Sicherheitsmanagement mit System Manager

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

Sicherheitsmanagement mit System Manager

Überblick über das Sicherheitsmanagement mit System Manager

Ab ONTAP 9.7 managen Sie die Cluster-Sicherheit mit System Manager.

Mit System Manager können Kunden anhand von Standardmethoden von ONTAP den Storage-Zugriff von Clients und Administratoren sichern und sich gegen Viren schützen. Fortschrittliche Technologien stehen zur Verschlüsselung von Daten im Ruhezustand und ALS WORM Storage zur Verfügung.

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

Client-Authentifizierung und -Autorisierung

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

Administratorauthentifizierung und RBAC

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

Virus-Scan

Sie können die integrierte Virenschutzfunktionalität des Storage-Systems verwenden, um Daten vor Viren oder anderen schädlichen Angriffen zu schützen. ONTAP Virus Scanning, genannt *Vscan*, kombiniert erstklassige Antivirensoftware von Drittanbietern mit ONTAP-Funktionen, die Ihnen die Flexibilität geben, die Sie benötigen, um zu kontrollieren, welche Dateien gescannt werden und wann.

Verschlüsselung

ONTAP bietet sowohl Software- als auch hardwarebasierte Verschlüsselungstechnologien, um sicherzustellen, dass Daten im Ruhezustand nicht gelesen werden können, wenn das Storage-Medium neu verwendet, zurückgegeben, verloren gegangen oder gestohlen wird.

WORM-Storage

SnapLock ist eine hochperformante Compliance-Lösung für Unternehmen, die WORM_-Storage (Write Once_, _Read Many) verwenden, um kritische Dateien zu regulatorischen und Governance-Zwecken in unveränderter Form aufzubewahren.

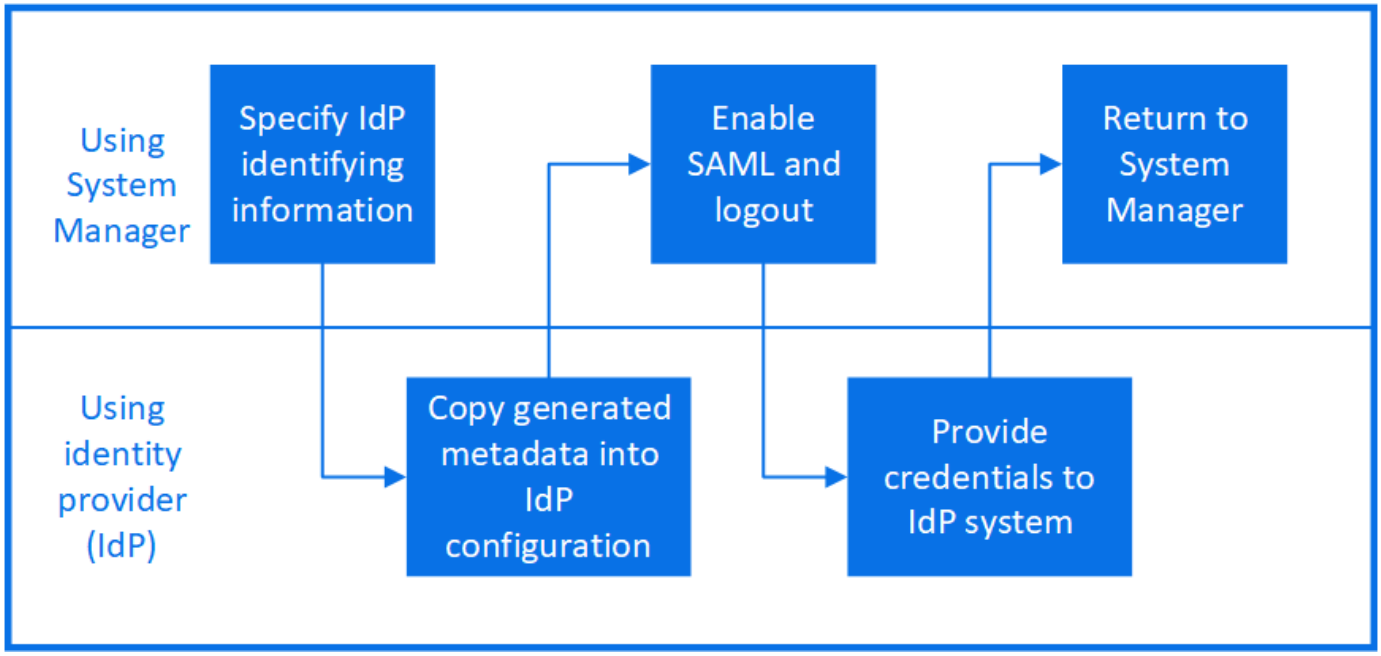
Einrichtung der Multi-Faktor-Authentifizierung

Die SAML-Authentifizierung (Security Assertion Markup Language) ermöglicht Benutzern die Anmeldung bei einer Anwendung über einen sicheren Identitäts-Provider (IdP).

Neben der standardmäßigen ONTAP-Authentifizierung ist in System Manager die SAML-basierte Authentifizierung als Option für die Multi-Faktor-Authentifizierung vorgesehen.

Security Assertion Markup Language (SAML) ist ein XML-basiertes Framework zur Authentifizierung und Autorisierung zwischen zwei Einheiten: Einem Service-Provider und einem Identitäts-Provider.

Aktivieren Sie die SAML-Authentifizierung



So aktivieren Sie die SAML-Authentifizierung:

Schritte

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://").
5. Ändern Sie die Host-System-Adresse, falls erforderlich.
6. Stellen Sie sicher, dass das richtige Zertifikat verwendet wird:
   - Wenn Ihr System nur mit einem Zertifikat mit dem Typ „Server“ zugeordnet war, wird dieses Zertifikat als Standard betrachtet und nicht angezeigt.
   - Wenn Ihr System mit mehreren Zertifikaten als Servertyp zugeordnet war, wird eines der Zertifikate angezeigt. Um ein anderes Zertifikat auszuwählen, klicken Sie auf **Ändern**.
7. Klicken Sie Auf **Speichern**. In einem Bestätigungsfenster werden die Metadateninformationen angezeigt, die automatisch in die Zwischenablage kopiert wurden.
8. Gehen Sie zum IdP-System, das Sie angegeben haben, und kopieren Sie die Metadaten aus der Zwischenablage, um die Systemmetadaten zu aktualisieren.
9. Kehren Sie zum Bestätigungsfenster (im System Manager) zurück und aktivieren Sie das Kontrollkästchen **Ich habe den IdP mit dem Host-URI oder Metadaten** konfiguriert.
10. Klicken Sie auf **Abmelden**, um SAML-basierte Authentifizierung zu aktivieren. Das IdP-System zeigt einen Authentifizierungsbildschirm an.

11. Geben Sie im IdP-System Ihre SAML-basierten Anmeldedaten ein. Nach der Überprüfung Ihrer Anmeldedaten werden Sie zur System Manager Startseite weitergeleitet.

Deaktivieren Sie die SAML-Authentifizierung

So deaktivieren Sie die SAML-Authentifizierung:

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie unter **SAML Authentication** auf die Schaltfläche **aktiviert**.
3. *Optional*: Sie können auch klicken Neben **SAML Authentication** deaktivieren Sie dann das Kontrollkästchen **SAML Authentication** aktivieren.

Kontrolle des Administratorzugriffs

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

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

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

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

Zuweisen einer Rolle zu einem Administrator

Weisen Sie einem Administrator eine Rolle wie folgt zu:

Schritte

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

Ändern der Administratorrolle

Ändern Sie die Rolle für einen Administrator wie folgt:

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.

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

Diagnostizieren und korrigieren Sie Probleme mit dem Dateizugriff

Schritte

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

   Die Trace-Ergebnisse werden in einer Tabelle angezeigt. Die Spalte **Gründe** gibt den Grund, warum auf eine Datei nicht zugegriffen werden konnte.
6. Klicken Sie Auf ⌄ In der linken Spalte der Ergebnistabelle können Sie die Zugriffsrechte für den Dateizugriff anzeigen.

Verwalten von Zertifikaten mit System Manager

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

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

Zeigen Sie Zertifikatinformationen an

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

Schritte

1. Klicken Sie in System Manager auf **Cluster > Einstellungen**.
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. Klicken Sie auf eine beliebige Zahl, um Details zu einer Kategorie von Zertifikaten anzuzeigen, oder klicken Sie auf → So zeigen Sie die Seite **Zertifikate** an, 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. Klicken Sie auf **Storage > Storage VMs**.

b. Wählen Sie die Storage-VM aus.

c. Öffnen Sie die Registerkarte **Einstellungen**.

d. Klicken Sie auf eine Zahl, die im Abschnitt **Zertifikat** angezeigt wird.

Nächste Schritte

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

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

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

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

Schritte

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

Löschen einer vertrauenswürdigen Zertifizierungsstelle

Mit System Manager können Sie eine vertrauenswürdige Zertifizierungsstelle löschen.

ⓘ Vertrauenswürdige Zertifikatbehörden, die mit ONTAP vorinstalliert wurden, können nicht gelöscht werden.

Schritte

1. Öffnen Sie die Registerkarte * Trusted Certificate Authorities*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Klicken Sie auf den Namen der vertrauenswürdigen Zertifizierungsstelle.
3. Klicken Sie Auf ⋮ Klicken Sie neben dem Namen auf **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. Klicken Sie auf den Namen der vertrauenswürdigen Zertifizierungsstelle.
3. Klicken Sie Auf ⋮ Klicken Sie neben dem Namen auf **verlängern**.

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. Klicken Sie Auf + 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 einen **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. Klicken Sie auf **+selbst signiertes Zertifikat generieren**.
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. Klicken Sie auf den Namen des Client-/Serverzertifikats.
3. Klicken Sie Auf ⋮ Klicken Sie neben dem Namen auf **Löschen**.

Erneuern eines Client-/Serverzertifikats

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

Schritte

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

Erstellen Sie eine neue lokale Zertifizierungsstelle

Mit System Manager können Sie eine neue lokale Zertifizierungsstelle erstellen.

Schritte

1. Öffnen Sie die Registerkarte * Lokale Zertifikatbehörden*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Klicken Sie Auf 

.
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. Klicken Sie auf den Namen der lokalen Zertifizierungsstelle.
3. Klicken Sie Auf ⋮ Klicken Sie neben dem Namen auf **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. Klicken Sie auf den Namen der lokalen Zertifizierungsstelle.
3. Klicken Sie Auf ⋮ Klicken Sie neben dem Namen auf **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. Klicken Sie auf den Namen der lokalen Zertifizierungsstelle.
3. Klicken Sie Auf ⋮ Klicken Sie neben dem Namen auf **verlängern**.