NetBackup™ Web UI 云管理指南

版本 **10.2**

VERITAS™

上次更新时间： 2023-04-28

法律声明

Veritas Technologies LLC
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 Veritas 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 Veritas 网站上找到：

https://sort.veritas.com/documents

文档反馈

您的反馈对我们非常重要。请提出您对本文档的改进建议，或者就本文档中的错误或疏漏进行报告。请注明所报告文本的文档标题、文档版本和章节标题。发送反馈到：

NB.docs@veritas.com

您也可以在以下 Veritas 社区站点中查看相关文档信息或进行提问：

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas 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

管理和保护云资产

本章节包括下列主题：

关于保护云资产

使用 NetBackup，现在可以保护云中工作负载。云数据保护框架利用 Snapshot Manager 基础架构加快云提供商的扩展。在 NetBackup 8.3 及更高版本中，Snapshot Manager 可保护 AWS、Azure、Azure Stack Hub 和 GCP 云中的资产。

下表介绍了这些任务。

表 1-1 配置云资产保护

任务	描述
在开始之前，请确保您拥有相应的权限。	要在 Web UI 中管理和保护云资产，您必须具有工作负载管理员角色或类似权限。NetBackup 安全管理员可以在单个资产级别、帐户或订购级别或者云提供商级别管理您的角色权限。 请参见 NetBackup Web UI 管理指南。 **注意：**要管理托管应用程序，您需要具有“管理资产”和“管理保护计划”权限。
部署 Snapshot Manager	在环境中安装 Snapshot Manager。 请参见第 11 页的“添加 Snapshot Manager”。 查看 Snapshot Manager 和 NetBackup 限制。 请参见第 8 页的“限制和注意事项”。
配置 Snapshot Manager	在 NetBackup 中注册 Snapshot Manager。 请参见《NetBackup Snapshot Client 管理指南》。
添加配置	将在 Web UI 中显示所有受支持的云提供商。 您需要为所需的云提供商添加云帐户（配置云插件）。您可以为每个提供商创建多个配置。 请参见第 12 页的“为 Snapshot Manager 添加云提供商”。 对于 Amazon，可以选择使用 IAM 角色。 请参见第 15 页的“AWS 配置的 IAM 角色”。
资产发现	NetBackup 将检索与 NetBackup 中配置的云帐户相关的云资产。资产填充在 NetBackup 资产数据库中。 默认情况下，资产发现每 2 小时进行一次，且可以进行配置。 对于应用程序，可以将发现间隔设置为 15-45 分钟。 请参见第 16 页的“发现 Snapshot Manager 上的资产”。

任务	描述
创建保护计划	创建保护计划。保护计划用于预定备份启动时段。 请参见 NetBackup Web UI 管理指南。 还可以为快照复制配置保护计划。请参见第 41 页的"配置 AWS 快照复制"。
选择保护虚拟机、应用程序或卷	对于每个云提供商，将显示搜索到的资产列表。将资产添加到保护计划。 请参见 NetBackup Web UI 管理指南。 也可以选择使用应用程序一致性快照保护应用程序。请参见第 47 页的"使用应用程序一致性快照保护云中的应用程序"。
恢复云资产	■ 可以使用恢复点恢复资产。 请参见第 65 页的"恢复云资产"。 请参见第 65 页的"恢复云资产"。 请参见第 72 页的"对云资产执行回滚恢复 "。 ■ 还可以使用 nbcloudrestore CLI 实用程序还原资产。 **注意：** 不要使用 bprestore CLI 进行还原 请参见 NetBackup 命令参考指南。
故障排除	请参见第 94 页的"对云工作负载保护问题进行故障排除"。

限制和注意事项

保护云工作负载时，请考虑以下事项

- Snapshot Manager 中不支持删除 NetBackup 主机条目及其关联的插件。
  如果删除在 NetBackup 中配置的插件，则无法恢复与该插件关联的任何 Snapshot Manager 映像。
- 有关 Snapshot Manager 功能的信息，请查看《NetBackup Snapshot Manager 安装和升级指南》。
- 如果您先前已安装 Snapshot Manager，则 Veritas 建议您升级 Snapshot Manager，而不是重新安装。
  如果确实重新安装 Snapshot Manager 服务器，则需要重新配置 Snapshot Manager 并执行所有与保护相关的步骤。
- 默认情况下，Snapshot Manager 配置了端口 443。

- 添加 Snapshot Manager 服务器后，主机将尝试使用 IPv6 地址发现云上的资产。如果在主机上找到 IPV6 地址，则会将应用程序配置为使用该地址。如果找不到 IPv6 地址，则使用 IPv4 地址。
- 对于 Snapshot Manager，不支持增强的审核功能。因此，当以非 root 而具有 NetBackup 管理员权限的用户身份添加或更新 Snapshot Manager 时，用户在审核期间会显示为 root。
- 如果使用 CloudFormation 模板部署 Snapshot Manager，则在使用该命令向 Snapshot Manager 节点注册主机上代理时，所使用的 IP 地址必须是专用 IP，而非公用 IP。

注意：Veritas 建议在 NetBackup 主服务器上启用交换空间，以用于对云资产组运行从快照备份作业。推荐的交换空间大小必须大于或等于系统内存的 1.5 倍。如果无法启用交换空间，建议使用具有更高内存配置的系统。

在 NetBackup 中配置 Snapshot Manager

可以使用 NetBackup Web UI 添加 Snapshot Manager。从 8.3 开始，Snapshot Manager 可以发现 Amazon Web Services 和 Microsoft Azure 美国政府云上的云资产。

请注意下列要点：

- 可以将多个 Snapshot Manager 关联到一个 NetBackup 主服务器。但是，只能将一个 Snapshot Manager 关联到一个 NetBackup 主服务器。
- 可以将多个介质服务器关联到一个 Snapshot Manager。只有链接到 NetBackup 主服务器的介质服务器才能链接到 Snapshot Manager。
- 现在，可以通过 NetBackup Web UI、REST API 和 CLI 管理资产的 Snapshot Manager 和控制发现，而无需与 Snapshot Manager 接口交互。
- 对于从快照备份作业，使用与 NetBackup 介质存储关联的服务器，而不是与 Snapshot Manager 关联的介质服务器。必须将与 NetBackup 介质存储关联的服务器连接到 Snapshot Manager，以便执行所有 Snapshot Manager 相关操作。

下表介绍了基本任务。

表 1-2 配置 Snapshot Manager

任务	描述
添加 Snapshot Manager	要在 NetBackup 中添加 Snapshot Manager，必须添加 Snapshot Manager 的凭据并验证其证书。请参见第 11 页的"添加 Snapshot Manager"。
添加云提供商	要发现 Snapshot Manager 上的资产，必须添加云提供商。请参见第 12 页的"为 Snapshot Manager 添加云提供商"。
发现 Snapshot Manager 上的资产	可以发现 Snapshot Manager 上的资产。请参见第 16 页的"发现 Snapshot Manager 上的资产"。
关联介质服务器	要将快照和还原工作流程卸载到介质服务器，必须将介质服务器关联到 Snapshot Manager。请参见第 16 页的"将介质服务器与 Snapshot Manager 相关联"。

配置第三方 CA 证书

可以使用自签名证书或第三方证书验证 Snapshot Manager。

请注意以下几点：

- 对于 Windows，可通过文件路径的形式提供证书，也可以在可信根证书颁发机构中安装第三方证书。
- 对于已添加的 Snapshot Manager，要从自签名证书切换到第三方证书，可以更新 `tpconfig` 命令或编辑 Snapshot Manager API，或者从 NetBackup Web UI 进行切换。

配置第三方 CA 证书

1 为 Snapshot Manager 生成第三方证书和私钥。

2 运行 /cloudpoint/scripts/cp_certificate_management.sh 脚本，将证书、密钥和信任存储区上传到 Snapshot Manager。

3 在 NetBackup 中，创建证书文件，并在 pem 文件中附加根证书和所有中间 CA 证书。

4 在 `/cloudpoint/openv/netbackup/` 下的 `bp.conf` 文件中，创建以下条目：

- ECA_TRUST_STORE_PATH = /cloudpoint/eca/trusted/cacerts.pem
- （可选）VIRTUALIZATION_CRL_CHECK = CHAIN
- （可选）ECA_CRL_PATH =/cloudpoint/eca/crl/

注意：CA 证书和 CRL 应存在于 `/cloudpoint/eca/trusted/cacerts.pem`（对于信任存储区）和 `/cloudpoint/eca/crl` 下（对于 CRL）。

- ECA_CRL_PATH 选项指定外部证书颁发机构 (CA) 的证书吊销列表 (CRL) 所在目录的路径。ECA_CRL_PATH 中的所有文件都必须采用 DER、PEM 和 P7B 格式。
- 仅当要检查证书的吊销状态时，才需要 VIRTUALIZATION_CRL_CHECK 选项。默认情况下，VIRTUALIZATION_CRL_CHECK 选项处于禁用状态。
- 可以禁用 VIRTUALIZATION_CRL_CHECK 选项的值：LEAF 或 CHAIN。对于 LEAF，根据 CRL 验证分支证书的吊销状态。对于 CHAIN，根据 CRL 验证证书链中所有证书的吊销状态。

注意：应按以下顺序上传证书：分支证书 > 中间证书 > 根证书。如果未按正确的顺序上传证书，Snapshot Manager 可能无法工作。

5 将 Snapshot Manager 添加到 NetBackup，或运行 `tpconfig` 命令以更新已添加到 NetBackup 的 Snapshot Manager 的证书。

添加 Snapshot Manager

可以使用 NetBackup Web UI 添加 Snapshot Manager。必须提供 Snapshot Manager 凭据并验证证书。

注意： 要允许从快照进行备份，需要在 Snapshot Manager 和 NetBackup 服务器之间建立双向连接

添加 Snapshot Manager

1 在左侧，单击“**云**”。

2 单击 **Snapshot Manager** 选项卡。

3 单击“**添加**”。

4 在 **Snapshot Manager** 字段中，输入以下内容之一：

- Snapshot Manager 的主机名或 IP 地址。
  主机名或 IP 地址必须与在 Snapshot Manager 安装期间配置 Snapshot Manager 时提供的主机名或 IP 地址相同。
- 如果配置了 DNS 服务器，则输入 Snapshot Manager 的 FDQN。

5 在“端口”字段中，输入 Snapshot Manager 的端口号。

默认端口值为 443。

6 单击“验证”。

7 在“验证证书”对话框中，单击“接受”。

8 输入在安装 Snapshot Manager 时提供的 Snapshot Manager 凭据。

9 单击“保存”。

注意：如果 NetBackup 安全级别设置为 VERY HIGH，则会显示其他字段“令牌”，您可以提供标准主机令牌。要在 Snapshot Manager 上生成 NetBackup 证书，必须使用该令牌。您可能需要联系安全管理员或备份管理员，请求生成令牌所需的其他安全权限。

为 Snapshot Manager 添加云提供商

可以保护 Amazon Web Services (AWS)、Google Cloud Platform (GCP)、Microsoft Azure 和 Microsoft Azure Stack Hub 云提供商上的资产。从 9.0 开始，Snapshot Manager 可以发现 Amazon Web Services 和 Microsoft Azure 美国政府云工作负载。

为 Snapshot Manager 添加云提供商

1 在左侧，单击“云”。

2 在要为其添加配置的云提供商下，单击“提供商”选项卡或单击“添加”。

3 在“添加配置”窗格中的“配置名称”字段中输入一个值。

4 选择首选 **Snapshot Manager**。

5 输入所需详细信息。

云提供商	参数	描述
Microsoft Azure	凭据类型：**应用程序服务主体**	
	租户 ID	在其中创建应用程序的 AAD 目录的 ID。
	客户端 ID	应用程序 ID。
	Secret key	应用程序的密钥。
	凭据类型：**System managed identity**	在 Azure 中的 Snapshot Manager 主机上启用系统托管标识。 **注意：** 为系统托管标识分配角色。
	凭据类型：**用户托管标识**	
	客户端 ID	连接到 Snapshot Manager 主机的用户托管标识的 ID。
	以下参数适用于上述所有凭据类型	
	区域	要在其中发现云资产的一个或多个区域。 **注意：**如果您配置的是政府云，请选择“美国政府亚利桑那州”、“美国政府德克萨斯州”或“美国政府弗吉尼亚州”。
	资源组前缀	要用来附加资源组中所有资源的字符串。
	即使未找到带前缀的资源组也保护资产	该复选框用于确定在资产未与任何资源组关联时是否对其进行保护。

云提供商	参数	描述
Microsoft Azure Stack Hub	*使用 AAD：* **Azure Stack Hub 资源管理器端点 URL**	采用以下格式的端点 URL，允许 Snapshot Manager 与 Azure 资源连接。 `https://management.<location>.<FQDN>`
	租户 ID	在其中创建应用程序的 AAD 目录的 ID。
	客户端 ID	应用程序 ID。
	密钥	应用程序的密钥。
	身份验证资源 URL（可选）	身份验证令牌发送到的 URL。
	使用 ADFS： **Azure Stack Hub 资源管理器端点 URL**	采用以下格式的端点 URL，允许 Snapshot Manager 与 Azure 资源连接。 `https://management.<location>.<FQDN>`
	租户 ID	在其中创建应用程序的 AAD 目录的 ID。
	客户端 ID	应用程序 ID。
	密钥	应用程序的密钥。
	身份验证资源 URL（可选）	身份验证令牌发送到的 URL。
Amazon AWS **注意：**如果 Snapshot Manager 配置了 IAM Config，则“**访问密钥**”和“**密钥**”选项不可用。	**访问密钥**	访问密钥 ID，与机密访问密钥一起指定时，授权 Snapshot Manager 与 AWS API 交互。
	密钥	应用程序的密钥。
	区域	要在其中发现云资产的一个或多个 AWS 区域。 **注意：**如果配置了政府云，请选择 us-gov-east-1 或 us-gov-west-1。

云提供商	参数	描述
Google Cloud Platform	**项目 ID**	从中管理资源的项目的 ID。在 JSON 文件中列为 `project_id`。
	客户端电子邮件	客户端 ID 的电子邮件地址。在 JSON 文件中列为 `client_email`。
	私钥	私钥。在 JSON 文件中列为 `private_key`。 **注意：**输入此密钥时不能带引号。不要在密钥的开头或结尾输入任何空格或回车符。
	区域	提供商在其中有业务运营的区域列表。

6 在“**添加配置**”窗格中，输入连接和身份验证详细信息。

7 单击“**保存**”。

将自动发现云提供商上的资产。

AWS 配置的 IAM 角色

如果在云中部署 Snapshot Manager，则可以将 AWS 配置配置为使用 IAM 角色进行身份验证。

请参见第 12 页的“为 Snapshot Manager 添加云提供商”。

在继续之前，请确保满足以下条件：

- 已在 AWS 中配置 IAM 角色。有关详细信息，请参见《NetBackup Snapshot Manager 安装和升级指南》。
- 将 NetBackup 和 Snapshot Manager 升级到最新版本后，需要更新凭据。运行以下命令：

```
tpconfig -update -snapshot_manager <snapshot manager host>
-snapshot_manager_user_id <snapshot manager user ID>
-manage_workload <workload type> -security_token <security token>
```

注意： 升级后，凭据将更新为仅支持 IAM 角色。

支持以下 IAM 角色实现：

- 源帐户：在这种情况下，需要保护的云资产与 Snapshot Manager 位于相同的 AWS 帐户。因此，AWS 云可识别 AWS 帐户 ID 和角色名称，您只需选择区域即可。

- 跨帐户：在这种情况下，需要保护的云资产与 Snapshot Manager 位于不同的 AWS 帐户。因此，需要输入目标帐户和目标角色名称详细信息以及区域，以便 Snapshot Manager 可以访问这些资产。
  需要在源和目标帐户之间建立信任关系。例如，如果以下是要用于配置插件的角色的角色 ARN：
  arn:aws:iam::935923755:role/TEST_IAM_ROLE
  因此，要配置插件，请提供 ARN 的最后一部分，其名称为 *TEST_IAM_ROLE*
  有关更多详细信息，请参考 *Amazon Web Services* 文档中的“使用 IAM 角色访问 AWS 帐户”相关信息。

将介质服务器与 Snapshot Manager 相关联

可以使用介质服务器卸载云的快照和还原作业。要实现此目标，必须将一个或多个介质服务器与 Snapshot Manager 相关联。介质服务器必须处于活动状态才能运行快照或还原作业。与 Snapshot Manager 关联的介质服务器也必须与 NetBackup 主服务器相关联。但是，发现作业仅在 NetBackup 主服务器上运行。

将介质服务器与 Snapshot Manager 相关联

1. 在左侧，单击“**云**”。
2. 单击 **Snapshot Manager** 选项卡。
3. 从 Snapshot Manager 旁边的菜单中，单击“**高级设置**”。
4. 在“**介质服务器**”选项卡上，选择要与 Snapshot Manager 关联的一个或多个介质服务器。
5. 单击“**保存**”。

发现 Snapshot Manager 上的资产

在 Snapshot Manager 中配置云提供商后，将触发自动发现以发现云中的资产。定期发现期间，NetBackup 每两小时从 Snapshot Manager 提取一次资产数据，而 Snapshot Manager 每一小时从云提供商配置提取一次资产数据。如果禁用 Snapshot Manager，则与该服务器关联的所有资产将不再受保护，也不与 NetBackup 同步。

如果需要，也可以通过对单个云提供商配置使用 *“发现”* 选项，手动触发云资产发现，还可以在 Snapshot Manager 上触发发现，以获取 Snapshot Manager 上的可用资产数据。

在第一次完全发现之后，NetBackup 随后会定期对已配置的 Snapshot Manager 执行资产增量发现。它仅检测在上次发现和当前发现之间发生的更改，如资产的添加、删除或修改。

注意：为了实现精确的增量发现，请确保在 NetBackup 主服务器和 Snapshot Manager 上根据所处时区正确地设置时间，以避免发现出现任何问题。

以下过程介绍了如何在 Snapshot Manager 级别执行发现，此操作实际上并不会发现云中的资产，而只是从 Snapshot Manager 获取时间点数据。

发现 Snapshot Manager 上的资产

1 在左侧，单击“**云**”。

2 单击 **Snapshot Manager** 选项卡

3 从 Snapshot Manager 旁边的菜单中，单击“**发现**”。

以下过程介绍了如何在配置级别执行发现，这会触发资产的深度发现并获取资产的时间点状态，从而检测云中资产的任何添加、修改或删除。

发现云提供商配置的资产

1 在左侧，单击“**云**”。

2 单击 **Snapshot Manager** 选项卡

3 单击要查看其云提供商的 Snapshot Manager IP 或主机名。

4 单击要查看其配置的提供商选项卡。

5 从配置名称旁边的菜单中，单击“**发现**”。

注意：如果云提供商配置上的发现所需时间超过 30 分钟，则发现操作将超时。但是，后续操作会继续，将 NetBackup 资产与 Snapshot Manager 资产同步。

更改 Snapshot Manager 的自动发现频率

使用 `nbgetconfig` 和 `nbsetconfig` 命令查看、添加或者更改自动发现选项。例如：

`CLOUD_AUTODISCOVERY_INTERVAL` = **秒数**

有关详细信息，请参见 NetBackup 管理指南，第 I 卷。

编辑 Snapshot Manager

可以更新 Snapshot Manager 凭据。但是，不能编辑 Snapshot Manager 的主机名、IP 地址或端口。

编辑 Snapshot Manager

1 在左侧，单击“**云**”。

2 单击 **Snapshot Manager** 选项卡。

3 从 Snapshot Manager 旁边的菜单中，单击“**编辑**”。

只能编辑 Snapshot Manager 的凭据。必须先验证证书才能更新凭据。

4 更新凭据。

5 在“**令牌**”字段中，为 Snapshot Manager 输入重新发布令牌

6 单击“**保存**”。

启用或禁用 Snapshot Manager

根据您的首选项，可以启用或禁用 Snapshot Manager。如果禁用 Snapshot Manager，则无法发现资产或分配保护计划。

启用或禁用 Snapshot Manager

1 在左侧，单击“**云**”。

2 单击 **Snapshot Manager** 选项卡。

3 根据 Snapshot Manager 状态，选择“**启用**”或“**禁用**”。

注意：禁用 Snapshot Manager 后，对该服务器相关资产的保护将开始失败。在这种情况下，请从保护计划取消订购资产或取消任何暂停的 SLP 操作，以避免在禁用期间看到作业失败。

（可选）添加 Snapshot Manager 扩展

该 Snapshot Manager 扩展用于扩展 Snapshot Manager 主机的容量，可在 Snapshot Manager 服务器达到其峰值性能容量时，为服务器上并行运行的大量请求提供服务。可以根据作业运行要求，在本地或云中安装一个或多个 Snapshot Manager 扩展，而不会给主机增加额外压力。扩展可以增加 Snapshot Manager 主机的处理容量。

此 Snapshot Manager 扩展可以具有与 Snapshot Manager 主机相同或更高的配置。

支持的 Snapshot Manager 扩展环境：

- 基于 VM 的扩展（适用于本地）
- 具有托管 Kubernetes 群集的基于云的扩展

请参考最新版本 NetBackup Snapshot Manager 安装和升级指南中的“部署 Snapshot Manager 扩展”一章。

管理智能云组

可根据一组过滤器（称为查询）定义智能云资产组，从而创建和保护动态资产组。NetBackup 会根据查询选择云虚拟机、应用程序或卷，并将其添加到组中。智能组会自动反映资产环境中的更改，因此在环境中添加或删除资产时，不必手动修改组中的资产列表。

然后，将保护计划应用于智能云资产组时，如果将来资产环境发生更改，则满足查询条件的所有资产将自动受到保护。

注意：只有您的角色对需要管理的云资产具有必要的 RBAC 权限时，才能创建、更新或删除智能组。NetBackup 安全管理员可授予您对与特定帐户或订购关联的资产类型（VM、PaaS、应用程序、卷、网络）的访问权限，或者授予您云提供商级别的访问权限。请参考《NetBackup Web UI 管理指南》。

创建智能云组

创建智能云组

1 在左侧，单击“**云**”。

2 单击“**智能组**”选项卡，然后单击“**+ 添加**”。

3 为组输入名称和描述。

4 选择云提供商、帐户 ID 和区域。

注意：如果未指定区域，则云智能组将跨区域保护资产。

5 选择“**资产类型**”。

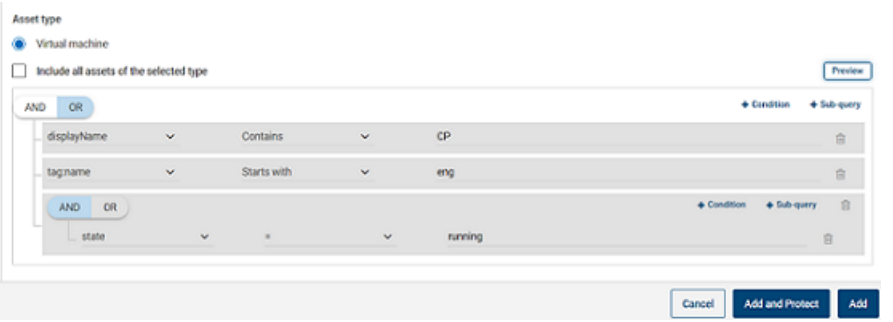
6 然后执行下列操作之一：

- 选择“**包括所选类型的所有资产**”。
  此选项使用默认查询选择所有资产，以便在保护计划运行时进行备份。
- 要仅选择满足特定条件的资产，请创建自己的查询：单击“**添加条件**”。

7 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。

请参见第 21 页的“用于创建智能云组的查询选项”一节。

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** 缩小查询范围：它仅选择其显示名称中具有 `cp`、还具有名为 `eng` 的标记并且处于正在运行状态的 VM。

注意：标记名称中不支持特殊字符 **'<'**。如果存在特殊字符，创建资产组将失败。

注意：NetBackup 中的已知限制 - 如果您创建的查询所具有的资产标记名称（从云提供商处引用）包含空格或特殊字符，例如 `(,)`, `&`, `\`, `/`, `"`, `[`, `]`, `{`, `}`，则稍后无法编辑该查询以编辑任何参数。这不会阻止您成功创建智能组，以及将保护计划应用于该智能组。只有“编辑查询”功能会受此限制影响。

要避免此问题，请确保标记名称不包含指定的特殊字符，并且使用新标记名称创建新查询。

也可以向条件中添加子查询。单击“**+ 子查询**”并单击 **AND** 或 **OR**，然后选择子查询条件的关键字、运算符和值。

8 要测试查询，请单击“**预览**”。

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资产。因此，查询在保护计划运行时稍后选择的资产可能与预览中当前列出的资产不同。

注意：当在“**智能组**”中使用查询时，如果查询条件包含非英文字符，则 NetBackup Web UI 可能不会显示与该查询匹配的资产的准确列表。

在任何属性上使用 `not equals` 过滤器条件所返回的资产将包括属性不存在值 (null) 的那些资产。对于多值属性（如 `tag`），不会返回与其中一个属性值都不匹配的资产

注意：单击“**预览**”或保存组时，如果为组选择资产，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“**智能组**”字段将为 `none`。

---

9 要保存组而不将其添加到保护计划，请单击“**添加**”。

要保存组并应用保护计划，请单击“**添加和保护**”。选择计划，然后单击“**保护**”。

用于创建智能云组的查询选项

注意：属性值可能与云提供商门户上显示的值不完全匹配。可以参考资产详细信息页面或云提供商对单个资产的 API 响应。

表 1-3 查询关键字

关键字	描述 （所有值都区分大小写）
`displayName`	资产的显示名称。
`state`	例如，正在运行、已停止等。
`tag`	分配给资产的标签，用于分类。
`instanceType/machineType/vmSize`	资产的实例/计算机类型或 VM 大小，具体取决于选择的云提供商。 例如，t2.large、t3.large 或 b2ms、d2sv3

表 1-4 查询运算符

运算符	说明
Starts with	匹配出现在字符串开头的值。
Ends with	匹配出现在字符串结尾的值。
Contains	匹配字符串内出现该值时输入的值。
=	仅匹配输入的值。
!=	匹配任何值（所输入的值除外）。

注意：创建智能组后，将无法编辑为其选择的云提供商，但是可以编辑名称和描述，并根据需要修改查询。

删除智能云组

删除智能云组

1 在左侧，单击“**云**”。

2 在“**智能组**”选项卡下找到该组。

3 如果该组不受保护，则选择该组，然后单击“**删除**”。

4 如果该组受到保护，请单击该组，向下滚动并单击“**删除保护**”。

5 然后在“**智能组**”选项卡下选择该组，单击“**删除**”。

保护云资产或智能云组

可以为云工作负载创建特定于云提供商的保护计划。然后，可以为与云提供商关联的资产订购特定于该提供商的保护计划。

注意：如果以前具有应用于不同云提供商资产的保护计划，则会自动转换为新的特定于提供商的格式。此转换在升级到 NetBackup 9.1 之后进行。例如，如果在一个保护计划中订购了来自 Google 云和 AWS 云的资产，则该保护计划将进行拆分。保护计划将拆分为适用于每个提供商的两个单独保护计划。

请参见第 23 页的“升级到 NetBackup 9.1 后转换保护计划”一节。部分。

使用以下步骤为保护计划订购云 VM、应用程序、卷或智能组。为保护计划订购资产时，需为资产指定预定义的备份设置。

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。

保护云资产或智能组

1 在左侧，单击“**云**”。

2 在“**虚拟机**”选项卡、“**应用程序**”选项卡、“**卷**”选项卡或“**智能组**”选项卡上，单击资产或资产组对应的框，然后单击“**添加保护**”。

3 选择保护计划，然后单击“**下一步**”。

4 用户可以调整以下设置：

- **日程表和保留**
- **存储选项**
  有关 Web UI 中的存储选项的更多信息，请查看 NetBackup Web UI 管理指南中的“配置存储”部分。
- **备份选项**

5 单击“**保护**”。

用于立即保护的“立即备份”选项

除了预定的保护计划外，还可以使用“**立即备份**”选项立即备份资产，防止出现任何计划外情况。

1. 选择云资产或智能组，然后单击“**立即备份**”。
2. 然后选择要应用的保护计划。仅与资产的特定云提供商相关的保护计划显示为选项。
3. 单击“**开始备份**”。

   随即会触发备份作业，可以在“**活动监视器**”页面上跟踪该备份作业。

有关更多信息，请参见 NetBackup Web UI 管理指南。

升级到 NetBackup 9.1 后转换保护计划

请注意以下有关将旧保护计划自动转换为新格式的要点。

- 将 NetBackup 升级到 9.1 后资产迁移完成时，保护计划转换开始。
- 未订购资产的旧保护计划不会转换为新格式。您可以手动删除它们。
- **转换之前或转换期间**
  - 旧保护计划中的所有资产将取消订购，而订购到转换后的保护计划中。
  - 旧保护计划无法订购新资产。

- 对于旧计划，“**立即备份**”操作将失败。
- 禁止自定义或编辑旧保护计划。

- **成功转换后**
  - 如果旧保护计划仅用于保护来自一个云提供商的资产，则在转换后新计划保留相同的名称和资产订购。
  - 如果旧保护计划用于保护来自多个云提供商的资产，则旧保护计划的名称将保持不变。转换后，保护计划名称将更新，以保留任何一个云提供商的资产订购。
    对于旧计划中的其他云提供商，转换后会创建新的保护计划，新保护计划中仅订购相应提供商各自的资产。新计划按以下格式命名：
    `<old_plan_name>_<cloud_provider>`。
  - 因此，可能会在 Web UI 的 *“保护计划”* 菜单中看到比之前更多的计划。
  - 转换成功消息显示在通知中，如下所示：
    在转换为新格式期间创建了保护计划 <protectionPlanName>。
    已成功将保护计划 <protectionPlanName> 转换为新格式。
    然后，可以开始照常管理和应用转换后的保护计划。

失败情形

请参考以下内容，了解如何处理保护计划转换期间或之后失败的情形。还要检查有关任何失败警报的通知，并采取必要操作。

- 某些资产可能无法从旧保护计划取消订购。在这种情况下，已成功取消订购的资产仍可继续转换。失败的资产转换过程每 4 小时重试一次。
- 转换后，某些资产可能无法自动重新订购到新计划。在这种情况下，需要手动将这些资产订购到转换后的保护计划。
- 将所需的访问权限分配给新的转换后的保护计划时，可能会失败。在这种情况下，需要手动分配访问权限。

自定义或编辑云资产或智能组的保护

您可以编辑保护计划的某些设置，包括日程表备份时段和其他选项。

自定义或编辑云资产的保护计划

1 在左侧，单击“**工作负载**” > **云**。

2 在“**虚拟机**”选项卡、“**应用程序**”选项卡、“**卷**”选项卡或“**智能组**”选项卡上，单击要为其自定义保护的资产。

3 单击“**自定义保护**” > “**继续**”。

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**
  为 Google 云资产启用/禁用区域快照，或者为 Azure 和 Azure Stack Hub 资产指定/更改快照目标资源组。

从云资产或智能组中删除保护

可为云资产取消订购保护计划。为资产取消订购计划后，将不再执行备份。

删除对云资产的保护

1 在左侧，单击“**云**”。

2 在“**虚拟机**”选项卡、“**应用程序**”选项卡、“**卷**”选项卡或“**智能组**”选项卡上，单击要删除保护的资产。

3 单击“**删除保护**”>“**是**”。

云资产清理

在清理周期内自动清理云资产，或根据以下条件手动清理云资产：

- 没有针对云资产的活动保护计划。
- 在过去 30 天（清理期限）内未发现资产。
- 不存在恢复点。
- 资产已标记为删除（已在 Snapshot Manager 上删除资产）。

用户可在 `bp.conf` 文件中更新资产清理期限并提供特定过滤条件，来增强此云资产清理条件。必须在 `bp.conf` 文件中配置以下参数：

- CLOUD.CLEANUP_AGE_MINUTES
- CLOUD.CLEANUP_FILTER

例如，

```
/usr/openv/netbackup/bin/nbsetconfig

nbsetconfig> CLOUD.CLEANUP_AGE_MINUTES = 180

nbsetconfig> CLOUD.CLEANUP_FILTER = "provider eq 'aws'"

nbsetconfig>
```

用户还可以使用具有以下请求正文的 `cleanup-assets` 命名查询手动运行 POST 查询，然后使用从 POST 响应中获取的查询 ID 运行 GET，如以下示例所述：

```
{
    "data":{
    "type":"query",
    "attributes":{
        "queryName":"cleanup-assets",
        "workloads":["cloud"],
        "parameters": {
            "cleanup_age_minutes": 180
        },
        "filter": "provider eq 'aws'"
      }
    }
}
```

云资产过滤

用户可以根据属性定义自定义过滤器，这些属性用于将资产列入“虚拟机”、“应用程序”、PaaS 和“卷”选项卡中。

创建过滤器

1 在左侧，单击“**云**”。

2 在“虚拟机”、“应用程序”、PaaS 或“卷”选项卡下，单击屏幕右上方的“**过滤器**”图标。

将显示“**创建过滤器**”选项。

3 单击“**创建过滤器**”选项，根据属性定义自定义过滤器，以将资产列入“虚拟机”、“应用程序”、PaaS 或“卷”选项卡中。

4 要创建过滤器，请输入以下参数的详细信息：

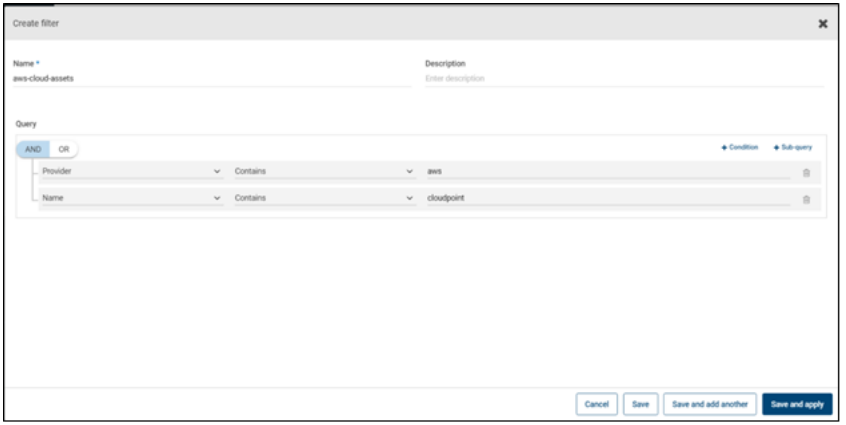
参数	描述
名称	过滤器的名称。
描述	提供过滤器的描述。
查询	要仅选择满足特定条件的资产，请创建自己的查询。

5 要仅选择满足特定条件的资产，请创建自己的查询：单击“**+ 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。

请参见第 21 页的“用于创建智能云组的查询选项”一节。

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** 缩小查询范围：它仅选择其显示名称中具有 `aws`、“**名称**”还为 `cloudpoint` 并且处于**正在运行状态**的 VM。

也可以向条件中添加子查询。单击“**+ 子查询**”并单击 **AND** 或 **OR**，然后选择子查询条件的关键字、运算符和值。

用于创建过滤器的查询选项

注意：属性值可能与云提供商门户上显示的值不完全匹配。可以参考资产详细信息页面或云提供商对单个资产的 API 响应。

表 1-5 查询关键字

关键字	描述 （所有值都区分大小写）
`Server type`	服务器的类型。
`Instance ID`	资产的实例 ID，具体取决于选择的云提供商。
`Instance name`	资产的实例名称，具体取决于选择的云提供商。

关键字	描述 （所有值都区分大小写）
Name	资产的显示名称。
Provider	资产的云提供商名称。
Region	资产的云提供商区域名称。
配置 ID	资产的配置 ID。
数据库服务	资产的数据库服务。
已删除	已删除的资产。
实体类型	资产的实体类型。
服务域	资产的服务域。
Snapshot Manager	向其注册资产的 Snapshot Manager 实例。

表 1-6 查询运算符

运算符	说明
Starts with	匹配出现在字符串开头的值。
Ends with	匹配出现在字符串结尾的值。
Contains	匹配字符串内出现该值时输入的值。
=	仅匹配输入的值。
!=	匹配任何值（所输入的值除外）。

AWS 和 Azure 政府云支持

从 8.3 开始，Snapshot Manager 可以发现 Amazon Web Services 和 Microsoft Azure 美国政府云工作负载。将 Snapshot Manager 添加到 NetBackup 后，可由 NetBackup 来保护工作负载。NetBackup 符合在 AWS 和 Azure 美国政府云工作负载上部署 Snapshot Manager 的法规要求（包括 IPv6 支持）。

配置 AWS 或 Azure 美国政府云后，系统会创建 AWS 和 Azure 代理服务，该服务将根据提供的区域发现云资产。发现的资产显示在 NetBackup 中。目前，仅发现和保护选定区域和映射端点中的工作负载。对于同一 Snapshot Manager 主机，不能同时使用公共云和政府云。

如果在插件资产操作正在进行时更新云插件，则可能会出现错误。

Snapshot Manager 支持以下 GovCloud（美国）区域：

云提供商	GovCloud（美国）区域
Amazon Web Services	■ us-gov-east-1 ■ us-gov-west-1
Microsoft Azure	■ 美国政府亚利桑那州 ■ 美国政府德克萨斯州 ■ 美国政府弗吉尼亚州

注意：PaaS 资产不支持政府云。

有关配置 AWS 和 Microsoft Azure 的信息，请参见第 12 页的"为 Snapshot Manager 添加云提供商"。

关于使用资源组保护 Microsoft Azure 资源

NetBackup 用于为包含受保护的虚拟机和卷的每个资源组定义对等资源组快照目标。

Microsoft Azure 中的所有资源都与一个资源组相关联。快照创建后，会与一个资源组关联。此外，每个资源组都与一个区域关联。请参见下面的内容：

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal

Snapshot Manager 创建快照并将快照置于资源所属的资源组中，即使在下列情况下也是如此：

- 没有为资源组提供前缀
- 未创建对等资源组
- 允许创建快照

您可以配置设置，以将快照置于非资源关联的资源组中。但是，请注意下列要点：

- 对等资源组必须与资源的资源组位于同一区域。
- 如果找不到对等资源组，则配置将确定快照创建是否成功。

要启用此功能，必须创建对等资源组。随后，Snapshot Manager 会附加与资源关联的资源组的前缀。创建快照时，对等资源组名称将基于与资源关联的前缀和资源组派生。

注意：现在，可以在创建保护计划时直接将快照与现有对等资源组相关联。但是，本部分所述的通过指定前缀定义对等资源组的功能仍然存在。

有关完整过程，请参考《NetBackup Web UI 管理指南》中有关创建保护计划的信息。

开始之前

- 对等资源组必须对使用资源组保护的资源可用。
- 如果指定了前缀，则插件配置的区域不得与其他配置重叠。

限制和注意事项

- 资源组名称中仅允许使用字母数字字符、句点、下划线、连字符或圆括号。
- 前缀长度必须少于 89 个字符。
- 不得使用 Azure 配置禁止用于资源组命名约定的字符。

关于资源组配置和结果

下表列出了虚拟机和资源组设置、资源配置和结果的各种场景。

表 1-7 配置和结果

资源组前缀	“即使未找到带前缀的资源组也保护资产”复选框	结果
未指定	未选择	NetBackup 将新创建的快照与资源的资源组相关联。
已指定	未选择	当满足以下条件时，NetBackup 会创建新的快照并将快照关联到对等资源组： ■ 已创建对等资源组。 ■ 对等资源组与资源组位于同一区域。 如果不满足以上条件，快照作业将失败。

资源组前缀	“即使未找到带前缀的资源组也保护资产”复选框	结果
已指定	已选择	当满足以下条件时，NetBackup 会创建新的快照并将快照关联到对等资源组： ■ 已创建对等资源组。 ■ 对等资源组与资源组位于同一区域。 如果未创建对等资源组或对等资源组位于其他区域，则新创建的快照将关联到受保护资源的资源组。

资源组配置示例

下表列出了资源组配置的示例。

表 1-8 示例配置

条件	配置	结果
■ 操作系统和所有磁盘都在同一资源组中。 ■ 对等资源组命名正确。 ■ 对等资源与资源的资源组位于同一区域。	■ 已提供资源组前缀值。 ■ 已选中“**即使未找到带前缀的资源组也保护资产**”复选框。	在对等资源组中创建快照。
■ 操作系统和所有磁盘都位于单独的资源组中。 ■ 对等资源组命名正确。 ■ 对等资源与资源的资源组位于同一区域。	■ 已提供资源组前缀值。 ■ 已选中“**即使未找到带前缀的资源组也保护资产**”复选框。	在对等资源组中创建快照。
■ 操作系统和所有磁盘都在同一资源组中。 ■ 对等资源组与资源的资源组在不同区域中创建。	■ 已提供资源组前缀值。 ■ 已选中“**即使未找到带前缀的资源组也保护资产**”复选框。	在原始资源组而不是对等资源组中创建快照。
■ 操作系统和所有磁盘都在同一资源组中。 ■ 未创建对等资源组。	■ 已提供资源组前缀值。 ■ 已选中“**即使未找到带前缀的资源组也保护资产**”复选框。	在原始资源组而不是对等资源组中创建快照。

条件	配置	结果
■ 操作系统和所有磁盘都位于单独的资源组 RG1 和 RG2 中。 ■ 对等资源组 RG1 命名正确，并与资源位于同一区域。 ■ 未创建对等资源组 RG2。	■ 已提供资源组前缀值。 ■ 已选中“**即使未找到带前缀的资源组也保护资产**”复选框。	在对等资源组 RG1 和原始资源组 RG2 中创建快照。
■ 操作系统和所有磁盘都在同一资源组中。 ■ 对等资源组命名正确。 ■ 对等资源组与资源的资源组位于不同区域。	■ 已提供资源组前缀值。 ■ 未选中“**即使未找到带前缀的资源组也保护资产**”复选框。	未创建快照，作业失败。
■ 操作系统和所有磁盘都在同一资源组中。 ■ 未创建对等资源组。	■ 已提供资源组前缀值。 ■ 未选中“**即使未找到带前缀的资源组也保护资产**”复选框。	未创建快照，作业失败。
■ 操作系统和所有磁盘都位于单独的资源组 RG1 和 RG2 中。 ■ RG1 和 RG2 的对等资源组（即 snapRG1 和 snapRG2）位于不同的区域。 ■ 对等资源组 snapRG1 与资源组 RG1 位于同一区域。 ■ 对等资源组 snapRG2 与资源组 RG2 位于不同区域。	■ 已提供资源组前缀值。 ■ 未选中“**即使未找到带前缀的资源组也保护资产**”复选框。	未创建快照，作业失败。

资源组权限故障排除

如果未将相应的权限分配给资源组，则对于与资源组关联的 Azure 资源，快照创建将失败。

解决方法：

要解决该问题，请执行以下步骤：

1. 导航到 https://portal.azure.com/#blade/HubsExtension/BrowseResourceGroups。

2. 单击要在快照中使用的资源组。
3. 单击“**访问控制 (IAM)**”。
4. 单击“**添加角色分配**”。
5. 选择 **Role as Owner**、**Assign Access to as User**，然后选择 **Application (created for Snapshot Manager, to make API calls)**。
6. 保存并尝试再次备份。

关于适用于云工作负载的 NetBackup 加速器

NetBackup 加速器减少了云备份的备份时间。NetBackup 使用参考快照来标识虚拟机中所做的更改。仅将已更改的数据块发送到 NetBackup 介质服务器，从而显著减少了 I/O 和备份时间。介质服务器结合新数据和之前的备份数据，并生成包括完整虚拟机文件的传统完全 NetBackup 映像。

NetBackup 支持对 AWS、Azure 和 Azure Stack 工作负载进行加速器备份。

注意：加速器主要适用于更改率不高的虚拟机数据。

加速器具有以下优势：

- 执行完全备份时比传统备份更快。在备份主机和服务器之间创建了使用较少网络带宽的压缩备份流。加速器仅发送备份中已更改的数据块。然后 NetBackup 创建包括已更改块数据的完全传统 NetBackup 映像。
- 加速器备份支持粒度恢复技术 (GRT)。
- 减少 Snapshot Manager 上的 I/O。
- 减少 Snapshot Manager 上的 CPU 负载。

NetBackup 加速器和虚拟机的结合使用方式

对于 Azure 和 Azure Stack 备份，选择加速器支持的存储类型（如 MSDP、OpenStorage、CloudStorage 和 MSDP-C（Azure 和 AWS））时，将激活加速器。

NetBackup 加速器为每台虚拟机创建备份流并备份映像，如下所示：

- 如果虚拟机没有任何先前备份，NetBackup 将执行完全备份。
- 在下一次备份时，NetBackup 将标识自上一次备份以来发生更改的数据。备份中仅包括已更改的块和标题的信息，用于创建完全 VM 备份。更改的块通过比较以前的参考快照和当前快照来标识。如果在保护计划中选择“**仅保留备份**”或“**在快照即将过期时启动备份**”选项，则保留快照以用于加速器目的，直到下次备份完成为止。

- 备份主机会向介质服务器发送一个由以下项目组成的 tar 备份流：虚拟机已更改的块、之前的备份 ID 和未更改块的数据范围（块的偏移和大小）。
- 介质服务器将读取虚拟机已更改的块、备份 ID 和未更改块的数据范围。根据备份 ID 和数据范围，介质服务器可以在现有备份中找到虚拟机的其余数据。
- 介质服务器会指示存储服务器创建包含以下项目的新的完全映像：新更改的块和位于存储服务器上现有的未更改的块。存储服务器可能不会写入现有的块，但是会将它们链接到映像。
- Microsoft Azure 不允许后续的增量快照数超过 200 个。如果在保护计划中选择“**保留快照和备份**”选项，并且为快照指定此类保留期限，则会导致增量快照数超过 200 个。然后会执行完全备份，而非加速器备份。建议保留合理的快照保留期限以利用加速器优势。
- 如果 VM 的配置发生更改，例如，如果在两次加速器备份之间将新磁盘添加到 VM，将针对该新磁盘执行完全备份，并针对现有磁盘执行加速器备份。

虚拟机加速器强制的重新扫描（日程表属性）

通过手动执行 ForcedRescan 命令，加速器强制的重新扫描有助于防止出现备份映像损坏问题。当使用“加速器强制的重新扫描”时，将备份虚拟机上的所有数据。此备份类似于首次为某个策略进行的加速器备份。对于强制的重新扫描作业，加速器的优化百分比为 0。该备份的持续时间类似于非加速器完全备份的持续时间。

强制重新扫描可增强安全性，并为下一次加速器备份建立基线。此功能可防止任何潜在的损坏，如暂存区域中数据校验和验证失败。

有关使用强制重新扫描的建议：

- 请勿对已关闭的 VM 触发强制重新扫描。
- 如果存储位置内存已满，可以在 UI 中看到通知。仅当存储位置有足够的内存可用时，才启动强制重新扫描。

NetBackup 会为每个受保护的 VM 创建一个名为 'ForcedRescan' 的日程表。要手动触发备份并强制重新扫描，请在命令提示符或 Linux 终端执行以下命令：

```
bpbackup -i -p <policy_name> -s ForcedRescan
```

例如，`bpbackup -i -p msdp_10mins_FRS+5d990ab5-f791-474f-885a-ae0c30f31c98 -s ForcedRescan`

可以通过 Web UI 从相关保护计划获取策略名称。

加速器备份和 NetBackup 目录库

使用加速器并不影响 NetBackup 目录库的大小。使用加速器的完全备份生成的目录库大小与不使用加速器的完全备份相同。同样也适用于增量式备份：使用加速器不需要比不使用加速器进行相同备份更多的目录库空间。

备份作业详细信息日志中的加速器消息

当虚拟机首次备份时，加速器不用于该备份。作业详细信息日志中会显示以下消息：

```
Jul 21, 2021 1:55:52 PM - Info bpbrm (pid=78332) accelerator enabled
Jul 21, 2021 1:55:53 PM - Info bpbrm (pid=78332) There is no
complete backup image match with track journal, a regular full
backup will be performed.

..

Jul 21, 2021 1:56:11 PM - Info bpbkar (pid=1301) accelerator sent
402666496 bytes out of 402664960 bytes to server, optimization 0.0%
```

当虚拟机的后续备份使用加速器时，将在作业详细信息日志中显示以下消息：

```
Jul 21, 2021 2:01:33 PM - Info bpbrm (pid=79788) accelerator enabled

..

Jul 21, 2021 2:02:00 PM - Info bpbkar (pid=1350) accelerator
sent 1196032 bytes out of 402664960 bytes to server, optimization
99.7%
```

此消息是加速器的关键跟踪。在此示例中，加速器将备份数据成功减少了 99.7%。

配置云工作负载的备份计划

为 Azure、Azure Stack、AWS 和 GCP 云工作负载创建保护计划时，可以在“添加备份日程表”对话框的“属性”选项卡中添加备份日程表。

有关如何创建保护计划的详细信息，请参见《NetBackup Web UI 管理指南》中的“管理保护计划”部分。

向云工作负载添加备份计划

1 在左侧，单击“**保护**”>“**保护计划**”，然后单击“**添加**”。

2 在“**基本属性**”中，输入“**名称**”和“**描述**”，然后从“**工作负载**”下拉列表选择“**云**”。

3 从下拉列表中选择“**云提供商**”，单击“**下一步**”。在“**计划**”中，单击“**添加计划**”。

在“**添加备份计划**”选项卡中，可以配置用于保留备份和快照的选项。

4 （仅适用于 Azure SQL PaaS 资产。）如果为保护计划选择了“**仅保护 PaaS 资产**”，请在“**备份类型**”中选择“**增量式备份**”或“**完全备份**”。对于增量式备份类型，NetBackup 执行初始完全备份，所有后续备份仅捕获数据库中的增量式更改。此功能可在很大程度上提高备份性能。如果架构发生更改，请从增量式备份返回完全备份，并在活动监视器中通知此活动。

在一个策略内，为完全备份分配的保留期限应比增量式备份长。完整的还原需要上一个完全备份加上所有后续增量式备份。如果完全备份在增量式备份前就失效了，则不可能还原所有的文件。请参见第 54 页的“关于 PaaS 工作负载的增量式备份”。

5 在“**循环**”下拉列表中，指定备份频率。

6 在“快照”和“备份”选项中，执行以下任一操作：

- 选择“**保留快照和备份**”选项以同时保留快照和备份。使用“**保留快照**”和“**保留备份**”下拉列表指定快照和备份的保留期限。从“**备份类型**”下拉列表中选择“**完全**”。选择“**仅在快照即将过期时才启动备份**”选项，可在保留的快照即将过期之前启动备份作业。
- 选择“**仅保留快照**”选项，可仅保留快照。使用“**保留快照**”下拉列表指定快照的保留期限。
  - （可选）如果已选择 Amazon AWS 作为提供商，并且通过选择上述两个选项之一选择了保留快照，则此时可以配置快照复制。有关云快照复制的更多信息，请参见第 41 页的“配置 AWS 快照复制”。
  - 选择“**启用快照复制**”。
  - 在表中，为复制的快照选择“**区域**”、“**AWS 帐户**”和“**保留期限**”。

注意：您配置的复制副本数显示在“**日程表**”选项卡“**日程表和保留**”表的“**快照副本**”列中。

- 选择“**仅保留备份**”选项，可仅保留备份。快照在备份后立即过期。使用“**保留备份**”下拉列表指定备份的保留期限。从“**备份类型**”下拉列表中选择“**完全**”。

注意：由于 NetBackup 仅支持从快照进行粒度还原，因此如果选择“**仅保留备份**”，则粒度恢复选项不可用。同样，如果选择“**仅保留备份**”，则 AWS 快照复制功能不起作用。

7 继续按照《NetBackup Web UI 管理指南》中的“管理保护计划”部分所述，在“**启动时段**”选项卡中创建计划。

不同备份选项的粒度恢复可用性

文件或文件夹的粒度恢复选项的可用性取决于为工作负载选择的不同备份选项。

- 选择“**保留快照和备份**”选项时，粒度恢复可用。
- 选择“**仅保留快照**”选项时，粒度恢复可用。
- 选择“**仅保留备份**”选项时，粒度恢复不可用。

备份和快照作业期间编制索引

- NetBackup 从快照执行基于 VxMS (Veritas Mapping Service) 的索引编制，以及在从快照备份作业期间执行内联索引。它可以在不考虑 Snapshot Manager 的区域和位置的情况下为文件编制索引。GCP、AWS、Azure 和 Azure Stack Hub 云当前支持基于 VxMS 的索引编制。
- 索引编制在实际备份或快照作业期间执行，但只能使用“**启用对文件和文件夹进行粒度恢复**”选项从快照副本恢复单个文件或文件夹。
- 创建 VM 资产的快照后，将触发每个资产的“从快照编制索引”作业。可以在“**活动监视器**”中检查索引编制作业详细信息。
- VxMS 调试日志和云连接器调试日志位于 Snapshot Manager 的 */cloudpoint/openv/dm/datamover.<datamover-id>/netbackup/logs* 文件夹中。

注意：如果 VM 未处于已连接状态，则 VM 备份将继续，且备份作业将标记为部分成功。在这种情况下，无法还原单个文件或文件夹，因为当 VM 未连接时索引编制不可用。

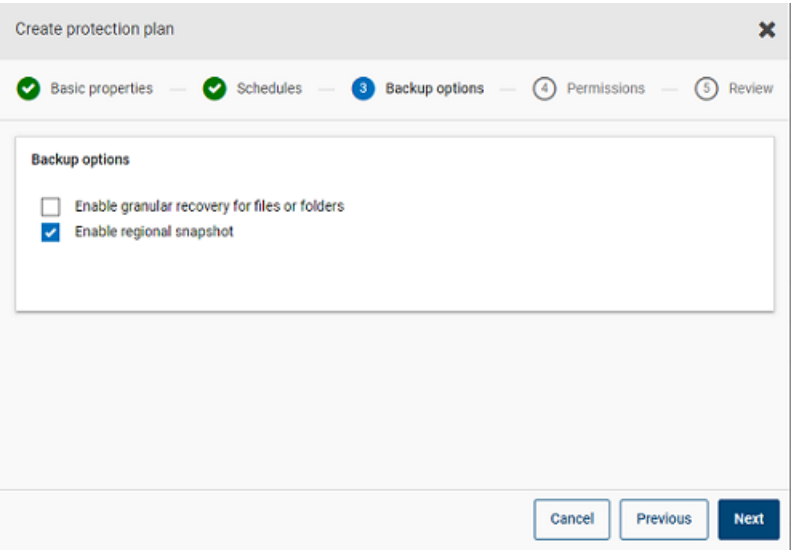
云工作负载的备份选项

注意：对于已连接的 VM，将尝试创建文件系统一致快照。如果稍后停止已连接的 VM，应用程序则会进入错误状态，而且会创建崩溃一致快照，而非文件系统一致快照。如果创建的快照是崩溃一致快照或文件系统一致快照，则您可以参考作业监视器并参阅日志。

Google 云的区域快照

在创建保护计划时，可以选择为 Google 云工作负载启用区域快照。

如果启用了区域快照选项，将在资产所在的同一区域中创建快照。否则，将在多区域位置创建快照。



Azure 和 Azure Stack Hub 的快照目标资源组

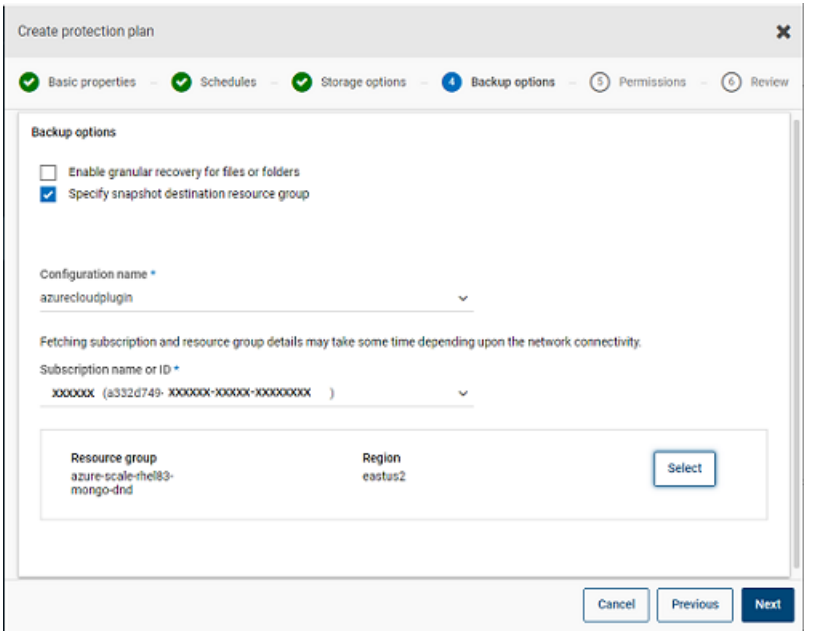
为 Azure 或 Azure Stack Hub 创建保护计划时，可以选择指定快照目标对等资源组。虽然通过指定前缀定义对等资源组的早期功能仍然存在，但现在可在创建保护计划时将快照直接关联到现有对等资源组。

如果在创建保护计划时选择了 Microsoft Azure 或 Azure Stack Hub 作为云提供商，可以选择“**指定快照目标资源组**”，以将快照关联到资产所在的同一区域内的特定对等资源组。然后为快照目标选择配置、订购和资源组。

快照存储在以下其中一个首选目标资源组中：

- 在保护计划中指定的目标资源组

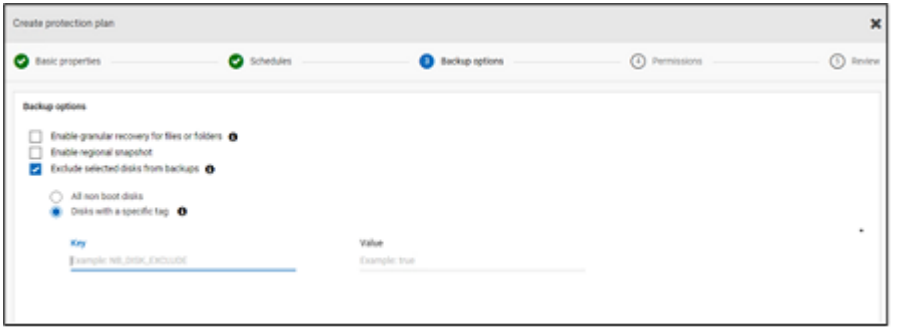
- 在插件配置中指定的带前缀的资源组（仅适用于 Azure）
- 如果在 NetBackup 中未指定目标资源组或带前缀的资源组，则为资产所在的资源组。



从备份中排除选定的磁盘

可以配置保护计划，以从备份和快照中排除某些磁盘，这适用于所有受支持的云供应商（包括 GCP）。这样，可避免不需要备份的磁盘的冗余映像，并通过减少要处理的数据量来加快备份速度。

如果要为 AWS、Azure、Azure Stack Hub 或 GCP 云创建保护计划，可以选择“**从备份中排除选定的磁盘**”选项并指定不应包含在备份映像中的磁盘。您可以选择在相应的云提供商帐户中排除所有非引导磁盘，或排除具有与其关联的特定标记的磁盘。



注意：已启用磁盘排除选项的保护计划只能应用于云 VM 类型资产和 VM 智能组。

从“恢复点”选项卡还原 VM 时，请参考“**包括磁盘**”列以查看备份映像中包括或排除的磁盘的列表。

有关完整过程，请参考《NetBackup Web UI 管理指南》中有关创建保护计划的信息。

注意：

- 对于 LVM，如果磁盘被部分排除，则系统可能无法正常启动。
- 如果磁盘上配置了不受支持的文件系统并且用户希望从快照中排除该磁盘，则即使排除了包含不受支持的文件系统的磁盘，该快照仍将是崩溃一致快照。
- 如果用户要排除该磁盘，则在 `/etc/fstab` 文件中创建快照之前，应将 **nofail** 标志附加到该数据磁盘。如果用户重新启动实例而不挂接此卷（例如，在将卷移动到另一个实例之后），则需要执行此操作，这样即使装入卷时出错，**nofail** 装入选项也允许实例启动。有关更多信息，请参考 `/etc/fstab` 文件中的以下示例条目：
  例如，**UUID=aebf131c-6957-451e-8d34-ec978d9581ae /data xfs defaults,nofail 0 2**
- 在云提供商的资产标记发生任何更改后，用户应确保能够正确发现这些资产。为资产预定策略运行后，仅根据发现的数据排除磁盘。如果用户在执行快照操作期间附加了标记，则不会将该**标记**视为排除的一部分。发现完成后，将在下一个保护周期中考虑该标记。
- 对于使用非英语区域设置的操作系统，如果用户在保护计划中选择基于标记的排除并且磁盘标记具有非英语字符，则即使这样磁盘排除也仍按预期运行。但在某些情况下，在 job(try) 日志和审核日志中无法正确捕获具有非英文字符的标记，但由于正确考虑了磁盘排除，因此不会影响功能。

快照复制

复制快照意味着将快照副本保存到其他位置。在 AWS 中，其他位置可以是以下位置之一：

- 同一帐户内的不同区域。
- 不同帐户中的同一区域。
- 不同帐户内的不同区域。

例如，AWS 云管理员的资产位于区域 X 中。这些资产的快照也将存储在区域 X 中。但是，也可以将快照复制到同一帐户内的 Y 区域或不同帐户中的 X/Y 区域，以获得更高级别的保护。在 NBU Snapshot Manager 术语中，原始位置 (X) 是复制源，复制快照的位置 (Y) 是复制目标。

复制分三个步骤执行。此机制在内部进行处理，整个过程对用户是完全透明的。

- 仅当跨帐户进行复制时，才共享快照。有关更多信息，请参见 AWS 文档的共享快照部分。
- 复制快照。有关更多信息，请参见 AWS 文档的 CopySnapshot 部分。
- 仅当跨帐户进行复制时，才取消共享快照。

配置 AWS 快照复制

复制快照的要求

- **复制未加密的快照**
  确保通过 NetBackup Snapshot Manager 使用 AWS 云提供商配置源和目标帐户/区域。对于复制未加密的快照，没有其他要求。
- **使用 AWS KMS 复制加密的快照**
  确保通过 NetBackup Snapshot Manager 使用 AWS 云提供商配置源和目标帐户/区域。
  此外，要跨帐户复制加密的快照，需要将加密 CMK 密钥从原始位置共享到目标帐户。（在目标帐户中复制快照时隐式使用此共享 KMS 密钥，复制的快照可以通过其他密钥进行复制）。
  源位置和目标位置应具有同名的加密密钥（KMS 密钥）：也就是说，它们应具有相同的密钥别名（就 AWS 而言）。
  如果目标中不存在同名的加密密钥，则使用目标位置中的默认 KMS 密钥对复制的快照进行加密。
- **跨帐户复制所需的权限**
  对于跨帐户复制，与快照源区域的 AWS 帐户（源 AWS 帐户）关联的 AWS IAM 用户或角色必须具有以下权限：

- 对于 EC2 实例，必须具有 `ModifySnapshotAttribute` 和 `CopySnapshot` 权限。
- 对于用于加密原始快照的 KMS 密钥，必须具有 `DescribeKey` 和 `ReEncrypt` 权限。

对于跨帐户复制，与快照复制目标区域的 AWS 帐户（目标 AWS 帐户）关联的 AWS IAM 用户或角色必须具有以下权限：

- 对于用于加密原始快照的 KMS 密钥，必须具有 `CreateGrant`、`DescribeKey` 和 `Decrypt` 权限。
- 对于执行原始快照的 `CopySnapshot` 操作时使用的 KMS 加密密钥，必须具有 `CreateGrant`、`Encrypt`、`Decrypt`、`DescribeKey` 和 `GenerateDataKeyWithoutPlainText` 权限。

可以选择将 AWS 云资产的快照从主位置复制到远程位置或辅助位置。Snapshot Manager 支持跨区域和跨帐户复制。使用快照复制，可获得以下优势：

- 保存一份云资产副本到其他目标，用于长期保留，以实现对审核要求的遵循。
- 如果某个区域发生中断，使用另一个区域的复制副本恢复云资产。
- 如果用户帐户被盗，使用另一个帐户的复制副本恢复云资产。

配置

要配置快照复制，请查看以下信息：

- 创建保护计划时，可以配置快照复制。请参见 NetBackup™ Web UI 管理指南。
- 对于跨帐户复制，您需要在源和目标帐户之间建立信任关系。有关更多详细信息，请参考 *Amazon Web Services* 文档中的“使用 IAM 角色跨 AWS 帐户”相关信息。

注意事项

配置云快照复制时，请注意以下事项：

- 即使配置了多个日程表，所有这些日程表都将使用同一个配置的复制目标区域。
- 只有 Amazon 云提供商支持云快照复制。

资产保护条件

如果要将云资产添加到保护计划中，且该保护计划配置了云快照复制，则在添加前请考虑以下事项：

- 必须将资产添加到保护计划中，该保护计划能将快照复制到其他区域。
  例如，无法为位于区域 ‘aws_account_1-us-east-1’ 中的资产订购复制到同一区域 ‘aws_account_1-us-east-1’ 的保护计划。
- 资产可以复制到同一区域中的不同帐户。

例如，可以为位于区域 'aws_account_1-us-east-1' 中的资产订购复制到同一区域但不同帐户 'aws_account_2-us-east-1' 的保护计划。

- Snapshot Manager 发现的资产必须复制到同一 Snapshot Manager 发现的区域。
  例如，无法为 Snapshot Manager CP1 发现的资产订购复制到 Snapshot Manager CP2 发现的区域的保护计划。
- 只能为 Amazon 资产订购针对云快照复制配置的保护计划。

管理并行快照复制

为提高性能，可以调整并行快照复制数。资产类型不同，Amazon 对单个目标区域上的并行快照复制的数量限制也不同。例如，RDS 的上限为 5，EBS 的上限为 5，EC2 的上限为 50。有关更多详细信息，请参考 *Amazon Web Services* 文档中的“复制快照”相关信息。

在 NetBackup 中，在 `bp.conf` 文件中使用以下参数定义了此限制：

```
MAX_CLOUD_SNAPSHOT_REPLICATION_JOBS_PER_DESTINATION
```

默认值为 5。

使用 AWS 快照复制

此部分详细介绍如何使用 AWS 快照复制功能创建快照副本，以及如何在需要时还原复制的快照。除非另有说明，否则有关这些步骤的详细信息，请参考《NetBackup™ Snapshot Manager 安装和升级指南》和《NetBackup Web UI 管理指南》。

创建快照复制

此部分介绍如何配置源区域，以在目标区域创建快照副本。

创建副本

1. 在 Web UI 中添加 Snapshot Manager (CP1)。请参见第 11 页的“添加 Snapshot Manager”。
2. 为源区域和目标区域添加 AWS 插件，以进行复制。
3. 创建保护计划，然后选择“**区域**”和“**帐户**”。请参见第 35 页的“配置云工作负载的备份计划”。
4. 使用 OnHost 代理连接并配置应用程序一致的访客 VM。
5. 触发基于快照的备份，然后使用保护计划复制快照。
6. 验证快照和副本的恢复点。

从目标区域中的快照副本还原

如果源区域失败，可以从已创建快照副本的目标区域还原属于源区域的 VM。由于源区域关闭，您最初需要还原目标区域中的 VM。

注意：无法从故障转移区域中的备用 Snapshot Manager 所发现的副本还原单个文件或文件夹。

在目标区域中还原

1. 通过 Web UI 禁用源区域中的服务器 CP1。请参见第 18 页的"启用或禁用 Snapshot Manager"。
2. 通过 Web UI 在目标区域注册新的 Snapshot Manager (CP2)。
3. 仅为目标区域和帐户添加 AWS 插件。完成发现。
4. 要还原 VM，请执行以下步骤：
   - 登录 NetBackup Web 用户界面。
   - 在左侧，单击"**工作负载**"下的"**云**"。在"**虚拟机**"选项卡上，单击要恢复的计算机。
   - 单击"**恢复点**"选项卡。在映像列表中，单击所需"**副本**"映像前面的"**还原**"，然后单击"**还原虚拟机**"。
   - 要更改 VM 的显示名称，请输入新名称。
   - 选择子网（具有 VPC 的子网路径）。
     请参见第 65 页的"恢复云资产"。
5. 向还原的 VM 添加适当的安全组以启用远程访问。
6. 从还原的 VM 卸载并重新安装 Snapshot Manager 代理，然后将这些 Snapshot Manager 代理注册到新的 CP2 服务器。
7. 从 AWS 提供商控制台运行深度发现。
8. 创建新的保护计划以保护还原的 VM。触发基于快照的备份。

从目标区域还原回源区域

源区域重新联机后，即可将 VM 从目标区域还原到源区域。

还原到源区域

1. 编辑 CP2 的 AWS 插件并添加源区域。
2. 创建新保护计划以在源区域中创建快照副本。
3. 触发基于快照的备份并复制。

4 在 Web UI 中禁用 CP2 服务器。请参见第 18 页的"启用或禁用 Snapshot Manager"。

5 启用 CP1 服务器，然后从 AWS 提供商控制台触发深度发现。

6 从目标区域执行 VM 的完全还原。

7 向还原的 VM 添加适当的安全组以启用远程访问。

8 从还原的 VM 卸载并重新安装 Snapshot Manager 代理，然后将这些 Snapshot Manager 代理注册到 CP1 服务器。

9 从 AWS 控制台运行深度发现。

10 使用现有保护计划保护新还原的 VM。

帐户复制的支持列表

表 1-9 相同帐户复制的支持列表

资产类型	源资产（区域 X）	源快照（区域 X）	复制的快照（区域 Y）
EBS 卷、EC2 实例和 RDS/Aurora	未加密	未加密	未加密
	挂接的磁盘使用默认 AWS KMS 密钥进行加密。	挂接的磁盘使用默认 AWS KMS 密钥进行加密。	挂接的磁盘使用默认 AWS KMS 密钥进行加密。
	使用 AWS KMS CMK 密钥（具有别名 ABC）加密。	使用 AWS KMS CMK 密钥（别名 ABC）加密。	使用具有名称（别名 ABC）的 AWS KMS CMK 密钥（如果存在）进行加密，否则使用默认 AWS KMS 密钥进行加密。

表 1-10 不同帐户相同区域复制的支持列表

资产类型	源资产（帐户 A 区域 X）	源快照（帐户 A 区域 X）	复制的快照（帐户 B 区域 Y）
EBS 卷、EC2 实例和 RDS/Aurora	未加密	未加密	未加密
	使用默认 AWS KMS 密钥加密。	使用默认 AWS KMS 密钥加密。	不支持
	使用 AWS KMS CMK 密钥（具有别名 ABC）加密。	使用 AWS KMS CMK 密钥（具有别名 ABC）加密。	使用具有名称（别名 ABC）的 AWS KMS CMK 密钥（如果存在）进行加密，否则使用默认 AWS KMS 密钥进行加密。

表 1-11 不同帐户不同区域复制的支持列表

资产类型	源资产（帐户 A 区域 X）	源快照（帐户 A 区域 X）	复制的快照（帐户 B 区域 Y）
EBS 卷和 EC2 实例	未加密	未加密	未加密
	使用默认 AWS KMS 密钥加密。	使用默认 AWS KMS 密钥加密。	不支持
	使用 AWS KMS CMK 密钥（具有别名 ABC）加密。	使用 AWS KMS CMK 密钥（具有别名 ABC）加密。	使用具有名称（别名 ABC）的 AWS KMS CMK 密钥（如果存在）进行加密，否则使用默认 AWS KMS 密钥进行加密。
RDS	未加密	未加密	未加密
	使用默认 AWS KMS 密钥加密。	使用默认 AWS KMS 密钥加密。	不支持
	使用默认 AWS KMS 密钥加密。	使用默认 AWS KMS 密钥加密。	不支持
Aurora	未加密	未加密	不支持
	使用默认 AWS KMS 密钥加密。	使用默认 AWS KMS 密钥加密。	不支持
	使用默认 AWS KMS 密钥加密。	使用默认 AWS KMS 密钥加密。	不支持

使用应用程序一致性快照保护云中的应用程序

可以为在云中虚拟机上部署的应用程序创建应用程序一致性（时间点）快照。这样，可以对应用程序执行时间点恢复。

对于这些工作负载，可以执行原始位置和备用位置还原。

对于备用位置还原，请注意以下事项：

- 对于 MS SQL 工作负载的备用位置还原，必须发现目标主机，但应用程序状态不应处于已连接或已配置状态。
- 对于 Oracle 工作负载的备用位置还原，必须发现目标主机，但应用程序状态不应处于已连接或已配置状态。

开始之前

确保数据库已准备好进行快照操作。有关详细信息，请查看 Veritas Snapshot Manager 文档中的插件配置说明。

配置应用程序以执行时间点恢复

1 连接到托管应用程序的虚拟机。

- 发现云资产后，转到“**虚拟机**”选项卡。
- 选择托管应用程序的虚拟机。在右上方，单击“**管理凭据**”。
- 输入凭据。如果未配置 VM 的凭据，则必须配置凭据。请参见《Web UI 管理指南》中的“管理凭据”一章。
- 连接虚拟机后，虚拟机状态将更新为“**已连接**”。

2 选择托管应用程序的虚拟机。在右上方，单击“**配置应用程序**”。

3 该过程完成后，应用程序状态将更新为“已配置”。

4 在下一次发现之后，应用程序将显示在“**应用程序**”选项卡下。

5 应用保护计划。请参见《NetBackup Web UI 管理指南》。

编辑或更新虚拟机凭据

1 转到“**虚拟机**”选项卡。

2 选择要更新其凭据的虚拟机。在右上方，单击“**管理凭据**”。

3 更新凭据。

编辑或更新应用程序配置

1 转到“**应用程序**”选项卡。

2 选择要更新的应用程序。在右上方，单击“**编辑配置**”

3 更新凭据，然后单击“**配置**”。

保护 PaaS 资产

您可以在 NetBackup 发现 PaaS 资产后对这些资产进行管理。资产显示在云工作负载下的 **PaaS** 和“**应用程序**”选项卡中。“**应用程序**”选项卡显示 RDS 资产，而 **PaaS** 选项卡显示非 RDS 资产。可以从这两个选项卡查看、保护和恢复 PaaS 资产。

保护 PaaS 资产的前提条件

通过 NetBackup，您可以发现、保护和还原不同云平台上的 PaaS 资产以获取各种资产。本部分详细介绍支持的平台和数据库。

支持的云提供商

NetBackup 支持使用以下云提供商保护 PaaS 资产：

- Microsoft Azure
- AWS
- GCP

不同提供商支持的数据库

下表列出了每个云提供商支持的数据库。

表 1-12 PaaS 支持的数据库

提供商	支持的数据库
Microsoft Azure	PostgreSQL、SQL Managed Instance、SQL、MariaDB 和 MySQL。 **不支持以下组件：** Azure SQL - 弹性池 Azure SQL Managed Instance - Azure Arc Azure PostgreSQL - Hyperscale (Citus) 服务器组和启用了 Azure Arc 的 PostgreSQL Hyperscale

提供商	支持的数据库
AWS	RDS SQL、RDS PostgreSQL、RDS MySQL、RDS MariaDB、RDS Aurora MySQL、RDS Aurora PostgreSQL 和 DynamoDB。
GCP	适用于 PostgreSQL 的云 SQL 和适用于 MySQL 的云 SQL

支持的平台

本部分详细介绍主服务器和介质服务器支持的平台。

表 1-13 PaaS 支持的平台

NetBackup 服务器	支持的平台
主服务器	RHEL、SUSE 和 Windows
介质服务器	RHEL
存储服务器	基础 MSDP 块存储或 MSDP 云存储 STU 上的通用共享

所需的云提供商权限

用于添加云提供商的凭据必须分配有《NetBackup Snapshot Manager 安装和升级指南》中所述的所有必需权限。

支持的端口

以下是不同 PaaS 数据库支持的端口。

表 1-14 PaaS 支持的端口

数据库 PaaS 工作负载	支持的端口
Azure SQL Server	1433
Azure SQL Managed Instance	1433
Azure MySQL	3306
Azure PostgreSQL	5432
Azure MariaDB	3306
GCP PostgreSQL	5432
GCP MySQL	3306
AWS DynamoDB	不适用

数据库 PaaS 工作负载	支持的端口
AWS RDS PostgreSQL	5432
AWS RDS MySQL	3306
AWS MariaDB	3306
AWS RDS AuroraDB Postgres	5432
AWS RDS AuroraDB MySQL	3306
AWS RDS SQL Server	1433

为 MySQL 数据库启用二进制日志记录

- 对于 AWS，请参见 https://aws.amazon.com/premiumsupport/knowledge-center/rds-mysql-functions/
- 对于 Azure，请将 `log_bin_trust_function_creators` 参数的值设置为 1，如链接中所述：
  https://learn.microsoft.com/en-us/azure/mysql/single-server/how-to-server-parameters
- 对于 GCP，请执行以下操作：
  - 打开实例，然后单击“**编辑**”。
  - 向下滚动到“**标志**”部分。
  - 要设置标志，请单击“**添加项目**”，从下拉菜单中选择 **log_bin_trust_function_creators** 标志，然后将其值设置为 on。
  - 单击“**保存**”以保存更改。可以在“**概述**”页面中的“**标志**”下确认所做的更改。

安装本机客户端实用程序

如果您使用自建 (BYO) 设置，则必须在 NetBackup 环境中安装本机客户端实用程序，PaaS 工作负载才能正常工作。

对于 Azure Kubernetes Service (AKS) 或 Elastic Kubernetes Service (EKS) 中的 NetBackup 部署，本机客户端实用程序将作为 NetBackup 介质服务器和主服务器的一部分打包，无需手动安装。

确保正确配置了网络设置（如防火墙、安全组和 DNS 配置），以访问云提供商内的数据库。

注意：如果其中任何一个软件包已经安装在介质服务器中，请删除软件包以避免与您安装的较新版本的软件包发生冲突。

安装 MySQL 客户端实用程序

注意：MySQL 客户端实用程序的建议版本为 8.0.31。

RPM 下载位置 https://downloads.mysql.com/archives/community/

要安装，请在终端中运行以下命令：

1. `rpm -ivh mysql-community-common-<version_no>.x86_64.rpm`
2. `rpm -ivh mysql-community-client-plugins- <version_no>.x86_64.rpm`
3. `rpm -ivh mysql-community-libs- <version_no>.x86_64.rpm`
4. `rpm -ivh mysql-community-client- <version_no>.x86_64.rpm`

注意：避免使用 MySQL 客户端实用程序 8.0.32 版本，因为 MySQL 报告了错误。

安装 *sqlpackage* 客户端实用程序

注意：`sqlpackage` 客户端实用程序的建议版本为 19.2（内部版本：16.0.6296.0）。

下载位置 https://docs.microsoft.com/en-us/sql/tools/
/sqlpackage-download?view=sql-server-ver15

https://packages.microsoft.com/rhel/7/prod/msodbcsql17-17.10.2.1-1.x86_64.rpm

https://packages.microsoft.com/rhel/7/
prod/unixODBC-2.3.7-1.rh.x86_64.rpm

要安装，请在终端中运行以下命令：

1. `cd ~`
2. `mkdir sqlpackage`
3. `unzip ~/Downloads/sqlpackage-linux-<version string>.zip -d ~/sqlpackage`
4. `echo "export PATH=\"\$PATH:$HOME/sqlpackage\""> ~/.bashrc`
5. `chmod a+x ~/sqlpackage/sqlpackage`

6 `source ~/.bashrc`

注意：确保将 `sqlpackage` 添加为默认路径变量。

7 `sqlpackage`

8 `rpm -ivh unixODBC-2.3.7-1.rh.x86_64.rpm`

9 `rpm -ivh msodbcsql17-17.10.2.1-1.x86_64.rpm`

RHEL 9 用户执行以下其他步骤：

1 从以下链接下载 Microsoft.NETCore.App.Runtime.linux-x64：

https://www.nuget.org/api/v2/package/Microsoft.NETCore.App.Runtime.linux-x64/6.0.10

找到 `microsoft.netcore.app.runtime.linux-x64.6.0.10.nupkg` 文件。

2 使用解压缩工具（如 7zip）提取文件。

3 导航到：

microsoft.netcore.app.runtime.linux-x64.6.0.10.nupkg\runtimes\linux-x64\lib\net6.0\

4 将 `System.Security.Cryptography.X509Certificates.dll` 文件从上述位置复制到 `/sqlpackage` 文件夹，该文件夹是在安装 ***sqlpackage*** 客户端实用程序任务的步骤 2 中创建的。

如果将 10.1 介质服务器挂接为具有 10.1.1 NetBackup 设置的外部介质服务器，请在 10.1 介质服务器上执行以下步骤。

对于 BYO NetBackup 设置：

- 运行命令：
  `mkdir -p <backup and restore ushare export path>`
- 在 `/etc/nfsmount.conf` 文件中检查 NFS 的 `Defaultvers` 值。
  - 如果 `Defaultvers` 值为 `nfs3`，则使用 `nolock` 选项装入备份和还原 ushare 路径。例如：`mount <ushare mount path> <ushare export path> -o nolock`
  - 如果 `Defaultvers` 为 `nfs4`，则装入备份和还原 ushare 路径，而不使用 `nolock` 选项。

对于在 AKS 和 EKS 环境中部署的 NetBackup：

- 运行命令：
  `mkdir -p <backup and restore ushare export path>`
- 从 `/etc/nfsmount.conf` 文件中检查 NFS 的 `Defaultvers` 值。

- 如果 `Defaultvers` 值为 `nfs3`，则使用 `nolock` 选项装入备份和还原 ushare 路径，例如：`mount <ushare mount path> <ushare export path> -o nolock`
- 如果 `Defaultvers` 值为 `nfs4`，则装入 v4 版本备份和还原 ushare 路径，而不使用 `nolock` 选项。

安装 Postgres 客户端实用程序

注意：Postgres 客户端实用程序的建议版本为 14.6。

下载位置
RHEL 7 https://download.postgresql.org/pub/repos/yum/14/redhat/rhel-7-x86_64/
RHEL 8 https://download.postgresql.org/pub/repos/yum/14/redhat/rhel-8-x86_64/
RHEL 9 https://download.postgresql.org/pub/repos/yum/14/redhat/rhel-9-x86_64/

要安装，请在终端中运行以下命令：

1. `rpm -ivh postgresql14-libs-14.6-1PGDG.rhel7.x86_64.rpm`
2. `rpm -ivh postgresql14-14.6-1PGDG.rhel7.x86_64.rpm`

注意：RHEL 8 和 9 上的 `postgresql14-14.6-1PGDG.rhel8.x86_64.rpm` 需要 `lz4 compression package` 和 `libicu`。

配置存储服务器以进行即时访问

以下是存储服务器支持即时访问所需的配置。

1. 确保已安装 NFS 和 NGINX。
2. 该 NGINX 版本必须与相应的正式 RHEL 版本中的 NGINX 版本相同。从相应的 RHEL yum 源 (EPEL) 安装该版本。
3. 确保从同一 RHEL yum 源（RHEL 服务器）安装 `policycoreutils` 和 `policycoreutils-python` 软件包。运行以下命令：
   - `semanage port -a -t http_port_t -p tcp 10087`
   - `setsebool -P httpd_can_network_connect 1`

4 确保任何装入点不会直接在存储服务器上装入 /mnt 文件夹。仅将装入点装入其子文件夹。

5 使用以下命令在 selinux 中启用 logrotate 权限：

```
semanage permissive -a logrotate_t
```

关于 PaaS 工作负载的增量式备份

NetBackup 支持 Azure SQL Server 工作负载的差异增量式备份。增量式备份显著缩短了 NetBackup 中的备份时段。在此方法中，NetBackup 仅备份自上次完全备份以来已更改的数据。

仅这些工作负载支持差异增量式备份，其中，在 Azure SQL Server 上启用了更改数据捕获功能。

用于 PaaS 工作负载增量式备份的准则：

- 在一个策略内，为完全备份分配的保留期限应比增量式备份长。完整的还原需要上一个完全备份加上所有后续增量式备份。如果完全备份在增量式备份前就失效了，则不可能还原所有的文件。
- 使用一个存储进行完全备份和增量式备份。
- 不要为增量式备份创建长期副本。
- 不要使随机增量式备份映像失效。使其失效可能会由于数据丢失而导致应用程序不一致。NetBackup 依赖于以前的完全备份和所有后续的增量式备份。
- 复制时，请确保将完全备份副本和增量式备份副本复制到目标存储。缺少任何以前的完全备份映像或增量式备份映像都可能导致数据丢失。
- 导入时，请确保将完全备份副本和所有增量式备份副本一起导入。缺少任何以前依赖的完全备份映像或增量式备份映像都可能导致失败。

限制和注意事项

保护云工作负载时，请考虑以下事项。

对于所有数据库

- Flex Appliance 和 Flex Scale 中的 NetBackup 部署不支持 PaaS 工作负载。
- 跨提供商的所有数据库仅支持默认端口。不支持使用自定义端口配置的工作负载实例。
- 备份和还原操作不支持包含字符 # 和 / 的数据库名称。此外，数据库名称应遵循云供应商建议的命名约定。
- 对于具有二线支持介质服务器（版本低于 10.1.1）且运行 Windows 的主服务器，不支持备份和还原具有多字节或非英语字符的数据库。

- 可以将 PaaS 备份映像复制到受支持的存储服务器。但是，在开始还原之前，需要将映像复制回启用了通用共享的 MSDP 服务器。请参见第 77 页的"从 AdvancedDisk 恢复复制的映像"。
- 在 NetBackup 10.2 中，可以使用基于托管标识的数据库身份验证对支持的 Azure PaaS 数据库执行备份和还原。对于 MariaDB 服务器，Azure 数据库不支持此功能。此功能需要至少一台 10.2 或更高版本的介质服务器。
- 对于 Azure 数据库的身份验证，建议使用用户分配的托管标识在所有介质服务器上运行。使用通过系统分配的托管标识创建且与某介质服务器或 vm-scale-set (AKS/EKS) 关联的数据库用户，则任何其他介质服务器或任何其他 vm-scale set (AKS/EKS) 中的介质不能再使用该数据库用户。

对于 PostgreSQL

- 不支持还原安全权限。
- 在还原期间，可以使用 `-no-owner` 和 `-no-privileges` 选项。还原后，备份时捕获的元数据显示在 Web UI 上还原活动进度日志中的所有者/ACL 下。
- 如果目标上不存在所有者/角色，还原不会失败。
- 还原后，数据库根据 NetBackup 中针对目标实例提供的凭据与角色相关联。
- 用户需要在还原后修改数据库的所有权。
- 如果在 GCP PostgreSQL 工作负载的服务器级别仅强制执行 SSL（安全套接字层）连接，则不支持备份和还原。
- 由于云提供商的限制，不支持将 Azure Postgres 数据库从单一服务器还原到灵活服务器，反之亦然。
- 在还原工作流程中，不支持在数据库名称中使用以下字符：&、(、)、<、>、\、|、/、;、`、‘ 和 “。
- 创建 PostgreSQL 服务器后添加的新用户不支持大写用户名。

对于 AWS DynamoDB

- 不支持区域和帐户的备用还原。
- 仅支持使用 NetBackup REST API 从其他主服务器还原导入的映像。

对于 AWS RDS SQL

- 仅支持 AWS RDS SQL 的 Express 和 Web 版本。
- 对于凭据验证，AWS RDS SQL 不支持 IAM。可以使用用户名和密码方法。
- 仅支持 **Amazon RDS** 数据管理类型。AWS RDS SQL 实例版本不支持“**RDS 自定义**”数据管理类型。

对于 MySQL

- 对于在低于 10.2 的版本上创建的备份，如果转储文件包含 CREATE DEFINER 语句，则还原操作需要超级用户权限。
- 在 10.2 或更高版本上创建的备份无法使用低于 10.2 的版本进行还原。
- 如果在 GCP MySQL 工作负载的服务器级别仅强制执行 SSL 连接，则不支持备份和还原。
- 可以将 MySQL 数据库还原到具有另一个 MySQL 版本的备用实例，而不是还原到备份实例，具体取决于 MySQL 的版本兼容性。

对于 Azure SQL 和 SQL Managed Instance

- 用作介质服务器的 Azure VM 应与 Azure Managed Instance 位于同一 Vnet 中。或者，如果介质服务器和 SQL Managed Instance 位于不同的 Vnet 中，则必须对这两个 Vnet 建立对等关系才能访问数据库实例。
- 在数据库或资源组上设置读取锁定时，备份失败。
- 在数据库或资源组上设置删除锁定时，备份部分成功。不会从 Azure 云门户删除 tempdb 失效条目。您需要手动删除它。
- 要在 Azure SQL Server 或 Azure Managed Instance 上还原数据库，必须根据需要在开始还原之前将目标服务器上的 AAD 管理员权限分配给以下对象：
  - 介质服务器的系统托管标识或用户托管标识。
  - 部署了 NetBackup 介质的 `vm-scale-set`（对于 AKS 或 EKS 部署）。

对于 Azure SQL 增量式备份

- 只能在数据库的 S3 及更高层上启用更改数据捕获 (CDC)。CDC 不支持子核心（基本、S0、S1、S2）Azure SQL 数据库。
- 对于表中具有加密列的数据库，您可能会遇到备份或还原问题。作为解决办法，Microsoft 建议使用 Publish/Extract 命令解决此问题。
- 对于表中包含 blob 数据的数据库，还原可能会失败。
- 在不同的存储服务器上复制增量式备份；NetBackup 为同一恢复点生成不同的副本号。如果尝试还原增量式副本，但未引用以前的完全备份和其他增量式备份，则还原将失败。
- 请注意，增量式备份只能在 NetBackup 10.2 及更高版本的介质服务器上运行。
- 用于云服务的用户 ID 必须具有启用和禁用 CDC 的权限。如果没有此权限，可能会看到以下错误：3842：“无法启用 CDC”和 3844：“无法禁用 CDC”。
- 如果数据库中存在名为 `cdc` 的自定义架构或用户，则任何启用 CDC 的尝试均会失败。保留术语 `cdc` 以供系统使用。

- 如果还原到 Standard 或 Enterprise 以外的任何版本，则操作会被阻止，因为 CDC 需要 SQL Server Standard 或 Enterprise 版本。系统会显示错误消息 932。
- 避免使用 BLOB 数据表备份数据库。如果表中包含 BLOB 数据，则备份可能会成功，但还原将失败。

发现 PaaS 资产

通过 NetBackup，您可以发现、保护和还原 PaaS 数据库资产。您也可以发现和还原由 Microsoft Azure 备份的 Azure SQL 数据库和 Azure SQL 托管数据库资产。支持的备份模式为“时间点备份”和“长期保留备份”。

注意：如果已将 NetBackup Snapshot Manager（以前称为 CloudPoint）从版本 10.0 升级到 10.1。对于具有自定义角色的所有用户，PaaS 资产在 **PaaS** 选项卡中标记为已删除。资产上不显示任何恢复点，而是显示具有相同名称的新资产。执行后续的预定资产清理（默认持续时间为 30 天）之后，旧资产将从 **PaaS** 选项卡中删除。要解决此问题，请将所有新资产的权限重新分配给现有 RBAC 角色或创建新的自定义角色。有关更多信息，请参见《NetBackup Web UI 管理指南》。

注意：如果将 Snapshot Manager 云插件配置从 Azure 服务主体更改为 Azure 托管标识，则以前发现的 PaaS 资产的状态将显示为“已删除”。NetBackup Snapshot Manager 每 24 小时移除一次已删除的资产，如果要在预定清理之前执行备份或恢复，请与 Veritas 技术支持联系。

要发现 PaaS 资产，请执行以下操作：

1 添加 Snapshot Manager。请参见第 11 页的“添加 Snapshot Manager”。

2 添加 Microsoft Azure、GCP 或 AWS 作为提供商。请参见第 12 页的“为 Snapshot Manager 添加云提供商”。

3 运行发现。请参见第 16 页的“发现 Snapshot Manager 上的资产”。

发现完成后，您可以在“云”工作负载的 **PaaS** 选项卡中找到所有已发现的 Azure PostgreSQL、MariaDB、SQL Managed Instance、SQL、MySQL 和适用于 PostgreSQL 的 GCP 云 SQL、适用于 MySQL 的云 SQL 或 AWS DynamoDB 资产。

所有已发现的 AWS RDS PostgreSQL、RDS MySQL、RDS MariaDB、RDS SQL 和 AuroraDB 资产都会显示在“**应用程序**”选项卡中。RDS 实例支持基于提供商快照的备份以及 NetBackup 托管备份。

NetBackup 可以管理和保护在 **PaaS** 选项卡下列出的所有资产。此外，Microsoft Azure 还可以备份 Azure SQL 数据库和 Azure SQL 托管数据库资产。

注意：按间隔创建和删除同名 PaaS 资产时，如果在发现后删除 PaaS 资产，Web UI 将显示旧数据，直到下一次定期发现运行。

查看 PaaS 资产

要查看 PaaS 资产，请执行以下操作：

1 在左侧，单击“**工作负载**”下的“**云**”。

2 在 **PaaS** 选项卡中，将显示可供您使用的资产。RDS 资产显示在“**应用程序**”选项卡中。

您可以在显示的资产中执行“**添加保护**”、“**立即备份**”、“**管理凭据**”操作。

对于 DynamoDB 资产，“**管理凭据**”选项不可用。

对于已删除的资产，您只能管理凭据。

管理 PaaS 凭据

您可以为“**云**”工作负载下的 **PaaS** 和“**应用程序**”选项卡中列出的数据库添加凭据。可以从 NetBackup 中的中央“**凭据管理**”控制台添加、编辑或删除 PaaS 凭据。

查看应用于数据库的凭据名称

您可以在 **PaaS** 选项卡的“**凭据名称**”列中查看为数据库配置的指定凭据。如果没有为特定资产配置凭据，则此字段为空。

要查看 PaaS 数据库的凭据，请执行以下操作：

1 在左侧，选择“**工作负载**”**>**“**云**”**> PaaS** 选项卡。

2 单击数据库列表表格上方的“**显示或隐藏列**”。

3 选择“**凭据名称**”可显示凭据名称列。

向数据库添加凭据

您可以为 **PaaS** 选项卡中列出的数据库添加或修改凭据。

添加或更改凭据

1 在左侧，单击“**工作负载**”>“**云**”。

在**PaaS**选项卡中，将显示可供您使用的资产。RDS 资产显示在“**应用程序**”选项卡中。

2 在表中选择数据库，然后单击“**管理凭据**”。

3 选择“**验证主机**”。验证主机必须是连接到 PaaS 工作负载的 RHEL 介质服务器。

您可以为数据库添加现有凭据或创建新的凭据：

- 要为帐户选择现有凭据，请选择“**从现有凭据中选择**”选项，然后从下面的表中选择所需凭据并单击“**下一步**”。
- 要为帐户添加新凭据，请选择“**添加凭据**”，然后单击“**下一步**”。为新凭据输入“**凭据名称**”、“**标记**”和“**描述**”。在“**服务凭据**”下：
  - 选择“**基于角色的数据库身份验证 (适用于支持的数据库服务)**”，以使用 AWS IAM、Azure 系统托管身份验证和用户托管身份验证。
    - 仅为 Amazon RDS 资产选择“**IAM 数据库身份验证 (仅适用于 Amazon RDS)**”，然后指定“**数据库用户名**”。
      请参见第 60 页的“创建 IAM 数据库用户名”。

      注意：如果 Snapshot Manager 在云中部署，且附加的 IAM 角色具有所需的权限。还必须在同一云环境中部署介质服务器并附加相同的 IAM 角色。否则，AWS 资产的备份作业将失败。

    - 根据需要选择“**Azure 系统托管标识身份验证**”或“**Azure 用户托管标识身份验证**”。输入数据库的用户名，然后单击“**下一步**”。要利用托管标识身份验证执行备份和还原操作，必须为源和目标数据库服务器配置 AAD 管理员。

      注意：如果 Snapshot Manager 部署在云中（附加的托管标识具有所需权限），请将同一标识附加到介质服务器。对于 AKS 和 EKS 部署，将相同的托管标识附加到 VM 扩展集。

  - 选择“**密码身份验证**”，然后指定数据库服务器的用户名和密码。单击“**下一步**”。
- 添加您希望有权访问凭据的角色。要向角色添加新权限，请执行以下操作：

- 单击“添加”。
- 选择角色。
- 选择您希望角色具有的凭据权限。
- 单击“保存”。

4 单击“下一步”以完成凭据创建。

有关凭据以及如何编辑或删除凭据的更多信息，请参见《NetBackup Web UI 管理指南》。

创建 IAM 数据库用户名

要创建 IAM 用户名，请执行以下操作：

1 在 RDS 数据库实例上启用 IAM 数据库身份验证。

2 使用主登录名 (rds_iam) 创建数据库用户

- 对于 MySQL，请使用主登录名 (rds_iam) 创建用户名：
  - mysql --protocol=tcp --host=instance_fqdn --user=admin -p --port=3306
  - CREATE USER iamuser IDENTIFIED WITH AWSAuthenticationPlugin as 'RDS';
  - GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, PROCESS, REFERENCES, INDEX, ALTER, SHOW DATABASES, LOCK TABLES, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, EVENT, TRIGGER ON *.* TO `iamuser`@'%' WITH GRANT OPTION;
- 对于 PostgreSQL，在服务器下创建用户。
  - psql -h instance_fqdn -U postgres
  - CREATE USER iamuser WITH LOGIN;
  - GRANT rds_iam TO iamuser;
  - ALTER ROLE iamuser WITH LOGIN CREATEDB;
  - GRANT postgres TO iamuser;

3 将 RDS 策略附加到 IAM 角色（该角色已附加到 NetBackup 介质服务器）。

创建系统或用户分配的托管标识用户名

对于 Azure SQL Server 和 Managed Instance

执行以下任一配置：

将托管标识用户配置为 AAD 管理员：

- 在 SQL Server 或 Managed Instance 上设置 AAD 管理员。
- 转到“设置”> Azure Active Directory >“设置管理员”。搜索并设置系统分配或用户分配的托管标识，然后保存。

注意：只有将系统分配的托管标识配置为 AAD 管理员的介质服务器才能执行备份和还原。

使用 SSMS 客户端在数据库上创建托管标识用户：

- 要为 SQL Server 设置 AAD 管理员以创建用户，请转到“设置”>“Active Directory 管理员”>“设置管理员”。选择 Active Directory 用户并保存。
- 登录到 SQL 数据库或托管数据库，以在该数据库下创建用户。

```
CREATE USER [<managed_identity>] FROM EXTERNAL PROVIDER;
ALTER ROLE db_owner ADD MEMBER [<managed_identity>];
```

- 在 SQL Server 上为该用户提供登录权限，请运行

```
# CREATE USER [<managed_identity>] FROM EXTERNAL PROVIDER;
# ALTER ROLE loginmanager ADD MEMBER [<managed_identity>];
```

注意：必须为使用系统分配的托管标识与数据库进行通信的所有介质服务器创建用户。

注意：要还原数据库，必须在目标服务器上将托管标识用户配置为 AAD 管理员。

对于 MySQL

- 要为 MySQL 服务器配置 AAD 管理员以创建用户，请转到“设置”>“Active Directory 管理员”>“设置管理员”。选择 Active Directory 用户并保存。
- 使用 Azure CLI 获取托管标识的客户端 ID，请运行

```
# az ad sp list --display-name <managed_identity> --query [*].appId
 --out tsv
```

- 使用 Azure CLI 生成访问令牌以登录，请运行：

```
# az account get-access-token --resource-type oss-rdbms
```

- 使用 AAD 管理员用户和访问令牌登录，请运行：

```
# mysql -h <server name> --user <user name>
--enable-cleartext-plugin --password=<token>
```

- 创建托管标识用户并授予权限，请运行：

```
# SET aad_auth_validate_oids_in_tenant = OFF;
  # CREATE AADUSER '<db_user>' IDENTIFIED BY
'<Generated_client_id>';
  # GRANT USAGE, DROP, SELECT, CREATE, SHOW VIEW, EVENT, LOCK
TABLES , ALTER, CREATE VIEW, INSERT, REFERENCES, ALTER ROUTINE,
PROCESS ON *.* TO '<db_user>'@'%'
```

对于 PostgreSQL

- 要为PostgreSQL服务器配置AAD管理员以创建用户，请转到“设置”>“Active Directory 管理员”>“设置管理员”。选择 Active Directory 用户并保存。
- 获取托管标识的客户端 ID：

```
 # az ad sp list --display-name <managed_identity>  --query
[*].appId --out tsv
```

- 生成登录所需的访问令牌，请运行：

```
# az account get-access-token --resource-type oss-rdbms
```

- 导出生成的令牌的密码，请运行：

```
# export PGPASSWORD=<token>
```

- 使用 AAD 管理员用户和访问令牌登录，请运行：

```
 # psql “host=<host name> port=5432 dbname=<dbname> user=<user
name> sslmode=require”
```

- 创建用户并授予权限，请运行：

```
# SET aad_auth_validate_oids_in_tenant = OFF;
  # CREATE ROLE <db_user> WITH LOGIN PASSWORD '<client_id>' IN
ROLE azure_ad_user;
  # GRANT azure_pg_admin TO <db_user>;
  # ALTER USER smipguser CREATEDB;
  # ALTER USER smipguser Replication;
```

注意：仅 MySQL 灵活服务器支持用户托管标识。托管标识支持不适用于 PostgreSQL 灵活服务器。

为 PaaS 资产添加保护

发现 PaaS 资产后，您可以在“**云**”工作负载的“**应用程序**”或 **PaaS** 选项卡中为其添加保护。

为 PaaS 资产添加保护

1 在左侧，单击“**工作负载**”>“**云**”。

2 要保护 AWS RDS 支持的数据库资产，请单击“**应用程序**”选项卡。对于其他 PaaS 资产，单击 **PaaS** 选项卡。

3 检查要保护的资产是否具有凭据。

请参见第 58 页的“查看应用于数据库的凭据名称”。。

如果“**凭据名称**”列为空，则需要为资产分配凭据。

请参见第 58 页的“向数据库添加凭据 ”。

4 要为资产添加保护，请选择资产并单击“**添加保护**”。

要想执行大多数操作，必须已为资产分配凭据。例如，如果要将资产分配给保护计划，或执行立即备份。

5 选择保护计划，然后单击“**下一步**”。

6 查看配置设置，然后单击“**保护**”。

执行立即备份

使用此选项，可以为所选资产创建一次性备份。此备份不会影响任何未来或预定的备份。

执行立即备份

1 在左侧，单击“**工作负载**”>“**云**”。

要备份 AWS RDS 支持的数据库资产，请单击“**应用程序**”选项卡。对于其他 PaaS 资产，单击 **PaaS** 选项卡。

注意：您可以查看并保护用户创建的数据库。系统数据库不会显示和受到保护，因为这些数据库需要云提供商的超级用户权限才能执行备份和还原。

2 选择资产，然后单击“**添加保护**”。

3 选择所需的保护计划，然后单击“**开始备份**”。

您可以在活动监视器中查看备份作业的状态。

数据库代理从介质服务器内（如果 NetBackup 是在 AKS 和 EKS 环境中部署的，则为容器）访问数据库，并在介质服务器（备份主机）上执行通用共享路径的 NFS 装入。

注意：对于 Azure SQL 数据库的增量式备份，即使资产受备份类型为差异增量式备份的保护计划保护，NetBackup 也会执行完全备份。

2

恢复云资产

本章节包括下列主题：

恢复云资产

可以从快照副本、副本、备份副本或复制副本还原 AWS、Azure、Azure Stack 和 GCP VM 资产。

还原 VM 时，NetBackup 将为您提供更改原始备份或快照副本的某些参数的选项。包括更改 VM 显示名称、更改 VM 的电源选项、在还原期间删除标记关联以及还原到备用网络等选项。也可以将 VM 还原到备用配置、其他区域、其他订购，以及将 VM 或磁盘还原到其他资源组。

- 对于 GCP：选择“**防火墙规则**”
- 对于 Azure：选择“**网络安全组**”
- 对于 AWS：选择“**安全组**”

关于 VM 的恢复前检查

恢复前检查可在还原启动前指出还原可能失败的方式。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。
- 目标网络是否存在
- VM 和磁盘的所选资源组是否存在
- 源 VM 快照是否存在（适用于从快照还原）

- 文件 `/cloudpoint/azurestack.conf` 中添加的暂存位置是否存在（适用于从 Azure Stack 的备份进行还原）
- 是否存在具有相同显示名称的 VM。
- 是否与 Snapshot Manager 连接以及是否已验证云凭据。

还原云资产支持的参数

下表汇总了还原不同云提供商的资产时可以更改的参数。

表 2-1 Azure、Azure Stack、GCP 和 AWS 快照和备份副本支持的参数

参数	快照副本			备份副本		
	Azure	Azure Stack	GCP 和 AWS	Azure	Azure Stack	GCP 和 AWS
更改 VM 显示名称	Y	Y	Y	Y	Y	Y
更改 VM 的电源状态	Y	Y	Y	Y	Y	Y
删除标记关联	Y	Y	Y	Y	Y	Y

还原到其他网络	Y	Y	Y	Y	Y	Y
订购 **ID**				Y	Y	Y
更改资源组	Y	Y		Y	Y	
更改 **VM** 的区域				Y	Y	Y
更改提供商配置				Y	Y	
更改磁盘的资源组	Y	Y		Y	Y	
区域	Y		Y	Y		Y

安全组/防火墙规则/网络安全组	Y	Y	Y	Y	Y	Y

恢复虚拟机

恢复 VM

1 在左侧，单击“**云**”。

2 单击“**虚拟机**”选项卡。

将显示相应类别的所有已发现的云资产。

3 双击要恢复的受保护资产。

4 单击“**恢复点**”选项卡。

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。对于 AWS 工作负载，您可以看到副本以及备份映像（如果提供）。

5 在“**副本**”列中，单击要恢复的副本。您可以看到备份、快照和复制副本（如果提供）。单击“**恢复**”。如果您未选择要还原的副本，系统则会选择主副本。

6 单击“**还原虚拟机**”。

7 在“恢复目标”页面中，执行以下操作：

如果还原备份副本，请根据需要修改以下参数的值：

- **配置**：要还原到其他配置，请从下拉列表中选择一个。
- **区域**：要还原到其他区域，请从下拉列表中选择一个。
- **订购**：要还原到其他订购，请从下拉列表中选择一个。仅适用于 Azure 和 Azure Stack。
- **资源组**：要还原到其他资源组，请单击搜索图标，然后在“**选择资源组**”对话框中选择所需的资源组。仅适用于 Azure 和 Azure Stack。

- **显示名称**：要更改显示名称，请在字段中输入新名称。在恢复前检查期间，系统会验证指定的显示名称。

  注意：除 AWS 工作负载之外，显示名称中不允许有以下特殊字符：` ~ ! @ # $ % ^ & * ( ) = + _ [ ] { } \\ | ; : ' \" , < > / ?."

如果还原快照副本，请仅指定“**资源组**”和“**显示名称**”。

8 单击“**下一步**”。

9 在“恢复选项”页面中：

- 如果还原备份副本，要还原到其他区域，请选择“**区域**”。要选择该区域中的可用网络，请单击“**网络配置**”旁边的搜索图标，然后选择一个目标网络进行恢复。
  用户还可以分别为 AWS、Azure 和 GCP 云提供商选择“**安全组/网络安全组/防火墙规则**”。
- （*仅适用于 GCP*）如果还原快照副本，要还原到其他区域，请选择“**区域**”。要选择该区域中的可用网络，请单击“**网络配置**”中的搜索图标，然后选择一个目标网络进行恢复。该列表显示此区域中的可用网络。
- 如果还原快照副本，要还原到其他区域，请选择“**区域**”。要选择该区域中的可用网络，请单击“**网络配置**”中的搜索图标，然后选择一个目标网络进行恢复。该列表显示此区域中的可用网络。
  用户还可以分别为 AWS、Azure 和 GCP 云提供商选择“**安全组/网络安全组/防火墙规则**”。

在“**高级**”部分中：

- 要使 VM 在恢复后保持开机状态，请选择“**恢复后打开电源**”。
- 要删除备份或创建快照时与资产关联的标记，请选择“**删除标记关联**”。

  注意：如果不选择“**删除标记关联**”选项，则资产的任何标记值在逗号前后都不应有空格。还原资产后，标记值中任何逗号前后的空格将被删除。例如，标记名称的值：**created_on**: *Fri, 02-Apr-2021 07:54:59 PM , EDT* 将转换为 *Fri,02-Apr-2021 07:54:59 PM,EDT*。可以手动编辑标记值以恢复空格。

注意：为区域选择“**无**”意味着 VM 不会放置在任何区域中，而为“**网络安全组/安全组/防火墙规则**”选择“**无**”意味着不会对已还原的 VM 应用任何安全规则。

10 单击“**下一步**”。恢复前检查开始。此阶段将验证所有恢复参数并显示错误（如果有）。可以在启动恢复之前修复错误。

11 单击“**启动恢复**”。

“还原活动”选项卡显示作业进度。

有关恢复状态码的信息，请参见《NetBackup 管理指南》或《NetBackup 状态码参考指南》，网址为：

http://www.veritas.com/docs/000003214

将应用程序和卷恢复到其原始位置

对于 GCP，还原在升级之前创建的快照时，如果源磁盘不存在，则会创建默认的已还原磁盘 pd-standard。

将应用程序和卷恢复到其原始位置

1 在左侧，单击“**云**”。

2 单击“**应用程序**”或“**卷**”选项卡。

将显示相应类别的所有已发现的云资产。

3 双击要恢复的受保护资产。

4 单击“**恢复点**”选项卡。在日历视图中，单击备份发生的日期。

可用映像以行的形式列出，并且每个映像都具有备份时间戳。

5 在首选恢复点的右上方，选择“**原始位置**”。

6 单击“**启动恢复**”。

7 在左侧，单击“**活动监视器**”以查看作业状态。

将应用程序和卷恢复到备用位置

注意事项

- 对于将 AWS 中的加密 VM 还原到备用位置，密钥对名称在源和目标区域中必须相同。如果不同，请在目标区域中创建与源区域中的密钥对一致的新密钥对。

将应用程序和卷恢复到备用位置

1 在左侧，单击“**云**”。

2 单击“**应用程序**”或“**卷**”选项卡。

将显示相应类别的所有已发现的云资产。

3 双击要恢复的受保护资产。

4 单击“**恢复点**”选项卡。在日历视图中，单击备份发生的日期。

可用映像以行的形式列出，并且每个映像都具有备份时间戳。

5 在首选恢复点的右上方，选择“**备用位置**”。

6 选择要还原云资产的位置。

7 单击“**启动恢复**”。

8 在左侧，单击“**活动监视器**”以查看作业状态。

具有只读卷的 GCP VM 的恢复场景

下表介绍了 NetBackup 如何处理具有只读卷的 GCP VM 的还原/恢复。

表 2-2 只读 GCP VM 的恢复场景

场景	处理
通过云工作负载下的“**卷**”选项卡，从挂接的只读磁盘的快照还原卷。	还原期间，磁盘将在读/写模式下挂接到原始位置或备用位置。
通过云工作负载下的“**虚拟机**”选项卡，从崩溃一致快照还原具有只读磁盘的 VM。	在将此类 VM 还原到其原始或备用位置期间，只读磁盘将在读/写模式下还原。

场景	处理
通过云工作负载下的“**虚拟机**”选项卡，从应用程序一致性快照还原具有只读磁盘的 VM。	可以将只读磁盘挂接到多个 VM，但 NetBackup 仅在一个 VM 下发现该磁盘。 对于 Windows VM，快照失败，并出现类似以下内容的 VSS 错误： **Failure: flexsnap.GenericError: Failed to take snapshot (error: Failed to create VSS snapshot of the selected volumes.)"** 对于 Linux VM，在其下搜索到磁盘的 VM 的快照可能成功，也可能失败，但由于缺少依赖关系，其余 VM 的快照将失败。错误示例： **linear_flow.Flow: create snapshot (test-win) of host linux-1(len=4)' requires ['snap_google-gcepd-us-west 2-b-7534340043 132122994'] but no other entity produces said requirements\n MissingDependencies** 在上述情况下，如果 Linux VM 的快照成功，将在读/写模式下还原只读磁盘。

对云资产执行回滚恢复

对云资产执行回滚恢复会重写原始资产上的现有数据。与虚拟机还原不同，回滚还原不会创建已还原映像的新副本，而是替换源上的现有数据。

注意：快照副本不支持回滚。此外，Azure Stack 和 GCP 工作负载不支持回滚还原。

对云资产执行回滚恢复

1 在左侧，单击“**云**”。

2 单击“**虚拟机**”。

将显示相应类别的所有已发现的云资产。

3 双击要恢复的受保护资产。

4 单击“**恢复点**”选项卡。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。在“**副本**”列中，单击要恢复的快照。单击“**恢复**”>“**回滚还原**”。

5 单击“**启动恢复**”。将重写现有数据。

6 在左侧，单击“**活动监视器**”>“**作业**”以查看作业状态。

恢复 PaaS 资产

PaaS 资产在“云”工作负载下列出。可以从“**应用程序**”选项卡还原 AWS RDS PostgreSQL、RDS MySQL、RDS MariaDB、RDS AuroraDB 和 RDS SQL Server 资产，从 **PaaS** 选项卡还原所有其他 PaaS 资产。Azure 资产的恢复流程因其受 NetBackup 保护还是受 Azure 保护而异。

从 NetBackup 10.2 开始，可以单独还原 MySQL 数据库的数据/架构和元数据。要还原元数据，您需要超级用户权限和至少一个 10.2 或更高版本的介质服务器。

注意：对于 MySQL 还原，如果没有管理员或 root 用户权限，则必须具有查看权限和还原权限。

执行即时访问恢复之前，请确保在主服务器的 `bp.conf` 文件中添加密钥 `MEDIA_SERVER_POD_CIDR`。对于在 AKS 或 EKS 环境中部署的 NetBackup，请将其值设置为介质服务器 pod 的子网（逗号分隔值）。例如：
MEDIA_SERVER_POD_CIDR=10.0.0.0/8, 10.0.0.0/16

恢复非 RDS PaaS 资产

可以从“云”工作负载下的 **PaaS** 选项卡还原非 RDS PaaS 资产。

要还原非 RDS PaaS **资产，请执行以下操作**：

1. 在左侧，单击“**工作负载**”下的“**云**”，然后单击 **PaaS** 选项卡。单击要恢复的资产的名称。
2. 单击“**恢复点**”选项卡，对于 Azure 资产，另外选择“**NetBackup 管理**”。

   可用的恢复点将显示在表中。
3. 单击要恢复的映像所在行的“**还原**”。
4. 默认情况下，“**名称**”字段中显示资产的原始名称。您可以在该字段中更改名称。以后可能无法更改此名称。
5. （可选）在“**目标实例**”字段中，资产的源实例默认处于选定状态。要还原到备用实例，请选择所需的实例。“**目标实例**”不可用于 DynamoDB 资产。
6. （可选，仅适用于 MySQL 数据库。）选择“**还原元数据**”以还原元数据，如视图、触发器、存储过程等。
7. （可选，仅适用于 MySQL 数据库。）对于用于还原的目标实例凭据：
   - 选择“**使用已关联的凭据**”，以使用已与实例关联的凭据，然后单击“**启动恢复**”。

- 选择“**使用不同的凭据**”来使用一组不同的凭据，可以是现有凭据，也可以创建新的凭据。
  请参见第 58 页的“向数据库添加凭据 ”。
  用于验证这些凭据的验证主机必须与备份期间使用的主机相同。如果备份期间使用的主机在还原期间进行凭据验证时不可用，则验证将失败。
  （可选）选择“**设置为默认凭据**”，可将这些凭据设置为资产的默认凭据。

8 单击“**启动恢复**”。

“**还原活动**”选项卡显示状态。

恢复基于 RDS 的 PaaS 资产

可以从“**云**”工作负载下的“**应用程序**” 选项卡还原基于 RDS 的 PaaS 资产。

要还原基于 RDS 的 PaaS 资产，请执行以下操作：

1 在左侧，单击“**工作负载**”下的“**云**”，然后单击“**应用程序**”选项卡。单击要恢复的资产的名称。

2 单击“**恢复点**”选项卡，然后在日历中选择要查看其恢复点的日期。

可用的恢复点将显示在右侧。

3 单击要恢复的映像所在行的“**还原**”。

4 在“**源数据库**”下，选择要还原的数据库。单击“**添加数据库**”，在“**添加数据库**”对话框中，选择所需的数据库，然后单击“**选择**”。

5 输入要添加到已还原数据库的前缀，或使用默认值。此字段必须具有值。

6 （可选）在“**目标实例**”字段中，资产的源实例默认处于选定状态。要还原到备用实例，请选择所需的实例。

7 （可选，仅适用于 MySQL 数据库。）选择“**还原元数据**”以还原元数据，如视图、触发器、存储过程等。

8 （可选，仅适用于 MySQL 数据库。）对于用于还原的目标实例凭据：

- 选择“**使用已关联的凭据**”，以使用已与实例关联的凭据，然后单击“**启动恢复**”。
- 选择“**使用不同的凭据**”来使用一组不同的凭据，可以是现有凭据，也可以创建新的凭据。
  请参见第 58 页的“向数据库添加凭据 ”。
  （可选）选择“**设置为默认凭据**”，可将这些凭据设置为资产的默认凭据。

- 选择验证主机以验证提供的凭据。

9 单击“**启动恢复**”。

“**还原活动**”选项卡显示状态。

这两个还原工作流程会针对恢复点隐式创建即时访问装入共享。

恢复 Azure 保护的资产

通过 NetBackup，您可以还原由 Microsoft Azure 备份的 Azure SQL 数据库和 Azure SQL 托管数据库资产。支持的备份模式为“时间点备份”和“长期保留备份”。

注意：不支持在实例池的弹性池中还原。

继续操作前，请确保您具有还原 PaaS 资产所需的权限。

要恢复时间点备份资产，请执行以下操作：

1 在左侧，单击“**云**”。

2 单击 **PaaS** 选项卡。

随即会显示所有发现的 PaaS 资产。

3 在“**恢复点类型**”下，选择“**受提供商保护**”。

4 单击要恢复的受保护 Azure SQL 数据库和 Azure SQL 托管数据库资产所在行的“**还原**”。

5 在“**恢复点**”选项卡中的“**时间点备份**”下，单击“**还原**”。

6 在“**还原点 (UTC)**”下选择日期和时间。您可以选择最早的还原点与以下还原点之间的任何还原点：

- 联机数据库的最新备份时间。
- 已删除数据库的数据库删除时间。

使用 UTC 时间，Microsoft Azure 可能会将所选时间舍入到最接近的可用恢复点。

Web UI 中显示的默认还原日期和时间可能因选定的 PaaS 资产而异。例如，对于 Azure SQL 数据库，默认还原时间是当前时间，对于 Azure SQL 托管数据库，默认还原时间比当前时间早 6 分钟。

7 （可选）对于 Azure SQL 数据库，请在“**数据库名称**”字段中输入已还原数据库的名称。数据库名称不能包含特殊字符，如 < > * % & : \ / 和 ? 或控制字符。数据库名称不能以句号或空格结尾。有关 Azure 资源命名规则的更多信息，请参见 https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules#microsoftsql

如果您不输入名称，NetBackup 将自动分配一个 *<dbName>_<Restored time in UTC>* 格式的名称。

8 （可选）对于 Azure SQL 托管数据库，请在“**托管实例**”字段中输入实例名称。默认情况下，将显示恢复点的实例名称。您还可以使用搜索选项搜索托管实例名称。可还原到您的订购所属的同一区域。

如果在搜索结果中找不到所需的托管实例，请执行手动发现。此外，请确保您对托管实例具有 RBAC 访问权限。

9 单击“**下一步**”。恢复前检查完成后，单击“**启动恢复**”。

可以在活动监视器中查看作业的状态。

要恢复长期保留备份资产，请执行以下操作：

1 在左侧，单击“**云**”。

2 单击 **PaaS** 选项卡。

随即会显示所有发现的 PaaS 资产。

3 单击要恢复的受保护资产所在行的“**还原**”。

4 在“**恢复点**”选项卡的“**长期保留备份**”下，针对要还原的映像单击“**还原**”。

5 （可选）对于 Azure SQL 数据库，请在“**数据库名称**”字段中输入已还原数据库的名称。数据库名称不能包含特殊字符，如 < > * % & : \ / 和 ? 或控制字符。数据库名称不能以句号或空格结尾。有关 Azure 资源命名规则的更多信息，请参见 https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules#microsoftsql

如果您不输入名称，NetBackup 将自动分配一个 *restore_<dbName>* 格式的名称。

6 （可选）对于 Azure SQL 托管数据库，请在“**托管实例**”字段中输入实例名称。默认情况下，将显示恢复点的实例名称。您还可以使用搜索选项搜索托管实例名称。可还原到您的订购所属的同一区域。

7 单击“**下一步**”。恢复前检查完成后，单击“**启动恢复**”。

可以在活动监视器中查看作业的状态。

注意：门户以及 Snapshot Manager 中的标记不会还原。但是，"createdby: cloudpoint" 标记是在通过 NetBackup 进行还原时创建的。

注意：对于受提供商保护的恢复作业，任何间歇性故障都会使恢复作业保持运行，直到运行下一次预定作业清理。

从 AdvancedDisk 恢复复制的映像

如果映像驻留在 AdvancedDisk 存储或 MSDP 云存储上，则 10.1 介质服务器无法从复制的映像启动 PaaS 还原。作为一种解决办法，可以执行以下步骤：

前提条件：

1. 对于 AdvancedDisk，与 MSDP 服务器关联的介质服务器版本必须是 10.1 或更高版本。
2. 对于 MSDP 云存储，用于恢复的介质服务器版本必须为 10.1.1。
3. 确保已在 MSDP 服务器上设置和配置 ushare。
4. 在此 MSDP 存储服务器上创建通用共享。确保在 ushare 的导出列表中添加相应的介质服务器主机名/IP。

要从 AdvancedDisk 进行恢复，请执行以下操作：

1 使用 Web UI 中的目录库，将映像手动复制到 MSDP 存储。有关详细信息，请参见《NetBackup Web UI 管理指南》。

注意：要从第二个副本进行复制，请在目录库视图中选择“复制”选项后再次单击“搜索”。

2 复制作业完成后，确保新恢复点在 Web UI 中对给定资产可见。

要启动还原作业，请参见第 73 页的“恢复 PaaS 资产”。

要使用 REST API 进行还原，请参见以下部分：`recovery/workloads/cloud/scenarios/asset/recover`。请参考 NetBackup API 文档。

注意：对于 RDS 实例恢复，如果从驻留在 AdvancedDisk 存储上的备份映像启动还原，则 NetBackup 不会显示任何错误或警告消息。

3

执行粒度还原

本章节包括下列主题：

关于粒度还原

NetBackup 支持在云虚拟机上对文件和文件夹执行粒度还原。可以创建快照、快照备份和还原，同时还可以查找和还原单个文件和文件夹。此外，也可以从虚拟机还原卷。

此过程称为粒度还原，即，将快照或备份中的每个文件视为一个粒度，通常称为单个文件还原。NetBackup 使用索引编制过程对快照或备份中的所有文件生成清单。仅当 NetBackup 已为快照编制索引时，才能从该快照还原特定文件。还可以从备份中还原特定文件，前提是该备份已由 NetBackup 编制索引。

下表可帮助您了解对卷、文件和文件夹启用粒度还原的流程：

表 3-1 粒度还原任务

任务	描述
连接虚拟机	连接要用于执行粒度还原的虚拟机。
发现虚拟机上的资产	使用“**发现**”选项。 导航到“云” **> Snapshot Manager >** ***Snapshot Manager*** **>** “操作” **>** “发现” 。
创建保护计划	创建保护计划。 确保在保护计划的“**备份选项**”中选中“**启用对文件或文件夹进行粒度恢复**”复选框。
为发现的资产订购保护计划	将在上一步中连接的 VM 上的资产添加到保护计划中，该保护计划具有启用了可索引属性的粒度还原。
执行保护计划	预定备份作业和索引编制，或使用“**立即备份**”选项。备份作业立即启动。
■ 还原文件或文件夹 ■ 还原卷 **注意：**备份副本不支持还原卷。	对文件、文件夹或卷执行粒度还原。

支持的环境列表

下表列出了支持的版本。

表 3-2 支持的版本

应用程序	版本
NetBackup	10.2
NetBackup 备份主机操作系统	RHEL 7.x 和 8.x
Snapshot Manager 主机操作系统	■ RHEL 7.x 及更高版本、RHEL 8.6 ■ Ubuntu 18.04 LTS 和 20.04 LTS **注意：**UI 上列出的操作系统版本 (Ubuntu 20.04 LTS) 是容器的版本。

应用程序	版本
云提供商	■ Amazon Web Services ■ Microsoft Azure ■ Microsoft Azure Stack Hub ■ Google Cloud Platform
Snapshot Manager 或代理实例类型	■ Amazon AWS：t2.large/t3.large ■ Microsoft Azure：D2s_V3Standard ■ Microsoft Azure Stack Hub：DS2_v2 Standard、DS3_v2 Standard ■ Google Cloud Platform：n1.Standard2 及更高版本
要保护的 Snapshot Manager 代理主机	■ Linux 操作系统：RHEL 7.x 和 RHEL 8.2、8.4 和 8.5 ■ Windows 操作系统版本：2012 R2、2016、2019 和 2022

支持的文件系统列表

下表提供了有关所支持文件系统的详细信息。

平台	发现的文件系统	分区布局
RHEL（具有一致快照属性） **注意：**对于 Google Cloud Platform，如果代理主机使用操作系统版本 RHEL 8.x，则必须在操作系统版本为 RHEL 8.x 的主机上安装 Snapshot Manager。	■ ext3 ■ ext4 ■ xfs	■ GPT ■ MBR ■ 无布局（直接 FS）
Windows（具有一致快照属性）	NTFS	■ GPT ■ MBR

注意：Ext2 文件系统版本不支持应用程序一致性快照。

注意：无论目标文件系统/分区类型（FAT、ReFS、LDM 或 LVM）如何，都允许使用 GRT。

开始之前

在执行粒度还原之前，请确保满足以下几点。通过启用粒度还原来保护配置的 Snapshot Manager 和 VM 具有以下要求：

- （*仅适用于快照*）
  - （Microsoft Azure 和 Azure Stack Hub）即使 Snapshot Manager 未与连接的 VM 部署在同一订购和区域中，但如果将备份日程表配置为保护计划的一部分，则也可以执行粒度还原。如果使用仅限快照保护计划日程表，则对于 Azure 和 Azure Stack Hub，需要将 Snapshot Manager 主机与 VM 部署在同一订购和区域中。
  - Amazon AWS：Snapshot Manager 主机和连接的 VM 必须位于同一帐户和区域中。
  - Google Cloud Platform：Snapshot Manager 主机和连接的 VM 必须位于同一项目中。
  - 必须配置云插件，以保护部署 Snapshot Manager 主机的区域中的资产。
  - 如果要将卷还原到同一虚拟机和位置，必须分离现有卷并释放插槽，然后尝试还原。
- 主机必须处于已连接状态，且必须具有所需的支持配置。
- 主机在连接时必须启用 **fsConsistent** 和 **indexable** 标志。indexable 标志适用于仅限快照保护计划日程表。
- 保护计划必须选中“**启用对文件和文件夹进行粒度还原**”复选框。
- 除了引导磁盘和在 /cloudpoint 上装入的磁盘以外，不应将任何额外的磁盘显式挂接到 Snapshot Manager 实例。
- 必须支持主机上的文件系统。
  请参见第 80 页的“支持的文件系统列表”。
- 为打开的 Snapshot Manager 主机配置端口 5671 和 443。
- 对于无代理还原，在 Linux 系统中，在可编制索引的虚拟机上配置端口 22。对于 Windows 平台，在可编制索引的虚拟机上配置端口 135、445 和动态/固定 WMI-IN 端口。
- 在从快照备份执行单个文件还原之前，请确保满足以下几点：
  - 受支持的 NetBackup 和 Snapshot Manager 10.2 及更高版本。
  - 仅当从启用了即时访问的 MSDP 存储服务器（版本必须为 10.2 及更高版本）还原备份映像时，粒度还原才起作用。
  - 必须将目标主机代理升级到最新版本。

- 在 Windows 目标主机上，管理员必须为磁盘启用挂接和分离策略。有关更多信息，请参考 AttachVirtualDisk 函数。
- （对于 Windows）要还原符号链接，必须使用所需的访问权限配置代理。
- 必须在选择“**粒度文件和还原**”选项的情况下进行备份。
- 目标虚拟机必须可以通过访问 NFS/SMB 来访问 MSDP 存储服务器。
- Windows 目标必须满足以下条件：
  - （对于使用访问控制列表还原 Windows 映像内容）Samba 用户凭据必须存储在 MSDP 存储服务器（正在导出即时访问共享）的 Windows 凭据管理器中：
    在 MSDP 服务器上，运行 `smbpasswd -a <username>` 命令以生成 Samba 凭据。
    将具有上述用户名和所生成密码的 MSDP 服务器的 DNS 名称或 IP 添加到 Windows 凭据管理器。
    如果 MSDP 服务器上不存在用户，则 `smbpasswd` 命令将失败。因此，请先使用 `useradd <username>` 命令添加用户，然后再使用 `smbpasswd` 命令。
  - （对于还原 Linux 映像内容）必须安装 NFS 客户端。

  有关如何在 MSDP 上启用 SMB/IA 的更多信息，请参考《NetBackup™ 重复数据删除指南》。
  使用 `/usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh` 预检查脚本验证 MSDP 服务器上的 SMB 配置。

限制和注意事项

执行粒度还原时，请注意下列要点。

- 还原作业完成后，将无法展开还原作业的“**文件列表**”部分中的目录。
- 如果目标位置上没有足够的空间，则还原操作将在复制操作开始之前失败。
- 在活动监视器摘要中，还原作业开始时，将显示当前文件，该文件是还原项中的第一个条目。作业完成后，摘要将变为空白。
- 活动监视器中已传输的字节数和估计的字节数未更新，显示为 0。
- 执行快照时，将忽略临时存储设备。（例如，Amazon AWS 实例存储卷和 Microsoft Azure 临时磁盘。）这些设备在编制索引时也会被忽略。
- 创建主机一致快照并为其编制索引时，会忽略在 LDM 磁盘上创建的文件系统。
- 在未重新启动旧代理（预安装）服务之前，LVM 资产的备用主机还原（GRT 和应用程序）可能会失败。为了支持恢复 LVM 资产，需要重新启动较旧的代理。

- 粒度还原 (GRT) 或单个文件还原 (SFR) 可借助 VxMS 索引编制来执行。VxMS 索引编制适用于所有 Snapshot Manager 支持的文件系统。对于 Azure、Azure Stack、AWS 云和 GCP，可以在基于装入的现有索引上执行 VxMS 索引编制。
- 仅当以只读形式装入时，EXT2 文件系统才支持主机一致快照。
- 如果主机上存在任何不受支持的文件系统，则可将该主机添加到为粒度还原创建的保护计划。粒度还原的保护计划将“**启用对文件或文件夹进行粒度恢复**”复选框的值设置为 true。
- Snapshot Manager 将可以运行的索引作业数传达给 NetBackup。然后，NetBackup 会中止请求。默认情况下，索引作业数初始化为 2。发现 Snapshot Manager 主机功能后，它将增加到可用的磁盘插槽数。但是，您可以在 flexsnap.conf 文件中更新索引编制 max_jobs=<value> 的值，以覆盖此限制。
- Snapshot Manager 主机会限制云提供商强制实施的磁盘插槽数。NetBackup 会中止对 Snapshot Manager 的索引编制请求。为了实现此请求，在云资产发现过程中，NetBackup 会获取 Snapshot Manager 主机功能。这些功能包括“**最大索引作业数**”参数。此参数用于限制在 NetBackup 中发送给 Snapshot Manager 和索引作业队列的请求数。默认情况下，最大并行索引编制作业数为 2。但是，一旦配置了发现 Snapshot Manager 主机的云插件，功能 API 便会根据挂接点和可用资源来获取最大作业数。可以通过在 Snapshot Manager 主机的 **config** 文件中添加 `indexing max_jobs=x` 条目来设置该限制。如果 Snapshot Manager 主机收到的索引编制请求数超过其能力，则请求将排队。
- 在编制索引期间，爬取文件、目录或其他条目时可能会发生操作系统错误。这些错误将被忽略，索引编制操作将继续。要还原缺少的文件，必须对父文件夹启动粒度还原操作。
- 从 Windows VM 创建或装入磁盘时，请添加驱动器盘符。此操作确保索引编制操作可以捕获正确的驱动器盘符。
- 在某些情况下，当您浏览以在恢复点中添加文件或文件夹时，装入点不可见。请考虑以下原因：
  - “/”（根文件系统）位于 LVM 上，并且
  - 装入点与“/”（根文件系统）没有直接关系。

  在这种情况下，请从右侧面板中搜索装入点，然后成功还原文件或文件夹。例如，如果磁盘是在 /mnt1/mnt2 上装入的，其中 /mnt1 是 "/"（LVM 设置上的根 FS）上的任何目录，mnt2 是 mnt1 内的装入点，则在左侧面板上的树中不会显示 "mnt2"。但是，可以在装入点内搜索和还原文件或文件夹。
- 要从 VM 快照恢复点还原文件和文件夹，Linux 服务器上的 `/etc/fstab` 文件必须具有基于文件系统 UUID（而不是设备路径）的条目。设备路径会发生变化，具体取决于 Linux 在系统引导期间发现设备的顺序。

- 将应用程序或文件系统从一个操作系统版本还原到另一个操作系统版本时，请参考操作系统和应用程序供应商的兼容性列表。建议不要将文件系统从较高版本还原到较低版本。
- 用户组无法将作为源的驱动器还原到作为目标的备用文件夹。用户组没有写入权限，无法创建新文件夹。
- 无代理连接无法通过粒度文件级还原（“还原文件和文件夹”选项）还原 Windows（或 EFS）加密的文件。但是，可以通过卷级还原来还原文件，然后解密该文件。
- 仅当基础磁盘具有 GPT 分区布局时，才能还原文件夹（结合点）上装入的卷中存储的文件。如果卷是使用驱动器盘符装入的，则不管基础磁盘的分区布局如何，都可以还原文件。
- 从快照备份执行单个文件还原时，请考虑以下限制：
  - 如果在源主机为 Linux 且目标主机为 Windows 的情况下还原文件/文件夹，则
    - 无法在 Windows 主机上还原文件属性，只能还原文件内容。
    - 如果要还原的选定文件/文件夹中存在任何符号链接，则不会还原符号链接。
  - 对于“原始位置还原”，跳过复制前的可用大小检查。
  - 如果在源主机为 Linux 且目标主机为 Linux 的情况下还原文件/文件夹，则不会还原套接字和块文件。
  - 当文件和文件夹驻留在 LDM 磁盘/动态磁盘/存储空间上时，不支持还原这些文件和文件夹。
  - 如果介质服务器或 PureDisk 重复数据删除引擎和 Veritas 置备文件系统后台驻留程序服务重新启动，则部分还原成功期间保留的实时装入将在保留期限到期之前删除/失效。
  - 如果介质服务器未升级到 10.2，则将使用 10.2 上的主服务器连接到 NetBackup Snapshot Manager。
  - 编制索引后，Windows 上的结合点在“**添加文件**”中显示为以下格式：卷{4e3f8396-490a-400a-8abf-5579cafd4c0f}。从备份执行单个文件还原操作时，如果在“**添加文件**”中选择了结合点，则选择“**将所有内容还原到其他位置**”，并在“高级”选项中启用“**需要还原访问控制列表**”。

从云虚拟机还原文件和文件夹

可以从云虚拟机还原单个文件或文件夹。

注意：对于 Microsoft Azure、Google Cloud Platform 和 Amazon AWS，NetBackup 支持使用管理器提供的密钥加密的云资产的快照和恢复。

还原文件或文件夹

1 在左侧，单击“**云**”。

2 单击“**虚拟机**”选项卡。

3 选择托管应用程序的虚拟机。在右上方，单击“**连接**”。

4 连接 VM 后，在右上方，单击“**添加保护**”。

5 选择为对文件和文件夹执行粒度恢复而创建的保护计划，然后单击“**下一步**”。

6 单击“**保护**”。

7 要执行保护计划，请单击“**立即备份**”。

8 当资产的一个快照和两个索引编制作业或者两个从快照备份作业都完成后，请单击“**恢复点**”选项卡。

9 对于首选恢复点，从“操作”菜单中选择“**还原文件和文件夹**”。

还可以通过单击“**恢复**”，然后针对特定类型的副本选择“**还原文件和文件夹**”，来还原“**快照**”和“**备份**”类型副本的文件和文件夹。

10 在“添加文件”步骤中，单击“**添加**”。

11 在“**添加文件和文件夹**”对话框中，选择要还原的文件，然后单击“**添加**”。

可以单击左侧的文件夹或驱动器，以展开并查看特定文件夹中的文件。可以根据文件的名称或扩展名搜索文件。

12 单击“**下一步**”。

13 在“恢复目标”步骤中，执行以下操作：

对话框	快照副本	备份副本
还原至	**目标 VM** - 选择 VM。此时将显示一个列表，其中包含与原始目标主机具有相同操作系统的所有已连接的 VM。如果不选择 VM，则会将这些文件还原到原始 VM。	■ **云提供商** - 选择要执行单个文件还原的云提供商。 ■ **配置** - 要还原到其他配置，请从下拉列表中选择一个。 ■ **区域** - 要还原到其他区域，请从下拉列表中选择一个。 ■ （*仅适用于 Azure 和 Azure Stack*）**订购** - 要还原到其他订购，请从下拉列表中选择一个。 ■ **目标 VM** - 选择 VM。对于跨平台还原，将显示包含所有已连接/断开连接的 VM 和 Linux/Windows VM 的列表。
还原目标选项	■ **将所有内容还原到原始位置** ■ **将所有内容还原到其他位置** 然后，必须提供目录位置。也可以输入位置的 UNC 路径。	

以下情况支持跨平台还原：

- NetBackup 和 Snapshot Manager 在一个云中，目标主机位于另一个云中。
- NetBackup 和 Snapshot Manager 在一个云中，另一个 Snapshot Manager 和目标主机位于另一个云中。
- NetBackup 和 Snapshot Manager 在一个云中，AIR（自动映像同步复制）还原在另一个域中进行。

14 如果选择了“**将所有内容还原到原始位置**”选项，请单击“**下一步**”，然后在“恢复选项”步骤中选择以下首选选项：

对话框	快照副本	备份副本
选项	■ **将字符串附加到文件名** 在“**字符串**”字段中，输入要用于附加的字符串。该字符串附加在文件的最后一个扩展名之前。 ■ **允许重写现有文件** 必须具有适当权限。	

对话框	快照副本	备份副本
高级选项	N/A	■ （*仅适用于 Windows 到 Windows 还原*）**还原访问控制列表时需要** - 选中该复选框以还原访问控制列表，这需要其他操作。 ■ **目标主机 NAT 网关 IP 地址** - 输入网络地址转换网关 IP 地址（如果目标 VM 位于网络网关之后且不可直接访问）。 **注意：**仅允许使用专用 IP 或主机名。

15 如果选择了“**将所有内容还原到其他位置**”选项，则提供“**用于还原的目录**”，然后单击“**下一步**”。

16 在“审查”步骤中，查看所选的选项，然后单击“**启动恢复**”。

将触发所选文件的还原作业。可以在活动监视器上查看作业详细信息。作业成功完成后，可以在作业详细信息中查看已还原文件的摘要。

注意：在还原到非相似环境（用户/组不匹配）期间，根据 uid/guid 分配对文件的权限。已还原的文件/文件夹必须对目标主机上的非预期用户/组具有权限。因此，成功还原所需文件后，用户必须根据要求修改访问权限。

请注意下列事项：

对于从快照或备份进行单个文件还原（源 Linux VM 到目标 Linux VM），还原硬链接时，请确保遵循以下准则：

- 在“**添加文件和文件夹**”对话框中选择文件夹和文件时，不要选择冗余条目。例如，选择一个文件夹和存在于同一文件夹中的文件，因为该文件夹已包含该文件。
- 即使选择了冗余条目，请确保不要在“恢复选项”步骤中选择“**允许重写现有文件**”选项。这将导致复制硬链接文件失败。

在云虚拟机上还原卷

可以在虚拟机上还原一个或多个卷。

还原卷

1 在左侧，单击“**云**”。

2 单击“**虚拟机**”选项卡。

3 选择托管应用程序的虚拟机。

4 连接 VM 后，在右上方，单击“**添加保护**”。

5 选择保护计划，然后单击“**下一步**”。

6 单击“**保护**”。

7 要执行保护计划，请单击“**立即备份**”。

8 要查看恢复点，请单击“**恢复点**”选项卡。

9 在首选恢复点的右上方，选择“**还原卷**”。

您还可以应用日期过滤器来跨恢复点进行搜索。

10 在“**还原卷**”对话框中，选择一个或多个卷。

11 从“**目标 VM**”列表中，选择要在其上还原卷的 VM。

如果从复制的 VM（非主 VM）进行还原，则不支持还原到原始位置。如果不选择 VM，则会将这些文件还原到原始 VM。

12 单击“**还原**”。

将触发所选卷的还原作业。可以在活动监视器上查看作业详细信息。

故障排除

对 Microsoft Azure 云的快照还原过程进行故障排除

在同一 VM 上连续（两次）触发还原操作时，还原操作过程中会出现错误。此错误可能导致以下问题：

- 原始操作系统磁盘中的标记不会复制到新创建的已还原操作系统磁盘。
- VM 还原因 ssh 故障而失败后，用户登录可能会失败。

解决方法：

检查 ssh 后台驻留程序是否正在系统上运行。否则，请执行 Microsoft 提供的以下文档中提及的步骤：

learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-ssh-connection

过滤不支持的文件和文件夹

如果尝试从不受 Snapshot Manager 支持的分区或文件系统还原文件或文件夹，则还原作业中将发生以下错误。

错误 nbcs (pid=<processs id>) **无法从快照还原资产** <资产名称> **的文件和文件夹**

解决方法：

如果要避免在浏览单个文件还原时列出 Snapshot Manager 不支持的文件或文件夹，请通过在 NetBackup 主服务器的 bp.conf 文件中设置以下标志来启用 CP DISKMAP 检查。

CP_DISKMAP_CHECK = true/yes

“从还原备份”操作部分成功

所选目标目录上的磁盘已满时，“从还原备份”操作部分成功。将显示以下消息：

```
Dec 29, 2022 2:57:51 PM - Info nbcs (pid=2244) Granular restore(SFR) is completed
    Dec 29, 2022 2:57:51 PM - Info nbcs (pid=2244) Summary of SFR Operation - Success
files/folders count: 0 ,
    Failed files/folders count: 1 , Warning files/folders
    count: 0, Skipped files/folders count: 0
    Dec 29, 2022 2:57:51 PM - Info nbcs (pid=2244)
    Detailed restore summary report is available on recovery target host at location:
    /var/log/flexsnap/restore/granular-restore-09b4d44d
    .
    .
    Dec 29, 2022 2:57:51 PM - Warning bprd (pid=1977) Granular Restore from backup
completed with error.
    Copy the files manually from live access mount:

ip-10-239-185-241:/mnt/vpfs_shares/vmfiles/8fcc/8fcc132b-a202-49a8-b654-81ff242a718a/livemount

    Dec 29, 2022 2:57:51 PM - end Restore; elapsed time 0:01:51
    the requested operation was partially successful(1)
```

对于从还原备份，如果成功创建了实时装入，则即使报告了除ASSET_NOT_FOUND之外的其他错误，也将其视为部分成功。如果没有在目标位置装入网络设备/文件系统且磁盘已满，则在作业详细信息中可以看到以下消息：

```
 Jan 02, 2023 12:11:16 AM - Error nbcs (pid=13934)
187776K space required for file/folder restore while 20K is total available space on
/disk1
```

在这种情况下，必须已在目标路径上装入其他网络设备/文件系统，因此 Snapshot Manager 代理会考虑设备/文件系统上的可用空间。但是，一旦它尝试复制文件就会失败，并将空间错误记录到摘要报告中。例如，

```
 /var/log/flexsnap/restore/granular-restore-09b4d44d in above Job details log
```

解决办法：

- 检查目标主机位置的摘要报告。例如，

```
/var/log/flexsnap/restore/granular-restore-09b4d44d
[root@ip-10-239-187-148 granular-restore-09b4d44d]# cat root-error.log
Dec 29 09:27:44: ERROR - FILE: /disk1/dl380g9-149-vm15_package.zip
[Error 28] IOError: No space left on device
```

- 如果由于磁盘空间导致文件复制操作失败，则创建一些空间并从实时装入复制文件。
  作业详细信息中可找到实时装入路径详细信息，如下所示：

```
Dec 29, 2022 2:57:51 PM - Warning bprd (pid=1977) Granular Restore from backup completed
 with error.
Copy the files manually from live access mount:
ip-10-239-185-241:/mnt/vpfs_shares/vmfiles/8fcc/8fcc132b-a202-49a8-b654-81ff242a718a/livemount
```

当用户选择已断开连接的目标虚拟机时，会观察到部分恢复

部分恢复可能是由于以下原因：

- 如果目标虚拟机已断开连接（未通过代理连接）。
- 复制目标虚拟机上的文件/文件夹时，如果出现任何故障。
- 在 Linux 目标虚拟机上还原 Windows 虚拟机内容。

在此类部分恢复情况下，创建的实例访问权限不会被删除，并且将在接下来的 24 小时内可用。

通过在 `bp.conf` 文件中设置 **CLOUD_VM_IA_RETENTION_INTERVAL_IN_HOURS** 项，可以配置实例访问保留间隔。（默认值为 24 小时）。

解决办法：

用户可以执行手动步骤来访问目标主机上的即时访问共享，然后手动复制所需的文件/文件夹。

（通过 NFS 复制文件）要在 Linux 主机上还原 Linux 映像内容，请执行以下操作：

- 要在 Linux 系统上装入 NFS 共享，请使用以下命令安装 NFS 客户端软件包：

```
$ sudo yum install nfs-utils
```

- 使用以下装入命令，在目标 Linux 主机上装入即时访问：

```
# Create a directory say /mnt/restore

$ mkdir -p /mnt/restore

# Mount the instant access

$ mount -t nfs <InstantAccessServer:InstantAccessPath> /mnt/restore
```

- 可以从活动管理器日志中检索即时访问路径，其格式如下：
  <InstantAccessServer>:/mnt/vpfs_shares/vmfiles/<id>/<InstantAccessId>/livemount

（SMB 访问）要在 Windows 目标主机上还原 Windows 映像内容（使用 ACL），请执行以下操作：

- 必须将源虚拟机映像的 MSDP 存储服务器的 SMB 凭据添加到 Windows 凭据管理器。
- 通过导航到“**活动监视器**”>“**作业详细信息**”，使用给定的实时装入来访问虚拟硬盘。
  虚拟硬盘在以 **vhd_** 作为前缀的文件夹下列出。
- 在“**操作**”选项卡下的“磁盘管理”对话框中，挂接所需的虚拟硬盘，然后单击“**确定**”。
- 在“添加驱动器盘符或路径”对话框中，选择“**分配以下驱动器盘符**”选项，将盘符分配给虚拟磁盘以浏览数据，然后单击“**确定**”。
- 导航到上述步骤中分配的驱动器，然后手动复制数据。

（实时装入）要在 Linux 目标主机上还原 Windows 映像内容，请执行以下操作：

- Linux 必须具有 cifs 软件包。使用 `# yum install cifs-utils` 命令获取软件包。
- 使用 `# mkdir <my_mount_dir>` 命令创建装入目录。
- 使用 Samba 用户名和密码装入导出的路径，如下所示：

```
mount -t cifs -o username=<sambauser>
//<InstantAccessServer>/<InstantAccessPath> <my_mount_dir>
```

- 使用以下命令复制文件：

```
# cp <my_mount_dir>/<file_path> <target_dir_path>
```

从快照的备份还原单个文件时遇到问题

问题/错误	描述	解决方法
要检查的日志路径	有关目标主机上还原详细信息的信息，请检查以下日志： ■ path/file: /tmp/flexsnap-agentless-onhost.log ■ /var/log/flexsnap/restore/granular-restore-*	要解决 Snapshot Manager 上单个文件还原期间发生的故障或异常，请参考 Snapshot Manager 主机上的以下日志： /cloudpoint/logs/flexsnap.log
恢复前检查失败	将文件和文件夹还原到已断开连接的目标虚拟机时，恢复前检查失败并显示以下错误： Target VM state: Target VM <vm_name> has no agent configured 如果启动恢复，还原操作将部分成功。	确保目标虚拟机处于连接状态并配置了代理，以成功进行还原。
将源 Linux VM 部分恢复到目标 Windows VM（无 NFS 客户端）	将文件和文件夹从源 Linux VM 还原到目标 Windows VM 而不在 Windows 目标计算机上安装 NFS 客户端时，恢复部分成功，并显示以下错误： Error nbcs (pid=42513) Invalid operation for asset: <asset_id> Warning bprd (pid=42045) Granular Restore from backup completed with error. Copy the files manually from live access mount: <livemount_path>. Note that live access mount is available only for 24 hrs.	从 Linux VM 还原到 Windows VM 之前，在 Windows 目标计算机上安装 NFS 客户端。
已删除的目标 VM 的还原作业失败	还原已从云环境中删除的目标 VM 上的文件和文件夹时，还原作业失败并显示以下错误： Error nbcs (pid=44859) Target VM not found, asset_id <asset_id>	选择其他目标 VM。
创建即时访问失败	如果未在 MSDP 存储服务器上启用即时访问，则在还原作业期间创建即时访问将失败。	使用以下预检查脚本，验证 MSDP 介质服务器是否支持即时访问： /usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh
目标 VM 没有用于连接虚拟磁盘的可用驱动器	如果包含所选文件的卷数超过目标主机上的可用驱动器数，则操作将失败。	从较少数量的卷还原文件和文件夹。
空间不足：'*\\driverMapping.json	如果配置了 MSDP 的介质服务器已启用 FIPS。	在安装了 MSDP 的介质服务器上禁用 FIPS，或将域用户 samba 凭据添加到目标 VM。

Azure 云提供商 VM 的问题

如果其中一个 VM 磁盘未初始化，则使用即时访问下载或还原 VM 文件将失败，并显示以下错误：

```
Jan 24, 2023 11:58:47 AM - Error NBWMC (pid=3716) Internal Error:
('failed to find operation system information, please check the source
 VM', ('Failed to expose
VMDK', 1006), None)
Failed to create the instant access mount.
(4001)
```

Libguestfs 是即时访问用于从 VM 备份检索文件的第三方工具。如果磁盘未初始化，libguestfs 将无法处理它。

解决办法：

初始化磁盘，备份 VM，然后尝试使用即时访问再次下载或还原 VM 文件。

4

对云资产的保护和恢复进行故障排除

本章节包括下列主题：

- 对云工作负载保护问题进行故障排除
- 对 PaaS 工作负载保护和恢复问题进行故障排除

对云工作负载保护问题进行故障排除

查看以下日志文件以对有关保护云资产的任何问题进行故障排除：

- 配置的日志文件
- 快照创建的日志文件
- 还原操作的日志文件
- 快照删除的日志文件

在故障排除期间，请确保您还查看了限制。请参见第 8 页的“限制和注意事项”。

有关故障排除问题，请参见 NetBackup 状态代码参考指南。

要查看 Snapshot Manager 日志文件，请参见《NetBackup Snapshot Manager 安装和升级指南》中的 Snapshot Manager 日志主题。

配置的日志文件

使用以下日志对云配置问题进行故障排除。

表 4-1 配置的日志文件

进程	日志
tpconfig tpconfig 命令是在 NetBackup 中注册 Snapshot Manager 的一种方法。	Windows *NetBackup install path*/volmgr/debug/tpcommand UNIX /usr/openv/volmgr/debug/tpcommand
nbwebservice 将使用 NetBackup REST API 配置插件。	Windows *NetBackup install path*/webserver/logs UNIX /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices
nbemm nbemm 会将 Snapshot Manager 和插件信息存储在 EMM 数据库中。	Windows *NetBackup install path*/path/logs/nbemm UNIX /usr/openv/logs/nbemm

资产发现的日志文件

使用以下日志对资产发现问题进行故障排除。

表 4-2 资产发现的日志文件

进程	日志
ncfnbcs 验证是否已完成发现。	Windows *NetBackup **安装路径***/bin/vxlogview -o 366 UNIX /usr/openv/netbackup/bin/vxlogview -o 366
Picloud 提供发现操作的详细信息。	Windows *NetBackup install path*/bin/vxlogview -i 497 UNIX /usr/openv/netbackup/bin/vxlogview -i 497

进程	日志
nbwebservice 获取有关属于发现操作的资产数据库工作流程的详细信息。 **注意**：有关添加到保护计划的资产的详细信息，请参考相同的日志文件。	Windows *NetBackup install path*/webserver/logs UNIX /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices

快照创建的日志文件

使用以下日志对快照创建问题进行故障排除。

表 4-3 快照创建的日志文件

进程	日志
nbpem NetBackup 活动监视器中提供了给定作业的 nbpem PID。	Windows *NetBackup install path*/bin/vxlogview –o 116 UNIX /usr/openv/netbackup/bin/vxlogview -o 116
nbjm NetBackup 活动监视器中提供了给定作业的 nbjm PID。	Windows *NetBackup install path*/bin/vxlogview –o 117 UNIX /usr/openv/netbackup/bin/vxlogview -o 117
nbcs NetBackup 活动监视器中提供了给定作业的 nbcs PID。	Windows *NetBackup install path*/bin/vxlogview –i 366 -P *nbcs_process_id* UNIX /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id* 可从以下位置获取 nbcs 日志： Windows *NetBackup install path*/logs/ncfnbcs UNIX /usr/openv/logs/ncfnbcs

进程	日志
nbrb 为给定作业提供介质服务器时需要 nbrb。对于云，从 Snapshot Manager 的关联介质服务器列表中选取特定介质服务器。	Windows *NetBackup install path*/bin/vxlogview –o 118 UNIX /usr/openv/netbackup/bin/vxlogview -i 118

还原操作的日志文件

使用以下日志对还原问题进行故障排除。

表 4-4

进程	日志
nbwebservice 快照还原操作由 NetBackup REST API 触发。	Windows *NetBackup install path*/webserver/logs UNIX /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices
bprd NetBackup REST API 与 bprd 通信以启动还原。	Windows *NetBackup install path*/netbackup/logs UNIX /usr/openv/netbackup/logs/bprd
ncfnbcs NetBackup 活动监视器中提供了给定作业的 nbcs PID。	Windows *NetBackup install path*/bin/vxlogview –i 366 -P *nbcs_process_id* UNIX /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id*

快照删除的日志文件

使用以下日志对快照删除问题进行故障排除。

表 4-5 快照删除的日志文件

进程	日志
bpdm 快照删除或清理操作由 bpdm 触发。	Windows *NetBackup install path*/netbackup/logs UNIX /usr/openv/netbackup/logs/bpdm
ncfnbcs NetBackup 活动监视器中提供了给定作业的 nbcs PID。	Windows *NetBackup install path*/bin/vxlogview –i 366 -P *nbcs_process_id* UNIX /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id*

备用位置还原期间恢复前检查失败并出现访问被拒绝错误

尝试从备份映像副本执行 VM 恢复时，如果没有为角色分配执行备用位置还原所需的权限，则恢复前检查操作期间会遇到错误。

如果仅具有执行原始位置恢复的权限，并且尝试执行备用位置恢复，则可能会发生这种情况。

解决方法

- 执行原始位置还原时，请勿更改恢复前页面中的任何预填充字段。
- 如果要执行备用位置恢复，请确保具有所需的权限。

对 PaaS 工作负载保护和恢复问题进行故障排除

备份失败并显示错误：3808 无法检查数据库是否存在。

可以在活动监视器中看到以下消息：

授权失败 - 消息：客户端 '<clientId> '<objetId>' 无权对范围 '<resoourceId>' 执行操作 'Microsoft.Sql/servers/databases/read'，或者范围无效。如果最近为您授予了访问权限，请刷新您的凭据。

解释：在以下情况下会出现此错误：Snapshot Manager 和 NetBackup 部署在 AKS 中，并且：

- 介质服务器 pod 节点池是与 Snapshot Manager 节点池不同的节点池
- 在 Snapshot Manager 虚拟机扩展集中启用了托管标识

解决办法：执行以下任一操作：

- 在用于备份和还原的介质服务器中，在扩展集中启用托管标识。此外，在附加到此托管标识的角色中分配所需权限。
- 在 MSDP 服务器上创建存储单元，并仅使用在扩展配置中启用了托管标识的介质服务器。

当数据库或资源组应用了只读锁定时，备份将失败，当应用了删除锁定时，备份将部分成功。

解释：如果将只读锁定或删除锁定属性应用于数据库或资源组，则会发生此问题。

解决办法：在执行任何备份或还原之前，从数据库或资源组中删除任何现有的只读锁定和删除锁定属性。

状态码 150：管理员请求了终止

解释：从活动监视器手动取消备份或还原作业且在部分还原操作期间于门户上创建了数据库时，会出现此错误。

解决办法：手动清理提供商门户上的数据库，以及通过数据库名称创建的特定目录下通用共享装入位置处的临时暂存位置。

活动监视器中的失效状态消息

解释：如果 Snapshot Manager 容器服务突然重新启动，受提供商保护的还原作业可能保持活动状态，您可能无法在活动监视器详细信息页面上看到更新的状态。

解决办法：在 Snapshot Manager 中使用以下命令重新启动工作流程容器：

```
docker restart flexsnap-workflow-system-0-min
flexsnap-workflow-general-0-min
```

重新启动容器后，还原作业将在活动监视器中更新为最新状态。

状态码 233：过早遇到 EOF

解释： 如果用于备份的客户端名称长度超过 255 个字符，则会显示此错误。

bpdbm 日志通过显示以下错误消息来确认此错误：

```
db_error_add_to_file: Length of client is too long. Got 278, but
limit is 255. read_next_image: db_IMAGEreceive() failed: text exceeded
allowed length (225)
```

注意：当主服务器是 RHEL 时，会出现此错误。

解决办法：重命名数据库，使客户端名称适合 255 个字符的长度。

Error: Broken pipe (32), premature end of file encountered EXITING with status 42, network read failed

解释：如果使用的客户端名称较长，则在备份期间会发生此错误，由于此目录库映像的文件路径长度超过 256 个字符，因此会失败并在活动监视器中显示上述错误消息。

bpdbm 日志通过显示以下错误消息来确认此错误：

```
<16> db_error_add_to_file: cannot stat(\\?\C:\Program Files\Veritas
\NetBackup\db\images \azure-midb-1afb87487dc04ddc8fafe453dccb7ca3+
nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+
testdb_bidinet02\1656000000\tmp\catstore\
BACKUPNOW+141a73e7-cdc4-4371-823a-f170447dba2d_
1656349831_FULL.f_imgUserGroupNames0): No such file or directory (2)
<16> ImageReadFilesFile::get_file_size: cannot stat(\\?\C:\Program
Files\Veritas\NetBackup\db
\images\azure-midb-1afb87487dc04ddc8fafe453d
ccb7ca3+nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+testdb_
bidinet02\1656000000\tmp\catstore\BACKUPNOW+141a73e7-cdc4-4371
-823a-f170447dba2d_1656349831_FULL.f_imgUserGroupNames0): No such
file or directory (2) <16> ImageReadFilesFile::executeQuery: Cannot
copy \\?\C:\Program
Files\Veritas\NetBackup\db\images\azure-midb-1afb87487dc04ddc8fafe453dccb7
ca3+nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+testdb_bidinet02\1
656000000\tmp\catstore\BACKUPNOW+141a73e7-cdc4-4371-823a-f170447d
ba2d_1656349831_FULL.f_imgUserGroupNames0
```

注意：当主服务器是 Windows 时，会出现此错误。

解决办法：重命名数据库，使文件路径长度适合 256 个字符的长度。

状态码 3801：无法完成请求的操作。

解释：NetBackup 无法成功执行请求的操作。

建议的操作：有关可能的失败原因，请参考活动监视器详细信息。

状态码 3817：无法完成备份前操作

解释：dbagentsutil 日志中显示的错误消息为 `pg_dump: error: query failed: ERROR: permission denied for table test;pg_dump: error: query was: LOCK TABLE public.test IN ACCESS SHARE MODE;Invoked operation: PRE_BACKUP failed`

如果尝试备份的数据库包含多个具有不同角色的表，则会发生这种情况。如果表有至少一个除数据库所有者之外的其他所有者，并且它不是数据库所有者角色的成员，则备份可能会失败。

推荐的操作：必须具有一个角色，该角色有权访问要备份或还原的数据库中的所有表。

例如，我们想备份包含两个表的 School 数据库。

- 对于 student 表，所有者是 postgres
- 对于 teacher 表，所有者是 schooladmin

创建新角色。比如说，NBUbackupadmin

运行以下命令以创建角色：

```
postgres=> CREATE USER NBUbackupadmin WITH PASSWORD '***********';

CREATE ROLE
```

要使此新角色成为 postgres 和 schooladmin 角色的成员，请运行：

```
postgres=> GRANT postgres TO NBUbackupadmin;

GRANT ROLE

postgres=> GRANT schooladmin TO NBUbackupadmin;

GRANT ROLE
```

注意：对于数据库中的所有表，您必须具有一个角色，该角色是表的所有者或所有者的成员。

备份失败，状态码为 40（网络连接断开）

解释：由于与介质服务器的连接断开，备份失败。

推荐的操作：如果策略启用了检查点，则可以重新启动备份作业。解决网络问题后，在 Web UI 中选择未完成的备份作业，然后单击“**继续**”。作业将从停止的点继续。如果策略中未启用检查点，则作业在 Web UI 中显示为失败的作业。

备份作业失败并显示错误：“无法备份数据库”

解释：作业详细信息包含其他详细信息：ManagedIdentityCredential 身份验证不可用。请求的身份未分配给此资源。分配的介质服务器未附加任何托管标识。

建议的操作：如果对 PaaS Azure SQL 和 Managed Instance 使用系统或用户托管标识，请将同一组权限/规则应用于介质服务器和 Snapshot Manager。如果使用用户托管标识，请将同一用户托管标识附加到介质服务器和 Snapshot Manager。

错误代码 3842 - 不支持相应 PaaS 资产的所请求备份类型。

仅 Azure SQL Server 支持差异增量式备份。选择不支持的备份类型时，将显示此错误。

错误代码 3843 或 3844 - 无法禁用 CDC。

当您无权启用或禁用 CDC 时显示此消息。

解释：向 NetBackup 授予在 Azure 环境中启用或禁用 CDC 所需的权限。

注意：不要手动启用 CDC。为 NetBackup 提供启用或禁用 CDC 的权限。

错误：客户端还原退出状态 5：还原操作无法恢复请求的文件，云策略还原错误 (2824)

错误：出错 - 无法还原名为 [<db_name>] 的数据库 [<db_name>]。出错 - 无法打开文件。错误编号 = 12：客户端还原退出状态 5：还原操作无法恢复请求的文件

解释：如果在 10.2 版介质上生成备份映像，并还原到旧版 (< 10.2) 介质服务器，则在还原期间会发生此错误。

解决办法：将还原介质更改为 10.2 并从存储中删除较旧的介质。