

Acronis

Acronis Cyber Infrastructure 3.5

面向 VMware vSphere 的 Backup
Gateway 快速入门指南

July 30, 2020

版权声明

版权所有 ©Acronis International GmbH, 2003-2020。保留所有权利。

“Acronis”、“Acronis Compute with Confidence”、“Acronis Recovery Manager”、“Acronis 安全区”、“Acronis True Image”、及 Acronis 标志均是 Acronis International GmbH 的商标。

Linux 为 Linus Torvalds 的注册商标。

VMware 和 VMware Ready 是 VMware, Inc. 在美国和/或其他管辖区的商标和/或注册商标。

Windows 和 MS-DOS 为 Microsoft Corporation 的注册商标。

引用的所有其他商标和版权均为其各自所有者的财产。

未经版权所有人的明确许可，禁止对本文档进行实质性修改并予以发布。

事先未征得版权所有人的许可，禁止出于商业目的，以任何标准（纸张）书籍形式，发布本作品及其衍生作品。

文档按“原样”提供，对于任何明示或暗示的条件、陈述和保证，包括任何对适销性、对特殊用途的适用性或不侵权的暗示保证，我方概不负责，除非上述免责声明被依法判定为无效。

三方代码可由软件和服务提供。此类第三方的许可证条款将在位于安装根目录中的 license.txt 文件中详细说明。您可以随时通过访问以下网址找到最新的三方代码列表以及与软件和服务使用相关的许可证条款：<http://kb.acronis.com/content/7696>。

Acronis 专利技术

本产品中使用的技术涵盖在以下一项或多项美国专利范围内并受这些专利保护，专利号为：7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234 以及正在申请的专利。

Contents

1. 关于本指南	1
1.1 要求	1
2. 配置网络	3
3. 创建虚拟机	6
4. 在虚拟机中部署 Acronis Cyber Infrastructure	11
4.1 部署管理节点	12
4.2 部署次要节点	13
5. 将空间添加至 Acronis Cyber Infrastructure	15
6. 通过 Backup Gateway 将 Acronis Backup 软件连接到存储后端	17
6.1 通过 Backup Gateway 连接到本地存储簇	18
6.2 通过 Backup Gateway 连接到外部 NFS 共享	20
6.3 通过 Backup Gateway 连接到公共云存储	23
6.3.1 重要要求和限制	25
6.3.2 设置 Backup Gateway	25

CHAPTER 1

关于本指南

本指南介绍了如何在 VMware vSphere 6.5 及更高版本中部署 Acronis Cyber Infrastructure 和配置 Backup Gateway。

简言之，您需要执行以下操作：

1. 配置网络。
2. 为 Acronis Cyber Infrastructure 创建虚拟机。
3. 在虚拟机中部署 Acronis Cyber Infrastructure。

所有这些步骤在后续章节中进行了详细描述。

部署了 Acronis Cyber Infrastructure 后，需要为您的方案配置它。设置 Backup Gateway 的步骤在通过 [Backup Gateway](#) 将 *Acronis Backup* 软件连接到存储后端 (page 17) 中提供。其他说明在 Administrator's Guide 中提供。

1.1 要求

- 对于 Backup Gateway 方案，可以在单个虚拟机中部署 Acronis Cyber Infrastructure。但对于一般目的的部署，建议创建三个或五个虚拟机以支持负载均衡和高可用性。
- 确保 vSphere 数据存储有足够的可用存储空间。每个虚拟机至少占用 425 GB（两个 200 GB 存储磁盘和一个 25 GB 系统磁盘）。Acronis Cyber Infrastructure 模板也占用大约 35 GB。
- 确保主机有足够的内存。对于一个节点的设置，最小为 4 GB 的 RAM。否则，至少需要 8 GB 的 RAM 用于管理节点，至少 4 GB 的 RAM 由每个次要节点占用。
- 为每个 Backup Gateway 簇使用一个单独的对象容器。

注解: Backup Gateway 方案的完整硬件要求在 Hardware Requirements 中进行了描述。

CHAPTER 2

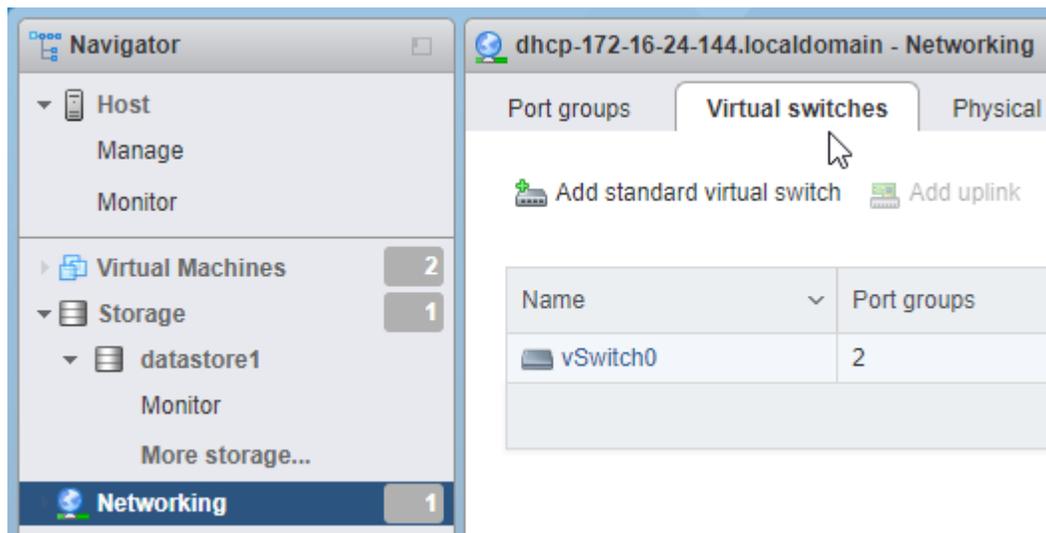
配置网络

Acronis Cyber Infrastructure 通常要求两个网络：公用网络用于外部连接，专用网络用于虚拟机之间的数据交换。尽管已设置了公用网络，仍建议创建专门的专用网络，即使它已存在。若要创建专用网络，需要具有自定义安全参数和端口组的虚拟交换机。

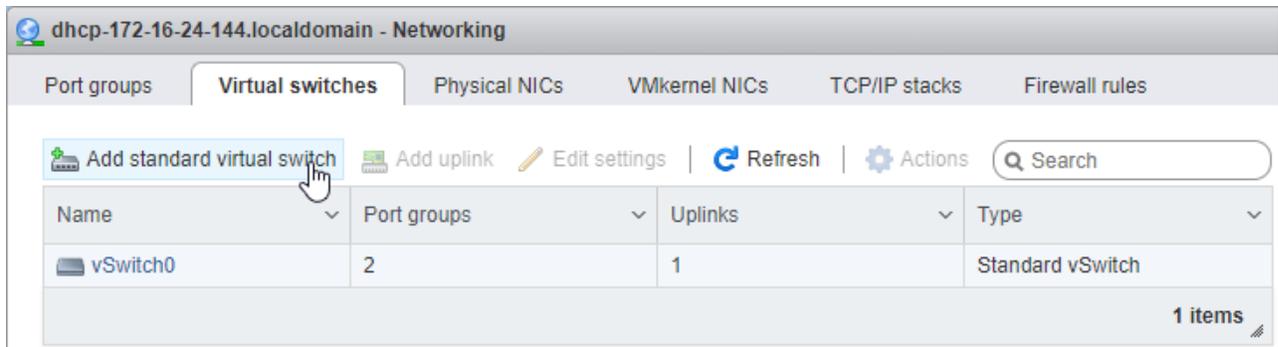
注解：完整网络要求在 Planning Network 中进行了描述。

若要创建虚拟交换机，请遵循以下步骤：

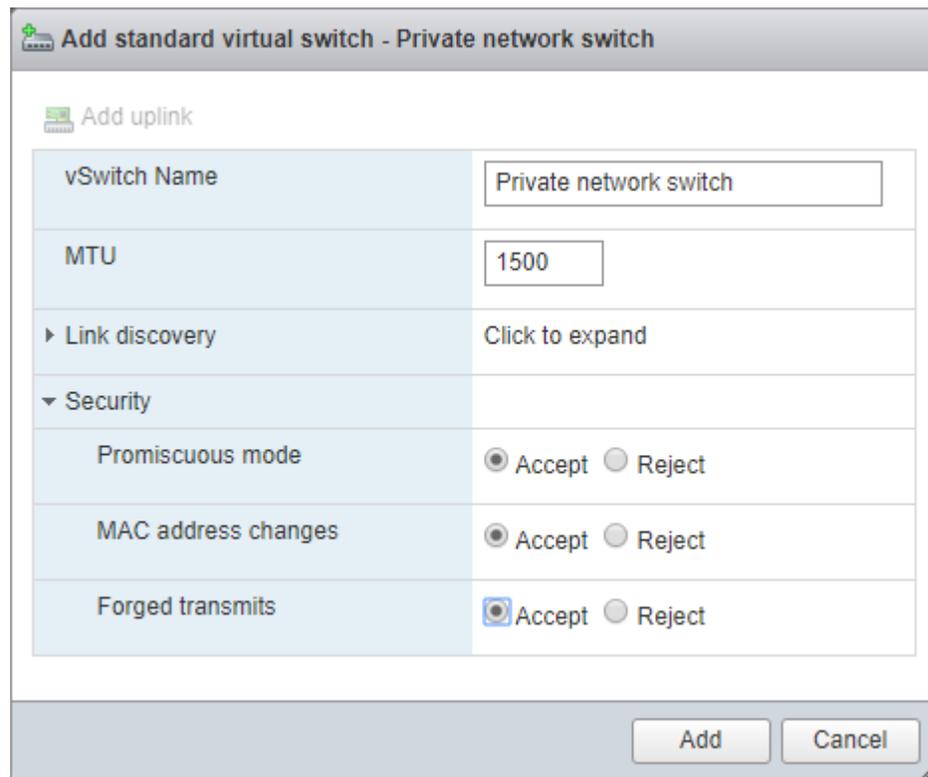
1. 在主机客户端中，单击左侧菜单中的**网络**。打开**虚拟交换机**选项卡。



2. 单击工具栏上的**添加标准虚拟交换机**。

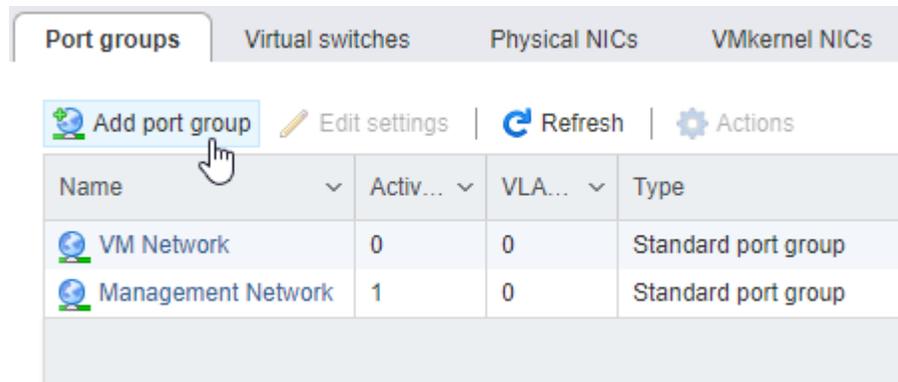


3. 输入交换机名称并展开安全性。对于混杂模式、MAC 地址更改和伪传输，选择接受。

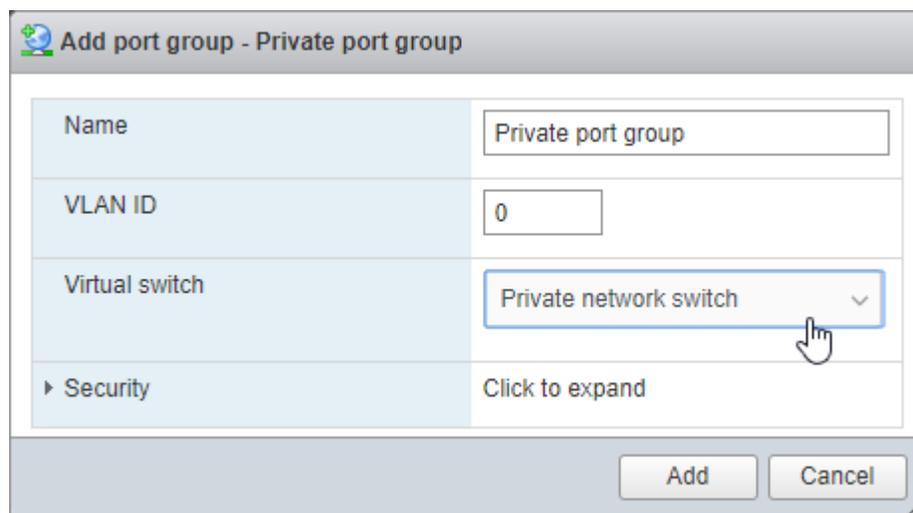


若要创建端口组，请遵循以下步骤：

1. 打开端口组选项卡并单击工具栏上的添加端口组。



2. 输入端口组名称。选择之前创建的虚拟交换机。



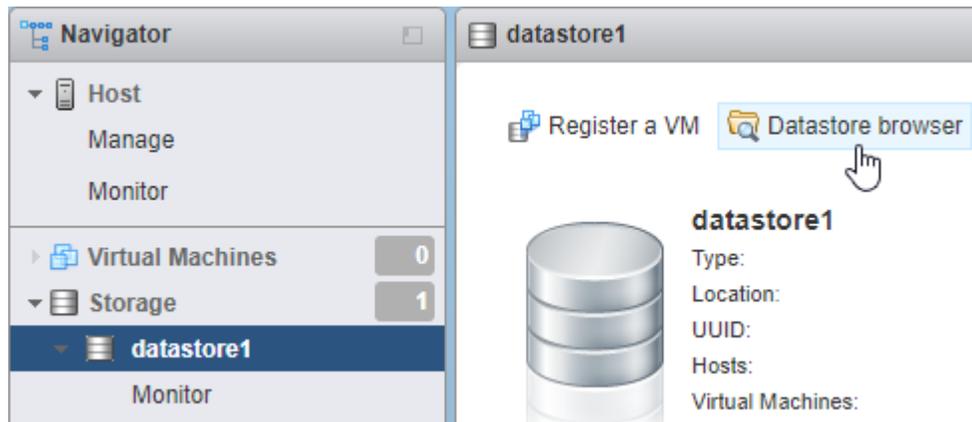
CHAPTER 3

创建虚拟机

首先，获取 Acronis Cyber Infrastructure 映像（2 个 VMDK 文件）。要这样做，请访问产品页面并提交请求。

接下来，将这 2 个 VMDK 文件上传到 VMware vSphere 数据存储：

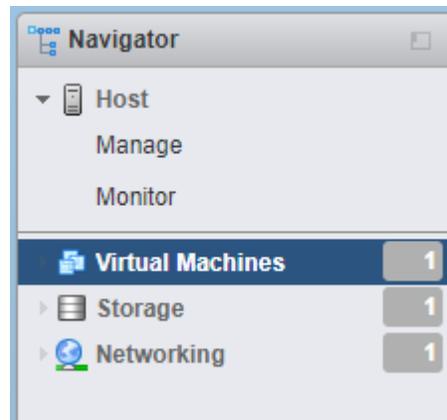
1. 在**导航器**面板中，单击所需的数据存储。单击工具栏上的**数据存储浏览器**。
2. 在**数据存储浏览器**窗口中，创建一个以虚拟机命名的目录。



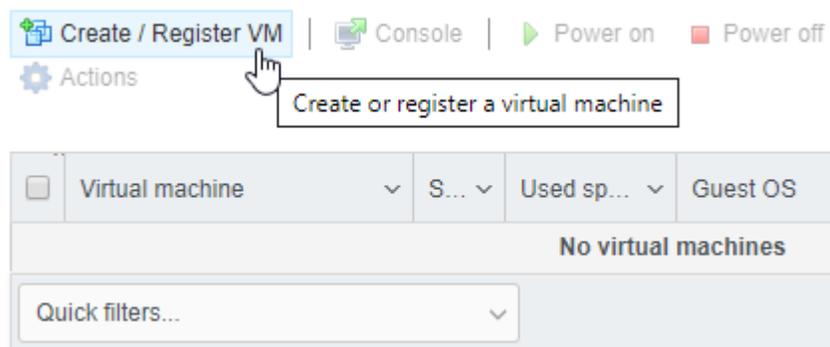
3. 将 Acronis Cyber Infrastructure 映像（两个 VMDK 文件）上传到此目录。

遵循以下步骤来为 Acronis Cyber Infrastructure 创建虚拟机：

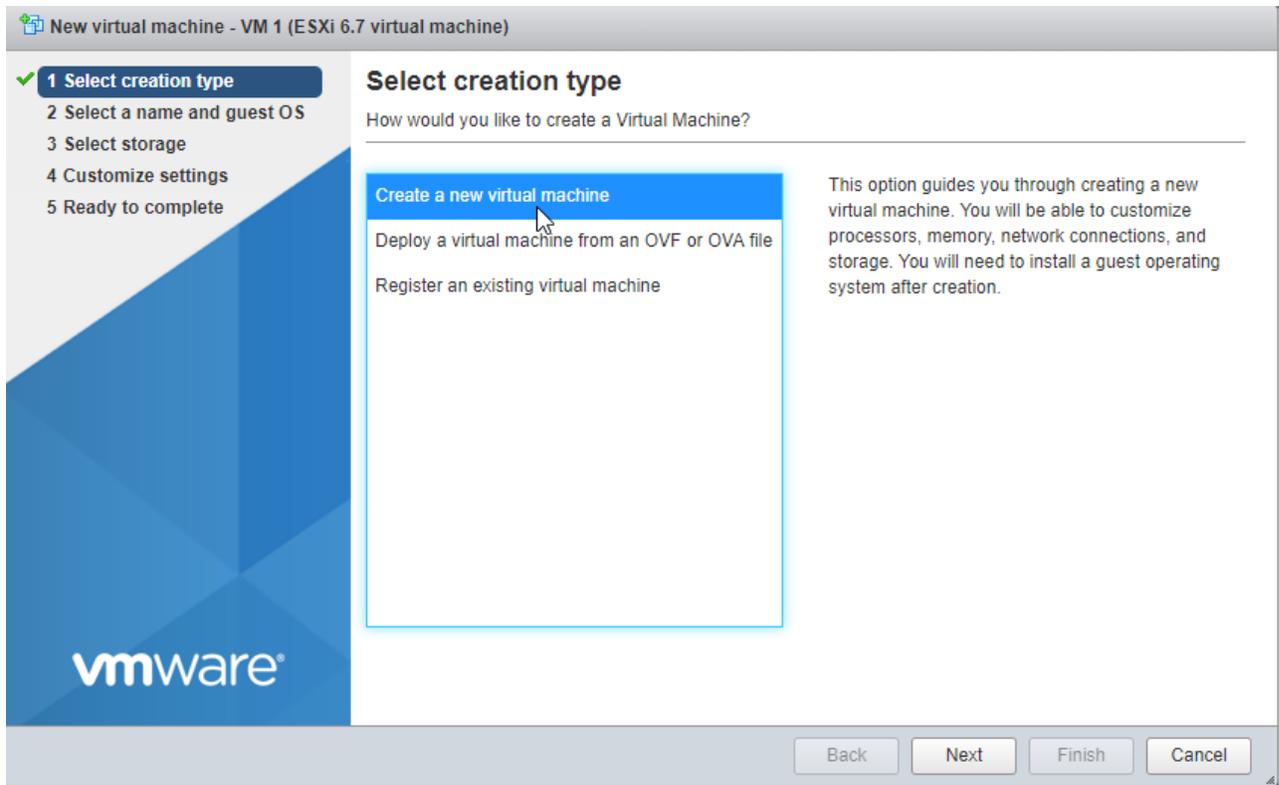
1. 在主机客户端中，单击左侧菜单中的**虚拟机**。



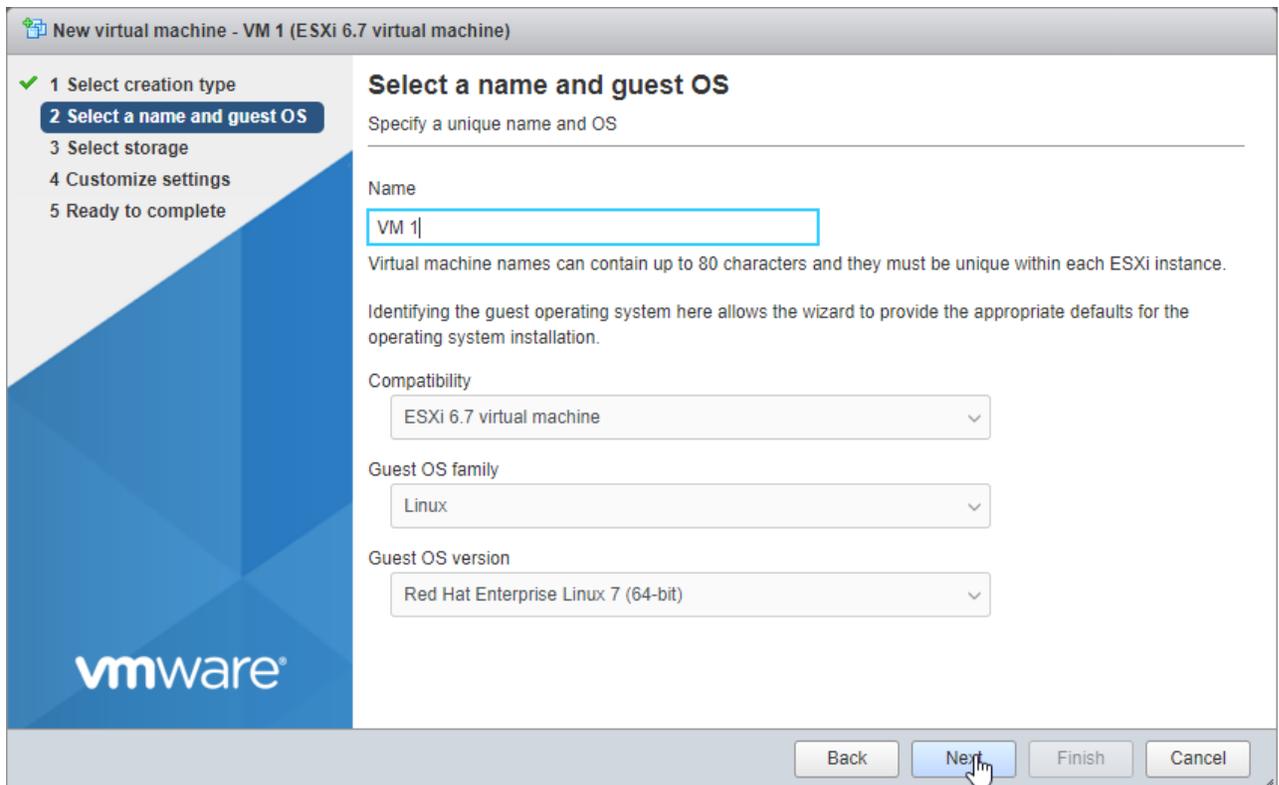
2. 单击工具栏上的**创建/注册 VM**。



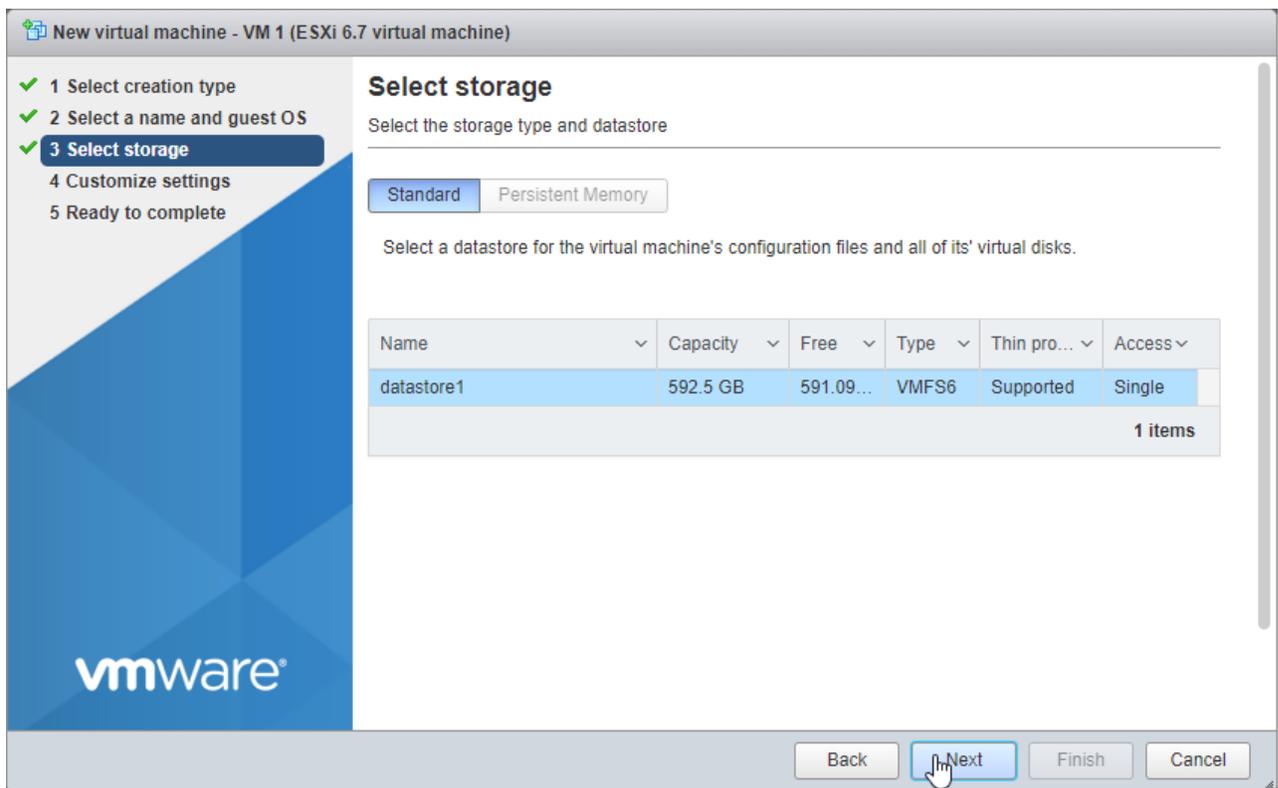
3. 在**新建虚拟机**向导中，在第 1 步中选择**创建新虚拟机**。单击下一步。



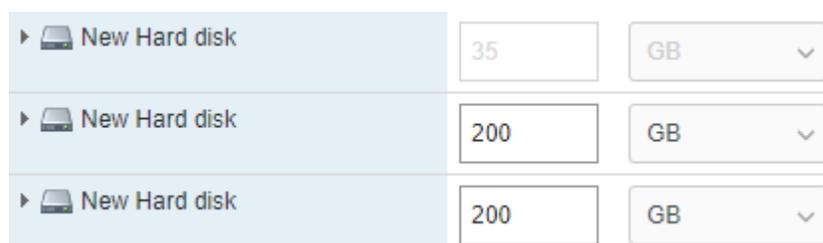
4. 在第 2 步中，输入虚拟机的名称并选择来宾操作系统。单击下一步。



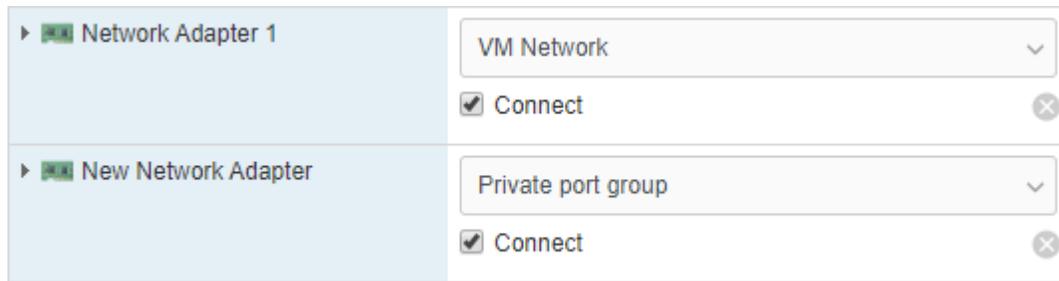
5. 在步骤 3 中，选择存储类型和数据存储。确保数据存储有足够的可用空间。



6. 在步骤 4 中，删除现有硬盘，并单击工具栏中的**添加硬盘**。选择**现有硬盘**并浏览到之前上传到数据存储的映像。单击**选择**。
7. 再次单击工具栏上的**添加硬盘**。选择**新标准硬盘**。将其大小设置为 200 GB。重复此步骤再添加一个 200 GB 的硬盘。总之，您应有三个硬盘：35 GB、200 GB 和 200 GB。



8. 在**自定义设置**窗口中，单击工具栏中的**添加网络适配器**。确保一个适配器连接到公用网络，而另一个连接到已创建的专用端口组。



9. 在步骤 5 中，检查配置并单击**完成**。

10. 在**导航器**菜单中选择虚拟机并启动它。

根据所需的方案重复这些步骤，以创建所需数量的虚拟机（请参阅[要求 \(page 1\)](#)）。

CHAPTER 4

在虚拟机中部署 Acronis Cyber Infrastructure

当虚拟机启动后，执行以下操作：

1. 以存储用户身份使用默认密码（即 password）登录。系统将提示您立即更改密码。例如：

```
You are required to change your password immediately (root enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user storage-user.
Changing password for storage-user.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

在（当前）UNIX 密码中，键入 password；在新密码和再次键入新密码中，键入新密码。将为存储用户和根用户同时更改该密码。

2. 再次以存储用户身份使用新密码登录，然后切换到根用户：

```
$ sudo su
```

3. 配置并启用 eth1 网络接口：

```
# cat > /etc/sysconfig/network-scripts/ifcfg-eth1 << EOF
ARPCHECK="no"
BOOTPROTO="static"
IPADDR=192.168.1.<node>
NETMASK=255.255.255.0
DEVICE="eth1"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
NAME="eth1"
```

```
ONBOOT="yes"
EOF
# ifup eth1
```

其中 <node> 是节点编号：2 用于管理节点，3 用于第一个次要节点等等。

4. 检查是否已指派 IP 地址，以及接口是否加大，例如 `ip -4 a show eth1`。

进一步的配置将根据节点角色的不同而不同。您将需要部署单个管理节点，还可能想要部署两个或四个次要节点。

4.1 部署管理节点

1. 要注册管理节点并初始化其管理面板，请作为根用户运行：

```
# echo '<passwd>' | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh \
-i <int_net> -x <ext_net>
# systemctl start vstorage-ui-backend
# systemctl start vstorage-ui-agent
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_IP>
```

其中 <passwd> 是所需的管理员密码；<int_net> 是内部（专用）网络接口；<ext_net> 是外部（公共）网络接口；<mn_IP> 是管理节点 IP 地址。

2. 重新启动虚拟机。管理面板 IP 地址将显示在终端的欢迎提示中。现在您可以在端口 8888 上登录到管理面板。使用 `admin` 用户名和在以前的步骤中提供的管理节点的根密码。

在管理面板中，您将在**基础架构 > 节点**屏幕上的**取消指派**列表中看到已部署的节点。

3. 在**基础架构 > 网络**屏幕上，单击**编辑**。使**计算 API** 流量类型可用于公用网络，并单击**保存**。

现在需要创建存储簇。请执行以下操作：

1. 打开**基础架构 > 节点**屏幕，并单击**取消指派**列表中的节点。
2. 在节点概述屏幕上，单击**创建簇**。
3. 在**簇**字段中，键入簇的名称。该名称可能仅包含拉丁字母（a-z、A-Z）、数字（0-9）、下划线（“_”）和连字符（“-”）。

✕ New cluster

Create cluster on node **node001**

Cluster

Storage interface

 ▼ 

 Encryption 

4. 单击**新建簇**。

存储簇已准备就绪。现在，可以继续部署次要节点（如果您的方案需要）。如果您仅需要单个节点用于 Backup Gateway，则继续通过 *Backup Gateway* 将 *Acronis Backup* 软件连接到存储后端 (page 17)。

4.2 部署次要节点

要在虚拟机中部署次要节点，请执行以下操作：

1. 从管理面板获取管理节点 IP 地址和标记。打开**基础架构 > 节点**。单击**添加节点**以调用具有管理节点 IP 地址和标记的屏幕。
2. 打开虚拟机终端并通过管理面板注册次要节点，如下所示：

```
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_addr> -t <token>
```

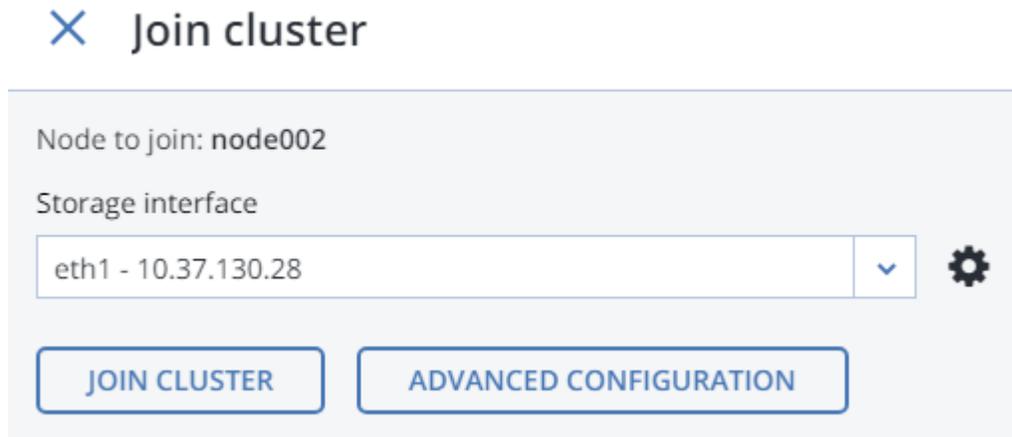
其中 <mn_addr> 是管理节点 IP 地址；<token> 是在管理面板中获取的标记。

在管理面板中，新注册的次要节点将显示在**基础架构 > 节点**屏幕中的**取消指派**列表中。

3. 将次要节点添加到存储簇：
 - 3.1. 在**基础架构 > 节点**屏幕上，单击取消指派的节点。

- 3.2. 在节点概述屏幕上，单击**加入簇**。
- 3.3. 确保连接到具有流量类型**存储**的网络的网络接口已在**存储接口**下拉列表中选中。

如果未配置节点网络接口，则单击齿轮图标，并将具有流量类型**存储**的网络指派给节点的网络接口。



- 3.4. 单击**加入簇**以使 Acronis Cyber Infrastructure 自动将角色指派给磁盘并将节点添加到当前簇。或者，单击**高级配置**将角色手动指派给每个驱动器。

为每个次要节点重复这些步骤。它们全部在存储簇中后，可以在**设置 > 管理节点 > 管理高可用性**屏幕上为管理节点启用高可用性。

现在，可以继续为所需的方案设置 Acronis Cyber Infrastructure。执行各种配置任务的说明在 Administrator's Guide 中提供。

CHAPTER 5

将空间添加至 Acronis Cyber Infrastructure

在创建新磁盘之前，请考虑进行大小调整的以下建议：

1. 如果有一个由多个节点组成的簇，则出于冗余原因，这些节点的大小应相同。然后，数据将在它们之间更均匀地分布。有关详细信息，请参阅 [Understanding Allocatable Disk Space](#)。
2. 具有相同大小的磁盘有助于更均匀地分配负载。在簇内部，磁盘使用情况与磁盘大小成正比。例如，如果有一个 10 TB 的磁盘和 2 TB 的磁盘，则 50% 的簇负载将分别使用 5 TB 和 1 TB。

如果要增加存储簇中的物理空间，可以将新的虚拟磁盘添加至节点。请勿在 Acronis Cyber Infrastructure 虚拟机上使用 VMware vSphere 的 **扩展磁盘** 选项，因为文件系统的大小将不会相应进行调整。因此，请创建一个新的虚拟磁盘并将其添加至虚拟机，如下所述。

按照 [将新硬盘添加至虚拟机](#) 中所述，将一个新的虚拟磁盘添加至虚拟机。之后，它将在 Acronis Cyber Infrastructure 的管理面板中节点的磁盘中列出。

在管理面板中，请按照以下步骤配置新的磁盘：

1. 在 **基础架构 > 节点** 屏幕中，单击具有已创建磁盘的节点。单击 **磁盘 >** 部分，以查看所有节点磁盘。
2. 具有 **已取消指派** 角色的磁盘是您先前创建的磁盘。选择它，然后单击右侧的 **指派**。
3. 在 **选择角色** 屏幕上，选择 **存储** 角色、某个级，然后根据需要启用校验和。有关详细信息，请参阅 [Assigning Disk Roles Manually](#)。

✕ Choose role

<input checked="" type="radio"/> Storage	Caching and checksumming
<input type="radio"/> Metadata	<input type="text" value="Enable checksumming"/> ▼
<input type="radio"/> Cache	Tier
<input type="radio"/> Metadata+Cache	<input type="text" value="Tier 0"/> ▼
<input type="radio"/> Unassigned	

CHAPTER 6

通过 Backup Gateway 将 Acronis Backup 软件连接到存储后端

Backup Gateway 存储访问点（也称为“网关”）旨在用于以下服务提供商：使用 Acronis Backup Cloud 和/或 Acronis Backup Advanced，并希望组织本地存储用于其客户端的备份数据。

Backup Gateway 使服务提供商能够轻松配置存储用于由 Acronis 使用的专有重复数据删除友好的数据格式。

Backup Gateway 支持以下存储后端：

- 借助擦除编码的具有软件冗余的存储簇
- NFS 共享
- 公共云，包括大量 S3 解决方案以及 Microsoft Azure、OpenStack Swift 和 Google Cloud Platform

尽管您的选择应取决于方案和需求，但建议在本地存储簇中保留 Acronis 备份数据。在此情况下，由于 WAN 优化和数据本地性，可以获得最佳性能。在 NFS 共享或公共云中保留备份意味着不可避免的数据传输和其他间接开支，这会降低整体性能。

注意以下内容：

- 在配置 Backup Gateway 时，需要在 Acronis 备份软件中提供管理员帐户的凭据。
- 如果 Backup Gateway 使用了不是本地而是外部存储（例如 NFS），则该外部存储必须提供冗余。Backup Gateway 不提供数据冗余或自行执行重复数据删除。
- 为了能够在 Acronis Backup Cloud 中注册 Backup Gateway，应为您的合作伙伴帐户禁用双重身份验证 (2FA)。

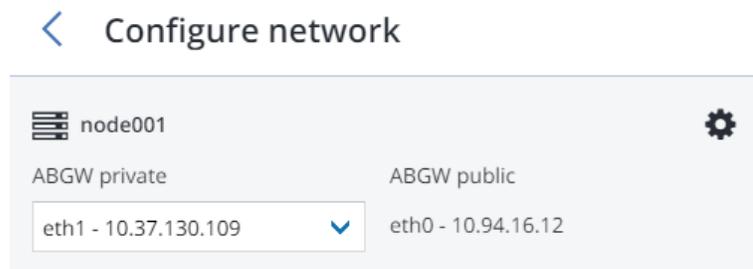
6.1 通过 Backup Gateway 连接到本地存储簇

在继续操作之前，确保目标存储有足够的空间用于现有和新的备份。

要设置 Backup Gateway，请执行以下操作：

1. 在**基础架构 > 网络**屏幕上，确保将 **ABGW 专用** 和 **ABGW 公用** 流量类型添加至要使用的网络。
2. 在剩余菜单中，单击**存储服务 > 备份存储**。
3. 选择要在其上运行网关服务的节点，并单击右侧菜单中的**创建网关**。
4. 选择此 **Acronis Cyber Infrastructure** 簇作为存储类型。
5. 确保在下拉列表中选择了正确的网络接口。单击**下一步**。

如果需要，请单击齿轮图标，并在**网络配置**屏幕上配置节点的网络接口。



6. 在**卷参数**选项卡上，选择所需的层、故障域和数据冗余模式。有关详细信息，请参阅 [Understanding Storage Tiers](#)、[Understanding Failure Domains](#) 和 [Understanding Data Redundancy](#)。

< Volume parameters

Tier:

Tier 0

Data redundancy: Erasure coding

Failure domain: Host

Encoding 1+0	0% overhead
Encoding 1+1	100% overhead
Encoding 1+2	200% overhead

BACK NEXT

按复制的冗余对于 Backup Gateway 不受支持。对于擦除编码，更改冗余方案已遭禁用，因为这可能会降低簇性能。原因是重新编码会长时间占用大量簇资源。如果仍要更改冗余方案，请联系技术支持。

单击下一步。

- 在 **DNS 配置** 选项卡中，指定此网关的外部 DNS 名称，例如 `backupgateway.example.com`。确保运行网关服务的每个节点都有一个开放端口，用于外出的 Internet 连接和从 Acronis 备份软件进来的连接。备份代理将使用此地址和端口来上传备份数据。

重要： 根据在管理面板中建议的示例配置 DNS 服务器。

重要： 每次在 Backup Gateway 簇中更改节点时，请相应地调整 DNS 设置。

< DNS configuration

DNS name

backup.example.com

This may require changing the DNS server configuration, which may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backup.example.com. (
2018120313 ;serial
1h ;refresh
30m ;retry
7d ;expiration
1h ) ;minimum
```

BACK NEXT

单击下一步。

8. 在在备份软件中注册窗格中，为 Acronis 产品指定以下信息：

重要： 确保为您的合作伙伴帐户禁用了双重身份验证 (2FA)。还可以按照 [Acronis Cyber Cloud](#) 文档中所述，为已启用 2FA 的租户内的特定用户禁用它，并指定用户凭据。

- 在**地址**中，指定 Acronis Backup Cloud 管理门户的地址（例如，<https://cloud.acronis.com/>）或主机名/IP 地址以及 Acronis Backup Advanced 管理服务器的端口（例如，<http://192.168.1.2:9877>）。
- 在**帐户**中，指定云中合作伙伴帐户或本地管理服务器上组织管理员的凭据。

9. 最后，单击**完成**。

6.2 通过 Backup Gateway 连接到外部 NFS 共享

注意以下限制：

- Acronis Cyber Infrastructure 在 NFS 卷的顶层不提供数据冗余。根据实施情况，NFS 共享可能使用自己的硬件和软件冗余。

- 在 Acronis Cyber Infrastructure 的当前版本中，仅有一个簇节点可能在 NFS 卷上存储备份。

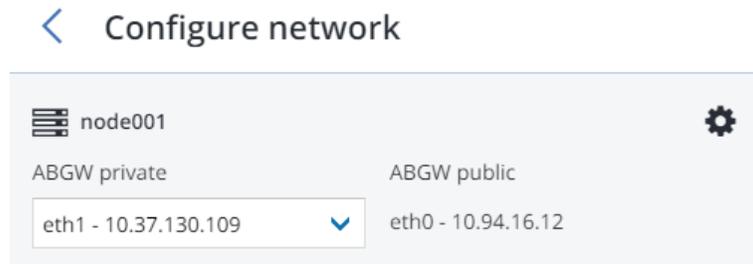
在继续操作之前，确保：

1. NFS 共享有足够的空间用于备份。
2. 每个 NFS 导出仅由一个网关使用。尤其是，不要配置两个 Acronis Cyber Infrastructure 安装以将相同的 NFS 导出用于备份存储。

要设置 Backup Gateway，请执行以下操作：

1. 在**基础架构 > 网络**屏幕上，确保将 **ABGW 专用**和 **ABGW 公用**流量类型添加至要使用的网络。
2. 在剩余菜单中，单击**存储服务 > 备份存储**。
3. 选择要在其上运行网关服务的节点，并单击右侧菜单中的**创建网关**。
4. 选择**网络文件系统**作为存储类型。
5. 确保在下拉列表中选择了正确的网络接口。单击**下一步**。

如果需要，请单击齿轮图标，并在**网络配置**屏幕上配置节点的网络接口。



6. 在**卷参数**选项卡上，指定 NFS 共享的主机名或 IP 地址以及导出名称。单击**下一步**。

< Volume parameters

NFS hostname or IP

Export name

NFS3 (no clustering)

NFS4

BACK NEXT

7. 在 **DNS 配置** 选项卡中，指定此网关的外部 DNS 名称，例如 `backupgateway.example.com`。确保运行网关服务的每个节点都有一个开放端口，用于外出的 Internet 连接和从 Acronis 备份软件进来的连接。备份代理将使用此地址和端口来上传备份数据。

重要： 根据在管理面板中建议的示例配置 DNS 服务器。

重要： 每次在 Backup Gateway 簇中更改节点时，请相应地调整 DNS 设置。

< DNS configuration

DNS name

backup.example.com

This may require changing the DNS server configuration, which may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backup.example.com. (
2018120313 ;serial
1h ;refresh
30m ;retry
7d ;expiration
1h ) ;minimum
```

BACK NEXT

单击下一步。

8. 在**在备份软件中注册**窗格中，为 Acronis 产品指定以下信息：

重要： 确保为您的合作伙伴帐户禁用了双重身份验证 (2FA)。还可以按照 [Acronis Cyber Cloud 文档](#) 中所述，为已启用 2FA 的租户内的特定用户禁用它，并指定用户凭据。

- 在**地址**中，指定 Acronis Backup Cloud 管理门户的地址（例如，<https://cloud.acronis.com/>）或主机名/IP 地址以及 Acronis Backup Advanced 管理服务器的端口（例如，<http://192.168.1.2:9877>）。
- 在**帐户**中，指定云中合作伙伴帐户或本地管理服务器上组织管理员的凭据。

9. 最后，单击**完成**。

6.3 通过 Backup Gateway 连接到公共云存储

借助 Backup Gateway，可以让 Acronis Backup Cloud 或 Acronis Backup Advanced 在多个公共云和本地对象存储解决方案中存储备份：

- Amazon S3

- IBM Cloud
- Alibaba Cloud
- Iij
- Cleversafe
- Cloudian
- Microsoft Azure
- Swift 对象存储
- 软层 (Swift)
- Google Cloud Platform
- Wasabi
- 使用 S3 的其他解决方案

但是，相较于本地存储簇，在公共云中存储备份数据将增加对备份的所有 I/O 请求的延迟并降低性能。出于此原因，建议使用本地存储簇作为存储后端。

备份是具有特定访问模式的冷数据：该数据不常访问，但预计在被访问时立即可用。对于此使用案例，经济高效的方式是选择拟用于长期存储不常访问数据的存储类。建议的存储类别包括：

- **不常访问**适用于 Amazon S3
- **Cool Blob Storage** 适用于 Microsoft Azure
- **Nearline** 和 **Coldline** 存储适用于 Google Cloud Platform

诸如 Amazon S3 Glacier、Azure Archive Blob 或 Google Archive 之类的存档存储类不能用于备份，因为它们不提供对数据的即时访问。高访问延迟（数小时）使技术上无法浏览存档、快速恢复数据以及创建增量备份。尽管存档存储通常非常经济高效，但请记住，存在诸多不同的成本因素。实际上，公共云存储的总成本包括用于存储数据、操作、流量、数据检索、早期删除等的费用。例如，存档存储服务可能会针对仅一个数据召回操作就收取六个月的存储费用。如果预计将更频繁地访问存储数据，则增加的成本会显著提高数据存储的总成本。为了避免低数据检索率并减少开支，建议您将 Acronis Cyber Cloud 用于存储备份数据。

6.3.1 重要要求和限制

1. 当使用公共云时，Backup Gateway 会使用本地存储作为分层区域以及保留服务信息。这表示要上传到公共云的数据将首先本地存储，仅在此之后发送到目标。出于此原因，本地存储持续且冗余很重要，以便数据不会丢失。有多种方法可以确保本地存储的持续和冗余。可以在多个簇节点上部署 Backup Gateway，并选择较好的冗余模式。如果在单个物理节点上通过网关部署 Acronis Cyber Infrastructure，可以通过在不同本地磁盘间复制它来使本地存储冗余。如果在虚拟机上通过网关部署 Acronis Cyber Infrastructure，则通过它在其上运行的虚拟化解决方案确保使其冗余。
2. 确保本地存储簇有足够的逻辑空间用于分层存储。例如，如果执行每日备份，请为至少 1.5 天的备份提供足够的空间。如果每日备份总计为 2TB，则提供至少 3TB 的逻辑空间。所需的原始存储将根据编码模式的不同而不同：在 1+2 模式下为 9TB（每个节点 3TB），在 3+2 模式下为 5TB（每个节点 1TB），等等。
3. 如果要在 Amazon S3 云中存储备份，请记住由于 Amazon S3 的最终一致性，Backup Gateway 有时可能阻止对此类备份的访问。这表示 Amazon S3 可能偶尔返回旧的数据，因为它需要时间来渲染可访问数据的最新版本。Backup Gateway 可检测此类延迟，并通过在云更新之前阻止访问来保护备份完整性。
4. 为每个 Backup Gateway 簇使用一个单独的对象容器。

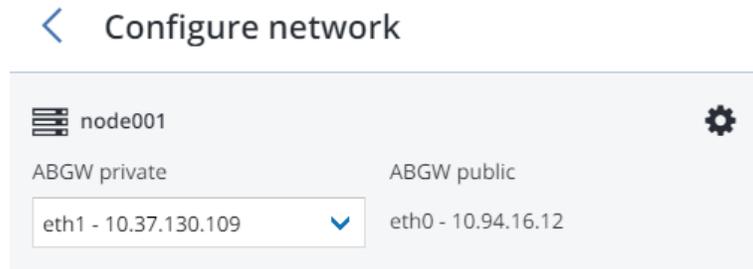
6.3.2 设置 Backup Gateway

在继续操作之前，确保目标存储有足够的空间用于备份。

要设置 Backup Gateway，请执行以下操作：

1. 在**基础架构 > 网络**屏幕上，确保将 **ABGW 专用**和 **ABGW 公用**流量类型添加至要使用的网络。
2. 在**剩余菜单**中，单击**存储服务 > 备份存储**。
3. 选择要在其上运行网关服务的节点，并单击右侧菜单中的**创建网关**。
4. 选择**公共云**作为存储类型。
5. 确保在下拉列表中选择了正确的网络接口。单击**下一步**。

如果需要，请单击齿轮图标，并在**网络配置**屏幕上配置节点的网络接口。



6. 在公共云参数窗格中，执行以下操作：

- 6.1. 选择一个公共云提供商。如果您的提供商兼容 S3 但不在列表中，请尝试兼容 **AuthV2 (S3)** 或兼容 **AuthV4 (S3)**。
- 6.2. 根据提供商，指定区域、身份验证 (关键) URL 或端点 URL。
- 6.3. 在使用 Swift 对象存储时，指定其要求的身份验证协议版本和属性。
- 6.4. 指定用户凭据。在使用 Google Cloud 时，选择具有密钥的 JSON 文件进行上传。
- 6.5. 指定要存储备份的文件夹（存储桶、容器）。该文件夹必须是可写的。

为每个 Backup Gateway 簇使用一个单独的对象容器。

单击下一步。

7. 在在备份软件中注册窗格中，为 Acronis 产品指定以下信息：

重要： 确保为您的合作伙伴帐户禁用了双重身份验证 (2FA)。还可以按照 Acronis Cyber Cloud 文档中所述，为已启用 2FA 的租户内的特定用户禁用它，并指定用户凭据。

- 在地址中，指定 Acronis Backup Cloud 管理门户的地址（例如，<https://cloud.acronis.com/>）或主机名/IP 地址以及 Acronis Backup Advanced 管理服务器的端口（例如，<http://192.168.1.2:9877>）。
- 在帐户中，指定云中合作伙伴帐户或本地管理服务器上组织管理员的凭据。

8. 最后，单击完成。