Storage Virtual Machines

System Manager Classic

NetApp
January 13, 2022

Table of Contents

Storage Virtual Machines . . . 1
- SVM Dashboard window . . . 1
- Monitoring SVMs . . . 2
- Editing SVM settings . . . 2
- Deleting SVMs . . . 3
- Starting SVMs . . . 4
- Stopping SVMs . . . 4
- Managing SVMs . . . 5
- Tracing file access to diagnose access errors on SVMs . . . 5
- Types of SVMs . . . 7
- Why you use SVMs . . . 7
- How ONTAP name service switch configuration works . . . 8
- Storage Virtual Machines window . . . 9
- Trace File Access window . . . 13

Storage Virtual Machines

You can use System Manager to manage the SVMs in your cluster.

Related information

SAN administration

ONTAP concepts

SVM Dashboard window

The dashboard provides a cumulative at-a-glance information about your storage virtual machine (SVM) and its performance. You can use the Dashboard window to view important information related to your SVM such as the protocols configured, the volumes that are nearing capacity, and the performance.

SVM Details

This window displays details about the SVM through various panels such as the Protocol Status panel, Volumes Nearing Capacity panel, Applications panel, and performance panel.

- **Protocol Status**

  Provides an overview of the protocols that are configured for the SVM. You can click the protocol name to view the configuration.

  If a protocol is not configured or if a protocol license is not available for the SVM, you can click the protocol name to configure the protocol or to add the protocol license.

- **Volumes Nearing Capacity**

  Displays information about the volumes that are nearing capacity utilization of 80 percent or more and that require immediate attention or corrective action.

- **Applications**

  Displays information about the top five applications of the SVM. You can view the top five applications based on either IOPS (from low to high or from high to low) or capacity (from low to high or from high to low). You must click the specific bar chart to view more information about the application. For capacity, the total space, used space, and available space are displayed, and for IOPS, the IOPS details are displayed. For L2/L3 applications, latency metrics are also displayed.

  The used size displayed in the Applications window does not equal the used size in the CLI.

  You can click **View details** to open the Applications window of the specific application. You can click **View all applications** to view all of the applications for the SVM.

  The refresh interval for the Applications panel is one minute.

- **SVM Performance**

Displays the performance metrics of the protocols in the SVM, including latency and IOPS.

If the information about SVM performance cannot be retrieved from ONTAP, you cannot view the respective graph. In such cases, System Manager displays the specific error message.

The refresh interval for the SVM Performance panel is 15 seconds.

Monitoring SVMs

The dashboard in System Manager enables you to monitor the health and performance of a storage virtual machine (SVM).

Steps

1. Click **Storage** > **SVMs**.
2. Select the name the SVM that you want to monitor.
3. View the details in the dashboard panels.

Editing SVM settings

You can use System Manager to edit the properties of storage virtual machines (SVMs), such as the name service switch, name mapping switch, and aggregate list.

About this task

- You can edit the values of the following SVM properties:
  - Name service switch
  - Protocols that are enabled to serve data

    The CIFS protocol that is configured on the SVM continues to serve data even when you disable the protocol on that SVM.

  - The list of aggregates that are available to create volumes

    For FlexVol volumes, you can assign aggregates only if you have delegated administration to an SVM administrator.

- System Manager does not display the values of the name service switch and the name mapping switch for an SVM that is created through the command-line interface or for the SVM services that are not configured and are not set to the default values by ONTAP.

  You can use the command-line interface to view the services because the Services tab is disabled.

  System Manager displays the name service switch and the name mapping switch of an SVM only when it is created by using System Manager or when the services of the SVM are set to the default values by ONTAP.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.

3. In the **Details** tab, modify the required data protocols.
4. In the **Resource Allocation** tab, choose one of the following methods to delegate volume creation:

If you want to provision volume creation…	Then…
For all aggregates	Select the **Do not delegate volume creation** option.
For specific aggregates	a. Select the **Delegate volume creation** option. b. Select the required aggregates for delegating volume creation.

5. In the **Service** tab, specify the name service switch sources for the required database types and the order in which they should be consulted to retrieve name service information.

   The default values for each of the database types are as follows:

   - hosts: files, dns
   - namemap: files
   - group: files
   - netgroup: files
   - passwd: files
6. Click **Save and Close**.

Related information

How ONTAP name service switch configuration works

Deleting SVMs

You can use System Manager to delete storage virtual machines (SVMs) that you no longer require from the storage system configuration.

Before you begin

You must have completed the following tasks:

1. Disabled the Snapshot copies, data protection (DP) mirrors, and load-sharing (LS) mirrors for all the volumes

   You must use the command-line interface (CLI) to disable LS mirrors.
2. Deleted all the igroups that belong to the SVM manually if you are deleting SVMs
3. Deleted all the portsets
4. Deleted all the volumes in the SVM, including the root volume
5. Unmapped the LUNs, taken them offline, and deleted them
6. Deleted the CIFS server if you are deleting SVMs

7. Deleted any customized user accounts and roles that are associated with the SVM
8. Deleted any NVMe subsystems associated with the SVM using the CLI.
9. Stopped the SVM

About this task

When you delete SVMs, the following objects associated with the SVM are also deleted:

- LIFs, LIF failover groups, and LIF routing groups
- Export policies
- Efficiency policies

If you delete SVMs that are configured to use Kerberos, or modify SVMs to use a different Service Principal Name (SPN), the original service principal of the SVM is not automatically deleted or disabled from the Kerberos realm. You must manually delete or disable the principal. You must have the Kerberos realm administrator's user name and password to delete or disable the principal.

If you want to move data from an SVM to another SVM before you delete the first SVM, you can use the SnapMirror technology to do so.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Starting SVMs

You can use System Manager to provide data access from a storage virtual machine (SVM) by starting the SVM.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM that you want to start, and then click **Start**.

Results

The SVM starts serving data to clients.

Stopping SVMs

You can use System Manager to stop a storage virtual machine (SVM) if you want to troubleshoot any issue with the SVM, delete the SVM, or stop data access from the SVM.

Before you begin

All the clients connected to the SVM must be disconnected.

If any clients are connected to the SVM when you stop it, data loss might occur.

About this task

- You cannot stop SVMs during storage failover (SFO).
- When you stop the SVM, an SVM administrator cannot log in to the SVM.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM that you want to stop, and then click **Stop**.

Results

The SVM stops serving data to clients.

Managing SVMs

A storage virtual machine (SVM) administrator can administer SVMs and their resources, such as volumes, protocols, and services, depending on the capabilities assigned by the cluster administrator. An SVM administrator cannot create, modify, or delete SVMs.

SVM administrators cannot log in to System Manager.

SVM administrators might have all or some of the following administration capabilities:

- Data access protocol configuration

  SVM administrators can configure data access protocols, such as NFS, CIFS, iSCSI, and Fibre Channel (FC) protocol (Fibre Channel over Ethernet or FCoE included).

- Services configuration

  SVM administrators can configure services such as LDAP, NIS, and DNS.

- Storage management

  SVM administrators can manage volumes, quotas, qtrees, and files.

- LUN management in a SAN environment
- Management of Snapshot copies of the volume
- Monitoring SVM

  SVM administrators can monitor jobs, network connection, network interface, and the SVM health.

Related information

ONTAP 9 Documentation Center

Tracing file access to diagnose access errors on SVMs

Starting with System Manager 9.6, you can diagnose CIFS or NFS file access errors on a storage virtual machine (SVM).

About this task

File access issues, such as an “access denied” error, are likely to occur when there are problems with a share configuration, permissions, or user mapping. You can use System Manager to help you resolve file access problems by viewing the access trace results for the file or share that a user wants to access. System Manager shows whether the file or share has effective read, write, or execute permissions and the reasons why access is or is not effective.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM that contains the files or shares for which file access errors were received.
3. Click **Trace File Access**.

   The Trace File Access window for the selected SVM shows the prerequisites and steps required to trace file access permissions.

4. Click **Continue** to begin the file tracing process.
5. Select the protocol that is used to access files or shares on the selected SVM.
6. In the **User Name** field, enter the name of the user who was trying to access the file or share.
7. Click ⚙ to specify more details to narrow the scope of the trace.

   The Advanced Options dialog window allows you to specify the following details:

   - **Client IP Address**: Specify the IP address of the client.
   - **File**: Specify the file name or file path to trace.
   - **Show in Trace Results**: Specify whether you want to view only access denied entries or all entries. Click **Apply** to apply the details you specified and to return to the Trace File Access window.

8. Click **Start Tracing**.

   The trace is initiated and a results table is displayed. The table is empty until users receive errors when requesting file access. The results table is refreshed every 15 seconds and displays messages in reverse chronological order.

9. Notify the affected user or users that they should try accessing the files within the next 60 minutes.

   Details of the denied file access requests are shown in the results table when errors occur for the specified username for the duration of the trace. The Reasons column identifies the problems that are preventing the user from accessing files and reasons why they occurred.

10. In the **Reasons** column of the result table, click **View Permissions** to view permissions for the file that the user is trying to access.

    - When the trace result shows a message saying that access is not granted for "Synchronize", "Read Control", "Read Attributes", "Execute", "Read EA", "Write", or "Read"', the message is indicating that the desired access has not been granted for the set of permissions listed. In order to view the actual permissions status, you need to view the permissions using the provided link.
    - If you specified the CIFS protocol, the Effective File and Share Permissions dialog box displays, listing both file and share permissions associated with the share and file that the user is trying to access.
    - If you specified the NFS protocol, the Effective File Permissions dialog box displays, listing the file permissions associated with the file that the user is trying to access. A check mark indicates that permissions are granted, and an “X” indicates that permissions are not granted.

    Click **OK** to return to the Trace File Access window.

11. The results table displays read-only data. You can perform the following actions with the results of the trace:
    - Click **Copy to Clipboard** to copy the results to the clipboard.
    - Click **Export Trace Results** to export the results to a comma-separatedvalues (CSV) file.
12. When you want to end the tracing operation, click **Stop Tracing**.

Types of SVMs

A cluster consists of four types of SVMs, which help in managing the cluster and its resources and data access to the clients and applications.

A cluster contains the following types of SVMs:

- Admin SVM

  The cluster setup process automatically creates the admin SVM for the cluster. The admin SVM represents the cluster.

- Node SVM

  A node SVM is created when the node joins the cluster, and the node SVM represents the individual nodes of the cluster.

- System SVM (advanced)

  A system SVM is automatically created for cluster-level communications in an IPspace.

- Data SVM

  A data SVM represents the data serving SVMs. After the cluster setup, a cluster administrator must create data SVMs and add volumes to these SVMs to facilitate data access from the cluster.

  A cluster must have at least one data SVM to serve data to its clients.

Unless otherwise specified, the term SVM refers to a data (data-serving) SVM.In the CLI, SVMs are displayed as Vservers.

Why you use SVMs

SVMs provide data access to clients regardless of the physical storage or controller, similar to any storage system. SVMs provide benefits such as nondisruptive operations, scalability, security, and unified storage.

SVMs provide the following benefits:

- Multi-tenancy

  SVM is the fundamental unit of secure multi-tenancy, which enables partitioning of the storage infrastructure so that it appears as multiple independent storage systems. These partitions isolate the data and management.

- Nondisruptive operations

  SVMs can operate continuously and nondisruptively for as long as they are needed. SVMs help clusters to operate continuously during software and hardware upgrades, addition and removal of nodes, and all administrative operations.

- Scalability

  SVMs meet on-demand data throughput and the other storage requirements.

- Security

  Each SVM appears as a single independent server, which enables multiple SVMs to coexist in a cluster while ensuring no data flows among them.

- Unified storage

  SVMs can serve data concurrently through multiple data access protocols. SVMs provide file-level data access through NAS protocols, such as CIFS and NFS, and block-level data access through SAN protocols, such as iSCSI, FC/FCoE, and NVMe. SVMs can serve data to SAN and NAS clients independently at the same time.

- Delegation of management

  SVM administrators have privileges assigned by the cluster administrator.

How ONTAP name service switch configuration works

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for…	Valid sources are…
hosts	Converting host names to IP addresses	files, dns
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap

Database type	Defines name service sources for…	Valid sources are…
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type…	To look up information in…	Managed by the command families…

files	Local source files	`vserver services name-service unix-user`
		
		`vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	External NIS servers as specified in the NIS domain configuration of the SVM	`vserver services name-service nis-domain`
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	`vserver services name-service ldap`
dns	External DNS servers as specified in the DNS configuration of the SVM	`vserver services name-service dns`

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

Related information

Editing SVM settings

Storage Virtual Machines window

You can use the Storage Virtual Machines window to manage your storage virtual machines (SVMs) and display information about them.

You cannot manage (create, delete, start, or stop) anSVM configured for disaster recovery (DR) by using System Manager. Also, you cannot view the storage objects associated with the SVM configured for disaster recovery in the application interface.

Command buttons

- **Create**

  Opens the Storage Virtual Machine (SVM) Setup wizard, which enables you to create a new SVM.

- **Edit**

  Opens the Edit Storage Virtual Machine dialog box, which enables you to modify the properties, such as the name service switch, name mapping switch, and aggregate list, of a selected SVM.

- **Delete**

  Deletes the selected SVMs.

- **Start**

  Starts the selected SVM.

- **Stop**

  Stops the selected SVM.

- **SVM Settings**

  Manages the storage, policies, and configuration for the selected SVM.

- **Protection Operations**

  Provides the following options:

  - **Initialize**

    Enables you to initialize the SVM relationship to perform a baseline transfer from the source SVM to the destination SVM.

  - **Update**

    Enables you to update data from the source SVM to the destination SVM.

  - **Activate Destination SVM**

    Enables you to activate the destination SVM.

  - **Resync from Source SVM**

    Enables you to initiate resynchronization of the broken relationship.

  - **Resync from Destination SVM (Reverse Resync)**

    Enables you to resynchronize the relationship from the destination SVM to the source SVM.

    - **Reactivate Source SVM**

      Enables you to reactivate the source SVM.

- **Refresh**

  Updates the information in the window.

- **Trace File Access**

  Enables you to trace the accessibility of a file or share on the selected SVM for a specified username.

SVM list

The SVM list displays the name of each SVM and the allowed protocols on it.

You can view only data SVMs by using System Manager.

- **Name**

  Displays the name of the SVM.

- **State**

  Displays the SVM state, such as Running, Starting, Stopped, or Stopping.

- **Subtype**

  Displays the subtype of the SVM, which can be one of the following:

    - default

      Specifies that the SVM is a data-serving SVM.

    - dp-destination

      Specifies that the SVM is configured for disaster recovery.

    - sync-source

      Specifies that the SVM is in the primary site of a MetroCluster configuration.

    - sync-destination

      Specifies that the SVM is in the surviving site of a MetroCluster configuration.

- **Allowed Protocols**

  Displays the allowed protocols, such as CIFS and NFS, on each SVM.

- **IPspace**

  Displays the IPspace of the associated SVM.

- **Volume Type**

Displays the allowed volume type, such as FlexVol volume, on each SVM.

- **Protected**

  Displays whether the SVM is protected or not.

- **Configuration State**

  Displays whether the configuration state of the SVM is locked or unlocked.

Details area

The area below the SVM list displays detailed information, such as the type of volumes allowed, language, and Snapshot policy, about the selected SVM.

You can also configure the protocols that are allowed on this SVM. If you have not configured the protocols while creating the SVM, you can click the protocol link to configure the protocol.

You cannot configure protocols for anSVM configured for disaster recovery by using System Manager.

If the FCP service is already started for the SVM, clicking the FC/FCoE link opens the Network Interfaces window.

The color indicates the status of the protocol configuration:

Status	Description
Green	LIFs exist and the protocol is configured. You can click the link to view the configuration details. Configuration might be partially completed. However, service is running. You can create the LIFs and complete the configuration from the Network Interfaces window.
Yellow	Indicates one of the following: • LIFs exist. Service is created but is not running. • LIFs exist. Service is not created. • Service is created. LIFs do not exist.
Grey	The protocol is not configured. You can click the protocol link to configure the protocol.
Grey border	The protocol license has expired or is missing. You can click the protocol link to add the licenses in the Licenses page.

You can also add the management interface and view details such as the protection relationships, protection

policy, NIS domain, and so on.

The **Details** area also includes a link to view the Public SSL Certificate for an SVM. When you click this link, you can perform the following tasks:

- View certificate details, the serial number, the start date, and the expiration date.
- Copy the certificate to the clipboard.
- Email the certificate details.

Peer Storage Virtual Machines area

Displays a list of the SVMs that are peered with the selected SVM along with details of the applications that are using the peer relationship.

Trace File Access window

Starting with System Manager 9.6, you can use the Trace File Access window to diagnose issues when you have problems accessing files and shares on an SVM using the CIFS or NFS protocol.

Command buttons

- **Continue**

  Starts the process of setting up and initiating a file access trace on the selected SVM.

- **Protocols**

  Allows you to select the protocol that is used to access files and shares on the selected SVM, either CIFS or NFS.

- **Advanced Options icon**

  Allows you to specify additional details to narrow the scope of the trace.

- **Show in Trace Results**

  Allows you to specify in the Advanced Options dialog box whether you want the trace results to display only file access requests that were denied or to display all file access requests—those that were successful and those that were denied.

- **Start Tracing**

  Allows you to start the trace. The results show access problems for file access requests submitted over the next 60 minutes.

- **Stop Tracing**

  Allows you to stop the trace.

- **View Permissions**

  Allows you to display permissions. When using the CIFS protocol, you can display effective file and share

permissions. When using the NFS protocol, you can display effective file permissions.

- **Copy to Clipboard**

  Allows you copy the results table to the clipboard.

- **Export Trace Results**

  Allows you to export the trace results to a file in comma-separated-values (.csv) format.

Entry fields

- **User Name**

  You enter the name of the user who received file access request errors that you want to trace.

- **Search trace results**

  You enter specific information that you want to find in the search results, and then you click **Enter**.

- **Client IP Address**

  In theAdvanced Options dialog box, you can specify the IP address of the client as an additional detail to narrow the scope of the trace.

- **File**

  In theAdvanced Options dialog box, you can specify the file or file path that you want to access as an additional detail to narrow the scope of the trace.

Results list for CIFS protocol tracing

When you specify the CIFS protocol, the results list displays the following data for your trace based on the parameters you specified. The data is displayed in reverse chronological order. If you stop tracing, the results remain in the list until you start another trace.

- Share: The name of the share that the system attempted to access, whether successful or not.
- Path: The file path of the file that the system attempted to access, whether successful or not.
- Client IP Address: The IP address of the client from which access requests were initiated.
- Reasons: The reasons the attempt to access the file or share was successful or not.

When the trace result shows a message saying that access is not granted for "Synchronize", "Read Control", "Read Attributes", "Execute", "Read EA", "Write", or "Read"', the message is indicating that the desired access has not been not granted for the set of permissions listed. In order to view the actual permissions status, you need to view the permissions using the provided link.

Results list for NFS protocol tracing

When you specify the NFS protocol, the results list displays the following data for your trace based on the parameters you specified. The data is displayed in reverse chronological order. If you stop tracing, the results remain in the list until you start another trace.

- Path: The file path of the file that the system attempted to access, whether successful or not.
- Client IP Address: The IP address of the client from which access requests were initiated.
- Reasons: The reasons the attempt to access the file or share was successful or not.

When the trace result shows a message saying that access is not granted for "Synchronize", "Read Control", "Read Attributes", "Execute", "Read EA", "Write", or "Read"', the message is indicating that the desired access has not been not granted for the set of permissions listed. In order to view the actual permissions status, you need to view the permissions using the provided link.

Related information

SMB/CIFS management

SMB/CIFS and NFS multiprotocol configuration