NetBackup™ for Nutanix AHV 管理指南

版本 11.0

VERITAS
now part of Cohesity

上次更新时间： 2026-01-21

法律声明

Cohesity, Inc.
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

技术支持

技术支持具有全球性支持中心。所有支持服务将会根据您的支持协议以及当时最新的企业技术支持政策进行交付。有关支持产品和服务以及如何联系技术支持的信息，请访问我们的网站：

https://www.veritas.com/support

您可以在下列 URL 上管理 Cohesity 帐户信息：

https://my.veritas.com

如果您对现有支持协议有疑问，请通过以下方式联系您所在地区的支持协议管理部门：

全球（日本除外）	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

文档

请确保您的文档是最新版本。每个文档都在第 2 页上显示上次更新日期。最新的文档可在 Cohesity 网站上找到。

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity Services and Operations Readiness Tools (SORT) 是一个网站，提供的信息和工具有助于自动处理及简化某些耗时的管理任务。根据具体产品，SORT 会帮助您准备安装和升级、识别您数据中心的风险并提高操作效率。要了解 SORT 为您的产品提供了哪些服务和工具，请参见数据表：

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目录

1

概述

本章节包括下列主题：

在 NetBackup Web UI 中配置和保护 AHV 资产的概述

表 1-1 配置和保护 AHV 资产的步骤

步骤	操作	描述
步骤 1	以默认安全管理员身份登录 NetBackup Web UI。然后将 AHV 用户添加到“**默认 AHV 管理员**”角色。或者，创建自定义 RBAC 角色以适配 AHV 管理员所需的权限。	**注意：**要执行 AHV 管理员任务，“**默认 AHV 管理员**”角色需要具有所需的最低权限。还可以创建自定义角色，为 AHV 管理员提供不同的访问权限。

步骤	操作	描述
步骤 2	为 AHV 群集配置以下项： ■ 在 AHV 群集和 NetBackup 主机之间配置安全通信。 ■ （可选）在 Nutanix Prism Central 和 NetBackup 主机之间配置安全通信。 ■ 在要用作备份或还原主机的 NetBackup 主机上启用 iSCSI。 ■ 在 Nutanix Prism 控制台中，将备份主机添加到允许列表。 **注意：**要在 Linux 备份或恢复主机上使用 NFS 协议，该主机需要在 Nutanix AHV Prism 控制台上的 NFS 允许列表中。有关详细信息，请单击此处。	请参见第 18 页的“在 AHV 群集和 NetBackup 主机之间以及 Nutanix Prism Central 和 NetBackup 主机之间配置安全通信”。 请参见第 20 页的“在 Linux 备份主机上安装 iSCSI 发起程序软件包”。 请参见第 20 页的“在 Windows 备份主机上启用 iSCSI 发起程序服务”。
步骤 3（可选）	配置和管理 Nutanix Prism Central。	请参见第 28 页的“添加新的 Nutanix Prism Central”。
步骤 4	配置和管理 AHV 群集。	请参见第 21 页的“配置 Nutanix AHV 群集的前提条件”。
步骤 5	添加和管理凭据。	请参见第 45 页的“添加新群集凭据”。
步骤 6	配置 AHV 保护计划。	请参见《NetBackup™ Web UI 管理指南》。
步骤 7	配置智能 VM 组。	请参见第 31 页的“创建智能 VM 组”。
步骤 8	保护 AHV VM 或智能 VM 组。	请参见第 60 页的“使用保护计划保护 AHV VM 或智能 VM 组”。
步骤 9	恢复 VM。	请参见第 67 页的“恢复 AHV 虚拟机”。

2

Nutanix AHV 管理员的 RBAC 角色

本章节包括下列主题：

Nutanix AHV 管理员的 RBAC 角色

NetBackup 支持使用基于角色的访问控制 (RBAC) 控制哪些用户可以访问哪些 Nutanix AHV 或其他资产。根据您的环境，您可能需要通过以下方式为 Nutanix AHV 管理员配置 RBAC。

表 2-1 Nutanix AHV 管理员需使用或创建的 RBAC 角色

所需的访问类型	使用或创建的角色	
管理 Nutanix AHV 资产和配置，并还原到 Nutanix AHV。	“**默认 AHV 管理员**”角色	

所需的访问类型	使用或创建的角色	
管理 Nutanix AHV 资产和 VMware 资产，具有跨 Hypervisor 支持。	“**默认 AHV 管理员**”和“**默认 VMware 管理员**”角色	借助这些角色，管理员还可以管理以下各项： Nutanix AHV 凭据。（“**工作负载**” > **Nutanix AHV** 中的“**Prism Central 服务器**”选项卡或“**AHV 群集**”选项卡。） vCenter、ESX Server 等的凭据。（“**工作负载**” > **VMware** 中的“**VMware 服务器**”选项卡）。
对 Nutanix AHV 的完全访问权限，以及 VMware 资产的其他权限。	创建自定义角色。	如果要从 VMware 备份映像还原并在恢复后使用 AHV 工作负载，则此角色非常有用。
对 VMware 的完全访问权限，以及 Nutanix AHV 资产的其他权限。	创建自定义角色。	如果使用 VMware 工作负载并要执行跨 Hypervisor 还原，则此角色非常有用。

请注意以下几点：

- 要创建 RBAC 角色，必须具有 RBAC 管理员角色或创建角色的权限。
- 要创建凭据，必须具有 RBAC 管理员角色或有权创建凭据的角色。“**默认 Nutanix AHV 管理员**”和“**默认 VMware 管理员**”角色可以为用户分配凭据，但无法在凭据管理中创建凭据。
- 要获取有关创建角色和凭据的帮助，请与 NetBackup 管理员联系。

为用户同时分配“默认 VMware 管理员”角色和“默认 AHV 管理员”角色

如果要为用户授予对所有 Nutanix AHV 资产和所有 VMware 资产的全局 RBAC 访问权限，请按照此过程操作。如果使用 VMware 工作负载并要跨 Hypervisor 进行还原，则此角色非常有用。此角色的好处是，不需要手动选择源资产和目标资产的所需权限。但是，无法限制此角色对特定资产的权限。在这种情况下，必须配置自定义角色。

为用户同时分配“默认 VMware 管理员”角色和“默认 AHV 管理员”角色

1 在左侧，选择“**安全**” > **RBAC**。

2 选择“**默认 VMware 管理员**”角色。然后选择“**用户**”选项卡。

3 输入组名或用户名。然后选择“**添加到列表**”。

4 要返回到角色列表，请选择“**关闭**”按钮。

5 选择“**默认 AHV 管理员**”角色。然后选择“**用户**”选项卡。

6 输入组名或用户名。然后选择“**添加到列表**”。

7 要查看分配给组或用户的角色，请选择“**用户**”选项卡。

创建自定义角色，使其拥有所有 Nutanix AHV 权限和其他 VMware 资产权限

如果要为用户授予对 Nutanix AHV 的 RBAC 全局访问权限以及特定 VMware 资产的权限，请按照此过程操作。如果要从 VMware 备份映像还原并在恢复后使用 AHV 工作负载，则此角色非常有用。

创建自定义角色，使其拥有所有 Nutanix AHV **权限和其他** VMware **资产权限**

1 在左侧，选择“**安全**”**> RBAC**，然后选择“**添加**”。

2 选择“**默认 AHV 管理员**”角色。然后选择“**下一步**”。

3 提供“**角色名称**”和描述。

例如，描述为：使用该角色的用户可以管理 Nutanix AHV 并提供 VMware 的特定权限。

4 在“**权限**”下，选择“**编辑**”。

5 转到“**AHV 资产**”。请注意，已针对该工作负载选择了所有权限。

6 转到“**VMware 资产**”。

7 选择以下权限：

- **查看**
- **管理访问**
- **还原**
- **查看作业**

8 选择“**分配**”。

9 在“**工作负载**”下，选择“**编辑**”。

10 从下列选项中进行选择：

- 要将工作负载的所需权限应用于所有现有和未来的 VMware 资产，请保持以下选项处于启用状态：“**将权限应用于所有现有和未来 VMware 资产**”。

- 要将所需权限仅应用于特定的 VMware 资产，请清除以下选项：“**将权限应用于所有现有和未来 VMware 资产**”。然后选择要对其应用权限的资产，并选择“**添加**”。

11 选择“**分配**”。

12 在“**用户**”下，选择“**编辑**”。然后添加您希望具有此 RBAC 角色的组或用户。

13 选择“**分配**”。

14 完成角色配置后，选择“**添加角色**”。

15 要查看分配给组或用户的角色，请选择“**用户**”选项卡。

创建自定义角色，使其拥有所有 VMware 权限和其他 Nutanix AHV 资产权限

如果要为用户授予对 VMware 的 RBAC 全局访问权限以及特定 Nutanix AHV 资产的权限，请按照此过程操作。

创建自定义角色，使其拥有所有 VMware **权限和其他** Nutanix AHV **资产权限**

1 在左侧，选择“**安全**”**> RBAC**，然后选择“**添加**”。

2 选择“**默认 VMware 管理员**”角色。然后选择“**下一步**”。

3 提供“**角色名称**”和描述。

例如，描述为：使用该角色的用户可以管理 VMware 并提供 Nutanix AHV 的特定权限。

4 在“**权限**”下，选择“**编辑**”。

5 转到“**VMware 资产**”。请注意，已针对该工作负载选择了所有权限。

6 转到“**AHV 资产**”**>**“**AHV 群集、VM 和存储容器**”。

7 选择除“**粒度还原**”以外的所有权限。

8 转到“**AHV 资产**”**> Prism Central**。

9 选择该组中的所有权限。

10 务必选择组“**AHV 智能 VM 组**”的所有权限。

11 选择“**分配**”。

12 在“**工作负载**”下，选择“**编辑**”。

13 从下列选项中进行选择：

- 要将工作负载的所需权限应用于所有现有和未来的 Nutanix AHV 资产，请保持以下选项处于启用状态：“**将权限应用于所有现有和未来 Nutanix AHV 资产**”。
- 要将所需权限仅应用于特定的 Nutanix AHV 资产，请清除以下选项：“**将权限应用于所有现有和未来 Nutanix AHV 资产**”。然后选择要对其应用权限的资产，并选择“**添加**”。

14 选择“**分配**”。

15 在“**用户**”下，选择“**编辑**”。然后添加您希望具有此 RBAC 角色的组或用户。

16 选择“**分配**”。

17 完成角色配置后，选择“**添加角色**”。

18 要查看分配给组或用户的角色，请选择“**用户**”选项卡。

3

管理 AHV 群集

本章节包括下列主题：

- 为 iSCSI 设置 CHAP
- 添加 AHV 访问主机
- 删除 AHV 访问主机
- 更改 AHV 资源类型的资源限制
- 更改 AHV 资产的自动发现频率
- 扫描恶意软件

保护 AHV 虚拟机的快速配置检查清单

可使用 NetBackup Web UI 保护和恢复在 AHV 平台上创建的虚拟机。此外，还可以使用 API 和命令行选项执行相同的操作。

请参见第 113 页的“使用 API 和命令行选项管理、保护或恢复 AHV 虚拟机”。

下表介绍了保护 AHV 虚拟机的大致步骤或检查清单：

表 3-1 使用 NetBackup 配置和保护 AHV 虚拟机

步骤概述	说明和参考
部署 NetBackup 以保护 AHV VM	大致而言，要保护 AHV VM，您需要： ■ NetBackup 主服务器 ■ NetBackup 介质服务器（推荐） ■ 可作为备份主机的 NetBackup 客户端 备份主机的操作系统必须是 Linux RHEL、SUSE 或 Windows。备份主机可以是 NetBackup 介质服务器、客户端或 NetBackup Appliance。 也支持将 NetBackup Appliance（包括 Flex Appliance 和 Flex Scale Appliance）作为可充当备份主机的 NetBackup 介质服务器。 NetBackup 使用无代理架构保护 AHV VM。NetBackup 与 AHV 群集之间的通信通过 Nutanix AHV API 进行。
配置 AHV 访问主机以执行备份和恢复	在备份和恢复期间，AHV 访问主机分别充当备份主机和恢复主机。访问主机参与备份和还原操作过程中的数据移动。 如果您计划使用的备份主机不是 NetBackup 介质服务器或设备，请将该备份主机添加到 NetBackup 的“**AHV 访问主机**”列表。 **注意：**如果备份主机不是介质服务器或设备，则需要安装 NetBackup 客户端。 请参见第 37 页的“添加 AHV 访问主机”。

步骤概述	说明和参考
实现 NetBackup 和 AHV 之间的安全通信	以下部分介绍在 NetBackup 和 AHV 之间设置安全通信的详细信息： ■ 安全通信 请参见第 18 页的“在 AHV 群集和 NetBackup 主机之间以及 Nutanix Prism Central 和 NetBackup 主机之间配置安全通信”。 ■ 通信端口 请参见第 23 页的“关于 NetBackup 用来与 AHV 进行通信的端口”。
管理 AHV 群集、Prism Central 服务器和智能 VM 组	■ 管理 AHV 群集 请参见第 24 页的“添加或浏览 AHV 群集”。 ■ 管理 Prism Central 服务器 请参见第 28 页的“添加新的 Nutanix Prism Central”。 ■ 管理智能 VM 组 请参见第 31 页的“创建智能 VM 组”。 请参见第 35 页的“删除智能 VM 组”。
保护 AHV VM	■ 前提条件： 添加 AHV 群集需要具有默认的 AHV 管理员角色。 ■ 最佳做法 请参见第 59 页的“保护 AHV 虚拟机之前的注意事项”。 ■ 保护虚拟机 请参见第 60 页的“使用保护计划保护 AHV VM 或智能 VM 组”。
Windows 备份主机的 iSCSI 传输	前提条件 对于 Windows 2012 或更高版本，iSCSI 客户端发起程序位于 Windows 上。默认情况下，iSCSI 发起程序服务在 Windows 上处于停止或禁用状态。 请参见第 20 页的“在 Windows 备份主机上启用 iSCSI 发起程序服务”。 **注意：**如果所选的备份或恢复主机位于 Windows 上，请确保 iSCSI 服务正在 Windows 计算机上运行，以避免备份或还原作业失败。

步骤概述	说明和参考
Linux 备份主机的 iSCSI 传输	前提条件 要使用 iSCSI，必须安装 `scsi-initiator-utils` 软件包。默认情况下，它安装在 RHEL/SUSE 上。 请参见第 20 页的"在 Linux 备份主机上安装 iSCSI 发起程序软件包"。 **注意：**要在 Linux 备份或恢复主机上使用 NFS 协议，该主机需要在 Nutanix AHV Prism 控制台上的 NFS 允许列表中。有关详细信息，请参考 https://www.veritas.com/content/support/en_US/doc/127664414-132725336-0/v127698742-132725336。 如果已在备份或恢复主机上安装 `iscsi-initiator-utils` 软件包，请确保 iSCSI 后台驻留程序正在运行。 ■ 要查看后台驻留程序的状态，请使用 `systemctl status iscsid` 命令。 ■ 如果后台驻留程序处于禁用状态，则先运行 `systemctl enable iscsid` 命令，然后运行 `systemctl start iscsid` 命令来启动 iSCSI 后台驻留程序。
配置 CHAP 设置以与 Nutanix AHV 群集进行 iSCSI 安全通信	单向 CHAP： ■ iSCSI 发起程序使用随机生成的 CHAP 密码/密钥对目标 (AHV) 进行身份验证。 双向 CHAP - 自动： ■ NetBackup 凭据管理服务 (CMS) 会自动生成带有前缀 AHV_ISCSI_MUTUAL_AUTO_ 的凭据，作为备份/恢复主机 CHAP 密码。此凭据用于执行 NetBackup 备份/恢复主机的 iSCSI 发起程序与目标 AHV 之间的双向身份验证。 您可以为这些自动生成的 CHAP 密码设置保留期限。自动生成的 CHAP 密码的默认保留期限为从创建日期起 90 天。 **注意：** 默认配置为单向 CHAP。要启用"**双向 CHAP**"选项，请执行以下操作： 请参见第 23 页的"配置 CHAP 设置以与 AHV 群集进行 iSCSI 安全通信"。
对 AHV 资源的使用设置全局限制	创建 VM 时会自动保护 VM，经过一段时间后，同时受保护的 VM 数量可能会变得很庞大。大量并行备份可能会影响 AHV 性能以及备份性能。 您可以设置全局限制，以便有效管理 AHV 资源。 请参见第 37 页的"更改 AHV 资源类型的资源限制"。

步骤概述	说明和参考
NetBackup 自动备份主机选择	“NetBackup 自动备份主机选择”选项在内部使用 NetBackup 介质服务器负载平衡将快照/备份作业分配给受支持的可用介质服务器。NetBackup 可避免将作业发送给繁忙的介质服务器。 **注意：**需要在介质服务器上使用 NetBackup 9.1 或更高版本进行应用程序一致备份。 前提条件 ■ 在 NetBackup Web UI 中，单击“**存储**”>“**磁盘存储**”。然后，单击“**存储服务器**”选项卡。添加所有支持的介质服务器进行负载平衡。 ■ 单击“**存储**”>“**存储单元**”。选择*“存储单元名称”*。在“**介质服务器**”下，单击“**编辑**”。然后，选择“**允许 NetBackup 自动选择**”。 ■ 创建AHV保护计划时，为“**选择要用于备份的服务器或主机**”设置选择“**自动**”。

在 AHV 群集和 NetBackup 主机之间以及 Nutanix Prism Central 和 NetBackup 主机之间配置安全通信

NetBackup 现在可以使用根证书或中间证书颁发机构 (CA) 证书来验证 AHV 群集和 Prism Central 服务器证书。

虚拟化服务器仅支持 PEM 证书格式。

以下过程适用于充当备份主机的 NetBackup 介质服务器和所有 AHV 访问主机。

要在 AHV 群集和 AHV 访问主机之间以及 AHV Prism Central 服务器和 AHV 访问主机之间配置安全通信，请执行以下操作：

1 使用 Linux 系统中的 `openssl s_client -connect Nutanix Cluster FQDN:9440 -showcerts < /dev/null` 命令获取 Nutanix 证书。

对于 Nutanix Prism Central，使用 `openssl s_client -connect Nutanix Prism Central FQDN:9440 -showcerts < /dev/null`

2 滚动到结果的末尾，然后复制从以下位置开始的最后一个证书：

```
-----BEGIN CERTIFICATE-----
<Certificate>
-----END CERTIFICATE-----
```

注意：确保复制 BEGIN 和 END CERTIFICATE 前后的五个短划线。

3 将信息粘贴到文本文件中，然后将其重命名为 *certificate file name*.pem，并将其复制到备份主机的路径中。建议的路径为：

- 对于 Linux：/usr/openv/netbackup。
- 对于 Windows：*install_path*\NetBackup。

4
- 对于 Linux：在备份主机的 bp.conf 中输入 PEM 文件路径 ECA_TRUST_STORE_PATH=/usr/openv/netbackup/*certificate file name*.pem。
- 对于 Windows：运行 *install_path*\NetBackup\bin\nbsetconfig 命令。

5 在访问主机上使用 nbsetconfig 命令配置以下 NetBackup 配置选项：

有关配置选项的更多信息，请参考 NetBackup 管理指南，第 I 卷。

有关外部 CA 支持的更多信息，请参考 NetBackup 安全和加密指南。

表 3-2

ECA_TRUST_STORE_PATH	指定包含所有可信根 CA 证书的证书文件的文件路径。 此选项特定于基于文件的证书。如果使用 Windows 证书存储库，则不应配置此选项。 如果已配置此外部 CA 选项，请将 Nutanix AHV CA 证书追加到现有的外部证书信任存储区。 如果未配置该选项，则将所有所需的 Nutanix AHV 服务器 CA 证书添加到信任存储区并设置该选项。
ECA_CRL_PATH	指定外部 CA 证书吊销列表 (CRL) 所在目录的路径。 如果已配置此外部 CA 选项，请将 AHV CRL 附加到 CRL 缓存。 如果未配置此选项，请先将所有所需的 CRL 添加到 CRL 缓存。然后设置此选项。

VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED	此选项会影响 AHV、RHV 和 VMware 安全通信。如果不使用此选项，则与工作负载的安全或不安全通信由每个工作负载和插件单独决定。 对于 Nutanix AHV，默认情况下启用安全通信。 可使用此选项跳过安全证书验证。 禁用此选项可跳过安全证书验证。 Cohesity 建议使用 ECA_TRUST_STORE_PATH 选项启用安全通信。
VIRTUALIZATION_CRL_CHECK	用于根据 CRL 验证虚拟化服务器证书的吊销状态。 默认情况下启用该选项。

在 Windows 备份主机上启用 iSCSI 发起程序服务

执行以下操作之一：

1
- 单击“**服务器管理器**”>“**工具**”>“**iSCSI 发起程序**”。
- 将显示一个消息窗口，**要立即启动该服务并在每次计算机重新启动时自动启动该服务，请单击“是”按钮**。单击“**是**”确认。

2 或者，要从管理工具启用 iSCSI 服务，请执行以下操作：
- 打开“**控制面板**”->“**管理工具**”->“**打开服务**”。
- 找到“**Microsoft iSCSI 发起程序服务**”。
- 右键单击它，然后单击“**启动**”。

注意：此服务的默认选项为“**手动**”。将设置更改为“**自动**”，以在您重新启动时自动启动服务。

3 如果计划使用 Nutanix iSCSI 分段网络，有关备份主机网络配置详细信息，请参见第 22 页的“关于对 Nutanix 分段 iSCSI 网络的支持”。。

在 Linux 备份主机上安装 iSCSI 发起程序软件包

要安装 iSCSI 发起程序软件包，请使用以下 yum 和 zypper 命令：

- `yum install iscsi-initiator-utils" - RedHat`。
- `zypper -n install open-iscsi" - SuSE`。
- 如果计划使用 Nutanix iSCSI 分段网络，有关备份主机网络配置详细信息，请参见第 22 页的“关于对 Nutanix 分段 iSCSI 网络的支持”。。

将 Java GUI/CLI 添加的群集迁移到 Web UI 中

Java GUI/CLI 和 Web UI 的凭据分开进行管理。

- 使用管理控制台或 CLI 添加的群集不会反映在 Web UI 中，反之亦然。
- 如果 Java GUI/CLI 中存在任何现有群集，用户必须手动在 Web UI 中添加这些群集及其凭据。

注意：在 Web UI 中添加群集后，如果从 Java GUI/CLI 中将其删除，则该群集仍然存在于 Web UI 中，反之亦然。

- 在 Web UI 中添加群集后，如果需要更新群集凭据，只能从 Web UI 进行更新。设想以下情形：
  - 某群集既存在于 Web UI 中，也存在于管理控制台中。
  - 仅在 Web UI 中更新群集凭据。
  - 从 Web UI 中删除了该群集。

  影响：由于 Java GUI 中添加的群集凭据未更新，因此 Java GUI 上的备份和还原可能会失败。
  建议：从 Java GUI 更新凭据。
- 在 Web UI 中添加群集后，即使从 Java GUI 中删除群集，使用现有策略的备份仍会成功。但在这种情况下，无法从 Java GUI 触发还原作业，因为还原作业要求 Java GUI 上存在群集。
- 如果从 Java GUI 和 Web UI 添加群集，然后从 Java GUI 将其删除，在 Web UI 中仍可看到该群集，反之亦然。
- 如果群集位于 Web UI 以及 Java GUI 中且其凭据在 Web UI 中进行了更新，随后从 Web UI 中删除了该群集，则备份和还原可能会失败，因为 Java UI 中添加的群集未更新。可能必须从 Java UI 更新凭据，才能使一切恢复正常。

配置 Nutanix AHV 群集的前提条件

前提条件：

在 Nutanix AHV 群集上配置 iSCSI 数据服务 IP

1 要使用“**使用分段 iSCSI 数据服务 IP**”或“**使用指定的分段 iSCSI 数据服务 IP**”选项，必须为 AHV 群集配置具有卷 (ABS) 功能的分段 iSCSI 网络接口。

2 如果计划在配置群集时选择“**使用 iSCSI 数据服务 IP**”选项，**Nutanix** 建议，必须在 Nutanix AHV 上配置 iSCSI 数据服务 IP。

转到 Nutanix AHV 群集 Prism 控制台，地址为 `https://Nutanix cluster FQDN/IP:9440`。

单击“**设置**”>“**群集详细信息**”>“**设置 iSCSI 数据服务 IP**”。

注意：如果未配置此设置：

对于 Windows 备份主机，备份还原作业将失败。

对于 Linux 备份主机，如果正确完成了分段 iSCSI 数据服务 IP 配置，则作业将回退以使用 NFS。

Windows 备份主机的备份还原作业失败，在“**活动监视器**”>“**作业详细信息**”中显示为“失败”状态。对于 Linux 备份主机，在作业详细信息中，从 iSCSI 到 NFS 的回退被认为是警告。

关于对 Nutanix 分段 iSCSI 网络的支持

NetBackup 支持使用 Nutanix iSCSI 分段网络分离备份通信。分离备份通信有助于减少生产资源负载，将适当大小的资源专用于提高备份恢复速度和安全性。默认情况下，备份恢复通信使用 iSCSI 数据服务 IP 通过 Nutanix 群集管理网络进行初始连接和发现。

在 AHV 群集配置期间，选择以下选项之一进行 iSCSI 传输：

- **使用 iSCSI 数据服务 IP**
- **使用分段的 iSCSI 数据服务 IP**
- **使用指定的分段 iSCSI 数据服务 IP**

有关更多详细信息，请参见第 24 页的“添加或浏览 AHV 群集”。

配置备份主机网络，以使用 Nutanix iSCSI 分段网络配置。

- iSCSI 分段网络与群集管理网络位于不同的子网上，因此必须将备份主机网络配置为连接到：
  - AHV 群集管理网络
  - iSCSI 分段网络。

为此，请为备份主机配置两个VLAN。一个对应于群集管理网络，另一个对应于计划用于备份恢复通信的分段 iSCSI 网络。

- 为了获得更好的性能，在备份主机上安装/配置NetBackup时，请使用与分段网络对应的主机名/IP 作为主机名。
- 在 Windows 主机上使用以下命令验证连接：
  - 单击“**服务器管理器**”>“**工具**”>“**iSCSI 发起程序**”。这将打开“**iSCSI 发起程序属性**”对话框。
  - 单击“**发现**”>“**发现门户**”，并根据为 AHV 群集配置的 iSCSI 目标类型提供 IP 地址。
  - DEFAULT：群集详细信息页面中的 iSCSI 数据服务 IP
  - SEGMENTED：群集详细信息页面中的分段 iSCSI 数据
  - SEGMENTED_SPECIFIC：在 NetBackup 中配置群集时指定的虚拟 IP。
- 在 Linux 主机上使用以下命令验证连接：
  - `iscsiadm -m discovery -t sendtargets -p` *`correct IP as per configured iSCSITargetType`*
  - DEFAULT：群集详细信息页面中的 iSCSI 数据服务 IP
  - SEGMENTED：群集详细信息页面中的分段 iSCSI 数据
- SEGMENTED_SPECIFIC：在 NetBackup 中配置群集时指定的虚拟 IP。如果存在连接问题，则会显示错误，例如：`iscsiadm: connect to <IP> timed out`

配置 CHAP 设置以与 AHV 群集进行 iSCSI 安全通信

CHAP 设置适用于配置到当前所选主服务器的所有 AHV 群集。

1. 在左侧，选择“**工作负载**”> **Nutanix AHV**。
2. 在顶部，单击“**AHV 设置**”。
3. 选择“**iSCSI 的 CHAP**”。
4. 选择适当的 CHAP 选项。

关于 NetBackup 用来与 AHV 进行通信的端口

下表介绍了 NetBackup 与 AHV 进行通信时所需的端口：

表 3-3 NetBackup 与 AHV 进行通信时所需的端口

端口	协议	目标	用途
860，3260	iSCSI over TCP	*双向	iSCSI 通过 SCSI 提供对存储设备的块级访问。 iSCSI 可促进通常通过以太网进行的数据传输。
3205	iSCSI over TCP	*双向	iSNS 能够模拟光纤通道 Fabric 服务并管理 iSCSI 和光纤通道设备，iSNS 服务器可用作整个存储网络的整合配置点
111	TCP	*双向	Portmapper
2049	TCP	*双向	NFS
9440	TCP	AHV 群集 AHV Prism Central 服务器	Prism 控制台，REST API

*必须在 AHV 访问主机和 AHV 群集之间双向打开端口。仅在从 AHV 访问主机到 AHV 群集的入站通信中打开端口 9440。

添加或浏览 AHV 群集

您可以添加和浏览 AHV 群集及其凭据。

添加 AHV 群集及其凭据

1 在左侧，单击“**工作负载**”>**Nutanix AHV**，然后单击“**AHV 群集**”选项卡。

2 单击“**添加**”，添加 AHV 群集，然后输入以下内容：

请参见第 96 页的“添加 AHV 凭据期间出错”。

- **群集名称**

  注意：NetBackup 建议使用 FQDN 添加 AHV 群集。群集名称必须限制在 218 个字符内。

- **REST API 端口（默认值：9440）**
  该端口必须在备份主机和 AHV 群集之间保持打开状态。
  请参见第 23 页的“关于 NetBackup 用来与 AHV 进行通信的端口”。

- 选中“**对此群集使用 Prism Central**”复选框，可保护虚拟机的 Prism Central 服务器相关属性。例如，捕获 VM 的虚拟私有云网络相关属性、项目、类别和所有者相关属性。
  请参见第 28 页的“添加新的 Nutanix Prism Central”。

  注意：选中此复选框之前，必须在 NetBackup 环境中添加 Prism Central 服务器。

- 从“**iSCSI 传输**”中选择以下选项之一。
  - **使用 iSCSI 数据服务 IP**
    使用 AHV 群集上配置的 iSCSI 数据服务 IP 作为 iSCSI 目标发现门户和初始连接点。

    注意：在以下情况下，此选项将回退到 Linux 备份主机上的 NFS：

    未在 AHV 群集上配置 iSCSI 数据服务 IP。

    未在备份主机上建立 iSCSI 连接。

  - **使用分段的 iSCSI 数据服务 IP**
    使用 AHV 群集上配置的分段 iSCSI 数据服务 IP 作为 iSCSI 目标发现门户和初始连接点。

    注意：如果未在 AHV 群集上完成配置，群集验证将失败。

    如果未在 AHV 群集上完成配置或备份主机没有所需的网络配置，则备份/恢复作业将失败。

  - **使用指定的分段 iSCSI 数据服务 IP**
    - 在“**虚拟 IP 地址**”字段中，提供有效的 IP 地址。
      提供与计划用于备份和恢复 iSCSI 数据通信的 Nutanix 分段 iSCSI 网络接口相对应的虚拟 IP。

    使用指定的 IP 地址作为 iSCSI 目标发现门户和初始连接点。如果虚拟 IP 地址来自任何一个已配置的分段 iSCSI 数据服务接口，NetBackup 将使用 Nutanix API 进行验证。

    注意：如果未在 AHV 群集上完成配置或备份主机没有所需的网络配置，则备份/恢复作业将失败。

3 ■ **选择备份主机**
此备份主机用于验证和发现。

注意：只有 NetBackup 9.1 或更高版本支持凭据验证和虚拟机发现。

■ **关联凭据**

执行以下操作之一：

- 选择现有凭据，请参见 NetBackup™ Web UI 管理指南中的“管理凭据”。
- 请参见第 45 页的“添加新群集凭据”。

注意：必须关联具有群集管理员角色的 AHV 群集用户的凭据。

4 单击“**添加和管理权限**”。

对所有输入执行验证。

选择有权访问此群集的角色。请参见 NetBackup™ Web UI 管理指南中的“管理基于角色的访问控制”。

5 要添加另一 AHV 群集的凭据，请单击“**添加**”。

AHV 群集上的内联操作

您可以在 AHV 群集上运行以下内联操作：

- **发现**：手动发现属于选定 AHV 群集的 VM 资产。
- **编辑**：修改 AHV 群集凭据。
- **删除**：删除 AHV 群集。
- **管理权限**：用于添加或管理所选群集的权限。

AHV 群集上的批量操作

您可以选择一个或多个 AHV 群集，并运行以下批量操作：

- **发现**：手动发现属于选定 AHV 群集的 VM 资产。

注意：按顺序对各群集依次触发发现操作。

- **验证**：

- 验证 AHV 群集的凭据。
- 如果选择“**使用分段 iSCSI 数据服务 IP**”，请验证是否在 Nutanix 群集上配置了分段 iSCSI 数据服务 IP 地址。
- 如果选择“**使用指定的分段 iSCSI 数据服务 IP**”，请验证指定的虚拟 IP 地址是否配置为 Nutanix 群集上的分段 iSCSI 数据服务 IP 地址。

- **删除**：删除 AHV 群集。

浏览 AHV 群集。

您可以浏览 AHV 群集，查找 VM 和存储容器及其详细信息。

浏览 AHV 群集

1 在左侧，单击 Nutanix AHV。

2 单击“**AHV 群集**”选项卡，然后开始搜索。

该列表包括您有权访问的 AHV 群集。

该选项卡按以下层次显示可以访问的 AHV 群集：

```
All
AHV_clusters
 cluster1
  VirtualMachine
  StorageContainer
 cluster2
  VirtualMachine
  StorageContainer
```

要查找群集，您可以在搜索字段中输入字符串。

3 单击 AHV 群集可查看其详细信息。

4 单击虚拟机可查看其保护状态、恢复点和还原活动。

5 单击“**添加保护**”为所选的 VM 订购保护计划。也可以选择“**立即备份**”、“**恢复**”和“**管理权限**”选项。

注意：在 NetBackup Web UI 11.0 中，可以使用 Nutanix-AHV 策略保护 VM。

6 单击存储容器可查看可用空间以及上次发现的时间。

注意：数据超过公布容量后，超出的数据将显示为负值。对于此类值，NetBackup Web UI 显示一个空字段，而对应的 API 显示特定存储容器的可用空间字段值为 -ve。

7 对于存储容器，可以“**管理权限**”。

注意：仅当选择存储容器时，才启用“**管理权限**”。

删除 AHV 群集

使用此过程可删除 AHV 群集。

删除 AHV 群集

1 在左侧，单击“**工作负载**”**> Nutanix AHV**，然后单击“**AHV 群集**”选项卡。

此选项卡列出了您有权访问的 AHV 群集的名称。还可以查看“**发现状态**”和“**上次发现尝试**”，确定上次发现服务器的 VM 和其他对象的时间。

2 找到并选择 AHV 群集。

3 选择“**操作**”**>**“**删除**”。

注意：如果删除群集，与删除的 AHV 群集相关联的所有虚拟机将不再受保护。您仍然可以恢复现有的备份映像，但此服务器上的 VM 备份将失败。

4 如果确定要删除该 AHV 群集，请单击“**删除**”。

添加新的 Nutanix Prism Central

您可以添加和浏览 Nutanix Prism Central 及其凭据。

添加 Nutanix Prism Central 和相应凭据

1 在左侧，单击 **Nutanix AHV**，然后单击“**Prism Central 服务器**”选项卡。

2 单击“**添加**”，添加 Nutanix Prism Central，然后输入以下内容：

- **Prism Central 服务器名称**

- **REST API 端口（默认值：9440）**
  该端口必须在备份主机和 AHV 群集之间保持打开状态。
- **备份主机**

  注意：备份主机版本必须是 NetBackup 10.1.1 或更高版本。操作系统必须是 Linux（RHEL 和 SUSE）或 Windows。

- **关联凭据**

  执行以下操作之一：

  - 为现有凭据添加 Prism Central 服务器凭据时，类别请选择 **AHV Prism Central**。有关更多信息，请参见 NetBackup™ Web UI 管理指南中的“管理凭据”。
  - 请参见第 30 页的“添加新的 Prism Central 服务器凭据”。

3 单击“**添加和管理权限**”

  对所有输入执行验证。

  选择有权访问此群集的角色。请参见 NetBackup™ Web UI 管理指南中的“管理基于角色的访问控制”。

4 要添加另一 AHV Prism Central 凭据，请单击“**添加**”。

Nutanix Prism Central 上的内联操作

您可以在 Nutanix Prism Central 上运行以下内联操作：

- **验证**：手动验证
- **编辑**：修改备份主机和 Nutanix Prism Central 凭据。
- **删除**：删除 Nutanix Prism Central。
- **管理权限**：用于添加或管理所选 Prism Central 的权限。

Nutanix Prism Central 上的批量操作

您可以选择一个或多个 Nutanix Prism Central，并运行以下批量操作：

- **验证**
- **删除**

添加新的 Prism Central 服务器凭据

1 在左侧，单击 **Nutanix AHV**，然后单击 **Nutanix Prism Central** 选项卡。

2 单击“**添加**”可添加新的 Prism Central 服务器。

3 在“**添加 AHV Prism Central**”**>**“**关联凭据**”页面上，单击“**添加新凭据**”。

4 输入“**凭据名称**”、“**标记**”和“**描述**”等详细信息。

5 在“**Nutanix Prism Central 的凭据**”部分中，添加关联的 Prism Central 服务器的“**用户名**”、“**密码**”和“**域**”。

注意：关联的凭据必须是具有 Prism Central Admin 角色的用户凭据。

6 单击“**下一步**”。

选择现有角色或添加新角色，以提供凭据的权限。

7 单击“**保存**”。

删除 Nutanix Prism Central

使用此过程可删除一个或多个 Nutanix Prism Central。

删除 Nutanix Prism Central

1 在左侧，单击 **Nutanix AHV**，然后单击“**Prism Central 服务器**”选项卡。

此选项卡列出了您有权访问的 Nutanix Prism Central 的名称。

2 找到并选择 AHV Prism Central。

3 选择一个或多个 Prism Central 服务器，然后单击“**操作**”**>**“**删除**”

注意：如果删除 Prism Central，将备份/恢复与删除的 Prism Central 服务器关联的所有虚拟机，但不包含项目、类别、所有者和虚拟私有云网络相关属性。

4 取消选择“**对与此 Prism Central 服务器关联的所有群集禁用“对此群集使用 Prism Central 服务器”。如果要使其保持启用状态，请取消选择。**”复选框（如果需要），然后单击“**删除**”

注意：删除 Nutanix Prism Central 后，不会自动为此 Prism Central 服务器的群集触发资产发现。因此，这些群集的 VM 将在“VM 详细信息”页面上显示 Prism Central 服务器和项目，直到触发下一次资产发现为止。

注意：如果环境中的群集与此 Prism Central 关联并已选中“**对此群集使用 Prism Central 服务器**”复选框，然后通过取消选中“**对与此 Prism Central 服务器关联的所有群集禁用“对此群集使用 Prism Central 服务器”**”复选框删除了此 Prism Central，则在添加关联的 Prism Central 服务器之前，后续备份或还原作业将失败。

创建智能 VM 组

您可以根据一组过滤器（称为查询）创建智能 VM 组。NetBackup 会自动根据查询选择虚拟机并将其添加到组中。然后，您可以对该组应用保护。请注意，智能组会自动反映 VM 环境中的更改，因此不必手动修改组中的 VM 列表。

注意：后台任务会将与查询匹配的新发现 VM 添加到智能 VM 组。此后台任务在 NetBackup Web 管理服务启动后 30 分钟运行。之后，该任务每 30 分钟运行一次。

创建智能 VM **组**

1 在左侧，单击“**工作负载**”**> Nutanix AHV**。

2 单击“**智能 VM 组**”选项卡，然后单击“**添加智能 VM 组**”。

3 为组输入名称和描述。

智能 VM 组显示名称的长度必须在 1-256 个字符之间。

4 在“**群集**”窗格中，单击“**添加群集**”。

注意：要创建组，必须至少具有一个群集。

- 在“**添加群集**”窗口中，选择要添加的群集。

注意：要添加群集，必须对群集具有查看和创建权限。

5 执行下列操作之一：

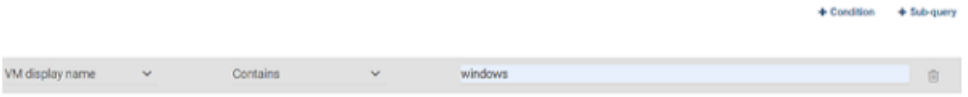
- 选择默认查询：“**包括所有 VM**”。
  运行保护计划时，AHV 群集的所有 VM 都将添加到智能 VM 组中。

- 创建自己的查询：单击“**添加条件**”。

6 要添加条件，请使用下拉列表选择关键字和运算符，然后输入值。

完成此过程之后将出现以下选项：用于创建智能 VM 组的查询选项。

以下是查询示例：

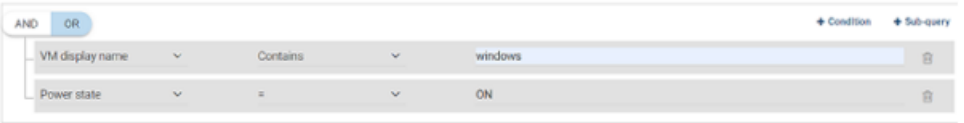


在此示例中，该查询将显示名称中具有 `windows` 的任何 VM 添加到组中。

要更改查询的效果，请单击“**+ 条件**”并单击 **AND** 或 **OR**，然后选择条件的关键字、运算符和值。例如：

此示例使用 **AND** 来缩小查询的范围：它仅选择显示名称中具有 `windows` 且还具有 `ON` 电源状态的 VM。如果某 VM 的显示名称中不含 `windows` 并且不具有 `ON` 电源状态，则不会将该 VM 添加到组中。

要扩大查询的范围，请使用 **OR**：



在此示例中，**OR** 会导致查询将以下内容添加到组中：

- 显示名称中具有 `windows` 的 VM（无论电源状态如何）。
- 具有 `ON` 电源状态的 VM（无论显示名称如何）。

7 要测试查询，请单击“**预览**”。

注意：基于查询的选择过程是动态的。虚拟环境中的更改可能会影响在保护计划运行时查询选择的 VM。因此，查询在保护计划运行后选择的 VM 可能与预览中当前列出的 VM 不同。

注意：单击“**预览**”或保存组时，如果为组选择 VM，则会将查询选项视为区分大小写。在“**虚拟机**”下，如果单击未为该组选择的 VM，则“**虚拟机组的成员**”字段将为 `none`。

但是，将组添加到保护计划时，在保护计划的备份运行时，某些查询选项将被视为不区分大小写。因此，同一个 VM 现在可以包括在组中并进行备份。

对于每个选项的案例行为，请参见以下主题：

用于创建智能 VM 组的查询选项

8 要保存组，请单击“**添加和管理权限**”。

注意：您可以编辑、保护和管理该组的权限。

- 添加保护计划：
  请参见第 60 页的“使用保护计划保护 AHV VM 或智能 VM 组”。
- 编辑或更新智能 VM 组：
  请参见第 35 页的“更新智能 VM 组”。
- 为 VM 组分配权限：
  请参见第 34 页的“为智能 VM 组分配权限”。

用于创建智能 VM 组的查询选项

表 3-4 查询关键字

关键字	描述
`displayName`	VM 的显示名称。 保护计划运行时区分大小写。
`powerState`	VM 的电源状态。 ON 和 OFF 区分大小写。

关键字	描述
vmUuid	VM 的实例 UUID。 例如： 501b13c3-52de-9a06-cd9a-ecb23aa975d1 保护计划运行时不区分大小写。
StorageContainerName	存储容器的名称。 保护计划运行时区分大小写。
Category	请确保满足以下条件： AHV 类别应用于 Nutanix Prism Central 服务器中的 VM。对于完全搜索，必须采用 **CategoryName:Value** 格式。

表 3-5 查询运算符

运算符	描述
Starts with	匹配出现在字符串开头的值。 例如，如果输入的值为 box，则此选项将匹配字符串 box_car 而非 flatbox。
Ends with	匹配出现在字符串结尾的值。 例如，如果输入的值为 dev，则此选项将匹配字符串 01dev 而非 01dev99 或 devOP。
Contains	匹配字符串内出现该值时输入的值。 例如：如果输入的值为 dev，则此选项将匹配 01dev、01dev99、devOP 和 development_machine 等字符串。
=	仅匹配输入的值。 例如，如果输入的值为 VMtest27，则此选项将匹配 VMTest27（相同大小写）而非 vmtest27、vmTEST27 或 VMtest28。
!=	匹配任何值（所输入的值除外）。

为智能 VM 组分配权限

为 VM 组分配权限之前需要考虑的事项。

- **查看/更新**
  - 您对组中的所有群集必须具有 VIEW 权限。

- 如果没有任何群集的 VIEW 权限，则您不能在“**虚拟机**”选项卡中预览组的 VM。
- 您对其没有权限的群集会显示锁符号。
- 已删除的群集将显示 **X** 符号。
- 要向现有 VM 组中添加新群集，必须对目标群集具有 VIEW 权限。
- 要更新 VM 组，对群集必须具有 VIEW 权限。但是，您可以删除不存在的群集或没有 VIEW 权限的群集。

- **保护**
  - 必须对组中的所有群集具有 PROTECT 权限。
  - 要保护 VM 组，必须对组的所有群集以及 VM 组具有 PROTECT 权限。
  - 如果对所有群集均无 PROTECT 权限，则会禁用“**立即备份**”。
  - 无论对群集的权限为何，均会启用“**删除保护**”。它仅由对 VM 组的权限驱动。

有关角色权限的详细信息，请参见 NetBackup Web UI 管理指南。

更新智能 VM 组

您可以编辑智能 VM 组。

编辑智能 VM 组

1. 在左侧，单击“**工作负载**” **> Nutanix AHV**。
2. 单击“**智能 VM 组**”选项卡，然后选择要编辑的 VM 组。
3. 在“**虚拟机**”选项卡中，单击“**编辑**”。

   在“**群集**”窗格中，单击“**添加群集**”。

注意：您可以删除或添加 VM 组。要添加智能 VM 组，请参见第 31 页的“创建智能 VM 组”。

删除智能 VM 组

使用以下过程删除智能 VM 组。

删除智能 VM 组

1 在左侧，单击“**工作负载**”**> Nutanix AHV**。

2 在“**智能 VM 组**”选项卡下找到该组。

3 如果该组不受保护，则单击其框，然后单击“**删除**”。

4 如果该组受到保护，则单击该组，向下滚动并单击锁定符号，然后单击“**取消订购**”。

5 单击“**删除**”。

为 iSCSI 设置 CHAP

CHAP 设置适用于在所选主服务器下配置的所有 AHV 群集。默认情况下，该配置设置为单向 CHAP。

注意：对于单向 CHAP 选项，不需要任何操作。

要启用双向 CHAP 选项，请执行以下操作：

1 在左侧，单击“**工作负载**”**> Nutanix AHV**。

2 在右上角，选择“**AHV 设置**”**>**“**iSCSI 的 CHAP**”，然后选择适当的“双向 CHAP”选项。

注意：对于双向 CHAP，NetBackup 凭据管理系统自动为所选备份或恢复主机生成具有 `AHV_ISCSI_MUTUAL_AUTO_` 前缀的凭据。在“**凭据管理**”选项卡中可以看到 iSCSI 双向 CHAP 凭据。

注意：默认情况下，由默认 AHV 管理员角色创建的用户看不到“双向 CHAP”选项自动生成的凭据。安全管理员/root 用户必须为特定用户提供凭据查看权限才能查看这些凭据。

“**凭据管理**”选项卡中自动生成的凭据无法编辑，只能删除。如果手动删除，将在生成此凭据的下一个作业运行时自动重新创建它。

添加 AHV 访问主机

NetBackup 使用名为“AHV 访问主机”的特殊主机。它是代表虚拟机执行备份的 NetBackup 客户端。访问主机是唯一安装了 NetBackup 介质服务器或客户端软件的主机。虚拟机上不需要 NetBackup 客户端软件。但是，访问主机必须能够访问虚拟机的存储容器。访问主机从存储容器读取数据，然后通过网络将这些数据发送到介质服务器。

AHV 访问主机以前称为 AHV 备份主机。执行还原时，访问主机称为恢复主机。

注意：确保在添加的所有访问主机上均安装了 NetBackup 介质服务器软件或客户端软件。

添加 AHV 访问主机

1. 在左侧，单击“**工作负载**”**> Nutanix AHV**。
2. 在右上角，选择“**AHV 设置**”**>**“**访问主机**”。

   NetBackup 将列出以前添加的所有访问主机。
3. 单击“**+ 添加**”。
4. 输入访问主机的 `Name/FQDN/IP`，然后单击“**添加**”。

删除 AHV 访问主机

删除 AHV 访问主机

1. 在左侧，单击“**工作负载**”**> Nutanix AHV**。
2. 在右上角，选择“**AHV 设置**”**>**“**访问主机**”。

   NetBackup 将列出以前添加的所有访问主机。
3. 找到 AHV 访问主机，然后单击删除图标。
4. 要确认删除，请单击“**删除**”。

更改 AHV 资源类型的资源限制

Nutanix AHV 资源限制控制可针对 Nutanix AHV 资源同时执行的备份数。这些设置适用于当前所选主服务器的所有 NetBackup 策略。

Nutanix AHV 可用的资源限制：

- **每个主机的备份作业数**

- **每个 AHV 群集的备份作业数**
- **每个存储容器的备份作业数**
- **每个 AHV 群集的快照作业数**

注意：对于每个资源，默认值为 0（没有限制）。

设置 Nutanix AHV **资源的资源限制**

1 在左侧，单击“**工作负载**”**> Nutanix AHV**。

2 在右上角，单击“**AHV 设置**”**>**“**资源限制**”。

对于每个资源，默认值为 **0**（没有限制）。

注意：“**每个 AHV 群集的快照作业数**”选项设置每个群集的同时快照操作数限制。仅在备份的快照创建阶段适用。它不会控制同时备份作业数。此设置可以控制多个快照操作对 AHV 群集的影响。要覆盖该 AHV 群集的全局快照设置，请添加特定 AHV 群集。

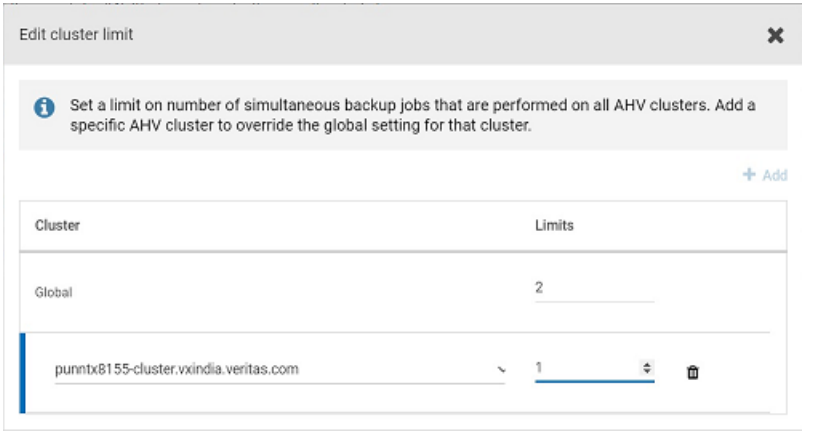
---

3 找到要更改的 AHV 资源，然后单击“**编辑**”。

4 从下列选项中进行选择。

为 AHV 资源类型设置全局限制。	找到“**全局**”设置，然后选择要应用的“**限制**”值。 此值限制可针对该资源类型同时执行的备份数。
为特定 AHV 资源设置限制。	单击“**添加**”。 从列表中选择资源。 选择要应用的“**限制**”值。 此值限制可针对所选资源同时执行的备份数。

以下示例显示所有 AHV 群集的全局限制为 **2**，所选 AHV 群集的全局限制为 **1**。



5 单击“**保存**”。

“**限制**”指示可针对该资源类型同时执行的备份数。此值为全局限制。“**覆盖**”值指示有多少资源的限制不同于全局限制。

注意：设置资源限制后，必须先运行几个作业，限制才会生效。

重置所有 AHV 资源的资源限制

重置所有 AHV 资源的资源限制

- 单击“**重置默认值**”可删除所有覆盖并将所有全局 AHV 资源限制设置为其默认值。

示例 - 为具有两个节点的 Nutanix 群集设置资源限制

请参考以下示例：

- Nutanix 群集具有两个节点。
- 每个节点托管 40 个 VM，因此群集中有 80 个 VM。
- **Nutanix-AHV** 策略有 20 个 VM。

当 NetBackup 连接到 Nutanix 环境进行备份时，会与每个 VM 建立一个连接。如果未设置资源限制，则共有 160 个运行的并行作业（80 个快照作业 + 80 个备份作业）。请参见本文章。

Nutanix 建议群集中的每个 CVM 最多有 20 个并行连接，这意味着每个节点上最多同时备份 20 个 VM。在我们的示例中，可以使用以下设置强制执行 20 个连接的限制：

每个节点的备份作业数	**20**
每个群集的备份作业数	**40**
每个存储容器的备份作业数	基于存储技术的特色设置限制。
每个群集的快照作业数	**10**

当备份开始时，活动监视器将显示作业，如下所示：

- 快照作业：20
- 活动作业：10（快照作业及其备份作业）
- 排队的作业：10
- 活动快照作业完成后，排队的快照作业变为活动状态。

更改 AHV 资产的自动发现频率

AHV 资产自动发现会定期执行。默认频率为每 8 小时执行一次。使用此过程可更改自动发现频率。

更改 AHV 资产的自动发现频率

1 在左侧，单击“**工作负载**” > **Nutanix AHV**。

2 在右侧，选择“**AHV 设置**” > “**自动发现**”。

3 选择“**频率**”>“**编辑**”。

4 使用向上或向下箭头选择需要 NetBackup 对 AHV 资产执行自动发现的频率。然后，单击“**保存**”。

可以选择的范围为 1-24 小时。要设置自动发现频率（以分钟或秒为单位）或禁用自动发现，必须使用 AHV 自动发现 API。

扫描恶意软件

NetBackup 10.5.1 及更高版本支持通过 Nutanix AHV 工作负载扫描 Nutanix 资产以查找恶意软件。

要触发恶意软件扫描，必须配置扫描主机。有关配置扫描主机的更多信息，请参考《NetBackup 安全和加密指南》中的“扫描主机配置”一章。

扫描备份映像

本节介绍扫描特定策略的客户端备份映像以查找恶意软件的过程。

扫描客户端备份映像策略以查找恶意软件

1 在左侧，选择“**检测和报告**”>“**恶意软件检测**”。

2 在“**恶意软件检测**”页面上，选择“**扫描恶意软件**”。

3 在“**搜索依据**”选项中，选择“**备份映像**”。

选择以下扫描类型之一：

- “恶意软件扫描”- 选择此选项可使用默认恶意软件扫描扫描映像。
- “YARA 扫描”- 选择此选项可使用 YARA 规则扫描映像。

  单击“**选择威胁源**”选项。

  在“**选择用于扫描的威胁源**”对话框中，选择所需的 YARA 规则或先前已上传的 YARA 规则的 zip 文件。

4 以下所有步骤均适用于“恶意软件扫描”扫描类型。

在“**扫描程序主机池**”选项中，从“**选择恶意软件扫描程序主机池**”中列出的扫描程序主机池列表中搜索并选择相应的主机池名称。

注意：选定扫描主机池中的扫描主机必须能够访问在配置了 NFS/SMB 共享类型的存储服务器上创建的即时访问装入。

---

5 在搜索条件中，查看并编辑以下内容：

- **策略名称**
  仅列出支持的策略类型。
- **客户端名称**
  显示具有受支持策略类型的备份映像的客户端。
- **策略类型**
  显示已启用恶意软件扫描的所有受支持策略。

注意：如果从 Nutanix-AHV 策略和保护计划备份中进行备份，Nutanix-AHV 策略将显示 Nutanix-AHV 映像。

警告：Hypervisor 策略类型显示 Nutanix AHV 和 RHV 映像。NetBackup 仅支持对 Nutanix AHV 映像进行恶意软件扫描。

- **备份类型**
- **副本数**
  如果所选副本不支持即时访问，则会跳过对备份映像进行恶意软件扫描。
- **磁盘池**
  列出了 MSDP (PureDisk)、OST（如 Data Domain）和 AdvancedDisk 存储类型磁盘池。
- **磁盘类型**
  列出了 MSDP (PureDisk)、OST（如 Data Domain）和 AdvancedDisk 磁盘类型。
- **感染状态**
  可以根据以下条件搜索备份映像的恶意软件感染状态：“恶意软件扫描检测到感染”、“文件哈希搜索检测到感染”、“未受感染”、“未扫描”或“全部”。
- 对于“**选择备份时段**”，验证日期和时间范围或进行更新。
- 选择“**检测到感染时中止恶意软件扫描**”选项后，受感染映像将不支持干净数据恢复。

6 单击“**搜索**”。

7 选择搜索条件，并确保所选扫描主机处于活动状态且可用。

8 从“**选择要扫描的备份**”表中，选择一个或多个映像进行扫描。

9 单击“**扫描恶意软件**”。

10 启动扫描后，将显示“**扫描状态**”。

以下是状态字段：

- **未扫描**
- **未受感染**
- **受感染**
- **失败**
  将鼠标悬停在状态上可查看扫描失败的原因。

  注意：任何未通过验证的备份映像都将被忽略。仅当备份映像存储在具有即时访问功能的存储上并且属于支持的策略类型时，才支持恶意软件扫描。

- **进行中**
- **挂起**

  注意：可以针对一个或多个进行中的作业和挂起的作业取消恶意软件扫描。

- **受感染恶意软件扫描已中止**

资产 (按工作负载类型)

注意：对于 YARA 扫描，仅支持 Kubernetes。

要扫描支持的资产以查找恶意软件，请执行以下操作：

1. 在左侧，在“**工作负载**”下选择支持的工作负载。
2. 选择已完成备份的资源。
   例如，Nutanix AHV。
3. 选择“**操作**”>“**扫描恶意软件**”。
4. 在“**恶意软件扫描**”页面上，执行以下操作：
   - 通过选择“**开始日期/时间**”和“**结束日期/时间**”，选择扫描的日期范围。
   - 选择“**扫描程序主机池**”。
   - 从“**当前感染状态**”列表中，选择以下选项之一：
     - **未扫描**
     - **未受感染**

- **恶意软件扫描检测到感染**
- **文件哈希搜索检测到感染**
- **全部**

5 单击“**扫描恶意软件**”。

注意：恶意软件扫描程序主机可以同时启动对三个映像的扫描。

---

6 启动扫描后，您可以看到“**恶意软件检测**”上的“**扫描状态**”，并看到以下字段：

- **未扫描**
- **未受感染**
- **受感染**
- **失败**

注意：验证失败的任何备份映像将被忽略。

- **进行中**
- **挂起**

4

管理凭据

本章节包括下列主题：

管理 AHV 群集凭据

此部分介绍了添加、更新和验证 AHV 群集凭据的过程。

添加新群集凭据

1. 在左侧，单击“**工作负载**”**>Nutanix AHV**，然后单击“**AHV 群集**”选项卡。
2. 单击“**添加**”以添加新群集。
3. 在“**添加 AHV 群集**”**>**“**关联凭据**”页面上，单击“**添加新凭据**”。
4. 在“**添加凭据**”页面上，输入“**凭据名称**”、“**用户名**”和“**密码**”等详细信息。
5. 单击“**下一步**”。

   选择或添加角色以便为凭据提供权限。
6. 单击“**保存**”。

注意：可以“**编辑**”或“**删除**”添加的凭据。

更新和验证 AHV 群集凭据

验证 AHV 凭据

1 在左侧，单击“**工作负载**”**> Nutanix AHV**，然后单击“**AHV 群集**”选项卡。

2
- 要验证特定群集的凭据，请找到并选择该 AHV 群集。然后，从“**凭据**”列或顶栏中单击“**验证**”。
- 要同时验证多个服务器的凭据，请找到并选择该 AHV 群集。然后，从顶栏中单击“**验证**”。

注意：NetBackup 将验证所选 AHV 群集的当前凭据。

如果凭据无效，NetBackup 会在“**凭据**”下指明“**无效**”。使用以下步骤更新 AHV 群集凭据。

更新 AHV 群集凭据

1 在左侧，单击“**工作负载**”**> Nutanix AHV**，然后单击“**AHV 群集**”选项卡。

2 找到并选择 AHV 群集。

3 选择“**操作**”**>**“**编辑**”。

4 根据需要更新凭据。

注意：添加或更新 AHV 群集凭据也会自动开始发现 AHV 群集。当在请求中提供备份主机信息时，将使用这些信息执行凭据验证以及发现。对于发现，NetBackup 9.1 是用作备份主机的 NetBackup 介质服务器或客户端支持的最低版本。

---

5 单击“**保存**”。

NetBackup 将验证所选 AHV 群集的更新凭据。

管理 Nutanix Prism Central 凭据

此部分介绍了添加、更新和验证 Nutanix Prism Central 凭据的过程。

添加新的 Nutanix Prism Central 凭据

1 在左侧，单击 **Nutanix AHV**，然后单击“**Prism Central 服务器**”选项卡。

2 单击“**添加**”可添加新的 Prism Central 服务器。

3 在“添加 **AHV Prism Central** 服务器”>“关联凭据”页面上，单击“添加新凭据”。

4 在“添加凭据”页面上，输入“凭据名称”、“用户名”和“密码”等详细信息。

5 单击“下一步”。

选择或添加角色以便为凭据提供权限。

6 单击“保存”。

注意：可以“编辑”或“删除”添加的凭据。

更新和验证 Nutanix Prism Central 凭据

验证 Prism Central **服务器凭据**

1 在左侧，单击 **Nutanix AHV**，然后单击“**Prism Central** 服务器”选项卡。

2
- 要验证特定 Prism Central 服务器凭据，请找到并选择该 Prism Central 服务器。然后，从“凭据”列或顶栏中单击“验证”。
- 要同时验证多个服务器的凭据，请找到并选择这些 Prism Central 服务器。然后，从顶栏中单击“验证”。

注意：NetBackup 将验证所选 Prism Central 服务器的当前凭据。

如果凭据无效，NetBackup 会在“凭据”下指明“无效”。使用以下步骤更新 Prism Central 服务器凭据。

更新 Prism Central **服务器凭据**

1 在左侧，单击 **Nutanix AHV**，然后单击“**Prism Central** 服务器”选项卡。

2 找到并选择 Prism Central 服务器。

3 选择“操作”>“编辑”。

4 根据需要更新凭据。

注意：添加或更新 Prism Central 服务器凭据也会自动开始发现 Prism Central 服务器。当在请求中提供备份主机信息时，将使用这些信息执行凭据验证以及发现。对于发现，NetBackup 9.1 是用作备份主机的 NetBackup 介质服务器或客户端支持的最低版本。

5 单击“**保存**”。

NetBackup 将验证所选 Prism Central 服务器的已更新凭据。

查看应用于资产的凭据名称

可以查看为资产类型配置的指定凭据。如果没有为特定资产配置凭据，则此字段为空。

查看 Nutanix AHV 群集的凭据

1 在左侧，选择“**工作负载**”**> Nutanix AHV**。

2 在“**AHV 群集**”选项卡上，找到“**凭据名称**”列。

编辑或删除指定的凭据

您可以在“**凭据管理**”中编辑指定凭据的属性，或删除指定的凭据 NetBackup。

编辑指定的凭据

可以编辑指定的凭据以更改以下内容：凭据标记、描述、类别、身份验证详细信息或权限。无法更改凭据名称。

注意：确保用于“**AHV 群集**”的凭据类别为 *AHV*，用于 **Nutanix Prism Central** 的凭据类别为 *Prism Central*。

编辑指定的凭据

1 在左侧，选择“**凭据管理**”。

2 在“**指定的凭据**”选项卡上，找到要编辑的凭据并选中对应的复选框。

3 选择“**编辑**”并根据需要更新凭据。

4 查看更改，然后选择“**完成**”。

删除指定的凭据

您可以删除不再需要与 NetBackup 一起使用的凭据。确保将其他凭据应用于使用待删除凭据的任何资产。否则，这些资产的备份和还原可能会失败。

删除指定的凭据

1 在左侧，选择“**凭据管理**”。

2 在“**指定的凭据**”选项卡上，找到要删除的凭据并选中对应的复选框。

3 选择“**删除**” > “**删除**”。

5

即时访问

本章节包括下列主题：

- 即时访问的前提条件
- 使用即时访问功能之前的注意事项和限制
- 创建即时访问 VM
- 从 VM 备份映像下载文件和文件夹
- 即时访问自建 (BYO)

即时访问的前提条件

如果使用即时访问，请确保 WORM 实例可以访问 AHV 群集服务器上的以下端口：

表 5-1 端口详细信息

实例	AHV 组件	端口号
WORM	AHV 群集服务器	9440

使用即时访问功能之前的注意事项和限制

请注意有关“即时访问虚拟机”功能的以下内容：

- 使用 NetBackup Web UI 或即时访问 API 从本地或云 LSU（逻辑存储单元）创建的备份副本支持此功能。
  有关云 LSU（逻辑存储单元）即时访问限制的更多信息，请参考《NetBackup 重复数据删除指南》。
- 从保护计划或策略创建的备份副本支持此功能。

- NetBackup Appliance、NetBackup Virtual Appliance、Flex Appliance 和自建 (BYO) 服务器均支持下载文件功能。

  Flex WORM 存储上的即时访问需要以下服务：

  - NGINX、NFS。SAMBA、WINBIND（如果需要 Active Directory）、SPWS、VPFS
- 此功能限于介质服务器重复数据删除池 (MSDP) 介质服务器或 WORM 存储服务器的 50 个并行装入点。如果具有 Flex Appliance，则此功能限于每个节点的 50 个并行装入点。
- 对于使用“**下载**”选项的文件或文件夹下载，以及创建 VM 即时访问功能，NetBackup Web UI 必须能够访问介质服务器，该介质服务器与主服务器用于连接到该介质服务器的名称或 IP 地址相同。
- 如果介质服务器设备使用第三方证书，则需要在使用此功能之前在 NetBackup 主服务器上创建某些配置。

  有关更多信息，请参考 NetBackup Appliance 安全指南中的“第三方证书”和“实施第三方 SSL 证书”部分。
- 在设备和 BYO Web 服务器 NGINX 中定义了 5-minutes-alive-session 阈值。选定进行下载的文件和文件夹必须在此阈值内进行压缩和下载。
- 在存储服务器和主服务器从早期 NetBackup 版本升级后，要确保即时访问有效运行，请使用以下命令重新启动已升级主服务器上的 NetBackup Web 服务：

  ```
  /usr/openv/netbackup/bin/nbwmc stop
  /usr/openv/netbackup/bin/nbwmc start
  ```
- 如果必须从 Windows VM 下载或还原文件或文件夹，请确保 Windows 注册表配置单元数小于10000。

  我们提供了关于注册表配置单元的更多信息。

限制

- 此功能不支持具有处于原始设备映射模式 (RDM) 或持久模式的磁盘的 VM。
- 对于 Windows 还原，不支持 ReFS 文件系统。
- 即时访问功能不支持 Windows 10 精简操作系统。要验证操作系统是否已压缩，请在备份 VM 之前，在命令提示符下运行 `compact "/compactos:query"`。要禁用压缩，请在备份 VM 之前，在命令提示符下运行 `"compact /compactos:never"`。然后，可以使用即时访问功能备份 VM。
- 即时访问功能不支持硬链接。如果从映像创建通用共享，并且映像具有硬链接文件，则 `vpfsd` 显示这些硬链接文件的大小为 0 字节。
- 对于 Linux VM，即时访问不支持镜像卷。

创建即时访问 VM

您可以从 NetBackup 备份映像创建即时访问 VM。该 VM 几乎立即可用，从而实现接近零恢复时间的目标。NetBackup 将 VM 的快照直接安装在备份存储设备上，以允许 AHV 群集将该快照视为正常 VM。

已安装的 VM 快照可用于各种用途。例如：

- 从 VM 恢复文件，或复制磁盘文件。
- 在 VM 上运行测试，例如测试修补程序。
- 故障排除或灾难恢复。
- 验证应用程序。

注意：自建 (BYO) 服务器支持此功能。此功能要求 NetBackup 备份映像存储在介质服务器重复数据删除池 (MSDP) 存储设备上。我们提供了有关使用即时访问 VM 的更多信息：

请参见第 50 页的"使用即时访问功能之前的注意事项和限制"。

创建即时访问 VM

1 在左侧，单击 **Nutanix AHV**。

2 找到并单击 VM。

3 单击“**恢复点**”选项卡，然后单击备份发生的日期。

可用映像显示在行中，其中每个映像都有备份时间戳。

4 在可以选择使用即时访问恢复的映像或映像副本上，单击“**恢复**”>“**创建即时访问虚拟机**”。

5 在“**恢复目标**”中查看“**还原至**”值。

默认值根据 VM 的备份映像填充。

- 要恢复到备用位置，请更改“**还原至**”选项中的默认群集。然后单击“**下一步**”。

注意：必须对存储容器或群集具有“**查看**”和“**查看还原目标**”权限，才能在目标下拉列表中列出预期的存储容器。

---

6 查看或更改“**恢复选项**”值。

创建新 VM ID 而非使用现有 ID	为 VM 创建新 ID，该 ID 不能与备份期间设置的现有值相同。 **注意：** VM ID 是 VM UUID。
在恢复后启动	在恢复完成后自动启动 VM。
启用迁移	自动将与即时访问 VM 关联的存储，从 NetBackup 存储移动到 Nutanix 群集的容器中。

7 查看或更改“高级”选项。

删除网络接口	删除备份期间为 VM 设置的网络接口。
保留 MAC 地址	保留备份期间为 VM 设置的 MAC 地址。

8 单击“**下一步**”运行“**恢复概览**”。

请参见第 85 页的“Nutanix AHV 的恢复前检查”。

9 单击“**启动恢复**”。

10 单击“**还原活动**”选项卡，以监控作业的进度。选择特定的作业，以查看其详细信息。

11 单击“**即时访问虚拟机**”选项卡，查看新 VM 的详细信息。

从 VM 备份映像下载文件和文件夹

您可以浏览 VM 的即时访问映像以下载文件和文件夹。

注意：我们提供了有关使用即时访问 VM 的更多信息：请参见第 50 页的“使用即时访问功能之前的注意事项和限制”。

从 VM 备份映像下载文件和文件夹

1 在左侧，单击 **Nutanix AHV**。

2 找到并单击 VM。

3 单击“**恢复点**”选项卡。在日历视图中，单击备份发生的日期。

可用映像成行列出，包含每个映像的备份时间戳。

4 在可以选择使用即时访问恢复的映像或映像副本上，单击“**恢复**”>“**下载文件和文件夹**”。

5 选择文件，然后单击“**添加**”以将文件添加到下载列表中。

单击文件夹可进行深入查看。使用文件夹路径导航回层次结构中的更高级别。

输入文件名可搜索文件。

下载列表将显示选定文件和文件夹以及每个文件的位置。

6 单击“**下一步**”。

7 创建下载软件包后，单击“**下载**”。

“**活动监视器**”选项卡将显示恢复状态。

即时访问自建 (BYO)

您可以自建 VM（使用 Red Hat Enterprise 操作系统）以支持 Nutanix AHV 即时访问。可以使用以下功能：

- 创建即时访问 VM。
- 将数据磁盘迁移到 Acropolis 操作系统 (AOS) 群集。
- 下载文件和文件夹。

要将即时访问用于在早期 NetBackup 版本中创建的 BYO VM，必须升级到 NetBackup 11.0 或更高版本。

即时访问自建 (BYO) 的前提条件

前提条件（全新安装和升级）：

- 装有 Red Hat Enterprise Linux 7.6 及更高版本的 BYO 存储服务器，与 NetBackup Appliance 操作系统版本相同。
- 安装了 docker/podman 的 BYO 存储服务器。
  - 该 docker/podman 版本必须与相应的正式 RHEL 版本中的 docker/podman 版本相同。需要从相应的 RHEL yum 源 (RHEL extra) 安装该版本。
  - 该 docker/podman 应用程序包含在环境路径中。
- 安装了 NFS 服务的 BYO 存储服务器。
- 安装了 NGINX 版本的 BYO 存储服务器。

- 该 NGINX 版本必须与相应的正式 RHEL 版本中的 NGINX 版本相同。需要从相应的 RHEL yum 源 (epel) 安装该版本。
- 确保从同一 RHEL yum 源（RHEL 服务器）安装 `policycoreutils` 和 `policycoreutils-python` 软件包，然后运行以下命令：
  - `semanage port -a -t http_port_t -p tcp 10087`
  - `setsebool -P httpd_can_network_connect 1`
- 确保存储服务器上的 /mnt 文件夹不直接由任何装入点装入。装入点应装入其子文件夹。
- 使用以下命令在 selinux 中启用 logrotate 权限：
  `semanage permissive -a logrotate_t`

- 对于 BYO，docker/podman 容器用于浏览 VMDK 文件。与容器相关的数据存储在下列位置：`/var/lib/` 且至少需要 20 GB 的可用空间。

即时访问自建 (BYO) 的硬件配置要求

表 5-2 硬件配置要求

CPU	内存	磁盘
■ 最低 2.2 GHz 时钟速率。 ■ 64 位处理器。 ■ 最少 4 个核心；建议使用 8 个核心。对于 64 TB 存储，Intel x86-64 体系结构需要八个核心。 ■ 在 CPU 配置中启用 VT-X 选项。	■ 16 GB（对于 8 TB 到 32 TB 的存储 - 为 1 TB 的存储分配 1 GB RAM）。 ■ 对于 32 TB 以上的存储，需要 32 GB RAM。 ■ 对于每个实时装入，还需要 500 MB RAM。	磁盘大小取决于备份大小。 请参考 NetBackup 和介质服务器重复数据删除池 (MSDP) 的硬件要求。

常见问题

以下是即时访问自建 (BYO) 的一些常见问题。

表 5-3 常见问题

常见问题	回答
在未安装 docker/podman 的情况下，配置或升级存储后，如何在 BYO 上启用即时访问文件浏览（用于文件下载和还原）？	按以下顺序执行步骤： 1 安装所需的 docker/podman 版本。 2 开始使用即时访问功能。 例如，可以下载文件、还原文件等。

常见问题	回答
在未安装 NGINX 服务的情况下，配置或升级存储后，如何在 BYO 上启用 Nutanix AHV 即时访问功能？	按以下顺序执行步骤： 1 安装所需的 nginx 服务版本。 2 请确保新的 BYO nginx 配置条目 `/etc/nginx/conf.d/byo.conf` 是原始 `/etc/nginx/nginx.conf` 文件 HTTP 部分的一部分。 3 运行命令 令：`/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`
如何解决 vpfs-config.log 文件中由 `Verifying that the MSDP REST API is available via https on port 10087` 引发的以下问题：	按以下顺序执行步骤： 1 通过 yum 工具安装 `policycoreutils` 和 `policycoreutils-python` 软件包。 2 添加 SELinux 在 10087 端口上绑定 Nginx 所需的以下规则。 ■ `semanage port -a -t http_port_t -p tcp 10087` ■ `setsebool -P httpd_can_network_connect 1` 3 运行以下命令 令：`/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`

常见问题	回答
对 BYO 的即时访问默认使用自签名证书且仅支持 *.pem 外部证书。 如何将其替换为外部 CA 签名的证书（*.pem 证书）（如果需要）？	要配置外部证书，请执行以下步骤。如果已生成新证书（证书必须包含介质服务器的长主机名和短主机名），请转到步骤 4。 1 创建 RSA 公钥或私钥对。 2 创建证书签名请求 (CSR)。 证书必须包含介质服务器的长主机名和短主机名。 3 外部证书颁发机构会创建证书。 4 将 `<PDDE Storage Path>/spws/var/keys/spws.cert` 替换为证书，并将 `<PDDE Storage Path>/spws/var/keys/spws.key` 替换为私钥。 5 运行以下命令以重新加载证书： `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`
如何为 gnome 中的即时访问实时装入共享禁用介质自动装入？ 如果已启用自动装入，则会从 gnome 中的实时装入共享装入源文件夹，并显示较小的磁盘。在这种情况下，即时访问功能无法正常运行。 装入的磁盘内容源为实时装入共享下的 `.../meta_bdev_dir/...` 文件夹，而装入目标位于 `/run/media/...` 文件夹。	按照准则禁用 gnome 自动装入： https://access.redhat.com/solutions/20107

常见问题	回答

如何能够解决 `/var/log/vpfs/vpfs-config.log` 文件中的以下问题?
 	
`**** Asking the NetBackup Webservice to trust the MSDP webserver (spws) **** /usr/openv/netbackup/bin/nblibcurlcmd failed (1):`
	按以下顺序执行步骤：
	
	1 确保 NetBackup 主服务器已启动，并且没有防火墙阻止 NetBackup 主服务器与存储服务器之间的连接。
	
	2 在存储服务器上运行以下命令以验证连接状态：
	
	`/usr/openv/netbackup/bin/bpclntcmd -pn`
	
	3 NetBackup 主服务器已启动并允许 NetBackup 主服务器与存储服务器之间的连接后，运行以下命令：
	
	`/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`

6

保护 AHV 虚拟机

本章节包括下列主题：

保护 AHV 虚拟机之前的注意事项

创建保护计划期间，需要注意一些验证：

- 如果日程表类型为“自动”，请确保所有 NetBackup 版本都如下所述：
  - 只有备份主机版本 8.3 或更高版本支持增量式计划。
  - 如果将 Windows 计算机充当备份主机，请确保版本为 9.1 或更高版本。

- 如果要使用“启用虚拟机静默”选项，请确保备份主机版本为 9.1 或更高版本。
- 如果智能 VM 组的类别属性为过滤器，则备份主机版本应为 10.4 或更高版本。

- 要保护 Nutanix Prism Central 相关的 VM 属性，需要 Nutanix Prism Central 配置。

注意：要保护 Nutanix Prism Central 相关的 VM 属性，请确保 NetBackup 主机版本为 10.1.1 或更高版本。

- Cohesity 建议在保护虚拟机或智能组时使用保护计划或策略。
- Cohesity 建议在恢复 API 中使用 `backupId` 作为恢复点，而不使用 `client` 和 `filter`。

注意：要使用策略保护 AHV VM，请确保 NetBackup 主服务器、介质服务器、客户端/备份主机已升级到 NetBackup 11.0 或更高版本。

使用保护计划保护 AHV VM 或智能 VM 组

使用以下过程可为资产（AHV VM 或智能 VM 组）订购保护计划。为资产订购保护计划时，为资产分配预定义的备份设置。

注意：分配给您的 RBAC 角色必须提供相应的访问权限，使您可以访问要管理的资产以及要使用的保护计划。如果对智能 VM 组进行保护，请确保构成该组的所有群集均具有保护权限。

要保护 AHV VM **或** VM **组，请执行以下操作：**

1. 在左侧，单击“**工作负载**”**> Nutanix AHV**。
2. 在“**虚拟机**”选项卡或“**智能 VM 组**”选项卡上，单击 VM 或 VM 组对应的框，然后单击“**添加保护**”。
3. 选择保护计划，然后单击“**下一步**”。
4. 用户可以调整以下一个或多个设置：
   - **日程表和保留**
     更改备份启动时段。
   - **备份选项**

选择要用于备份的服务器或主机。

注意：如果此处选择了“**自动**”选项，并且此保护计划用于保护类别为过滤器的智能 VM 组，请确保至少有一台与存储单元关联的 10.4 或更高版本的介质服务器。

- **高级选项**
  为保护计划启用虚拟机静默。

5 单击“**保护**”。

所选内容的结果将显示在“**虚拟机**”或“**智能 VM 组**”下。

使用策略备份 AHV VM 或智能组

下面是使用策略保护 Nutanix-AHV 资产的过程。

配置策略以备份资产的步骤

1 登录到 NetBackup Web UI。

2 单击“**保护**”，然后单击“**策略**”。

3 单击“**添加**”。将显示“创建策略”页面。

4 在“**属性**”选项卡上，执行以下操作：

- 指定“**策略名称**”。
- 选择 Nutanix-AHV 作为“**策略类型**”。
- 根据需要配置其他值。

5 在“**日程表**”选项卡上，单击“**添加**”，然后指定备份日程表参数。

6 单击“**虚拟机**”选项卡，然后选择“智能组”或“单个虚拟机”选项。

7 单击 **Nutanix-AHV** 选项卡，然后选择要备份的服务器或主机。

8 单击“**创建**”。

保护 VPC 内的 AHV VM

在 NetBackup 10.2 版本中，Nutanix Prism Central 服务器内托管在虚拟专用网络上的虚拟机可以受到保护。此外，NetBackup 还使用配置的 Nutanix Prism Central 保护 VM 的以下属性。

- **项目**：具有一组通用要求或通用结构和功能的一组用户。项目提供用于管理资源使用情况的用户角色的逻辑分组。
- **关联类别**：类别是将实体分组到键值对中。通常，会根据某些条件将新实体分配到某个类别。然后，策略可以绑定到分配有特定类别值（按特定类别值分组）的实体。
- **VPC 网络属性**：分配给 VPC 内 VM 的主 IP 和辅助 IP。
- **项目所有者**：在 Nutanix Prism Central 内共同部署 CALM 的项目用户/所有者。

保护 VPC **上的** VM

1 配置 Nutanix Prism Central。

注意：对于配置的群集，仅当选中“**使用 Prism Central**”复选框时，NetBackup 才使用 Nutanix Prism Central 保护 VM 的其他属性。

请参见第 28 页的“添加新的 Nutanix Prism Central”。

2 在 NetBackup 中添加所有 Nutanix AHV 群集，并选中“**使用 Prism Central**”复选框。

请参见第 24 页的“添加或浏览 AHV 群集”。

3 有关保护 VM 的完整信息，请参见以下部分：

请参见第 60 页的“使用保护计划保护 AHV VM 或智能 VM 组”。

注意：如果在保护计划中针对“选择用于备份的服务器或主机”选择“**自动**”选项，并且存储单元与低于 10.2 版本的 NetBackup 介质服务器关联，则备份作业可能会使用更低版本的介质服务器作为备份主机。

在这种情况下，备份作业完成后不会保护 Nutanix Prism Central 属性。

保护已启用 AHV VM 的 vTPM

可信平台模块 (TPM) 用于管理安全服务的加密密钥，如加密和硬件（及软件）的完整性保护等服务。AHV 虚拟可信平台模块 (vTPM) 是基于软件的 TPM 2.0 规范模拟，可作为虚拟设备运行。

NetBackup 使用 Nutanix-AHV 策略和 Nutanix 保护计划保护启用了 vTPM 的 VM。

必须配置 Nutanix Prism Central 和 Prism 群集凭据。

请参见第 28 页的“添加新的 Nutanix Prism Central”。

请参见第 45 页的“管理 AHV 群集凭据”。

限制

- Nutanix 不支持备份存储在 vTPM 中的信息。
- 计算机类型非 Q35 的 Nutanix VM 不支持 vTPM。

有关更多信息和建议，请参考 Nutanix 文档。

自定义 AHV 资产的保护设置

您可以自定义保护计划的某些设置，包括日程表。

自定义 AHV 资产的保护设置

1 在左侧，单击“**工作负载**”**> Nutanix AHV**。

2 执行以下操作之一：

- 编辑 VM 的设置
  在“**虚拟机**”选项卡上，单击要编辑的 VM。
- 编辑智能 VM 组的设置
  在“**智能 VM 组**”选项卡上，单击要编辑的组。

3 单击“**自定义保护**”**>**“**继续**”。

4 用户可以编辑以下一项或多项设置：

- 备份启动时段。
  请参见第 64 页的“日程表和保留”。
- **备份选项**
  请参见第 64 页的“备份选项”。

5 单击“**保护**”。

修改 AHV 资产的策略

本节详细介绍如何根据要求编辑策略。以下是编辑策略的过程。

编辑策略

1 在左窗格中，展开“**保护**”，然后单击“**策略**”。将显示“**策略**”页面。

2 选择所需的策略，然后单击“**编辑**”。将显示“**编辑策略**”页面。

3 修改所需的值，然后单击“**保存**”。

日程表和保留

- 启动时段。
  - 设置可以启动备份的时段。

备份选项

用户可以调整以下设置以订购保护计划。

1 选择要用于备份的服务器或主机作为访问主机。

代表虚拟机执行备份的主机。用户可以选择“自动”，以允许 NetBackup 根据存储单元选取介质服务器。或者，用户可以从列表中选择另一台主机。这些主机是环境中的其他介质服务器或配置为访问主机的主机。

注意：在使用 9.1 之前版本的备份主机备份 VM 期间，如果不同群集中存在具有同一 UUID 的 VM，则此 VM 的“**上次成功备份**”状态列不会更新。但是，VM 备份成功，您可以查看恢复点并进行恢复。

---

2 **高级选项**

要启用，请参见第 64 页的“启用虚拟机静止的前提条件”。

- **启用虚拟机静默**
- **如果静默快照失败，则启用未静默快照。**

默认情况下，NetBackup 创建快照之前，虚拟机上的 I/O 处于静默状态。在大多数情况下，应使用此默认设置。如果不静默文件活动，就无法保证快照的数据一致性。如果禁用静默，则必须分析备份数据以确保一致性。

启用虚拟机静止的前提条件

- 默认情况下，对于在 Nutanix 群集中运行的 VM，Nutanix 访客工具 (NGT) 功能处于禁用状态。Nutanix 建议安装 NGT，并且在某些情况下，计划创建已启用虚拟机静止的应用程序一致快照时，VM 上具有 pre-freeze 和 post- thaw 脚本。

注意：需要使用 NetBackup 介质服务器 9.1 版或更高版本进行应用程序一致备份。

- 要安装 NGT 并添加脚本，请参见此处。

从 VM 或智能 VM 组中删除保护

可以为 VM 或智能 VM 组取消订购保护计划。为资产取消订购计划后，将不再执行备份。

注意：为资产取消订购保护计划时，资产可能会在 Web UI 的“**受以下对象保护**”列中显示“**传统策略**”。为资产订购保护计划并对该资产运行备份时，可能会发生这种情况。然后，在资产具备有效备份映像时，为资产取消订购保护计划。Web UI 显示“**传统策略**”，但可能存在也可能不存在保护资产的活动策略。

从 VM 或智能 VM 组中删除保护

1 在左侧，单击“**工作负载**”**> Nutanix AHV**。

2 在“**虚拟机**”选项卡或“**智能 VM 组**”选项卡上，选择 VM 或智能 VM 组。

3 单击“**删除保护**”**>**“**是**”。

在“**虚拟机**”或“**智能 VM 组**”下，资产将列为“**不受保护**”。

查看 VM 或智能 VM 组的保护状态

可以查看用于保护 VM 或智能 VM 组的保护计划。

查看 VM 或智能 VM 组的保护状态

1 在左侧，单击“**工作负载**”**> Nutanix AHV**。

2 在网格上，单击“**显示或隐藏列**”。单击“**受策略保护**”。

3 在“**虚拟机**”选项卡或“**智能 VM 组**”选项卡上，选择 VM 或智能 VM 组。

“**保护**”选项卡显示资产订购计划的详细信息。

注意：如果资产已备份，但状态却指示尚未备份，请参见请参见第 97 页的“新发现的 VM 的状态错误”。

4 如果资产未受保护，请单击“**添加保护**”以选择保护计划。

请参见第 60 页的“使用保护计划保护 AHV VM 或智能 VM 组”。

7

恢复 AHV 虚拟机

本章节包括下列主题：

恢复 AHV 虚拟机之前的注意事项

确保恢复或备份主机可以通过端口 9440 与 AHV 群集和 Prism Central 服务器（如果已安装）进行通信。

关于恢复前检查

恢复前检查将验证以下内容：

- 是否使用受支持的字符以及显示名称长度。
- 是否存在具有相同显示名称的 VM。
- 是否与 AHV 服务器连接以及 AHV 凭据验证。
- AHV 群集是否可用。
- 存储容器的可用空间。

恢复 AHV 虚拟机

可以将 VM 恢复到原始备份位置，也可以将其恢复到其他位置。可以选择从备份映像的默认副本恢复，也可以选择从备用副本（如果存在）恢复。默认副本也称为主副本。

恢复 VM

1 在左侧，单击“**工作负载**”**> Nutanix AHV**。

2 找到并单击 VM。

3 单击“**恢复点**”选项卡。在左侧的日历视图中，单击以绿点指示的备份发生的日期。

可用映像以行的形式列出，并且每个映像都具有备份时间戳。

4 在要恢复的映像上，选择以下映像恢复选项之一：

- **恢复**
  从备份映像的默认副本恢复。
- **从默认副本中恢复**
  从备份映像的默认副本恢复。如果存在多个副本，则会显示此选项。
- **nn 个副本**
  从备份映像的默认副本或其他副本恢复。NetBackup 允许最多创建同一备份映像的 10 个副本。选择此选项时，将显示所有可用副本。对于每个副本，将显示“**存储名称**”、“**存储服务器**”和“**存储服务器类型**”。对于要恢复的副本，单击“**恢复**”。

5 在“**恢复目标**”中查看“**还原至**”值。

默认值根据 VM 的备份映像填充。

- 要恢复到备用位置，请更改“**还原至**”选项中的默认群集。然后单击“**下一步**”。

注意：必须对存储容器或群集具有“**查看**”和“**查看还原目标**”权限，才能在目标下拉列表中列出预期的存储容器。

6 查看或更改“**恢复选项**”值。

允许重写现有虚拟机	删除目标上具有相同显示名称的任何 VM。必须在恢复开始之前删除该 VM。否则，恢复将失败。
在恢复后启动	在恢复完成后自动启动 VM。
恢复主机	指示要用于执行恢复的主机。默认情况下，恢复主机是执行备份的主机。
创建新 VM ID 而非使用现有 ID	为 VM 创建新 ID，该 ID 不能与备份期间设置的现有值相同。 **注意：** VM ID 是 VM UUID。
从快照还原 VM	允许从快照还原 VM。 **注意：**如果快照不可用，则从备份映像还原 VM。

7 查看或更改“**高级**”选项。

删除网络接口	删除网络接口（对于在同一 AHV 服务器的不同群集上的备用还原无效） **注意：** 要还原到备用位置，必须选择此选项。
保留 MAC 地址	保留备份期间为 VM 设置的 MAC 地址。

8 单击“**下一步**”运行“**恢复概览**”。

这将对恢复目标和恢复选项页面中提供的值运行恢复前检查。检查 AHV 群集和存储容器是否连接以及是否存在。确定存储容器是否有可用空间，并检查其他要求。

请参见第 85 页的“Nutanix AHV 的恢复前检查”。

9 单击“**启动恢复**”。

10 单击“**还原活动**”选项卡，以监控作业的进度。选择特定的作业，以查看其详细信息。

在 VPC 中恢复 AHV VM

在 VPC 上恢复 VM 具有下面列出的某些限制：

- 对于备用还原，如果选中“**删除网络接口**”复选框，则还原操作将成功。但是，不会还原项目、类别、所有者信息和 VPC 相关信息等属性。
- 如果触发备份时 VM 中配置了网络，并且用户尝试使用此备份映像进行备用还原，但未选中“**删除网络接口**”复选框，则还原操作将失败。
- 如果在触发备份时 VM 已配置项目，但在触发还原时项目不存在，则还原作业将失败。
- 如果在触发备份时 VM 已配置类别，但在触发还原时类别不存在，则还原作业将失败。
- 在还原时，如果 Nutanix Prism Central 服务器或项目中不存在 VM 用户，则还原操作将失败。
- 仅考虑还原类型为 ASSIGNED 的 IP 地址。已识别的 IP 类型将被忽略，用户必须在还原后手动配置 IP。
- 如果 VM 具有启用了 Span 端口的 NIC，则在还原后，会将其忽略。必须使用 Nutanix CLI 在 NIC 上手动添加和配置 Span 端口。
- 如果已执行原始位置还原，则会还原 VM 以及项目、类别、所有者详细信息和其他与 VPC 相关的属性。
- 尝试备份/还原已从一个 Prism Central 移动到另一个 Prism Central 的群集的 VM 时，会出现未定义的行为。
- 需要版本为 10.2 或更高版本的备份主机来备份/还原项目、类别和其他虚拟私有云 (VPC) 相关属性。如果使用版本低于 10.2 的备份主机，则在 VPC 环境中不存在 VM 时，备份/还原将完成而不捕获与 VPC 相关的属性。如果 VM 位于 VPC 环境中，并且通过版本低于 10.2 的备份主机触发还原，则还原可能会失败。

恢复已启用 vTPM 的 AHV VM

NetBackup 为已启用 vTPM 的 AHV VM 恢复 vTPM 配置。

必须配置 Prism Central 和 Prism 群集凭据。

请参见第 28 页的“添加新的 Nutanix Prism Central”。

请参见第 45 页的“管理 AHV 群集凭据”。

要恢复已启用 vTPM 的 VM，请参考以下部分：

请参见第 67 页的“恢复 AHV 虚拟机”。

限制

- Nutanix 不支持恢复存储在 vTPM 中的信息。
- 计算机类型非 Q35 的 Nutanix VM 不支持 vTPM。

- 即时访问 VM 还原不支持 vTPM 配置还原。

关于 Nutanix AHV 无代理文件和文件夹还原

NetBackup 9.1 及更高版本支持 Nutanix AHV 无代理文件和文件夹还原。它可用于将单个文件或文件夹还原到任何目标主机。目标主机可以是托管在 AHV 或其他虚拟机管理程序上的虚拟机，甚至是未安装客户端 NetBackup 的物理机。此还原使用匹配目标主机平台的 VxUpdate 软件包，在目标主机上部署 NetBackup 恢复工具。完成还原过程后，无代理文件和文件夹还原将会清理恢复工具和暂存位置。恢复过程使用 NetBackup 主机作为恢复主机，其通过网络与目标主机相连。此恢复主机可以是 NetBackup 服务器或客户端。

文件和文件夹还原过程概述

1. NetBackup 主服务器接收来自 NetBackup Web UI 或无代理恢复 API 的输入。该输入为要还原的文件或文件夹以及目标主机凭据。所需的凭据为：
   - Windows：如果 UAC 已禁用，则用户必须属于本地管理员组。如果启用了 UAC，则用户必须是域用户，已添加到本地管理员组中。
   - Linux：用户必须是具有所有权限的 root 或 sudoer 用户。
2. 主服务器将请求的数据发送到恢复主机。
3. 恢复主机确认它具有执行还原所需的 VxUpdate 恢复软件包。如果没有，恢复主机将从使用 VxUpdate 的主服务器下载所需的软件包。
4. 恢复主机将 VxUpdate 软件包的恢复工具复制到目标主机。Linux 恢复和目标主机使用 SSH 协议执行恢复操作。Windows 恢复和目标主机使用 WMI、SMB 协议执行恢复操作。
5. 包含要还原的文件和文件夹的数据流文件暂存在恢复主机上的暂存位置。
6. 在恢复主机暂存位置创建的文件将复制到目标主机上的暂存位置。
7. 调用恢复工具，恢复所选文件或文件夹以及 ACL 和元数据详细信息。
8. NetBackup 执行必要的清理，即使还原操作成功/失败。存储在目标主机和恢复主机上暂存位置的所有临时文件都将删除。但是，如果出现故障，则以默认配置将证据从目标主机采集到恢复主机。
9. NetBackup 支持使用以下平台作为目标主机操作系统，以进行无代理文件还原：
   - Windows
   - Red Hat Enterprise Linux (RHEL)
   - SUSE Linux (SLES)
   - Ubuntu

有关目标主机操作系统版本的可支持性，请参见 NetBackup 软件兼容性列表 - 8.1 及更高版本中的“NetBackup 客户端”部分。

恢复无代理文件和文件夹的前提条件

仅当源 AHV VM 在指定的操作系统（如 Red Hat Linux、SUSE Linux、Ubuntu 或 Windows）上运行时，才能执行文件或文件夹恢复。此外，要从完全无代理 VM 备份创建文件系统映射，文件系统必须兼容。有关 AHV 兼容性，请参见虚拟环境中对 NetBackup 的支持。

注意：如果需要为不受支持的操作系统提供单个文件和文件夹还原支持，请使用 NetBackup 标准策略类型保护此类 VM。

表 7-1 恢复文件和文件夹的前提条件

步骤概述	说明和参考
基于代理的还原	■ 如果目标主机安装了 NetBackup 客户端或服务器，则执行基于代理的还原。 ■ 对于 Windows，此类客户端或服务器的 NetBackup 版本必须为 8.1 及更高版本，对于 Linux，必须为 8.2 及更高版本。 **注意：**如果选择 Linux 版本 8.1 或更早版本，将显示无代理还原选项。 ■ 对于基于代理的还原，必须在目标主机中指定 NetBackup 配置的主机名。 ■ 如果登录的 NetBackup 用户具有足够的权限，您可以浏览 NetBackup 主机的列表并选择一个用于还原文件或文件夹。如果登录的用户没有足够的 RBAC 权限，则需要手动指定目标主机。 ■ 对于基于代理的还原，必须在目标主机中指定 NetBackup 配置的主机名或 IP。 如果源 AHV VM 在 Linux 平台上运行，可以将文件或文件夹还原到任何受支持的 Linux 平台目标主机。 **注意：**如果已从目标主机卸载 NetBackup，仍然可以启动基于代理的还原，但会失败。

步骤概述	说明和参考
无代理还原	如果目标主机未安装 NetBackup 客户端或服务器，则执行无代理还原。 ■ 您需要指定目标主机 FQDN 或 IP 地址。 ■ NetBackup 从 NetBackup 配置中检测主机是否为非 NetBackup 计算机，并显示无代理还原选项。 **注意：** IPv4 和 IPv6 IP 地址均受支持。在 IPv6 中，不支持标准 CIDR 格式。
目标主机	■ 目标主机是要从 AHV VM 备份还原文件或文件夹的主机。主机名必须采用 FQDN 格式或 IP 地址。 ■ 可以选择将文件或文件夹还原到任何目标主机，该主机部署在 AHV、其他虚拟机管理程序或者甚至物理主机上。 **注意：** 确保可从恢复主机访问目标主机。 ■ 源和目标主机平台必须同类。Windows 源的主机文件可以还原到 Windows 目标主机上，Linux 源的 VM 文件可以还原到 Linux 目标主机上。 ■ 目标主机上的默认目标主机暂存目录为用户主目录。您可以提供自定义暂存位置。 前提条件： ■ NetBackup 不会创建目标主机暂存位置，该位置必须存在并具有写入和执行权限。 ■ 目标主机暂存位置必须有足够的空间用于还原操作。这包括还原文件大小、NetBackup 还原软件包（对于 Windows，约为 150 MB；对于 Linux，约为 100 MB）和 NetBackup 操作日志空间。 **注意：** 如果暂存位置路径位于系统驱动器上，则必须为其他正在运行的进程留出足够空间。

步骤概述	说明和参考
Linux 目标主机	■ 无代理目标计算机必须在受支持的操作系统平台上运行。有关 AHV 兼容性，请参见虚拟环境中对 NetBackup 的支持 ■ Tar 实用程序应位于目标主机上的默认路径中，并且路径已添加到系统路径变量中。 ■ NetBackup 仅支持 ASCII 格式的主机名。对于采用非 ASCII 格式的主机名，可以使用 IP 地址作为目标主机。 ■ 您可以配置与目标主机的最大 SSH 连接数，默认值为 10。 ■ 恢复主机和目标主机之间的 SSH 端口应打开。如果配置了任何防火墙，则 SSH 端口应在防火墙的例外列表中。 ■ 要还原到目标主机上的网络路径，请提供正确的导出权限。例如，`rw`、`sync`、`no_root_squash`。

步骤概述	说明和参考
SSH 连接要求	■ 到 Linux 目标主机的无代理还原使用 SSH 服务来执行。它必须在目标主机上运行。 ■ 目标主机上的 SSH 通信超时必须大于 5 分钟。 ■ 使用 SSH 与目标主机通信时，NetBackup 使用密码 `aes256-ctr`。 ■ SSH 版本必须为 1.2 或更高版本。 ■ 支持自定义 SSH 端口。 **注意：**默认 SSH 端口为 22。 ■ 支持以下项： ■ 密钥交换算法： ■ `diffie_helman_group_exchange_sha256` ■ `ecdh_sha2_nistp256` ■ `cdh_sha2_nistp384` ■ `ecdh_sha2_nistp521` ■ `diffie_helman_group14_sha1` ■ 主机密钥 ■ `ssh-rsa` ■ `ssh-dss` ■ `ecdsa-sha2-nistp256` ■ `ecdsa-sha2-nistp384` ■ `ecdsa-sha2-nistp521` ■ 哈希方法 ■ `sha256 Hex encoded`

步骤概述	说明和参考
SUDO 用户还原	■ Linux 目标主机上必须已存在 Sudo 用户。 ■ 确保已在 sudoers 文件中配置非 root 用户。 示例： ■ `<sudo-username> ALL = (ALL)` ■ `<sudo-username> ALL = (ALL) NOPASSWD` ■ 必须在 sudoers 文件中为非 root 用户配置单个条目。 ■ Linux sudo 用户必须拥有自定义暂存位置的所有权以及读取、写入和执行权限。 可以使用 SSH 私钥代替密码。 请参见第 79 页的“SSH 密钥指纹”。

步骤概述	说明和参考
Windows 目标主机	

步骤概述	说明和参考

	■ 无代理目标计算机必须在受支持的操作系统平台上运行。有关 AHV 兼容性，请参见虚拟环境中对 NetBackup 的支持。
	■ 必须配置 WMI，并确保恢复主机和目标主机均可访问 WMI。有关 WMI 和 SMB 要求，请参见 https://www.veritas.com/support/en_US/article.100040135。
	■ 接受 ASCII 格式的主机名。对于 Unicode 主机名，请使用 IP 地址而不是主机名。
	■ Windows 主机上必须运行以下服务：
	  ■ DCOM
	  ■ RPC
	  ■ WMI
	  ■ 文件和打印机共享
	■ 默认情况下，主机上会启用“**管理员共享**”。如果已禁用，从 GPO 中，用户需要在暂存位置驱动器或暂存位置所在的驱动器上启用“管理员共享”。
	注意：默认情况下，管理员用户具有访问 WMI 和 DCOM 所需的权限。如果 DCOM 和 WMI 权限出现任何问题，请参考 Microsoft 文档。
	  ■ 用于分配 DCOM 和 WMI 权限的用户或组：
	  在分配 **DCOM** 和 **WMI** 权限的两种方法中，使用以下选项之一：
	  ■ 用户必须属于管理员组，所以您可以将权限分配给管理员组。
	  ■ 将权限分配给特定用户。
	■ 支持 UAC 和非 UAC 环境：
	  ■ 目标主机本地管理员组中添加的内置管理员和域用户具有执行无代理还原所需的权限。
	  注意： UAC 远程限制：对于管理员组中的本地用户，建议使用基于代理的还原。但是，用户仍可以通过禁用 UAC 过滤来执行无代理还原。
	  要禁用 UAC 远程限制，请参见此处
	■ **暂存位置**要求：
	  ■ 默认位置为用户主目录，如果提供自定义路径，则用户必须有权访问该路径。
	  ■ 必须为绝对路径。
	  注意：不支持软链接、硬链接、网络路径等。
	  ■ 它应有足够的空间用于还原操作，包括：
	  ■ 还原文件大小。
	  ■ NetBackup 还原软件包（约 150 MB）。

步骤概述	说明和参考
	■ NetBackup 操作日志空间。根据详细级别，日志要求将有所不同。 **注意：**如果此路径位于系统驱动器上，则必须为其他正在运行的进程留出足够空间。 ■ 路径的最大字符限制为 260。但是，NetBackup 大约需要 110 个字符来构成临时位置。因此，应选择少于 150 个字符的路径。 ■ 如果暂存位置和还原位置位于同一驱动器上，则可能需要双倍的还原大小空间。 ■ 支持同一用户的并行还原作业。但是，如果指定了相同的目标文件夹，则还原的数据可能状态不一致。
WMI 和 SMB 要求	■ 到 Windows 目标主机的无代理还原使用 Windows Management Instrumentation (WMI) 和服务器消息块 (SMB) 协议。 ■ 确保在防火墙设置中打开 WMI 和 SMB 端口。 ■ 默认 DCOM 端口 135 ■ 默认 SMB 端口 445 ■ 动态端口 49152-65535 **注意：**您的环境也可以具有静态固定端口。 ■ 通过启用 SMB 加密对基于 SMB 的数据传输进行加密。有关更多详细信息，请参考 Microsoft 文档。 ■ 支持 SMB 版本 3.0。如果您的主机版本较旧，您可以将其禁用。请参考 Microsoft 指南。

步骤概述	说明和参考
恢复主机	恢复主机是安装了 NetBackup 介质服务器/客户端的主机，用于与提供的目标主机进行通信。 ■ 具有 NetBackup 9.1 及更高版本的恢复主机必须与目标主机建立连接。 ■ Linux 恢复主机必须与 Linux 目标主机建立 SSH 连接，Windows 恢复主机必须与 Windows 目标主机建立 WMI 和 SMB 连接。 ■ 恢复主机必须为同类平台。将文件从 Windows AHV VM 还原到目标 Windows 主机时，需要 Windows 恢复主机。同样，将文件从 Linux AHV VM 还原到目标 Linux 主机时，需要 Linux 恢复主机。 **注意：** 要将文件还原到 Ubuntu 目标主机，请使用 RHEL 或 SUSE 作为恢复主机。 ■ 仅支持具有 NetBackup 9.1 服务器或客户端的恢复主机。 ■ 如果导出权限正确，则恢复主机上作为暂存位置的网络路径有效。例如，`rw`、`sync`、`no_root_squash`。 ■ 恢复主机上的默认暂存位置为： ■ 对于 Linux：`/{install-path}/openv/var/tmp/staging` ■ 对于 Windows：`{install-path}\NetBackup\Temp\staging` ■ 可以使用 `bpsetconfig` 更改默认暂存位置。 ■ 执行 `<NetBackup path>/bin/admincmd/bpsetconfig`。 ■ 设置 `AGENTLESS_RHOST_STAGING_PATH = <Path>`。
其他	■ 确保在 /etc/ssh/sshd_config 文件中将 SUSE 目标主机的 `PasswordAuthentication` 设置为 `Yes`。然后，重新启动 ssh 服务。 **注意：** 默认情况下，SUSE 目标主机的 `passwordAuthentication` 值设置为 `No`。

SSH 密钥指纹

要获取 Linux 目标主机的 SSH 密钥指纹，请执行以下操作：

1 在 RHEL 或 SUSE 操作系统目标主机上使用以下命令来获取 `SHA256-based RSA` 密钥。

```
cat /etc/ssh/ssh_host_rsa_key.pub |awk '{print $2}' |base64 -d |sha256sum |
awk '{print $1}'
```

注意：命令的输出为 RSA 密钥。同样，更改公钥路径，执行该命令，以获得在目标主机上配置的 ecdsa 或 DSS SSH 密钥指纹。

- RSA 密钥示例：

```
cat /etc/ssh/ssh_host_rsa_key.pub |awk '{print $2}'|base64 -d
 |
sha256sum |awk '{print $1}'
```

- 命令输出：

```
b2352722053ac9f40bc1XXXXXXXXXXXXXXXXXXXXXXXXXX419fa241ba9431fd6b9
```

2 复制 RSA 指纹。添加目标主机详细信息时，可以提供此 SSH 密钥指纹。或者，也可以在“**恢复主机**”页面上单击“**获取 SSH 密钥指纹**”，然后验证显示的 SSH 密钥指纹。

要生成 SSH 私钥，请执行以下操作：

1 在 Linux 目标主机上执行以下命令：

- `ssh-keygen -t rsa`
- `-t option supports "ecdsa | rsa | dss"`

2 必须在目标 `vm ~/.ssh/authorized_keys` 文件中添加/附加目标主机公钥。

使用 Nutanix AHV 无代理还原恢复文件和文件夹

使用 Nutanix AHV 无代理还原恢复文件和文件夹

1 确保目标主机已启动，并且通过网络连接到还原过程中要使用的恢复主机。

2 在左侧，单击“**工作负载**”**> Nutanix AHV**。

3 找到并选择包含要还原的文件和文件夹的 AHV VM。

此 VM 称为源 VM。

4 单击“**恢复点**”选项卡。在日历视图中，选择备份发生的日期。

5 可用映像以行的形式列出，并且每个映像都具有备份时间戳。

6 在要从中恢复的映像上，单击“**恢复**”**>**“**还原文件和文件夹**”。

7 在“**选择文件**”窗格中，指定要恢复的文件和文件夹，然后单击“**下一步**”。下文将这些文件或文件夹称为源文件或源文件夹。

8 单击“**下一步**”。

9 在“**恢复目标**”页面上，执行以下操作：

- 手动输入 IP/主机名。
- 如果需要，请在目标主机上输入暂存位置。
- 选择适当的文件还原选项。
- 选择正确的恢复主机。
- 根据操作系统类型添加正确的凭据。

请参见第 82 页的“恢复目标选项”。

10 在“**恢复选项**”页面上，从以下选项中进行选择：

- **将字符串附加到文件名**：将指定字符串附加到目标文件名的文件扩展名之前。此值仅适用于文件。
- **重写现有文件**：重写目标位置中的同名文件或文件夹。
- **在不跨越装入点的情况下还原目录**
- **为硬链接创建新文件**
- **重命名软链接的目标**

注意：“**为硬链接创建新文件**”和“**重命名软链接的目标**”选项只能将所有内容还原到其他目录。

11 单击“**下一步**”。

12 在“**审查**”页面上：“审查”页面显示恢复前检查的状态。NetBackup 执行恢复前验证，以确认还原作业是否使用您提供的输入成功运行。

请参见第 85 页的“Nutanix AHV 的恢复前检查”。

- 如果恢复前操作失败，将显示失败的可能原因。对于需要更正的特定输入，单击“**更改**”按钮。
- 如果恢复前检查成功，请单击“**启动恢复**”。

恢复目标选项

表 7-2 恢复目标选项

步骤概述	说明和参考
目标主机	■ 目标主机字段预填充了上次成功发现 VM 的各个 AHV 群集时，存储的源 AHV VM 主机名/IP。 **警告：**如果已安装 NetBackup 客户端，并为其配置了提供的主机名或 IP，则执行基于代理的还原。 ■ 如果要在另一 NetBackup 客户端上执行还原，请单击“搜索”，然后从列表中选择所需客户端。 **注意：**确保选择具有同类平台的客户端。 ■ 如果搜索选项不可用，请手动输入目标主机。 ■ 如果要在未安装 NetBackup 客户端的主机上执行还原，请在目标主机中输入主机 FQDN 或 IP。将显示“**无代理还原**”选项。
无代理还原选项	■ **更改目标主机上的暂存位置**：如果要提供默认暂存位置以外的其他暂存位置，请输入所需的路径。暂存位置路径必须仅包含 ASCII 字符。 **注意：**默认暂存位置为用户主目录。 ■ **文件还原选项**：根据要求，选择以下适当的文件还原选项之一： ■ **将所有内容还原到原始目录** ■ **将所有内容还原到不同目录**提供不同的还原目录路径。 ■ **精简现有目录结构**：选择此选项，可在从不同目录选择文件时将所有内容还原到单个目录，而不创建任何子文件夹。

步骤概述	说明和参考
恢复主机	■ “**恢复主机**”字段会预填充备份主机，该主机用于所选 AHV VM 的备份操作。 **注意：**如果所选 VM 和备份主机平台不同类，则“**恢复主机**”字段将为空。 **注意：** 要将文件还原到 Ubuntu 目标主机，请使用 RHEL 或 SUSE 作为恢复主机。 ■ 单击搜索以选择另一恢复主机。此时会显示兼容介质服务器的列表。如果要选择 NetBackup 客户端作为恢复主机，请单击“**介质服务器**”**>**“**客户端**”。 ■ 如果搜索选项不可用，请手动输入恢复主机。 **注意：**恢复主机应与源 VM 属于同类平台，并且必须安装 NetBackup 9.1 或更高版本的服务器或客户端。 ■ 在灵活扩展环境中，如果介质服务器选项卡中未列出所有介质服务器，则用户需要介质服务器的查看权限，或者可以手动键入介质服务器以继续。 ■ 如果之前已在同一目标主机上执行还原，则恢复主机会根据执行此还原的用户的预分配权限，预填充以前使用的恢复主机。

步骤概述	说明和参考
Linux SSH 连接	对于所选源 Linux VM SSH 连接，将显示以下选项： ■ **目标主机 SSH 端口**指定目标主机的 SSH 端口。默认值为 22。 如果之前已在同一目标主机上执行还原，SSH 端口会根据执行此还原的用户的预分配权限，预填充以前使用的值。 ■ **目标主机 SSH 密钥指纹**要对目标主机进行身份验证，请提供十六进制格式的 SSH 密钥指纹。 ■ 您可以手动输入目标主机 SSH 密钥指纹，也可以单击“**获取 SSH 密钥指纹**”。 ■ **获取 SSH 密钥指纹**：如果“获取 SSH 密钥指纹”选项不可用，则必须手动提供 SSH 密钥指纹。请参见第 79 页的“SSH 密钥指纹”。 ■ 如果之前已在同一目标主机上执行还原，SSH 密钥指纹会根据执行此还原的用户的预分配权限，预填充以前使用的值。可以重写预填充的值以重新建立信任。 ■ **获取 SSH 密钥指纹** ■ 显示 SSH 密钥指纹列表，以及在目标主机上配置的 NetBackup 支持的密钥类型。 ■ 选择列出的指纹之一，然后单击“**确定**”。NetBackup 将使用所选指纹与目标主机建立信任。 ■ **目标主机凭据** ■ **用户名**指定目标主机用户名。此用户必须是 root 或非 root sudoer。 **Sudoer 用户** 请参见第 71 页的“恢复无代理文件和文件夹的前提条件”。 ■ **提供密码**选择此选项可选择基于密码的身份验证。 ■ **密码**为提供的用户指定目标主机密码。 ■ **提供 SSH 私钥**选择此选项可选择基于 SSH 私钥的身份验证。请参见第 79 页的“SSH 密钥指纹”。 ■ **SSH 私钥**：指定 SSH 私钥。 ■ **密钥密码**如果使用密码创建 SSH 私钥，请指定密钥密码
Windows WMI 连接	■ **用户名**指定目标主机用户名。此用户可以是域用户或本地用户，并且必须属于本地管理员组。支持的用户名格式为 **localusername** 或 **domain\username**。 ■ **密码**：为所指定用户指定目标主机密码。

Nutanix AHV 的恢复前检查

表 7-3 Nutanix AHV 的恢复前检查

验证	说明和参考	输入源
恢复主机空间	检查恢复主机暂存位置上是否具有所需的空间。	恢复主机
目标主机连接	检查是否可从恢复主机访问目标主机。	目标主机和目标主机端口
目标主机凭据	检查提供的目标主机凭据是否有效。	目标主机凭据
本地磁盘上的目标主机暂存位置	检查目标主机暂存位置是否不是网络路径。	目标主机暂存位置
目标主机暂存位置空间	检查目标主机暂存位置上是否具有所需的空间。 **注意：**所需空间是所选文件的总大小，其中包含 NetBackup 还原软件包所需的空间以及日志和其他文件所需的空间。	目标主机暂存位置
目标主机暂存位置权限	检查提供的用户是否为所有者，并且是否对目标主机暂存位置具有 RBAC 权限。	目标主机暂存位置
目标主机默认暂存位置路径	检查提供的目标主机暂存位置路径是否包含有效字符。NetBackup 不支持在目标主机暂存位置路径中使用非 ASCII 字符。	目标主机暂存位置
目标主机操作系统	检查目标主机是否具有支持的操作系统。	常规
VxUpdate 软件包	检查主服务器上是否存在所需的 VxUpdate 软件包。	常规
Linux 目标主机特定检查		
目标主机 SSH 密钥指纹	检查目标主机 SSH 密钥指纹是否有效，以与恢复主机中的目标主机建立信任。	目标主机 SSH 密钥指纹

验证	说明和参考	输入源
目标主机上的 Tar 存在情况	检查目标主机上是否存在 `tar`。	目标主机

关于 Nutanix-AHV 基于代理的文件和文件夹还原

NetBackup 9.1 及更高版本支持对单个文件和文件夹进行 Nutanix-AHV 基于代理的文件和文件夹还原。通过基于代理的还原，可以在具有 NetBackup 客户端的主机上还原单个 Nutanix-AHV 文件。基于代理的目标主机可以是托管在 AHV 或其他虚拟机管理程序上的虚拟机，甚至是安装了客户端 NetBackup 的物理机。

基于代理的文件和文件夹恢复的前提条件

- 可以从源 AHV VM 备份映像执行单个文件和文件夹恢复。访客操作系统和文件系统必须兼容，才能创建文件系统映射。
  有关访客操作系统和文件系统对单个文件还原的支持，请参考 *Nutanix AHV SCL*。
  在虚拟环境中对 NetBackup <versions> 的支持
- 可以从源 AHV VM 备份执行单个文件恢复。NetBackup 主服务器、介质服务器和备份主机必须为 NetBackup 9.1 或更高版本。
- 如果目标主机安装了 NetBackup 客户端或服务器，则执行基于代理的还原。客户端或目标主机必须为 NetBackup 8.1 或更高版本 (Windows) 或 8.2 或更高版本 (Linux)。

  注意：如果选择 Linux 版本 8.1 或更早版本，将显示无代理还原选项。

  必须在目标主机中指定 NetBackup 配置的主机名或 IP，才能完成基于代理的还原。
- 具有查看 NetBackup 主机所需 RBAC 权限的用户可以浏览并选择用于还原文件或文件夹的 NetBackup 主机。
  没有所需 RBAC 权限的用户必须手动为目标主机指定 NetBackup 配置的主机名或 IP。
- 以下是用户执行基于代理的文件和文件夹还原所需的最低 RBAC 权限。

表 7-4 所有 AHV 资产的权限

操作	说明	其他必需操作	其他可选操作
粒度还原	从 AHV 资产还原单个文件或文件夹。 在源 VM 上必须拥有此权限。	全局 > NetBackup 管理 > NetBackup 备份映像 > 查看 全局 > NetBackup 管理 > NetBackup 备份映像 > 查看内容 全局 > NetBackup 管理 > NetBackup 主机 > 查看 资产 > 资产 > 使用客户端还原文件	资产 > 资产 > 重写文件和文件夹

表 7-5 所有 AHV 资产的权限

操作	说明	其他必需操作	其他可选操作
粒度还原	从 AHV 资产还原单个文件或文件夹。 在源 VM 上必须拥有此权限。	全局 > NetBackup 管理 > NetBackup 备份映像 > 查看 全局 > NetBackup 管理 > NetBackup 备份映像 > 查看内容 全局 > NetBackup 管理 > NetBackup 主机 > 查看 资产 > 资产 > 使用客户端还原文件	资产 > 资产 > 重写文件和文件夹

使用基于 Nutanix AHV 代理的还原恢复文件和文件夹

使用基于 Nutanix AHV 代理的还原恢复文件和文件夹

1 确保目标主机已启动，并且通过网络连接到还原过程中要使用的恢复主机。

2 在左侧，单击“**工作负载**”**> Nutanix AHV**。

3 找到并选择包含要还原的文件和文件夹的 AHV VM。

下文将此 VM 称为源 VM。

4 单击“**恢复点**”选项卡。在日历视图中，选择备份发生的日期。

可用映像以行的形式列出，并且每个映像都具有备份时间戳。

5 在要从中恢复的映像上，单击“**恢复**”>“**还原文件和文件夹**”。

6 在“**选择文件**”窗格上，指定要恢复的文件和文件夹，然后单击“**下一步**”。下文将这些文件或文件夹称为源文件或源文件夹。

7 在“**恢复目标**”页面上，执行以下操作：

- 选择目标主机。
  - 目标主机输入必须为 FQDN 或 IP 地址。如果您具有查看主机的权限，请单击搜索图标，此时会显示已存在 NetBackup 客户端的主机，然后选择所需主机。

  注意：下拉列表中仅提供 NetBackup 版本 8.1 或更高版本。

- 选择适当的文件还原选项。

请参见第 82 页的“恢复目标选项”。

8 在“**恢复选项**”页面上，选择以下选项之一：

- **将字符串附加到文件名**：将指定字符串附加到目标文件名的文件扩展名之前。此值仅适用于文件。
- **重写现有文件**：重写目标位置中的同名文件或文件夹。
- **在不跨越装入点的情况下还原目录**
  跳过所选目录中装入的文件系统。清除此复选框可还原所选目录中装入的文件系统
- **为硬链接创建新文件**
- **重命名软链接的目标**

  注意：“**为硬链接创建新文件**”和“**重命名软链接的目标**”选项只能将所有内容还原到其他目录。

9 单击“**下一步**”。

10 在“**审查**”页面上：复查所有先前选择的选项。

11 单击“**启动恢复**”。

限制

- 不支持单个文件的跨平台恢复操作。只能将 Windows 文件还原到 Windows 访客操作系统，Linux 文件则只能还原到支持的 Linux 访客操作系统。也就是说，恢复主机必须与要还原的文件使用相同的平台。
- 在恢复过程中，NetBackup 在硬链接及其原始文件之间重新创建链接。仅在这种情况下，必须在同一作业中还原链接文件及其目标文件。

  注意：如果在单独的还原作业中逐一还原每个文件，则这些文件将还原为单独的文件，而不会重新建立链接。

- 对于双启动虚拟机，NetBackup 不支持恢复单个文件或文件夹。
- 有关客户端平台和文件系统支持及限制，请参见 https://www.veritas.com/content/support/en_US/doc/NB_70_80_VE。
- “**精简现有目录结构**”和“**将字符串附加到文件名**”选项仅适用于文件，不适用于目录。
- 如果选择“**精简现有目录结构**”和“**重写现有文件**”选项，则包含多个具有相同文件名的文件时，可能会导致错误的还原。

  注意： 还原完成后，上次还原的文件可用。

- 如果选择“**精简现有目录结构**”选项，而未选择“**重写现有文件**”，则还原会成功，但在还原完成后，被还原的第一个文件仍然存在。为防止出现此问题，还原多个同名文件时，不要选择“**精简现有目录结构**”。
- 如果在同一 VM 上同时执行备份和还原，一个或两个作业可能会产生意外结果。

  注意：如果备份或还原退出时 NetBackup 状态码不是零，一个可能的原因是，在同一 VM 上同时执行了多项作业。

- 如果所选的还原数据包含任何隐藏文件，如 `.bashrc`、`.bash_history`，则不支持“**将字符串附加到文件名**”还原选项。
- Nutanix 无代理还原只能用于还原文件和文件夹。
- 如果 NetBackup 对暂存目录没有足够权限或暂存目录中空间不足，还原作业将失败。

注意：如果 NetBackup 客户端已存在于目标 VM 上，则 Cohesity 不建议执行 Nutanix AHV 无代理还原。在此类情况下，NetBackup 管理员必须使用基于代理的还原。

- 在 Windows 目标主机上，不支持将目标还原到映射驱动器。
- NetBackup 不支持使用 `openSSH` 与 Windows 目标主机通信。在这种情况下，还原作业将失败。
- NetBackup 不支持在目标主机暂存位置路径中使用非 ASCII 字符。
- NetBackup 对 Windows 目标主机仅支持 NTLM 身份验证类型。
- 在 9.1 版本之前备份的 AHV 映像无法从 Web UI 还原。要还原这些映像，用户必须使用 NetBackup 管理控制台。
- 如果备份主机的版本为 NetBackup 9.1 或更高版本，则即使备份是从 NetBackup 管理控制台执行的，AHV 备份映像在 Web UI 上也可用。
  关于 Web UI 上的备份映像：
  - 如果资产发现成功，在从 NetBackup 管理控制台进行备份后，备份映像将在 Web UI 上可用。
  - 如果主服务器和备份主机已升级到 9.1，并且已从 NetBackup 管理控制台进行备份，则配置 Web UI 时，必须运行资产发现以查看备份映像。
  - 如果主服务器已升级到 9.1，但备份主机的版本仍低于 9.1，则从 NetBackup 管理控制台进行备份。然后，如果配置 Web UI，则即使在资产发现后也看不到备份映像。

8

保护 Nutanix Cloud Clusters (NC2)

本章节包括下列主题：

保护 AWS 上的 Nutanix Cloud Clusters (NC2)

Nutanix Cloud Clusters (NC2) 是 Nutanix Cloud Platform 的一个扩展，有助于企业在 AWS 上运行 Nutanix Cloud Platform 软件。该扩展在公有云超大规模业者环境中复制本地使用的核心 Nutanix HCI 软件，从而使私有云和公有云可享有同样的虚拟化和软件定义的优势。

有关 AWS 上的 Nutanix Cloud Clusters (NC2) 的更多信息，请参考 Nutanix 联机文档。

在 Nutanix Cloud Clusters (NC2) 环境中，可以使用 NetBackup 10.4 及更高版本保护虚拟机。在 Nutanix Cloud Clusters (NC2) 环境中部署 Nutanix 群集和 Prism Central 后，可以在 NetBackup Web UI 中对其进行配置，配置方式与本地 Nutanix 群集和 Prism Central 类似。在 NetBackup 中成功配置群集后，将发现虚拟机。随后，可以使用为 AHV 工作负载设计的保护计划保护这些虚拟机。

注意：NetBackup 保护 Nutanix Cloud Clusters (NC2) 环境中的虚拟机，保护方式与本地 Nutanix 群集中的虚拟机类似。有关使用 NetBackup 保护 Nutanix 本地虚拟机的更多详细信息，请参考《NetBackup™ for Nutanix AHV 管理指南》中的“管理 AHV 群集”一章。

保护 Azure 上的 Nutanix Cloud Clusters (NC2)

Nutanix Cloud Clusters (NC2) 是 Nutanix Cloud Platform 的一个扩展，有助于企业在 Microsoft Azure 云服务上运行 Nutanix Cloud Platform 软件。该扩展在公有云超大规模业者环境中复制本地使用的核心 Nutanix HCI 软件，从而使私有云和公有云可享有同样的虚拟化和软件定义的优势。

有关 Azure 上的 Nutanix Cloud Clusters (NC2) 的更多信息，请参考 Nutanix 联机文档。

在 Nutanix Cloud Clusters (NC2) 环境中，可以使用 NetBackup 10.4 及更高版本保护虚拟机。在 Nutanix Cloud Clusters (NC2) 环境中部署 Nutanix 群集和 Prism Central 后，可以在 NetBackup Web UI 中对其进行配置，配置方式与本地 Nutanix 群集和 Prism Central 类似。在 NetBackup 中成功配置群集后，将发现虚拟机。随后，可以使用为 AHV 工作负载设计的保护计划保护这些虚拟机。

注意：NetBackup 保护 Nutanix Cloud Clusters (NC2) 环境中的虚拟机，保护方式与本地 Nutanix 群集中的虚拟机类似。

有关使用 NetBackup 保护 Nutanix 本地虚拟机的更多详细信息，请参考《NetBackup™ for Nutanix AHV 管理指南》中的“管理 AHV 群集”一章。

9

对 AHV 操作进行故障排除

本章节包括下列主题：

故障排除 AHV 操作：创建 AHV 即时访问虚拟机的过程中出错

下表介绍了尝试创建 AHV 即时访问虚拟机时可能出现的问题。

表 9-1 创建 AHV 即时访问虚拟机的过程中出错

错误消息或原因	说明及推荐操作
`Failed to create the VM in the Nutanix AHV cluster. Error: Already used VM UUID: <VM UUID>. Return value 114. Failed to create an instant access virtual machine (VM). (4004)`	在创建即时访问 VM 之前，系统会检查 Nutanix 群集中是否已存在 VM UUID。若存在，恢复将失败。 解决办法： 1 启动恢复过程。 2 选择“**创建即时访问虚拟机**”。 3 在“**恢复选项**”页面上，选择“**创建新 VM ID 而非使用现有 ID**” 4 继续恢复，单击“**启动恢复**”。

`Failed to create an instant access virtual machine (VM).`
 	
`Error details`
 	
`Only the Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems are supported.`
	即时访问当前仅支持 RHEL 和 SLES。如果尝试恢复不受支持的操作系统 VM，则会失败。
	推荐的操作：
	对于具有不受支持的操作系统的介质服务器，使用传统的完全恢复。

`Failed to create an instant access virtual machine (VM). Specification for create VM cannot be prepared, as RetainMacAddress and RemoveNetworkInterface`
 	
`can't be used together.`
	如果同时使用 `RetainMacAddress` 和 `RemoveNetworkInterface`，API 规格将无效。
	推荐的操作：
	如果删除了网络接口控制器 (NIC)，请勿保留 MAC 地址。如果需要保留 MAC 地址，NIC 卡必须保持配置状态。

错误消息或原因	说明及推荐操作
Failed to create an instant access virtual machine (VM). Error details Create instant access VM capability for Nutanix is supported from NetBackup 11.1 and above.	无法使用 NetBackup 11.0.0.1 及更早版本创建即时访问 VM。 推荐的操作： 确保已使用 NetBackup 11.1 或更高版本完成还原。
Failed to create the VM in the Nutanix AHV cluster. Error: InUse: MAC address <MAC address> is in use: 18. Return value 114. Failed to create an instant access virtual machine (VM). (4004)	当原始 VM 仍然存在于 Nutanix 群集且 MAC 地址已在使用时，会发生此情况，导致冲突。 推荐的操作： 确保在即时访问恢复之前删除或关闭原始 VM，以避免 MAC 地址复制。

NetBackup for AHV 的故障排除提示

有关 AHV 故障排除的更多信息，请查看下列详细信息：

- 对于发现作业失败：
  - 在活动监视器中查看作业的“**作业详细信息**”部分。
  - 查看 ncfnbcs 日志。
- 对于快照作业失败：
  - 在活动监视器中查看作业的“**作业详细信息**”部分。
  - 查看 bpfis 日志。
  - 对于与 AHV 相关的错误，请查看 AHV Prism 控制台上的“**警报**”。
- 对于备份作业失败：

- 在活动监视器中查看作业的“**作业详细信息**”部分。
- 查看 bpbkar 和 VxMS 日志。
- 对于与 AHV 快照相关的错误，请查看 AHV Prism 控制台上的“**警报**”。

- 对于还原作业失败：
  - 还原作业失败，错误为 2822（Hypervisor 策略还原错误）
  - 在活动监视器中查看作业的“**作业详细信息**”部分。
  - 查看 bprd、bpVMutil、VxMS 或 ncfnbrestore 日志。
  - 对于与 AHV 相关的错误，请查看 AHV Prism 控制台上的“**警报**”。

添加 AHV 凭据期间出错

表 9-2 添加 AHV 凭据期间出错

错误消息或原因	说明及推荐操作
NetBackup 9.1 或更高版本支持虚拟机发现和凭据验证。所选服务器/备份主机具有 NetBackup 版本 8.3。	升级服务器/备份主机，或选择具有所需 NetBackup 版本的另一个服务器/备份主机。

在 AHV 虚拟机发现阶段期间出错

下表介绍了尝试发现 AHV 虚拟机时可能出现的问题。

表 9-3 在 AHV 虚拟机发现阶段期间遇到错误

错误消息或原因	说明及推荐操作
添加正确的 AHV 群集凭据后，未发现 AHV 资产。VM 发现操作失败。	立即运行发现，然后重试备份。AHV 群集名称的最大允许长度为 255 个字符，如果字符数超过 95 个，资产发现会失败。 解决方法： ■ 确保 AHV 群集名称不超过 95 个字符。

错误消息或原因	说明及推荐操作
发现作业失败，错误为200。调度程序未找到任何备份或要部署 NetBackup 的客户端。	确保策略或智能 VM 组中指定的查询正确。最近已将需要保护的 VM 添加到 AHV 群集，或者 VM 配置已更改，并且现在未触发自动发现或发现。 ■ 如果使用 `tpconfig` 添加 AHV 群集凭据，则资产发现将不起作用。 解决方法： 从 NetBackup Web UI 中，针对指定的 AHV 群集单击“**发现**”。 确保使用 API 或 NetBackup Web UI 添加 AHV 群集凭据。

新发现的 VM 的状态错误

下表介绍了尝试发现 AHV 虚拟机时可能出现的问题。

表 9-4 新发现的 VM 的状态错误

错误消息或原因	说明及推荐操作
VM 的上次成功备份状态指示它未进行备份。	在 NetBackup Web UI 中，新发现的 VM 的上次成功备份状态未指示其已备份。 在某些情况下，例如智能 VM 组，在发现与所提供查询相匹配的新 VM 之前便已备份该 VM，如以下场景所示： ■ 默认情况下，自动发现每 8 小时执行一次。 ■ 新 VM 已添加到环境中。 ■ 在发现完成之前，备份作业已成功完成。 例如，使用现有策略的备份作业，备份选择条件中包含新 VM。 ■ 在 NetBackup Web UI 中，VM 的上次成功备份状态未更新，仍指示其尚未进行备份。 解决方法： ■ 如果遇到类似情况，仍然可以浏览恢复点并将其恢复。 但是，只有在群集上触发发现并且在发现后成功完成 VM 的另一次备份后，上次成功备份状态才会更新。

备份 AHV 虚拟机时遇到错误

下表介绍了备份 AHV 虚拟机时可能出现的问题：

表 9-5 备份 AHV 虚拟机时出错

错误消息或原因	说明及推荐操作
在 NetBackup 备份操作后，不会删除 AHV 群集上的 VM 快照。	如果挂接到 VM 的磁盘处于不活动状态，则 AHV 群集不会在备份操作完成后删除 VM 快照。 解决方法： ■ 执行备份操作前，验证挂接到 VM 的磁盘的状态并确保它们处于活动状态。 ■ 确保磁盘并非在 VM 运行时挂接，从而防止磁盘处于不活动状态。
MSiSCSI 服务已禁用。在备份主机上启用 MSiSCSI 服务。	在 Windows 备份主机上启用 Microsoft iSCSI 发起程序服务 (MSiSCSI)，然后重新运行作业。

错误消息或原因	说明及推荐操作
无法建立连接。验证 iSCSI 服务是否已安装并正在运行。	

错误消息或原因	说明及推荐操作
	■ 对于 Windows：在备份主机上启用 Microsoft iSCSI 发起程序服务。 **注意：**仅在 Windows 操作系统中显示错误。 ■ 对于 Linux，此错误以警告形式显示，它将重新使用 NFS 进行备份/还原。如果使用分段 iSCSI 数据服务，备份/还原将失败。 确保在 Nutanix UI 的 `Filesystem Whitelists` 选项中添加了备份主机，以通过 NFS 传输进行备份。 为了使 Linux 能够使用 iSCSI：在备份主机上安装/启用 iSCSI 发起程序软件包，然后重新运行该作业。 ■ 在 Linux 主机上使用以下命令验证连接：`iscsiadm -m discovery -t sendtargets -p` *`correct IP as per configured iSCSITargetType`* 根据 iSCSI 传输类型使用以下 IP 地址： ■ 对于 iSCSI 数据服务：群集详细信息页面中的 iSCSI 数据服务 IP ■ 对于分段：使用群集详细信息页面中的分段 iSCSI 数据。 ■ 对于指定的分段：使用在 NetBackup 中配置群集时指定的虚拟 IP。 ■ 在 Windows 主机上使用以下命令验证连接： ■ 单击“**服务器管理器**”->“**工具**”->“**iSCSI 发起程序**”。这将打开“**iSCSI 发起程序属性**”对话框。 ■ 单击“**发现**”>“**发现门户**”，并根据为 AHV 群集配置的 iSCSI 目标类型提供 IP 地址。 ■ 默认：群集详细信息页面中的 iSCSI 数据服务 IP ■ SEGMENTED：群集详细信息页面中的分段 iSCSI 数据 ■ SEGMENTED_SPECIFIC：在 NetBackup 中配置群集时指定的虚拟 IP。 ■ 如果在使用 Flex Scale 一体机时遇到此错误消息，请注意，只有 NetBackup 主服务器不支持 iSCSI 数据路径，而支持 NFS 作为数据路径。 但是，如果需要使用 iSCSI 数据路径，建议使用介质服务器，而不使用主服务器。介质服务器可高效管理 iSCSI 数据路径，从而确保备份和还原功能正常。 ■ 如果在使用 Flex Appliance 作为备份/恢复主机时遇到此错误： ■ 编辑配置以使用默认选项（使用 NFS 传输）。 ■ 使用具有所需 iSCSI 和网络配置的其他备份/恢复主机。 ■ 更新保护计划以使用特定备份主机。

错误消息或原因	说明及推荐操作
	■ 使用具有所需 iSCSI 和网络配置的恢复主机。
身份验证失败。验证提供的发起程序 CHAP 是否正确。	提供的 CHAP 密钥无效，或者 iSCSI 发起程序名称对于每个备份或恢复主机不唯一。为每个备份/恢复主机设置唯一的 iSCSI 发起程序名称。
获取 iSCSI 的外部数据服务 IP 地址失败。在 Nutanix 群集 {Nutanix AHV clusterName} 上设置 IP 地址后重新运行作业。	在 Nutanix AHV 群集上设置 iSCSI 的外部数据服务 IP 地址。有关更多详细信息，请参见第 21 页的"配置 Nutanix AHV 群集的前提条件"。 **注意：**对于 Linux，将重新使用 NFS 进行备份/还原。
一台或多台备份主机不支持 NetBackup 版本。在所有 Linux 或 Windows 备份主机上使用 NetBackup 9.1 或更高版本，以使用 Nutanix 保护计划中的自动备份主机选项。	为 Nutanix 保护计划中的备份主机选择“**自动**”选项时，将发生此错误。将备份主机升级到最新 NetBackup 版本。
对于 NetBackup 介质服务器负载平衡，请确保备份主机具有 Red Hat Enterprise Linux、SUSE Linux Enterprise Server 或 Microsoft Windows 操作系统。	为 Nutanix 保护计划中的备份主机选择“**自动**”选项时，将发生此错误。 对于 Nutanix AHV，支持的介质服务器为： ■ Red Hat Enterprise Linux ■ SUSE Linux Enterprise Server ■ Microsoft Windows 操作系统
介质服务器上现有的 NetBackup 版本不支持增量式备份日程表。	将备份主机上的 NetBackup 升级到最新版本。
无法为特定 Nutanix 群集设置资源限制。	如果已从 NetBackup 环境中删除设置了资源限制的群集，则在某些情况下，会禁用“**+ 添加**”选项以设置资源限制。 推荐的操作 删除已删除群集的资源限制，然后为其余群集设置资源限制。

错误消息或原因	说明及推荐操作

快照作业失败，错误代码为 156，作业详细信息如下：
 	
`Critical bpbrm (pid=30139) from client 9c5dcb07-65d2 -4761-b861-9e517edcf5b6_ <Nutanix-cluster>`
 	
`abc.cbus.com FTL - Value 2 that specifies GUID is not supported for the nameuse`
	如果保护计划是使用“**备份选项**”>“**选择要用于备份的服务器或主机**”>“**自动**”创建的，并且所选存储单元已配置具有 NetBackup 9.1 或之前版本的介质服务器。当此保护计划用于备份 AHV VM 或智能 VM 组时，快照作业可能会失败。
	
	推荐的操作
	
	在所选存储单元中配置的所有介质服务器都必须升级到 NetBackup 9.1。
	
	为避免在升级其他介质服务器时作业失败，请在“**保护**”>“**自定义保护**”>“**备份选项**”选项中，手动选择特定介质服务器或备份主机作为用于备份的服务器或主机，而不是使用默认的“**自动**”选项。建议使用已升级的介质服务器。所有介质服务器升级完成后，使用“**保护**”>“**还原原始设置**”以返回原始设置。

错误 1
 	
`iscsiadm: Could not login to [iface: default, target: iqn.2010-06.com.nutanix: nbubackup -2d29da9d-f964- 4157-9595-f0319090bb01-tgt0, portal: xx.xx.xx.xx,3260]`
 	
`iscsiadm: initiator reported error (24 - iSCSI login failed due to authorization failure)`
 	
`iscsiadm: Could not log into all portals`
 	
错误 2
 	
`iscsiadm: Could not execute operation on all records: encountered iSCSI database failure`
 	
错误 3
 	
`iscsiadm: could not read session targetname: 5`
 	
`iscsiadm: could not find session info for session28`
	备份/还原作业的成功作业详细信息选项卡中显示这些错误。这些错误是执行 `iscsiadm` 命令的输出。这些错误间歇发生，可能是由于 iSCSI 网络上负载过重所致。NetBackup 执行重试操作以修复这些错误。重试操作成功后，备份/还原作业也会成功。
	
	推荐的操作
	
	无需在 NetBackup 端执行任何操作。用户仍然可以对 `iscsiadm` 进行故障排除，并确保 iSCSI 安装/配置正确以避免此类错误。

错误消息或原因	说明及推荐操作
`iscsid: Ignoring CHAP algorithm request for MD5 due to crypto lib configuration iscsid: Couldn't set CHAP algorithm list`	请参见 In FIPS enabled environment, NetBackup backup/restore of Nutanix AHV VMs (Virtual Machines) using iSCSI fails
错误代码：4798 未为 AHV 群集选择“对此群集使用 Prism Central 服务器”选项。	备份期间的发现作业可能会失败，并显示 Nutanix 智能 VM 组错误。 查看并修复智能 VM 组的以下可能原因： ■ 是在类别过滤器作为过滤器查询之一的情况下创建的，以及 ■ 创建智能 VM 组后，将更新一个或多个 Nutanix 群集，以取消选中“**对此群集使用 Prism Central 服务器**”选项，并在此类 IVMG 上触发“**立即备份**”操作。
错误消息： 找不到 AHV 群集的 Prism Central，服务器 = *Server details*	备份作业失败并显示给定错误。 查看并修复以下可能的原因： ■ 如果智能 VM 组由来自同一 Prism Central 服务器的一个或多个群集组成，并且为其定义了类别过滤器，则触发 IVM 组保护时，Prism Central 服务器将被删除/无法访问。 ■ 如果智能 VM 组由来自不同 Prism Central 服务器的两个或多个群集组成，并且为其定义了类别过滤器，则触发智能 VM 组保护时，一个或多个 Prism Central 服务器将被删除/无法访问。
错误消息： 保护计划订购可能失败并显示错误。 遇到无效的 API 请求 `error message: backupHost: Backup host with a NetBackup version earlier than 10.4 is not supported for IntelligentVM group Category filter.`	如果在智能 VM 组中使用过滤器类别，则将其订购到保护计划可能会失败并显示给定错误。 ■ 确保保护计划中提到的备份主机必须具有 NetBackup 10.4 或更高版本。

错误消息或原因	说明及推荐操作

备份作业失败，并显示错误代码 800。
 	
`Error nbjm(pid=113200) NetBackup status: 800, EMM status :Use NetBackup media server version 10.4 or later to protect Nutanix Intelligent VM groups with category filters.`
 	
.
 	
`Error nbpem(pid=113293) backup of client MEDIA_SERVER exited with status 800 (resource request failed).`
	描述
	
	如果保护计划是使用“**备份选项**”>“**选择要用于备份的服务器或主机**”>“**自动**”创建的，并且所选存储单元已配置具有低于 NetBackup 10.4 版本的介质服务器。则使用此保护计划备份类别属性为过滤器的智能 VM 组时，备份作业将失败。
	
	推荐的操作：
	
	必须将在所选存储单元中配置的至少一个介质服务器升级到 NetBackup v10.4 或更高版本。

备份作业失败并显示以下错误消息：
 	
错误 1
 	
`Begin Application Resolver:Resolver Discovery`
 	
错误 2
 	
`Error nbpem(pid=98395) Invalid URI.`
 	
错误 3
 	
`Error nbpem (pid=98395) backup of client falcna12c3.abcus.com exited with status 4232 Invalid Discovery Query URI).`
	描述
	
	为智能 VM 组订购具有备份主机版本 10.3 或更低版本的保护计划，并使用过滤器类别修改智能 VM 组时。
	
	然后，备份作业运行后将失败并显示错误消息。由于较低版本的备份主机无法识别过滤器类别。
	
	推荐的操作：
	
	通过自定义保护计划，将备份主机升级到 10.4 或更高版本。有关更多详细信息，请参见第 63 页的“自定义 AHV 资产的保护设置”。

还原 AHV 虚拟机时出错

下表介绍了还原 AHV 虚拟机时可能出现的问题。

表 9-6 还原 AHV 虚拟机时遇到错误

错误消息或原因	说明及推荐操作
在 Windows 主服务器上，VM 恢复到备用位置失败。	对于 Windows NetBackup 主服务器，请确保重命名文件以空行结尾。

错误消息或原因	说明及推荐操作
修改恢复目标时无法更改“**AHV 群集**”。	如果看不到 AHV 群集列表，您可能无法访问 RBAC 中的 AHV 群集。 请与 NetBackup 安全管理员联系，以解决此问题。
AHV 群集中存在具有相同 UUID 的 VM 且未启用重写 VM 的选项时，恢复前检查成功运行，但 VM 还原失败。 显示以下错误消息： 信息 `bpVMutil` (`pid=1196`) FTL - 存在虚拟机但未指定重写选项，无法继续还原。结束还原；运行时间 Hypervisor 策略还原错误。(2822)	恢复前检查通过比较 VM 显示名称（而不是 UUID）确定 VM 是否存在，因此检查会成功完成。但是，如果未设置重写选项，则已存在具有相同 UUID 的 VM 时，还原作业将失败。 解决办法： **使用新的 UUID 还原 VM。** 1 启动恢复过程。 2 在“**恢复选项**”页面中，单击“**高级**”。 3 启用“**创建新的 VM UUID**”。 4 继续恢复过程，然后单击“**启动恢复**”以进行还原。 **重写具有相同 UUID 的现有 VM。** 1 启动恢复过程。 2 在“**恢复选项**”页面上，启用“**重写现有虚拟机**”选项。 3 继续恢复过程，然后单击“**启动恢复**”以进行还原。
尝试恢复使用 Web UI 从其他域导入的 AHV VM 映像时，恢复前检查将失败，并显示默认情况下恢复主机是备份过程中使用的同一访问主机。	在恢复导入的 AHV VM 映像期间，请选择目标域中的访问主机作为恢复主机，或者选择目标主服务器。
`MSiSCSI` 服务已禁用。在恢复主机上启用 `MSiSCSI` 服务。	在 Windows 备份恢复主机上启用 Microsoft iSCSI 发起程序服务 (`MSiSCSI`)，然后重新运行作业。
无法连接到恢复主机。	无法访问用于无代理还原的恢复主机。 推荐的操作： 确保可以从主服务器访问恢复主机，并且恢复主机安装了 NetBackup 介质服务器或客户端软件。

错误消息或原因	说明及推荐操作
指定的恢复主机必须运行 NetBackup 版本 9.1 或更高版本才能支持无代理还原。	文件或文件夹的无代理还原要求恢复主机安装 NetBackup 版本 9.1 或更高版本。 推荐的操作： 验证恢复主机上的 NetBackup 版本。应该为 9.1 或更高版本。 在 UNIX NetBackup 服务器和客户端上，验证 `/usr/openv/netbackup/bin/version` 文件。 在 Windows NetBackup 服务器上，验证 `install_path\netbackup\version.txt` 文件。
恢复主机暂存位置不存在。	恢复主机上不存在用于无代理还原的暂存位置路径。 推荐的操作： ■ 确保恢复主机的默认暂存位置路径或用户配置的暂存位置路径有效。NetBackup 将恢复主机上的以下位置用作默认暂存位置： ■ 对于 UNIX：`{installpath}/openv/tmp/staging`。 ■ 对于 Windows：`{installpath}\Netbackup\Temp\staging\`。 ■ 确保使用的暂存位置路径存在。对于用户配置的暂存位置，验证在 `bp.conf` 参数 **AGENTLESS_RHOST_STAGING_PATH = "path"** 中指定的恢复主机路径是否有效。
在恢复主机的暂存位置未找到 tar 映像。	在恢复主机暂存位置未找到 tar 映像。此映像是无代理还原所必需的。 推荐的操作： 联系 Cohesity Technical Support 并从恢复主机共享 `bpVMutil` 日志。
内部错误导致恢复验证失败。	运行无代理还原的恢复前验证时发生内部错误。 推荐的操作： 保存恢复主机上的 **bpVMutil** 日志并与 Cohesity 技术支持联系。
恢复主机上没有足够的可用空间。	恢复主机可能没有足够的空间将选定的文件复制到用于无代理还原的暂存位置。 推荐的操作： 根据所选文件或文件夹的总大小，确保恢复主机暂存位置上有足够的可用空间。或者，选择具有足够可用空间的其他恢复主机来执行无代理还原。
目标主机上不存在 tar 实用程序。	在目标主机上找不到 tar 实用程序。此实用程序是无代理还原所必需的。 推荐的操作： 部署 tar 实用程序后重试。
指定的暂存位置在目标主机上不存在，或者用户没有所需的访问权限。	推荐的操作： 确保目标主机暂存位置存在，并且用户具有足够权限访问该位置。

错误消息或原因	说明及推荐操作
用户对目标主机暂存位置没有所需的权限。	用户没有在目标主机上继续还原所需的权限。 推荐的操作： 确保目标主机暂存位置存在，并且用户对该暂存位置具有最低写入和运行权限。
用户没有 root/管理员权限。要还原文件和文件夹，请为用户提供 root 或管理员权限。	用户没有在目标主机上继续还原所需的权限。 推荐的操作： 在 Windows 目标主机上，提供属于本地管理员组的凭据。对于 Linux 目标主机，使用具有 ALL 权限的 root 或 sudo 帐户的凭据。
无法从恢复主机访问目标主机的管理员共享。	无法从恢复主机访问远程主机的管理员共享，因此无法执行无代理还原。 推荐的操作： ■ 确保正确设置防火墙例外。 ■ 确保“文件和打印机共享”处于启用状态。 ■ 确保 GPO/软件限制策略或防病毒未阻止访问。 ■ 确保目标主机可访问，并确保输入正确的凭据并拥有适当的权限。
要在用户帐户控制 (UAC) 环境中进行无代理文件或文件夹还原，请在 Windows 目标主机上提供属于本地管理员组的域用户的凭据。	推荐的操作： 对于用户帐户控制 (UAC) 环境中的无代理还原，提供域用户凭据。此用户必须是 Windows 目标主机上本地管理员组的一部分。
无法执行无代理还原。	收到无代理还原失败的意外原因。 推荐的操作： 与 Cohesity 技术支持联系并共享相应的日志。
操作系统不匹配。确保恢复主机的操作系统与备份的 VM 操作系统匹配。	只有当恢复主机的操作系统与备份的VM操作系统相同时，才能进行无代理还原。 推荐的操作： 备用恢复主机必需与备份的 VM 具有相同的操作系统。
无法检索备份映像操作系统。	无法检索用于执行无代理还原的备份映像的操作系统。这是一个内部错误。
恢复主机操作系统与提供的通信模式不兼容。确保恢复主机的操作系统与提供的通信模式兼容。	无代理恢复或恢复前检查请求中提供的恢复主机操作系统类型和通信类型不兼容。 推荐的操作： 验证恢复主机的操作系统类型和通信类型是否兼容： ■ Linux：通信类型必须为 SSH。 ■ Windows：通信类型必须为 WMI。

错误消息或原因	说明及推荐操作
目标主机 SSH 私钥无效。	无代理恢复或恢复前检查请求的 sshKey 字段必须是目标主机的有效非空 ssh 私钥。 推荐的操作： 如果身份验证类型为 SSH_KEY，则验证已指定 sshKey 字段，并且它不为空。
无代理文件或文件夹还原不支持目标主机操作系统。	无代理还原要求在目标主机上部署恢复软件包，因此不支持目标主机操作系统。 推荐的操作： 仅 SUSE Linux Enterprise Server、Microsoft Windows、Red Hat Enterprise Linux (RHEL) 和 Ubuntu 是受支持的平台。 有关支持此功能的平台，请参考 NetBackup 兼容性列表。
目标主机用户名或密码无效。	必须在无代理恢复或恢复前检查请求的身份验证详细信息中指定用户名和密码字段。 推荐的操作： 验证已在恢复和恢复前检查请求的身份验证详细信息中指定了用户名和密码字段，这些字段正确并且不为空。
目标主机暂存位置路径包含非 ASCII 字符。	目标主机暂存位置路径仅支持 ASCII 字符。 推荐的操作： 在目标主机上提供仅包含 ACSII 字符的自定义暂存位置。
指定的路径在本地磁盘上不存在。	目标主机暂存位置不应为网络路径。 推荐的操作： 在目标主机上的本地磁盘上指定一个自定义暂存位置。
与目标主机的 WMI 连接失败。	恢复主机与目标主机的 WMI 连接失败。 推荐的操作： ■ 要与 WMI 和 DCOM 服务连接，用户必须具有连接到远程 WMI 服务所需的权限。 ■ 要设置防火墙例外，以允许 WMI 通信通过防火墙。 ■ GPO/软件限制策略或防病毒未阻止访问。 ■ 确保目标主机可访问。验证给定目标主机凭据。 ■ 确保目标主机与域的信任关系完好无损。跨域进行通信时，这些域之间必须存在双向信任关系。
未在远程服务器上找到指定的文件。	未在远程服务器上找到指定的文件。 推荐的操作： 确保目标主机上的指定暂存位置存在，或指定其他有效的暂存位置。

错误消息或原因	说明及推荐操作
存在与目录同名的文件。	目标主机上存在一个预先存在的文件，名称与暂存位置的目录路径中的名称相同。 推荐的操作： 检查远程主机上预先存在的文件是否与暂存位置的名称和路径相同。如果存在该文件，请重命名或删除该文件。或者另外指定一个暂存位置。
无法验证用户的管理权限。	目标主机用户没有管理权限，无法继续执行无代理文件和文件夹还原操作。 推荐的操作： 在 Windows 目标主机上，使用属于本地管理员组的凭据。 对于 Linux 目标主机，使用具有 **ALL** 权限的 root 或 sudo 帐户的凭据。
无法使用 Windows API 连接网络资源。	无法从恢复主机访问目标主机的管理员共享，因此无法执行无代理文件或文件夹还原。 推荐的操作： 在无代理文件和文件夹还原操作过程中，SMB 管理员共享是使用用户提供的凭据从恢复主机创建到目标主机上的。当无代理还原的目标主机具有 Windows 操作系统，并且无法从恢复主机访问目标主机的管理员共享时，通常会出现此错误。确保在目标主机上满足以下要求。 ■ 正确设置防火墙例外。 ■ “文件和打印机共享”处于启用状态。 ■ GPO/软件限制策略或防病毒未阻止访问。 ■ 可通过有效凭据访问目标主机。
无法在目标主机上检索用户的主目录。指定自定义暂存位置。	无法在目标主机上检索主目录上用户的默认暂存位置。输入有效的自定义暂存位置路径。 推荐的操作： 确保用户的主目录存在，或使用有效的自定义暂存位置进行尝试。

错误消息或原因	说明及推荐操作
无法与主机建立 SSH 会话。	确保满足以下所有条件，然后重试。 ■ Aes256-ctr 是用于通信的受支持密码。确保恢复主机和目标主机均支持此密码。 ■ 确保恢复主机和目标主机至少支持以下基于哈希的消息身份验证代码 (HMAC) 协议之一： ■ hmac-sha2-256 ■ hmac-sha2-512 ■ 确保用于生成主机密钥的方法是以下方法之一： ■ ECDSA_SHA2_NISTP256 ■ ECDSA_SHA2_NISTP384 ■ ECDSA_SHA2_NISTP521 ■ SSH_RSA ■ SSH_DSS
无法验证主机的 SSH 密钥指纹。	提供的目标主机 SSH 密钥指纹不正确。 推荐的操作： 验证目标主机的 SSH 密钥指纹，然后重试。
无法使用提供的用户名或密码对主机进行身份验证。	使用提供的用户名和密码进行目标主机身份验证失败。 推荐的操作： 验证目标主机的用户名或密码是否正确，然后重试。
无法使用指定的 SSH 密钥对主机进行身份验证。	使用提供的 SSH 私钥进行目标主机身份验证失败。 推荐的操作： 验证用于生成目标主机 SSH 私钥的 SSH 私钥和密钥密码有效。然后重试。确保相应公钥存在于目标主机 /root/.ssh 文件夹中的 authorized_keys 文件中。
在目标主机上找不到匹配的 SSH 密钥指纹主机密钥方法。	在目标主机上找不到指定的 SSH 密钥指纹主机密钥方法。 推荐的操作： 确保指定的 SSH 密钥指纹支持的主机密钥方法在目标主机上可用。或者提供在目标主机上配置的主机密钥方法的 SSH 指纹。
将单个文件还原到具有 NetBackup 客户端软件的虚拟机时，还原失败。	在将单个文件还原到具有 NetBackup 客户端的虚拟机时，请确保防火墙不干涉还原。如果防火墙停止了还原，请关闭防火墙并重试还原。

错误消息或原因	说明及推荐操作
从 Linux 虚拟机还原文件时装入点不可用。	对于 Linux 虚拟机，仅支持在 ext2、ext3、ext4 和 xfs 文件系统上还原单个文件。 如果分区使用其他某个文件系统格式化，备份将成功，但是 NetBackup 无法映射文件的文件系统地址。结果，NetBackup 将无法还原来自该分区的各个文件。只能单独还原位于 ext2、ext3、ext4 和 xfs 分区上的文件。 **注意：**要从原始装入点还原各个文件，“/”（根）分区必须格式化为 ext2、ext3、ext4 或 xfs 文件系统。如果“/”（根）分区格式化为其他文件系统（如 ButterFS），则装入点将无法解析。在这种情况下，可以从 /dev 级别（如 /dev/sda1）还原 ext2、ext3、ext4 或 xfs 文件。不能从文件的原始装入点级别还原文件。
对于没有使用持久性设备命名的 Linux VM，多个磁盘控制器（如 IDE、SCSI 和 SATA）可能会使单独文件的恢复变得复杂。	出现该问题是因为非持久性设备命名（如 /dev/sda 和 /dev/sdb）可能会导致装入点在重新启动后发生意外更改。如果 VM 具有 SCSI 磁盘和 SATA 磁盘，则“**还原文件和文件夹**”>“**添加文件和文件夹**”导航界面可能会显示错误的 VM 文件装入点。例如，浏览文件并进行还原时，最初位于 /vol_a 下的文件可能显示在 /vol_b 下。还原成功，但还原后的文件可能不在其原始目录中。 **推荐的操作：** 在还原后的 VM 上搜索文件并将其移动到适当的位置。为了防止在包含多个磁盘控制器的 Linux VM 上发生此问题，Veritas 建议使用持久性设备命名方法装入文件系统。使用持久性命名即可使设备装入保持一致，从以后的备份中还原文件时将不会发生此问题。对于持久性设备命名，可通过 UUID 装入设备。 以下是 /etc/fstab 文件的示例，该文件包含使用 UUID 装入的设备： ■ UUID=93a21fe4-4c55-4e5a-8124-1e2e1460fece /boot ext4 defaults 1 2。 ■ UUID=55a24fe3-4c55-4e6a-8124-1e2e1460fadf /vola ext3 defaults 0 0。 要查找设备 UUID，可以使用以下命令之一： ■ blkid ■ ls -l /dev/disk/by-uuid/

错误消息或原因	说明及推荐操作
对于没有持久性设备命名的 Ubuntu VM，“**还原文件和文件夹**”>“**添加文件和文件夹**”导航界面可能会显示错误的 VM 文件装入点，并且单个文件的恢复可能会失败。	此问题是由非持久性设备命名所致，并可能会导致装入点发生意外更改。对于 Ubuntu VM，“**还原文件和文件夹**”>“**添加文件和文件夹**”导航界面可能会显示错误的VM文件装入点。例如，浏览以还原文件和文件夹时，这些文件和文件夹可能出现在 `/dev/ubuntu-vg/ubuntu-lv` 下，并且单个文件的恢复可能会失败。 **推荐的操作：** 为了防止在 Ubuntu VM 上发生此问题，Cohesity 建议使用持久性设备命名方法装入文件系统。使用持久性命名即可使设备装入保持一致，从以后的备份中还原文件时将不会发生此问题。对于持久性设备命名，可通过 UUID 装入设备。 以下是 `/etc/fstab` 文件的示例，该文件包含使用 UUID 装入的设备： ■ UUID=93a21fe4-4c55-4e5a-8124-1e2e1460fece /boot ext4 defaults 1 2。 ■ UUID=55a24fe3-4c55-4e6a-8124-1e2e1460fadf /vola ext3 defaults 0 0。 要查找设备 UUID，可以使用以下命令之一： ■ `blkid` ■ `ls -l /dev/disk/by-uuid/`

创建虚拟机失败，无法继续执行还原。
`bpVMutil`
`pid=3144`
	如果用于还原虚拟私有云 (VPC) 环境中 VM 的备份主机版本为 NetBackup 10.1.1 或更早版本，还原作业将失败。
	推荐的操作
	使用备份主机版本 NetBackup 10.1.1 或更高版本还原 VPC 环境中的 VM。

从快照还原作业完成并显示部分成功状态。	如果 AHV 群集未根据 iSCSI 传输选项进行正确配置，则从快照还原作业完成并显示部分成功状态。 解决办法 根据 iSCSI 传输设置验证并修复以下错误： ■ 默认情况下：已配置 iSCSI 数据服务 IP。 ■ 对于分段：未配置分段 IP 地址。 ■ 对于 segmented_specified：未配置分段 iSCSI 接口，或者指定的 IP 地址与任何配置的分段 iSCSI 接口的虚拟 IP 都不匹配。
Nutanix-AHV 策略不支持 NetBackup 版本低于 11.0 的备份主机。	Cohesity 建议将 NetBackup 升级到最新版本。
NetBackup 状态：213，EMM 状态：NetBackup 介质服务器版本太低，无法执行此操作。没有可供使用的存储单元 (213)。	检查 Nutanix-AHV 策略中使用的存储单元。在其上创建存储单元的介质服务器应为 NetBackup 11.0 或更高版本。 有关更多详细信息，请查看以下路径中的日志：`/usr/openv/logs/nbwebservice`

10

适用于 AHV 的 API 和命令行选项

本章节包括下列主题：

- 使用 API 和命令行选项管理、保护或恢复 AHV 虚拟机
- 适用于 AHV 配置的其他 NetBackup 选项
- 有关重命名文件的其他信息

使用 API 和命令行选项管理、保护或恢复 AHV 虚拟机

本主题列出了用于保护或恢复 AHV 虚拟机的 API 和命令行选项。本主题仅介绍重要变量和选项。

本主题包含以下部分：

- 请参见第 114 页的“添加 AHV 群集”一节。
- 请参见第 114 页的“设置 iSCSI CHAP 设置 API”一节。
- 请参见第 115 页的“创建 AHV VM 备份策略”一节。
- 请参见第 116 页的“在原始位置对 AHV VM 进行恢复前检查”一节。
- 请参见第 117 页的“在其他位置对 AHV VM 进行恢复前检查”一节。
- 请参见第 117 页的“在原始位置还原 AHV VM”一节。
- 请参见第 119 页的“将 AHV VM 还原到备用位置”一节。

有关 API 和命令行的详细信息，请参考以下资料：

- 以下位置列出了所有 NetBackup API：
  Services and Operations Readiness Tools (SORT) > 知识库 > 文档

- 有关这些命令的更多信息，请参考《NetBackup 命令参考指南》。

添加 AHV 群集

表 10-1 添加 AHV 群集

API 或命令行选项	重要变量和选项
POST /netbackup/asset-service/queries GET /netbackup/asset-service/queries/{aqcId}	■ clusterName 是 AHV 群集的名称。 ■ backuphost 是 NetBackup 客户端的主机名。 ■ credentialName 是与 AHV 群集关联的凭据。 **注意：**必须存在具有所提及 credentialName 的凭据。
tpconfig 命令	■ virtual_machine 是 AHV 群集的名称。 ■ vm_type 是 9。数字 9 代表 AHV 群集。

设置 iSCSI CHAP 设置 API

表 10-2 设置 iSCSI CHAP 设置 API

API 或命令行选项	重要变量和选项
GET /netbackup/config/iscsi-settings/ {workloadType}	■ workloadType 指定支持的工作负载。 ■ 获取指定工作负载类型的全局 iSCSI 设置。

POST
/netbackup/config/iscsi-settings/
{workloadType}
	■ 更改指定工作负载类型的全局 iSCSI 设置。
	■ authType 为身份验证类型。例如：
	  ■ ONEWAY_CHAP
	  ■ MUTUAL_CHAP_AUTOMATIC
	■ passwordRenewalIntervalDays 仅适用于“双向 CHAP 自动”选项。
	注意：有效值为 1 - 365 天。

创建 AHV VM 备份策略

表 10-3 创建 AHV VM 备份策略

API 或命令行选项	重要变量和选项
POST /netbackup/config/policies/	■ policyType 为 Hypervisor。 ■ 使用 Web UI 时，policyType 为 Nutanix-AHV。 ■ backuphost 是代表虚拟机执行备份的 NetBackup 客户端的主机名。 ■ 对于 Nutanix AHV，添加 Add useVirtualMachine = 6。 ■ snapshotMethodArgs 可具有以下值以使用 VM UUID 备份 VM： ■ 在 backupSelections > selections 中，使用过滤器选项 Nutanix-ahv:/?filter=uuid Equal *<uuid_filter>*” 过滤具有特定 UUID 的 AHV VM。除了 UUID 之外，还可以使用针对智能 VM 组提到的其他过滤条件。
admincmd 命令	■ 在 bpplclients -add *<discoveryhost>* Hypervisor Hypervisor 中，Hypervisor 发现主机为列入允许列表的 Windows 或 Linux 主机。 ■ 在 bpplinfo 中，策略类型 (-pt) 为 Hypervisor。 ■ 在 bpplinclude 中，使用过滤器选项 Nutanix-ahv:/?filter=uuid Equal *<uuid_filter>*” 过滤具有特定 UUID 的 AHV VM。 ■ 在 bpplinfo 中 ■ 对于 AHV VM，use_virtual_machine 的值为 **6**。 ■ snapshot_method 的值为 Hypervisor_snap。

创建策略后，为策略创建日程表或触发策略备份等其他命令保持不变。有关这些命令的更多信息，请参考《NetBackup 命令参考指南》。

在原始位置对 AHV VM 进行恢复前检查

表 10-4 在原始位置对 AHV VM 进行恢复前检查

API 或命令行选项	重要变量和选项

`POST /netbackup/recovery/workloads /nutanix-ahv/scenarios/full-vm /pre-recovery-check`	■ `client` 是备份时使用的标识符。它可以是 `displayName` 或 `UUID`。
	■ `ahvCluster` 是备用 AHV 群集的名称。
	■ `recoveryHost` 是要用作 VM 恢复主机的服务器，以执行此恢复前检查。
	■ `vmDisks` 表示一个或多个虚拟机磁盘。
	■ `source` 是虚拟机磁盘的源路径。格式必须为 `/storage_container/disk_uuid`。
	■ `destination` 是虚拟机磁盘的目标路径。其格式应为 `/storage_container`。
	■ 设置以下值：
	`powerOnAfterRecovery`
	`overwriteExistingVm`
	`removeNetworkInterfaces`
	`retainVmGuid`
	`retainNicMacAddress`

在其他位置对 AHV VM 进行恢复前检查

表 10-5 在其他位置对 AHV VM 进行恢复前检查

API 或命令行选项	重要变量和选项

`POST /netbackup/recovery/workloads /nutanix-ahv/scenarios/full-vm /pre-recovery-check`	■ `client` 是备份时使用的标识符。它可以是 `displayName` 或 `UUID`。
	■ `ahvCluster` 是备用 AHV 群集的名称。
	■ `recoveryHost` 是要用作 VM 恢复主机的服务器，以执行此恢复前检查。
	■ `vmDisks` 表示一个或多个虚拟机磁盘。
	■ `source` 是虚拟机磁盘的源路径。格式必须为 `/storage_container/disk_uuid`。
	■ `destination` 是虚拟机磁盘的目标路径。其格式应为 `/storage_container`。
	■ 设置以下值：
	`powerOnAfterRecovery`
	`overwriteExistingVm`
	`removeNetworkInterfaces`
	`retainVmGuid`
	`retainNicMacAddress`

在原始位置还原 AHV VM

表 10-6 在原始位置还原 AHV VM

API 或命令行选项	重要变量和选项

`POST /netbackup/recovery/workloads/ahv/ scenarios/full-vm/recover`	■ `client` 是备份时使用的标识符。它可以是 `display name` 或 `UUID`。
	■ `recoveryHost` 是充当执行此恢复的 VM 恢复主机的服务器。
	■ 设置以下值：
	`powerOnAfterRecovery`
	`overwriteExistingVm`
	`removeNetworkInterfaces`
	`retainVmGuid`
	`retainNicMacAddress`

API 或命令行选项	重要变量和选项
bprestore 命令	■ vmproxy 指定备份主机的名称或 FQDN。 ■ vmserver 是 AHV 群集的名称。 ■ vmpoweron，用于在 VM 还原后启动 VM。 ■ vmsn，用于删除 VM 网络接口。 ■ vmid，用于保留 VM 的原始 VM UUID。或者，使用 -K 选项保留具有相同 UUID 的现有 VM 而不重写。 ■ -R选项定义重命名文件的路径。使用重命名文件可将 VM 恢复到备用位置，或更改 VM 配置。 重命名文件示例： change *vmname* to *new_vm_name* change */storage_domain_1/disk1_UUID* to /storage_domain_2/ change */storage_domain_1/disk2_UUID* to /storage_domain_2/ change *cluster* to *new_cluster_name* **注意：**对于 Windows NetBackup 主机，必须在重命名文件条目的末尾添加一个空行。请参见请参见第 121 页的"有关重命名文件的其他信息"。

将 AHV VM 还原到备用位置

表 10-7 将 AHV VM 还原到备用位置

API 或命令行选项	重要变量和选项
POST /netbackup/recovery/workloads/ahv /scenarios/full-vm/recover	■ client 是备份时使用的标识符。它可以是 displayName 或 UUID。 ■ ahvCluster 是备用 AHV 群集的名称。 ■ recoveryHost 是充当执行此恢复的 VM 恢复主机的服务器。 ■ vmDisks 表示一个或多个虚拟机磁盘。 ■ source 是虚拟机磁盘的源路径。其格式应为 /storage_container/disk_uuid。 ■ destination 是虚拟机磁盘的目标路径。其格式应为 /storage_container。 ■ 设置以下值： powerOnAfterRecovery overwriteExistingVm removeNetworkInterfaces retainVmGuid retainNicMacAddress

API 或命令行选项	重要变量和选项
bprestore 命令	■ vmproxy 指定备份主机的名称或 FQDN。 ■ vmserver 是 AHV 群集的名称。 ■ 使用以下值修改 VM 配置： ■ vmpoweron，用于在 VM 还原后启动 VM。 ■ vmsn，用于删除 VM 网络接口。 ■ vmid，用于保留 VM 的原始 VM UUID。或者，使用 -K 选项保留具有相同 UUID 的现有 VM 而不重写。 ■ -R选项定义重命名文件的路径。使用重命名文件可将 VM 恢复到备用位置，或更改 VM 配置。 重命名文件示例： change *vmname* to *new_vm_name* change */storage_domain_1/disk1_UUID* to /storage_domain_2/ change */storage_domain_1/disk2_UUID* to /storage_domain_2/ change *cluster* to *new_cluster_name* **注意：**对于 Windows NetBackup 主机，必须在重命名文件条目的末尾添加一个空行。 请参见第 121 页的"有关重命名文件的其他信息"。

适用于 AHV 配置的其他 NetBackup 选项

可使用以下 NetBackup 命令选项进行其他 AHV 配置：

NetBackup 服务器的 NUTANIX_AUTODISCOVERY_INTERVAL 选项。此选项控制 NetBackup 扫描 AHV 群集以发现要在 NetBackup Web UI 中显示的虚拟机的频率。

NetBackup 会首先尝试对上次发现尝试成功的同一主机执行自动发现。如果对该主机执行自动发现失败，NetBackup 将按以下顺序再次尝试对其他主机执行自动发现：

1. NetBackup 主服务器
2. 访问主机、客户端或代理服务器
3. 介质服务器

表 10-8

用法	重要变量和选项
POST /netbackup/asset-service/queries GET /netbackup/asset-service/queries/{aqcId}	■ clusterName 是 AHV 群集的名称。 ■ backuphost 是 NetBackup 客户端的主机名。 ■ credentialName 是与 AHV 群集关联的凭据。
tpconfig 命令	■ virtual_machine 是 AHV 群集的名称。 ■ vm_type 是 9。数字 9 代表 AHV 群集。

有关重命名文件的其他信息

- 您可以为所有磁盘或某些特定的磁盘列表指定目标存储容器。
- 如果没有为其中一个磁盘指定目标存储容器，则该磁盘将还原到原始位置。
- 如果为不存在或无效的磁盘指定目标存储容器，则 VM 还原将失败。
- 对于 Windows 备份主机，必须在所有重命名文件条目之后添加一个空行（回车）。

对于以下场景，在 /usr/openv/tmp 目录中创建或修改 rename 文件：

- 将 VM 恢复到备用容器
- 使用修改的 VM 名称将 VM 恢复到同一容器或备用容器

如果重命名文件不可用，则必须在 NetBackup 主服务器上创建它并将其另存为 rename.txt。

要设置备用位置或修改配置，请以给定格式在 rename 文件中添加以下行：

场景	要在 rename 文件中添加的行
更改虚拟机名称	change vmname to *newVMname*
将虚拟机恢复到其他 AHV 容器	change /<*original_container1*>/<*disk_uuid1*> to /<*alternate_container1*>

示例 rename 文件

通过以下 rename.txt，可以更改 VM 名称。

change vmname to *newVMname*

在 rename 文件中进行必要的更改后，您可以运行 `bprestore` 命令。