Zertifikate

SANtricity 11.6

NetApp
February 12, 2024

Inhalt

Zertifikate

Konzepte

Funktionsweise von Zertifikaten

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

Zertifikate stellen sicher, dass die Webkommunikation in verschlüsselter Form, privat und unverändert, nur zwischen dem angegebenen Server und dem angegebenen Client übertragen wird. Mit System Manager können Sie Zertifikate zwischen dem Browser auf einem Host-Managementsystem (als Client fungieren) und den Controllern in einem Storage-System (als Server fungieren) 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.

Signierte Zertifikate

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, das 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.

- Zwischenzertifikate — 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 Serverzertifikat, das 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. Ein selbst signiertes Zertifikat verwendet jedoch nicht die gleiche Vertrauenskette wie ein CA-signiertes Zertifikat.

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, die für den Schlüsselverwaltungsserver verwendet werden

Wenn Sie einen externen Schlüsselverwaltungsserver mit der Laufwerkssicherheitsfunktion verwenden, können Sie auch Zertifikate zur Authentifizierung zwischen diesem Server und den Controllern verwalten.

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.

Laufzeit	Beschreibung
Client-Zertifikat	Für das Management von Sicherheitsschlüssel validiert ein Client-Zertifikat die Controller des Speicherarrays, damit der Schlüsselverwaltungsserver ihre IP-Adressen anvertrauen kann.
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.
Zertifikat für Schlüsselmanagement-Server	Für das Sicherheitsschlüsselmanagement validiert ein Zertifikat für den Schlüsselmanagement-Server den Server, damit das Storage-Array seiner IP-Adresse vertrauen kann.
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.
OCSP-Server	Der OCSP-Server (Online Certificate Status Protocol) ermittelt, ob die Zertifizierungsstelle vor ihrem geplanten Ablaufdatum Zertifikate widerrufen hat und blockiert dann den Zugriff des Benutzers auf einen Server, wenn das Zertifikat widerrufen wird.
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.

Anleitungen

Verwenden Sie CA-signierte Zertifikate für Controller

Sie können Zertifikate von CA-signierte für die sichere Kommunikation zwischen den Controllern und dem Browser erhalten, der für den Zugriff auf System Manager verwendet wird.

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 für die Controller abschließen und einreichen

Sie müssen zuerst für jeden Controller im Speicher-Array eine CSR-Datei (Certificate Signing Request) generieren und dann die Datei(en) an eine Zertifizierungsstelle (CA) senden.

Bevor Sie beginnen

- Sie müssen die IP-Adresse oder den DNS-Namen jedes Controllers kennen.

Über diese Aufgabe

Der CSR stellt Informationen über Ihre Organisation, die IP-Adresse oder den DNS-Namen des Controllers und ein Schlüsselpaar zur Verfügung, das den Webserver im Controller identifiziert. Während dieser Aufgabe wird eine CSR-Datei erzeugt, wenn es nur einen Controller im Speicher-Array und zwei CSR-Dateien gibt, wenn es zwei Controller gibt.

> Generieren Sie nach der Übermittlung an die CA keine neue CSR. Wenn Sie eine CSR erstellen, erstellt das System ein privates und öffentliches Schlüsselpaar. Der öffentliche Schlüssel ist Teil des CSR, während der private Schlüssel im Schlüsselspeicher aufbewahrt wird. Wenn Sie die signierten Zertifikate erhalten und in den Schlüsselspeicher importieren, stellt das System sicher, dass sowohl der private als auch der öffentliche Schlüssel das ursprüngliche Paar sind. Daher dürfen Sie nach dem Einreichen einer CSR an die CA keine neue CSR generieren. Wenn Sie dies tun, generieren die Controller neue Schlüssel, und die Zertifikate, die Sie von der CA erhalten, funktionieren nicht.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte **Array Management** die Option **Complete CSR** aus.

   > Wenn ein Dialogfeld angezeigt wird, in dem Sie aufgefordert werden, ein selbstsigniertes Zertifikat für den zweiten Controller anzunehmen, klicken Sie zum Fortfahren auf **Selbstsigniertes Zertifikat akzeptieren**.

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 Speicher-Array oder Geschäft befindet.
- **Bundesland/Region (optional)** — der Staat oder die Region, in der sich Ihr Speicher-Array oder Ihr Geschäft befindet.
- **Land ISO Code** — der zweistellige ISO-Code Ihres Landes (International Organization for Standardization), wie z. B. die USA.

> Einige Felder sind möglicherweise bereits mit den entsprechenden Informationen ausgefüllt, z. B. mit der IP-Adresse des Controllers. Ändern Sie die vorausgefüllten Werte nur, wenn Sie sich sicher sind, dass sie nicht korrekt sind. Wenn Sie zum Beispiel noch keinen CSR-Vorgang abgeschlossen haben, wird die Controller-IP-Adresse auf „`localhost.`“ gesetzt. In diesem Fall müssen Sie „`localhost`“ in den DNS-Namen oder die IP-Adresse des Controllers ändern.

4. Überprüfen oder geben Sie die folgenden Informationen über Controller A in Ihrem Speicher-Array ein:
   - **Controller Ein gemeinsamer Name** — die IP-Adresse oder der DNS-Name von Controller A wird standardmäßig angezeigt. Stellen Sie sicher, dass diese Adresse korrekt ist. Sie muss mit den Angaben übereinstimmen, die Sie für den Zugriff auf System Manager im Browser eingeben.
   - **Controller Eine alternative IP-Adresse** — Wenn der gemeinsame Name eine IP-Adresse ist, können Sie optional weitere IP-Adressen oder Aliase für Controller A eingeben Verwenden Sie für mehrere Einträge ein kommagetrenntes Format.
   - **Controller Ein alternativer DNS-Name** — Wenn der gemeinsame Name ein DNS-Name ist, geben Sie weitere DNS-Namen für Controller A. 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. Wenn das Speicher-Array nur über einen Controller verfügt, steht die **Finish**-Taste zur Verfügung. Wenn das Speicher-Array über zwei Controller verfügt, steht die Schaltfläche **Weiter** zur Verfügung.

> Klicken Sie nicht auf den Link **Skip this Step**, wenn Sie eine CSR-Anfrage erstellen. Dieser Link wird in Fehlerwiederherstellungssituationen bereitgestellt. In seltenen Fällen kann eine CSR-Anfrage auf einem Controller fehlschlagen, aber nicht auf dem anderen. Über diesen Link können Sie den Schritt zum Erstellen einer CSR-Anfrage für Controller A überspringen, wenn er bereits definiert ist, und mit dem nächsten Schritt zum erneuten Erstellen einer CSR-Anfrage auf Controller B fortfahren

5. Wenn nur ein Controller vorhanden ist, klicken Sie auf **Fertig stellen**. Wenn zwei Controller vorhanden sind, klicken Sie auf **Weiter**, um die Daten für Controller B einzugeben (wie oben), und klicken Sie dann auf **Fertig stellen**.

   Für einen einzelnen Controller wird eine CSR-Datei auf Ihr lokales System heruntergeladen. Für Dual Controller werden zwei CSR-Dateien heruntergeladen. Der Speicherort des Downloads hängt von Ihrem Browser ab.

6. Suchen Sie die heruntergeladenen CSR-Dateien. Der Speicherort des Ordners hängt vom Browser ab.
7. Senden Sie die CSR-Datei(en) an eine CA und fordern Sie signierte Zertifikate im PEM-Format an.
8. Warten Sie, bis die Zertifizierungsstelle die Zertifikate zurückgibt, und gehen Sie dann zu Schritt 2: Importieren Sie signierte Zertifikate für Controller.

Schritt 2: Importieren Sie signierte Zertifikate für Controller

Nachdem Sie signierte Zertifikate erhalten haben, importieren Sie die Dateien für die Controller.

Bevor Sie beginnen

- Die CA hat signierte Zertifikatdateien zurückgegeben.
- Die Dateien sind auf Ihrem lokalen System verfügbar.
- Wenn die CA ein verkettetes Zertifikat (z. B. eine .p7b-Datei) lieferte, müssen Sie die verkettete Datei in einzelne Dateien entpacken: Das Stammzertifikat, ein oder mehrere Zwischenzertifikate und die Serverzertifikate, die die Controller identifizieren. Sie können die Windows verwenden `certmgr` Dienstprogramm zum Auspacken der Dateien (Rechtsklick und wählen Sie **Alle Aufgaben › Export**). Wenn die Exporte abgeschlossen sind, wird für jede Zertifikatdatei in der Kette eine CER-Datei angezeigt.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Sie die Zertifikatdateien hochladen.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte **Array Management** die Option **Import**.

   Es wird ein Dialogfeld zum Importieren der Zertifikatdatei(en) geöffnet.

3. Klicken Sie auf die Schaltflächen **Durchsuchen**, um zuerst die Root- und Zwischendateien auszuwählen und dann jedes Serverzertifikat für die Controller auszuwählen. Die Root- und Zwischendateien sind für beide Controller gleich. Nur die Serverzertifikate sind für jeden Controller eindeutig.

   Die Dateinamen werden im Dialogfeld angezeigt.

4. Klicken Sie Auf **Import**.

   Die Datei(en) werden hochgeladen und validiert.

Ergebnisse

Die Sitzung wird automatisch beendet. Sie müssen sich erneut anmelden, damit die Zertifikate wirksam werden. Wenn Sie sich erneut anmelden, wird das neue CA-signierte Zertifikat für Ihre Sitzung verwendet.

Managementzertifikate zurücksetzen

Sie können die Zertifikate auf den Controllern von der Verwendung von CA-signierten Zertifikaten zurück auf die werkseitig eingestellten, selbstsignierten Zertifikate zurücksetzen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- CA-signierte Zertifikate müssen bereits importiert werden.

Über diese Aufgabe

Mit der Funktion Reset werden die aktuellen CA-signierten Zertifikatdateien von jedem Controller gelöscht. Die Controller werden dann mithilfe selbstsignierter Zertifikate wiederhergestellt.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte **Array Management** die Option **Zurücksetzen**.

   Es wird ein Dialogfeld „Bestätigen **Management Certificates** zurücksetzen“ 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

Die Controller werden mithilfe von selbstsignierten Zertifikaten wiederhergestellt. Das System fordert Benutzer daher auf, das selbstsignierte Zertifikat für ihre Sitzungen manuell anzunehmen.

Anzeigen importierter Zertifikatinformationen

Auf der Seite Zertifikate können Sie den Zertifikatstyp, die ausstellende Behörde und den gültigen Datumsbereich der Zertifikate für das Speicher-Array anzeigen.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie Menü:Einstellungen[Zertifikate].
2. Wählen Sie eine der Registerkarten aus, um Informationen zu den Zertifikaten anzuzeigen.

Registerkarte	Beschreibung
Array-Management	Zeigen Sie Informationen zu den für jeden Controller importierten CA-signierten Zertifikaten an, einschließlich der Root-Datei, der Zwischendatei(en) und der Serverdatei(en).
Bewährt	Informationen über alle anderen Arten von Zertifikaten anzeigen, die für die Controller importiert wurden. Verwenden Sie das Filterfeld unter **Zertifikate anzeigen, die…** sind, um entweder vom Benutzer installierte oder vorinstallierte Zertifikate anzuzeigen. • **Vom Benutzer installiert**. Zertifikate, die ein Benutzer auf das Speicher-Array hochgeladen hat. Dies kann vertrauenswürdige Zertifikate enthalten, wenn der Controller als Client (anstelle eines Servers), LDAPS-Zertifikate und Identity Federation-Zertifikate fungiert. • **Vorinstalliert**. Im Speicher-Array enthaltene selbstsignierte Zertifikate.
Verschlüsselungs-Management	Zeigen Sie Informationen zu den für einen externen Schlüsselverwaltungsserver importierten CA-signierten Zertifikaten an.

Importieren Sie Zertifikate für Controller, wenn Sie als Clients fungieren

Wenn der Controller eine Verbindung zurückweist, weil er die Vertrauenskette für einen Netzwerkserver nicht validieren kann, können Sie ein Zertifikat über die Registerkarte „Trusted“ importieren, auf der der Controller (als Client agiert) die Kommunikation von diesem Server akzeptieren kann.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Die Zertifikatdateien werden auf Ihrem lokalen System installiert.

Über diese Aufgabe

Das Importieren von Zertifikaten aus der Registerkarte „Trusted“ ist möglicherweise erforderlich, wenn Sie zulassen möchten, dass andere Server die Controller kontaktieren (z. B. ein LDAP-Server oder ein Syslog-Server, der TLS verwendet).

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte * Trusted* die Option **Import** aus.

   Es wird ein Dialogfeld zum Importieren der vertrauenswürdigen Zertifikatdateien geöffnet.

3. Klicken Sie auf **Durchsuchen**, um die Zertifikatdateien für die Controller auszuwählen.

   Die Dateinamen werden im Dialogfeld angezeigt.

4. Klicken Sie Auf **Import**.

Ergebnisse

Die Dateien werden hochgeladen und validiert.

Überprüfung des Zertifikatsannuls aktivieren

Sie können automatische Überprüfungen auf widerrief Zertifikate aktivieren, sodass ein OCSP-Server (Online Certificate Status Protocol) Benutzer daran blockiert, nicht sichere Verbindungen zu machen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Auf beiden Controllern wird ein DNS-Server konfiguriert, wodurch ein vollständig qualifizierter Domain-Name für den OCSP-Server verwendet werden kann. Diese Aufgabe ist auf der Seite Hardware verfügbar.
- Wenn Sie Ihren eigenen OCSP-Server angeben möchten, müssen Sie die URL dieses Servers kennen.

Über diese Aufgabe

Die automatische Überprüfung des Widerrufs ist hilfreich, wenn die CA ein Zertifikat falsch ausgestellt hat oder ein privater Schlüssel gefährdet ist.

Während dieser Aufgabe können Sie einen OCSP-Server konfigurieren oder den in der Zertifikatdatei

angegebenen Server verwenden. Der OCSP-Server prüft, ob die CA Zertifikate vor ihrem geplanten Ablaufdatum widerrufen hat, und blockiert dann den Zugriff des Benutzers auf einen Standort, wenn das Zertifikat widerrufen wird.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie die Registerkarte * Trusted* aus.

> Sie können auch die Überprüfung des Widerrufs über die Registerkarte * Key Management* aktivieren.

3. Klicken Sie auf **Sonstige Aufgaben**, und wählen Sie im Dropdown-Menü die Option **Überprüfung der Widerruherstellung aktivieren** aus.
4. Wählen Sie **Ich möchte die Sperrprüfung aktivieren** aus, damit im Kontrollkästchen ein Häkchen angezeigt wird und im Dialogfeld zusätzliche Felder angezeigt werden.
5. Im Feld **OCSP Responder Address** können Sie optional eine URL für einen OCSP Responder-Server eingeben. Wenn Sie keine Adresse eingeben, verwendet das System die URL des OCSP-Servers aus der Zertifikatsdatei.
6. Klicken Sie auf **Testadresse**, um sicherzustellen, dass das System eine Verbindung zur angegebenen URL öffnen kann.
7. Klicken Sie Auf **Speichern**.

Ergebnisse

Wenn das Speicher-Array versucht, eine Verbindung mit einem Server mit einem widerrufenen Zertifikat herzustellen, wird die Verbindung verweigert und ein Ereignis protokolliert.

Vertrauenswürdige Zertifikate löschen

Sie können die vom Benutzer installierten Zertifikate löschen, die zuvor über die Registerkarte „Vertrauenswürdig“ importiert wurden.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Wenn Sie ein vertrauenswürdiges Zertifikat mit einer neuen Version aktualisieren, muss das aktualisierte Zertifikat importiert werden, bevor Sie das alte Zertifikat löschen.

> Möglicherweise verlieren Sie den Zugriff auf ein System, wenn Sie ein Zertifikat löschen, das zur Authentifizierung der Controller und eines anderen Servers, z. B. eines LDAP-Servers verwendet wird, bevor Sie ein Ersatzzertifikat importieren.

Über diese Aufgabe

Diese Aufgabe beschreibt das Löschen von vom Benutzer installierten Zertifikaten. Die vorinstallierten, selbstsignierten Zertifikate können nicht gelöscht werden.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie die Registerkarte * Trusted* aus.

In der Tabelle sind die vertrauenswürdigen Zertifikate des Speicher-Arrays aufgeführt.

3. Wählen Sie in der Tabelle das Zertifikat aus, das Sie entfernen möchten.
4. Klicken Sie auf **Sonstige Aufgaben › Löschen**

   Das Dialogfeld Vertrauenswürdiges Zertifikat bestätigen wird geöffnet.

5. Typ `delete` Klicken Sie im Feld auf **Löschen**.

Verwenden Sie CA-signierte Zertifikate zur Authentifizierung mit einem Schlüsselverwaltungsserver

Für die sichere Kommunikation zwischen einem Schlüsselverwaltungsserver und den Speicher-Array-Controllern müssen Sie die entsprechenden Zertifikatssätze konfigurieren.

Bevor Sie beginnen

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

Über diese Aufgabe

Die Authentifizierung zwischen den Controllern und einem Schlüsselverwaltungsserver ist ein zweistufiges Verfahren.

Schritt 1: CSR für die Authentifizierung mit einem Schlüsselverwaltungsserver abschließen und einreichen

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) generieren und dann mithilfe des CSR ein signiertes Clientzertifikat von einer Zertifizierungsstelle (CA) anfordern, die vom Schlüsselverwaltungsserver vertrauenswürdig ist. Sie können auch mithilfe der heruntergeladenen CSR-Datei ein Client-Zertifikat vom Schlüsselverwaltungsserver erstellen und herunterladen.

Bevor Sie beginnen

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

Über diese Aufgabe

Diese Aufgabe beschreibt, wie Sie die CSR-Datei generieren, die Sie dann verwenden, um ein signiertes Client-Zertifikat von einer CA anzufordern, die vom Schlüsselverwaltungsserver vertrauenswürdig ist. Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der wichtige Management-Server seine KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen kann. Während dieser Aufgabe müssen Sie Informationen über Ihr Unternehmen angeben.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte * Key Management* die Option **Complete CSR** aus.
3. Geben Sie die folgenden Informationen ein:
   - **Allgemeiner Name** — Ein Name, der diese CSR identifiziert, wie z.B. den Namen des Speicherarrays, der in den Zertifikatdateien angezeigt wird.
   - **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 oder der Ort, in dem sich Ihre Organisation befindet.
- **Bundesland/Region (optional)** — der Staat oder die Region, in der sich Ihre Organisation befindet.
- **Land ISO Code** — der zweistellige ISO-Code (International Organization for Standardization), wie die USA, wo sich Ihre Organisation befindet.

4. Klicken Sie Auf **Download**.

   Eine CSR-Datei wird auf Ihrem lokalen System gespeichert.

5. Fordern Sie ein signiertes Clientzertifikat von einer Zertifizierungsstelle an, die vom Schlüsselverwaltungsserver vertrauenswürdig ist.
6. Wenn Sie ein Clientzertifikat besitzen, gehen Sie zu Schritt 2: Importieren Sie Zertifikate für den Schlüsselverwaltungsserver.

Schritt 2: Importieren Sie Zertifikate für den Schlüsselverwaltungsserver

Im nächsten Schritt importieren Sie Zertifikate zur Authentifizierung zwischen dem Storage-Array und dem Schlüsselverwaltungsserver. Es gibt zwei Arten von Zertifikaten: Das Clientzertifikat überprüft die Controller des Speicherarrays, während das Zertifikat für den Schlüsselverwaltungsserver den Server validiert.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Sie haben eine signierte Client-Zertifikatdatei (siehe Schritt 1: CSR für die Authentifizierung mit einem Schlüsselverwaltungsserver abschließen und einreichen), und Sie haben diese Datei auf den Host kopiert, auf den Sie auf System Manager zugreifen. Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der wichtige Management-Server seine KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen kann.
- Sie müssen die Serverzertifikatdatei vom Schlüsselverwaltungsserver abrufen und diese Datei anschließend auf den Host kopieren, auf dem Sie auf System Manager zugreifen. Ein Zertifikat für den Schlüsselmanagementserver validiert den Schlüsselmanagementserver, damit das Storage-Array seiner IP-Adresse vertrauen kann.

> Weitere Informationen zum Serverzertifikat finden Sie in der Dokumentation für Ihren Schlüsselverwaltungsserver.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Zertifikatdateien für die Authentifizierung zwischen den Speicher-Array-Controllern und dem Schlüsselverwaltungsserver hochgeladen werden. Sie müssen sowohl die Client-Zertifikatdatei für die Controller als auch die Serverzertifikatdatei für den Schlüsselverwaltungsserver laden.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte * Key Management* die Option **Import** aus.

   Es wird ein Dialogfeld zum Importieren der Zertifikatdateien geöffnet.

3. Klicken Sie neben **Select Client Certificate** auf die Schaltfläche **Browse**, um die Clientzertifikatdatei für

die Controller des Speicherarrays auszuwählen.

Der Dateiname wird im Dialogfeld angezeigt.

4. Neben **Wählen Sie das Serverzertifikat des Schlüsselverwaltungsservers**, klicken Sie auf die Schaltfläche **Durchsuchen**, um die Serverzertifikatdatei für Ihren Schlüsselverwaltungsserver auszuwählen.

   Der Dateiname wird im Dialogfeld angezeigt.

5. Klicken Sie Auf **Import**.

   Die Dateien werden hochgeladen und validiert.

Export von Zertifikaten für den Schlüsselverwaltungsserver

Sie können ein Zertifikat für einen Schlüsselverwaltungsserver auf Ihrem lokalen Computer speichern.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie die Registerkarte * Key Management* aus.
3. Wählen Sie in der Tabelle das Zertifikat aus, das Sie exportieren möchten, und klicken Sie dann auf **Exportieren**.

   Ein Dialogfeld „Speichern“ wird geöffnet.

4. Geben Sie einen Dateinamen ein und klicken Sie auf **Speichern**.

FAQs

Warum wird das Dialogfeld „Zugriff auf anderen Controller nicht möglich“ angezeigt?

Wenn Sie bestimmte Vorgänge im Zusammenhang mit CA-Zertifikaten ausführen (z. B. ein Zertifikat importieren), wird möglicherweise ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, ein selbstsigniertes Zertifikat für den zweiten Controller anzunehmen.

In Speicher-Arrays mit zwei Controllern (Duplexkonfigurationen) wird dieses Dialogfeld manchmal angezeigt, wenn SANtricity System Manager nicht mit dem zweiten Controller kommunizieren kann oder wenn Ihr Browser das Zertifikat während eines bestimmten Punktes nicht akzeptieren kann.

Wenn dieses Dialogfeld geöffnet wird, klicken Sie auf **Selbstsigniertes Zertifikat akzeptieren**, um fortzufahren. Wenn Sie in einem anderen Dialogfeld zur Eingabe eines Passworts aufgefordert werden, geben

Sie Ihr Administratorpasswort ein, das zum Zugriff auf System Manager verwendet wird.

Wenn dieses Dialogfeld erneut angezeigt wird und Sie keine Zertifikataufgabe abschließen können, führen Sie einen der folgenden Schritte aus:

- Verwenden Sie einen anderen Browsertyp, um auf diesen Controller zuzugreifen, das Zertifikat zu akzeptieren und fortzufahren.
- Greifen Sie mit System Manager auf den zweiten Controller zu, akzeptieren Sie das selbstsignierte Zertifikat, kehren Sie dann zum ersten Controller zurück und fahren Sie fort.

Wie weiß ich, welche Zertifikate zum externen Verschlüsselungsmanagement in System Manager hochgeladen werden müssen?

Für das externe Verschlüsselungsmanagement importieren Sie zwei Arten von Zertifikaten zur Authentifizierung zwischen dem Storage-Array und dem Schlüsselverwaltungsserver, damit sich die beiden Entitäten gegenseitig vertrauen können.

Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der wichtige Management-Server seine KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen kann. Um ein Client-Zertifikat zu erhalten, verwenden Sie System Manager, um eine CSR für das Speicher-Array abzuschließen. Anschließend können Sie die CSR auf einen Schlüsselverwaltungsserver hochladen und von dort aus ein Clientzertifikat generieren. Wenn Sie über ein Clientzertifikat verfügen, kopieren Sie diese Datei auf den Host, auf den Sie auf System Manager zugreifen.

Ein Zertifikat für den Schlüsselmanagementserver validiert den Schlüsselmanagementserver, damit das Storage-Array seiner IP-Adresse vertrauen kann. Rufen Sie die Serverzertifikatdatei vom Schlüsselverwaltungsserver ab, und kopieren Sie diese Datei dann auf den Host, auf dem Sie auf System Manager zugreifen.

Was muss ich über die Überprüfung des Annullierung von Zertifikaten wissen?

Mit System Manager können Sie mithilfe eines OCSP-Servers (Online Certificate Status Protocol) nach widerrufenen Zertifikaten suchen, anstatt Zertifikatsperrlisten (Certificate Revocation Lists, CRLs) hochzuladen.

Zurückwiderrufen Zertifikate sollten nicht mehr vertrauenswürdig sein. Ein Zertifikat kann aus mehreren Gründen widerrufen werden; beispielsweise wenn die Zertifizierungsstelle (CA) das Zertifikat nicht ordnungsgemäß ausgestellt hat, ein privater Schlüssel kompromittiert wurde oder die identifizierte Entität nicht den Richtlinienanforderungen entspricht.

Nachdem Sie in System Manager eine Verbindung zu einem OCSP-Server hergestellt haben, führt das Speicherarray eine Widerrufs-Prüfung durch, wenn es eine Verbindung zu einem AutoSupport-Server, einem externen Schlüsselverwaltungsserver (EKMS), einem Lightweight Directory Access Protocol over SSL (LDAPS)-Server oder einem Syslog-Server herstellt. Das Speicher-Array versucht, die Zertifikate dieser Server zu validieren, um sicherzustellen, dass sie nicht widerrufen wurden. Der Server gibt dann für dieses Zertifikat einen Wert von „gut“, „gesperrt“ oder „unbekannt“ zurück. Wenn das Zertifikat widerrufen wird oder das Array nicht den OCSP-Server kontaktieren kann, wird die Verbindung abgelehnt.

> Wenn Sie eine OCSP-Antwortadresse in System Manager oder in der Befehlszeilenschnittstelle (CLI) angeben, wird die OCSP-Adresse, die in der Zertifikatsdatei gefunden wurde, überschrieben.

Für welche Servertypen wird die Überprüfung des Widerrufs aktiviert?

Das Speicher-Array führt Sperrprüfungen durch, wenn es eine Verbindung zu einem AutoSupport-Server, einem externen Schlüsselverwaltungsserver (EKMS), einem Lightweight Directory Access Protocol over SSL (LDAPS)-Server oder einem Syslog-Server herstellt.