Manage your configuration

SnapCenter Plug-in for VMware vSphere 5.0

NetApp
August 30, 2024

Table of Contents

Manage your configuration

Modify the time zones for backups

When you configure a backup schedule for a SnapCenter Plug-in for VMware vSphere resource group, the schedule is automatically set for the time zone in which SnapCenter VMware plug-in is deployed. You can modify that time zone by using the SnapCenter Plug-in for VMware vSphere management GUI or maintenance console.

Before you begin

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

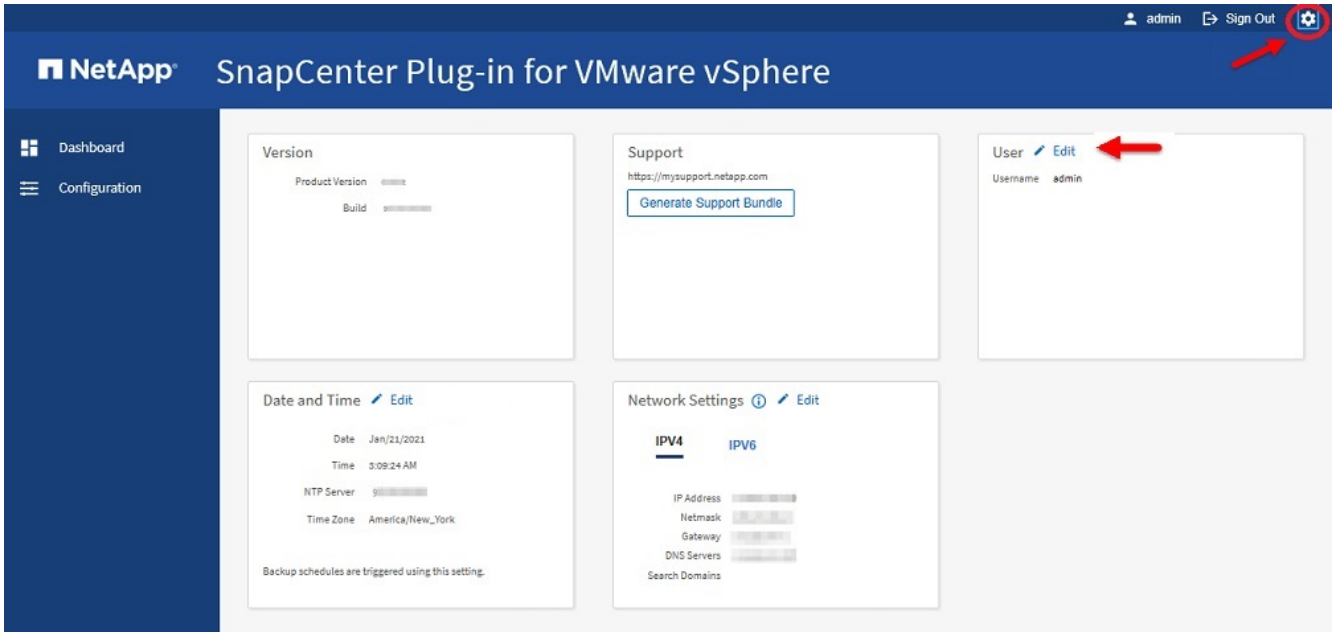
- The IP address was displayed when the SnapCenter VMware plug-in was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter VMware plug-in or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter VMware plug-in management GUI.

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

2. Click the Settings icon in the top toolbar.



3. On the **Settings** page, in the **Date and Time** section, click **Edit**.
4. Select the new time zone and click **Save**.

   The new time zone will be used for all backups performed by the SnapCenter VMware plug-in.

Modify the logon credentials

You can modify the logon credentials for the SnapCenter Plug-in for VMware vSphere management GUI.

Before you begin

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

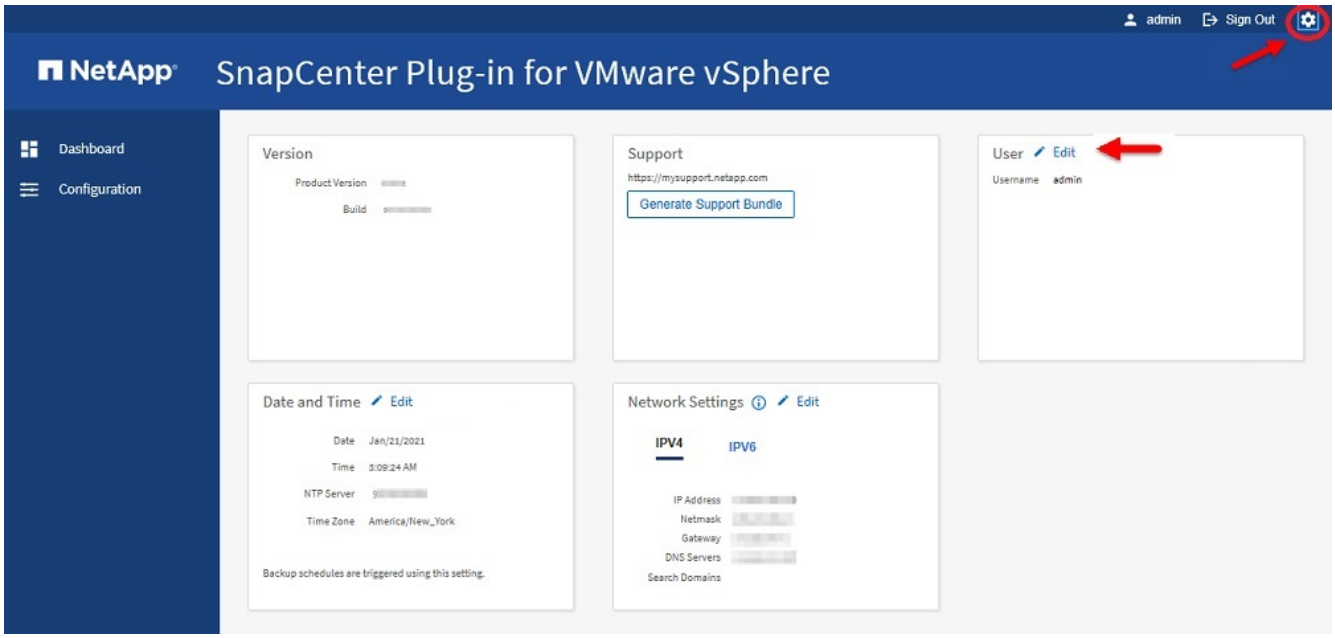
- The IP address was displayed when the SnapCenter VMware plug-in was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter VMware plug-in or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter VMware plug-in management GUI.

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

2. Click the Settings icon in the top toolbar.



3. On the **Settings** page, in the **User** section, click **Edit**.
4. Enter the new password and click **Save**.

   It might take several minutes before all the services come back up.

Modify the vCenter logon credentials

You can modify the vCenter logon credentials that are configured in SnapCenter Plug-in for VMware vSphere. These settings are used by the plug-in to access vCenter.
When you change the vCenter password, you need to unregister ONTAP tools for

VMware vSphere and re-registered it with the new password for the vVol backups to work seamlessly.

Before you begin

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

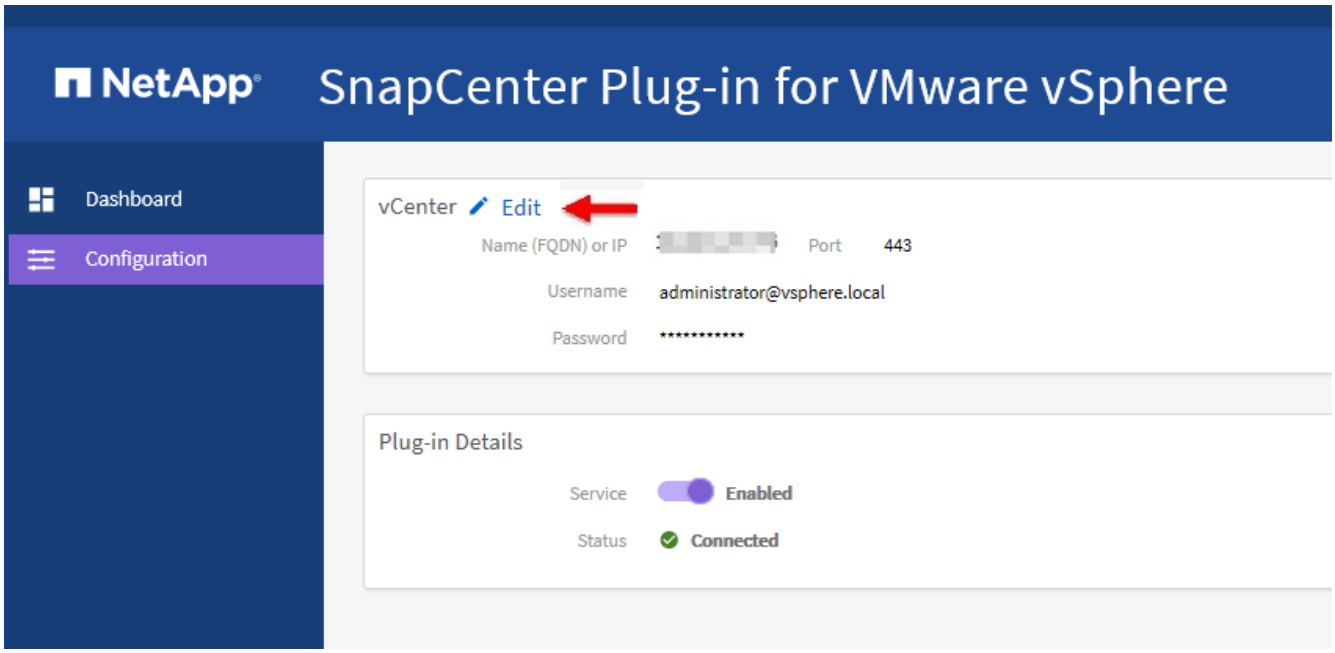
- The IP address was displayed when the SnapCenter VMware plug-in was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter VMware plug-in or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter VMware plug-in management GUI.

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

2. In the left navigation pane, click **Configuration**.



3. On the **Configuration** page, in the **vCenter** section, click **Edit**.
4. Enter the new password and then click **Save**.

   Do not modify the port number.

Modify the network settings

You can modify the network settings that are configured in SnapCenter Plug-in for VMware vSphere. These settings are used by the plug-in to access vCenter.

Before you begin

You must know the IP address and the log on credentials for the SnapCenter Plug-in for VMware vSphere

management GUI. You must also note down the MFA token generated from the maintenance console.

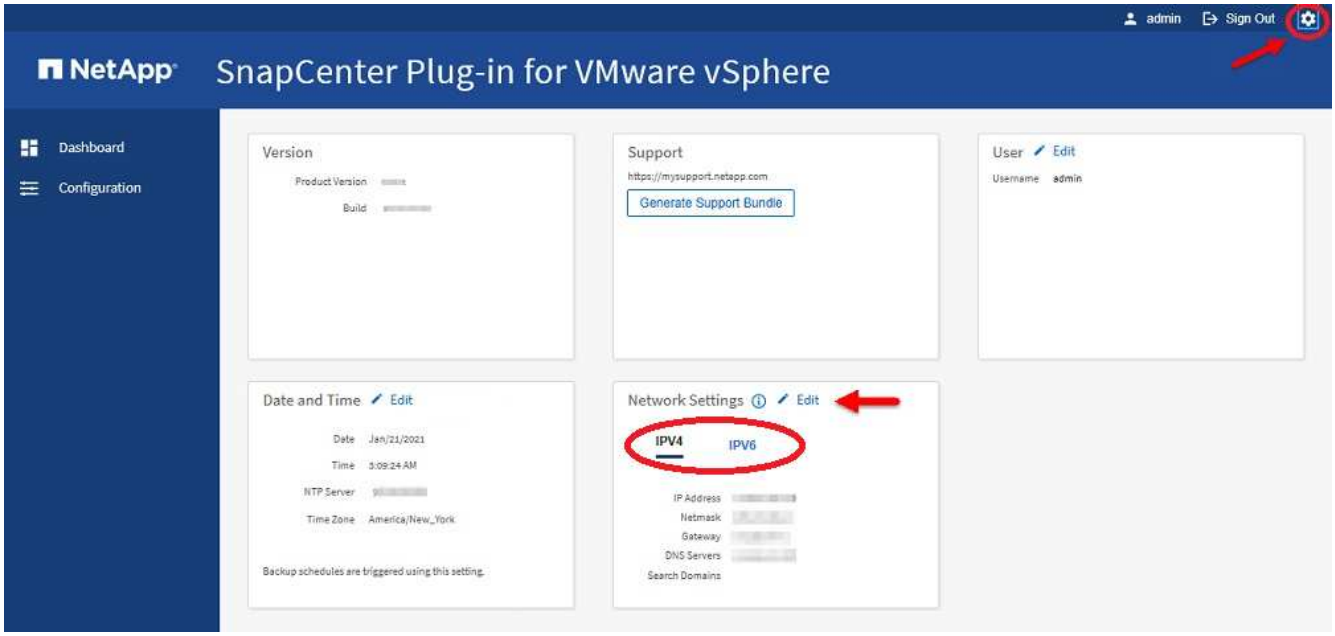
- The IP address was displayed when the SnapCenter VMware plug-in was deployed.
- Use the log in credentials provided during the deployment of the SnapCenter VMware plug-in or as later modified.
- Generate a 6-digit MFA token using the maintenance console System Configuration options.

Steps

1. Log in to the SnapCenter VMware plug-in management GUI.

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

2. Click the Settings icon in the top toolbar.



3. On the **Settings** page, in the **Network Settings** section, click **IPv4** or **IPv6**, and then click **Edit**.

   Enter the new information and click **Save**.

4. If you are removing a network setting, do the following:
   - IPv4: In the **IP Address** field, enter `0.0.0.0` and then click **Save**.
   - IPv6: In the **IP Address** field: enter `: :0` and then click **Save**.

> If you are using both IPv4 and IPv6, you cannot remove both network settings. The remaining network must specify the DNS Servers and Search Domains fields.

Modify configuration default values

To improve operational efficiency, you can modify the `scbr.override` configuration file to change default values. These values control settings such as the number of VMware snapshots that are created or deleted during a backup or the amount of time before a backup script stops running.

The `scbr.override` configuration file is used by the SnapCenter Plug-in for VMware vSphere in environments that support SnapCenter application-based data protection operations. If this file does not exist, then you must create it from the template file.

Create the scbr.override configuration file

The `scbr.override` configuration file is used by the SnapCenter Plug-in for VMware vSphere in environments that support SnapCenter application-based data protection operations.

1. Go to `/opt/netapp/scvservice/standalone_aegis/etc/scbr/scbr.override-template`.
2. Copy the `scbr.override-template` file to a new file called `scbr.override` in the `\opt\netapp\scvservice\standalone_aegis\etc\scbr` directory.

Properties you can override

You can use properties that are listed in the `scbr.override` configuration file to change default values.

- By default, the template uses hash symbol to comment the configuration properties. To use a property to modify a configuration value, you must remove the # characters.
- You must restart the service on the SnapCenter Plug-in for VMware vSphere host for the changes to take effect.

You can use the following properties that are listed in the `scbr.override` configuration file to change default values.

- **dashboard.protected.vm.count.interval=7**

  Specifies the number of days for which the dashboard displays VM protection status.

  The default value is "7".

- **disable.weakCiphers=true**

  Disables the following weakCiphers for the communication channel between SnapCenter Plug-in for VMware vSphere and SnapCenter, and any additional weakCiphers that are listed in `include.weakCiphers`:
  TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256
  TLS_RSA_WITH_AES_256_GCM_SHA384

- **global.ds.exclusion.pattern**

  Specifies one or more traditional or vVol datastores to be excluded from backup operations. You can specify the datastores using any valid Java regular expression.

  Example 1: The expression `global.ds.exclusion.pattern=.*21` excludes datastores that have a common pattern; for example `datastore21` and `dstest21` would be excluded.

Example 2: The expression `global.ds.exclusion.pattern=ds-.*|^vol123` excludes all datastores that contain `ds-` (for example `scvds-test`) or begin with `vol123`.

- **guestFileRestore.guest.operation.interval=5**

  Specifies the time interval, in seconds, that SnapCenter Plug-in for VMware vSphere monitors for completion of guest operations on the guest (Online Disk and Restore Files). The total wait time is set by `guestFileRestore.online.disk.timeout` and `guestFileRestore.restore.files.timeout`.

  The default value is "5".

- **guestFileRestore.monitorInterval=30**

  Specifies the time interval, in minutes, that the SnapCenter VMware plug-in monitors for expired guest file restore sessions. Any session that is running beyond the configured session time is disconnected.

  The default value is "30".

- **guestFileRestore.online.disk.timeout=100**

  Specifies the time, in seconds, that the SnapCenter VMware plug-in waits for an online disk operation on a guest VM to complete. Note that there is an additional 30-second wait time before the plug-in polls for completion of the online disk operation.

  The default value is "100".

- **guestFileRestore.restore.files.timeout=3600**

  Specifies the time, in seconds, that the SnapCenter VMware plug-in waits for a restore files operation on a guest VM to complete. If the time is exceeded, the process is ended and the job is marked as failed.

  The default value is "3600" (1 hour).

- **guestFileRestore.robocopy.directory.flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP**

  Specifies the extra robocopy flags to use when copying directories during guest file restore operations.

  Do not remove `/NJH` or add `/NJS` because this will break the parsing of the restore output.

  Do not allow unlimited retries (by removing the `/R` flag) because this might cause endless retries for failed copies.

  The default values are "`/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /e /NJH /NDL /NP`".

- **guestFileRestore.robocopy.file.flags=/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP**

  Specifies the extra robocopy flags to use when copying individual files during guest file restore operations.

  Do not remove `/NJH` or add `/NJS` because this will break the parsing of the restore output.

  Do not allow unlimited retries (by removing the `/R` flag) because this might cause endless retries for failed copies.

  The default values are "`/R:0 /W:0 /ZB /CopyAll /EFSRAW /A-:SH /NJH /NDL /NP`".

- **guestFileRestore.sessionTime=1440**

  Specifies the time, in minutes, that SnapCenter Plug-in for VMware vSphere keeps a guest file restore session active.

  The default value is "1440" (24 hours).

- **guestFileRestore.use.custom.online.disk.script=true**

  Specifies whether to use a custom script for onlining disks and retrieving drive letters when creating guest file restore sessions. The script must be located at `[Install Path] \etc\guestFileRestore_onlineDisk.ps1`. A default script is provided with the installation. The values `[Disk_Serial_Number]`, `[Online_Disk_Output]`, and `[Drive_Output]` are replaced in the script during the attach process.

  The default value is "false".

- **include.esx.initiator.id.from.cluster=true**

  Specifies that the SnapCenter VMware plug-in should include iSCSI and FCP initiator IDs from all the ESXi hosts in the cluster in the application over VMDK workflows.

  The default value is "false".

- **include.weakCiphers**

  When `disable.weakCiphers` is set to `true`, specifies the weak ciphers that you want to be disabled in addition to the weak ciphers that `disable.weakCiphers` disables by default.

- **max.concurrent.ds.storage.query.count=15**

  Specifies the maximum number of concurrent calls that the SnapCenter VMware plug-in can make to the SnapCenter Server to discover the storage footprint for the datastores. The plug-in makes these calls when you restart the Linux service on the SnapCenter VMware plug-in VM host.

- **nfs.datastore.mount.retry.count=3**

  Specifies the maximum number of times the SnapCenter VMware plug-in tries to mount a volume as a NFS Datastore in vCenter.

  The default value is "3".

- **nfs.datastore.mount.retry.delay=60000**

  Specifies the time, in milliseconds, that the SnapCenter VMware plug-in waits between attempts to mount a volume as a NFS Datastore in vCenter.

  The default value is "60000" (60 seconds).

- **script.virtual.machine.count.variable.name= VIRTUAL_MACHINES**

  Specifies the environmental variable name that contains the virtual machine count. You must define the variable before you execute any user-defined scripts during a backup job.

  For example, VIRTUAL_MACHINES=2 means that two virtual machines are being backed up.

- **script.virtual.machine.info.variable.name=VIRTUAL_MACHINE.%s**

  Provides the name of the environmental variable that contains information about the nth virtual machine in the backup. You must set this variable before executing any user defined scripts during a backup.

  For example, the environmental variable VIRTUAL_MACHINE.2 provides information about the second virtual machine in the backup.

- **script.virtual.machine.info.format= %s|%s|%s|%s|%s**

  Provides information about the virtual machine. The format for this information, which is set in the environment variable, is the following: `VM name|VM UUID| VM power state (on|off)|VM snapshot taken (true|false)|IP address(es)`

  The following is an example of the information you might provide:

  ```
  VIRTUAL_MACHINE.2=VM 1|564d6769-f07d-6e3b-
  68b1f3c29ba03a9a|POWERED_ON||true|10.0.4.2
  ```

- **storage.connection.timeout=600000**

  Specifies the amount of time, in milliseconds, that the SnapCenter Server waits for a response from the storage system.

  The default value is "600000" (10 minutes).

- **vmware.esx.ip.kernel.ip.map**

  There is no default value. You use this value to map the ESXi IP address to the VMkernel IP address. By default, the SnapCenter VMware plug-in uses the management VMkernel adapter IP address of the ESXi host. If you want the SnapCenter VMware plug-in to use a different VMkernel adapter IP address, you must provide an override value.

  In the following example, the management VMkernel adapter IP address is 10.225.10.56; however, the SnapCenter VMware plug-in uses the specified address of 10.225.11.57 and 10.225.11.58. And if the management VMkernel adapter IP address is 10.225.10.60, the plug-in uses the address 10.225.11.61.

  ```
  vmware.esx.ip.kernel.ip.map=10.225.10.56:10.225.11.57,10.225.11.58;
  10.225.10.60:10.225.11.61
  ```

- **vmware.max.concurrent.snapshots=30**

  Specifies the maximum number of concurrent VMware snapshots that the SnapCenter VMware plug-in performs on the server.

  This number is checked on a per datastore basis and is checked only if the policy has "VM consistent" selected. If you are performing crash-consistent backups, this setting does not apply.

  The default value is "30".

- **vmware.max.concurrent.snapshots.delete=30**

  Specifies the maximum number of concurrent VMware snapshot delete operations, per datastore, that the SnapCenter VMware plug-in performs on the server.

This number is checked on a per datastore basis.

The default value is "30".

- **vmware.query.unresolved.retry.count=10**

  Specifies the maximum number of times the SnapCenter VMware plug-in retries sending a query about unresolved volumes because of "…time limit for holding off I/O…" errors.

  The default value is "10".

- **vmware.quiesce.retry.count=0**

  Specifies the maximum number of times the SnapCenter VMware plug-in retries sending a query about VMware snapshots because of "…time limit for holding off I/O…" errors during a backup.

  The default value is "0".

- **vmware.quiesce.retry.interval=5**

  Specifies the amount of time, in seconds, that the SnapCenter VMware plug-in waits between sending the queries regarding VMware snapshot "…time limit for holding off I/O…" errors during a backup.

  The default value is "5".

- **vmware.query.unresolved.retry.delay= 60000**

  Specifies the amount of time, in milliseconds, that the SnapCenter VMware plug-in waits between sending the queries regarding unresolved volumes because of "…time limit for holding off I/O…" errors. This error occurs when cloning a VMFS datastore.

  The default value is "60000" (60 seconds).

- **vmware.reconfig.vm.retry.count=10**

  Specifies the maximum number of times the SnapCenter VMware plug-in retries sending a query about reconfiguring a VM because of "…time limit for holding off I/O…" errors.

  The default value is "10".

- **vmware.reconfig.vm.retry.delay=30000**

  Specifies the maximum time, in milliseconds, that the SnapCenter VMware plug-in waits between sending queries regarding reconfiguring a VM because of "…time limit for holding off I/O…" errors.

  The default value is "30000" (30 seconds).

- **vmware.rescan.hba.retry.count=3**

  Specifies the amount of time, in milliseconds, that the SnapCenter VMware plug-in waits between sending the queries regarding rescanning the host bus adapter because of "…time limit for holding off I/O…" errors.

  The default value is "3".

- **vmware.rescan.hba.retry.delay=30000**

Specifies the maximum number of times the SnapCenter VMware plug-in retries requests to rescan the host bus adapter.

The default value is "30000".

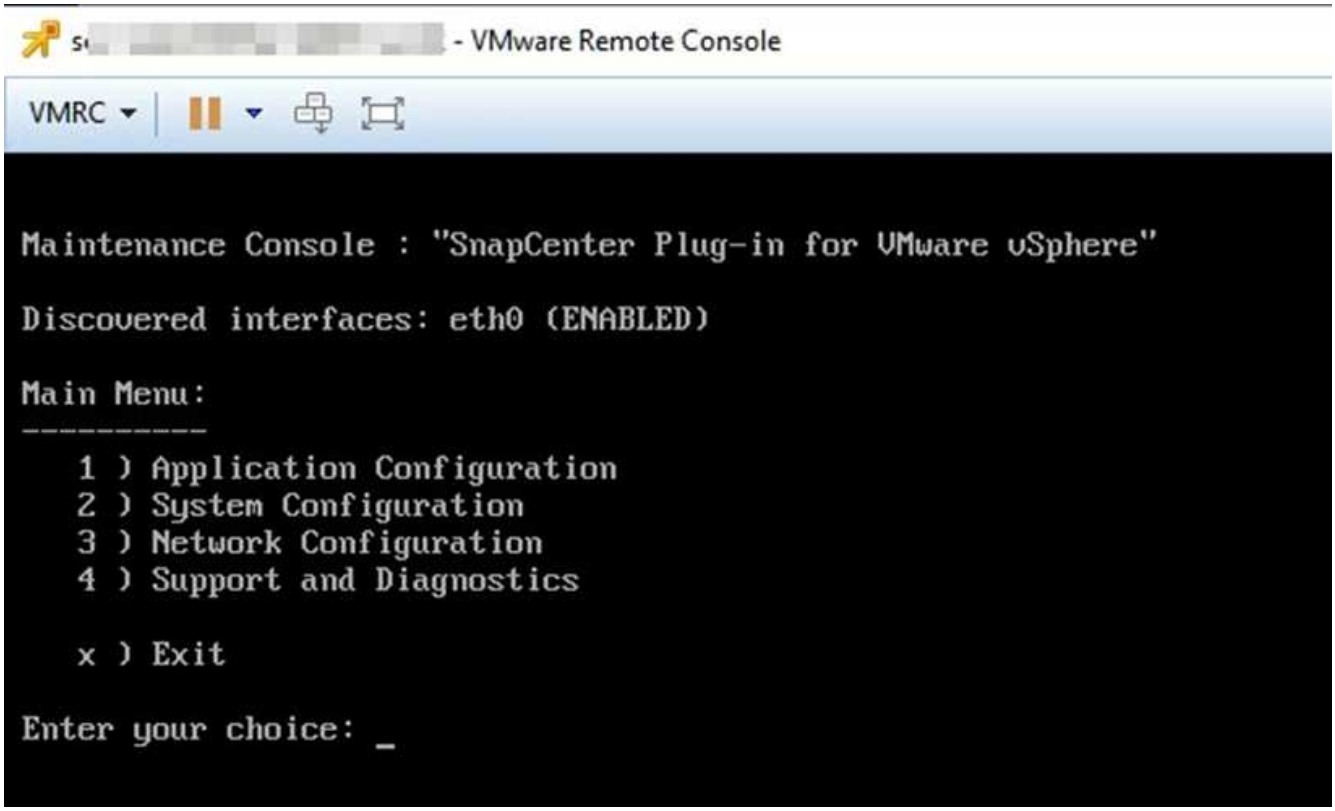
Enable SSH for SnapCenter Plug-in for VMware vSphere

When the SnapCenter VMware plug-in is deployed, SSH is disabled by default.

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** 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, select menu option **2) System Configuration**.
4. From the System Configuration Menu, select menu option **6) Enable SSH access** and then enter “**y**” at the confirmation prompt.
5. Wait for the message “Enabling SSH Access…” then press **Enter** to continue, and then enter **X** at the prompt to exit Maintenance Mode.

Copyright information

Trademark information