Zertifikate verwenden

SANtricity 11.7

NetApp
February 12, 2024

Inhalt

Zertifikate verwenden

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

Über diese Aufgabe

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

Schritt 1: Schließen Sie CSRs für die Controller ab

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) für jeden Controller im Speicher-Array generieren.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie eine CSR-Datei aus System Manager generiert wird. Der CSR stellt Informationen über Ihr Unternehmen und entweder die IP-Adresse oder den DNS-Namen des Controllers zur Verfügung. Während dieser Aufgabe wird eine CSR-Datei erzeugt, wenn das Speicher-Array einen Controller und zwei CSR-Dateien hat, wenn es zwei Controller hat.

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

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. Der DNS-Name kann nicht mit einem Platzhalter beginnen.
   - **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. Der DNS-Name kann nicht mit einem Platzhalter beginnen. 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. Gehen Sie zu Schritt 2: Senden Sie die CSR-Dateien.

Schritt 2: Senden Sie die CSR-Dateien

Nachdem Sie die CSR-Dateien (Certificate Signing Request) erstellt haben, senden Sie die Dateien an eine Zertifizierungsstelle (CA). 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 heruntergeladenen CSR-Dateien.
2. Senden Sie die CSR-Dateien 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: Signierte Zertifikate für Controller importieren.

Schritt 3: Signierte Zertifikate für Controller importieren

Nachdem Sie von der Zertifizierungsstelle (CA) signierte Zertifikate erhalten haben, importieren Sie die Dateien für die Controller.

Bevor Sie beginnen

- Die CA hat signierte Zertifikatdateien zurückgegeben. Diese Dateien enthalten das Stammzertifikat, ein oder mehrere Zwischenzertifikate und die Serverzertifikate.
- 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 die Serverzertifikate, die die Controller identifizieren. 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 das Sie auf System Manager zugreifen.

Schritte

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

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

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

   Die Dateien werden hochgeladen und validiert.

Ergebnis

Die Sitzung wird automatisch beendet. Sie müssen sich erneut anmelden, damit die Zertifikate wirksam werden. Wenn Sie sich erneut anmelden, werden die neuen CA-signierten Zertifikate 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 Menü:Einstellungen[Zertifikate].
2. Wählen Sie auf der Registerkarte Array Management die Option **Zurücksetzen**.

   Es wird ein Dialogfeld zum Zurücksetzen der Managementzertifikate bestätigen 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 installiertes** — Zertifikate, die ein Benutzer in das Speicher-Array hochgeladen hat, die vertrauenswürdige Zertifikate enthalten können, 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 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.

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 Menü: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 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**.

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. Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der wichtige Management-Server seine KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen kann.

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. 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. Sie müssen sowohl die Client-Zertifikatdatei für die Controller als auch die Serverzertifikatdatei für den Schlüsselverwaltungsserver laden.

Bevor Sie beginnen

- 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 eine Zertifikatdatei vom Schlüsselverwaltungsserver abrufen und diese Datei anschließend auf den Host kopieren, auf den Sie auf System Manager zugreifen. Ein Zertifikat für den Schlüsselmanagementserver validiert den Schlüsselmanagementserver, damit das Storage-Array seiner

IP-Adresse vertrauen kann. Sie können für den Schlüsselverwaltungsserver ein Root-, Intermediate- oder Serverzertifikat verwenden.

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

Schritte

1. Wählen Sie Menü:Einstellungen[Zertifikate].
2. Wählen Sie auf der Registerkarte Schlüsselverwaltung 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. Sie können für den Schlüsselverwaltungsserver ein Stammzertifikat, ein Zwischenzertifikat oder ein Serverzertifikat auswählen.

   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 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**.