Post deployment required operations and issues

SnapCenter Plug-in for VMware vSphere 4.4

NetApp
March 31, 2021

This PDF was generated from https://docs.netapp.com/us-en/sc-plugin-vmware-vsphere/scpivs44_post_deployment_required_operations_and_issues.html#manage-authentication-errors on March 31, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Post deployment required operations and issues 1
Register SnapCenter Plug-in for VMware vSphere with SnapCenter Server 4

Post deployment required operations and issues

After deploying SnapCenter Plug-in for VMware vSphere, you should complete the required operations.

- If you are a new SnapCenter user, you must add storage VMs to SnapCenter before you can perform any data protection operations. When adding storage VMs, specify the management LIF. You can also add a cluster and specify the cluster management LIF. For information about adding storage, see Adding storage.
- If you are an existing SnapCenter user, you must migrate your existing SnapCenter VM and datastore backups and metadata. For information about migrating, see Migration overview.

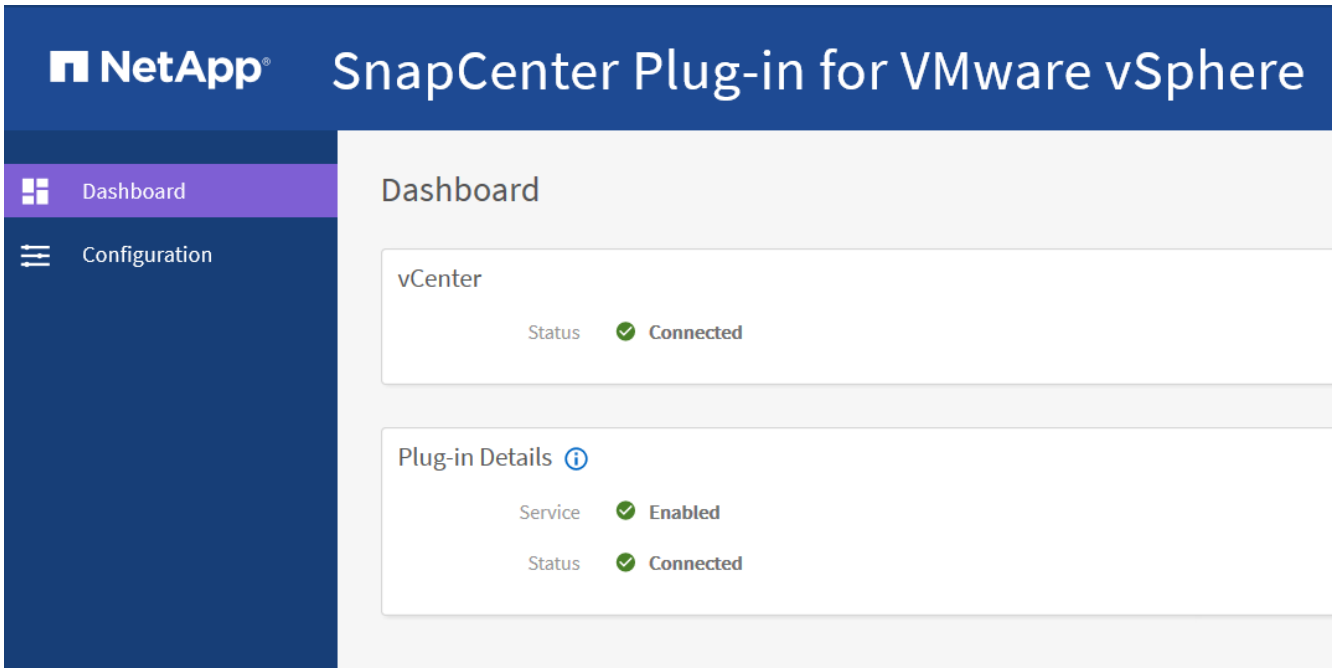
Your deployment might encounter the following issues:

- After deploying the virtual appliance, the **Backup Jobs** tab on the Dashboard might not load in the following scenarios:
  - You are running IPv4 and have two IP addresses for the SnapCenter VMware vSphere host. As a result, the job request is sent to an IP address that is not recognized by the SnapCenter Server. To prevent this issue, add the IP address that you want to use, as follows:
    a. Navigate to the location where the SnapCenter VMware plug-in is deployed: `/opt/netapp/scvservice/standalone_aegis/etc`
    b. Open the file network- interface.properties.
    c. In the `network.interface=10.10.10.10` field, add the IP address that you want to use.
  - You have two NICs.
- After deploying the SnapCenter VMware plug-in, the MOB entry in vCenter for SnapCenter Plug-in for VMware vSphere might still show the old version number. This can occur when other jobs are running in the vCenter. vCenter will eventually update the entry.
- After a deployment, or after an upgrade on a VM where Virtual Storage Console for VMware vSphere (VSC) was previously installed, the following might occur:
  - Right-click menus that are documented for mount, unmount, attach, and detach operations do not appear.
  - The VMware vSphere web client GUI does not match the documentation.
  - The Dashboard is not displayed correctly.
  - During normal use, a page display (for example, the Resource Groups page) might stall or get stuck loading.

To correct any of these issues, do the following:

1. Clear the browser cache and then check if the GUI is operating properly.

   If the problem persists, then restart the VMware vSphere web client service



2. Log in to vCenter, then click **Menu** in the toolbar, and then select **SnapCenter Plug-in for VMware vSphere**.

Manage authentication errors

If you do not use the Admin credentials, you might receive an authentication error after deploying SnapCenter Plug-in for VMware vSphere or after migrating. If you encounter an authentication error, you must restart the service.

Steps

1. Log on to the SnapCenter VMware plug-in management GUI using the format `https://<appliance-IP-address>:8080`.
2. Restart the service.

Create credentials for migrating backups

If you are a SnapCenter customer and have VM consistent or VM crash-consistent backups, or application-consistent backups of virtualized data, you must migrate those backups to SnapCenter Plug-in for VMware vSphere. Before migrating, you must add the SnapCenter VMware plug-in credentials to SnapCenter Server.

Before you begin

- You must be running SnapCenter Server 4.2 or later.
- You must have deployed and enabled SnapCenter Plug-in for VMware vSphere.

Steps

1. In the left navigation pane of the SnapCenter GUI, click **Settings**.
2. In the Settings page, click **Credentials**, and then click **New** to start the wizard.
3. Enter the credential information as listed in the following table:

For this field…	Do this…
Credential name	Enter a name for the credentials.
Username	Enter the username specified when SnapCenter Plug-in for VMware vSphere was deployed.
Password	Enter the password specified when SnapCenter Plug-in for VMware vSphere was deployed.
Authentication	Select **Linux**.

Register SnapCenter Plug-in for VMware vSphere with SnapCenter Server

If you want to perform application-over-VMDK workflows in SnapCenter (application-based protection workflows for virtualized databases and file systems), you must register SnapCenter Plug-in for VMware vSphere with the SnapCenter Server.

If you are a SnapCenter user and you upgraded to SnapCenter 4.2 and migrated your application-over-VMDK backups to SnapCenter Plug-in for VMware, the migration command automatically registers the plug-in.

Before you begin

- You must be running SnapCenter Server 4.2 or later.
- You must have deployed and enabled SnapCenter Plug-in for VMware vSphere.

About this task

- You register SnapCenter Plug-in for VMware vSphere with SnapCenter Server by using the SnapCenter GUI to add a “vsphere” type host.

  Port 8144 is predefined for communication within the SnapCenter VMware plug-in.

  You can register multiple instances of SnapCenter Plug-in for VMware vSphere on the same SnapCenter Server 4.2 to support application-based data protection operations on VMs. You cannot register the same SnapCenter Plug-in for VMware vSphere on multiple SnapCenter Servers.

- For vCenters in Linked Mode, you must register the SnapCenter Plug-in for VMware vSphere for each vCenter.

Steps

1. In the SnapCenter GUI left navigation pane, click **Hosts**.
2. Verify that the **Managed Hosts** tab is selected at the top, then locate the virtual appliance host name and verify that it resolves from the SnapCenter Server.
3. Click **Add** to start the wizard.
4. On the **Add Hosts** dialog box, specify the host you want to add to the SnapCenter Server as listed in the following table:

For this field…	Do this…
Host Type	Select **vSphere** as the type of host.
Host name	Verify the IP address of the virtual appliance.

For this field…	Do this…
Credential	Enter the username and password for the SnapCenter VMware plug-in that was provided during the deployment.

5. Click **Submit**.

   When the VM host is successfully added, it is displayed on the Managed Hosts tab.

6. In the left navigation pane, click **Settings**, then click the **Credential** tab, and then click ➕ **Add** to add credentials for the virtual appliance.
7. Provide the credential information that was specified during the deployment of SnapCenter Plug-in for VMware vSphere.

   ℹ️ You must select Linux for the Authentication field.

After you finish

If the SnapCenter Plug-in for VMware vSphere credentials are modified, you must update the registration in SnapCenter Server using the SnapCenter Managed Hosts page.

Register SnapCenter Plug-in for VMware vSphere with SnapCenter Server

If you want to perform application-over-VMDK workflows in SnapCenter (application-based protection workflows for virtualized databases and file systems), you must register SnapCenter Plug-in for VMware vSphere with the SnapCenter Server.

If you are a SnapCenter user and you upgraded to SnapCenter 4.2 and migrated your application-over-VMDK backups to SnapCenter Plug-in for VMware, the migration command automatically registers the plug-in.

Before you begin

- You must be running SnapCenter Server 4.2 or later.
- You must have deployed and enabled SnapCenter Plug-in for VMware vSphere.

About this task

- You register SnapCenter Plug-in for VMware vSphere with SnapCenter Server by using the SnapCenter GUI to add a “vsphere” type host.

  Port 8144 is predefined for communication within the SnapCenter VMware plug-in.

  You can register multiple instances of SnapCenter Plug-in for VMware vSphere on the same SnapCenter Server 4.2 to support application-based data protection operations on VMs. You cannot register the same SnapCenter Plug-in for VMware vSphere on multiple SnapCenter Servers.

- For vCenters in Linked Mode, you must register the SnapCenter Plug-in for VMware vSphere for each vCenter.

Steps

1. In the SnapCenter GUI left navigation pane, click **Hosts**.

2. Verify that the **Managed Hosts** tab is selected at the top, then locate the virtual appliance host name and verify that it resolves from the SnapCenter Server.
3. Click **Add** to start the wizard.
4. On the **Add Hosts** dialog box, specify the host you want to add to the SnapCenter Server as listed in the following table:

For this field…	Do this…
Host Type	Select **vSphere** as the type of host.
Host name	Verify the IP address of the virtual appliance.
Credential	Enter the username and password for the SnapCenter VMware plug-in that was provided during the deployment.

5. Click **Submit**.

   When the VM host is successfully added, it is displayed on the Managed Hosts tab.

6. In the left navigation pane, click **Settings**, then click the **Credential** tab, and then click **Add** to add credentials for the virtual appliance.
7. Provide the credential information that was specified during the deployment of SnapCenter Plug-in for VMware vSphere.

   You must select Linux for the Authentication field.

After you finish

If the SnapCenter Plug-in for VMware vSphere credentials are modified, you must update the registration in SnapCenter Server using the SnapCenter Managed Hosts page.

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.