

# Acronis

## Acronis Cyber Infrastructure 3.5

### 评估指南

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

<b>1. 简介</b>	<b>1</b>
<b>2. 规划基础架构</b>	<b>2</b>
2.1 硬件要求	2
2.2 了解存储策略	3
<b>3. 管理存储簇</b>	<b>6</b>
3.1 安装 Acronis Cyber Infrastructure	6
3.2 配置网络	7
3.3 创建存储簇	8
<b>4. 管理计算簇</b>	<b>10</b>
4.1 创建计算簇	10
4.2 分配资源	12
4.2.1 创建域、项目和用户	12
4.2.2 创建存储策略	13
4.2.3 创建计算网络	14
4.3 创建虚拟机	14
<b>5. 导出存储空间</b>	<b>16</b>
5.1 通过 iSCSI 导出存储空间	16
5.1.1 创建目标组	17
5.1.2 创建卷	17
5.1.3 将卷附加至目标组	17
5.1.4 从 VMware vSphere 访问 iSCSI 目标	17
5.2 通过 S3 导出存储空间	18
5.2.1 创建 S3 簇	19
5.2.2 管理 S3 用户和存储桶	19

5.3	通过 NFS 导出存储空间 . . . . .	20
5.3.1	创建 NFS 簇 . . . . .	21
5.3.2	创建 NFS 共享 . . . . .	21
5.3.3	创建和加载 NFS 导出 . . . . .	21
<b>6.</b>	<b>通过 Backup Gateway 将 Acronis Cyber Backup Cloud 软件连接到存储后端 . . . . .</b>	<b>23</b>
6.1	配置备份网关 . . . . .	24
6.2	配置 Acronis Cyber Backup Cloud . . . . .	25
<b>7.</b>	<b>监视存储簇 . . . . .</b>	<b>26</b>
<b>8.</b>	<b>启用高可用性 . . . . .</b>	<b>27</b>
8.1	管理节点的高可用性 . . . . .	27
8.2	服务的高可用性 . . . . .	28
8.3	测试高可用性 . . . . .	28

## CHAPTER 1

# 简介

Acronis Cyber Infrastructure 代表面向服务提供商和最终客户的新一代超融合基础架构。它是一种横向扩展、经济高效的多用途网络安全保护解决方案，结合了通用存储和高性能虚拟化功能。

Acronis Cyber Infrastructure 与 Acronis Cyber Cloud 产品套件、Acronis Cyber Backup 无缝协作。它最大程度地减少了数据中心所需的技术数量，并提供了其他性能改进。

本指南有助于您开始使用 Acronis Cyber Infrastructure，并概述了评估其主要功能的以下步骤：

1. 安装和配置 Acronis Cyber Infrastructure。
2. 创建存储簇。
3. 创建计算簇并分配其资源。
4. 创建虚拟机。
5. 通过 iSCSI、S3、NFS、Backup Gateway 导出存储空间。
6. 浏览内置监控工具。
7. 启用并测试高可用性。

可能有许多不同的方案，但在本指南中，我们将引导您完成最常见的方案。出于评估目的，本指南中概述的过程都是典型的简化过程。但是，Acronis Cyber Infrastructure 受完整的详细文档套件支持，您应参阅该文档套件以获取进一步帮助。有关详细信息，请参阅快速入门指南、安装指南、管理员指南、自助服务指南和存储用户指南。

## CHAPTER 2

# 规划基础架构

## 2.1 硬件要求

有许多受支持的硬件配置在 [Planning Node Hardware Configurations](#) 中进行了描述。但出于评估目的，我们建议部署三个节点。这是为了确保在一个节点发生故障时，簇可以正常工作而不会丢失数据。下表列出了三个节点中每个节点的 \* 最低 \* 硬件要求。为了实现高可用性，需要三个满足具有存储和计算的管理节点要求的节点。

表 2.1.1: 最低节点硬件要求

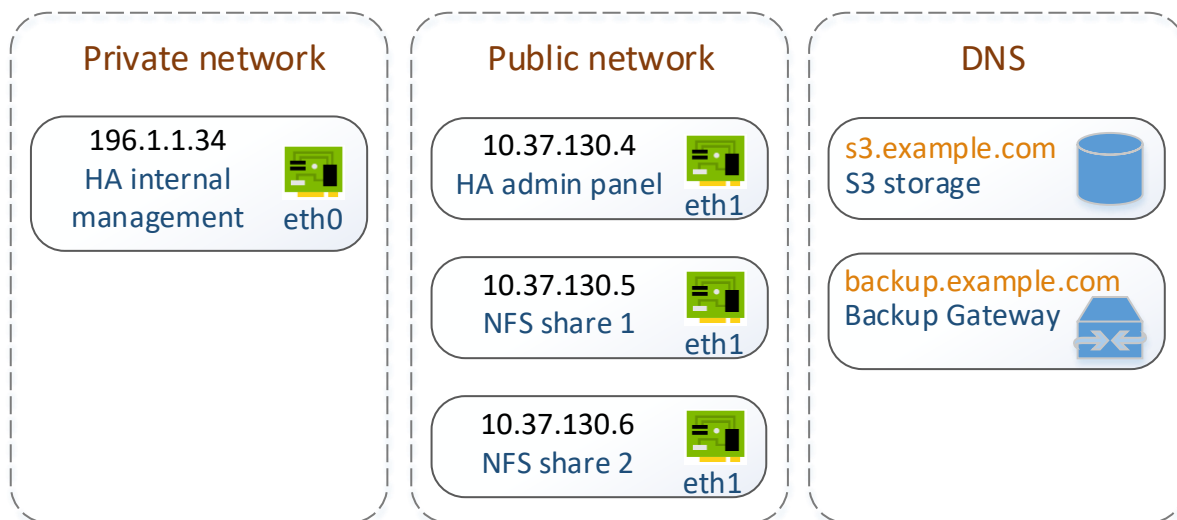
类型	具有存储和计算的管理节点	具有存储和计算的辅助节点	具有存储和 Backup Gateway 的管理节点
CPU	64 位 x86 处理器，已启用 AMD-V 或 Intel VT 硬件虚拟化扩展		
	16 个核心 *	8 个核心 *	4 个核心 *
RAM	32 GB	16 GB	8 GB
存储器	1 个磁盘：系统 + 元数据， 100+ GB SATA HDD 1 个磁盘：存储，SATA HDD， 所需大小	1 个磁盘：系统，100 GB SATA HDD 1 个磁盘：元数据，100 GB SATA HDD（仅在簇中的前三个 节点上） 1 个磁盘：存储，SATA HDD， 所需大小	1 个磁盘：系统 + 元数据， 120 GB SATA HDD 1 个磁盘：存储，SATA HDD，所需大小
网络	1 GbE 用于专用网络，1 GbE (VLAN 标记) 用于公共网络	1 GbE 用于专用网络，1 GbE (VLAN 标记) 用于公共网络	2 x 1 GbE

\* 此处的 CPU 核心是多核处理器中的物理核心（不考虑超线程）。

还需要公共网络中至少两个 IP（用于高可用性管理面板和每个 NFS 共享）、专用网络中一个 IP（用于高可用性管理节点），以及两个 DNS 名称（用于 S3 和 Backup Gateway）。

以下是我们评估方案的网络布局示例。您的主机名和地址可能会因设置而异。

## Reserved addresses

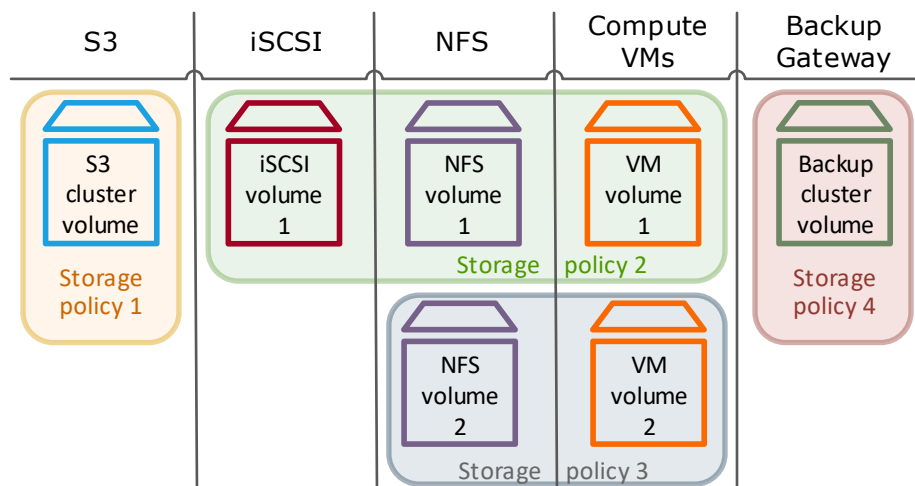


备份代理程序使用 DNS 名称将备份发送到云存储，并从云存储中检索备份。如果客户端计算机和 Acronis Cyber Infrastructure 节点位于不同的数据中心，强烈建议您在其中一个首选 DNS 服务中配置 DNS 名称：Azure DNS for Azure、Amazon Route 53 for Amazon 或 Google Cloud DNS for Google。如果由于某种原因无法实现，必须手动将 DNS 名称添加到每个节点上的 `/etc/hosts` 文件中。另一方面，如果客户端计算机和 Acronis Cyber Infrastructure 节点位于同一数据中心，则可以使用本地 DNS 代替公共 DNS，以加快备份速度。本地 DNS 只能与本地 IP 地址一起使用，因此在这种情况下我们建议使用 NAT。

建议您在我们的评估方案中使用 Google Chrome 浏览器访问 Acronis Cyber Infrastructure 和 S3 存储。

## 2.2 了解存储策略

Acronis Cyber Infrastructure 可用于以下情形：iSCSI 块存储、NFS 文件存储、S3 对象存储、备份存储（用于存储在 Acronis Cyber Backup 解决方案中创建的备份）。还可以使用其内置虚拟机监控程序来创建计算虚拟机 (VM)。在所有这些情形中，数据的通用单位是卷。对于计算服务，卷是可以附加至 VM 的虚拟驱动器。对于 iSCSI、S3、Backup Gateway 和 NFS，卷是用于导出空间的数据单位。在所有这些情况下，当创建一个卷时，需要定义其**冗余模式、级和故障域**。这些参数构成了一个**存储策略**，用于定义卷必须达到的冗余程度以及卷需要放置到的位置。



冗余意味着数据存储在不同的存储节点上，即使某些节点发生故障，数据也保持高可用性。如果存储节点不可访问，则该节点上的数据副本将由在正常运行的存储节点间分发的新数据副本所取代。存储节点在停机时间过后启动后，将更新其上的过时数据。

通过复制，Acronis Cyber Infrastructure 将卷分成固定大小的片段（数据区块）。每个区块根据存储策略中设置的次数进行多次复制。如果故障域是主机，则副本存储在不同的存储节点上，因此每个节点只有给定区块的一个副本。

通过擦除编码（或仅编码），传入数据流拆分为一定大小的多个段。然后，每个段本身都不被复制；取而代之的是，将一定数量 (M) 的此类段组织在一起，并创建一定数量 (N) 的奇偶校验片段以实现冗余。所有片段在 M+N 个存储节点（选择自所有可用节点）上进行分发。数据可在任意 N 个存储节点发生故障时仍就可用，而不会丢失数据。在擦除编码冗余模式的名称中指出 M 和 N 的值。例如，在 5+2 模式下，传入数据拆分为 5 个段，并另外添加 2 个奇偶校验片段（相同大小）以实现冗余。有关冗余、数据开销、节点数和原始空间要求的详细信息，请参阅 Administrator's Guide。

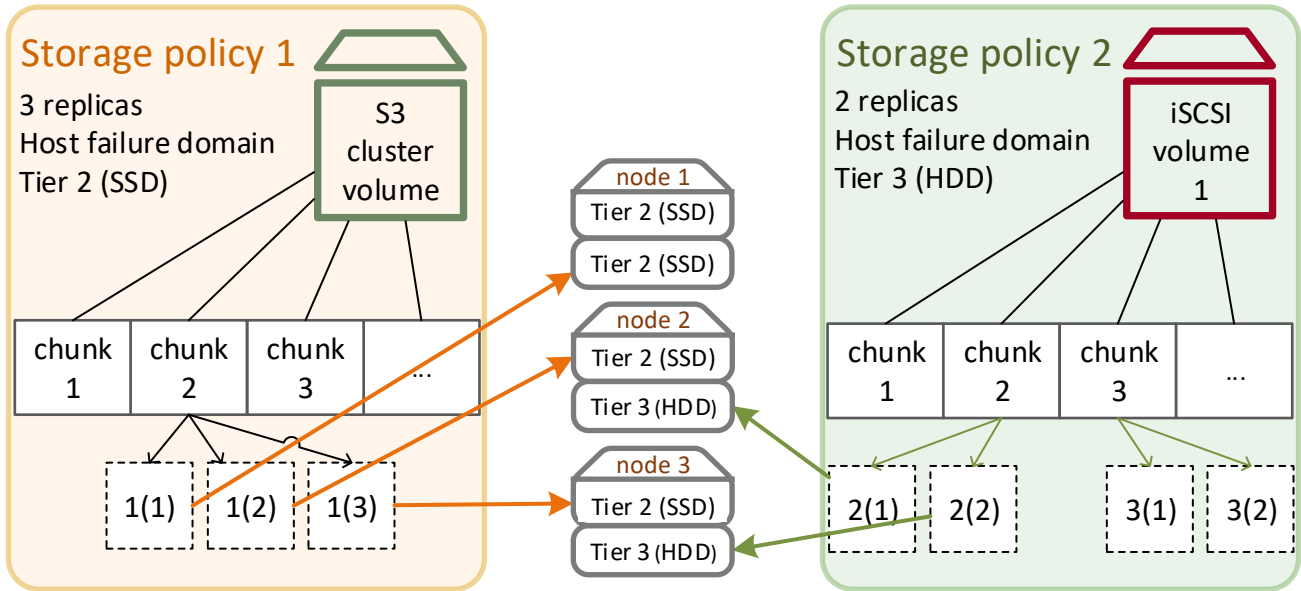
为了更好地了解存储策略，让我们通过示例方案看一下其主要组成部分（级、故障域和冗余）。例如，您有三个带有多个存储节点的节点：快速 SSD 和大容量 HDD。节点 1 仅具有 SSD。节点 2 和 3 同时具有 SSD 和 HDD。您要通过 iSCSI 和 S3 导出存储空间，因此需要为每个工作负载定义合适的存储策略。

- 第一个参数**级**定义了一组磁盘，这些磁盘由针对特定存储工作负载制定的标准（通常是驱动器类型）组合在一起。对于此示例方案，可以将 SSD 驱动器分组为级 2，将 HDD 驱动器分组为级 3。可以在创建存储簇或向其添加节点时将磁盘指派给某个级（请参阅[创建存储簇 \(page 8\)](#)）。请注意，只有节点 2 和 3 具有 HDD，将用于级 3。第一个节点的 SSD 不能用于级 3。
- 第二个参数**故障域**定义一个范围，在该范围内一组存储服务可能会以相关的方式发生故障。默认故障域是主机。每个数据区块都复制到不同的存储节点，每个节点仅有一个副本。如果某个节点发生故障，仍可以从运行状况良好的节点访问数据。磁盘也可以是故障域，尽管它仅与单节点簇有关。由于在本方案中您有三个节点，因此建议您选择主机故障域。



- 第三个参数**冗余**应配置为适合磁盘和级。在我们的评估示例中，您有三个节点：它们都将 SSD 置于级 2 上。因此，如果在存储策略中选择级 2，则可以将三个节点用于 1 个、2 个或 3 个副本。但是，只有两个节点将 HDD 置于级 3 上。因此，如果在存储策略中选择级 3，则只可以在两个节点上存储 1 个或 2 个副本。在这两种情况下，还可以使用编码，但对于我们的评估，让我们继续使用复制：SSD 的 3 个副本和 HDD 的 2 个副本。

综上所述，生成的存储策略为：



## CHAPTER 3

# 管理存储簇

本章概述了安装 Acronis Cyber Infrastructure 并配置其初始设置以进行进一步部署的步骤。首先，需要在管理节点上创建基本的基础架构，然后采用类似方式向其添加辅助节点。建议您添加两个辅助节点以进行评估。然后，配置网络并在节点上创建存储簇。

## 3.1 安装 Acronis Cyber Infrastructure

要获得发行版 ISO 映像，可以访问产品页面并提交请求以获取试用版。

还可以从 Acronis Cyber Cloud 下载 ISO。要执行该操作，请转至管理门户，然后在左侧菜单中依次选择**设置 > 位置**。单击**添加备份存储**，然后在打开的窗口中单击**下载 ISO** 按钮。在已获得发行版映像后，请继续安装 Acronis Cyber Infrastructure。

1. 使用发行版 ISO 映像准备可启动媒体：将该映像加载到 IPMI 虚拟驱动器、创建可启动的 USB 驱动器或设置 PXE 服务器。从选择的媒体启动服务器。
2. 在欢迎屏幕上，选择**安装 Acronis Cyber Infrastructure**。接下来，阅读并接受最终用户许可协议
3. 为 NIC 配置一个静态 IP 地址并提供一个主机名。不建议使用动态 IP，因为它可能会导致访问节点时出现问题。检查网络设置是否正确无误。在此阶段，可以 ping 静态 IP 以检查网络是否正常运行。然后，选择您所在的时区。
4. 指定要安装的节点类型：管理或辅助。
  - 如果要部署第一个节点，请选择一个用于内部管理的专用网络接口（在我们的示例中为 eth0），为管理面板选择一个公共接口（在我们的示例中为 eth1）。该节点将成为管理节点。另外，创建管理面板密码。
  - 如果要部署辅助节点，请提供管理节点的 IP 地址和标记。按照**创建存储簇 (page 8)**中所述，打开管理面板。在**基础架构 > 节点**屏幕上，单击**添加节点**以查看管理节点 IP 地址和标记。

5. 选择用于操作系统的磁盘。然后，输入并确认根帐户的密码并单击**开始安装**。
6. 安装完成后，该节点将自动重新启动。对于管理节点，该节点的欢迎提示将显示管理面板的 IP 地址。在端口 8888 上登录到管理面板。使用” admin” 用户名和先前创建的管理面板密码。对于辅助节点，它将显示在管理面板中的**基础架构 > 节点**屏幕上的**取消指派**列表上。
7. 要获取有关已创建节点的详细信息，请转至**基础架构 > 节点**屏幕，然后单击节点的名称。可以单击**磁盘 >** 以配置或查看节点磁盘，也可以单击**网络 >** 以配置节点的网络接口。

## 3.2 配置网络

现在，已在管理节点和两个辅助节点上安装了 Acronis Cyber Infrastructure，需要设置网络和接口。将单独的网络用于内部和公共流量。这样做将阻止公共流量影响簇 I/O 性能，还会阻止可能来自外部的服务拒绝攻击。

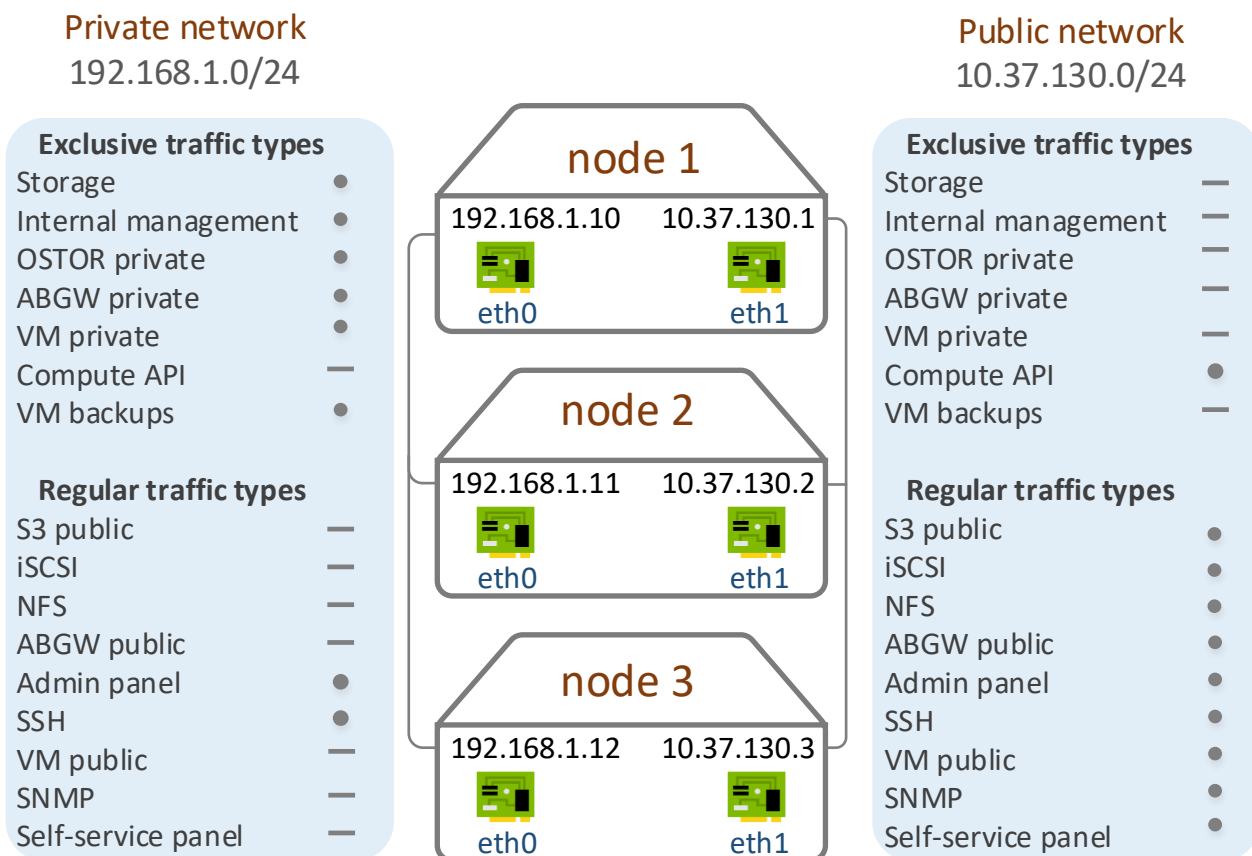
1. 要配置网络，请转至管理面板上的**基础架构 > 网络**屏幕。高级配置在 Managing Networks and Traffic Types 中进行讨论，但对于我们的简化部署而言，它足以用于自定义默认的**公共**和**专用**网络，如下所示：

表 3.2.1: 简化的网络设置

网络	流量类型
公开可见	计算 API、S3 公用、iSCSI、NFS、ABGW 公用、管理面板、SSH、VM 公用、SNMP、自助服务面板
专用	存储、内部管理、OSTOR 专用、ABGW 专用、VM 专用、管理面板、SSH

2. 要配置接口，请转至**基础架构 > 节点**屏幕，然后单击节点的名称。在节点视图上，单击**网络 >**。对于管理节点，两个接口均已设置。然而，仍然需要为每个辅助节点配置公共网络接口。选择一个接口，然后单击右侧菜单上的**指派网络**。选择**公共**。现在，应该将一个接口连接到专用网络，将另一个接口指派给公共网络。对每个辅助节点重复这些步骤，以将它们连接到专用网络和公用网络。
3. 将在群集节点上打开的端口取决于将在相应节点上运行的服务以及与之关联的流量类型。有关端口和服务的详细信息，请参阅 Planning Network。
4. 确保 DNS 设置正确无误。要执行该操作，请转至**设置 > 簇 DNS**屏幕。检查簇 DNS 是否已正确配置，并指向可以解析外部主机名的 DNS。

下图显示了我们将为评估方案构建的示例网络基础结构：



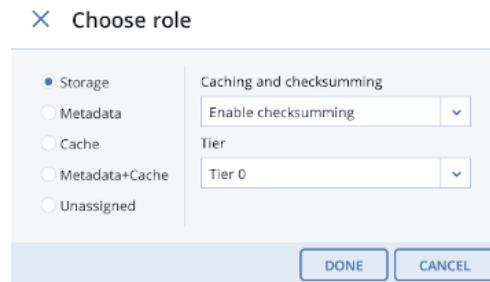
**注解:** 如果只有一个网络，请勿通过两个接口将一个节点连接到该网络。如果是一个网络，请使用该节点的一个公共接口。

## 3.3 创建存储簇

现在，您已经创建了管理节点和辅助节点并配置了网络连接，可以继续创建存储簇。

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**，然后键入一个名称。要添加辅助节点，单击右侧窗格中的**加入簇**。
3. 对于该评估方案，您需要将节点的存储磁盘指派给各个级（请参阅**了解存储策略 (page 3)**）。对于节点 1，将 SSD 指派给级 2。要执行该操作，请单击**高级配置**。系统会将您转至**加入簇**或**新建簇**面板上的节点上的驱动器列表。在列表上选择一个或多个驱动器，然后单击右侧的**配置**。在**选择角色**屏幕上，选择所需的级。使用类似

方法，为节点 2 和 3 将 SSD 指派给级 2，将 HDD 指派给级 3。有关磁盘角色的详细信息，请参阅《管理员指南》中的“创建存储簇”。



× Choose role

Storage

Metadata

Cache

Metadata+Cache

Unassigned

Caching and checksumming

Enable checksumming

Tier

Tier 0

DONE CANCEL

- 单击**新建簇**或**加入簇**。在**配置摘要**屏幕上，检查磁盘设置。单击**继续**。可以在**基础架构 > 节点**屏幕上监控磁盘配置进度。

## CHAPTER 4

# 管理计算簇

Acronis Cyber Infrastructure 提供了高性能虚拟化，其基本组件是计算簇。它允许管理员创建多个租户、虚拟机和软件定义的网络，以及轻松部署容器编排解决方案（如 Kubernetes）。

在本部分里，我们将介绍计算簇的两种常见方案：

- 服务提供商 (SP) 为最终客户提供虚拟化服务。在这种情况下，SP 可以受益于带有白标、多租户以及易于管理和分配资源的自助服务面板。
- 企业计划在其基础架构中采用新软件。它可以部署虚拟机并在其中安装软件，以供所有员工访问和使用。

尽管这两种方案彼此之间存在显著差异，但是 Acronis Cyber Infrastructure 中的过程相似：

1. 创建计算簇。
2. 将资源分配给域、项目（租户）和用户。
3. 为最终用户创建虚拟机。

在本章中，我们将介绍其中的每个步骤。

## 4.1 创建计算簇

要创建计算簇，请打开**计算**屏幕、单击**创建计算簇**，然后在**配置计算簇**窗口中执行以下操作：

1. 在**节点**部分中，选择要添加至计算簇的节点。如果您按照**配置网络** (page 7) 的说明进行操作，则每个选定节点的网络状态应为**已配置**。单击**下一步**。

### Configure compute cluster ✕

- Nodes
- Public network
- Add-on services
- Summary

Select nodes to add to the compute cluster.

<input checked="" type="checkbox"/>	Name ↑	Node status	IP address	Network state
<input checked="" type="checkbox"/>	node001 ⓘ	Healthy	192.168.1.10	<span style="color: green;">✔</span> Configured <span style="float: right;">⚙️</span>
<input checked="" type="checkbox"/>	node002	Healthy	192.168.1.11	<span style="color: green;">✔</span> Configured <span style="float: right;">⚙️</span>
<input checked="" type="checkbox"/>	node003	Healthy	192.168.1.12	<span style="color: green;">✔</span> Configured <span style="float: right;">⚙️</span>

Next

2. 如果您有可以使用的 IP 地址集区，则可以在**公共网络**部分中启用 IP 地址管理。对于虚拟路由器、浮动公共 IP 地址和网络负载均衡器，这也是必需的。否则，可以禁用 IP 地址管理。
3. 如果您还要评估其他服务，则可以在**附加组件服务**部分中安装其他服务。或者，您也可以以后按照 Administrator' s Guide 中所述进行操作。
4. 在**概要**部分中，查看配置，然后单击 **Create cluster**。

### Configure compute cluster ✕

- Nodes
- Public network
- Add-on services
- Summary

Review the compute cluster details and go back to change them if necessary.

Nodes  
node001 (192.168.1.10)  
node002 (192.168.1.11)  
node003 (192.168.1.12)

---

Physical network  
Public

---

Add-on services  
Kubernetes service  
Load balancer service  
Billing metering service








Back
Create cluster

可以在**计算**屏幕上监控计算簇部署。

## 4.2 分配资源

### 4.2.1 创建域、项目和用户

Acronis Cyber Infrastructure 中有三个用户角色：系统管理员、域管理员和项目成员。下表显示了在服务提供商和企业中扮演这些角色的典型用户，以及他们的工作区：管理面板或自助服务面板。

 Role	 Service Provider	 Managed Service Provider	 Enterprise	
 System administrator	Infrastructure administrator of the SP	Infrastructure administrator of the MSP	Infrastructure administrator of the enterprise	<b>Admin panel</b>
 Domain administrator	System admin of the SP's client	System admin of the MSP	System admin of an enterprise subsidiary	<b>Domain (self-service)</b>
 Project member	End user of the SP's client	End user of the MSP's client	End users in the enterprise	<b>Project (self-service)</b>

- 系统管理员可以完全控制 Acronis Cyber Infrastructure，并且可以访问管理面板。这是您在安装 Acronis Cyber Infrastructure 时默认获得的角色。这些通常是 MSP 的基础架构管理员或企业的主要 IT 部门，具体取决于您的业务案例。
- 域管理员负责管理其域。域是虚拟化项目（租户）和用户（最终客户）的集合。域管理员有权访问自助服务面板。他们可以创建用户，并在允许的配额内使用项目资源：部署和管理虚拟机、映像、卷、网络、路由器、浮动 IP 和 SSH 密钥。
- 项目成员可以使用自助服务面板来管理其项目中的资源：部署和管理虚拟机、映像、卷、网络、路由器、浮动 IP 和 SSH 密钥。项目是一组由配额定义且可供指派用户访问的计算资源和存储资源。

域管理员和项目成员角色均具有某些限制。例如，他们无法在节点之间迁移虚拟机，因为在该抽象级别上不存在节点。



在我们的评估方案中，您是系统管理员。在创建了计算簇后，您需要创建域、项目、一些最终用户，并将其指派给该项目。然后，为 VM 卷创建存储策略并定义其冗余参数。接下来，配置虚拟网络连接。之后，域用户将有权通过自助服务面板访问其域和项目。在该处，他们将能够创建自己的虚拟机、卷、网络等。

---

**注解：** 自助服务面板 IP 地址显示在管理面板中的**设置 > 自助服务**屏幕上。

---

在 **Self-Service Guide** 中描述了在自助服务面板中执行的操作。对于我们的评估，我们将坚持在管理面板上对计算簇进行操作。

1. 创建域。要执行此操作，请登录到管理面板，然后打开**设置 > 项目和用户**屏幕。单击右上角的**创建域**。为新域指定一个名称和描述。单击**创建**。
2. 为新域创建一个管理员帐户。要执行此操作，请选择新创建的域，然后单击**创建用户**。指定登录名和密码，然后选择**域管理员**角色。选中**映像上传**方框，以允许新管理员上传映像来部署虚拟机。单击**创建**。
3. 创建项目。要执行此操作，请导航至域的**项目**选项卡，然后单击**创建项目**。设置配额，然后单击**创建**。确保您拥有的 CPU、RAM、存储和网络资源足以部署虚拟机（以及附加组件服务，您应选择启用它们）。
4. 创建项目成员。要执行此操作，请转至**域用户**选项卡，然后单击**创建用户**。指定登录名和密码，然后选择**项目成员**角色。选择要向其指派新成员的项目，然后单击**创建**。
5. (可选) 在**设置 > 自助服务**屏幕上，通过添加徽标和选择颜色主题来自定义自助服务面板的外观。通过这种方法，（例如托管服务提供商）可以为最终客户提供品牌化的虚拟化服务。

## 4.2.2 创建存储策略

为了创建新的存储策略，请转至**计算 > 存储**屏幕、打开**存储策略**选项卡，然后单击**创建存储策略**。指定一个名称、级、故障域和冗余方案。对于评估方案，请选择**2 个副本模式**和**主机**作为**故障域**。

现在，已完成创建存储策略，可以在创建虚拟机时将它选择用于卷（请参阅**创建虚拟机 (page 14)**）。还可以直接在**卷**选项卡上创建卷时应用它。

可以在项目配额中使用存储策略。在项目之前创建的策略将在其配额中启用。在项目之后创建的策略将不会自动为该项目启用。您将需要编辑该项目的配额，并手动选择策略。

### 4.2.3 创建计算网络

在部署虚拟机之前，需要在**计算 > 网络**屏幕上配置网络连接。专用虚拟网络使与其连接的虚拟机可以相互通信。例如，公用虚拟网络将虚拟机连接到现有物理网络，因此它们可以访问 Internet。

为了创建一个新网络，单击**创建虚拟网络**并指定其类型。为该新网络提供一个名称、子网 CIDR（例如 192.168.0.1/24）和网关。单击**下一步**以继续。如果您有虚拟机的 IP 地址集区，则可以启用内置 DHCP 服务器以将这些 IP 地址自动指派给虚拟机。单击**创建虚拟网络**以完成该过程。

结合使用虚拟网络，可以创建浮动 IP。浮动 IP 是可以手动指派给虚拟机的专用 IP 地址的公共 IP 地址。即使它只有专用 IP 地址，它也可以让您从公共网络访问虚拟机。要创建浮动 IP，首先需要将公共网络和专用网络与虚拟路由器相链接。有关更多详细信息，请参阅 [Managing Floating IP Addresses](#)。

## 4.3 创建虚拟机

现在，您已经创建了计算簇、域和项目、存储策略以及网络，可以继续创建虚拟机。

在我们的评估方案中，您将从映像创建虚拟机。可以上传一个映像，也可以使用默认附带的 Cirros 映像。要上传映像，请打开**计算 > 虚拟机 > 映像**选项卡。可以使用 ISO 映像和模板（采用 QCOW2 云映像格式的即用型卷，其中已安装操作系统和应用程序）。单击**添加映像**，然后从本地计算机中选择 ISO 映像。为新映像指定一个名称，然后从下拉列表中选择一个兼容操作系统。如果要将此映像用作模板用于将来 VM 部署，请选中**在所有项目之间共享**方框。单击**添加**。

---

**注解：**Acronis Cyber Infrastructure 支持各种 Windows 和 Linux 来宾操作系统，可以从中部署虚拟机（请参阅 [Supported Guest Operating Systems](#)）。此外，它还使用了许多获得专利的创新技术来优化已部署 VM 的性能。例如，基于 Windows 的 VM 应如同部署在 Hyper-V 上一样执行。

---

1. 在**计算 > 虚拟机**屏幕上，单击**创建虚拟机**，然后指定一个名称。
2. 要从映像创建 VM，请选择先前已上传的映像。在**卷**部分中，您将看到基于映像数据自动添加的可启动卷。可以更改卷的存储策略。要执行该操作，请单击**卷**部分中的铅笔符号、单击**卷**窗口中的省略号图标、选择**编辑**，然后在**编辑卷**窗口中更改策略。还可以在此处将新卷添加至 VM。
3. 在**规格**部分中，选择规格。这是一个预设，用于定义虚拟机有多少个虚拟 CPU 和多少内存。
4. 在**网络**部分中，将接口添加至虚拟机应连接到的虚拟网络。
5. 单击**部署**以开始创建虚拟机。查看新虚拟机的状态。在它的状态变为**活动**后，即表示该 VM 已准备就绪。

为了访问新创建的虚拟机，请单击其名称，然后在右窗格中单击**中控台**。在 VM 的**监控**选项卡上，可以查看它所使用的资源量。

---

**注解：** 还可以使用 virt-v2v 工具从 VMware vCenter 迁移虚拟机，如 Migrating Virtual Machines from VMware vCenter 中所述。

---

在虚拟机准备就绪后，即可对它执行各种操作：停止和启动、暂停和恢复、重新启动、迁移等。有关更多详细信息，请参阅 Managing Virtual Machines。

## CHAPTER 5

# 导出存储空间

Acronis Cyber Infrastructure 允许您导出存储空间：

- 作为块存储（通过 iSCSI），以满足虚拟化、数据库和其他需求。可以采用类似 SAN 的方式通过 iSCSI 以 LUN 块设备的形式将簇磁盘空间导出到外部物理主机或虚拟主机。
- 作为对象存储，以通过 S3 兼容协议存储无限数量的文件。使用通过类似 Dropbox 应用程序提供的访问，类似 S3 的对象存储可以存储诸如媒体文件、备份和 Open Xchange 文件之类的的数据。在将数据从 Amazon S3 迁移至 Acronis Cyber Infrastructure 后，最终用户可以针对 S3 运行相应应用程序。他们还可以构建自己的与 Amazon S3 兼容的对象存储服务。
- 通过 NFS。可以将节点组织为可以在其中创建 NFS 共享的高度可用 NFS 簇。在每个共享中，可以创建多个 NFS 导出，这是用户数据的实际导出目录。可以使用标准命令加载每个导出。在技术方面，NFS 卷基于对象存储。NFS 簇会生成完美的冷和暖文件存储，但不建议用于性能要求较高的热工作负载。为了能与 VMware vSphere 最佳集成，建议使用 iSCSI 协议。

## 5.1 通过 iSCSI 导出存储空间

Acronis Cyber Infrastructure 让您可以采用类似 SAN 的方式通过 iSCSI 以 LUN 块设备的形式将簇磁盘空间导出到外部操作系统和第三方虚拟化解解决方案。

可以创建在不同存储节点上运行的多组冗余目标。可以向每个目标组附加多个存储卷，这些存储卷具有由存储层提供的自身冗余。目标将这些卷导出为 LUN。

目标组中的每个节点可以托管该组的单个目标。如果目标组中的其中一个节点与其目标一起发生故障，则同一组中正常运行的目标将继续提供对先前由发生故障的目标服务的 LUN 的访问。

## 5.1.1 创建目标组

要创建目标组，请依次打开**存储服务 > 块存储 > 目标组**，然后单击**创建目标组**。将打开一个向导。请执行以下操作：

1. 对于**名称和类型**，输入一个目标组名称并选择 iSCSI。接下来，选择至少两个节点添加至目标组，以实现高可用性。
2. 对于**目标**，选择要添加至目标组的 iSCSI 接口。对于**卷**，选择要附加至目标组 LUN 的卷，也可以以后添加它们。对于评估方案，请跳过**访问控制**设置。
3. 对于**概要**，查看目标组详细信息。单击**创建**。

新创建的目标组将显示在**目标组**选项卡上。其目标将自动启动。单击组名称即可查看其详细信息。在**目标**选项卡上，可以为新目标添加更多节点。还可以在**LUN**选项卡上查看或添加 LUN。

## 5.1.2 创建卷

1. 打开**存储服务 > 块存储 > 卷**，然后单击**创建卷**。将打开一个向导。
2. 对于**名称和大小**，输入一个卷名称并指定其大小。请注意，卷可以以后扩展，但不能缩减。
3. 对于**存储策略**，选择冗余模式、存储级和故障域。
4. 对于**概要**，查看卷详细信息。单击**创建**。

## 5.1.3 将卷附加至目标组

1. 打开**存储服务 > 块存储 > 目标组**、单击所需目标组的省略号图标，然后单击**添加 LUN**。
2. 在打开的**附加**窗口中，选择要附加至目标组的卷或创建它们。单击**应用**。
3. 在**目标组**选项卡上，单击所需的**目标组**名称，然后转到**LUN**选项卡。可以在此处查看所有可用的 LUN。

## 5.1.4 从 VMware vSphere 访问 iSCSI 目标

可以从 Linux、Microsoft Hyper-V 和 VMware vSphere 访问 iSCSI 目标。有关从 Linux 和 Microsoft Hyper-V 访问的更多详细信息，请参阅 [Accessing iSCSI Targets](#)。以下部分介绍了用于评估的 VMware vSphere 方案。

在使用具有 VMware vSphere 的 Acronis Cyber Infrastructure 卷之前，需要对它进行正确配置才能与 ALUA 主动/被动存储阵列一起使用。建议您使用以下命令将默认的路径策略更改为 RR 策略：

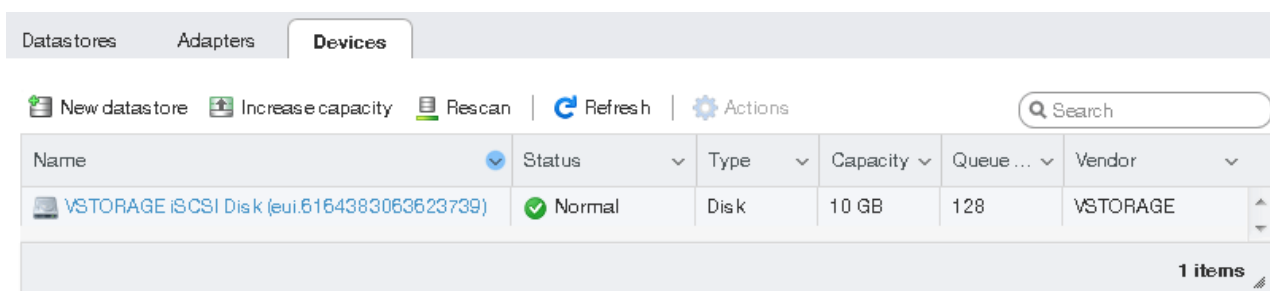
```
# esxcli storage nmp satp set -s VMW_SATP_ALUA -P VMW_PSP_RR
```

现在，可以重新启动主机，然后通过 iSCSI 从导出的 Acronis Cyber Infrastructure 卷创建数据存储。登录到 VMware ESXi Web 面板并执行以下操作：

1. 在导航器中，转至**存储 > 适配器**选项卡，然后单击**软件 iSCSI**。
2. 在**配置 iSCSI** 窗口中，选择**启用**。在**动态目标**部分中，单击**添加动态目标**，然后输入节点的 IP 地址。

**注解：**可以在管理面板中查看 IP 地址。在**基础架构 > 节点**屏幕上，单击所需节点，然后在**网络**部分上复制其公用网络 IP。

3. 单击**保存配置**。
4. 继续到**设备**选项卡，并单击**刷新**。新添加的磁盘将显示在设备列表中。



5. 选择磁盘并单击**新数据存储**。在显示的向导中，输入数据存储的名称并选择分区选项。单击**完成**以对磁盘分区。

**警告：**对磁盘分区将从磁盘上擦除所有数据。

6. 可以使用的磁盘将显示在数据存储的列表中。选择它，然后单击**数据库浏览器**以查看其内容并上传文件，以便您可以继续检查其可访问性。

## 5.2 通过 S3 导出存储空间

Acronis Cyber Infrastructure 让您可以采用 S3 兼容对象存储的形式将簇磁盘空间导出给客户。

对象存储经过优化，可用于存储数十亿个对象，尤其适用于应用程序存储、静态 Web 内容托管、在线存储服务、大数据和备份。相较于其他类型的存储，主要区别在于对象的某些部分无法修改，因此如果对象发生更改，将改为创建该对象的新版本。该方法消除了发生冲突的问题。

Acronis Cyber Infrastructure 可以存储 S3 簇数据的副本，并让它们在多个地理上分布的数据中心中保持最新。地理复制缩短了本地 S3 用户访问远程 S3 簇中数据或远程 S3 用户访问本地 S3 簇中数据的响应时间，因为他们不需要 Internet 连接。地理复制预定在任何数据被修改后就更新副本。其性能取决于 Internet 连接速度、冗余模式和簇性能。如果您有多个可用空间足够的数据中心，建议在这些数据中心中驻留的 S3 簇之间设置地理复制，如 Exporting Storage via S3 中所述。

在创建 S3 簇之前，请确保您有 S3 网关的 DNS 名称。

## 5.2.1 创建 S3 簇

要创建 S3 簇，请执行以下操作：

1. 在左侧菜单中，依次单击**存储服务** > **S3**。为我们的评估方案选择三个节点，然后在右侧菜单中单击**创建 S3 簇**。
2. 接下来，选择存储策略。
3. 为将由最终用户用于访问对象存储的 S3 端点指定外部（公共可解析）DNS 名称。例如，s3.example.com。单击**继续**。
4. 在下拉列表中，选择 S3 端点协议：HTTP 或 HTTPS，或者两者。对于我们的简单评估方案，建议您选择 HTTPS，然后选中**生成自签名证书**复选框。单击**完成**，以创建 S3 簇。

在完成创建 S3 簇后，请打开 **S3 概述** 屏幕以查看簇状态、主机名、已用磁盘容量、用户数、I/O 活动和 S3 服务的状态。

要检查 S3 簇是否已成功部署并可供用户访问，请通过浏览器访问 `https://<S3_DNS_name>`。您应该收到以下 XML 响应：

```
<Error>
<Code>AccessDenied</Code>
<Message/>
</Error>
```

要开始使用 S3 存储，还需要创建至少一个 S3 用户。

## 5.2.2 管理 S3 用户和存储桶

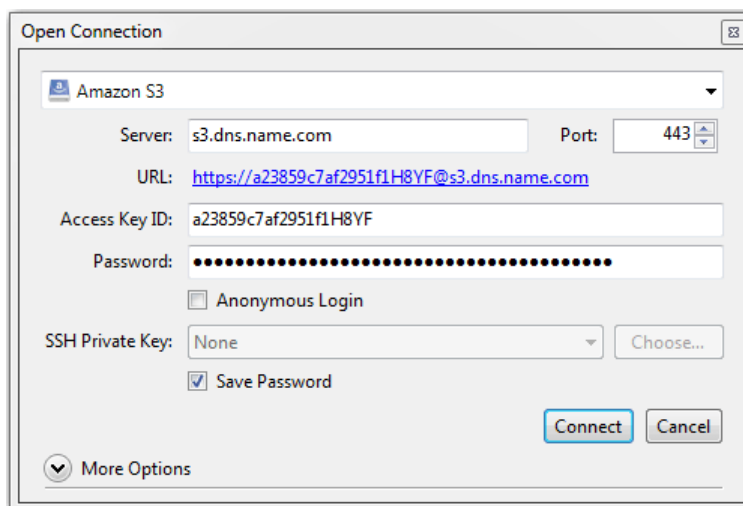
要添加 S3 用户，请执行以下操作：

1. 在**存储服务** > **S3** > **用户** 屏幕上，单击**添加用户**。
2. 指定一个电子邮件地址作为用户登录名，然后单击**添加**。

要在使用用户凭据的情况下使用所生成的密钥自动登录到 S3 门户，请转到管理面板、选择一个用户，然后单击**浏览**。在该工作区中，可以创建新的存储桶并监控现有存储桶的内容。

还可以使用诸如 CyberDuck、MountainDuck 或 Backup Exec 之类的第三方应用程序登录到 S3 存储。对于我们的评估方案，按照以下步骤操作，通过 CyberDuck 连接至 S3 存储：

1. 在 CyberDuck 中，单击**打开连接**。
2. 从 Acronis Cyber Infrastructure 管理面板获取凭据：
  - 在**存储服务 > S3 > 概述**选项卡上，获取 S3 端点的 DNS 名称。
  - 在**存储服务 > S3 > 用户**选项卡上，获取**访问密钥 ID**和**密码**。选择所需用户，然后单击右侧的**密钥**。这将显示访问密钥 ID 和安全访问密钥。
3. 在 CyberDuck 中指定您的凭据：



4. 建立连接后，可以查看现有存储桶并创建新的存储桶。依次单击**文件 > 新建文件夹**以创建存储桶。指定新存储桶的名称，然后单击**创建**。使用符合 DNS 命名约定的存储桶名称。

要管理存储桶中的文件，您需要以用户身份登录到 S3 门户。有关详细信息，请参阅 [Accessing S3 Buckets](#)。

## 5.3 通过 NFS 导出存储空间

Acronis Cyber Infrastructure 让您可以将节点组织为可以在其中创建 NFS 共享的高度可用 NFS 簇。NFS 共享是某个卷的访问点，因此可以为其指派 IP 地址或 DNS 名称。可以依次为相应卷指派冗余类型、级和故障域。在每个共享中，可以创建多个 NFS 导出，这是用户数据的实际导出目录。每个导出在其他属性中都有一个路径，该路径与共享的 IP 地址相结合，唯一标识网络上的导出，让您可以使用标准工具加载它。



在技术方面，NFS 卷基于对象存储。除了提供高可用性和可扩展性之外，对象存储还消除了对可保留在 NFS 簇中文件数量和数据大小的限制。每个共享都适用于保留数以亿计的任何大小的文件。但是，此类可扩展性意味着 I/O 开销浪费在文件大小更改和重写上。因此，NFS 簇会生成完美的冷和暖文件存储，但不建议用于实现热和高性能以及用于经常重写的数据（如正在运行的虚拟机）。例如，最好通过 iSCSI 将 Acronis Cyber Infrastructure 与 VMware 中的解决方案集成，以提高性能。

### 5.3.1 创建 NFS 簇

1. 在左侧菜单中，依次单击**存储服务 > NFS**。
2. 选择节点，然后在右侧菜单中单击**创建 NFS 簇**。对于评估方案，建议您选择三个节点。
3. 单击**创建**。

在完成创建 NFS 簇后，可以继续创建 NFS 共享。

### 5.3.2 创建 NFS 共享

1. 在**存储服务 > NFS > 共享**屏幕上，单击**添加 NFS 共享**。
2. 在**添加 NFS 共享**面板上，指定一个名称（例如，share1）和公共网络中唯一可解析的静态 IP 地址。
3. 在**共享大小**中，指定相应大小。对于访问导出的用户，此值将是文件系统大小。
4. 选择所需的级、故障域和数据冗余类型。单击**完成**。

在完成创建共享后，可以继续创建 NFS 导出。

### 5.3.3 创建和加载 NFS 导出

1. 在**存储服务 > NFS > 共享**屏幕上，在所需共享的相应行中，单击**导出**列中的数字。这将打开共享屏幕。
2. 在共享屏幕上，单击**添加导出**、指定 root 为导出名称并指定 / 为路径，然后选择**读取和写入**访问模式。这将创建一个具有默认路径的目录，该目录指定共享中的导出位置，并用于（结合使用共享的 IP 地址）加载导出。根导出将显示在导出列表中。
3. 在创建根导出后，可以按照文档 Storage User's Guide 中所述，在 Linux 或 macOS 上加载它。对于我们的评估方案，在 Linux 上使用以下命令加载它：

```
# mkdir /mnt/nfs
# mount -t nfs -o vers=4.0 <share_IP>:/<share_name>/ /mnt/nfs
```

其中：

- `-o vers=4.0` 是要使用的 NFS 版本。
- `<share_IP>` 是共享 IP 地址。还可以使用共享主机名。
- `/<share_name>/` 是根导出路径，如 `share1`。
- `/mnt/nfs` 是用于将导出加载到的现有本地目录。

要检查已加载的存储，可以运行 `df -h`。

## CHAPTER 6

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

Acronis Cyber Infrastructure 已与 Acronis Cyber Backup 和 Acronis Cyber Backup Cloud 集成。其 Backup Gateway 功能将存储后端连接至 Acronis Cyber Cloud。

Backup Gateway 旨在用于以下服务提供商：使用 Acronis Cyber Backup Cloud 或 Acronis Cyber Backup Advanced，并希望组织本地存储用于其客户端的备份数据。Acronis Backup 协议已针对本地和远程网络进行了优化，因此它可用于分支机构备份方案。

此外，还可以将备份存储在云服务上，例如 Google Cloud、Microsoft Azure 和 Amazon S3。在这种情况下，存储将用作公共云或私有云的代理服务器。Acronis Cyber Infrastructure 支持多种公共云，例如 Amazon S3、Microsoft Azure、Google Cloud 和 Alibaba Cloud。此外，它还支持私有云中的对象存储。因此，客户的数据可以在相应的公共云或私有云中进行存储并管理。

借助 Backup Gateway，还可以通过 NFS 协议在 NAS 上存储备份。在这种情况下，客户的数据将在相应 NAS 上进行存储并管理。

在本部分里，我们将介绍如何在 Acronis Cyber Infrastructure 中配置备份网关、在 Acronis Cyber Cloud 中创建新客户，然后在 Acronis Cyber Backup Cloud 中设置备份的存储。Acronis Cyber Backup 的相应步骤与之相似。

---

**注解：**我们假定您已经为 Acronis Cyber Cloud 创建了一个合作伙伴帐户，并拥有所有必需的凭据。如果没有，您可以转到产品页面并提交请求。

---

## 6.1 配置备份网关

在配置备份网关之前，请确保 DNS 配置满足**硬件要求** (page 2) 中所述的要求。此外，应为具有 **ABGW 公用**角色的网络接口的入站/出站连接打开端口 44445（这是我们评估方案中的公用网络）。

1. 通过使用 Acronis Cyber Infrastructure 管理面板，为存储和管理客户的备份创建新的存储。为此，请登录到 Acronis Cyber Infrastructure，然后依次导航到**存储服务**、**备份存储**。
2. 可以在此处查看存储簇中可用作备份目标的所有节点。选择所需节点，然后单击**创建网关**。在右侧面板中，单击**此簇**。在我们的评估方案中，客户的数据将在存储群集节点上进行存储并管理。
3. 选择将应用于客户的备份的合适数据冗余方案。
4. 指定 DNS 名称，它将与选定簇相关联并用于在 Acronis Cyber Backup Cloud 内注册该簇（如 backup.example.com）。有关更多详细信息，请参阅**硬件要求** (page 2)。新的 DNS 名称与选定簇中每个节点的 IP 地址相关联。备份操作的特定节点由备份代理程序自动选择。它取决于多个因素，例如节点可用性和负载。

### < DNS configuration

DNS name

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**。

5. 指定 Acronis Cyber Backup Cloud 实例的 URL。默认情况下，它是 <https://cloud.acronis.com>。如果使用 Acronis Cyber Backup，则在此阶段应使用相应计算机的 IP 地址来访问 Backup Management Console。对于该评估方案，请提供 Acronis Cyber Cloud 管理员帐户的登录名和密码。单击**下一步**。

您可能希望在公开可见之前在本地测试 DNS 设置。为此，可以将相应 DNS 名称添加至将用于访问备份网关的计算机上的 `/etc/hosts` 文件。例如，`192.168.1.10 backup.example.com`。

- 部署将立即开始。结束后，您将看到三个选项卡：**概述**、**节点**和**地理复制**。例如，在**概述**选项卡上，可以查看已注册网关及其性能的相关信息。

---

**注解：** 如果当前存储没有公共 IP 地址和 DNS 名称，则 Acronis Cyber Cloud 的 Web 还原工具将无法正常工作。

---

## 6.2 配置 Acronis Cyber Backup Cloud

- 登录到 Acronis Cyber Cloud 管理中控制台。然后，导航至**设置 > 位置**。确保系统使用派生自 DNS 名称的相应名称创建了新的备份目标。按照 [Acronis Backup 用户指南](#)中所述，设置备份代理程序。
- 创建新客户，然后在 Acronis Cyber Cloud 中指派新的备份目标。为此，请单击右上角的**新建**，然后选择**客户**。指定客户姓名、模式和语言。接下来，选择要提供给新客户的服务，例如 Acronis Cyber Backup Cloud。然后，指定客户的设备和工作负载，例如服务器和工作站。在**位置**部分中，单击当前位置名称以显示所有可用选项。选择所需存储。填写其他字段，例如客户的电子邮件、语言、名字和姓氏，然后单击**完成**以完成整个过程。
- 要确认您的帐户，请检查您的电子邮件并按照激活请求中的步骤进行操作。
- 在创建客户后，请以管理员身份登录到 Acronis Cyber Cloud，然后打开**客户端**屏幕。单击创建的客户以打开其**概述**屏幕。单击**管理服务**以打开客户的 Cyber Backup Management Console。
- 在**设备**屏幕上，单击工具栏上的**添加**。选择要添加的设备。对于我们的评估方案，请选择操作系统当前在使用的工作站。将下载备份代理程序安装程序。
- 在备份代理程序安装程序中，单击**安装**。在**几乎完成...**屏幕上，单击**注册计算机**。接下来，输入设备注册信息并确认。确保您使用的是已创建的客户帐户：检查右上角的用户。注册完成后，添加的设备将显示在客户的 Backup Management Console 的**设备 > 所有设备**屏幕上。
- 要从客户的计算机创建备份，请单击相应设备，然后在右侧菜单中选择**备份**。单击**添加备份计划**，然后指定其详细信息。对于我们的评估方案，请在**备份内容**中选择**文件/文件夹**。接着，选择要备份的项目、目标云存储，然后在**预定**中选择**无**。单击**创建**，然后备份计划将在左侧列出。单击**立即运行**以开始备份过程。
- 该过程完成后，即可在**备份 > 位置**屏幕上查看已备份的文件。单击所需客户以查看您以前上传的文件。双击备份名称即可在右侧显示其详细信息。可以单击**恢复文件/文件夹**以导航到上传的文件，并根据需要下载它们。

## CHAPTER 7

# 监视存储簇

Acronis Cyber Infrastructure 提供了内置的监视工具，包括预集成的 Prometheus 引擎和预配置的 Grafana 仪表板，可显示服务状态、可用性和性能，以及网络带宽、迁移/复制储备、内存和 CPU 使用情况。通过 100% 兼容的 OpenStack API，可以与第三方系统集成。可以确保系统顺畅地启动和运行，并在问题影响最终用户或第三方系统之前就可以对其进行故障排除。

1. 要监控存储簇，请转至**监控 > 仪表板**屏幕。在此处，可以获取有关选定存储簇以下时长的常规信息：过去 30 分钟；1、6 和 12 小时；以及过去七天。显示的信息包括读写操作、区块服务的运行状况以及物理和逻辑空间使用情况。有关更多详细信息，请参阅 [Monitoring the Storage Cluster](#)。
2. 对于高级监控，请转至**监控 > 仪表板**屏幕，然后单击 **Grafana 仪表板**。将打开一个单独的浏览器选项卡，其中包含存储簇、硬件节点、导出等的预配置 Grafana 仪表板。两个仪表板专用于 Backup Gateway。要查看每个图表的详细说明，请参阅 [Monitoring Backup Gateway](#)。
3. 还可以在**存储服务 > 备份存储**屏幕上监控备份网关。在此处，可以查看有关已部署的备份存储簇及其性能的信息。此外，还可以获取有关选定备份网关的地理复制信息，以及从旧版本 Acronis Cyber Infrastructure 迁移的数据的信息。最后，可以获取有关公共云（例如 Amazon S3、Microsoft Azure、Google Cloud 或 Alibaba Cloud）中存储使用情况的信息。

## CHAPTER 8

# 启用高可用性

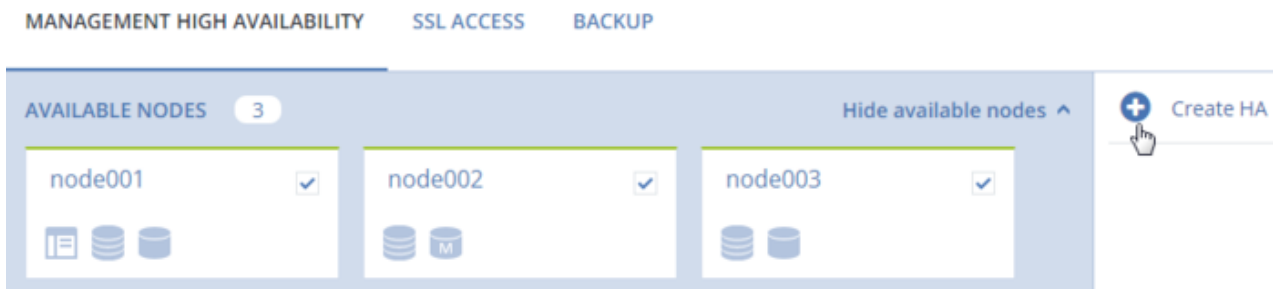
即使 Acronis Cyber Infrastructure 服务所在的节点发生故障，高可用性也可以使这些服务保持运行。在这种情况下，来自发生故障节点的服务将重定位至运行状况正常的节点。

您先前已经构建了一个由三个节点组成的簇，现在可以使其更具弹性和冗余性。要执行该操作，请为管理节点、管理面板和服务启用高可用性。

## 8.1 管理节点的高可用性

要为管理节点和管理面板启用高可用性，请按以下步骤操作：

1. 在 **设置 > 管理节点** 屏幕上，打开 **管理高可用性** 选项卡。



2. 选择三个节点，然后单击**创建 HA**。将自动选择管理节点。
3. 对于**配置网络**，请确保为每个节点选择一个专用网络接口用于内部管理，并将至少一个公共网络接口指派给管理面板。
4. 对于**配置网络**，请提供一个或多个唯一的静态 IP 地址。
5. 在为管理节点启用高可用性后，可以使用指定的静态 IP 地址（在端口 8888 上）登录到管理面板。

## 8.2 服务的高可用性

基于高度可用的元数据服务和启用的管理节点 HA，Acronis Cyber Infrastructure 将为以下服务提供其他高可用性：

- 管理面板。如果管理节点发生故障或无法通过网络访问，则另一个节点上的管理面板实例将接管该面板的服务，以便它仍可以通过相同的专用 IP 地址进行访问。服务的重新定位可能需要几分钟时间。启用管理面板 HA 以及管理节点 HA。
- 虚拟机。如果计算节点出现故障或无法通过网络进行访问，则托管在该节点上的虚拟机将根据其可用资源被转移到其他运行状况良好的计算节点。计算簇只能承受一个节点发生故障。默认情况下，在创建计算簇后会自动为虚拟机启用高可用性，也可以根据需要手动禁用。
- iSCSI 服务。如果指向通过 iSCSI 导出的卷的活动路径发生故障（例如，具有活动 iSCSI 目标的存储节点发生故障或无法通过网络访问），则会通过正常运行节点上的目标重新路由该活动路径。只要有至少一条指向通过 iSCSI 导出的卷的路径，则仍可访问这些导出的卷。
- S3 服务。如果 S3 节点发生故障或无法通过网络访问，则托管在其上的名称服务器和对象服务器组件将自动进行平衡并在其他 S3 节点之间迁移。S3 网关不会自动进行迁移；它们的高可用性基于 DNS 记录。添加或删除 S3 网关时，您需要手动维护 DNS 记录。在启用管理节点 HA 并基于三个或更多节点创建 S3 簇之后，将自动为 S3 服务启用高可用性。由三个节点组成的 S3 簇可能会丢失一个节点并保持继续运行。
- NFS 共享。如果存储节点发生故障或无法通过网络访问，则位于其上的 NFS 卷将在其他 NFS 节点之间迁移。创建 NFS 簇后，将自动为存储节点上的 NFS 卷启用高可用性。
- 备份网关服务。如果某个备份网关节点发生故障或无法通过网络访问，则备份网关簇中的其他节点将继续提供对所选存储后端的访问。备份网关不会自动进行迁移；它们的高可用性基于 DNS 记录。添加或删除备份网关时，需要手动维护 DNS 记录。在基于两个或更多节点创建备份网关簇后，将自动为备份网关启用高可用性（不适用于外部 NFS）。将继续对存储后端提供访问，直到备份网关簇中至少一个节点运行状况良好为止。

## 8.3 测试高可用性

本部分将模拟管理节点发生故障的事件：

1. 强行关闭 Acronis Cyber Infrastructure 管理节点的电源。



---

**注解:** 如果服务所在的节点由于内核崩溃、断电等原因而发生故障，或者无法通过网络进行访问，则高可用性 (HA) 可确保服务正常提供。正常关机不视为故障事件。要测试 HA，应强行关闭节点的电源或断开节点与网络电缆的连接。

---

2. 打开**基础架构 > 节点**屏幕。发生故障的节点的状态为**脱机**，并以红色亮显。
3. 即使一个节点发生故障并且现在不可用，仍可以访问以下服务：
  - 管理面板。
  - 虚拟机。
  - iSCSI: 在 VMware vSphere 中，仍可以访问通过 iSCSI 导出的卷。
  - S3: 仍可以通过 CyberDuck 访问存储桶。
  - NFS: 在已加载的根导出中，仍可以访问上传的数据。
  - Backup Gateway: 在 Backup Management Console 中，仍可以导航到先前创建的备份（如果正确配置了 DNS 名称，则可以访问该备份）。

您刚刚进行了一个演示，其中强行关闭了某个节点的电源，导致服务和数据被撤离到运行状况正常的节点上，并在不停机的情况下仍然可用。