Zertifikate

SANtricity 11.8

NetApp
June 24, 2024

Inhalt

Zertifikate

Zertifikatübersicht

Mit der Zertifikatverwaltung können Sie Zertifikatsignierungsanforderungen (CSRs) erstellen, Zertifikate importieren und vorhandene Zertifikate verwalten.

Was sind Zertifikate?

Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und Server für eine sichere Kommunikation im Internet identifizieren. Es gibt zwei Arten von Zertifikaten: Ein *signiertes Zertifikat* wird von einer Zertifizierungsstelle (CA) validiert und ein *selbst-signiertes Zertifikat* wird vom Eigentümer des Unternehmens anstelle eines Dritten validiert.

Weitere Informationen:

- "Funktionsweise von Zertifikaten"
- "Terminologie des Zertifikats"

Wie konfiguriere ich Zertifikate?

In der Zertifikatverwaltung können Sie Zertifikate für die Management Station konfigurieren, die Unified Manager hostet, und auch Zertifikate für die Controller in den Arrays importieren.

Weitere Informationen:

- "Verwenden Sie CA-signierte Zertifikate für das Managementsystem"
- "Importieren Sie Zertifikate für Arrays"

Konzepte

Funktionsweise von Zertifikaten

Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und Server für eine sichere Kommunikation im Internet identifizieren.

Signierte Zertifikate

Zertifikate stellen sicher, dass die Webkommunikation in verschlüsselter Form, privat und unverändert, nur zwischen dem angegebenen Server und dem angegebenen Client übertragen wird. Mit Unified Manager können Sie Zertifikate für den Browser auf einem Host-Managementsystem und die Controller in den ermittelten Speicher-Arrays verwalten.

Ein Zertifikat kann von einer vertrauenswürdigen Behörde signiert werden, oder es kann selbst signiert werden. „Unterzeichnen“ bedeutet einfach, dass jemand die Identität des Eigentümers validiert und festgestellt hat, dass seine Geräte vertrauenswürdig sind. Die Storage Arrays werden mit einem automatisch generierten, selbstsignierten Zertifikat auf jedem Controller ausgeliefert. Sie können weiterhin die selbst signierten Zertifikate verwenden oder CA-signierte Zertifikate für eine sicherere Verbindung zwischen den Controllern und den Host-Systemen erhalten.

Auch wenn CA-signierte Zertifikate einen besseren Schutz bieten (zum Beispiel die Verhinderung von man-in-the-Middle-Angriffen), verlangen sie auch Gebühren, die teuer sein können, wenn Sie ein großes Netzwerk haben. Im Gegensatz dazu sind selbstsignierte Zertifikate weniger sicher, aber sie sind kostenlos. Daher werden selbst signierte Zertifikate am häufigsten für interne Testumgebungen eingesetzt, nicht in Produktionsumgebungen.

Ein signiertes Zertifikat wird von einer Zertifizierungsstelle (CA) validiert, einer vertrauenswürdigen Drittorganisation. Signierte Zertifikate enthalten Angaben über den Eigentümer der Einheit (in der Regel Server oder Website), Datum der Zertifikatausgabe und -Ablauf, gültige Domains für das Unternehmen und eine digitale Signatur bestehend aus Buchstaben und Zahlen.

Wenn Sie einen Browser öffnen und eine Webadresse eingeben, führt Ihr System eine Zertifikatprüfung im Hintergrund durch, um zu bestimmen, ob Sie eine Verbindung zu einer Website herstellen, die ein gültiges, von einer Zertifizierungsstelle signiertes Zertifikat enthält. In der Regel enthält eine mit einem signierten Zertifikat gesicherte Website ein Vorhängeschloss-Symbol und eine https-Bezeichnung in der Adresse. Wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die kein CA-signiertes Zertifikat enthält, zeigt Ihr Browser eine Warnung an, dass die Website nicht sicher ist.

Die CA führt Schritte durch, um Ihre Identität während des Anwendungsprozesses zu überprüfen. Sie senden möglicherweise eine E-Mail an Ihr registriertes Unternehmen, überprüfen Ihre Geschäftsadresse und führen eine HTTP- oder DNS-Verifizierung durch. Wenn der Anwendungsprozess abgeschlossen ist, sendet die Zertifizierungsstelle digitale Dateien zum Laden auf einem Host-Managementsystem. In der Regel umfassen diese Dateien eine Kette des Vertrauens, wie folgt:

- **Root** — an der Spitze der Hierarchie befindet sich das Stammzertifikat, welches einen privaten Schlüssel enthält, der zum Signieren anderer Zertifikate verwendet wird. Das Root identifiziert eine bestimmte CA-Organisation. Wenn Sie dieselbe Zertifizierungsstelle für alle Netzwerkgeräte verwenden, benötigen Sie nur ein Stammzertifikat.
- **Intermediate** — Abzweigung von der Wurzel sind die Zwischenzertifikate. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.
- **Server** — unten in der Kette befindet sich das Server-Zertifikat, welches Ihre spezifische Entität, wie z.B. eine Website oder ein anderes Gerät, identifiziert. Jeder Controller in einem Storage Array benötigt ein separates Serverzertifikat.

Selbstsignierte Zertifikate

Jeder Controller im Speicher-Array verfügt über ein vorinstalliertes, selbstsigniertes Zertifikat. Ein selbst signiertes Zertifikat ähnelt einem CA-signierten Zertifikat, außer dass es vom Eigentümer des Unternehmens anstelle eines Dritten validiert wird. Wie ein Zertifikat mit einer Zertifizierungsstelle enthält auch ein selbstsigniertes Zertifikat einen eigenen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt und über eine HTTPS-Verbindung zwischen einem Server und einem Client gesendet werden.

Selbstsignierte Zertifikate werden von Browsern nicht „`Trusted`“. Jedes Mal, wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die nur ein selbstsigniertes Zertifikat enthält, wird im Browser eine Warnmeldung angezeigt. Sie müssen in der Warnmeldung auf einen Link klicken, der Ihnen die Nutzung der Website ermöglicht. Dadurch akzeptieren Sie im Wesentlichen das selbstsignierte Zertifikat.

Zertifikate für Unified Manager

Die Unified Manager-Schnittstelle wird mit dem Web Services Proxy auf einem Host-System installiert. Wenn Sie einen Browser öffnen und eine Verbindung zu Unified Manager herstellen möchten, versucht der Browser, durch die Suche nach einem digitalen Zertifikat zu überprüfen, ob der Host eine vertrauenswürdige Quelle ist.

Wenn der Browser kein von einer Zertifizierungsstelle signiertes Zertifikat für den Server findet, wird eine Warnmeldung angezeigt. Von dort aus können Sie auf der Website fortfahren, um das selbstsignierte Zertifikat für diese Sitzung zu akzeptieren. Oder Sie können signierte digitale Zertifikate von einer Zertifizierungsstelle erhalten, damit die Warnmeldung nicht mehr angezeigt wird.

Zertifikate für Controller

Während einer Unified Manager-Sitzung werden möglicherweise zusätzliche Sicherheitsmeldungen angezeigt, wenn Sie versuchen, auf einen Controller zuzugreifen, der kein von einer Zertifizierungsstelle signiertes Zertifikat hat. In diesem Fall können Sie dem selbst signierten Zertifikat dauerhaft vertrauen oder die CA-signierten Zertifikate für die Controller importieren, damit der Web Services Proxy-Server eingehende Clientanforderungen von diesen Controllern authentifizieren kann.

Terminologie des Zertifikats

Die folgenden Begriffe gelten für das Zertifikatmanagement.

Laufzeit	Beschreibung
CA	Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer, die sichere Verbindungen zwischen Clients und Servern ermöglichen.
CSR	Eine Zertifikatsignierungsanforderung (CSR) ist eine Nachricht, die von einem Antragsteller an eine Zertifizierungsstelle (CA) gesendet wird. Der CSR überprüft die Informationen, die die Zertifizierungsstelle zum ausstellen eines Zertifikats benötigt.
Zertifikat	Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).
Zertifikatskette	Eine Dateihierarchie, die den Zertifikaten eine Sicherheitsschicht hinzufügt. In der Regel umfasst die Kette ein Stammzertifikat oben in der Hierarchie, ein oder mehrere Zwischenzertifikate und die Serverzertifikate, die die Entitäten identifizieren.
Zwischenzertifikat	Ein oder mehrere Zwischenzertifikate verzweigen von der Root in der Zertifikatkette. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.
Schlüsselspeicher	Ein Schlüsselspeicher ist ein Repository auf Ihrem Host-Managementsystem, das private Schlüssel enthält, zusammen mit ihren entsprechenden öffentlichen Schlüsseln und Zertifikaten. Diese Schlüssel und Zertifikate identifizieren Ihre eigenen Einheiten, z. B. die Controller.

Laufzeit	Beschreibung
Stammzertifikat	Das Stammzertifikat befindet sich oben in der Hierarchie in der Zertifikatskette und enthält einen privaten Schlüssel, der zum Signieren anderer Zertifikate verwendet wird. Das Root identifiziert eine bestimmte CA-Organisation. Wenn Sie dieselbe Zertifizierungsstelle für alle Netzwerkgeräte verwenden, benötigen Sie nur ein Stammzertifikat.
Signiertes Zertifikat	Ein Zertifikat, das von einer Zertifizierungsstelle (CA) validiert wird. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Darüber hinaus enthält ein signiertes Zertifikat Details über den Eigentümer des Unternehmens (in der Regel ein Server oder eine Website) und eine digitale Signatur bestehend aus Buchstaben und Zahlen. Ein signiertes Zertifikat nutzt eine Vertrauenskette und wird daher am häufigsten in Produktionsumgebungen verwendet. Auch als „CA-signiertes Zertifikat“ oder als „Managementzertifikat“ bezeichnet.
Selbstsigniertes Zertifikat	Ein selbstsigniertes Zertifikat wird vom Eigentümer des Unternehmens validiert. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Es enthält auch eine digitale Signatur, die aus Buchstaben und Zahlen besteht. Ein selbstsigniertes Zertifikat verwendet nicht dieselbe Vertrauenskette wie ein CA-signiertes Zertifikat und wird daher am häufigsten in Testumgebungen eingesetzt. Auch als vorinstalliertes Zertifikat bezeichnet.
Serverzertifikat	Das Server-Zertifikat befindet sich unten in der Zertifikatskette. Es identifiziert Ihre spezifische Einheit, z. B. eine Website oder ein anderes Gerät. Jeder Controller in einem Storage-System benötigt ein separates Serverzertifikat.
Treuhandgeschäft	Ein Truststore ist ein Repository, das Zertifikate von vertrauenswürdigen Drittanbietern, wie z. B. CAS, enthält.

Verwenden Sie CA-signierte Zertifikate für das Managementsystem

Sie können CA-signierte Zertifikate für den sicheren Zugriff auf das Verwaltungssystem, das Unified Manager hostet, abrufen und importieren.

Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

Über diese Aufgabe

Die Verwendung von CA-signierten Zertifikaten ist ein dreistufiges Verfahren.

Schritt 1: Eine CSR-Datei ausfüllen

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) generieren, die Ihre Organisation und das Host-System identifiziert, auf dem der Web Services Proxy und Unified Manager installiert sind.

Alternativ können Sie eine CSR-Datei mit einem Tool wie OpenSSL generieren und zu überspringen Schritt 2: CSR-Datei senden.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte Verwaltung die Option **CSR abschließen** aus.
3. Geben Sie die folgenden Informationen ein, und klicken Sie dann auf **Weiter**:
   - **Organisation** — der vollständige, rechtliche Name Ihres Unternehmens oder Ihrer Organisation. Fügen Sie Suffixe wie Inc. Oder Corp. Mit ein
   - **Organisationseinheit (optional)** — die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet.
   - **Stadt/Ort** — die Stadt, in der sich Ihr Hostsystem oder Ihr Geschäft befindet.
   - **Bundesland/Region (optional)** — der Staat oder die Region, in der sich Ihr Hostsystem oder Ihr Geschäft befindet.
   - **Land ISO Code** — der zweistellige ISO-Code Ihres Landes (International Organization for Standardization), wie z. B. die USA.
4. Geben Sie die folgenden Informationen über das Hostsystem ein, auf dem der Web Services Proxy installiert ist:
   - **Allgemeiner Name** — die IP-Adresse oder der DNS-Name des Hostsystems, auf dem der Web Services Proxy installiert ist. Stellen Sie sicher, dass diese Adresse korrekt ist, sie muss mit den Angaben übereinstimmen, die Sie für den Zugriff auf Unified Manager im Browser eingeben. Verwenden Sie kein http:// oder https://. Der DNS-Name kann nicht mit einem Platzhalter beginnen.
   - **Alternative IP-Adressen** — Wenn der allgemeine Name eine IP-Adresse ist, können Sie optional weitere IP-Adressen oder Aliase für das Host-System eingeben. Verwenden Sie für mehrere Einträge ein kommagetrenntes Format.
   - **Alternative DNS-Namen** — Wenn der gemeinsame Name ein DNS-Name ist, geben Sie weitere DNS-Namen für das Host-System ein. Verwenden Sie für mehrere Einträge ein kommagetrenntes Format. Falls es keine alternativen DNS-Namen gibt, aber Sie im ersten Feld einen DNS-Namen eingegeben haben, kopieren Sie diesen Namen hier. Der DNS-Name kann nicht mit einem Platzhalter beginnen.
5. Stellen Sie sicher, dass die Host-Informationen richtig sind. Wenn dies nicht der Fall ist, schlagen die von der Zertifizierungsstelle zurückgegebenen Zertifikate fehl, wenn Sie versuchen, sie zu importieren.
6. Klicken Sie Auf **Fertig Stellen**.
7. Gehen Sie zu Schritt 2: CSR-Datei senden.

Schritt 2: CSR-Datei senden

Nachdem Sie eine CSR-Datei (Certificate Signing Request) erstellt haben, senden Sie sie an eine Certificate Authority (CA), um signierte Managementzertifikate für das System zu erhalten, das Unified Manager und den Web Services Proxy hostet.

Systeme der E-Series erfordern ein PEM-Format (Base64 ASCII-Kodierung) für signierte Zertifikate, das die folgenden Dateitypen umfasst: .Pem, .crt, .cer oder .key.

Schritte

1. Suchen Sie die heruntergeladene CSR-Datei.

   Der Speicherort des Downloads hängt von Ihrem Browser ab.

2. Senden Sie die CSR-Datei an eine CA (z. B. Verisign oder DigiCert), und fordern Sie signierte Zertifikate im PEM-Format an.

   Nachdem Sie eine CSR-Datei an die CA gesendet haben, generieren SIE keine andere CSR-Datei. Wenn Sie eine CSR generieren, erstellt das System ein privates und öffentliches Schlüsselpaar. Der öffentliche Schlüssel ist Teil der CSR, während der private Schlüssel im Schlüsselspeicher des Systems aufbewahrt wird. Wenn Sie die signierten Zertifikate erhalten und importieren, stellt das System sicher, dass sowohl der private als auch der öffentliche Schlüssel das ursprüngliche Paar sind. Wenn die Schlüssel nicht übereinstimmen, funktionieren die signierten Zertifikate nicht und Sie müssen neue Zertifikate von der CA anfordern.

3. Wenn die Zertifizierungsstelle die signierten Zertifikate zurückgibt, gehen Sie zu Schritt 3: Import Management Zertifikate.

Schritt 3: Import Management Zertifikate

Nachdem Sie von der Zertifizierungsstelle (CA) signierte Zertifikate erhalten haben, importieren Sie die Zertifikate in das Host-System, auf dem die Web Services Proxy- und Unified Manager-Schnittstelle installiert sind.

Bevor Sie beginnen

- Sie haben von der Zertifizierungsstelle signierte Zertifikate erhalten. Diese Dateien umfassen das Stammzertifikat, ein oder mehrere Zwischenzertifikate und das Serverzertifikat.
- Wenn die CA eine verkettete Zertifikatdatei (z. B. eine .p7b-Datei) lieferte, müssen Sie die verkettete Datei in einzelne Dateien entpacken: Das Stammzertifikat, ein oder mehrere Zwischenzertifikate und das Serverzertifikat. Sie können die Windows verwenden `certmgr` Dienstprogramm zum Auspacken der Dateien (Rechtsklick und wählen Sie Menü:Alle Aufgaben[Export]). Base-64-Kodierung wird empfohlen. Wenn die Exporte abgeschlossen sind, wird für jede Zertifikatdatei in der Kette eine CER-Datei angezeigt.
- Sie haben die Zertifikatdateien auf das Hostsystem kopiert, auf dem der Web Services Proxy ausgeführt wird.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte Verwaltung die Option **Import**.

   Es wird ein Dialogfeld zum Importieren der Zertifikatdateien geöffnet.

3. Klicken Sie auf **Durchsuchen**, um zuerst die Stamm- und Zwischenzertifikatdateien auszuwählen und dann das Serverzertifikat auszuwählen. Wenn Sie die CSR aus einem externen Tool generiert haben, müssen Sie auch die private Schlüsseldatei importieren, die zusammen mit der CSR erstellt wurde.

   Die Dateinamen werden im Dialogfeld angezeigt.

4. Klicken Sie Auf **Import**.

Ergebnisse

Die Dateien werden hochgeladen und validiert. Die Zertifikatinformationen werden auf der Seite Zertifikatverwaltung angezeigt.

Managementzertifikate zurücksetzen

Sie können das Managementzertifikat in den ursprünglichen, werkseitig selbstsignierten Status zurücksetzen.

Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

Über diese Aufgabe

Diese Aufgabe löscht das aktuelle Managementzertifikat vom Host-System, auf dem Web Services Proxy und Unified Manager installiert sind. Nach dem Zurücksetzen des Zertifikats wird das Host-System auf das selbstsignierte Zertifikat zurückgesetzt.

Schritte

1. Wählen Sie **Einstellungen > Zertifikate**.
2. Wählen Sie die Registerkarte **Array Management** und dann **Reset**.

   Das Dialogfeld „Zertifikat zurücksetzen bestätigen“ wird geöffnet.

3. Typ `reset` Klicken Sie im Feld auf **Zurücksetzen**.

   Nach der Aktualisierung Ihres Browsers kann der Browser den Zugriff auf die Zielseite blockieren und melden, dass die Website HTTP Strict Transport Security verwendet. Diese Bedingung tritt auf, wenn Sie wieder auf selbstsignierte Zertifikate wechseln. Um die Bedingung zu löschen, die den Zugriff auf das Ziel blockiert, müssen Sie die Browserdaten aus dem Browser löschen.

Ergebnisse

Das System setzt auf die Verwendung des selbstsignierten Zertifikats des Servers zurück. Das System fordert Benutzer daher auf, das selbstsignierte Zertifikat für ihre Sitzungen manuell anzunehmen.

Verwenden Sie Array-Zertifikate

Importieren Sie Zertifikate für Arrays

Bei Bedarf können Zertifikate für die Speicher-Arrays importiert werden, sodass sie sich mit dem System authentifizieren können, das Unified Manager hostet. Zertifikate können von einer Zertifizierungsstelle (CA) signiert oder selbst signiert werden.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Wenn Sie vertrauenswürdige Zertifikate importieren, müssen die Zertifikate für die Speicher-Array-Controller mit System Manager importiert werden.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte * Trusted* aus.

   Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

3. Wählen Sie entweder Menü:Import[Certificates], um ein CA-Zertifikat oder Menü zu importieren:Importieren[Self-signierte Speicher-Array-Zertifikate], um ein selbstsigniertes Zertifikat zu importieren.

   Um die Ansicht einzuschränken, können Sie das Filterfeld **Zertifikate anzeigen verwenden, das…** ist, oder Sie können die Zertifikatzeilen sortieren, indem Sie auf eine der Spaltenüberschrift klicken.

4. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf **Import**.

   Das Zertifikat wird hochgeladen und validiert.

Vertrauenswürdige Zertifikate löschen

Sie können ein oder mehrere nicht mehr benötigte Zertifikate löschen, z. B. ein abgelaufenes Zertifikat.

Bevor Sie beginnen

Importieren Sie das neue Zertifikat, bevor Sie das alte löschen.

> Beachten Sie, dass das Löschen eines Root- oder Zwischenzertifikats mehrere Speicher-Arrays beeinflussen kann, da diese Arrays dieselben Zertifikatdateien gemeinsam nutzen können.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte * Trusted* aus.
3. Wählen Sie ein oder mehrere Zertifikate in der Tabelle aus, und klicken Sie dann auf **Löschen**.

   > Die Funktion **Löschen** steht für vorinstallierte Zertifikate nicht zur Verfügung.

   Das Dialogfeld Vertrauenswürdiges Zertifikat bestätigen wird geöffnet.

4. Bestätigen Sie den Löschvorgang, und klicken Sie dann auf **Löschen**.

   Das Zertifikat wird aus der Tabelle entfernt.

Lösen Sie nicht vertrauenswürdige Zertifikate

Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array versucht, eine sichere Verbindung zu Unified Manager herzustellen, die Verbindung jedoch nicht als sicher bestätigt werden kann.

Auf der Zertifikatsseite können Sie nicht vertrauenswürdige Zertifikate auflösen, indem Sie ein selbstsigniertes Zertifikat aus dem Speicher-Array importieren oder ein Zertifikat der Zertifizierungsstelle importieren, das von einem vertrauenswürdigen Dritten ausgestellt wurde.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das die Berechtigungen für den Sicherheitsadministrator enthält.
- Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat importieren möchten:
  - Sie haben für jeden Controller im Speicher-Array eine Zertifikatsignierungsanforderung (.CSR-Datei) generiert und an die CA gesendet.
  - Die CA hat vertrauenswürdige Zertifikatdateien zurückgegeben.
  - Die Zertifikatdateien sind auf Ihrem lokalen System verfügbar.

Über diese Aufgabe

Möglicherweise müssen Sie zusätzliche vertrauenswürdige CA-Zertifikate installieren, wenn eine der folgenden Optionen zutrifft:

- Sie haben kürzlich ein Speicher-Array hinzugefügt.
- Ein oder beide Zertifikate sind abgelaufen.
- Ein oder beide Zertifikate werden widerrufen.
- Ein oder beide Zertifikate fehlen ein Stammzertifikat oder ein Zwischenzertifikat.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte * Trusted* aus.

   Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

3. Wählen Sie entweder Menü:Import[Certificates], um ein CA-Zertifikat oder Menü zu importieren:Importieren[Self-signierte Speicher-Array-Zertifikate], um ein selbstsigniertes Zertifikat zu importieren.

   Um die Ansicht einzuschränken, können Sie das Filterfeld **Zertifikate anzeigen verwenden, das…** ist, oder Sie können die Zertifikatzeilen sortieren, indem Sie auf eine der Spaltenüberschrift klicken.

4. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf **Import**.

   Das Zertifikat wird hochgeladen und validiert.

Verwalten von Zertifikaten

Anzeigen von Zertifikaten

Sie können zusammenfassende Informationen für ein Zertifikat anzeigen, das die Organisation, die das Zertifikat verwendet, die Behörde, die das Zertifikat ausgestellt hat, den Gültigkeitszeitraum und die Fingerabdrücke (eindeutige Kennungen) umfasst.

Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie eine der folgenden Registerkarten aus:
   - **Management** — zeigt das Zertifikat für das System, das den Web Services Proxy hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Die Lösung ermöglicht den sicheren Zugriff auf Unified Manager.
   - **Trusted** — zeigt Zertifikate an, auf die Unified Manager für Speicher-Arrays und andere Remote-Server, z. B. einen LDAP-Server, zugreifen kann. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.
3. Um weitere Informationen zu einem Zertifikat anzuzeigen, wählen Sie seine Zeile aus, wählen Sie die Ellipsen am Zeilenende aus und klicken Sie dann auf **Ansicht** oder **Export**.

Exportieren von Zertifikaten

Sie können ein Zertifikat exportieren, um die vollständigen Details anzuzeigen.

Bevor Sie beginnen

Um die exportierte Datei zu öffnen, müssen Sie über eine Zertifikatanzeige-Anwendung verfügen.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie eine der folgenden Registerkarten aus:
   - **Management** — zeigt das Zertifikat für das System, das den Web Services Proxy hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Die Lösung ermöglicht den sicheren Zugriff auf Unified Manager.
   - **Trusted** — zeigt Zertifikate an, auf die Unified Manager für Speicher-Arrays und andere Remote-Server, z. B. einen LDAP-Server, zugreifen kann. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.
3. Wählen Sie auf der Seite ein Zertifikat aus, und klicken Sie dann am Ende der Zeile auf die Ellipsen.
4. Klicken Sie auf **Exportieren** und speichern Sie dann die Zertifikatdatei.
5. Öffnen Sie die Datei in Ihrer Zertifikatanzeige-Anwendung.