

NetBackup™ Add-in for Microsoft SCVMM Console Guide

Release 11.0

NetBackup™ Add-in for Microsoft SCVMM Console Guide

Last updated: 2025-03-05

Legal Notice

Copyright © 2025 Cohesity, Inc. All rights reserved.

Cohesity, Veritas, the Cohesity Logo, Veritas Logo, Veritas Alta, Cohesity Alta, and NetBackup are trademarks or registered trademarks of Cohesity, Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Cohesity is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Cohesity product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Cohesity, Inc. and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Cohesity, Inc. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Cohesity as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Cohesity, Inc.
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Cohesity account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Cohesity website:

<https://sort.veritas.com/documents>

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Cohesity community site:

<http://www.veritas.com/community/>

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Introduction and notes	6
	About the NetBackup Add-in for System Center Virtual Machine Manager (SCVMM)	6
	Notes on the NetBackup Add-in for SCVMM	7
Chapter 2	Installing the NetBackup Add-in for SCVMM	8
	Requirements for the NetBackup Add-in for SCVMM	8
	Installing the NetBackup Add-in for SCVMM	8
	Installation message: Add-in cannot be installed	14
	Installation message regarding localized environments	17
	Configuring the add-in for an external certificate	18
	Reconfiguring the add-in for a NetBackup CA-signed certificate	19
	Uninstalling the NetBackup Add-in for SCVMM	21
	Configuring the NetBackup Recovery Wizard	21
	Creating an authentication token for the NetBackup add-in for SCVMM	22
	Authorizing the NetBackup add-in to restore virtual machines	24
	Adding or deleting an additional host name or IP address for an authentication token	28
	Revoking an authorization token	31
	Renewing an authorization token	32
	Listing all current authorization tokens	33
Chapter 3	Recovering virtual machines	35
	Notes on restoring Hyper-V virtual machines with the Recovery Wizard	35
	Accessing the Recovery Wizard	36
	Restore Virtual Machine Wizard screens	37
	Virtual Machine Selection screen	37
	Backup Image Selection screen	38
	Select Another Image screen	40
	Restore Options screen	40
	Review Settings screen	43

	Checking the status of a recovery job	44
Chapter 4	Troubleshooting	47
	About logging for the NetBackup Add-in for SCVMM	47
	Viewing log messages for the NetBackup Add-in for SCVMM	48
	Changing the logging level for the NetBackup Add-in for SCVMM	50
	The pre-recovery checks in the Recovery Wizard of the NetBackup Add-in for SCVMM return out-of-date information about the VM	51
	Next button in the NetBackup Add-in Recovery Wizard is enabled even though required input has not been entered	52
	The NetBackup Add-in Recovery Wizard does not prompt to overwrite the VM, and the recovery fails	53
	Troubleshooting primary server communication failures in the NetBackup Add-in for SCVMM	53

Introduction and notes

This chapter includes the following topics:

- [About the NetBackup Add-in for System Center Virtual Machine Manager \(SCVMM\)](#)
- [Notes on the NetBackup Add-in for SCVMM](#)

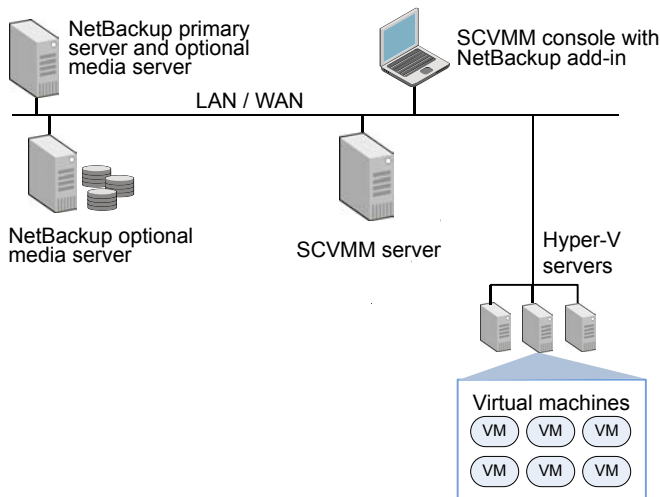
About the NetBackup Add-in for System Center Virtual Machine Manager (SCVMM)

You can use the NetBackup Add-in for Microsoft System Center Virtual Machine Manager (SCVMM) to recover virtual machines from NetBackup backup images.

You can use the add-in to do the following in the SCVMM console:

- Recover the full virtual machine to its original location or to an alternate location.
- Monitor the progress of recovery jobs that the add-in initiated.

[Figure 1-1](#) shows an SCVMM environment with NetBackup servers and the NetBackup add-in.

Figure 1-1 NetBackup and SCVMM environment with NetBackup add-in

Notes on the NetBackup Add-in for SCVMM

Note the following about the NetBackup add-in:

- This release of the NetBackup add-in for SCVMM does not support the following: Monitoring of virtual machine backups, restore of individual files from virtual machine backups, or restore of the virtual machine to a staging location. See [“Notes on restoring Hyper-V virtual machines with the Recovery Wizard”](#) on page 35.
- To use the NetBackup add-in, you must log on to the SCVMM console with the Administrator role. For any user that is logged on with a different role, the add-in functionality is disabled.
- The NetBackup add-in must be installed by every user who wants to use it. See [“Accessing the Recovery Wizard”](#) on page 36.
- Regarding future versions of the NetBackup Add-in for SCVMM: Due to Microsoft limitations on 3rd party add-ins, the NetBackup add-in does not support upgrades to the existing version of the add-in. When a new release of the add-in is available, the current version must be uninstalled.

Note: You can upgrade SCVMM without needing to reinstall the add-in.

Installing the NetBackup Add-in for SCVMM

This chapter includes the following topics:

- [Requirements for the NetBackup Add-in for SCVMM](#)
- [Installing the NetBackup Add-in for SCVMM](#)
- [Installation message: Add-in cannot be installed](#)
- [Installation message regarding localized environments](#)
- [Configuring the add-in for an external certificate](#)
- [Reconfiguring the add-in for a NetBackup CA-signed certificate](#)
- [Uninstalling the NetBackup Add-in for SCVMM](#)
- [Configuring the NetBackup Recovery Wizard](#)

Requirements for the NetBackup Add-in for SCVMM

For a list of supported NetBackup versions and SCVMM versions, see the *NetBackup Software Compatibility List* (SCL) available from the following location:

[NetBackup Compatibility List for all Versions](#)

Installing the NetBackup Add-in for SCVMM

This topic describes how to obtain the installation files and install the NetBackup Add-in for SCVMM.

Table 2-1 NetBackup Add-in for SCVMM: installation requirements

Requirement	Notes
NetBackup add-in installation file	You can download the installation file <code>NetBackup_11.0_Plugins.zip</code> from the following location: https://my.veritas.com/
SCVMM console host	Download the installation .zip file to the SCVMM console host, or to a different Windows host. Note: The Windows host must have network connectivity to the SCVMM server.
SCVMM server(s) and their credentials	When the add-in is installed, it runs in the SCVMM console. The following are required to complete the add-in installation: <ul style="list-style-type: none">■ Host name or IP address of each SCVMM server.■ User name and password of each SCVMM server.■ Port number for each SCVMM server (default is 443).
Additional user access	Additional user access may be needed in the following situation: <ul style="list-style-type: none">■ User Account Control is enabled on the SCVMM console host.■ The user who installs the add-in is not the user who installed the System Center. See “Installation message: Add-in cannot be installed” on page 14.

To install the NetBackup Add-in for SCVMM

- 1 On the MyVeritas website, log on with your MyVeritas account:
<https://my.veritas.com/>
For logon assistance, see your account Administrator, or contact Cohesity:
[Veritas Support](#)
Email: CustomerCare@veritas.com
- 2 Click **Licensing** on the **MyVeritas** menu bar.
The Veritas Entitlement Management System (VEMS) appears.
- 3 Click **Entitlements**, then click **More Options**.
- 4 In the **Product Name** field, enter NetBackup and click **Apply Filters**.
Your NetBackup product entitlements appear in the list.

- 5 For one of the NetBackup products in the list, click the Download Product icon under **Actions**.

A list of NetBackup product versions appears.

- 6 For one of the NetBackup products, click the Download Product icon again.
- 7 Select the `NetBackup_11.0_Plugins.zip` file and download the file to the SCVMM console host.

For assistance with the Veritas Entitlement Management System, see the following article:

[Veritas Entitlement Management User's Guide](#)

- 8 Unzip the downloaded `NetBackup_11.0_Plugins.zip` file and locate the `VRTSNBUAddIn.zip` file.

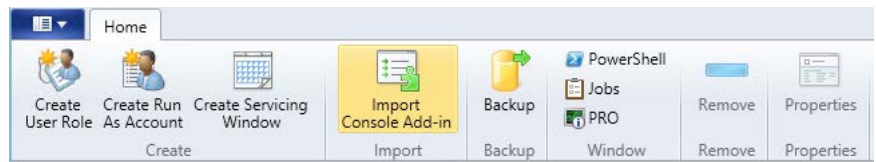
The path to the `VRTSNBUAddIn.zip` file is the following:

```
\NB_11.0_Plugins\NBscvmmAddIn\NetBackup_scvmmAddIn_Win\VRTSNBUAddIn.zip
```

Note: Do not unzip the `VRTSNBUAddIn.zip` file. That zip file is needed for installation of the add-in.

Zip files for other NetBackup plug-ins are also included in the downloaded `NetBackup_11.0_Plugins.zip` file. Those files are not required for the NetBackup Add-in for SCVMM.

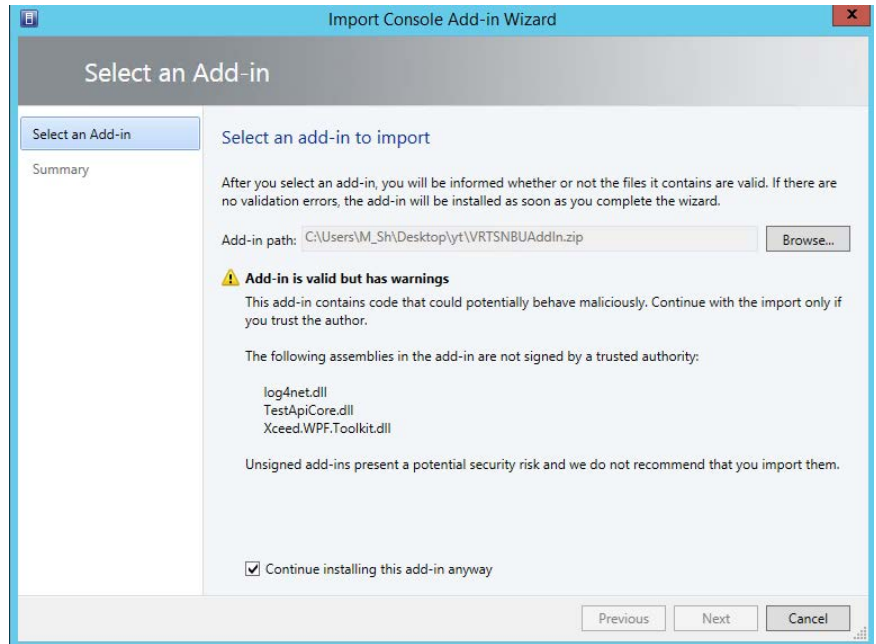
- 9 Launch the SCVMM console and connect to the SCVMM server.
You need the server's host name or IP address, and its logon credentials.
- 10 In the SCVMM console, open the **Settings** workspace, then click the **Import Console Add-in** option in the SCVMM ribbon.



The **Import Console Add-in Wizard** appears.

- 11** In the **Select an Add-in** screen, click **Browse** and browse for the `VRTSNBUAddIn.zip` file.

Several warnings appear. These warnings can be safely ignored.



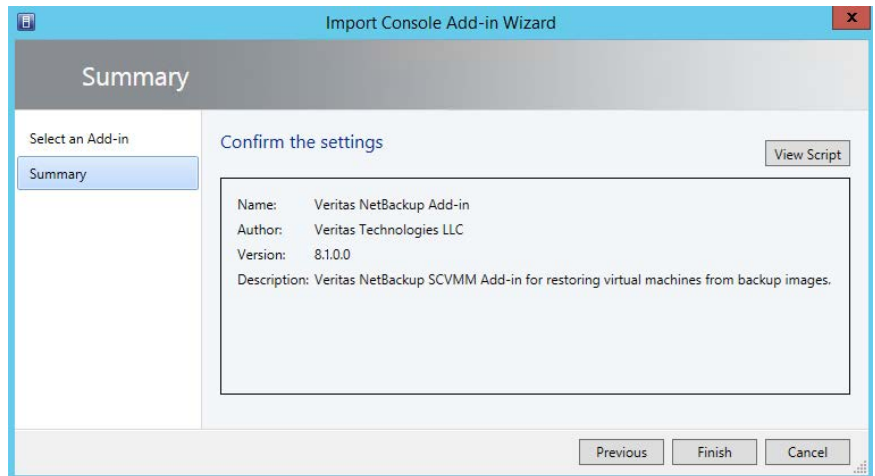
- 12** Click **Continue installing this add-in anyway**.

If the **Import Console Add-in Wizard** states "The Add-in cannot be installed," you may need additional user access.

See ["Installation message: Add-in cannot be installed"](#) on page 14.

When you have the required user access, browse for the NetBackup add-in file again (step 11) and continue this installation procedure.

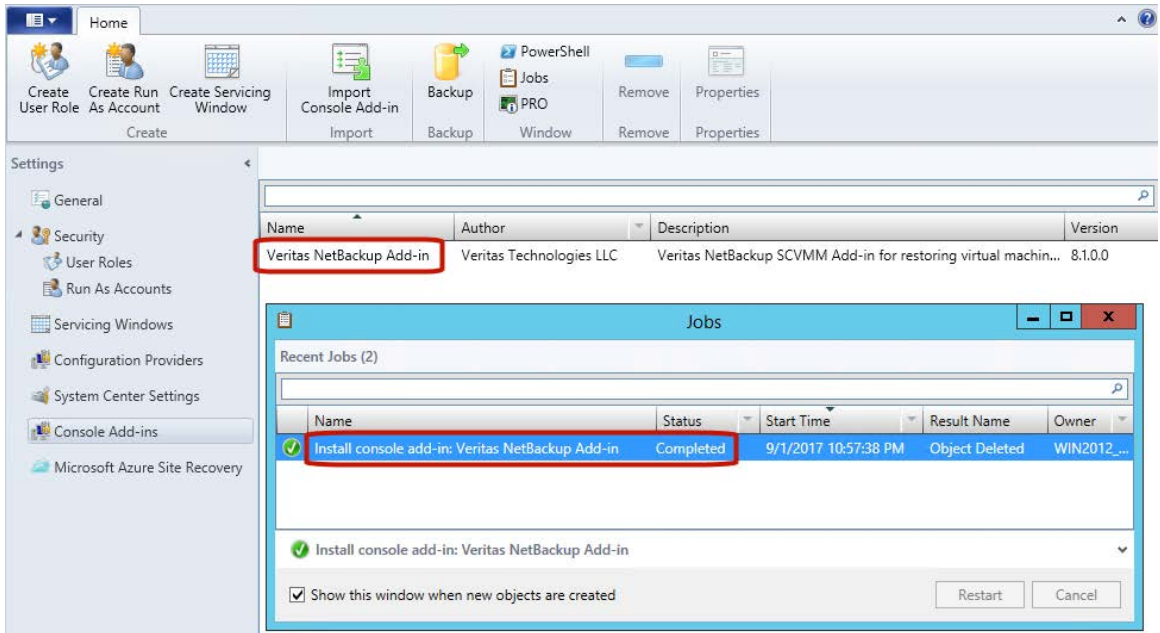
13 On the **Summary** screen, click **Finish**.



If the NetBackup add-in is installed on a Windows host that has a non-English system locale, SCVMM may issue a message when the installation completes.

See [“Installation message regarding localized environments”](#) on page 17.

The imported add-in appears in the **Jobs** window of the SCVMM console, and in the **Settings** workspace under **Console Add-ins**.



- 14 If you had logged into the SCVMM console with your own credentials, restart the SCVMM console when prompted.

Note: If you selected the **Use current Microsoft Windows session identity** option, a restart is not required.

Note: To use the NetBackup add-in, you must log on to the SCVMM console with the Administrator role. If you log on to SCVMM with a different role, the add-in functionality is disabled.

Note: The first time you use the NetBackup add-in, an End User License Agreement (EULA) appears. To use the add-in, you must accept the EULA.

- 15 If the NetBackup primary server uses an external certificate, see the following topic:

See [“Configuring the add-in for an external certificate”](#) on page 18.

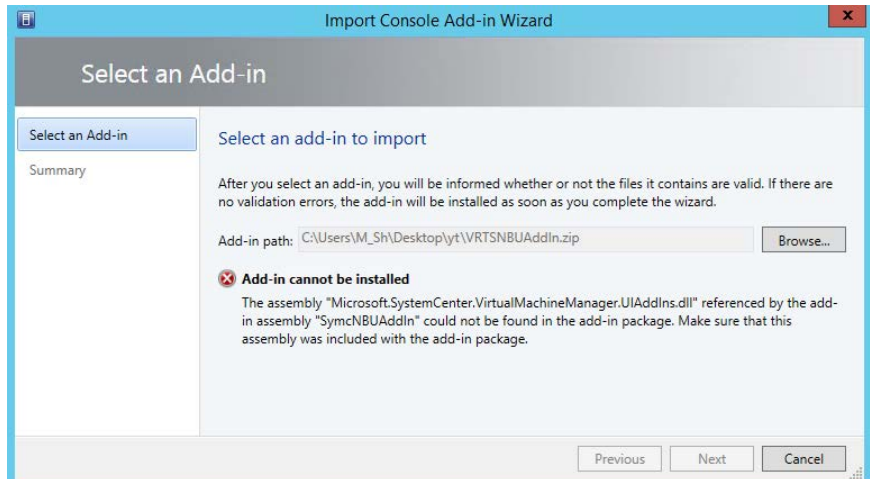
Installation message: Add-in cannot be installed

Lack of user permissions may cause the error "Add-in cannot be installed" during installation of the NetBackup Add-in for SCVMM.

For example, the error may occur in the following situation:

- User Account Control is enabled on the SCVMM console host, and
- The user who installs the add-in on the SCVMM console is not the user who installed the System Center.

During the add-in installation, the following message appears:

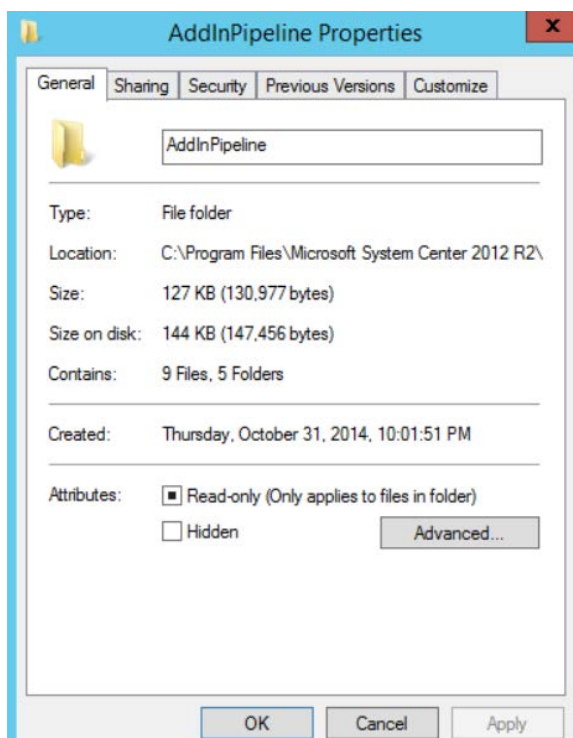


To grant installation permissions to all authenticated users on the SCVMM console host

- 1 On the SCVMM console host, browse to the following location:

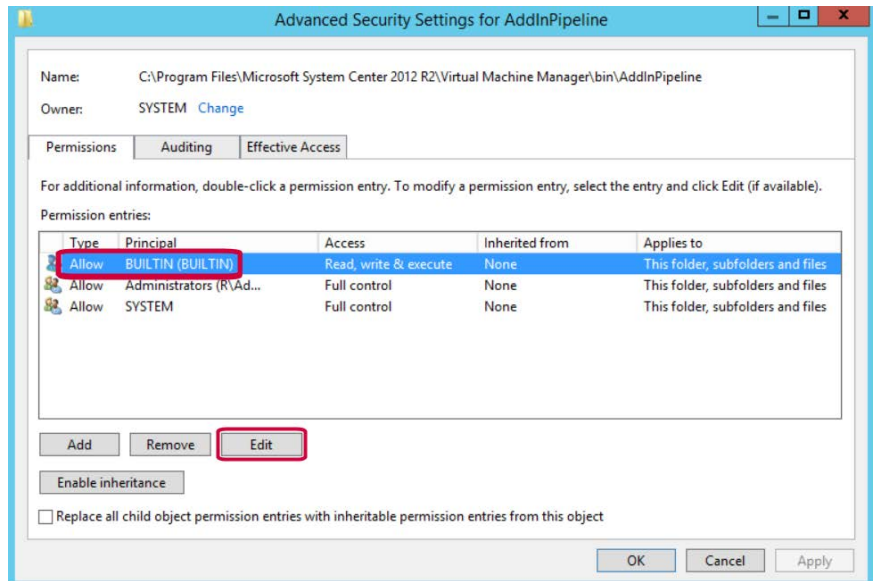
C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\bin

- 2 Right-click the AddInPipeline folder, and click **Properties**.

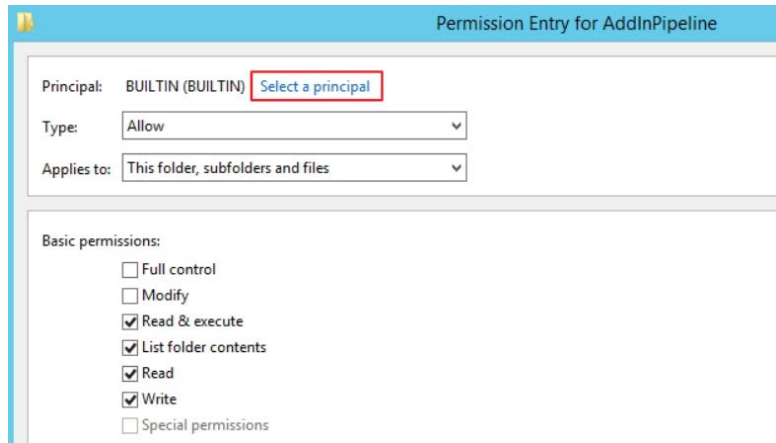


- 3 Click **Advanced** on the **Security** tab, and click **Continue**.

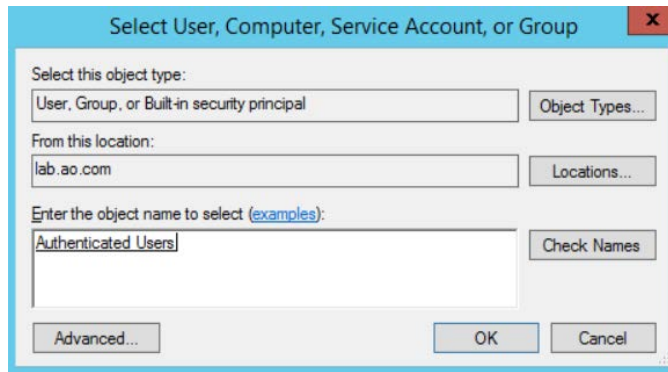
- 4 Select the **BUILTIN** group, and click **Edit**.



- 5 Click **Select a principal**.



- 6 Enter **Authenticated Users**, and click **OK**.



- 7 To close each properties dialog, click **OK**.

The following Microsoft article contains further information on this issue:

<http://support.microsoft.com/kb/2904712>

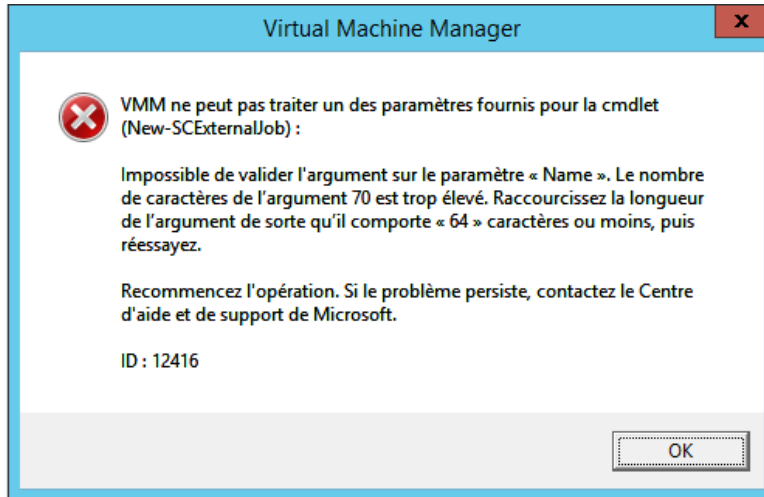
- 8 To install the NetBackup Add-in for SCVMM:

See [“Installing the NetBackup Add-in for SCVMM”](#) on page 8.

Installation message regarding localized environments

If the NetBackup add-in is installed on a Windows host that has a non-English system locale, SCVMM may issue a message when the installation completes. The message states that an argument cannot be validated because it contains more than 64 characters. The error results from a Microsoft limitation on the length of the add-in name, which varies with the selected locale.

For example: The following appears if Windows was set to the French system locale:



Note: This message can be ignored. The add-in is installed correctly.

Configuring the add-in for an external certificate

The add-in communicates with the NetBackup primary server securely by means of certificate-based authentication. By default, the primary server uses NetBackup CA-signed certificates. As an alternative, the primary server can be configured to use an externally issued certificate. In that case, use the following procedure to configure the add-in for the external certificate.

Configure the add-in for an external certificate

- 1 Enter the following command on the primary server:

Windows

```
install_path\NetBackup\wmc\bin\install\configureCertsForPlugins.bat
-registerExternalCert -certPath "path_to_external_certificate_file"
-privateKeyPath "path_to_certificate_key_file"
-trustStorePath "path_to_ca_certificate_file"
```

UNIX, Linux

```
/usr/opensv/wmc/bin/install/configureCertsForPlugins
-registerExternalCert -certPath "path_to_external_certificate_file"
-privateKeyPath "path_to_certificate_key_file"
-trustStorePath "path_to_ca_certificate_file"
```

For example:

```
configureCertsForPlugins.bat -registerExternalCert -certPath  
"c:\server.pem" -privateKeyPath "c:\key.pem" -trustStorePath  
"c:\intermediateOrRootCA.pem"
```

This command configures the add-in to use the external certificate by importing the certificate into the keystore on the primary server. The command options are as follows:

- **-certPath:** Specifies the path to the certificate for the web server. This file should have a single certificate in PEM format.
- **-privateKeyPath:** Specifies the path to the private key for the web server certificate.
- **-trustStorePath:** Specifies the path to the certificate of the intermediate or root certification authority that has issued the web server certificate. This file should have a single certificate in PEM format. The subject of this certificate should match the issuer of the web server certificate.

For further information on external certificates, see the [NetBackup Security and Encryption Guide](#).

- 2 Restart the `NetBackup Web Management Console` service on the primary server.

In the Activity monitor: Select the **Daemons** tab. Locate the service and select **Actions > Stop**. When the service has stopped, select **Actions > Start**.

- 3 Renew the authentication token on the primary server:

See [“Renewing an authorization token”](#) on page 32.

Note: Perform this step for each add-in that needs to communicate with the primary server.

- 4 On the add-in, remove the existing primary server and then add the primary server that now has the renewed token:

See [“Authorizing the NetBackup add-in to restore virtual machines”](#) on page 24.

Reconfiguring the add-in for a NetBackup CA-signed certificate

If the primary server is reconfigured to use a NetBackup CA-signed certificate, use the following procedure to configure the add-in for that certificate.

Reconfigure the add-in to use a NetBackup CA-signed certificate

- 1 Enter the following command on the primary server:

Windows

```
install_path\NetBackup\wmc\bin\install\configureCertsForPlugins.bat  
-registerNBCAcert
```

UNIX/Linux:

```
/usr/opensv/wmc/bin/install/configureCertsForPlugins  
-registerNBCAcert
```

This command reconfigures the add-in to use the NetBackup CA-signed certificate.

- 2 Restart the NetBackup Web Management Console service on the primary server.

In the Activity monitor: Select the **Daemons** tab. Locate the service and select **Actions > Stop**. When the service has stopped, select **Actions > Start**.

- 3 Renew the authentication token on the primary server:

See [“Renewing an authorization token”](#) on page 32.

Note: Perform this step for each add-in that needs to communicate with the primary server.

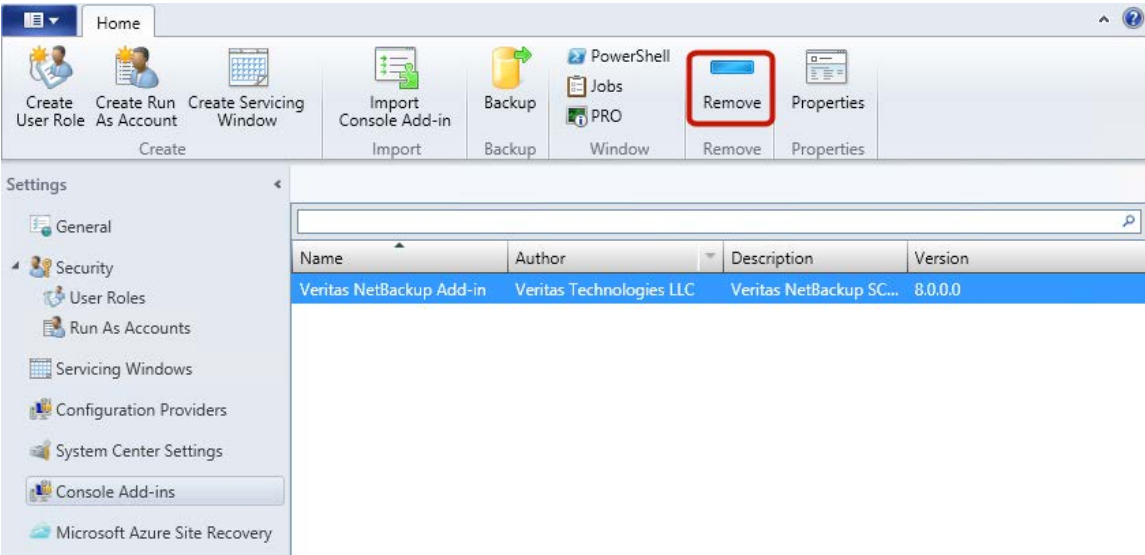
- 4 On the add-in, remove the existing primary server and then add the primary server that now has the renewed token:

See [“Authorizing the NetBackup add-in to restore virtual machines”](#) on page 24.

Uninstalling the NetBackup Add-in for SCVMM

To uninstall the NetBackup Add-in for SCVMM

- 1
- In the SCVMM console, open the **Settings** workspace.
- 2
- In the **Console Add-ins** node, click on the Veritas NetBackup Add-in and then click **Remove**.



- 3
- When you are prompted to confirm the removal, click **Yes**.
The uninstallation should appear in the **Jobs** window of the SCVMM console.

Configuring the NetBackup Recovery Wizard

To use the NetBackup Recovery Wizard to restore virtual machines, configure the following:

Table 2-2 Configuring the NetBackup Recovery Wizard

Step	Description	Reference topic
1	Create an authentication token file.*	See “Creating an authentication token for the NetBackup add-in for SCVMM” on page 22.

Table 2-2 Configuring the NetBackup Recovery Wizard (*continued*)

Step	Description	Reference topic
2	Authorize the NetBackup Add-in to restore virtual machines.	See “Authorizing the NetBackup add-in to restore virtual machines” on page 24.

*In certain circumstances, it may be necessary to associate an authentication token with additional SCVMM console host names or IP addresses:

See [“Adding or deleting an additional host name or IP address for an authentication token”](#) on page 28.

Creating an authentication token for the NetBackup add-in for SCVMM

To allow the add-in to restore VMs, generate an authentication token on the NetBackup primary server (or certificate on the NetBackup appliance as primary server). When an authentication token is created on a primary server and deployed on the NetBackup add-in, it allows that add-in to restore any Hyper-V backups from that primary server.

To create an authentication token on the NetBackup primary server

- 1 Enter the following on the primary server:

Windows

```
install_path\NetBackup\wmc\bin\install\manageClientCerts.bat  
-create clientName
```

UNIX, Linux

```
/usr/openv/wmc/bin/install/manageClientCerts -create clientName
```

clientName is the DNS name of the SCVMM console host where the add-in is installed. The `manageClientCerts` command returns the location of a compressed file that contains the authentication token.

Note: If the SCVMM console host is a separate host from the SCVMM server, generate the token for the SCVMM console host (not for the SCVMM server host name).

- 2 Provide the compressed authentication token file to the SCVMM server administrator.

Caution: Be sure to share or send the compressed file in a secure manner.

With the primary server token, the add-in can be authorized to restore virtual machines.

See “[Authorizing the NetBackup add-in to restore virtual machines](#)” on page 24.

To create an authentication token (certificate) on the NetBackup appliance as primary server

- 1 To generate the certificate, see the "Manage > Certificates" topic in the *NetBackup Appliance Administrator's Guide*, available from this location:

<http://www.veritas.com/docs/000002217>

- 2 Provide the compressed certificate file to the SCVMM administrator.

Caution: Be sure to share or send the compressed file in a secure manner.

With the primary server certificate, the add-in can be authorized to restore virtual machines.

See “[Authorizing the NetBackup add-in to restore virtual machines](#)” on page 24.

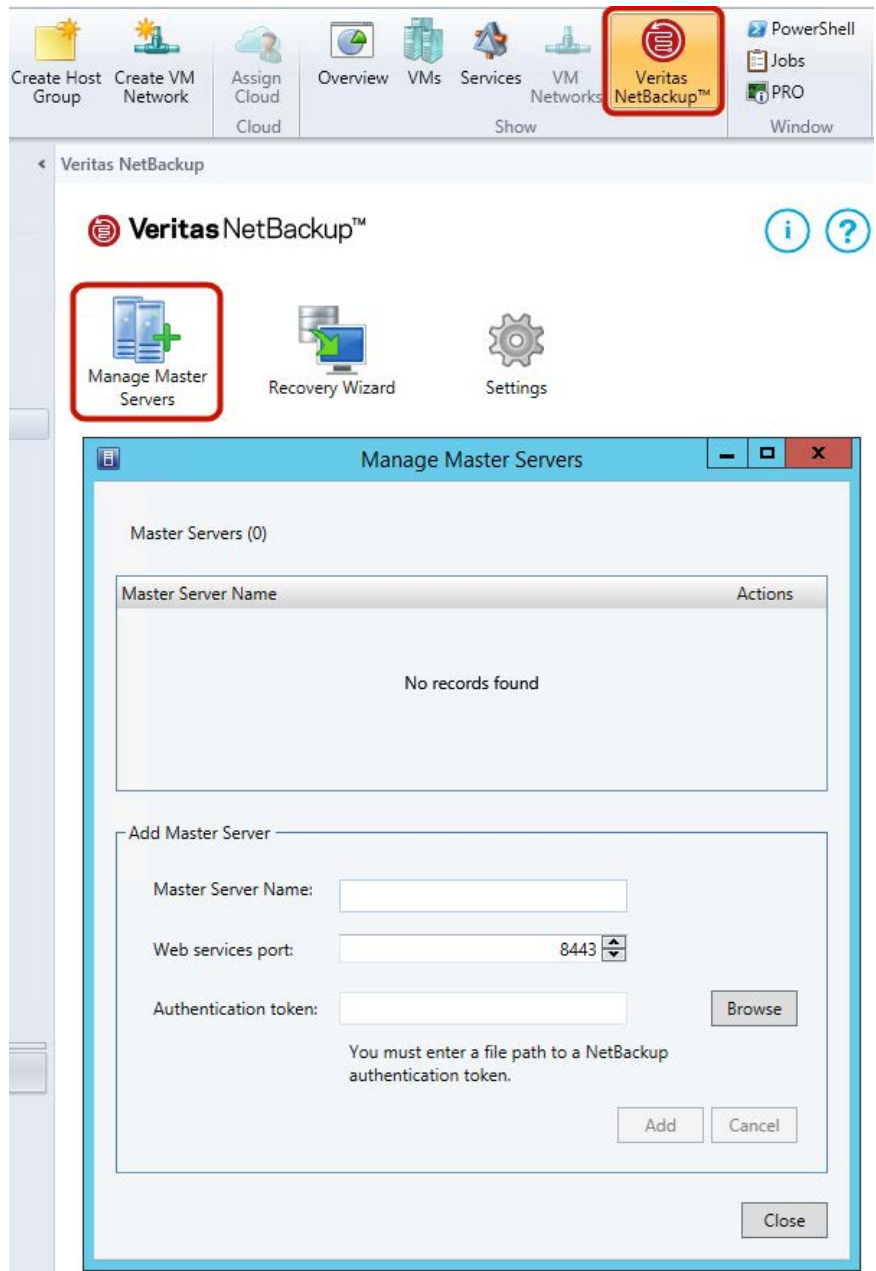
Authorizing the NetBackup add-in to restore virtual machines

The NetBackup primary server initiates and controls the backup of virtual machines. To use the add-in to restore virtual machines, you must obtain a primary server authentication token from the NetBackup administrator. Then you can authorize the add-in to restore the virtual machines that were backed up by that primary server.

To authorize the add-in to restore virtual machines (or to edit or delete an authorization)

- 1 Ask the NetBackup administrator to provide an authentication token file.
See [“Creating an authentication token for the NetBackup add-in for SCVMM”](#) on page 22.
- 2 Copy the authentication token file to the computer or laptop where the SCVMM console is launched.
Make a note of the location.
- 3 In the SCVMM console ribbon, click the **NetBackup** option.

4 Click **Manage Master Servers**.



- 5 Enter the following under **Add Master Server** to specify a NetBackup primary server and its authentication token.

Add Master Server

■ **Master Server Name**

Enter the fully qualified domain name of the primary server.

■ **Web services port**

If the NetBackup administrator has not changed the port, accept the default (8443). Otherwise, contact the administrator for the correct port number.

■ **Authentication token**

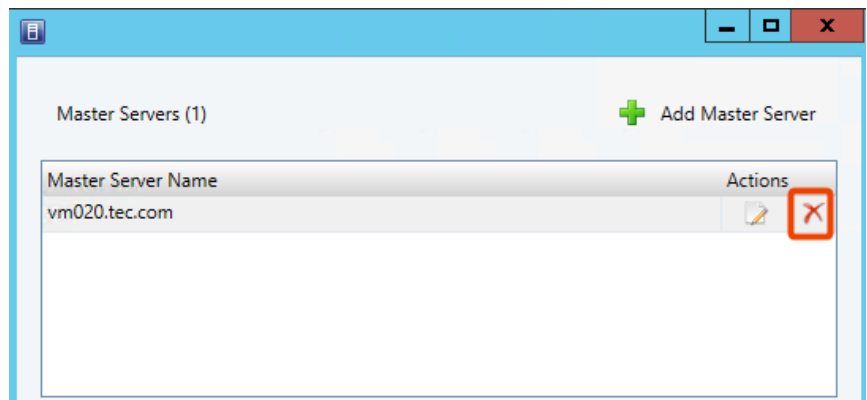
Click **Browse** to select the authentication token file that the NetBackup administrator provided.

Click **Add**. The server is added to the list of primary servers that the add-in can communicate with.

- 6 To verify that the SCVMM console can communicate with the primary server, click **Check Status**.

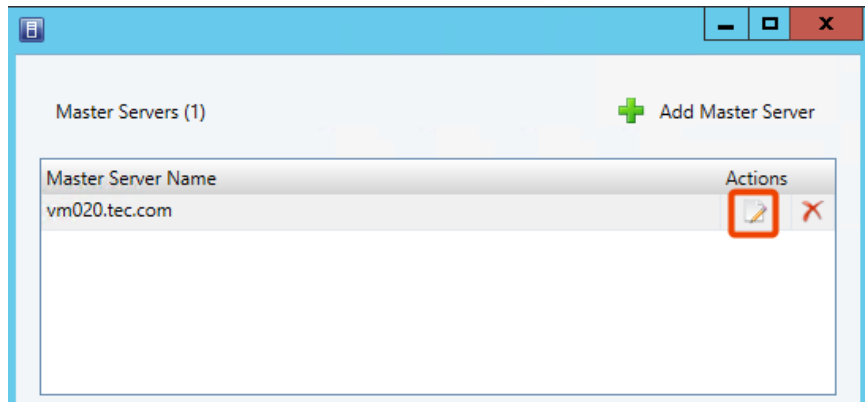
If the communication is successful, the **Connection Status** field reads **Connected**.

- 7 To add other primary servers and their authentication tokens, click **Add Master Server** in the upper right and repeat step 5 and 6.
- 8 To delete an authorization, click the delete icon next to the primary server name.

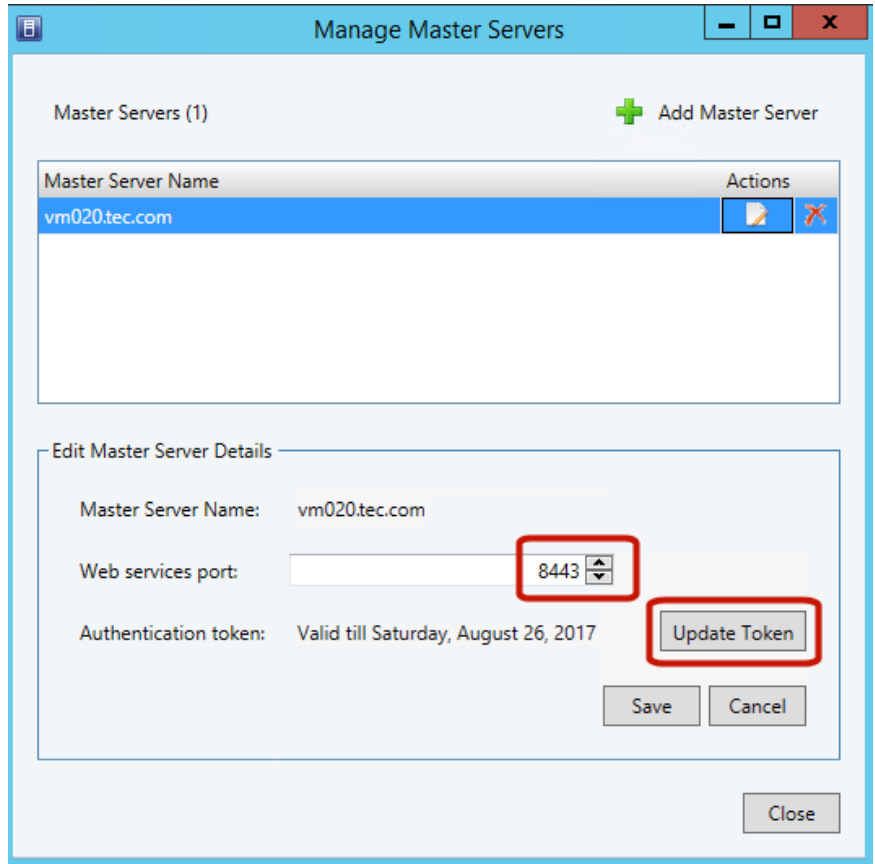


When the authorization is deleted, the add-in can no longer restore from the backups that the primary server performed.

- 9 To edit an authorization, click the edit icon opposite the primary server name.



You can enter a different web services port, or click **Update Token** to select a different authentication token.



10 Click **Save**.

11 Click **Close**.

Adding or deleting an additional host name or IP address for an authentication token

The `manageClientCerts` command generates an authentication token for a specific SCVMM console host. The token gives the SCVMM console host access to the NetBackup primary server where the token was generated. The token works if the SCVMM console host name is identical to the name that was entered on the `manageClientCerts` command.

For some environments, it may be necessary to allow the token to work with additional host names or IP addresses. An example is a clustered SCVMM server:

the request for access to the NetBackup primary may come from a different host name or IP address than the one that was provided when the token was generated.

To allow access to NetBackup from such environments, you can use the `manageClientCerts` command to do the following:

- Add another host name (or IP address) of the SCVMM console host for the existing token. The added host name or IP address is referred to as an *alias*.
Note: You can add multiple aliases for a token.
Note that IPv4 and IPv6 addresses are supported.
- Delete a host name or IP address from a token.
- Allow the token to be used on any SCVMM console host.
- List existing aliases for a token.

The `manageClientCerts` command is in the following location:

Windows:

```
install_path\NetBackup\wmc\bin\install\manageClientCerts.bat
```

UNIX, Linux:

```
/usr/opensv/wmc/bin/install/manageClientCerts
```

Table 2-3 Add a host name or IP address for an existing authentication token

Task	Enter the following on the NetBackup primary server:
Add a host name	<pre>manageClientCerts -addAlias <i>host_name_used_to_generate_token</i> -HOST <i>additional_host_name_for_token</i></pre> <p>Where <i>host_name_used_to_generate_token</i> is the host name that was specified when the token was generated, and <i>additional_host_name_for_token</i> is the additional host name of the SCVMM console host.</p> <p>For example:</p> <pre>manageClientCerts -addAlias SCVMM1 -HOST SCVMM1.example.com</pre> <p>Command output:</p> <pre>Successful -addAlias, for client: SCVMM1, type: HOST, alias: SCVMM1.example.com</pre> <p>In this example, the added host name is <code>SCVMM1.example.com</code>.</p> <p>Note: You can add multiple host names for a token. Add one host name for each instance of <code>manageClientCerts</code>.</p>

Table 2-3 Add a host name or IP address for an existing authentication token (*continued*)

Task	Enter the following on the NetBackup primary server:
Add an IP address or range of IP addresses	<pre>manageClientCerts -addAlias host_name_used_to_generate_token -IP IP_address_for_token IP_address_with_netmask_for_token</pre> <p>Where <i>host_name_used_to_generate_token</i> is the host name that was specified when the token was generated. The IP address to add can be a single address (<i>IP_address_for_token</i>) or a range of addresses (<i>IP_address_with_netmask_for_token</i>).</p> <p>For example:</p> <p>To add a single IP address:</p> <pre>manageClientCerts -addAlias SCVMM1 -IP 10.80.154.1</pre> <p>To add a range of IP addresses using a netmask:</p> <pre>manageClientCerts -addAlias SCVMM1 -IP 10.80.154.0/29</pre> <p>In this example, 10.80.154.0/29 allows 6 hosts with IP addresses from 10.80.154.1 to 10.80.154.7 to use the same token.</p> <p>Note: For a range of IP addresses, <code>manageClientCerts</code> supports IP net masking, sometimes called Classless Inter-Domain Routing notation (CIDR).</p> <p>Note: You can add multiple IP addresses for a token. If not adding a range of addresses, add one IP address for each instance of <code>manageClientCerts</code>.</p> <p>Note: IPv4 and IPv6 addresses are supported.</p>
Allow the token to operate with any host	<pre>manageClientCerts -addAlias host_name_used_to_generate_token -ANY</pre> <p>Where <i>host_name_used_to_generate_token</i> is the host name that was specified when the token was generated. <code>-ANY</code> allows any host or any IP address to communicate with the NetBackup server by means of this token.</p> <p>Caution: Use the <code>-ANY</code> option with care. Allowing any host to use the token may introduce a security risk.</p>

Table 2-4 Remove a host name or IP address from an existing authentication token

Task	Enter the following on the NetBackup primary server:
Delete a host name	<pre>manageClientCerts -deleteAlias host_name_used_to_generate_token -HOST host_name_to_delete</pre> <p>Where <i>host_name_used_to_generate_token</i> is the host name that was specified when the token was generated, and <i>host_name_to_delete</i> is the name to be removed.</p>

Table 2-4 Remove a host name or IP address from an existing authentication token (*continued*)

Task	Enter the following on the NetBackup primary server:
Delete an IP address	<pre>manageClientCerts -deleteAlias host_name_used_to_generate_token -IP IP_address_to_delete</pre> <p>Where <i>host_name_used_to_generate_token</i> is the host name that was specified when the token was generated, and <i>IP_address_to_delete</i> is the IP address to be removed.</p>
Delete the -ANY option	<pre>manageClientCerts -deleteAlias host_name_used_to_generate_token -ANY</pre> <p>Where <i>host_name_used_to_generate_token</i> is the host name that was specified when the token was generated. The -ANY option is removed from the token. If particular aliases (host names or IP addresses) had been added for the token, those aliases remain in force.</p>

Table 2-5 List the host names or IP addresses (aliases) that have been defined for a token

Task	Enter the following on the NetBackup primary server:
List host names or IP addresses (aliases)	<pre>manageClientCerts -listAliases host_name_used_to_generate_token</pre> <p>Where <i>host_name_used_to_generate_token</i> is the host name that was specified when the token was generated.</p> <p>For example:</p> <pre>manageClientCerts -listAliases SCVMM1</pre> <p>Command output:</p> <pre>Aliases for SCVMM1: HOST = SCVMM1.example.com</pre> <p>In this example, the alias is <code>SCVMM1.example.com</code>. If the token was set with the -ANY option (to accept connections from any host or any IP address), the -listAliases output is the following:</p> <pre>Aliases for SCVMM1: HOST = *</pre>

Further assistance is available:

See [“Troubleshooting primary server communication failures in the NetBackup Add-in for SCVMM”](#) on page 53.

Revoking an authorization token

You can delete or revoke an authentication token, as follows.

To revoke the authorization token

- ◆ Enter the following on the primary server:

Windows

```
install_path\NetBackup\wmc\bin\install\manageClientCerts.bat  
-delete clientName
```

UNIX, Linux

```
/usr/opensv/wmc/bin/install/manageClientCerts -delete clientName
```

Where *clientName* is the DNS name of the SCVMM console host where the add-in is installed.

The `-delete` option removes the authentication token and its compressed file from the primary server. The add-in is no longer authorized to restore virtual machines from the backups that this primary server made.

Renewing an authorization token

You can renew an authentication token that has expired, as follows.

Note: Authentication tokens expire after one year.

To renew an authentication token

- 1 Enter the following on the primary server:

Windows

```
install_path\NetBackup\wmc\bin\install\manageClientCerts.bat  
-renew clientName
```

UNIX, Linux

```
/usr/opensv/wmc/bin/install/manageClientCerts -renew clientName
```

Where *clientName* is the DNS name of the SCVMM console host where the add-in is installed.

The `-renew` option deletes the token and creates a new one. Any aliases that existed for the token are retained.

See [“Listing all current authorization tokens”](#) on page 33.

See [“Adding or deleting an additional host name or IP address for an authentication token”](#) on page 28.

- 2 Use the add-in's **Register Master Servers** option to re-register the primary server using the renewed authentication token.

See [“Authorizing the NetBackup add-in to restore virtual machines”](#) on page 24.

Listing all current authorization tokens

You can list all the current authentication tokens that were generated on the current primary server.

To list all current authorization tokens

- ◆ Enter the following on the primary server:

Windows

```
install_path\NetBackup\wmc\bin\install\manageClientCerts.bat -list
```

UNIX, Linux

```
/usr/opensv/wmc/bin/install/manageClientCerts -list
```

Sample output:

Client	Expiry Date
SCVMM_console_host_1	Thu Feb 06 16:16:51 GMT+05:30 2016
SCVMM_console_host_2	Fri Feb 07 11:22:53 GMT+05:30 2016

The command lists the SCVMM console hosts for which the tokens were created as well as their expiration dates. It can help diagnose communication problems between the SCVMM console host and the primary server when a certificate has expired.

- For well-formatted output, set the command prompt or shell screen size to more than 100 units.
- Server names that are longer than 40 characters are truncated: Characters beyond the first 40 are replaced with "...".

Recovering virtual machines

This chapter includes the following topics:

- [Notes on restoring Hyper-V virtual machines with the Recovery Wizard](#)
- [Accessing the Recovery Wizard](#)
- [Restore Virtual Machine Wizard screens](#)
- [Checking the status of a recovery job](#)

Notes on restoring Hyper-V virtual machines with the Recovery Wizard

Use the NetBackup **Recovery Wizard** in the SCVMM console to restore a virtual machine from its NetBackup image.

Note the following about the NetBackup Add-in Recovery Wizard:

- The NetBackup Recovery Wizard is for restore of an entire virtual machine, not for restore of individual files. To restore individual files from the virtual machine backup, use the NetBackup Backup, Archive, and Restore interface. See the topics on restoring individual files in the *NetBackup for Hyper-V Administrator's Guide*.
- The NetBackup Recovery Wizard does not support restore to a staging location. To restore the virtual machine to a staging location, use the NetBackup Backup, Archive, and Restore interface.
- Changes that are made through Hyper-V Manager on individual Hyper-V hosts or clusters can take up to 24 hours to be reflected in the SCVMM Console. Until then, the NetBackup add-in Recovery Wizard may not have the latest virtual

machine configuration state. In that case, the Recovery Wizard's pre-recovery checks related to the VM's location may not be based on the most recent data in SCVMM. You may have to make a different selection in the Recovery Wizard. See [“The pre-recovery checks in the Recovery Wizard of the NetBackup Add-in for SCVMM return out-of-date information about the VM”](#) on page 51.

- The NetBackup web UI includes the following enhancements for restoring a VM:
 - A new VM GUID is generated by default when you restore a VM to an alternate location.
 - A new VM display name can be specified when you restore a VM.

Note: The NetBackup Recovery Wizard does not support these restore enhancements. Use the NetBackup web UI or the `nbrestorevm` command to generate a new GUID or set a new display name when restoring a VM.

- For the pre-requisites for using the Recovery Wizard:
See [“Configuring the NetBackup Recovery Wizard”](#) on page 21.

Accessing the Recovery Wizard

In the SCVMM console, you can launch the Recovery Wizard from the NetBackup add-in as described in this topic.

Note: To have access to the add-in, you must install it yourself. If you did not install it, the **NetBackup** option does not appear in the SCVMM ribbon.

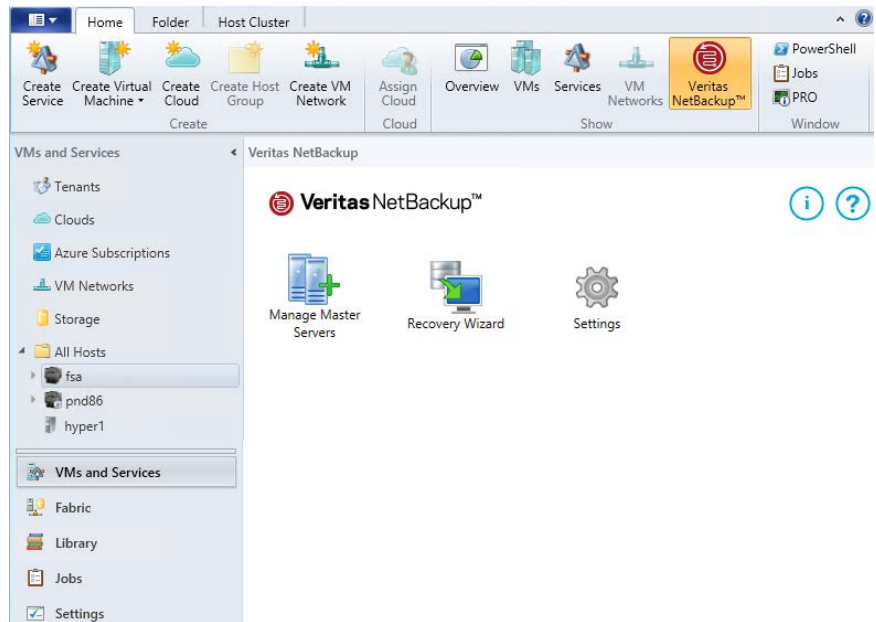
To access the Recovery Wizard

- 1 In the SCVMM console, open the **VMs and Services** workspace.
- 2 Click **All Hosts**.

- 3 In the SCVMM ribbon, click the **NetBackup** option.

The first time you use the NetBackup add-in, an End User License Agreement (EULA) appears. To use the add-in, you must accept the EULA.

The components of the NetBackup add-in appear.



- 4 Click the **Recovery Wizard**.

The Virtual Machine Selection screen appears.

See [“Virtual Machine Selection screen”](#) on page 37.

Restore Virtual Machine Wizard screens

Use the following screens in the NetBackup add-in to restore a Hyper-V virtual machine.

Virtual Machine Selection screen

Use this screen to specify the virtual machine to restore.

Figure 3-1 Virtual Machine Selection screen in the NetBackup Recovery Wizard for SCVMM

Table 3-1 Fields in the Virtual Machine Selection screen of the NetBackup Recovery Wizard

Field	Description
Master Server	Use the drop-down list to select the primary server that made the backup. If the primary server is not in the drop-down, you must add the server to the master server list. See “Authorizing the NetBackup add-in to restore virtual machines” on page 24.
VM Identifier	Enter the display name, host name, or GUID of the virtual machine that you want to restore. Note: This field is not case-sensitive.
Next	When you are done, click Next to go to the next screen of the wizard.

Backup Image Selection screen

Use this screen to select a backup image from which to restore the virtual machine.

Figure 3-2 Backup Image Selection screen in the NetBackup Recovery Wizard for SCVMM

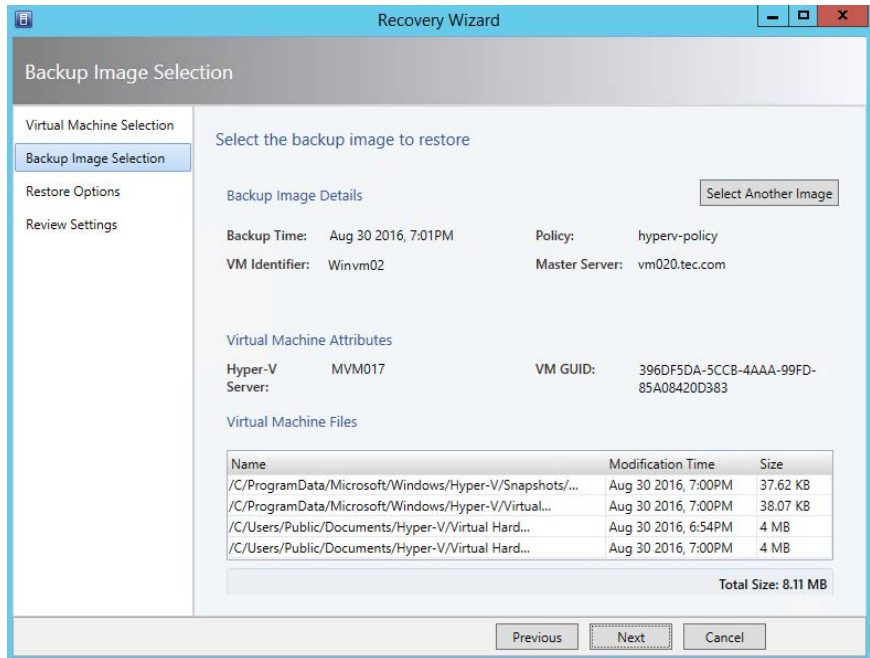


Table 3-2 Fields in the Backup Image Selection screen

Field	Description
Backup Image Attributes	Lists the information about the virtual machine backup image. By default, the most recent backup image is displayed.
Select Another Image	Click this option to select a different backup image. See the table in the following topic: See “Select Another Image screen” on page 40.
Virtual Machine Attributes	Lists the information about the virtual machine at the time it was backed up.
Virtual Machine Files	Lists the files that are included in the virtual machine image. Note: To see the entire path, you can pull the Name column border to the right, or hover over the row to display a tool tip.
Next	When you are done, click Next to go to the next screen of the wizard.

Select Another Image screen

Use the **Select Another Image** screen to find a backup image, then select the image in the lower pane and click **Select**. The virtual machine files from that image are displayed in the **Backup Image Selection** screen.

Figure 3-3 Select Another Image screen in the NetBackup Recovery Wizard for SCVMM

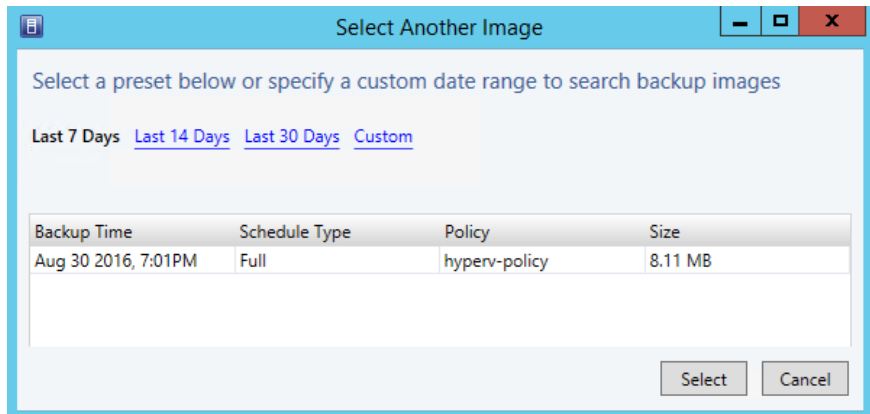


Table 3-3 Fields in the Select Another Image screen

Field	Description
Last 7 Days	Shows the backup images that were made within the last week, last 2 weeks, last month, or within a period that you specify.
Last 14 Days	
Last 30 Days	
Custom	Click Custom to select the period. Use the pull-down arrows to select a different date, and click Search . The images that fall within the search dates are displayed.
	Select an image and click Select .

Restore Options screen

Use this screen to specify destination options for the restored virtual machine.

Figure 3-4 Restore Options screen in the NetBackup Recovery Wizard for SCVMM

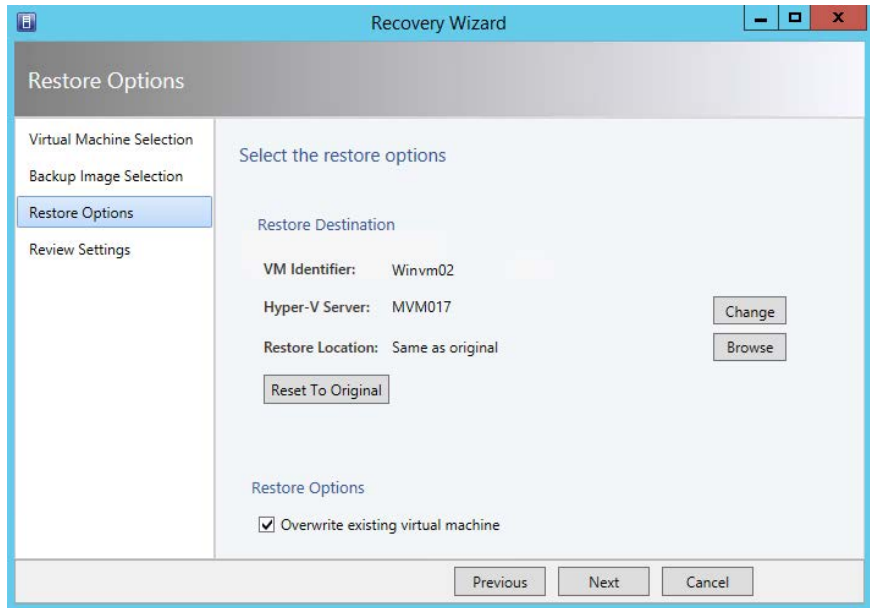


Table 3-4 Fields in the Restore Options screen

Fields	Description
Restore Destination	Lists the details on the restore destination.
VM identifier	The display name or other identifier of the virtual machine to restore.
Hyper-V server	<p>The Hyper-V server on which to restore the virtual machine. The default is the original server.</p> <p>To restore the virtual machine to an alternate Hyper-V server, click Change and use the pull-down to select a different server.</p> <p>The pull-down lists the Hyper-V servers that the SCVMM server manages.</p>

Table 3-4 Fields in the Restore Options screen (*continued*)

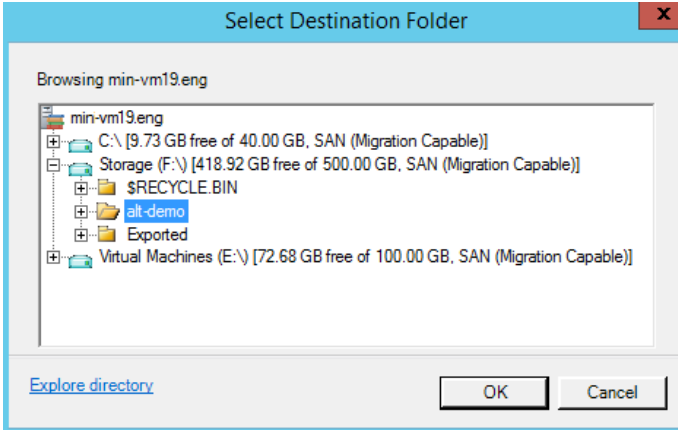
Fields	Description
Restore Location	<p>The directory in which to restore the virtual machine. The default is the original directory.</p> <p>To select an alternate restore directory, click Browse and select the directory:</p>  <p>Note: To create a new directory for the restore location, click the Explore directory link at the bottom of the Select Destination Folder dialog. Administrator privileges may be required.</p> <p>Note: When browsing for directories, the Microsoft RemoteFileBrowserDialog widget may display a dynamic volume with its GUID instead of with a volume letter. You can still select a destination folder under the GUID-identified volume. See the following Microsoft article on this issue:</p> <p>Using Dynamic Disks to host virtual machine files in Virtual Machine Manager</p>
Reset to Original	Resets the restore location to the original Hyper-V server and original directory.
Restore Options	Lists the restore options.
Overwrite existing virtual machine	<p>If a virtual machine with the same display name exists at the destination, that virtual machine must be deleted before the restore begins. Otherwise, the restore fails.</p> <p>Select this option to delete the existing virtual machine.</p>

Table 3-4 Fields in the Restore Options screen (*continued*)

Fields	Description
Next	When you are done, click Next to go to the next screen of the wizard.

Review Settings screen

Use this screen to review the settings that are used for the recovery and to start the recovery.

Figure 3-5 Review Settings screen in the NetBackup Recovery Wizard for SCVMM

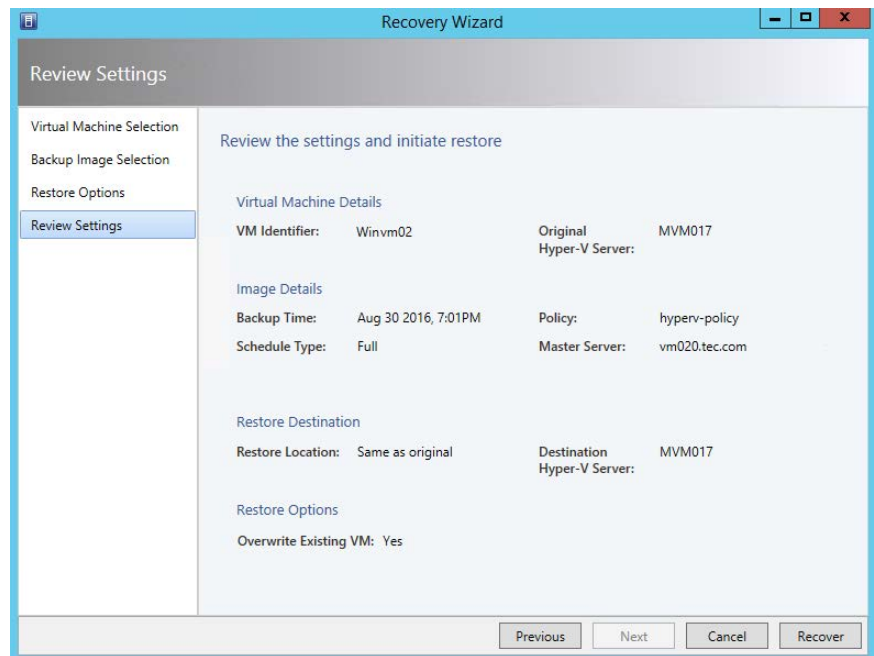


Table 3-5 Fields in the Review Settings screen

Field	Description
Virtual Machine Details	Lists the details of the virtual machine that is selected for restore.
Image Details	Lists the details of the backup image from which the virtual machine is to be restored.

Table 3-5 Fields in the Review Settings screen (*continued*)

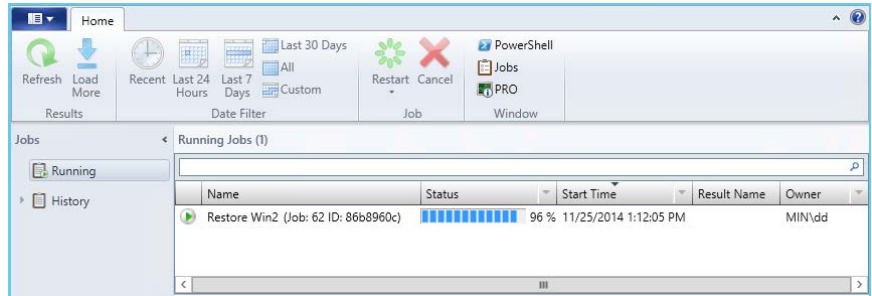
Field	Description
Restore Destination	Lists the details of the restore destination.
Restore Options	Lists the restore options.
Recover	<p>Runs pre-recovery checks to validate your selections. If the checks are successful, it starts the recovery.</p> <p>When you click Recover, a pop-up shows the job ID of the recovery job. The following topic explains how to check the status of the recovery:</p> <p>See “Checking the status of a recovery job” on page 44.</p> <p>Note: If changes to the VM were recently made through Hyper-V Manager (not through SCVMM), the pre-recovery checks may encounter out-of-date information about the VM.</p> <p>See “The pre-recovery checks in the Recovery Wizard of the NetBackup Add-in for SCVMM return out-of-date information about the VM” on page 51.</p>

Checking the status of a recovery job

You can check the status of a recovery job that is in progress and view the history of all recovery jobs.

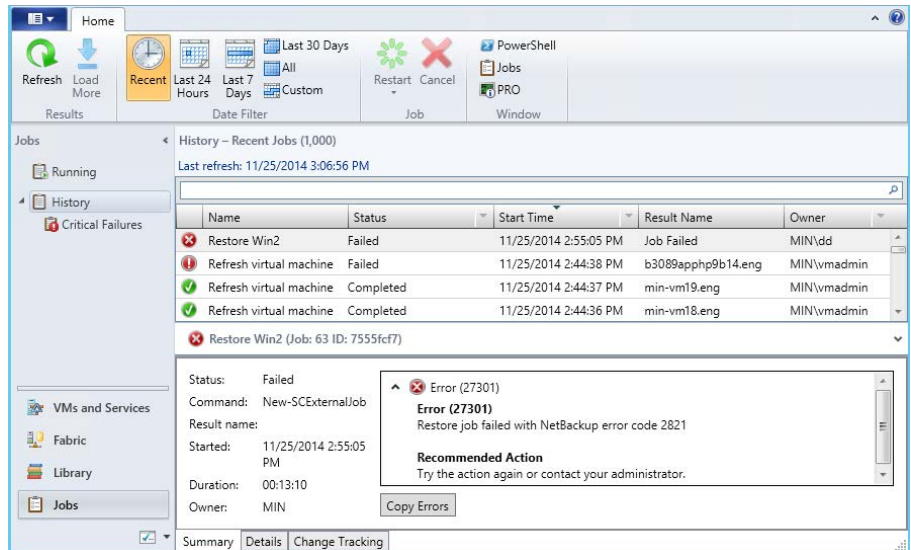
To check the status of a recovery job

- 1 In the SCVMM console, open the **Jobs** workspace.
- 2 For the jobs that are in progress, click **Running**.



The **Status** column shows the job's percent completion.

- 3 For a listing of recent jobs and past jobs, click **History**.



For all jobs not in progress, the **Status** column reads **Completed** or **Failed**.

If the NetBackup primary server is disconnected or goes down during the recovery, the **Status** column is updated to:

Failed - Lost connection with NetBackup Master Server.

Note: You can reorder the listing by clicking on a column header.

Note: The **Restart** and **Cancel** buttons are not supported and are grayed out.

Troubleshooting

This chapter includes the following topics:

- [About logging for the NetBackup Add-in for SCVMM](#)
- [Viewing log messages for the NetBackup Add-in for SCVMM](#)
- [Changing the logging level for the NetBackup Add-in for SCVMM](#)
- [The pre-recovery checks in the Recovery Wizard of the NetBackup Add-in for SCVMM return out-of-date information about the VM](#)
- [Next button in the NetBackup Add-in Recovery Wizard is enabled even though required input has not been entered](#)
- [The NetBackup Add-in Recovery Wizard does not prompt to overwrite the VM, and the recovery fails](#)
- [Troubleshooting primary server communication failures in the NetBackup Add-in for SCVMM](#)

About logging for the NetBackup Add-in for SCVMM

The NetBackup Add-in for SCVMM records log messages about the following activities:

- Restoring VMs by means of the NetBackup add-in.
- Adding or removing NetBackup primary servers from the NetBackup add-in.

Table 4-1 Logging for NetBackup Add-in for SCVMM

Logging details	Description
Log message format	yyyy-mm-dd hh:mm:ss,ms [pid] message For example: 2014-09-24 14:57:32,408 [1] INFO - Loading SCVMMAddin
Logging levels	Several logging levels (verbosity) are available: See “Changing the logging level for the NetBackup Add-in for SCVMM” on page 50.
Log location	The log location depends on where SCVMM is installed and who is logged on. The following is an example log location for user JDoe: C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\JDoe\SymcNBUAddIn\Logs See “Viewing log messages for the NetBackup Add-in for SCVMM ” on page 48.
Log retention period	All log messages are written to the same log file in a 24-hour period. Each log file is retained for 7 days and then is automatically deleted.

Viewing log messages for the NetBackup Add-in for SCVMM

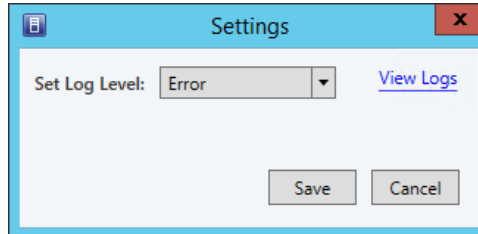
Note: Log files are retained for 7 days and then are automatically deleted.

Note: If no log-related activity occurs in the NetBackup add-in during a 24-hour period, no log file is created.

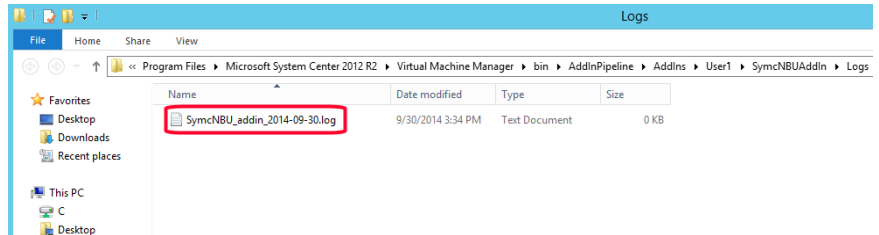
To view the NetBackup Add-in for SCVMM log messages

- 1 In the SCVMM console, open the **VMs and Services** workspace.
- 2 Click **All Hosts**.
- 3 In the SCVMM ribbon, click the **NetBackup** option.

- 4 Click **Settings**.
- 5 Click **View Logs**.



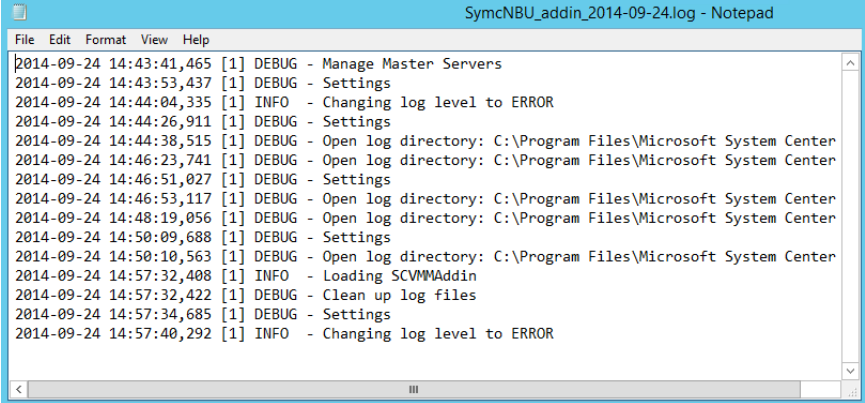
The log files are shown as follows:



Note: The logs are written to the directory where you installed the NetBackup add-in.

- 6 Double-click on a log file.

The log file opens as follows:



```

2014-09-24 14:43:41,465 [1] DEBUG - Manage Master Servers
2014-09-24 14:43:53,437 [1] DEBUG - Settings
2014-09-24 14:44:04,335 [1] INFO - Changing log level to ERROR
2014-09-24 14:44:26,911 [1] DEBUG - Settings
2014-09-24 14:44:38,515 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:46:23,741 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:46:51,027 [1] DEBUG - Settings
2014-09-24 14:46:53,117 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:48:19,056 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:50:09,688 [1] DEBUG - Settings
2014-09-24 14:50:10,563 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:57:32,408 [1] INFO - Loading SCVMMAddin
2014-09-24 14:57:32,422 [1] DEBUG - Clean up log files
2014-09-24 14:57:34,685 [1] DEBUG - Settings
2014-09-24 14:57:40,292 [1] INFO - Changing log level to ERROR
  
```

- 7 When you are finished, close the **Logs** window and click **Cancel**.

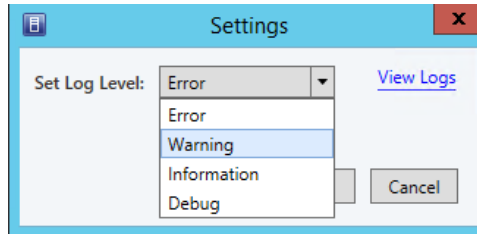
Changing the logging level for the NetBackup Add-in for SCVMM

To change the logging level

- 1 In the SCVMM console, open the **VMs and Services** workspace.
- 2 Click **All Hosts**.
- 3 Click the **NetBackup** option in the SCVMM console ribbon.
- 4 Click **Settings**.

The pre-recovery checks in the Recovery Wizard of the NetBackup Add-in for SCVMM return out-of-date information about the VM

- 5 Use the **Set Log Level** pull-down to select a different level.



By default, logging is set to the minimum level of detail (Error level). The following levels are available:

Error	The default level.
Warning	Includes the error messages.
Information	Includes the warning and the error messages.
Debug	Includes the information, warning, and error messages - the highest level of detail.

- 6 Click **Save**.

The pre-recovery checks in the Recovery Wizard of the NetBackup Add-in for SCVMM return out-of-date information about the VM

When you click **Recover** on the **Review Settings** screen of the Recovery Wizard, the wizard runs pre-recovery checks to validate your selections and the recovery destination. However, if changes to the VM were recently made through Hyper-V Manager (not through SCVMM), the pre-recovery checks may encounter out-of-date information about the VM. Changes that are made through Hyper-V Manager on individual Hyper-V hosts or clusters can take up to 24 hours to be reflected in SCVMM. This delay is due to the Microsoft SCVMM refresh cycle, which the NetBackup add-in does not control.

For example: If the VM was recently deleted through the Hyper-V Manager, the deletion may not be reflected yet in SCVMM. In this case, the add-in's pre-recovery checks report that the VM still exists. The following message appears:

Next button in the NetBackup Add-in Recovery Wizard is enabled even though required input has not been entered

A virtual machine with the same identity exists on <host> and the overwrite option was not selected. Please review restore options and select overwrite to continue.

To recover the VM, go back to the wizard's **Restore Options** screen and select **Overwrite existing virtual machine**, and rerun the recovery.

Note: In an SCVMM environment, Microsoft recommends making VM configuration changes through SCVMM (not through the Hyper-V Manager on individual hosts or clusters). Changes that are made through the SCVMM Console are reflected immediately in SCVMM. The add-in's pre-recovery checks therefore reflect the current state of the VM.

Next button in the NetBackup Add-in Recovery Wizard is enabled even though required input has not been entered

In the Recovery Wizard of the NetBackup Add-in for SCVMM, the **Next** button is enabled even if some required input has not been entered. In the following case, the Recovery Wizard of the NetBackup Add-in for SCVMM enables the **Next** button prematurely:

- On the **Add-in's Manage Master Servers** screen, an authentication token was added for an invalid primary server. For example: The token was generated for an existing primary server, but the server name was entered incorrectly on the **Manage Master Servers** screen.
- A second primary server and its authentication token are added, and the primary server's name is entered correctly.

When you select the second primary server in the wizard's **Virtual Machine Selection** screen, you can click **Next** without selecting a VM identifier. The wizard lets you progress from screen to screen without completing the input for each screen. If you continue without making the required input, the **Recovery** button on the wizard's last screen is grayed out.

Note: The wizard's **Next** button should remain grayed out until the input for each screen is completed. To run the restore, go back through the wizard and make the required entries. You should also delete the invalid primary server.

The NetBackup Add-in Recovery Wizard does not prompt to overwrite the VM, and the recovery fails

The NetBackup Add-in for Microsoft SCVMM Console does not complete a VM recovery in the following situation:

- On the **Virtual Machine Selection** screen of the **Add-in Recovery Wizard**, the VM is identified by its GUID or host name (not its display name).
- On the **Restore Options** screen of the wizard, the **Overwrite existing virtual machine** option is not selected.
- The same VM exists at the recovery destination.

When you click **Recover**, the wizard should detect the VM at the recovery destination and then prompt you to select the overwrite option. However, the prompt does not appear; the recovery job starts but then fails with status 2821.

To recover the VM, select **Overwrite existing virtual machine** on the **Restore Options** screen and rerun the recovery.

Troubleshooting primary server communication failures in the NetBackup Add-in for SCVMM

To recover VMs, the add-in must have a registered NetBackup primary server with a valid and correct authentication token. The NetBackup administrator generates the authentication token on a specific NetBackup primary server for a specific SCVMM console host. The token gives the SCVMM console host access to the NetBackup primary server where the token was generated. (Note: you can validate authentication tokens for currently registered primary servers by means of the **Manage Master Servers** option in the add-in.)

If the TCP/IP address or host name of the SCVMM console host does not exactly match the information in the authentication token, the following operations fail: the Manage Master Servers operation, and VM recovery. Error messages such as the following may appear:

```
Unable to connect the Netbackup Master Server. Do you want to add
this master server?
```

```
Authentication failed. Please verify that the master server token is
valid and correct using the 'Manage Master Servers' dialog box
```

To correctly determine the problem and the corrective action, you must review the VxUL log file. On the primary server, enter the following command:

```
vxlogview -i nbwebsevice -p nb -L -E
```

Error example 1

The log file includes messages similar to the following:

```
02/17/2017 10:03:37.831 [Error] Remote host name does not match the
name in the certificate, remote name:scvmm02.domain.com, name from
certificate:scvmm02
```

In the log snip shown, the name in the token is `scvmm02` and the required name is `scvmm02.domain.com`.

Cohesity recommends that you revoke the existing token, generate a new token with the required name, and use the new token on the SCVMM console host. If you cannot do that, add the SCVMM console host's fully qualified domain name as an alias for the existing token, as follows:

```
manageClientCerts -addAlias scvmm02 -HOST scvmm02.domain.com
```

As an alternative, you can use the `-ANY` option:

```
manageClientCerts -addAlias scvmm02 -ANY
```

`-ANY` allows any host or any IP address to communicate with the NetBackup server by means of this token.

Caution: The `-ANY` option is not a secure method for restores. Please see the *NetBackup Commands Reference Guide* for more information on the `manageClientCerts` command.

Error example 2

The log file includes messages similar to the following:

```
02/17/2017 16:18:13.951 [Error] Remote host name does not match the
name in the certificate, remote name:10.10.10.11, name from
certificate:scvmm02
```

In the log snip shown, the name in the token is `scvmm02` and the required name is `10.10.10.11`.

Cohesity recommends that you revoke the existing token, generate a new token with the required name, and use the new token on the SCVMM console host. If you cannot do that, add the SCVMM console host's TCP/IP address as an alias for the existing token, as follows:

```
manageClientCerts -addAlias scvmm02 -IP 10.10.10.11
```

As an alternative, you can use the `-ANY` option:

```
manageClientCerts -addAlias scvmm02 -ANY
```

-ANY allows any host or any IP address to communicate with the NetBackup server by means of this token.

Caution: The -ANY option is not a secure method for restores.

Additional information is available:

See [“Adding or deleting an additional host name or IP address for an authentication token”](#) on page 28.

See the `manageClientCerts` command in the *NetBackup Commands Reference Guide*.