



了解SnapCenter软件

SnapCenter software

NetApp
February 20, 2026

目录

了解SnapCenter软件	1
SnapCenter 概述	1
主要功能:	1
SnapCenter架构和组件	2
SnapCenter中的安全性功能	5
CA 证书概述	6
双向SSL通信	6
基于证书的身份验证概述	6
多因素身份验证 (MFA)	6
SnapCenter中基于角色的访问控制	6
SnapCenter中的RBAC类型	7
分配给预定义SnapCenter角色的权限	8
SnapCenter中的灾难恢复	11
SnapCenter 服务器灾难恢复	11
SnapCenter 插件和存储灾难恢复	12
SnapCenter所需的许可证	12
SnapCenter中的SnapMirror活动同步	14
数据保护的关键概念	14
Resources	15
Resource group	15
策略	15
一致性组 (CG)	15
前处理脚本和后处理脚本的使用	15
SnapCenter支持的存储系统和应用程序	16
支持的存储系统	16
支持的应用程序和数据库	17
SnapCenter凭据的身份验证方法	17
Windows 身份验证	17
不可信域身份验证	17
本地工作组身份验证	17
SQL Server 身份验证	17
Linux 身份验证	18
AIX 身份验证	18
Oracle 数据库身份验证	18
Oracle ASM 身份验证	18
RMAN 目录身份验证	18

了解SnapCenter软件

SnapCenter 概述

SnapCenter software是一个简单、集中且可扩展的平台，用于应用程序一致的数据保护。它保护混合云中ONTAP系统上的应用程序、数据库、主机文件系统和虚拟机。

SnapCenter使用NetApp Snapshot、 SnapRestore、 FlexClone、 SnapMirror和SnapVault技术来提供：

- 快速，节省空间，应用程序一致且基于磁盘的备份
- 快速、详细的恢复和应用程序一致的恢复
- 快速，节省空间的克隆

SnapCenter包括SnapCenter服务器和轻量级插件。您可以自动将插件部署到远程应用程序主机，安排备份、验证和克隆操作，并监控数据保护操作。

您可以在本地或公共云上安装SnapCenter来保护数据。

- 本地保护以下内容：
 - 位于ONTAP FAS、AFF或ASA主系统上并复制到ONTAP FAS、AFF或ASA二级系统的数据
 - ONTAP Select 主系统上的数据
 - 位于ONTAP FAS、AFF或ASA主系统和二级系统上并受本地StorageGRID对象存储保护的数据
 - ONTAP ASA R2主系统和二级系统上的数据
- 在混合云中本地保护以下内容：
 - 位于ONTAP FAS、AFF或ASA主系统上并复制到Cloud Volumes ONTAP的数据
 - 位于ONTAP FAS、AFF或ASA主系统和辅助系统上的数据，使用NetApp备份和恢复集成保护到云中的对象和归档存储
- 在公有云中保护以下内容：
 - 位于 Cloud Volumes ONTAP（原 ONTAP 云）主系统上的数据
 - Amazon FSX for ONTAP 上的数据
 - 主Azure NetApp Files (Oracle、Microsoft SQL和SAP HANA)上的数据

主要功能：

SnapCenter提供以下主要功能：

- 为不同应用程序提供应用程序一致的集中式数据保护

支持对Microsoft Exchange Server、Microsoft SQL Server、Linux或AIX上的Oracle数据库、SAP HANA数据库、IBM DB2、PostgreSQL、MySQL以及ONTAP系统上运行的Windows主机文件系统进行数据保护。SnapCenter 还支持 MongoDB、Storage、MaxDB、Sybase ASE、ORASCMP 等应用程序的保护。

- 基于策略的备份

基于策略的备份利用NetApp Snapshot 技术来创建快速、节省空间、应用程序一致的基于磁盘的备份。您可以通过更新现有的保护关系来设置这些备份到二级存储的自动保护。

- 多种资源的备份

您可以使用SnapCenter资源组一次备份同一类型的多个资源（应用程序、数据库或主机文件系统）。

- 还原和恢复

SnapCenter 可以快速，精细地恢复备份，并实现应用程序一致且基于时间的恢复。您可以从混合云中的任意目标进行还原。

- 克隆

SnapCenter提供快速、节省空间且应用程序一致的克隆。您可以在混合云中的任意目的地进行克隆。

- 单用户管理图形用户界面

SnapCenter提供单一界面来管理任何混合云目标中的备份和克隆。

- REST API ， Windows cmdlet ， UNIX 命令

SnapCenter提供了REST API、用于实现与任何业务流程软件集成以及使用Windows PowerShell cmdlet和命令行界面的大多数功能。

- 集中式数据保护信息板和报告

- 基于角色的访问控制(Role-Based Access Control、RBAC)、用于确保安全性和委派

- 具有高可用性的内置存储库数据库、用于存储所有备份元数据

- 自动推送安装插件

- 高可用性

- 灾难恢复（DR）

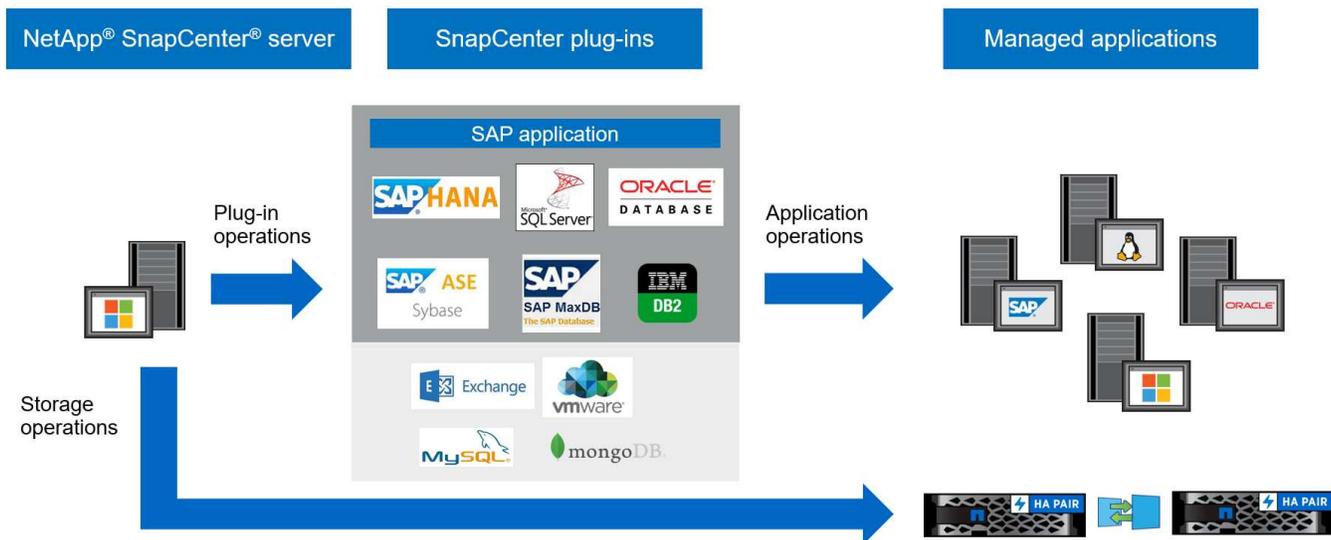
- SnapLock "[了解更多信息](#)"

- SnapMirror主动同步(最初作为SnapMirror业务连续性[SM-BC)发布)

- 同步镜像 "[了解更多信息](#)"

SnapCenter架构和组件

SnapCenter采用分层设计，包含中央管理服务器和插件主机。服务器和插件主机可以位于不同的位置。



SnapCenter包括SnapCenter服务器、适用于Windows的SnapCenter插件软件包和适用于Linux的SnapCenter插件软件包。每个软件包都包含适用于各种应用程序和基础架构组件的插件。

SnapCenter 服务器

SnapCenter服务器支持Microsoft Windows和Linux (RHEL 8.x、RHEL 9.x、SLES 15 SP5)操作系统。SnapCenter服务器包括Web服务器、基于HTML5的集中式用户界面、PowerShell cmdlet、REST API和SnapCenter存储库。

SnapCenter将其操作的相关信息存储在SnapCenter存储库中。

SnapCenter 插件

每个 SnapCenter 插件都支持特定环境，数据库和应用程序。

插件名称	包含在安装包中	需要其他插件	安装在主机上	支持的平台
适用于Microsoft SQL Server的SnapCenter插件	适用于Windows的插件软件包	适用于 Windows 的插件	SQL Server 主机	Windows
适用于Windows的SnapCenter插件	适用于Windows的插件软件包		Windows 主机	Windows
适用于Microsoft Exchange Server的SnapCenter插件	适用于Windows的插件软件包	适用于 Windows 的插件	Exchange Server 主机	Windows
适用于Oracle数据库的SnapCenter插件	适用于Linux的插件软件包和适用于AIX的插件软件包	适用于 UNIX 的插件	Oracle 主机	Linux 或 AIX

插件名称	包含在安装包中	需要其他插件	安装在主机上	支持的平台
适用于SAP HANA数据库的SnapCenter插件	适用于Linux的插件软件包和适用于Windows的插件软件包	适用于UNIX的插件或适用于Windows的插件	HDBSQL 客户端主机	Linux 或 Windows
适用于IBM DB2的SnapCenter插件	适用于Linux的插件软件包和适用于Windows的插件软件包	适用于UNIX的插件或适用于Windows的插件	DB2主机	Linux、AIX或Windows
适用于PostgreSQL的SnapCenter插件	适用于Linux的插件软件包和适用于Windows的插件软件包	适用于UNIX的插件或适用于Windows的插件	PostgreSQL主机	Linux 或 Windows
适用于MySQL的SnapCenter插件	适用于Linux的插件软件包和适用于Windows的插件软件包	适用于 UNIX 的插件或适用于 Windows 的插件	MySQL主机	Linux 或 Windows
适用于MongoDB的SnapCenter插件	适用于Linux的插件软件包和适用于Windows的插件软件包	适用于UNIX的插件或适用于Windows的插件	MongoDB主机	Linux 或 Windows
适用于ORASCPM的SnapCenter插件(Oracle应用程序)	适用于Linux的插件软件包和适用于Windows的插件软件包	适用于UNIX的插件或适用于Windows的插件	Oracle 主机	Linux 或 Windows
适用于SAP ASE的SnapCenter插件	适用于Linux的插件软件包和适用于Windows的插件软件包	适用于UNIX的插件或适用于Windows的插件	SAP主机	Linux 或 Windows
适用于SAP MaxDB的SnapCenter插件	适用于Linux的插件软件包和适用于Windows的插件软件包	适用于UNIX的插件或适用于Windows的插件	SAP MaxDB主机	Linux 或 Windows
适用于存储的SnapCenter插件	适用于Linux的插件软件包和适用于Windows的插件软件包	适用于UNIX的插件或适用于Windows的插件	存储主机	Linux 或 Windows

SnapCenter Plug-in for VMware vSphere支持虚拟机 (VM)、数据存储库和虚拟机磁盘 (VMDK) 的崩溃一致性和VM 一致性备份和还原操作。它还支持虚拟化数据库和文件系统的应用程序一致的备份和恢复操作。

要保护数据库、文件系统、虚拟机或虚拟机上的数据存储区，请部署SnapCenter Plug-in for VMware vSphere。欲了解详细信息，请参阅 ["适用于 VMware vSphere 的 SnapCenter 插件文档"](#)。

SnapCenter 存储库

SnapCenter 存储库有时称为 NSM 数据库，用于存储每个 SnapCenter 操作的信息和元数据。

SnapCenter Server 安装默认安装 MySQL Server 存储库数据库。如果您已经安装了 MySQL Server 并想要执行 SnapCenter Server 的全新安装，则必须卸载 MySQL Server。

SnapCenter 支持 MySQL Server 8.0.37 或更高版本作为 SnapCenter 存储库数据库。如果您将早期版本的 MySQL Server 与早期版本的 SnapCenter 一起使用，则 SnapCenter 升级过程会将 MySQL Server 升级到版本 8.0.37 或更高版本。

SnapCenter 存储库存储以下信息和元数据：

- 备份，克隆，还原和验证元数据
- 报告，作业和事件信息
- 主机和插件信息
- 角色，用户和权限详细信息
- 存储系统连接信息

SnapCenter 中的安全性功能

SnapCenter 采用严格的安全性和身份验证功能，可确保数据安全。

SnapCenter 包括以下安全功能：

- 与 SnapCenter 的所有通信都使用基于 SSL 的 HTTP（HTTPS）。
- SnapCenter 中的所有凭据均使用高级加密标准（Advanced Encryption Standard，AES）加密进行保护。
- 支持符合联邦信息处理标准(FIPS)的安全算法。
- 支持使用客户提供的授权CA证书。
- 支持使用传输层安全(Transport Layer Security、TLS) 1.3与ONTAP进行通信。您还可以使用TLS 1.2在客户端和服务器之间进行通信。
- 支持一组特定的SSL加密套件、以确保整个网络通信的安全性。 ["了解更多信息。"](#)(英文)。
- SnapCenter 安装在公司的防火墙内，用于访问 SnapCenter 服务器并在 SnapCenter 服务器和插件之间进行通信。
- SnapCenter API 和操作访问使用使用 AES 加密加密的令牌，这些令牌将在 24 小时后过期。
- SnapCenter 与 Windows Active Directory 集成，用于控制访问权限的登录和基于角色的访问控制（Role-Based Access Control，RBAC）。
- ONTAP for Windows和Linux主机上的SnapCenter 支持IPsec。 ["了解更多信息。"](#)
- SnapCenter PowerShell cmdlet 可保护会话安全。
- 默认情况下，如果 15 分钟处于非活动状态， SnapCenter 会向您发出警告，指出您将在 5 分钟后注销。

处于非活动状态 20 分钟后，SnapCenter 将注销，您必须重新登录。您可以修改注销期限。

- 在5次错误登录尝试后、登录被暂时禁用。
- 支持SnapCenter 服务器和ONTAP 之间的CA证书身份验证。"[了解更多信息](#)"。
- 完整性验证程序已添加到SnapCenter 服务器和插件中、它会在全新安装和升级操作期间验证所有已发送的二进制文件。

CA 证书概述

SnapCenter 服务器安装程序可在安装期间启用集中式 SSL 证书支持。为了增强服务器和插件之间的安全通信，SnapCenter 支持使用客户提供的授权 CA 证书。

您应在安装 SnapCenter 服务器和相应插件后部署 CA 证书。有关详细信息，请参见 "[生成 CA 证书 CSR 文件](#)"。

您还可以为适用于 VMware vSphere 的 SnapCenter 插件部署 CA 证书。有关详细信息，请参见 "[创建和导入证书](#)"。

双向SSL通信

双向SSL通信可确保SnapCenter服务器与插件之间的相互通信安全。

基于证书的身份验证概述

基于证书的身份验证可验证尝试访问SnapCenter插件主机的各个用户的真实性。用户应导出不带专用密钥的SnapCenter服务器证书、并将其导入到插件主机受信任存储中。仅当启用了双向SSL功能时、基于证书的身份验证才起作用。

多因素身份验证（MFA）

MFA通过安全断言标记语言(SAML)使用第三方身份提供程序(IdP)来管理用户会话。此功能可选择使用TOTP、生物识别、推送通知等多种因素以及现有用户名和密码、从而增强身份验证的安全性。此外、它还支持客户使用自己的用户身份提供程序在其产品组合中获得统一的用户登录(SSO)。

MFA仅适用于SnapCenter 服务器UI登录。登录通过IdP Active Directory联合身份验证服务(AD FS)进行身份验证。您可以在AD FS上配置各种身份验证因素。SnapCenter 是服务提供商、您应将SnapCenter 配置为AD FS 中的依赖方。要在SnapCenter 中启用MFA、您需要AD FS元数据。

有关启用MFA的信息、请参见 "[启用多因素身份验证](#)"。

SnapCenter中基于角色的访问控制

SnapCenter基于角色的访问控制 (RBAC) 和ONTAP权限允许SnapCenter管理员向用户或组分配资源访问权限。这种集中管理的访问使应用程序管理员能够在指定环境中安全地工作。

您应该创建或修改角色并为用户添加资源访问权限。首次设置SnapCenter时，将 Active Directory 用户或组添加到角色并将资源分配给这些用户或组。



SnapCenter不会创建用户或组帐户。在操作系统或数据库的 Active Directory 中创建用户或组帐户。

SnapCenter中的RBAC类型

SnapCenter支持以下类型的基于角色的访问控制：

- SnapCenter RBAC
- 应用程序级 RBAC
- 适用于VMware vSphere RBAC的SnapCenter插件
- ONTAP 权限

SnapCenter RBAC

SnapCenter具有预定义的角色，您可以将用户或组分配给这些角色。

- SnapCenter 管理员角色
- 应用程序备份和克隆管理员角色
- 备份和克隆查看器角色
- 基础架构管理员角色

当您为用户分配角色时，SnapCenter会在“作业”页面上显示与该用户相关的作业，除非该用户具有 SnapCenterAdmin 角色。

您还可以创建新角色并管理权限和用户。您可以为用户或组分配访问主机，存储连接和资源组等 SnapCenter 对象的权限。

您可以为同一林中的用户和组以及属于不同林的用户分配 RBAC 权限。您不能为属于林间嵌套组的用户分配 RBAC 权限。



创建自定义角色时，请确保它包含 SnapCenterAdmin 角色的所有权限。如果您仅复制部分权限，SnapCenter将阻止您执行所有操作。

用户通过用户界面或 PowerShell cmdlet 登录时必须进行身份验证。如果用户有多个角色，则登录后选择一个角色。运行 API 也需要身份验证。

应用程序级 RBAC

SnapCenter 使用凭据验证授权的 SnapCenter 用户是否也具有应用程序级别的权限。

例如，要在 SQL Server 环境中执行数据保护操作，请设置正确的 Windows 或 SQL 凭据。如果要在 ONTAP 存储上的 Windows 文件系统环境中执行数据保护操作，SnapCenter 管理员角色必须在 Windows 主机上具有管理员权限。

同样，如果您想在 Oracle 数据库上执行数据保护操作，并且如果数据库主机上禁用了操作系统 (OS) 身份验证，则必须使用 Oracle 数据库或 Oracle ASM 凭据设置凭据。SnapCenter 服务器根据操作使用其中一种方法对设置的凭据进行身份验证。

适用于 VMware vSphere RBAC 的 SnapCenter 插件

如果您使用 SnapCenter VMware 插件进行 VM 一致的数据保护，则 vCenter Server 可提供额外级别的 RBAC。SnapCenter VMware 插件支持 vCenter Server RBAC 和 ONTAP RBAC。 ["了解更多信息"](#)

注意：NetApp 建议您为 SnapCenter Plug-in for VMware vSphere 创建一个 ONTAP 角色，并为其分配所有必需的权限。

ONTAP 权限

您应该创建具有访问存储系统所需权限的 vsadmin 帐户。 ["了解更多信息"](#)

分配给预定义 SnapCenter 角色的权限

将用户添加到角色时，分配 StorageConnection 权限以启用存储虚拟机 (SVM) 通信，或者将 SVM 分配给用户以授予使用 SVM 的权限。存储连接权限允许用户创建 SVM 连接。

例如，SnapCenter 管理员可以创建 SVM 连接并将其分配给 App Backup 和 Clone Admin 用户，而这些用户无法创建或编辑 SVM 连接。如果没有 SVM 连接，用户就无法执行备份、克隆或恢复操作。

SnapCenter 管理员角色

SnapCenter 管理员角色已启用所有权限。您不能修改此角色的权限。您可以将用户和组添加到角色或将其删除。

应用程序备份和克隆管理员角色

应用程序备份和克隆管理员角色具有为应用程序备份和克隆相关任务执行管理操作所需的权限。此角色不具有主机管理，配置，存储连接管理或远程安装的权限。

权限	enabled	创建	读取	更新	删除
Resource Group	不适用	是的。	是的。	是的。	是的。
策略	不适用	是的。	是的。	是的。	是的。
备份	不适用	是的。	是的。	是的。	是的。
主机	不适用	是的。	是的。	是的。	是的。
存储连接	不适用	否	是的。	否	否
克隆	不适用	是的。	是的。	是的。	是的。
配置	不适用	否	是的。	否	否
信息板	是的。	不适用	不适用	不适用	不适用

权限	enabled	创建	读取	更新	删除
报告	是的。	不适用	不适用	不适用	不适用
还原	是的。	不适用	不适用	不适用	不适用
资源	是的。	是的。	是的。	是的。	是的。
插件安装 / 卸载	否	不适用		不适用	不适用
migration	否	不适用	不适用	不适用	不适用
挂载	是的。	是的。	不适用	不适用	不适用
卸载	是的。	是的。	不适用	不适用	不适用
完整卷还原	否	否	不适用	不适用	不适用
二级保护	否	否	不适用	不适用	不适用
作业监控器	是的。	不适用	不适用	不适用	不适用

备份和克隆查看器角色

备份和克隆查看者角色具有所有权限的只读查看。此角色还具有发现、报告和访问仪表板的权限。

权限	enabled	创建	读取	更新	删除
Resource Group	不适用	否	是的。	否	否
策略	不适用	否	是的。	否	否
备份	不适用	否	是的。	否	否
主机	不适用	否	是的。	否	否
存储连接	不适用	否	是的。	否	否
克隆	不适用	否	是的。	否	否
配置	不适用	否	是的。	否	否
信息板	是的。	不适用	不适用	不适用	不适用

权限	enabled	创建	读取	更新	删除
报告	是的。	不适用	不适用	不适用	不适用
还原	否	否	不适用	不适用	不适用
资源	否	否	是的。	是的。	否
插件安装 / 卸载	否	不适用	不适用	不适用	不适用
migration	否	不适用	不适用	不适用	不适用
挂载	是的。	不适用	不适用	不适用	不适用
卸载	是的。	不适用	不适用	不适用	不适用
完整卷还原	否	不适用	不适用	不适用	不适用
二级保护	否	不适用	不适用	不适用	不适用
作业监控器	是的。	不适用	不适用	不适用	不适用

基础架构管理员角色

基础架构管理员角色已启用主机管理，存储管理，配置，资源组，远程安装报告，并访问信息板。

权限	enabled	创建	读取	更新	删除
Resource Group	不适用	是的。	是的。	是的。	是的。
策略	不适用	否	是的。	是的。	是的。
备份	不适用	是的。	是的。	是的。	是的。
主机	不适用	是的。	是的。	是的。	是的。
存储连接	不适用	是的。	是的。	是的。	是的。
克隆	不适用	否	是的。	否	否
配置	不适用	是的。	是的。	是的。	是的。
信息板	是的。	不适用	不适用	不适用	不适用

权限	enabled	创建	读取	更新	删除
报告	是的。	不适用	不适用	不适用	不适用
还原	是的。	不适用	不适用	不适用	不适用
资源	是的。	是的。	是的。	是的。	是的。
插件安装 / 卸载	是的。	不适用	不适用	不适用	不适用
migration	否	不适用	不适用	不适用	不适用
挂载	否	不适用	不适用	不适用	不适用
卸载	否	不适用	不适用	不适用	不适用
完整卷还原	否	否	不适用	不适用	不适用
二级保护	否	否	不适用	不适用	不适用
作业监控器	是的。	不适用	不适用	不适用	不适用

SnapCenter中的灾难恢复

通过SnapCenter灾难恢复(DR)功能、您可以从资源损坏或服务器崩溃等灾难中恢复。它有助于还原SnapCenter存储库、服务器计划、配置组件以及适用于SQL Server的SnapCenter插件及其存储。

本节介绍SnapCenter中的两种灾难恢复类型：

SnapCenter 服务器灾难恢复

- SnapCenter 服务器数据会进行备份、并且可以在不向SnapCenter 服务器添加任何插件或由服务器管理的情况下进行恢复。
- 二级SnapCenter 服务器应安装在与主SnapCenter 服务器相同的安装目录和端口上。
- 对于多因素身份验证(MFA)、请在SnapCenter服务器灾难恢复期间关闭所有浏览器选项卡、然后重新打开浏览器以重新登录。这将清除现有或活动会话Cookie并更新正确的配置数据。
- SnapCenter灾难恢复功能使用REST API备份SnapCenter服务器。请参阅。 ["用于 SnapCenter 服务器灾难恢复的 REST API 工作流"](#)
- 与审核设置相关的配置文件不会在灾难恢复备份中进行备份、在还原操作后、也不会备份到灾难恢复服务器上。您应手动重复审核日志设置。

SnapCenter 插件和存储灾难恢复

DR仅适用于适用于SQL Server的SnapCenter插件。如果此插件已关闭、请切换到另一个SQL主机、然后按照几个步骤恢复数据。请参阅。"[适用于 SQL Server 的 SnapCenter 插件的灾难恢复](#)"

SnapCenter使用ONTAP SnapMirror复制数据、可通过将中的数据同步到二级站点来用于灾难恢复。要启动故障转移、请中断SnapMirror复制。在回退期间、反向执行同步、以便将数据从灾难恢复站点复制回主位置。

SnapCenter所需的许可证

SnapCenter 需要多个许可证才能对应用程序，数据库，文件系统和虚拟机进行数据保护。您安装的 SnapCenter 许可证类型取决于您的存储环境和要使用的功能。

许可证	必要时
基于 SnapCenter 标准控制器	<p>对于FAS、AFF、ASA为必需项</p> <p>SnapCenter标准版许可证是一种基于控制器的许可证、包含在NetApp ONTAP One中。如果您拥有 SnapManager 套件许可证，则还可以获得 SnapCenter 标准许可证授权。如果您要在FAS、AFF或ASA存储中试用SnapCenter、可以联系销售代表来获取NetApp ONTAP One评估版许可证。</p> <p>有关NetApp ONTAP One附带的许可证的信息，请参阅 "NetApp ONTAP One附带的许可证"。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> SnapCenter 也作为数据保护包的一部分提供。如果您购买的是 A400 或更高版本，则应购买数据保护包。</div>
SnapMirror 或 SnapVault	<p>ONTAP</p> <p>如果在 SnapCenter 中启用了复制，则需要 SnapMirror 或 SnapVault 许可证。</p>
SnapRestore	<p>用于还原和验证备份。</p> <p>在主存储系统上</p> <ul style="list-style-type: none">• 在 SnapVault 目标系统上执行远程验证和从备份中还原时需要使用。• SnapMirror 目标系统上执行远程验证所需的。

许可证	必要时
FlexClone	<p>克隆数据库和验证操作所需。</p> <p>在主存储系统和二级存储系统上。</p> <ul style="list-style-type: none"> 在 SnapVault 目标系统上需要此功能才能从二级存储备份创建克隆。 在 SnapMirror 目标系统上需要使用此功能从二级 SnapMirror 备份创建克隆。
协议许可证	<ul style="list-style-type: none"> LUN 的 iSCSI 或 FC 许可证 SMB 共享的 CIFS 许可证 NFS 类型 VMDK 的 NFS 许可证 VMFS 类型 VMDK 的 iSCSI 或 FC 许可证 <p>如果源卷不可用，则 SnapMirror 目标系统需要提供数据。</p>
SnapCenter 标准许可证（可选）	<p>二级目标</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>建议（但不要求）将 SnapCenter 标准版许可证添加到二级目标。如果二级目标上未启用 SnapCenter 标准许可证，则在执行故障转移操作后，您将无法使用 SnapCenter 备份二级目标上的资源。但是，要执行克隆和验证操作，二级目标需要 FlexClone 许可证。</p> </div>
单邮箱恢复（SMBR）许可证	<p>如果您使用适用于 Exchange 的 SnapCenter 插件管理 Microsoft Exchange Server 数据库和单邮箱恢复（SMBR），则需要为 SMBR 提供额外的许可证，此许可证需要根据用户邮箱单独购买。</p> <p>NetApp®Single Mailbox Recovery已于2023年5月12日终止提供(EOA)。有关详细信息、请参见 "CP-00507"。在支持授权期间、NetApp将继续通过2020年6月24日推出的营销部件号为已购买邮箱容量、维护和支持的客户提供支持。</p> <p>NetApp Single Mailbox Recovery是Ontrack提供的合作伙伴产品。Ontrack PowerControls提供的功能与NetApp Single Mailbox Recovery类似。在EOA日期2023年5月12日之后、客户可以从Ontrack (通过licensingteam@ontrack.com)购买新的Ontrack PowerControls软件许可证以及Ontrack PowerControls维护和支持续订、以实现邮箱粒度恢复。</p>



SnapCenter 高级版和 SnapCenter NAS 文件服务许可证已弃用，不再可用。Amazon FSx for NetApp ONTAP、ONTAP Select、Cloud Volumes ONTAP和Azure NetApp Files不再需要标准许可证和基于容量的许可证。

您应安装一个或多个 SnapCenter 许可证。有关如何添加许可证的信息，请参见 ["添加基于 SnapCenter 标准控制器的许可证"](#)。

SnapCenter中的SnapMirror活动同步

通过SnapMirror主动同步、即使在整个站点发生故障时、业务服务也可以继续运行、从而支持应用程序使用二级副本透明地进行故障转移。使用SnapMirror活动同步触发故障转移无需手动干预或额外编写脚本。

有关SnapMirror活动同步的详细信息，请参阅 ["SnapMirror活动同步概述"](#)。

对于SnapMirror主动同步、请确保满足各种硬件、软件和系统配置要求。有关信息、请参见 ["前提条件"](#)

此功能支持的插件包括适用于SQL Server的SnapCenter插件、适用于Windows的SnapCenter插件、适用于Oracle数据库的SnapCenter插件、适用于SAP HANA数据库的SnapCenter插件、适用于Microsoft Exchange Server的SnapCenter插件以及适用于Unix的SnapCenter插件。

安装SnapCenter服务器和插件后，您应该启用SnapCenter的 REST API 来检测SnapMirror活动同步关系。

- 在SnapCenter服务器主机上，编辑 `C:\Program Files\NetApp\SMCore\SMCoreServiceHost.dll.config` 文件以将 `IsRestEnabledForStorageConnection` 参数的值修改为 `true`，然后重新启动SnapCenter SMCore 服务。
- 在 Windows 插件主机上：
 - 编辑 `C:\Program Files\NetApp\SnapCenter\SMCore\SMCoreServiceHost.dll.config` 文件，将 `IsRestEnabledForStorageConnection` 参数的值修改为 `true`。
 - 编辑 `C:\Program Files\NetApp\SnapCenter\SMCore\SnapDriveService.dll.config` 文件，将 `IsRestEnabledForStorageConnection` 参数的值修改为 `true`。
 - 重新启动SnapCenter SMCore 服务。



要在SnapCenter中支持主机启动程序接近、应在ONTAP中设置其值、即源或目标。

SnapCenter中不支持的使用情形：

- 如果在ONTAP中将SnapMirror活动同步关系上的策略从 `_automatedfailover_` 更改为 `_automatedfailoverdew双工_`、从而将现有的非对称SnapMirror活动同步工作负载转换为对称工作负载、则SnapCenter不支持这种转换。
- 如果某个资源组有备份(已在SnapCenter中受保护)、然后将SnapMirror活动同步关系上的存储策略从 `_automatedfailover_` 更改为ONTAP中的 `_automatedfailoverdew双工_`、则SnapCenter不支持这种做法。

数据保护的关键概念

在使用SnapCenter之前、请了解有关备份、克隆和还原的重要概念。

Resources

资源包括使用SnapCenter备份或克隆的数据库、Windows文件系统或文件共享。根据您的环境、资源可能还包括数据库实例、SQL Server可用性组、Oracle数据库、RAC数据库或自定义应用程序组。

Resource group

资源组是主机或集群上的一组资源、可能来自多个主机和集群。根据指定的计划、对资源组执行的操作将应用于其所有资源。您可以对单个资源或组执行按需或计划备份。



如果共享资源组中的一台主机进入维护模式、则该组的所有计划操作都将在所有主机上暂停。

使用相关插件备份特定资源：适用于数据库的数据库插件、适用于文件系统的文件系统插件以及适用于VMware vSphere的VM和数据存储库SnapCenter插件。

策略

策略用于指定数据保护操作的备份频率、副本保留、复制、脚本和其他特征。

创建资源组或执行按需备份时、可以选择一个或多个策略。

资源组定义了需要保护的内容以及保护时间。策略用于说明如何执行保护。例如、如果需要备份主机的所有数据库或文件系统、则可以创建一个资源组、其中包含主机中的所有数据库或文件系统。然后、可以将两个策略附加到资源组：每日策略和每小时策略。

创建资源组并附加策略时、可以将其配置为每天执行完整备份、并为日志备份创建另一个计划、该计划为每小时执行一次。

自定义的前处理脚本和后处理脚本可用于数据保护操作。通过这些脚本、可以在执行数据保护作业之前或之后实现自动化。例如、脚本可以自动通知数据保护作业失败或出现警告。在设置脚本和后处理脚本之前、了解创建这些脚本的要求至关重要。

一致性组 (CG)

一致性组是作为单个单元进行管理的卷的集合。CG 同步以确保跨存储单元和卷的数据一致性。在ONTAP中，它们为跨多个卷的应用程序工作负载提供了轻松的管理和保护保障。详细了解["一致性组"](#)。

前处理脚本和后处理脚本的使用

自定义的前处理脚本和后处理脚本可以在作业之前或之后自动执行数据保护任务。例如、您可以添加一个脚本、用于在作业失败或出现警告时向您发出通知。在设置这些脚本之前、请确保您了解这些脚本的要求。

支持的脚本类型

Windows支持以下类型的脚本：

- 批处理文件
- PowerShell 脚本
- Perl 脚本

UNIX支持以下类型的脚本：

- Perl 脚本
- Python脚本
- Shell脚本



除了默认的bash shell之外、还支持其他shell、例如sh-shell、k-shell和c-shell。

脚本路径

在非虚拟化和虚拟化存储系统上作为SnapCenter操作的一部分运行的所有前处理脚本和后处理脚本都在插件主机上执行。

- Windows脚本应位于插件主机上。



预处理脚本或后处理脚本路径不应包含驱动器或共享。路径应与scripts_path相关。

- UNIX脚本应位于插件主机上。



脚本路径会在执行时进行验证。

指定脚本的位置

脚本在备份策略中指定。备份作业启动时、策略会自动将脚本与要备份的资源关联起来。创建备份策略时，您可以指定 prestpt 和 postScript 参数。



您不能指定多个脚本。

脚本超时

默认情况下、超时设置为60秒。您可以修改超时值。

脚本输出

Windows预处理和后处理脚本输出文件的默认目录为Windows\System32。

UNIX预处理和后处理脚本没有默认位置。您可以将输出文件重定向到任何首选位置。

SnapCenter支持的存储系统和应用程序

您应了解SnapCenter支持的存储系统、应用程序和数据库。

支持的存储系统

- NetApp ONTAP 9.12.1及更高版本
- Azure NetApp Files

- 适用于 NetApp ONTAP 的 Amazon FSX

Amazon FSx for NetApp ONTAP支持通过传输控制协议 (TCP) 实现的非易失性内存快速传输 (NVMe)。

有关适用于 NetApp ONTAP 的 Amazon FSX 的信息，请参见 "[Amazon FSX for NetApp ONTAP 文档](#)"。

- 运行NetApp ONTAP 9.16.1 及更高版本的NetApp ASA r2 系统

如果您使用的是SnapCenter Server 6.2 和SnapCenter插件 6.2，则应该使用ONTAP 9.17.1。

支持的应用程序和数据库

SnapCenter支持不同应用程序和数据库的保护。

SnapCenter支持在基于Amazon Web Services (AWS)的VMware Cloud软件定义的数据中心(SDDC)环境中保护Oracle和Microsoft SQL工作负载。<https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-Oracle-MS-SQL-workloads-using-NetApp-SnapCenter-in-VMware-Cloud-on-AWS/ba-p/449168>["了解更多信息"]^[英文]

SnapCenter凭据的身份验证方法

凭据使用不同的身份验证方法、具体取决于应用程序或环境。凭据用于对用户进行身份验证，以使用户可以执行 SnapCenter 操作。您应创建一组凭据来安装插件、而创建另一组凭据来执行数据保护操作。

Windows 身份验证

Windows 身份验证方法根据 Active Directory 进行身份验证。对于 Windows 身份验证，Active Directory 是在 SnapCenter 之外设置的。SnapCenter 无需进行额外配置即可进行身份验证。要添加主机、安装插件软件包和计划作业、您需要Windows凭据。

不可信域身份验证

SnapCenter允许属于不可信域的用户和组创建Windows凭据。要成功进行身份验证，您应向 SnapCenter 注册不可信域。

本地工作组身份验证

SnapCenter 允许使用本地工作组用户和组创建 Windows 凭据。本地工作组用户和组的Windows身份验证不会在创建Windows凭据期间进行、而是会延迟到执行主机注册和其他主机操作后再进行。

SQL Server 身份验证

SQL 身份验证方法针对 SQL Server 实例进行身份验证。这意味着必须在 SnapCenter 中发现 SQL Server 实例。因此，在添加 SQL 凭据之前，您必须添加主机，安装插件软件包并刷新资源。要执行诸如在SQL Server上计划或发现资源等操作、您需要使用SQL Server身份验证。

Linux 身份验证

Linux 身份验证方法可针对 Linux 主机进行身份验证。在从 SnapCenter 图形用户界面远程添加 Linux 主机和安装适用于 Linux 的 SnapCenter 插件软件包的初始步骤中，您需要进行 Linux 身份验证。

AIX 身份验证

AIX 身份验证方法可针对 AIX 主机进行身份验证。在从 SnapCenter 图形用户界面远程添加 AIX 主机和安装适用于 AIX 的 SnapCenter 插件软件包的初始步骤中，您需要 AIX 身份验证。

Oracle 数据库身份验证

Oracle 数据库身份验证方法可针对 Oracle 数据库进行身份验证。如果在数据库主机上禁用了操作系统（OS）身份验证，则需要使用 Oracle 数据库身份验证对 Oracle 数据库执行操作。因此、在添加Oracle数据库凭据之前、您应使用sysdba Privileges在Oracle数据库中创建一个Oracle用户。

Oracle ASM 身份验证

Oracle ASM 身份验证方法可针对 Oracle 自动存储管理（Automatic Storage Management，ASM）实例进行身份验证。如果您需要访问Oracle ASM实例、并且数据库主机上已禁用操作系统身份验证、则需要进行Oracle ASM身份验证。在添加Oracle ASM凭据之前、请在ASM实例中使用系统Privileges创建一个Oracle用户。

RMAN 目录身份验证

RMAN 目录身份验证方法根据 Oracle Recovery Manager（RMAN）目录数据库进行身份验证。如果您已配置外部目录机制并将数据库注册到目录数据库，则需要添加 RMAN 目录身份验证。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。