



Installation requirements for SnapCenter Plug-in for Microsoft Windows

SnapCenter Software

Archana, Soumik Das
September 08, 2021

This PDF was generated from https://docs.netapp.com/us-en/snapcenter/protect-scw/reference_installation_requirements_for_snapcenter_plug_in_for_microsoft_windows.html on September 16, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Installation requirements for SnapCenter Plug-in for Microsoft Windows 1
 - Host requirements to install SnapCenter Plug-ins Package for Windows 1
 - Set up your credentials for the Plug-in for Windows 2
 - Configure gMSA on Windows Server 2012 or later 3

Installation requirements for SnapCenter Plug-in for Microsoft Windows

You should be aware of certain installation requirements before you install the Plug-in for Windows.

Before you begin to use the Plug-in for Windows, the SnapCenter administrator must install and configure SnapCenter Server and perform prerequisite tasks.


- You must have SnapCenter admin privileges to install the Plug-in for Windows.

The SnapCenter admin role must have admin privileges.

- You must have installed and configured the SnapCenter Server.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in or if the user belongs to a local workgroup user, you must disable UAC on the host.
- You must set up SnapMirror and SnapVault if you want backup replication.

Host requirements to install SnapCenter Plug-ins Package for Windows

Before you install the SnapCenter Plug-ins Package for Windows, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating Systems	Microsoft Windows For the latest information about supported versions, see the NetApp Interoperability Matrix Tool .
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	5 GB  You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.

Item	Requirements
Required software packages	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.5.2 or later • Windows Management Framework (WMF) 4.0 or later • PowerShell 4.0 or later <p>For the latest information about supported versions, see the NetApp Interoperability Matrix Tool.</p>

Set up your credentials for the Plug-in for Windows

SnapCenter uses credentials to authenticate users for SnapCenter operations. You should create credentials for installing SnapCenter plug-ins, and additional credentials for performing data protection operations on Windows file systems.

What you will need

- You must set up Windows credentials before installing plug-ins.
- You must set up the credentials with administrator privileges, including administrator rights, on the remote host.
- If you set up credentials for individual resource groups, and the user does not have full admin privileges, you must assign at least the resource group and backup privileges to the user.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Credential**.
3. Click **New**.
4. In the Credential page, do the following:

For this field...	Do this...
Credential name	Enter a name for the credentials.

For this field...	Do this...
User name/Password	<p>Enter the user name and password used for authentication.</p> <ul style="list-style-type: none"> • Domain administrator or any member of the administrator group <p>Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the Username field are as follows:</p> <ul style="list-style-type: none"> ◦ NetBIOS\UserName ◦ Domain FQDN\UserName ◦ UserName@upn <ul style="list-style-type: none"> • Local administrator (for workgroups only) <p>For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the Username field is as follows: <code>UserName</code></p> <p>Do not use double quotes (") in passwords.</p>
Password	Enter the password used for authentication.

5. Click **OK**.

After you finish setting up credentials, you might want to assign credential maintenance to a user or group of users on the **User and Access** page.

Configure gMSA on Windows Server 2012 or later

Windows Server 2012 or later enables you to create a group Managed Service Account (gMSA) that provides automated service account password management from a managed domain account.

What you will need

- You should have a Windows Server 2012 or later domain controller.
- You should have a Windows Server 2012 or later host, which is a member of the domain.

Steps

1. Create a KDS root key to generate unique passwords for each object in your gMSA.
2. For each domain, run the following command from the Windows domain controller: Add-KDSRootKey -EffectiveImmediately
3. Create and configure your gMSA:
 - a. Create a user group account.
 - b. Add computer objects to the group.
 - c. Use the user group you just created to create the gMSA.

For example,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
```

- d. Run Get-ADServiceAccount command to verify the service account.
4. Configure the gMSA on your hosts:
 - a. Enable the Active Directory module for Windows PowerShell on the host where you want to use the gMSA account.

To do this, run the following command from PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                               Name                               Install
State
-----
[ ] Active Directory Domain Services      AD-Domain-Services              Available

PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
-----
True      No                Success      {Active Directory Domain
Services, Active ...
WARNING: Windows automatic updating is not enabled. To ensure that
your newly-installed role or feature is
automatically updated, turn on Windows Update.
```

- b. Restart your host.
 - c. Install the gMSA on your host by running the following command from the PowerShell command prompt: Install-AdServiceAccount <gMSA>

- d. Verify your gMSA account by running the following command: `Test-AdServiceAccount <gMSA>`
5. Assign the administrative privileges to the configured gMSA on the host.
6. Add the Windows host by specifying the configured gMSA account in the SnapCenter Server.

SnapCenter Server will install the selected plug-ins on the host and the specified gMSA will be used as the service log on account during the plug-in installation.

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.