Management von Sicherheitsschlüsseln

SANtricity 11.8

NetApp
April 05, 2024

Inhalt

Management von Sicherheitsschlüsseln

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 zugreifen können.

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 einen Sicherheitsschlüssel-Identifier** — (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.

   - **Passphrase definieren/Passphrase erneut eingeben** — 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).
4. Wenn Sie bei externen Sicherheitsschlüsseln den alten Sicherheitsschlüssel löschen möchten, wenn der neue Schlüssel erstellt wird, aktivieren Sie unten im Dialogfeld das Kontrollkästchen „aktuellen Sicherheitsschlüssel löschen…“.

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

5. 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.

6. 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.

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.

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:
   - **Key Management Server-Adresse** — Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein, der für die Schlüsselverwaltung verwendet wird.
   - **Nummer des Key Management-Ports** — Geben Sie die Portnummer ein, die für die Kommunikation mit dem Key Management Interoperability Protocol (KMIP) verwendet wird.

     Optional: Sie können einen anderen Schlüsselserver hinzufügen, indem Sie auf **Schlüsselserver hinzufügen** klicken.
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.

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)

> **Bitte notieren Sie Ihren Eintrag für den späteren Gebrauch**. 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.

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 bei Nutzung des internen Verschlüsselungsmanagements

Wenn Sie das interne Verschlüsselungsmanagement konfiguriert haben und später sichere Laufwerke von einem Speicher-Array auf ein anderes verschieben, müssen Sie den Sicherheitsschlüssel dem neuen Speicher-Array neu zuweisen, um Zugriff auf die verschlüsselten Daten auf den Laufwerken zu erhalten.

Bevor Sie beginnen

- Auf dem Quell-Array (dem Array, in dem Sie die Laufwerke entfernen) haben Sie Volume-Gruppen exportiert und die Laufwerke entfernt. Auf dem Ziel-Array haben Sie die Laufwerke neu installiert.

  > Die Funktion „Exportieren/Importieren“ wird in der Benutzeroberfläche von System Manager nicht unterstützt. Sie müssen die Befehlszeilenschnittstelle (CLI) verwenden, um eine Volume-Gruppe in ein anderes Storage-Array zu exportieren bzw. zu importieren.

  Detaillierte Anweisungen für die Migration einer Volume-Gruppe finden Sie in "NetApp Knowledge Base". Befolgen Sie die entsprechenden Anweisungen für neuere Arrays, die von System Manager oder für ältere Systeme gemanagt werden.

- 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.
- 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

Wenn Sie die interne Schlüsselverwaltung verwenden, wird der Sicherheitsschlüssel lokal auf dem Speicher-Array gespeichert. Ein Sicherheitsschlüssel ist eine Zeichenkette, die vom Controller und den Laufwerken für Lese-/Schreibzugriff freigegeben wird. Wenn die Laufwerke physisch aus dem Array entfernt und in einem anderen installiert werden, können sie erst betrieben werden, wenn Sie den richtigen Sicherheitsschlüssel angeben.

> Sie können entweder einen internen Schlüssel aus dem persistenten Speicher des Controllers oder einen externen Schlüssel von einem Schlüsselmanagementserver erstellen. In diesem Thema wird das Entsperren von Daten beschrieben, wenn das *interne* Verschlüsselungsmanagement verwendet wird. Wenn Sie *External* Key Management verwendet haben, lesen Sie "Entsperren von Laufwerken bei Verwendung von externer Schlüsselverwaltung". Wenn Sie ein Controller-Upgrade durchführen und alle Controller gegen die neueste Hardware austauschen, müssen Sie die verschiedenen Schritte ausführen, wie im E-Series und SANtricity Dokumentationszentrum in beschrieben "Entsperren von Laufwerken".

Nach der Neuinstallation von Secure-Enabled-Laufwerken in einem anderen Array erkennt das Array die Laufwerke und zeigt den Zustand „Need Attention“ sowie den Status „Security Key needed“ an. Um die Laufwerkdaten zu entsperren, wählen Sie die Sicherheitsschlüsseldatei aus und geben den Passphrase für den Schlüssel ein. (Dieser 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. **Optional:** bewegen Sie die Maus über eine Laufwerksnummer, um die Position des Laufwerks zu sehen (Regalnummer und Einschubnummer).
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.

Nachdem Sie fertig sind

Auf dem Ziel-Array (dem Array mit den neu installierten Laufwerken) können Sie nun Volume-Gruppen importieren.

> Die Funktion „Exportieren/Importieren“ wird in der Benutzeroberfläche von System Manager nicht unterstützt. Sie müssen die Befehlszeilenschnittstelle (CLI) verwenden, um eine Volume-Gruppe in ein anderes Storage-Array zu exportieren bzw. zu importieren.

Detaillierte Anweisungen für die Migration einer Volume-Gruppe finden Sie in "NetApp Knowledge Base".

Entsperren von Laufwerken bei Verwendung von externer Schlüsselverwaltung

Wenn Sie die externe Schlüsselverwaltung konfiguriert haben und später sichere Laufwerke von einem Speicher-Array auf ein anderes verschieben, müssen Sie den Sicherheitsschlüssel dem neuen Speicher-Array neu zuweisen, um Zugriff auf die

verschlüsselten Daten auf den Laufwerken zu erhalten.

Bevor Sie beginnen

- Auf dem Quell-Array (dem Array, in dem Sie die Laufwerke entfernen) haben Sie Volume-Gruppen exportiert und die Laufwerke entfernt. Auf dem Ziel-Array haben Sie die Laufwerke neu installiert.

  > Die Funktion „Exportieren/Importieren“ wird in der Benutzeroberfläche von System Manager nicht unterstützt. Sie müssen die Befehlszeilenschnittstelle (CLI) verwenden, um eine Volume-Gruppe in ein anderes Storage-Array zu exportieren bzw. zu importieren.

  Detaillierte Anweisungen für die Migration einer Volume-Gruppe finden Sie in "NetApp Knowledge Base". Befolgen Sie die entsprechenden Anweisungen für neuere Arrays, die von System Manager oder für ältere Systeme gemanagt werden.

- 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.
- Sie müssen die IP-Adresse und die Port-Nummer des Verschlüsselungsmanagementservers kennen.
- Sie haben eine signierte Client-Zertifikatdatei für die Controller des Speicher-Arrays und haben diese Datei auf den Host kopiert, auf dem 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.

Über diese Aufgabe

Wenn Sie die externe Schlüsselverwaltung verwenden, wird der Sicherheitsschlüssel extern auf einem Server gespeichert, der zum sicheren Schutz von Sicherheitsschlüsseln entwickelt wurde. Ein Sicherheitsschlüssel ist eine Zeichenkette, die vom Controller und den Laufwerken für Lese-/Schreibzugriff freigegeben wird. Wenn die Laufwerke physisch aus dem Array entfernt und in einem anderen installiert werden, können sie erst betrieben werden, wenn Sie den richtigen Sicherheitsschlüssel angeben.

> Sie können entweder einen internen Schlüssel aus dem persistenten Speicher des Controllers oder einen externen Schlüssel von einem Schlüsselmanagementserver erstellen. In diesem Thema wird das Entsperren von Daten beschrieben, wenn *External* Verschlüsselungsmanagement verwendet wird. Wenn Sie _interne Schlüsselverwaltung verwendet haben, lesen Sie "Entsperren Sie Laufwerke bei Nutzung des internen Verschlüsselungsmanagements". Wenn Sie ein Controller-Upgrade durchführen und alle Controller gegen die neueste Hardware austauschen, müssen Sie die verschiedenen Schritte ausführen, wie im E-Series und SANtricity Dokumentationszentrum in beschrieben "Entsperren von Laufwerken".

Nach der Neuinstallation von Secure-Enabled-Laufwerken in einem anderen Array erkennt das Array die Laufwerke und zeigt den Zustand „Need Attention“ sowie den Status „Security Key needed“ an. Um die Laufwerkdaten zu entsperren, importieren Sie die Sicherheitsschlüsseldatei und geben den Passphrase für

den Schlüssel ein. (Dieser Passphrase entspricht nicht dem Administratorkennwort des Speicherarrays.) Während dieses Prozesses konfigurieren Sie das Speicher-Array so, dass ein externer Schlüsselverwaltungsserver verwendet wird, und der sichere Schlüssel kann dann aufgerufen werden. Sie müssen die Kontaktinformationen des Servers angeben, damit das Speicherarray eine Verbindung herstellen und den Sicherheitsschlüssel abrufen kann.

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* die Option **External Key erstellen** aus.
3. Schließen Sie den Assistenten mit den erforderlichen Verbindungsinformationen und Zertifikaten ab.
4. Klicken Sie auf **Kommunikation testen**, um den Zugriff auf den externen Schlüsselverwaltungsserver zu gewährleisten.
5. Wählen Sie * Sichere Laufwerke Entsperren*.

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

6. **Optional:** bewegen Sie die Maus über eine Laufwerksnummer, um die Position des Laufwerks zu sehen (Regalnummer und Einschubnummer).
7. 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.

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

   Die eingegebenen Zeichen sind maskiert.

9. 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.

Nachdem Sie fertig sind

Auf dem Ziel-Array (dem Array mit den neu installierten Laufwerken) können Sie nun Volume-Gruppen importieren.

> Die Funktion „Exportieren/Importieren“ wird in der Benutzeroberfläche von System Manager nicht unterstützt. Sie müssen die Befehlszeilenschnittstelle (CLI) verwenden, um eine Volume-Gruppe in ein anderes Storage-Array zu exportieren bzw. zu importieren.

Detaillierte Anweisungen für die Migration einer Volume-Gruppe finden Sie in "NetApp Knowledge Base".