Konfigurieren Sie die Sicherheitsschlüssel

SANtricity 11.7

NetApp
February 12, 2024

Inhalt

Konfigurieren Sie die Sicherheitsschlüssel

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:

   - **Einen Sicherheitsschlüssel-Identifier definieren** — Sie können entweder den Standardwert akzeptieren (Speicherarray-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).

Beachten Sie, 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**.

Ergebnisse

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.

- 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

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.
   - **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 KMIP-Kommunikation verwendet wird. Die am häufigsten für die Kommunikation mit dem Verschlüsselungsmanagement-Server verwendete Portnummer ist 5696.

     Optional: Wenn Sie einen Backup Key Server konfigurieren möchten, klicken Sie auf **Add Key Server** und geben Sie dann die Informationen dieses Servers ein. Der zweite Schlüsselserver wird verwendet, wenn der primäre Schlüsselserver nicht erreicht werden kann. Stellen Sie sicher, dass jeder Schlüsselserver Zugriff auf dieselbe Schlüsseldatenbank hat. Andernfalls wird das Array Fehler senden und kann den Backup-Server nicht verwenden.

> Es wird immer nur ein einziger Schlüsselserver verwendet. Wenn das Speicher-Array den primären Schlüsselserver nicht erreichen kann, kontaktiert das Array den Backup-Schlüsselserver. Beachten Sie, dass die Parität zwischen beiden Servern beibehalten werden muss. Andernfalls kann es zu Fehlern kommen.

   - **Client-Zertifikat auswählen** — Klicken Sie auf die erste **Durchsuchen**-Schaltfläche, um die Zertifikatdatei für die Speicher-Array-Controller auszuwählen.

- **Wählen Sie das Serverzertifikat des Schlüsselverwaltungsservers** — Klicken Sie auf die zweite Schaltfläche **Durchsuchen**, um die Zertifikatdatei für den Schlüsselverwaltungsserver auszuwählen. Sie können für den Schlüsselverwaltungsserver ein Stammzertifikat, ein Zwischenzertifikat oder ein Serverzertifikat auswählen.

4. Klicken Sie Auf **Weiter**.
5. Unter **Create/Backup Key** können Sie einen Sicherungsschlüssel für Sicherheitszwecke erstellen.

   - (Empfohlen) um einen Sicherungsschlüssel zu erstellen, lassen Sie das Kontrollkästchen aktiviert, und geben Sie dann einen Passphrase ein und bestätigen Sie ihn. 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).

   Beachten Sie, 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.

   +

   - Wenn Sie keinen Sicherungsschlüssel erstellen möchten, deaktivieren Sie das Kontrollkästchen.

   Beachten Sie, dass bei einem Verlust des Zugriffs auf den externen Schlüsselserver und ohne Backup-Schlüssel der Zugriff auf die Daten auf den Laufwerken verloren geht, wenn sie zu einem anderen Storage-Array migriert werden. Diese Option ist die einzige Methode zum Erstellen eines Sicherungsschlüssels in System Manager.

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.