Prepare for installing the SnapCenter Server

SnapCenter Software 4.5

NetApp
July 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/snapcenter-45/install/reference_domain_and_workgroup_requirements.html on July 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Prepare for installing the SnapCenter Server . . . 1
- Domain and workgroup requirements . . . 1
- Space and sizing requirements . . . 1
- SAN host requirements . . . 2
- Supported storage systems and applications . . . 3
- Supported browsers . . . 3
- Connection and port requirements . . . 3
- SnapCenter licenses . . . 6
  - Single Mailbox Recovery (SMBR) licenses . . . 8
- Authentication methods for your credentials . . . 9
  - Windows authentication . . . 9
  - Untrusted domain authentication . . . 9
  - Local workgroup authentication . . . 9
  - SQL Server authentication . . . 9
  - Linux authentication . . . 9
  - AIX authentication . . . 9
  - Oracle database authentication . . . 10
  - Oracle ASM authentication . . . 10
  - RMAN catalog authentication . . . 10
- Storage connections and credentials . . . 10

Prepare for installing the SnapCenter Server

Domain and workgroup requirements

The SnapCenter Server can be installed on systems that are either in a domain or in workgroup. The user used for installation should have admin privileges on the machine in case of both workgroup and domain.

For installing SnapCenter Server and SnapCenter plug-ins on Windows hosts, you should use one of the following:

- **Active Directory domain**

  You must use a Domain user with local administrator rights. The Domain user must be a member of the local Administrator group on the Windows host.

- **Workgroups**

  You must use a local account that has local administrator rights.

While domain trusts, multi-domain forests, and cross-domain trusts are supported, cross-forest domains are not supported. The Microsoft documentation about Active Directory Domains and Trusts contains more information.

After installing the SnapCenter Server, you should not change the domain in which the SnapCenter host is located. If you remove the SnapCenter Server host from the domain it was in when the SnapCenter Server was installed and then try to uninstall SnapCenter Server, the uninstall operation fails.

Space and sizing requirements

Before you install the SnapCenter Server, you should be familiar with the space and sizing requirements. You should also apply the available system and security updates.

Item	Requirements
Operating Systems	Microsoft Windows Only English, German, Japanese, and simplified Chinese version of the operating systems are supported. For the latest information about supported versions, see NetApp Interoperability Matrix Tool.
Minimum CPU count	4 cores

Item	Requirements
Minimum RAM	8 GB The MySQL Server buffer pool uses 20 percent of the total RAM.
Minimum hard drive space for the SnapCenter Server software and logs	4 GB If you have the SnapCenter repository in the same drive where SnapCenter Server is installed, then it is recommended to have 10 GB.
Minimum hard drive space for the SnapCenter repository	6 GB NOTE: If you have the SnapCenter Server in the same drive where SnapCenter repository is installed, then it is recommended to have 10 GB.
Required software packages	• Microsoft .NET Framework 4.5.2 or later • Windows Management Framework (WMF) 4.0 or later • PowerShell 4.0 or later For the latest information about supported versions, see NetApp Interoperability Matrix Tool.

SAN host requirements

If your SnapCenter host is part of a FC/iSCSI environment, you might need to install additional software on the system to enable access to ONTAP storage.

SnapCenter does not include Host Utilities or a DSM. If your SnapCenter host is part of a SAN environment, you might need to install and configure the following software:

- Host Utilities

  The Host Utilities support FC and iSCSI, and it enables you to use MPIO on your Windows Servers. For information, see Host Utilities documentation.

- Microsoft DSM for Windows MPIO

  This software works with Windows MPIO drivers to manage multiple paths between NetApp and Windows host computers.

  A DSM is required for high availability configurations.

If you were using ONTAP DSM, you should migrate to Microsoft DSM. For more information, see How to migrate from ONTAP DSM to Microsoft DSM.

Supported storage systems and applications

You should know the supported storage system, applications, and databases.

- SnapCenter supports ONTAP 8.3.0 and later to protect your data.
- SnapCenter supports Amazon FSx for NetApp ONTAP from SnapCenter Software 4.5 P1 patch release.

  If you are using Amazon FSx for NetApp ONTAP, ensure that the SnapCenter Server host plug-ins are upgraded to 4.5 P1 patch release to perform data protection operations.

  For information about Amazon FSx for NetApp ONTAP, see Amazon FSx for NetApp ONTAP documentation.

- SnapCenter supports protection of different applications and databases.

  For detailed information about the supported applications and databases, see NetApp Interoperability Matrix Tool.

Supported browsers

SnapCenter Software can be used on multiple browsers.

- Chrome

  If you are using v66, you might fail to launch SnapCenter GUI.

- Internet Explorer

  SnapCenter UI does not load properly if you are using IE 10 or earlier versions. You should upgrade to IE 11.

  - Only default-level security is supported.

    Making changes to Internet Explorer security settings results in significant browser display issues.

  - Internet Explorer compatibility view must be disabled.
- Microsoft Edge

For the latest information about supported versions, see NetApp Interoperability Matrix Tool.

Connection and port requirements

You should ensure that the connections and ports requirements are met before installing the SnapCenter Server and application or database plug-ins.

- Applications cannot share a port.

Each port must be dedicated to the appropriate application.

- For customizable ports, you can select a custom port during installation if you do not want to use the default port.

  You can change a plug-in port after installation by using the Modify Host wizard.

- For fixed ports, you should accept the default port number.
- Firewalls
  - Firewalls, proxies, or other network devices should not interfere with connections.
  - If you specify a custom port when you install SnapCenter, you should add a firewall rule on the plug-in host for that port for the SnapCenter Plug-in Loader.

The following table lists the different ports and their default values.

Type of port	Default port
SnapCenter port	8146 (HTTPS), bidirectional, customizable, as in the URL *https://server:8146* Used for communication between the SnapCenter client (the SnapCenter user) and the SnapCenter Server. Also used for communication from the plug-in hosts to the SnapCenter Server. To customize the port, see Install the SnapCenter Server using the install wizard.
SnapCenter SMCore communication port	8145 (HTTPS), bidirectional, customizable The port is used for communication between the SnapCenter Server and the hosts where the SnapCenter plug-ins are installed. To customize the port, see Install the SnapCenter Server using the install wizard.
MySQL port	3306 (HTTPS), bidirectional The port is used for communication between SnapCenter and MySQL repository database. You can create secured connections from the SnapCenter Server to the MySQL server. Learn more

Type of port	Default port
Windows plug-in hosts	135, 445 (TCP) In addition to ports 135 and 445, the dynamic port range specified by Microsoft should also be open. Remote install operations use the Windows Management Instrumentation (WMI) service, which dynamically searches this port range. For information on the dynamic port range supported, see Service overview and network port requirements for Windows The ports are used for communication between the SnapCenter Server and the host on which the plug-in is being installed. To push plug-in package binaries to Windows plug-in hosts, the ports must be open only on the plug-in host, and they can be closed after installation.
Linux or AIX plug-in hosts	22 (SSH) The ports are used for communication between the SnapCenter Server and the host where the plug-in is being installed. The ports are used by SnapCenter to copy plug-in package binaries to Linux or AIX plug-in hosts and should be open or excluded from the firewall or iptables.
SnapCenter Plug-ins Package for Windows, SnapCenter Plug-ins Package for Linux or SnapCenter Plug-ins Package for AIX	8145 (HTTPS), bidirectional, customizable The port is used for communication between SMCore and hosts where the plug-ins package is installed. The communication path also needs to be open between the SVM management LIF and the SnapCenter Server. To customize the port, see Add hosts and install SnapCenter Plug-in for Microsoft Windows or Add hosts and install SnapCenter Plug-ins package for Linux or AIX.
SnapCenter Plug-in for Oracle Database	27216, customizable The default JDBC port is used by the plug-in for Oracle for connecting to the Oracle database. To customize the port, see Add hosts and install SnapCenter Plug-ins package for Linux or AIX.

Type of port	Default port
Custom plug-ins for SnapCenter	9090 (HTTPS), fixed This is an internal port that is used only on the custom plug-in host; no firewall exception is required. Communication between the SnapCenter Server and custom plug-ins is routed through port 8145.
ONTAP cluster or SVM communication port	443 (HTTPS), bidirectional80 (HTTP), bidirectional The port is used by the SAL (Storage Abstraction Layer) for communication between the host running SnapCenter Server and SVM. The port is currently also used by the SAL on SnapCenter for Windows Plug-in hosts for communication between the SnapCenter plug-in host and SVM.
SnapCenter Plug-in for SAP HANA Database vCode Spell Checkerports	3instance_number13 or 3instance_number15, HTTP or HTTPS, bidirectional, and customizable For a multitenant database container (MDC) single tenant, the port number ends with 13; for non MDC, the port number ends with 15. For example, 32013 is the port number for instance 20 and 31015 is the port number for instance 10. To customize the port, see Add hosts and install plug-in packages on remote hosts.
Domain controller communication port	See the Microsoft documentation to identify the ports that should be opened in the firewall on a domain controller for authentication to work properly. It is necessary to open the Microsoft required ports on the domain controller so that the SnapCenter Server, Plug-in hosts, or other Windows client can authenticate the users.

To modify the port details, see Modify plug-in hosts.

SnapCenter licenses

SnapCenter requires several licenses to enable data protection of applications, databases, file systems, and virtual machines. The type of SnapCenter licenses you install depends on your storage environment and the features that you want to use.

License	Where required
SnapCenter Standard controller-based	Required for FAS and AFF SnapCenter Standard license is a controller-based license and is included as part of the premium bundle. If you have the SnapManager Suite license, you also get the SnapCenter Standard license entitlement. If you want to install SnapCenter on a trial basis with FAS or AFF storage, you can obtain a Premium Bundle evaluation license by contacting the sales representative. SnapCenter is also offered as part of data protection bundle. If you have purchased A400 or later, you should purchase the data protection bundle.
SnapCenter Standard capacity-based	Required with ONTAP Select and Cloud Volumes ONTAP If you are a Cloud Volumes ONTAP or ONTAP Select customer, you need to procure a per TB capacity-based license based on the data managed by SnapCenter. By default, SnapCenter ships a built-in 90-day 100 TB SnapCenter Standard capacity-based trial license. For other details, contact the sales representative.
SnapMirror or SnapVault	ONTAP Either SnapMirror or SnapVault license is required if replication is enabled in SnapCenter.
SnapRestore	Required to restore and verify backups. On primary storage systems • Required on SnapVault destination systems to perform remote verification and to restore from a backup. • Required on SnapMirror destination systems to perform remote verification.

License	Where required
FlexClone	Required to clone databases and verification operations. On primary and secondary storage systems • Required on SnapVault destination systems to create clones from secondary vault backup. • Required on SnapMirror destination systems to create clones from secondary SnapMirror backup.
Protocols	• iSCSI or FC license for LUNs • CIFS license for SMB shares • NFS license for NFS type VMDKs • iSCSI or FC license for VMFS type VMDKs Required on SnapMirror destination systems to serve data if a source volume is unavailable.
SnapCenter Standard licenses (optional)	Secondary destinations It is recommended, but not required, that you add SnapCenter Standard licenses to secondary destinations. If SnapCenter Standard licenses are not enabled on secondary destinations, you cannot use SnapCenter to backup resources on the secondary destination after performing a failover operation. However, a FlexClone license is required on secondary destinations to perform clone and verification operations.

SnapCenter Advanced and SnapCenter NAS File Services licenses are deprecated, and are no longer available.

You should install one or more SnapCenter licenses. For information on how to add licenses, see Add SnapCenter Standard controller-based licenses or Add SnapCenter Standard capacity-based licenses.

Single Mailbox Recovery (SMBR) licenses

If you are using SnapCenter Plug-in for Exchange to manage Microsoft Exchange Server databases and Single Mailbox Recovery (SMBR), you would need additional license for SMBR which needs to be purchased separately based on user mailbox.

NetApp® Single Mailbox Recovery has come to the end of availability (EOA) on May 12, 2023. For more information, refer CPC-00507. NetApp will continue to support customers that have purchased mailbox capacity, maintenance, and support through marketing part numbers introduced on June 24, 2020, for the

duration of the support entitlement.

NetApp Single Mailbox Recovery is a partner product provided by Ontrack. Ontrack PowerControls offers capabilities that are similar to those of NetApp Single Mailbox Recovery. Customers can procure new Ontrack PowerControls software licenses and Ontrack PowerControls maintenance and support renewals from Ontrack (through licensingteam@ontrack.com) for granular mailbox recovery after the May 12, 2023, EOA date.

Authentication methods for your credentials

Credentials use different authentication methods depending upon the application or environment. Credentials authenticate users so they can perform SnapCenter operations. You should create one set of credentials for installing plug-ins and another set for data protection operations.

Windows authentication

The Windows authentication method authenticates against Active Directory. For Windows authentication, Active Directory is set up outside of SnapCenter. SnapCenter authenticates with no additional configuration. You need a Windows credential to perform tasks such as adding hosts, installing plug-in packages, and scheduling jobs.

Untrusted domain authentication

SnapCenter allows the creation of Windows credentials using users and groups belonging to the untrusted domains. For the authentication to succeed, you should register the untrusted domains with SnapCenter.

Local workgroup authentication

SnapCenter allows the creation of Windows credentials with local workgroup users and groups. The Windows authentication for local workgroup users and groups does not happen at the time of Windows credential creation but is deferred until the host registration and other host operations are performed.

SQL Server authentication

The SQL authentication method authenticates against a SQL Server instance. This means that a SQL Server instance must be discovered in SnapCenter. Therefore, before adding a SQL credential, you must add a host, install plug-in packages, and refresh resources. You need SQL Server authentication for performing operations such as scheduling on SQL Server or discovering resources.

Linux authentication

The Linux authentication method authenticates against a Linux host. You need Linux authentication during the initial step of adding the Linux host and installing the SnapCenter Plug-ins Package for Linux remotely from the SnapCenter GUI.

AIX authentication

The AIX authentication method authenticates against an AIX host. You need AIX authentication during the initial step of adding the AIX host and installing the SnapCenter Plug-ins Package for AIX remotely from the SnapCenter GUI.

Oracle database authentication

The Oracle database authentication method authenticates against an Oracle database. You need an Oracle database authentication to perform operations on the Oracle database if the operating system (OS) authentication is disabled on the database host. Therefore, before adding a Oracle database credential, you should create an Oracle user in the Oracle database with sysdba privileges.

Oracle ASM authentication

The Oracle ASM authentication method authenticates against an Oracle Automatic Storage Management (ASM) instance. If you are required to access the Oracle ASM instance and if the operating system (OS) authentication is disabled on the database host, you need an Oracle ASM authentication. Therefore, before adding an Oracle ASM credential, you should create an Oracle user with sysasm privileges in the ASM instance.

RMAN catalog authentication

The RMAN catalog authentication method authenticates against the Oracle Recovery Manager (RMAN) catalog database. If you have configured an external catalog mechanism and registered your database to catalog database, you need to add RMAN catalog authentication.

Storage connections and credentials

Before performing data protection operations, you should set up the storage connections and add the credentials that the SnapCenter Server and the SnapCenter plug-ins will use.

- **Storage connections**

  The storage connections give the SnapCenter Server and SnapCenter plug-ins access to the ONTAP storage. Setting up these connections also involves configuring AutoSupport and Event Management System (EMS) features.

- **Credentials**
  - Domain administrator or any member of the administrator group

    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:

    - *NetBIOS\UserName*
    - *Domain FQDN\UserName*
    - *UserName@upn*
  - Local administrator (for workgroups only)

    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: *UserName*

- Credentials for individual resource groups

  If you set up credentials for individual resource groups and the username does not have full admin privileges, you must assign at least the resource group and backup privileges to the username.

Copyright information

Copyright © 2026 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.