Monitor and report

SnapCenter Plug-in for VMware vSphere 4.9

NetApp
August 30, 2024

Table of Contents

Monitor and report . . . 1
- View status information . . . 1
- Monitor jobs . . . 2
- Download job logs . . . 3
- Access reports . . . 4
- Generate a support bundle from the SnapCenter Plug-in for VMware vSphere GUI . . . 6
- Generate a support bundle from the maintenance console . . . 7
- Audit logs . . . 8

Monitor and report

View status information

You can view status information on the vSphere client Dashboard. Status information is updated once an hour.

Steps

1. In the left Navigator pane of the vSphere client, click **Dashboard**, select a vCenter Server, and then click the **Status** tab in the dashboard pane.
2. View overview status information or click a link for more details, as listed in the following table.

This dashboard tile…	Displays the following information…
Recent job activities	The three to five most recent backup, restore, and mount jobs. • Click on a job ID to see more details about that job. • Click **See all** to go to the Job Monitor tab for more details on all jobs.
Jobs	A count of each job type (backup, restore, and mount) performed within the selected time window. Hover the cursor over a section of the chart to see more details for that category.

This dashboard tile…	Displays the following information…
Latest Protection Summary	Summaries of the data protection status of primary and secondary VMs or datastores within the selected time window. • Click the drop-down menu to select **VMs** or **Datastores**. • For secondary storage, select **SnapVault** or **SnapMirror**. • Hover the cursor over a section of a chart to see the count of VMs or Datastores in that category. In the Successful category, the most recent backup is listed for each resource. • You can change the time window by editing the configuration file. The default is 7 days. For more information, see Customize your configuration. • Internal counters are updated after each primary or secondary backup. The dashboard tile is refreshed every six hours. The refresh time cannot be changed. Note: If you use a mirror-vault protection policy, then the counters for the protection summary are displayed in the SnapVault summary chart, not in the SnapMirror chart.
Configuration	The total number of each type of object managed by the SnapCenter Plug-in for VMware vSphere.
Storage	The total number of Snapshot copies, SnapVault, and SnapMirror Snapshot copies, generated and the amount of storage used for primary and secondary Snapshot copies. The line graph separately plots primary and secondary storage consumption on a day-by-day basis over a rolling 90-day period. Storage information is updated once every 24 hours at 1:08 A.M. Storage Savings is the ratio of logical capacity (Snapshot copy savings plus storage consumed) to the physical capacity of primary storage. The bar chart illustrates the storage savings. Hover the cursor over a line on the chart to see detailed day-by-day results.

Monitor jobs

After performing any data protection operation using the VMware vSphere client, you can

monitor the job status from the Job Monitor tab in the Dashboard and view job details.

Steps

1. In the left Navigator pane of the vSphere client, click **Dashboard**, when two or more vCenters are configured in linked mode, select a vCenter Server, and then click the **Job Monitor** tab in the Dashboard pane.
   The Job Monitor tab lists each job and its status, start time, and end time. If the job names are long, you might need to scroll to the right to view the start and end times. The display is refreshed every 30 seconds.
   - Select the refresh icon in the toolbar to refresh the display on-demand.
   - Select the filter icon to choose the time range, type, tag, and status of jobs you want displayed. The filter is case sensitive.
   - Select the refresh icon in the Job Details window to refresh the display while the job is running.

If the Dashboard does not display job information, see the KB article: SnapCenter vSphere client dashboard does not display jobs.

Download job logs

You can download the job logs from the Job Monitor tab on the Dashboard of the SnapCenter VMware vSphere client.

If you encounter unexpected behavior while using the VMware vSphere client, you can use the log files to identify the cause and resolve the problem.

> The default value for retaining job logs is 30 days; the default value for retaining jobs is 90 days. Job logs and jobs that are older than the configured retention are purged every six hours. You can use the Configuration `jobs/cleanup` REST APIs to modify how long jobs and job logs are retained. You cannot modify the purge schedule.

Steps

1. In the left Navigator pane of the vSphere client, click **Dashboard**, select a vCenter Server, and then click the **Job Monitor** tab in the Dashboard pane.
2. Select the download icon in the Job Monitor title bar.

   You might need to scroll to the right to see the icon.

   You can also double-click a job to access the Job Details window and then click **Download Job Logs**.

Result

Job logs are located on the Linux VM host where the SnapCenter VMware plug-in is deployed. The default job log location is `/var/log/netapp`.

If you tried to download job logs but the log file named in the error message has been deleted, you might encounter the following error: `HTTP ERROR 500 Problem accessing /export-scv-logs`. To correct this error, check the file access status and permissions for the file named in the error message and correct the access problem.

Access reports

You can request reports for one or more jobs from the dashboard.

The Reports tab contains information on the jobs that are selected on the Jobs page in the Dashboard. If no jobs are selected, the Reports tab is blank.

Steps

1. In the left Navigator pane of the vSphere client, click **Dashboard**, select a vCenter Server, and then click the **Reports** tab.
2. For Backup Reports, you can do the following:
   a. Modify the report

      Select the filter icon to modify the time range, job status type, resource groups, and policies to be included in the report.

   b. Generate a detailed report

      Double-click any job to generate a detailed report for that job.
3. Optional: On the Reports tab, click **Download** and select the format (HTML or CSV).

   You can also click the download icon to download plug-in logs.

Types of reports from the VMware vSphere client

The VMware vSphere client for SnapCenter provides customizable report options that provide you with details about your data protection jobs and plug-in resource status. You can generate reports for primary protection only.

> Backup schedules are executed in the time zone in which the SnapCenter VMware plug-in is deployed. vCenter reports data in the time zone in which the vCenter is located. Therefore, if the SnapCenter VMware plug-in and the vCenter are in different time zones, data in the VMware vSphere client Dashboard might not be the same as the data in the reports.

The Dashboard displays information on migrated backups only after backups post-migration are performed.

Report type	Description
Backup Report	Displays overview data about backup jobs. Click a section/status on the graph to see a list of jobs with that status on the **Reports** tab. For each job, the report lists the job ID, corresponding resource group, backup policy, start time and duration, status, and job details which includes the job name (Snapshot copy name) if the job completed, and any warning or error messages. You can download the Report table in HTML or CSV format. You can also download the Job Monitor job logs for all the jobs (not just the jobs in the report). Deleted backups are not included in the report.
Mount Report	Displays overview data about mount jobs. Click a section/status on the graph to see a list of jobs with that status on the Reports tab. For each job, the report lists the job ID, job status, job name, and job start and end times. The job name includes the Snapshot copy name. For example: `Mount Backup <snapshot-copy-name>` You can download the Report table in HTML or CSV format. You can also download the Job Monitor job logs for all the jobs (not just the jobs in the report).
Restore Report	Displays overview status information about restore jobs. Click a section/status on the graph to see a list of jobs with that status on the Reports tab. For each job, the report lists the job ID, job status, job name, and job start and end times. The job name includes the Snapshot copy name. For example: `Restore Backup <snapshot-copy-name>` You can download the Report table in HTML or CSV format. You can also download the Job Monitor job logs for all the jobs (not just the jobs in the report).

Report type	Description
Last Protection Status of VMs or Datastores Report	Displays overview information about the protection status, during the configured number of days, for VMs and datastores managed by the SnapCenter VMware plug-in. The default is 7 days. To modify the value in the properties file, see Modify configuration default values. Click a section/status on the primary protection chart to see a list of VMs or datastores with that status on the **Reports** tab. The VM or Datastores Protection Status Report for protected VMs and datastores displays the names of VMs or datastores that have been backed up during the configured number of days, the latest Snapshot copy name, and the start and end times for the latest backup run. The VM or Datastores Protection Status Report for unprotected VMs or datastores displays the names of VMs or datastores that do not have any successful backups during the configured number of days. You can download the Report table in HTML or CSV format. You can also download the Job Monitor job logs for all the jobs (not just the jobs in the report). This report is refreshed every hour when the plug-in cache is refreshed. Therefore, the report might not display VMs or datastores that were recently backed up.

Generate a support bundle from the SnapCenter Plug-in for VMware vSphere GUI

Before you begin

To log on to the SnapCenter Plug-in for VMware vSphere management GUI, you must know the IP address and the log in credentials. You must also note down the MFA token generated from the maintenance console.

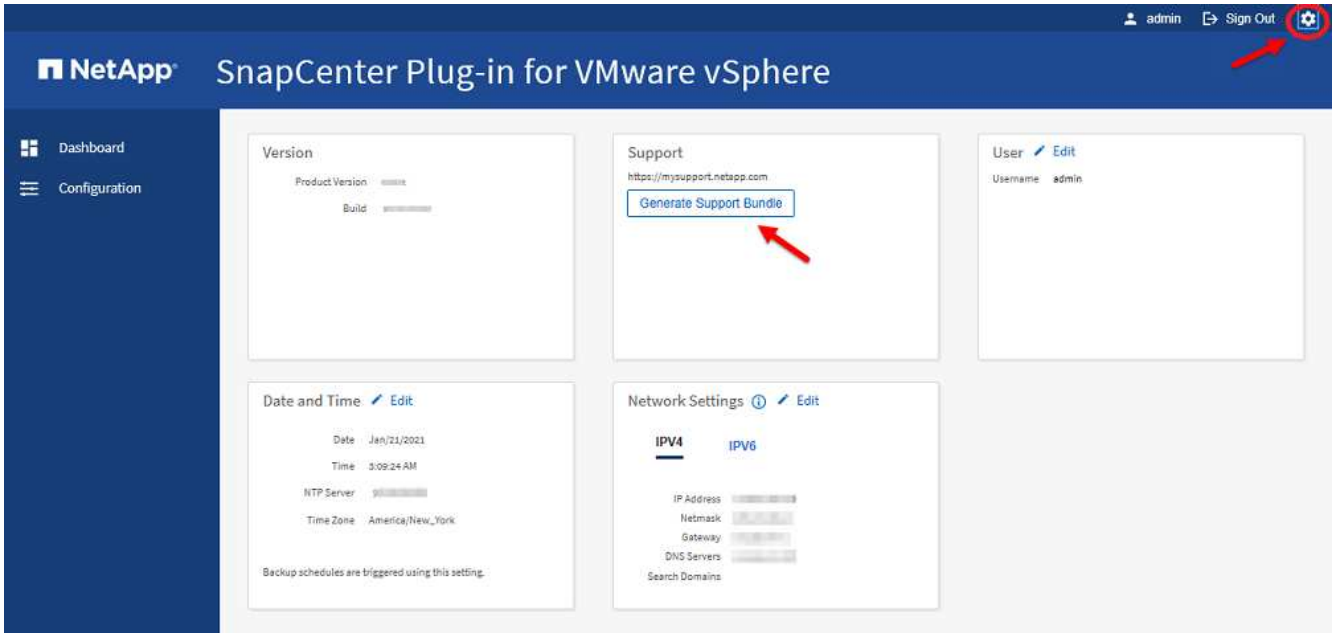
- The IP address was displayed when the SnapCenter VMware plug-in was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter VMware plug-in or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere GUI.

   Use the format `https://<OVA-IP-address>:8080`.

2. Click the Settings icon in the top toolbar.



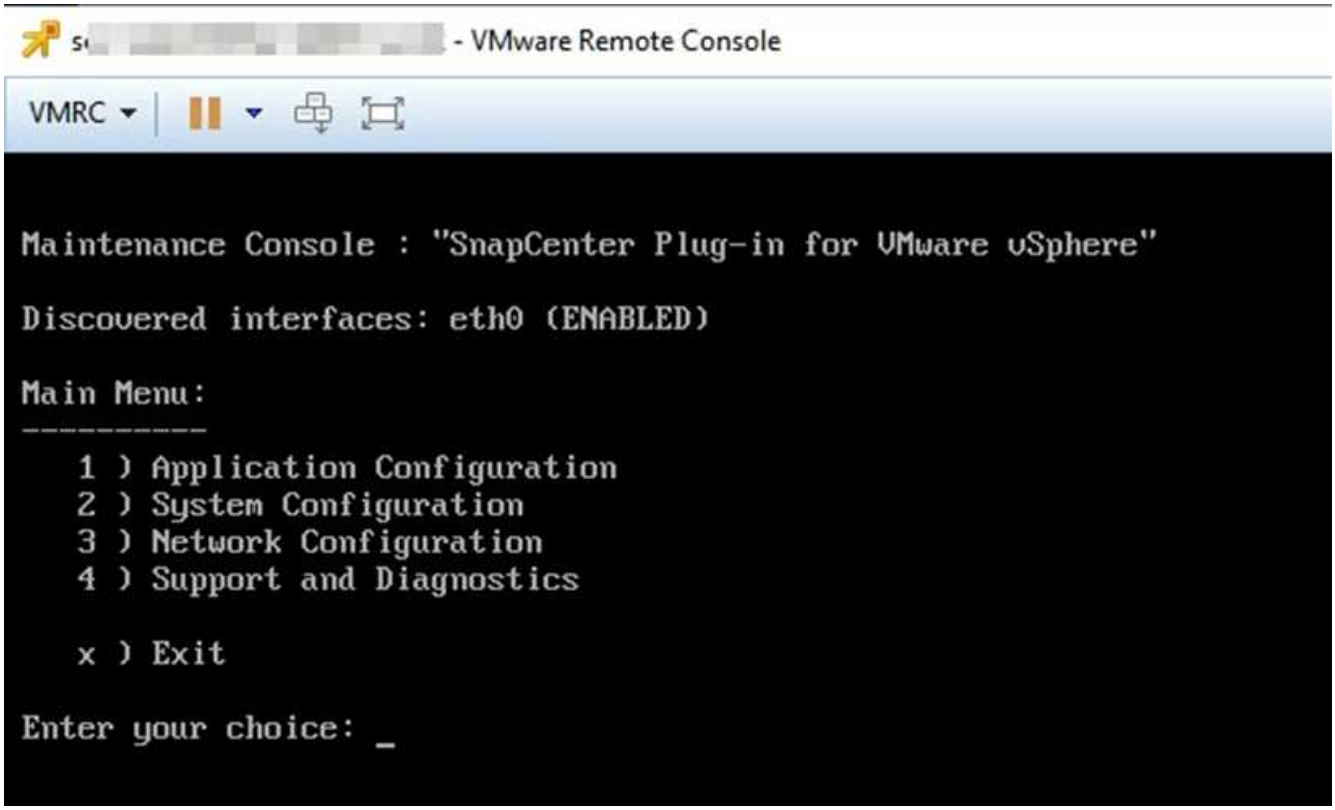
3. On the **Settings** page, in the **Support** section, click **Generate Support** Bundle.
4. After the support bundle is generated, click the link that is provided to download the bundle to NetApp.

Generate a support bundle from the maintenance console

Steps

1. From the VMware vSphere client, select the VM where the SnapCenter VMware plug-in is located.
2. Right-click the VM, then on the **Summary** tab of the virtual appliance click **Launch Remote Console or Launch Web Console** to open a maintenance console window, and then log on.

   For information on accessing and logging on to the maintenance console, see Access the Maintenance Console.



3. From the Main Menu, enter option **4) Support and Diagnostics**.
4. From the Support and Diagnostics Menu, enter option **1) Generate support bundle**.

To access the support bundle, on the Support and Diagnostics Menu enter option **2) Access Diagnostic Shell**. In the console, navigate to `/support/support/<bundle_name>.tar.gz`.

Audit logs

Audit log is a collection of events in a chronological order, which is written to a file within the appliance. The audit log files are generated at `/var/log/netapp/audit` location and the file names follow one of the below naming conventions:

- audit.log: Active audit log file that is in use.
- audit-%d{yyyy-MM-dd-HH-mm-ss}.log.gz: Rolled over audit log file. The date and time in the file name indicates when the file was created, for example: audit-2022-12-15-16-28-01.log.gz.

In the SCV plug-in user interface, you can view and export the audit log details from **Dashboard** > **Settings** > **Audit Logs** Tab
You can view operation audit in the audit logs. The audit logs are downloaded with the Support bundle.

If Email settings are configured, SCV sends an Email notification in the event of an Audit Log Integrity Verification failure. An Audit Log Integrity Verification failure can happen when one of the files is tampered or deleted.

The default configurations of the audit files are:

- Audit log file in use can grow to a maximum of 10 MB

- A maximum of 10 audit log files are retained

To modify the default configurations add a key value pair in the /opt/netapp/scvservice/standalone_aegis/etc/scbr/scbr.properties and restart the scvservice.

The configurations for audit log files are:

- auditMaxROFiles=<xx>, where xx is the max number of rolled over audit log files, for example: auditMaxROFiles=15.
- auditLogSize=<XX>MB, where xx is the size of the file in MB, for example: auditLogSize=15MB.

Rolled over audit logs are periodically verified for integrity. SCV provides REST APIs to view logs and verify their integrity. A built-in schedule triggers and assigns one of the following integrity statuses.

Status	Description
TAMPERED	Audit log file content is modified
NORMAL	Audit log file is unmodified
ROLLOVER DELETE	- Audit log file is deleted based on retention - By default, only 10 files are retained
UNEXPECTED DELETE	Audit log file is deleted
ACTIVE	- Audit log file is in use - Only applicable to audit.log

Events are categorize into three major categories:

- Data Protection Events
- Maintenance Console Events
- Admin Console Events

Data Protection Events

The resources in SCV are:

- Storage System
- Resource Group
- Policy
- Backup

The following table lists the operations that can be performed on each resource:

Resources	Operations
Storage System	Created, Modified, Deleted
Resource Group	Created, Modified, Deleted, Suspended, Resumed
Policy	Created, Modified, Deleted

Backup	Created, Renamed, Deleted, Mounted, Unmounted, Restored VMDK, Restored VM, Attach VMDK, Detach VMDK, Guest File Restore

Maintenance Console Events

The administrative operations in the maintenance console are audited.
Available maintenance console options are:

1. Start / Stop services
2. Change username & password
3. Change MySQL password
4. Configure MySQL Backup
5. Restore MySQL Backup
6. Change 'maint' user password
7. Change time zone
8. Change NTP Server
9. Disable SSH access
10. Increase jail disk size
11. Upgrade
12. Install VMware Tools (We are working on replace this with open-vm tools)
13. Change IP address settings
14. Change domain name search settings
15. Change static routes
16. Access diagnostic shell
17. Enable remote diagnostic access

Admin Console Events

The following operations in the Admin Console UI are audited:

- Settings
  - Change admin credentials
  - Change timezone
  - Change NTP Server
  - Change IPv4 / IPv6 settings
- Configuration
  - Change vCenter Credentials
  - Plug-in Enable / Disable

Configure syslog servers

Audit logs are stored within the appliance and are periodically verified for integrity. Event forwarding allows the you to obtain events from the source or forwarding computer and store it in a centralized computer, which is the Syslog Server. Data is encrypted in transit between the source and the destination.

Before you begin

You must have administrator privileges.

About this task

This task helps you to configure the syslog server.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere.
2. In the left navigation pane, select **Settings** > **Audit Logs** > **Settings**.
3. In the **Audit Log Settings** pane, select **Send audit logs to Syslog server**
4. Enter the following details:
    - Syslog Server IP
    - Syslog Server Port
    - RFC format
    - Syslog Server Certificate
5. Click **SAVE** to save the Syslog server settings.

Change audit log settings

You can change the default configurations of the log settings.

Before you begin

You must have administrator privileges.

About this task

This task helps you to change the default audit log settings.

Steps

1. Log in to the SnapCenter Plug-in for VMware vSphere.
2. In the left navigation pane, select **Settings** > **Audit Logs** > **Settings**.
3. In the **Audit Log Settings** pane, enter the **Number of audit entries** and **Audit log size limit** according to your requirements.

Copyright information

Trademark information