Onboard-Schlüsselverwaltung konfigurieren

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/encryption-at-rest/enable-onboard-key-management-96-later-nse-task.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

Onboard-Schlüsselverwaltung konfigurieren 1
Integrierte Schlüsselverwaltung in ONTAP 9.6 und höher aktivieren 1
Integrierte Schlüsselverwaltung in ONTAP 9.5 und früher aktivieren 3
Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder ONTAP SED 5

Onboard-Schlüsselverwaltung konfigurieren

Integrierte Schlüsselverwaltung in ONTAP 9.6 und höher aktivieren

Mit dem Onboard Key Manager können Clusterknoten gegenüber einem FIPS-Laufwerk oder SED authentifiziert werden. Der Onboard Key Manager ist ein integriertes Tool, das Authentifizierungsschlüssel für Knoten aus demselben Speichersystem bereitstellt wie Ihre Daten. Der Onboard Key Manager ist FIPS-140-2 Level 1-konform.

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Der Onboard Key Manager muss auf jedem Cluster aktiviert sein, der auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

Sie müssen den `security key-manager onboard enable` Befehl jedes Mal ausführen, wenn Sie dem Cluster einen Knoten hinzufügen. In MetroCluster Konfigurationen müssen Sie `security key-manager onboard enable` zuerst auf dem lokalen Cluster und anschließend `security key-manager onboard sync` auf dem Remote-Cluster ausführen, wobei jeweils dieselbe Passphrase verwendet werden muss.

Weitere Informationen zu `security key-manager onboard enable` und `security key-manager onboard sync` finden sich in der "ONTAP-Befehlsreferenz".

Standardmäßig ist die Eingabe der Passphrase für den Schlüsselmanager beim Neustart eines Knotens nicht erforderlich. Außer bei MetroCluster kann die `cc-mode-enabled=yes` Option verwendet werden, um zu verlangen, dass Benutzer die Passphrase nach einem Neustart eingeben.

Wenn der Onboard Key Manager im Common Criteria-Modus aktiviert ist (`cc-mode-enabled=yes`, ändert sich das Systemverhalten wie folgt:

- Das System überwacht im Common Criteria-Modus aufeinanderfolgende fehlgeschlagene Cluster-Passphrasenversuche.

  Wenn NetApp Storage Encryption (NSE) aktiviert ist und die korrekte Cluster-Passphrase beim Systemstart nicht eingegeben wird, kann sich das System nicht an seinen Laufwerken authentifizieren und startet automatisch neu. Um dies zu korrigieren, ist die korrekte Cluster-Passphrase an der Boot-Eingabeaufforderung einzugeben. Nach dem Start erlaubt das System innerhalb eines Zeitraums von 24 Stunden bis zu 5 aufeinanderfolgende Versuche, die Cluster-Passphrase für jeden Befehl, der die Cluster-Passphrase als Parameter benötigt, korrekt einzugeben. Wird das Limit erreicht (zum Beispiel wenn die Cluster-Passphrase 5-mal hintereinander falsch eingegeben wurde), muss entweder das Ablaufintervall von 24 Stunden (Zeitüberschreitung) abgewartet oder der Node neu gestartet werden, um das Limit zurückzusetzen.

- Systemabbildaktualisierungen verwenden das NetApp RSA-3072-Codesignaturzertifikat zusammen mit SHA-384-codesignierten Digests zur Überprüfung der Abbildintegrität, anstelle des üblichen NetApp RSA-2048-Codesignaturzertifikats und SHA-256-codesignierten Digests.

  Der Upgrade-Befehl überprüft anhand verschiedener digitaler Signaturen, ob der Image-Inhalt verändert oder beschädigt wurde. Wenn die Validierung erfolgreich ist, geht das

Image-Update zum nächsten Schritt über. Wenn die Validierung nicht erfolgreich ist, schlägt das Image-Update fehl. Weitere Informationen zu `cluster image` finden sich in der "ONTAP-Befehlsreferenz".

Der integrierte Schlüsselmanager speichert Schlüssel im flüchtigen Speicher. Der Inhalt des flüchtigen Speichers wird beim Neustart oder Anhalten des Systems gelöscht. Unter normalen Betriebsbedingungen wird der Inhalt des flüchtigen Speichers innerhalb von 30 Sekunden nach dem Anhalten des Systems gelöscht.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen Schlüsselverwaltungsserver (KMIP) verwenden, muss die externe Schlüsselverwaltungsdatenbank gelöscht worden sein.

  "Umstellung vom externen auf das integrierte Schlüsselmanagement"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung muss konfiguriert werden, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Starten Sie den Befehl zum Einrichten des Schlüsselmanagers:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   Setzen Sie `cc-mode-enabled=yes` so, dass Benutzer nach einem Neustart die Passphrase des Schlüsselmanagers eingeben müssen. Die `- cc-mode-enabled` Option wird in MetroCluster Konfigurationen nicht unterstützt. Der `security key-manager onboard enable` Befehl ersetzt den `security key-manager setup` Befehl.

   Das folgende Beispiel startet den Befehl zur Einrichtung des Schlüsselmanagers auf cluster1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

2. Geben Sie eine Passphrase mit 32 bis 256 Zeichen ein oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

   Ist die angegebene Passphrase für den “cc-mode” kürzer als 64 Zeichen, tritt eine Verzögerung von fünf Sekunden auf, bevor die Passphrase-Aufforderung im Rahmen der Schlüsselmanager-Einrichtung erneut angezeigt wird.

3. Bei der Aufforderung zur Passphrase-Bestätigung wird die Passphrase erneut eingegeben.
4. Überprüfen, ob das System die Authentifizierungsschlüssel erstellt:

   ```
   security key-manager key query -node node
   ```

   Der `security key-manager key query` Befehl ersetzt den `security key-manager query key` Befehl.

   Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Die Passphrase sollte an einem sicheren Ort außerhalb des Speichersystems für die zukünftige Verwendung aufbewahrt werden.

Das System sichert wichtige Verwaltungsinformationen automatisch in der replizierten Datenbank (RDB) für den Cluster. Diese Informationen sollten für die Notfallwiederherstellung zusätzlich manuell gesichert werden.

Verwandte Informationen

- "Cluster Image-Befehle"
- "security key-manager external enable"
- "security key-manager key query"
- "security key-manager onboard enable"
- "Umstellung vom externen auf das integrierte Schlüsselmanagement"

Integrierte Schlüsselverwaltung in ONTAP 9.5 und früher aktivieren

Mit dem Onboard Key Manager können Clusterknoten gegenüber einem FIPS-Laufwerk oder SED authentifiziert werden. Der Onboard Key Manager ist ein integriertes Tool, das Authentifizierungsschlüssel für Knoten aus demselben Speichersystem bereitstellt wie Ihre Daten. Der Onboard Key Manager ist FIPS-140-2 Level 1-konform.

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Der Onboard Key Manager ist auf jedem Cluster zu aktivieren, der auf verschlüsselte Volumes oder selbstverschlüsselnde Datenträger zugreift.

Über diese Aufgabe

Sie müssen den `security key-manager setup` Befehl jedes Mal ausführen, wenn Sie dem Cluster einen Knoten hinzufügen.

Bei einer MetroCluster Konfiguration gelten folgende Richtlinien:

- In ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` auf dem Remote-Cluster ausgeführt werden, wobei auf beiden Clustern dieselbe Passphrase verwendet wird.
- Vor ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster ausgeführt werden, etwa 20 Sekunden gewartet werden und dann `security key-manager setup` auf dem Remote-Cluster ausgeführt werden, wobei jeweils die gleiche Passphrase verwendet wird.

Standardmäßig ist die Eingabe der Passphrase für den Schlüsselmanager beim Neustart eines Knotens nicht erforderlich. Ab ONTAP 9.4 kann die `-enable-cc-mode yes` Option verwendet werden, um zu verlangen, dass Benutzer die Passphrase nach einem Neustart eingeben.

Für NVE: Wenn `-enable-cc-mode yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt. Für `volume create` muss `-encrypt true` nicht angegeben werden. Für `volume move start` muss `-encrypt-destination true` nicht angegeben werden.

Nach einem fehlgeschlagenen Passphrase-Versuch ist ein erneuter Neustart des Knotens erforderlich.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen Schlüsselverwaltungsserver (KMIP) verwenden, löschen Sie die externe Schlüsselverwaltungsdatenbank.

  "Umstellung vom externen auf das integrierte Schlüsselmanagement"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung wird konfiguriert, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Die Einrichtung des Schlüsselmanagers wird gestartet:

   `security key-manager setup -enable-cc-mode yes|no`

   > Ab ONTAP 9.4 kann die `-enable-cc-mode yes` Option verwendet werden, um zu verlangen, dass Benutzer nach einem Neustart die Passphrase des Schlüsselmanagers eingeben. Für NVE: Wenn `-enable-cc-mode yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt.

   Das folgende Beispiel zeigt den Beginn der Einrichtung des Schlüsselmanagers auf Cluster1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. Geben Sie `yes` an der Eingabeaufforderung ein, um die integrierte Schlüsselverwaltung zu konfigurieren.
3. Bei der Aufforderung zur Eingabe der Passphrase ist eine Passphrase mit 32 bis 256 Zeichen einzugeben, oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

   > Ist die angegebene Passphrase für den “cc-mode” kürzer als 64 Zeichen, tritt eine Verzögerung von fünf Sekunden auf, bevor die Passphrase-Aufforderung im Rahmen der Schlüsselmanager-Einrichtung erneut angezeigt wird.

4. Bei der Aufforderung zur Passphrase-Bestätigung wird die Passphrase erneut eingegeben.
5. Überprüfen, ob die Schlüssel für alle Knoten konfiguriert sind:

   `security key-manager show-key-store`

Weitere Informationen zu `security key-manager show-key-store` finden sich in der "ONTAP-Befehlsreferenz".

```
cluster1::> security key-manager show-key-store

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

Nachdem Sie fertig sind

ONTAP sichert automatisch wichtige Verwaltungsinformationen in der replizierten Datenbank (RDB) für den Cluster.

Nachdem die Passphrase des Onboard Key Managers konfiguriert wurde, sollten die Informationen manuell an einem sicheren Ort außerhalb des Speichersystems gesichert werden. Siehe "Onboard-Schlüsselverwaltungsinformationen manuell sichern".

Verwandte Informationen

- "Onboard-Schlüsselverwaltungsinformationen manuell sichern"
- "security key-manager setup"
- "security key-manager show-key-store"
- "Umstellung vom externen auf das integrierte Schlüsselmanagement"

Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder ONTAP SED

Mit dem `storage encryption disk modify` Befehl lässt sich einem FIPS-Laufwerk oder SED ein Datenauthentifizierungsschlüssel zuweisen. Clusterknoten verwenden diesen Schlüssel, um auf die Daten auf dem Laufwerk zuzugreifen.

Über diese Aufgabe

Ein Self-Encrypting Drive ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert gesetzt ist. Die Hersteller Secure ID (MSID) mit der Schlüssel-ID 0x0 ist der Standardwert für SAS-Laufwerke. Für NVMe-Laufwerke ist der

Standardwert ein Nullschlüssel, dargestellt als leere Schlüssel-ID. Wird die Schlüssel-ID einem Self-Encrypting Drive zugewiesen, ändert das System dessen Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Einem FIPS-Laufwerk oder SED einen Authentifizierungsschlüssel für Daten zuweisen:

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   Weitere Informationen zu `storage encryption disk modify` finden sich in der "ONTAP-Befehlsreferenz".

   Mit dem `security key-manager key query -key-type NSE-AK` Befehl lassen sich die Schlüssel-IDs anzeigen.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

2. Überprüfen, ob die Authentifizierungsschlüssel zugewiesen wurden:

   `storage encryption disk show`

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   [...]
   ```

Verwandte Informationen

- "storage encryption Disk anzeigen"
- "storage encryption disk show-status"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.