Administer

ONTAP Select

NetApp
October 23, 2024

Table of Contents

Administer

Before you begin administering ONTAP Select

After creating an ONTAP Select cluster, you can support the deployment by performing various administrative tasks. There are a few general considerations to be aware of.

In general, the procedures you can perform using the Deploy web interface fall into one of three categories.

Deploy an ONTAP Select cluster

You can deploy a single-node or multi-node cluster. See Deploy an ONTAP Select cluster for more information.

Perform a procedure with an existing ONTAP Select cluster

The administrative procedures are organized in various categories, such as *Security* and *Clusters*.

Perform a procedure on the Deploy utility

There are several procedures specific to Deploy (such as changing the administrator's password).

Administer ONTAP Select

There are many different administrative procedures available as part of supporting ONTAP Select. In addition, there are procedures specific to the Deploy administrative utility. The most important of these procedures are presented below. In general, all use the Deploy web user interface.

You can also use the command line interface to administer ONTAP Select.

Perform additional ONTAP configuration

After an ONTAP Select cluster is deployed, you can configure and manage the cluster just as you would a hardware-based ONTAP system. For example, you can use ONTAP System Manager or the ONTAP CLI to configure the ONTAP Select cluster.

NetApp client software

You can connect to ONTAP Select using the following supported NetApp client software:

- ONTAP System Manager
- Active IQ Unified Manager
- OnCommand Insight
- OnCommand Workflow Automation
- SnapCenter
- Virtual Storage Console for VMware vSphere

To identify the supported versions of the client software, review the NetApp Interoperability Matrix Tool. If the client software supports ONTAP 9, then the same version is also supported with ONTAP Select.

The use of SnapCenter and the corresponding plug-ins requires server-based licenses. Storage system licensing of the SnapCenter plug-ins is not currently supported with ONTAP Select.

Any other NetApp client software that is not included in the list is not supported by ONTAP Select.

Possible configuration options

There are several options available when configuring the cluster, including the following:

- Creating the networking configuration
- Laying out your aggregates
- Creating the data storage VMs (SVMs)

Purchased licenses with storage capacity

If you decided not to install the license files with storage capacity as part of deploying the ONTAP Select cluster, you must acquire and install the license files before the grace period expires for clusters running with a purchased license.

Mirrored aggregates

There are data spare disks created by the Deploy administration utility on each ONTAP Select node from the usable datastore space (such as, Pool0 and Pool1). To implement high availability for your data on a multi-node cluster, you must create a mirrored aggregate using these spares.

Upgrade the ONTAP Select nodes

After deploying an ONTAP Select cluster, you can upgrade the ONTAP image at each node in the cluster as needed.

You cannot use the Deploy administration utility to perform upgrades of existing ONTAP Select nodes. The Deploy utility can only be used to create new ONTAP Select clusters.

General procedure

At a high level, you should use the following steps to upgrade an existing ONTAP Select node.

1. Navigate to downloads page at the NetApp Support Site.

   NetApp Support Downloads

2. Click **ONTAP Select Node Upgrade**.
3. Select and download the appropriate upgrade image responding to all prompts as needed.

   Review the Release Notes for additional information and any required procedures before upgrading an ONTAP Select node.

4. Upgrade the ONTAP Select node using the standard ONTAP upgrade procedures with the ONTAP Select upgrade file. For information on supported upgrade paths, see the Supported ONTAP upgrade paths.

Revert an ONTAP Select node

You cannot revert an ONTAP Select node to a version prior to the one on which it was originally installed. For example:

ONTAP Select 9.7 is initially installed

You can upgrade the node to version 9.8 and then revert back to version 9.7 if needed.

ONTAP Select 9.8 is initially installed

You cannot revert to version 9.7 because this version is prior to the version that was originally installed.

Use the VMXNET3 network driver

VMXNET3 is the default network driver included with new cluster deployments on VMware ESXi. If you upgrade an existing ONTAP Select node running ONTAP Select 9.4 or earlier, the network driver is not automatically upgraded. You must manually upgrade to VMXNET3. You should contact NetApp support for assistance with the upgrade.

Related information

- ONTAP upgrade overview

Diagnostics and support

There are several related diagnostic and support tasks you can perform as part of administering ONTAP Select.

Configure the Deploy system

You should set the basic system configuration parameters that affect how the Deploy utility operates.

About this task

The Deploy configuration data is used by AutoSupport.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Administration** tab at the top of the page.
3. Click **Settings & AutoSupport** and then click  .
4. Provide the configuration data as appropriate for your environment and click **Modify**.

   If you use a proxy server, you can configure the proxy URL as follows:
   `http://USERNAME:PASSWORD@<FQDN|IP>:PORT`

   Example
   `http://user1:mypassword@proxy.company-demo.com:80`

Display the ONTAP Select Deploy event messages

The ONTAP Select Deploy utility includes an event logging facility that provides information about the activity of the system. You should view the contents of the event log to debug any issues or when directed to do so by support.

About this task

You can filter the list of event messages based on several characteristics, including:

- Status
- Type
- Category
- Instance
- Time
- Description

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Administration** tab at the top of the page.
3. Click **Events & Jobs** and then click **Events**.
4. Optionally click **Filter** and create a filter to limit the event messages displayed.

Enable AutoSupport

You can enable and disable the AutoSupport feature as needed.

About this task

AutoSupport is the primary troubleshooting tool used by NetApp in supporting ONTAP Select. Therefore, you should not disable AutoSupport unless absolutely necessary. If you do disable AutoSupport, data is still collected but not transmitted to NetApp.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Administration** tab at the top of the page.
3. Click **Settings & AutoSupport** and then click ⋮.
4. Enable or disable the AutoSupport feature as needed.

Generate and download an AutoSupport package

ONTAP Select includes the ability to generate an AutoSupport package. You should generate a package to debug any issues or when directed to do so by support.

About this task

You can generate the following AutoSupport packages under the direction and guidance of NetApp support:

- Deploy logs
  Log files created by the ONTAP Select Deploy utility
- Troubleshooting
  Troubleshooting and debugging information about the hypervisor hosts and ONTAP Select nodes
- Performance
  Performance information about the hypervisor hosts and ONTAP Select nodes

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Administration** tab at the top of the page.

3. Click **Settings & AutoSupport** and then click ⋮.
4. Click **Generate**.
5. Select the type and provide a description for the package; you can optionally provide a case number.
6. Click **Generate**.

   Each AutoSupport package is assigned a unique sequence identification number.

7. Optionally under **AutoSupport History**, select the correct package and click the download icon to save the AutoSupport file to your local workstation.

Security

There are several related tasks you can perform as part of securing an ONTAP Select deployment.

Change the Deploy administrator password

You can change the password for the Deploy virtual machine administrator account as needed using the web user interface.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the figure icon at the top right of the page and select **Change Password**.
3. Provide the current and new password as prompted and click **Submit**.

Add a management server account

You can add a management server account to the Deploy credential store database.

Before you begin

You should be familiar with the types of credentials and how they are used by ONTAP Select Deploy.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Administration** tab at the top of the page.
3. Click **Management Servers** and then click **Add vCenter**.
4. Enter the following information and click **Add**.

In this field …	Do the following …
Name/IP Address	Provide the domain name or IP address of the vCenter server.
Username	Enter the account user name to access vCenter.
Password	Enter the password for the associated user name.

5. After the new management server is added, you can optionally click ⋮ and select one of the following:
   - Update credentials

- Verify credentials
- Remove management server

Configure MFA

Beginning with ONTAP Select 9.13.1, multifactor authentication (MFA) is supported for the ONTAP Select Deploy administrator account:

- ONTAP Select Deploy CLI MFA login using YubiKey Personal Identity Verification (PIV) or Fast IDentity Online (FIDO2) authentication
- ONTAP Select Deploy CLI MFA login using ssh-keygen

ONTAP Select Deploy CLI MFA login using YubiKey PIV or FIDO2 authentication

YubiKey PIV

Configure the YubiKey PIN and generate or import the Remote Support Agent (RSA) or Elliptic Curve Digital Signature Algorithm (ECDSA) private key and certificate with the steps in TR-4647: Multifactor authentication in ONTAP.

- For Windows: The **YubiKey PIV Client configuration for Windows** section of the technical report.
- For MacOS: The **YubiKey PIV client configuration For MAC OS and Linux** section of the technical report.

FIDO2

If you choose to opt for YubiKey FIDO2 authentication, configure the YubiKey FIDO2 PIN using the YubiKey Manager and generate the FIDO2 key with a PuTTY-CAC (Common Access Card) for Windows or ssh-keygen for MacOS. The steps to do this are in the technical report TR-4647: Multifactor authentication in ONTAP.

- For Windows: The **YubiKey FIDO2 client configuration for Windows** section of the technical report.
- For MacOS: The **YubiKey FIDO2 client configuration For Mac OS and Linux** section of the technical report.

Obtain the YubiKey PIV or FIDO2 public key

Obtaining the public key depends on whether you're a Windows or MacOS client, and if you are using PIV or FIDO2.

For Windows:

- Export the PIV public key using the **Copy to Clipboard** feature under SSH → Certificate as described in the section **Configuring the Windows PuTTY-CAC SSH Client for YubiKey PIV Authentication** on page 16 of TR-4647.
- Export the FIDO2 public key using the **Copy to Clipboard** feature under SSH → Certificate as described in the section **Configuring the Windows PuTTY-CAC SSH Client for YubiKey FIDO2 Authentication** on page 30 of TR-4647.

For MacOS:

- The PIV public key should be exported using the `ssh-keygen -e` command as described in the section **Configure the Mac OS or Linux SSH Client for YubiKey PIV authentication** on page 24 of TR-4647.

- The FIDO2 public key is in the `id_ecdsa_sk.pub` file or `id_edd519_sk.pub` file, depending on whether you use ECDSA or EDD519, as described in the section **Configure the MAC OS or Linux SSH client for YubiKey FIDO2 authentication** on page 39 of TR-4647.

Configure the public key in ONTAP Select Deploy

SSH is used by the administrator account for the public key authentication method. The command used is the same whether the authentication method is the standard SSH public key authentication or YubiKey PIV or FIDO2 authentication.

For hardware-based SSH MFA, the authentication factors in addition to the public key configured on ONTAP Select Deploy are as follows:

- The PIV or FIDO2 PIN
- Possession of the YubiKey hardware device. For FIDO2, this is confirmed by physically touching the YubiKey during the authentication process.

Before you begin

Set the PIV or FIDO2 public key which is configured for the YubiKey. The ONTAP Select Deploy CLI command `security publickey add -key` is the same for PIV or FIDO2 and the public key string is different.

The public key is obtained from:

- The **Copy to Clipboard** function for PuTTY-CAC for PIV and FIDO2 (Windows)
- Exporting the public key in an SSH compatible format using the `ssh-keygen -e` command for PIV
- The public key file located in the `~/.ssh/id_***_sk.pub` file for FIDO2 (MacOS)

Steps

1. Find the generated key in the `.ssh/id_***.pub` file.
2. Add the generated key to ONTAP Select Deploy using the `security publickey add -key <key>` command.

```
(ONTAPdeploy) security publickey add -key "ssh-rsa <key>
user@netapp.com"
```

3. Enable MFA Authentication with the `security multifactor authentication enable` command.

```
(ONTAPdeploy) security multifactor authentication enable
MFA enabled Successfully
```

Log in to ONTAP Select Deploy using YubiKey PIV Authentication over SSH

You can log in to ONTAP Select Deploy using YubiKey PIV Authentication over SSH.

Steps

1. After the YubiKey token, the SSH client, and ONTAP Select Deploy are configured, you can use MFA

YubiKey PIV authentication over SSH.

2. Log in to ONTAP Select Deploy. If you are using the Windows PuTTY-CAC SSH client, a dialog will pop-up prompting you to enter your YubiKey PIN.
3. Log in from your device with the YubiKey connected.

Example output

```
login as: admin
Authenticating with public key "<public_key>"
Further authentication required
<admin>'s password:

NetApp ONTAP Select Deploy Utility.
Copyright (C) NetApp Inc.
All rights reserved.

Version: NetApp Release 9.13.1 Build:6811765 08-17-2023 03:08:09

(ONTAPdeploy)
```

ONTAP Select Deploy CLI MFA login using ssh-keygen

The `ssh-keygen` command is a tool for creating new authentication key pairs for SSH. The key pairs are used for automating logins, single sign-on, and for authenticating hosts.

The `ssh-keygen` command supports several public key algorithms for authentication keys.

- The algorithm is selected with the `-t` option
- The key size is selected with the `-b` option

Example output

```
ssh-keygen -t ecdsa -b 521
ssh-keygen -t ed25519
ssh-keygen -t ecdsa
```

Steps

1. Find the generated key in the `.ssh/id_***.pub` file.
2. Add the generated key to ONTAP Select Deploy using the `security publickey add -key <key>` command.

   ```
   (ONTAPdeploy) security publickey add -key "ssh-rsa <key>
   user@netapp.com"
   ```

3. Enable MFA Authentication with the `security multifactor authentication enable` command.

```
(ONTAPdeploy) security multifactor authentication enable
MFA enabled Successfully
```

4. Log in to the ONTAP Select Deploy system after enabling MFA. You should receive an output similar to the following example.

```
[<user ID> ~]$ ssh <admin>
Authenticated with partial success.
<admin>'s password:

NetApp ONTAP Select Deploy Utility.
Copyright (C) NetApp Inc.
All rights reserved.

Version: NetApp Release 9.13.1 Build:6811765 08-17-2023 03:08:09

(ONTAPdeploy)
```

Migrate from MFA to single-factor authentication

MFA can be disabled for the Deploy administrator account using the following methods:

- If you can log in to the Deploy CLI as an administrator using Secure Shell (SSH), disable MFA by running the `security multifactor authentication disable` command from the Deploy CLI.

```
(ONTAPdeploy) security multifactor authentication disable
MFA disabled Successfully
```

- If you cannot log in to the Deploy CLI as an administrator using SSH:
  1. Connect to the Deploy virtual machine (VM) video console through vCenter or vSphere.
  2. Log in to the Deploy CLI using the administrator account.
  3. Run the `security multifactor authentication disable` command.

```
Debian GNU/Linux 11 <user ID> tty1

<hostname> login: admin
Password:

NetApp ONTAP Select Deploy Utility.
Copyright (C) NetApp Inc.
All rights reserved.

Version: NetApp Release 9.13.1 Build:6811765 08-17-2023 03:08:09

(ONTAPdeploy) security multifactor authentication disable
MFA disabled successfully

(ONTAPdeploy)
```

- The administrator can delete the public key with:
  `security publickey delete -key`

Confirming connectivity among the ONTAP Select nodes

You can test the network connectivity among two or more ONTAP Select nodes on the internal cluster network. You typically run this test before a multi-node cluster is deployed to detect issues that might cause the operation to fail.

Before you begin

All the ONTAP Select nodes included in the test must be configured and powered on.

About this task

Each time you start a test, a new process run is created in the background and assigned a unique run identifier. Only one run can be active at a time.

The test has two modes that control its operation:

- Quick
  This mode performs a basic non-disruptive test. A PING test is performed, along with a test of the network MTU size and the vSwitch.
- Extended
  This mode performs a more comprehensive test over all the redundant network paths. If you run this on an active ONTAP Select cluster, the performance of the cluster can be impacted.

It is recommended that you always perform a quick test before creating a multi-node cluster. After the quick test completes successfully, you can optionally perform an extended test based on your production requirements.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.

2. Click the **Administration** tab at the top of the page and click **Network Checker**.
3. Click **Start New Run** and select the hosts and networks for the HA pair

   You can add and configure additional HA pairs as needed.

4. Click **Start** to begin the network connectivity test.

Administering the Deploy mediator services

Each ONTAP Select two-node cluster is monitored by the mediator service, which assists in managing the HA capability shared by the nodes.

View the status of the mediator service

You can view the status of the mediator service with respect to each of the two-node clusters defined to the ONTAP Select Deploy utility.

About this task

You can view the configuration of each mediator, including the current status, the two ONTAP Select nodes, and the iSCSI target where the HA control information is stored. Hover over the objects on the page to display detailed information.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Administration** tab at the top of the page and click **Mediators**.
3. Optionally click **Filter** to customize your view of the two-node clusters monitored by the mediator service.

ONTAP Select clusters

There are several related tasks you can perform to administer an ONTAP Select cluster.

Move an ONTAP Select cluster offline and online

After you've created a cluster, you can move it offline and online as needed.

Before you begin

After a cluster is created it is initially in the online state.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Clusters** tab at the top of the page and select the desired cluster from the list.
3. Click ⋮ on the right of the cluster and select **Take Offline**.

   If the offline option is not available, the cluster is already in the offline state.

4. Click **Yes** in the popup window to confirm the request.
5. Click **Refresh** occasionally to confirm the cluster is offline.
6. To bring the cluster back online, click ⋮ and select **Bring Online**.

7. Click **Refresh** occasionally to confirm the cluster is online.

Delete an ONTAP Select cluster

You can delete an ONTAP Select cluster when it is no longer needed.

Before you begin

The cluster must be in the offline state.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Clusters** tab at the top of the page and select the desired cluster from the list.
3. Click ⋮ on the right of the cluster and select **Delete**.

   If the delete option is not available, then the cluster is not in an offline state.

4. Click **Refresh** occasionally to confirm the cluster is removed from the list.

Refresh the Deploy cluster configuration

After creating an ONTAP Select cluster, you can make changes to the cluster or the virtual machine configuration outside of the Deploy utility using the ONTAP or hypervisor administration tools. The configuration of a virtual machine can also change after it is migrated.

When these changes to the cluster or virtual machine occur, the Deploy utility configuration database is not automatically updated and can become out of sync with the state of the cluster. You should perform a cluster refresh in these and other situations to update the Deploy database based on the current state of the cluster.

Before you begin

Required information

You must have the current configuration information for the cluster, including:

- ONTAP administrator credentials
- Cluster management IP address
- Names of the nodes in the cluster

Stable cluster state

The cluster must be in a stable state. You cannot refresh a cluster when it is in the process of being created or deleted, or when it is in the *create_failed* or *delete_failed* state.

After a VM migration

After a virtual machine running ONTAP Select has been migrated, you must create a new host using the Deploy utility before performing a cluster refresh.

About this task

You can perform a cluster refresh to update the Deploy configuration database using the web user interface.

ⓘ Instead of using the Deploy GUI, you can use the cluster refresh command in the Deploy CLI shell to refresh a cluster.

Cluster and virtual machine configuration

Some of the configuration values that can change and cause the Deploy database to become out of sync include:

- Cluster and node names
- ONTAP network configuration
- ONTAP version (after an upgrade)
- Virtual machine names
- Host network names
- Storage pool names

Cluster and node states

An ONTAP Select cluster or node can be in a state that prevents it from operating properly. You should perform a cluster refresh operation to correct the following conditions:

- Node in *unknown* state
  An ONTAP Select node can be in the *unknown state* for several reasons, including the node is not found.
- Cluster in *degraded* state
  If a node is powered off, it might still appear to be online in the Deploy utility. In this situation, the cluster is in a *degraded* state.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Clusters** tab at the top left of the page and select the desired cluster from the list.
3. Click ⋮ on the right side of the page and select **Cluster Refresh**.
4. Under **Cluster Credentials**, provide the ONTAP administrator password for the cluster.
5. Click **Refresh**.

After you finish

If the operation is successful, the field *Last Refresh* is updated. You should back up the Deploy configuration data after the cluster refresh operation has completed.

Nodes and hosts

Access the ONTAP Select video console

You can access the video console of the hypervisor virtual machine where ONTAP Select is running.

About this task

You might need to access the virtual machine console to troubleshoot an issue or when asked to do so by NetApp support.

Steps

1. Access the vSphere client and sign in.

2. Navigate to the appropriate location in the hierarchy to locate the ONTAP Select virtual machine.
3. Right click the virtual machine and select **Open Console**.

Resize the ONTAP Select cluster nodes

After deploying an ONTAP Select cluster, you can upgrade the hypervisor instance type of the nodes using the Deploy administration utility.

> You can perform the cluster nodes resizing operation when using the capacity tiers licensing model and the capacity pools licensing model.

> Resizing to the large instance type is only supported on ESXi.

Before you begin

The cluster must be in the online state.

About this task

This task describes how to use the Deploy web user interface. You can also use the Deploy CLI to perform the instance resizing. Regardless of which interface you use, the time needed for the resizing operation can vary significantly based on several factors and may take an extended amount of time to complete. You can only resize a node to a larger size.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Cluster** tab at the top of the page and select the desired cluster from the list.
3. On the cluster details page, click the gear icon at the right of the page and select **Instance Resize**.
4. Select the **Instance Type** and provide the ONTAP credentials then click **Modify**.

After you finish

You must wait for the resize operation to complete.

Replace a failed drive when using SW RAID

When a drive using software RAID fails, ONTAP Select assigns a spare drive if one is available and starts the rebuild process automatically. This is similar to how ONTAP works on FAS and AFF. However if no spare drive is available, you need to add one to the ONTAP Select node.

> Both the removal of the failed drive and the addition of a new drive (marked as a spare) must be performed through ONTAP Select Deploy. Attaching a drive to the ONTAP Select VM using vSphere is not supported.

Identify the failed drive

When a drive fails you need to use the ONTAP CLI to identify the failed disk.

KVM

Before you begin

You must have the VM ID of the ONTAP Select virtual machine, as well as the ONTAP Select and ONTAP Select Deploy administrator account credentials.

About this task

You should only use this procedure when the ONTAP Select node is running on KVM and configured to use software RAID.

Steps

1. At the ONTAP Select CLI, identify the disk to be replaced:
   a. Identify the disk by serial number, UUID, or target address in the virtual machine.

```
disk show -fields serial,vmdisk-target-address,uuid
```

   b. Optionally, display a complete list of the spare disk capacity with the partitioned disks.
   storage aggregate show-spare-disks
2. At the Linux command line interface, locate the disk.
   a. Examine the system devices, searching for the disk serial number or UUID (disk name):

```
find /dev/disk/by-id/<SN|ID>
```

   b. Examine the virtual machine configuration, searching for the target address:

```
virsh dumpxml VMID
```

ESXi

Steps

1. Sign in to the ONTAP CLI using the administrator account.
2. Identify the disk drive that failed.

```
<cluster name>::> storage disk show -container-type broken
Usable Disk Container Container
Disk Size Shelf Bay Type Type Name Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
NET-1.4 893.3GB - - SSD broken - sti-rx2540-346a'
```

Remove the failed drive

After you identify the drive that failed, remove the disk.

KVM using Deploy

You can detach a disk from a KVM host as part of replacing the disk or when it is no longer needed.

Before you begin

You must have the ONTAP Select and ONTAP Select Deploy administrator account credentials.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Select the **Clusters** tab at the top of the page and select the desired cluster from the list.
3. Select **+** next to the desired HA pair or node.

   If the option is disabled, Deploy is currently refreshing the storage information.

4. Select **Edit Storage** on the **Edit Node Storage** page.
5. Deselect the disks to be detached from the node, enter the ONTAP administrator credentials, and select **Edit Storage** to apply the changes.
6. Select **Yes** to confirm the warning in the popup window.
7. Select the **Events** tab for the cluster to monitor and confirm the detach operation.

   You can remove the physical disk from the host if it is no longer needed.

KVM using CLI

After you identify the disk, follow the steps below.

Steps

1. Detach the disk from the virtual machine:
   a. Dump the configuration.

```
virsh dumpxml VMNAME > /PATH/disk.xml
```

   b. Edit the file and remove everything except the disk to be detached from the virtual machine.

   The target address for the disk should correspond to the vmdisk-target-address field in ONTAP.

```
<disk type='block' device='lun'>
  <driver name='qemu' type='raw' cache='directsync'/>
  <source dev='/dev/disk/by-id/ata-
Micron_5100_MTFDDAK960TCC_171616D35277'/>
  <backingStore/>
  <target dev='sde' bus='scsi'/>
  <alias name='scsi0-0-0-4'/>
  <address type='drive' controller='0' bus='0' target='0'
unit='4'/>
</disk>
```

c. Detach the disk.

```
virsh detach-disk --persistent /PATH/disk.xml
```

2. Replace the physical disk:

   You can use a utility such as `ledctl locate=` to locate the physical disk if needed.

   a. Remove the disk from the host.
   b. Select a new disk and install it in the host if necessary.
3. Edit the original disk configuration file and add the new disk.

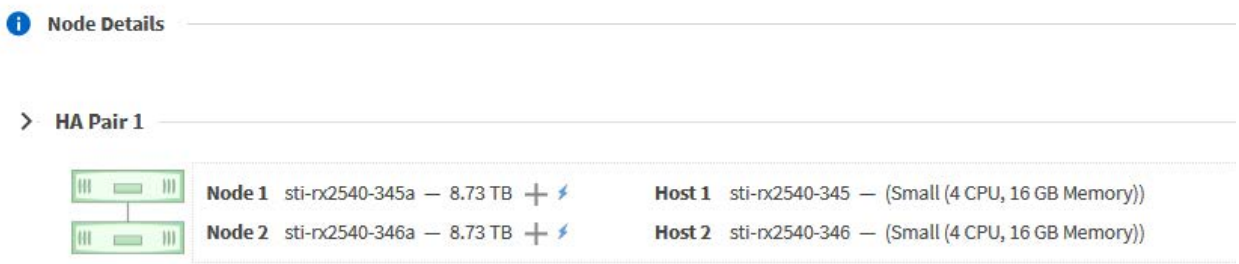
   You should update the disk path and any other configuration information as needed.

```
<disk type='block' device='lun'>
  <driver name='qemu' type='raw' cache='directsync'/>
  <source dev='/dev/disk/by-id/ata-
Micron_5100_MTFDDAK960TCC_171616D35277'/>
  <backingStore/>
  <target dev='sde' bus='scsi'/>
  <alias name='scsi0-0-0-4'/>
  <address type='drive' controller='0' bus='0' target='0' unit='4'/>
</disk>
```

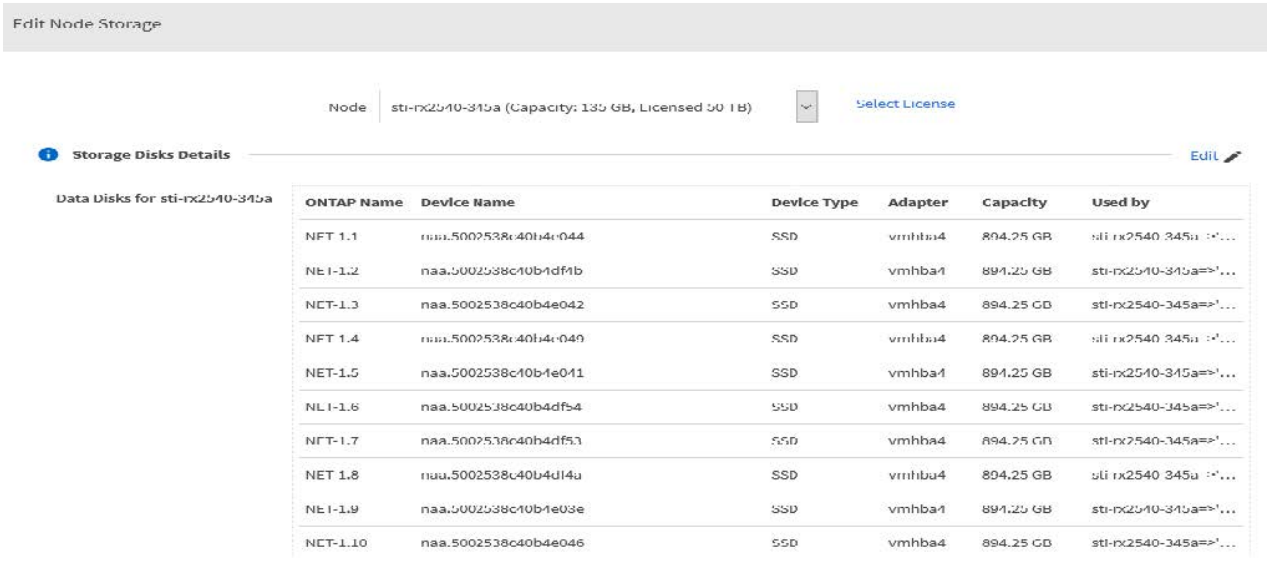
ESXi

Steps

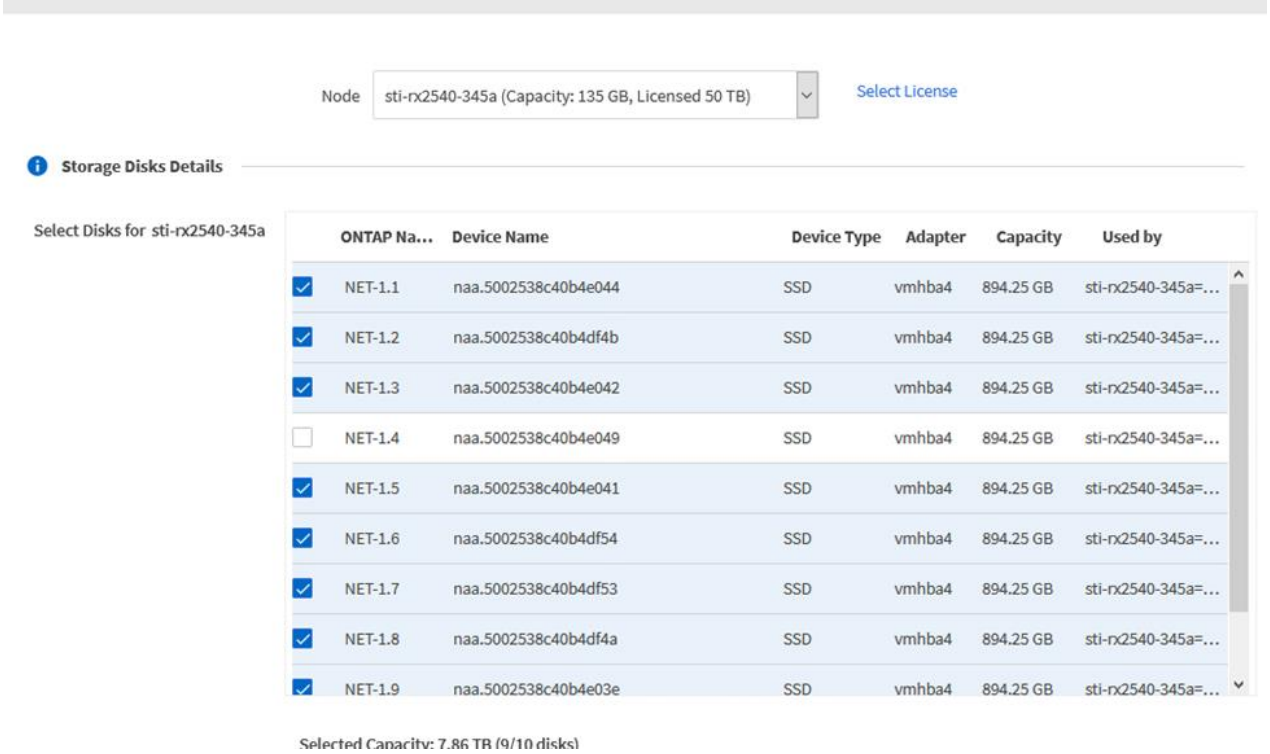
1. Sign in to the Deploy web user interface using the administrator account.
2. Select the **Clusters** tab and select the relevant cluster.



3. Select **+** to expand the storage view.

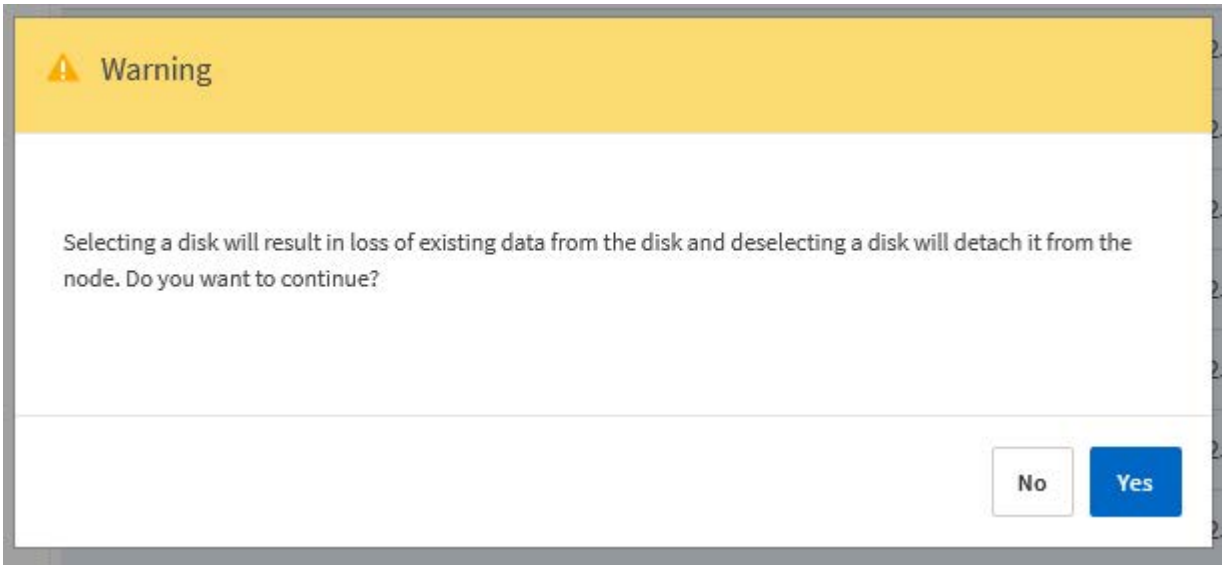


4. Select **Edit** to make changes to the attached disks and uncheck the failed drive.



5. Provide the cluster credentials and select **Edit Storage**.

6. Confirm the operation.



Add the new spare drive

After you remove the failed drive, add the spare disk.

KVM using Deploy

Attaching a disk using Deploy

You can attach a disk to a KVM host as part of replacing a disk or to add more storage capacity.

Before you begin

You must have the ONTAP Select and ONTAP Select Deploy administrator account credentials.

The new disk must be physically installed on the KVM Linux host.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Select the **Clusters** tab at the top of the page and select the desired cluster from the list.
3. Select **+** next to the desired HA pair or node.

   If the option is disabled, Deploy is currently refreshing the storage information.

4. Select **Edit Storage** on the **Edit Node Storage** page.
5. Select the disks to be attached to the node, enter the ONTAP administrator credentials, and select **Edit Storage** to apply the changes.
6. Select the **Events** tab to monitor and confirm the attach operation.
7. Examine the node storage configuration to confirm that the disk is attached.

KVM using CLI

After you identify and remove the failed drive, you can attach a new drive.

Steps

1. Attach the new disk to the virtual machine.

```
virsh attach-disk --persistent /PATH/disk.xml
```

Results

The disk is assigned as a spare and is available to ONTAP Select. It may take a minute or longer for the disk to become available.

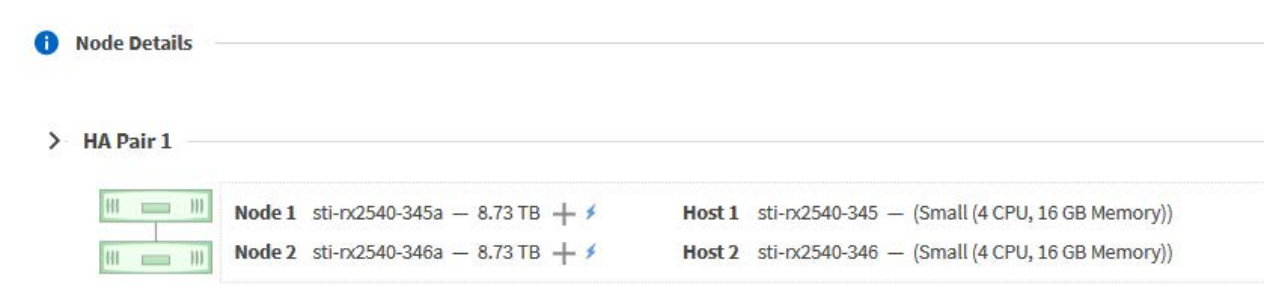
After you finish

Because the node configuration has changed, you should perform a cluster refresh operation using the Deploy administration utility.

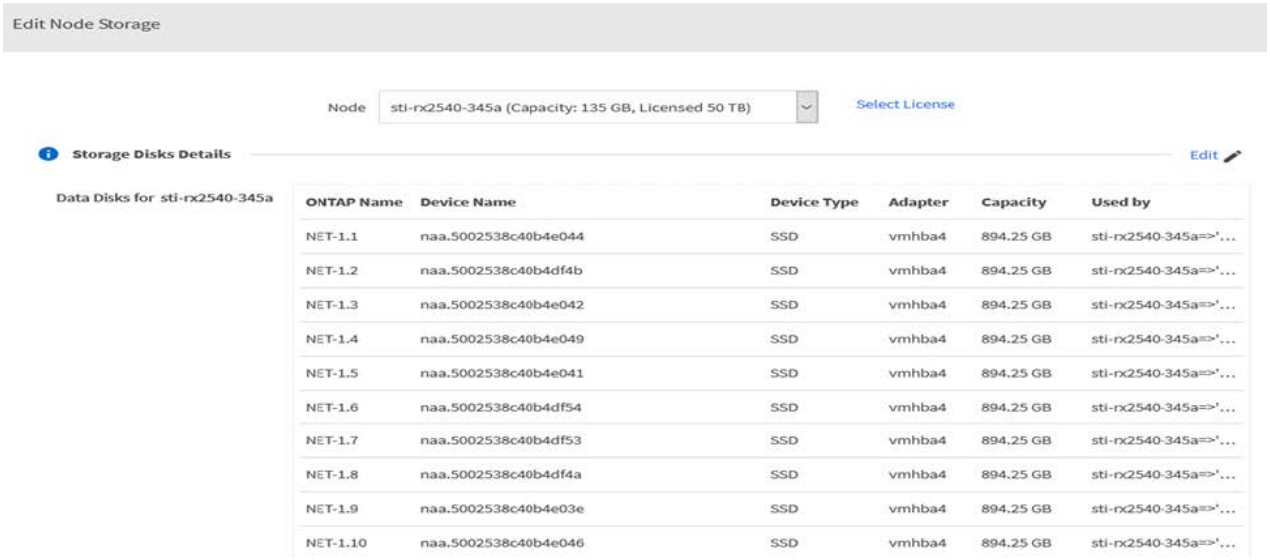
ESXi

Steps

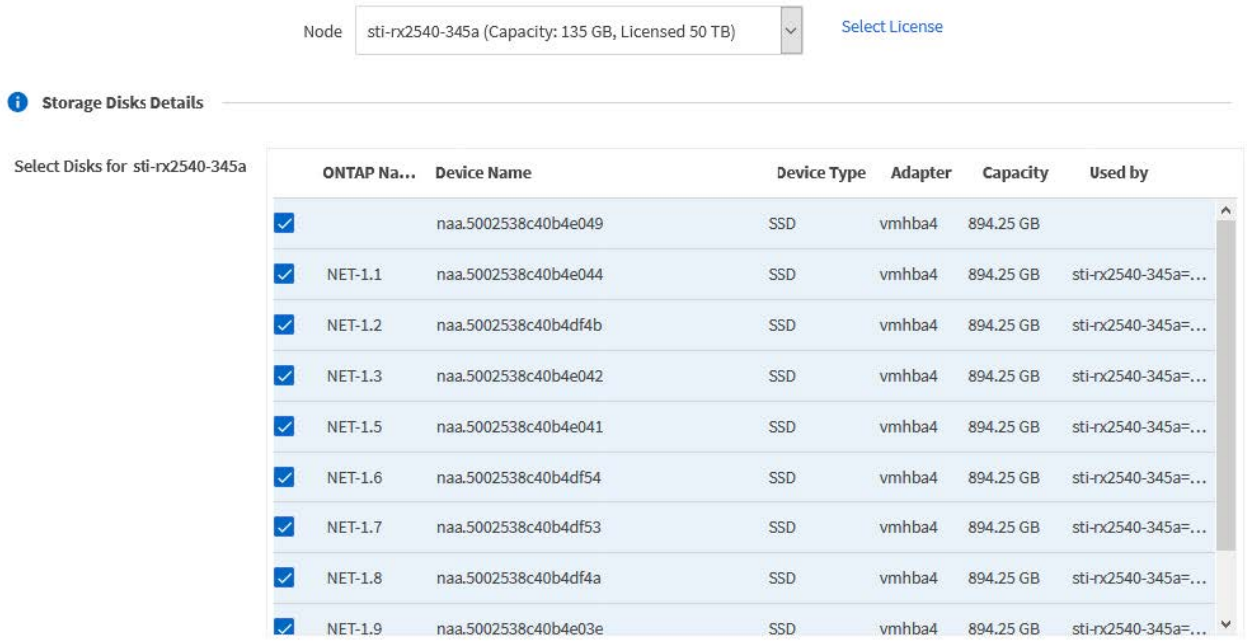
1. Sign in to the Deploy web user interface using the administrator account.
2. Select the **Clusters** tab and select the relevant cluster.



3. Select **+** to expand the storage view.

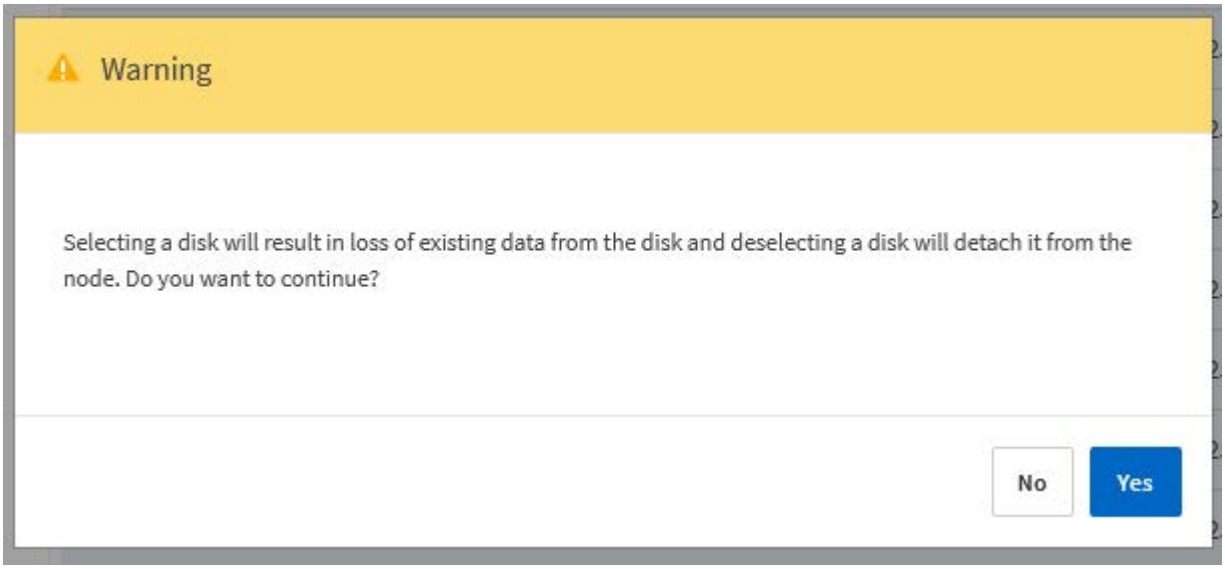


4. Select **Edit** and confirm that the new drive is available and select it.



5. Provide the cluster credentials and select **Edit Storage**.

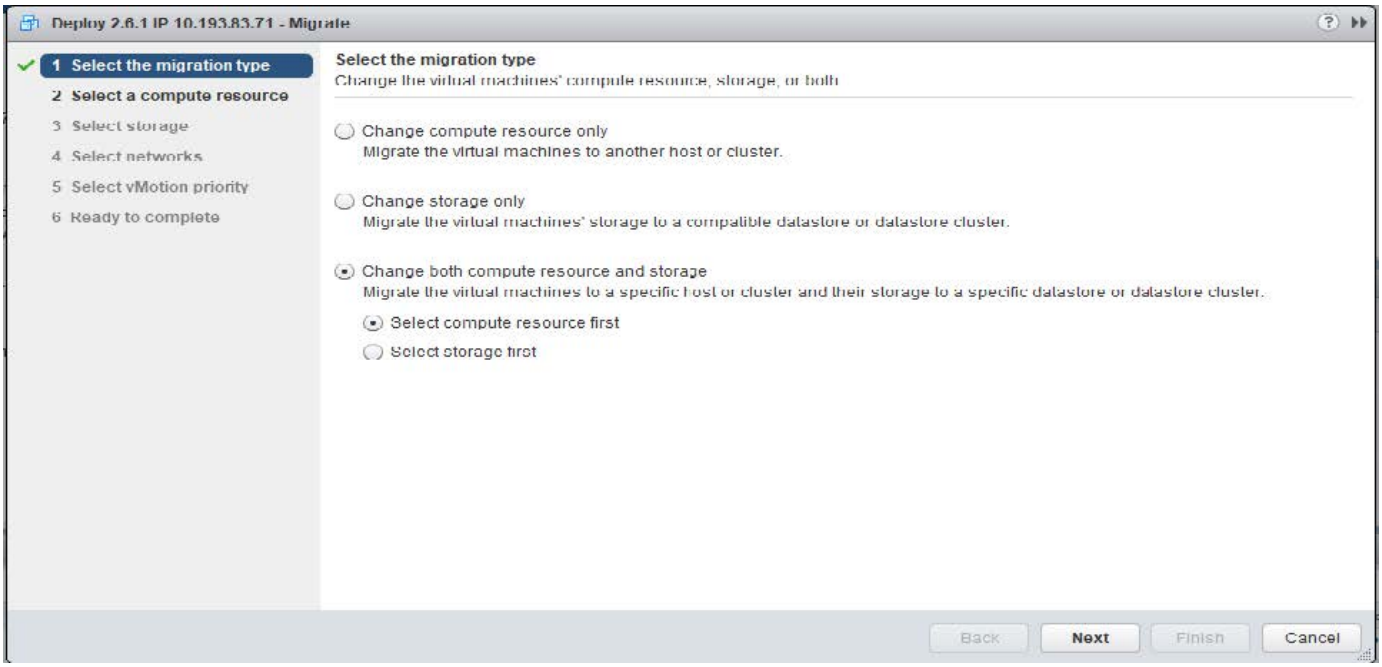
6. Confirm the operation.



Upgrade to VMFS6 using Storage vMotion

VMware does not support an in-place upgrade from VMFS 5 to VMFS 6. You can use Storage vMotion to transition from a VMFS 5 datastore to a VMFS 6 datastore for an existing ONTAP Select node.

For ONTAP Select virtual machines, Storage vMotion can be used for single-node and multi-node clusters. It can be used for both storage-only as well as compute and storage migrations.



Before you begin

Make sure the new host can support the ONTAP Select node. For example, if a RAID controller and DAS storage are used on the original host, a similar configuration should exist on the new host.

Severe performance issues can result if the ONTAP Select VM is rehosted in an unsuitable environment.

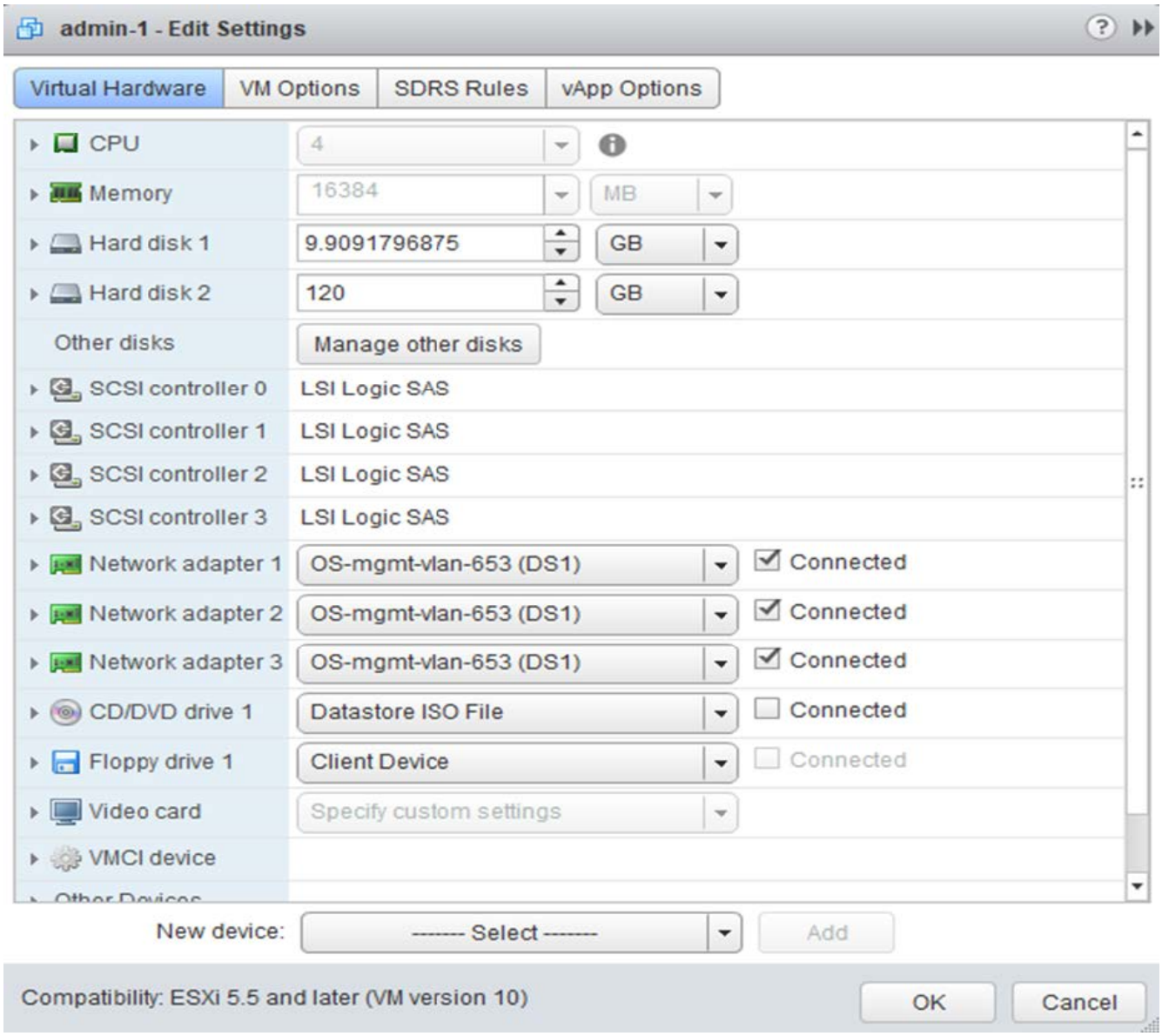
Steps

1. Shut down the ONTAP Select virtual machine.

   If the node is part of an HA pair, perform a storage failover first.

2. Clear the **CD/DVD drive** option.

   This step does not apply if you installed ONTAP Select without using ONTAP Deploy.



3. After the Storage vMotion operation completes, power on the ONTAP Select virtual machine.

   If this node is part of an HA pair, you can perform a manual giveback.

4. Perform a `cluster refresh` operation using the Deploy utility and confirm it is successful.
5. Back up the Deploy utility database.

After you finish

When the Storage vMotion operation completes, you should use the Deploy utility to perform a `cluster refresh` operation. The `cluster refresh` updates the ONTAP Deploy database with the new location of the ONTAP Select node.

ONTAP Select licenses

There are several related tasks you can perform as part of administering the ONTAP Select licenses.

Manage the capacity tier licenses

You can add, edit, and delete ONTAP Select capacity tier licenses as needed.

Steps

1. Sign in to the Deploy utility through the web interface using the administrator account.
2. Click the **Administration** tab at the top of the page.
3. Click **Licenses** and click **Capacity Tier**.
4. Optionally click **Filter** and to limit the licenses displayed.
5. To replace an existing license; select a license, click ⋮, and select **Update**.
6. To add a new license, click **Add** at the top of the page and then click **Upload License(s)** and select a license file from your local workstation.

Manage the capacity pool licenses

You can add, edit, and delete ONTAP Select capacity pool licenses as needed.

Steps

1. Sign in to the Deploy utility through the web interface using the administrator account.
2. Click the **Administration** tab at the top of the page.
3. Click **Licenses** and click **Capacity Pools**.
4. Optionally click **Filter** and to limit the licenses displayed.
5. Optionally select a license and click ⋮ to manage an existing license.
6. To add a new license or renew an existing license, click **Add** at the top of the page and then click **Upload License(s)** and select a license file from your local workstation.
7. To see a list of the capacity pools:
   a. Click **Summary**.
   b. Select and expand a pool to see the clusters and nodes leasing storage from the pool.
   c. View the current status of the license under **License Information**.
   d. You can change the duration of the leases issued for the pool under Lease expiration.
8. To see a list of the clusters:
   a. Click **Details**.
   b. Select and expand the cluster to see storage utilization.

Reinstall a capacity pool license

Every active capacity pool license is locked to a specific License Manager instance, which is contained within an instance of the Deploy administration utility. If you are using a capacity pool license and then restore or recover the Deploy instance, the original license is no longer valid. You must generate a new capacity license file, and then install the license to the new Deploy instance.

Before you begin

- Determine all the capacity pool licenses used by the original Deploy instance.
- If you restore a backup as part of creating the new Deploy instance, determine if the backup is current and up-to-date.

- Locate the ONTAP Select nodes that were most recently created by the original Deploy instance (only if an up-to-date backup from the original Deploy instance is not restored to the new Deploy instance).
- Restore or recreate the Deploy instance

About this task

At a high level, this task is composed of three parts. You must regenerate and install all the capacity pool licenses used by the Deploy instance. After all the licenses have been reinstalled to the new Deploy instance, you can reset the serial sequence number if needed. Finally, if the Deploy IP address has changed, you must update every ONTAP Select node that uses a capacity pools license.

Steps

1. Contact NetApp support and have all the capacity pool licenses for the original Deploy instance unbound and unregistered.
2. Acquire and download a new license file for each of the capacity pool licenses.

   See Acquire a capacity pool license for more information.

3. Install the capacity pool licenses at the new Deploy instance:
   a. Sign in to the Deploy utility web user interface using the administrator account.
   b. Click the **Administration** tab at the top of the page.
   c. Click **Licenses** and then click **Capacity Pool**.
   d. Click **Add** and then **Upload License(s)** to select and upload the licenses.
4. If you created the new Deploy instance without restoring a backup, or you used a backup that was not current and up-to-date, you must update the serial sequence number:
   a. Sign in to the Deploy utility command line interface using the administrator account.
   b. Display the serial number for a node most recently created by the original Deploy instance:

      ```
      node show -cluster-name CLUSTER_NAME -name NODE_NAME -detailed
      ```

   c. Extract the last eight digits from the twenty-digit node serial number to obtain the last serial sequence number used by the original Deploy instance.
   d. Add 20 to the serial sequence number to create the new serial sequence number.
   e. Set the serial sequence number for the new Deploy instance:

      ```
      license-manager modify -serial-sequence SEQ_NUMBER
      ```

5. If the IP address assigned to the new Deploy instance is different than the IP address of the original Deploy instance, you must update the IP address at every ONTAP Select node that uses a capacity pools license:
   a. Sign in to the ONTAP command line interface of the ONTAP Select node.
   b. Enter advanced privilege mode:

      ```
      set adv
      ```

   c. Display the current configuration:

      ```
      system license license-manager show
      ```

   d. Set the License Manager (Deploy) IP address used by the node:

```
system license license-manager modify -host NEW_IP_ADDRESS
```

Convert an evaluation license to a production license

You can upgrade an ONTAP Select evaluation cluster to use a production capacity tier license with the Deploy administration utility.

Before you begin

- Each node must have enough storage allocated to support the minimum required for a production license.
- You must have capacity tier licenses for each node in the evaluation cluster.

About this task

Performing a modification of the cluster license for a single-node cluster is disruptive. However, this is not the case with a multi-node cluster because the conversion process reboots each node one at a time to apply the license.

Steps

1. Sign in to the Deploy utility web user interface using the administrator account.
2. Click the **Clusters** tab a the top of the page and select the desired cluster.
3. At the top of the cluster details page, click **Click here** to modify the cluster license.

   You can also click **Modify** next to evaluation license in the **Cluster Details** section.
4. Select an available production license for each node or upload additional licenses as needed.
5. Provide the ONTAP credentials and click **Modify**.

   The license upgrade for the cluster can take several minutes. Allow the process to complete before leaving the page or making any other changes.

After you finish

The twenty-digit node serial numbers originally assigned to each node for the evaluation deployment are replaced by the nine-digit serial numbers from the production licenses used for the upgrade.

Manage an expired capacity pool license

Generally, when a license expires, nothing happens. However, you cannot install a different license because the nodes are associated with the expired license. Until you renew the license, you should *not* do anything that would bring the aggregate offline, such as a reboot or failover operation. The recommended action is to expedite the license renewal.

For more information about ONTAP Select and license renewal, see the Licenses, installation, upgrades, and reverts section in the FAQ.

Manage add-on licenses

For the ONTAP Select product, add-on licenses are applied directly within ONTAP and are not managed through ONTAP Select Deploy. See Manage licenses overview (cluster administrators only) and Enable new features by adding license keys for more information.

Copyright information

Trademark information