Sicherheitsschlüsselmanagement

SANtricity 11.5

NetApp
February 12, 2024

Inhalt

Sicherheitsschlüsselmanagement

Konzepte

Funktionsweise der Laufwerkssicherheitsfunktion

Laufwerkssicherheit ist eine Funktion des Storage Arrays, die eine zusätzliche Sicherheitsschicht bietet – entweder mit vollständigen Festplatten-Verschlüsselung (FDE) oder FIPS-Laufwerken (Federal Information Processing Standard). Wenn diese Laufwerke zusammen mit der Sicherheitsfunktion des Laufwerks verwendet werden, benötigen sie einen Sicherheitsschlüssel für den Zugriff auf ihre Daten. Wenn die Laufwerke physisch aus dem Array entfernt werden, können sie erst betrieben werden, wenn sie in einem anderen Array installiert sind. Zu diesem Zeitpunkt befinden sie sich in einem Sicherheitsstatus, bis der richtige Sicherheitsschlüssel bereitgestellt wird.

So implementieren Sie Drive Security

Um die Laufwerkssicherheit zu implementieren, führen Sie die folgenden Schritte aus.

1. Rüsten Sie Ihr Storage-Array mit sicheren Laufwerken aus – entweder mit FDE- oder mit FIPS-Laufwerken. (Für Volumes, die FIPS-Unterstützung erfordern, verwenden Sie nur FIPS-Laufwerke. Durch das Mischen von FIPS- und FDE-Laufwerken in einer Volume-Gruppe oder einem Pool werden alle Laufwerke als FDE-Laufwerke behandelt. Außerdem kann ein FDE-Laufwerk nicht zu einer Ersatzfestplatte in einer reinen FIPS-Volume-Gruppe oder einem Pool hinzugefügt oder verwendet werden.)
2. Erstellen Sie einen Sicherheitsschlüssel, d. h. eine Zeichenkette, die vom Controller und den Laufwerken für Lese-/Schreibzugriff freigegeben wird. Sie können entweder einen internen Schlüssel aus dem persistenten Speicher des Controllers oder einen externen Schlüssel von einem Schlüsselmanagementserver erstellen. Für das externe Verschlüsselungsmanagement muss eine Authentifizierung mit dem Verschlüsselungsmanagement-Server eingerichtet werden.
3. Aktivieren Sie die Laufwerkssicherheit für Pools und Volume-Gruppen:
   - Erstellen Sie einen Pool oder eine Volume-Gruppe (suchen Sie in der Spalte **Secure-able** in der Tabelle Kandidaten nach **Ja**).
   - Wählen Sie einen Pool oder eine Volume-Gruppe aus, wenn Sie ein neues Volume erstellen (suchen Sie nach **Ja** neben **sicher-fähig** in der Tabelle für Pool- und Volume-Gruppen Kandidaten).

Wie Drive Security auf der Laufwerksebene funktioniert

Ein sicheres Laufwerk mit FDE oder FIPS verschlüsselt Daten beim Schreiben und entschlüsselt Daten beim Lesen. Diese Ver- und Entschlüsselung hat keine Auswirkungen auf die Leistung oder den Anwender-Workflow. Jedes Laufwerk verfügt über einen eigenen eindeutigen Verschlüsselungsschlüssel, der nie vom Laufwerk übertragen werden kann.

Die Sicherheitsfunktion des Laufwerks bietet zusätzlichen Schutz durch sichere Laufwerke. Wenn auf diesen Laufwerken Volume-Gruppen oder -Pools zur Laufwerkssicherheit ausgewählt sind, suchen die Laufwerke nach einem Sicherheitsschlüssel, bevor sie den Zugriff auf die Daten zulassen. Die Laufwerkssicherheit für Pools und Volume-Gruppen kann jederzeit aktiviert werden, ohne dass bestehende Daten auf dem Laufwerk beeinträchtigt werden. Allerdings können Sie die Laufwerksicherheit nicht deaktivieren, ohne alle Daten auf dem Laufwerk zu löschen.

So arbeitet Drive Security auf Ebene des Storage Arrays

Mit der Laufwerkssicherheitsfunktion erstellen Sie einen Sicherheitsschlüssel, der von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln die sicher-aktivierten Laufwerke in den Status Sicherheitsverriegelt, bis der Controller den Sicherheitsschlüssel anwendet.

Wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt und in einem anderen Speicher-Array neu installiert wird, befindet sich das Laufwerk in einem gesperrten Zustand. Das neu aufgelegene Laufwerk sucht nach dem Sicherheitsschlüssel, bevor es die Daten wieder zugänglich macht. Um die Daten zu entsperren, wenden Sie den Sicherheitsschlüssel aus dem Quell-Speicher-Array an. Nach erfolgreicher Entsperrung verwendet das neu aufgelegte Laufwerk dann den bereits im Ziel-Speicher-Array gespeicherten Sicherheitsschlüssel und die importierte Sicherheitsschlüsseldatei wird nicht mehr benötigt.

> Für das interne Verschlüsselungsmanagement wird der tatsächliche Sicherheitsschlüssel auf dem Controller an einem nicht zugänglichen Ort gespeichert. Sie ist weder in menschlich lesbarem Format, noch ist sie vom Benutzer zugänglich.

So arbeitet Drive Security auf Volume-Ebene

Wenn Sie einen Pool oder eine Volume-Gruppe aus sicheren Laufwerken erstellen, können Sie auch die Laufwerksicherheit für diese Pools oder Volume-Gruppen aktivieren. Mit der Option Laufwerkssicherheit können die Laufwerke und damit verbundene Volume-Gruppen und Pools sicher-*enabled* erstellt werden.

Beachten Sie die folgenden Richtlinien, bevor Sie Volume-Gruppen und -Pools mit sicheren Aktivierung erstellen:

- Volume-Gruppen und Pools müssen vollständig aus sicheren Laufwerken bestehen. (Für Volumes, die FIPS-Unterstützung erfordern, verwenden Sie nur FIPS-Laufwerke. Durch das Mischen von FIPS- und FDE-Laufwerken in einer Volume-Gruppe oder einem Pool werden alle Laufwerke als FDE-Laufwerke behandelt. Außerdem kann ein FDE-Laufwerk nicht zu einer Ersatzfestplatte in einer reinen FIPS-Volume-Gruppe oder einem Pool hinzugefügt oder verwendet werden.)
- Volume-Gruppen und Pools müssen sich im optimalen Zustand befinden.

Funktionsweise von Sicherheitsschlüsselmanagement

Bei der Implementierung der Laufwerkssicherheitsfunktion benötigen die sicheren Laufwerke (FIPS oder FDE) einen Sicherheitsschlüssel für den Datenzugriff. Ein Sicherheitsschlüssel ist eine Zeichenkette, die zwischen diesen Laufwerkstypen und den Controllern in einem Speicher-Array gemeinsam verwendet wird.

Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln die sicher-aktivierten Laufwerke in den Status Sicherheitsverriegelt, bis der Controller den Sicherheitsschlüssel anwendet. Wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird, sind die Daten des Laufwerks gesperrt. Wenn das Laufwerk in einem anderen Speicher-Array neu installiert wird, sucht es nach dem Sicherheitsschlüssel, bevor es die Daten wieder zugänglich macht. Um die Daten zu entsperren, müssen Sie den ursprünglichen Sicherheitsschlüssel anwenden.

Sie können Sicherheitsschlüssel mit einer der folgenden Methoden erstellen und verwalten:

- Internes Verschlüsselungsmanagement auf dem persistenten Speicher des Controllers.
- Externes Verschlüsselungskeymanagement auf einem externen Verschlüsselungsmanagement-Server.

Internes Verschlüsselungsmanagement

Interne Schlüssel befinden sich im persistenten Speicher des Controllers. Führen Sie folgende Schritte durch, um das interne Verschlüsselungsmanagement zu implementieren:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.
3. Erstellen Sie einen internen Sicherheitsschlüssel, der das Definieren einer Kennung und einer Passphrase beinhaltet. Die Kennung ist eine Zeichenfolge, die dem Sicherheitsschlüssel zugeordnet ist und auf dem Controller und allen Laufwerken gespeichert ist, die mit dem Schlüssel verknüpft sind. Der Passphrase wird verwendet, um den Sicherheitsschlüssel für Sicherungszwecke zu verschlüsseln. Um einen internen Schlüssel zu erstellen, gehen Sie zu Menü:Einstellungen[System > Sicherheitsschlüsselverwaltung > Internen Schlüssel erstellen].

Der Sicherheitsschlüssel wird auf dem Controller an einem nicht zugänglichen Ort gespeichert. Anschließend können sichere Volume-Gruppen und -Pools erstellt oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktiviert werden.

Externes Verschlüsselungskeymanagement

Externe Schlüssel werden mithilfe eines Key Management Interoperability Protocol (KMIP) auf einem separaten Verschlüsselungsmanagement-Server aufbewahrt. Um externes Verschlüsselungsmanagement zu implementieren, führen Sie die folgenden Schritte aus:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.
3. Füllen Sie eine Client Certificate Signing Request (CSR) für die Authentifizierung zwischen dem Speicher-Array und dem Schlüsselverwaltungsserver aus, und laden Sie sie herunter. Wechseln Sie zum Menü:Einstellungen[Zertifikate > Schlüsselverwaltung > CSR abschließen].
4. Erstellen und laden Sie mithilfe der heruntergeladenen CSR-Datei ein Client-Zertifikat vom Schlüsselverwaltungsserver herunter.
5. Stellen Sie sicher, dass das Clientzertifikat und eine Kopie des Zertifikats für den Schlüsselverwaltungsserver auf Ihrem lokalen Host verfügbar sind.
6. Erstellen eines externen Schlüssels, der die IP-Adresse des Verschlüsselungsmanagement-Servers und die Port-Nummer, die für die KMIP-Kommunikation verwendet wird, definiert. Während dieses Prozesses laden Sie auch Zertifikatdateien. Um einen externen Schlüssel zu erstellen, gehen Sie zu Menü:Einstellungen[System > Sicherheitsschlüsselverwaltung > External Key erstellen].

Das System stellt mit den eingegebenen Anmeldedaten eine Verbindung zum Schlüsselverwaltungsserver her. Anschließend können sichere Volume-Gruppen und -Pools erstellt oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktiviert werden.

Terminologie der Laufwerksicherheit

Erfahren Sie, wie die Bedingungen für die Laufwerksicherheit auf Ihr Speicherarray

angewendet werden.

Laufzeit	Beschreibung
Laufwerkssicherheit	Laufwerkssicherheit ist eine Funktion des Storage Arrays, die eine zusätzliche Sicherheitsschicht bietet – entweder mit vollständigen Festplatten-Verschlüsselung (FDE) oder FIPS-Laufwerken (Federal Information Processing Standard). Wenn diese Laufwerke zusammen mit der Sicherheitsfunktion des Laufwerks verwendet werden, benötigen sie einen Sicherheitsschlüssel für den Zugriff auf ihre Daten. Wenn die Laufwerke physisch aus dem Array entfernt werden, können sie erst betrieben werden, wenn sie in einem anderen Array installiert sind. Zu diesem Zeitpunkt befinden sie sich in einem Sicherheitsstatus, bis der richtige Sicherheitsschlüssel bereitgestellt wird.
FDE-Laufwerke	Vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) ermöglicht die Verschlüsselung auf Festplattenlaufwerken auf Hardware-Ebene. Die Festplatte enthält einen ASIC-Chip, der Daten während des Schreibvorgangs verschlüsselt und die Daten beim Lesen entschlüsselt.
FIPS-Laufwerke	FIPS-Laufwerke verwenden Federal Information Processing Standards (FIPS) 140-2 Level 2. Es handelt sich im Wesentlichen um FDE-Laufwerke, die den Standards der US-Regierung entsprechen, um solide Verschlüsselungsalgorithmen und -Methoden sicherzustellen. FIPS-Laufwerke haben höhere Sicherheitsstandards als FDE-Laufwerke.
Management- Client	Ein lokales System (Computer, Tablet usw.), das einen Browser für den Zugriff auf System Manager enthält.

Laufzeit	Beschreibung
Ausdruck übergeben	Der Passphrase wird verwendet, um den Sicherheitsschlüssel für Sicherungszwecke zu verschlüsseln. Der gleiche Passphrase, der für die Verschlüsselung des Sicherheitsschlüssels verwendet wird, muss angegeben werden, wenn der gesicherte Sicherheitsschlüssel als Ergebnis einer Laufwerksmigration oder eines Kopftauschens importiert wird. Ein Passphrase kann zwischen 8 und 32 Zeichen lang sein. Der Passphrase für die Laufwerksicherheit ist unabhängig vom Administratorkennwort des Speicherarrays.
Secure-fähige Laufwerke	Sichere Laufwerke können entweder vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) sein, die Daten während des Schreibvorgangs verschlüsseln und Daten während Lesevorgängen entschlüsseln. Diese Laufwerke gelten als sicher-*fähig*, da sie mit der Sicherheitsfunktion des Laufwerks für zusätzliche Sicherheit verwendet werden können. Wenn die Laufwerkssicherheitsfunktion für Volume-Gruppen und -Pools aktiviert ist, die mit diesen Laufwerken verwendet werden, werden die Laufwerke sicher-*Enabled*.
Secure-Enabled Laufwerke	Secure-Enabled-Laufwerke werden mit der Drive Security-Funktion verwendet. Wenn Sie die Laufwerkssicherheitsfunktion aktivieren und dann Laufwerksicherheit auf einem Pool oder einer Volume-Gruppe auf Secure-*fähigen*-Laufwerken anwenden, werden die Laufwerke sicher-*aktiviert_*. Lese- und Schreibzugriff ist nur über einen Controller verfügbar, der mit dem korrekten Sicherheitsschlüssel konfiguriert ist. Diese zusätzliche Sicherheit verhindert einen nicht autorisierten Zugriff auf die Daten auf einem Laufwerk, das physisch vom Storage-Array entfernt wird.

Laufzeit	Beschreibung
Sicherheitsschlüssel	Ein Sicherheitsschlüssel ist eine Zeichenkette, die von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln die sicher-aktivierten Laufwerke in den Status Sicherheitsverriegelt, bis der Controller den Sicherheitsschlüssel anwendet. Wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird, sind die Daten des Laufwerks gesperrt. Wenn das Laufwerk in einem anderen Speicher-Array neu installiert wird, sucht es nach dem Sicherheitsschlüssel, bevor es die Daten wieder zugänglich macht. Um die Daten zu entsperren, müssen Sie den ursprünglichen Sicherheitsschlüssel anwenden. Sie können Sicherheitsschlüssel mit einer der folgenden Methoden erstellen und verwalten: • Internes Verschlüsselungsmanagement – Erstellen und Warten von Sicherheitsschlüsseln im persistenten Speicher des Controllers • Externes Verschlüsselungsmanagement — Erstellen und Verwalten von Sicherheitsschlüsseln auf einem externen Schlüsselverwaltungsserver.
Kennung des Sicherheitsschlüssels	Die Security Key-ID ist eine Zeichenfolge, die dem Sicherheitsschlüssel bei der Schlüsselerstellung zugeordnet ist. Die Kennung wird auf dem Controller und auf allen Laufwerken gespeichert, die mit dem Sicherheitsschlüssel verbunden sind.

Anleitungen

Interner Sicherheitsschlüssel erstellen

Zur Verwendung der Laufwerkssicherheitsfunktion können Sie einen internen Sicherheitsschlüssel erstellen, der von den Controllern und sicheren Laufwerken im Speicher-Array gemeinsam genutzt wird. Interne Schlüssel befinden sich im persistenten Speicher des Controllers.

Bevor Sie beginnen

- Sichere Laufwerke müssen im Speicher-Array installiert sein. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
- Die Laufwerkssicherheitsfunktion muss aktiviert sein. Andernfalls wird während dieser Aufgabe ein Dialogfeld **Sicherheitsschlüssel nicht erstellen** geöffnet. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.

Wenn sowohl FDE- als auch FIPS-Laufwerke im Storage Array installiert werden, nutzen sie alle denselben Sicherheitsschlüssel.

Über diese Aufgabe

In dieser Aufgabe definieren Sie eine Kennung und eine Passphrase, die dem internen Sicherheitsschlüssel zugeordnet werden sollen.

Der Passphrase für die Laufwerksicherheit ist unabhängig vom Administratorkennwort des Speicherarrays.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter **Security Key Management** die Option **Interner Schlüssel erstellen**.

   Wenn Sie noch keinen Sicherheitsschlüssel generiert haben, wird das Dialogfeld **Sicherheitsschlüssel erstellen** geöffnet.

3. Geben Sie Informationen in die folgenden Felder ein:

   - Definieren Sie eine Sicherheitsschlüssel-ID: Sie können entweder den Standardwert akzeptieren (Storage Array Name und Zeitstempel, der von der Controller-Firmware generiert wird) oder Ihren eigenen Wert eingeben. Sie können bis zu 189 alphanumerische Zeichen ohne Leerzeichen, Satzzeichen oder Symbole eingeben.

     Zusätzliche Zeichen werden automatisch generiert und an beide Enden der eingegebenen Zeichenfolge angehängt. Die generierten Zeichen stellen sicher, dass die Kennung eindeutig ist.

   - Passphrase definieren/Passphrase erneut eingeben — Geben Sie eine Passphrase ein und bestätigen Sie diese. Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:
     - Ein Großbuchstabe (einer oder mehrere). Beachten Sie, dass die Passphrase Groß- und Kleinschreibung beachtet.
     - Eine Nummer (eine oder mehrere).
     - Ein nicht-alphanumerisches Zeichen wie !, *, @ (eines oder mehrere).

   Achten Sie darauf, Ihre Einträge zur späteren Verwendung aufzuzeichnen. Wenn Sie ein sicheres Laufwerk aus dem Speicher-Array verschieben müssen, müssen Sie die Kennung kennen und den Ausdruck übergeben, um Laufwerkdaten zu entsperren.

4. Klicken Sie Auf **Erstellen**.

   Der Sicherheitsschlüssel wird auf dem Controller an einem nicht zugänglichen Ort gespeichert. Zusammen mit dem eigentlichen Schlüssel gibt es eine verschlüsselte Schlüsseldatei, die von Ihrem Browser heruntergeladen wird.

   Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

5. Notieren Sie sich die Schlüsselkennung, den Passphrase und den Speicherort der heruntergeladenen Schlüsseldatei, und klicken Sie dann auf **Schließen**.

Ergebnis

Sie können jetzt sichere Volume-Gruppen oder -Pools erstellen oder die Sicherheit bei vorhandenen Volume-Gruppen und -Pools aktivieren.

> Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln alle sicheren Laufwerke in den Status Sicherheitsverriegelt. In diesem Zustand sind die Daten nicht zugänglich, bis der Controller den korrekten Sicherheitsschlüssel während der Laufwerkinitialisierung anwendet. Wenn ein gesperrtes Laufwerk physisch entfernt und in einem anderen System installiert wird, verhindert der Status „Sicherheitsgesperrt“ unbefugten Zugriff auf seine Daten.

Nachdem Sie fertig sind

Sie sollten den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass die Schlüsseldatei nicht beschädigt ist.

Externen Sicherheitsschlüssel erstellen

Um die Laufwerkssicherheitsfunktion mit einem Schlüsselverwaltungsserver verwenden zu können, müssen Sie einen externen Schlüssel erstellen, der vom Schlüsselverwaltungsserver und den sicheren Laufwerken im Speicher-Array gemeinsam genutzt wird.

Bevor Sie beginnen

- Sichere Laufwerke müssen im Array installiert werden. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.

  > Wenn sowohl FDE- als auch FIPS-Laufwerke im Storage Array installiert werden, nutzen sie alle denselben Sicherheitsschlüssel.

- Die Laufwerkssicherheitsfunktion muss aktiviert sein. Andernfalls wird während dieser Aufgabe ein Dialogfeld **Sicherheitsschlüssel nicht erstellen** geöffnet. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.
- Die Client- und Server-Zertifikate sind auf Ihrem lokalen Host verfügbar, sodass sich das Storage-Array und der Schlüsselverwaltungsserver gegenseitig authentifizieren können. Das Clientzertifikat validiert die Controller, während das Serverzertifikat den Schlüsselverwaltungsserver validiert.

Über diese Aufgabe

In dieser Aufgabe definieren Sie die IP-Adresse des Schlüsselverwaltungsservers und die verwendete Portnummer und laden dann Zertifikate für die externe Schlüsselverwaltung.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter * Security Key Management* die Option **External Key erstellen** aus.

   > Wenn derzeit die interne Schlüsselverwaltung konfiguriert ist, wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden, zu bestätigen, dass Sie zur externen Schlüsselverwaltung wechseln möchten.

   Das Dialogfeld * External Security Key erstellen* wird geöffnet.

3. Geben Sie unter **Verbinden mit Key Server** Informationen in die folgenden Felder ein:
   - Adresse des Schlüsselverwaltungsservers — Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein, der für die Schlüsselverwaltung verwendet wird.
   - Port-Nummer des Verschlüsselungsmanagement — Geben Sie die Portnummer ein, die für die Kommunikation mit dem Key Management Interoperability Protocol (KMIP) verwendet wird. Die am häufigsten für die Kommunikation mit dem Verschlüsselungsmanagement-Server verwendete Portnummer ist 5696.
   - Client-Zertifikat auswählen — Klicken Sie auf die erste Schaltfläche Durchsuchen, um die Zertifikatdatei für die Speicher-Array-Controller auszuwählen.
   - Server-Zertifikat des Schlüsselverwaltungsservers auswählen - Klicken Sie auf die zweite Schaltfläche Durchsuchen, um die Zertifikatdatei für den Schlüsselverwaltungsserver auszuwählen.
4. Klicken Sie Auf **Weiter**.
5. Geben Sie unter **Create/Backup Key** Informationen in das folgende Feld ein:
   - Passphrase definieren/Passphrase erneut eingeben — Geben Sie eine Passphrase ein und bestätigen Sie diese. Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:
     - Ein Großbuchstabe (einer oder mehrere). Beachten Sie, dass die Passphrase Groß- und Kleinschreibung beachtet.
     - Eine Nummer (eine oder mehrere).
     - Ein nicht-alphanumerisches Zeichen wie !, *, @ (eines oder mehrere).

   > Achten Sie darauf, Ihre Einträge zur späteren Verwendung aufzuzeichnen. Wenn Sie ein sicheres Laufwerk aus dem Speicher-Array verschieben möchten, müssen Sie den Passphrase kennen, um die Laufwerkdaten zu entsperren.

6. Klicken Sie Auf **Fertig Stellen**.

   Das System stellt mit den eingegebenen Anmeldedaten eine Verbindung zum Schlüsselverwaltungsserver her. Anschließend wird eine Kopie des Sicherheitsschlüssels auf Ihrem lokalen System gespeichert.

   > Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

7. Notieren Sie Ihren Passphrase und den Speicherort der heruntergeladenen Schlüsseldatei und klicken Sie dann auf **Schließen**.

   Auf der Seite wird die folgende Meldung mit zusätzlichen Links zur externen Schlüsselverwaltung angezeigt:

   ```
   Current key management method: External
   ```

8. Testen Sie die Verbindung zwischen dem Speicher-Array und dem Schlüsselverwaltungsserver, indem Sie **Testkommunikation** wählen.

   Die Testergebnisse werden im Dialogfeld angezeigt.

Ergebnisse

Wenn das externe Verschlüsselungsmanagement aktiviert ist, können Sie sicher aktivierte Volume-Gruppen oder -Pools erstellen oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktivieren.

Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln alle sicheren Laufwerke in den Status Sicherheitsverriegelt. In diesem Zustand sind die Daten nicht zugänglich, bis der Controller den korrekten Sicherheitsschlüssel während der Laufwerkinitialisierung anwendet. Wenn ein gesperrtes Laufwerk physisch entfernt und in einem anderen System installiert wird, verhindert der Status „Sicherheitsgesperrt“ unbefugten Zugriff auf seine Daten.

Nachdem Sie fertig sind

- Sie sollten den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass die Schlüsseldatei nicht beschädigt ist.

Sicherheitsschlüssel ändern

Sie können jederzeit einen Sicherheitsschlüssel durch einen neuen Schlüssel ersetzen. Möglicherweise müssen Sie einen Sicherheitsschlüssel ändern, wenn Ihr Unternehmen eine potenzielle Sicherheitsverletzung hat und sicherstellen möchte, dass nicht autorisierte Mitarbeiter nicht auf die Daten der Laufwerke zugreifen können.

Bevor Sie beginnen

Ein Sicherheitsschlüssel ist bereits vorhanden.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie ein Sicherheitsschlüssel geändert und durch einen neuen ersetzt wird. Nach diesem Vorgang wird der alte Schlüssel nicht validiert.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter * Security Key Management* die Option **Change Key**.

   Das Dialogfeld **Sicherheitsschlüssel ändern** wird geöffnet.

3. Geben Sie die folgenden Felder ein.

   - Definieren Sie eine Security Key ID — (nur für interne Sicherheitsschlüssel.) Akzeptieren Sie den Standardwert (Storage Array-Name und Zeitstempel, der von der Controller-Firmware generiert wird) oder geben Sie Ihren eigenen Wert ein. Sie können bis zu 189 alphanumerische Zeichen ohne Leerzeichen, Satzzeichen oder Symbole eingeben.

     Zusätzliche Zeichen werden automatisch generiert und an beide Enden der eingegebenen Zeichenfolge angehängt. Die generierten Zeichen tragen dazu bei, dass die Kennung eindeutig ist.

   - Definieren Sie eine Passphrase/geben Sie die Passphrase ein — Geben Sie in jedes dieser Felder Ihren Passphrase ein. Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:
     - Ein Großbuchstabe (einer oder mehrere). Beachten Sie, dass die Passphrase Groß- und Kleinschreibung beachtet.
     - Eine Nummer (eine oder mehrere).
     - Ein nicht-alphanumerisches Zeichen wie !, *, @ (eines oder mehrere).

Achten Sie darauf, Ihre Einträge für eine spätere Verwendung aufzuzeichnen — Wenn Sie ein sicheres Laufwerk aus dem Speicher-Array verschieben müssen, müssen Sie die Kennung und den Ausdruck kennen, um die Laufwerkdaten zu entsperren.

4. Klicken Sie Auf **Ändern**.

   Der neue Sicherheitsschlüssel überschreibt den vorherigen Schlüssel, der nicht mehr gültig ist.

   Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

5. Notieren Sie sich die Schlüsselkennung, den Passphrase und den Speicherort der heruntergeladenen Schlüsseldatei, und klicken Sie dann auf **Schließen**.

Nachdem Sie fertig sind

Sie sollten den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass die Schlüsseldatei nicht beschädigt ist.

Wechsel von externem zu internem Verschlüsselungsmanagement

Sie können die Verwaltungsmethode für die Laufwerksicherheit von einem externen Schlüsselserver in die interne Methode ändern, die vom Speicher-Array verwendet wird. Der zuvor für das externe Verschlüsselungsmanagement definierte Sicherheitsschlüssel wird dann für das interne Verschlüsselungsmanagement verwendet.

Bevor Sie beginnen

Ein externer Schlüssel wurde erstellt.

Über diese Aufgabe

In dieser Aufgabe deaktivieren Sie die externe Schlüsselverwaltung und laden eine neue Sicherungskopie auf Ihren lokalen Host herunter. Der vorhandene Schlüssel wird weiterhin für die Laufwerksicherheit verwendet, wird aber intern im Speicher-Array verwaltet.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter * Security Key Management* die Option **External Key Management deaktivieren** aus.

   Das Dialogfeld * External Key Management* deaktivieren wird geöffnet.

3. Geben Sie unter **Passphrase definieren/Passphrase erneut eingeben** einen Passphrase für die Sicherung des Schlüssels ein und bestätigen Sie diesen. Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:

   - Ein Großbuchstabe (einer oder mehrere). Beachten Sie, dass die Passphrase Groß- und Kleinschreibung beachtet.
   - Eine Nummer (eine oder mehrere).
   - Ein nicht-alphanumerisches Zeichen wie !, *, @ (eines oder mehrere).

Notieren Sie sich Ihre Einträge für die spätere Verwendung. Wenn Sie ein sicheres Laufwerk aus dem Speicher-Array verschieben müssen, müssen Sie die Kennung kennen und den Ausdruck übergeben, um Laufwerkdaten zu entsperren.

4. Klicken Sie Auf **Deaktivieren**.

   Der Backup-Schlüssel wird auf Ihren lokalen Host heruntergeladen.

5. Notieren Sie sich die Schlüsselkennung, den Passphrase und den Speicherort der heruntergeladenen Schlüsseldatei, und klicken Sie dann auf **Schließen**.

Ergebnisse

Die Laufwerksicherheit wird jetzt intern über das Speicher-Array verwaltet.

Nachdem Sie fertig sind

- Sie sollten den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass die Schlüsseldatei nicht beschädigt ist.

Bearbeiten der Einstellungen des Verschlüsselungsmanagementservers

Wenn Sie die externe Schlüsselverwaltung konfiguriert haben, können Sie die Einstellungen des Verschlüsselungsmanagementservers jederzeit anzeigen und bearbeiten.

Bevor Sie beginnen

Externes Verschlüsselungsmanagement muss konfiguriert werden.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter **Security Key Management** die Option **Key Management Server-Einstellungen anzeigen/bearbeiten** aus.
3. Bearbeiten Sie die Informationen in den folgenden Feldern:
   - Adresse des Schlüsselverwaltungsservers — Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein, der für die Schlüsselverwaltung verwendet wird.
   - KMIP-Port-Nummer – Geben Sie die Portnummer ein, die für die Kommunikation mit dem Key Management Interoperability Protocol (KMIP) verwendet wird.
4. Klicken Sie Auf **Speichern**.

Sicherheitsschlüssel sichern

Nach dem Erstellen oder Ändern eines Sicherheitsschlüssels können Sie eine Sicherungskopie der Schlüsseldatei erstellen, falls das Original beschädigt wird.

Bevor Sie beginnen

- Ein Sicherheitsschlüssel ist bereits vorhanden.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Sie einen zuvor erstellten Sicherheitsschlüssel sichern. Während dieses Verfahrens erstellen Sie einen neuen Passphrase für das Backup. Diese Passphrase muss nicht mit

der Passphrase übereinstimmen, die bei der Erstellung des ursprünglichen Schlüssels oder der letzten Änderung verwendet wurde. Der Passphrase wird nur auf das Backup angewendet, das Sie erstellen.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter * Security Key Management* die Option **Back Up Key**.

   Das Dialogfeld **Sicherheitsschlüssel sichern** wird geöffnet.

3. Geben Sie in den Feldern **Passphrase definieren/Passphrase erneut eingeben** einen Passphrase für dieses Backup ein und bestätigen Sie diesen.

   Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:

   - Ein Großbuchstabe (einer oder mehrere)
   - Eine Nummer (eine oder mehrere)
   - Ein nicht-alphanumerisches Zeichen wie !, *, @ (ein oder mehrere)

   Notieren Sie Ihren Eintrag für die spätere Verwendung. Sie benötigen den Passphrase, um auf die Sicherung dieses Sicherheitsschlüssels zuzugreifen.

4. Klicken Sie Auf **Sichern**.

   Ein Backup des Sicherheitsschlüssels wird auf Ihren lokalen Host heruntergeladen, und dann wird das Dialogfeld **Sicherheitsschlüssel sichern/aufzeichnen** geöffnet.

   Der Pfad für die heruntergeladene Sicherheitsschlüsseldatei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

5. Zeichnen Sie Ihren Passphrase an einem sicheren Ort auf, und klicken Sie dann auf **Schließen**.

Nachdem Sie fertig sind

Sie sollten den Sicherungsschlüssel überprüfen.

Validierung des Sicherheitsschlüssels

Sie können den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass er nicht beschädigt wurde, und um sicherzustellen, dass Sie über einen korrekten Passphrase verfügen.

Bevor Sie beginnen

Ein Sicherheitsschlüssel wurde erstellt.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Sie den zuvor erstellten Sicherheitsschlüssel validieren. Dies ist ein wichtiger Schritt, um sicherzustellen, dass die Schlüsseldatei nicht beschädigt ist und der Passphrase korrekt ist, wodurch sichergestellt wird, dass Sie später auf die Laufwerkdaten zugreifen können, wenn Sie ein sicheres Laufwerk von einem Speicher-Array in ein anderes verschieben.

Schritte

1. Wählen Sie Menü:Einstellungen[System].

2. Wählen Sie unter * Security Key Management* die Option **Validate Key** aus.

   Das Dialogfeld **Sicherheitsschlüssel validieren** wird geöffnet.

3. Klicken Sie auf **Durchsuchen** und wählen Sie dann die Schlüsseldatei aus (z. B. `drivesecurity.slk`).
4. Geben Sie die Passphrase ein, die mit der ausgewählten Taste verknüpft ist.

   Wenn Sie eine gültige Schlüsseldatei auswählen und den Ausdruck übergeben, steht die Schaltfläche **Validieren** zur Verfügung.

5. Klicken Sie Auf **Validieren**.

   Die Ergebnisse der Validierung werden im Dialogfeld angezeigt.

6. Wenn in den Ergebnissen „der Sicherheitsschlüssel erfolgreich validiert wurde“ angezeigt wird, klicken Sie auf **Schließen**. Wenn eine Fehlermeldung angezeigt wird, befolgen Sie die im Dialogfeld angezeigten Anweisungen.

Entsperren Sie Laufwerke mit einem Sicherheitsschlüssel

Wenn Sie sichere Laufwerke von einem Speicher-Array in ein anderes verschieben, müssen Sie den entsprechenden Sicherheitsschlüssel in das neue Speicher-Array importieren. Durch das Importieren des Schlüssels werden die Daten auf den Laufwerken freigeschaltet.

Bevor Sie beginnen

- Das Ziel-Storage-Array (in dem Sie die Laufwerke verschieben) muss bereits einen Sicherheitsschlüssel konfiguriert haben. Die migrierten Laufwerke werden erneut auf das Ziel-Storage-Array übertragen.
- Sie müssen den Sicherheitsschlüssel kennen, der mit den Laufwerken verknüpft ist, die Sie entsperren möchten.
- Die Sicherheitsschlüsseldatei steht auf dem Management-Client zur Verfügung (das System mit einem Browser, der zum Zugriff auf System Manager verwendet wird). Wenn Sie die Laufwerke in ein Storage-Array verschieben, das von einem anderen System gemanagt wird, müssen Sie die Sicherheitsschlüsseldatei auf diesen Management-Client verschieben.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Daten in sicheren Laufwerken entsperrt werden, die von einem Speicher-Array entfernt und in einem anderen neu installiert wurden. Sobald das Array die Laufwerke erkannt hat, wird ein Zustand „Achtung erforderlich“ sowie der Status „Sicherheitsschlüssel erforderlich“ für diese neu gelegenen Laufwerke angezeigt. Sie können Laufwerkdaten entsperren, indem Sie ihren Sicherheitsschlüssel in das Storage-Array importieren. Während dieses Vorgangs wählen Sie die Sicherheitsschlüsseldatei aus und geben den Passphrase für den Schlüssel ein.

Der Passphrase entspricht nicht dem Administratorkennwort des Speicherarrays.

Wenn andere sichere Laufwerke im neuen Speicher-Array installiert sind, verwenden sie möglicherweise einen anderen Sicherheitsschlüssel als den, den Sie importieren. Während des Importvorgangs wird der alte Sicherheitsschlüssel nur verwendet, um die Daten für die zu installierenden Laufwerke freizuschalten. Wenn die Entsperrung erfolgreich ist, werden die neu installierten Laufwerke erneut auf den Sicherheitsschlüssel des Ziel-Speicher-Arrays codiert.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter * Security Key Management* * * Secure Drives entsperren* aus.

   Das Dialogfeld * Sichere Laufwerke entsperren* wird geöffnet. Alle Laufwerke, für die ein Sicherheitsschlüssel erforderlich ist, sind in der Tabelle aufgeführt.

3. Halten Sie optional die Maus über eine Laufwerksnummer, um die Position des Laufwerks (Shelf-Nummer und Einschubnummer) zu sehen.
4. Klicken Sie auf **Durchsuchen** und wählen Sie dann die Sicherheitsschlüsseldatei aus, die dem Laufwerk entspricht, das Sie entsperren möchten.

   Die ausgewählte Schlüsseldatei wird im Dialogfeld angezeigt.

5. Geben Sie den Passphrase ein, der dieser Schlüsseldatei zugeordnet ist.

   Die eingegebenen Zeichen sind maskiert.

6. Klicken Sie Auf **Entsperren**.

   Wenn der Entsperrvorgang erfolgreich ist, wird im Dialogfeld „die zugeordneten sicheren Laufwerke wurden entsperrt“ angezeigt.

Ergebnisse

Wenn alle Laufwerke gesperrt und dann entsperrt sind, wird jeder Controller im Speicher-Array neu gestartet. Wenn sich jedoch bereits einige nicht freigeschaltete Laufwerke im Ziel-Speicher-Array befinden, werden die Controller nicht neu gestartet.

FAQs

Was muss ich vor der Erstellung eines Sicherheitsschlüssels wissen?

Ein Sicherheitsschlüssel wird von Controllern und sicheren Laufwerken innerhalb eines Storage-Arrays gemeinsam verwendet. Wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird, schützt der Sicherheitsschlüssel die Daten vor unberechtigtem Zugriff.

Sie können Sicherheitsschlüssel mit einer der folgenden Methoden erstellen und verwalten:

- Internes Verschlüsselungsmanagement auf dem persistenten Speicher des Controllers.
- Externes Verschlüsselungskeymanagement auf einem externen Verschlüsselungsmanagement-Server.

Bevor Sie einen internen Sicherheitsschlüssel erstellen, müssen Sie Folgendes tun:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.

Sie können dann einen internen Sicherheitsschlüssel erstellen, der die Definition einer Kennung und einer

Passphrase beinhaltet. Die Kennung ist eine Zeichenfolge, die dem Sicherheitsschlüssel zugeordnet ist und auf dem Controller und allen Laufwerken gespeichert ist, die mit dem Schlüssel verknüpft sind. Der Passphrase wird verwendet, um den Sicherheitsschlüssel für Sicherungszwecke zu verschlüsseln. Wenn Sie fertig sind, wird der Sicherheitsschlüssel auf dem Controller an einem nicht zugänglichen Ort gespeichert. Anschließend können sichere Volume-Gruppen und -Pools erstellt oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktiviert werden.

Bevor Sie einen externen Sicherheitsschlüssel erstellen, müssen Sie Folgendes tun:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.
3. Füllen Sie eine Client Certificate Signing Request (CSR) für die Authentifizierung zwischen dem Speicher-Array und dem Schlüsselverwaltungsserver aus, und laden Sie sie herunter. Wechseln Sie zum Menü:Einstellungen[Zertifikate > Schlüsselverwaltung > CSR abschließen].
4. Erstellen und laden Sie mithilfe der heruntergeladenen CSR-Datei ein Client-Zertifikat vom Schlüsselverwaltungsserver herunter.
5. Stellen Sie sicher, dass das Clientzertifikat und eine Kopie des Zertifikats für den Schlüsselverwaltungsserver auf Ihrem lokalen Host verfügbar sind.

Anschließend können Sie einen externen Schlüssel erstellen, der die IP-Adresse des Verschlüsselungsmanagement-Servers und die für die KMIP Kommunikation verwendete Port-Nummer umfasst. Während dieses Prozesses laden Sie auch Zertifikatdateien. Nach Abschluss des Vorgangs stellt das System eine Verbindung zum Schlüsselverwaltungsserver mit den von Ihnen eingegebenen Anmeldedaten her. Anschließend können sichere Volume-Gruppen und -Pools erstellt oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktiviert werden.

Warum muss ich eine Passphrase definieren?

Der Passphrase wird verwendet, um die auf dem lokalen Management-Client gespeicherte Sicherheitsschlüsseldatei zu verschlüsseln und zu entschlüsseln. Ohne den Passphrase kann der Sicherheitsschlüssel nicht entschlüsselt und verwendet werden, um Daten von einem sicheren Laufwerk zu entsperren, wenn er in einem anderen Speicher-Array neu installiert wird.

Warum sind Sicherheitsinformationen wichtig?

Wenn Sie die Informationen über die Sicherheitsschlüssel verlieren und kein Backup haben, können Sie Daten verlieren, wenn Sie sichere Laufwerke verschieben oder ein Controller-Upgrade durchführen. Sie benötigen einen Sicherheitsschlüssel, um die Daten auf den Laufwerken zu entsperren.

Achten Sie darauf, die Sicherheitsschlüsselkennung, den zugehörigen Passphrase und den Speicherort auf dem lokalen Host, auf dem die Sicherheitsschlüsseldatei gespeichert wurde, zu notieren.

Was muss ich vor dem Sichern eines Sicherheitsschlüssels beachten?

Wenn Ihr ursprünglicher Sicherheitsschlüssel beschädigt wird und Sie kein Backup

haben, verlieren Sie den Zugriff auf die Daten auf den Laufwerken, wenn sie von einem Speicher-Array zu einem anderen migriert werden.

Vor dem Sichern eines Sicherheitsschlüssels sollten Sie folgende Richtlinien beachten:

- Stellen Sie sicher, dass Sie die Kennung des Sicherheitsschlüssels kennen und den Satz der ursprünglichen Schlüsseldatei übergeben.

> Nur interne Schlüssel verwenden Kennungen. Beim Erstellen der Kennung wurden automatisch zusätzliche Zeichen generiert und an beide Enden der Identifikationszeichenfolge angehängt. Die generierten Zeichen stellen sicher, dass die Kennung eindeutig ist.

- Sie erstellen einen neuen Passphrase für das Backup. Diese Passphrase muss nicht mit der Passphrase übereinstimmen, die bei der Erstellung des ursprünglichen Schlüssels oder der letzten Änderung verwendet wurde. Der Passphrase wird nur auf das Backup angewendet, das Sie erstellen.

> Der Passphrase für die Laufwerksicherheit sollte nicht mit dem Administratorkennwort des Speicherarrays verwechselt werden. Der Passphrase für die Laufwerksicherheit schützt Backups eines Sicherheitsschlüssels. Das Administratorpasswort schützt das gesamte Speicherarray vor unberechtigtem Zugriff.

- Die Backup-Sicherheitsschlüsseldatei wird auf den Management-Client heruntergeladen. Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab. Stellen Sie sicher, dass Sie den Speicherort Ihrer Sicherheitsschlüssel-Informationen notieren.

Was muss ich wissen, bevor sichere Laufwerke entsperrt werden?

Um die Daten von einem sicheren Laufwerk zu entsperren, das in ein neues Speicher-Array migriert wird, müssen Sie dessen Sicherheitsschlüssel importieren.

Beachten Sie vor dem Entsperren von sicheren Laufwerken die folgenden Richtlinien:

- Das Ziel-Storage-Array (in dem Sie die Laufwerke verschieben) muss bereits über einen Sicherheitsschlüssel verfügen. Die migrierten Laufwerke werden erneut auf das Ziel-Storage-Array übertragen.
- Bei den zu migrierenden Laufwerken kennen Sie die Security Key Identifier und den Passphrase, der der Sicherheitsschlüsseldatei entspricht.
- Die Sicherheitsschlüsseldatei steht auf dem Management-Client zur Verfügung (das System mit einem Browser, der zum Zugriff auf System Manager verwendet wird).

Zugriff auf Lese-/Schreibzugriffe

Das Fenster **Drive Settings** enthält Informationen über die Attribute **Drive Security**. „Read/Write Accessible“ ist eines der Attribute, das anzeigt, ob Daten eines Laufwerks gesperrt wurden.

Um **Drive Security** -Attribute anzuzeigen, gehen Sie zur Seite Hardware. Wählen Sie ein Laufwerk aus, klicken Sie auf **Einstellungen anzeigen** und dann auf **Weitere Einstellungen anzeigen**. Unten auf der Seite ist der Wert für das Attribut Lesen/Schreiben, auf das zugegriffen werden kann, **Ja**, wenn das Laufwerk entsperrt ist. Der Wert für das Attribut Read/Write, das auf die Zugriffsberechtigung zugegriffen werden kann,

lautet **Nein, ungültiger Sicherheitsschlüssel**, wenn das Laufwerk gesperrt ist. Sie können ein sicheres Laufwerk entsperren, indem Sie einen Sicherheitsschlüssel importieren (gehen Sie zu Menü:Einstellungen[System > Sichere Laufwerke entsperren]).

Was muss ich über die Validierung des Sicherheitsschlüssels wissen?

Nachdem Sie einen Sicherheitsschlüssel erstellt haben, sollten Sie die Schlüsseldatei überprüfen, um sicherzustellen, dass sie nicht beschädigt ist.

Wenn die Validierung fehlschlägt, gehen Sie wie folgt vor:

- Wenn die Sicherheitsschlüsselkennung nicht mit der Kennung auf dem Controller übereinstimmt, suchen Sie die richtige Sicherheitsschlüsseldatei, und versuchen Sie die Validierung erneut.
- Wenn der Controller den Sicherheitsschlüssel nicht zur Validierung entschlüsseln kann, haben Sie möglicherweise den Passphrase falsch eingegeben. Überprüfen Sie den Passphrase, geben Sie ihn ggf. erneut ein, und versuchen Sie dann erneut die Validierung. Wenn die Fehlermeldung erneut angezeigt wird, wählen Sie eine Sicherungskopie der Schlüsseldatei (falls verfügbar) aus, und versuchen Sie die Validierung erneut.
- Wenn Sie den Sicherheitsschlüssel immer noch nicht validieren können, ist die Originaldatei möglicherweise beschädigt. Erstellen Sie ein neues Backup des Schlüssels und validieren Sie diese Kopie.

Worin besteht der Unterschied zwischen internem Sicherheitsschlüssel und externem Sicherheitsschlüsselmanagement?

Wenn Sie die * Drive Security*-Funktion implementieren, können Sie einen internen Sicherheitsschlüssel oder einen externen Sicherheitsschlüssel verwenden, um Daten zu sperren, wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird.

Ein Sicherheitsschlüssel ist eine Zeichenkette, die von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Interne Schlüssel befinden sich im persistenten Speicher des Controllers. Externe Schlüssel werden mithilfe eines Key Management Interoperability Protocol (KMIP) auf einem separaten Verschlüsselungsmanagement-Server aufbewahrt.