Zertifikate

SANtricity 11.5

NetApp
February 12, 2024

Inhalt

Zertifikate

Konzepte

Funktionsweise von CA-Zertifikaten

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.

Wenn Sie einen Browser öffnen und über den Controller-Managementport eine Verbindung zum System Manager herstellen möchten, versucht der Browser zu überprüfen, ob der Controller des Speicherarrays eine vertrauenswürdige Quelle ist. Wenn der Browser ein digitales Zertifikat für den Controller nicht finden kann, wird darauf aufmerksam gemacht, dass das Zertifikat nicht von einer anerkannten Behörde signiert ist und Sie werden gefragt, ob Sie fortfahren möchten. Wenn Sie diese Warnung nicht mehr sehen möchten, müssen Sie ein signiertes digitales Zertifikat von einer Zertifizierungsstelle erhalten.

Wenn Sie einen externen Schlüsselverwaltungsserver mit der Laufwerkssicherheitsfunktion verwenden, können Sie auch Zertifikate zur Authentifizierung zwischen diesem Server und den Controllern erstellen oder das selbstsignierte Zertifikat vom Speicher-Array akzeptieren.

Zur Verwendung eines digitalen Zertifikats von einer vertrauenswürdigen Behörde sind folgende Schritte erforderlich:

1. Gehen Sie zum Menü:Einstellungen[Zertifikate]. Ihre Benutzeranmeldung muss Sicherheitsadministratorberechtigungen enthalten; andernfalls wird **Zertifikate** nicht auf der Seite angezeigt.
2. Erstellen Sie für jeden Controller oder für einen Schlüsselverwaltungsserver eine Zertifikatsignierungsanforderung (CSR).
3. Senden Sie die .CSR-Datei(en) an eine CA, und warten Sie dann, bis sie Ihnen die Zertifikate schicken.
4. Importieren Sie das vertrauenswürdige Zertifikat (Zwischen- und Stammzertifikat) aus der Zertifizierungsstelle. Diese Zertifikate stellen einen Vertrauenspunkt für eine CA-Hierarchie her.
5. Importieren Sie die signierten Managementzertifikate für jeden Controller oder den Schlüsselverwaltungsserver.

Terminologie des Zertifikats

Erfahren Sie, wie die Zertifikatsbedingungen auf Ihr Speicher-Array angewendet werden.

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.

Laufzeit	Beschreibung
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).
Client-Zertifikat	Für das Management von Sicherheitsschlüssel validiert ein Client-Zertifikat die Controller des Speicherarrays, damit der Schlüsselverwaltungsserver ihre IP-Adressen anvertrauen kann.
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.
Managementzertifikat	Ein Managementzertifikat wird von einer Zertifizierungsstelle (CA) genehmigt und ermöglicht einen sicheren Zugriff auf die Webanwendung. Auch als "signiertes Zertifikat" bezeichnet.
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.
Selbstsigniertes Zertifikat	Ein selbstsigniertes Zertifikat ist auf dem Controller vorinstalliert. Wenn die Site-Verbindung selbst signiert ist, wird eine Warnmeldung angezeigt, bevor Sie mit der Webanwendung fortfahren können.
Vertrauenswürdiges Zertifikat	Ein vertrauenswürdiges Zertifikat einer Zertifizierungsstelle (CA) ist ein bekanntes Zertifikat oben in der Zertifikathierarchie. Auch als „Stammzertifikat“ bezeichnet.

Anleitungen

Füllen Sie eine CSR (CA Certificate Signing Request) für die Controller aus

Um ein Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) für die Controller des Speicherarrays zu erhalten, müssen Sie zuerst eine CSR-Datei (Certificate Signing Request) für jeden Controller im Speicher-Array generieren.

Bevor Sie beginnen

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

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Sie die CSR-Dateien (Certificate Signing Requests) generieren, die Sie an eine CA senden, um signierte Managementzertifikate für die Controller zu erhalten. Sie müssen Informationen über Ihr Unternehmen, die IP-Adresse oder den DNS-Namen der Controller angeben. 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.

Schritte

1. Wählen Sie Menü: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. Bei Dual-Controllern werden zwei .CSR-Dateien heruntergeladen. Der Speicherort des Downloads hängt von Ihrem Browser ab.

6. Senden Sie die .CSR-Datei(en) an Ihre CA.

Nachdem Sie fertig sind

Wenn Sie die digitalen Zertifikate erhalten, importieren Sie die entsprechenden Zertifikatdateien, die die CA an Sie gesendet hat.

Vertrauenswürdige Zertifikate für Controller importieren

Nachdem Sie digitale Zertifikate von einer Zertifizierungsstelle (CA) erhalten haben, können Sie die Zertifikatskette (Zwischen- und Stammverzeichnis) für die Controller importieren.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Sie haben eine Anfrage zur Zertifikatssignierung (.CSR-Datei) erstellt und an die CA gesendet.
- Die CA hat vertrauenswürdige Zertifikatdateien zurückgegeben.
- Die Zertifikatdateien werden auf Ihrem lokalen System installiert.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Sie die vertrauenswürdigen Zertifikate für die Controller des Speicherarrays hochladen.

Schritte

1. Wählen Sie Menü: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.

Nachdem Sie fertig sind

Importieren Sie das Managementzertifikat.

Importieren Sie ein Managementzertifikat für Controller

Nach dem Import der vertrauenswürdigen Zertifikatskette importieren Sie für jeden Controller im Speicher-Array eine Management (signierte) Zertifikatdatei.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Die vertrauenswürdigen Zertifikate wurden importiert.
- Die CA hat für jeden Controller eine Management-Zertifikatdatei zurückgegeben.
- Die Managementzertifikatdatei(en) stehen auf Ihrem lokalen System zur Verfügung.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Sie die Management-Zertifikatdateien für die Controller-Authentifizierung hochladen.

Schritte

1. Wählen Sie Menü: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 **Durchsuchen**, um die Datei für Controller A. auszuwählen Wenn es zwei Controller gibt, klicken Sie auf die zweite Schaltfläche **Durchsuchen**, um die Datei für Controller B auszuwählen

   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.

Anzeigen importierter Zertifikatinformationen

Auf der Seite Zertifikate können Sie den Zertifikatstyp, die ausstellende Behörde und den gültigen Datumsbereich der zuvor importierten Zertifikate anzeigen.

Bevor Sie beginnen

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

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Informationen für vom Benutzer installierte oder vorinstallierte Zertifikate angezeigt werden.

Schritte

1. Wählen Sie Menü:Einstellungen[Zertifikate].
2. Wählen Sie eine der Registerkarten aus, um Informationen zu Managementzertifikaten für die Controller, vertrauenswürdige Zertifikate und Zertifikate für einen Schlüsselverwaltungsserver anzuzeigen.

Registerkarte	Beschreibung
Array-Management	Zeigen Sie Informationen zu allen Serverzertifikaten an, die für die Controller importiert wurden.
Bewährt	Informationen zu allen vertrauenswürdigen (Root-) 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 zum Speicher-Array hochgeladen hat (einschließlich vertrauenswürdiger Zertifikate, LDAPS-Zertifikate und Identity Federation-Zertifikaten). • **Vorinstalliert**. Im Speicher-Array enthaltene Zertifikate.
Verschlüsselungs-Management	Informationen zu allen Management-Zertifikaten anzeigen, die für einen externen Schlüsselverwaltungsserver importiert wurden.

Vertrauenswürdige Zertifikate löschen

Sie können alle vom Benutzer importierten Zertifikate löschen.

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 das System, wenn Sie ein Zertifikat löschen, das zur Authentifizierung der Managementzertifikate oder des LDAP-Servers des Speicherarrays verwendet wird, bevor Sie ein Ersatzzertifikat importieren.

Über diese Aufgabe

Diese Aufgabe beschreibt das Löschen von vom Benutzer importierten Zertifikaten. Vordefinierte Zertifikate können nicht gelöscht werden.

Schritte

1. Wählen Sie Menü: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 Menü:Sonstige Aufgaben[Löschen].

   Das Dialogfeld Vertrauenswürdiges Zertifikat bestätigen wird geöffnet.
5. Typ `delete` Klicken Sie im Feld auf **Löschen**.

Managementzertifikate zurücksetzen

Sie können die Managementzertifikate auf dem Speicher-Array wieder in den werkseitig selbstsignierten Status zurücksetzen.

Bevor Sie beginnen

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

Über diese Aufgabe

Durch das Zurücksetzen der Managementzertifikate auf dem Speicher-Array werden die aktuellen Managementzertifikate von jedem der Controller gelöscht. Nach dem Zurücksetzen der Zertifikate werden die Controller mit selbstsignierten Zertifikaten zurückgesetzt.

Schritte

1. Wählen Sie Menü:Einstellungen[Zertifikate].
2. Wählen Sie auf der Registerkarte **Array Management** die Option **Zurücksetzen**.

   Das Dialogfeld „Management-Zertifikate zurücksetzen bestätigen*“ wird geöffnet.
3. Typ `reset` Klicken Sie im Feld auf **Zurücksetzen**.

Ergebnisse

Nach der Aktualisierung des Browsers werden die Controller mithilfe von selbstsignierten Zertifikaten wiederhergestellt. Das System fordert Benutzer daher auf, das selbstsignierte Zertifikat für ihre Sitzungen manuell anzunehmen.

Füllen Sie die Anforderung zum Signieren des CA-Zertifikats (CSR) für einen Schlüsselserver aus

Um ein Zertifikat für eine Zertifizierungsstelle (Certificate Authority, CA) für einen Schlüsselverwaltungsserver zu erhalten, müssen Sie zuerst eine CSR-Datei (Certificate

Signing Request) erstellen.

Bevor Sie beginnen

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

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Sie die CSR-Dateien (Certificate Signing Requests) generieren, die Sie an eine CA senden, um signierte Zertifikate für einen Schlüsselverwaltungsserver zu erhalten. Während dieser Aufgabe müssen Sie Informationen über Ihr Unternehmen angeben.

Schritte

1. Wählen Sie Menü: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. Senden Sie die .CSR-Datei(en) an Ihre CA.

Nachdem Sie fertig sind

Wenn Sie die Client- und Serverzertifikate vom Schlüsselverwaltungsserver beziehen, importieren Sie diese zur Authentifizierung mit den Speicher-Array-Controllern.

Importieren Sie die Zertifikate für den Schlüsselverwaltungsserver

Für das externe Verschlüsselungsmanagement importieren Sie Zertifikate zur Authentifizierung zwischen dem Storage-Array und dem Verschlüsselungsmanagement-Server, damit sich die beiden Einheiten gegenseitig vertrauen können. Es gibt zwei Arten von Zertifikaten: Das Clientzertifikat überprüft die Controller, 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.
- Für das Speicherarray ist ein Clientzertifikat verfügbar.

Ein Client-Zertifikat validiert die Controller des Speicherarrays, damit der Schlüsselverwaltungsserver ihren IP-Adressen vertrauen kann. Um ein Client-Zertifikat zu erhalten, müssen Sie eine CSR für das Speicher-Array ausfüllen und es anschließend auf den Schlüsselverwaltungsserver hochladen. Generieren Sie vom Server ein Clientzertifikat.

- Das Zertifikat für den Schlüsselmanagement-Server ist verfügbar.

Ein Zertifikat für den Schlüsselmanagementserver validiert den Server, damit das Speicherarray seine IP-Adresse anvertrauen kann. Um ein Zertifikat für den Schlüsselverwaltungsserver zu erhalten, müssen Sie es vom Schlüsselverwaltungsserver generieren.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Zertifikatdateien für die Authentifizierung zwischen den Speicher-Array-Controllern und dem Schlüsselverwaltungsserver hochgeladen werden.

Schritte

1. Wählen Sie Menü: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 auf die Schaltflächen **Durchsuchen**, um die Dateien auszuwählen.

   Die Dateinamen werden im Dialogfeld angezeigt.

4. Klicken Sie Auf **Import**.

   Die Datei(en) 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 Menü: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**.

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. Die automatische Überprüfung des Widerrufs ist hilfreich, wenn die Zertifizierungsstelle (CA) ein Zertifikat nicht ordnungsgemäß ausgestellt hat oder wenn ein privater Schlüssel kompromittiert wird.

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

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 Menü:Einstellungen[Zertifikate].
2. Wählen Sie die Registerkarte * Trusted* aus.

> Sie können auch die Überprüfung des Widerrufs über die Registerkarte Schlüsselverwaltung 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**.

Ergebnis

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

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 müssen in System Manager hochgeladen werden?

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 Speicherarrays, damit der Schlüsselverwaltungsserver ihren IP-Adressen vertrauen kann. Um ein Client-Zertifikat zu erhalten, müssen Sie eine CSR für das Speicher-Array ausfüllen und es anschließend auf den Schlüsselverwaltungsserver hochladen. Generieren Sie vom Server ein Clientzertifikat, und importieren Sie es dann mit System Manager.

Ein Zertifikat für den Schlüsselmanagementserver validiert den Schlüsselmanagementserver, damit das Storage-Array seiner IP-Adresse vertrauen kann. Um ein Zertifikat für den Schlüsselverwaltungsserver zu erhalten, müssen Sie es vom Schlüsselverwaltungsserver generieren.

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.