



# **SnapCenter** 服务文档

## SnapCenter Service

NetApp  
May 03, 2022

This PDF was generated from <https://docs.netapp.com/zh-cn/cloud-manager-snapcenter/index.html> on May 03, 2022. Always check docs.netapp.com for the latest.

# 目录

SnapCenter 服务文档 .....	1
SnapCenter 服务的新增功能 .....	2
2021 年 12 月 21 日 .....	2
2021 年 10 月 13 日 .....	2
入门 .....	3
了解 SnapCenter 服务 .....	3
入门 .....	4
创建连接器和启用 SnapCenter 服务的前提条件 .....	5
在 Azure 中为 SnapCenter 服务创建连接器 .....	9
为 Azure NetApp Files 启用 SnapCenter 服务 .....	9
安装 HDBSQL 客户端 .....	13
使用 SnapCenter 服务保护 SAP HANA 系统 .....	15
添加 SAP HANA 系统 .....	15
备份 SAP HANA 系统 .....	16
还原 SAP HANA 系统 .....	17
管理操作 .....	18
对问题进行故障排除 .....	19
知识和支持 .....	21
注册以获得支持 .....	21
获取帮助 .....	22
法律声明 .....	24
版权 .....	24
商标 .....	24
专利 .....	24
隐私政策 .....	24
开放源代码 .....	24

# SnapCenter 服务文档

# SnapCenter 服务的新增功能

了解 SnapCenter 服务的新增功能。

## 2021 年 12 月 21 日

### Apache Log4j 漏洞的修复

SnapCenter 服务 1.0.1 将 Apache Log4j 从 2.9.1 版升级到 2.17 版，以解决以下漏洞： CVE-2021-44228 ， CVE-2021-4104 和 CVE-2021-45105 。

SnapCenter 服务集群应自动更新到最新版本。您应确保 SnapCenter 服务 UI 中的版本显示集群为 1.0.1.1251 或更高版本。

## 2021 年 10 月 13 日

### 支持 SnapCenter 服务 1.0.0

- SnapCenter 服务可为在 NetApp ® 云存储上运行的应用程序提供数据保护功能。在 NetApp Cloud Manager 中启用的 SnapCenter 服务可为驻留在 Azure NetApp Files （ ANF ） 上的 SAP HANA ® 系统提供高效，应用程序一致且基于策略的备份和还原。

["了解 SnapCenter 服务"](#)

- 您应创建一个连接器，启用 SnapCenter 服务，添加 SAP HANA 系统，然后执行备份和还原操作。

["入门"](#)

# 入门

## 了解 SnapCenter 服务

SnapCenter 服务可为在 NetApp® 云存储上运行的应用程序提供数据保护功能。NetApp Cloud Manager 中启用的 SnapCenter 服务可为 Azure NetApp Files 上的 SAP HANA® 系统提供高效，应用程序一致且基于策略的备份和还原。

### 架构

SnapCenter 服务的架构包括以下组件。

- SnapCenter 服务 UI 与 Cloud Manager UI 集成在一起。

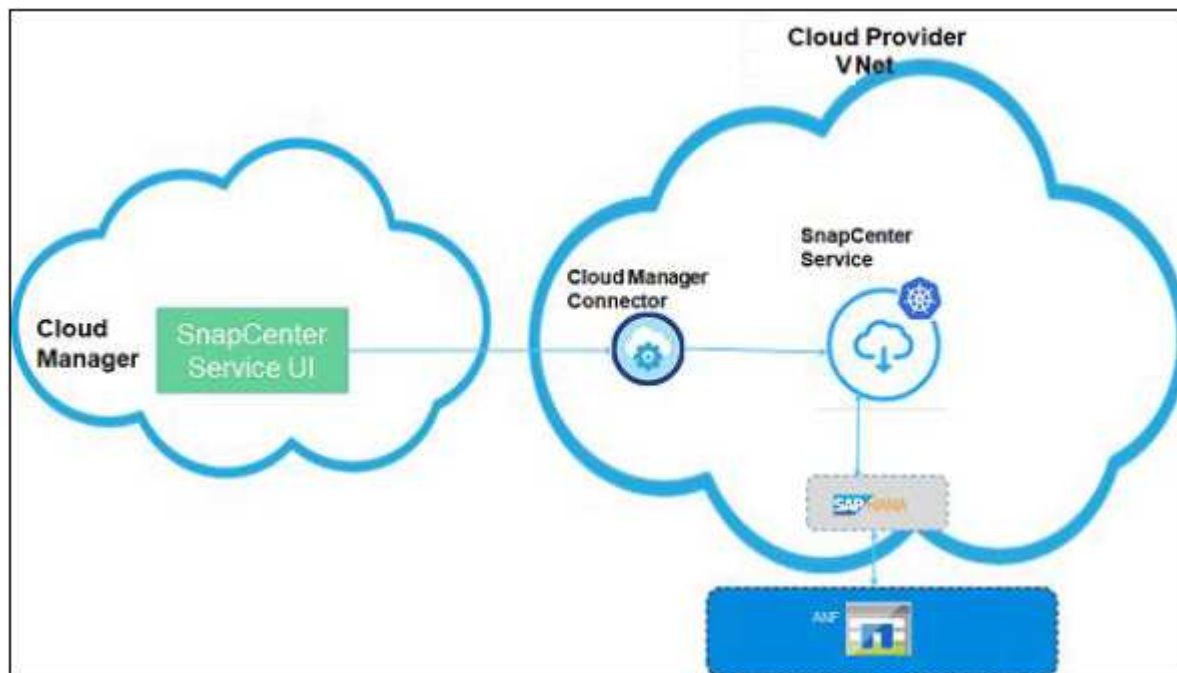
SnapCenter 服务 UI 可通过由 NetApp 管理的 Cloud Manager SaaS 框架提供，该框架可提供多种存储和数据管理功能。

- Cloud Manager Connector 是 Cloud Manager 的一个组件，用于管理 SnapCenter 服务和其他几项服务的生命周期。
- SnapCenter 服务是一组托管在 Azure Kubernetes Service （AKS）上的数据保护服务，用于编排数据保护工作流。



Cloud Manager 连接器和 SnapCenter 服务部署在您的云网络中。

下图显示了 SnapCenter 服务的每个组件之间的关系：



对于任何用户发起的请求，SnapCenter 服务 UI 都会与云管理器 SaaS 进行通信，在验证请求后，云管理器 SaaS 会将此调用转发到云管理器连接器。然后，连接器会与 SnapCenter 服务进行通信，而 SnapCenter 服务会调用 Azure NetApp Files 管理 API 和 HANA 系统命令来执行数据保护操作。

SnapCenter 服务可以部署在与 HANA 系统相同的 vNet 中，也可以部署在不同的 vNet 中。如果 SnapCenter 服务和 HANA 系统位于不同的网络上，则应在它们之间建立网络连接。

## 支持的功能

SnapCenter 服务支持以下功能。

- 添加 SAP HANA 系统
  - 备份 SAP HANA 系统
    - 既支持基于快照的备份，也支持基于文件的备份
    - 支持 SAP HANA 系统的按需备份
    - 支持使用系统定义的策略或自定义策略对 SAP HANA 系统进行计划备份
- 您可以在策略中指定不同的计划频率，例如每小时，每天，每周和每月。
- 支持备份非数据卷和全局非数据卷
  - 根据策略保留备份
  - 从用户指定的备份还原 SAP HANA 系统
  - 监控备份和其他作业
  - 管理 HANA 系统上的数据和日志备份目录
  - 在信息板上显示保护摘要，配置详细信息和作业状态
  - 通过电子邮件发送警报

## 限制

SnapCenter 服务 1.0 具有以下限制。

- 不支持国际化，您应使用英语浏览器。
  - 只有具有 " 帐户管理员 " 角色的 Cloud Manager 用户才能启用 SnapCenter 服务。
  - 与 Azure Kubernetes Service （ AKS ） 集群节点故障相关的限制
    - 在 AKS 集群中，如果其中一个节点脱机，正在运行的作业可能会失败，但后续作业将被执行。
    - 在 AKS 集群中，如果其中一个节点发生故障，您将无法添加 SAP HANA 系统，但其他操作将在没有任何问题描述的情况下运行。
- 您应启动节点以添加 HANA 系统。
- 计划程序不支持高可用性配置。

如果计划程序使用的 MySQL 节点发生故障，您应启动该节点以继续执行计划的操作。

## 入门

开始使用 SnapCenter 服务，只需几个步骤即可保护您的数据。

您应该 ["注册到 NetApp Cloud Central"](#)，["登录到 Cloud Manager"](#)，然后设置 ["NetApp 帐户"](#)。

只有帐户管理员才能部署 SnapCenter 服务。但是，帐户管理员和 SnapCenter 管理员可以执行不同的操作。 ["了解更多信息。"](#)

您应确保所有 ["前提条件"](#) 要创建连接器并启用 SnapCenter 服务，需要满足此要求。

您应该 ["在 Azure 中为 SnapCenter 服务创建连接器"](#)。

如果您的连接器满足所有前提条件，则可以使用该连接器。

在 Cloud Manager 中创建 Azure NetApp Files 工作环境，以创建和管理 NetApp 帐户，容量池，卷和快照。 ["了解更多信息。"](#)

您应该 ["启用 SnapCenter 服务"](#) 使用 Cloud Manager UI。启用 SnapCenter 服务后，将创建托管 SnapCenter 服务的 Azure Kubernetes Service （AKS）集群。

您应该 ["安装 HDBSQL 客户端"](#) 对 SAP HANA 数据库执行数据保护操作。HDBSQL 客户端用于与 SAP HANA 系统进行通信。

您应手动执行此操作 ["添加 SAP HANA 系统"](#)。

然后，您可以 ["备份 SAP HANA 系统"](#) 使用系统定义的策略或自定义策略。如果发生数据丢失，您可以 ["还原 SAP HANA 系统"](#) 使用该系统的备份。

## 创建连接器和启用 SnapCenter 服务的前提条件

在 Azure 中创建连接器并启用 SnapCenter 服务之前，您应确保满足某些要求。

- 确保为 Connector 选择的子网不应与为 Azure Kubernetes Service （AKS）预留的以下 IP 地址范围重叠：169.254.0.0/16 ， 172.30.0.0/16 ， 172.31.0.0/16 和 192.0.2.0/24 。
- 确保选定子网中未运行任何 AKS 。
- 确保所选子网可以通过相应的端口访问 SAP HANA 系统。
- 如果所选子网的 vNet 与 SAP HANA 系统的 vNet 不同，请确保 VNets 可以通过 VPN 网关，对等或其他方式彼此通信。
- 如果要在防火墙后启用 SnapCenter 服务，应执行中所述的操作 [\[Network requirements\]](#)。

您应事先确定是否要在防火墙后启用 SnapCenter 服务。启用 SnapCenter 服务后，您无法将其配置为在防火墙后运行。这是一个 AKS 限制。

### 网络要求

设置您的网络，以便 Connector 可以管理云环境中的资源和流程。

#### 防火墙配置

如果要在防火墙后启用 SnapCenter 服务，应执行以下操作。



如果您使用的是 Azure 防火墙，则可以使用脚本执行这些步骤。有关信息，请参见 [\[Azure Firewall configuration\]](#)。

• 步骤 \*

1. 将以下网络规则添加到防火墙。

目标端点	协议	Port	注释
"服务标签" — AzureCloud 。 < 地区 > : 1194	UDP	1194.	如果您计划使用专用连接器和专用 SnapCenter 服务集群，则不需要此功能。
"服务标签" — AzureCloud 。 < 地区 > : 9000	TCP	9000	如果您计划使用专用连接器和专用 SnapCenter 服务集群，则不需要此功能。
FQDN — ntp.ubuntu.com:123	UDP	123.	Azure 虚拟机中的时间同步需要此功能。
"服务标签" — AzureCloud 。 < 地区 > : 443	TCP	443.	如果您计划使用专用连接器和专用 SnapCenter 服务集群，则不需要此功能。

2. 在防火墙中添加具有以下 FQDN 标记和端口详细信息的应用程序规则：

- FQDN 标记— AzureKubernetes Service
- HTTPS : 443

3. 添加一个应用程序规则，将以下端点作为目标 FQDN ，并将协议和端口设置为 HTTPS : 443 。

端点	目的
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	支持 Cloud Manager 在大多数 Azure 区域部署和管理 Cloud Volumes ONTAP 。
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	支持 Cloud Manager 在 Azure Germany 地区部署和管理 Cloud Volumes ONTAP 。
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	支持 Cloud Manager 在 Azure US Gov 区域部署和管理 Cloud Volumes ONTAP 。
<a href="https://api.services.cloud.netpp.com">https://api.services.cloud.netpp.com</a>	允许向 NetApp Cloud Central 发出 API 请求。
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	提供对软件映像、清单和模板的访问。
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	使 Connector 能够访问和下载清单，模板和 Cloud Volumes ONTAP 升级映像。



端点	目的
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	访问运行 Docker 的基础架构中容器组件的软件映像，并提供解决方案以实现与 Cloud Manager 的服务集成。
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	使 NetApp 能够从审计记录流化数据。
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	与 Cloud Manager 服务进行通信，其中包括 NetApp 帐户。
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	与 NetApp Cloud Central 进行通信以实现集中式用户身份验证。
<a href="https://support.netapp.com">https://support.netapp.com</a>	与 NetApp AutoSupport 通信。
<a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	与 NetApp 沟通以获得系统许可和支持注册。
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a>	使 NetApp 能够收集对支持问题进行故障排除所需的信息。
* .blob.core.windows.net	使用代理时，HA 对需要此参数。
<a href="https://auth0.com">https://auth0.com</a>	Auth0 身份验证必需。
<a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://production.cloudflare.docker.com">https://production.cloudflare.docker.com</a>	检索 SnapCenter 服务 workflow 引擎的依赖关系。
<a href="https://exeranl-log.cloudmanager.netapp.com">https://exeranl-log.cloudmanager.netapp.com</a>	允许通信将日志传输到 Cloud Manager 日志存储库。


4. 选择要安装 SnapCenter 服务的子网。
5. 使用路由创建路由表：
  - 将流量从子网转发到防火墙内部 IP 地址
  - 将流量从防火墙公有 IP 地址转发到 Internet。
6. 将路由表附加到子网。

有关 Cloud Manager Connector 的网络要求的信息，请参见 "[连接器的网络连接要求](#)"。

## Azure 防火墙配置

如果要在 Azure 防火墙后启用 SnapCenter 服务，应执行以下操作。

- 您需要的内容 \*
- 您应已创建防火墙（经典模式）。
- 您应已为 SnapCenter 服务创建 vNet 和子网。
- 如果您的防火墙资源和 SnapCenter 服务的 vNet 位于不同的租户中，则应登录到 Azure Shell 中的两个租户。
- 如果您的防火墙 vNet 和 SnapCenter vNet 不同，则应在 VNet 之间建立对等关系。
- 步骤 \*

1. 下载 "[scs\\_azure\\_firewall\\_config.sh](#)" 脚本到本地系统。
2. 登录到 "[Microsoft Azure 门户](#)"。
3. 

单击  打开云 Shell 并选择 Bash 控制台。

- 将脚本上传到 Azure Cloud Shell。
- 分配运行脚本的权限。

```
chmod +x ./SCS azure firewall config.sh
```

- c. 运行脚本。

```
. /scs_azure_firewall_config.sh -fwsubid <Firewall_SubscriptionID> -fwname <Firewall_name>  
-fwrg <Firewall_Resource_group> -scssubid <SnapCenter_Service_SubscriptionID> -scsvnet  
<SnapCenter_Service_vNet_name> -scssubnet <SnapCenter_Service_Subnet_Net_Group>  
-SnapSC_Service_SVM_SVM_SVM_SVM_SVM_SVM_SVM_SVM_SVM_SVM_SVM_SVM_SVM_SVM_SVM_SVM.  
SVM.<SnapCenter> -SC Service SVM`
```



如果尚未创建资源组，则此脚本将创建该资源组。创建连接器时，您可以使用同一资源组，以便所有与 SnapCenter 服务相关的资源都位于同一资源组中。

- 结果 \*
- 已配置防火墙规则。
- 此时将为 SnapCenter 服务创建一个资源组。
- 此时将在 SnapCenter 服务资源组中创建路由表。
- 此时将配置路由表规则。
- 路由表已连接到子网。

连接到 HANA 系统

SnapCenter 服务集群需要使用 HDBSQL 命令与用户网络中的 HANA 系统进行通信。需要允许使用各种网络架构在 SnapCenter 集群和 HANA 系统之间建立通信通道，例如：

- 连接器和 SnapCenter 服务集群部署在与 HANA 系统相同的 vNet 中
- 连接器和 SnapCenter 服务集群部署在与 HANA 系统不同的 vNet 中，并使用 vNet 对等在 2 个 vNet 之间建立通信。
- 连接器和 SnapCenter 服务集群部署在与 HANA 系统不同的 vNet 中，并使用 VPN 网关在 2 个 vNet 之间建立通信。

## 安全组配置

如果在 HANA 系统中配置了网络安全组（Network Security Group，NSG），则应允许从 SnapCenter 服务的端口到 HANA 系统的端口进行入站通信，如用户存储密钥中所指定。

- 协议：所有 TCP
- 子网： SnapCenter AKS 集群子网

- 用途：执行 HDBSQL 命令

SnapCenter AKS 集群中运行的 HANA 服务支持与启用了 SSL 的 HANA 系统进行 SSL 通信。

## 在 Azure 中为 SnapCenter 服务创建连接器

客户管理员应先部署 Connector，然后才能使用 Cloud Manager 功能。借助此连接器，Cloud Manager 可以管理公有云环境中的资源和流程。

默认情况下，您可以从 Azure Marketplace 在 Azure 中创建 Connector。执行步骤至时 ["从 Azure Marketplace 创建连接器"](#)，您应记住以下几点：

- 无论在何处指定适用于 Cloud Volumes ONTAP 的 Cloud Manager，SnapCenter 服务都可以使用这种方式。
- 对于 Cloud Manager Name，请指定您的 Connector VM 名称以更好地进行标识。此名称将在 Cloud Manager UI 中显示为连接器名称。
- 如果您在未配置公有 IP 的情况下配置了连接器或配置了防火墙，则应使用跳转主机连接到连接器计算机。

如果您有 ["用户同意"](#) 在 Azure Active Directory 中启用，或者如果租户管理员可以提供同意，您可以从 Cloud Manager UI 创建 Connector。

### 已启用用户同意

如果在 Azure Active Directory 中启用了用户同意，["从 Cloud Manager 创建 Connector"](#)。

### 已禁用用户同意

#### 1. 执行以下操作之一：

- 如果在 Active Directory 中配置了管理员同意工作流，则应执行此操作 ["请求管理员同意"](#)。
- 如果未配置管理员同意工作流，您应：
  - i. ["构建用于授予租户范围管理员同意的 URL"](#)。



将客户端 ID 指定为 `989efff4-9a9e-46fa-9f17-de39e15714f9`。这是在 Cloud Manager 向导中命名的 Cloud Manager Azure 应用程序 ID。

- ii. 请租户管理员在浏览器中运行此 URL，并征得其同意。

管理员可以忽略显示的错误

#### 2. ["从 Cloud Manager 创建 Connector"](#)。



要连接到计算机，需要用户名和密码或在创建 Connector 时提供的密钥

## 为 Azure NetApp Files 启用 SnapCenter 服务

您可以使用 SnapCenter 管理器 UI 启用 Cloud 服务。启用 SnapCenter 服务后，将创建托

## 管 SnapCenter 服务的 Azure Kubernetes Service (AKS) 集群。

- 您需要的内容 \*
- 您应在 Azure 订阅中注册 "microsoft.ContainerService" 资源提供程序。有关信息，请参见 ["如何注册资源提供程序"](#)。
- 您应确保所有 ["前提条件"](#) 已满足。
- 关于此任务 \*

AKS 集群将在创建 Connector 时选择的同一资源组和子网中创建。如果在创建连接器时未使用公有 IP 地址，则会在专用模式下创建 AKS 集群。

要创建和管理 AKS 集群，需要为用户分配具有必要权限的托管身份。此时将创建分配给用户的托管身份，并应将其分配给 Connector VM。

- 步骤 \*
- 1. Log in to Cloud Manager.
- 2. 选择在 Cloud Manager 中创建的 Connector。

确保 Connector 与要保护的 SAP HANA 系统建立了网络连接。

3. 单击 \* 所有服务 \* > \* SnapCenter \* > \* 启用 \*。
4. 执行以下操作之一：
  - 如果您已从 Cloud Manager UI 创建连接器，并且您有权创建和分配角色，则 SnapCenter 服务安装会自动创建分配给用户的托管身份。
    - i. 选择 \* 使用 Azure 登录 \*。
    - ii. 在 Get Ready 页面上，单击 \* 继续 \*。
    - iii. 指定 Azure 凭据。



您应确保 Azure 登录帐户具有足够的权限。有关权限以及如何分配权限的信息，请参见 [\[Permissions required for Azure login account\]](#)。

- 如果您已从 Azure Marketplace 创建 Connector，或者您无权创建和分配角色，请按照以下步骤创建用户分配的托管身份。
  - i. 选择 \* 使用 Azure 命令行界面脚本 \*。
  - ii. 如果您对 Azure 帐户没有足够的权限，请联系您的管理员。

有关权限以及如何分配权限的信息，请参见 [\[Permissions required for Azure login account\]](#)。

- iii. 下载 ["prerequisite\\_azure.sh"](#) 脚本到本地系统。
- iv. 登录到 ["Microsoft Azure 门户"](#)。
- v.  单击 打开云 Shell 并选择 Bash 控制台。
- vi. 将脚本上传到 Azure Cloud Shell。
- vii. 分配运行脚本的权限。

```
chmod +x ./prerequisite_azure.sh
```

viii. 运行脚本。

```
`。 /prerequisite_azure.sh -s <subscription_ID> -g <connector_resourcegroup_name> -c  
<connector_vm_name>`
```

5. 在集群配置页面上，执行以下操作：

a. 选择集群配置。

- 如果选择 \* 高可用性 \*，则会在可用区域中创建一个包含 3 个工作节点的 Azure Kubernetes Service (AKS) 集群。
- 如果选择 \* 单节点 \*，则会创建一个具有单节点的 AKS 集群。

b. 指定 Kubernetes Pod 地址范围。

确保 Kubernetes Pod 地址范围不会与所连接的虚拟网络，对等虚拟网络和内部网络的 IP 范围重叠。此外，此范围不应与服务地址范围和 Docker 网桥地址重叠。

c. 指定 Kubernetes Service 地址。

确保 Kubernetes 服务地址范围不会与所连接的虚拟网络，对等虚拟网络和内部网络的 IP 范围重叠。此外，此范围不应与 Pod 地址范围和 Docker 网桥地址重叠。

d. 指定 Docker 网桥网络。

确保 Docker 网桥地址不会与所连接的虚拟网络，对等虚拟网络和内部网络的 IP 范围重叠。此外，此范围不应与 Pod 地址范围和服务地址范围重叠。

e. 如果在创建连接器时不使用公有 IP，并且您正在 vNet 上使用自定义 DNS 服务器，请选择 \* 支持自定义 DNS 服务器 \*。



您应在专用 DNS 区域中为托管自定义 DNS 服务器的 VN 创建虚拟网络链接。专用 DNS 区域名称和资源组名称将显示在用户界面上。

6. 在 Review 页面上，查看详细信息并单击 \* 启用 \*。

7. 成功启用 SnapCenter 服务后，单击 \* 完成 \*。

• 结果 \*

•

成功启用 SnapCenter 服务后，将创建 AKS 集群。您可以单击来查看 AKS 集群详细信息 。



如果无法启用 SnapCenter 服务，则可以修复此问题描述并单击 \* 重试 \*。

• 创建分配给用户的托管身份后，该身份将分配给自定义角色。

◦ 分配给用户的托管身份将分配给在 Connector 资源组范围内具有以下权限的自定义角色：

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.ContainerService/managedClusters/read",
"Microsoft.ContainerService/managedClusters/write",
"Microsoft.ContainerService/managedClusters/delete",
"Microsoft.ContainerService/managedClusters/listClusterUserCredential
/action",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Network/networkInterfaces/read"
```

- 分配给用户的托管身份将分配给在 Connector 的 vNet 范围内具有以下权限的自定义角色：

```
"Microsoft.Authorization/roleAssignments/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/join/action"
```

- 如果在子网上配置路由表以路由到防火墙，则分配给用户的托管身份将分配给路由表范围内具有以下权限的自定义角色。

```
"Microsoft.Network/routeTables/*",
"Microsoft.Network/networkInterfaces/effectiveRouteTable/action",
"Microsoft.Network/networkWatchers/nextHop/action"
```

- 如果安装的 Connector 不使用公有 IP，则分配给用户的托管身份将分配给专用 DNS 区域范围内具有以下权限的自定义角色。

```
"Microsoft.Network/privateDnsZones/*"
```

## Azure 登录帐户所需的权限

Azure 登录帐户用于创建分配给用户的托管身份，所需角色以及将此身份分配给 Connector VM。



登录帐户的凭据不会存储在 SnapCenter 服务的任何位置，也不会用于调用 API。这些凭据仅在 UI 中使用。

### • 步骤 \*

1. 使用创建自定义角色 "[SnapCenter\\_Deployment\\_Role1.json](#)" 文件

您应将 SnapCenter\_Deployment\_Role1.json 文件中的 <subscription\_ID> 替换为 Azure 订阅 ID。

2. 将角色分配给 Connector 资源组范围内的登录帐户。
3. 使用创建自定义角色 "[SnapCenter\\_Deployment\\_Rol2.json](#)" 文件

您应将 SnapCenter\_Deployment\_Rol2.json 文件中的 <subscription\_ID> 替换为 Azure 订阅 ID 。

4. 在 Connector 的 vNet 或更高版本范围内将角色分配给登录帐户。
5. 如果您有 "已配置防火墙"，使用创建自定义角色 "[SnapCenter-Deployment-Role3.json](#)" 文件

您应将 SnapCenter\_Deployment\_Role3.json 文件中的 <subscription\_ID> 替换为 Azure 订阅 ID 。

6. 在连接到 SnapCenter 子网的路由表范围内，将角色分配给登录帐户。

## 安装 HDBSQL 客户端

启用 SnapCenter 服务后，安装 HDBSQL 客户端以对 SAP HANA 数据库执行数据保护操作。HDBSQL 客户端用于与 SAP HANA 系统进行通信。

### • 步骤 \*

1. 从 SAP 帐户下载 HDB 客户端软件。

它是扩展名为 ( .sar ) 的归档文件。示例：IMDb\_CLIENT20\_008\_20-80002082.sar



HDB 客户端软件版本应为 2.4.202.1590784230 或更高版本。

2. 从 SAP 帐户下载最新的 SAPCAR 实用程序。示例：SAPCAR\_1010-70006178.EXC
3. 在 Cloud Manager 用户界面上，单击 \* 连接器 \* 以获取连接器名称。
4. 登录到 "[Microsoft Azure 门户](#)"。
5. 单击 \* 虚拟机 \*。
6. 搜索 Cloud Manager 连接器并复制分配给该连接器的公有 IP 地址。

如果此连接器未启用公有 IP ，则应使用跳转主机。

7. 将 SAPCAR 实用程序和 HDB 客户端归档 ( .sar ) 文件复制到 Connector 计算机。

要将文件复制到连接器路径，您需要凭据或在创建连接器时提供的密钥。

- scp <SAPCAR\_utility> <username>@ <IP\_address> : /home/<username>
- scp <HDB\_Client\_archive> < 用户名 >@ <IP\_address> : /home/< 用户名 >

此文件将复制到 //home/< 用户名 >\_。

8. 使用 ssh 凭据或密钥登录到 Connector VM 。
9. 在 Connector VM 中运行以下命令，以便在 AKS 中安装 HDBSQL 客户端。

- a. sudo cp /home/<username>/<sacpar\_utility>  
/var/lib/docker/volumes/cloudmanager\_snapcenter\_volume/\_data/

- b. `sUdo cp /home/< 用户名 >/< HDB_Client_archive>  
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/`
- c. `sUdo Docker exec -it cloudmanager_snapcenter /bin/bash  
/opt/netapp/hdbclient/hdbclient.sh -archivefile <HDB_Client_archive>  
-archiveutil <SAPCAR_utility>`

- [查找更多信息](#) \*

["如何使用 SCP 移动文件"](#)



# 使用 SnapCenter 服务保护 SAP HANA 系统

## 添加 SAP HANA 系统

手动添加 SAP HANA 系统。不支持自动发现 SAP HANA 系统。

添加 SAP HANA 系统时，您应添加 HDB 用户存储密钥。HDB 安全用户存储密钥用于将 SAP HANA 系统的连接信息安全地存储在客户端上，而 HDBSQL 客户端使用安全用户存储密钥连接到 SAP HANA 系统。



如果 AKS 集群中的某个节点已关闭，则无法添加或修改 SAP HANA 系统。

### • 步骤 \*

1. 在 SnapCenter 服务页面上，单击 \* SAP HANA 系统 \* > \* 添加 \*。
2. 在 System Details 页面上，执行以下操作：
  - a. 选择系统类型：
  - b. 指定 SAP HANA 系统的 SID。
  - c. 指定 SAP HANA 系统名称。
  - d. 单击 HDB 安全用户存储密钥文本框以添加用户存储密钥详细信息。

指定密钥名称，系统详细信息，用户名和密码。

- e. 单击 \* 添加 \*。



如果要添加多主机 SAP HANA 系统，则应为每个主机添加用户存储密钥。

3. 单击 \* 继续 \*。
4. 在存储占用空间页面上，执行以下操作：
  - a. 选择工作环境并指定 NetApp 帐户。
  - b. 选择所需的卷。
  - c. 单击 \* 添加存储 \*。
5. 单击 \* 继续 \*。
6. 查看所有详细信息，然后单击 \* 添加 \*。

您还可以编辑或删除已添加到 SnapCenter 服务的 SAP HANA 系统。删除 SAP HANA 系统后，所有关联的备份和目录条目都将被删除，并且不再受到保护。

## 添加非数据卷

添加多租户数据库容器或单个容器类型 SAP HANA 系统后，您可以添加 HANA 系统的非数据卷。

### • 步骤 \*

1. 在 SnapCenter 服务页面上，单击 SAP HANA 系统。

此时将显示添加到 SnapCenter 服务的所有系统。

2. 单击 ... 对应于要添加非数据卷的多租户数据库容器或单个容器类型系统。
3. 单击 \* 添加非数据卷 \*。
4. 单击 \* 添加新存储 \*。

## 备份 SAP HANA 系统

您可以使用系统定义或自定义策略对 SAP HANA 系统执行按需备份或计划备份。SnapCenter 服务既支持基于快照的备份，也支持基于文件的备份。

### 创建备份策略

策略用于指定备份类型，备份频率，计划，保留类型，保留数量，以及数据保护操作的其他特征。您可以使用 Cloud Manager UI 创建策略。

默认情况下，可以使用两个系统定义的策略，分别用于基于快照的备份操作和基于文件的备份操作。

- 步骤 \*

1. 在 SnapCenter 服务页面上，单击 \* 策略 \* > \* 添加 \*。
2. 在创建备份策略页面上，执行以下操作：
  - a. 指定策略名称。
  - b. 选择要使用此策略创建的备份类型。
  - c. 指定备份名称。

默认情况下会添加后缀时间戳。您可以选择备份名称中应包含的其他后缀，并定义后缀的显示顺序。

- d. 指定计划备份的计划频率以及开始和结束时间。
  - e. 指定要保留的快照副本数或指定应保留快照副本的天数。
3. 单击 \* 添加 \*。

您可以通过单击来查看，编辑或删除策略 ... 与策略对应。

### 创建按需备份

通过关联策略或不关联任何策略来创建 SAP HANA 系统的按需备份。

- 步骤 \*

1. 在 SnapCenter 服务页面上，单击 \* SAP HANA 系统 \*。

此时将显示添加到 SnapCenter 服务的所有系统。

2. 单击 ... 对应于要保护的系统。
3. 单击 \* 按需备份 \*。

4. 在按需备份页面上，执行以下操作之一：

- 如果要将备份与策略关联，请选择该策略并单击 \* 创建备份 \*。
- 如果不希望将备份与策略关联，请执行以下操作：
  - i. 在策略字段中，选择 \* 无 \*。
  - ii. 选择备份类型。

如果要备份非数据卷，则只能选择 \* 基于 Snapshot \* 作为备份类型。

- iii. 指定保留期限。
- iv. 单击 \* 创建备份 \*。

## 创建计划备份

通过将策略与 SAP HANA 系统关联来创建计划备份。

### • 步骤 \*

1. 在 SnapCenter 服务页面上，单击 \* SAP HANA 系统 \*。

此时将显示添加到 SnapCenter 服务的所有系统。

2. 单击 ... 对应于要保护的系统。
3. 单击 \* 保护 \*。
4. 选择要用于保护 SAP HANA 系统的策略。
5. 单击 \* 保护 \*。

- 查找更多信息 \*<https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-backup-anf-overview.html>["使用 SnapCenter 服务在 Azure NetApp Files 上执行 SAP HANA 备份和恢复"]

## 还原 SAP HANA 系统

如果数据丢失，请从该系统的备份之一还原 SAP HANA 系统。

仅支持存储还原。在还原之前，应使用 SAP HANA Studio 或 SAP HANA Cockpit 将 HANA 系统置于恢复模式，因为不支持 HANA 系统恢复。

### • 步骤 \*

1. 在 SnapCenter 服务页面上，单击 \* SAP HANA 系统 \*。

此时将显示添加到 SnapCenter 服务的系统。

2. 单击 ... 与要还原的系统对应。
3. 单击 \* 查看备份 \*。
4. 在备份部分中，单击 ... 对应于要用于还原系统的备份。
5. 单击 \* 还原 \*。

6. 查看此消息并选择 \* 是, 还原 \* 进行确认。



还原数据库后, 如果您使用 HANA Studio 对 SAP HANA 系统执行时间点恢复, 则可能会还原 SnapCenter 服务根据保留设置删除的数据备份目录条目。如果由于恢复操作而还原了已删除的数据备份目录条目, 则 SnapCenter 服务将无法检测和删除这些条目。这可能会导致 SnapCenter 服务无法正确清理日志目录。您可以验证 SnapCenter 服务中的备份条目, 以确定哪些所有数据备份目录条目是新还原的, 并手动删除这些条目。

- 查找更多信息 \*<https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-backup-anf-overview.html>使用 SnapCenter 服务在 Azure NetApp Files 上执行 SAP HANA 备份和恢复"^]

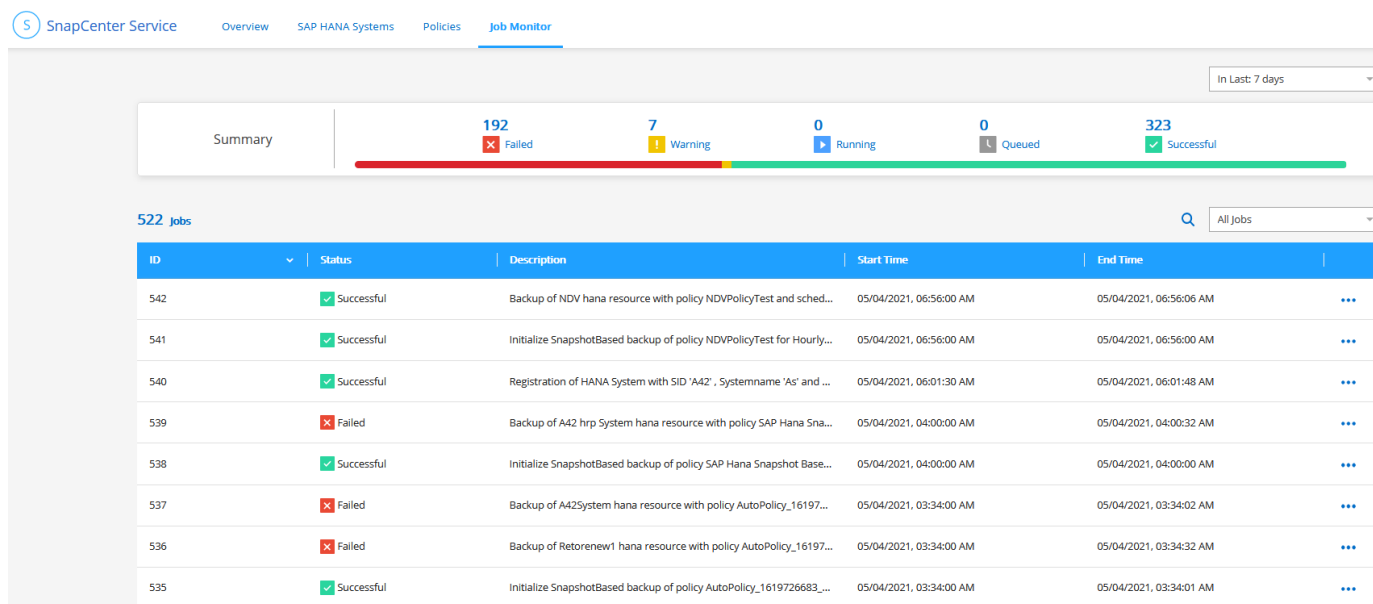
## 管理操作

您可以监控已执行作业的状态, 接收电子邮件通知以及查看信息板。

### 监控作业

单击 SnapCenter 服务页面上的 \* 作业监控 \* 以查看作业状态。作业监控页面将显示整体摘要并列出所有作业。

然后, 您可以单击 ... 对应于特定作业以查看详细信息。

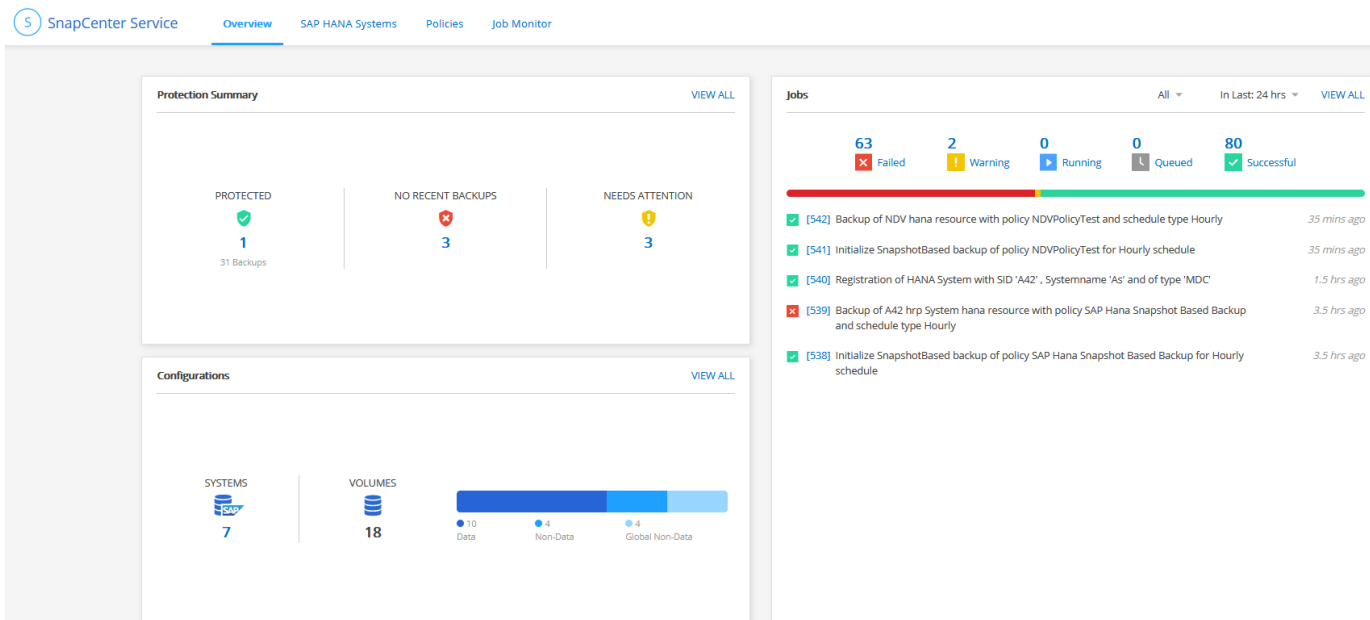


### 电子邮件通知

默认情况下, 对于失败的按需备份, 计划的备份和还原操作, 系统会发送电子邮件通知。只有具有 " 帐户管理员 " 角色的 Cloud Manager 用户才会收到此电子邮件。

### 查看信息板

单击 SnapCenter 服务页面上的 \* 概述 \* 以查看保护摘要, 配置详细信息和作业状态。



## 对问题进行故障排除

### 问题描述： Redis Pod 卡在 CrashLoopBackOff 状态

在高可用性配置中，如果问题描述集群的所有节点均已关闭，则 集群不会恢复工作状态。重新启动所有节点时，您可能会发现所有 Redis Pod 均处于 CrashLoopBackOff 状态。

- 解决方案 \* 您应运行以下命令来还原系统。

1. 登录到 Connector 。

2. 删除所有 Redis Pod 。

```
▪ docker exec -it cloudmanager_snapcenter - sh
```

```
▪ kubectl scale -replicas=0 STS sc-V 依赖关系 -Redis-node -n SnapCenter
```

3. 验证是否已删除所有 Redis Pod 。 kubectl get Pod -n SnapCenter

4. 如果未删除 Redis Pod ，请运行以下命令：

```
▪ kubectl delete pod sc-V 依赖关系 -Redis-node-0 -n SnapCenter
```

```
▪ kubectl delete pod sc-V 依赖关系 -Redis-node-1 -n SnapCenter
```

```
▪ kubectl delete pod sc-V 依赖关系 -Redis-node-2 -n SnapCenter
```

5. 删除所有 Redis Pod 后，运行： kubectl scale -replicas=3 STS SC-B依赖 关系 -Redis -node -n SnapCenter

6. 验证所有已删除的 Pod 是否均已启动且正在运行。 Kubectl get Pod -n SnapCenter

### 问题描述：重新启动集群节点后，作业失败

在高可用性配置中，如果问题描述集群的所有节点均已关闭，则 集群不会恢复工作状态。重新启动所有节点时，您可能会看到作业失败，粒度任务变为灰色或超时。

- 解决方案 \* 您应运行以下命令：

1. 登录到 Connector。
2. 保存 RabbitMQ 状态集（STS）部署。
  - `docker exec -it cloudmanager_snapcenter - sh`
  - `kubectl get STS rabbitmq -o YAML -n SnapCenter > rabbitmq_STS.YAML`
3. 确定连接到 RabbitMQ Pod 的永久性卷（PV）。`kubectl get PV grep rabbitmq`
4. 删除附加到 RabbitMQ Pod 的永久性卷声明（Persistent Volume Claim，PVC）。`kubectl get pvc -n SnapCenter pvc grep rabbitmq hk {'print $1'} | xargs kubectl delete pc -n SnapCenter`
5. 删除先前在步骤 3 中确定的每个 PV。`kubectl delete pv "PVname"`
6. 创建 RabbitMQ STS。`kubectl create -f rabbitmq_STS.YAML -n SnapCenter`

## 问题描述：创建租户数据库期间，备份操作失败

- 问题描述创建租户数据库时，如果启动按需备份或计划备份，备份操作将失败。

创建租户数据库是对解决方案 HANA 系统执行的维护操作。

在创建租户数据库之前，应使用 SnapCenter 服务将 SAP HANA 系统置于维护模式。将 SAP HANA 系统置于维护模式后，无法启动任何操作。

创建租户数据库后，您应将 SAP HANA 系统恢复为生产模式。

# 知识和支持

## 注册以获得支持

在向 NetApp 技术支持创建支持案例之前，您需要先将 NetApp 支持站点帐户添加到 Cloud Manager 中，然后注册获取支持。

### 添加 NSS 帐户

通过支持信息板，您可以从一个位置添加和管理所有 NetApp 支持站点帐户。

#### 步骤

1. 如果您还没有 NetApp 支持站点帐户，["注册一个"](#)。
2. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。



3. 单击 \* NSS 管理 > 添加 NSS 帐户 \*。
4. 出现提示时，单击 \* 继续 \* 以重定向到 Microsoft 登录页面。

NetApp 使用 Microsoft Azure Active Directory 作为身份提供程序来提供特定于支持和许可的身份验证服务。

5. 在登录页面上，提供 NetApp 支持站点注册的电子邮件地址和密码以执行身份验证过程。

此操作可使 Cloud Manager 使用您的 NSS 帐户。

请注意，此帐户必须是客户级别的帐户（而不是来宾或临时帐户）。

### 注册您的帐户以获得支持

支持注册可从 Cloud Manager 的支持信息板中获取。

#### 步骤

1. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。



2. 在 \* 资源 \* 选项卡中，单击 \* 注册支持 \*。
3. 选择要注册的 NSS 凭据，然后单击 \* 注册 \*。

## 获取帮助

NetApp 通过多种方式为 Cloud Manager 及其云服务提供支持。全天候提供丰富的免费自助支持选项，例如知识库（KB）文章和社区论坛。您的支持注册包括通过 Web 服务单提供的远程技术支持。

### 自助支持

这些选项每周 7 天，每天 24 小时免费提供：

- ["知识库"](#)

通过 Cloud Manager 知识库搜索，查找有助于解决问题的文章。

- ["社区"](#)

加入 Cloud Manager 社区，关注正在进行的讨论或创建新的讨论。

- 文档。

您当前正在查看的 Cloud Manager 文档。

- [mailto: ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com)（反馈电子邮件）

我们非常重视您的反馈意见。提交反馈以帮助我们改进 Cloud Manager。

### NetApp 支持

除了上述自助支持选项之外，您还可以在激活支持后与 NetApp 支持工程师合作解决任何问题。



## 步骤

1. 在 Cloud Manager 中，单击 \* 帮助 > 支持 \*。
2. 在 "Technical Support" 下选择一个可用选项：
  - a. 单击 \* 致电我们 \* 可查找 NetApp 技术支持的电话号码。
  - b. 单击 \* 打开问题描述 \*，选择一个选项，然后单击 \* 发送 \*。

NetApp 代表将审核您的案例，并尽快与您联系。

# 法律声明

法律声明提供对版权声明、商标、专利等的访问。

## 版权

<http://www.netapp.com/us/legal/copyright.aspx>

## 商标

NetApp、NetApp 徽标和 NetApp 商标页面上列出的标记是 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。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## 专利

有关 NetApp 拥有的专利的最新列表，请访问：

<https://www.netapp.com/us/media/patents-page.pdf>

## 隐私政策

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## 开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

- "有关 Cloud Manager 3.9 的注意事项"

## Copyright Information

Copyright © 2022 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.