Konfigurieren Sie selbstverschlüsselnde Festplatten (SEDs)

Veröffentlicht: 2025-03-28

In diesem Handbuch wird erklärt, wie Sie selbstverschlüsselnde Festplatten (SEDs) in den folgenden unterstützten Appliances konfigurieren:

- VON 10300
- SEIT 9300
- SEIT 8320
- BETA 9350
- EXA 5300
- Intrusion Detection System 9230

SEDs verschlüsseln kontinuierlich Daten, die auf das Laufwerk geschrieben werden. Die Art der Verschlüsselung ist hardwareabhängig und wird mit FIPS 140-2 oder 140-3 validiert. Daten auf diesen Laufwerken werden geschützt, indem vor dem Abrufen der Daten ein Schlüssel zum Entsperren der verschlüsselten Laufwerke erforderlich ist. Die Laufwerke sind nur dann vor Diebstahl geschützt, wenn die Festplatten gesichert sind.

Sie können die Sicherheit für virtuelle Laufwerke auf SEDs entweder bei oder nach der Erstellung der virtuellen Festplatte konfigurieren. Sichere virtuelle Festplatten können nicht entsichert werden, ohne dass alle Daten auf dem Laufwerk gelöscht werden.

Es gibt zwei Optionen, um Sicherheit und Verschlüsselung auf installierten Laufwerken zu aktivieren:

Lokales Schlüsselmanagement (LKM)

Aktivieren Sie die Sicherheit über den PowerEdge RAID Controller (PERC) und konfigurieren Sie einen Sicherheitsschlüssel und eine Passphrase, die lokal auf dem Controller gespeichert werden. Diese Methode schützt Daten im Ereignis eines Diebstahls eines physischen Laufwerks, jedoch nicht im Falle eines gesamten Systemdiebstahls. Weitere Informationen zur Konfiguration von LKM finden Sie unter Sicherheitsschlüssel und RAID-Management.

Sicheres Unternehmensschlüsselmanagement (SEKM)

Verwalten Sie Schlüssel über einen Schlüsselverwaltungsdienst und aktivieren Sie die Sicherheit auf installierten Laufwerken vom iDRAC9 aus. Da die Schlüssel extern in einem Schlüsselverwaltungsdienst gespeichert werden, sind die Daten auf diesen Laufwerken im Ereignis eines Systemdiebstahls geschützt. Weitere Informationen zur Konfiguration von SEKM finden Sie im Abschnitt „PowerEdge RAID Controller (PERC)“ in der SEKM-Konfigurations- und Bereitstellungsleitfaden.

Nachdem Sie entweder LKM oder SEKM aktiviert haben, müssen Sie Ihre vorhandenen virtuellen Laufwerke verschlüsseln.

LKM auf dem RAID-Controller über die iDRAC-Weboberfläche konfigurieren

Wenn Sie das System lieber mit Local Key Management (LKM) sichern möchten, können Sie die Sicherheit über den RAID-Controller aktivieren.

1. Starten Sie iDRAC von einem beliebigen unterstützten Browser aus.
2. Klicken Sie in der iDRAC-Weboberfläche auf **Aufbewahrung**, und klicken Sie dann auf **Überblick**.
3. klicken **Steuerungen**.
4. In der Steuerungen Abschnitt, klicken **Bearbeiten** aus der Aktionsliste neben dem Controller, den Sie konfigurieren möchten.

Hinweis: Es gibt zwei Controller: einen für die internen Festplatten, auf denen Firmware und Konfiguration gespeichert werden, und einen für Extended Storage Units (ESUs), die Pakete speichern.

5. In der Controller-Eigenschaften Abschnitt, klicken **Sicherheit**.
6. Aus dem **Sicherheit (Verschlüsselung)** auflisten, klicken **Sicherheitsschlüssel erstellen**.
7. Klicken Sie **Weiter**.
8. Für die **Sicherheitsschlüssel-ID**, geben Sie die Schlüssel-ID ein, die zum Sichern virtueller Laufwerke erforderlich ist.
9. Für die **Passphrase für Sicherheitsschlüssel**, geben Sie das Passwort ein, das zum Sichern der virtuellen Laufwerke erforderlich ist.

   Hinweis: Bei der Passphrase wird zwischen Groß- und Kleinschreibung unterschieden. Die Mindestlänge beträgt 8 Zeichen und die Höchstlänge 32 Zeichen. Stellen Sie sicher, dass die Zeichen mindestens eine Zahl, einen Kleinbuchstaben, einen Großbuchstaben und ein nichtalphanumerisches Zeichen enthalten.
10. Für die **Bestätigen Sie die Passphrase des Sicherheitsschlüssels**, geben Sie das Passwort erneut ein.
11. klicken **Zu „Ausstehend“ hinzufügen**.

Nächste Schritte
Als Nächstes verschlüsseln Sie ein vorhandenes virtuelles Laufwerk.

SEKM für die Laufwerksverschlüsselung über die iDRAC-Weboberfläche konfigurieren

Bevor Sie beginnen
Bevor Sie Secure Enterprise Key Management (SEKM) konfigurieren, stellen Sie sicher, dass Sie Ihren externen Key Management Server (KMS) konfigurieren, der Schlüssel verwaltet, mit denen Speicherlaufwerke über iDRAC gesperrt und entsperrt werden können. Weitere Informationen finden Sie im speziellen Abschnitt für Ihr KMS in der SEKM-Konfigurations- und Bereitstellungsleitfaden.

Wenn Sie das System lieber mit SEKM sichern möchten, können Sie die Sicherheit vom RAID-Controller aus konfigurieren.

1. Starten Sie iDRAC von einem beliebigen unterstützten Browser aus.
2. Klicken Sie in der iDRAC-Weboberfläche auf **Aufbewahrung**, und klicken Sie dann auf **Überblick**.
3. Klicken Sie **Steuerungen**.
4. In der Steuerungen Abschnitt, klicken Sie **Bearbeiten**aus der Aktionsliste neben dem Controller, den Sie konfigurieren möchten.

   Hinweis: Es gibt zwei Controller: einen für die internen Festplatten, auf denen Firmware und Konfiguration gespeichert sind, und einen für Extended Storage Units (ESU), die Pakete speichern.
5. In der Controller-Eigenschaften Abschnitt, klicken Sie **Sicherheit**.
6. Aus dem **Sicherheit (Verschlüsselung)** auflisten, klicken **Sicherer Enterprise Key Manager**.
7. Klicken Sie **Zu ausstehend hinzufügen**.
8. Klicken Sie **Beim nächsten Neustart**.

   Es wird eine Meldung angezeigt, die darauf hinweist, dass die Job-ID erstellt wurde.
9. Gehe zum **Auftragswarteschlange** Seite und stellen Sie sicher, dass diese Job-ID markiert ist als **Geplant**.
10. Starten Sie den Server neu, um den Konfigurationsjob auszuführen.
11. Gehe zum **Auftragswarteschlange** Seite, um den geplanten Job anzuzeigen.

Nach dem Neustart des Server wird der Konfigurationsjob in der Automated Task Application ausgeführt, um SEKM auf dem PERC zu aktivieren. Der Server wird automatisch neu gestartet.

Nächste Schritte
Als Nächstes ein vorhandenes virtuelles Laufwerk verschlüsseln.

Verschlüsseln Sie ein virtuelles Laufwerk

Sie können die Sicherheit für virtuelle Laufwerke auf vorhandenen SEDs konfigurieren. Sichere virtuelle Festplatten können nicht ungesichert werden, ohne dass alle Daten auf dem Laufwerk gelöscht werden.

1. Starten Sie iDRAC von einem beliebigen unterstützten Browser aus.
2. Klicken Sie in der iDRAC-Weboberfläche auf **Aufbewahrung**, und klicken Sie dann auf **Überblick**.
3. klicken **Virtuelle Festplatten**.
4. klicken **Virtuelles Laufwerk verschlüsseln** aus der Liste Aktionen für das virtuelle Laufwerk, das verschlüsselt werden soll.
5. klicken **Zu „Ausstehend“ hinzufügen**.
6. klicken **Bewerben Sie sich jetzt**.