Authentifizierung und Zugriffssteuerung

ONTAP 9

NetApp
February 12, 2026

Inhalt

Authentifizierung und Zugriffssteuerung

Übersicht über Authentifizierung und Zugriffssteuerung

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

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

Wenn Sie den klassischen System Manager verwenden (nur in ONTAP 9.7 und früher verfügbar), finden Sie weitere Informationen unter "System Manager Classic (ONTAP 9.0 bis 9.7)"

Client-Authentifizierung und -Autorisierung

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

Administratorauthentifizierung und RBAC

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

Managen Sie die Administratorauthentifizierung und RBAC

Erfahren Sie mehr über die Administratorauthentifizierung und RBAC in ONTAP

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

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

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

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

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

- "Active Directory"

Ab ONTAP 9.13.1 können Sie einen öffentlichen SSH-Schlüssel als primäre oder sekundäre Authentifizierungsmethode für einen Active Directory-Benutzer verwenden.

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

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

- "LDAP oder NIS"

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

ONTAP Administratorauthentifizierung und RBAC Workflow

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

1 Füllen Sie das Konfigurationsarbeitsblatt aus

Bevor Sie Anmeldekonten erstellen und die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) einrichten, sollten Sie die Informationen zu jedem Element in der erfassen "Konfigurationsarbeitsblätter".

2 Stellen Sie fest, ob das Administratorkonto lokal oder Remote ist

- **If local:** enable "Passwort", "SSH", "SSH MFA"oder "SSL" Access.
- **Falls Remote:** bestimmen Sie die Art des Remote-Zugriffs. Je nach Zugriffstyp "Aktivieren Sie den Active Directory-Zugriff", , "Aktivieren Sie LDAP- oder NIS-Zugriff"oder "SAML-Authentifizierung konfigurieren (nur für Admin-SVM)".

3 Richten Sie den rollenbasierten Zugriff ein

Die einem Administrator zugewiesene Rolle legt die Befehle fest, auf die der Administrator zugreifen kann. Die Rolle wird beim Erstellen des Administratorkontos zugewiesen und kann später ausgeführt werden"Geändert". Sie können vordefinierte Rollen für und "SVM" Administratoren oder "Definieren Sie benutzerdefinierte Rollen" nach Bedarf verwenden"Cluster".

4 Verwalten von Administratorkonten

Abhängig davon, wie Sie den Kontozugriff aktiviert haben, müssen Sie möglicherweise eine "Öffentlicher Schlüssel mit einem lokalen Konto" verwalten "Öffentliche Schlüssel und X.509-Zertifikate" , konfigurieren "Cisco Duo 2FA für SSH-Anmeldungen" , installieren Sie eine "DIGITALES Zertifikat für DEN CA-signierten Server" oder konfigurieren "Active Directory" , "LDAP oder NIS" Zugriff. Sie können jede dieser Aufgaben vor oder nach der Aktivierung des Kontozugriffs ausführen.

5 **Konfigurieren Sie zusätzliche Sicherheitsfunktionen**

- "Management der Verifizierung von mehreren Administratoren" Wenn Sie sicherstellen möchten, dass für bestimmte Vorgänge die Genehmigung von designierten Administratoren erforderlich ist.
- "Dynamische Autorisierung verwalten" Wenn Sie zusätzliche Autorisierungsprorüfungen auf Basis der Vertrauensebene eines Benutzers dynamisch anwenden möchten.
- "Konfigurieren der Just-in-Time-Berechtigungserweiterung (JIT)" wenn Sie Benutzern vorübergehend den Zugriff auf erhöhte Berechtigungen zum Ausführen bestimmter Aufgaben gestatten möchten.

Worksheets zur ONTAP-Administratorauthentifizierung und Einrichtung von RBAC

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

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Erstellen oder Ändern von Anmeldekonten

Sie geben diese Werte mit dem `security login create` Befehl an, wenn Sie Anmeldekonten für den Zugriff auf eine Storage-VM aktivieren. Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

```
`security login modify`Wenn Sie ändern, wie ein Konto auf eine Storage-VM zugreift, geben Sie mit dem Befehl dieselben Werte an. Erfahren Sie mehr über `security login modify` in der link:https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html["ONTAP-Befehlsreferenz"^].
```

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der Storage-VM, auf die das Konto zugreift. Der Standardwert ist der Name der Admin-Storage-VM für das Cluster.	
`-user-or-group-name`	Der Benutzername oder der Gruppenname des Kontos. Wenn Sie einen Gruppennamen angeben, können Sie auf jeden Benutzer in der Gruppe zugreifen. Sie können einem Benutzernamen oder Gruppennamen mehrere Anwendungen zuordnen.	

`-application`	Die Applikation, die für den Zugriff auf die Storage-VM verwendet wird: • `http` • `ontapi` • `snmp` • `ssh`	
`-authmethod`	Die Methode, die zur Authentifizierung des Kontos verwendet wird: • `cert` Für SSL-Zertifikatauthentifizierung • `domain` Für Active Directory-Authentifizierung • `nsswitch` Für LDAP- oder NIS-Authentifizierung • `password` Für die Authentifizierung des Benutzerpassworts • `publickey` Zur Authentifizierung mit öffentlichen Schlüsseln • `community` Für SNMP-Community-Strings • `usm` Für SNMP-Benutzersicherheitsmodell • `saml` Für die SAML-Authentifizierung (Security Assertion Markup Language)	
`-remote-switch-ipaddress`	Die IP-Adresse des Remote-Switch. Bei dem Remote-Switch kann es sich um einen Cluster-Switch-Switch-Health-Monitor (CSHM) oder einen Fibre Channel (FC)-Switch handelt, der von der MetroCluster-Systemzustandsüberwachung (MCC-HM) überwacht wird. Diese Option ist nur anwendbar, wenn die Anwendung ist `snmp` und die Authentifizierungsmethode ist `usm`.	

`-role`	Die Zugriffskontrollrolle, die dem Konto zugewiesen ist: • Für den Cluster (die Admin-Storage-VM) ist der Standardwert `admin` . • Für eine Datenspeicher-VM ist der Standardwert `vsadmin` .	
`-comment`	(Optional) Beschreibungstext des Kontos. Sie sollten den Text in doppelte Anführungszeichen (") einschließen.	
`-is-ns-switch-group`	Ob das Konto ein LDAP-Gruppenkonto oder ein NIS-Gruppenkonto ist (`yes`oder `no`).	
`-second-authentication -method`	Zweite Authentifizierungsmethode bei Multi-Faktor-Authentifizierung: • `none` Wenn Sie die Multifaktor-Authentifizierung nicht verwenden, ist der Standardwert • `publickey` Für die Authentifizierung mit öffentlichen Schlüsseln, wenn das `authmethod` Passwort oder nsswitch ist • `password` Für die Authentifizierung des Benutzerpassworts, wenn der `authmethod` Public Key ist • `nsswitch` Zur Authentifizierung des Benutzerpassworts, wenn die authmethod publickey ist Die Reihenfolge der Authentifizierung ist immer der öffentliche Schlüssel gefolgt vom Passwort.	

`-is-ldap-fastbind`	Beginnend mit ONTAP 9.11.1, wenn auf true gesetzt, aktiviert LDAP fast bind für nswitch Authentifizierung; der Standardwert ist false. Um LDAP fast bind zu verwenden, muss der `-authentication-method` Wert auf gesetzt `nsswitch` werden. "Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs".	

Konfigurieren Sie die Sicherheitsinformationen von Cisco Duo

Sie geben diese Werte mit dem `security login duo create` Befehl an, wenn Sie die zwei-Faktor-Authentifizierung mit Cisco Duo samt SSH-Anmeldungen für eine Storage VM aktivieren. Erfahren Sie mehr über `security login duo create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Die Speicher-VM (in der ONTAP-CLI als vServer bezeichnet), auf die die Duo-Authentifizierungseinstellungen zutreffen.	
`-integration-key`	Ihr Integrationsschlüssel, den Sie erhalten, wenn Sie Ihre SSH-Anwendung bei Duo registrieren.	
`-secret-key`	Ihr Geheimschlüssel, den Sie erhalten, wenn Sie Ihre SSH-Anwendung bei Duo registrieren.	
`-api-host`	Der API-Hostname, der beim Registrieren Ihrer SSH-Anwendung bei Duo ermittelt wird. Beispiel: `api-<HOSTNAME>.duosecurity.com`	

`-fail-mode`	Bei Service- oder Konfigurationsfehlern, die die Duo-Authentifizierung verhindern, schlagen `safe secure` Sie fehl (Zugriff zulassen) oder (Zugriff verweigern). Der Standardwert ist `safe`, was bedeutet, dass die Duo-Authentifizierung umgangen wird, wenn sie aufgrund von Fehlern wie dem Duo-API-Server nicht zugänglich ist.	
`-http-proxy`	Verwenden Sie den angegebenen HTTP-Proxy. Wenn der HTTP-Proxy eine Authentifizierung erfordert, geben Sie die Anmeldeinformationen in die Proxy-URL ein. Beispiel: `http-proxy=http://username:password@proxy.example.org:8080`	
`-autopush`	Entweder `true` oder `false`. Der Standardwert ist `false`. Wenn `true`, sendet Duo automatisch eine Push-Login-Anfrage an das Telefon des Benutzers, um zu einem Telefonanruf zurückkehren, wenn Push nicht verfügbar ist. Beachten Sie, dass dadurch die Kenncode-Authentifizierung effektiv deaktiviert wird. Wenn `false`, wird der Benutzer aufgefordert, eine Authentifizierungsmethode auszuwählen. Wenn mit konfiguriert `autopush = true`, empfehlen wir die Einstellung `max-prompts = 1`.	

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

`-pushinfo`	Diese Option bietet zusätzliche Informationen in der Push-Benachrichtigung, z. B. den Namen der Anwendung oder des Dienstes, auf den zugegriffen wird. Dadurch können Benutzer überprüfen, ob sie sich beim richtigen Dienst anmelden, und erhalten eine zusätzliche Sicherheitsebene.	

Definieren benutzerdefinierter Rollen

Sie geben diese Werte mit dem `security login role create` Befehl an, wenn Sie eine benutzerdefinierte Rolle definieren. Erfahren Sie mehr über `security login role create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	(Optional) der Name der Storage-VM (in der ONTAP-CLI als vServer bezeichnet), die mit der Rolle verknüpft ist.	
`-role`	Der Name der Rolle.	
`-cmddirname`	Der Befehl oder das Befehlsverzeichnis, auf das die Rolle Zugriff erhält. Sie sollten Unterverzeichnisnamen in doppelte Anführungszeichen (") einschließen. "`volume snapshot`"`Beispiel: . Sie müssen eingeben `DEFAULT`, um alle Befehlsverzeichnisse anzugeben.	

`-access`	(Optional) der Zugriffsebene 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 seinen Unterverzeichnissen • `all` Gewährt Zugriff auf alle Befehle im Befehlsverzeichnis und seinen Unterverzeichnissen Für *nonintrinsische Befehle* (Befehle, die nicht in `create`, `modify`, , `delete` oder enden `show`): • `none` (Der Standardwert für benutzerdefinierte Rollen) verweigert den Zugriff auf den Befehl • `readonly` Trifft nicht zu • `all` Gewährt Zugriff auf den Befehl Um den Zugriff auf intrinsische Befehle zu gewähren oder zu verweigern, müssen Sie das Befehlsverzeichnis angeben.	
`-query`	(Optional) das Abfrageobjekt, das zum Filtern der Zugriffsebene verwendet wird, die in Form einer gültigen Option für den Befehl oder für einen Befehl im Befehlsverzeichnis angegeben ist. Sie sollten das Abfrageobjekt in doppelte Anführungszeichen (") einschließen. Wenn das Befehlsverzeichnis beispielsweise lautet `volume`, `"-aggr aggr0"` würde das Abfrageobjekt den Zugriff `aggr0` nur für das Aggregat ermöglichen.	

Einem Benutzerkonto einen öffentlichen Schlüssel zuordnen

Sie geben diese Werte mit dem `security login publickey create` Befehl an, wenn Sie einen öffentlichen SSH-Schlüssel mit einem Benutzerkonto verknüpfen. Erfahren Sie mehr über `security login publickey create` in der "ONTAP-Befehlsreferenz".

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

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

Konfigurieren Sie die globalen Einstellungen für die dynamische Autorisierung

Ab ONTAP 9.15.1 geben Sie diese Werte mit dem `security dynamic-authorization modify` Befehl an. Erfahren Sie mehr über `security dynamic-authorization modify` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert

`-vserver`	Der Name der Storage-VM, für die die Einstellung für die Vertrauensbewertung geändert werden soll. Wenn Sie diesen Parameter nicht angeben, wird die Einstellung auf Cluster-Ebene verwendet.	
`-state`	Der dynamische Autorisierungsmodus. Mögliche Werte: • `disabled`: (Standard) die dynamische Autorisierung ist deaktiviert. • `visibility`: Dieser Modus ist nützlich zum Testen der dynamischen Autorisierung. In diesem Modus wird die Vertrauensbewertung mit jeder eingeschränkten Aktivität überprüft, jedoch nicht erzwungen. Jede Aktivität, die abgelehnt worden wäre oder zusätzlichen Authentifizierungsherausforderungen unterliegen würde, wird jedoch protokolliert. • `enforced`: Für den Einsatz bestimmt, nachdem Sie `visibility` die Tests mit Mode abgeschlossen haben. In diesem Modus wird die Vertrauensbewertung mit jeder eingeschränkten Aktivität überprüft, und Aktivitätsbeschränkungen werden erzwungen, wenn die Bedingungen für Einschränkungen erfüllt sind. Das Unterdrückungsintervall wird ebenfalls erzwungen, wodurch zusätzliche Authentifizierungsherausforderungen innerhalb des angegebenen Intervalls verhindert werden.	

`-suppression-interval`	Verhindert zusätzliche Authentifizierungsherausforderungen innerhalb des angegebenen Intervalls. Das Intervall ist im ISO-8601-Format und akzeptiert Werte von 1 Minute bis einschließlich 1 Stunde. Bei Einstellung auf 0 wird das Unterdrückungsintervall deaktiviert, und der Benutzer wird immer aufgefordert, eine Authentifizierungsherausforderung zu erstellen, wenn eine solche erforderlich ist.	
`-lower-challenge-boundary`	Die prozentuale Grenze für die Herausforderung der unteren Multi-Faktor-Authentifizierung (MFA). Der gültige Bereich liegt zwischen 0 und 99. Der Wert 100 ist ungültig, da dadurch alle Anfragen abgelehnt werden. Der Standardwert ist 0.	
`-upper-challenge-boundary`	Die obere Grenze für den MFA-Challenge-Prozentsatz. Der gültige Bereich liegt zwischen 0 und 100. Dieser Wert muss gleich oder größer sein als der Wert der unteren Grenze. Ein Wert von 100 bedeutet, dass jede Anfrage entweder abgelehnt wird oder einer zusätzlichen Authentifizierungsherausforderung unterliegt; es gibt keine Anfragen, die ohne eine Herausforderung erlaubt sind. Der Standardwert ist 90.	

Installieren Sie ein digitales Zertifikat für einen CA-signierten Server

Sie geben diese Werte mit dem `security certificate generate-csr` Befehl an, wenn Sie eine digitale Zertifikatsignierungsanforderung (CSR) für die Authentifizierung einer Speicher-VM als SSL-Server generieren. Erfahren Sie mehr über `security certificate generate-csr` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert

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

Sie geben diese Werte mit dem `security certificate install` Befehl an, wenn Sie ein CA-signiertes digitales Zertifikat zur Authentifizierung des Clusters oder der Speicher-VM als SSL-Server installieren. In der folgenden Tabelle sind nur die Optionen aufgeführt, die für die Kontenkonfiguration relevant sind. Erfahren Sie mehr über `security certificate install` 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 Public Key-Zertifikat der Root-CA des SSL-Clients • `server-ca` Für das Public Key-Zertifikat der Root-CA des SSL-Servers, dessen Client ONTAP ist • `client` Für ein selbstsigniertes oder CA-signiertes digitales Zertifikat und einen privaten Schlüssel für ONTAP als SSL-Client	

Konfigurieren Sie den Active Directory-Domänencontroller-Zugriff

Sie geben diese Werte mit dem `security login domain-tunnel create` Befehl an, wenn Sie bereits einen SMB-Server für eine Datenspeicher-VM konfiguriert haben und Sie die Storage-VM als Gateway oder *Tunnel* für den Active Directory-Domänencontroller-Zugriff auf das Cluster konfigurieren möchten. Erfahren Sie mehr über `security login domain-tunnel create` in der "ONTAP-Befehlsreferenz".

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

Sie geben diese Werte mit dem `vserver active-directory create` Befehl an, wenn Sie keinen SMB-Server konfiguriert haben und Sie ein Storage-VM-Computerkonto in der Active Directory-Domäne erstellen möchten. Erfahren Sie mehr über `vserver active-directory create` in der "ONTAP-Befehlsreferenz".

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

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

Konfigurieren Sie den LDAP- oder NIS-Serverzugriff

Sie 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. Erfahren Sie mehr über `vserver services name-service ldap client create` in der "ONTAP-Befehlsreferenz".

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

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

Sie geben diese Werte mit dem `vserver services name-service ldap create` Befehl an, wenn Sie eine LDAP-Client-Konfiguration mit der Speicher-VM verknüpfen. Erfahren Sie mehr über `vserver services name-service ldap create` in der "ONTAP-Befehlsreferenz".

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

Sie geben diese Werte mit dem `vserver services name-service nis-domain create` Befehl an, wenn Sie eine NIS-Domänenkonfiguration auf einer Storage VM erstellen. Erfahren Sie mehr über `vserver services name-service nis-domain create` 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 Domäne.	
`-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 Reihenfolge für die Nachschlagen von Namensdienstquellen angeben. Erfahren Sie mehr über `vserver services name-service ns-switch create` in der "ONTAP-Befehlsreferenz".

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

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

Konfigurieren Sie den SAML-Zugriff

Ab ONTAP 9.3 geben Sie diese Werte mit dem `security saml-sp create` Befehl zum Konfigurieren der SAML-Authentifizierung an. Erfahren Sie mehr über `security saml-sp create` in der "ONTAP-Befehlsreferenz".

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

`-cert-ca` Und `-cert-serial`, oder `-cert-common-name`	Die Serverzertifikatdetails des Host des Service-Providers (ONTAP-System). Sie können entweder die Zertifizierungsstelle des Dienstanbieters und die Seriennummer des Zertifikats oder den allgemeinen Serverzertifikats eingeben.	
`-verify-metadata-server`	Ob die Identität des IdP-Metadatenservers validiert werden muss `true`oder `false`). Es empfiehlt sich, diesen Wert immer auf `true`zu setzen.	

Erstellen von Anmeldekonten

Erfahren Sie mehr über das Erstellen von ONTAP-Anmeldekonten

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

Cluster- und SVM-Administratoren

Ein_Cluster-Administrator_ greift auf die Admin-SVM für das Cluster zu. `admin`Beim Einrichten des Clusters werden automatisch die Admin-SVM und ein Cluster-Administrator mit dem reservierten Namen erstellt.

Ein Cluster-Administrator mit der Standardrolle `admin` kann den gesamten Cluster und seine Ressourcen verwalten. Der Cluster-Administrator kann bei Bedarf weitere Cluster-Administratoren mit unterschiedlichen Rollen erstellen.

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

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

Namenskonventionen

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

- „adm“
- „Bin“
- „cli“

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

Zusammengeführte Rollen

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

Aktivieren Sie den Zugriff auf lokales Konto

Hier erfahren Sie, wie Sie den Zugriff auf ein lokales ONTAP-Konto aktivieren

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

Verwandte Informationen

- "Sicherheits-Login erstellen"

Aktivieren Sie den Zugriff auf das Kennwort des ONTAP-Kontos

Mit dem `security login create` Befehl können Sie Administratorkonten für den Zugriff auf einen Admin oder eine Daten-SVM mit einem Passwort aktivieren. Nachdem

Sie den Befehl eingegeben haben, werden Sie zur Eingabe des Passworts aufgefordert.

Über diese Aufgabe

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

Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

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

Schritt

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

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

   Mit dem folgenden Befehl `admin1 backup` kann das Cluster-Administratorkonto mit der vordefinierten Rolle mit`engCluster` einem Passwort auf die Admin-SVM zugreifen. Nachdem Sie den Befehl eingegeben haben, werden Sie zur Eingabe des Passworts aufgefordert.

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

   Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

Aktivieren Sie den SSH-Zugriff auf den öffentlichen Schlüssel des ONTAP-Kontos

Sie können mit dem `security login create` Befehl Administratorkonten für den Zugriff auf einen Admin oder eine Daten-SVM mit einem öffentlichen SSH-Schlüssel aktivieren.

Über diese Aufgabe

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

  Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto

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

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

  Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

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

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

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

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

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

Bevor Sie beginnen

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

Schritt

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

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

   Mit dem folgenden Befehl kann das SVM-Administratorkonto `svmadmin1` mit der vordefinierten `vsadmin-volume` Rolle`engData1` über einen öffentlichen SSH-Schlüssel auf die SVM zugreifen:

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

   Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

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

Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto

Aktivieren Sie Multi-Faktor-Authentifizierungskonten (MFA)

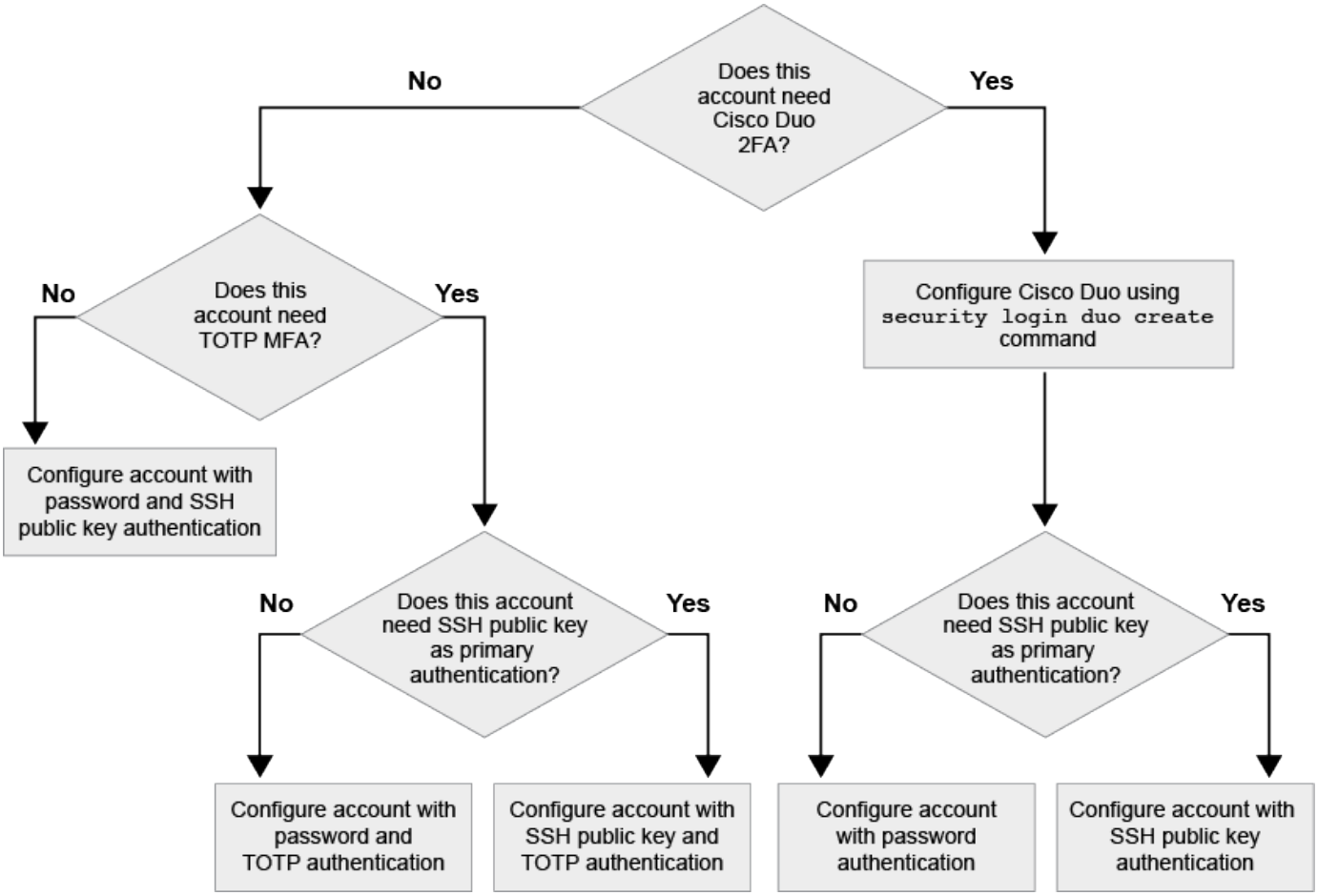
Informieren Sie sich über die ONTAP-Multi-Faktor-Authentifizierung

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

Je nach Ihrer Version von ONTAP können Sie eine Kombination aus einem öffentlichen SSH-Schlüssel, einem Benutzerpasswort und einem zeitbasierten Einmalpasswort (TOTP) zur mehrstufigen Authentifizierung verwenden. Wenn Sie Cisco Duo (ONTAP 9.14.1 und höher) aktivieren und konfigurieren, dient es als zusätzliche Authentifizierungsmethode, die die bestehenden Methoden für alle Benutzer ergänzt.

Verfügbar ab…	Erste Authentifizierungsmethode	Zweite Authentifizierungsmethode
ONTAP 9.14.1	Öffentlicher SSH-Schlüssel	TOTP
	Benutzerkennwort	TOTP
	Öffentlicher SSH-Schlüssel	Cisco Duo
	Benutzerpasswort	Cisco Duo
ONTAP 9.13.1	Öffentlicher SSH-Schlüssel	TOTP
	Benutzerpasswort	TOTP
ONTAP 9,3	Öffentlicher SSH-Schlüssel	Benutzerpasswort

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



Multifaktor-Authentifizierung mit ONTAP über SSH und TOTP

Dank der Multi-Faktor-Authentifizierung (MFA) können Sie die Sicherheit erhöhen, da

Benutzer zur Anmeldung bei einem Administrator oder einer Daten-SVM zwei Authentifizierungsmethoden bereitstellen müssen.

Über diese Aufgabe

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

  Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

  "Ändern der Rolle, die einem Administrator zugewiesen ist"

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

  "Einem Benutzerkonto einen öffentlichen Schlüssel zuordnen"

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

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

Aktivieren Sie MFA mit öffentlichem SSH-Schlüssel und Benutzerpasswort

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

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

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

```
`admin2` `admin```engData1``Mit dem folgenden Befehl muss sich das SVM-
Administratorkonto mit der vordefinierten Rolle mit einem öffentlichen
SSH-Schlüssel und einem Benutzerpasswort bei der SVM anmelden:
```

```
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".
```

Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

Aktivieren Sie MFA mit TOTP

Ab ONTAP 9.13.1 können Sie die Sicherheit erhöhen, indem Sie lokale Benutzer über einen öffentlichen SSH-Schlüssel oder ein Benutzerkennwort und ein zeitbasiertes Einmalpasswort (TOTP) bei einem Administrator oder einer Daten-SVM einloggen müssen. Nachdem das Konto für MFA mit TOTP aktiviert wurde, muss sich der lokale Benutzer bei anmelden"Schließen Sie die Konfiguration ab".

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

Bevor Sie beginnen

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

Schritte

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

Aktivieren Sie MFA mit Benutzerpasswort und TOTP

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

   Für neue Benutzerkonten

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

   Für bestehende Benutzerkonten

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

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

   ```
   security login show
   ```

Aktivieren Sie MFA mit öffentlichem SSH-Schlüssel und TOTP

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

   Für neue Benutzerkonten

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

   Für bestehende Benutzerkonten

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

   Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

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

```
security login show
```

Erfahren Sie mehr über `security login show` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

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

  "Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto"

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

  "Konfigurieren Sie das lokale Benutzerkonto für MFA mit TOTP"

Verwandte Informationen

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

Konfigurieren Sie lokale ONTAP-Benutzerkonten für MFA mit TOTP

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

Bevor Sie beginnen

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

  Microsoft Authenticator, Google Authenticator, Authy und jeder andere TOTP-kompatible Authenticator wird unterstützt.

Schritte

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

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

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

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

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

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

Verwandte Informationen

- "Sicherheits-Login totp erstellen"
- "Sicherheits-Login-TOTP-Show"

Setzen Sie den geheimen TOTP-Schlüssel für ein ONTAP-Benutzerkonto zurück

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

Setzen Sie TOTP zurück, wenn Ihr Schlüssel kompromittiert ist

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

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

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

3. Neuen TOTP-Schlüssel erstellen:

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

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

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

Setzen Sie TOTP zurück, wenn Ihr Schlüssel verloren geht

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

Bevor Sie beginnen

Der TOTP-Schlüssel muss von einem Speicheradministrator deaktiviert werden. Wenn Sie kein Storage-

Administratorkonto haben, wenden Sie sich an Ihren Storage-Administrator, um den Schlüssel zu deaktivieren.

Schritte

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

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

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

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

Verwandte Informationen

- "Sicherheits-Login totp erstellen"
- "Sicherheits-Login-Topp löschen"
- "Sicherheits-Login-TOTP-Show"

Deaktivieren Sie den geheimen TOTP-Schlüssel für ein ONTAP-Benutzerkonto

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

Über diese Aufgabe

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

Schritt

1. Deaktivieren Sie den geheimen TOTP-Schlüssel:

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

Erfahren Sie mehr über `security login totp modify` in der "ONTAP-Befehlsreferenz".

Aktivieren Sie den Zugriff auf das ONTAP-Konto des SSL-Zertifikats

Mit dem `security login create` Befehl können Sie Administratorkonten für den Zugriff auf einen Admin oder eine Daten-SVM mit einem SSL-Zertifikat aktivieren.

Über diese Aufgabe

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

zugreifen kann.

Erstellen und Installieren eines CA-signierten Serverzertifikats

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

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

Ändern der Rolle, die einem Administrator zugewiesen ist

> Für Clusteradministratorkonten wird die Zertifikatauthentifizierung mit den `http` `ontapi` `rest` Anwendungen , und unterstützt. Bei SVM-Administratorkonten wird die Zertifikatauthentifizierung nur mit den `ontapi` und `rest`-Applikationen unterstützt.

Schritt

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

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

   Mit dem folgenden Befehl `svmadmin2` `vsadmin` kann das SVM-Administratorkonto mit der Standardrolle`engData2` über ein digitales SSL-Zertifikat auf die SVM zugreifen.

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

   Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

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

Erstellen und Installieren eines CA-signierten Serverzertifikats

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Aktivieren Sie den Zugriff auf das Active Directory-ONTAP-Konto

Sie können mit dem `security login create` Befehl Active Directory (AD) Benutzer- oder Gruppenkonten für den Zugriff auf einen Administrator oder eine Daten-SVM aktivieren. Jeder Benutzer der AD-Gruppe kann mit der Rolle, die der Gruppe zugewiesen ist, auf die SVM zugreifen.

Über diese Aufgabe

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

Active Directory-Domänencontroller-Zugriff wird konfiguriert

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

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

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

- Ab ONTAP 9.11.1 können Sie verwenden"Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs", wenn es vom AD-LDAP-Server unterstützt wird.
- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, können Sie `security login modify` die Rolle später mit dem Befehl hinzufügen.

  Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

  Ändern der Rolle, die einem Administrator zugewiesen ist

> DER Zugriff auf das Konto `SSH ontapi rest` für ANZEIGENGRUPPEN wird nur mit den Anwendungen , und unterstützt. AD-Gruppen werden mit der SSH-Authentifizierung für öffentliche Schlüssel, die häufig für Multi-Faktor-Authentifizierung verwendet wird, nicht unterstützt.

Bevor Sie beginnen

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

Schritt

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

   Für AD-Nutzer:

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

ONTAP-Version	Primäre Authentifizierung	Sekundäre Authentifizierung	Befehl

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

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

Für AD-Gruppen:

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

Nachdem Sie fertig sind

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

Active Directory-Domänencontroller-Zugriff wird konfiguriert

Verwandte Informationen

- "Sicherheits-Login erstellen"

Aktivieren Sie den Zugriff auf das LDAP- oder NIS-ONTAP-Konto

Sie können den `security login create` Befehl verwenden, um LDAP- oder NIS-Benutzerkonten für den Zugriff auf einen Administrator oder eine Daten-SVM zu aktivieren. Wenn Sie keinen LDAP- oder NIS-Serverzugriff auf die SVM konfiguriert haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Über diese Aufgabe

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

  Konfigurieren des LDAP- oder NIS-Serverzugriffs

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

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

  Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

  Ändern der Rolle, die einem Administrator zugewiesen ist

- Ab ONTAP 9.4 wird Multi-Faktor-Authentifizierung (MFA) für Remote-Benutzer über LDAP- oder NIS-Server unterstützt.
- Ab ONTAP 9.11.1 können Sie verwenden"Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs", wenn es vom LDAP-Server unterstützt wird.
- Aufgrund eines bekannten LDAP-Problems sollten Sie das `':'` Zeichen (Doppelpunkt) nicht in einem Feld von LDAP-Benutzerkontoinformationen verwenden (z. B. `gecos` , `userPassword` usw.). Andernfalls schlägt die Suche für diesen Benutzer fehl.

Bevor Sie beginnen

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

Schritte

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

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

   "Erstellen oder Ändern von Anmeldekonten"

Mit dem folgenden Befehl wird das LDAP- oder NIS-Clusteradministratorkonto `guest2` mit der vordefinierten `backup` Rolle aktiviert, um auf die Admin-SVM zuzugreifen`engCluster`.

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

Erfahren Sie mehr über `security login create` 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
```

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

Im folgenden Beispiel wird die MFA-Authentifizierung aktiviert:

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

Nachdem Sie fertig sind

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

Konfigurieren des LDAP- oder NIS-Serverzugriffs

Verwandte Informationen

- "Sicherheitsanmeldung"

Management von Zugriffssteuerungsrollen

Erfahren Sie mehr über das Management von ONTAP-Zugriffskontrollrollen

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

Ändern Sie die Rolle, die einem ONTAP-Administrator zugewiesen wurde

Mit dem `security login modify` Befehl können Sie die Rolle eines Cluster- oder SVM-Administratorkontos ändern. Sie können eine vordefinierte oder benutzerdefinierte Rolle zuweisen.

Bevor Sie beginnen

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

Schritt

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

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

   "Erstellen oder Ändern von Anmeldekonten"

   Mit dem folgenden Befehl wird die Rolle des AD Cluster-Administratorkontos `DOMAIN1\guest1` in die vordefinierte Rolle geändert `readonly`.

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

   Mit dem folgenden Befehl wird die Rolle der SVM-Administratorkonten im AD-Gruppenkonto `DOMAIN1\adgroup` in die benutzerdefinierte `vol_role` Rolle geändert.

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

   Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

Definieren Sie benutzerdefinierte Rollen für ONTAP-Administratoren

Mit dem `security login role create` Befehl können Sie eine benutzerdefinierte Rolle definieren. Sie können den Befehl so oft wie nötig ausführen, um die genaue Kombination der Funktionen zu erreichen, die Sie mit der Rolle verknüpfen möchten.

Über diese Aufgabe

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

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

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

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

Sie können einem SVM-Administrator keine Rolle zuweisen, die Zugriff auf einen Befehl oder ein Befehlsverzeichnis gewährt, der nur für den `admin` Cluster-Administrator verfügbar ist, z. B. auf das `security` Befehlsverzeichnis.

Bevor Sie beginnen

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

Schritt

1. Definieren einer benutzerdefinierten Rolle:

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

   Die folgenden Befehle gewähren der `vol_role` Rolle vollen Zugriff auf die Befehle im `volume` Befehlsverzeichnis und schreibgeschützten Zugriff auf die Befehle im `volume snapshot` Unterverzeichnis.

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

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

   Die folgenden Befehle gewähren der `SVM_storage` Rolle schreibgeschützten Zugriff auf die Befehle im `storage` Befehlsverzeichnis, keinen Zugriff auf die Befehle im `storage encryption` Unterverzeichnis und vollen Zugriff auf den `storage aggregate plex offline` nicht-intrinsischen 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
   ```

   Erfahren Sie mehr über `security login role create` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Rolle für Sicherheits-Login erstellen"
- "Plex des Storage-Aggregats ist offline"
- "Storage-Verschlüsselung"

Vordefinierte Rollen für ONTAP-Cluster-Administratoren

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

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

Diese Rolle…	Verfügt über diese Zugriffsebene…	Zu den folgenden Befehlen oder Befehlsverzeichnissen
Admin	Alle	Alle Befehlsverzeichnisse (`DEFAULT`)
Admin-no-fsa (ab ONTAP 9.12.1 verfügbar)	Lese-/Schreibzugriff	• Alle Befehlsverzeichnisse (`DEFAULT`) • `security login rest-role` • `security login role`
Schreibgeschützt	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Keine

`volume file show-disk-usage`	AutoSupport	Alle
• `set` • `system node autosupport`	Keine	Alle anderen Befehlsverzeichnisse (`DEFAULT`)
Backup	Alle	`vserver services ndmp`
readonly	`volume`	Keine
Alle anderen Befehlsverzeichnisse (`DEFAULT`)	readonly	Alle
• `security login password` Nur zur Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • `set`	• Ab ONTAP 9.8 schreibgeschützt • Vor ONTAP 9.8 keine	`security`
readonly	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 wird dem vordefinierten `autosupport` Konto zugewiesen, das von AutoSupport OnDemand verwendet wird. ONTAP verhindert `autosupport`, dass Sie das Konto ändern oder löschen. ONTAP hindert Sie auch daran, die `autosupport` Rolle anderen Benutzerkonten zuzuweisen.

Verwandte Informationen

- "Sicherheitsanmeldung"
- "Einstellen"
- "Datenmenge"
- "vserver Services ndmp"

Vordefinierte Rollen für ONTAP SVM-Administratoren

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

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

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

Vsadmin-Volume	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Verwalten von Volumes, außer Verschieben von Volumes • Managen von Kontingenten, qtrees, Snapshots und Dateien • Verwalten von LUNs • Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Dienste konfigurieren: DNS, LDAP und NIS • Monitoring der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
Vsadmin-Protokoll	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Konfiguration von Protokollen: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP • Dienste konfigurieren: DNS, LDAP und NIS • Verwalten von LUNs • Monitoring der Netzwerkschnittstelle • Monitoring des Systemzustands der SVM
Vsadmin-Backup	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Verwalten des NDMP-Betriebs • Erstellung eines wiederhergestellten Lese-/Schreibvorgangs eines Volumes • Verwalten von SnapMirror Beziehungen und Snapshots • Anzeigen von Volumes und Netzwerkinformationen

Vsadmin-snaplock	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Verwalten von Volumes, außer Verschieben von Volumes • Managen von Kontingenten, qtrees, Snapshots und Dateien • Durchführung von SnapLock-Vorgängen einschließlich privilegierter Löschung • Konfiguration von Protokollen: NFS und SMB • Dienste konfigurieren: DNS, LDAP und NIS • Überwachen von Jobs • Monitoring von Netzwerkverbindungen und Netzwerkschnittstelle
Vsadmin-Readonly	• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen • Monitoring des Systemzustands der SVM • Monitoring der Netzwerkschnittstelle • Anzeigen von Volumes und LUNs • Anzeigen von Services und Protokollen

Managen Sie den Zugriff auf ONTAP Administratoren mit System Manager

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

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

- Einem lokalen Konto einen öffentlichen Schlüssel zuordnen.
- Installieren Sie ein digitales Zertifikat für einen CA-signierten Server.
- Konfiguration des AD-, LDAP- oder NIS-Zugriffs

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

Zuweisen einer Rolle zu einem Administrator

Weisen Sie einem Administrator eine Rolle wie folgt zu:

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie → neben **Users and Roles** aus.

3. Wählen Sie + Add unter **Users** aus.
4. Geben Sie einen Benutzernamen an, und wählen Sie im Dropdown-Menü für **Role** eine Rolle aus.
5. Geben Sie eine Anmeldemethode und ein Kennwort für den Benutzer an.

Ändern der Administratorrolle

Ändern Sie die Rolle für einen Administrator wie folgt:

Schritte

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

Zugriff auf JIT-Berechtigungserhöhung in ONTAP

Ab ONTAP 9.17.1 können Cluster-Administratoren "Konfigurieren Sie die Just-in-Time-Berechtigungserweiterung (JIT)." Damit können ONTAP -Benutzer ihre Berechtigungen vorübergehend erweitern, um bestimmte Aufgaben auszuführen. Wenn JIT für einen Benutzer konfiguriert ist, kann dieser seine Berechtigungen vorübergehend auf eine Rolle erweitern, die über die erforderlichen Berechtigungen zur Ausführung einer Aufgabe verfügt. Nach Ablauf der Sitzung kehrt der Benutzer zu seiner ursprünglichen Zugriffsebene zurück.

Clusteradministratoren können die Dauer konfigurieren, für die ein Benutzer auf JIT-Rechteerweiterungen zugreifen kann. Beispielsweise können Clusteradministratoren den Benutzerzugriff auf JIT-Rechteerweiterungen mit einem Limit von 30 Minuten pro Sitzung (der Sitzungsgültigkeitsdauer) für einen Zeitraum von 30 Tagen (der JIT-Gültigkeitsdauer) konfigurieren. Während dieses 30-tägigen Zeitraums kann der Benutzer seine Rechte beliebig oft erweitern, die Sitzungsdauer ist jedoch auf 30 Minuten begrenzt.

Über diese Aufgabe

- Die JIT-Berechtigungserweiterung ist nur für Benutzer verfügbar, die per SSH auf ONTAP zugreifen. Die Berechtigungserweiterung ist nur innerhalb der aktuellen SSH-Sitzung verfügbar. Sie können die Berechtigungserweiterung jedoch innerhalb beliebig vieler gleichzeitiger SSH-Sitzungen erweitern.
- Die JIT-Berechtigungserhöhung wird nur für Benutzer unterstützt, die sich per Kennwort, NSSwitch oder Domänenauthentifizierung anmelden. Die Multi-Faktor-Authentifizierung (MFA) wird für die JIT-Berechtigungserhöhung nicht unterstützt.
- Die JIT-Sitzung eines Benutzers wird beendet, wenn die konfigurierte Sitzungs- oder JIT-Gültigkeitsdauer abläuft oder wenn ein Cluster-Administrator den JIT-Zugriff für den Benutzer widerruft.

Bevor Sie beginnen

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

Schritte

1. Erhöhen Sie vorübergehend Ihre Berechtigungen auf die konfigurierte Rolle:

```
security jit-privilege elevate
```

Nach Eingabe dieses Befehls werden Sie aufgefordert, Ihr Anmeldekennwort einzugeben. Wenn für Ihr Konto JIT-Zugriff konfiguriert ist, erhalten Sie für die konfigurierte Sitzungsdauer erweiterte Zugriffsrechte. Nach Ablauf der Sitzungsdauer kehren Sie zu Ihrer ursprünglichen Zugriffsebene zurück. Sie können Ihre Berechtigungen innerhalb der konfigurierten JIT-Gültigkeitsdauer beliebig oft erhöhen.

2. Zeigen Sie die verbleibende Zeit Ihrer JIT-Sitzung an:

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

Wenn Sie sich derzeit 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
```

Wenn Sie sich derzeit in einer JIT-Sitzung befinden, beendet dieser Befehl die JIT-Sitzung und stellt Ihre ursprüngliche Zugriffsebene wieder her.

Konfigurieren der JIT-Berechtigungserhöhung in ONTAP

Ab ONTAP 9.17.1 können Clusteradministratoren Just-in-Time (JIT)-Berechtigungserhöhungen konfigurieren, um ONTAP Benutzern die vorübergehende Erhöhung ihrer Berechtigungen für bestimmte Aufgaben zu ermöglichen. Wenn JIT für einen Benutzer konfiguriert ist, kann dieser vorübergehend "ihre Privilegien erhöhen" einer Rolle, die über die erforderlichen Berechtigungen zum Ausführen einer Aufgabe verfügt. Nach Ablauf der Sitzungsdauer kehrt der Benutzer zu seiner ursprünglichen Zugriffsebene zurück.

Clusteradministratoren können die Dauer konfigurieren, für die ein Benutzer auf JIT-Rechteerweiterungen zugreifen kann. Beispielsweise können Sie den JIT-Rechtezugriff mit einem Sitzungslimit von 30 Minuten (Sitzungsgültigkeitsdauer) für einen Zeitraum von 30 Tagen (JIT-Gültigkeitsdauer) konfigurieren. Während dieses 30-tägigen Zeitraums kann der Benutzer seine Rechte beliebig oft erweitern, die Sitzungsdauer ist jedoch auf 30 Minuten begrenzt.

Die JIT-Berechtigungserweiterung unterstützt das Prinzip der geringsten Rechte und ermöglicht Benutzern die Ausführung von Aufgaben, die erhöhte Rechte erfordern, ohne ihnen diese Rechte dauerhaft zu gewähren. Dies reduziert das Risiko unbefugten Zugriffs oder versehentlicher Änderungen am System. Die folgenden Beispiele beschreiben einige gängige Anwendungsfälle für die JIT-Berechtigungserweiterung:

- Erlauben Sie vorübergehenden Zugriff auf die `security login create` Und `security login delete` Befehle zum Aktivieren des Onboardings und Offboardings von Benutzern.
- Erlauben Sie vorübergehenden Zugriff auf `system node image update` Und `system node upgrade-revert` während eines Update-Fensters. Nach Abschluss des Updates wird der Befehlszugriff widerrufen.

- Erlauben Sie vorübergehenden Zugriff auf `cluster add-node` , `cluster remove-node` , Und `cluster modify` um die Clustererweiterung oder -neukonfiguration zu ermöglichen. Sobald die Clusteränderungen abgeschlossen sind, wird der Befehlszugriff widerrufen.
- Erlauben Sie vorübergehenden Zugriff auf `volume snapshot restore` um Wiederherstellungsvorgänge und die Verwaltung von Sicherungszielen zu ermöglichen. Sobald die Wiederherstellung oder Konfiguration abgeschlossen ist, wird der Befehlszugriff widerrufen.
- Erlauben Sie vorübergehenden Zugriff auf `security audit log show` um die Überprüfung und den Export des Prüfprotokolls während einer Konformitätsprüfung zu ermöglichen.

finden Sie unter Gängige JIT-Anwendungsfälle .

Clusteradministratoren können JIT-Zugriff für ONTAP -Benutzer einrichten und die standardmäßigen JIT-Gültigkeitszeiträume entweder global im gesamten Cluster oder für bestimmte SVMs konfigurieren.

Über diese Aufgabe

- Die JIT-Berechtigungserweiterung ist nur für Benutzer verfügbar, die per SSH auf ONTAP zugreifen. Erhöhte Berechtigungen sind nur innerhalb der aktuellen SSH-Sitzung des Benutzers verfügbar, können aber innerhalb beliebig vieler gleichzeitiger SSH-Sitzungen erhöht werden.
- Die JIT-Berechtigungserhöhung wird nur für Benutzer unterstützt, die sich per Kennwort, NSSwitch oder Domänenauthentifizierung anmelden. Die Multi-Faktor-Authentifizierung (MFA) wird für die JIT-Berechtigungserhöhung nicht unterstützt.

Bevor Sie beginnen

- Sie müssen ein ONTAP Clusteradministrator auf der `admin` Berechtigungsstufe zum Ausführen der folgenden Aufgaben.

Ändern der globalen JIT-Einstellungen

Sie können die JIT-Standardeinstellungen global im gesamten ONTAP Cluster oder für eine bestimmte SVM ändern. Diese Einstellungen bestimmen die Standardgültigkeitsdauer der Sitzung und die maximale JIT-Gültigkeitsdauer für Benutzer, die für den JIT-Zugriff konfiguriert sind.

Über diese Aufgabe

- Die Standardeinstellung `default-session-validity-period` Der maximale Wert beträgt eine Stunde. Diese Einstellung bestimmt, wie lange ein Benutzer in einer JIT-Sitzung auf erhöhte Berechtigungen zugreifen kann, bevor er diese erneut erhöhen muss.
- Die Standardeinstellung `max-jit-validity-period` Der Wert beträgt 90 Tage. Diese Einstellung bestimmt den maximalen Zeitraum, in dem ein Benutzer nach dem konfigurierten Startdatum auf JIT-Erweiterungen zugreifen kann. Sie können die JIT-Gültigkeitsdauer für einzelne Benutzer konfigurieren, sie darf jedoch die maximale JIT-Gültigkeitsdauer nicht überschreiten.

Schritte

1. Überprüfen Sie die aktuellen JIT-Einstellungen:

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

   `-vserver` ist optional. Wenn Sie keine SVM angeben, zeigt der Befehl die globalen JIT-Einstellungen an.

2. Ändern Sie die JIT-Einstellungen global oder für eine SVM:

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

Wenn Sie keine SVM angeben, ändert der Befehl die globalen JIT-Einstellungen. Im folgenden Beispiel wird die Standarddauer einer JIT-Sitzung auf 45 Minuten und die maximale JIT-Dauer auf 30 Tage für SVM festgelegt. `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-Erhöhung zugreifen und JIT-Sitzungen für maximal 30 Tage nach ihrem konfigurierten Startdatum initiieren.

Konfigurieren des JIT-Berechtigungserweiterungszugriffs für einen Benutzer

Sie können ONTAP Benutzern erweiterte JIT-Berechtigungen zuweisen.

Schritte

1. Überprüfen Sie den aktuellen JIT-Zugriff für einen Benutzer:

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

`-username` ist optional. Wenn Sie keinen Benutzernamen angeben, zeigt der Befehl den JIT-Zugriff für alle Benutzer an.

2. Weisen Sie einem Benutzer neuen JIT-Zugriff zu:

```
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 Clusterebene zugewiesen.
   - `-role` ist die RBAC-Rolle, auf die der Benutzer hochgestuft wird. Wenn nicht angegeben, `-role` standardmäßig `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. Wenn nicht angegeben, wird die globale oder SVM `default-session-validity-period` verwendet wird.
   - `-jit-validity-period` ist die maximale Dauer, für die ein Benutzer JIT-Sitzungen nach dem konfigurierten Startdatum initiieren kann. Wenn nicht angegeben, `session-validity-period` verwendet wird. Dieser Parameter darf den globalen oder SVM-Wert nicht überschreiten. `max-jit-validity-period` .
   - `-start-time` ist das Datum und die Uhrzeit, ab denen der Benutzer JIT-Sitzungen starten kann. Wenn nicht angegeben, werden das aktuelle Datum und die aktuelle Uhrzeit verwendet.

     Das folgende Beispiel ermöglicht `ontap_user` für den Zugriff auf die `admin` Rolle für 1 Stunde, bevor eine neue JIT-Sitzung gestartet werden muss. `ontap_user` können ab 13:00 Uhr am 1. Juli 2025 JIT-

Sitzungen für einen Zeitraum von 60 Tagen einleiten:
`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. Widerrufen Sie bei Bedarf den JIT-Zugriff eines Benutzers:

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

Dieser Befehl widerruft den JIT-Zugriff eines Benutzers, auch wenn dieser noch nicht abgelaufen ist. Wenn `-vserver` Wenn kein Wert angegeben ist, wird der JIT-Zugriff auf Clusterebene widerrufen. Befindet sich der Benutzer in einer aktiven JIT-Sitzung, wird diese beendet.

Gängige JIT-Anwendungsfälle

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

Anwendungsfall	Befehle	Details
Benutzer- und Rollenverwaltung	• `security login create` • `security login delete`	Erhöhen Sie vorübergehend die Berechtigungen, um während des Onboardings oder Offboardings Benutzer hinzuzufügen/zu entfernen oder Rollen zu ändern.
Zertifikatsverwaltung	• `security certificate create` • `security certificate install`	Gewähren Sie kurzfristigen Zugriff für die Installation oder Erneuerung von Zertifikaten.
SSH/CLI-Zugriffskontrolle	• `security login create -application ssh`	Gewähren Sie vorübergehend SSH-Zugriff zur Fehlerbehebung oder für den Anbietersupport.
Lizenzmanagement	• `system license add` • `system license delete`	Gewähren Sie Rechte zum Hinzufügen oder Entfernen von Lizenzen während der Aktivierung oder Deaktivierung von Funktionen.
System-Upgrades und Patches	• `system node image update` • `system node upgrade-revert`	Erhöhen Sie die Berechtigung für das Upgrade-Fenster und widerrufen Sie sie dann.

Anwendungsfall	Befehle	Details
Netzwerksicherheitseinstellungen	• `security login role create` • `security login role modify`	Erlauben Sie vorübergehende Änderungen an netzwerkbezogenen Sicherheitsrollen.
Clusterverwaltung	• `cluster add-node` • `cluster remove-node` • `cluster modify`	Erhöhen Sie die Anzahl für die Clustererweiterung oder -neukonfiguration.
SVM-Verwaltung	• `vserver create` • `vserver delete` • `vserver modify`	Gewähren Sie einer SVM vorübergehend Administratorrechte für die Bereitstellung oder Außerbetriebnahme.
Volumenverwaltung	• `volume create` • `volume delete` • `volume modify`	Erhöhen Sie die Berechtigungen für die Bereitstellung, Größenänderung oder Entfernung von Volumes.
Snapshot-Verwaltung	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	Erhöhen Sie die Berechtigungen zum Löschen oder Wiederherstellen von Snapshots während der Wiederherstellung.
Netzwerkkonfiguration	• `network interface create` • `network port vlan create`	Gewähren Sie Rechte für Netzwerkänderungen während Wartungsfenstern.
Festplatten-/Aggregatverwaltung	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	Erhöhen Sie die Berechtigungen zum Hinzufügen oder Entfernen von Datenträgern oder zum Verwalten von Aggregaten.
Datensicherung	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	Vorübergehend erhöhen, um SnapMirror -Beziehungen zu konfigurieren oder wiederherzustellen.

Anwendungsfall	Befehle	Details
Leistungsoptimierung	• `qos policy-group create` • `qos policy-group modify`	Erhöhen Sie die Leistung zur Fehlerbehebung oder Optimierung.
Zugriff auf das Überwachungsprotokoll	• `security audit log show`	Erhöhen Sie die Berechtigungen vorübergehend für die Überprüfung oder den Export des Überwachungsprotokolls während Compliance-Prüfungen.
Ereignis- und Alarmverwaltung	• `event notification create` • `event notification modify`	Erhöhen Sie die Berechtigungen zum Konfigurieren oder Testen von Ereignisbenachrichtigungen oder SNMP-Traps.
Compliance-gesteuerter Datenzugriff	• `volume show` • `security audit log show`	Gewähren Sie Prüfern vorübergehend schreibgeschützten Zugriff, damit sie vertrauliche Daten oder Protokolle überprüfen können.
Überprüfungen des privilegierten Zugriffs	• `security login show` • `security login role show`	Erhöhen Sie vorübergehend die Berechtigungen, um privilegierten Zugriff zu überprüfen und darüber zu berichten. Gewähren Sie für begrenzte Zeit schreibgeschützten, erhöhten Zugriff.

Verwandte Informationen

- "Cluster"
- "Ereignisbenachrichtigung"
- "Netzwerk"
- "QoS-Richtliniengruppe"
- "Sicherheit"
- "snapmirror"
- "Lagerung"
- "System"
- "Datenmenge"
- "vserver"

Verwalten von Administratorkonten

Erfahren Sie mehr über das Managen von ONTAP-Administratorkonten

Je nachdem, wie Sie den Kontozugriff aktiviert haben, müssen Sie möglicherweise einen öffentlichen Schlüssel mit einem lokalen Konto verknüpfen, ein digitales Zertifikat für einen CA-signierten Server installieren oder AD-, LDAP- oder NIS-Zugriff konfigurieren.

Sie können alle diese Aufgaben vor oder nach der Aktivierung des Kontozugriffs ausführen.

Verknüpfen Sie einen öffentlichen Schlüssel mit einem ONTAP-Administratorkonto

Bei der SSH-Authentifizierung für den öffentlichen Schlüssel müssen Sie den öffentlichen Schlüssel einem Administratorkonto zuweisen, bevor das Konto auf die SVM zugreifen kann. Mit dem `security login publickey create` Befehl können Sie einen Schlüssel mit einem Administratorkonto verknüpfen.

Über diese Aufgabe

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

Bevor Sie beginnen

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

Schritte

1. Einen öffentlichen Schlüssel einem Administratorkonto zuordnen:

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

   Erfahren Sie mehr über `security login publickey create` in der "ONTAP-Befehlsreferenz".

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

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

   Erfahren Sie mehr über `security login publickey show` in der "ONTAP-Befehlsreferenz".

Beispiel

Mit dem folgenden Befehl wird ein öffentlicher Schlüssel mit dem SVM-Administratorkonto `svmadmin1` für die SVM verknüpft `engData1`. Der öffentliche Schlüssel wird mit der Indexnummer 5 belegt.

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

Verwalten von öffentlichen SSH-Schlüsseln und X.509-Zertifikaten für ONTAP-Administratoren

Um die SSH-Authentifizierungssicherheit mit Administratorkonten zu erhöhen, können Sie `security login publickey` den öffentlichen SSH-Schlüssel und seine Zuordnung zu X.509-Zertifikaten mit dem Befehlssatz verwalten.

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

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

Über diese Aufgabe

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

Bevor Sie beginnen

- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Sie müssen den SSH-Schlüssel generiert haben.
- Wenn Sie nur das X.509-Zertifikat auf Gültigkeit prüfen müssen, können Sie ein selbstsigniertes Zertifikat verwenden.
- Wenn Sie das X.509-Zertifikat auf Ablaufdatum und Widerruf prüfen müssen:
  - Sie müssen das Zertifikat von einer Zertifizierungsstelle erhalten haben.
  - Sie müssen die Zertifikatskette (Zwischen- und Stammzertifizierungsstellen) mithilfe von `security certificate install` Befehlen installieren. Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".
  - Sie müssen OCSP für SSH aktivieren. Anweisungen hierzu finden Sie unter "Überprüfen Sie, ob digitale Zertifikate mit OCSP gültig sind" .

Schritte

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

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

   Erfahren Sie mehr über `security login publickey create` in der "ONTAP-Befehlsreferenz".

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

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

   Erfahren Sie mehr über `security login publickey show` in der "ONTAP-Befehlsreferenz".

Beispiel

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

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

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

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

Bevor Sie beginnen

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

Schritte

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

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

   Erfahren Sie mehr über `security login publickey modify` in der "ONTAP-Befehlsreferenz".

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

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

Beispiel

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

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

Entfernen Sie den öffentlichen Schlüssel und die Zertifikatzuordnung aus einem Administratorkonto

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

Bevor Sie beginnen

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

Schritte

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

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

Erfahren Sie mehr über `security login publickey delete` in der "ONTAP-Befehlsreferenz".

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

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

Beispiel

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

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

Verwandte Informationen

- "Sicherheits-Login-Publickey"

Konfigurieren Sie Cisco Duo 2FA für ONTAP-SSH-Anmeldungen

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

Wenn Sie die Duo-Authentifizierung für SSH-Anmeldungen aktivieren, müssen Benutzer ein Gerät registrieren, wenn sie sich das nächste Mal über SSH anmelden. Informationen zur Anmeldung finden Sie im Cisco Duo "Dokumentation der Anmeldung".

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

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

Konfigurieren Sie Cisco Duo

Sie können mit dem `security login duo create` Befehl eine Cisco Duo-Konfiguration für das gesamte Cluster oder für eine bestimmte Storage-VM (in der ONTAP-CLI als vServer bezeichnet) erstellen. Wenn Sie dies tun, ist Cisco Duo für SSH-Anmeldungen für dieses Cluster oder diese Storage-VM aktiviert. Erfahren Sie mehr über `security login duo create` in der "ONTAP-Befehlsreferenz".

Schritte

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

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

Ändern Sie die Cisco Duo-Konfiguration

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

Schritte

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

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

Entfernen Sie die Cisco Duo-Konfiguration

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

Schritte

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

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

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

Cisco Duo-Konfiguration anzeigen

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

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Zeigen Sie die Cisco Duo-Konfiguration für diese Storage-VM. Optional können Sie mit dem `vserver` Parameter eine Storage-VM angeben und den Namen der Storage-VM ersetzen für `<STORAGE_VM_NAME>`:

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

   Sie sollten eine Ausgabe wie die folgende sehen:

```
Vserver: testcluster
Enabled: true

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

Erstellen Sie eine Duo-Gruppe

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

Schritte

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

```
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 Sie mit dem optionalen `-excluded-users` Parameter angeben, werden nicht in den Duo-Authentifizierungsprozess einbezogen.

Zeigen Sie Duo-Gruppen an

Sie können vorhandene Cisco Duo-Gruppeneinträge mit dem `security login duo group show` Befehl anzeigen. Erfahren Sie mehr über `security login duo group show` in der "ONTAP-Befehlsreferenz".

Schritte

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

Gruppe auf Cluster-Ebene angezeigt:

```
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 Sie mit dem optionalen `-excluded-users` Parameter angeben, werden nicht angezeigt.

Entfernen Sie eine Duo-Gruppe

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

Schritte

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

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

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

Umgehen Sie die Duo-Authentifizierung für Benutzer

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

Alle Duo-Benutzer ausschließen

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

Schritte

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

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

Benutzer der Duo-Gruppe ausschließen

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

Schritte

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

```
security login 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 Sie mit dem `-excluded-users` Parameter angeben, werden nicht in den Duo-Authentifizierungsprozess einbezogen.

Erfahren Sie mehr über `security login duo group modify` in der "ONTAP-Befehlsreferenz".

Lokale Duo-Benutzer ausschließen

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

Erstellen und installieren Sie ein CA-signiertes Serverzertifikat in ONTAP

Auf Produktionssystemen ist es eine Best Practice, ein von CA signiertes digitales Zertifikat zur Authentifizierung des Clusters oder der SVM als SSL-Server zu installieren. Sie können mit dem `security certificate generate-csr` Befehl eine Zertifikatsignierungsanforderung (CSR) generieren und mit dem `security certificate install` Befehl das Zertifikat installieren, das Sie von der Zertifizierungsstelle zurückerhalten. Erfahren Sie mehr über `security certificate generate-csr` und `security certificate install` in der "ONTAP-Befehlsreferenz".

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

Mit dem `security certificate generate-csr` Befehl können Sie eine Zertifikatsignierungsanforderung (CSR) generieren. Nach Bearbeitung Ihrer Anfrage sendet Ihnen die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Bevor Sie beginnen

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

Schritte

1. CSR erstellen:

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

Mit dem folgenden Befehl wird ein CSR mit einem 2048-Bit privaten Schlüssel erstellt, der durch die Hashing-Funktion erzeugt `SHA256` wird, um von der Gruppe in der `IT` Abteilung eines Unternehmens verwendet `Software` zu werden, dessen benutzerdefinierter gemeinsamer Name `server1.companyname.com` in Sunnyvale, Kalifornien, USA liegt. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet `web@example.com`. Das System zeigt den CSR und den privaten Schlüssel in der Ausgabe an.

Beispiel für das Erstellen einer CSR

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

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<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. Kopieren Sie die Zertifikatsanforderung aus der CSR-Ausgabe, und senden Sie sie in elektronischer Form (z. B. E-Mail) an eine vertrauenswürdige Drittanbieter-CA zum Signieren.

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

Installieren Sie ein CA-signiertes Serverzertifikat

Sie können mit dem `security certificate install` Befehl ein CA-signiertes Serverzertifikat auf einer SVM installieren. ONTAP fordert Sie auf, die Stammzertifikate und Zwischenzertifikate der Zertifizierungsstelle (CA) anzugeben, die die Zertifikatskette des Serverzertifikats bilden. Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

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

Schritt

1. Installieren eines CA-signierten Serverzertifikats:

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

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

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

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

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

- "Sicherheitszertifikat generieren-csr"

Managen Sie ONTAP Zertifikate mit System Manager

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

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

Zeigen Sie Zertifikatinformationen an

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

Schritte

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

Nächste Schritte

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

Auf dieser Registerkarte…	Sie können folgende Verfahren durchführen…
• Vertrauenswürdige Zertifizierungsstellen*	• [install-trusted-cert] • Löschen einer vertrauenswürdigen Zertifizierungsstelle • Eine vertrauenswürdige Zertifizierungsstelle erneuern
Client/Server-Zertifikate	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]

Lokale Zertifikatbehörden	• Erstellen Sie eine neue lokale Zertifizierungsstelle • Unterzeichnen Sie ein Zertifikat mithilfe einer lokalen Zertifizierungsstelle • Lokale Zertifizierungsstelle löschen • Erneuern Sie eine lokale Zertifizierungsstelle

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

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

Schritte

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

Installieren Sie eine vertrauenswürdige Zertifizierungsstelle (Hinzufügen)

Sie können weitere vertrauenswürdige Zertifizierungsstellen in System Manager installieren.

Schritte

1. Öffnen Sie die Registerkarte * Trusted Certificate Authorities*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie 

.
3. Führen Sie im Fenster * Vertrauenswürdige Zertifizierungsstelle hinzufügen* folgende Schritte aus:
   - Geben Sie einen **Namen** ein.
   - Wählen Sie für den **Scope** eine Storage-VM aus.
   - Geben Sie einen **gemeinsamen Namen** ein.
   - Wählen Sie einen **Typ** aus.
   - Geben Sie **Zertifikatdetails** ein oder importieren Sie sie.

Löschen einer vertrauenswürdigen Zertifizierungsstelle

Mit System Manager können Sie eine vertrauenswürdige Zertifizierungsstelle löschen.

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

Schritte

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

Eine vertrauenswürdige Zertifizierungsstelle erneuern

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

Schritte

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

Installieren Sie ein Client-/Serverzertifikat (hinzufügen)

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

Schritte

1. Öffnen Sie die Registerkarte **Client/Server Certificates**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie + Add.
3. Führen Sie im Fenster **Client/Server-Zertifikat hinzufügen** folgende Schritte aus:
   - Geben Sie einen **Zertifikatnamen** ein.
   - Wählen Sie für den **Scope** eine Storage-VM aus.
   - Geben Sie einen **gemeinsamen Namen** ein.
   - Wählen Sie einen **Typ** aus.
   - Geben Sie **Zertifikatdetails** ein oder importieren Sie sie. Sie können entweder aus einer Textdatei die Zertifikatdetails einschreiben oder kopieren und einfügen oder den Text aus einer Zertifikatdatei importieren, indem Sie auf **Import** klicken.
   - Geben Sie den **privaten Schlüssel** ein. Sie können entweder aus einer Textdatei den privaten Schlüssel einschreiben oder kopieren und einfügen oder den Text aus einer privaten Schlüsseldatei importieren, indem Sie auf **Import** klicken.

Erstellen (Hinzufügen) eines selbstsignierten Client/Server-Zertifikats

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

Schritte

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

- Wählen Sie einen **Typ** aus.
- Wählen Sie eine **Hash-Funktion** aus.
- Wählen Sie eine * Tastengröße* aus.
- Wählen Sie eine **Storage-VM** aus.

Löschen Sie ein Client-/Serverzertifikat

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

Schritte

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

Erneuern eines Client-/Serverzertifikats

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

Schritte

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

Erstellen Sie eine neue lokale Zertifizierungsstelle

Mit System Manager können Sie eine neue lokale Zertifizierungsstelle erstellen.

Schritte

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

Unterzeichnen Sie ein Zertifikat mithilfe einer lokalen Zertifizierungsstelle

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

Schritte

1. Öffnen Sie die Registerkarte * Lokale Zertifikatbehörden*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der lokalen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Namen und dann **Zertifikat signieren**.

4. Füllen Sie das Formular **Signieren einer Zertifikatsignierungsanforderung** aus.
    - Sie können entweder den Inhalt der Zertifikatsignierung einfügen oder eine Zertifikatsignierungsanfragedatei importieren, indem Sie auf **Import** klicken.
    - Geben Sie die Anzahl der Tage an, für die das Zertifikat gültig sein soll.

Lokale Zertifizierungsstelle löschen

Mit System Manager können Sie eine lokale Zertifizierungsstelle löschen.

Schritte

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

Erneuern Sie eine lokale Zertifizierungsstelle

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

Schritte

1. Öffnen Sie die Registerkarte * Local Certificate Authority*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der lokalen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Namen, und klicken Sie dann auf **erneuern**.

Konfigurieren Sie den Zugriff auf den Active Directory-Domänencontroller in ONTAP

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

ONTAP unterstützt die folgenden Authentifizierungsservices für Domänencontroller:

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

ONTAP unterstützt die folgenden Sitzungsschlüsselalgorithmen für sichere Netlogon-Verbindungen:

Sitzungsschlüsselalgorithmus	Verfügbar ab…

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

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

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

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

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

Konfigurieren Sie einen Authentifizierungstunnel

Falls Sie bereits einen SMB-Server für eine Daten-SVM `security login domain-tunnel create` konfiguriert haben, können Sie die SVM mit dem Befehl als Gateway bzw. *Tunnel* für AD-Zugriff auf das Cluster konfigurieren.

Vor ONTAP 9.16.1 müssen Sie einen Authentifizierungstunnel verwenden, um Clusteradministratorkonten mit AD zu managen.

Bevor Sie beginnen

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

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

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

Schritte

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

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

Erfahren Sie mehr über `security login domain-tunnel create` in der "ONTAP-Befehlsreferenz".

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

Mit dem folgenden Befehl wird die Daten-SVM mit SMB-Aktivierung als Authentifizierungstunnel konfiguriert `engData`.

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

Erstellen Sie ein SVM-Computerkonto in der Domäne

Wenn Sie keinen SMB-Server für eine Daten-SVM konfiguriert haben, können Sie mit dem `vserver active-directory create` Befehl ein Computerkonto für die SVM in der Domäne erstellen.

Über diese Aufgabe

Nachdem Sie den `vserver active-directory create` Befehl eingegeben haben, werden Sie aufgefordert, die Anmeldeinformationen für ein AD-Benutzerkonto mit ausreichender Privileges anzugeben, um der angegebenen Organisationseinheit in der Domäne Computer hinzuzufügen. Das Passwort des Kontos darf nicht leer sein.

Ab ONTAP 9.16.1 können Sie dieses Verfahren verwenden, um Clusteradministratorkonten mit AD zu verwalten.

Bevor Sie beginnen

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

Schritte

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

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

Ab ONTAP 9.16.1 akzeptiert der `-vserver` Parameter die Admin-SVM. Erfahren Sie mehr über `vserver active-directory create` in der "ONTAP-Befehlsreferenz".

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

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

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

Enter the user name: Administrator

Enter the password:
```

Konfigurieren Sie den LDAP- oder NIS-Serverzugriff in ONTAP

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

Konfigurieren Sie den LDAP-Serverzugriff

Sie müssen den LDAP-Serverzugriff auf eine SVM konfigurieren, bevor LDAP-Konten auf die SVM zugreifen können. Sie können den `vserver services name-service ldap client create` Befehl verwenden, um eine LDAP-Client-Konfiguration auf der SVM zu erstellen. Mit dem `vserver services name-service ldap create` Befehl können Sie die LDAP-Client-Konfiguration der SVM zuordnen.

Über diese Aufgabe

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

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

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

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

Bevor Sie beginnen

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

Schritte

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

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

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

Erfahren Sie mehr über `vserver services name-service ldap client create` in der "ONTAP-Befehlsreferenz".

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

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

> Der `-ldap-servers` Feld ersetzt das `-servers` Feld. Sie können das `-ldap-servers` , um entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server anzugeben.

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

   Erfahren Sie mehr über `vserver services name-service ldap create` in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl ordnet die LDAP-Client-Konfiguration `corp` der SVM `engData`zu 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` Der Befehl führt eine automatische Konfigurationsvalidierung durch und meldet eine Fehlermeldung, wenn ONTAP den Nameserver nicht kontaktieren kann.

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

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

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

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

Sie können die `name service check` Befehl zum Überprüfen des Status der Nameserver.

Konfigurieren Sie den NIS-Serverzugriff

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

Bevor Sie beginnen

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

Schritt

1. Erstellen einer NIS-Domänenkonfiguration auf einer SVM:

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

   Erfahren Sie mehr über `vserver services name-service nis-domain create` in der "ONTAP-Befehlsreferenz".

   > Der `-nis-servers` Feld ersetzt das `-servers` Feld. Sie können das `-nis-servers` , um entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server anzugeben.

   Mit dem folgenden Befehl wird eine NIS-Domänenkonfiguration auf SVM erstellt `engData`. Die NIS-Domain `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
```

Erstellen Sie einen Namensdienstschalter

Mit der Namensdienst-Switch-Funktion können Sie LDAP oder NIS als alternative Namensdienstquellen verwenden. Sie können den `vserver services name-service ns-switch modify` Befehl verwenden, um die Reihenfolge für Namensdienstquellen festzulegen.

Bevor Sie beginnen

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

Schritt

1. Geben Sie die Suchreihenfolge für Namensdienstquellen an:

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

   Erfahren Sie mehr über `vserver services name-service ns-switch modify` in der "ONTAP-Befehlsreferenz".

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

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

Ändern Sie ein ONTAP-Administratorkennwort

Sie sollten Ihr Anfangspasswort sofort nach der ersten Anmeldung am System ändern. Als SVM-Administrator können Sie mit dem `security login password` Befehl Ihr eigenes Passwort ändern. Als Cluster-Administrator können Sie mit dem `security login password` Befehl das Administratorpasswort ändern.

Über diese Aufgabe

Das neue Passwort muss folgende Bedingungen erfüllen:

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

> Mit dem `security login role config modify` Befehl können Sie die Passwortregeln für Konten ändern, die einer bestimmten Rolle zugeordnet sind.

Bevor Sie beginnen

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

Schritt

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

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

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

Verwandte Informationen

- "Sicherheits-Login-Rollenkonfiguration ändern"
- "Sicherheits-Login-Passwort"

Sperren und Entsperren eines ONTAP-Administratorkontos

Mit dem `security login lock` Befehl können Sie ein Administratorkonto sperren und mit dem `security login unlock` Befehl das Konto entsperren.

Bevor Sie beginnen

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

Schritte

1. Administratorkonto sperren:

   `security login lock -vserver SVM_name -username user_name`

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

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

   Erfahren Sie mehr über `security login lock` in der "ONTAP-Befehlsreferenz".

2. Administratorkonto entsperren:

   `security login unlock -vserver SVM_name -username user_name`

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

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

   Erfahren Sie mehr über `security login unlock` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Sicherheitsanmeldung"

Fehlgeschlagene Anmeldeversuche in ONTAP verwalten

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

Wie Sie wissen, dass Anmeldeversuche fehlgeschlagen sind

Das Event Management System (EMS) informiert Sie jede Stunde über fehlgeschlagene Anmeldeversuche. In der `audit.log` Datei finden Sie einen Datensatz mit fehlgeschlagenen Anmeldeversuchen.

Was tun, wenn wiederholte Anmeldeversuche fehlschlagen

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

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

Sie können die `security login role config modify` folgenden Aufgaben mit dem Befehl ausführen. Erfahren Sie mehr über `security login role config modify` in der "ONTAP-Befehlsreferenz".

Langfristig können Sie die folgenden zusätzlichen Schritte einleiten:

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

SHA-2 auf ONTAP-Administratorkontokennwörtern erzwingen

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

Über diese Aufgabe

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

- Zeigt Benutzerkonten an, die mit der angegebenen Hash-Funktion übereinstimmen.
- Verfallen von Konten, die eine angegebene Hash-Funktion verwenden (z. B. MD5), sodass die Benutzer ihre Passwörter bei der nächsten Anmeldung ändern müssen.
- Konten sperren, deren Passwörter die angegebene Hash-Funktion verwenden.
- Wenn Sie auf eine Version vor ONTAP 9 zurücksetzen, setzen Sie das Kennwort des Clusteradministrators zurück, damit es mit der Hash-Funktion (MD5) kompatibel ist, die von der früheren Version unterstützt wird.

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

Schritte

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

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

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

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

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

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

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

Verwandte Informationen

- "Sicherheits-Login-Passwortablauf"
- "Sicherheits-Login entsperren"

Diagnostizieren und korrigieren Sie Probleme mit dem ONTAP-Dateizugriff mit System Manager

Ab ONTAP 9.8 können Sie Probleme mit dem Dateizugriff nachverfolgen und anzeigen.

Schritte

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

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

6. Klicken Sie in der linken Spalte der Ergebnistabelle auf ⌄ , um die Zugriffsrechte für die Datei

anzuzeigen.

Management der Verifizierung von mehreren Administratoren

Informieren Sie sich über die Verifizierung durch mehrere ONTAP Administratoren

Ab ONTAP 9.11.1 können Sie mithilfe von MAV (Multi-Admin Verification) sicherstellen, dass bestimmte Vorgänge, wie das Löschen von Volumes oder Snapshots, nur nach Genehmigungen von designierten Administratoren ausgeführt werden können. So werden gefährdete, böswillige oder unerfahrene Administratoren daran gehindert, unerwünschte Änderungen vorzunehmen oder Daten zu löschen.

Die Konfiguration der Prüfung für mehrere Administratoren umfasst:

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

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

Wenn die Verifizierung mehrerer Administratoren aktiviert ist, sind für jeden geschützten Vorgang folgende Schritte erforderlich:

1. Wenn ein Benutzer den Vorgang initiiert, wird ein angezeigt "Die Anforderung wird generiert."
2. Bevor der Vorgang ausgeführt werden kann, muss mindestens einer ausgeführt werden "MAV-Administrator muss genehmigen."
3. Nach der Genehmigung wird der Benutzer aufgefordert und schließt den Vorgang ab.

> Wenn Sie die Multi-Admin-Verifizierungsfunktion ohne MAV-Administratorgenehmigung deaktivieren müssen, wenden Sie sich an den NetApp -Support und erwähnen Sie Folgendes"NetApp Knowledge Base: So deaktivieren Sie die Multi-Admin-Verifizierung, wenn der MAV-Admin nicht verfügbar ist" .

Die Überprüfung durch mehrere Administratoren ist nicht für Volumes oder Workflows gedacht, die mit hoher Automatisierung arbeiten, da jede automatisierte Aufgabe vor Abschluss des Vorgangs eine Genehmigung erfordert. Wenn Sie Automatisierung und MAV gemeinsam nutzen möchten, sollten Sie Abfragen für bestimmte MAV-Vorgänge verwenden. Beispielsweise können Sie `volume delete` MAV-Regeln nur auf Volumes anwenden, auf denen keine Automatisierung involviert ist. Sie können diese Volumes einem bestimmten Namensschema zuweisen.

> Die Verifizierung mehrerer Administratoren ist bei Cloud Volumes ONTAP nicht verfügbar.

Funktionsweise der Multiadmin-Überprüfung

Die Überprüfung durch mehrere Administratoren umfasst:

- Eine Gruppe von einem oder mehreren Administratoren mit Genehmigung und Veto-Befugnissen.
- Eine Reihe von geschützten Operationen oder Befehlen in einer Tabelle *rules*.

- Eine *rules Engine* zur Identifizierung und Steuerung der Ausführung geschützter Vorgänge.

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

Systemdefinierte Regeln

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

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

  Steuert die Konfiguration der Verifizierungsfunktion für mehrere Administratoren.

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

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

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

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

- `security multi-admin-verify request` Betrieb

  Kontrollieren Sie den Genehmigungsprozess.

Regelgeschützte Befehle

Zusätzlich zu den systemdefinierten Vorgängen sind die folgenden Befehle standardmäßig geschützt, wenn die Multi-Admin-Verifizierung aktiviert ist. Sie können die Regeln jedoch ändern, um den Schutz für diese Befehle aufzuheben:

- "Sicherheits-Login-Passwort"
- "Sicherheits-Login entsperren"
- "Einstellen"

Jede ONTAP Version bietet mehr Befehle, die Sie durch Verifizierungsregeln für mehrere Administratoren schützen können. Wählen Sie Ihre ONTAP-Version aus, um eine vollständige Liste der zum Schutz verfügbaren Befehle zu erhalten.

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

*Dieser Befehl ist nur mit CLI verfügbar und in einigen Versionen für System Manager nicht verfügbar.

Funktionsweise der Multi-Admin-Genehmigung

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

Sie können Folgendes konfigurieren:

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

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

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

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

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

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

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

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

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

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

Wenn sich der Anforderer in derselben Genehmigungsgruppe für den Vorgang befindet, wird er eine E-Mail

erhalten, wenn seine Anfrage genehmigt wird.

> Ein Anforderer kann seine eigenen Anfragen nicht genehmigen, selbst wenn er sich in der Genehmigungsgruppe befindet (obwohl er E-Mail-Benachrichtigungen für seine eigenen Anfragen erhalten kann). Anfragesteller, die sich nicht in Genehmigungsgruppen befinden (d. h. nicht MAV-Administratoren), erhalten keine E-Mail-Benachrichtigungen.

Funktionsweise der geschützten Operation

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

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

MAV-Regeln werden ausgewertet, bevor der geschützte Vorgang ausgeführt wird. Das bedeutet, dass Regeln basierend auf dem aktuellen Systemzustand durchgesetzt werden. Wenn beispielsweise eine MAV-Regel erstellt wird für `volume modify` mit einer Abfrage von `-size 5GB` , mit `volume modify` Für die Größenänderung eines 5-GB-Volumes auf 2 GB ist eine MAV-Genehmigung erforderlich, für die Größenänderung eines 2-GB-Volumes auf 5 GB jedoch nicht.

Verwandte Informationen

- "Cluster"
- "lun"
- "Sicherheit"
- "Snaplock Legal-Hold-Ende"
- "Speicheraggregat"
- "Storage-Verschlüsselung"
- "System"

Management von ONTAP-Administratorgenehmigungsgruppen für MAV

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

Über diese Aufgabe

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

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

Sie können MAV so konfigurieren, dass MAV-Administratoren darauf aufmerksam gemacht werden, dass Genehmigungsanforderungen ausstehen. Dazu müssen Sie E-Mail-Benachrichtigungen konfigurieren -

insbesondere die `Mail From` `Mail Server` Parameter und - oder Sie können diese Parameter löschen, um die Benachrichtigung zu deaktivieren. Ohne E-Mail-Warnmeldungen müssen MAV-Administratoren die Genehmigungswarteschlange manuell prüfen.

Ab ONTAP 9.15.1 können Sie Active Directory (AD)-Benutzer als MAV-Administratoren konfigurieren. Der AD-Benutzer muss"als ONTAP -Administrator konfiguriert" .

System Manager Verfahren

Wenn Sie zum ersten Mal eine MAV-Genehmigungsgruppe erstellen möchten, finden Sie weitere Informationen im System Manager-Verfahren bis "Aktivieren Sie die Verifizierung für mehrere Administratoren."

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

1. Identifizieren Sie die Administratoren, die eine Überprüfung durch mehrere Administratoren erhalten.
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie neben **Users and Roles.** auf →
   c. Klicken Sie + Add unter **Benutzer.**
   d. Ändern Sie den Dienstplan nach Bedarf.

      Weitere Informationen finden Sie unter "Kontrolle des Administratorzugriffs"
2. Erstellen oder Ändern der MAV-Genehmigungsgruppe:
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie → im Abschnitt **Sicherheit** neben **Multi-Admin Approval**. (Das Symbol wird angezeigt ⚙ , wenn MAV noch nicht konfiguriert ist.)
      - Name: Geben Sie einen Gruppennamen ein.
      - Genehmiger: Wählen Sie Genehmiger aus einer Benutzerliste aus.
      - E-Mail-Adresse: E-Mail-Adresse(n) eingeben.
      - Standardgruppe: Wählen Sie eine Gruppe aus.

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

CLI-Verfahren

1. Stellen Sie sicher, dass für die `Mail From` `Mail Server` Parameter und Werte festgelegt wurden. Geben Sie Ein:

   ```
   event config show
   ```

   Die Anzeige sollte wie folgt lauten:

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

Um diese Parameter zu konfigurieren, geben Sie Folgendes ein:

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

Erfahren Sie mehr über `event config show` und `event config modify` in der "ONTAP-Befehlsreferenz".

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

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

Erfahren Sie mehr über `security login show`, `security login modify` und `security login create` in der "ONTAP-Befehlsreferenz".

3. Erstellen Sie die MAV-Genehmigungsgruppe:

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

   - `-vserver` - Nur die Admin-SVM wird in dieser Version unterstützt.
   - `-name` - Der MAV-Gruppenname, bis zu 64 Zeichen.
   - `-approvers`– Die Liste eines oder mehrerer Genehmiger. Für AD-Benutzer verwenden Sie das Format `domain\user` . Beispiel: `mydomain\pavan` .
   - `-email` - Eine oder mehrere E-Mail-Adressen, die benachrichtigt werden, wenn eine Anfrage erstellt, genehmigt, Veto eingelegt oder ausgeführt wird.

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

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

4. Gruppenerstellung und -Mitgliedschaft überprüfen:

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

   Beispiel:

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

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

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

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

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Aktiviert oder deaktiviert die Multi-Admin-Verifizierung in ONTAP

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

Über diese Aufgabe

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

> Wenn Sie die Multi-Admin-Verifizierungsfunktion ohne MAV-Administratorgenehmigung deaktivieren müssen, wenden Sie sich an den NetApp -Support und erwähnen Sie Folgendes"NetApp Knowledge Base: So deaktivieren Sie die Multi-Admin-Verifizierung, wenn der MAV-Admin nicht verfügbar ist" .

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

Genehmigungsgruppen

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

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

Erforderliche Genehmiger

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

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

Ablauf der Genehmigung (Stunden, Minuten, Sekunden)

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

Ausführungsablauf (Stunden, Minuten, Sekunden)

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

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

System Manager Verfahren

1. Identifizieren Sie die Administratoren, die eine Überprüfung durch mehrere Administratoren erhalten.
   a. Klicken Sie Auf **Cluster > Einstellungen.**
   b. Klicken Sie neben **Users and Roles.** auf →
   c. Klicken Sie + Add unter **Benutzer.**
   d. Ändern Sie den Dienstplan nach Bedarf.

      Weitere Informationen finden Sie unter "Kontrolle des Administratorzugriffs"

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

b. Klicken Sie im Abschnitt **Sicherheit** neben **Multi-Admin Approval**.

c. Klicken Sie auf + Add , um mindestens eine Genehmigungsgruppe hinzuzufügen.

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

d. Fügen Sie mindestens eine Regel hinzu.

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

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

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

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

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

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

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

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

So deaktivieren Sie die Multi-Admin-Verifizierung:

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

   Zum Abschluss dieses Vorgangs ist eine MAV-Genehmigung erforderlich.

CLI-Verfahren

Bevor die MAV-Funktionalität in der CLI aktiviert "MAV-Administratorgruppe"wird, muss mindestens eine erstellt worden sein.

Wenn Sie… wollen	Geben Sie diesen Befehl ein

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

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

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

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

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Managen Sie Verifizierungsregeln für mehrere Administratoren für geschützte Vorgänge in ONTAP

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

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

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

Sie können Regeln zum Schutz erstellen"Über diese Befehle". Sie können jeden Befehl schützen, beginnend mit der ONTAP-Version, in der Sicherungsfunktionen für den Befehl zum ersten Mal verfügbar sind.

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

Zusätzlich zu den systemdefinierten Vorgängen sind die folgenden Befehle standardmäßig geschützt, wenn die Multi-Admin-Verifizierung aktiviert ist. Sie können die Regeln jedoch ändern, um den Schutz für diese Befehle aufzuheben:

- "Sicherheits-Login-Passwort"
- "Sicherheits-Login entsperren"
- "Einstellen"

Regelbeschränkungen

Wenn Sie eine Regel erstellen, können Sie optional die `-query` Option angeben, um die Anforderung auf eine Teilmenge der Befehlsfunktionalität zu beschränken. Die `-query` Option kann auch verwendet werden, um Konfigurationselemente wie SVM, Volume und Snapshot Namen einzuschränken.

Beispielsweise kann im `volume snapshot delete` Befehl auf festgelegt werden `-snapshot !hourly*,!daily*,!weekly*`, `-query` d. h., dass Volume-Snapshots mit stündlichen, täglichen oder wöchentlichen Attributen 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*
```

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

Standardmäßig legen Regeln fest, dass ein entsprechender `security multi-admin-verify request create "protected_operation"` Befehl automatisch generiert wird, wenn ein geschützter Vorgang eingegeben wird. Sie können diese Standardeinstellung so ändern, 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 der Genehmiger
- Genehmigungsgruppen
- Ablauffrist der Genehmigung
- Ablauffrist der Ausführung

System Manager Verfahren

Wenn Sie zum ersten Mal eine Regel für einen geschützten Vorgang hinzufügen möchten, lesen Sie das Verfahren von System Manager zu "Aktivieren Sie die Verifizierung für mehrere Administratoren."

So ändern Sie den vorhandenen Regelsatz:

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

CLI-Verfahren

Alle `security multi-admin-verify rule` Befehle erfordern eine MAV-Administratorgenehmigung vor der Ausführung außer `security multi-admin-verify rule show`.

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

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

Regel ändern	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Löschen Sie eine Regel	`security multi-admin-verify rule delete -operation "protected_operation"`
Regeln anzeigen	`security multi-admin-verify rule show`

Verwandte Informationen

- "Sicherheitsregel „Multi-Admin-Verify“"
- "Sicherheitsanmeldung ändern"

Ausführung von MAV-geschützten Vorgängen in ONTAP anfordern

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

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

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

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

System Manager Verfahren

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

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

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

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

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

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

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

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

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

CLI-Verfahren

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

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

   - `volume delete`

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

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

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

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

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

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

2. Den Status der Anfrage überprüfen und auf die MAV-Benachrichtigung antworten.
   a. Wenn der Antrag genehmigt wird, beantworten Sie die CLI-Meldung, um den Vorgang abzuschließen.

      Beispiel:

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

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

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

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

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

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

Beispiel:

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

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

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

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

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Management von Anforderungen für MAV-geschützte Vorgänge in ONTAP

Wenn Administratoren in einer MAV-Genehmigungsgruppe (MAV-Administratoren) über eine ausstehende Anforderung zur Ausführung einer Operation benachrichtigt werden, müssen sie innerhalb einer festgelegten Zeit (Ablauf der Genehmigung) mit einer Genehmigungs- oder Vetonachricht antworten. Wenn nicht genügend Genehmigungen eingehen, muss der Antragsteller die Anfrage löschen und eine neue stellen.

Über diese Aufgabe

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

> `multi-admin-verify`Anfragen im Endzustand können automatisch überschrieben oder entfernt werden. Verwenden Sie die"Überwachungsprotokoll" um frühere Anfragen zu überprüfen.

Die folgenden Informationen aus der Anforderungswarteschlange können angezeigt werden:

Betrieb

Der geschützte Vorgang, für den die Anforderung erstellt wird.

Abfrage

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

Status

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

Erforderliche Genehmiger

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

Ausstehende Genehmiger

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

Ablauf der Genehmigung

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

Ablauf der Ausführung

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

Anwender genehmigt

Die MAV-Administratoren, die den Antrag genehmigt haben.

Vetoed durch den Benutzer

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

Storage-VM (vServer)

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

Der Benutzer wurde angefordert

Der Benutzername des Benutzers, der die Anforderung erstellt hat.

Uhrzeit erstellt

Die Uhrzeit, zu der die Anfrage erstellt wurde.

Nach Genehmigung der Zeit

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

Kommentar

Kommentare, die mit der Anfrage verknüpft sind.

Benutzer erlaubt

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

System Manager

MAV-Administratoren erhalten E-Mail-Nachrichten mit Einzelheiten zur Genehmigungsanfrage, dem Ablaufzeitraum der Anfrage und einem Link zum Genehmigen oder Ablehnen der Anfrage. Sie können auf ein Genehmigungsdialogfeld zugreifen, indem Sie auf den Link in der E-Mail klicken oder im System Manager zu **Ereignisse und Jobs > Anfragen** navigieren.

Das Fenster **Anfragen** ist verfügbar, wenn die Multi-Admin-Verifizierung aktiviert ist. Es zeigt ausstehende Anfragen basierend auf der Anmelde-ID und der MAV-Rolle des Benutzers (Genehmiger oder nicht) an.

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

  Wird eine Anfrage von einem Genehmiger abgelehnt, sind keine weiteren Maßnahmen möglich.
- Abfrage (alle Parameter oder Werte für die angeforderte Operation)
- Benutzer Wird Angefordert
- Die Anfrage Läuft Ab Am
- (Anzahl der ausstehenden Genehmiger
- (Anzahl der möglichen Genehmiger

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

CLI

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

Wenn Sie… wollen	Geben Sie diesen Befehl ein
Genehmigen einer Anfrage	`security multi-admin-verify request approve` *nn*
Veto auf eine Anfrage	`security multi-admin-verify request veto` *nn*
Zeigt alle Anfragen, ausstehende Anfragen oder eine einzelne Anforderung an	`security multi-admin-verify request { show

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

Beispiel:

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

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


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

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

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

Beispiel:

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

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


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

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

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

Verwandte Informationen

- "Sicherheit Multi-Admin-Verify"

Dynamische Autorisierung verwalten

Erfahren Sie mehr über die dynamische Autorisierung von ONTAP

Ab ONTAP 9.15.1 können Administratoren dynamische Autorisierungen konfigurieren und aktivieren, um die Sicherheit des Remote-Zugriffs auf ONTAP zu erhöhen und gleichzeitig potenzielle Schäden zu minimieren, die durch einen böswilligen Akteur verursacht werden können. Mit ONTAP 9.15.1 bietet die dynamische Autorisierung einen ersten Rahmen für die Zuweisung einer Sicherheitsbewertung für Benutzer. Wenn ihre Aktivität verdächtig aussieht, werden sie durch zusätzliche Berechtigungsprüfungen oder die völlige Ablehnung eines Vorgangs in Frage gestellt. Administratoren können Regeln erstellen, Vertrauenswerte zuweisen und Befehle einschränken, um zu bestimmen, wann bestimmte Aktivitäten für einen Benutzer zugelassen oder verweigert werden.

Administratoren können Cluster-weit oder für einzelne Storage VMs eine dynamische Autorisierung aktivieren.

Wie die dynamische Autorisierung funktioniert

Die dynamische Autorisierung verwendet ein System zur Vertrauensbewertung, um Benutzern je nach den Autorisierungsrichtlinien eine andere Vertrauensebene zuzuweisen. Je nach Vertrauensstufe des Benutzers kann eine Aktivität, die er durchführt, zugelassen oder verweigert werden, oder der Benutzer kann zur weiteren Authentifizierung aufgefordert werden.

"Dynamische Autorisierung anpassen"Weitere Informationen zum Konfigurieren von Gewichtungen für die Kriterienbewertung und anderen dynamischen Autorisierungsattributen finden Sie unter.

Vertrauenswürdige Geräte

Wenn die dynamische Autorisierung verwendet wird, ist die Definition eines vertrauenswürdigen Geräts ein Gerät, das von einem Benutzer verwendet wird, um sich bei ONTAP unter Verwendung der Authentifizierung mit öffentlichem Schlüssel als eine der Authentifizierungsmethoden anzumelden. Dem Gerät wird vertraut, weil nur dieser Benutzer den entsprechenden privaten Schlüssel besitzt.

Beispiel für eine dynamische Autorisierung

Nehmen wir das Beispiel von drei verschiedenen Benutzern, die versuchen, ein Volume zu löschen. Beim Versuch, den Vorgang durchzuführen, wird die Risikoeinstufung für jeden Benutzer untersucht:

- Der erste Benutzer meldet sich von einem vertrauenswürdigen Gerät mit sehr wenigen früheren Authentifizierungsfehlern an, wodurch seine Risikoeinstufung gering wird. Der Vorgang ist ohne zusätzliche Authentifizierung zulässig.
- Der zweite Benutzer meldet sich von einem vertrauenswürdigen Gerät mit einem moderaten Prozentsatz früherer Authentifizierungsfehler an, was die Risikoeinstufung moderat macht. Er wird zur zusätzlichen Authentifizierung aufgefordert, bevor der Vorgang zugelassen wird.
- Der dritte Benutzer meldet sich von einem nicht vertrauenswürdigen Gerät mit einem hohen Prozentsatz früherer Authentifizierungsfehler an, wodurch die Risikoeinstufung hoch ist. Der Vorgang ist nicht zulässig.

Wie es weiter geht

- "Aktivieren oder Deaktivieren der dynamischen Autorisierung"
- "Dynamische Autorisierung anpassen"

Aktivieren oder deaktivieren Sie die dynamische Autorisierung in ONTAP

Ab ONTAP 9.15.1 können Administratoren die dynamische Autorisierung entweder im `visibility` Modus zum Testen der Konfiguration konfigurieren und aktivieren, oder im `enforced` Modus, um die Konfiguration für CLI-Benutzer zu aktivieren, die sich über SSH verbinden. Wenn Sie keine dynamische Autorisierung mehr benötigen, können Sie diese deaktivieren. Wenn Sie die dynamische Autorisierung deaktivieren, bleiben die Konfigurationseinstellungen verfügbar, und Sie können sie später verwenden, wenn Sie sie erneut aktivieren möchten.

Erfahren Sie mehr über `security dynamic-authorization modify` in der "ONTAP-Befehlsreferenz".

Dynamische Autorisierung für Tests aktivieren

Sie können die dynamische Autorisierung im Sichtbarkeitsmodus aktivieren, sodass Sie die Funktion testen und sicherstellen können, dass Benutzer nicht versehentlich gesperrt werden. In diesem Modus wird die Vertrauensbewertung mit jeder eingeschränkten Aktivität überprüft, jedoch nicht erzwungen. Jede Aktivität, die abgelehnt worden wäre oder zusätzlichen Authentifizierungsherausforderungen unterliegen würde, wird jedoch protokolliert. Als Best Practice sollten Sie die beabsichtigten Einstellungen in diesem Modus testen, bevor Sie sie durchsetzen.

> Sie können diesen Schritt ausführen, um die dynamische Autorisierung zum ersten Mal zu aktivieren, auch wenn Sie noch keine anderen dynamischen Autorisierungseinstellungen konfiguriert haben. "Dynamische Autorisierung anpassen"Weitere Schritte zum Konfigurieren anderer dynamischer Autorisierungseinstellungen zur Anpassung an Ihre Umgebung finden Sie unter.

Schritte

1. Aktivieren Sie die dynamische Autorisierung im Sichtbarkeitsmodus, indem Sie globale Einstellungen konfigurieren und den Funktionsstatus in ändern `visibility`. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Fett formatierte Parameter sind erforderlich:

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Überprüfen Sie das Ergebnis mit dem `show` Befehl, um die globale Konfiguration anzuzeigen:

```
security dynamic-authorization show
```

Dynamische Autorisierung im erzwungenen Modus aktivieren

Sie können die dynamische Autorisierung im erzwungenen Modus aktivieren. In der Regel verwenden Sie diesen Modus, nachdem Sie die Tests im Sichtmodus abgeschlossen haben. In diesem Modus wird die Vertrauensbewertung mit jeder eingeschränkten Aktivität überprüft, und Aktivitätsbeschränkungen werden erzwungen, wenn die Bedingungen für Einschränkungen erfüllt sind. Das Unterdrückungsintervall wird ebenfalls erzwungen, wodurch zusätzliche Authentifizierungsherausforderungen innerhalb des angegebenen Intervalls verhindert werden.

> Bei diesem Schritt wird davon ausgegangen, dass Sie die dynamische Autorisierung zuvor im `visibility` Modus konfiguriert und aktiviert haben. Dies wird dringend empfohlen.

Schritte

1. Aktivieren Sie die dynamische Autorisierung im `enforced` Modus, indem Sie den Status in `enforced`ändern. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung

anzupassen. Fett formatierte Parameter sind erforderlich:

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

2. Überprüfen Sie das Ergebnis mit dem `show` Befehl, um die globale Konfiguration anzuzeigen:

```
security dynamic-authorization show
```

Dynamische Autorisierung deaktivieren

Sie können die dynamische Autorisierung deaktivieren, wenn Sie die zusätzliche Authentifizierungssicherheit nicht mehr benötigen.

Schritte

1. Deaktivieren Sie die dynamische Autorisierung, indem Sie den Status in ändern `disabled`. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Fett formatierte Parameter sind erforderlich:

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Überprüfen Sie das Ergebnis mit dem `show` Befehl, um die globale Konfiguration anzuzeigen:

```
security dynamic-authorization show
```

   Erfahren Sie mehr über `security dynamic-authorization show` in der "ONTAP-Befehlsreferenz".

Wie es weiter geht

(Optional) "Dynamische Autorisierung anpassen"Informationen zum Konfigurieren anderer dynamischer Autorisierungseinstellungen finden Sie in, je nach Umgebung.

Passen Sie die dynamische Autorisierung in ONTAP an

Als Administrator können Sie verschiedene Aspekte Ihrer dynamischen Autorisierungskonfiguration anpassen, um die Sicherheit von SSH-Verbindungen des Remote-Administrators zu Ihrem ONTAP-Cluster zu erhöhen.

Sie können die folgenden dynamischen Autorisierungseinstellungen je nach Ihren Sicherheitsanforderungen anpassen:

- Konfigurieren Sie die globalen Einstellungen für die dynamische Autorisierung
- Konfigurieren Sie die Komponenten für die dynamische Autorisierung der Vertrauensbewertung
- Konfigurieren Sie einen benutzerdefinierten Anbieter für Vertrauensbewertung
- Eingeschränkte Befehle konfigurieren
- Konfigurieren Sie dynamische Autorisierungsgruppen

Konfigurieren Sie die globalen Einstellungen für die dynamische Autorisierung

Sie können globale Einstellungen für die dynamische Autorisierung konfigurieren, einschließlich der zu sicheren Speicher-VM, des Unterdrückungsintervalls für Authentifizierungsherausforderungen und der Einstellungen für die Vertrauensbewertung.

Erfahren Sie mehr über `security login domain-tunnel create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Konfigurieren Sie globale Einstellungen für dynamische Autorisierung. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen:

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

2. Die resultierende Konfiguration anzeigen:

```
security dynamic-authorization show
```

Eingeschränkte Befehle konfigurieren

Wenn Sie die dynamische Autorisierung aktivieren, enthält die Funktion einen Standardsatz von eingeschränkten Befehlen. Sie können diese Liste an Ihre Bedürfnisse anpassen. "Multi-Admin Verification (MAV)-Dokumentation"Informationen zur Standardliste der eingeschränkten Befehle finden Sie im.

Fügen Sie einen eingeschränkten Befehl hinzu

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

Erfahren Sie mehr über `security dynamic-authorization rule create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Fügen Sie den Befehl hinzu. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

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

2. Zeigt die resultierende Liste der eingeschränkten Befehle an:

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

Entfernen Sie einen eingeschränkten Befehl

Sie können einen Befehl aus der Liste der Befehle entfernen, die mit dynamischer Autorisierung eingeschränkt sind.

Erfahren Sie mehr über `security dynamic-authorization rule delete` in der "ONTAP-Befehlsreferenz".

Schritte

1. Entfernen Sie den Befehl. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

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

2. Zeigt die resultierende Liste der eingeschränkten Befehle an:

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

Konfigurieren Sie dynamische Autorisierungsgruppen

Standardmäßig gilt die dynamische Autorisierung für alle Benutzer und Gruppen, sobald Sie sie aktivieren. Sie können jedoch mit dem `security dynamic-authorization group create` Befehl Gruppen erstellen, sodass die dynamische Autorisierung nur für diese spezifischen Benutzer gilt.

Fügen Sie eine dynamische Autorisierungsgruppe hinzu

Sie können eine dynamische Autorisierungsgruppe hinzufügen.

Erfahren Sie mehr über `security dynamic-authorization group create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen Sie die Gruppe. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

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

2. Anzeigen der resultierenden dynamischen Autorisierungsgruppen:

```
security dynamic-authorization group show
```

Entfernen einer dynamischen Berechtigungsgruppe

Sie können eine dynamische Autorisierungsgruppe entfernen.

Erfahren Sie mehr über `security dynamic-authorization group delete` in der "ONTAP-Befehlsreferenz".

Schritte

1. Löschen Sie die Gruppe. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. Anzeigen der resultierenden dynamischen Autorisierungsgruppen:

```
security dynamic-authorization group show
```

Konfigurieren Sie die Komponenten für die dynamische Autorisierung der Vertrauensbewertung

Sie können die maximale Gewichtung der Bewertung konfigurieren, um die Priorität der Bewertungskriterien zu ändern oder bestimmte Kriterien aus der Risikobewertung zu entfernen.

> Als Best Practice sollten Sie die Standardwerte für die Gewichtung der Punktzahl beibehalten und nur bei Bedarf anpassen.

Erfahren Sie mehr über `security dynamic-authorization trust-score-component modify` in der "ONTAP-Befehlsreferenz".

Im Folgenden finden Sie die Komponenten, die Sie zusammen mit der Standardbewertung und den

Prozentgewichtungen ändern können:

Kriterien	Komponentenname	Standardgewicht für Rohwert	Standardgewichtung in Prozent
Vertrauenswürdiges Gerät	`trusted-device`	20	50
Authentifizierungsverlauf der Benutzeranmeldung	`authentication-history`	20	50

Schritte

1. Komponenten der Vertrauensbewertung ändern. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. Anzeigen der resultierenden Komponenteneinstellungen für die Vertrauensbewertung:

```
security dynamic-authorization trust-score-component show
```

Setzt die Vertrauensbewertung für einen Benutzer zurück

Wenn einem Benutzer aufgrund von Systemrichtlinien der Zugriff verweigert wird und seine Identität nachgewiesen werden kann, kann der Administrator die Vertrauensbewertung des Benutzers zurücksetzen.

Erfahren Sie mehr über `security dynamic-authorization user-trust-score reset` in der "ONTAP-Befehlsreferenz".

Schritte

1. Fügen Sie den Befehl hinzu. Unter Konfigurieren Sie die Komponenten für die dynamische Autorisierung der Vertrauensbewertung finden Sie eine Liste der Komponenten der Vertrauensbewertung, die Sie zurücksetzen können. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Zeigen Sie Ihre Vertrauensbewertung an

Ein Benutzer kann seine eigene Vertrauensbewertung für eine Anmeldesitzung anzeigen.

Schritte

1. Ihr Vertrauenswert anzeigen:

   ```
   security login whoami
   ```

   Sie sollten eine Ausgabe wie die folgende sehen:

   ```
   User: admin
   Role: admin
   Trust Score: 50
   ```

   Erfahren Sie mehr über `security login whoami` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie einen benutzerdefinierten Anbieter für Vertrauensbewertung

Wenn Sie bereits Bewertungsmethoden von einem externen Anbieter für Vertrauensbewertungen erhalten, können Sie den benutzerdefinierten Anbieter der dynamischen Autorisierungskonfiguration hinzufügen.

Bevor Sie beginnen

- Der benutzerdefinierte Anbieter für Vertrauensbewertung muss eine JSON-Antwort zurückgeben. Folgende Syntaxanforderungen müssen erfüllt sein:
  - Das Feld, das die Vertrauensstellung zurückgibt, muss ein skalares Feld sein und kein Element eines Arrays.
  - Das Feld, das die Vertrauensbewertung zurückgibt, kann ein verschachteltes Feld sein, `trust_score.value` z. B. .
  - In der JSON-Antwort muss ein Feld vorhanden sein, das eine numerische Vertrauensbewertung zurückgibt. Wenn dies nicht nativ verfügbar ist, können Sie ein Wrapper-Skript schreiben, um diesen Wert zurückzugeben.
- Der angegebene Wert kann entweder eine Vertrauensbewertung oder eine Risikobewertung sein. Der Unterschied besteht darin, dass die Vertrauensbewertung in aufsteigender Reihenfolge erfolgt, wobei eine höhere Bewertung ein höheres Vertrauensniveau bedeutet, während die Risikobewertung in absteigender Reihenfolge erfolgt. Ein Vertrauenswert von 90 für einen Score-Bereich von 0 bis 100 zeigt beispielsweise an, dass die Bewertung sehr vertrauenswürdig ist und wahrscheinlich zu einem „Zulassen“ ohne zusätzliche Herausforderung führt. während ein Risiko-Score von 90 für einen Score-Bereich von 0 bis 100 auf ein hohes Risiko hinweist und wahrscheinlich zu einem „Deny“ ohne zusätzliche Herausforderung führt.
- Auf den benutzerdefinierten Anbieter für die Vertrauensbewertung muss über die ONTAP-REST-API zugegriffen werden können.
- Der benutzerdefinierte Anbieter für die Vertrauensbewertung muss mit einem der unterstützten Parameter konfiguriert werden. Benutzerdefinierte Anbieter von Vertrauensbewertungen, die eine Konfiguration erfordern, die nicht in der unterstützten Parameterliste enthalten ist, werden nicht unterstützt.

  Erfahren Sie mehr über `security dynamic-authorization trust-score-component create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Fügen Sie einen benutzerdefinierten Anbieter für Vertrauensbewertung hinzu. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. Die resultierenden Einstellungen für den Anbieter der Vertrauensbewertung anzeigen:

```
security dynamic-authorization trust-score-component show
```

Konfigurieren Sie benutzerdefinierte Provider-Tags für die Vertrauensbewertung

Sie können mit externen Anbietern von Vertrauensbewertungen über Tags kommunizieren. Auf diese Weise können Sie Informationen in der URL an den Anbieter der Vertrauensstellung senden, ohne vertrauliche Informationen preiszugeben.

Erfahren Sie mehr über `security dynamic-authorization trust-score-component create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Aktivieren Sie die Tags für Anbieter von Vertrauensbewertung. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den `-vserver` Parameter nicht verwenden, wird der Befehl auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

   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"
```

Authentifizierung und Autorisierung mit OAuth 2.0

Überblick über die Implementierung von ONTAP OAuth 2.0

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

Die Unterstützung für OAuth 2.0 wurde erstmals mit ONTAP 9.14.0 eingeführt, sodass die Verfügbarkeit von der von Ihnen verwendeten ONTAP Version abhängt. "Versionshinweise zu ONTAP"Weitere Informationen finden Sie im.

Funktionen und Vorteile

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

Unterstützung für den Standard OAuth 2.0

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

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

Getestet mit gängigen Autorisierungsservern

Die Implementierung von ONTAP OAuth 2.0 wurde mit mehreren gängigen Servern oder Services basierend auf der ONTAP-Version wie folgt getestet:

- ONTAP 9.16.1 (Unterstützung für Gruppen-UUID für Namenszuordnungen und externe Rollen):
  - Microsoft Entra-ID
- ONTAP 9.14.1 (Unterstützung für OAuth 2.0-Standardfunktionen)
  - Auth0
  - Active Directory Federation Service (ADFS)

- Keycloak

Unter finden "Autorisierungsserver und Zugriffstoken" Sie weitere Informationen zu den Funktionen der einzelnen ONTAP Versionen.

Unterstützung für mehrere gleichzeitige Autorisierungsserver

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

Integration in die REST-Rollen

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

Option zur Verwendung von Zugriffstoken mit Senderbeschränkungen

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

Implementierung und Konfiguration

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

OAuth 2.0 Einheiten innerhalb von ONTAP

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

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

ONTAP-Kernkonfiguration

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

- ONTAP Befehlszeilenschnittstelle

- System Manager
- ONTAP REST API

Umwelt und unterstützende Dienstleistungen

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

Unterstützte ONTAP-Clients

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

Ausgewählte Terminologie

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

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

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

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

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

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

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

HTTP-Autorisierungskopf
: Eine Kopfzeile, die in der HTTP-Anforderung enthalten ist, um den Client und die zugehörigen Berechtigungen als Teil eines REST-API-Aufrufs zu identifizieren. Je nachdem, wie Authentifizierung und

Autorisierung durchgeführt werden, stehen verschiedene Varianten oder Implementierungen zur Verfügung. Wenn ein OAuth 2.0-Zugriffstoken an ONTAP übergeben wird, wird das Token als *Bearer Token* identifiziert.

HTTP-Basisauthentifizierung

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

FAPI

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

GEHRUNG

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

Weitere Ressourcen

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

Protokolle und Standards

- "RFC 6749: Das OAuth 2.0 Authorization Framework"
- "RFC 7519: JSON Web Tokens (JWT)"
- "RFC 7523: JSON Web Token (JWT) Profile für OAuth 2.0 Client Authentication and Authorization Grants"
- "RFC 7662: OAuth 2.0 Token-Introspektion"
- "RFC 7800: Proof-of-Possession Key für JWTs"
- "RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication und Certificate-bound Access Tokens"

Organisationen

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

Produkte und Services

- "Auth0"
- "Eintragungs-ID"
- "ADFS-Übersicht"
- "Keycloak"

Zusätzliche Tools und Dienstprogramme

- "JWT von Auth0"
- "OpenSSL"

NetApp Dokumentation und Ressourcen

- "Dokumentation zur ONTAP Automatisierung"

Konzepte

OAuth 2.0-Autorisierungsserver und Zugriffstoken in ONTAP

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

OAuth 2.0-Autorisierungsserver

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

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

Administration

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

- Benutzer- und Benutzerauthentifizierung
- Bereich
- Administrative Trennung durch Mandanten und Bereiche
- Richtlinienumsetzung
- Anbindung an verschiedene externe Dienste
- Unterstützung für andere Identitätsprotokolle (z. B. SAML)

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

Definieren auf ONTAP

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

Die wichtigsten Aspekte der ONTAP-Konfiguration sind im Folgenden aufgeführt. "OAuth 2.0-Bereitstellungsszenarien"Weitere Informationen finden Sie unter.

Wie und wo die Zugriffstoken validiert werden

Es gibt zwei Optionen für die Validierung von Zugriffstoken.

- Lokale Validierung

  ONTAP kann Zugriffstoken lokal anhand der Informationen validieren, die vom Autorisierungsserver

bereitgestellt werden, der das Token ausgestellt hat. Die vom Autorisierungsserver abgerufenen Informationen werden von ONTAP zwischengespeichert und in regelmäßigen Abständen aktualisiert.

- Fernintrospektion

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

Netzwerkspeicherort

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

Wie die Autorisierungsserver definiert werden

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

Erfahren Sie mehr über `security oauth2 client create` in der "ONTAP-Befehlsreferenz".

Anzahl der Autorisierungsserver

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

In ONTAP unterstützte Funktionen von OAuth 2.0

Die Unterstützung für OAuth 2.0 war zunächst mit ONTAP 9.14.1 verfügbar und wird weiterhin durch nachfolgende Versionen erweitert. Die von ONTAP unterstützten OAuth 2.0-Funktionen werden im Folgenden beschrieben.

> Funktionen, die mit einer bestimmten ONTAP Version eingeführt wurden, werden an zukünftige Versionen weitergeführt.

ONTAP 9.16.1

ONTAP 9.16.1 erweitert die Standard-OAuth 2.0-Funktionen, um Entra-ID-spezifische Erweiterungen für native Entra-ID-Gruppen aufzunehmen. Dies beinhaltet die Verwendung von GUIDs im Zugriffstoken anstelle von Namen. Darüber hinaus bietet die Version Unterstützung für externe Rollenzuordnung, um die nativen Identitäts-Provider-Rollen ONTAP-Rollen mithilfe des Felds „Rollen“ im Zugriffstoken zuzuordnen.

ONTAP 9.14.1

Ab ONTAP 9.14.1 werden Autorisierungsserver über die folgenden Standardfunktionen von OAuth 2.0 für Anwendungen unterstützt, die Folgendes verwenden:

- OAuth 2.0 mit den Standardfeldern einschließlich „iss“, „aud“ und „Exp“ wie in und "RFC 7519: JSON Web Token (JWT)" beschrieben "RFC6749: Das OAuth 2.0-Genehmigungs-Framework". Dazu gehört auch die Unterstützung für die eindeutige Identifizierung von Benutzern über Felder im Zugriffstoken wie „upn“, „appid“, „sub“, „username“ oder „Preferred_username“.

- ADFS-anbieterspezifische Erweiterungen für Gruppennamen mit dem Feld „Gruppe“.
- Anbieterspezifische Azure Erweiterungen für Gruppen-UUIDs mit dem Feld „Gruppe“.
- ONTAP-Erweiterungen zur Autorisierungsunterstützung mithilfe von eigenständigen und benannten Rollen im Bereich des Zugriffstoken OAuth 2.0. Dazu gehören die Felder „Umfang“ und „scp“ sowie Gruppennamen innerhalb des Bereichs.

Verwenden von OAuth 2.0-Zugriffstoken

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

Abrufen eines Zugriffstoken

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

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

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

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

Grant-Typen

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

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

JWT-Inhalt

Ein OAuth 2.0-Zugriffstoken ist als JWT formatiert. Der Inhalt wird basierend auf Ihrer Konfiguration vom Autorisierungsserver erstellt. Die Token sind jedoch für die Client-Anwendungen undurchsichtig. Ein Kunde hat

keinen Grund, ein Token zu prüfen oder sich des Inhalts bewusst zu sein.

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

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

Weitere Informationen finden Sie unter "RFC 7519: JSON Web Tokens" .

Client-Autorisierung

Übersicht und Optionen für die ONTAP-Clientautorisierung

Die ONTAP OAuth 2.0 Implementierung ist flexibel und robust und bietet Ihnen die Funktionen, die Sie zur Sicherung Ihrer ONTAP Umgebung benötigen. Es stehen mehrere Konfigurationsoptionen zur Verfügung, die sich gegenseitig ausschließen. Die Autorisierungsentscheidungen basieren letztlich auf den ONTAP-REST-Rollen, die entweder in den OAuth 2.0-Zugriffstoken enthalten sind oder von diesen abgeleitet wurden.

Sie können nur verwenden"ONTAP REST-Rollen", wenn Sie die Autorisierung für OAuth 2.0 konfigurieren. Die früheren herkömmlichen ONTAP Rollen werden nicht unterstützt.

ONTAP wendet je nach Konfiguration die am besten geeignete Autorisierungsoption an. Weitere Informationen dazu, wie ONTAP Client-Zugriffsentscheidungen trifft, finden Sie unter"Wie ONTAP den Zugriff bestimmt".

OAuth 2.0 eigenständige Oszilloskope

Diese Bereiche enthalten eine oder mehrere benutzerdefinierte REST-Rollen, die jeweils in einer einzigen Zeichenfolge im Zugriffstoken eingekapselt sind. Sie sind unabhängig von den Rollendefinitionen von ONTAP. Sie müssen die Bereichszeichenfolgen auf Ihrem Autorisierungsserver konfigurieren. Weitere Informationen finden Sie unter "Eigenständige Oszilloskope von OAuth 2.0" .

Lokale ONTAP-REST-Rollen

Es kann eine einzelne benannte REST-Rolle verwendet werden, entweder erstellt oder benutzerdefiniert. Die scope Syntax für eine benannte Rolle ist **ontap-role-**<URL-encoded-ONTAP-role-name>. Wenn die Rolle ONTAP beispielsweise der scope string ist `admin`, wird dies der Fall sein `ontap-role-admin`.

Benutzer

Der Benutzername im Zugriffstoken, der mit Zugriff auf die Anwendung "http" definiert ist, kann verwendet

werden. Anhand der definierten Authentifizierungsmethode wird ein Benutzer in der folgenden Reihenfolge getestet: Passwort, Domäne (Active Directory), nsswitch (LDAP).

Gruppen

Die Autorisierungsserver können so konfiguriert werden, dass sie ONTAP-Gruppen für die Autorisierung verwenden. Wenn die lokalen ONTAP-Definitionen überprüft werden, aber keine Zugriffsentscheidung getroffen werden kann, werden die Active Directory („Domain“)- oder LDAP („nsswitch“)-Gruppen verwendet. Gruppeninformationen können auf zwei Arten angegeben werden:

- OAuth 2.0-Scope-String

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

- In der „Gruppe“-Forderung

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

Sehen "Arbeiten mit OAuth 2.0- oder SAML-IdP-Gruppen in ONTAP" für weitere Informationen.

Eigenständige OAuth 2.0-Bereiche in ONTAP

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

Format der Bereichszeichenfolge

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

ONTAP-Literal

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

Cluster

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

- Cluster-UUID

  Identifiziert ein einzelnes Cluster.

- Sternchen (*)

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

Sie können den ONTAP-CLI-Befehl verwenden `cluster identity show`, um die UUID Ihres Clusters anzuzeigen. Falls nicht angegeben, gilt der Umfang für alle Cluster. Erfahren Sie mehr über `cluster identity show` in der "ONTAP-Befehlsreferenz".

Rolle

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

Zugangsstufe

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

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

SVM

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

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

REST-API-URI

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

Beispiele für den Umfang

Im Folgenden werden einige Beispiele für eigenständige Oszilloskope vorgestellt.

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

Bietet dem Benutzer, dem diese Rolle zugewiesen `/cluster` ist, den Zugriff auf den Endpunkt zu lesen, zu erstellen und zu ändern.

CLI-Verwaltungstool

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

Der Befehl `security oauth2 scope` hat zwei Anwendungsfälle basierend auf Ihrer Eingabe:

- CLI-Parameter für den Umfang einer Zeichenfolge

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

- Scope-String zu CLI-Parametern

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

Beispiel

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

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

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

Erfahren Sie mehr über `security oauth2 scope` in der "ONTAP-Befehlsreferenz".

OAuth 2.0 externe Rollenzuordnung in ONTAP

Eine externe Rolle wird bei einem Identifizieren-Anbieter definiert, der für die Verwendung durch ONTAP konfiguriert ist. Sie können Zuordnungsbeziehungen zwischen diesen externen Rollen und den ONTAP Rollen mit der ONTAP CLI erstellen und verwalten.

Sie können auch die externe Rollenzuordnungsfunktion mit der ONTAP REST-API konfigurieren. Erfahren Sie mehr in der "Dokumentation zur ONTAP Automatisierung".

Externe Rollen in einem Zugriffstoken

Hier ist ein Fragment eines JSON-Zugriffstoken, der zwei externe Rollen enthält.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Konfiguration

Sie können die externe Rollenzuordnungsfunktion über die ONTAP-Befehlszeilenschnittstelle verwalten.

Erstellen

Mit dem Befehl können Sie eine Rollenzuordnungskonfiguration definieren `security login external-role-mapping create`. Sie müssen auf der ONTAP **admin** Berechtigungsebene sein, um diesen Befehl sowie die damit verbundenen Optionen ausgeben zu können.

Parameter

Die Parameter, die zum Erstellen einer Gruppenzuordnung verwendet werden, werden im Folgenden beschrieben.

Parameter	Beschreibung
`external-role`	Der Name der Rolle, die beim externen Identitätsanbieter definiert wurde.
`provider`	Der Name des Identitätsanbieters. Dies sollte die Kennung für das System sein.
`ontap-role`	Gibt die vorhandene ONTAP-Rolle an, der die externe Rolle zugeordnet ist.

Beispiel

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Erfahren Sie mehr über `security login external-role-mapping create` in der "ONTAP-Befehlsreferenz".

Zusätzliche CLI-Vorgänge

Der Befehl unterstützt mehrere zusätzliche Vorgänge, darunter:

- Anzeigen
- Ändern

- Löschen

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Wie ONTAP den Client-Zugriff bestimmt

Um OAuth 2.0 richtig zu entwickeln und zu implementieren, müssen Sie verstehen, wie Ihre Autorisierungskonfiguration von ONTAP verwendet wird, um Zugriffsentscheidungen für die Clients zu treffen. Die wichtigsten Schritte zur Bestimmung des Zugriffs sind unten auf der Grundlage der ONTAP Version dargestellt.

Es gab keine signifikanten Updates für OAuth 2.0 mit ONTAP 9.15.1. Wenn Sie Version 9.15.1 verwenden, lesen Sie die Beschreibung für ONTAP 9.14.1.

Verwandte Informationen

- "In ONTAP unterstützte Funktionen von OAuth 2.0"

ONTAP 9.16.1

ONTAP 9.16.1 erweitert die Standard-OAuth 2.0-Unterstützung um Microsoft-Entra-ID-spezifische Erweiterungen für native Entra-ID-Gruppen sowie externe Rollenzuordnung.

Bestimmen Sie den Client-Zugriff für ONTAP 9.16.1

Schritt 1: Eigenständige Bereiche

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

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

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

Schritt 2: Überprüfen Sie die lokale Rollenmarkierung

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

- Wenn der Wert lautet, `true` fahren Sie mit Schritt 3 fort.
- Wenn der Wert `false` verarbeitet wird, endet und der Zugriff verweigert wird.

Schritt 3: Benannte ONTAP REST-Rolle

Wenn das Zugriffstoken eine benannte REST-Rolle im Feld oder oder `scp` als Antrag enthält `scope`, verwendet ONTAP diese Rolle, um die Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

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

Schritt 4: Benutzer

Extrahieren Sie den Benutzernamen aus dem Zugriffstoken und versuchen Sie, ihn mit Benutzern zu vergleichen, die Zugriff auf die Anwendung „http“ haben. Die Benutzer werden anhand der Authentifizierungsmethode in der folgenden Reihenfolge untersucht:

- Passwort
- Domäne (Active Directory)
- Nsswitch (LDAP)

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

Wenn ein Benutzer nicht stimmt oder kein Benutzername im Zugriffstoken vorhanden ist, fahren Sie mit Schritt 5 fort.

Schritt 5: Gruppen

Wenn eine oder mehrere Gruppen enthalten sind, wird das Format überprüft. Wenn die Gruppen als UUIDs dargestellt werden, wird eine interne Gruppenzuordnungstabelle durchsucht. Bei einer Gruppenübereinstimmung und einer zugehörigen Rolle verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW**- oder **DENY** -Entscheidung, und die Verarbeitung wird beendet. Weitere Informationen finden Sie unter "Arbeiten mit OAuth 2.0- oder SAML-IdP-Gruppen in ONTAP" .

Wenn Gruppen als Namen dargestellt und mit Domain- oder nsswitch-Autorisierung konfiguriert werden,

versucht ONTAP, sie einer Active Directory- bzw. LDAP-Gruppe zuzuordnen. Wenn eine Gruppenübereinstimme vorhanden ist, verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

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

ONTAP 9.14.1

Die Unterstützung von OAuth 2.0 wird mit ONTAP 9.14.1 auf Basis der Standard-OAuth 2.0-Funktionen eingeführt.

Bestimmen Sie den Client-Zugriff für ONTAP 9.14.1

Schritt 1: Eigenständige Bereiche

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

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

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

Schritt 2: Überprüfen Sie die lokale Rollenmarkierung

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

- Wenn der Wert lautet, `true` fahren Sie mit Schritt 3 fort.
- Wenn der Wert `false` verarbeitet wird, endet und der Zugriff verweigert wird.

Schritt 3: Benannte ONTAP REST-Rolle

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

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

Schritt 4: Benutzer

Extrahieren Sie den Benutzernamen aus dem Zugriffstoken und versuchen Sie, ihn mit Benutzern zu vergleichen, die Zugriff auf die Anwendung „http“ haben. Die Benutzer werden anhand der Authentifizierungsmethode in der folgenden Reihenfolge untersucht:

- Passwort
- Domäne (Active Directory)
- Nsswitch (LDAP)

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

Wenn ein Benutzer nicht stimmt oder kein Benutzername im Zugriffstoken vorhanden ist, fahren Sie mit Schritt 5 fort.

Schritt 5: Gruppen

Wenn eine oder mehrere Gruppen eingeschlossen und mit einer Domain- oder nsswitch-Autorisierung konfiguriert sind, versucht ONTAP, sie einer Active Directory- bzw. LDAP-Gruppe zuzuordnen.

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

Wenn keine Gruppenübereinstimme vorhanden ist oder keine Gruppe im Zugriffstoken vorhanden ist,

wird der Zugriff verweigert und die Verarbeitung wird beendet.

OAuth 2.0-Bereitstellungsszenarien mit ONTAP

Beim Definieren eines Autorisierungsservers für ONTAP stehen verschiedene Konfigurationsoptionen zur Verfügung. Basierend auf diesen Optionen können Sie einen Autorisierungsserver definieren, der für Ihre Umgebung geeignet ist, und dabei eines von mehreren Bereitstellungsszenarien verwenden.

Zusammenfassung der Konfigurationsparameter

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

> Der für einen einzelnen Parameter oder ein Feld verwendete Name kann je nach ONTAP-Administratorschnittstelle variieren. Um den Unterschieden in den administrativen Schnittstellen Rechnung zu tragen, wird für jeden Parameter in der Tabelle ein einziger generischer Name verwendet. Der genaue Name, der mit einer bestimmten Schnittstelle verwendet wird, sollte je nach Kontext offensichtlich sein.

Parameter	Beschreibung
Name	Der Name des Autorisierungsservers, der ONTAP bekannt ist.
Applikation	Die ONTAP-interne Anwendung, für die die Definition gilt. Dies muss **http** sein.
Aussteller-URI	Der FQDN mit Pfad, der den Standort oder die Organisation identifiziert, der die Token ausgibt.
Provider-JWKS-URI	Der FQDN mit Pfad und Dateiname, bei dem ONTAP die JSON-Webschlüsselsätze erhält, die zur Validierung der Zugriffstoken verwendet werden.
JWKS-Aktualisierungsintervall	Das Zeitintervall, in dem festgelegt wird, wie oft ONTAP Zertifikatsinformationen vom Provider JWKS URI aktualisiert. Der Wert wird im ISO-8601-Format angegeben.
Introspektion Endpunkt	Der FQDN mit Pfad, den ONTAP zur Remote-Token-Validierung durch Introspektion verwendet.
Client-ID	Der Name des Clients, wie er auf dem Autorisierungsserver definiert ist. Wenn dieser Wert enthalten ist, müssen Sie auch den zugehörigen Client-Schlüssel basierend auf der Schnittstelle angeben.
Ausgehender Proxy	Damit wird der Zugriff auf den Autorisierungsserver ermöglicht, wenn sich ONTAP hinter einer Firewall befindet. Der URI muss im Curl-Format vorliegen.
Verwenden Sie ggf. lokale Rollen	Ein boolesches Flag, das bestimmt, ob die lokalen ONTAP-Definitionen verwendet werden, einschließlich einer benannten REST-Rolle und lokalen Benutzern.
Anspruch des Remote-Benutzers	Ein alternativer Name, den ONTAP für lokale Benutzer verwendet. Verwenden Sie das `sub` Feld im Zugriffstoken, um mit dem lokalen Benutzernamen zu übereinstimmen.

Parameter	Beschreibung
Zielgruppe	Dieses Feld definiert die Endpunkte, an denen das Zugriffstoken verwendet werden kann.

Bereitstellungsszenarien

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

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

Lokale Validierung

Die folgenden Bereitstellungsszenarien basieren auf der lokalen Tokenvalidierung durch ONTAP.

Verwenden Sie eigenständige Bereiche ohne Proxy

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

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

Sie müssen die Gültigkeitsbereiche auch auf dem Autorisierungsserver hinzufügen.

Verwenden Sie eigenständige Bereiche mit einem Proxy

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

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

Sie müssen die Gültigkeitsbereiche auch auf dem Autorisierungsserver hinzufügen.

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

Dieses Bereitstellungsszenario verwendet lokale Benutzerrollen mit Standardnamenszuordnung. Der Remote-Benutzer-Anspruch verwendet den Standardwert von `sub`. Daher wird dieses Feld im Zugriffstoken verwendet,

um mit dem lokalen Benutzernamen zu übereinstimmen. Der Benutzername darf maximal 40 Zeichen lang sein. Der Autorisierungsserver befindet sich hinter einer Firewall, Sie müssen also auch einen Proxy konfigurieren. Sie müssen die folgenden Parameter angeben:

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Lokale Rollen verwenden, falls vorhanden (`true`)
- Ausgehender Proxy
- Aussteller

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

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

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

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Lokale Rollen verwenden, falls vorhanden (`true`)
- Anspruch des Remote-Benutzers
- Ausgehender Proxy
- Aussteller-URI
- Zielgruppe

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

Fernintrospektion

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

Verwenden Sie eigenständige Bereiche ohne Proxy

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

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

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

Verwandte Informationen

- "Sicherheit OAuth2 Client Show"

ONTAP Client-Authentifizierung mit OAuth 2.0 Mutual TLS

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

Gegenseitiges TLS mit OAuth 2.0

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

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

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

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

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

Grundlegende Implementierungsablaufs

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

Schritt 1: Erstellen und installieren Sie ein Client-Zertifikat

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

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

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

Schritt 2: Konfigurieren Sie ONTAP für die Verwendung von MTLS

Sie müssen ONTAP für die Verwendung von MTLS konfigurieren. Diese Konfiguration erfolgt für jeden Autorisierungsserver separat. Zum Beispiel `security oauth2 client` wird mit der CLI der Befehl mit dem optionalen Parameter verwendet `use-mutual-tls`. Weitere Informationen finden Sie unter "Implementieren Sie OAuth 2.0 in ONTAP" .

Schritt 3: Client fordert ein Zugriffstoken an

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

Schritt 4: Der Autorisierungsserver generiert das Zugriffstoken

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

Schritt 5: Client-Anwendung präsentiert das Zugriffstoken an ONTAP

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

Schritt 6: ONTAP überprüft Client und Token.

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

Verwandte Informationen

- "Sicherheit OAuth2-Client"

Konfiguration und Implementierung

Bereiten Sie die Bereitstellung von OAuth 2.0 mit ONTAP vor

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

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

Geschützte Ressourcen und Client-Applikationen

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

Identifizierung von Client-Applikationen

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

Bestehende ONTAP REST-Rollen und lokale Benutzer prüfen

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

Globaler Übergang zu OAuth 2.0

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

Autorisierungsserver

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

Wählen Sie den Autorisierungsserver aus, und installieren Sie ihn

Sie müssen einen oder mehrere Autorisierungsserver auswählen und installieren. Es ist wichtig, sich mit den Konfigurationsoptionen und -Verfahren Ihrer Identitätsanbieter vertraut zu machen, einschließlich der Definition von Geltungsbereichen. Beachten Sie, dass einige Autorisierungsserver, einschließlich Microsoft Entra-ID, Gruppen darstellen, die UUIDs anstelle von Namen verwenden.

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

ONTAP verwendet das Zertifikat des Autorisierungsservers, um die von den Clients präsentierten signierten

Zugriffstoken zu validieren. Dazu benötigt ONTAP das Stammzertifizierungsstellenzertifikat und alle Zwischenzertifikate. Diese sind möglicherweise mit ONTAP vorinstalliert. Wenn nicht, müssen Sie sie installieren.

Bewerten Sie den Netzwerkstandort und die -Konfiguration

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

Client-Authentifizierung und -Autorisierung

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

Eigenständige Bereiche oder lokale ONTAP-Identitätsdefinitionen

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

Optionen mit lokaler ONTAP-Verarbeitung

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

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

Lokale Validierung oder Remote-Introspektion

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

Zugriffstoken, die durch den Absender eingeschränkt sind

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

Gruppen als UUIDs und Identitätszuordnung

Wenn Sie einen Autorisierungsserver verwenden, der Gruppen mit UUIDs repräsentiert, müssen Sie planen, wie diese Gruppen Gruppennamen und möglicherweise zugehörigen Rollen zugeordnet werden.

Administrationsschnittstelle

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

- Befehlszeilenschnittstelle
- System Manager
- REST API

Wie Clients Zugriffstoken anfordern

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

ONTAP konfigurieren

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

Definieren Sie REST-Rollen und lokale Benutzer

Basierend auf Ihrer Autorisierungskonfiguration kann die lokale ONTAP-Identifizieren-Verarbeitung verwendet werden. In diesem Fall müssen Sie die REST-Rollen und Benutzerdefinitionen überprüfen und definieren. Je nach Autorisierungsserver kann dies auch die Verwaltung von Gruppen auf Basis von UUID-Werten umfassen.

Kernkonfiguration

Zur Durchführung der zentralen ONTAP-Konfiguration sind drei wichtige Schritte erforderlich:

- Installieren Sie optional das Stammzertifikat (und alle Zwischenzertifikate) für die Zertifizierungsstelle, die das Zertifikat des Autorisierungsservers signiert hat.
- Definieren Sie den Autorisierungsserver.
- Aktivieren Sie die OAuth 2.0-Verarbeitung für den Cluster.

Implementieren Sie OAuth 2.0 in ONTAP

Die Bereitstellung der zentralen OAuth 2.0-Funktionalität umfasst drei Hauptschritte.

Bevor Sie beginnen

Sie müssen die Bereitstellung von OAuth 2.0 vorbereiten, bevor Sie ONTAP konfigurieren. Sie müssen beispielsweise den Autorisierungsserver beurteilen, einschließlich der Art und Weise, wie das Zertifikat signiert wurde und ob es sich hinter einer Firewall befindet. Weitere Informationen finden Sie unter "Bereiten Sie die Bereitstellung von OAuth 2.0 mit ONTAP vor" .

Schritt 1: Installieren Sie die Stammzertifizierungen des Autorisierungsservers

ONTAP enthält eine große Anzahl vorinstallierter Stammzertifizierungsstellen-Zertifikate. So wird in vielen Fällen das Zertifikat für Ihren Autorisierungsserver von ONTAP ohne zusätzliche Konfiguration sofort erkannt. Je nachdem, wie das Zertifikat des Autorisierungsservers signiert wurde, müssen Sie möglicherweise ein Stammzertifizierungszertifikat und alle Zwischenzertifikate installieren.

Befolgen Sie die Anweisungen unten, um das Zertifikat zu installieren, falls es benötigt wird. Installieren Sie alle erforderlichen Zertifikate auf Cluster-Ebene.

Wählen Sie das richtige Verfahren, je nachdem, wie Sie auf ONTAP zugreifen.

Beispiel 1. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Klicken Sie neben **Certificates** auf →.
4. Klicken Sie auf der Registerkarte **Vertrauenswürdige Zertifizierungsstellen** auf **Hinzufügen**.
5. Klicken Sie auf **Import** und wählen Sie die Zertifikatdatei aus.
6. Vervollständigen Sie die Konfigurationsparameter für Ihre Umgebung.
7. Klicken Sie Auf **Hinzufügen**.

CLI

1. Starten Sie die Installation:

   ```
   security certificate install -type server-ca
   ```

2. Suchen Sie nach der folgenden Konsolenmeldung:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Öffnen Sie die Zertifikatdatei mit einem Texteditor.
4. Kopieren Sie das gesamte Zertifikat einschließlich der folgenden Zeilen:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. Fügen Sie das Zertifikat nach der Eingabeaufforderung in das Terminal ein.
6. Drücken Sie **Enter**, um die Installation abzuschließen.
7. Vergewissern Sie sich, dass das Zertifikat installiert ist, indem Sie eine der folgenden Methoden verwenden:

   ```
   security certificate show-user-installed

   security certificate show
   ```

Schritt 2: Konfigurieren des Autorisierungsservers

Sie müssen mindestens einen Autorisierungsserver für ONTAP definieren. Sie sollten die Parameterwerte auf Grundlage Ihres Konfigurations- und Bereitstellungsplans auswählen. Überprüfen Sie "OAuth2-Bereitstellungsszenarien"die genauen Parameter, die für Ihre Konfiguration erforderlich sind.

Um eine Autorisierungsserverdefinition zu ändern, können Sie die vorhandene Definition löschen und eine neue erstellen.

Das folgende Beispiel basiert auf dem ersten einfachen Bereitstellungsszenario unter "Lokale Validierung". Eigenständige Bereiche werden ohne Proxy verwendet.

Wählen Sie das richtige Verfahren, je nachdem, wie Sie auf ONTAP zugreifen. Das CLI-Verfahren verwendet symbolische Variablen, die Sie vor der Ausgabe des Befehls ersetzen müssen.

Beispiel 2. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Klicken Sie neben **OAuth 2.0 Authorization** auf **+**.
4. Wählen Sie **Weitere Optionen**.
5. Geben Sie die erforderlichen Werte für Ihre Bereitstellung an, z. B.:
   - Name
   - Anwendung (http)
   - Provider-JWKS-URI
   - Aussteller-URI
6. Klicken Sie Auf **Hinzufügen**.

CLI

1. Erstellen Sie die Definition erneut:

   ```
   security oauth2 client create -config-name <NAME> -provider-jwks-uri
   <URI_JWKS> -application http -issuer <URI_ISSUER>
   ```

   Beispiel:

   ```
   security oauth2 client create \
   -config-name auth0 \
   -provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
   realm/protocol/openid-connect/certs \
   -application http \
   -issuer https://superzap.dev.netapp.com:8443/realms/my-realm
   ```

   Erfahren Sie mehr über `security oauth2 client create` in der "ONTAP-Befehlsreferenz".

Schritt 3: Aktivieren Sie OAuth 2.0

Der letzte Schritt ist die Aktivierung von OAuth 2.0. Dies ist eine globale Einstellung für das ONTAP Cluster.

Aktivieren Sie die OAuth 2.0-Verarbeitung erst, wenn Sie bestätigen, dass ONTAP, die Autorisierungsserver und alle unterstützenden Dienste ordnungsgemäß konfiguriert wurden.

Wählen Sie das richtige Verfahren, je nachdem, wie Sie auf ONTAP zugreifen.

Beispiel 3. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Klicken Sie neben **OAuth 2.0 Authorization** auf →.
4. Aktivieren Sie **OAuth 2.0-Autorisierung**.

CLI

1. OAuth 2.0 aktivieren:

   ```
   security oauth2 modify -enabled true
   ```

2. Bestätigen Sie, dass OAuth 2.0 aktiviert ist:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "Sicherheit OAuth2 ändern"
- "Sicherheit OAuth2 Show"

Führen Sie einen ONTAP REST API-Aufruf mit OAuth 2.0 aus.

Die OAuth 2.0-Implementierung in ONTAP unterstützt REST-API-Client-Applikationen. Sie können einen einfachen REST API-Aufruf mit Curl ausgeben, um mit OAuth 2.0 zu beginnen. Im folgenden Beispiel wird die ONTAP Cluster-Version abgerufen.

Bevor Sie beginnen

Sie müssen die Funktion OAuth 2.0 für Ihren ONTAP-Cluster konfigurieren und aktivieren. Dazu gehört auch die Definition eines Autorisierungsservers.

Schritt 1: Erwerben Sie ein Zugriffstoken

Sie müssen ein Zugriffstoken erwerben, um es mit dem REST-API-Aufruf zu verwenden. Die Token-Anforderung wird außerhalb von ONTAP ausgeführt, und die genaue Vorgehensweise hängt vom Autorisierungsserver und seiner Konfiguration ab. Sie können das Token über einen Webbrowser, mit einem Curl-Befehl oder mit einer Programmiersprache anfordern.

Zur Veranschaulichung wird unten ein Beispiel gezeigt, wie ein Zugriffstoken von Keycloak mit Curl angefordert werden kann.

Keycloak Beispiel

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

Sie sollten das zurückgegebene Token kopieren und speichern.

Schritt 2: Geben Sie den REST API-Aufruf aus

Nachdem Sie über ein gültiges Zugriffstoken verfügen, können Sie einen Curl-Befehl mit dem Zugriffstoken verwenden, um einen REST-API-Aufruf auszustellen.

Parameter und Variablen

Die beiden Variablen im Beispiel Curl sind in der folgenden Tabelle beschrieben.

Variabel	Beschreibung
FQDN_IP-DOLLAR	Der vollständig qualifizierte Domain-Name oder die IP-Adresse der ONTAP Management LIF.
ACCESS_TOKEN IN HÖHE VON USD	Das vom Autorisierungsserver ausgegebene Zugriffstoken OAuth 2.0.

Sie sollten diese Variablen zuerst in der Bash Shell-Umgebung festlegen, bevor Sie das Curl-Beispiel ausgeben. Geben Sie beispielsweise in der Linux CLI den folgenden Befehl ein, um die FQDN-Variable festzulegen und anzuzeigen:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

Nachdem beide Variablen in Ihrer lokalen Bash Shell definiert wurden, können Sie den Curl-Befehl kopieren und in die CLI einfügen. Drücken Sie **Enter**, um die Variablen zu ersetzen und den Befehl auszugeben.

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

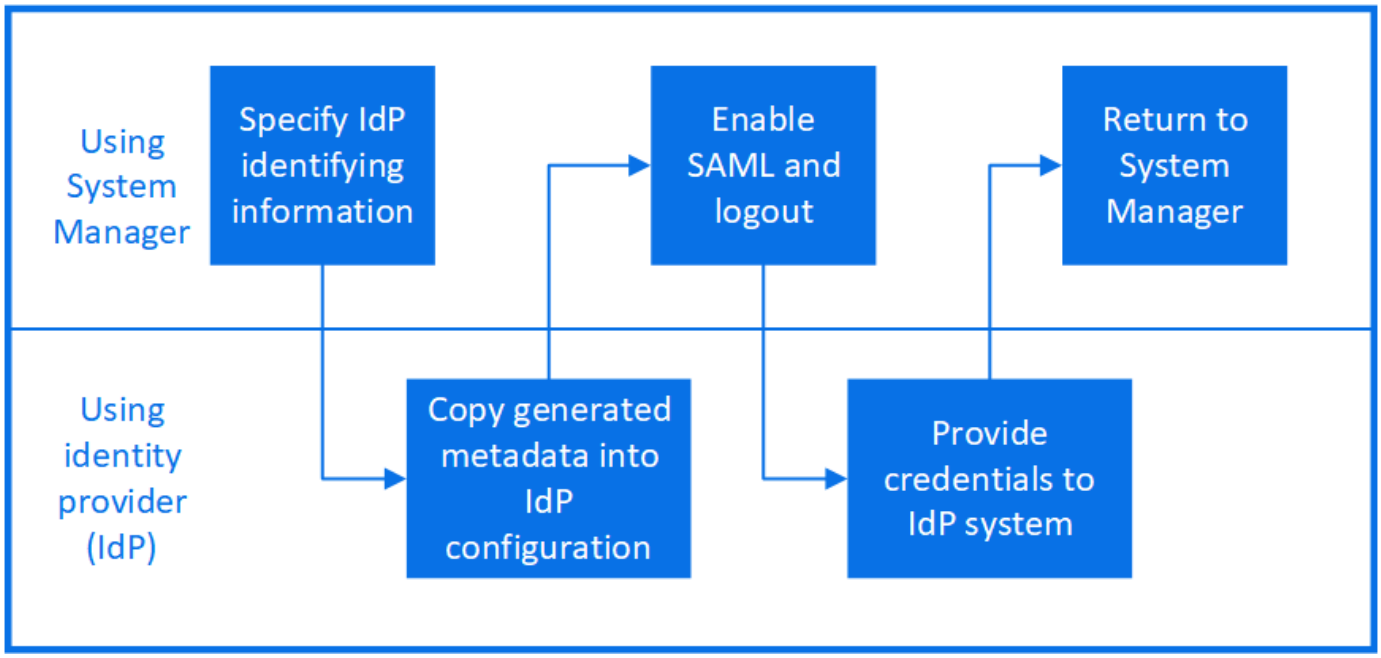
Konfigurieren der SAML-Authentifizierung für Remote ONTAP -Benutzer

Ab ONTAP 9.3 können Sie die SAML-Authentifizierung (Security Assertion Markup Language) für Webdienste konfigurieren. Wenn die SAML-Authentifizierung konfiguriert und aktiviert ist, werden Benutzer von einem externen Identitätsanbieter (IdP) anstelle von Verzeichnisdienstanbietern wie Active Directory und LDAP authentifiziert. Wenn die SAML-Authentifizierung deaktiviert ist, werden die konfigurierten Verzeichnisdienstanbieter wie Active Directory und LDAP zur Authentifizierung verwendet.

Aktivieren Sie die SAML-Authentifizierung

Führen Sie die folgenden Schritte durch, um die SAML-Authentifizierung mit System Manager oder mit der CLI zu aktivieren. Wenn auf Ihrem Cluster ONTAP 9.7 oder eine frühere Version ausgeführt wird, sind die zu befolgenden Schritte in System Manager unterschiedlich. Weitere Informationen finden Sie in der System Manager Online-Hilfe, die auf Ihrem System verfügbar ist.

Nach der Aktivierung der SAML-Authentifizierung können nur Remotebenutzer, die für die SAML-Authentifizierung konfiguriert sind, auf die System Manager-GUI zugreifen. Lokale Benutzer können nach der Aktivierung der SAML-Authentifizierung nicht mehr auf die System Manager-GUI zugreifen.



Über diese Aufgabe

- SAML-Authentifizierung gilt nur für ONTAP `http` Und `ontapi` Anwendungen.

  Der `http` Und `ontapi` Anwendungen werden von den folgenden Webdiensten verwendet: Service Processor Infrastructure, ONTAP APIs und System Manager.

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

- Ab ONTAP 9.17.1 können vom IdP bereitgestellte Gruppeninformationen ONTAP Rollen zugeordnet werden. Dadurch können Sie Benutzern Rollen basierend auf den im IdP definierten Gruppen zuweisen. Weitere Informationen finden Sie unter "Arbeiten mit OAuth 2.0- oder SAML-IdP-Gruppen in ONTAP" .

Die folgenden IDPs wurden mit System Manager validiert:

- Microsoft Entra ID (validiert mit ONTAP 9.17.1 und höher)
- Active Directory Federation Services
- Cisco Duo (validiert mit den folgenden ONTAP -Versionen:)
  - 9.7P21 und höher 9.7 Versionen (siehe "Dokumentation zu System Manager Classic")
  - 9.8P17 und spätere 9.8-Patch-Versionen
  - 9.9.1P13 und spätere 9.9.1-Patch-Versionen
  - 9.10.1P9 und spätere 9.10.1-Patch-Versionen
  - 9.11.1P4 und spätere 9.11.1-Patch-Versionen
  - 9.12.1 und höhere Versionen
- Shibboleth

Bevor Sie beginnen

- Der IdP, den Sie für die Fernauthentifizierung verwenden möchten, muss konfiguriert. Sie benötigen die URI des IdP. IdP-URI ist die Webadresse, an die ONTAP Authentifizierungsanfragen sendet und von der es Antworten empfängt.
- Port 443 muss zwischen dem ONTAP Cluster und dem IdP geöffnet sein.
- Der ONTAP Cluster und der IdP müssen jeweils den vollqualifizierten Domänennamen des anderen anpingen können. Stellen Sie sicher, dass DNS ordnungsgemäß konfiguriert ist und das Cluster-Zertifikat nicht abgelaufen ist.
- Fügen Sie bei Bedarf die vertrauenswürdige Zertifizierungsstelle (CA) des IdP zu ONTAP hinzu. Sie können "Verwalten Sie ONTAP -Zertifikate mit System Manager" . Möglicherweise müssen Sie das ONTAP Clusterzertifikat im IdP konfigurieren.
- Sie müssen auf die ONTAP -Cluster zugreifen können "Serviceprozessor (SP)" Konsole. Wenn SAML falsch konfiguriert ist, müssen Sie es über die SP Konsole deaktivieren.
- Wenn Sie Entra ID verwenden (gültig ab ONTAP 9.17.1), müssen Sie Entra ID mit den ONTAP Metadaten konfigurieren, bevor Sie die ONTAP SAML-Konfiguration erstellen. Entra ID stellt die IdP-URI erst bereit, wenn sie mit den ONTAP Metadaten konfiguriert ist. Die IdP-URI wird zum Erstellen der ONTAP SAML-Konfiguration benötigt.
  - Wenn Sie SAML mit System Manager konfigurieren, lassen Sie das Feld „IdP-URI“ leer, bis System Manager die ONTAP Metadaten bereitstellt. Konfigurieren Sie die Entra-ID mit den ONTAP Metadaten und kopieren Sie anschließend die IdP-URI in System Manager, bevor Sie die SAML-Konfiguration aktivieren.
  - Wenn Sie SAML über die ONTAP -Befehlszeilenschnittstelle konfigurieren, müssen Sie die ONTAP Metadaten generieren, bevor Sie die ONTAP -SAML-Konfiguration aktivieren. Sie können die ONTAP Metadatendatei mit dem folgenden Befehl generieren:

    ```
    security saml-sp default-metadata create -sp-host <ontap_host_name>
    ```

    `ontap_host_name` ist der Hostname oder die IP-Adresse des Hosts des SAML-Dienstanbieters, in

diesem Fall des ONTAP Systems. Standardmäßig wird die Cluster-Verwaltungs-IP-Adresse verwendet. Optional können Sie die Zertifikatsinformationen des ONTAP Servers angeben. Standardmäßig werden die Zertifikatsinformationen des ONTAP Webservers verwendet.

Konfigurieren Sie die Entra-ID mit den bereitgestellten Metadaten. Sie müssen die Entra-ID konfigurieren, bevor Sie die ONTAP SAML-Konfiguration erstellen. Fahren Sie nach der Konfiguration von Entra mit dem folgenden CLI-Verfahren fort.

- Sie können die ONTAP Metadaten für die Entra-ID erst generieren, wenn alle Knoten im Cluster auf Version 9.17.1 basieren.

Schritte

Führen Sie je nach Umgebung die folgenden Schritte aus:

System Manager

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie neben **SAML Authentication** auf ⚙.
3. Vergewissern Sie sich, dass das Kontrollkästchen **SAML-Authentifizierung aktivieren** aktiviert ist.
4. Geben Sie die URL der IdP-URI ein (einschließlich "https://"). Wenn Sie Entra ID verwenden, überspringen Sie diesen Schritt.
5. Ändern Sie bei Bedarf die Hostsystemadresse. Dies ist die Adresse, an die der IdP nach der Authentifizierung weiterleitet. Die Standardeinstellung ist die IP-Adresse der Clusterverwaltung.
6. Stellen Sie sicher, dass das richtige Zertifikat verwendet wird:
   - Wenn Ihr System nur mit einem Zertifikat mit dem Typ „Server“ zugeordnet war, wird dieses Zertifikat als Standard betrachtet und nicht angezeigt.
   - Wenn Ihr System mit mehreren Zertifikaten als Servertyp zugeordnet war, wird eines der Zertifikate angezeigt. Um ein anderes Zertifikat auszuwählen, klicken Sie auf **Ändern**.
7. Klicken Sie Auf **Speichern**. In einem Bestätigungsfenster werden die Metadateninformationen angezeigt, die automatisch in die Zwischenablage kopiert wurden.
8. Wechseln Sie zum angegebenen IdP-System und kopieren Sie die Metadaten aus der Zwischenablage, um die Systemmetadaten zu aktualisieren. Wenn Sie Entra ID verwenden, kopieren Sie die IdP-URI in ONTAP, nachdem Sie Entra ID mit den Systemmetadaten konfiguriert haben.
9. Kehren Sie zum Bestätigungsfenster (im System Manager) zurück und aktivieren Sie das Kontrollkästchen **Ich habe den IdP mit dem Host-URI oder Metadaten** konfiguriert.
10. Klicken Sie auf **Abmelden**, um SAML-basierte Authentifizierung zu aktivieren. Das IdP-System zeigt einen Authentifizierungsbildschirm an.
11. Geben Sie auf der IdP-Anmeldeseite Ihre SAML-basierten Anmeldeinformationen ein. Nach der Überprüfung Ihrer Anmeldeinformationen werden Sie zur Startseite des System Managers weitergeleitet.

CLI

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

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

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

   > ⓘ Einige URLs enthalten das Fragezeichen (?). Das Fragezeichen aktiviert die aktive Hilfe der ONTAP Befehlszeile. Um eine URL mit einem Fragezeichen einzugeben, müssen Sie zunächst die aktive Hilfe mit dem Befehl deaktivieren. `set -active -help false` Die Die aktive Hilfe kann später wieder mit dem Befehl `set -active -help true`. im "ONTAP-Befehlsreferenz" .

   `ontap_host_name` Ist der Hostname oder die IP-Adresse des Hosts des SAML-Dienstanbieters, in diesem Fall das ONTAP-System. Standardmäßig wird die IP-Adresse der Cluster-Management-LIF verwendet.

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

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

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

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

2. Vom IdP-Host aus Konfigurieren Sie den IdP mit den ONTAP -Host-Metadaten. Wenn Sie die Entra-ID verwenden, haben Sie diesen Schritt bereits abgeschlossen.
3. Sobald der IdP konfiguriert ist, aktivieren Sie die SAML-Konfiguration:

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

   Jeder vorhandene Benutzer, der auf die `http` oder `ontapi`-Anwendung zugreift, wird automatisch für die SAML-Authentifizierung konfiguriert.

4. Wenn Sie Benutzer für das `http` oder `ontapi` Anwendung nach der SAML-Konfiguration, geben Sie SAML als Authentifizierungsmethode für die neuen Benutzer an. Vor ONTAP 9.17.1 wird automatisch ein SAML-Login für bestehende `http` oder `ontapi` Benutzer, wenn SAML aktiviert ist. Neue Benutzer müssen für SAML konfiguriert werden. Ab ONTAP 9.17.1 werden alle mit `password` , `domain` , oder `nsswitch` Authentifizierungsmethoden werden automatisch gegenüber dem IdP authentifiziert, wenn SAML aktiviert ist.

   a. Erstellen Sie eine Anmeldemethode für neue Benutzer mit SAML-Authentifizierung . `user_name` muss mit dem im IdP konfigurierten Benutzernamen übereinstimmen:

      > Der `user_name` Wert ist case-sensitiv. Sofern Sie nicht Entra ID verwenden, geben Sie nur den Benutzernamen an und lassen Sie jeglichen Teil der Domäne weg. Wenn Sie Entra ID verwenden, können Sie den Benutzernamen mit der Domäne erstellen, zum Beispiel *user_name@domain.com*.

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

      Beispiel:

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

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

`security login show`

Beispiel:

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked
Method
-------------- ----------- ------------- ---------------- ------
--------------
admin          console     password      admin            no
none
admin          http        password      admin            no
none
admin          http        saml          admin            -
none
admin          ontapi      password      admin            no
none
admin          ontapi      saml          admin            -
none
admin          service-processor
                           password      admin            no
none
admin          ssh         password      admin            no
none
admin1         http        password      backup           no
none
admin1         http        saml          backup           -
none
```

+
Erfahren Sie mehr über `security login show` in der "ONTAP-Befehlsreferenz".

Deaktivieren Sie die SAML-Authentifizierung

Sie können die SAML-Authentifizierung deaktivieren, wenn Sie die Authentifizierung von Remote-System-Manager-Benutzern über einen externen Identitätsanbieter (IdP) beenden möchten. Bei deaktivierter SAML-Authentifizierung werden die lokale Benutzerauthentifizierung oder die konfigurierten Verzeichnisdienstanbieter wie Active Directory und LDAP zur Benutzerauthentifizierung verwendet.

Führen Sie je nach Umgebung die folgenden Schritte aus:

Beispiel 4. Schritte

System Manager

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie unter **SAML Authentication** auf die Schaltfläche **aktiviert**.
3. *Optional*: Sie können auch neben **SAML Authentication** klicken und dann das Kontrollkästchen **SAML Authentication** aktivieren deaktivieren.

CLI

1. SAML-Authentifizierung deaktivieren:

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

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

   ```
   security saml-sp delete
   ```

Konfigurieren eines Drittanbieter-IdP

Über diese Aufgabe

Um sich bei ONTAP zu authentifizieren, müssen Sie möglicherweise die Einstellungen Ihres IdP ändern. Die folgenden Abschnitte enthalten Konfigurationsinformationen für unterstützte IdPs.

Eintragungs-ID

Erstellen Sie beim Konfigurieren von Entra ID eine neue Anwendung und konfigurieren Sie die SAML-Anmeldung mit den von ONTAP bereitgestellten Metadaten. Bearbeiten Sie nach der Anwendungserstellung den Abschnitt „Attribute und Ansprüche“ der SAML-Anwendungseinstellungen wie folgt:

Einstellung	Wert
Name	urn:oid:0.9.2342.19200300.100.1.1
Namespace	*Leer lassen*
Namensformat	URI
Quelle	Attribut
Quellattribut	Benutzer.Benutzerprinzipalname

Wenn Sie Gruppen mit Entra-ID verwenden möchten, fügen Sie einen Gruppenanspruch mit den folgenden Einstellungen hinzu:

Einstellung	Wert
Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Namespace	*Leer lassen*
Quellattribut	Gruppen-ID

Entra ID stellt Gruppeninformationen im UUID-Format bereit. Weitere Informationen zur Verwendung von Gruppen mit Entra ID finden Sie unter "Verwalten von Gruppen mit UUIDs" .

Die im Abschnitt „SAML-Zertifikat“ der SAML-Einstellungen der Anwendung angegebene *App Federation Metadata URL* ist die IdP-URI, die Sie in ONTAP eingeben.

Informationen zur Konfiguration der Entra ID Multifaktor-Authentifizierung finden Sie unter "Planen einer Microsoft Entra-Multifaktor-Authentifizierungsbereitstellung" .

Weitere Informationen finden Sie im "Entra-ID-Dokumentation" .

Active Directory Federation Services

Beim Konfigurieren von Active Directory Federation Services (AD FS) müssen Sie eine neue, anspruchsorientierte Vertrauensstellung (Relying Party Trust) mit den von ONTAP bereitgestellten Service-Provider-Metadaten hinzufügen. Sobald die Vertrauensstellung erstellt ist, fügen Sie der Anspruchsausstellungsrichtlinie der Vertrauensstellungsstelle mithilfe der Vorlage „LDAP-Attribute als Ansprüche senden“ die folgenden Anspruchsregeln hinzu:

Attributspeicher	LDAP-Attribut	Ausgehender Anspruchstyp
Active Directory	SAM-Kontoname	Namens-ID
Active Directory	SAM-Kontoname	urn:oid:0.9.2342.19200300.100.1.1
Active Directory	Namensformat	urn:oasis:names:tc:SAML:2.0:attrname-format:uri

Attributspeicher	LDAP-Attribut	Ausgehender Anspruchstyp
Active Directory	Tokengruppen – Qualifiziert durch Domänennamen	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Active Directory	sAMAccountName	urn:oid:1.2.840.113556.1.4.221

AD FS stellt Gruppeninformationen im Namensformat bereit. Weitere Informationen zur Verwendung von Gruppen mit AD FS finden Sie unter "Verwalten von Gruppen mit Namen" .

Weitere Informationen finden Sie im "AD FS-Dokumentation" .

Cisco Duo

Weitere Informationen finden Sie im "Cisco Duo-Dokumentation" für Konfigurationsinformationen.

Shibboleth

Vor der Konfiguration des Shibboleth-IdP müssen Sie einen LDAP-Server konfiguriert haben.

Wenn Sie SAML auf ONTAP aktivieren, speichern Sie die bereitgestellten Host-Metadaten-XML. Ersetzen Sie auf dem Host, auf dem Shibboleth installiert ist, den Inhalt von `metadata/sp-metadata.xml` mit der Host-Metadaten-XML im Shibboleth IdP-Stammverzeichnis.

Weitere Informationen finden Sie unter "Shibboleth" .

Fehlerbehebung bei der SAML-Konfiguration

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

Über diese Aufgabe

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

Schritte

1. Melden Sie sich bei der erweiterten Berechtigungsebene an:

   ```
   set -privilege advanced
   ```

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

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

   Beispiel:

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

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

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

Erfahren Sie mehr über `security saml-sp status show` in der "ONTAP-Befehlsreferenz".

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

   `security saml-sp repair -node <node_name>`

   Beispiel:

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

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

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

   Erfahren Sie mehr über `security saml-sp repair` in der "ONTAP-Befehlsreferenz".

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

   `security saml-sp status show -instance`

Beispiel:

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

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

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

Erfahren Sie mehr über `security saml-sp status show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "ONTAP-Befehlsreferenz"
- "Sicherheit saml-SP"
- "Sicherheits-Login erstellen"

Arbeiten mit OAuth 2.0- oder SAML-IdP-Gruppen in ONTAP

ONTAP bietet verschiedene Optionen zum Konfigurieren von Gruppen basierend auf Ihrem OAuth 2.0-Autorisierungsserver oder SAML-Identitätsanbieter (IdP). Die Gruppen können dann Rollen zugeordnet werden, die von ONTAP zur Zugriffsbestimmung verwendet werden.

Ab ONTAP 9.17.1 können vom SAML-IdP bereitgestellte Gruppeninformationen ONTAP Rollen zugeordnet werden. Dadurch können Sie Benutzern Rollen basierend auf den im IdP definierten Gruppen zuweisen. Weitere Informationen finden Sie unter "Konfigurieren Sie die SAML-Authentifizierung" . Ab ONTAP 9.14.1 unterstützt ONTAP die Gruppennamenauthentifizierung für OAuth 2.0. Ab ONTAP 9.16.1 unterstützt ONTAP die OAuth 2.0-Gruppen-UUID-Authentifizierung und Rollenzuordnung. Weitere Informationen finden Sie unter "Überblick über die Implementierung von ONTAP OAuth 2.0" .

Wie Gruppen identifiziert werden

Wenn Sie eine Gruppe auf einem Autorisierungsserver oder SAML-IdP konfigurieren, wird diese identifiziert und in einem OAuth 2.0-Zugriffstoken oder einer SAML-Assertion über einen Namen oder eine UUID

übertragen. Bevor Sie ONTAP konfigurieren, müssen Sie wissen, wie Ihr Autorisierungsserver oder SAML-IdP mit Gruppen umgeht.

> Wenn mehrere Gruppen in einem Zugriffstoken enthalten sind, versucht ONTAP, jede Gruppe zu verwenden, bis eine Übereinstimmung vorhanden ist.

Gruppennamen

Viele Autorisierungsserver und SAML-Identitätsanbieter, wie beispielsweise Active Directory Federation Service (ADFS), identifizieren und repräsentieren Gruppen anhand eines Namens. Hier sehen Sie ein Fragment eines von ADFS generierten JSON OAuth 2.0-Zugriffstokens, das mehrere Gruppen enthält. Sehen Verwalten von Gruppen mit Namen für weitere Informationen.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

Gruppen-UUIDs

Einige Autorisierungsserver und SAML-Identitätsanbieter, wie Microsoft Entra ID, identifizieren und repräsentieren Gruppen mithilfe einer UUID. Hier sehen Sie ein Fragment eines von Entra ID generierten OAuth 2.0-Zugriffstokens, das mehrere Gruppen enthält. Sehen Verwalten von Gruppen mit UUIDs für weitere Informationen.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Verwalten von Gruppen mit Namen

Wenn Ihr Autorisierungsserver oder SAML-Identitätsanbieter Namen zur Identifizierung von Gruppen verwendet, müssen Sie sicherstellen, dass jede Gruppe für Ihren ONTAP Cluster definiert ist. Abhängig von Ihrer Sicherheitsumgebung ist die Gruppe möglicherweise bereits definiert.

Hier ist ein Beispiel für einen CLI-Befehl zur Definition einer ONTAP Gruppe. Beachten Sie, dass eine

benannte Gruppe aus dem Beispiel-Zugriffstoken verwendet wird. Sie benötigen die ONTAP Berechtigungsebene **admin**, um den Befehl ausführen zu können.

Beispiel

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

Verwenden `-authentication-method domain` oder `nsswitch` für SAML IdP- und OAuth 2.0-Autorisierungsservergruppen.

Sie können diese Funktion auch über die ONTAP REST API konfigurieren. Weitere Informationen finden Sie im "Dokumentation zur ONTAP Automatisierung" .

Verwalten von Gruppen mit UUIDs

Wenn Ihr Autorisierungsserver oder SAML-Identitätsanbieter Gruppen mithilfe von UUID-Werten darstellt, müssen Sie vor der Verwendung einer Gruppe eine zweistufige Konfiguration durchführen. Ab ONTAP 9.16.1 stehen zwei Mapping-Funktionen zur Verfügung, die mit Entra ID getestet wurden. Entra ID für OAuth 2.0 wird ab ONTAP 9.16.1 und Entra ID für SAML ab ONTAP 9.17.1 unterstützt. Sie benötigen die ONTAP Berechtigungsebene **admin**, um die CLI-Befehle ausführen zu können.

Sie können diese Funktionen auch mit der ONTAP-REST-API konfigurieren. Erfahren Sie mehr in der "Dokumentation zur ONTAP Automatisierung".

Ordnen Sie eine Gruppen-UUID einem Gruppennamen zu

Wenn Sie einen Autorisierungsserver oder SAML-Identitätsanbieter verwenden, der Gruppen mithilfe von UUID-Werten darstellt, müssen Sie die Gruppen-UUIDs Gruppennamen zuordnen. Die wichtigsten ONTAP CLI-Operationen werden unten beschrieben.

Erstellen

Sie können eine neue Gruppenzuordnungskonfiguration mit dem `security login group create` Befehl. Die Gruppen-UUID und der Name sollten mit der Konfiguration auf dem Autorisierungsserver oder SAML-IdP übereinstimmen. Erfahren Sie mehr über `security login group create` im "ONTAP-Befehlsreferenz" .

Parameter

Die Parameter, die zum Erstellen einer Gruppenzuordnung verwendet werden, werden im Folgenden beschrieben.

Parameter	Beschreibung
`vserver`	Gibt optional den Namen der SVM (vServer) an, mit der die Gruppe verknüpft ist. Wenn sie nicht angegeben ist, ist die Gruppe dem ONTAP-Cluster zugeordnet.
`name`	Der eindeutige Name der Gruppe, die ONTAP verwendet.
`type`	Dieser Wert gibt den Identitätsanbieter an, von dem die Gruppe stammt.
`uuid`	Gibt die universell eindeutige Kennung der Gruppe an, wie sie vom Autorisierungsserver oder SAML-IdP bereitgestellt wird.

Hier sehen Sie ein Beispiel für einen CLI-Befehl, der eine Gruppe für ONTAP definiert. Beachten Sie, dass eine UUID-Gruppe aus dem Beispiel-Zugriffstoken verwendet wird.

Beispiel

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

Nach dem Erstellen der Gruppe wird eine eindeutige schreibgeschützte Ganzzahl-ID für die Gruppe generiert.

Zusätzliche CLI-Vorgänge

Der Befehl unterstützt mehrere zusätzliche Vorgänge, darunter:

- Anzeigen
- Ändern
- Löschen

Sie können die Option verwenden `show`, um die eindeutige Gruppen-ID abzurufen, die für eine Gruppe generiert wurde. Erfahren Sie mehr über `show` in der "ONTAP-Befehlsreferenz".

Ordnen Sie eine Gruppen-UUID einer Rolle zu

Wenn Sie einen Autorisierungsserver oder SAML-IdP verwenden, der Gruppen mithilfe von UUID-Werten darstellt, können Sie die Gruppe einer Rolle zuordnen. Weitere Informationen zur rollenbasierten Zugriffskontrolle in ONTAP finden Sie unter "Erfahren Sie mehr über das Management von ONTAP-Zugriffskontrollrollen". Die wichtigsten ONTAP CLI-Operationen werden unten beschrieben. benötigen die ONTAP Berechtigungsebene **admin**, um die Befehle ausführen zu können.

> Sie müssen zuerst Ordnen Sie eine Gruppen-UUID einem Gruppennamen zu und rufen Sie die für die Gruppe generierte eindeutige Ganzzahl-ID ab. Sie benötigen die ID, um die Gruppe einer Rolle zuzuordnen.

Erstellen

Sie können eine neue Rollenzuordnung mit dem `security login group role-mapping create` Befehl. Erfahren Sie mehr über `security login group role-mapping create` im "ONTAP-Befehlsreferenz" .

Parameter

Im Folgenden werden die Parameter beschrieben, mit denen eine Gruppe einer Rolle zugeordnet werden kann.

Parameter	Beschreibung
`group-id`	Gibt die eindeutige ID an, die mit dem Befehl für die Gruppe generiert `security login group create` wurde.
`role`	Der Name der ONTAP-Rolle, der die Gruppe zugeordnet ist.

Beispiel

```
security login group role-mapping create -group-id 1 -role admin
```

Zusätzliche CLI-Vorgänge

Der Befehl unterstützt mehrere zusätzliche Vorgänge, darunter:

- Anzeigen
- Ändern
- Löschen

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Externe Rollenzuordnung"

Authentifizierung und Autorisierung mit WebAuthn MFA

Erfahren Sie mehr über die WebAuthn-Multifaktor-Authentifizierung für ONTAP System Manager-Benutzer

Ab ONTAP 9.16.1 können Administratoren die Multifaktor-Authentifizierung (MFA) von WebAuthn für Benutzer aktivieren, die sich bei System Manager anmelden. Somit können sich System Manager Anmeldungen über einen FIDO2 Schlüssel (z. B. einen YubiKey) als zweite Form der Authentifizierung anmelden. WebAuthn MFA ist standardmäßig für neue und bestehende ONTAP-Benutzer deaktiviert.

WebAuthn MFA wird für Benutzer und Gruppen unterstützt, die die folgenden Authentifizierungstypen für die erste Authentifizierungsmethode verwenden:

- Benutzer: Passwort, Domain oder nsswitch
- Gruppen: Domain oder nsswitch

Nachdem Sie WebAuthn MFA als zweite Authentifizierungsmethode für einen Benutzer aktiviert haben, wird der Benutzer nach der Anmeldung bei System Manager aufgefordert, einen Hardware-Authentifikator zu registrieren. Nach der Registrierung wird der private Schlüssel im Authentifikator gespeichert und der öffentliche Schlüssel im ONTAP gespeichert.

ONTAP unterstützt eine WebAuthn-Anmeldeinformation pro Benutzer. Wenn ein Benutzer einen Authentifikator verliert und ersetzt werden muss, muss der ONTAP-Administrator die WebAuthn-Anmeldeinformationen für den Benutzer löschen, damit der Benutzer bei der nächsten Anmeldung einen neuen Authentifikator registrieren kann.

Benutzer, für die WebAuthn MFA als zweite Authentifizierungsmethode aktiviert ist, müssen den FQDN (z. B. "https://myontap.example.com") anstelle der IP-Adresse (z. B. "https://192.168.100.200") verwenden, um auf System Manager zuzugreifen. Bei Benutzern mit aktiviertem WebAuthn MFA werden Versuche, sich unter Verwendung der IP-Adresse beim System Manager anzumelden, abgelehnt.

Aktivieren Sie WebAuthn MFA für Benutzer oder Gruppen von ONTAP System Manager

Als ONTAP-Administrator können Sie WebAuthn MFA für einen Benutzer oder eine Gruppe des System Managers aktivieren, indem Sie entweder einen neuen Benutzer oder eine neue Gruppe hinzufügen, wobei die Option WebAuthn MFA aktiviert ist, oder die Option für einen vorhandenen Benutzer oder eine vorhandene Gruppe aktivieren.

Nachdem Sie WebAuthn MFA als zweite Authentifizierungsmethode für einen Benutzer oder eine Gruppe aktiviert haben, wird der Benutzer (oder alle Benutzer dieser Gruppe) bei der nächsten Anmeldung bei System Manager aufgefordert, ein Hardware-FIDO2-Gerät zu registrieren. Diese Registrierung wird vom lokalen Betriebssystem des Benutzers durchgeführt und besteht in der Regel aus dem Einfügen des Sicherheitsschlüssels, dem Erstellen eines Passschlüssels und dem Berühren des Sicherheitsschlüssels (sofern unterstützt).

Aktivieren Sie WebAuthn MFA beim Erstellen eines neuen Benutzers oder einer neuen Gruppe

Sie können einen neuen Benutzer oder eine neue Gruppe mit aktiviertem WebAuthn MFA entweder mit dem System-Manager oder der ONTAP-CLI erstellen.

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie das Pfeilsymbol neben **Users and Roles**.
3. Wählen Sie unter **Benutzer Hinzufügen** aus.
4. Geben Sie einen Benutzer- oder Gruppennamen an und wählen Sie im Dropdown-Menü für **Rolle** eine Rolle aus.
5. Geben Sie eine Anmeldemethode und ein Kennwort für den Benutzer oder die Gruppe an.

   WebAuthn MFA unterstützt Anmeldemethoden von "Password", "Domain" oder "nsswitch" für Benutzer und "Domain" oder "nsswitch" für Gruppen.
6. Wählen Sie in der Spalte **MFA für HTTP enabled** aus.
7. Wählen Sie **Speichern**.

CLI

1. Erstellen Sie einen neuen Benutzer oder eine neue Gruppe mit aktiviertem WebAuthn MFA.

   Im folgenden Beispiel wird WebAuthn MFA durch Auswahl von „publickey“ für die zweite Authentifizierungsmethode aktiviert:

   ```
   security login create -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

   Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

Aktivieren Sie WebAuthn MFA für einen vorhandenen Benutzer oder eine vorhandene Gruppe

Sie können WebAuthn MFA für einen vorhandenen Benutzer oder eine vorhandene Gruppe aktivieren.

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie das Pfeilsymbol neben **Users and Roles**.
3. Wählen Sie in der Liste der Benutzer und Gruppen das Optionsmenü für den Benutzer oder die Gruppe aus, den Sie bearbeiten möchten.

   WebAuthn MFA unterstützt Anmeldemethoden von "Password", "Domain" oder "nsswitch" für Benutzer und "Domain" oder "nsswitch" für Gruppen.
4. Wählen Sie in der Spalte **MFA für HTTP** für diesen Benutzer **Enabled** aus.
5. Wählen Sie **Speichern**.

CLI

1. Ändern Sie einen vorhandenen Benutzer oder eine vorhandene Gruppe, um WebAuthn MFA für diesen Benutzer oder diese Gruppe zu aktivieren.

   Im folgenden Beispiel wird WebAuthn MFA durch Auswahl von „publickey“ für die zweite Authentifizierungsmethode aktiviert:

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

   Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

Deaktivieren Sie WebAuthn MFA für ONTAP System Manager-Benutzer

Als ONTAP-Administrator können Sie WebAuthn MFA für einen Benutzer oder eine Gruppe deaktivieren, indem Sie den Benutzer oder die Gruppe mit dem Systemmanager oder der ONTAP-CLI bearbeiten.

Deaktivieren Sie WebAuthn MFA für einen vorhandenen Benutzer oder eine vorhandene Gruppe

Sie können WebAuthn MFA für einen vorhandenen Benutzer oder eine vorhandene Gruppe jederzeit deaktivieren.

> Wenn Sie registrierte Anmeldeinformationen deaktivieren, bleiben die Anmeldeinformationen erhalten. Wenn Sie die Anmeldeinformationen in Zukunft erneut aktivieren, werden dieselben Anmeldeinformationen verwendet, sodass der Benutzer sich bei der Anmeldung nicht erneut registrieren muss.

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie das Pfeilsymbol neben **Users and Roles**.
3. Wählen Sie in der Liste der Benutzer und Gruppen den Benutzer oder die Gruppe aus, den Sie bearbeiten möchten.
4. Wählen Sie in der Spalte **MFA für HTTP** für diesen Benutzer **disabled** aus.
5. Wählen Sie **Speichern**.

CLI

1. Ändern Sie einen vorhandenen Benutzer oder eine vorhandene Gruppe, um WebAuthn MFA für diesen Benutzer oder diese Gruppe zu deaktivieren.

   Im folgenden Beispiel wird WebAuthn MFA deaktiviert, indem für die zweite Authentifizierungsmethode „none“ ausgewählt wird.

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method none \
                         -application http \
                         -role admin
   ```

   Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

Zeigen Sie die MFA-Einstellungen für ONTAP WebAuthn an und verwalten Sie die Anmeldeinformationen

Als ONTAP-Administrator können Sie Cluster-weite WebAuthn-MFA-Einstellungen anzeigen und Benutzer- und Gruppenanmeldeinformationen für WebAuthn MFA verwalten.

Cluster-Einstellungen für WebAuthn MFA anzeigen

Sie können die Clustereinstellungen für WebAuthn MFA mithilfe der ONTAP-CLI anzeigen.

Schritte

1. Zeigen Sie die Clustereinstellungen für WebAuthn MFA an. Sie können optional eine Storage-VM mit dem Argument angeben `vserver`:

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

   Erfahren Sie mehr über `security webauthn show` in der "ONTAP-Befehlsreferenz".

Unterstützte öffentliche WebAuthn-MFA-Algorithmen anzeigen

Sie können die unterstützten Public-Key-Algorithmen für WebAuthn MFA für eine Speicher-VM oder für einen Cluster anzeigen.

Schritte

1. Listen Sie die unterstützten öffentlichen WebAuthn MFA-Algorithmen auf. Sie können optional eine Storage-VM mit dem Argument angeben `vserver`:

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

Erfahren Sie mehr über `security webauthn supported-algorithms show` in der "ONTAP-Befehlsreferenz".

Registrierte WebAuthn-MFA-Anmeldedaten anzeigen

Als ONTAP-Administrator können Sie die registrierten WebAuthn-Anmeldeinformationen für alle Benutzer anzeigen. Benutzer, die dieses Verfahren nicht von Administratoren verwenden, können nur ihre eigenen registrierten WebAuthn-Anmeldedaten anzeigen.

Schritte

1. Registrierte WebAuthn-MFA-Anmeldedaten anzeigen:

```
security webauthn credentials show
```

Erfahren Sie mehr über `security webauthn credentials show` in der "ONTAP-Befehlsreferenz".

Entfernen Sie eine registrierte WebAuthn-MFA-Anmeldeinformation

Sie können registrierte WebAuthn-MFA-Anmeldeinformationen entfernen. Dies ist nützlich, wenn der Hardwareschlüssel eines Benutzers verloren gegangen ist, gestohlen wurde oder nicht mehr verwendet wird. Sie können auch registrierte Anmeldeinformationen entfernen, wenn der Benutzer noch über den ursprünglichen Hardwareauthentifizator verfügt, ihn aber durch einen neuen ersetzen möchte. Nach dem Entfernen der Anmeldeinformationen wird der Benutzer aufgefordert, den Ersatz-Authentifikator zu registrieren.

Durch das Entfernen von registrierten Anmeldeinformationen für einen Benutzer wird WebAuthn MFA für den Benutzer nicht deaktiviert. Wenn ein Benutzer einen Hardware-Authentifikator verliert und sich vor dem Ersetzen anmelden muss, müssen Sie die Anmeldeinformationen mithilfe dieser Schritte und auch für den Benutzer entfernen"Deaktivieren Sie WebAuthn MFA".

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie das Pfeilsymbol neben **Users and Roles**.
3. Wählen Sie in der Liste der Benutzer und Gruppen das Optionsmenü für den Benutzer oder die Gruppe aus, dessen Anmeldeinformationen Sie entfernen möchten.
4. Wählen Sie **MFA für HTTP-Anmeldeinformationen entfernen**.
5. Wählen Sie **Entfernen**.

CLI

1. Löschen Sie die registrierten Anmeldedaten. Beachten Sie Folgendes:
   - Sie können optional eine Storage-VM des Benutzers angeben. Wenn sie nicht angegeben sind, werden die Zugangsdaten auf Cluster-Ebene entfernt.
   - Sie können optional einen Benutzernamen des Benutzers angeben, für den Sie die Anmeldeinformationen löschen möchten. Wenn sie nicht angegeben ist, werden die Anmeldeinformationen für den aktuellen Benutzer entfernt.

     ```
     security webauthn credentials delete -vserver <storage_vm_name>
     -username <username>
     ```

     Erfahren Sie mehr über `security webauthn credentials delete` in der "ONTAP-Befehlsreferenz".

Verwalten von Webservices

Web Services-Übersicht verwalten

Sie können einen Webdienst für das Cluster oder eine Storage Virtual Machine (SVM) aktivieren bzw. deaktivieren, die Einstellungen für Webservices anzeigen und festlegen, ob Benutzer einer Rolle auf einen Webservice zugreifen können.

Es gibt folgende Möglichkeiten, Web-Services für das Cluster oder eine SVM zu managen:

- Aktivieren oder Deaktivieren eines bestimmten Webservice
- Festlegen, ob der Zugriff auf einen Webdienst nur auf verschlüsseltes HTTP (SSL) beschränkt ist
- Anzeigen der Verfügbarkeit von Webservices
- Benutzern einer Rolle den Zugriff auf einen Webservice zu ermöglichen oder zu verdrängen
- Anzeigen der Rollen, die auf einen Webdienst zugreifen dürfen

Damit ein Benutzer auf einen Webdienst zugreifen kann, müssen alle folgenden Bedingungen erfüllt sein:

- Der Benutzer muss authentifiziert sein.

  Beispielsweise kann ein Webdienst einen Benutzernamen und ein Kennwort anfordern. Die Antwort des Benutzers muss mit einem gültigen Konto übereinstimmen.

- Der Benutzer muss mit der richtigen Zugriffsmethode eingerichtet sein.

  Authentifizierung ist nur für Benutzer mit der richtigen Zugriffsmethode für den angegebenen Webdienst erfolgreich. Für den Webservice der ONTAP-API (`ontapi`) müssen Benutzer über die `ontapi` Zugriffsmethode verfügen. Für alle anderen Webdienste müssen Benutzer über die `http` Zugriffsmethode verfügen.

  > Sie verwenden die `security login` Befehle, um die Zugriffsmethoden und Authentifizierungsmethoden von Benutzern zu verwalten.

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

  > Sie verwenden die `vserver services web access` Befehle, um den Zugriff einer Rolle auf einen Webdienst zu steuern.

Wenn eine Firewall aktiviert ist, muss die Firewallrichtlinie für die Nutzung von LIF für Web-Services so eingerichtet sein, dass HTTP oder HTTPS möglich sind.

Wenn Sie HTTPS für den Webservice-Zugriff verwenden, muss auch die SSL für das Cluster oder die SVM mit dem Webservice aktiviert sein. Des Weiteren müssen Sie ein digitales Zertifikat für das Cluster oder die SVM vorlegen.

Verwalten des Zugriffs auf ONTAP -Webdienste

Ein Webservice ist eine Anwendung, auf die Benutzer über HTTP oder HTTPS zugreifen können. Der Clusteradministrator kann die Web-Protokoll-Engine einrichten, SSL konfigurieren, einen Webdienst aktivieren und Benutzern einer Rolle den Zugriff auf einen Webdienst ermöglichen.

Ab ONTAP 9.6 werden die folgenden Webservices unterstützt:

- Service-Prozessor-Infrastruktur (`spi`)

  Dieser Service stellt Protokoll, Core Dump und MIB-Dateien für HTTP- oder HTTPS-Zugriff über die Cluster-Management-LIF oder Node-Management-LIF bereit. Die Standardeinstellung ist `enabled`.

  Bei einer Anfrage zum Zugriff auf die Protokolldateien oder Core-Dump-Dateien eines Knotens wird der `spi` Der Webdienst erstellt automatisch einen Einhängepunkt von einem Knoten zum Stammvolume eines anderen Knotens, auf dem sich die Dateien befinden. Sie müssen den Einhängepunkt nicht manuell erstellen.

- ONTAP-APIs (`ontapi`)

  Mit diesem Service können Sie ONTAP APIs ausführen und administrative Funktionen mit einem Remote-Programm ausführen. Die Standardeinstellung ist `enabled`.

  Dieser Service ist möglicherweise für einige externe Verwaltungstools erforderlich. Wenn Sie beispielsweise System Manager verwenden, sollten Sie diesen Service aktiviert lassen.

- Data ONTAP-Ermittlung(`disco`)

  Dieser Service ermöglicht Off-Box-Managementapplikationen, den Cluster im Netzwerk zu erkennen. Die

Standardeinstellung ist `enabled`.

- Support-Diagnose (`supdiag`)

  Dieser Service steuert den Zugriff auf eine privilegierte Umgebung des Systems, um die Problemanalyse und -Behebung zu unterstützen. Die Standardeinstellung ist `disabled`. Sie sollten diesen Service nur aktivieren, wenn Sie sich unter Anleitung durch den technischen Support richten.

- System Manager (`sysmgr`)

  Dieser Service steuert die Verfügbarkeit von System Manager, der in ONTAP enthalten ist. Die Standardeinstellung ist `enabled`. Dieser Service wird nur auf dem Cluster unterstützt.

- Firmware Baseboard Management Controller (BMC) Update (`FW_BMC`)

  Mit diesem Service können Sie BMC-Firmware-Dateien herunterladen. Die Standardeinstellung ist `enabled`.

- ONTAP Dokumentation (`docs`)

  Dieser Service bietet Zugriff auf die ONTAP-Dokumentation. Die Standardeinstellung ist `enabled`.

- ONTAP RESTful APIs(`docs_api`

  Dieser Service bietet Zugriff auf die Dokumentation der ONTAP RESTful API. Die Standardeinstellung ist `enabled`.

- Datei hochladen und herunterladen (`fud`)

  Dieser Service bietet Datei-Upload und Download. Die Standardeinstellung ist `enabled`.

- ONTAP-Nachrichten (`ontapmsg`)

  Dieser Service unterstützt eine Schnittstelle für Veröffentlichung und Abonnements, über die Sie Ereignisse abonnieren können. Die Standardeinstellung ist `enabled`.

- ONTAP-Portal (`portal`)

  Dieser Service implementiert das Gateway auf einem virtuellen Server. Die Standardeinstellung ist `enabled`.

- ONTAP RESTful-Schnittstelle (`rest`)

  Dieser Service unterstützt eine RESTful Schnittstelle, über die alle Elemente der Cluster-Infrastruktur per Remote-Zugriff gemanagt werden. Die Standardeinstellung ist `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

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

- SAML-Dienstanbieter (`saml-sp`)

Dieser Service bietet Services wie SP-Metadaten und den Assertion Consumer Service an den Service Provider. Die Standardeinstellung ist `enabled`.

Ab ONTAP 9.7 werden die folgenden zusätzlichen Services unterstützt:

- Sicherungsdateien Für Die Konfiguration (`backups`)

  Dieser Service ermöglicht Ihnen das Herunterladen von Backup-Konfigurationsdateien. Die Standardeinstellung ist `enabled`.

- ONTAP-Sicherheit(`security`)

  Dieser Service unterstützt das CSRF-Token-Management für eine erweiterte Authentifizierung. Die Standardeinstellung ist `enabled`.

Verwalten Sie die Webprotokollengine in ONTAP

Sie können die Web Protocol Engine auf dem Cluster so konfigurieren, dass festgelegt wird, ob Webzugriff zulässig ist und welche SSL-Versionen verwendet werden können. Sie können auch die Konfigurationseinstellungen für die Web-Protokoll-Engine anzeigen.

Sie haben folgende Möglichkeiten, die Web-Protokoll-Engine auf Cluster-Ebene zu verwalten:

- Sie können angeben, ob Remote-Clients HTTP oder HTTPS für den Zugriff auf Webdienstinhalte verwenden können `system services web modify -external`, indem Sie den Befehl mit dem Parameter verwenden.
- Mit dem `security config modify` Befehl mit dem `-supported-protocol` Parameter können Sie festlegen, ob SSLv3 für den sicheren Webzugriff verwendet werden soll. SSLv3 ist standardmäßig deaktiviert. Transport Layer Security 1.0 (TLSv1.0) ist aktiviert und kann bei Bedarf deaktiviert werden.

  Erfahren Sie mehr über `security config modify` in der "ONTAP-Befehlsreferenz".

- Sie können den Compliance-Modus des Federal Information Processing Standard (FIPS) 140-2 für Cluster-weite Webservice-Schnittstellen auf Kontrollebene aktivieren.

  ⓘ Der FIPS 140-2-2-Compliance-Modus ist standardmäßig deaktiviert.

  - **Wenn der FIPS 140-2-Compliance-Modus deaktiviert ist** können Sie den FIPS 140-2-Compliance-Modus aktivieren `is-fips-enabled true` `security config modify`, indem Sie den Parameter für den `security config show` Befehl auf setzen und dann den Online-Status mit dem Befehl bestätigen.
  - **Wenn der FIPS 140-2-Konformitätsmodus aktiviert ist**
    - Ab ONTAP 9.11.1 sind TLSv1, TLSv1.1 und SSLv3 deaktiviert, und nur TSLv1.2 und TSLv1.3 bleiben aktiviert. Sie wirkt sich auf andere interne und externe Systeme und Kommunikation mit ONTAP 9 aus. Wenn Sie den FIPS 140-2 Compliance-Modus aktivieren und anschließend deaktivieren, bleiben TLSv1, TLSv1.1 und SSLv3 deaktiviert. Je nach vorheriger Konfiguration bleibt entweder TLSv1.2 oder TLSv1.3 aktiviert.
    - Für Versionen von ONTAP vor 9.11.1 sind TLSv1 und SSLv3 deaktiviert, und nur TLSv1.1 und TLSv1.2 bleiben aktiviert. ONTAP verhindert, dass Sie TLSv1 und SSLv3 aktivieren, wenn der Compliance-Modus nach FIPS 140-2 aktiviert ist. Wenn Sie den FIPS 140-2-Compliance-Modus

aktivieren und anschließend deaktivieren, bleiben TLSv1 und SSLv3 deaktiviert, jedoch sind je nach vorheriger Konfiguration entweder TLSv1.2 oder TLSv1.1 und TLSv1.2 aktiviert.

- Sie können die Konfiguration der Sicherheit für das gesamte Cluster mit dem `system security config show` Befehl anzeigen.

  Erfahren Sie mehr über `security config show` in der "ONTAP-Befehlsreferenz".

Wenn die Firewall aktiviert ist, muss die Firewallrichtlinie für die logische Schnittstelle (LIF) eingerichtet werden, die für Webservices verwendet werden soll, damit HTTP- oder HTTPS-Zugriff möglich ist.

Wenn Sie HTTPS für den Webservice-Zugriff verwenden, muss auch die SSL für das Cluster oder die Storage Virtual Machine (SVM) mit dem Web-Service aktiviert sein. Des Weiteren müssen Sie ein digitales Zertifikat für das Cluster oder die SVM angeben.

In MetroCluster Konfigurationen werden die von Ihnen vorgenommenen Änderungen an der Web Protocol Engine eines Clusters nicht im Partner-Cluster repliziert.

ONTAP -Befehle zur Verwaltung der Webprotokoll-Engine

Sie verwenden die `system services web` Befehle, um die Web-Protokoll-Engine zu verwalten. Mit den `system services firewall policy create` `network interface modify` Befehlen und können Sie zulassen, dass Webzugriffsanfragen durch die Firewall geleitet werden.

Ihr Ziel ist	Befehl
Konfigurieren Sie die Web Protocol Engine auf Cluster-Ebene: • Aktiviert oder deaktiviert die Web Protocol Engine für das Cluster • Aktivieren oder deaktivieren Sie SSLv3 für das Cluster • Aktivieren oder Deaktivieren der Compliance nach FIPS 140-2 für sichere Web-Services (HTTPS)	`system services web modify`
Anzeige der Konfiguration der Web Protocol Engine auf Cluster-Ebene, Ermittlung der Funktionsfähigkeit der Webprotokolle im gesamten Cluster und Anzeige der online-aktivierten FIPS 140-2-Compliance-Funktionen	`system services web show`
Zeigt die Konfiguration der Web-Protokoll-Engine auf Node-Ebene und die Aktivitäten der Webservice-Handhabung für die Knoten im Cluster an	`system services web node show`

Ihr Ziel ist	Befehl
Erstellen Sie eine Firewallrichtlinie oder fügen Sie einem vorhandenen Firewallrichtlinie HTTP- oder HTTPS-Protokollservice hinzu, um Webzugriffsanfragen durch die Firewall zu durchlaufen	`system services firewall policy create` Wenn Sie den `-service` Parameter auf `http` oder `https` setzen, können Webzugriffsanfragen über die Firewall geleitet werden.
Zuordnen einer Firewallrichtlinie zu einer logischen Schnittstelle	`network interface modify` Sie können den `-firewall-policy` Parameter verwenden, um die Firewallrichtlinie einer logischen Schnittstelle zu ändern.

Verwandte Informationen

- "Änderung der Netzwerkschnittstelle"

Konfigurieren des Zugriffs auf ONTAP Webdienste

Durch die Konfiguration des Zugriffs auf Webservices können autorisierte Benutzer HTTP oder HTTPS verwenden, um auf den Service-Inhalt des Clusters oder eine Storage Virtual Machine (SVM) zuzugreifen.

Schritte

1. Wenn eine Firewall aktiviert ist, stellen Sie sicher, dass in der Firewallrichtlinie für die LIF HTTP- oder HTTPS-Zugriffe eingerichtet sind, die für Web-Services verwendet werden:

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

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

      Sie setzen den `-service` Parameter des `system services firewall policy create` Befehls auf `http` oder `https`, um die Richtlinie für den Webzugriff zu aktivieren.

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

      Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

      Sie verwenden den `network interface modify` Befehl mit dem `-firewall-policy` Parameter, um die Firewallrichtlinie für eine LIF anzuwenden.

   Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

2. Um die Web-Protokoll-Engine auf Cluster-Ebene zu konfigurieren und den Zugriff auf Web-Service-Inhalte `system services web modify` zu ermöglichen, verwenden Sie den Befehl.

3. Wenn Sie planen, sichere Webservices (HTTPS) zu verwenden, aktivieren Sie SSL und stellen Sie mit dem `security ssl modify` Befehl digitale Zertifikatinformationen für den Cluster oder die SVM bereit.

   Erfahren Sie mehr über `security ssl modify` in der "ONTAP-Befehlsreferenz".

4. Um einen Web Service für das Cluster oder die SVM zu aktivieren, verwenden Sie den `vserver services web modify` Befehl.

   Sie müssen diesen Schritt für jeden Service wiederholen, den Sie für das Cluster oder die SVM aktivieren möchten.

5. Um eine Rolle für den Zugriff auf Webservices im Cluster oder der SVM `vserver services web access create` zu autorisieren, verwenden Sie den Befehl.

   Die Rolle, die Sie Zugriff gewähren, muss bereits vorhanden sein. Sie können vorhandene Rollen mit dem `security login role show` Befehl anzeigen oder mit dem `security login role create` Befehl neue Rollen erstellen.

   Erfahren Sie mehr über `security login role show` und `security login role create` in der "ONTAP-Befehlsreferenz".

6. Für eine Rolle, die für den Zugriff auf einen Webdienst autorisiert wurde, stellen Sie sicher `security login show`, dass die Benutzer auch mit der richtigen Zugriffsmethode konfiguriert sind, indem Sie die Ausgabe des Befehls überprüfen.

   Um auf den Webservice der ONTAP API zuzugreifen `ontapi`, muss ein Benutzer mit der `ontapi` Zugriffsmethode konfiguriert werden. Um auf alle anderen Webservices zugreifen `http` zu können, muss ein Benutzer mit der Zugriffsmethode konfiguriert sein.

   Erfahren Sie mehr über `security login show` in der "ONTAP-Befehlsreferenz".

   ⓘ Sie verwenden den `security login create` Befehl, um eine Zugriffsmethode für einen Benutzer hinzuzufügen. Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

ONTAP -Befehle zur Verwaltung von Webdiensten

Mit den `vserver services web` Befehlen managen Sie die Verfügbarkeit von Web-Services für das Cluster oder eine Storage Virtual Machine (SVM). Sie verwenden die `vserver services web access` Befehle, um den Zugriff einer Rolle auf einen Webdienst zu steuern.

Ihr Ziel ist	Befehl
Konfigurieren eines Webservice für das Cluster oder anSVM: • Aktivieren oder Deaktivieren eines Webservice • Geben Sie an, ob nur HTTPS für den Zugriff auf einen Webdienst verwendet werden kann	`vserver services web modify`

Ihr Ziel ist	Befehl
Anzeigen der Konfiguration und Verfügbarkeit von Webservices für das Cluster oder eine anSVM	`vserver services web show`
Autorisieren eine Rolle für den Zugriff auf einen Web-Service auf dem Cluster oder einer anSVM	`vserver services web access create`
Zeigen Sie die Rollen an, die für den Zugriff auf Webservices im Cluster oder auf anSVM autorisiert sind	`vserver services web access show`
Verhindern Sie, dass eine Rolle auf einen Webservice auf dem Cluster oder einer anSVM zugreift	`vserver services web access delete`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

Befehle zum Verwalten von Mount-Punkten auf ONTAP -Knoten

Der `spi` Webdienst erstellt automatisch einen Bereitstellungspunkt von einem Node zum Root-Volume eines anderen Node, wenn auf die Protokolldateien oder Kerndateien des Node zugegriffen werden soll. Obwohl Sie Mount-Punkte nicht manuell verwalten müssen, können Sie dies mithilfe der `system node root-mount` Befehle tun.

Ihr Ziel ist	Befehl
Erstellen Sie manuell einen Mount-Punkt von einem Node zum Root-Volume eines anderen Nodes	`system node root-mount create` Von einem Node zum anderen kann nur ein einzelner Bereitstellungspunkt vorhanden sein.
Zeigen Sie vorhandene Mount-Punkte auf den Nodes im Cluster an, einschließlich der Zeit, die ein Mount-Punkt erstellt wurde, und des aktuellen Status	`system node root-mount show`
Löschen Sie einen Bereitstellungspunkt von einem Node zum Root-Volume eines anderen Node, und erzwingen Sie die Verbindungen zum Mount-Punkt zum Schließen	`system node root-mount delete`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

SSL in ONTAP verwalten

Verwenden Sie die `security ssl` Befehle, um das SSL-Protokoll für das Cluster oder eine SVM (Storage Virtual Machine) zu managen. Das SSL-Protokoll verbessert die Sicherheit des Webzugriffs, indem es ein digitales Zertifikat verwendet, um eine

verschlüsselte Verbindung zwischen einem Webserver und einem Browser herzustellen.

Sie haben folgende Möglichkeiten, SSL für das Cluster oder eine Storage Virtual Machine (SVM) zu verwalten:

- Aktivieren von SSL
- Generieren und Installieren eines digitalen Zertifikats und Verknüpfen eines Zertifikats mit dem Cluster oder der SVM
- Anzeigen der SSL-Konfiguration zur Bestätigung, ob SSL aktiviert wurde, und, falls verfügbar, der Name des SSL-Zertifikats
- Einrichtung von Firewallrichtlinien für das Cluster oder SVM, um Webzugriffsanfragen durchzuführen
- Definieren, welche SSL-Versionen verwendet werden können
- Beschränkung des Zugriffs auf nur HTTPS-Anforderungen für einen Webdienst

Befehle zum Verwalten von SSL

Mit den `security ssl` Befehlen managen Sie das SSL-Protokoll für den Cluster oder eine Storage Virtual Machine (SVM).

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

Erfahren Sie mehr über `security ssl modify` und `security ssl show` in der "ONTAP-Befehlsreferenz".

Verwenden Sie HSTS für ONTAP Webdienste

HTTP Strict Transport Security (HSTS) ist ein Mechanismus für Websicherheitsrichtlinien, der Websites vor Man-in-the-Middle-Angriffen wie Protokoll-Downgrades und Cookie-Hijacking schützt. Durch die erzwungene Verwendung von HTTPS stellt HSTS sicher, dass die gesamte Kommunikation zwischen dem Browser des Benutzers und dem Server verschlüsselt ist. Ab ONTAP 9.17.1 kann ONTAP HTTPS-Verbindungen für ONTAP Webdienste erzwingen.

> HSTS wird vom Webbrowser erst erzwungen, nachdem eine erste sichere HTTPS-Verbindung mit ONTAP hergestellt wurde. Wenn der Browser keine erste sichere Verbindung herstellt, wird HSTS nicht erzwungen. Informationen zur HSTS-Verwaltung finden Sie in der Dokumentation Ihres Browsers.

Über diese Aufgabe

- Ab Version 9.17.1 ist HSTS für neu installierte ONTAP Cluster standardmäßig aktiviert. Beim Upgrade auf 9.17.1 ist HSTS standardmäßig deaktiviert. Sie müssen HSTS nach dem Upgrade aktivieren.
- HSTS wird für alle unterstützt "ONTAP -Webdienste" .

Bevor Sie beginnen

- Für die folgenden Aufgaben sind erweiterte Berechtigungen erforderlich.

HSTS-Konfiguration anzeigen

Sie können die aktuelle HSTS-Konfiguration anzeigen, um zu überprüfen, ob sie aktiviert ist, und die Einstellung für das maximale Alter anzeigen.

Schritte

1. Verwenden Sie die `system services web show` Befehl zum Anzeigen der aktuellen Webdienstkonfiguration, einschließlich der HSTS-Einstellungen:

```
cluster-1::system services web*> show

                   External Web Services: true
                               HTTP Port: 80
                              HTTPS Port: 443
                         Protocol Status: online
                      Per Address Limit: 80
                    Wait Queue Capacity: 192
                           HTTP Enabled: true
                 CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
         Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                           HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

Aktivieren Sie HSTS und legen Sie das Höchstalter fest

Ab ONTAP 9.17.1 ist HSTS auf neuen ONTAP Clustern standardmäßig aktiviert. Wenn Sie einen vorhandenen Cluster auf 9.17.1 oder höher aktualisieren, müssen Sie HSTS manuell aktivieren, um die Verwendung von HTTPS zu erzwingen. Sie können HSTS aktivieren und das maximale Alter festlegen. Sie können das maximale Alter jederzeit ändern, wenn HSTS aktiviert ist. Sobald HSTS aktiviert ist, erzwingen Browser sichere Verbindungen erst, nachdem eine erste sichere Verbindung hergestellt wurde.

Schritte

1. Verwenden Sie die `system services web modify` Befehl zum Aktivieren von HSTS oder Ändern des Höchstalters:

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age` Gibt die Dauer in Sekunden an, für die der Browser die HTTPS-Erzwingung speichert. Der Standardwert beträgt 63072000 Sekunden (zwei Jahre).

HSTS deaktivieren

Browser speichern die Einstellung für das maximale HSTS-Alter bei jeder Verbindung und setzen HSTS während der gesamten Dauer durch, selbst wenn HSTS auf ONTAP deaktiviert ist. Nach der Deaktivierung dauert es bis zur konfigurierten maximalen Altersdauer, bis der Browser die HSTS-Durchsetzung beendet. Sollte während dieser Zeit keine sichere Verbindung möglich sein, erlauben Browser, die HSTS erzwingen, keinen Zugriff auf ONTAP Webdienste, bis das Problem behoben ist oder die maximale Altersgrenze des Browsers abgelaufen ist.

Schritte

1. Deaktivieren Sie HSTS mit dem `system services web modify` Befehl:

```
system services web modify -hsts-enabled false
```

Verwandte Informationen

"RFC 6797 – HTTP Strict Transport Security (HSTS)"

Beheben von Problemen beim Zugriff auf ONTAP Webdienste

Konfigurationsfehler führen zu Problemen mit dem Webservice-Zugriff. Sie können die Fehler beheben, indem Sie sicherstellen, dass LIF, Firewall-Richtlinie, Web-Protokoll-Engine, Web-Services, digitale Zertifikate, Und die Benutzerzugriffsautorisierung sind alle richtig konfiguriert.

Die folgende Tabelle hilft Ihnen bei der Identifizierung und Behebung von Fehlern bei der Webservice-Konfiguration:

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Ihr Webbrowser gibt einen `unable to connect failure to establish a connection` Fehler oder zurück, wenn Sie versuchen, auf einen Webdienst zuzugreifen.	Ihr LIF ist möglicherweise falsch konfiguriert.	Stellen Sie sicher, dass Sie die LIF anpingen können, die den Webservice bereitstellt. Sie verwenden den `network ping` Befehl, um eine LIF zu pingen.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Ihre Firewall ist möglicherweise falsch konfiguriert. Sie verwenden die `system services firewall policy` Befehle zum Verwalten von Firewallrichtlinien. Sie verwenden den `network interface modify` Befehl mit dem `-firewall -policy` Parameter, um eine Richtlinie einer LIF zuzuordnen.	Vergewissern Sie sich, dass eine Firewallrichtlinie eingerichtet ist, um HTTP oder HTTPS zu unterstützen und die Richtlinie der logischen Schnittstelle, die den Webservice bereitstellt, zugewiesen ist.	Ihre Web-Protokoll-Engine ist möglicherweise deaktiviert.
Stellen Sie sicher, dass die Web Protocol Engine aktiviert ist, damit Webservices verfügbar sind. Sie verwenden die `system services web` Befehle, um die Web-Protokoll-Engine für den Cluster zu verwalten.	Ihr Webbrowser gibt einen `not found` Fehler zurück, wenn Sie versuchen, auf einen Webdienst zuzugreifen.	Der Webdienst ist möglicherweise deaktiviert.
Stellen Sie sicher, dass jeder Webdienst, auf den Sie Zugriff zulassen möchten, individuell aktiviert ist. Sie verwenden den `vserver services web modify` Befehl, um einen Webdienst für den Zugriff zu aktivieren.	Der Webbrowser meldet sich nicht bei einem Webdienst mit dem Kontonamen und Passwort eines Benutzers an.	Der Benutzer kann nicht authentifiziert werden, die Zugriffsmethode ist nicht korrekt oder der Benutzer ist nicht berechtigt, auf den Webdienst zuzugreifen.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Stellen Sie sicher, dass das Benutzerkonto vorhanden ist und mit der richtigen Zugriffsmethode und Authentifizierungsmethode konfiguriert ist. Stellen Sie außerdem sicher, dass die Rolle des Benutzers für den Zugriff auf den Webdienst autorisiert ist. Sie verwenden die `security login` Befehle, um Benutzerkonten und ihre Zugriffsmethoden und Authentifizierungsmethoden zu verwalten. Für den Zugriff auf den Webservice der ONTAP-API ist die `ontapi` Zugriffsmethode erforderlich. Für den Zugriff auf alle anderen Webdienste `http` ist die Zugriffsmethode erforderlich. Sie verwenden die `vserver services web access` Befehle, um den Zugriff einer Rolle auf einen Webdienst zu verwalten.	Sie stellen eine Verbindung zu Ihrem Webdienst über HTTPS her, und Ihr Webbrowser zeigt an, dass die Verbindung unterbrochen wird.	Möglicherweise ist SSL nicht auf dem Cluster oder der Storage Virtual Machine (SVM) aktiviert, die den Webservice bereitstellt.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Vergewissern Sie sich, dass für den Cluster oder die SVM SSL aktiviert ist und das digitale Zertifikat gültig ist. Sie verwenden die `security ssl` Befehle, um die SSL-Konfiguration für HTTP-Server `security certificate show` zu verwalten, und den Befehl, um digitale Zertifikatinformation en anzuzeigen.	Sie stellen eine Verbindung zu Ihrem Webdienst über HTTPS her, und Ihr Webbrowser zeigt an, dass die Verbindung nicht vertrauenswürdig ist.	Möglicherweise verwenden Sie ein selbstsigniertes digitales Zertifikat.

Verwandte Informationen

- "Was sind Best Practices für die Netzwerkkonfiguration für ONTAP?"
- "Netzwerk-Ping"
- "Änderung der Netzwerkschnittstelle"
- "Sicherheitszertifikat generieren-csr"
- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "Sicherheit SSL"

Überprüfen Sie die Identität der Remoteserver mit Zertifikaten

Erfahren Sie mehr über die Überprüfung der Identität von Remote-Servern mithilfe von Zertifikaten in ONTAP

ONTAP unterstützt die Funktionen für Sicherheitszertifikate zur Überprüfung der Identität von Remote-Servern.

Die ONTAP Software ermöglicht sichere Verbindungen unter Verwendung dieser digitalen Zertifikatfunktionen und -Protokolle:

- Online Certificate Status Protocol (OCSP) validiert den Status von digitalen Zertifikatsanforderungen von ONTAP-Diensten mithilfe von SSL- und TLS-Verbindungen (Transport Layer Security). Diese Funktion ist standardmäßig deaktiviert.
- Die ONTAP-Software enthält standardmäßig vertrauenswürdige Stammzertifikate.
- KMIP-Zertifikate (Key Management Interoperability Protocol) ermöglichen die gegenseitige

Authentifizierung eines Clusters und eines KMIP-Servers.

Überprüfen Sie die Gültigkeit digitaler Zertifikate mit OCSP in ONTAP

Mithilfe des Online Certificate Status Protocol (OCSP) können ONTAP -Anwendungen, die TLS-Kommunikation (Transport Layer Security) verwenden, den Status digitaler Zertifikate empfangen, wenn OCSP aktiviert ist. Sie können OCSP-Zertifikatsprüfungen für bestimmte Anwendungen jederzeit aktivieren oder deaktivieren. Standardmäßig ist die Überprüfung des OCSP-Zertifikatsstatus deaktiviert.

Bevor Sie beginnen

Sie benötigen einen erweiterten Zugriff auf die Berechtigungsebene, um diese Aufgabe ausführen zu können.

Über diese Aufgabe

OCSP unterstützt folgende Anwendungen:

- AutoSupport
- Event Management System (EMS)
- LDAP über TLS
- Key Management Interoperability Protocol (KMIP)
- Audit-Protokollierung
- FabricPool
- SSH (ab ONTAP 9.13.1)

Schritte

1. Stellen Sie die Berechtigungsebene auf erweitert: `set -privilege advanced`.
2. Um OCSP-Zertifikatsprüfungen für bestimmte ONTAP-Anwendungen zu aktivieren oder zu deaktivieren, verwenden Sie den entsprechenden Befehl.

Wenn Sie möchten, dass OCSP-Zertifikatsprüfungen für einige Anwendungen…	Verwenden Sie den Befehl…
Aktiviert	`security config ocsp enable -app app name`
Deaktiviert	`security config ocsp disable -app app name`

Mit dem folgenden Befehl wird OCSP-Unterstützung für AutoSupport und EMS aktiviert.

```
cluster::*> security config ocsp enable -app asup,ems
```

Wenn OCSP aktiviert ist, erhält die Anwendung eine der folgenden Antworten:

◦ Gut - das Zertifikat ist gültig und die Kommunikation wird fortgesetzt.

- Widerrufen: Das Zertifikat wird von der ausstellenden Zertifizierungsstelle dauerhaft als nicht vertrauenswürdig eingestuft und die Kommunikation kann nicht fortgesetzt werden.
- Unbekannt – der Server verfügt über keine Statusinformationen zum Zertifikat und die Kommunikation kann nicht fortgesetzt werden.
- OCSP-Serverinformationen fehlen im Zertifikat - der Server fungiert als deaktiviert und fährt mit der TLS-Kommunikation fort, aber es erfolgt keine Statusüberprüfung.
- Keine Antwort vom OCSP-Server - die Anwendung schlägt fehl.

3. Verwenden Sie den entsprechenden Befehl, um OCSP-Zertifikatsprüfungen für alle Anwendungen mithilfe von TLS-Kommunikation zu aktivieren oder zu deaktivieren.

Wenn Sie möchten, dass OCSP-Zertifikatsprüfungen für alle Anwendungen durchgeführt werden…	**Verwenden Sie den Befehl…**
Aktiviert	`security config ocsp enable -app all`
Deaktiviert	`security config ocsp disable -app all`

Wenn alle Applikationen aktiviert sind, wird eine signierte Antwort empfangen, die angibt, dass das angegebene Zertifikat in Ordnung, annulliert oder unbekannt ist. Im Fall eines annulliert Zertifikats kann die Anwendung nicht fortgesetzt werden. Wenn die Anwendung keine Antwort vom OCSP-Server erhält oder der Server nicht erreichbar ist, wird die Anwendung nicht fortgesetzt.

4. Verwenden Sie den `security config ocsp show` Befehl, um alle Anwendungen anzuzeigen, die OCSP unterstützen, und ihren Supportstatus.

```
cluster::*> security config ocsp show
         Application                     OCSP Enabled?
         --------------------            ---------------------
         autosupport                     false
         audit_log                       false
         fabricpool                      false
         ems                             false
         kmip                            false
         ldap_ad                         true
         ldap_nis_namemap                true
         ssh                             true

         8 entries were displayed.
```

Verwandte Informationen

- "Sicherheitskonfiguration OCSP aktivieren"

- "Sicherheitskonfiguration OCSP deaktivieren"
- "Sicherheitskonfiguration OCSP anzeigen"

Standardzertifikate für TLS-basierte Anwendungen in ONTAP anzeigen

ONTAP bietet einen Standardsatz vertrauenswürdiger Stammzertifikate für ONTAP -Anwendungen mit Transport Layer Security (TLS).

Bevor Sie beginnen

Die Standardzertifikate werden nur während der Erstellung oder während eines Upgrades auf der Admin-SVM installiert.

Über diese Aufgabe

Die aktuellen Applikationen, die als Client fungieren und eine Zertifikatvalidierung erfordern, sind AutoSupport, EMS, LDAP, Audit Logging, FabricPool, Und KMIP.

Wenn Zertifikate ablaufen, wird eine EMS-Nachricht aufgerufen, die den Benutzer zum Löschen der Zertifikate auffordert. Die Standardzertifikate können nur auf der erweiterten Berechtigungsebene gelöscht werden.

> Das Löschen der Standardzertifikate kann dazu führen, dass einige ONTAP-Anwendungen nicht wie erwartet funktionieren (z. B. AutoSupport- und Audit-Protokollierung).

Schritt

1. Sie können die Standardzertifikate, die auf der Admin-SVM installiert sind, anzeigen. Verwenden Sie dazu den Befehl „Security Certificate show“:

   `security certificate show -vserver –type server-ca`

   ```
   cluster1::> security certificate show

   Vserver    Serial Number   Certificate Name
   Type
   ---------- --------------- ----------------------------------------
   ---------
   vs0        4F4E4D7B         www.example.com
   server
       Certificate Authority:  www.example.com
             Expiration Date: Thu Feb 28 16:08:28 2013
   ```

   Erfahren Sie mehr über `security certificate show` in der "ONTAP-Befehlsreferenz".

Cluster und KMIP-Server authentifizieren sich gegenseitig

Gegenseitige Authentifizierung des ONTAP Clusters und eines KMIP-Servers – Übersicht

Durch die gegenseitige Authentifizierung des Clusters und eines externen

Schlüsselmanagers wie einem KMIP-Server (Key Management Interoperability Protocol) kann der Schlüsselmanager mithilfe von KMIP über SSL mit dem Cluster kommunizieren. Sie tun dies, wenn eine Applikation oder eine bestimmte Funktion (z. B. die Storage-Verschlüsselung) sicheren Datenzugriff mit sicheren Schlüsseln erfordert.

Generieren Sie eine Zertifikatsignierungsanforderung für das Cluster in ONTAP

Sie können den `generate-csr` Befehl Sicherheitszertifikat verwenden, um eine Zertifikatsignierungsanforderung (CSR) zu generieren. Nach Bearbeitung Ihrer Anfrage sendet Ihnen die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Bevor Sie beginnen

Um diese Aufgabe auszuführen, müssen Sie ein Cluster-Administrator oder SVM-Administrator sein.

Schritte

1. CSR erstellen:

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

Erfahren Sie mehr über `security certificate generate-csr` in der "ONTAP-Befehlsreferenz".

Der folgende Befehl erzeugt einen CSR mit einem 2,048-bit privaten Schlüssel, der von der SHA256 Hashing-Funktion erzeugt wird, zur Verwendung durch die Software-Gruppe in der IT-Abteilung eines Unternehmens mit individuellem gemeinsamen Namen server1.companyname.com, mit Sitz in Sunnyvale, Kalifornien, USA. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet web@example.com. Das System zeigt den CSR und den privaten Schlüssel in der Ausgabe an.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

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

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

Installieren Sie ein CA-signiertes Serverzertifikat für den ONTAP Cluster

Damit ein SSL-Server die Authentifizierung des Clusters oder der Storage Virtual Machine (SVM) als SSL-Client aktiviert, installieren Sie ein digitales Zertifikat mit dem Clienttyp auf dem Cluster oder der SVM. Anschließend stellen Sie dem SSL-Serveradministrator das Client-Ca-Zertifikat zur Installation auf dem Server zur Verfügung.

Bevor Sie beginnen

Sie müssen bereits das Stammzertifikat des SSL-Servers auf dem Cluster oder der SVM mit dem `server-ca` Zertifikatstyp installiert haben.

Schritte

1. Um ein selbstsigniertes digitales Zertifikat für die Clientauthentifizierung `security certificate create type client` zu verwenden, verwenden Sie den Befehl mit dem Parameter.

   Erfahren Sie mehr über `security certificate create` in der "ONTAP-Befehlsreferenz".

2. Gehen Sie wie folgt vor, um ein von einer Zertifizierungsstelle signiertes digitales Zertifikat für die Clientauthentifizierung zu verwenden:

   a. Generieren Sie mithilfe des `generate-csr` Befehls „Sicherheitszertifikat“ eine Anforderung für die Signierung eines digitalen Zertifikats (CSR).

      ONTAP zeigt die CSR-Ausgabe an, die eine Zertifikatanforderung und einen privaten Schlüssel enthält, und erinnert Sie daran, die Ausgabe in eine Datei zu kopieren, um sie später verwenden zu können.

   b. Senden Sie die Zertifikatsanforderung von der CSR-Ausgabe in einem elektronischen Formular (z. B. E-Mail) an eine vertrauenswürdige CA zum Signieren.

      Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten Zertifikats für zukünftige Referenz aufbewahren.

   Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat.

   a. Installieren Sie das CA-signierte Zertifikat `security certificate install` mit dem Befehl mit dem `-type client` Parameter.
   b. Geben Sie das Zertifikat und den privaten Schlüssel ein, wenn Sie dazu aufgefordert werden, und drücken Sie dann **Enter**.
   c. Geben Sie bei der Aufforderung zusätzliche Root- oder Zwischenzertifikate ein, und drücken Sie dann **Enter**.

      Sie installieren ein Zwischenzertifikat auf dem Cluster oder der SVM, wenn eine Zertifikatkette, die an der vertrauenswürdigen Stammzertifizierungsstelle beginnt und mit dem Ihnen ausgestellten SSL-Zertifikat endet, die Zwischenzertifikate fehlen. Ein Zwischenzertifikat ist ein vom vertrauenswürdigen

Stammverzeichnis herausgegebenem untergeordneten Zertifikat, das speziell für die Ausgabe von Serverzertifikaten der Endeinheit ausgegeben wird. Das Ergebnis ist eine Zertifikatskette, die an der vertrauenswürdigen Stammzertifizierungsstelle beginnt, durch das Zwischenzertifikat geht und mit dem Ihnen ausgestellten SSL-Zertifikat endet.

3. Geben Sie `client-ca` dem Administrator des SSL-Servers das Zertifikat des Clusters oder der SVM zur Installation auf dem Server an.

   Mit dem Befehl Security Certificate show mit den `-instance -type client-ca` Parametern und werden die `client-ca` Zertifikatinformationen angezeigt.

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"

Installieren Sie ein CA-signiertes Client-Zertifikat für den KMIP-Server in ONTAP

Der Zertifikatsubtyp des Key Management Interoperability Protocol (KMIP) (der Parameter -subtype kmip-cert) legt gemeinsam mit den Client- und Server-Ca-Typen fest, dass das Zertifikat für die wechselseitige Authentifizierung des Clusters und einen externen Schlüsselmanager, z. B. einen KMIP-Server, verwendet wird.

Über diese Aufgabe

Installieren Sie ein KMIP-Zertifikat, um einen KMIP-Server als SSL-Server für das Cluster zu authentifizieren.

Schritte

1. Verwenden Sie den `security certificate install` Befehl mit den `-type server-ca -subtype kmip-cert` Parametern und, um ein KMIP-Zertifikat für den KMIP-Server zu installieren.
2. Wenn Sie aufgefordert werden, geben Sie das Zertifikat ein, und drücken Sie anschließend die Eingabetaste.

   ONTAP erinnert Sie daran, dass Sie eine Kopie des Zertifikats zur späteren Verwendung aufbewahren.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


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

cluster1::>
```

Verwandte Informationen

- "Sicherheitszertifikat installieren"