Physical Resources

Physical Resources

The **Physical Resources** menu option displays a summary of your physical resources and customizable reports. You can view or manage the following physical resources:

- Volume Groups
- vFilers
- SVMs
- VLANs
- Servers

- Service Profiles
- VNX LUNs
- Block Storage Pools
- RAID Groups
- File Storage Pools
- VNX Volumes
- Rack Servers
- CloudSense Reports

Volume Groups

Invicta volume groups combine the physical disks or drives that are mounted on your system into a single administrative unit. Logical volumes are created on top of the volume groups to provide flexibility for managing physical resources. You can view the Volume Groups report by choosing **Volume Groups** under **Physical Resources**.

The Volume Groups report displays all available volume groups, as well as following information:

- Account Name
- Volume Group Name
- Size (GB)
- Size Available (GB)
- Status
- SSNs
- Group/User

vFilers

vFilers are NetApp ONTAP 7-mode virtual containers that are deployed on physical storage arrays, creating multiple instances within controllers. They are used to partition the storage and network resources of a single storage system, providing the appearance of multiple storage systems on the network. You can view the vFilers report by choosing **vFilers** under **Physical Resources**.

The vFiler report displays all available vFilers, as well as the following information:

- Account Name
- Filer
- Name
- IP Space
- IP Address

- Subnet mask
- DNS Name
- DNS Server
- Admin Host
- UUID
- Group/User

You can view additional details about a vFiler by clicking the row with the vFiler and clicking **View Details**.

Permissions Required for vFilers

The following table shows a list of the available NetApp vFiler actions and permissions required:

Task	End User Permissions
Viewing vFiler Details, on page 3	Default
Setting up a vFiler, on page 4	Additional permissions required
Setting up CIFS on a vFiler, on page 4	Additional permissions required

Viewing vFiler Details

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler that you want to view.

Step 4 Click **View Details** to view the following information about the vFiler:

- Storage Summary—Displays an overview report of the vFiler.
- Volumes—Displays all the volumes associated with the vFiler. The information for each volume includes the account name, filer name, vFiler name, name, type, containing aggregate, state, and resource usage data.
- SnapMirrors—Displays the SnapMirrors associated with the vFiler. SnapMirrors replicate snapshots between two vFilers. The information for each SnapMirror includes the account name, filer name, source location, destination location, state, transfer statistics, contents, and the base snapshot.

Setting up a vFiler

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler that you want to set up.

Step 4 Click **Setup**.

Step 5 On the **Setup vFiler** screen, complete required fields, including the following:

a) From the **Interface Name** drop-down list, choose a VLAN interface.

b) Check the protocols that you want the vFiler to support.
The vFiler can support NFS, CIFS, and iSCSI protocols.

Step 6 Click **Submit**.

Setting up CIFS on a vFiler

NetApp vFilers support NFS, iSCSI, and CIFS protocols. You can set up CIFS vFilers using the following procedure.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler on which you want to set up CIFS.

Step 4 Click **Setup CIFS**.

Step 5 On the **Setup CIFS** screen, complete required fields, including the following:

a) From the **Authentication** drop-down list, choose the authentication style.
The authentication style determines the method by which clients are authenticated when connecting to the CIFS server.

b) From the **Security Style** drop-down list, choose **NTFS** or **Multi-Protocol**.
The security style determines whether the CIFS service supports multiprotocol access.

c) In the **Organization Unit** field, enter the name of the organization unit that the CIFS service becomes a member of.

Step 6 Click **Submit**.

vFiler Volumes

You can view the details and manage the volumes associated with a vFiler. You can view the vFiler Volumes report by choosing **vFiler Volumes** from the vFilers details page.

The vFiler Volumes report displays all the volumes associated with a vFiler, as well as the following information:

- Account Name
- Filer Name
- vFiler Name
- Name
- Type
- Containing Aggregate
- Available, Used, and Total space (GB)
- Percentage Used
- Space Guarantee
- Snapshot Reserved
- Dedup Enabled
- Storage Savings and Storage Efficiency
- Blocks Reserved
- Export Path
- CIFS Share Name
- Security Style
- Mirror Status

You can view additional details about a vFiler volume by clicking the row with the vFiler volume and clicking **View Details**.

Permissions Required for vFiler Volumes

The following table shows a list of the available vFiler volume actions and permissions required:

Task	End User Permissions
Viewing vFiler Volume Details, on page 7	Default

Task	End User Permissions
Creating a vFiler Volume, on page 8	Additional permissions required
Resizing a vFiler Volume, on page 8	Additional permissions required
Taking a vFiler Volume Offline or Online, on page 9	Additional permissions required
Enabling and Disabling Deduplication on a vFiler Volume, on page 9	Additional permissions required
Exporting a vFiler Volume Using NFS, on page 10	Additional permissions required
Creating a vFiler Volume Snapshot, on page 11	Additional permissions required
Resizing the Snapshot Reserve for a vFiler Volume, on page 11	Additional permissions required
Creating a CIFS Share on a vFiler Volume, on page 12	Additional permissions required
Setting CIFS Share Access on a vFiler Volume, on page 13	Additional permissions required
Creating a Qtree on a vFiler Volume, on page 14	Additional permissions required

vFiler Volume LUNs

You can view the logical unit numbers (LUNs) that are associated with an vFiler volume by selecting a volume and viewing the details for the volume.

The LUNs report displays information about the vFiler LUN:

- Account Name
- Filer Name
- Name
- Type
- Containing Aggregate
- State
- Available (GB)
- Used (GB)
- Total (GB)
- Percentage Used

- Space Guarantee
- Snapshot Reserved
- Dedup Enabled
- Storage Savings
- Storage Efficiency

You can view the overview details and perform the following actions on a LUN associated with a vFiler volume:

- Create
- Offline/Online
- Unmap iGroup
- Map iGroup
- Resize
- Move
- Clone
- Modify ID
- Delete

To access these options, your administrator must provide permission by enabling the appropriate End User Self-Service option in your group's VDC.

The actions are also available when viewing LUNs associated with the SVM. See SVM LUNs, on page 33.

Viewing vFiler Volume Details

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler associated with the volume that you want to view.

Step 4 Click **View Details**.

Step 5 On the detail page for the vFiler, click **Volumes**.

Step 6 Click the row with the volume that you want to view.

Step 7 Click **View Details** to view the details about the vFiler infrastructure storage volume.
The infrastructure storage volume report displays information including the associated vFiler, path, mode, storage capacity, share state, and multi-protocol type.

Creating a vFiler Volume

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler on which you want to create a volume.

Step 4 Click **View Details**.

Step 5 On the detail page for the vFiler, click **Volumes**.

Step 6 Click **Create**.

Step 7 On the **Create Flexible Volume** screen, complete the required fields, including the following:

a) Check the aggregate account under which you want to create the volume.

b) From the **Space Guarantee** drop-down list, choose the guarantee type for the volume.
The space guarantee determines how space for a volume is allocated from its containing aggregate.

Step 8 Click **Create**.

Resizing a vFiler Volume

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler associated with the volume that you want to resize.

Step 4 Click **View Details**.

Step 5 On the detail page for the vFiler, click **Volumes**.

Step 6 Click the row with the volume that you want to resize.

Step 7 From the **More Actions** drop-down list, choose **Resize**.

Step 8 On the **Resize Volume** screen, complete the required fields, including the following:

a) Enter the new volume size.

b) From the **Size Unit** drop-down list, choose the size unit for the volume.

c) Check **File System Size Fixed** if you want the associated file system to remain the same size.
If this option is checked, the file system does not grow or shrink when a volume is added or removed.

Step 9 Click **Resize**.

Taking a vFiler Volume Offline or Online

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler associated with the volume that you want to take offline or bring online.

Step 4 Click **View Details**.

Step 5 On the detail page for the vFiler, click **Volumes**.

Step 6 Click the row with the volume that you want to take offline or bring online.

Step 7 Click one of the following:

- **Offline**
- **Online**

Step 8 Click **Submit**.

Enabling and Disabling Deduplication on a vFiler Volume

You can enable or disable deduplication on vFiler volume. Deduplication is a method of reducing disk space usage by eliminating duplicate blocks on a vFiler volume, where only a single instance of each unique data block is stored.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **vFilers**.
Step 3 Click the row with the vFiler associated with the volume on which you want to enable or disable deduplication.
Step 4 Click **View Details**.
Step 5 On the detail page for the vFiler, click **Volumes**.
Step 6 Click the row with the volume on which you want to enable or disable deduplication.
Step 7 From the **More Actions** drop-down list, choose one of the following:

- **Dedup On**
- **Dedup Off**

Step 8 Click **Enable** or **Disable**.
On the **Volumes** page, the **Dedup Enabled** field changes to Yes or No depending on the action performed.

Exporting a vFiler Volume Using NFS

You can export a vFiler volume as a file through NFS.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **vFilers**.
Step 3 Click the row with the vFiler associated with the volume that you want to export using NFS.
Step 4 Click **View Details**.
Step 5 On the detail page for the vFiler, click **Volumes**.
Step 6 Click the row with the volume that you want to export using NFS.
Step 7 From the **More Actions** drop-down list, choose **NFS Export**.
Step 8 On the **NFS Export** screen, complete the required fields, including the following:
a) In the **Export Path** field, enter the export path where the volume is going to be mounted in the UNIX environment.
b) Check **nosuid** to prohibit suid programs to operate off the NFS file system.
Step 9 Click **Export**.

Creating a vFiler Volume Snapshot

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler associated with the volume of which you want to take a snapshot.

Step 4 Click **View Details**.

Step 5 On the detail page for the vFiler, click **Volumes**.

Step 6 Click the row with the volume of which you want to take a snapshot.

Step 7 From the **More Actions** drop-down list, choose **Snapshot**.

Step 8 On the **Create Snapshot** screen, complete the required fields, including the following:

a) Check **Is Valid LUN Clone Snapshot** if SnapVault is used to request the action so that all backup snapshots for the LUN clones are locked.
This ensures the consistency of the snapshot.

b) Check **Async** to create the snapshot asynchronously.

Step 9 Click **Create**.

Resizing the Snapshot Reserve for a vFiler Volume

You can resize the snapshot space allocated on a volume. The snapshot reserve within a volume can be defined in terms of percentage.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **vFilers**.
Step 3 Click the row with the vFiler associated with the volume for which you want to resize the snapshot reserve.
Step 4 Click **View Details**.
Step 5 On the detail page for the vFiler, click **Volumes**.
Step 6 Click the row with the volume for which you want to resize the snapshot reserve.
Step 7 From the **More Actions** drop-down list, choose **Resize Snapshot**.
Step 8 On the **Resize Snapshot Reserve** screen, enter the new percentage of volume space to reserve for snapshots.
Step 9 Click **Resize**.

Creating a CIFS Share on a vFiler Volume

You can create a CIFS share on a vFiler volume. A CIFS share is a named access point on a volume that enables CIFS clients to access files on a file server.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **vFilers**.
Step 3 Click the row with the vFiler associated with the volume on which you want to create a CIFS share.
Step 4 Click **View Details**.
Step 5 On the detail page for the vFiler, click **Volumes**.
Step 6 Click the row with the volume on which you want to create a CIFS share.
Step 7 From the **More Actions** drop-down list, choose **Create CIFS Share**.
Step 8 On the **Add CIFS Share** screen, enter the new share name and any applicable comments.
Step 9 Click **Share**.

What to Do Next

Set the access permissions for the CIFS share. See Setting CIFS Share Access on a vFiler Volume, on page 13.

Setting CIFS Share Access on a vFiler Volume

Once you create a CIFS share on a vFiler volume, you can set the share access for selected user roles and groups. You can set the share access to one of the following:

- Read
- Change
- Full Control
- No Access

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler associated with the volume on which you want to set CIFS share access.

Step 4 Click **View Details**.

Step 5 On the detail page for the vFiler, click **Volumes**.

Step 6 Click the row with the volume on which you want to set CIFS share access.

Step 7 From the **More Actions** drop-down list, choose **Set CIFS Share Access**.

Step 8 On the **Set CIFS Share Access** screen, complete the required fields, including the following:

a) From the **Select Role** drop-down list, choose a role to provide permissions for the CIFS share directory.
b) In the **Role ID** field, enter the domain user name or group name.
c) From the **Access Type** drop-down list, choose the type of access permission for the user or group.

Step 9 Click **Submit**.

Creating a Qtree on a vFiler Volume

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **vFilers**.
Step 3 Click the row with the vFiler associated with the volume on which you want to create a qtree.
Step 4 Click **View Details**.
Step 5 On the detail page for the vFiler, click **Volumes**.
Step 6 Click the row with the volume on which you want to create a qtree.
Step 7 From the **More Actions** drop-down list, choose **Create QTree**.
Step 8 On the **Create QTree** screen, enter the qtree name.
Step 9 Click **Create**.

SnapMirrors

NetApp SnapMirror software is an enterprise-level disaster recovery and data distribution solution. SnapMirror is a data replication feature of Data ONTAP that mirrors data to one or more network filers at high speed over LAN or WAN connections. You can view the SnapMirrors report by choosing **SnapMirrors** from the vFilers details page.

The SnapMirrors report displays all the SnapMirrors associated with a vFiler, as well as the following information:

- Account Name
- File Name
- Source and Destination Location
- Status
- State
- Last Transfer Type, Size, and Duration
- Transfer Progress
- Current Transfer Type and Error
- Lag Time
- Mirror Time Stamp
- Contents
- Base Snapshot

You can view scheduled SnapMirror relationships and status history by clicking on the row with the SnapMirror and clicking **View Details**.

Permissions Required for SnapMirrors

The following table shows a list of the available SnapMirror actions and permissions required:

Task	End User Permissions
Viewing SnapMirror Details, on page 15	Default

Viewing SnapMirror Details

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **vFilers**.

Step 3 Click the row with the vFiler associated with the SnapMirror that you want to view.

Step 4 Click **View Details**.

Step 5 On the detail page for the vFiler, click **SnapMirrors**.

Step 6 Click the row with the SnapMirror that you want to view.

Step 7 Click **View Details** to view the following information about the SnapMirror:

- Schedules—Displays scheduled SnapMirror relationships. The information includes the account name, the filer name, the source name, the destination location, the replication time, schedule duration information, and the max transfer rate.
- Status History—Displays the status of the schedules for the selected SnapMirror relationship.

Storage Virtual Machines

Storage Virtual Machines (SVMs), formerly known as NetApp virtual storage servers (Vservers), are virtualized servers that support multiple protocols and unified storage. SVMs securely isolate the shared virtualized data storage and network, and each SVM appears as a single dedicated server to the clients.

SVMs provide data access to clients without regard to physical storage or controller, similar to any storage system. SVMs use the storage and network resources of the cluster, but they contain volumes and logical interfaces (LIFs) that are exclusive to each SVM.

Each SVM contains at least one volume and one logical interface, and each SVM has a separate administrator authentication domain and can be managed independently by an SVM administrator. An SVM administrator can manage an SVM and its resources, such as volumes, protocols, and services, depending on the capabilities assigned by the cluster administrator.

Each cluster must have at least one SVM to serve data. Multiple SVMs can coexist in a single cluster without being bound to any single node in a cluster, but they must be bound to the physical cluster on which they exist.

You can view the SVMs report by choosing **SVMs** under **Physical Resources**. The SVMs report displays all available SVMs, as well as the following information:

- Account Name
- Cluster Name
- Name
- Type
- State
- NFS Service Status
- Root Volume
- Aggregate
- LIFs
- Max Volumes
- Allowed Protocols
- Antivirus On Access Policy
- Quota Policy
- Name Service Switch
- Name Mapping Switch
- Node Name
- Group/User
- Tag

You can view additional details about an SVM by clicking the row with the SVM and clicking **View Details**.

Permissions Required for Storage Virtual Machines

The following table shows a list of the available SVM management actions and permissions required:

Task	End User Permissions
Viewing SVM Details, on page 17	Default

Viewing SVM Details

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM that you want to view.

Step 4 Click **View Details** to view the following information about the SVM:

- Volumes—A volume is a logical disk whose structure is made visible to users when you export the volume to a UNIX host through an NFS mount, or to a Windows host through a CIFS share. A volume is the most inclusive of the logical containers. It can store files and directories, qtrees, and LUNs.
- Volume LIF Association—The Volume LIF Association screen displays the LIFs that are associated with volumes available in the SVM,
- LUNs—A logical unit number (LUN) is used to identify a logical unit, which is a device that is addressed by the SCSI protocol or by similar protocols such as Fibre Channel or iSCSI. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).
- QTrees—A qtree is similar in concept to a partition. It creates a subset of a volume to which a quota can be applied to limit the qtree size. As a special case, a qtree can be the entire volume. A qtree is more flexible than a partition because you can change the size of a qtree at any time.
- Quotas—A quota limits the amount of disk space and the number of files that a particular user or group can consume. A quota can also restrict the total space and files used in a qtree, or the usage of users and groups within a qtree.
- Initiator Groups—Initiator groups (igroups) specify which hosts can access specified LUNs on the storage system. Initiator groups are protocol-specific.
- Initiators—Hosts that can access specified LUNs on the storage system.
- CIFS Shares—The CIFS protocol is used with Microsoft operating systems for remote file operations (mapping network drives), browsing (through the network neighborhood icon), authentication, and remote printer services. The core of native Microsoft networking is built around its CIFS services.
- DNS—You can view the domain, configured name servers, and state of each DNS in the SVM account.
- IP Hostname—The IP address and name of each host in the SVM account.
- SIS Policies—Single Instance Storage policies can be used for compression and/or deduplication.
- Export Rules—Export rules determine how client access requests to volumes are handled.
- Export Policies—Export policies contain one or more export rules.
- Port Sets—A port set consists of a group of Fibre Channel (FC) target ports. You bind a port set to an igroup, to make the LUN available only on a subset of the storage system's target ports. Any host in the igroup can access the LUNs only by connecting to the target ports in the port set.
- WWPN Aliases—A World Wide Port Name (WWPN) is a unique, 64-bit identifier displayed as a 16-character hexadecimal value in Data ONTAP. However, SAN Administrators may find it easier to identify FC ports using an alias instead, especially in larger SANs. You can create multiple aliases for a WWPN, but you cannot use the same alias for multiple WWPNs.

SVM Volumes

You can view the details of the volumes associated with an SVM by choosing **Volumes** on the SVM details page. The Volumes report displays all the volumes associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- SVM
- Name
- Type
- Is SVM Root
- Containing Aggregate
- Node Name
- Status
- Available, Used, and Total space (GB)
- Space Saved by Compression
- Space Saved by Deduplication
- Security Style
- Snapshot Policy
- Export Policy
- Percentage Used
- Space Guarantee
- Snapshot Reserved
- Junction Path
- CIFS Share Name
- Dedupe Enabled
- Group/User

You can view additional details about a volume associated with an SVM by clicking on the row with the volume and clicking **View Details**.

Permissions Required for SVM Volumes

The following table shows a list of the available SVM volume actions and permissions required:

Task	End User Permissions
Viewing SVM Volume Details, on page 20	Default
Creating an SVM Volume, on page 21	Additional permissions required
Taking an SVM Volume Offline or Online, on page 21	Additional permissions required
Resizing an SVM Volume, on page 22	Additional permissions required
Cloning an SVM Volume, on page 22	Additional permissions required
Creating a Multi-Volume Snapshot, on page 23	Additional permissions required
Moving an SVM Volume, on page 23	Additional permissions required
Mounting and Unmounting an SVM Volume, on page 24	Additional permissions required
Enabling and Disabling Deduplication on an SVM Volume, on page 25	Additional permissions required
Starting Deduplication on an SVM Volume, on page 25	Additional permissions required
Stopping Deduplication on an SVM Volume, on page 26	Additional permissions required
Creating a Qtree on an SVM Volume, on page 27	Additional permissions required
Running Inventory Collection on an SVM Volume, on page 27	Additional permissions required
Setting the Snapshot Reserve for an SVM Volume, on page 28	Additional permissions required
Assigning an SVM Volume to a Group, on page 28	Additional permissions required
Unassigning an SVM Volume from a Group, on page 29	Additional permissions required

SVM Volume LUNs

You can view the LUNs that are associated with an SVM volume by selecting a volume and viewing the details for the volume. The LUNs report displays information about the LUN, including the associated SVM and volume name, the LUN ID, state, and capacity details.

You can view the overview details and perform the following actions on a LUN associated with an SVM volume:

- Create
- Delete
- Resize
- Offline/Online
- Map iGroup
- Unmap iGroup
- Toggle Space Reservation

To access these options, your administrator must provide permission by enabling the appropriate End User Self-Service option in your group's VDC.

The actions are also available when viewing LUNs associated with the SVM. See SVM LUNs, on page 33.

Viewing SVM Volume Details

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM associated with the volume that you want to view.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Volumes**.

Step 6 Click the row with the volume that you want to view.

Step 7 Click **View Details** to view the details about the SVM volume.
SVM details include a summary or overview of the SVM Volume, and reports for associated LUNs, qtrees, quotas, and snapshots.

Creating an SVM Volume

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM on which you want to create a volume.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Volumes**.

Step 6 Click **Create Volume**.

Step 7 On the **Create Volume** screen, complete required fields, including the following:

a) From the **Volume Type** drop-down list, choose the volume type.
You can choose from read-write, data-protection, or data-cache.

b) Check the snapshot policy to apply to the volume.

Step 8 Click **Submit**.

Taking an SVM Volume Offline or Online

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM associated with the volume that you want to take offline or bring online.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Volumes**.

Step 6 Click the row with the volume that you want to take offline or bring online.

Step 7 Click one of the following:

- **Offline**
- **Online**

Step 8 Click **Submit**.

Resizing an SVM Volume

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume that you want to resize.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume that you want to resize.
Step 7 From the **More Actions** drop-down list, choose **Resize**.
Step 8 On the **Resize Volume** screen, complete the required fields, including the following:
a) Enter the new volume size.
b) Choose the size unit from the **Size Unit** drop-down list.
Step 9 Click **Resize**.

Cloning an SVM Volume

You can clone an existing SVM Volume to create a copy of the volume with the same qualities. You can choose the parent volume snapshot to apply to the cloned volume.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume that you want to clone.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume that you want to clone.
Step 7 From the **More Actions** drop-down list, choose **Clone Volume**.
Step 8 On the **Clone Cluster Volume** screen, complete the required fields, including the following:
a) In the **Volume Name** field, enter the name for the new volume.

b) Check a parent snapshot to apply to the new volume.

Step 9 Click **Submit**.

Creating a Multi-Volume Snapshot

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM for which you want to create a multi-volume snapshot.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Volumes**.

Step 6 Click **Create Multi-Snapshot**.

Step 7 On the **Create Multi-Volume Snapshot** screen, complete required fields, including the following:

a) Check the volumes that you want to include in the snapshot.

b) In the **Snapshot Name** field, enter a name for the snapshot.

Step 8 Click **Submit**.

Moving an SVM Volume

You can move an SVM volume to a different aggregate within the same SVM to balance storage capacity and improve performance if needed. A volume move does not disrupt client access during the move.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume that you want to move.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume that you want to move.
Step 7 From the **More Actions** drop-down list, choose **Move**.
Step 8 On the **Clone Cluster Volume** screen, choose an aggregate from the **Aggregate Name** drop-down list.
Step 9 Click **Submit**.

Mounting and Unmounting an SVM Volume

You can mount or unmount an SVM volume on or from a specified junction path. The junction path must begin with a forward slash and cannot end with a forward slash. If you unmount a volume, all the data within the junction point is inaccessible to the client. However, the data within the volume is not lost.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume that you want to mount or unmount.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume that you want to mount or unmount.
Step 7 From the **More Actions** drop-down list, choose **Mount** or **Unmount**.
Step 8 If mounting the volume, enter the junction path in the **Junction Path** field.
Step 9 Click **Submit**.

Enabling and Disabling Deduplication on an SVM Volume

You can enable data deduplication on the SVM volume to remove duplicate entries. Deduplication eliminates duplicate data blocks within an SVM volume, and stores only unique data blocks.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume on which you want to enable or disable deduplication.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume on which you want to enable or disable deduplication.
Step 7 From the **More Actions** drop-down list, choose **Enable Dedupe** or **Disable Dedupe**.
Step 8 Click **Submit**.

Starting Deduplication on an SVM Volume

You can start deduplication on an SVM volume. The volume must be online and have deduplication enabled. The deduplication operation fails if there is already another deduplication operation active on the volume. When deduplication is started, a checkpoint is created either at the end of each stage or on an hourly basis. If deduplication is stopped, you can restart deduplication from the execution state saved in the checkpoint.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume on which you want to start deduplication.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume on which you want to start deduplication.
Step 7 From the **More Actions** drop-down list, choose **Start Dedupe**.
Step 8 On the **Start Dedupe** screen, complete the required fields, including the following:
a) From the **Build-metadata** drop-down list, choose **True** to build metadata without sharing, if scanning old data. The **True** option builds deduplication metadata by scanning the entire file system. Once the metadata is built, existing data can be shared with newly written data on subsequent deduplication operations.

b) From the **QoS Policy** drop-down list, choose **background** or **best-effort**.
The default value is **best-effort**. If **best-effort** is specified, the deduplication operation may have some impact on the data that serves client operations. If **background** is specified, the deduplication operation runs with minimum or no impact on the data that serves client operations.

c) From the **Queue-operation** drop-down list, choose **True** to queue the deduplication operation.
The deduplication operation is queued only if another operation is already in progress.

d) From the **Restart-checkpoint** drop-down list, choose **True** to restart from a previous checkpoint.

e) From the **Scan** drop-down list, choose **True** to scan the filesystem to process all existing data.

f) From the **Scan-all** drop-down list, choose **True** to scan the entire volume without applying shared block optimization.

Step 9 Click **Submit**.

Stopping Deduplication on an SVM Volume

You can stop deduplication on all active and queued deduplication operations.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM associated with the volume on which you want to stop deduplication.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Volumes**.

Step 6 Click the row with the volume on which you want to stop deduplication.

Step 7 From the **More Actions** drop-down list, choose **Stop Dedupe**.

Step 8 On the **Stop Dedupe** screen, choose **True** from the **All-operations** drop-down list.

Step 9 Click **Submit**.

Creating a Qtree on an SVM Volume

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume on which you want to create a qtree.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume on which you want to create a qtree.
Step 7 From the **More Actions** drop-down list, choose **Create QTree**.
Step 8 On the **Create QTree** screen, enter a name for the qtree.
Step 9 Click **Submit**.

Running Inventory Collection on an SVM Volume

You can perform an inventory collection at the SVM volume level to discover and retrieve information on all elements associated with the volume.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume on which you want to run a volume inventory collection.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume on which you want to run a volume inventory.
Step 7 From the **More Actions** drop-down list, choose **Inventory**.
Step 8 Click **Submit**.

Setting the Snapshot Reserve for an SVM Volume

You can set the snapshot space allocated on a volume. The snapshot reserve within a volume can be defined in terms of percentage.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume for which you want to set the snapshot reserve.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume for which you want to set the snapshot reserve.
Step 7 From the **More Actions** drop-down list, choose **Set Snapshot Reserve**.
Step 8 On the **Cluster Volume Set Snapshot Reserve** screen, enter the percentage of volume space to reserve for snapshots.
Step 9 Click **Submit**.

Assigning an SVM Volume to a Group

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume that you want to assign to a group.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume that you want to assign to a group.
Step 7 From the **More Actions** drop-down list, choose **Assign to Group**.
Step 8 On the **Assign Volume to Group** screen, check the user group ID to which you want to assign the volume.
Step 9 Click **Submit**.

Unassigning an SVM Volume from a Group

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume that you want to unassign from a group.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume that you want to unassign from a group.
Step 7 From the **More Actions** drop-down list, choose **Unassign from Group**.
Step 8 Click **Submit**.

SVM Volume Snapshots

A snapshot is an image of a volume that captures the state of the filesystem at a point in time. You can use snapshots to back up a file or volume for planned or unplanned recovery. You can create a snapshot, and use the snapshot to restore a volume or file. You can also partially restore a file to restore a database in the LUN without touching other databases stored in the LUN. You can view the Snapshots report by choosing **Snapshots** from the SVM volumes details page.

The Snapshots report displays all the snapshots associated with an SVM volume and the following information:

- Account Name
- Filer Name
- SVM
- Volume Name
- Name
- Busy
- Used Size (MB)
- Total Size (MB)

Permissions Required for SVM Volume Snapshots

The following table shows a list of the available SVM volume snapshot actions and permissions required:

Task	End User Permissions
Creating a Snapshot for an SVM Volume, on page 30	Additional permissions required
Restoring an SVM Volume from a Snapshot, on page 31	Additional permissions required
Using a Snapshot to Restore a File on an SVM Volume, on page 31	Additional permissions required
Using a Snapshot to Partially Restore a File on an SVM Volume, on page 32	Additional permissions required

Creating a Snapshot for an SVM Volume

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM associated with the volume for which you want to create a snapshot.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Volumes**.

Step 6 Click the row with the volume for which you want to create a snapshot.

Step 7 From the **More Actions** drop-down list, choose **View Details**.

Step 8 On the detail page for the volume, click **Snapshots**.

Step 9 Click **Create**.

Step 10 On the **Create Snapshot** screen, complete required fields, including the following:

a) In the **Snapshot Name** field, enter a name for the snapshot.

b) Check **Async** to create the snapshot asynchronously.
Asynchronous mode creates snapshots of the volume periodically.

Step 11 Click **Create**.

Restoring an SVM Volume from a Snapshot

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume that you want to restore from a snapshot.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume that you want to restore from a snapshot.
Step 7 From the **More Actions** drop-down list, choose **View Details**.
Step 8 On the detail page for the volume, click **Snapshots**.
Step 9 Click the row with the snapshot from which you want to restore the volume.
Step 10 Click **Restore Volume**.
Step 11 Click **Submit**.

Using a Snapshot to Restore a File on an SVM Volume

You can restore a single file in an SVM volume to a version saved in a snapshot. You can restore a file over an existing version of the file in the SVM volume or to a different location within the same SVM volume.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume on which you want to restore a file from a snapshot.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume on which you want to restore a file from a snapshot.
Step 7 From the **More Actions** drop-down list, choose **View Details**.
Step 8 On the detail page for the volume, click **Snapshots**.
Step 9 Click the row with the snapshot from which you want to restore a file on the volume.
Step 10 Click **Restore File**.
Step 11 On the **Cluster Volume Snapshot Restore File** screen, complete required fields, including the following:

a) In the **File Path** field, enter the absolute path of the file that you want to restore.
b) In the **Restore Path** field, enter the new restore path for the file.
This option specifies a destination location inside the volume where the file will be restored. If you do not enter a new restore path, the file will be restored at the same location entered in the **File Path** field. The restore path should refer to a location within the same volume that contains the source file.

Step 12 Click **Submit**.

Using a Snapshot to Partially Restore a File on an SVM Volume

You can partially restore a single file in an SVM volume. Partially restoring a file restores a range of bytes in a file from the version of the file saved in the snapshot. This action can be used to restore specific pieces of LUNs and NFS or CIFS container files that are used by a host to store multiple sources of data. If a host is storing multiple user databases in the same LUN, you can partially restore a database in the LUN without touching the other databases.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the volume on which you want to partially restore a file from a snapshot.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Volumes**.
Step 6 Click the row with the volume on which you want to partially restore a file from a snapshot.
Step 7 From the **More Actions** drop-down list, choose **View Details**.
Step 8 On the detail page for the volume, click **Snapshots**.
Step 9 Click the row with the snapshot from which you want to restore a file on the volume.
Step 10 Click **Partial Restore File**.
Step 11 On the **Cluster Volume Snapshot Partial Restore File** screen, complete required fields, including the following:
a) In the **File Path** field, enter the absolute path of the file that you want to restore.
b) In the **Start Byte** field, enter the start byte number.
The start byte number is the starting byte offset in the file to partially restore. The first byte of the file is byte zero. The start byte must be a multiple of 4096. In addition, the start byte must not exceed the size of the source or destination file.
c) In the **Byte Count** field, enter the number of bytes that you want to restore.
The byte count is the total number of bytes to restore, beginning at the start byte. The byte count must be a multiple of 4096. The maximum number of bytes that can be restored is 16 MB. The byte count must not exceed the range of the source or destination file.

Step 12 Click **Submit**.

SVM LUNs

You can view the details of the LUNs associated with an SVM by choosing **LUNs** from the SVM details page. The LUNs report displays all the LUNs associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- SVM
- Volume
- Name
- LUN ID
- Datastore
- Hostnode
- Path
- State
- Read Only
- Size and Sized Used (GB)
- Mapped To
- Space Reservation Enabled
- Share State
- OS Type

You can view additional details about a LUN associated with an SVM by clicking on the row with the LUN and clicking **View Details**.

Permissions Required for SVM LUNs

The following table shows a list of the available SVM LUN actions and permissions required:

Task	End User Permissions
Viewing SVM LUN Details, on page 34	Default
Creating an SVM LUN, on page 35	Additional permissions required
Resizing an SVM LUN, on page 35	Additional permissions required

Task	End User Permissions
Cloning an SVM LUN, on page 36	Additional permissions required
Taking an SVM LUN Offline or Online, on page 37	Additional permissions required
Mapping an SVM LUN to an Initiator Group, on page 37	Additional permissions required
Unmapping an SVM LUN from an Initiator Group, on page 38	Additional permissions required
Toggling the Space Reservation on an SVM LUN, on page 38	Additional permissions required

Viewing SVM LUN Details

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM associated with the LUN that you want to view.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **LUNs**.

Step 6 Click the row with the volume that you want to view.

Step 7 Click **View Details** to view the following information about the SVM LUN:

- Name
- Account name
- IP address
- Pod name
- ID
- Space reservation—If this field is true, space reservation is enabled.
- Mapped—If this field is true, the LUN is mapped.
- Multiprotocol type
- Online—If this field is true, the LUN is online.
- Path
- Staging—If this field is true, the LUN is a staging area LUN.

Creating an SVM LUN

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM on which you want to create a LUN.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **LUNs**.

Step 6 Click **Create LUN**.

Step 7 On the **Create LUN** screen, complete required fields, including the following:

a) From the **Select Volume** drop-down list, choose the volume on which to create the LUN.
b) In the **LUN Name** field, enter the name of the LUN.
c) In the **Size** field, enter the size for the LUN.
d) From the **Size Unit** drop-down list, choose the size unit for the LUN.
e) From the **OS Type** drop-down list, choose the operating system type for the LUN.

Step 8 Click **Submit**.

Resizing an SVM LUN

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM associated with the LUN that you want to resize.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **LUNs**.

Step 6 Click the row with the LUN that you want to resize.

Step 7 From the **More Actions** drop-down list, choose **Resize**.

Step 8 On the **Resize LUN** screen, complete the required fields, including the following:

a) Enter the new LUN size.

b) From the **Size Unit** drop-down list, choose the size unit for the LUN.

Step 9 Click **Submit**.

Cloning an SVM LUN

You can clone an existing SVM LUN to create a copy of the LUN with the same qualities. You can choose a snapshot to apply to the cloned LUN.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM associated with the LUN that you want to clone.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **LUNs**.

Step 6 Click the row with the LUN that you want to clone.

Step 7 From the **More Actions** drop-down list, choose **Clone**.

Step 8 On the **Clone Cluster LUN** screen, complete the required fields, including the following:

a) Check **Snapshot Clone** to choose a snapshot to apply to the new volume.

b) In the **New LUN Name** field, enter the name for the new LUN.

Step 9 Click **Submit**.

Taking an SVM LUN Offline or Online

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the LUN that you want to take offline or bring online.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **LUNs**.
Step 6 Click the row with the LUN that you want to take offline or bring online.
Step 7 Click **Offline/Online**.
Step 8 Click **Submit**.

Mapping an SVM LUN to an Initiator Group

An initiator group (igroup) specifies which initiators can have access to a LUN. When you map a LUN on a storage system to an initiator group, you grant all the initiators in that group access to that LUN.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the LUN that you want to map to an igroup.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **LUNs**.
Step 6 Click the row with the LUN that you want to map to an igroup.
Step 7 From the **More Actions** drop-down list, choose **Map iGroup**.
Step 8 On the **Map LUN to iGroup** screen, complete the required fields, including the following:
a) From the **Initiator Group** drop-down list, choose the igroup to which you want to map the SVM LUN.
b) Check **Specify LUN ID** to specify the LUN ID.
A LUN must have a unique ID so that the host can identify and access the LUN. If a LUN ID is not specified, the system automatically generates a LUN ID.
Step 9 Click **Submit**.

Unmapping an SVM LUN from an Initiator Group

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the LUN that you want to unmap from an igroup.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **LUNs**.
Step 6 Click the row with the LUN that you want to unmap from an igroup.
Step 7 From the **More Actions** drop-down list, choose **UnMap iGroup**.
Step 8 Click **Submit**.

Toggling the Space Reservation on an SVM LUN

You can enable or disable the space reservation setting for an SVM LUN. Enabling the space reservation setting on a LUN reserves the space required for that LUN on the volume. If you disable the reservation setting, the LUN appears to provide more space than the volume can currently provide.

Note If you disable space reservations, write operations to an SVM LUN may fail due to insufficient disk space.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the LUN on which you want to toggle the space reservation.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **LUNs**.
Step 6 Click the row with the LUN on which you want to toggle the space reservation.
Step 7 From the **More Actions** drop-down list, choose **Toggle Space Reservation**.
Step 8 Click **Submit**.

SVM Initiator Groups

An initiator group (igroup) specifies which initiators can have access to a LUN. You can view the details of the initiator groups associated with an SVM by choosing **Initiator Groups** from the SVMs details page. The Initiator Groups report displays all the initiator groups associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- SVM
- Name
- Group Type
- OS Type
- Portset Name

Permissions Required for SVM Initiator Groups

The following table shows a list of the available SVM initiator group actions and permissions required:

Task	End User Permissions
Creating an SVM Initiator Group, on page 40	Additional permissions required
Renaming an SVM Initiator Group, on page 41	Additional permissions required
Binding a Port Set to an SVM Initiator Group, on page 41	Additional permissions required

Task	End User Permissions
Unbinding a Port Set from an SVM Initiator Group, on page 42	Additional permissions required

Creating an SVM Initiator Group

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM on which you want to create an initiator group.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Initiator Groups**.

Step 6 Click **Create**.

Step 7 On the **Create Initiator Group** screen, complete required fields, including the following:

a) In the **Initiator Group Name** field, enter the name of the new initiator group.

b) From the **Group Type** drop-down list, choose the type of initiator group that you want to create. You can create an initiator group that uses either FC or iSCSI connections.

c) From the **OS Type** drop-down list, choose the operating system type for the initiator group.

d) Click the port set to bind to the initiator group.

Step 8 Click **Submit**.

Renaming an SVM Initiator Group

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the initiator group that you want to rename.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Initiator Groups**.
Step 6 Click the row with the initiator group that you want to rename.
Step 7 Click **Rename**.
Step 8 On the **Rename iGroup** screen, enter the new initiator group name.
Step 9 Click **Submit**.

Binding a Port Set to an SVM Initiator Group

After you create a port set, you can bind the port set to an initiator group so that the host knows which ports to access. If you do not bind an initiator group to a port set, and you map a LUN to the initiator group, the initiators in the initiator group will have unrestricted access to the LUN on any port on the storage system.

Note You cannot bind an initiator group to an empty port set. If the port set is empty, the initiators in the initiator group do not have any ports by which to access the LUN.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the initiator group that you want to bind to a port set.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Initiator Groups**.
Step 6 Click the row with the initiator group that you want to bind to a port set.
Step 7 Click **Bind Portset**.
Step 8 On the **Bind Portset to iGroup** screen, choose the port set to bind to the initiator group.
Step 9 Click **Submit**.

Unbinding a Port Set from an SVM Initiator Group

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the initiator group that you want to unbind from a port set.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Initiator Groups**.
Step 6 Click the row with the initiator group that you want to unbind to from a port set.
Step 7 Click **Unbind Portset**.
Step 8 Click **Submit**.

SVM Initiators

An initiator is a host that can access specified LUNs on the storage system. Each initiator is identified by a World Wide Port Name (WWPN). All initiators in the same initiator group must run the same operating system. An initiator cannot be a member of two initiator groups with different operating system types. An initiator also cannot be in multiple initiator groups that are mapped to the same LUN. You can view the Initiators report by choosing **Initiators** from the SVMs details page.

The Initiators report displays all the initiators associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- Name
- Initiator Group
- Group Type
- OS Type

Permissions Required for SVM Initiators

The following table shows a list of the available SVM initiator actions and permissions required:

Task	End User Permissions
Creating an SVM Initiator, on page 43	Additional permissions required

Creating an SVM Initiator

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM on which you want to create an initiator.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Initiators**.

Step 6 Click **Create**.

Step 7 On the **Create Initiator** screen, complete required fields, including the following:

a) In the **Initiator Group Name** field, enter the name of the initiator group to which you want to add the initiator.
b) In the **Initiator Name** field, enter the name of the new initiator.
c) Check the WWPN alias to associate with the initiator.
d) Check **Force** to forcibly add the initiator.

Step 8 Click **Submit**.

SVM CIFS Shares

A CIFS share is a named access point on a volume that enables CIFS clients to access files on a file server. You can view the CIFS Shares report by choosing **CIFS Shares** from the SVMs details page. The CIFS Shares report displays all the CIFS shares associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- Share Name
- Mount Point
- User/Group
- Access Control
- Description

Permissions Required for SVM CIFS Shares

The following table shows a list of the available CIFS share actions and permissions required:

Task	End User Permissions
Creating a CIFS Share on an SVM, on page 44	Additional permissions required
Setting CIFS Share Access on an SVM, on page 45	Additional permissions required

Creating a CIFS Share on an SVM

When you create an SVM CIFS share, you can specify share access. You can specify which users or which group can access the share, and set the control permissions.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM on which you want to create a CIFS share.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **CIFS Shares**.

Step 6 Click **Create**.

Step 7 On the **Create CIFS Share** screen, complete required fields, including the following:

a) From the **Volume Name** drop-down list, choose the volume on which you want to create the CIFS share.

b) Check **Set Share Access** to specify the permission level and users or groups who have access to the CIFS share.

Step 8 Click **Submit**.

Setting CIFS Share Access on an SVM

Once you create a CIFS share on an SVM, you can set the share access for selected user roles and groups. You can set the share access to one of the following:

- Full Control
- Read
- Change
- No Access

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM on which you want to set CIFS share access.
Step 4 Click **View Details**.
Step 5 Click the row with the vFiler associated with the volume on which you want to set CIFS share access.
Step 6 Click **View Details**.
Step 7 On the detail page for the SVM, click **CIFS Shares**.
Step 8 Click the row with the account on which you want to set CIFS share access.
Step 9 Click **Set Share Access**.
Step 10 On the **Create CIFS Share Access** screen, complete the required fields, including the following:
a) From the **Permission** drop-down list, choose the type of access permission for the user or group.
b) In the **User or Group** field, enter the user or group name for which the permissions are listed.
Step 11 Click **Submit**.

SVM SIS Policies

You can define a Single Instance Storage (SIS) policy to perform SIS operations that include compression and deduplication. Data compression can be used on demand, or as a scheduled background operation. The policy can include deduplication, which is a method of reducing disk space usage by eliminating duplicate

data blocks on a FlexVol volume, where only a single instance of each unique data block is stored. You can view the SIS Policies report by choosing **SIS Policies** from the SVMs details page.

The SIS Policies report displays all the SIS policies associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- SVM
- Policy Name
- QoS Policy
- Scheduled
- Enabled
- Duration
- Comment

Permissions Required for SVM SIS Policies

The following table shows a list of the available SVM SIS policy actions and permissions required:

Task	End User Permissions
Creating an SIS Policy for an SVM, on page 46	Additional permissions required

Creating an SIS Policy for an SVM

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM for which you want to create an SIS policy.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **SIS Policies**.

Step 6 Click **Create**.

Step 7 On the **Create SIS Policy on SVM** screen, complete required fields, including the following:

a) From the **Enabled** drop-down list, choose **true** to enable the SIS policy on the SVM.

b) From the **QoS Policy** drop-down list, choose **background** or **best-effort**.

The default value is **best-effort**. If **best-effort** is specified, the deduplication operation may have some impact on the data serving client operations by maximizing the utilization of system resources. If **background** is specified, the deduplication operation runs with minimum or no impact on the data serving client operations.

c) In the **Duration** field, enter the duration in hours for which the scheduled SIS operation runs.
d) In the **Schedule** drop-down list, choose the schedule to apply when the policy is set on a volume.

Step 8 Click **Submit**.

SVM Export Policies

An export policy includes export rules to control client access to volumes. An export policy must exist on an SVM for clients to access data. An export policy must be associated with each volume to configure client access to the volume.

A single SVM can contain multiple export policies. An SVM with multiple volumes can have the following::

- Different export policies assigned to each volume of the SVM for individual client access control to each volume.
- The same export policy assigned to multiple volumes of the SVM for identical client access control without having to create a new export policy for each volume.

You can view the Export Policies report by choosing **Export Policies** from the SVMs details page.

The Export Policies report displays all the export policies associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- SVM
- Policy Name

Permissions Required for SVM Export Policies

The following table shows a list of the available SVM export policy actions and permissions required:

Task	End User Permissions
Creating an Export Policy for an SVM, on page 48	Additional permissions required

Creating an Export Policy for an SVM

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM for which you want to create an export policy.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Export Policies**.
Step 6 Click **Create**.
Step 7 On the **Create Export Policy** screen, enter the export policy name in the **Policy Name** field.
Step 8 Click **Submit**.

What to Do Next

Create an export rule to add to the export policy. See Creating an SVM Export Rule, on page 49.

SVM Export Rules

Export rules determine how to handle the client access requests to volumes. At least one export rule needs to be added to an export policy to allow access to clients. If an export policy contains more than one rule, the rules are processed based on a rule index. You can specify the rule's index number when creating the rule. You can rearrange the order in which the export rules are processed.

The permissions defined in a rule are applied to the clients that match criteria specified in the export rule. You can view the Export Rules report by choosing **Export Rules** from the SVMs details page.

The Export Rules report displays all the export rules associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- Policy Name
- Client Match
- Rule Index
- RO Access Rule
- RW Access Rule
- Access Protocol
- NTFS Unix Secure Ops

- Chown Mode

Permissions Required for SVM Export Rules

The following table shows a list of the available SVM export rule actions and permissions required:

Task	End User Permissions
Creating an SVM Export Rule, on page 49	Additional permissions required

Creating an SVM Export Rule

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM for which you want to create an export rule.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Export Rules**.

Step 6 Click **Create**.

Step 7 On the **Create Export Rule** screen, complete required fields, including the following:

a) From the **Policy Name** drop-down list, choose an export policy to which you want to add the new export rule. The export policy must already be created. See Creating an Export Policy for an SVM, on page 48.

b) From the **Access Protocol** drop-down list, choose an access protocol to which you want to apply the export rule.

c) In the **Client Mach Spec** field, enter the client or clients to which the export rule applies. You can specify the match in any of the following formats:

- As a hostname; for instance, host1
- As an IPv4 address; for instance, 10.1.12.24
- As an IPv4 address with a subnet mask expressed as in bits; for instance, 10.1.12.10/4
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
- As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng
- As a domain name preceded by a period; for instance, .example.com

d) In the **Read Only Access Rule** drop-down list, choose one of the following options to define the security type for read-only access to volumes:

- **Any—**To allow read access to the volume regardless of the security type of the incoming request. The effective security type of the incoming request remains the same.

Note If the security type of the incoming request is AUTH_NONE, read access is granted to the incoming request as an anonymous user.

- **None—**To allow read access to the volume as an anonymous user if the security type of the incoming request is not explicitly listed in the list of values in the read-only rule. The effective security type of the incoming request becomes none.
- **Never—**To not allow any access to the volume regardless of the security type of the incoming request.
- **KRB5—**To allow read access to the volume if the security type of the incoming request is Kerberos 5. The effective security type of the incoming request becomes krb5.
- **NTLM—**To allow read access to the volume if the security type of the incoming request is CIFS NTLM. The effective security type of the incoming request becomes ntlm.
- **Sys—**To allow read access to the volume if the security type of the incoming request is AUTH_SYS. The effective security type of the incoming request becomes sys.

e) In the **Read Write Access Rule** drop-down list, choose one of the following options to define the security type for read-write access to volumes:

- **Any—**To allow read-write access to the volume regardless of the effective security type of the incoming request.
- **None—**To allow read-write access to the volume as an anonymous user if the effective security type of the incoming request is none.

  Note If the effective security type of the incoming request is none, write access is granted to the incoming request as an anonymous user.
- **Never—**To not allow read-write access to the volume regardless of the effective security type of the incoming request.
- **KRB5—**To allow read-write access to the volume if the effective security type of the incoming request is Kerberos 5.
- **NTLM—**To allow read-write access to the volume if the effective security type of the incoming request is CIFS NTLM.
- **Sys—**To allow read-write access to the volume if the effective security type of the incoming request is AUTH_SYS.

f) In the **Rule Index** field, enter the index number of the export rule that specifies order of the rule in the export policy.

Step 8 Click **Submit**.

SVM Snapshot Policies

A snapshot policy automatically manages snapshot policy schedules on the SVM. A snapshot policy can have up to five snapshot policy schedules, and specifies the frequency and the maximum number of automatically created snapshot copies.

A snapshot policy can be used to specify a NetApp SnapMirror label that identifies the snapshots made according to a designated schedule. SnapMirror labels are used to identify snapshots to transfer to SnapVault. If a prefix is specified in the snapshot policy, snapshots are created with the prefix in the snapshot name.

Using prefixes in snapshot names provides more flexibility than using schedule names in naming the automatic snapshots.

You can view the Snapshot Policies report by choosing **Snapshot Policies** from the SVMs details page.

The Snapshot Policies report displays all the snapshot policies associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- SVM
- Name
- Policy Owner
- Enabled
- Total Schedules
- Comment

You can view additional details about a snapshot policy by clicking the row with the snapshot policy and clicking **View Details**.

Permissions Required for SVM Snapshot Policies

The following table shows a list of the available SVM snapshot policy actions and permissions required:

Task	End User Permissions
Viewing SVM Snapshot Policy Details, on page 52	Default
Creating a Snapshot Policy on an SVM, on page 52	Additional permissions required
Enabling and Disabling a Snapshot Policy on an SVM, on page 53	Additional permissions required
Creating a Snapshot Policy Schedule for an SVM Snapshot Policy, on page 53	Additional permissions required

Viewing SVM Snapshot Policy Details

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM associated with the snapshot policy that you want to view.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Snapshot Policies**.

Step 6 Click the row with the snapshot policy that you want to view.

Step 7 Click **View Details** to view the details about the snapshot policy.
The snapshot policy report displays information about associated snapshot policy schedules. The snapshot policy schedule details include the account name, cluster name, SVM, policy name, schedule name, prefix, count, and SnapMirror label.

Creating a Snapshot Policy on an SVM

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM for which you want to create a snapshot policy.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Snapshot Policies**.

Step 6 Click **Create**.

Step 7 On the **Create Snapshot Policy** screen, complete required fields, including the following:

a) From the **Schedule** drop-down list, choose the cron job or schedule interval to add to the policy.
b) In the **Count** field, enter the number of snapshots to retain for the schedule.
c) In the **Prefix** field, enter the prefix text to include in the created snapshot names.
d) Check **Is Enabled** to enable the snapshot policy.

Step 8 Click **Submit**.

Enabling and Disabling a Snapshot Policy on an SVM

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM on which you want to enable or disable a snapshot policy.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Snapshot Policies**.
Step 6 Click the row with the snapshot policy that you want to enable or disable.
Step 7 Click **Enable/Disable**.
Step 8 On the **Enable/Disable Snapshot Policy** screen, check or uncheck **Is Enabled** to enable or disable the snapshot policy.
Step 9 Click **Submit**.

Creating a Snapshot Policy Schedule for an SVM Snapshot Policy

You can create a snapshot policy schedule for a snapshot policy that is associated with an SVM.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with snapshot policy for which you want to create a snapshot policy schedule.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Snapshot Policies**.
Step 6 Click the row with the snapshot policy for which you want to create a snapshot policy.
Step 7 Click **View Details**.
Step 8 On the detail page for the snapshot policy, click **Create**.
Step 9 On the **Add Snapshot Policy Schedule** screen, complete required fields, including the following:
a) From the **Schedule** drop-down list, choose the cron job or schedule interval to add to the policy.
b) In the **Count** field, enter the number of snapshots to retain for the schedule.
c) In the **Prefix** field, enter the prefix text to include in the created snapshot names.
Step 10 Click **Submit**.

SVM Port Sets

A port set consists of a group of Fibre Channel (FC) target ports. You bind a port set to an igroup, to make the LUN available only on a subset of the storage system's target ports. Any host in the igroup can access the LUNs only by connecting to the target ports in the port set.

If an igroup is not bound to a port set, the LUNs mapped to the igroup are available on all of the storage system FC target ports. The igroup controls which initiators LUNs are exported to. The port set limits the target ports on which those initiators have access.

You can view the Portsets report by choosing **Portsets** from the SVMs details page.

The Portsets report displays all the port sets associated with an SVM, as well as following details:

- Account Name
- Cluster Name
- SVM
- Name
- Portset Type
- Total Ports
- Ports

Permissions Required for SVM Port Sets

The following table shows a list of the available SVM port set actions and permissions required:

Task	End User Permissions
Creating an SVM Port Set, on page 55	Additional permissions required
Destroying an SVM Port Set, on page 55	Additional permissions required
Adding a Port to an SVM Port Set, on page 56	Additional permissions required
Removing a Port from an SVM Port Set, on page 56	Additional permissions required

Creating an SVM Port Set

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM on which you want to create a port set.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **Portsets**.

Step 6 Click **Create**.

Step 7 On the **Create Portset** screen, complete required fields, including the following:

a) In the **Portset Name** field, enter the name of the new port set.

b) From the **Portset Type** drop-down list, choose the port set protocol type.
You can choose between the following protocol types:

- **ISCSI**
- **FCP**
- **MIXED**

Step 8 Click **Submit**.

What to Do Next

Add a port to the port set. See Adding a Port to an SVM Port Set, on page 56.

Destroying an SVM Port Set

Note You cannot destroy a port set if the port set is bound to an initiator group. See Unbinding a Port Set from an SVM Initiator Group, on page 42.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with port set that you want to destroy.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Portsets**.
Step 6 Click the row with the port set that you want to destroy.
Step 7 Click **Destroy**.
Step 8 On the **Destroy Portset** screen, check **Force** to forcibly destroy the port set.
If you use the **Force** option, you can destroy the port set even if it is still bound to an igroup.
Step 9 Click **Submit**.

Adding a Port to an SVM Port Set

After you create a port set, you can add FC target ports to the port set.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with the port set to which you want to add a port.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Portsets**.
Step 6 Click the row with the port set to which you want to add a port.
Step 7 Click **Add Port**.
Step 8 On the **Add Port To Portset** screen, choose the LIF identity or port to add to the port set.
A LIF is a logical interface or IP address associated with a physical port.
Step 9 Click **Submit**.

Removing a Port from an SVM Port Set

You can remove an FC port from a port set.

Note You cannot remove the last port in the port set if the port set is bound to an igroup. To remove the last port, first unbind the port set from the igroup, then remove the port. See Unbinding a Port Set from an SVM Initiator Group, on page 42.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **SVMs**.
Step 3 Click the row with the SVM associated with port set from which you want to remove a port.
Step 4 Click **View Details**.
Step 5 On the detail page for the SVM, click **Portsets**.
Step 6 Click the row with the port set from which you want to remove a port.
Step 7 Click **Remove Port**.
Step 8 On the **Remove Port From Portset** screen, choose the port name from the **Port Name** drop-down list.
Step 9 Click **Submit**.

SVM WWPN Aliases

A WWPN is a unique, 64-bit identifier displayed as a 16-character hexadecimal value in Data ONTAP. Your administrators may find it easier to identify FC ports using an alias instead. You can view the details of WWPN aliases associated with an SVM. You can view the WWPN Aliases report by choosing **WWPN Aliases** from the SVMs details page.

The WWPN Aliases report displays all the WWPN aliases associated with an SVM, as well as the following information:

- Account Name
- Cluster Name
- SVM
- WWPN Alias
- WWPN

Permissions Required for SVM WWPN Aliases

The following table shows a list of the available SVM WWPN alias actions and permissions required:

Task	End User Permissions
Creating a WWPN Alias on an SVM, on page 58	Additional permissions required

Creating a WWPN Alias on an SVM

You can create multiple aliases for a WWPN, but you cannot use the same alias for multiple WWPNs.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **SVMs**.

Step 3 Click the row with the SVM for which you want to create a WWPN alias.

Step 4 Click **View Details**.

Step 5 On the detail page for the SVM, click **WWPN Aliases**.

Step 6 Click **Create**.

Step 7 On the **Create WWPN Alias** screen, complete required fields, including the following:

a) In the **WWPN Alias** field, enter the alias text for the WWPN.
The alias can consist of up to 32 characters and can contain only the letters A through Z, numbers 0 to 9, hyphens (-), underscores (_), left braces ({), right braces (}), and periods (.).

b) In the **WWPN** field, enter the Fiber Channel Protocol (FCP) initiator WWPN.

Step 8 Click **Submit**.

What to Do Next

Add a port to the port set. See Adding a Port to an SVM Port Set, on page 56.

VLANs

VLANs are groups of devices on LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on several different LAN segments. VLANs provide logical segmentation of networks by creating separate broadcast domains. A VLAN can span multiple physical network segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

You can view the VLANs report by choosing **VLANs** under **Physical Resources**.

The VLANS report displays all available VLANS and the following information:

- Pod
- Device IP

- VLAN ID
- VLAN Name
- VLAN Status
- Ports
- Group/User

Servers

You can monitor and view the details for all available physical servers. You can view the Servers report by choosing **Servers** under **Physical Resources**.

The Servers report displays all available physical servers, as well as the following information:

- Name
- Model
- Total Memory (MB)
- Associated Status
- Operation Status
- Service Profile
- Power State
- IP Address

Permissions Required for Servers

The following table shows a list of the available server management actions and permissions required:

Task	End User Permissions
Powering a Server On or Off, on page 60	Additional permissions required
Associating a Server with a Service Profile, on page 60	Additional permissions required
Disassociating a Server, on page 60	Additional permissions required
Launching the KVM Console for a Server, on page 61	Additional permissions required

Powering a Server On or Off

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **Servers**.

Step 3 Click the row with the server you want to power on or off.

Step 4 Click one of the following:

- **Power ON**
- **Power OFF**

Step 5 Click **Submit**.

Associating a Server with a Service Profile

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **Servers**.

Step 3 Click the row with the server with which you want to associate a service profile.

Step 4 Click **Associate**.

Step 5 On the **Associate Server** screen, check the profiles that you want to associate with the server.

Step 6 Click **Associate**.

Disassociating a Server

Disassociating a server disassociates it from all associated service profiles.

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **Servers**.
Step 3 Click the row with the server that you want to disassociate.
Step 4 Click **Disassociate**.
Step 5 On the **Disassociate Server** screen, click **Disassociate**.

Launching the KVM Console for a Server

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

You must have Java Run-Time Environment (JRE) installed on your system.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **Servers**.
Step 3 Click the row with the server for which you want to launch the KVM console.
Step 4 Click **Launch KVM Console**.
Step 5 Click **Submit**.
A `kvm.jlp` file downloads to your system.
Step 6 Navigate to the location of the download and double-click the `kvm.jlp` file.
The KVM console opens in a separate window.

Service Profiles

A service profile ensures that the associated server hardware has the configuration required to support the applications it hosts. The service profile maintains configuration information about the server hardware, interfaces, fabric connectivity, and server and network identity.

Every active server must be associated with a service profile.

Note At any given time, each server can be associated with only one service profile. Similarly, each service profile can be associated with only one server at a time.

After a service profile is associated with a server, the server is ready to have an operating system and applications installed, and you can use the service profile to review the configuration of the server. If the server associated with a service profile fails, the service profile does not automatically fail over to another server.

When a service profile is disassociated from a server, the identity and connectivity information for the server is reset to factory defaults.

You can view the Service Profiles report by choosing **Service Profiles** under **Physical Resources**.

The Service Profiles report displays the following information for each available service profile:

- DN
- Name
- Associated Status
- Type
- FSM Status
- Assigned Server/Server Pool
- Operation State
- Config State
- Assign State
- Group/User
- Template Instance
- Policy Owner
- Maintenance Policy
- Storage Profile
- vMedia Policy

You can view additional details about a service profile by clicking the row with the service profile and clicking **View Details**.

Permissions Required for Service Profiles

The following table shows a list of the available service profile management actions and permissions required:

Task	End User Permissions
Viewing Service Profile Details, on page 63	Default
Disassociating a Service Profile from a Server, on page 64	Additional permissions required

Task	End User Permissions
Requesting an Inventory Collection, on page 64	Additional permissions required

Viewing Service Profile Details

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **Service Profiles**.

Step 3 Click the row with the service profile that you want to view.

Step 4 Click **View Details** to view the following details about the service profile:

- UCS Account Name
- Name
- Dn
- Associated State
- Assigned to Server/Server Pool
- Assigned State
- Config State
- Operational State
- Associated VSANs
- Associated VLANs
- Owner
- Source Template Name
- Vcon Profile Name
- Agent Policy
- Boot Policy
- Dynamic Connection Policy
- Host Fw Policy
- Local Disk Policy
- Management Policy
- Management Fw Policy
- Scrub Policy
- Sol Policy
- Stats Policy

- Outband IPv4: Management IP Address Policy

Disassociating a Service Profile from a Server

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **Service Profiles**.
Step 3 Click the row with the profile that you want to disassociate.
Step 4 Click **Disassociate**.
Step 5 On the **Disassociate Service Profile** screen, click **Disassociate**.

Requesting an Inventory Collection

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 On the **Physical Resources** page, click **Service Profiles**.
Step 2 On the **Collect Inventory** page, click the row with the profile for which you want to request an inventory collection, then click **Request Inventory Collection**.
Step 3 Click **Submit**.

VNX LUNs

EMC VNX LUNs are logical unit numbers (LUNs) that are used to identify storage entities in volumes on block or file storage arrays. You can view the VNX LUNs report by choosing **VNX LUNs** under **Physical Resources**.

The VNX LUNs report displays all available VNX LUNs, as well as the following information:

- Account Name
- Name
- ID
- Storage Pool
- RAID Group ID
- User Capacity (GB)
- Current Owner
- Default Owner
- Read Cache Enabled
- Write Cache Enaled
- Group/User

VNX Volumes

EMC VNX volumes reside in the block or file storage pools that distribute storage space to file systems. You can view the VNX Volumes report by choosing **VNX Volumes** under **Physical Resources**.

The VNX Volumes report displays all available VNX volume groups, as well as the following information:

- Volume Name
- Type
- Storage Capacity (GB)
- Free Capacity (GB)
- Storage Pool
- Data Movers

Block Storage Pools

Block storage pools are groups of available disk volumes on collections of storage-area network (SAN) disks. They are used to allocate available storage to file systems. You can view the Block Storage Pools report by choosing **Block Storage Pools** under **Physical Resources**.

The Block Storage Pool report displays all available block storage pools, as well as the following information:

- Account Name
- Name
- Description
- Total Capacity (GB)
- Used Capacity (GB)

- Free Capacity (GB)
- Physical Capacity (GB)
- RAID Type
- Storage Pool ID
- Number of LUNs
- Group/User

RAID Groups

RAID (Redundant Array of Independent Disks) provides a way of storing the same data in different places on multiple hard disks. By placing data on multiple disks, input/output operations can overlap in a balanced way, improving performance. You can view the RAID Groups report by choosing **RAID Groups** under **Physical Resources**.

The RAID Groups report displays all available RAID groups, as well as the following information:

- Account Name
- RAID Group ID
- RAID ID
- Drive Type
- Raw Capacity (GB)
- Logical Capacity (GB)
- Free Capacity (GB)
- Power Savings Setting
- Number of LUNs
- Number of Disks
- Percent Expanded
- Group/User

File Storage Pools

File storage pools are groups of available disk volumes on collections of network file system (NFS) disks that are used to allocate available storage to file systems. You can view the File Storage Pools report by choosing **File Storage Pools** under **Physical Resources**.

The File Storage Pools report displays all available file storage pools, as well as following information:

- Name
- Description
- Storage Capacity (GB)

- Storage Used (GB)
- Type
- Disk Type
- Uses Volumes
- Used By
- Group/User

Rack Servers

You can view the Rack Servers report by choosing **Rack Servers** under **Physical Resources**.

The Rack Servers report displays all available rack servers, as well as the following information:

- Account Name
- Model
- Operation Status
- UUID
- Power State
- IP Address

Permissions Required for Rack Servers

The following table shows a list of the available rack server management actions and permissions required:

Task	End User Permissions
Powering a Rack Server On or Off, on page 68	Additional permissions required
Shutting Down a Rack Server, on page 68	Additional permissions required
Performing a Hard Reset on a Rack Server, on page 69	Additional permissions required
Power Cycling a Rack Server, on page 69	Additional permissions required
Launching the KVM Console for a Rack Server, on page 69	Additional permissions required

Powering a Rack Server On or Off

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **Rack Servers**.

Step 3 Click the row with the server you want to power on or off.

Step 4 Click one of the following:

- **Power ON**
- **Power OFF**

Step 5 Click **Submit**.

Shutting Down a Rack Server

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **Rack Servers**.

Step 3 Click the row with the rack server that you want to shut down.

Step 4 Click **Shut Down**.

Step 5 Click **Submit**.

Performing a Hard Reset on a Rack Server

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **Rack Servers**.
Step 3 Click the row with the rack server on which you want to perform a hard reset.
Step 4 Click **Hard Reset**.
Step 5 Click **Submit**.

Power Cycling a Rack Server

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **Rack Servers**.
Step 3 Click the row with the rack server on which you want to perform a power cycle.
Step 4 Click **Power Cycle**.
Step 5 Click **Submit**.

Launching the KVM Console for a Rack Server

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

You must have Java Run-Time Environment (JRE) installed on your system.

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **Rack Servers**.

Step 3 Click the row with the rack server for which you want to launch the KVM console.

Step 4 Click **Launch KVM Console**.

Step 5 Click **Submit**.
A `kvm.jlp` file downloads to your system.

Step 6 Navigate to the location of the download and double-click the `kvm.jlp` file.
The KVM console opens in a separate window.

CloudSense Reports

CloudSense analytics provide visibility into the infrastructure resources utilization, critical performance metrics across the IT infrastructure stack, and capacity in real time. CloudSense reports can show significant improvements in capacity trending, forecasting, reporting, and planning of virtual and cloud infrastructures.

The following reports are available from CloudSense, but the number of reports available in the system for a user depends on your user role:

- Billing Report for a Customer
- ENC Storage Inventory Report
- NetApp Storage Inventory Report
- NetApp Storage Savings Per Group
- NetApp Storage Savings Report
- Network Impact Assessment Report
- Organizational Usage of Virtual Computing Infrastructure
- PNSC Account Summary Report
- Physical Infrastructure Inventory Report for a Group
- Storage Dedupe Status Report
- Storage Inventory Report for a Group
- Thin Provisioned Space Report
- UCS Data Center Inventory Report
- VM Activity Report by Group
- VMware Host Performance Summary
- Virtual Infrastructure and Assets Report

Note If the CloudSense option is enabled for MSP administrators, only reports relevant to their customer organizations are displayed.

Permissions Required for CloudSense Reports

The following table shows a list of the available CloudSense management actions and permissions required:

Task	End User Permissions
Generating a CloudSense Report, on page 71	Default
Opening a CloudSense Report, on page 72	Additional permissions required
Emailing a CloudSense Report, on page 72	Additional permissions required
Deleting a CloudSense Report, on page 72	Additional permissions required

Generating a CloudSense Report

Step 1 Choose **Physical Resources**.

Step 2 On the **Physical Resources** page, click **CloudSense**.

Step 3 Click **Generate Report**.

Step 4 On the **Generate Report** screen, choose the type of report that you want to generate from the **Report Type** drop-down list.

Step 5 Click **Submit**.

Opening a CloudSense Report

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **CloudSense**.
Step 3 Click the row with the report that you want to open.
Step 4 Click **Open Report**.

Emailing a CloudSense Report

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **CloudSense**.
Step 3 Click the row with the report that you want to email.
Step 4 Click **Email Report**.

Deleting a CloudSense Report

Before You Begin

To access this option, your administrator must provide permission in your user role, or in the End User Self-Service policy in your group's VDC.

Step 1 Choose **Physical Resources**.
Step 2 On the **Physical Resources** page, click **CloudSense**.
Step 3 Click the row with the report that you want to delete.
Step 4 Click **Delete Report**.