Configure NetApp volume and aggregate encryption

ONTAP 9

NetApp
February 02, 2026

Table of Contents

Configure NetApp volume and aggregate encryption

Learn about ONTAP NetApp volume and aggregate encryption

NetApp Volume Encryption (NVE) is a software-based technology for encrypting data at rest one volume at a time. An encryption key accessible only to the storage system ensures that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen.

Understanding NVE

With NVE, both metadata and data (including snapshots) are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume. An external key management server or Onboard Key Manager (OKM) serves keys to nodes:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). It is a best practice to configure external key management servers on a different storage system from your data.
- The Onboard Key Manager is a built-in tool that serves keys to nodes from the same storage system as your data.

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager. The VE license is included with ONTAP One. Whenever an external or onboard key manager is configured there is a change in how the encryption of data at rest is configured for brand new aggregates and brand new volumes. Brand new aggregates will have NetApp Aggregate Encryption (NAE) enabled by default. Brand new volumes that are not part of an NAE aggregate will have NetApp Volume Encryption (NVE) enabled by default. If a data storage virtual machine (SVM) is configured with its own key-manager using multi-tenant key management, then the volume created for that SVM is automatically configured with NVE.

You can enable encryption on a new or existing volume. NVE supports the full range of storage efficiency features, including deduplication and compression. Beginning with ONTAP 9.14.1, you can enable NVE on existing SVM root volumes.

> If you are using SnapLock, you can enable encryption only on new, empty SnapLock volumes. You cannot enable encryption on an existing SnapLock volume.

You can use NVE on any type of aggregate (HDD, SSD, hybrid, array LUN), with any RAID type, and in any supported ONTAP implementation, including ONTAP Select. You can also use NVE with hardware-based encryption to “double encrypt” data on self-encrypting drives.

When NVE is enabled, the core dump is also encrypted.

Aggregate-level encryption

Ordinarily, every encrypted volume is assigned a unique key. When the volume is deleted, the key is deleted with it.

Beginning with ONTAP 9.6, you can use *NetApp Aggregate Encryption (NAE)* to assign keys to the containing aggregate for the volumes to be encrypted. When an encrypted volume is deleted, the keys for the aggregate are preserved. The keys are deleted if the entire aggregate is deleted.

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager.

NVE and NAE volumes can coexist on the same aggregate. Volumes encrypted under aggregate-level encryption are NAE volumes by default. You can override the default when you encrypt the volume.

You can use the `volume move` command to convert an NVE volume to an NAE volume, and vice versa. You can replicate an NAE volume to an NVE volume.

You cannot use `secure purge` commands on an NAE volume.

When to use external key management servers

Although it is less expensive and typically more convenient to use the onboard key manager, you should set up KMIP servers if any of the following are true:

- Your encryption key management solution must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
- You need a multi-cluster solution, with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location different from the data.

Scope of external key management

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a named SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.
  - Beginning with ONTAP 9.17.1, you can use Barbican KMS to protect NVE keys only for data SVMs.
  - Beginning with ONTAP 9.10.1, you can use Azure Key Vault and Google Cloud KMS to protect NVE keys only for data SVMs. This is available for AWS's KMS beginning in 9.12.0.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

A list of validated external key managers is available in the NetApp Interoperability Matrix Tool (IMT). You can find this list by entering the term "key managers" into the IMT's search feature.

Cloud KMS providers such as Azure Key Vault and AWS KMS do not support KMIP. As a result, they are not listed on IMT.

Support details

The following table shows NVE support details:

Resource or feature	Support details
Platforms	AES-NI offload capability required. See the Hardware Universe (HWU) to verify that NVE and NAE are supported for your platform.

Encryption	Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you add a volume encryption (VE) license and have an onboard or external key manager configured. If you need to create an unencrypted aggregate, use the following command:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	If you need to create a plain text volume, use the following command:
	
	`volume create -encrypt false`
	
	Encryption is not enabled by default when:
	
	• VE license is not installed.
	• Key manager is not configured.
	• Platform or software does not support encryption.
	• Hardware encryption is enabled.

ONTAP	All ONTAP implementations. Support for Cloud Volumes ONTAP is available in ONTAP 9.5 and later.
Devices	HDD, SSD, hybrid, array LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Data volumes and existing SVM root volumes. You cannot encrypt data on MetroCluster metadata volumes. In versions of ONTAP earlier than 9.14.1, you cannot encrypt data on the SVM root volume with NVE. Beginning with ONTAP 9.14.1, ONTAP supports NVE on SVM root volumes.

Aggregate-level encryption	Beginning with ONTAP 9.6, NVE supports aggregate-level encryption (NAE): • You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. • You cannot rekey an aggregate-level encryption volume. • Secure-purge is not supported on aggregate-level encryption volumes. • In addition to data volumes, NAE supports encryption of SVM root volumes and the MetroCluster metadata volume. NAE does not support encryption of the root volume.
SVM scope	MetroCluster is supported beginning with ONTAP 9.8. Beginning with ONTAP 9.6, NVE supports SVM scope for external key management only, not for Onboard Key Manager.
Storage efficiency	Deduplication, compression, compaction, FlexClone. Clones use the same key as the parent, even after splitting the clone from the parent. You should perform a `volume move` on a split clone, after which the split clone will have a different key.
Replication	• For volume replication, the source and destination volumes can have different encryption settings. Encryption can be configured for the source and unconfigured for the destination, and vice versa. Configured encryption on the source will not be replicated to the destination. Encryption must be configured manually on the source and destination. Refer to Configure NVE and Encrypt volume data with NVE. • For SVM replication, the destination volume is automatically encrypted, unless the destination does not contain a node that supports volume encryption, in which case replication succeeds, but the destination volume is not encrypted. • For MetroCluster configurations, each cluster pulls external key management keys from its configured key servers. OKM keys are replicated to the partner site by the configuration replication service.
Compliance	SnapLock is supported in both Compliance and Enterprise modes, for new volumes only. You cannot enable encryption on an existing SnapLock volume.
FlexGroup volumes	FlexGroup volumes are supported. Destination aggregates must be of the same type as source aggregates, either volume-level or aggregate-level. Beginning with ONTAP 9.5, in-place rekey of FlexGroup volumes is supported.
7-Mode transition	Beginning with 7-Mode Transition Tool 3.3, you can use the 7-Mode Transition Tool CLI to perform copy-based transition to NVE-enabled destination volumes on the clustered system.

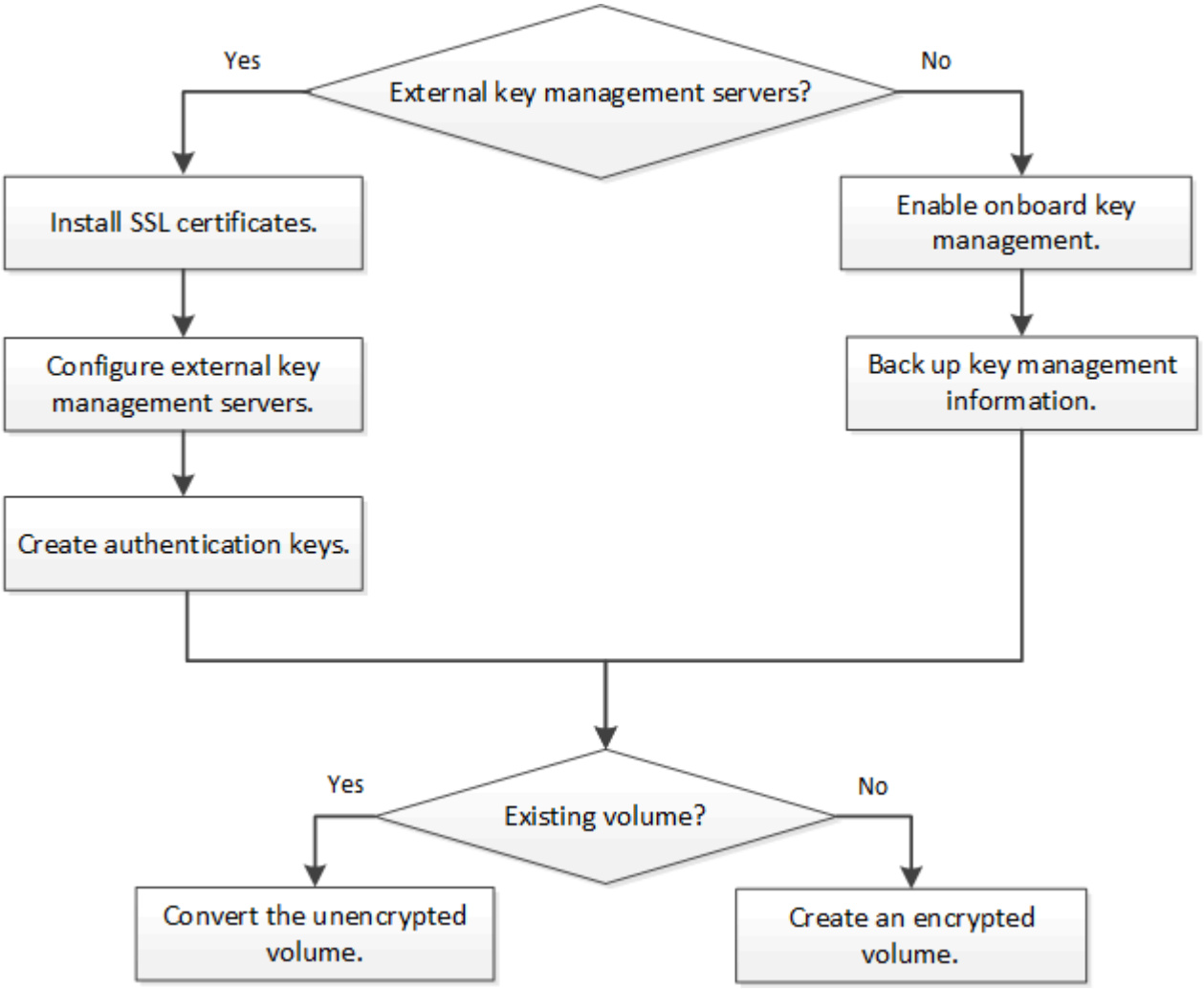
Related information

- FAQ - NetApp Volume Encryption and NetApp Aggregate Encryption

- storage aggregate create

ONTAP NetApp Volume Encryption workflow

You must configure key management services before you can enable volume encryption. You can enable encryption on a new volume or on an existing volume.



You must install the VE license and configure key management services before you can encrypt data with NVE. Before installing the license, you should determine whether your ONTAP version supports NVE.

Configure NVE

Determine whether your ONTAP cluster version supports NVE

You should determine whether your cluster version supports NVE before you install the license. You can use the `version` command to determine the cluster version.

About this task

The cluster version is the lowest version of ONTAP running on any node in the cluster.

Steps

1. Determine whether your cluster version supports NVE:

   ```
   version -v
   ```

   NVE is not supported if the command output displays the text `1Ono-DARE` (for "no Data At Rest Encryption"), or if you are using a platform that is not listed in Support details.

Install the volume encryption license on an ONTAP cluster

A VE license entitles you to use the feature on all nodes in the cluster. This license is required before you can encrypt data with NVE. It is included with ONTAP One.

Prior to ONTAP One, the VE license was included with the Encryption bundle. The Encryption bundle is no longer offered, but is still valid. Although not currently required, existing customers can choose to upgrade to ONTAP One.

Before you begin

- You must be a cluster administrator to perform this task.
- You must have received the VE license key from your sales representative or have ONTAP One installed.

Steps

1. Verify that the VE license is installed.

   The VE license package name is `VE`.

2. If the license is not installed, use System Manager or the ONTAP CLI to install it.

Configure external key management

Learn about configuring external key management with ONTAP NetApp Volume Encryption

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). In addition to the Onboard Key Manager, ONTAP supports several external key management servers.

Beginning with ONTAP 9.10.1, you can use Azure Key Vault or Google Cloud Key Manager Service to protect your NVE keys for data SVMs. Beginning with ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See Configure clustered key servers. Beginning with ONTAP 9.12.0, you can use AWS' KMS to protect your NVE keys for data SVMs. Beginning with ONTAP 9.17.1, you can use OpenStack's Barbican KMS to protect your NVE keys for data SVMs.

Manage external key managers with ONTAP System Manager

Beginning with ONTAP 9.7, you can store and manage authentication and encryption keys with the Onboard Key Manager. Beginning with ONTAP 9.13.1, you can also use external key managers to store and manage these keys.

The Onboard Key Manager stores and manages keys in a secure database that is internal to the cluster. Its

scope is the cluster. An external key manager stores and manages keys outside the cluster. Its scope can be the cluster or the storage VM. One or more external key managers can be used. The following conditions apply:

- If the Onboard Key Manager is enabled, an external key manager cannot be enabled at the cluster level, but it can be enabled at the storage VM level.
- If an external key manager is enabled at the cluster level, the Onboard Key Manager cannot be enabled.

When using external key managers, you can register up to four primary key servers per storage VM and cluster. Each primary key server can be clustered with up to three secondary key servers.

Configure an external key manager

To add an external key manager for a storage VM, you should add an optional gateway when you configure the network interface for the storage VM. If the storage VM was created without the network route, you will have to create the route explicitly for the external key manager. See Create a LIF (network interface).

Steps

You can configure an external key manager starting from different locations in System Manager.

1. To configure an external key manager, perform one of the following starting steps.

Workflow	Navigation	Starting step
Configure Key Manager	**Cluster** > **Settings**	Scroll to the **Security** section. Under **Encryption**, select . Select **External Key Manager**.
Add local tier	**Storage** > **Tiers**	Select **+ Add Local Tier**. Check the check box labeled "Configure Key Manager". Select **External Key Manager**.
Prepare storage	**Dashboard**	In the **Capacity** section, select **Prepare Storage**. Then, select "Configure Key Manager". Select **External Key Manager**.
Configure encryption (key manager at storage VM scope only)	**Storage** > **Storage VMs**	Select the storage VM. Select the **Settings** tab. In the **Encryption** section under **Security**, select .

2. To add a primary key server, select + Add , and complete the **IP Address or Host Name** and **Port** fields.
3. Existing installed certificates are listed in the **KMIP Server CA Certificates** and **KMIP Client Certificate** fields. You can perform any of the following actions:
   - Select to select installed certificates that you want to map to the key manager. (Multiple service CA certificates can be selected, but only one client certificate can be selected.)
   - Select **Add New Certificate** to add a certificate that has not already been installed and map it to the external key manager.
   - Select × next to the certificate name to delete installed certificates that you do not want to map to the external key manager.
4. To add a secondary key server, select **Add** in the **Secondary Key Servers** column, and provide its details.

5. Select **Save** to complete the configuration.

Edit an existing external key manager

If you have already configured an external key manager, you can modify its settings.

Steps

1. To edit the configuration of an external key manager, perform one of the following starting steps.

Scope	Navigation	Starting step
Cluster scope external key manager	**Cluster** > **Settings**	Scroll to the **Security** section. Under **Encryption**, select ⋮, then select **Edit External Key Manager**.
Storage VM scope external key manager	**Storage** > **Storage VMs**	Select the storage VM. Select the **Settings** tab. In the **Encryption** section under **Security**, select ⋮, then select **Edit External Key Manager**.

2. Existing key servers are listed in the **Key Servers** table. You can perform the following operations:
   - Add a new key server by selecting + Add .
   - Delete a key server by selecting ⋮ at the end of the table cell that contains the name of the key server. The secondary key servers associated with that primary key server are also removed from the configuration.

Delete an external key manager

An external key manager can be deleted if the volumes are unencrypted.

Steps

1. To delete an external key manager, perform one of the following steps.

Scope	Navigation	Starting step
Cluster scope external key manager	**Cluster** > **Settings**	Scroll to the **Security** section. Under **Encryption**, select select ⋮, then select **Delete External Key Manager**.
Storage VM scope external key manager	**Storage** > **Storage VMs**	Select the storage VM. Select the **Settings** tab. In the **Encryption** section under **Security**, select ⋮, then select **Delete External Key Manager**.

Migrate keys among key managers

When multiple key managers are enabled on a cluster, keys must be migrated from one key manager to another. This process is completed automatically with System Manager.

- If the Onboard Key Manager or an external key manager is enabled at a cluster level, and some volumes are encrypted, then when you configure an external key manager at the storage VM level, the keys must be migrated from the Onboard Key Manager or external key manager at the cluster level to the external key manager at the storage VM level. This process is completed automatically by System Manager.

- If volumes were created without encryption on a storage VM, then keys do not need to be migrated.

Install SSL certificates on the ONTAP cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

Before you begin

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.
- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.
- The SSL KMIP client certificate must not be password-protected.
- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.
- In a MetroCluster environment, you must install the same KMIP SSL certificates on both clusters.

You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

Steps

1. Install the SSL KMIP client certificates for the cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   You are prompted to enter the SSL KMIP public and private certificates.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Related information

- security certificate install

Enable external key management for NVE in ONTAP 9.6 and later

Use KMIP servers to secure the keys the cluster uses to access encrypted data. Beginning with ONTAP 9.6, you have the option to configure a separate external key manager to secure the keys that a data SVM uses to access encrypted data.

Beginning with ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see Configure clustered external key servers.

About this task

You can connect up to four KMIP servers to a cluster or SVM. Use at least two servers for redundancy and disaster recovery.

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a data SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.
- For multitenant environments, install a license for *MT_EK_MGMT* by using the following command:

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  Learn more about `system license add` in the ONTAP command reference.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

You can configure onboard key management at the cluster scope and external key management at the SVM scope. You can use the `security key-manager key migrate` command to migrate keys from onboard key management at the cluster scope to external key managers at the SVM scope.

Learn more about `security key-manager key migrate` in the ONTAP command reference.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- The KMIP server must be reachable from each node's node-management LIF.
- You must be a cluster or SVM administrator to perform this task.
- In a MetroCluster environment:
  - MetroCluster must be fully configured before enabling external key management.
  - You must install the same KMIP SSL certificate on both clusters.
  - An external key manager must be configured on both clusters.

Steps

1. Configure key manager connectivity for the cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

The `security key-manager external enable` command replaces the `security key-manager setup` command. If you run the command at the cluster login prompt, *`admin_SVM`* defaults to the admin SVM of the current cluster. You can run the `security key-manager external modify` command to change the external key management configuration.

The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Configure a key manager an SVM:

   `security key-manager external enable -vserver SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

   - If you run the command at the SVM login prompt, `SVM` defaults to the current SVM. You can run the `security key-manager external modify` command to change the external key management configuration.
   - In a MetroCluster environment, if you are configuring external key management for a data SVM, you do not have to repeat the `security key-manager external enable` command on the partner cluster.

   The following command enables external key management for `svm1` with a single key server listening on the default port 5696:

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Repeat the last step for any additional SVMs.

   You can also use the `security key-manager external add-servers` command to configure additional SVMs. The `security key-manager external add-servers` command replaces the `security key-manager add` command. Learn more about `security key-manager external add-servers` in the ONTAP command reference.

4. Verify that all configured KMIP servers are connected:

   `security key-manager external show-status -node node_name`

The `security key-manager external show-status` command replaces the `security key-manager show -status` command. Learn more about `security key-manager external show-status` in the ONTAP command reference.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ---------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                         available
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available
node2
      svm1
               keyserver.svm1.com:5696                         available
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available

8 entries were displayed.
```

5. Optionally, convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   An external key manager must be fully configured before you convert the volumes.

Related information

- Configure clustered external key servers
- system license add
- security key-manager key migrate
- security key-manager external add-servers
- security key-manager external show-status

Enable external key management for NVE in ONTAP 9.5 and earlier

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.
- In a MetroCluster environment, you must install the same KMIP SSL certificate on both clusters.

Steps

1. Configure key manager connectivity for cluster nodes:

   `security key-manager setup`

   The key manager setup starts.

   In a MetroCluster environment, you must run this command on both clusters. Learn more about `security key-manager setup` in the ONTAP command reference.

2. Enter the appropriate response at each prompt.
3. Add a KMIP server:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   In a MetroCluster environment, you must run this command on both clusters.

4. Add an additional KMIP server for redundancy:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   In a MetroCluster environment, you must run this command on both clusters.

5. Verify that all configured KMIP servers are connected:

   `security key-manager show -status`

   Learn more about the commands described in this procedure in the ONTAP command reference.

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

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. Optionally, convert plain text volumes to encrypted volumes.

   ```
   volume encryption conversion start
   ```

   An external key manager must be fully configured before you convert the volumes. In a MetroCluster environment, an external key manager must be configured on both sites.

Manage NVE keys for ONTAP data SVMs with a cloud provider

Beginning with ONTAP 9.10.1, you can use Azure Key Vault (AKV) and Google Cloud Platform's Key Management Service (Cloud KMS) to protect your ONTAP encryption keys in a cloud-hosted application. Beginning with ONTAP 9.12.0, you can also protect NVE keys with AWS' KMS.

AWS KMS, AKV and Cloud KMS can be used to protect NetApp Volume Encryption (NVE) keys only for data SVMs.

About this task

Key management with a cloud provider can be enabled with the CLI or the ONTAP REST API.

When using a cloud provider to protect your keys, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com for Azure; oauth2.googleapis.com for Cloud KMS). If the cluster network is not configured correctly, the cluster will not properly use the key management service.

When utilizing a cloud provider key management service, you should be aware of the following limitations:

- Cloud-provider key management is not available for NetApp Storage Encryption (NSE) and NetApp Aggregate Encryption (NAE). External KMIPs can be used instead.
- Cloud-provider key management is not available for MetroCluster configurations.
- Cloud-provider key management can only be configured on a data SVM.

Before you begin

- You must have configured the KMS on the appropriate cloud provider.
- The ONTAP cluster's nodes must support NVE.
- You must have installed the Volume Encryption (VE) and multi-tenant Encryption Key Management (MTEKM) licenses. These licenses are included with ONTAP One.

- You must be a cluster or SVM administrator.
- The data SVM must not include any encrypted volumes or employ a key manager. If the data SVM includes encrypted volumes, you must migrate them before configuring the KMS.

Enable external key management

Enabling external key management depends on the specific key manager you use. Choose the tab of the appropriate key manager and environment.

AWS

Before you begin

- You must create a grant for the AWS KMS key that will be used by the IAM role managing encryption. The IAM role must include a policy that allows the following operations:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`
    +
    For more information, see AWS documentation for grants.

Enable AWS KMV on an ONTAP SVM

1. Before you begin, obtain both the access key ID and secret key from your AWS KMS.
2. Set the privilege level to advanced:
   `set -priv advanced`
3. Enable AWS KMS:
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. When prompted, enter the secret key.
5. Confirm the AWS KMS was configured correctly:
   `security key-manager external aws show -vserver` *`svm_name`*

   Learn more about `security key-manager external aws` in the ONTAP command reference.

Azure

Enable Azure Key Vault on an ONTAP SVM

1. Before you begin, you need to obtain the appropriate authentication credentials from your Azure account, either a client secret or certificate.
   You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`. Learn more about `cluster show` in the ONTAP command reference.
2. Set privileged level to advanced
   `set -priv advanced`
3. Enable AKV on the SVM
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}`
   When prompted, enter either the client certificate or client secret from your Azure account.
4. Verify AKV is enabled correctly:
   `security key-manager external azure show vserver` *`svm_name`*
   If the service reachability is not OK, establish the connectivity to the AKV key management service via the data SVM LIF.

   Learn more about `security key-manager external azure` in the ONTAP command reference.

Google Cloud

Enable Cloud KMS on an ONTAP SVM

1. Before you begin, obtain the private key for the Google Cloud KMS account key file in a JSON format. This can be found in your GCP account.
   You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`. Learn more about `cluster show` in the ONTAP command reference.
2. Set privileged level to advanced:
   `set -priv advanced`
3. Enable Cloud KMS on the SVM
   `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
   When prompted, enter the contents of the JSON file with the Service Account Private Key
4. Verify that Cloud KMS is configured with the correct parameters:
   `security key-manager external gcp show vserver svm_name`
   The status of `kms_wrapped_key_status` will be `"UNKNOWN"` if no encrypted volumes have been created.
   If the service reachability is not OK, establish the connectivity to the GCP key management service via data SVM LIF.

   Learn more about `security key-manager external gcp` in the ONTAP command reference.

If one or more encrypted volumes is already configured for a data SVM and the corresponding NVE keys are managed by the admin SVM onboard key manager, those keys should be migrated to the external key management service. To do this with the CLI, run the command:
`security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM`
New encrypted volumes cannot be created for the tenant's data SVM until all NVE keys of the data SVM are successfully migrated.

Related information

- Encrypting volumes with NetApp encryption solutions for Cloud Volumes ONTAP
- security key-manager external

Manage ONTAP keys with Barbican KMS

Beginning with ONTAP 9.17.1, you can use OpenStack's Barbican KMS to protect ONTAP encryption keys. Barbican KMS is a service for securely storing and accessing keys. Barbican KMS can be used to protect NetApp Volume Encryption (NVE) keys for data SVMs. Barbican relies on OpenStack Keystone, OpenStack's identity service, for authentication.

About this task

You can configure key management with Barbican KMS with the CLI or the ONTAP REST API. With the 9.17.1 release, Barbican KMS support has the following limitations:

- Barbican KMS is not supported for NetApp Storage Encryption (NSE) and NetApp Aggregate Encryption (NAE). Alternatively, you can use external KMIPs or the Onboard Key Manager (OKM) for NSE and NVE keys.
- Barbican KMS is not supported for MetroCluster configurations.
- Barbican KMS can only be configured for a data SVM. It is not available for the admin SVM.

Unless otherwise noted, administrators at the `admin` privilege level can perform the following procedures.

Before you begin

- Barbican KMS and OpenStack Keystone must be configured. The SVM you are using with Barbican must have network access to the Barbican and OpenStack Keystone servers.
- If you are using a custom Certificate Authority (CA) for the Barbican and OpenStack Keystone servers, you must install the CA certificate with `security certificate install -type server-ca -vserver <admin_svm>`.

Create and activate a Barbican KMS configuration

You can create a new Barbican KMS configuration for an SVM and activate it. An SVM can have multiple inactive Barbican KMS configurations, but only one can be active at a time.

Steps

1. Create a new inactive Barbican KMS configuration for an SVM:

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` is the key identifier of the Barbican key encryption key (KEK). Enter a full URL, including `https://`.

     Some URLs include the question mark (?) character. The question mark activates the ONTAP command line active help. In order to enter a URL with a question mark, you need to first disable active help with the command `set -active-help false`. Active help can later be re-enabled with the command `set -active-help true`. Learn more in the ONTAP command reference.

   - `-keystone-url` is the URL of the OpenStack Keystone authorization host. Enter a full URL, including `https://`.
   - `-application-cred-id` is the application credentials ID.

     After entering this command, you will be prompted for the application credentials secret key. This command creates an inactive Barbican KMS configuration.

     The following example creates a new inactive Barbican KMS configuration named `config1` for the SVM `svm1`:

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. Activate the new Barbican KMS configuration:

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

You can use this command to switch between Barbican KMS configurations. If there is already an active Barbican KMS configuration on the SVM, it will be made inactive and the new configuration will be activated.

3. Verify that the new Barbican KMS configuration is active:

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

This command will provide the status of the active Barbican KMS configuration on the SVM or node. For example, if the SVM `svm1` on node `node1` has an active Barbican KMS configuration, the following command will return the status of that configuration:

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Update the credentials and settings of a Barbican KMS configuration

You can view and update the current settings of an active or inactive Barbican KMS configuration.

Steps

1. View the current Barbican KMS configurations for an SVM:

```
security key-manager external barbican show -vserver <svm_name>
```

The key ID, OpenStack Keystone URL, and application credentials ID are displayed for each Barbican KMS configuration on the SVM.

2. Update the settings of a Barbican KMS configuration:

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

This command updates the timeout and verification settings of the specified Barbican KMS configuration. `timeout` determines the time in seconds ONTAP will wait for Barbican to respond before the connection fails. The default `timeout` is ten seconds. `verify` and `verify-host` determine if the identity and hostname respectively of Barbican host should be verified before connecting. By default, these parameters are set to `true`. The `vserver` and `config-name` parameters are required. The other parameters are optional.

3. If needed, update the credentials of an active or inactive Barbican KMS configuration:

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

After entering this command, you will be prompted for the new application credentials secret key.

4. If needed, restore a missing SVM key encryption key (KEK) for an active Barbican KMS configuration:
   a. Restore a missing SVM KEK with `security key-manager external barbican restore`:

```
security key-manager external barbican restore -vserver <svm_name>
```

This command will restore the SVM KEK for the active Barbican KMS configuration by communicating with the Barbican server.

5. If needed, rekey the SVM KEK for a Barbican KMS configuration:
   a. Set the privilege level to advanced:

```
set -privilege advanced
```

   b. Rekey the SVM KEK with `security key-manager external barbican rekey-internal`:

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

This command generates a new SVM KEK for the specified SVM and re-wraps the volume encryption keys with the new SVM KEK. The new SVM KEK will be protected by the active Barbican KMS configuration.

Migrate keys between Barbican KMS and the Onboard Key Manager

You can migrate keys from Barbican KMS to the Onboard Key Manager (OKM), and vice-versa. To learn more about the OKM, refer to Enable onboard key management in ONTAP 9.6 and later.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. If needed, migrate keys from Barbican KMS to the OKM:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` is the name of the SVM with the Barbican KMS configuration.

3. If needed, migrate keys from the OKM to Barbican KMS:

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Disable and delete a Barbican KMS configuration

You can disable an active Barbican KMS configuration with no encrypted volumes, and you can delete an inactive Barbican KMS configuration.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Disable an active Barbican KMS configuration:

```
security key-manager keystore disable -vserver <svm_name>
```

If NVE encrypted volumes exist on the SVM, you must decrypt them or migrate the keys before disabling the Barbican KMS configuration. Activating a new Barbican KMS configuration does not require decrypting NVE volumes or migrating keys, and will disable the current active Barbican KMS configuration.

3. Delete an inactive Barbican KMS configuration:

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

Enable onboard key management for NVE in ONTAP 9.6 and later

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable the Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

About this task

You must run the `security key-manager onboard sync` command each time you add a node to the cluster.

If you have a MetroCluster configuration, you must run the `security key-manager onboard enable` command on the local cluster first, then run the `security key-manager onboard sync` command on the remote cluster, using the same passphrase on each. When you run the `security key-manager onboard enable` command from the local cluster and then synchronize on the remote cluster, you do not need to run the `enable` command again from the remote cluster.

Learn more about `security key-manager onboard enable` and `security key-manager onboard sync` in the ONTAP command reference.

By default, you are not required to enter the key manager passphrase when a node is rebooted. You can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

When configuring ONTAP data at rest encryption, to meet the requirements for Commercial Solutions for Classified (CSfC) you must use NSE with NVE and ensure the Onboard Key Manager is enabled in Common Criteria mode. See CSfC Solution Brief.

When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:

- The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.

  If you fail to enter the cluster passphrase 5 times, wait 24 hours or reboot the node to reset the limit.

- System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.

  The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The system proceeds to the next step in the image update process if validation succeeds; otherwise, it fails the image update. Learn more about `cluster image` in the ONTAP command reference.

The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. The system clears volatile memory within 30 seconds when it is halted.

Before you begin

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure the Onboard Key Manager.

Steps

1. Start the key manager setup:

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

   Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. The `- cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

2. Enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

   If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

3. At the passphrase confirmation prompt, reenter the passphrase.
4. Verify that the authentication keys have been created:

   ```
   security key-manager key query -key-type NSE-AK
   ```

The `security key-manager key query` command replaces the `security key-manager query key` command.

Learn more about `security key-manager key query` in the ONTAP command reference.

5. Optionally, you can convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   The Onboard Key Manager must be fully configured before you convert the volumes. In a MetroCluster environment, the Onboard Key Manager must be configured on both sites.

After you finish

Copy the passphrase to a secure location outside the storage system for future use.

After configuring the Onboard Key Manager passphrase, manually back up the information to a secure location outside the storage system. See Back up onboard key management information manually.

Related information

- cluster image commands
- security key-manager external enable
- security key-manager key query
- security key-manager onboard enable

Enable onboard key management for NVE in ONTAP 9.5 and earlier

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

About this task

You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

After a failed passphrase attempt, you must reboot the node again.

Before you begin

- If you use NSE or NVE with an external key management (KMIP) server, delete the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.
- Configure the MetroCluster environment before configuring the Onboard Key Manager.

Steps

1. Start the key manager setup:

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

   Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted.

   The following example starts setting up the key manager on cluster1 without requiring that the passphrase be entered after every reboot:

   ```
   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. Enter `yes` at the prompt to configure onboard key management.
3. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

   If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

4. At the passphrase confirmation prompt, reenter the passphrase.
5. Verify that keys are configured for all nodes:

   `security key-manager show-key-store`

```
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
```

Learn more about `security key-manager show-key-store` in the ONTAP command reference.

6. Optionally, convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   Configure the Onboard Key Manager before converting volumes. In MetroCluster environments, configure it on both sites.

After you finish

Copy the passphrase to a secure location outside the storage system for future use.

When you configure the Onboard Key Manager passphrase, back up the information to a secure location outside the storage system in case of a disaster. See Back up onboard key management information manually.

Related information

- Back up onboard key management information manually
- Transitioning to onboard key management from external key management
- security key-manager show-key-store

Enable onboard key management in newly added ONTAP nodes

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

For ONTAP 9.6 and later, you must run the `security key-manager onboard sync` command each time you add a node to the cluster.

For ONTAP 9.5 and earlier, you must run the `security key-manager setup` command each time you add a node to the cluster.

If you add a node to a cluster with onboard key management, run this command to refresh missing keys.

If you have a MetroCluster configuration, review these guidelines:

- Beginning with ONTAP 9.6, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

  Learn more about `security key-manager onboard enable` and `security key-manager onboard sync` in the ONTAP command reference.

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

If the passphrase attempt fails, reboot the node. After the reboot, you can try entering the passphrase again.

Related information

- cluster image commands
- security key-manager external enable
- security key-manager onboard enable

Encrypt volume data with NVE or NAE

Learn about encrypting ONTAP volume data with NVE

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default when you have the VE license and onboard or external key management. For ONTAP 9.6 and earlier, you can enable encryption on a new volume or on an existing volume. You must have installed the VE license and enabled key management before you can enable

volume encryption. NVE is FIPS-140-2 level 1 compliant.

Enable aggregate-level encryption with VE license in ONTAP

Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you have the VE license and onboard or external key management. Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted.

About this task

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

An aggregate enabled for aggregate-level encryption is called an *NAE aggregate* (for NetApp Aggregate Encryption). All volumes in an NAE aggregate must be encrypted with NAE or NVE encryption. With aggregate-level encryption, volumes you create in the aggregate are encrypted with NAE encryption by default. You can override the default to use NVE encryption instead.

Plain text volumes are not supported in NAE aggregates.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Enable or disable aggregate-level encryption:

To…	Use this command…
Create an NAE aggregate with ONTAP 9.7 or later	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Create an NAE aggregate with ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Convert a non-NAE aggregate to an NAE aggregate	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Convert an NAE aggregate to a non-NAE aggregate	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Learn more about `storage aggregate modify` in the ONTAP command reference.

The following command enables aggregate-level encryption on `aggr1`:

- ONTAP 9.7 or later:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 or earlier:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

Learn more about `storage aggregate create` in the ONTAP command reference.

2. Verify that the aggregate is enabled for encryption:

`storage aggregate show -fields encrypt-with-aggr-key`

The following command verifies that `aggr1` is enabled for encryption:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

Learn more about `storage aggregate show` in the ONTAP command reference.

After you finish

Run the `volume create` command to create the encrypted volumes.

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

Enable encryption on a new volume in ONTAP

You can use the `volume create` command to enable encryption on a new volume.

About this task

You can encrypt volumes using NetApp Volume Encryption (NVE) and, beginning with ONTAP 9.6, NetApp Aggregate Encryption (NAE). To learn more about NAE and NVE, refer to the volume encryption overview.

Learn more about the commands described in this procedure in the ONTAP command reference.

The procedure to enable encryption on a new volume in ONTAP varies based on the version of ONTAP you are using and your specific configuration:

- Beginning with ONTAP 9.4, if you enable `cc-mode` when you set up the Onboard Key Manager, volumes you create with the `volume create` command are automatically encrypted, whether or not you specify `-encrypt true`.

- In ONTAP 9.6 and earlier releases, you must use `-encrypt true` with `volume create` commands to enable encryption (provided you did not enable `cc-mode`).
- If you want to create an NAE volume in ONTAP 9.6, you must enable NAE at the aggregate level. Refer to Enable aggregate-level encryption with the VE license for more details on this task.
- Beginning with ONTAP 9.7, newly created volumes are encrypted by default when you have the VE license and onboard or external key management. By default, new volumes created in an NAE aggregate will be of type NAE rather than NVE.
  - In ONTAP 9.7 and later releases, if you add `-encrypt true` to the `volume create` command to create a volume in an NAE aggregate, the volume will have NVE encryption instead of NAE. All volumes in an NAE aggregate must be encrypted with either NVE or NAE.

Plaintext volumes are not supported in NAE aggregates.

Steps

1. Create a new volume and specify whether encryption is enabled on the volume. If the new volume is in an NAE aggregate, by default the volume will be an NAE volume:

To create…	Use this command…
An NAE volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
An NVE volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + In ONTAP 9.6 and earlier where NAE is not supported, `-encrypt true` specifies that the volume should be encrypted with NVE. In ONTAP 9.7 and later where volumes are created in NAE aggregates, `-encrypt true` overrides the default encryption type of NAE to create an NVE volume instead.
A plain text volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

   Learn more about `volume create` in the ONTAP command reference.

2. Verify that volumes are enabled for encryption:

   ```
   volume show -is-encrypted true
   ```

   Learn more about `volume show` in the ONTAP command reference.

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically "pushes" an encryption key to the server when you encrypt a volume.

Enable NAE or NVE on an existing ONTAP volume

You can use either the `volume move start` or the `volume encryption conversion start` command to enable encryption on an existing volume.

About this task

You can use the `volume encryption conversion start` command to enable encryption of an existing volume "in place," without having to move the volume to a different location. Alternatively, you can use the `volume move start` command.

Enable encryption on an existing volume with the volume encryption conversion start command

You can use the `volume encryption conversion start` command to enable encryption of an existing volume "in place," without having to move the volume to a different location.

After you start a conversion operation, it must be completed. If you encounter a performance issue during the operation, you can run the `volume encryption conversion pause` command to pause the operation, and the `volume encryption conversion resume` command to resume the operation.

You cannot use `volume encryption conversion start` to convert a SnapLock volume.

Steps

1. Enable encryption on an existing volume:

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

   Learn more about `volume encryption conversion start` in the ONTAP command reference.

   The following command enables encryption on existing volume `vol1`:

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   The system creates an encryption key for the volume. The data on the volume is encrypted.

2. Verify the status of the conversion operation:

   `volume encryption conversion show`

   Learn more about `volume encryption conversion show` in the ONTAP command reference.

   The following command displays the status of the conversion operation:

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. When the conversion operation is completed, verify that the volume is enabled for encryption:

   `volume show -is-encrypted true`

   Learn more about `volume show` in the ONTAP command reference.

   The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically "pushes" an encryption key to the server when you encrypt a volume.

Enable encryption on an existing volume with the volume move start command

You can use the `volume move start` command to enable encryption by moving an existing volume. You can use the same aggregate or a different aggregate.

About this task

- Beginning with ONTAP 9.8, you can use `volume move start` to enable encryption on a SnapLock or FlexGroup volume.
- Beginning with ONTAP 9.4, if you enable "cc-mode" when you set up the Onboard Key Manager, volumes you create with the `volume move start` command are automatically encrypted. You need not specify `-encrypt-destination true`.
- Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be moved. A volume encrypted with a unique key is called an *NVE volume* (meaning it uses NetApp Volume Encryption). A volume encrypted with an aggregate-level key is called an *NAE volume* (for NetApp Aggregate Encryption). Plaintext volumes are not supported in NAE aggregates.
- Beginning with ONTAP 9.14.1, you can encrypt an SVM root volume with NVE. For more information, see Configure NetApp Volume Encryption on an SVM root volume.

Before you begin

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

Delegating authority to run the volume move command

Steps

1. Move an existing volume and specify whether encryption is enabled on the volume:

To convert…	Use this command…

A plaintext volume to an NVE volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`
An NVE or plaintext volume to an NAE volume (assuming aggregate-level encryption is enabled on the destination)	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
An NAE volume to an NVE volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
An NAE volume to a plaintext volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
An NVE volume to a plaintext volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

Learn more about `volume move start` in the ONTAP command reference.

The following command converts a plaintext volume named `vol1` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Assuming aggregate-level encryption is enabled on the destination, the following command converts an NVE or plaintext volume named `vol1` to an NAE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

The following command converts an NAE volume named `vol2` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

The following command converts an NAE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

The following command converts an NVE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. View the encryption type of cluster volumes:

   `volume show -fields encryption-type none|volume|aggregate`

   The `encryption-type` field is available in ONTAP 9.6 and later.

   Learn more about `volume show` in the ONTAP command reference.

   The following command displays the encryption type of volumes in `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Verify that volumes are enabled for encryption:

   `volume show -is-encrypted true`

   Learn more about `volume show` in the ONTAP command reference.

   The following command displays the encrypted volumes on `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically pushes an encryption key to the server when you encrypt a volume.

Configure NVE on an ONTAP SVM root volume

Beginning with ONTAP 9.14.1, you can enable NetApp Volume Encryption (NVE) on a storage VM (SVM) root volume. With NVE, the root volume is encrypted with a unique key, enabling greater security on the SVM.

About this task

NVE on an SVM root volume can only be enabled after the SVM has been created.

Before you begin

- The SVM root volume must not be on an aggregate encrypted with NetApp Aggregate Encryption (NAE).
- You must have enabled encryption with the Onboard Key Manager or an external key manager.
- You must be running ONTAP 9.14.1 or later.
- To migrate an SVM containing a root volume encrypted with NVE, you must convert the SVM root volume to a plain text volume after the migration completes then re-encrypt the SVM root volume.
  - If the destination aggregate of the SVM migration uses NAE, the root volume inherits NAE by default.
- If the SVM is in an SVM disaster recovery relationship:
  - Encryption settings on a mirrored SVM are not copied to the destination. If you enable NVE on the source or destination, you must separately enable NVE on the mirrored SVM root volume.
  - If all aggregates in the destination cluster use NAE, the SVM root volume will use NAE.

Steps

You can enable NVE on an SVM root volume with the ONTAP CLI or System Manager.

CLI

You can enable NVE on the SVM root volume in-place or by moving the volume between aggregates.

Encrypt the root volume in place

1. Convert the root volume to an encrypted volume:

   `volume encryption conversion start -vserver` *`svm_name`* `-volume` *`volume`*

2. Confirm the encryption succeeded. The `volume show -encryption-type volume` displays a list of all volumes using NVE.

Encrypt the SVM root volume by moving it

1. Initiate a volume move:

   `volume move start -vserver` *`svm_name`* `-volume` *`volume`* `-destination-aggregate` *`aggregate`* `-encrypt-with-aggr-key false -encrypt-destination true`

   Learn more about `volume move` in the ONTAP command reference.

2. Confirm the `volume move` operation succeeded with the `volume move show` command. The `volume show -encryption-type volume` displays a list of all volumes using NVE.

System Manager

1. Navigate to **Storage** > **Volumes**.
2. Next to the name of the SVM root volume you want to encrypt, select ⋮ then **Edit**.
3. Under the **Storage and Optimization** heading, select **Enable encryption**.
4. Select **Save**.

Configure NVE on an ONTAP node root volume

Beginning with ONTAP 9.8, you can use NetApp Volume Encryption to protect the root volume of your node.

About this task

This procedure applies to the node root volume. It does not apply to SVM root volumes. SVM root volumes can be protected through aggregate-level encryption and, beginning with ONTAP 9.14.1, NVE.

Once root volume encryption begins, it must complete. You cannot pause the operation. Once encryption is complete, you cannot assign a new key to the root volume and you cannot perform a secure-purge operation.

Before you begin

- Your system must be using an HA configuration.
- Your node root volume must already be created.
- Your system must have an onboard key manager or an external key management server using the Key Management Interoperability Protocol (KMIP).

Steps

1. Encrypt the root volume:

   `volume encryption conversion start -vserver SVM_name -volume root_vol_name`

2. Verify the status of the conversion operation:

   `volume encryption conversion show`

3. When the conversion operation is complete, verify that the volume is encrypted:

   `volume show -fields`

   The following shows example output for an encrypted volume.

```
::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
vserver    volume is-encrypted
---------- ------ ------------
xyz        vol0   true
```

Copyright information

Trademark information