität des IdP-Metadatenservers validiert werden muss `true` oder `false`. Die empfohlene Vorgehensweise ist, diesen Wert immer auf `true` zu setzen.	

Anmeldekonten erstellen

Informationen zu ONTAP Administrator-Anmeldekonten

Sie können lokale oder Remote-Cluster- und SVM-Administratorkonten aktivieren. Bei einem lokalen Konto befinden sich die Kontoinformationen, der öffentliche Schlüssel oder das Sicherheitszertifikat auf dem Speichersystem. AD-Kontoinformationen werden auf einem Domänencontroller gespeichert. LDAP- und NIS-Konten befinden sich auf LDAP- bzw. NIS-Servern.

Cluster- und SVM-Administratoren

Ein Clusteradministrator greift auf die administrative SVM des Clusters zu. Die administrative SVM und ein Clusteradministrator mit dem reservierten Namen `admin` werden beim Einrichten des Clusters automatisch erstellt.

Ein Clusteradministrator mit der Standard `admin`rolle kann den gesamten Cluster und seine Ressourcen verwalten. Der Clusteradministrator kann bei Bedarf weitere Clusteradministratoren mit unterschiedlichen Rollen erstellen.

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

SVM-Administratoren wird standardmäßig die `vsadmin` Rolle zugewiesen. Der Cluster-Administrator kann SVM-Administratoren bei Bedarf unterschiedliche Rollen zuweisen.

Namenskonventionen

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

- "adm"
- "bin"
- "cli"

- "Daemon"
- "ftp"
- "Spiele"
- "halt"
- "lp"
- "Mail"
- "man"
- "naroot"
- "netapp"
- "News"
- "niemand"
- "Operator"
- "root"
- "shutdown"
- "sshd"
- "sync"
- "sys"
- "uucp"
- "www"

Zusammengeführte Rollen

Wenn Sie mehrere Remote-Konten für denselben Benutzer aktivieren, wird diesem Benutzer die Vereinigung aller für die Konten festgelegten Rollen zugewiesen. Das heißt, wenn einem LDAP- oder NIS-Konto die `vsadmin` Rolle und dem Active Directory Gruppe Konto desselben Benutzers die `vsadmin-volume` Rolle zugewiesen ist, meldet sich der AD-Benutzer mit den umfassenderen `vsadmin` Berechtigungen an. Die Rollen werden als „zusammengeführt“ bezeichnet.

Lokalen Kontozugriff aktivieren

Informationen zum Zugriff auf das lokale ONTAP Administratorkonto

Bei einem lokalen Konto befinden sich die Kontoinformationen, der öffentliche Schlüssel oder das Sicherheitszertifikat auf dem Speichersystem. Der `security login create` Befehl kann verwendet werden, um lokalen Konten den Zugriff auf eine Admin- oder Daten-SVM zu ermöglichen.

Verwandte Informationen

- "security login create"

Aktivierung des Passwortzugriffs für ein ONTAP Administratorkonto

Sie können den `security login create`Befehl verwenden, um Administratorkonten den Zugriff auf eine Admin- oder Daten-SVM mit einem Passwort zu ermöglichen. Nach

Eingabe des Befehls erfolgt eine Aufforderung zur Eingabe des Passworts.

Über diese Aufgabe

Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, kann die Rolle später mit dem `security login modify` Befehl hinzugefügt werden.

Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Lokalen Administratorkonten den Zugriff auf eine SVM mithilfe eines Kennworts ermöglichen:

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

   Der folgende Befehl ermöglicht dem Cluster-Administratorkonto `admin1` mit der vordefinierten `backup` Rolle den Zugriff auf die Admin-SVM`engCluster` mit einem Passwort. Nach Eingabe des Befehls erfolgt eine Aufforderung zur Eingabe des Passworts.

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

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

SSH-Zugriff mit öffentlichem Schlüssel für ein ONTAP Administratorkonto wird aktiviert

Mit dem `security login create`Befehl kann Administratoren der Zugriff auf eine Admin- oder Daten-SVM mit einem öffentlichen SSH-Schlüssel ermöglicht werden.

Über diese Aufgabe

- Der öffentliche Schlüssel muss mit dem Konto verknüpft sein, bevor das Konto auf die SVM zugreifen kann.

  Verknüpfung eines öffentlichen Schlüssels mit einem Benutzerkonto

  Diese Aufgabe kann vor oder nach der Aktivierung des Kontozugriffs durchgeführt werden.

- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, kann die Rolle später mit dem `security login modify` Befehl hinzugefügt werden.

  Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

Wenn Sie den FIPS-Modus in Ihrem Cluster aktivieren möchten, müssen bestehende SSH-Public-Key-Konten ohne die unterstützten Schlüsselalgorithmen mit einem unterstützten Schlüsseltyp neu konfiguriert werden. Die Konten sollten neu konfiguriert werden, bevor FIPS aktiviert wird, da sonst die Authentifizierung des Administrators fehlschlägt.

Die folgende Tabelle zeigt die für ONTAP SSH-Verbindungen unterstützten Host-Schlüssel-Algorithmen. Diese

Schlüsseltypen gelten nicht für die Konfiguration der öffentlichen SSH-Authentifizierung.

ONTAP Release	Im FIPS-Modus unterstützte Schlüsseltypen	Unterstützte Schlüsseltypen im Nicht-FIPS-Modus
9.11.1 und später	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 und früher	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa

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

Weitere Informationen finden sich unter "Netzwerksicherheit mithilfe von FIPS konfigurieren".

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Lokale Administratorkonten erhalten Zugriff auf eine SVM mithilfe eines öffentlichen SSH-Schlüssels:

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

   Der folgende Befehl ermöglicht dem SVM-Administratorkonto `svmadmin1` mit der vordefinierten `vsadmin-volume` Rolle den Zugriff auf die SVM`engData1` mithilfe eines öffentlichen SSH-Schlüssels:

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

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Wenn einem Administratorkonto noch kein öffentlicher Schlüssel zugeordnet ist, muss dies erfolgen, bevor das Konto auf die SVM zugreifen kann.

Verknüpfung eines öffentlichen Schlüssels mit einem Benutzerkonto

Für ein ONTAP Administratorkonto wird der Zugriff auf SSL-Zertifikate aktiviert.

Mit dem `security login create`Befehl kann Administratoren der Zugriff auf eine Admin- oder Daten-SVM mit einem SSL-Zertifikat ermöglicht werden.

Über diese Aufgabe

- Ein von einer Zertifizierungsstelle signiertes digitales Serverzertifikat muss installiert werden, bevor das Konto auf die SVM zugreifen kann.

  Generieren und Installieren eines von der CA signierten Serverzertifikats

Diese Aufgabe kann vor oder nach der Aktivierung des Kontozugriffs durchgeführt werden.

- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, kann die Rolle später mit dem `security login modify` Befehl hinzugefügt werden.

  Ändern der einem Administrator zugewiesenen Rolle

> Für Cluster-Administratorkonten wird die Zertifikatsauthentifizierung mit den `http`, `ontapi` und `rest` Anwendungen unterstützt. Für SVM-Administratorkonten wird die Zertifikatsauthentifizierung nur mit den `ontapi` und `rest` Anwendungen unterstützt.

Schritt

1. Lokale Administratorkonten erhalten 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
   ```

   Der folgende Befehl aktiviert das SVM-Administratorkonto `svmadmin2` mit der Standard `vsadmin`-Rolle, um mit einem SSL-Digitalzertifikat auf die SVM`engData2` zuzugreifen.

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

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Falls noch kein von einer Zertifizierungsstelle signiertes Server-Digitalzertifikat installiert wurde, muss dies erfolgen, bevor das Konto auf die SVM zugreifen kann.

Generieren und Installieren eines von der CA signierten Serverzertifikats

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Multifaktor-Authentifizierung (MFA) Konten aktivieren

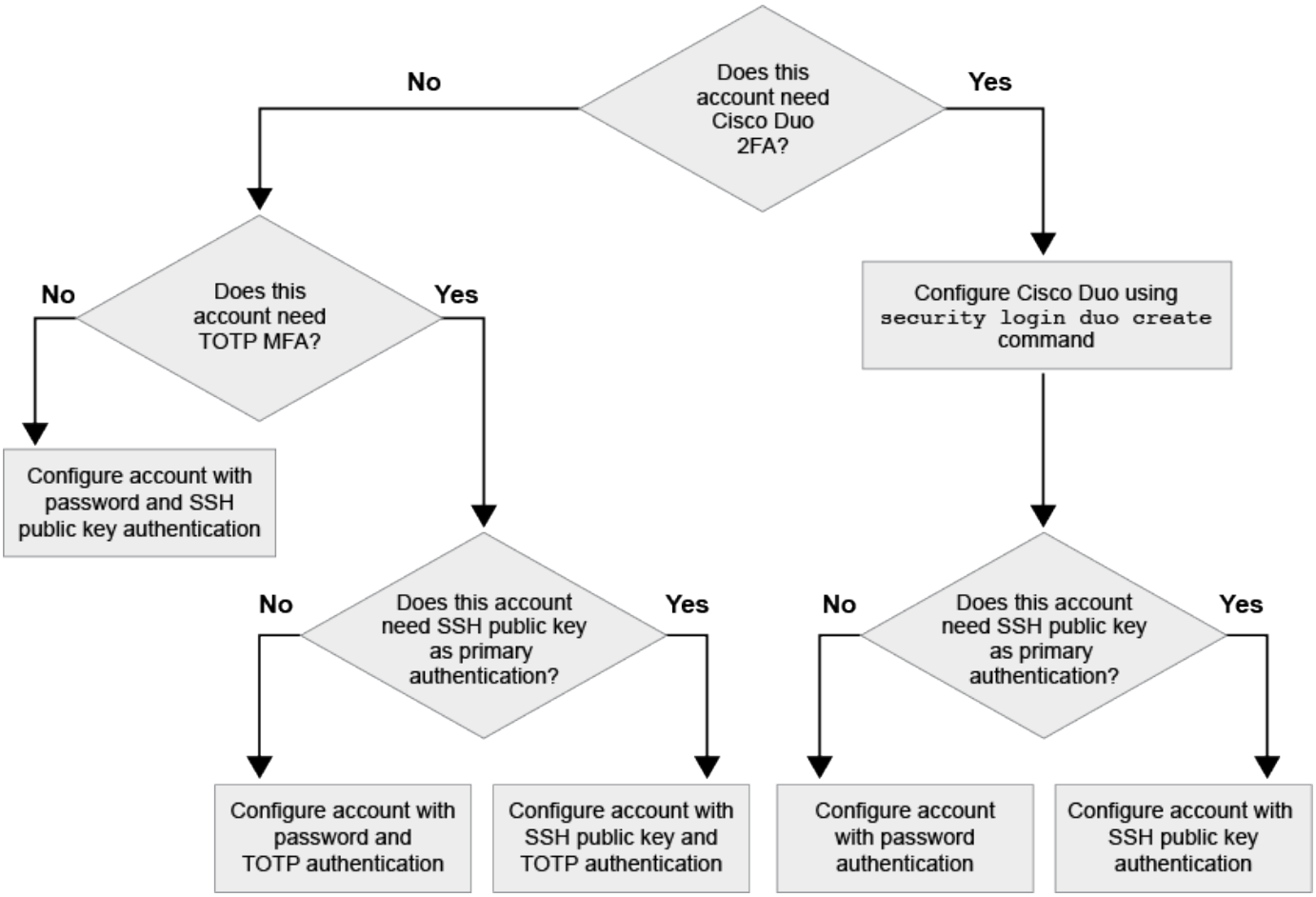
Informationen zur ONTAP Multifaktor Authentifizierung

Die Multifaktor Authentifizierung (MFA) bietet die Möglichkeit, die Sicherheit zu erhöhen, indem von den Benutzern zwei Authentifizierungsverfahren verlangt werden, um sich bei einer Admin- oder Datenspeicher-VM anzumelden.

Abhängig von Ihrer ONTAP Version kann eine Kombination aus einem SSH Public Key, einem Benutzerpasswort und einem zeitbasierten Einmalpasswort (TOTP) für die Multifaktor Authentifizierung verwendet werden. Bei Aktivierung und Konfiguration von Cisco Duo (ONTAP 9.14.1 und höher) dient es als zusätzliches Authentifizierungsverfahren und ergänzt die bestehenden Methoden für alle Benutzer.

Verfügbar ab…	Erstes Authentifizierungsverfahren	Zweites Authentifizierungsverfahren
ONTAP 9.14.1	SSH öffentlicher Schlüssel	TOTP
	Benutzerpasswort	TOTP
	SSH öffentlicher Schlüssel	Cisco Duo
	Benutzerpasswort	Cisco Duo
ONTAP 9.13.1	SSH öffentlicher Schlüssel	TOTP
	Benutzerpasswort	TOTP
ONTAP 9.3	SSH öffentlicher Schlüssel	Benutzerpasswort

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



ONTAP Multifaktor Authentifizierung mit SSH und TOTP aktivieren

Die Multifaktor-Authentifizierung (MFA) bietet die Möglichkeit, die Sicherheit zu erhöhen, indem von Benutzern zwei Authentifizierungsverfahren verlangt werden, um sich bei einer Admin- oder Daten-SVM anzumelden.

Über diese Aufgabe

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, kann die Rolle später mit dem `security login modify` Befehl hinzugefügt werden.

  Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

  "Ändern der einem Administrator zugewiesenen Rolle"

- Wenn ein öffentlicher Schlüssel zur Authentifizierung verwendet wird, muss der öffentliche Schlüssel mit dem Konto verknüpft werden, bevor das Konto auf die SVM zugreifen kann.

  "Einem Benutzerkonto wird ein öffentlicher Schlüssel zugeordnet."

  Diese Aufgabe kann vor oder nach der Aktivierung des Kontozugriffs durchgeführt werden.

- Ab ONTAP 9.12.1 ist die Verwendung von Yubikey Hardware-Authentifizierungsgeräten für die SSH-Client-MFA mit den Authentifizierungsstandards FIDO2 (Fast IDentity Online) oder Personal Identity Verification (PIV) möglich.

Multi-Faktor-Authentifizierung mit öffentlichem SSH-Schlüssel und Benutzerpasswort aktivieren

Ab ONTAP 9.3 kann ein Cluster-Administrator lokale Benutzerkonten einrichten, um sich mit MFA unter Verwendung eines öffentlichen SSH-Schlüssels und eines Benutzerpassworts anzumelden.

1. Multi-Faktor-Authentifizierung für das lokale Benutzerkonto mit öffentlichem SSH-Schlüssel und Benutzerpasswort aktivieren:

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

   Der folgende Befehl erfordert das SVM-Administratorkonto `admin2` mit der vordefinierten `admin` Rolle, um sich bei der SVM`engData1` sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem Benutzerpasswort anzumelden:

   ```
   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".
   ```

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

MFA mit TOTP aktivieren

Ab ONTAP 9.13.1 lässt sich die Sicherheit erhöhen, indem lokale Benutzer verpflichtet werden, sich sowohl mit

einem öffentlichen SSH-Schlüssel oder Benutzerpasswort als auch mit einem zeitbasierten Einmalpasswort (TOTP) an einer Admin- oder Daten-SVM anzumelden. Nachdem das Konto für die Multi-Faktor-Authentifizierung (MFA) mit TOTP aktiviert wurde, muss sich der lokale Benutzer bei "Konfiguration abschließen" anmelden.

TOTP ist ein Algorithmus, der anhand der aktuellen Zeit ein Einmalpasswort generiert. Wenn TOTP verwendet wird, ist es immer die zweite Form der Authentifizierung nach dem SSH Public Key oder dem Benutzerpasswort.

Bevor Sie beginnen

Um diese Aufgaben auszuführen, ist die Rolle eines Speicheradministrators erforderlich.

Schritte

MFA kann so eingerichtet werden, dass als erstes Authentifizierungsverfahren entweder ein Benutzerpasswort oder ein SSH Public Key und als zweites Authentifizierungsverfahren TOTP verwendet wird.

MFA mit Benutzerpasswort und TOTP aktivieren

1. Ein Benutzerkonto kann für die Multifaktor Authentifizierung mit Benutzerpasswort und TOTP verwendet werden.

   Für neue Benutzerkonten

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

   Für bestehende Benutzerkonten

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

2. Es sollte überprüft werden, ob die Multi-Faktor-Authentifizierung mit TOTP aktiviert ist:

   ```
   security login show
   ```

MFA mit SSH Public Key und TOTP aktivieren

1. Ein Benutzerkonto für die Multifaktor-Authentifizierung mit einem öffentlichen SSH-Schlüssel und TOTP aktivieren.

   Für neue Benutzerkonten

   ```
   security login create -vserver <svm_name> -user-or-group-name
   ```

```
<user_or_group_name> -application ssh -authentication-method
publickey -second-authentication-method totp -role <role> -comment
<comment>
```

Für bestehende Benutzerkonten

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

Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Es sollte überprüft werden, ob die Multi-Faktor-Authentifizierung mit TOTP aktiviert ist:

```
security login show
```

Weitere Informationen zu `security login show` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

- Wenn einem Administratorkonto noch kein öffentlicher Schlüssel zugeordnet ist, muss dies erfolgen, bevor das Konto auf die SVM zugreifen kann.

  "Verknüpfung eines öffentlichen Schlüssels mit einem Benutzerkonto"

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

  "Lokales Benutzerkonto für MFA mit TOTP konfigurieren"

Verwandte Informationen

- "Multifaktor-Authentifizierung in ONTAP 9 (TR-4647)"
- "ONTAP-Befehlsreferenz"

Lokale ONTAP Benutzerkonten für MFA mit TOTP konfigurieren

Ab ONTAP 9.13.1 können Benutzerkonten mit Multifaktor-Authentifizierung (MFA) unter Verwendung eines zeitbasierten Einmalpassworts (TOTP) konfiguriert werden.

Bevor Sie beginnen

- Der Speicheradministrator muss "MFA mit TOTP verwenden" als zweites Authentifizierungsverfahren für Ihr Benutzerkonto festlegen.
- Das Authentifizierungsverfahren für das primäre Nutzerkonto sollte ein Benutzerpasswort oder ein öffentlicher SSH-Schlüssel sein.
- Sie müssen Ihre TOTP-App so konfigurieren, dass sie mit Ihrem Smartphone funktioniert und Ihren TOTP-Geheimschlüssel erstellen.

Microsoft Authenticator, Google Authenticator, Authy und alle anderen TOTP-kompatiblen Authentifizierungsprogramme werden unterstützt.

Schritte

1. Melden Sie sich mit Ihrem aktuellen Authentifizierungsverfahren bei Ihrem Nutzerkonto an.

   Das aktuelle Authentifizierungsverfahren sollte ein Benutzerpasswort oder ein öffentlicher SSH-Schlüssel sein.

2. Die TOTP-Konfiguration für Ihr Konto erstellen:

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

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

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

Verwandte Informationen

- "security login totp create"
- "security login totp show"

TOTP-Geheimschlüssel für ein ONTAP Benutzerkonto zurücksetzen

Zum Schutz der Kontosicherheit sollte der TOTP-Geheimschlüssel deaktiviert und ein neuer erstellt werden, falls dieser kompromittiert oder verloren geht.

TOTP zurücksetzen, falls Ihr Schlüssel kompromittiert wurde

Wenn Ihr TOTP-Geheimschlüssel kompromittiert wurde, Sie aber noch Zugriff darauf haben, kann der kompromittierte Schlüssel entfernt und ein neuer erstellt werden.

1. Melden Sie sich mit Ihrem Benutzerpasswort oder Ihrem öffentlichen SSH-Schlüssel und Ihrem kompromittierten TOTP-Geheimschlüssel bei Ihrem Benutzerkonto an.
2. Den kompromittierten TOTP-Geheimschlüssel entfernen:

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

> Ab ONTAP 9.19.1 muss ein gültiger TOTP-Code oder Scratch-Code eingegeben werden, um den TOTP-Geheimschlüssel mithilfe der ONTAP CLI zu löschen. Das Löschen des TOTP-Geheimschlüssels über die ONTAP REST API ist nicht möglich.

3. Einen neuen TOTP-Geheimschlüssel erstellen:

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

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

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

TOTP zurücksetzen, falls der Schlüssel verloren gegangen ist

Wenn Ihr TOTP-Geheimschlüssel verloren geht, sollte Ihr Speicheradministrator "Der Schlüssel ist deaktiviert" kontaktiert werden. Nachdem Ihr Schlüssel deaktiviert wurde, kann das erste Authentifizierungsverfahren zur Anmeldung und zur Konfiguration eines neuen TOTP verwendet werden.

Bevor Sie beginnen

Der TOTP-Geheimschlüssel muss von einem Storage-Administrator deaktiviert werden. Wenn kein Storage-Administratorkonto vorhanden ist, sollte der Storage-Administrator kontaktiert werden, damit der Schlüssel deaktiviert wird.

Schritte

1. Nachdem das TOTP-Geheimnis von einem Speicheradministrator deaktiviert wurde, kann das primäre Authentifizierungsverfahren genutzt werden, um sich beim lokalen Konto anzumelden.
2. Einen neuen TOTP-Geheimschlüssel erstellen:

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

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

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

Verwandte Informationen

- "security login totp create"
- "security login totp löschen"
- "security login totp show"

Der TOTP-Geheimschlüssel für ein ONTAP Benutzerkonto wird deaktiviert.

Geht der geheime Schlüssel für das zeitbasierte Einmalpasswort (TOTP) eines lokalen Benutzers verloren, muss der verlorene Schlüssel von einem Speicheradministrator deaktiviert werden, bevor der Benutzer einen neuen TOTP-Schlüssel erstellen kann.

Über diese Aufgabe

Diese Aufgabe kann nur von einem Cluster-Administratorkonto aus durchgeführt werden.

Schritt

1. TOTP-Geheimschlüssel deaktivieren:

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

   Weitere Informationen zu `security login totp modify` finden sich in der "ONTAP-Befehlsreferenz".

Aktivierung des Active Directory-Zugriffs für ONTAP Administratorkonten

Der `security login create`-Befehl kann verwendet werden, um Active Directory (AD) Benutzer- oder Gruppenkonten den Zugriff auf eine Admin- oder Daten-SVM zu ermöglichen. Jedes Mitglied der Active Directory Gruppe kann mit der der Gruppe zugewiesenen Rolle auf die SVM zugreifen.

Über diese Aufgabe

- Der Zugriff des AD-Domänencontrollers auf den Cluster oder die SVM muss konfiguriert werden, bevor das Konto auf die SVM zugreifen kann.

  Konfiguration des Zugriffs auf Active Directory Domänencontroller

  Diese Aufgabe kann vor oder nach der Aktivierung des Kontozugriffs durchgeführt werden.

- Ab ONTAP 9.13.1 kann ein SSH Public Key als primäres oder sekundäres Authentifizierungsverfahren zusammen mit einem AD-Benutzerpasswort verwendet werden.

  Wenn ein SSH-Public-Key als primäres Authentifizierungsverfahren verwendet wird, findet keine AD-Authentifizierung statt.

- Ab ONTAP 9.11.1 kann "LDAP Fast Bind für die nsswitch-Authentifizierung für ONTAP NFS SVMs verwenden" verwendet werden, sofern dies vom AD LDAP-Server unterstützt wird.
- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, kann die Rolle später mit dem `security login modify` Befehl hinzugefügt werden.

  Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

  Ändern der einem Administrator zugewiesenen Rolle

> Der Zugriff auf Active Directory Gruppenkonten wird nur mit den `SSH`, `ontapi` und `rest` Anwendungen unterstützt. Active Directory Gruppen werden nicht mit der SSH Public Key Authentifizierung unterstützt, die häufig für die Multifaktor Authentifizierung verwendet wird.

Bevor Sie beginnen

- Die Clusterzeit muss innerhalb von fünf Minuten mit der Zeit auf dem AD-Domänencontroller synchron sein.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. AD-Benutzer- oder Gruppenadministratorkonten können für den Zugriff auf eine SVM aktiviert werden:

Für AD-Benutzer*innen:

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

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

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

Für Active Directory Gruppen:

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

Nachdem Sie fertig sind

Wenn der Zugriff des AD-Domänencontrollers auf den Cluster oder die SVM nicht konfiguriert wurde, ist dies erforderlich, bevor das Konto auf die SVM zugreifen kann.

Konfiguration des Zugriffs auf Active Directory Domänencontroller

Verwandte Informationen

- "security login create"

LDAP- oder NIS-Zugriff für ONTAP Administratorkonten kann aktiviert werden.

Der `security login create` Befehl kann verwendet werden, um LDAP- oder NIS-Benutzerkonten den Zugriff auf eine Admin- oder Daten-SVM zu ermöglichen. Wenn der LDAP- oder NIS-Serverzugriff auf die SVM nicht konfiguriert wurde, ist dies erforderlich, bevor das Konto auf die SVM zugreifen kann.

Über diese Aufgabe

- LDAP- oder NIS-Serverzugriff auf die SVM muss konfiguriert werden, bevor das Konto auf die SVM zugreifen kann.

  Konfiguration des LDAP- oder NIS-Serverzugriffs

  Diese Aufgabe kann vor oder nach der Aktivierung des Kontozugriffs durchgeführt werden.

- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, kann die Rolle später mit dem `security login modify` Befehl hinzugefügt werden.

  Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

  Ändern der einem Administrator zugewiesenen Rolle

- Ab ONTAP 9.4 wird die Multifaktor-Authentifizierung (MFA) für Remote-Benutzer über LDAP- oder NIS-Server unterstützt.
- Ab ONTAP 9.11.1 kann "LDAP Fast Bind für die nsswitch-Authentifizierung für ONTAP NFS SVMs verwenden" verwendet werden, sofern dies vom LDAP-Server unterstützt wird.
- Aufgrund eines bekannten LDAP-Problems sollte das `':'` (Doppelpunkt) Zeichen in keinem Feld der LDAP-Benutzerkontoinformationen (zum Beispiel `gecos`, `userPassword` usw.) verwendet werden. Andernfalls schlägt der Suchvorgang für diesen Benutzer fehl.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

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

   ```
   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]
   ```

   "Erstellen oder Ändern von Anmeldekonten"

   Der folgende Befehl ermöglicht dem LDAP- oder NIS-Cluster-Administratorkonto `guest2` mit der vordefinierten `backup` Rolle den Zugriff auf die Admin-SVM`engCluster`.

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

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

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
   ```

   Das Authentifizierungsverfahren kann als `publickey` und das zweite Authentifizierungsverfahren als `nsswitch` angegeben werden.

   Das folgende Beispiel zeigt, wie die MFA-Authentifizierung aktiviert wird:

   ```
   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 der LDAP- oder NIS-Serverzugriff auf die SVM nicht konfiguriert wurde, ist dies erforderlich, bevor das Konto auf die SVM zugreifen kann.

Konfiguration des LDAP- oder NIS-Serverzugriffs

Verwandte Informationen

- "Security Login"

Zugriffskontrollrollen verwalten

Informationen zu ONTAP Zugriffskontrollrollen

Die einem Administrator zugewiesene Rolle bestimmt, auf welche Befehle der Administrator Zugriff hat. Die Rolle wird zugewiesen, wenn das Konto für den Administrator erstellt wird. Es kann bei Bedarf eine andere Rolle zugewiesen oder benutzerdefinierte Rollen definiert werden.

Die einem ONTAP Administrator zugewiesene Rolle ändern

Sie können den `security login modify` Befehl verwenden, um die Rolle eines Cluster- oder SVM-Administratorkontos zu ändern. Es kann eine vordefinierte oder eine benutzerdefinierte Rolle zugewiesen werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Die Rolle eines Cluster- oder SVM-Administrators ändern:

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

   "Erstellen oder Ändern von Anmeldekonten"

   Der folgende Befehl ändert die Rolle des AD-Cluster-Administratorkontos `DOMAIN1\guest1` zur vordefinierten `readonly` Rolle.

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

   Der folgende Befehl ändert die Rolle der SVM-Administratorkonten im Active Directory Gruppe Konto `DOMAIN1\adgroup` zur benutzerdefinierten `vol_role` Rolle.

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

   Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

Benutzerdefinierte Rollen für ONTAP Administratoren definieren

Sie können den `security login role create`Befehl verwenden, um eine benutzerdefinierte Rolle zu definieren. Der Befehl kann beliebig oft ausgeführt werden, um die genaue Kombination von Funktionen zu erreichen, die mit der Rolle verknüpft werden soll.

Über diese Aufgabe

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

  Ein Befehlsverzeichnis (`volume`, beispielsweise, ist eine Gruppe zusammengehöriger Befehle und Befehlsunterverzeichnisse. Sofern in diesem Verfahren nicht anders beschrieben, gewährt oder verweigert die Zugriffsberechtigung für ein Befehlsverzeichnis den Zugriff auf jeden Befehl in diesem Verzeichnis und seinen Unterverzeichnissen.

- Der Zugriff auf bestimmte Befehle oder Unterverzeichnisse hat Vorrang vor dem Zugriff auf das übergeordnete Verzeichnis.

  Wird eine Rolle mit einem Befehlsverzeichnis definiert und anschließend mit einer anderen Zugangsstufe für einen bestimmten Befehl oder ein Unterverzeichnis des übergeordneten Verzeichnisses neu definiert, so überschreibt die für den Befehl oder das Unterverzeichnis angegebene Zugangsstufe diejenige des übergeordneten Verzeichnisses.

> Einem SVM-Administrator kann keine Rolle zugewiesen werden, die Zugriff auf einen Befehl oder ein Befehlsverzeichnis gewährt, das nur dem `admin`Cluster Administrator zur Verfügung steht, beispielsweise das `security`Befehlsverzeichnis.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Eine benutzerdefinierte Rolle festlegen:

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

   Die folgenden Befehle gewähren der `vol_role` Rolle vollen Zugriff auf die Befehle im `volume` Befehlsverzeichnis und Lesezugriff 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 gewähren der `SVM_storage` Rolle Lesezugriff auf die Befehle im `storage` Befehlsverzeichnis, keinen Zugriff auf die Befehle im `storage encryption` Unterverzeichnis und vollen Zugriff auf den `storage aggregate plex offline` nichtintrinsischen 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
```

Weitere Informationen zu `security login role create` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "security login role create"
- "Storage Aggregate Plex offline"
- "Speicherverschlüsselung"

Vordefinierte Rollen für ONTAP Clusteradministratoren

Die vordefinierten Rollen für Clusteradministratoren sollten die meisten Ihrer Anforderungen abdecken. Bei Bedarf können benutzerdefinierte Rollen erstellt werden. Standardmäßig wird einem Clusteradministrator die vordefinierte `admin` Rolle zugewiesen.

Die folgende Tabelle enthält die vordefinierten Rollen für Cluster-Administratoren:

Diese Rolle…	Verfügt über diese Zugriffsebene…	Zu den folgenden Befehlen oder Befehlsverzeichnissen
Administrator	alle	Alle Befehlsverzeichnisse (`DEFAULT`
admin-no-fsa (verfügbar ab ONTAP 9.12.1)	Lesen/Schreiben	• Alle Befehlsverzeichnisse (`DEFAULT` • `security login rest-role` • `security login role`

Nur lesen	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Keine
`volume file show-disk-usage`	AutoSupport	alle
• `set` • `system node autosupport`	keine	Alle anderen Befehlsverzeichnisse (`DEFAULT`)
Backup	alle	`vserver services ndmp`
schreibgeschützt	`volume`	keine
Alle anderen Befehlsverzeichnisse (`DEFAULT`)	schreibgeschützt	alle
• `security login password` Nur zur Verwaltung des lokalen Passworts und der Schlüsselinformationen des eigenen Benutzerkontos • `set`	• Ab ONTAP 9.8 ist readonly • Vor ONTAP 9.8 keine	`security`
schreibgeschützt	Alle anderen Befehlsverzeichnisse (`DEFAULT`)	SnapLock

alle	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`	keine
• `volume move governor` • `volume move recommend`	keine	Alle anderen Befehlsverzeichnisse (`DEFAULT`)
keine	keine	Alle Befehlsverzeichnisse (`DEFAULT`

Die `autosupport` Rolle ist dem vordefinierten `autosupport` Konto zugewiesen, das von AutoSupport OnDemand verwendet wird. ONTAP verhindert, dass das `autosupport` Konto geändert oder gelöscht wird. ONTAP verhindert außerdem, dass die `autosupport` Rolle anderen Benutzerkonten zugewiesen wird.

Verwandte Informationen

- "Security Login"
- "Set"
- "Volumen"
- "vserver services ndmp"

Vordefinierte Rollen für ONTAP SVM Administratoren

Die vordefinierten Rollen für SVM-Administratoren sollten die meisten Ihrer Anforderungen abdecken. Bei Bedarf können benutzerdefinierte Rollen erstellt werden. Standardmäßig wird einem SVM-Administrator die vordefinierte `vsadmin` Rolle zugewiesen.

Die folgende Tabelle listet die vordefinierten Rollen für SVM-Administratoren auf:

Rollenname	Fähigkeiten

vsadmin	• Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos • Verwaltung von Volumes, ausgenommen Volume-Verschiebungen • Verwaltung von Kontingenten, Qtrees, Snapshots und Dateien • Verwaltung von LUNs • Ausführen von SnapLock-Operationen, außer privilegiertem Löschen • Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Konfiguration von Diensten: DNS, LDAP und NIS • Überwachungsaufträge • Überwachung von Netzwerkverbindungen und Netzwerkschnittstellen • Überwachung des Gesundheitszustands der SVM
vsadmin-volume	• Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos • Verwaltung von Volumes, ausgenommen Volume-Verschiebungen • Verwaltung von Kontingenten, Qtrees, Snapshots und Dateien • Verwaltung von LUNs • Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Konfiguration von Diensten: DNS, LDAP und NIS • Überwachung der Netzwerkschnittstelle • Überwachung des Gesundheitszustands der SVM
vsadmin-protocol	• Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos • Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Konfiguration von Diensten: DNS, LDAP und NIS • Verwaltung von LUNs • Überwachung der Netzwerkschnittstelle • Überwachung des Gesundheitszustands der SVM

vsadmin-backup	• Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos • Verwaltung von NDMP-Operationen • Ein wiederhergestelltes Volume für lesen/schreiben aktivieren • Verwaltung von SnapMirror-Beziehungen und Snapshots • Anzeige von Volumen und Netzwerkinformationen
vsadmin-snaplock	• Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos • Verwaltung von Volumes, ausgenommen Volume-Verschiebungen • Verwaltung von Kontingenten, Qtrees, Snapshots und Dateien • Durchführen von SnapLock-Operationen, einschließlich privilegiertem Löschen • Konfiguration von Protokollen: NFS und SMB • Konfiguration von Diensten: DNS, LDAP und NIS • Überwachungsaufträge • Überwachung von Netzwerkverbindungen und Netzwerkschnittstellen
vsadmin-readonly	• Verwaltung der lokalen Passwort- und Schlüsselinformationen des eigenen Benutzerkontos • Überwachung des Gesundheitszustands der SVM • Überwachung der Netzwerkschnittstelle • Anzeigen von Volumes und LUNs • Anzeigen von Diensten und Protokollen

ONTAP Administratorzugriff mit System Manager verwalten

Die einem Administrator zugewiesene Rolle bestimmt, welche Funktionen der Administrator mit System Manager ausführen kann. System Manager stellt vordefinierte Rollen für Cluster-Administratoren und Storage-VM-Administratoren bereit. Die Rolle wird beim Erstellen des Administratorkontos zugewiesen oder kann später geändert werden.

Je nachdem, wie der Kontozugriff aktiviert wurde, kann es erforderlich sein, eine der folgenden Aktionen durchzuführen:

- Ein öffentlicher Schlüssel wird mit einem lokalen Konto verknüpft.
- Ein von einer Zertifizierungsstelle signiertes digitales Serverzertifikat installieren.
- AD-, LDAP- oder NIS-Zugriff konfigurieren.

Diese Aufgaben können vor oder nach der Aktivierung des Kontozugriffs durchgeführt werden.

Einem Administrator eine Rolle zuweisen

Einem Administrator wird wie folgt eine Rolle zugewiesen:

Schritte

1. **Cluster > Einstellungen** auswählen.
2. Wählen Sie → neben **Benutzer und Rollen** aus.
3. Wählen Sie + Add unter **Benutzer** aus.
4. Geben Sie einen Benutzernamen an und wählen Sie im Dropdown-Menü für **Rolle** eine Rolle aus.
5. Eine Anmeldemethode und ein Passwort für den Benutzer angeben.

Ändern der Administratorrolle

Die Rolle eines Administrators kann wie folgt geändert werden:

Schritte

1. **Cluster > Einstellungen** auswählen.
2. Wählen Sie den Namen des Benutzers aus, dessen Rolle Sie ändern möchten, und klicken Sie dann auf das ⋮ Symbol, das neben dem Benutzernamen erscheint.
3. Klicken Sie auf **Bearbeiten**.
4. Im Dropdown-Menü für **Rolle** eine Rolle auswählen.

Verwendung der JIT-Berechtigungserweiterung in ONTAP

Ab ONTAP 9.17.1 können Cluster-Administratoren "Just-in-Time (JIT) Privileg-Erweiterung konfigurieren" ONTAP Benutzern die Möglichkeit geben, ihre Berechtigungen vorübergehend zu erhöhen, um bestimmte Aufgaben auszuführen. Wenn JIT für einen Benutzer konfiguriert ist, kann dieser seine Berechtigungen vorübergehend auf eine Rolle anheben, die über die erforderlichen Berechtigungen zur Ausführung einer Aufgabe verfügt. Nach Ablauf der Sitzung kehrt der Benutzer zu seiner ursprünglichen Zugangsstufe zurück.

Cluster-Administratoren können die Dauer konfigurieren, für die ein Benutzer Zugriff auf die JIT-Berechtigungserweiterung hat. Beispielsweise kann der Zugriff eines Benutzers auf die JIT-Berechtigungserweiterung mit einem Sitzungslimit von 30 Minuten (dem *Sitzungsgültigkeitszeitraum*) für einen Zeitraum von 30 Tagen (dem *JIT-Gültigkeitszeitraum*) konfiguriert werden. Während des 30-tägigen Zeitraums kann der Benutzer seine Berechtigungen beliebig oft erweitern, jedoch ist jede Sitzung auf 30 Minuten begrenzt.

Über diese Aufgabe

- Die JIT-Berechtigungserweiterung steht nur Benutzern zur Verfügung, die mit SSH auf ONTAP zugreifen. Erweiterte Berechtigungen stehen nur innerhalb der aktuellen SSH-Sitzung zur Verfügung, können jedoch in beliebig vielen gleichzeitigen SSH-Sitzungen genutzt werden.
- Die JIT-Berechtigungserweiterung wird nur für Benutzer unterstützt, die sich mit Passwort-, nsswitch- oder Domänenauthentifizierung anmelden. Multifaktor-Authentifizierung (MFA) wird für die JIT-Berechtigungserweiterung nicht unterstützt.

- Die JIT-Sitzung eines Benutzers wird beendet, wenn die konfigurierte Sitzungs- oder JIT-Gültigkeitsdauer abläuft oder wenn ein Cluster-Administrator JIT-Zugriff für den Benutzer widerruft.

Bevor Sie beginnen

- Um auf die JIT-Berechtigungserweiterung zuzugreifen, muss ein Clusteradministrator den JIT-Zugriff für Ihr Konto konfigurieren. Der Clusteradministrator legt die Rolle fest, auf die Sie Ihre Berechtigungen erweitern können, sowie die Dauer, für die Sie auf erweiterte Berechtigungen zugreifen können.

Schritte

1. Vorübergehende Erhöhung der Berechtigungen auf die konfigurierte Rolle:

   ```
   security jit-privilege elevate
   ```

   Nach Eingabe dieses Befehls werden Sie zur Eingabe Ihres Anmeldepassworts aufgefordert. Wenn JIT access für Ihr Konto konfiguriert ist, wird Ihnen für die konfigurierte Sitzungsdauer eine erhöhte Zugangsstufe gewährt. Nach Ablauf der Sitzungsdauer kehren Sie zu Ihrer ursprünglichen Zugangsstufe zurück. Innerhalb des konfigurierten JIT-Gültigkeitszeitraums kann die Erhöhung Ihrer Berechtigungen beliebig oft erfolgen.

2. Die verbleibende Zeit in Ihrer JIT-Sitzung wird angezeigt:

   ```
   security jit-privilege show-remaining-time
   ```

   Wenn Sie sich aktuell in einer JIT-Sitzung befinden, zeigt dieser Befehl die verbleibende Zeit an.

3. Beenden Sie Ihre JIT-Sitzung bei Bedarf vorzeitig:

   ```
   security jit-privilege reset
   ```

   Falls Sie sich aktuell in einer JIT-Sitzung befinden, beendet dieser Befehl die JIT-Sitzung und stellt Ihre ursprüngliche Zugangsstufe wieder her.

JIT-Zugangsstufenerhöhung in ONTAP konfigurieren

Ab ONTAP 9.17.1 können Cluster-Administratoren die Just-in-Time (JIT) Privilegienerhöhung konfigurieren, damit ONTAP Benutzer ihre Berechtigungen vorübergehend erhöhen können, um bestimmte Aufgaben auszuführen. Wenn JIT für einen Benutzer konfiguriert ist, kann er vorübergehend "ihre Privilegien erhöhen" zu einer Rolle wechseln, die über die erforderlichen Berechtigungen zur Ausführung einer Aufgabe verfügt. Nach Ablauf der Sitzungsdauer kehrt der Benutzer zu seiner ursprünglichen Zugangsstufe zurück.

Cluster-Administratoren können die Dauer konfigurieren, für die ein Benutzer Zugriff auf die JIT-Berechtigungserweiterung hat. Beispielsweise kann der Benutzerzugriff auf die JIT-Elevation mit einem Sitzungszeitlimit von 30 Minuten (dem *Sitzungsgültigkeitszeitraum*) für einen Zeitraum von 30 Tagen (dem *JIT-Gültigkeitszeitraum*) konfiguriert werden. Während des 30-tägigen Zeitraums kann der Benutzer seine Berechtigungen beliebig oft erweitern, jedoch ist jede Sitzung auf 30 Minuten begrenzt.

Die JIT-Berechtigungserweiterung unterstützt das Prinzip der minimalen Berechtigungen und ermöglicht Benutzern die Ausführung von Aufgaben, die erhöhte Berechtigungen erfordern, ohne ihnen diese Berechtigungen dauerhaft zu erteilen. Dies trägt dazu bei, das Risiko unberechtigten Zugriffs oder versehentlicher Änderungen am System zu verringern. Die folgenden Beispiele beschreiben einige gängige Anwendungsfälle für die JIT-Berechtigungserweiterung:

- Temporärer Zugriff auf die `security login create`- und `security login delete`-Befehle ermöglicht das Onboarding und Offboarding von Benutzern.
- Temporärer Zugriff auf `system node image update` und `system node upgrade-revert` kann während eines Aktualisierungsfensters gewährt werden. Nach Abschluss der Aktualisierung wird der Befehlszugriff widerrufen.
- Vorübergehender Zugriff auf `cluster add-node`, `cluster remove-node` und `cluster modify` ermöglicht die Clustererweiterung oder Neukonfiguration. Nach Abschluss der Clusteränderungen wird der Befehlszugriff entzogen.
- Temporärer Zugriff auf `volume snapshot restore` wird gewährt, um Wiederherstellungsvorgänge und die Verwaltung von Sicherungszielen zu ermöglichen. Nach Abschluss der Wiederherstellung oder Konfiguration wird der Befehlszugriff entzogen.
- Temporärer Zugriff auf `security audit log show` kann gewährt werden, um die Überprüfung und den Export des Revisionsprotokolls während einer Compliance-Prüfung zu ermöglichen.

Eine ausführlichere Liste gängiger JIT-Anwendungsfälle ist unter Häufige Anwendungsfälle für JIT zu finden.

Cluster-Administratoren können den JIT Zugang für ONTAP Benutzer einrichten und die standardmäßigen JIT Gültigkeitszeiträume entweder global für den gesamten Cluster oder für bestimmte SVMs konfigurieren.

Über diese Aufgabe

- Die JIT-Berechtigungserweiterung steht nur Benutzern zur Verfügung, die mit SSH auf ONTAP zugreifen. Erweiterte Berechtigungen sind nur innerhalb der aktuellen SSH-Sitzung des Benutzers verfügbar, können jedoch in beliebig vielen gleichzeitigen SSH-Sitzungen genutzt werden.
- Die JIT-Berechtigungserweiterung wird nur für Benutzer unterstützt, die sich mit Passwort-, nsswitch- oder Domänenauthentifizierung anmelden. Multifaktor-Authentifizierung (MFA) wird für die JIT-Berechtigungserweiterung nicht unterstützt.

Bevor Sie beginnen

- Sie müssen ONTAP Cluster-Administrator auf der `admin`Zugangsstufe sein, um die folgenden Aufgaben auszuführen.

Globale JIT Einstellungen anpassen

Sie können die Standard-JIT-Einstellungen global für den gesamten ONTAP Cluster oder für eine bestimmte SVM ändern. Diese Einstellungen legen die Standardgültigkeitsdauer der Sitzung und die maximale JIT-Gültigkeitsdauer für Benutzer fest, die für den JIT-Zugang konfiguriert sind.

Über diese Aufgabe

- Der Standard `default-session-validity-period`wert beträgt eine Stunde. Diese Einstellung legt fest, wie lange ein Benutzer in einer JIT-Sitzung auf erhöhte Berechtigungen zugreifen kann, bevor eine erneute Erhöhung erforderlich ist.
- Der Standard `max-jit-validity-period`wert beträgt 90 Tage. Diese Einstellung legt den maximalen Zeitraum fest, in dem ein Benutzer nach dem konfigurierten Startdatum auf die JIT-Elevation zugreifen kann. Die JIT-Gültigkeitsdauer kann für einzelne Benutzer konfiguriert werden, sie darf jedoch die maximale JIT-Gültigkeitsdauer nicht überschreiten.

Schritte

1. Aktuelle JIT-Einstellungen prüfen:

```
security jit-privilege show -vserver <svm_name>
```

`-vserver` ist optional. Wenn keine SVM angegeben wird, zeigt der Befehl die globalen JIT-Einstellungen.

2. Die JIT-Einstellungen können global oder für eine SVM angepasst werden:

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

Wird keine SVM angegeben, ändert der Befehl die globalen JIT-Einstellungen. Das folgende Beispiel legt die Standard-JIT-Sitzungsdauer auf 45 Minuten und die maximale JIT-Dauer auf 30 Tage für SVM fest `svm1`:
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

In diesem Beispiel können Benutzer jeweils 45 Minuten lang auf die JIT-Berechtigungserweiterung zugreifen und JIT-Sitzungen für maximal 30 Tage nach dem konfigurierten Startdatum initiieren.

JIT-Zugangsstufe für einen Benutzer konfigurieren

Sie können ONTAP Benutzern die Zugangsstufe für JIT-Berechtigungserweiterung zuweisen.

Schritte

1. Aktueller JIT Zugriff für einen Benutzer:

```
security jit-privilege user show -username <username>
```

`-username` ist optional. Wenn kein Benutzername angegeben wird, zeigt der Befehl den JIT-Zugang für alle Benutzer an.

2. Neuen JIT Zugang für einen Benutzer zuweisen:

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- Wenn `-vserver`nicht angegeben ist, wird der JIT Zugriff auf Cluster Ebene zugewiesen.
- `-role` ist die RBAC Rolle, zu der der Benutzer erhöht wird. Falls nicht angegeben, `-role` ist der Standardwert `admin`.
- `-session-validity-period` ist die Dauer, für die der Benutzer auf die erhöhte Rolle zugreifen kann, bevor eine neue JIT-Sitzung gestartet werden muss. Falls nicht angegeben, wird der globale oder SVM `default-session-validity-period` verwendet.

- `-jit-validity-period` ist die maximale Dauer, für die ein Benutzer JIT-Sitzungen nach dem konfigurierten Startdatum initiieren kann. Falls nicht angegeben, wird der `session-validity-period` verwendet. Dieser Parameter darf den globalen oder SVM- `max-jit-validity-period` nicht überschreiten.
- `-start-time` ist das Datum und die Uhrzeit, ab der der Benutzer JIT-Sitzungen initiieren kann. Falls nicht angegeben, werden das aktuelle Datum und die aktuelle Uhrzeit verwendet.

  Das folgende Beispiel ermöglicht `ontap_user` den Zugriff auf die `admin` Rolle für 1 Stunde, bevor eine neue JIT-Sitzung gestartet werden muss. `ontap_user` kann JIT-Sitzungen für einen Zeitraum von 60 Tagen ab dem 1. Juli 2025 um 13:00 Uhr initiieren:
  `security jit-privilege user create -username ontap_user -role admin -session -validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. Bei Bedarf den JIT-Zugang eines Benutzers widerrufen:

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

Dieser Befehl widerruft die JIT-Zugangsstufe eines Benutzers, selbst wenn diese noch nicht abgelaufen ist. Wenn `-vserver` nicht angegeben ist, wird die JIT-Zugangsstufe auf Clusterebene widerrufen. Befindet sich der Benutzer in einer aktiven JIT-Sitzung, wird die Sitzung beendet.

Häufige Anwendungsfälle für JIT

Die folgende Tabelle enthält gängige Anwendungsfälle für die JIT-Berechtigungserweiterung. Für jeden Anwendungsfall muss eine RBAC-Rolle konfiguriert werden, um Zugriff auf die relevanten Befehle zu ermöglichen. Jeder Befehl ist mit der ONTAP Command Reference verlinkt, die weitere Informationen zum Befehl und seinen Parametern enthält.

Anwendungsfall	Befehle	Details
Benutzer- und Rollenverwaltung	• `security login create` • `security login delete`	Temporäre Rechteerweiterung zum Hinzufügen oder Entfernen von Benutzern oder zum Ändern von Rollen während des Onboardings oder Offboardings.
Zertifikatsverwaltung	• `security certificate create` • `security certificate install`	Kurzfristiger Zugriff für die Installation oder Verlängerung des Zertifikats wird gewährt.
SSH/CLI Zugriffskontrolle	• `security login create -application ssh`	Vorübergehender SSH-Zugriff für die Fehlerbehebung oder den Support durch den Hersteller.
Lizenzverwaltung	• `system license add` • `system license delete`	Berechtigungen zum Hinzufügen oder Entfernen von Lizenzen während der Aktivierung oder Deaktivierung von Funktionen gewähren.

Anwendungsfall	Befehle	Details
Systemaktualisierungen und Patches	• `system node image update` • `system node upgrade-revert`	Für das Upgrade-Fenster erhöhen, dann widerrufen.
Netzwerksicherheitseinstellungen	• `security login role create` • `security login role modify`	Temporäre Änderungen an netzwerkbezogenen Sicherheitsrollen ermöglichen.
Clusterverwaltung	• `cluster add-node` • `cluster remove-node` • `cluster modify`	Für Clustererweiterung oder -rekonfiguration Elevate verwenden.
SVM Management	• `vserver create` • `vserver delete` • `vserver modify`	Einem SVM vorübergehend Administratorrechte für die Bereitstellung oder Außerbetriebnahme zuweisen.
Volumenmanagement	• `volume create` • `volume delete` • `volume modify`	Elevate für Volume-Bereitstellung, -Größenänderung oder -Entfernung.
Snapshot Verwaltung	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	Für das Löschen oder Wiederherstellen von Snapshots während der Wiederherstellung sind erhöhte Berechtigungen erforderlich.
Netzwerkkonfiguration	• `network interface create` • `network port vlan create`	Rechte für Netzwerkänderungen während Wartungsfenstern gewähren.
Festplatten-/Aggregatverwaltung	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	Elevate dient zum Hinzufügen oder zur Entfernung von Datenträgern oder zum Verwalten von Aggregaten.
Datenschutz	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	Temporär erhöhen, um SnapMirror-Beziehungen zu konfigurieren oder wiederherzustellen.
Leistungsoptimierung	• `qos policy-group create` • `qos policy-group modify`	Elevate zur Fehlerbehebung bei der Performance oder zum Tuning.

Anwendungsfall	Befehle	Details
Zugriff auf das Revisionsprotokoll	• `security audit log show`	Temporär für die Überprüfung oder den Export des Revisionsprotokolls während Compliance-Prüfungen erhöhen.
Ereignis- und Alarmmanagement	• `event notification create` • `event notification modify`	Elevate dient zum Konfigurieren oder Testen von Ereignisbenachrichtigungen oder SNMP Traps.
Compliance-gesteuerter Datenzugriff	• `volume show` • `security audit log show`	Vorübergehender Lesezugriff für Prüfer, um sensible Daten oder Protokolle zu überprüfen.
Überprüfungen des privilegierten Zugriffs	• `security login show` • `security login role show`	Vorübergehende Erhöhung zur Überprüfung und Berichterstattung über privilegierten Zugriff. Schreibgeschützter, erhöhter Zugriff für eine begrenzte Zeit.

Verwandte Informationen

- "Cluster"
- "Ereignisbenachrichtigung"
- "Netzwerk"
- "QoS Richtliniengruppe"
- "Sicherheit"
- "SnapMirror"
- "Storage"
- "System"
- "Volumen"
- "vserver"

Administratorkonten verwalten

Informationen zu ONTAP Administratorkonten

Je nachdem, wie Sie den Kontozugriff aktiviert haben, kann es erforderlich sein, einen öffentlichen Schlüssel mit einem lokalen Konto zu verknüpfen, ein von einer Zertifizierungsstelle signiertes Server-Digitalzertifikat zu installieren oder den Zugriff auf AD, LDAP oder NIS zu konfigurieren. Alle diese Aufgaben können vor oder nach der Aktivierung des Kontozugriffs ausgeführt werden.

Einem ONTAP Administratorkonto einen öffentlichen Schlüssel zuordnen

Für die SSH Public Key Authentifizierung muss der öffentliche Schlüssel einem

Administratorkonto zugeordnet werden, bevor das Konto auf die SVM zugreifen kann. Mit dem `security login publickey create` Befehl kann ein Schlüssel einem Administratorkonto zugeordnet werden.

Über diese Aufgabe

Wenn ein Konto über SSH sowohl mit einem Passwort als auch mit einem öffentlichen SSH-Schlüssel authentifiziert wird, erfolgt die Authentifizierung des Kontos zuerst mit dem öffentlichen Schlüssel.

Bevor Sie beginnen

- Der SSH-Schlüssel muss generiert worden sein.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Einem Administratorkonto wird ein öffentlicher Schlüssel zugeordnet:

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

   Weitere Informationen zu `security login publickey create` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Änderung kann durch Anzeigen des öffentlichen Schlüssels überprüft werden:

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

   Weitere Informationen zu `security login publickey show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel

Der folgende Befehl verknüpft einen öffentlichen Schlüssel mit dem SVM-Administratorkonto `svmadmin1` für die SVM `engData1`. Dem öffentlichen Schlüssel wird die Indexnummer 5 zugewiesen.

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

SSH Public Keys und X.509-Zertifikate für ONTAP Administratoren verwalten

Für erhöhte Sicherheit bei der SSH-Authentifizierung mit Administratorkonten kann das `security login publickey` Befehlssatz verwendet werden, um den öffentlichen SSH-Schlüssel und dessen Zuordnung zu X.509-Zertifikaten zu verwalten.

Einem Administratorkonto werden ein öffentlicher Schlüssel und ein X.509-Zertifikat zugeordnet.

Ab ONTAP 9.13.1 kann ein X.509-Zertifikat mit dem öffentlichen Schlüssel verknüpft werden, der dem Administratorkonto zugeordnet ist. Dadurch ergibt sich zusätzliche Sicherheit, da bei der SSH-Anmeldung für dieses Konto eine Überprüfung auf Zertifikatsablauf oder -sperrung erfolgt.

Über diese Aufgabe

Wenn ein Konto über SSH sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem X.509-Zertifikat authentifiziert wird, prüft ONTAP die Gültigkeit des X.509-Zertifikats, bevor die Authentifizierung mit dem öffentlichen SSH-Schlüssel erfolgt. Die SSH-Anmeldung wird verweigert, wenn das Zertifikat abgelaufen oder widerrufen ist, und der öffentliche Schlüssel wird automatisch deaktiviert.

Bevor Sie beginnen

- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Der SSH-Schlüssel muss generiert worden sein.
- Wenn lediglich das X.509-Zertifikat auf Ablauf überprüft werden soll, kann ein selbstsigniertes Zertifikat verwendet werden.
- Falls das X.509-Zertifikat auf Ablauf und Widerruf überprüft werden soll:
  - Sie müssen das Zertifikat von einer Zertifizierungsstelle (CA) erhalten haben.
  - Sie müssen die Zertifikatskette (Zwischen- und Stammzertifizierungsstellenzertifikate) mit `security certificate install` Befehlen installieren. Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".
  - Sie müssen OCSP für SSH aktivieren. Weitere Anweisungen sind unter "Die Gültigkeit digitaler Zertifikate wird mithilfe von OCSP überprüft." zu finden.

Schritte

1. Einem Administratorkonto werden ein öffentlicher Schlüssel und ein X.509-Zertifikat zugeordnet:

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

   Weitere Informationen zu `security login publickey create` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Änderung kann durch Anzeigen des öffentlichen Schlüssels überprüft werden:

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

   Weitere Informationen zu `security login publickey show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel

Der folgende Befehl verknüpft einen öffentlichen Schlüssel und ein X.509-Zertifikat mit dem SVM-Administratorkonto `svmadmin2` für die SVM `engData2`. Dem öffentlichen Schlüssel wird die Indexnummer 6 zugewiesen.

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

Die Zertifikatszuordnung vom öffentlichen SSH-Schlüssel für ein Administratorkonto entfernen

Sie können die aktuelle Zertifikatszuordnung vom öffentlichen SSH-Schlüssel des Kontos entfernen, während der öffentliche Schlüssel beibehalten wird.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Die X.509-Zertifikatszuordnung von einem Administratorkonto entfernen und den vorhandenen SSH-öffentlichen Schlüssel beibehalten:

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

   Weitere Informationen zu `security login publickey modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Änderung kann durch Anzeigen des öffentlichen Schlüssels überprüft werden:

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

Beispiel

Der folgende Befehl entfernt die X.509-Zertifikatszuordnung vom SVM-Administratorkonto `svmadmin2` für die SVM `engData2` mit der Indexnummer 6.

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

Die Zuordnung des öffentlichen Schlüssels und des Zertifikats von einem Administratorkonto entfernen

Sie können die aktuelle Konfiguration des öffentlichen Schlüssels und des Zertifikats aus einem Konto entfernen.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Den öffentlichen Schlüssel und die Zuordnung eines X.509-Zertifikats von einem Administratorkonto entfernen:

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

   Weitere Informationen zu `security login publickey delete` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Änderung kann durch Anzeigen des öffentlichen Schlüssels überprüft werden:

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

Beispiel

Der folgende Befehl entfernt einen öffentlichen Schlüssel und ein X.509-Zertifikat vom SVM-Administratorkonto `svmadmin3` für die SVM `engData3` mit der Indexnummer 7.

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

Verwandte Informationen

- "security login publickey"

Cisco Duo 2FA für ONTAP SSH-Anmeldungen konfigurieren

Ab ONTAP 9.14.1 kann ONTAP so konfiguriert werden, dass Cisco Duo für die Zwei-Faktor-Authentifizierung (2FA) bei SSH-Anmeldungen verwendet wird. Duo wird auf Clusterebene konfiguriert und gilt standardmäßig für alle Benutzerkonten. Alternativ kann Duo auf Ebene der Storage VM (früher als vserver bezeichnet) konfiguriert werden, wobei es dann nur für Benutzer dieser Storage VM gilt. Wenn Duo aktiviert und konfiguriert ist, dient es als zusätzliches Authentifizierungsverfahren und ergänzt die bestehenden Methoden für alle Benutzer.

Wenn Sie die Duo Authentifizierung für SSH-Anmeldungen aktivieren, müssen Benutzer beim nächsten Anmelden per SSH ein Gerät registrieren. Informationen zur Registrierung enthält die Cisco Duo "Einschreibungsdokumentation".

Mit der ONTAP-Befehlszeilenschnittstelle können die folgenden Aufgaben mit Cisco Duo durchgeführt werden:

- Cisco Duo konfigurieren
- Cisco Duo Konfiguration ändern
- Cisco Duo Konfiguration entfernen
- Cisco Duo Konfiguration anzeigen
- Eine Duo Gruppe entfernen
- Duo Gruppen anzeigen
- Duo Authentifizierung für Benutzer umgehen

Cisco Duo konfigurieren

Sie können eine Cisco Duo Konfiguration entweder für den gesamten Cluster oder für eine bestimmte Storage VM (in der ONTAP CLI als vserver bezeichnet) mit dem `security login duo create` Befehl erstellen. In diesem Fall ist Cisco Duo für SSH-Anmeldungen für diesen Cluster oder diese Storage VM aktiviert. Weitere Informationen zu `security login duo create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Im Cisco Duo Admin Panel anmelden.

2. Zu **Anwendungen > UNIX Application** wechseln.
3. Notieren Sie Ihren Integrationsschlüssel, Ihren geheimen Schlüssel und Ihren API-Hostnamen.
4. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
5. Cisco Duo Authentifizierung für diese Storage-VM aktivieren, wobei die Informationen aus Ihrer Umgebung anstelle der Werte in Klammern einzusetzen sind:

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

Cisco Duo Konfiguration ändern

Sie können die Art und Weise ändern, wie Cisco Duo Benutzer authentifiziert (zum Beispiel wie viele Authentifizierungsaufforderungen gestellt werden oder welcher HTTP-Proxy verwendet wird). Wenn die Cisco Duo-Konfiguration für eine Storage-VM (in der ONTAP CLI als vserver bezeichnet) geändert werden muss, kann der `security login duo modify` Befehl verwendet werden. Weitere Informationen zu `security login duo modify` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Im Cisco Duo Admin Panel anmelden.
2. Zu **Anwendungen > UNIX Application** wechseln.
3. Notieren Sie Ihren Integrationsschlüssel, Ihren geheimen Schlüssel und Ihren API-Hostnamen.
4. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
5. Die Cisco Duo Konfiguration für diese Storage-VM kann angepasst werden, indem die Werte in Klammern durch die aktualisierten Informationen aus Ihrer Umgebung ersetzt werden:

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

Cisco Duo Konfiguration entfernen

Sie können die Cisco Duo Konfiguration entfernen, wodurch die Notwendigkeit entfällt, dass sich SSH-Benutzer bei der Anmeldung mit Duo authentifizieren. Zum Entfernen der Cisco Duo Konfiguration für eine

Storage VM (in der ONTAP CLI als vserver bezeichnet) kann der `security login duo delete` Befehl verwendet werden. Weitere Informationen zu `security login duo delete` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Entfernen Sie die Cisco Duo Konfiguration für diese Storage-VM, wobei Sie den Namen Ihrer Storage-VM für `<STORAGE_VM_NAME>` einsetzen:

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

   Dadurch wird die Cisco Duo Konfiguration für diese Storage-VM dauerhaft gelöscht.

Cisco Duo Konfiguration anzeigen

Die bestehende Cisco Duo Konfiguration für eine Storage VM (in der ONTAP CLI als vserver bezeichnet) lässt sich mit dem `security login duo show` Befehl anzeigen. Weitere Informationen zu `security login duo show` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Die Cisco Duo Konfiguration für diese Storage-VM anzeigen. Optional kann der `vserver` Parameter verwendet werden, um eine Storage-VM anzugeben, wobei der Name der Storage-VM für `<STORAGE_VM_NAME>` eingesetzt wird:

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

   Sie sollten eine Ausgabe ähnlich der folgenden sehen:

   ```
   Vserver: testcluster
   Enabled: true

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

Eine Duo Gruppe erstellen

Es ist möglich, Cisco Duo so zu konfigurieren, dass nur die Benutzer einer bestimmten Active Directory-, LDAP- oder lokalen Nutzergruppe in den Duo-Authentifizierungsprozess einbezogen werden. Wenn eine Duo-Gruppe erstellt wird, werden nur die Benutzer dieser Gruppe zur Duo-Authentifizierung aufgefordert. Eine Duo-Gruppe kann mit dem `security login duo group create` Befehl erstellt werden. Beim Erstellen einer Gruppe besteht optional die Möglichkeit, bestimmte Benutzer dieser Gruppe vom Duo-Authentifizierungsprozess auszuschließen. Weitere Informationen zu `security login duo group create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Die Duo-Gruppe wird erstellt, wobei die Informationen aus Ihrer Umgebung anstelle der Werte in Klammern eingesetzt werden. Wenn der `-vserver` Parameter weggelassen wird, erfolgt die Erstellung der Gruppe auf Clusterebene:

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

   Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen. Benutzer, die mit dem optionalen `-excluded-users` Parameter angegeben werden, sind nicht in den Duo-Authentifizierungsprozess einbezogen.

Duo Gruppen anzeigen

Vorhandene Cisco Duo Gruppeneinträge lassen sich mit dem `security login duo group show` Befehl anzeigen. Weitere Informationen zu `security login duo group show` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Die Duo-Gruppeneinträge werden angezeigt, wobei die Werte in Klammern durch Informationen aus Ihrer Umgebung ersetzt werden. Wenn der `-vserver` Parameter weggelassen wird, erscheint die Gruppe auf Clusterebene:

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

   Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen. Benutzer, die mit dem optionalen `-excluded-users` Parameter angegeben werden, werden nicht angezeigt.

Eine Duo Gruppe entfernen

Ein Duo-Gruppeneintrag kann mit dem `security login duo group delete` Befehl entfernt werden. Wenn eine Gruppe entfernt wird, sind die Benutzer dieser Gruppe nicht mehr im Duo Authentifizierungsprozess enthalten. Weitere Informationen zu `security login duo group delete` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Der Duo-Gruppeneintrag wird entfernt, wobei die Werte in Klammern durch Informationen aus Ihrer Umgebung ersetzt werden. Wenn der `-vserver` Parameter weggelassen wird, erfolgt die Entfernung der Gruppe auf Clusterebene.

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

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

Duo Authentifizierung für Benutzer umgehen

Es besteht die Möglichkeit, alle Benutzer oder bestimmte Benutzer vom Duo SSH-Authentifizierungsprozess auszuschließen.

Alle Duo Nutzer ausschließen

Die Cisco Duo SSH-Authentifizierung kann für alle Benutzer deaktiviert werden.

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Cisco Duo Authentifizierung für SSH-Benutzer deaktivieren, wobei der Vserver-Name durch `<STORAGE_VM_NAME>` ersetzt wird:

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

Diese Einstellung `-is-enabled false` deaktiviert die Duo Authentifizierung, entfernt die Duo-Konfiguration jedoch nicht aus dem SSH-Anmeldepfad. In manchen Umgebungen kann für SSH-Anmeldungen weiterhin ein interaktiver Authentifizierungsablauf erforderlich sein, was nicht-interaktive SSH-Anmeldungen verhindern kann. Zur Wiederherstellung des nicht-interaktiven SSH-Anmeldeverhaltens ist die Duo-Konfiguration vollständig mit `security login duo delete -vserver <STORAGE_VM_NAME>` zu entfernen.

Duo Gruppenbenutzer ausschließen

Bestimmte Benutzer, die Teil einer Duo-Gruppe sind, können vom Duo SSH-Authentifizierungsprozess ausgeschlossen werden.

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Cisco Duo Authentifizierung für bestimmte Benutzer in einer Gruppe deaktivieren. Der Gruppenname und die Liste der auszuschließenden Benutzer sind anstelle der Werte in Klammern einzusetzen:

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

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

Weitere Informationen zu `security login duo group modify` finden sich in der "ONTAP-Befehlsreferenz".

Lokale Duo Nutzer ausschließen

Bestimmte lokale Nutzer können von der Nutzung der Duo Authentifizierung ausgeschlossen werden, indem das Cisco Duo Admin Panel verwendet wird. Anleitungen finden sich in der "Cisco Duo Dokumentation".

Ein von einer Zertifizierungsstelle signiertes Serverzertifikat in ONTAP generieren und installieren

Auf Produktionssystemen empfiehlt es sich, zur Authentifizierung des Clusters oder der SVM als SSL-Server ein von einer Zertifizierungsstelle signiertes digitales Zertifikat zu installieren. Sie können den `security certificate generate-csr`Befehl verwenden, um eine Zertifikatsignierungsanforderung (CSR) zu generieren, und den `security certificate install`Befehl, um das von der Zertifizierungsstelle erhaltene Zertifikat zu installieren. Weitere Informationen zu `security certificate generate-csr` und `security certificate install` finden Sie in der "ONTAP-Befehlsreferenz".

Generieren einer Certificate Signing Request

Mit dem `security certificate generate-csr` Befehl lässt sich eine Zertifikatsignierungsanforderung (CSR) generieren. Nach der Bearbeitung Ihrer Anforderung sendet die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Eine CSR generieren:

```
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
```

Der folgende Befehl erstellt eine CSR mit einem 2048-Bit-Privatschlüssel, der von der `SHA256` Hash-Funktion generiert wird. Die CSR ist für die Verwendung durch die `Software` Gruppe in der `IT` Abteilung eines Unternehmens mit Sitz in Sunnyvale, California, USA bestimmt. Der benutzerdefinierte Common Name des Unternehmens lautet `server1.companyname.com`. Die E-Mail-Adresse des SVM Kontaktadministrators lautet `web@example.com`. Das System zeigt die CSR und den Privatschlüssel in der Ausgabe an.

▼ **Beispiel für das Erstellen eines CSR**

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

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. Die Zertifikatsanforderung aus der CSR-Ausgabe kopieren und in elektronischer Form (z. B. per E-Mail) zur Signierung an eine vertrauenswürdige Drittzertifizierungsstelle senden.

   Die Zertifizierungsstelle muss das signierte Zertifikat im Base64-kodierten PEM- oder PKCS12-Format zurückgeben.

   Nach Bearbeitung Ihres Antrags sendet Ihnen die Zertifizierungsstelle das signierte digitale Zertifikat. Eine Kopie des privaten Schlüssels und des von der Zertifizierungsstelle signierten digitalen Zertifikats sollte aufbewahrt werden.

Ein von einer Zertifizierungsstelle signiertes Serverzertifikat installieren

Sie können den `security certificate install` Befehl verwenden, um ein von einer Zertifizierungsstelle (CA) signiertes Serverzertifikat auf einer SVM zu installieren. ONTAP fordert Sie zur Eingabe der Root- und Zwischenzertifikate der Zertifizierungsstelle (CA) auf, die die Zertifikatskette des Serverzertifikats bilden. Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Ein von einer Zertifizierungsstelle signiertes Serverzertifikat installieren:

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

ONTAP fordert Sie zur Eingabe der Stamm- und Zwischenzertifikate der Zertifizierungsstelle 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 dazu, dass die Installation des Serverzertifikats fehlschlägt.

Der folgende Befehl installiert das CA-signierte Serverzertifikat und die Zwischenzertifikate auf SVM `engData2`.

▼ Beispiel für die Installation eines CA-signierten Serverzertifikats und von Zwischenzertifikaten

```
cluster1::>security certificate install -vserver engData2 -type server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----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-----
<certificate_value>
-----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-----
<certificate_value>
-----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.
```

Verwandte Informationen

- "security certificate generate-csr"

ONTAP Zertifikate mit System Manager verwalten

Ab ONTAP 9.10.1 kann mit System Manager die Verwaltung von vertrauenswürdigen Zertifizierungsstellen, Client-/Server-Zertifikaten und lokalen (Onboard) Zertifizierungsstellen erfolgen.

Mit System Manager können Sie die von anderen Anwendungen empfangenen Zertifikate verwalten, sodass die Kommunikation dieser Anwendungen authentifiziert werden kann. Auch die eigenen Zertifikate, die Ihr System gegenüber anderen Anwendungen identifizieren, lassen sich verwalten.

Zertifikatsinformationen anzeigen

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

Schritte

1. Im System Manager **Cluster > Einstellungen** auswählen.
2. Scrollen Sie zum Bereich **Sicherheit**. Im Abschnitt **Zertifikate** werden folgende Details angezeigt:
   - Die Anzahl der gespeicherten vertrauenswürdigen Zertifizierungsstellen.
   - Die Anzahl der gespeicherten Client-/Serverzertifikate.
   - Die Anzahl der gespeicherten lokalen Zertifizierungsstellen.
3. Wählen Sie eine beliebige Zahl aus, um Details zu einer Zertifikatskategorie anzuzeigen, oder wählen Sie → aus, um die Seite **Zertifikate** zu öffnen, die Informationen zu allen Kategorien enthält. Die Liste zeigt die Informationen für den gesamten Cluster an. Um Informationen nur für eine bestimmte Storage-VM anzuzeigen, sind die folgenden Schritte erforderlich:
   a. Wählen Sie **Speicher > Speicher-VMs**.
   b. Die Storage-VM auswählen.
   c. Zur Registerkarte **Einstellungen** wechseln.
   d. Wählen Sie eine Nummer im Abschnitt **Zertifikat** aus.

Nächste Schritte

- Auf der Seite **Zertifikate** können Sie Generieren einer Certificate Signing Request.
- Die Zertifikatsinformationen sind in drei Registerkarten unterteilt, eine für jede Kategorie. Von jeder Registerkarte aus lassen sich die folgenden Aufgaben durchführen:

Auf dieser Registerkarte…	Sie können diese Verfahren durchführen…
Vertrauenswürdige Zertifizierungsstellen	• Eine vertrauenswürdige Zertifizierungsstelle installieren (hinzufügen) • Eine vertrauenswürdige Zertifizierungsstelle löschen • Eine vertrauenswürdige Zertifizierungsstelle erneuern

Client/Server-Zertifikate	• Ein Client-/Serverzertifikat installieren (hinzufügen) • [gen-cs-cert] • Löschen eines Client/Server-Zertifikats • Benachrichtigungen zum Zertifikatsablauf ändern (beginnend mit ONTAP 9.20.1) • Ein Client-/Serverzertifikat erneuern
Lokale Zertifizierungsstellen	• Eine neue lokale Zertifizierungsstelle erstellen • Ein Zertifikat mit einer lokalen Zertifizierungsstelle signieren • Lokale Zertifizierungsstelle löschen • Eine lokale Zertifizierungsstelle erneuern

Benachrichtigungen zum Zertifikatsablauf ändern

Ab ONTAP 9.20.1 zeigt System Manager 30 Tage vor Ablauf eines Zertifikats für einen Cluster oder eine Storage Virtual Machine (SVM) eine Dashboard-Systemstatuswarnung an. Die Warnung wird täglich aktualisiert, um die Anzahl der verbleibenden Tage bis zum Ablauf anzuzeigen.

Sie können den standardmäßigen Warnschwellenwert von 30 Tagen auf eine beliebige Anzahl von Tagen zwischen 0 und 90 ändern. Sie können die Benachrichtigung auch deaktivieren, sodass sie nicht angezeigt wird, oder Benachrichtigungen für bereits abgelaufene Zertifikate unterdrücken, während Sie weiterhin Benachrichtigungen für bevorstehende Abläufe erhalten.

Schritte

1. Im System Manager **Cluster > Einstellungen** auswählen.
2. Unter **Zertifikate** erfolgt die Auswahl von → und anschließend von **Zertifikateinstellungen**.
3. Aktualisierung des Schwellenwerts für die Ablaufwarnung sowie Deaktivierung oder Unterdrückung der Warnung:
   - Eine Aktualisierung des **Warnschwellenwerts** auf eine beliebige Anzahl von Tagen zwischen 0 und 90 ist möglich.
   - Mit **Ablaufwarnungen deaktivieren** lässt sich die Warnung deaktivieren.
   - Mit **Benachrichtigungen über abgelaufene Zertifikate unterdrücken** werden Benachrichtigungen für bereits abgelaufene Zertifikate ausgeblendet, während Benachrichtigungen für bevorstehende Ablaufdaten weiterhin empfangen werden.

Generieren einer Certificate Signing Request

Sie können mit System Manager auf jeder Registerkarte der Seite **Zertifikate** eine Zertifikatsignierungsanforderung (CSR) generieren. Ein privater Schlüssel und eine zugehörige CSR werden generiert, die von einer Zertifizierungsstelle signiert werden können, um ein öffentliches Zertifikat zu erstellen.

Schritte

1. Die Seite **Zertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. **+CSR generieren** auswählen.
3. Vervollständigen Sie die Angaben zum Betreffnamen:
   a. Einen **allgemeinen Namen** eingeben.

b. Ein **Land** auswählen.

c. Eine **Organisation** eingeben.

d. Eine **Organisationseinheit** eingeben.

4. Wenn Sie die Standardeinstellungen überschreiben möchten, wählen Sie **Weitere Optionen** und geben zusätzliche Informationen an.

Eine vertrauenswürdige Zertifizierungsstelle installieren (hinzufügen)

Im System Manager lassen sich zusätzliche vertrauenswürdige Zertifizierungsstellen installieren.

Schritte

1. Die Registerkarte **Vertrauenswürdige Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie + Add .
3. Im Fenster **Vertrauenswürdige Zertifizierungsstelle hinzufügen** sind die folgenden Schritte auszuführen:
   - Einen **Namen** eingeben.
   - Für den **Bereich** eine Storage-VM auswählen.
   - Einen **allgemeinen Namen** eingeben.
   - Einen **Typ** auswählen.
   - Geben Sie die **Zertifikatsdetails** ein oder importieren Sie diese.

Eine vertrauenswürdige Zertifizierungsstelle löschen

Mit System Manager kann eine vertrauenswürdige Zertifizierungsstelle gelöscht werden.

ⓘ Vorinstallierte vertrauenswürdige Zertifizierungsstellen mit ONTAP können nicht gelöscht werden.

Schritte

1. Die Registerkarte **Vertrauenswürdige Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie den Namen der vertrauenswürdigen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Namen und dann **Löschen** aus.

Eine vertrauenswürdige Zertifizierungsstelle erneuern

Mit System Manager ist es möglich, eine vertrauenswürdige Zertifizierungsstelle zu erneuern, deren Gültigkeit abgelaufen ist oder demnächst abläuft.

Schritte

1. Die Registerkarte **Vertrauenswürdige Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie den Namen der vertrauenswürdigen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Zertifikatsnamen dann **Erneuern**.

Ein Client-/Serverzertifikat installieren (hinzufügen)

Mit System Manager können zusätzliche Client-/Serverzertifikate installiert werden.

Schritte

1. Die Registerkarte **Client/Serverzertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie 

.
3. Im Fenster **Client-/Serverzertifikat hinzufügen** sind die folgenden Schritte auszuführen:
   - Einen **Zertifikatsnamen** eingeben.
   - Für den **Bereich** eine Storage-VM auswählen.
   - Einen **allgemeinen Namen** eingeben.
   - Einen **Typ** auswählen.
   - Geben Sie die **Zertifikatsdetails** ein oder importieren Sie diese. Die Zertifikatsdetails können entweder direkt eingegeben oder aus einer Textdatei kopiert und eingefügt werden. Alternativ lässt sich der Text aus einer Zertifikatsdatei durch Klicken auf **Import** importieren.
   - Geben Sie den **privaten Schlüssel** ein. Sie können den privaten Schlüssel entweder direkt eingeben oder aus einer Textdatei kopieren und einfügen oder den Text aus einer privaten Schlüsseldatei importieren, indem Sie auf **Import** klicken.

Ein selbstsigniertes Client-/Serverzertifikat generieren (hinzufügen)

Mit System Manager lassen sich zusätzliche selbstsignierte Client/Server-Zertifikate generieren.

Schritte

1. Die Registerkarte **Client/Serverzertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. **+Selbstsigniertes Zertifikat generieren** auswählen.
3. Im Fenster **Selbstsigniertes Zertifikat generieren** Folgendes ausführen:
   - Einen **Zertifikatsnamen** eingeben.
   - Für den **Bereich** eine Storage-VM auswählen.
   - Einen **allgemeinen Namen** eingeben.
   - Einen **Typ** auswählen.
   - Eine **Hashfunktion** auswählen.
   - Wählen Sie eine **Schlüssellänge**.
   - Eine **Speicher-VM** auswählen.

Löschen eines Client/Server-Zertifikats

Mit System Manager können Sie Client-/Serverzertifikate löschen.

Schritte

1. Die Registerkarte **Client/Serverzertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie den Namen des Client/Server-Zertifikats aus.
3. Wählen Sie ⋮ neben dem Namen aus und klicken Sie auf **Löschen**.

Ein Client-/Serverzertifikat erneuern

Mit System Manager kann ein Client/Server-Zertifikat erneuert werden, das abgelaufen ist oder demnächst abläuft.

Schritte

1. Die Registerkarte **Client/Serverzertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie den Namen des Client/Server-Zertifikats aus.
3. Wählen Sie ⋮ neben dem Namen und klicken Sie auf **Erneuern**.

Eine neue lokale Zertifizierungsstelle erstellen

Mit System Manager kann eine neue lokale Zertifizierungsstelle erstellt werden.

Schritte

1. Den Tab **Lokale Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie + Add .
3. Im Fenster **Lokale Zertifizierungsstelle hinzufügen** Folgendes ausführen:
   - Einen **Namen** eingeben.
   - Für den **Bereich** eine Storage-VM auswählen.
   - Einen **allgemeinen Namen** eingeben.
4. Wenn Sie die Standardeinstellungen überschreiben möchten, wählen Sie **Weitere Optionen** und geben zusätzliche Informationen an.

Ein Zertifikat mit einer lokalen Zertifizierungsstelle signieren

Im System Manager kann eine lokale Zertifizierungsstelle verwendet werden, um ein Zertifikat zu signieren.

Schritte

1. Den Tab **Lokale Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Den Namen der lokalen Zertifizierungsstelle auswählen.
3. Wählen Sie ⋮ neben dem Namen dann **Zertifikat signieren**.
4. Das Formular **Antrag auf Unterzeichnung eines Zertifikats** ausfüllen.
   - Sie können entweder den Inhalt der Zertifikatsignierung einfügen oder eine Zertifikatsignierungsanforderungsdatei durch Klicken auf **Import** importieren.
   - Geben Sie die Anzahl der Tage an, für die das Zertifikat gültig ist.

Lokale Zertifizierungsstelle löschen

Mit System Manager kann eine lokale Zertifizierungsstelle gelöscht werden.

Schritte

1. Die Registerkarte **Local Certificate Authority** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Den Namen der lokalen Zertifizierungsstelle auswählen.
3. Wählen Sie ⋮ neben dem Namen und dann **Löschen**.

Eine lokale Zertifizierungsstelle erneuern

Mit System Manager können Sie eine lokale Zertifizierungsstelle erneuern, deren Gültigkeit abgelaufen ist oder demnächst abläuft.

Schritte

1. Die Registerkarte **Local Certificate Authority** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Den Namen der lokalen Zertifizierungsstelle auswählen.
3. Wählen Sie ⋮ neben dem Namen und klicken Sie auf **Erneuern**.

Konfigurieren des Zugriffs auf Active Directory-Domänencontroller in ONTAP

Sie müssen den Zugriff des AD-Domänencontrollers auf den Cluster oder die SVM konfigurieren, bevor ein AD-Konto auf die SVM zugreifen kann. Wenn bereits ein SMB-Server für eine Daten-SVM konfiguriert wurde, kann die SVM als Gateway oder Tunnel für den AD-Zugriff auf den Cluster verwendet werden. Wenn kein SMB-Server konfiguriert wurde, kann ein Computerkonto für die SVM in der AD-Domäne erstellt werden.

ONTAP unterstützt die folgenden Domänencontroller-Authentifizierungsdienste:

- Kerberos
- LDAP
- Netlogon
- Lokale Sicherheitsautorität (LSA)

ONTAP unterstützt die folgenden Sitzungsschlüssel-Algorithmen für sichere Netlogon Verbindungen:

Session key Algorithmus	Verfügbar ab…
HMAC-SHA256, basierend auf dem Advanced Encryption Standard (AES). Wenn auf Ihrem Cluster ONTAP 9.9.1 oder einer früheren Version ausgeführt wird und Ihr Domänencontroller AES für sichere Netlogon-Dienste erzwingt, schlägt die Verbindung fehl. In diesem Fall ist der Domänencontroller so zu konfigurieren, dass er stattdessen starke Schlüsselverbindungen mit ONTAP akzeptiert.	ONTAP 9.10.1
DES und HMAC-MD5 (wenn ein starker Schlüssel gesetzt ist)	Alle ONTAP 9 Versionen

Wenn AES-Sitzungsschlüssel während des Aufbaus eines sicheren Netlogon-Kanals verwendet werden sollen, ist zu überprüfen, ob AES auf Ihrer SVM aktiviert ist.

- Ab ONTAP 9.14.1 ist AES standardmäßig aktiviert, wenn eine SVM erstellt wird, und es ist nicht erforderlich, die Sicherheitseinstellungen der SVM zu ändern, um AES-Sitzungsschlüssel während der Herstellung eines sicheren Netlogon-Kanals zu verwenden.
- In ONTAP 9.10.1 bis 9.13.1 ist AES beim Erstellen einer SVM standardmäßig deaktiviert. AES muss mit dem folgenden Befehl aktiviert werden:

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

Beim Upgrade auf ONTAP 9.14.1 oder höher ändert sich die AES-Einstellung für bestehende SVMs, die mit älteren ONTAP-Versionen erstellt wurden, nicht automatisch. Der Wert dieser Einstellung muss weiterhin aktualisiert werden, um AES auf diesen SVMs zu aktivieren.

Einen Authentifizierungstunnel konfigurieren

Wenn Sie bereits einen SMB-Server für eine Daten-SVM konfiguriert haben, kann mit dem `security login domain-tunnel create` Befehl die SVM als Gateway (oder Tunnel) für den AD-Zugriff auf den Cluster konfiguriert werden.

Vor ONTAP 9.16.1 ist ein Authentifizierungstunnel erforderlich, um Cluster-Administratorkonten mit AD zu verwalten.

Bevor Sie beginnen

- Es muss ein SMB-Server für eine Daten-SVM konfiguriert sein.
- Ein AD-Domänenbenutzerkonto muss für den Zugriff auf die Admin-SVM des Clusters aktiviert sein.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Ab ONTAP 9.10.1 ist bei Verwendung eines SVM-Gateways (Domain-Tunnel) für den AD-Zugriff die Nutzung von Kerberos für die Admin-Authentifizierung möglich, sofern NTLM in Ihrer AD-Domäne deaktiviert ist. In früheren Versionen wurde Kerberos bei der Admin-Authentifizierung für SVM-Gateways nicht unterstützt. Diese Funktionalität ist standardmäßig verfügbar, eine Konfiguration ist nicht erforderlich.

Zuerst wird immer die Kerberos-Authentifizierung versucht. Im Falle eines Fehlschlags wird anschließend die NTLM-Authentifizierung versucht.

Schritte

1. Eine SMB-fähige Daten-SVM als Authentifizierungstunnel für den Zugriff des AD-Domänencontrollers auf den Cluster konfigurieren:

   ```
   security login domain-tunnel create -vserver <svm_name>
   ```

   Weitere Informationen zu `security login domain-tunnel create` finden sich in der "ONTAP-Befehlsreferenz".

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

   Der folgende Befehl konfiguriert die SMB-fähige Daten-SVM `engData` als Authentifizierungstunnel.

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

Ein SVM-Computerkonto in der Domäne erstellen

Wenn für eine Daten-SVM kein SMB-Server konfiguriert wurde, kann mit dem `vserver active-directory create` Befehl ein Computerkonto für die SVM in der Domäne erstellt werden.

Über diese Aufgabe

Nach Eingabe des `vserver active-directory create` Befehls werden Sie aufgefordert, die Anmeldeinformationen für ein AD-Benutzerkonto mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit in der Domäne anzugeben. Das Kennwort des Kontos darf nicht leer sein.

Ab ONTAP 9.16.1 lässt sich dieses Verfahren zur Verwaltung von Cluster-Administratorkonten mit AD nutzen.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Ein Computerkonto für eine SVM in der AD-Domäne erstellen:

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

Ab ONTAP 9.16.1 akzeptiert der `-vserver` Parameter die Admin-SVM. Weitere Informationen zu `vserver active-directory create` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl erstellt ein Computerkonto mit dem Namen `ADSERVER1` in der Domäne `example.com` für SVM `engData`. Nach Eingabe des Befehls erfolgt eine Aufforderung zur Eingabe der Anmeldeinformationen des AD-Benutzerkontos.

```
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:
```

LDAP- oder NIS-Serverzugriff in ONTAP konfigurieren

Sie müssen den LDAP- oder NIS-Serverzugriff auf eine SVM konfigurieren, bevor LDAP- oder NIS-Konten auf die SVM zugreifen können. Die Switch-Funktion ermöglicht die Verwendung von LDAP oder NIS als alternative Namensdienstquellen.

LDAP Serverzugriff konfigurieren

Sie müssen den LDAP-Serverzugriff auf eine SVM konfigurieren, bevor LDAP-Konten auf die SVM zugreifen können. Mit dem `vserver services name-service ldap client create` Befehl lässt sich eine LDAP-Client-Konfiguration auf der SVM erstellen. Anschließend kann der `vserver services name-service ldap create` Befehl verwendet werden, um die LDAP-Client-Konfiguration mit der SVM zu verknüpfen.

Über diese Aufgabe

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

- MS-AD-BIS (das bevorzugte Schema für die meisten Windows 2012 und späteren AD-Server)
- AD-IDMU (Windows 2008, Windows 2016 und spätere AD-Server)
- AD-SFU (Windows 2003 und ältere AD-Server)
- RFC-2307 (UNIX LDAP-Server)

Es empfiehlt sich, die Standardschemata zu verwenden, sofern keine anderen Anforderungen bestehen. Falls dies der Fall ist, kann ein eigenes Schema erstellt werden, indem ein Standardschema kopiert und die Kopie angepasst wird. Weitere Informationen:

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

Bevor Sie beginnen

- Es muss eine "CA-signiertes digitales Serverzertifikat" auf der SVM installiert sein.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

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

   ```
   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 Daten-SVMs unterstützt. Für den Zugriff auf Admin-SVMs wird es nicht unterstützt.

   Weitere Informationen zu `vserver services name-service ldap client create` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl erstellt eine LDAP-Client-Konfiguration mit dem Namen `corp` auf SVM `engData`. Der Client stellt anonyme Bindungen zu den LDAP-Servern mit den IP-Adressen 172.160.0.100 und 172.16.0.101 her. Der Client verwendet das RFC-2307-Schema für LDAP-Abfragen. Die Kommunikation zwischen Client und Server wird mit 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
   ```

Das `-ldap-servers` Feld ersetzt das `-servers` Feld. Das `-ldap-servers` Feld kann verwendet werden, um entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server anzugeben.

2. Die LDAP-Client-Konfiguration mit der SVM verknüpfen: `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client -enabled <true|false>`

   Weitere Informationen zu `vserver services name-service ldap create` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl verknüpft die LDAP-Client-Konfiguration `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
   ```

   Der `vserver services name-service ldap create` Befehl führt eine automatische Konfigurationsprüfung durch und gibt eine Fehlermeldung aus, wenn ONTAP den Nameserver nicht erreichen kann.

3. Der Status der Nameserver kann mit dem Befehl vserver services name-service ldap check validiert werden.

   Der folgende Befehl validiert LDAP-Server auf der SVM vs0.

   ```
   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".                                                  |
   ```

   Mit dem `name service check` Befehl lässt sich der Status der Nameserver validieren.

NIS Serverzugriff konfigurieren

Sie müssen den NIS-Serverzugriff auf eine SVM konfigurieren, bevor NIS-Konten auf die SVM zugreifen können. Mit dem `vserver services name-service nis-domain create` Befehl lässt sich eine NIS-Domänenkonfiguration auf einer SVM erstellen.

Bevor Sie beginnen

- Alle konfigurierten Server müssen verfügbar und erreichbar sein, bevor die NIS-Domäne auf der SVM konfiguriert wird.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Erstellen einer NIS-Domänenkonfiguration auf einer SVM:

   `vserver services name-service nis-domain create -vserver <SVM_name> -domain <client_configuration> -nis-servers <NIS_server_IPs>`

   Weitere Informationen zu `vserver services name-service nis-domain create` finden sich in der "ONTAP-Befehlsreferenz".

   > Das `-nis-servers` Feld ersetzt das `-servers` Feld. Das `-nis-servers` Feld kann verwendet werden, um entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server anzugeben.

   Der folgende Befehl erstellt eine NIS-Domänenkonfiguration auf SVM `engData`. Die NIS-Domäne `nisdomain` 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 -nis-servers 192.0.2.180
```

Einen Namensdienstschalter erstellen

Die Funktion zum Umschalten des Namensdienstes ermöglicht die Verwendung von LDAP oder NIS als alternative Namensdienstquellen. Mit dem `vserver services name-service ns-switch modify` Befehl kann die Reihenfolge der Namensdienstquellen festgelegt werden.

Bevor Sie beginnen

- Der Zugriff auf LDAP- und NIS-Server muss konfiguriert sein.
- Um diese Aufgabe auszuführen, ist die Rolle als Cluster-Administrator oder SVM-Administrator erforderlich.

Schritt

1. Die Suchreihenfolge für Namensdienstquellen angeben:

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

   Weitere Informationen zu `vserver services name-service ns-switch modify` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl legt die Suchreihenfolge der Name-Service-Quellen LDAP und NIS für die `passwd` Datenbank auf SVM `engData` fest.

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

Ändern eines ONTAP Administratorpassworts

Sie sollten Ihr anfängliches ONTAP Administratorpasswort unmittelbar nach der ersten Anmeldung und anschließend regelmäßig ändern, um die Sicherheit Ihres Clusters zu gewährleisten.

Ab ONTAP 9.20.1 zeigt der System Manager, sofern Ihr Benutzerkonto für Benachrichtigungen zum Passwortablauf konfiguriert ist, 14 Tage vor Ablauf Ihres Passworts eine Warnmeldung an. Die Meldung wird bei jeder Anmeldung aktualisiert und zeigt die verbleibenden Tage an.

Über diese Aufgabe

Das neue Passwort muss folgende Regeln erfüllen:

- Es darf den Benutzernamen nicht enthalten
- Es muss mindestens acht Zeichen lang sein
- Es muss mindestens einen Buchstaben und eine Zahl enthalten
- Es kann nicht dasselbe sein wie die letzten sechs Passwörter

Der `security login role config modify`Befehl kann verwendet werden, um die Passwortregeln für Konten zu ändern, die einer bestimmten Rolle zugeordnet sind.

Bevor Sie beginnen

- Sie müssen Cluster- oder SVM-Administrator sein, um Ihr eigenes Passwort zu ändern.
- Sie müssen Cluster-Administrator sein, um das Passwort eines anderen Administrators zu ändern.

Schritte

Das Ändern Ihres Passworts ist über System Manager oder die ONTAP Befehlszeilenschnittstelle (CLI) möglich.

System Manager

1. Im System Manager **Cluster > Einstellungen** auswählen.
2. Unter **Benutzer und Rollen** können Sie **Benutzer** auswählen.
3. Es ist ⋮ neben dem Benutzerkonto auszuwählen, für das das Passwort geändert werden muss, und anschließend **Change password**.
4. Neues Passwort eingeben.
5. Zur Bestätigung wird das neue Passwort erneut eingegeben und anschließend **Speichern** ausgewählt.

CLI

Wenn Sie SVM-Administrator sind, können Sie den `security login password` Befehl verwenden, um Ihr eigenes Passwort zu ändern. Wenn Sie Cluster-Administrator sind, können Sie den `security login password` Befehl verwenden, um das Passwort eines beliebigen Administrators zu ändern.

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

   Der folgende Befehl ändert das Kennwort des Administrators `admin1` für die SVM

`vs1.example.com`. Danach geben Sie das aktuelle Kennwort sowie das neue Kennwort zur Bestätigung zweimal ein.

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

Verwandte Informationen

- "security login role config modify"
- "security login password"

Konfiguration von ONTAP Benachrichtigungen zum Ablauf von ONTAP Benutzerpasswörtern in System Manager

Ab ONTAP 9.20.1 erhält der Benutzer, wenn die einem Benutzerkonto zugeordnete Rolle für Benachrichtigungen zum Passwortablauf konfiguriert ist, direkt nach der Anmeldung in System Manager eine Banner-Benachrichtigung oben auf der Seite, beginnend 14 Tage vor dem Ablauf des Passworts. Die Benachrichtigung wird bei jeder Anmeldung aktualisiert und zeigt die Anzahl der verbleibenden Tage bis zum Ablauf des Passworts an. Sie können Benachrichtigungen zum Passwortablauf beim Hinzufügen oder Bearbeiten einer Administratorrolle konfigurieren.

Schritte

1. **Cluster > Einstellungen** auswählen.
2. Neben **Benutzer und Rollen** → auswählen.
3. Die Benachrichtigungen zum Ablauf von Passwörtern werden beim Hinzufügen oder Bearbeiten einer Benutzerrolle konfiguriert.
   - Für die Konfiguration beim Hinzufügen einer Benutzerrolle ist unter **Rollen** + Add auszuwählen. Anschließend folgen die Eingabe eines Namens für die Rolle sowie die Auswahl der Gültigkeitsdauer des Passworts und einer Benachrichtigung zum Passwortablauf.
   - Bei der Bearbeitung einer Benutzerrolle erfolgt die Konfiguration unter **Rollen** durch Auswahl der Benutzerrolle. Anschließend erfolgt unter **Bearbeiten** die Auswahl des Gültigkeitszeitraums des Passworts.
   - Wählen Sie **Add**.

Ergebnis

Der Benutzer erhält im System Manager direkt nach der Anmeldung ein Banner mit einer Warnmeldung am oberen Seitenrand, beginnend mit der ausgewählten Anzahl von Tagen vor dem Ablauf des Passworts. Die Benachrichtigung wird bei jeder Anmeldung aktualisiert und zeigt die verbleibenden Tage bis zum Ablauf des Passworts an.

Sperren und Entsperren eines ONTAP Administratorkontos

Sie können den `security login lock`-Befehl verwenden, um ein Administratorkonto zu sperren, und den `security login unlock`-Befehl, um das Konto zu entsperren.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgaben ausführen zu können.

Schritte

1. Administratorkonto sperren:

   `security login lock -vserver SVM_name -username user_name`

   Der folgende Befehl sperrt das Administratorkonto `admin1` für die SVM `vs1.example.com`:

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

   Weitere Informationen zu `security login lock` finden sich in der "ONTAP-Befehlsreferenz".

2. Entsperren eines Administratorkontos:

   `security login unlock -vserver SVM_name -username user_name`

   Der folgende Befehl entsperrt das Administratorkonto `admin1` für die SVM `vs1.example.com`:

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

   Weitere Informationen zu `security login unlock` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Security Login"

Fehlgeschlagene Anmeldeversuche in ONTAP verwalten

Wiederholte fehlgeschlagene Anmeldeversuche können darauf hindeuten, dass ein Eindringling versucht, auf das Speichersystem zuzugreifen. Es stehen verschiedene Maßnahmen zur Verfügung, um sicherzustellen, dass kein unbefugter Zugriff erfolgt.

Woran Sie erkennen, dass Anmeldeversuche fehlgeschlagen sind

Das Ereignismanagementsystem (EMS) benachrichtigt Sie stündlich über fehlgeschlagene Anmeldeversuche. Ein Protokoll der fehlgeschlagenen Anmeldeversuche befindet sich in der `audit.log` Datei.

Was zu tun ist, wenn wiederholte Anmeldeversuche fehlschlagen

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

- Es wird verlangt, dass Passwörter aus einer Mindestanzahl von Großbuchstaben, Kleinbuchstaben,

Sonderzeichen und/oder Ziffern bestehen.

- Nach einem fehlgeschlagenen Anmeldeversuch eine Verzögerung anwenden
- Die Anzahl zulässiger fehlgeschlagener Anmeldeversuche ist begrenzt, und Benutzer werden nach der festgelegten Anzahl fehlgeschlagener Versuche gesperrt.
- Konten, die für eine bestimmte Anzahl von Tagen inaktiv sind, verlieren ihre Gültigkeit und werden gesperrt.

Sie können den `security login role config modify` Befehl verwenden, um diese Aufgaben auszuführen. Weitere Informationen zu `security login role config modify` finden sich in der "ONTAP-Befehlsreferenz".

Langfristig sind folgende zusätzliche Schritte möglich:

- Mit dem `security ssh modify` Befehl lässt sich die Anzahl fehlgeschlagener Anmeldeversuche für alle neu erstellten SVMs begrenzen. Weitere Informationen zu `security ssh modify` finden sich in der "ONTAP-Befehlsreferenz".
- Bestehende MD5-Algorithmus-Konten werden auf den sichereren SHA-512 Algorithmus migriert, indem von den Benutzern verlangt wird, ihre Passwörter zu ändern.

SHA-2 für Passwörter von ONTAP Administratorenkonten erzwingen

Administratorkonten, die vor ONTAP 9.0 erstellt wurden, verwenden nach dem Upgrade weiterhin MD5-Passwörter, bis die Passwörter manuell geändert werden. MD5 ist weniger sicher als SHA-2. Nach dem Upgrade empfiehlt es sich, die Benutzer von MD5-Konten darauf hinzuweisen, ihre Passwörter zu ändern, damit die standardmäßige SHA-512-Hashfunktion verwendet wird.

Über diese Aufgabe

Die Passwort-Hash-Funktion ermöglicht Folgendes:

- Benutzerkonten, die der angegebenen Hash-Funktion entsprechen, werden angezeigt.
- Konten, die eine bestimmte Hash-Funktion verwenden (z. B. MD5), laufen ab, wodurch die Benutzer gezwungen werden, bei ihrem nächsten Login ihr Passwort zu ändern.
- Konten, deren Passwörter die angegebene Hash-Funktion verwenden, werden gesperrt.
- Beim Zurücksetzen auf eine Version vor ONTAP 9 ist das eigene Passwort des Cluster-Administrators zurückzusetzen, damit es mit der von der früheren Version unterstützten Hash-Funktion (MD5) kompatibel ist.

ONTAP akzeptiert vorab gehashte SHA-2-Passwörter nur über das NetApp Manageability SDK (`security-login-create` und `security-login-modify-password`.

Schritte

1. Die MD5-Administratorkonten auf die SHA-512-Passwort-Hash-Funktion migrieren:
   a. Alle MD5-Administratorkonten ablaufen lassen: `security login expire-password -vserver * -username * -hash-function md5`

      Dadurch müssen MD5-Kontobenutzer ihr Passwort beim nächsten Login ändern.

b. Benutzer von MD5-Konten sollten sich über eine Konsole oder eine SSH-Sitzung anmelden.

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

2. Für MD5-Konten, deren Benutzer sich nicht innerhalb eines bestimmten Zeitraums anmelden, um ihr Passwort zu ändern, wird die Kontomigration erzwungen:

   a. Konten sperren, die weiterhin die MD5-Hashfunktion verwenden (erweiterte Berechtigungsstufe): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

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

   b. Die Konten werden entsperrt, wenn die Benutzer bereit sind, ihre Passwörter zu ändern: `security login unlock -vserver` *`svm_name`* `-username` *`user_name`*

   c. Benutzer melden sich über eine Konsole oder eine SSH-Sitzung bei ihren Konten an und ändern ihre Passwörter, wenn das System sie dazu auffordert.

Verwandte Informationen

- "security login expire-password"
- "security login unlock"

Diagnose und Behebung von ONTAP Dateizugriffsproblemen mit System Manager

Ab ONTAP 9.8 lassen sich Bedenken beim Dateizugriff nachverfolgen und anzeigen.

Schritte

1. Im System Manager unter **Storage > Storage-VMs** auswählen.
2. Die Storage-VM auswählen, auf der eine Ablaufverfolgung durchgeführt werden soll.
3. Klicken Sie auf **Mehr**.
4. **Dateizugriff nachverfolgen** auswählen.
5. Den Benutzernamen und die Client-IP-Adresse angeben, anschließend auf **Start Tracing** klicken.

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

6. In der linken Spalte der Ergebnistabelle auf klicken, um die Dateizugriffsberechtigungen anzuzeigen.

Multi-Admin-Verifizierung verwalten

Informationen zur ONTAP Multi-Admin-Verifizierung

Ab ONTAP 9.11.1 kann die Multi-Admin-Verifizierung (MAV) verwendet werden, um sicherzustellen, dass bestimmte Vorgänge, wie das Löschen von Volumes oder Snapshots, nur nach Genehmigung durch autorisierte Administratoren ausgeführt werden können. Dadurch wird verhindert, dass kompromittierte, böswillige oder unerfahrene Administratoren unerwünschte Änderungen vornehmen oder Daten löschen.

Die Konfiguration der Multi-Admin-Verifizierung umfasst Folgendes:

- "Erstellung einer oder mehrerer Administrator-Genehmigungsgruppen."
- "Aktivierung der Multi-Admin-Verifizierungsfunktion."
- "Hinzufügen oder Ändern von Regeln."

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

Wenn die Multi-Admin-Verifizierung aktiviert ist, sind für den Abschluss jeder geschützten Operation diese Schritte erforderlich:

1. Wenn ein Benutzer den Vorgang initiiert, "Eine Anfrage wird generiert."
2. Bevor die Operation ausgeführt werden kann, muss mindestens eine "Der MAV-Administrator muss zustimmen."
3. Nach der Genehmigung erhält der Benutzer eine Aufforderung und schließt den Vorgang ab.

> Falls Sie die Multi-Admin-Verifizierungsfunktion ohne Zustimmung des MAV-Administrators deaktivieren müssen, wenden Sie sich an den NetApp Support und geben Sie Folgendes an "NetApp Knowledge Base: Wie die Multi-Admin-Verifizierung deaktiviert werden kann, wenn der MAV-Administrator nicht verfügbar ist".

Die Multi-Admin-Verifizierung ist nicht für Volumes oder Workflows mit hohem Automatisierungsgrad vorgesehen, da jede automatisierte Aufgabe vor Abschluss genehmigt werden müsste. Wenn Automatisierung und MAV gemeinsam eingesetzt werden sollen, wird empfohlen, Abfragen für spezifische MAV-Operationen zu verwenden. Beispielsweise könnten `volume delete` MAV-Regeln nur auf Volumes angewendet werden, bei denen keine Automatisierung erfolgt, und diese Volumes könnten mit einem bestimmten Namensschema gekennzeichnet werden.

> Die Multi-Admin-Verifizierung ist bei Cloud Volumes ONTAP nicht verfügbar.

Funktionsweise der Multi-Admin-Verifizierung

Die Multi-Admin-Verifizierung umfasst:

- Eine Gruppe von einem oder mehreren Administratoren mit Genehmigungs- und Vetorechten.
- Eine Reihe geschützter Operationen oder Befehle in einer *Regeltabelle*.
- Eine *Regel-Engine* zur Identifizierung und Steuerung der Ausführung geschützter Operationen.

> Genehmigungsgruppen unterstützen stets einzelne Administratoren. Ab ONTAP 9.20.1 können Genehmigungsgruppen auch Gruppen von Identitätsanbietern (IdP), Active Directory (AD) oder LDAP (nsswitch) umfassen. Unterstützte Gruppentypen sind Entra ID, ADFS, AD-Domänengruppen und LDAP-Gruppen. Änderungen an der Gruppenmitgliedschaft eines Benutzers im Identitätsanbieter werden beim nächsten erfolgreichen Login des Benutzers wirksam. Eine MAV Neukonfiguration ist nicht erforderlich.

MAV-Regeln werden nach rollenbasierter Zugriffssteuerung (RBAC) ausgewertet. Daher müssen Administratoren, die geschützte Operationen ausführen oder genehmigen, bereits über die minimalen RBAC-Berechtigungen für diese Operationen verfügen. "Weitere Informationen zu RBAC".

Systemdefinierte Regeln

Wenn die Multi-Admin-Verifizierung (auch als *guard-rail*-Regeln bekannt) aktiviert ist, legen systemdefinierte Regeln eine Reihe von MAV-Operationen fest, um das Risiko einer Umgehung des MAV-Prozesses selbst zu begrenzen. Diese Operationen können nicht aus der Regeltabelle entfernt werden. Sobald MAV aktiviert ist, erfordern mit einem Sternchen (*) gekennzeichnete Operationen vor der Ausführung die Genehmigung durch einen oder mehrere Administratoren, mit Ausnahme von **show**-Befehlen.

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

  Steuert die Konfiguration der Multi-Admin-Verifizierungsfunktionalität.

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

  Die Mitgliedschaft im Administratorenkreis mit Multi-Admin-Verifizierungsberechtigungen wird kontrolliert.

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

  Die Befehlsgruppe, die eine Überprüfung durch mehrere Administratoren erfordert, kann gesteuert werden.

- `security multi-admin-verify request`Operationen

  Den Genehmigungsprozess kontrollieren.

Regelgeschützte Befehle

Zusätzlich zu den systemdefinierten Operationen sind die folgenden Befehle standardmäßig geschützt, wenn die Multi-Admin-Verifizierung aktiviert ist, aber die Regeln können geändert werden, um den Schutz für diese Befehle aufzuheben:

- "security login password"
- "security login unlock"
- "Set"

Jede ONTAP Version bietet mehr Befehle, die mit Multi-Admin-Verifizierungsregeln geschützt werden können. Für die vollständige Liste der zum Schutz verfügbaren Befehle ist die jeweilige ONTAP Version auszuwählen.

9.19.1

- `cluster date modify`[3]
- `cluster log-forwarding create`[3]
- `cluster log-forwarding delete`[3]
- `cluster log-forwarding modify`[3]
- `cluster peer delete`
- `cluster time-service ntp server create`[3]
- `cluster time-service ntp server delete`[3]
- `cluster time-service ntp key create`[3]
- `cluster time-service ntp key delete`[3]

- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- placement rebalance performance config modify [7]
- qos adaptive-policy-group create [7]
- qos adaptive-policy-group modify [7]
- qos adaptive-policy-group delete [7]
- qos adaptive-policy-group rename [7]
- qos policy-group create [7]
- qos policy-group modify [7]
- qos policy-group delete [7]
- qos policy-group rename [7]
- qos settings cache modify [7]
- qos settings cluster-options modify [7]
- qos settings nested-qos-svm-vol [7]
- qos settings read-ahead create [7]
- qos settings read-ahead modify [7]
- qos settings read-ahead delete [7]
- qos settings throughput-floors-v2 [7]
- qos workload modify [7]
- qos workload delete [7]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware volume safe-extension-list add [6]
- security anti-ransomware volume safe-extension-list remove [6]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security dynamic-authorization modify [7]
- security ipsec config modify [3]
- security ipsec policy create [3]

- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login password [6]
- security login publickey create
- security login publickey delete
- security login publickey modify
- security login unlock [6]
- security multi-admin-verify modify [6]
- security multi-admin-verify approval-group create [6]
- security multi-admin-verify approval-group delete [6]
- security multi-admin-verify approval-group modify [6]
- security multi-admin-verify approval-group replace [6]
- security multi-admin-verify rule create [6]
- security multi-admin-verify rule delete [6]
- security multi-admin-verify rule modify [6]
- security key-manager external gcp disable [7]
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security us-eo-cybersecurity modify [6]
- security webauthn credentials delete [4]
- set [6]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]

- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume modify [3]
- volume rename [5]
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume file retention set [6]
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]

- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot rename [6]
- volume snapshot restore [6]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver consistency-group snapshot rename [7]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]

- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.18.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware volume safe-extension-list add [6]
- security anti-ransomware volume safe-extension-list remove [6]

- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login password [6]
- security login publickey create
- security login publickey delete
- security login publickey modify
- security login unlock [6]
- security multi-admin-verify modify [6]
- security multi-admin-verify approval-group create [6]
- security multi-admin-verify approval-group delete [6]
- security multi-admin-verify approval-group modify [6]
- security multi-admin-verify approval-group replace [6]
- security multi-admin-verify rule create [6]
- security multi-admin-verify rule delete [6]
- security multi-admin-verify rule modify [6]
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security us-eo-cybersecurity modify [6]
- security webauthn credentials delete [4]
- set [6]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]

- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume modify [3]
- volume rename [5]
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume file retention set [6]
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]

- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot rename [6]
- volume snapshot restore [6]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]

- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.17.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]

- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]

- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume rename [5]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore

- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.16.1

- `cluster date modify` [3]
- `cluster log-forwarding create` [3]
- `cluster log-forwarding delete` [3]
- `cluster log-forwarding modify` [3]
- `cluster peer delete`
- `cluster time-service ntp server create` [3]
- `cluster time-service ntp server delete` [3]
- `cluster time-service ntp key create` [3]
- `cluster time-service ntp key delete` [3]
- `cluster time-service ntp key modify` [3]
- `cluster time-service ntp server modify` [3]
- `event config modify`
- `event config set-mail-server-password` [3]
- `lun delete` [3]
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` [2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` [2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` [3]
- `security saml-sp create` [3]
- `security saml-sp delete` [3]

- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]

- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]

- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.15.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]

- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` [2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` [2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` [3]
- `security saml-sp create` [3]
- `security saml-sp delete` [3]
- `security saml-sp modify` [3]
- `snaplock legal-hold end` [3]
- `storage aggregate delete` [3]
- `storage encryption disk destroy` [3]
- `storage encryption disk modify` [3]
- `storage encryption disk revert-to-original-state` [3]
- `storage encryption disk sanitize` [3]
- `system bridge run-cli` [3]
- `system controller flash-cache secure-erase run` [3]
- `system controller service-event delete` [3]
- `system health alert delete` [3]
- `system health alert modify` [3]
- `system health policy definition modify` [3]
- `system node autosupport modify` [3]
- `system node autosupport trigger modify` [3]
- `system node coredump delete` [3]

- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]

- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security login create
- security login delete

- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create [2]
- vserver modify [2]
- vserver peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume pause [1]
- security login create
- security login delete
- security login modify

- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

9.12.1/9.11.1

- cluster peer delete
- event config modify
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snapshot autodelete modify
- volume snapshot delete

- `volume snapshot policy add-schedule`
- `volume snapshot policy create`
- `volume snapshot policy delete` *
- `volume snapshot policy modify`
- `volume snapshot policy modify-schedule`
- `volume snapshot policy remove-schedule`
- `volume snapshot restore`
- `vserver peer delete`

1. Neuer regelgeschützter Befehl für 9.13.1
2. Neuer regelgeschützter Befehl für 9.14.1
3. Neuer regelgeschützter Befehl für 9.15.1
4. Neuer regelgeschützter Befehl für 9.16.1
5. Neuer regelgeschützter Befehl für 9.17.1
6. Neuer regelgeschützter Befehl für 9.18.1
7. Neuer regelgeschützter Befehl für 9.19.1

*Dieser Befehl ist nur über die CLI verfügbar und ist in einigen Versionen von System Manager nicht verfügbar.

Funktionsweise der Genehmigung durch mehrere Administratoren

Jedes Mal, wenn eine geschützte Operation auf einem MAV-geschützten Cluster eingeleitet wird, wird eine Ausführungsanforderung für die Operation an die zuständige MAV-Administratorengruppe gesendet.

Sie können Folgendes konfigurieren:

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

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

- Die Anzahl der MAV Administratorgruppen.
  - Für jede geschützte Betriebsregel ist eine MAV Gruppe zugewiesen.
  - Für mehrere MAV-Gruppen lässt sich festlegen, welche MAV-Gruppe eine bestimmte Regel genehmigt.
- Die Anzahl der MAV-Genehmigungen, die zur Durchführung eines geschützten Vorgangs erforderlich sind.
- Eine *Genehmigungsablauffrist*, innerhalb derer ein MAV-Administrator auf eine Genehmigungsanfrage reagieren muss.
- Ein Ablaufzeitraum für die Ausführung, innerhalb dessen der anfragende Administrator den Vorgang abschließen muss.

Sobald diese Parameter konfiguriert sind, ist für deren Änderung die Genehmigung durch MAV erforderlich.

MAV-Administratoren können ihre eigenen Anfragen zur Ausführung geschützter Operationen nicht genehmigen. Daher:

- MAV sollte auf Clustern mit nur einem Administrator nicht aktiviert werden.
- Wenn es in der MAV-Gruppe nur eine Person gibt, kann dieser MAV-Administrator keine geschützten Operationen initiieren; reguläre Administratoren müssen geschützte Operationen initiieren, und der MAV-Administrator kann nur genehmigen.
- Wenn MAV-Administratoren geschützte Vorgänge ausführen können sollen, ist entweder eine Genehmigungsgruppe mit mindestens einem benannten Genehmiger mehr als der Anzahl der erforderlichen Genehmigungen oder eine Genehmigungsgruppe zu konfigurieren, die Identity Provider (IdP)-, AD- oder LDAP-Gruppen umfasst. Mitglieder konfigurierter IdP-, AD- oder LDAP-Gruppen können Anfragen genehmigen, ohne einzeln als benannte Genehmiger aufgeführt zu sein. In beiden Fällen müssen neben dem anfragenden Administrator genügend berechtigte Genehmiger verfügbar sein, um die erforderlichen Genehmigungen zu erteilen.

MAV-Administratoren können Genehmigungsanfragen in E-Mail-Benachrichtigungen (über EMS) erhalten oder die Anfragewarteschlange abfragen. Wenn sie eine Anfrage erhalten, stehen ihnen drei Aktionen zur Auswahl:

- 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.
- Eine Anfrage wird genehmigt oder abgelehnt.
- Ein genehmigter Antrag wird ausgeführt.

Wenn der Antragsteller zur selben Genehmigungsgruppe für den Vorgang gehört, erhält er eine E-Mail, wenn sein Antrag genehmigt wurde.

> Ein Antragsteller kann seine eigenen Anträge nicht genehmigen, selbst wenn er Mitglied der Genehmigungsgruppe ist (obwohl er E-Mail-Benachrichtigungen für seine eigenen Anträge erhalten kann). Antragsteller, die keiner Genehmigungsgruppe angehören (das heißt, die keine MAV-Administratoren sind), erhalten keine E-Mail-Benachrichtigungen.

Wie die Ausführung geschützter Operationen funktioniert

Wird die Ausführung einer geschützten Operation genehmigt, setzt der anfragende Benutzer die Operation nach Aufforderung fort. Wird die Operation abgelehnt, muss der anfragende Benutzer die Anfrage löschen, bevor er fortfahren kann.

MAV-Regeln werden nach den RBAC-Berechtigungen ausgewertet. Daher kann ein Benutzer ohne ausreichende RBAC-Berechtigungen für die Ausführung einer Operation den MAV-Anforderungsprozess nicht initiieren.

MAV-Regeln werden vor der Ausführung des geschützten Vorgangs ausgewertet. Das bedeutet, dass die Regeln auf Basis des aktuellen Systemzustands angewendet werden. Wenn beispielsweise eine MAV-Regel für `volume modify` mit einer Abfrage von `-size 5GB` erstellt wird, erfordert die Verwendung von `volume modify` zur Größenänderung eines 5GB-Volumes auf 2GB eine MAV-Genehmigung, während die Größenänderung eines 2GB-Volumes auf 5GB keine Genehmigung erfordert.

Verwandte Informationen

- "Cluster"
- "LUN"
- "Sicherheit"
- "snaplock Legal-Hold Ende"
- "Speicheraggregat"
- "Speicherverschlüsselung"
- "System"

ONTAP Administrator-Genehmigungsgruppen für MAV verwalten

Bevor die Multi-Admin-Verifizierung (MAV) aktiviert wird, ist eine Administrator-Genehmigungsgruppe zu erstellen, die mindestens einen Administrator mit Genehmigungs- oder Vetorecht enthält. Nach der Aktivierung der Multi-Admin-Verifizierung erfordern Änderungen an der Mitgliedschaft der Genehmigungsgruppe die Zustimmung eines der bestehenden berechtigten Administratoren.

Über diese Aufgabe

Sie können bestehende Administratoren zu einer MAV Gruppe hinzufügen oder neue Administratoren erstellen.

Die MAV-Funktionalität berücksichtigt bestehende Einstellungen der rollenbasierten Zugriffssteuerung (RBAC). Potenzielle MAV-Administratoren müssen über ausreichende Berechtigungen zum Ausführen geschützter Operationen verfügen, bevor sie zu MAV-Administratorgruppen hinzugefügt werden. "Weitere Informationen zu RBAC."

Sie können MAV so konfigurieren, dass MAV-Administratoren über ausstehende Genehmigungsanfragen benachrichtigt werden. Hierfür ist die Konfiguration von E-Mail-Benachrichtigungen erforderlich, insbesondere der `Mail From` und `Mail Server` Parameter, oder diese Parameter können gelöscht werden, um die Benachrichtigung zu deaktivieren. Ohne E-Mail-Benachrichtigungen müssen MAV-Administratoren die Genehmigungswarteschlange manuell prüfen.

Ab ONTAP 9.15.1 ist es möglich, Active Directory (AD)-Benutzer als MAV-Administratoren zu konfigurieren. Der AD-Benutzer muss "Als ONTAP Administrator konfiguriert" sein.

Ab ONTAP 9.20.1 können Genehmigungsgruppen auch Identity Provider (IdP)-, Active Directory (AD)- oder LDAP (nsswitch)-Gruuppen umfassen. Zu den unterstützten Gruppentypen gehören Entra ID (ehemals Azure AD), ADFS, AD-Domänengruppen und LDAP-Gruppen.

Änderungen an der Gruppenzugehörigkeit eines Benutzers beim Identitätsanbieter werden bei der nächsten erfolgreichen Anmeldung des Benutzers wirksam. Eine Neukonfiguration von MAV ist nicht erforderlich.

> Bevor Sie eine IdP-, Active Directory- oder LDAP-Gruppe zu einer MAV-Genehmigungsgruppe hinzufügen können, muss die Gruppe bereits über einen konfigurierten Anmeldezugriff verfügen und in der `security login group`Tabelle mit einer Rollenzuordnung registriert sein. Die entsprechenden Verfahren sind nachfolgend aufgeführt.

System Manager Verfahren

Wenn zum ersten Mal eine MAV-Genehmigungsgruppe erstellt werden soll, bietet die System Manager Vorgehensweise weitere Informationen zu "Multi-Admin-Verifizierung aktivieren."

Eine bestehende Genehmigungsgruppe kann geändert oder eine zusätzliche Genehmigungsgruppe erstellt werden:

1. Administratoren für den Erhalt der Multi-Admin-Verifizierung festlegen.
   a. **Cluster > Einstellungen** auswählen.
   b. Die Auswahl von → erfolgt neben **Benutzer, Gruppen und Rollen.**
   c. Unter **Users** erfolgt die Auswahl von + Add .
   d. Die Liste kann bei Bedarf angepasst werden.

      Weitere Informationen sind unter "Administratorzugriff kontrollieren." verfügbar.

2. Ab ONTAP 9.20.1 ist vor dem Hinzufügen einer IdP-, AD- oder LDAP-Gruppe als MAV-Genehmiger zunächst eine Registrierung der Gruppe erforderlich, damit in der MAV-Konfiguration auf sie verwiesen werden kann.
   a. Unter **Gruppen** erfolgt das Hinzufügen einer Gruppe über + Add .

      Eingabe des Gruppennamens. Das UUID-Feld ist nur für Microsoft Entra-Gruppen erforderlich; andere Identitätsanbieter verwenden den Gruppennamen.

   b. Unter **Gruppe-Rollen-Zuordnung** erfolgt die Auswahl von + Add und der Gruppe sowie die Zuweisung einer Rolle mit ausreichenden Berechtigungen zur Genehmigung von MAV-Anfragen.
3. MAV-Genehmigungsgruppe erstellen oder ändern:
   a. **Cluster > Einstellungen** auswählen.
   b. Wählen Sie → neben **Genehmigung durch mehrere Administratoren** im Abschnitt **Sicherheit** aus. (Das ⚙-Symbol wird angezeigt, wenn MAV noch nicht konfiguriert ist.)
      - Name: Einen Gruppennamen eingeben.
      - Genehmiger (Benutzer): Auswahl einzelner Genehmiger aus einer Benutzerliste.
      - Genehmiger (Gruppen): Ab ONTAP 9.20.1 können Sie optional eine oder mehrere registrierte IdP-, Active Directory- oder LDAP-Gruppen auswählen.
      - E-Mail-Adresse: E-Mail-Adresse(n) eingeben.
      - Standardgruppe: eine Gruppe auswählen.

Für die Bearbeitung einer bestehenden Konfiguration ist nach der Aktivierung von MAV eine MAV-Genehmigung erforderlich.

CLI Prozedur

1. Überprüfen Sie, ob für die `Mail From` und `Mail Server` Parameter Werte festgelegt wurden. Folgendes eingeben:

   ```
   event config show
   ```

   Die Anzeige sollte in etwa wie folgt aussehen:

   ```
   cluster01::> event config show
                              Mail From:  admin@localhost
                            Mail Server:  localhost
   ```

```
                            Proxy URL:  -
                           Proxy User:  -
 Publish/Subscribe Messaging Enabled:  true
```

Zum Konfigurieren dieser Parameter wird Folgendes eingegeben:

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

Weitere Informationen zu `event config show` und `event config modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Es sind Administratoren zu bestimmen, die an der Multi-Admin-Verifizierung teilnehmen.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben
Aktuelle Administratoren anzeigen	`security login show`
Anmeldeinformationen der aktuellen Administratoren ändern	`security login modify` *<parameters>*
Neue Administratorkonten erstellen	`security login create -user-or-group -name` *admin_name* `-application ssh -authentication-method password`

Weitere Informationen zu `security login show`, `security login modify` und `security login create` in der "ONTAP-Befehlsreferenz".

3. Ab ONTAP 9.20.1 ist beim Hinzufügen einer IdP-, AD- oder LDAP-Gruppe als MAV-Genehmiger zunächst zu prüfen, ob für die Gruppe der Anmeldezugriff konfiguriert ist; anschließend ist sie für MAV zu registrieren.

   Falls für die Gruppe noch kein Anmeldezugriff konfiguriert ist, ist Folgendes einzugeben:

   `security login create -user-or-group-name` *group_name* `-application http|ssh -authentication-method domain|nsswitch|saml|oauth2 -role` *role*

   Anschließend wird die Gruppe registriert, damit in der MAV Konfiguration auf sie verwiesen und sie einer Rolle zugeordnet werden kann:

   `security login group create -vserver` *svm_name* `-name` *group_name* `[-uuid` *uuid*`]`

   `security login group role-mapping create -group-id` *group_id* `-role` *role*

   Der `-uuid` Parameter ist nur für Microsoft Entra ID-Gruppen erforderlich. Active Directory-Domänengruppen, ADFS/SAML-Gruppen und LDAP-(nsswitch)-Gruuppen werden nur anhand des Namens identifiziert.

   Beispiel: Die folgenden Befehle registrieren die Active Directory-Gruppe `mydomain\mav_approvers` für MAV und ordnen sie der `admin` Rolle zu.

```
cluster-1::> security login group create -vserver cluster-1 -name
mydomain\mav_approvers
```

```
cluster-1::> security login group show -vserver cluster-1

     Vserver: cluster-1
  Group Name: mydomain\mav_approvers
    Group ID: 1
  Group UUID: -
     Comment: -

cluster-1::> security login group role-mapping create -group-id 1 -role
admin
```

Weitere Informationen zu `security login group create` und `security login group role-mapping create` finden sich in der "ONTAP-Befehlsreferenz".

4. Die MAV-Genehmigungsgruppe erstellen:

   `security multi-admin-verify approval-group create [ -vserver` *`svm_name`*`] -name` *`group_name`* `[-approvers` *`approver1`*`[,`*`approver2`*`…]] [-groups` *`group1`*`[,`*`group2`*`…]] [[-email` *`address1`*`], `*`address1`*`…]`

   - `-vserver` - Nur die Admin-SVM wird in dieser Version unterstützt.
   - `-name` - Der MAV Gruppenname, maximal 64 Zeichen.
   - `-approvers` - Die Liste eines oder mehrerer einzelner Genehmiger. Für AD-Benutzer gilt das Format `domain\user`. Beispielsweise `mydomain\pavan`.
   - `-groups` - Die Liste einer oder mehrerer IdP-, AD- oder LDAP-Gruppen, die in die Genehmigungsgruppe aufgenommen werden sollen. Jede Gruppe muss bereits in der `security login group`Tabelle mit einer Rollenzuordnung registriert sein.
   - `-email` - Eine oder mehrere E-Mail-Adressen, die benachrichtigt werden, wenn eine Anfrage erstellt, genehmigt, abgelehnt oder ausgeführt wird.

     Beispiel: Der folgende Befehl erstellt eine MAV-Gruppe mit zwei einzelnen Genehmigern und einer Entra ID Gruppe.

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

5. Gruppenerstellung und Mitgliedschaft überprüfen:

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

   Beispiel:

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name        Approvers        Approver Groups
Email
```

```
-------  --------------- -----------------
------------------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      entra-group-mav-approvers
pavan@myfirm.com,julia@myfirm.com
```

Diese Befehle dienen zur Änderung der ursprünglichen MAV Gruppenkonfiguration.

Hinweis: Alle erfordern die Genehmigung durch den MAV-Administrator, bevor sie ausgeführt werden.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben
Gruppenmerkmale oder vorhandene Mitgliederinformationen ändern	`security multi-admin-verify approval-group modify [-vserver svm_name] -name group_name [-approvers approver1 [,approver2…]] [-groups group1[, group2…]] [[-email address1], address1… ]`
Mitglieder hinzufügen oder entfernen	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]] [-groups-to-add group1[,group2…]][-groups-to-remove group1[,group2…]]`
Gruppe löschen	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Multi-Admin-Verifizierung in ONTAP aktivieren oder deaktivieren

Multi-Admin-Verifizierung (MAV) muss explizit aktiviert werden. Nach der Aktivierung der Multi-Admin-Verifizierung ist die Genehmigung durch Administratoren einer MAV-Genehmigungsgruppe (MAV-Administratoren) erforderlich, um sie zu löschen.

Über diese Aufgabe

Sobald MAV aktiviert ist, erfordert die Änderung oder Deaktivierung von MAV die Genehmigung des MAV-Administrators.

> Falls Sie die Multi-Admin-Verifizierungsfunktion ohne Zustimmung des MAV-Administrators deaktivieren müssen, wenden Sie sich an den NetApp Support und geben Sie Folgendes an "NetApp Knowledge Base: Wie die Multi-Admin-Verifizierung deaktiviert werden kann, wenn der MAV-Administrator nicht verfügbar ist".

Wenn MAV aktiviert ist, können die folgenden Parameter global festgelegt werden.

Genehmigungsgruppen

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

Wenn MAV mit Autonomous Ransomware Protection verwendet wird, sollte eine neue oder bestehende Genehmigungsgruppe definiert werden, die für die Genehmigung von Anfragen zum Pausieren, Deaktivieren und Löschen von verdächtigem Ransomware-Schutz zuständig ist.

Erforderliche Genehmiger

Die Anzahl der Genehmiger, die zur Ausführung einer geschützten Operation erforderlich ist. Die Standard- und Mindestanzahl beträgt 1.

Die erforderliche Anzahl an Genehmigern muss kleiner sein als die Gesamtzahl der eindeutigen Genehmiger in den Standard Genehmigungsgruppen.

Ablauf der Genehmigung (Stunden, Minuten, Sekunden)

Die Frist, innerhalb derer ein MAV-Administrator auf eine Genehmigungsanfrage reagieren muss. Der Standardwert beträgt eine Stunde (1h), der minimale unterstützte Wert ist eine Sekunde (1s), und der maximal unterstützte Wert ist 14 Tage (14d).

Ablauf der Ausführung (Stunden, Minuten, Sekunden)

Der Zeitraum, innerhalb dessen der anfragende Administrator die Operation abschließen muss. Der Standardwert beträgt eine Stunde (1h), der minimale unterstützte Wert ist eine Sekunde (1s), und der maximal unterstützte Wert ist 14 Tage (14d).

Sie können auch jeden dieser Parameter für bestimmte "Betriebsregeln." überschreiben.

System Manager Verfahren

1. Administratoren für den Erhalt der Multi-Admin-Verifizierung festlegen.
   a. **Cluster > Einstellungen** auswählen.
   b. Die Auswahl von → erfolgt neben **Benutzer, Gruppen und Rollen.**
   c. Unter **Users** erfolgt die Auswahl von + Add .
   d. Die Liste kann bei Bedarf angepasst werden.

   Weitere Informationen sind unter "Administratorzugriff kontrollieren." verfügbar.

2. Ab ONTAP 9.20.1 müssen Sie, wenn Sie eine IdP-, AD- oder LDAP-Gruppe als MAV-Genehmiger verwenden möchten, die Gruppe registrieren und einer Rolle zuordnen:
   a. Unter **Gruppen** erfolgt das Hinzufügen einer Gruppe über + Add . Das UUID-Feld ist nur für Microsoft Entra Gruppen erforderlich; andere Identitätsanbieter verwenden den Gruppennamen.
   b. Unter **Gruppe-Rollen-Zuordnung** erfolgt die Auswahl von + Add und der Gruppe sowie die Zuweisung einer Rolle mit ausreichenden Berechtigungen zur Genehmigung von MAV-Anfragen.
3. Die Multi-Admin-Verifizierung wird aktiviert, indem mindestens eine Genehmigungsgruppe erstellt und mindestens eine Regel hinzugefügt wird.
   a. **Cluster > Einstellungen** auswählen.
   b. Wählen Sie ⚙ neben **Genehmigung durch mehrere Administratoren** im Abschnitt **Sicherheit** aus.
   c. Über + Add lässt sich mindestens eine Genehmigungsgruppe hinzufügen.

- Name – Ein Gruppenname wird eingegeben.
- Genehmiger (Benutzer): Auswahl von Genehmigern aus einer Liste von Benutzern.
- Genehmiger (Gruppen) – Ab ONTAP 9.20.1 ist optional die Auswahl einer oder mehrerer registrierter IdP-, AD- oder LDAP-Gruppen möglich.
- E-Mail-Adresse – E-Mail-Adresse(n) eingeben.
- Standardgruppe – Eine Gruppe auswählen.

d. Fügen Sie mindestens eine Regel hinzu.
   - Betrieb – Ein unterstützter Befehl aus der Liste kann ausgewählt werden.
   - Abfrage – Beliebige gewünschte Befehlsoptionen und Werte eingeben.
   - Optionale Parameter; leer lassen, um die globalen Einstellungen anzuwenden, oder einen anderen Wert für spezifische Regeln zuweisen, um die globalen Einstellungen zu überschreiben.
     - Erforderliche Anzahl an Genehmigern
     - Genehmigungsgruppen
e. Mit **Erweiterte Einstellungen** können die Standardeinstellungen angezeigt oder geändert werden.
   - Erforderliche Anzahl an Genehmigern (Standard: 1)
   - Ablauf der Ausführungsanforderung (Standard: 1 Stunde)
   - Ablauf der Genehmigungsanfrage (Standard: 1 Stunde)
   - Mailserver*
   - Von E-Mail-Adresse*

   *Diese Einstellungen aktualisieren die E-Mail-Einstellungen, die unter „Benachrichtigungsverwaltung“ verwaltet werden. Eine Aufforderung zur Festlegung erfolgt, falls sie noch nicht konfiguriert wurden.

f. Zum Abschließen der MAV Erstkonfiguration ist **Aktivieren** auszuwählen.

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 bestehende Konfiguration anzeigen, indem Sie → auswählen. Zum Bearbeiten einer bestehenden Konfiguration ist eine MAV Genehmigung erforderlich.

Deaktivieren der Multi-Admin-Verifizierung:

1. **Cluster > Einstellungen** auswählen.
2. Wählen Sie ⚙ neben **Genehmigung durch mehrere Administratoren** im Abschnitt **Sicherheit** aus.
3. Es ist die Umschaltfläche „Enabled“ auszuwählen.

   Für die Durchführung dieses Vorgangs ist eine MAV-Genehmigung erforderlich.

CLI Prozedur

Bevor die MAV-Funktionalität über die CLI aktiviert werden kann, muss mindestens ein "MAV Administratorgruppe" erstellt worden sein.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben

MAV-Funktionalität aktivieren	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`
	
	Beispiel: Der folgende Befehl aktiviert MAV mit 1 Genehmigungsgruppe, 2 erforderlichen Genehmigern und Standardablaufzeiten.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Die Erstkonfiguration wird abgeschlossen, indem mindestens ein "Betriebsregel." hinzugefügt wird

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

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

MAV-Funktionalität deaktivieren (erfordert MAV-Genehmigung)	`security multi-admin-verify modify -enabled false`

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Multi-Admin-Verifizierungsregeln für geschützte Vorgänge in ONTAP verwalten

Sie erstellen Regeln zur Verifizierung durch mehrere Administratoren (MAV), um Vorgänge zu kennzeichnen, die eine Genehmigung erfordern. Immer wenn ein Vorgang initiiert wird, werden geschützte Vorgänge abgefangen und eine Genehmigungsanfrage erstellt.

Regeln können vor der Aktivierung von MAV von jedem Administrator mit entsprechenden RBAC-Funktionen erstellt werden, aber sobald MAV aktiviert ist, erfordert jede Änderung am Regelsatz die Genehmigung durch MAV.

Pro Operation kann nur eine MAV-Regel erstellt werden; beispielsweise können nicht mehrere `volume-snapshot-delete` Regeln erstellt werden. Alle gewünschten Regelbeschränkungen müssen in einer einzigen Regel enthalten sein.

Sie können Regeln zum Schutz von "diese Befehle" erstellen. Jeder Befehl kann ab der ONTAP Version geschützt werden, in der die Schutzfunktion für den jeweiligen Befehl erstmals verfügbar war.

Die Regeln für die MAV-Systemstandardbefehle, die `security multi-admin-verify` "Befehle", können nicht geändert werden.

Zusätzlich zu den systemdefinierten Operationen sind die folgenden Befehle standardmäßig geschützt, wenn die Multi-Admin-Verifizierung aktiviert ist, aber die Regeln können geändert werden, um den Schutz für diese Befehle aufzuheben:

- "security login password"
- "security login unlock"
- "Set"

Regelbeschränkungen

Beim Erstellen einer Regel kann optional die `-query` Option angegeben werden, um die Anfrage auf eine Teilmenge der Befehlsfunktionalität zu beschränken. Die `-query` Option kann ebenfalls verwendet werden, um Konfigurationselemente wie die SVM, das Volume und Snapshot-Namen einzuschränken.

Beispielsweise kann im `volume snapshot delete` Befehl `-query` auf `-snapshot !hourly*,!daily*,!weekly*` gesetzt werden, was bedeutet, dass Volume-Snapshots mit dem Präfix „hourly“, „daily“ oder „weekly“ vom MAV-Schutz ausgeschlossen werden.

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

Ausgeschlossene Konfigurationselemente wären durch MAV nicht geschützt, und jeder

Administrator könnte sie löschen oder umbenennen.

Standardmäßig ist festgelegt, dass ein entsprechender `security multi-admin-verify request create "protected_operation"` Befehl automatisch generiert wird, wenn eine geschützte Operation aufgerufen wird. Diese Standardeinstellung kann so geändert werden, dass der `request create` Befehl separat eingegeben werden muss.

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

- Erforderliche Anzahl an Genehmigern
- Genehmigungsgruppen
- Ablaufzeitraum der Genehmigung
- Ablaufzeitraum für die Ausführung

System Manager Verfahren

Wenn zum ersten Mal eine Regel für geschützte Vorgänge hinzugefügt werden soll, bietet die System Manager-Vorgehensweise weitere Informationen zu "Multi-Admin-Verifizierung aktivieren."

Das bestehende Regelwerk kann wie folgt geändert werden:

1. **Cluster > Einstellungen** auswählen.
2. Wählen Sie neben **Genehmigung durch mehrere Administratoren** im Abschnitt **Sicherheit** aus.
3. Wählen Sie + Add , um mindestens eine Regel hinzuzufügen; Sie können auch bestehende Regeln ändern oder löschen.
   - Betrieb – Ein unterstützter Befehl aus der Liste kann ausgewählt werden.
   - Abfrage – Beliebige gewünschte Befehlsoptionen und Werte eingeben.
   - Optionale Parameter – Leer lassen, um die globalen Einstellungen anzuwenden, oder für bestimmte Regeln einen anderen Wert zuweisen, um die globalen Einstellungen zu überschreiben.
     - Erforderliche Anzahl an Genehmigern
     - Genehmigungsgruppen

CLI Prozedur

Alle `security multi-admin-verify rule`Befehle erfordern vor ihrer Ausführung die Genehmigung durch den MAV-Administrator, außer `security multi-admin-verify rule show`.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben
Regel erstellen	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [-approval-groups group1[,group2…]] [parameters]`

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben

Anmeldeinformationen der aktuellen Administratoren ändern	`security login modify <parameters>`
	
	Beispiel: Die folgende Regel erfordert eine Genehmigung zum Löschen des Root Volume.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`
	
	Mit dem `-approval-groups` Parameter lassen sich eine oder mehrere MAV-Genehmigungsgruppen für diese Regel angeben, wodurch die globale Genehmigungsgruppeneinstellung nur für diesen Vorgang überschrieben wird.

Eine Regel ändern	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Eine Regel löschen	`security multi-admin-verify rule delete -operation "protected_operation"`
Regeln anzeigen	`security multi-admin-verify rule show`
Alle verfügbaren MAV-geschützten Operationen	`security multi-admin-verify registered-operations show`

Verfügbare durch MAV schützbare Operationen

Ab ONTAP 9.20.1 können Sie alle Operationen anzeigen, die im aktuellen Cluster durch MAV geschützt werden können. Dies erleichtert die Erstellung einer Regel, ohne externe Dokumentation zur Ermittlung gültiger Operationsnamen konsultieren zu müssen.

```
security multi-admin-verify registered-operations show
```

Beispiel:

```
cluster1::> security multi-admin-verify registered-operations show
Operation
----------------------------------------
cluster peer delete
security login delete
security login modify
volume delete
volume move start
volume snapshot delete
...
```

Die Liste der Operationen variiert je nach ONTAP Version und Cluster-Persönlichkeit.

Sie können die Ausgabe anhand des Operationsnamens mithilfe des Parameters `-operation` filtern, einschließlich des Abgleichs mit Platzhaltern.

Beispiel:

```
cluster1::> security multi-admin-verify registered-operations show
-operation security*
Operation
---------------------------------
security anti-ransomware volume attack clear-suspect
security anti-ransomware volume disable
security anti-ransomware volume event-log modify
security audit modify
security login delete
...
```

Verwandte Informationen

- "Regel für die Multi-Admin-Verify-Sicherheit"
- "security login modify"

Ausführung von MAV-geschützten Vorgängen in ONTAP anfordern

Wenn ein geschützter Vorgang oder Befehl auf einem Cluster mit aktivierter Multi-Admin-Verifizierung (MAV) initiiert wird, fängt ONTAP den Vorgang automatisch ab und fordert die Generierung einer Anfrage an, die von einem oder mehreren Administratoren einer MAV-Genehmigungsgruppe (MAV-Administratoren) genehmigt werden muss. Alternativ ist es möglich, eine MAV-Anfrage ohne den Dialog zu erstellen.

Wird der Antrag genehmigt, ist innerhalb der Antragsfrist auf die Anfrage zu antworten, um den Vorgang abzuschließen. Wird der Antrag abgelehnt oder sind die Antrags- oder Ablauffristen überschritten, ist der Antrag zu löschen und erneut einzureichen.

Die MAV-Funktionalität berücksichtigt bestehende RBAC-Einstellungen. Das heißt, Ihre Administratorrolle muss über ausreichende Berechtigungen verfügen, um einen geschützten Vorgang unabhängig von den MAV-Einstellungen auszuführen. "Weitere Informationen zu RBAC".

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

System Manager Verfahren

Wenn ein Benutzer auf einen Menüpunkt klickt, um eine Operation auszulösen und die Operation geschützt ist, wird eine Genehmigungsanfrage generiert und der Benutzer erhält eine Benachrichtigung, die in etwa wie folgt aussieht:

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

Das Fenster **Anfragen mehrerer Administratoren** ist verfügbar, wenn MAV aktiviert ist und zeigt ausstehende Anfragen basierend auf der Anmelde-ID des Benutzers und der MAV-Rolle (Genehmiger oder nicht) an. Für jede ausstehende Anfrage werden die folgenden Felder angezeigt:

- Betrieb
- Index (Nummer)
- Status (Ausstehend, Genehmigt, Abgelehnt, Ausgeführt oder Abgelaufen)

  Wird ein Antrag von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.

- Abfrage (beliebige Parameter oder Werte für die angeforderte Operation)
- Anfordernder Benutzer
- Anfrage läuft am
- (Anzahl der) ausstehenden Genehmiger
- (Anzahl) potenzieller Genehmiger

Wenn die Anfrage genehmigt wird, kann der anfragende Benutzer den Vorgang innerhalb der Ablauffrist erneut ausführen.

Wenn der Benutzer den Vorgang ohne Genehmigung wiederholt, wird eine Benachrichtigung ähnlich der folgenden angezeigt:

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

CLI Prozedur

1. Die geschützte Operation kann direkt oder mit dem MAV-Anforderungsbefehl ausgeführt werden.

   Beispiele: Zum Löschen eines Volumes kann einer der folgenden Befehle verwendet werden:

   - `volume delete`

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

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

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

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

```
       auto-generated and requires approval.
```

- `security multi-admin-verify request create "volume delete"`

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

2. Der Status der Anfrage und die Antwort auf die MAV-Mitteilung werden geprüft.

   a. Wenn die Anfrage genehmigt wird, erfolgt eine Antwort auf die CLI-Nachricht, um den Vorgang abzuschließen.

   Beispiel:

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

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

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

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

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

b. Wird der Antrag abgelehnt oder ist die Frist abgelaufen, sollte der Antrag gelöscht und entweder erneut eingereicht oder der MAV-Administrator kontaktiert werden.

Beispiel:

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

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

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

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

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Verwaltung von MAV geschützten Operationsanforderungen in ONTAP

Wenn Administratoren in einer MAV-Genehmigungsgruppe (MAV-Administratoren) über eine ausstehende Ausführungsanfrage benachrichtigt werden, müssen sie innerhalb einer festgelegten Frist (Ablauf der Genehmigung) mit einer Genehmigungs- oder Ablehnungsnachricht antworten. Wenn nicht genügend Genehmigungen eingehen, muss der Anfragende die Anfrage löschen und eine neue stellen.

Über diese Aufgabe

Genehmigungsanfragen werden mit Indexnummern gekennzeichnet, die in E-Mail-Nachrichten und in der Anzeige der Anfragewarteschlange enthalten sind.

`multi-admin-verify`Anfragen im Endstatus können automatisch überschrieben oder entfernt werden. Die "Revisionsprotokoll" kann zur Überprüfung vorheriger Anfragen verwendet werden.

Ab ONTAP 9.20.1 können Mitglieder einer konfigurierten Genehmigergruppe für IdP, AD oder LDAP Anfragen genehmigen oder ablehnen, ohne als namentlich genannte Genehmiger aufgeführt zu sein. Änderungen an der Gruppenzugehörigkeit eines Benutzers im Identitätsanbieter werden bei der nächsten erfolgreichen Anmeldung des Benutzers wirksam. Eine Neukonfiguration von MAV ist nicht erforderlich.

Folgende Informationen aus der Anfragewarteschlange können angezeigt werden:

Betrieb
Die geschützte Operation, für die die Anfrage erstellt wird.

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

Status
Der aktuelle Status des Antrags: ausstehend, genehmigt, abgelehnt, abgelaufen, ausgeführt. Wird ein Antrag von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.

Erforderliche Genehmiger
Die Anzahl der MAV-Administratoren, die die Anfrage genehmigen müssen. Ein Benutzer kann den Parameter required-approvers für die Vorgangsregel festlegen. Wenn ein Benutzer required-approvers für die Regel nicht festlegt, wird der Wert required-approvers aus der globalen Einstellung angewendet.

Ausstehende Genehmiger
Die Anzahl der MAV-Administratoren, die noch erforderlich sind, um die Anfrage zu genehmigen, damit die Anfrage als genehmigt markiert wird.

Potenzielle Genehmigergruppen
Ab ONTAP 9.20.1 sind dies die IdP-, Active Directory- oder LDAP-Gruppen, deren Mitglieder berechtigt sind, die Anfrage zu genehmigen oder abzulehnen.

Ablauf der Genehmigung
Die Frist, innerhalb derer ein MAV-Administrator auf eine Genehmigungsanfrage reagieren muss. Jeder autorisierte Benutzer kann die Genehmigungsfrist für eine Vorgangsregel festlegen. Ist keine Genehmigungsfrist für die Regel festgelegt, wird die Genehmigungsfrist aus der globalen Einstellung angewendet.

Ablauf der Ausführung
Der Zeitraum, innerhalb dessen der anfragende Administrator den Vorgang abschließen muss. Jeder autorisierte Benutzer kann das Ausführungsablaufdatum für eine Vorgangsregel festlegen. Wenn kein Ausführungsablaufdatum für die Regel festgelegt ist, wird das Ausführungsablaufdatum aus der globalen Einstellung übernommen.

Genehmigte Nutzer
Die MAV-Administratoren, die den Antrag genehmigt haben.

Benutzer hat sein Veto eingelegt

Die MAV-Administratoren, die den Antrag abgelehnt haben.

Storage VM (vserver)

Die SVM, der die Anfrage zugeordnet ist. In dieser Version wird nur die admin SVM unterstützt.

Benutzeranfrage

Der Benutzername des Benutzers, der die Anfrage erstellt hat.

Erstellungszeit

Der Zeitpunkt, zu dem die Anfrage erstellt wurde.

Genehmigungszeit

Der Zeitpunkt, zu dem sich der Status der Anfrage auf „genehmigt“ geändert hat.

Kommentar

Alle Kommentare, die mit der Anfrage in Verbindung stehen.

Zugelassene Benutzer

Die Liste der Benutzer, die berechtigt sind, die geschützte Operation durchzuführen, für die die Anfrage genehmigt wurde. Wenn `users-permitted`leer ist, kann jeder Benutzer mit den entsprechenden Berechtigungen die Operation durchführen.

System Manager

MAV-Administratoren erhalten E-Mails mit Details zur Genehmigungsanfrage, deren Gültigkeitsdauer und einem Link zur Genehmigung oder Ablehnung der Anfrage. Sie können den Genehmigungsdialog über den Link in der E-Mail aufrufen oder in System Manager zu **Events & Jobs > Multi-Admin Requests** navigieren.

Das Fenster **Multi-Admin Requests** ist verfügbar, wenn die Multi-Admin-Verifizierung aktiviert ist, und zeigt ausstehende Anfragen basierend auf der Anmelde-ID des Benutzers und der MAV-Rolle (Genehmiger oder nicht) an. Mit **My Approvals** werden nur die Anfragen aufgelistet, für die der angemeldete Benutzer berechtigt ist zu handeln, einschließlich Anfragen, die über die Mitgliedschaft in einer IdP-, Active Directory- oder LDAP-Genehmigergruppe verfügbar sind.

- Betrieb
- Index (Nummer)
- Status (Ausstehend, Genehmigt, Abgelehnt, Ausgeführt oder Abgelaufen)

  Wird ein Antrag von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.
- Abfrage (beliebige Parameter oder Werte für die angeforderte Operation)
- Anfordernder Benutzer
- Anfrage läuft am
- (Anzahl der) ausstehenden Genehmiger
- Potenzielle Genehmiger (ab ONTAP 9.20.1 umfasst dies Benutzer, die als benannte Genehmiger oder durch Mitgliedschaft in einer berechtigten IdP-, Active Directory- oder LDAP-Genehmigergruppe infrage kommen)

MAV-Administratoren verfügen in diesem Fenster über zusätzliche Steuerungsmöglichkeiten; sie können

einzelne Vorgänge oder ausgewählte Gruppen von Vorgängen genehmigen, ablehnen oder löschen. Wenn der MAV-Administrator jedoch der Requesting User ist, kann er seine eigenen Anfragen nicht genehmigen, ablehnen oder löschen.

CLI

1. Wenn Sie per E-Mail über ausstehende Anfragen benachrichtigt werden, sollten Sie die Indexnummer und die Gültigkeitsdauer der Genehmigung der Anfrage beachten. Die Indexnummer kann auch mithilfe der Optionen **show** oder **show-pending** in der folgenden Tabelle angezeigt werden.
2. Den Antrag genehmigen oder ablehnen.

Wenn Sie Folgendes tun möchten…	Diesen Befehl eingeben
Eine Anfrage genehmigen	`security multi-admin-verify request approve` *nn*
Einen Antrag ablehnen	`security multi-admin-verify request veto` *nn*
Alle Anfragen, ausstehende Anfragen oder eine einzelne Anfrage anzeigen	`security multi-admin-verify request { show show-pending } [`*nn*`] { -fields` *field1*`[,`*field2*`…]`	`[-instance ] }` Sie können alle Anfragen in der Warteschlange oder nur ausstehende Anfragen anzeigen. Bei Eingabe der Indexnummer werden nur die Informationen dazu angezeigt. Informationen zu bestimmten Feldern (mithilfe des `-fields` Parameters) oder zu allen Feldern (mithilfe des `-instance` Parameters) können angezeigt werden.
Eine Anfrage löschen	`security multi-admin-verify request delete` *nn*

Beispiel:

Die folgende Sequenz genehmigt eine Anfrage, 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
Potential Approver Groups: entra-group-mav-approvers
   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: -
```

Ab ONTAP 9.20.1 enthält der `security multi-admin-verify request show` Befehl ein `Potential Approver Groups` Feld, in dem alle IdP-, AD- oder LDAP-Gruppen aufgeführt sind, deren Mitglieder berechtigt sind, die Anfrage zu genehmigen oder abzulehnen.

Beispiel:

Die folgende Sequenz legt ein Veto gegen eine Anfrage ein, 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         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: -
```

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Dynamische Autorisierung verwalten

Informationen zu ONTAP dynamischer Autorisierung

Ab ONTAP 9.15.1 können Administratoren die dynamische Autorisierung konfigurieren und aktivieren, um die Sicherheit des Fernzugriffs auf ONTAP zu erhöhen und gleichzeitig potenzielle Schäden durch einen böswilligen Akteur zu begrenzen. Mit ONTAP 9.15.1 bietet die dynamische Autorisierung ein erstes Framework zur Vergabe eines Sicherheitswerts an Benutzer. Wenn deren Aktivitäten verdächtig erscheinen, werden zusätzliche Autorisierungsprüfungen durchgeführt oder eine Operation vollständig verweigert. Administratoren können Regeln erstellen, Vertrauenswertungen zuweisen und Befehle einschränken, um festzulegen, wann bestimmte Aktivitäten für einen Benutzer erlaubt oder verweigert werden. Administratoren können die dynamische Autorisierung clusterweit oder für einzelne Storage-VMs aktivieren.

Wie dynamische Autorisierung funktioniert

Die dynamische Autorisierung verwendet ein Vertrauensbewertungssystem, um Benutzern je nach Autorisierungsrichtlinien unterschiedliche Vertrauensstufen zuzuweisen. Abhängig von der Vertrauensstufe des Benutzers kann eine von ihm durchgeführte Aktivität zugelassen oder verweigert werden, oder der Benutzer kann zur weiteren Authentifizierung aufgefordert werden.

Weitere Informationen darüber, wie Kriteriengewichtungen und andere dynamische Autorisierungsattribute konfiguriert werden, enthält "Dynamische Autorisierung anpassen".

Vertrauenswürdige Geräte

Wenn die dynamische Autorisierung verwendet wird, ist ein vertrauenswürdiges Gerät ein Gerät, das von einem Benutzer zur Anmeldung bei ONTAP verwendet wird, wobei die Public-Key-Authentifizierung als eine der Authentifizierungsmethoden genutzt wird. Das Gerät gilt als vertrauenswürdig, da nur dieser Benutzer im Besitz des zugehörigen privaten Schlüssels ist.

Beispiel für dynamische Autorisierung

Nehmen wir das Beispiel von drei verschiedenen Benutzern, die versuchen, ein Volume zu löschen. Wenn sie versuchen, den Vorgang auszuführen, wird die Risikobewertung für jeden Benutzer geprüft:

- Die erste Benutzerin meldet sich von einem vertrauenswürdigen Gerät an, bei dem es zuvor nur sehr wenige Authentifizierungsfehler gab, wodurch ihre Risikobewertung niedrig ist; der Vorgang ist ohne

zusätzliche Authentifizierung zulässig.

- Die zweite Benutzerin meldet sich von einem vertrauenswürdigen Gerät mit einem moderaten Prozentsatz vorheriger Authentifizierungsfehler an, was die Risikobewertung als moderat einstuft; sie wird zur zusätzlichen Authentifizierung aufgefordert, bevor die Operation zugelassen wird.
- Der dritte Benutzer meldet sich von einem nicht vertrauenswürdigen Gerät mit einem hohen Prozentsatz vorheriger Authentifizierungsfehler an, was zu einer hohen Risikobewertung führt; der Vorgang ist nicht zulässig.

Was kommt als Nächstes

- "Dynamische Autorisierung aktivieren oder deaktivieren"
- "Dynamische Autorisierung anpassen"

Dynamische Autorisierung in ONTAP aktivieren oder deaktivieren

Ab ONTAP 9.15.1 können Administratoren die dynamische Autorisierung entweder im `visibility` Modus testen oder im `enforced` Modus für CLI-Benutzer, die sich über SSH verbinden, aktivieren und konfigurieren. Wenn die dynamische Autorisierung nicht mehr benötigt wird, kann sie deaktiviert werden. Bei Deaktivierung der dynamischen Autorisierung bleiben die Konfigurationseinstellungen erhalten und können später wiederverwendet werden, falls sie erneut aktiviert werden soll.

Weitere Informationen zu `security dynamic-authorization modify` finden sich in der "ONTAP-Befehlsreferenz".

Dynamische Autorisierung für Tests aktivieren

Sie können die dynamische Autorisierung im Sichtbarkeitsmodus aktivieren, wodurch die Funktion getestet werden kann und sichergestellt ist, dass Benutzer nicht versehentlich ausgesperrt werden. In diesem Modus wird der Vertrauenswert bei jeder eingeschränkten Aktivität überprüft, aber nicht durchgesetzt. Allerdings wird jede Aktivität, die abgelehnt worden wäre oder zusätzlichen Authentifizierungsanforderungen unterliegen würde, protokolliert. Als bewährte Methode gilt, die gewünschten Einstellungen in diesem Modus zu testen, bevor sie durchgesetzt werden.

> ⓘ Sie können diesen Schritt ausführen, um die dynamische Autorisierung erstmals zu aktivieren, auch wenn Sie noch keine weiteren Einstellungen für die dynamische Autorisierung konfiguriert haben. Weitere Schritte zur Konfiguration anderer Einstellungen für die dynamische Autorisierung, um diese an Ihre Umgebung anzupassen, sind unter "Dynamische Autorisierung anpassen" zu finden.

Schritte

1. Dynamische Autorisierung im Sichtbarkeitsmodus kann durch Konfiguration globaler Einstellungen und Änderung des Funktionsstatus auf `visibility` aktiviert werden. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization modify \
-state visibility \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
```

```
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Das Ergebnis lässt sich mit dem `show` Befehl zur Anzeige der globalen Konfiguration überprüfen:

```
security dynamic-authorization show
```

Dynamische Autorisierung im erzwungenen Modus aktivieren

Sie können die dynamische Autorisierung im erzwungenen Modus aktivieren. In der Regel wird dieser Modus nach Abschluss der Tests mit dem Sichtbarkeitsmodus verwendet. In diesem Modus wird der Vertrauenswert bei jeder eingeschränkten Aktivität geprüft, und Aktivitätseinschränkungen werden durchgesetzt, wenn die Einschränkungsbedingungen erfüllt sind. Das Unterdrückungsintervall wird ebenfalls durchgesetzt, wodurch zusätzliche Authentifizierungsaufforderungen innerhalb des angegebenen Intervalls verhindert werden.

Dieser Schritt setzt voraus, dass Sie die dynamische Autorisierung zuvor im `visibility` -Modus konfiguriert und aktiviert haben, was dringend empfohlen wird.

Schritte

1. Dynamische Autorisierung im `enforced` Modus aktivieren, indem der Status auf `enforced` geändert wird. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization modify \
-state enforced \
-vserver <storage_VM_name>
```

2. Das Ergebnis lässt sich mit dem `show` Befehl zur Anzeige der globalen Konfiguration überprüfen:

```
security dynamic-authorization show
```

Dynamische Autorisierung deaktivieren

Die dynamische Autorisierung kann deaktiviert werden, wenn die zusätzliche Sicherheit bei der Authentifizierung nicht mehr benötigt wird.

Schritte

1. Die dynamische Autorisierung wird deaktiviert, indem ihr Status auf `disabled` geändert wird. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization modify \
-state disabled \
```

```
-vserver <storage_VM_name>
```

2. Das Ergebnis lässt sich mit dem `show` Befehl zur Anzeige der globalen Konfiguration überprüfen:

```
security dynamic-authorization show
```

Weitere Informationen zu `security dynamic-authorization show` finden sich in der "ONTAP-Befehlsreferenz".

Was kommt als Nächstes

(Optional) Je nach Ihrer Umgebung kann auf "Dynamische Autorisierung anpassen" verwiesen werden, um weitere Einstellungen für die dynamische Autorisierung zu konfigurieren.

Dynamische Autorisierung in ONTAP anpassen

Als Administrator können verschiedene Aspekte der dynamischen Autorisierungskonfiguration angepasst werden, um die Sicherheit von Remote-Administrator-SSH-Verbindungen zu Ihrem ONTAP Cluster zu erhöhen.

Die folgenden dynamischen Autorisierungseinstellungen können entsprechend Ihren Sicherheitsanforderungen angepasst werden:

- Globale Einstellungen für die dynamische Autorisierung konfigurieren
- Dynamische Autorisierungs-Vertrauensbewertungs-Komponenten konfigurieren
- Einen benutzerdefinierten Vertrauensbewertungsanbieter konfigurieren
- Eingeschränkte Befehle konfigurieren
- Dynamische Autorisierungsgruppen konfigurieren

Globale Einstellungen für die dynamische Autorisierung konfigurieren

Globale Einstellungen für dynamisch Autorisierung können konfiguriert werden, einschließlich der zu sichernden Storage-VM, des Unterdrückungsintervalls für Authentifizierungsherausforderungen und der Einstellungen für den Vertrauenswert.

Weitere Informationen zu `security login domain-tunnel create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Globale Einstellungen für dynamische Autorisierung konfigurieren. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Die Werte in Klammern <> an die eigene Umgebung anpassen:

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
```

```
-vserver <storage_VM_name>
```

2. Die resultierende Konfiguration wird angezeigt:

```
security dynamic-authorization show
```

Eingeschränkte Befehle konfigurieren

Wenn Sie die dynamische Autorisierung aktivieren, enthält die Funktion eine Standardliste eingeschränkter Befehle. Diese Liste kann an Ihre Anforderungen angepasst werden. Informationen zur Standardliste der eingeschränkten Befehle sind in der "Dokumentation zur Multi-Admin-Verifizierung (MAV)" zu finden.

Einen eingeschränkten Befehl hinzufügen

Sie können einen Befehl zur Liste der Befehle hinzufügen, die durch dynamische Autorisierung eingeschränkt sind.

Weitere Informationen zu `security dynamic-authorization rule create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Fügen Sie den Befehl hinzu. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization rule create \
-query <query> \
-operation <text> \
-index <integer> \
-vserver <storage_VM_name>
```

2. Die resultierende Liste der eingeschränkten Befehle wird angezeigt:

```
security dynamic-authorization rule show
```

Einen eingeschränkten Befehl entfernen

Sie können einen Befehl aus der Liste der Befehle entfernen, die durch dynamische Autorisierung eingeschränkt sind.

Weitere Informationen zu `security dynamic-authorization rule delete` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Den Befehl entfernen. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization rule delete \
-operation <text> \
-vserver <storage_VM_name>
```

2. Die resultierende Liste der eingeschränkten Befehle wird angezeigt:

```
security dynamic-authorization rule show
```

Dynamische Autorisierungsgruppen konfigurieren

Standardmäßig gilt die dynamische Autorisierung für alle Benutzer und Gruppen, sobald sie aktiviert ist. Es können jedoch Gruppen mit dem `security dynamic-authorization group create` Befehl erstellt werden, sodass die dynamische Autorisierung nur für diese spezifischen Benutzer gilt.

Eine dynamische Autorisierungsgruppe hinzufügen

Es kann eine dynamische Autorisierungsgruppe hinzugefügt werden.

Weitere Informationen zu `security dynamic-authorization group create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Die Gruppe wird erstellt. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization group create \
-name <group-name> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. Die resultierenden dynamischen Autorisierungsgruppen werden angezeigt:

```
security dynamic-authorization group show
```

Eine dynamische Autorisierungsgruppe entfernen

Sie können eine dynamische Autorisierungsgruppe entfernen.

Weitere Informationen zu `security dynamic-authorization group delete` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Die Gruppe wird gelöscht. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization group delete \
-name <group-name> \
-vserver <storage_VM_name>
```

2. Die resultierenden dynamischen Autorisierungsgruppen werden angezeigt:

```
security dynamic-authorization group show
```

Dynamische Autorisierungs-Vertrauensbewertungs-Komponenten konfigurieren

Sie können die maximale Gewichtung der Punktzahl konfigurieren, um die Priorität der Bewertungskriterien zu ändern oder bestimmte Kriterien aus der Risikobewertung zu entfernen.

> Als bewährte Vorgehensweise sollten die Standardwerte für die Gewichtung der Punktzahl beibehalten und nur bei Bedarf angepasst werden.

Weitere Informationen zu `security dynamic-authorization trust-score-component modify` finden sich in der "ONTAP-Befehlsreferenz".

Im Folgenden sind die Komponenten aufgeführt, die Sie anpassen können, zusammen mit ihrem Standardwert und den prozentualen Gewichtungen:

Kriterien	Komponentenname	Standardgewichtung der Rohpunktzahl	Standardprozentgewicht
Vertrauenswürdiges Gerät	`trusted-device`	20	50
Authentifizierungsverlauf der Benutzeranmeldung	`authentication-history`	20	50

Schritte

1. Komponenten der Vertrauensbewertung anpassen. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization trust-score-component modify \
-component <component-name> \
-weight <integer> \
-vserver <storage_VM_name>
```

2. Die resultierenden Einstellungen der Vertrauensbewertungskomponente werden angezeigt:

```
security dynamic-authorization trust-score-component show
```

Die Vertrauensbewertung für einen Benutzer zurücksetzen

Wird einem Benutzer aufgrund von Systemrichtlinien der Zugriff verweigert und kann er seine Identität nachweisen, kann der Administrator den Vertrauenswert des Benutzers zurücksetzen.

Weitere Informationen zu `security dynamic-authorization user-trust-score reset` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Fügen Sie den Befehl hinzu. Siehe Dynamische Autorisierungs-Vertrauensbewertungs-Komponenten konfigurieren für eine Liste der Komponenten der Vertrauensbewertung, die zurückgesetzt werden können. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization user-trust-score reset \
-username <username> \
-component <component-name> \
-vserver <storage_VM_name>
```

Vertrauensbewertung anzeigen

Ein Benutzer kann seinen eigenen Vertrauenswert für eine Anmeldesitzung anzeigen.

Schritte

1. Ihr Vertrauenswert wird angezeigt:

```
security login whoami
```

Sie sollten eine Ausgabe ähnlich der folgenden sehen:

```
User: admin
Role: admin
Trust Score: 50
```

Weitere Informationen zu `security login whoami` finden sich in der "ONTAP-Befehlsreferenz".

Einen benutzerdefinierten Vertrauensbewertungsanbieter konfigurieren

Wenn Sie bereits Scoring-Methoden von einem externen Trust-Score-Anbieter erhalten, kann der benutzerdefinierte Anbieter zur dynamischen Autorisierungskonfiguration hinzugefügt werden.

Bevor Sie beginnen

- Der Anbieter für benutzerdefinierte Vertrauensbewertungen muss eine JSON-Antwort zurückgeben. Folgende Syntaxanforderungen müssen erfüllt sein:
  - Das Feld, das den Vertrauenswert zurückgibt, muss ein Skalarfeld und kein Element eines Arrays sein.
  - Das Feld, das den Vertrauenswert zurückgibt, kann ein verschachteltes Feld sein, wie

`trust_score.value`.

- Die JSON-Antwort muss ein Feld enthalten, das einen numerischen Vertrauenswert zurückgibt. Falls dies nicht nativ verfügbar ist, kann ein Wrapper-Skript geschrieben werden, das diesen Wert zurückgibt.

- Der angegebene Wert kann entweder ein Vertrauenswert oder ein Risikowert sein. Der Unterschied besteht darin, dass der Vertrauenswert in aufsteigender Reihenfolge angegeben wird, wobei ein höherer Wert ein höheres Vertrauensniveau bedeutet, während der Risikowert in absteigender Reihenfolge angegeben wird. Beispielsweise zeigt ein Vertrauenswert von 90 bei einem Wertebereich von 0 bis 100 an, dass der Wert sehr vertrauenswürdig ist und wahrscheinlich ohne zusätzliche Prüfung zu einer „Erlaubnis“ führt, während ein Risikowert von 90 bei einem Wertebereich von 0 bis 100 ein hohes Risiko anzeigt und wahrscheinlich ohne zusätzliche Prüfung zu einer „Ablehnung“ führt.
- Der Anbieter für benutzerdefinierte Vertrauensbewertungen muss über die ONTAP REST API zugänglich sein.
- Der benutzerdefinierte Vertrauensbewertungsanbieter muss über einen der unterstützten Parameter konfigurierbar sein. Benutzerdefinierte Vertrauensbewertungsanbieter, die eine Konfiguration erfordern, die nicht in der Liste der unterstützten Parameter enthalten ist, werden nicht unterstützt.

  Weitere Informationen zu `security dynamic-authorization trust-score-component create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einen benutzerdefinierten Trust Score Provider hinzufügen. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization trust-score-component create \
-component <text> \
-provider-uri <text> \
-score-field <text> \
-min-score <integer> \
-max-score <integer> \
-weight <integer> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. Die resultierenden Einstellungen des Vertrauensbewertungsanbieters werden angezeigt:

```
security dynamic-authorization trust-score-component show
```

Benutzerdefinierte Trust Score Provider-Tags konfigurieren

Sie können mithilfe von Tags mit externen Anbietern von Vertrauensbewertungen kommunizieren. Dies ermöglicht das Senden von Informationen in der URL an den Anbieter von Vertrauensbewertungen, ohne sensible Informationen offenzulegen.

Weitere Informationen zu `security dynamic-authorization trust-score-component create`

finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Trust-Score-Anbieter-Tags aktivieren. Die Werte in Klammern <> sind an die eigene Umgebung anzupassen. Wird der `-vserver` Parameter nicht verwendet, erfolgt die Ausführung des Befehls auf Clusterebene. Parameter in Fettdruck sind erforderlich:

```
security dynamic-authorization trust-score-component create \
-component <component_name> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
-provider-uri <provider_URI> \
-score-field <REST_API_score_field> \
-secret-access-key "<key_text>"
```

Beispiel:

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.