概念
HCI

NetApp
October 11, 2024

目录

概念

NetApp HCI 产品概述

NetApp HCI 是一种企业级混合云基础架构设计，集存储，计算，网络和虚拟机管理程序于一体，并增加了跨公有和私有云的功能。

NetApp 的分解式混合云基础架构支持独立扩展计算和存储，适应工作负载并提供有保障的性能。

- 满足混合多云需求
- 独立扩展计算和存储
- 跨混合多云简化数据服务流程编排

NetApp HCI 的组件

下面简要介绍了 NetApp HCI 环境的各个组件：

- NetApp HCI 可提供存储和计算资源。您可以使用 * NetApp 部署引擎 * 向导部署 NetApp HCI 。成功部署后，计算节点将显示为 ESXi 主机，您可以在 VMware vSphere Web Client 中对其进行管理。
- * 管理服务 * 或微服务包括 Active IQ 收集器，适用于 vCenter 插件的 QoSSIOC 和 mNode 服务；它们会作为服务包进行频繁更新。从 Element 11.3 版开始， * 管理服务 * 托管在管理节点上，以便在主要版本之外更快地更新选定的软件服务。管理节点 * （ mNode ）是一个虚拟机，它与一个或多个基于 Element 软件的存储集群并行运行。它用于升级和提供系统服务，包括监控和遥测，管理集群资产和设置，运行系统测试和实用程序，以及启用 NetApp 支持访问以进行故障排除。

  详细了解 "管理服务版本"。

- 使用 * NetApp 混合云控制 * ，您可以管理 NetApp HCI 。您可以使用 NetApp SolidFire Active IQ 升级管理服务，扩展系统，收集日志以及监控安装。您可以通过浏览到管理节点的 IP 地址登录到 NetApp Hybrid Cloud Control 。
- 适用于vCenter Server*的NetApp Element 插件是一个与vSphere用户界面(UI)集成的基于Web的工具。此插件是 VMware vSphere 的一个扩展，可扩展且用户友好的界面，可管理和监控运行 * NetApp Element 软件 * 的存储集群。此插件可替代 Element UI 。您可以使用此插件用户界面发现和配置集群，并管理，监控和分配集群容量中的存储，以配置数据存储库和虚拟数据存储库（对于虚拟卷）。集群在网络上显示为一个本地组，该组通过虚拟 IP 地址呈现给主机和管理员。您还可以通过实时报告功能监控集群活动，包括执行各种操作时可能发生的任何事件的错误和警报消息。

  详细了解 "适用于 vCenter Server 的 NetApp Element 插件"。

- 默认情况下， NetApp HCI 会将性能和警报统计信息发送到 * NetApp SolidFire Active IQ * 服务。在您的正常支持合同中， NetApp 支持部门会监控这些数据，并在出现任何性能瓶颈或潜在系统问题时向您发出警报。如果您还没有 NetApp 支持帐户，则需要创建一个（即使您已有 SolidFire Active IQ 帐户），以便可以利用此服务。

  详细了解 "NetApp SolidFire Active IQ"。

NetApp HCI URL

以下是您在 NetApp HCI 中使用的常见 URL：

URL	说明
`https://[IPv4 address of Bond1G interface on a storage node]`	访问NetApp部署引擎向导以安装和配置NetApp HCI。"了解更多信息。"
<code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt; </code>	访问NetApp混合云控制以升级、扩展和监控NetApp HCI安装以及更新管理服务。"了解更多信息。"
`https://[IP address]:442`	从每节点UI中、访问网络和集群设置并利用系统测试和实用程序。"了解更多信息。"
`https://<ManagementNodeIP>:9443`	在 vSphere Web Client 中注册 vCenter 插件软件包。
`https://activeiq.solidfire.com`	监控数据并接收任何性能瓶颈或潜在系统问题的警报。
`https://<ManagementNodeIP>/mnode`	使用管理节点中的 REST API UI 手动更新管理服务。
`https://[storage cluster MVIP address]`	访问 NetApp Element 软件 UI 。

了解更多信息

- "适用于 vCenter Server 的 NetApp Element 插件"
- "NetApp HCI 资源页面"

用户帐户

要访问系统上的存储资源，您需要设置用户帐户。

用户帐户管理

用户帐户用于控制对基于 NetApp Element 软件的网络上存储资源的访问。要创建卷，至少需要一个用户帐户。

创建卷时，系统会将其分配给帐户。如果已创建虚拟卷，则帐户为存储容器。

以下是一些其他注意事项：

- 帐户包含访问分配给它的卷所需的 CHAP 身份验证。
- 一个帐户最多可以分配 2000 个卷，但一个卷只能属于一个帐户。
- 可以从 NetApp Element 管理扩展点管理用户帐户。

使用 NetApp Hybrid Cloud Control ，您可以创建和管理以下类型的帐户：

- 存储集群的管理员用户帐户
- 权威用户帐户
- 卷帐户，仅适用于创建这些帐户的存储集群。

存储集群管理员帐户

运行 NetApp Element 软件的存储集群中可以存在两种类型的管理员帐户：

- * 主集群管理员帐户 *：此管理员帐户是在创建集群时创建的。此帐户是对集群具有最高访问级别的主管理帐户。此帐户类似于 Linux 系统中的 root 用户。您可以更改此管理员帐户的密码。
- * 集群管理员帐户 *：您可以为集群管理员帐户授予有限的管理访问权限，以便在集群中执行特定任务。分配给每个集群管理员帐户的凭据用于对存储系统中的 API 和 Element UI 请求进行身份验证。

> 要通过每节点 UI 访问集群中的活动节点，需要使用本地（非 LDAP ）集群管理员帐户。访问尚未加入集群的节点不需要帐户凭据。

您可以通过创建，删除和编辑集群管理员帐户，更改集群管理员密码以及配置 LDAP 设置来管理用户的系统访问来管理集群管理员帐户。

有关详细信息，请参见 "SolidFire和Element文档中心"。

权威用户帐户

权威用户帐户可以针对与节点和集群的 NetApp Hybrid Cloud Control 实例关联的任何存储资产进行身份验证。使用此帐户，您可以管理所有集群中的卷，帐户，访问组等。

权威用户帐户可从 NetApp Hybrid Cloud Control 中右上角的 User Management 选项菜单进行管理。

"权威存储集群"是NetApp混合云控制用于对用户进行身份验证的存储集群。

在权威存储集群上创建的所有用户均可登录到 NetApp Hybrid Cloud Control 。在其他存储集群上创建的用户无法登录到 Hybrid Cloud Control 。

- 如果您的管理节点只有一个存储集群，则它是权威集群。
- 如果您的管理节点有两个或更多存储集群，其中一个集群将被分配为权威集群，只有该集群中的用户才能登录到 NetApp Hybrid Cloud Control 。

虽然许多 NetApp Hybrid Cloud Control 功能可用于多个存储集群，但身份验证和授权具有必要的限制。身份验证和授权的限制是，权威集群中的用户可以对与 NetApp Hybrid Cloud Control 关联的其他集群执行操作，即使他们不是其他存储集群上的用户也是如此。在继续管理多个存储集群之前，您应确保在权威集群上定义的用户已在具有相同权限的所有其他存储集群上定义。您可以从 NetApp Hybrid Cloud Control 管理用户。

卷帐户

特定于卷的帐户仅特定于创建它们的存储集群。通过这些帐户，您可以在网络中为特定卷设置权限，但在这些卷之外不起作用。

卷帐户在 NetApp Hybrid Cloud Control Volumes 表中进行管理。

了解更多信息

- "管理用户帐户"
- "了解集群"

- "NetApp HCI 资源页面"
- "适用于 vCenter Server 的 NetApp Element 插件"
- "SolidFire和Element文档中心"

数据保护

NetApp HCI 数据保护术语包括不同类型的远程复制，卷快照，卷克隆，保护域以及双 Helix 技术的高可用性。

NetApp HCI 数据保护包括以下概念：

- [远程复制类型]
- [用于数据保护的卷快照]
- [卷克隆]
- SolidFire 存储的备份和还原过程概述
- [保护域]
- 双 Helix 高可用性

远程复制类型

数据的远程复制可以采用以下形式：

- [集群之间的同步和异步复制]
- 仅 Snapshot 复制
- 使用 SnapMirror 在 Element 和 ONTAP 集群之间进行复制

请参阅。 "TR-4741： NetApp Element 软件远程复制"

集群之间的同步和异步复制

对于运行 NetApp Element 软件的集群，可以通过实时复制快速创建卷数据的远程副本。

您可以将一个存储集群与最多四个其他存储集群配对。您可以从集群对中的任一集群同步或异步复制卷数据，以实现故障转移和故障恢复。

同步复制

同步复制会持续将数据从源集群复制到目标集群，并受延迟，数据包丢失，抖动和带宽的影响。

同步复制适用于以下情况：

- 在短距离内复制多个系统
- 源本地的灾难恢复站点
- 对时间敏感的应用程序和数据库保护

- 业务连续性应用程序，要求在主站点关闭时将二级站点用作主站点

异步复制

异步复制可将数据从源集群持续复制到目标集群，而无需等待目标集群的确认。在异步复制期间，写入在源集群上提交后会向客户端（应用程序）确认。

异步复制适用于以下情况：

- 灾难恢复站点远离源，应用程序不允许网络造成延迟。
- 连接源集群和目标集群的网络存在带宽限制。

仅 **Snapshot** 复制

仅快照数据保护功能可将特定时间点发生更改的数据复制到远程集群。仅复制在源集群上创建的快照。而源卷的活动写入则不是。

您可以设置快照复制的频率。

Snapshot 复制不会影响异步或同步复制。

使用 **SnapMirror** 在 **Element** 和 **ONTAP** 集群之间进行复制

借助 NetApp SnapMirror 技术，您可以将使用 NetApp Element 软件创建的快照复制到 ONTAP 以实现灾难恢复。在 SnapMirror 关系中， Element 是一个端点，而 ONTAP 是另一个端点。

SnapMirror 是一种有助于灾难恢复的 NetApp Snapshot ® 复制技术，用于从主存储故障转移到地理位置偏远的站点上的二级存储。SnapMirror 技术会在二级存储中创建工作数据的副本或镜像，如果主站点发生中断，您可以继续使用该副本或镜像来提供数据。数据在卷级别进行镜像。

主存储中的源卷与二级存储中的目标卷之间的关系称为数据保护关系。这些集群称为卷所在的端点，包含复制数据的卷必须建立对等关系。通过对等关系，集群和卷可以安全地交换数据。

SnapMirror 在 NetApp ONTAP 控制器上本机运行，并集成到 Element 中，而 Element 则在 NetApp HCI 和 SolidFire 集群上运行。控制 SnapMirror 的逻辑驻留在 ONTAP 软件中；因此，所有 SnapMirror 关系都必须至少涉及一个 ONTAP 系统才能执行协调工作。用户主要通过 Element UI 管理 Element 和 ONTAP 集群之间的关系；但是，某些管理任务位于 NetApp ONTAP System Manager 中。用户还可以通过命令行界面和 API 管理 SnapMirror ，这些 CLI 和 API 在 ONTAP 和 Element 中均可用。

请参见 "TR-4651： NetApp SolidFire SnapMirror 架构和配置"(需要登录)。

您必须使用 Element 软件在集群级别手动启用 SnapMirror 功能。默认情况下， SnapMirror 功能处于禁用状态，并且在新安装或升级过程中不会自动启用此功能。

启用 SnapMirror 后，您可以从 Element 软件中的数据保护选项卡创建 SnapMirror 关系。

用于数据保护的卷快照

卷快照是卷的时间点副本，您可以稍后使用它将卷还原到该特定时间。

虽然快照与卷克隆类似，但快照只是卷元数据的副本，因此您无法挂载或写入这些副本。创建卷快照也只需少量系统资源和空间，因此创建快照的速度比克隆快。

您可以将快照复制到远程集群，并将其用作卷的备份副本。这样，您就可以使用复制的快照将卷回滚到特定时间点；您也可以从复制的快照创建卷的克隆。

您可以将快照从 SolidFire 集群备份到外部对象存储或另一个 SolidFire 集群。将快照备份到外部对象存储时，必须与允许读 / 写操作的对象存储建立连接。

您可以为单个或多个卷创建快照以进行数据保护。

卷克隆

一个或多个卷的克隆是数据的时间点副本。克隆卷时，系统会创建卷的快照，然后为该快照引用的数据创建一份副本。

这是一个异步过程，此过程所需的时间量取决于要克隆的卷大小和当前集群负载。

集群一次最多支持每个卷运行两个克隆请求，一次最多支持八个活动卷克隆操作。超过这些限制的请求将排队等待稍后处理。

SolidFire 存储的备份和还原过程概述

您可以将卷备份和还原到其他 SolidFire 存储以及与 Amazon S3 或 OpenStack Swift 兼容的二级对象存储。

您可以将卷备份到以下位置：

- SolidFire 存储集群
- Amazon S3 对象存储
- OpenStack Swift 对象存储

从 OpenStack Swift 或 Amazon S3 还原卷时，您需要原始备份过程中的清单信息。如果要还原的卷是在 SolidFire 存储系统上备份的，则不需要清单信息。

保护域

保护域是指一个节点或一组已分组在一起的节点，在保持数据可用性的同时，任何部分甚至所有节点都可能发生故障。通过保护域，存储集群可以在丢失机箱（机箱关联性）或整个域（机箱组）时自动进行修复。

保护域布局会将每个节点分配给特定的保护域。

支持两种不同的保护域布局，称为保护域级别。

- 在节点级别，每个节点都位于其自己的保护域中。
- 在机箱级别，只有共享机箱的节点才位于同一保护域中。
  - 将节点添加到集群时，系统会自动从硬件确定机箱级别布局。
  - 在每个节点位于单独机箱中的集群中，这两个级别在功能上是相同的。

您可以手动 "启用保护域监控"使用适用于vCenter Server的NetApp Element插件。您可以根据节点或机箱域选择保护域阈值。

创建新集群时，如果您使用的存储节点位于共享机箱中，则可能需要考虑使用保护域功能设计机箱级别的故障保

护。

您可以定义自定义保护域布局，其中每个节点都与一个且仅与一个自定义保护域相关联。默认情况下，每个节点都分配到相同的默认自定义保护域。

请参阅。 "SolidFire 和 Element 12.2 文档中心"

双 **Helix** 高可用性

双 Helix 数据保护是一种复制方法，可在系统中的所有驱动器之间至少分布两个冗余数据副本。通过 " 无 RAID " 方法，系统可以在存储系统的所有级别承受多个并发故障并快速修复。

了解更多信息

- "NetApp HCI 资源页面"
- "适用于 vCenter Server 的 NetApp Element 插件"

集群

集群是一组节点，作为一个整体运行，用于提供存储或计算资源。从 NetApp HCI 1.8 开始，您可以拥有一个包含两个节点的存储集群。存储集群在网络上显示为一个逻辑组，然后可作为块存储访问。

NetApp HCI 中的存储层由 NetApp Element 软件提供，管理层由适用于 vCenter Server 的 NetApp Element 插件提供。存储节点是指包含一组驱动器的服务器，这些驱动器通过绑定 10G 网络接口相互通信。每个存储节点都连接到两个网络：存储和管理，每个网络都有两个独立的链路，用于实现冗余和性能。每个节点在每个网络上都需要一个 IP 地址。您可以使用新的存储节点创建集群，也可以向现有集群添加存储节点以提高存储容量和性能。

权威存储集群

权威存储集群是 NetApp Hybrid Cloud Control 用于对用户进行身份验证的存储集群。

如果您的管理节点只有一个存储集群，则它是权威集群。如果您的管理节点有两个或更多存储集群，其中一个集群将被分配为权威集群，只有该集群中的用户才能登录到 NetApp Hybrid Cloud Control 。要了解哪个集群是权威集群、您可以使用 `GET /mnode/about`API。在响应中、字段中的IP地址 `token_url`是权威存储集群的管理虚拟IP地址(MVIP)。如果您尝试以非权威集群上的用户身份登录到 NetApp Hybrid Cloud Control ，则登录尝试将失败。

许多 NetApp Hybrid Cloud Control 功能都设计用于多个存储集群，但身份验证和授权存在限制。身份验证和授权的限制是，权威集群中的用户可以对与 NetApp Hybrid Cloud Control 关联的其他集群执行操作，即使他们不是其他存储集群上的用户也是如此。在继续管理多个存储集群之前，您应确保在权威集群上定义的用户已在具有相同权限的所有其他存储集群上定义。

您可以使用 NetApp Hybrid Cloud Control 管理用户。

在继续管理多个存储集群之前，您应确保在权威集群上定义的用户已在具有相同权限的所有其他存储集群上定义。您可以 "管理用户"从Element软件用户界面(Element Web UI)中进行设置。

有关使用管理节点存储集群资产的详细信息、请参见"创建和管理存储集群资产"。

孤立容量

如果新添加的节点占用的集群总容量超过 50% ，则此节点的某些容量将变为不可用（ " 孤立 " ），以使其符合容量规则。在添加更多存储容量之前，情况始终如此。如果添加的节点非常大，并且也不遵守容量规则，则先前的孤立节点将不再处于孤立状态，而新添加的节点将变为孤立状态。应始终成对添加容量，以免发生这种情况。当节点变为孤立时，会引发相应的集群故障。

双节点存储集群

从 NetApp HCI 1.8 开始，您可以设置一个包含两个存储节点的存储集群。

- 您可以使用某些类型的节点来构成双节点存储集群。请参阅。 "NetApp HCI 1.8 发行说明"

> 在双节点集群中，存储节点仅限于具有 480 GB 和 960 GB 驱动器的节点，并且节点的型号类型必须相同。

- 双节点存储集群最适合工作负载不依赖于大容量和高性能要求的小型部署。
- 除了两个存储节点之外，一个双节点存储集群还包括两个 * NetApp HCI 见证节点 * 。

> 详细了解"见证节点。"

- 您可以将双节点存储集群扩展为三节点存储集群。三节点集群可通过提供从存储节点故障中自动修复的功能来提高故障恢复能力。
- 双节点存储集群提供的安全特性和功能与传统的四节点存储集群相同。
- 双节点存储集群与四节点存储集群使用相同的网络。网络可在 NetApp HCI 部署期间使用 NetApp 部署引擎向导进行设置。

存储集群仲裁

Element 软件会从选定节点创建存储集群，从而维护已复制的集群配置数据库。要保持集群故障恢复能力所需的仲裁，至少需要三个节点才能加入集群集合。双节点集群中的见证节点用于确保有足够的存储节点来构成有效的集合仲裁。要创建集合，存储节点优先于见证节点。对于涉及双节点存储集群的最少三节点集合，使用两个存储节点和一个见证节点。

> 在具有两个存储节点和一个见证节点的三节点集合中，如果一个存储节点脱机，则集群将进入降级状态。在两个见证节点中，只有一个节点可以在集合中处于活动状态。无法将第二个见证节点添加到集合中，因为它会执行备份角色。集群将保持降级状态，直到脱机存储节点恢复联机状态或替代节点加入集群为止。

如果见证节点发生故障，则其余见证节点将加入此集合，以形成一个三节点集合。您可以部署一个新的见证节点来替换出现故障的见证节点。

双节点存储集群中的自动修复和故障处理

如果传统集群中某个节点上的硬件组件发生故障，则集群可以重新平衡该组件上发生故障的数据，并将这些数据重新分配给集群中的其他可用节点。在双节点存储集群中，此自动修复功能不可用，因为集群必须至少有三个物理存储节点可用于自动修复。当双节点集群中的一个节点发生故障时，双节点集群不需要重新生成第二个数据副本。系统会为剩余活动存储节点中的块数据复制新写入。更换故障节点并加入集群后，两个物理存储节点之间的数据将重新平衡。

包含三个或更多节点的存储集群

将两个存储节点扩展到三个存储节点可以在发生节点和驱动器故障时自动修复，从而提高集群的故障恢复能力，但不会提供额外容量。您可以使用进行扩展"NetApp Hybrid Cloud Control UI"。从双节点集群扩展为三节点集群时，容量可能会处于孤立状态(请参见[孤立容量])。在安装之前， UI 向导会显示有关孤立容量的警告。在存储节点发生故障时，仍可使用一个见证节点来保持集合仲裁，而另一个见证节点处于备用状态。将三节点存储集群扩展为四节点集群时，容量和性能将会提高。在四节点集群中，不再需要见证节点来构成集群仲裁。您可以扩展到多达 64 个计算节点和 40 个存储节点。

了解更多信息

- "NetApp HCI 双节点存储集群 | TR-4823"
- "适用于 vCenter Server 的 NetApp Element 插件"
- "SolidFire 和 Element 软件文档中心"

节点

节点是指分组到集群中以提供块存储和计算功能的硬件或虚拟资源。

NetApp HCI 和 Element 软件为集群定义了各种节点角色。四种节点角色类型分别为 * 管理节点 * ， * 存储节点 * ， * 计算节点 * 和 * NetApp HCI 见证节点 * 。

管理节点

管理节点（有时缩写为 mNode ）与存储集群交互以执行管理操作，但不是存储集群的成员。管理节点会定期通过 API 调用收集有关集群的信息，并将此信息报告给 Active IQ 以进行远程监控（如果已启用）。管理节点还负责协调集群节点的软件升级。

管理节点是与一个或多个基于 Element 软件的存储集群并行运行的虚拟机（ VM ）。除了升级之外，它还可用于提供包括监控和遥测在内的系统服务，管理集群资产和设置，运行系统测试和实用程序，以及启用 NetApp 支持访问以进行故障排除。从 Element 11.3 版开始，管理节点充当微服务主机，可以在主要版本之外更快地更新选定的软件服务。这些微服务或管理服务（例如 Active IQ 收集器，适用于 vCenter 插件的 QoSSIOC 以及管理节点服务）会作为服务包进行频繁更新。

存储节点

NetApp HCI 存储节点是为 NetApp HCI 系统提供存储资源的硬件。节点中的驱动器包含用于数据存储和数据管理的块和元数据空间。每个节点都包含 NetApp Element 软件的出厂映像。可以使用 NetApp Element 管理扩展点管理 NetApp HCI 存储节点。

计算节点

NetApp HCI 计算节点是一种硬件，用于提供在 NetApp HCI 安装中进行虚拟化所需的计算资源，例如 CPU ，内存和网络连接。由于每个服务器都运行 VMware ESXi ，因此必须在 vSphere 的主机和群集菜单中的插件外部执行 NetApp HCI 计算节点管理（添加或删除主机）。无论它是四节点存储集群还是双节点存储集群，对于 NetApp HCI 部署，计算节点的最小数量仍为 2 个。

见证节点

NetApp HCI 见证节点是指在计算节点上与基于 Element 软件的存储集群并行运行的 VM 。见证节点不托管分区或块服务。见证节点可在存储节点发生故障时启用存储集群可用性。您可以按照与其他存储节点相同的方式管理和升级见证节点。一个存储集群最多可以有四个见证节点。其主要目的是确保存在足够的集群节点以构成有效的集合仲裁。

- 最佳实践： * 将见证节点 VM 配置为使用计算节点的本地数据存储库（默认设置为 NDE ），请勿在共享存储（例如 SolidFire 存储卷）上配置它们。要防止虚拟机自动迁移，请将见证节点虚拟机的分布式资源计划程序（ DRS ）自动化级别设置为 * 已禁用 * 。这样可以防止两个见证节点在同一计算节点上运行并创建非高可用性（ HA ）对配置。

详细了解"见证节点资源要求"和"见证节点 IP 地址要求"。

在双节点存储集群中，至少会部署两个见证节点，以便在见证节点出现故障时实现冗余。在 NetApp HCI 安装过程安装见证节点时， VMware vCenter 中会存储一个 VM 模板，您可以使用该模板重新部署见证节点，以防其意外删除，丢失或损坏。如果您需要更换托管见证节点的计算节点出现故障，也可以使用此模板重新部署见证节点。有关说明，请参见“*重新部署双节点和三节点存储集群的见证节点*"此处""一节。

了解更多信息

- "NetApp HCI 双节点存储集群 | TR-4823"
- "适用于 vCenter Server 的 NetApp Element 插件"
- "SolidFire 和 Element 软件文档中心"

存储

维护模式

如果您需要使某个存储节点脱机以进行维护，例如软件升级或主机修复，则可以通过为该节点启用维护模式来最大限度地减少对该存储集群其余部分的 I/O 影响。您可以对设备节点以及 SolidFire 企业 SDS 节点使用维护模式。

只有当存储节点运行状况良好（没有阻止的集群故障）且存储集群能够容忍单个节点故障时，才能将此存储节点过渡到维护模式。为运行状况良好且容错的节点启用维护模式后，该节点不会立即过渡；它会一直受到监控，直到满足以下条件为止：

- 节点上托管的所有卷均已进行故障转移
- 此节点不再托管为任何卷的主节点
- 系统会为要进行故障转移的每个卷分配一个临时备用节点

满足这些条件后，节点将过渡到维护模式。如果在 5 分钟内未满足这些条件，则节点将不会进入维护模式。

禁用存储节点的维护模式时，系统会一直监控此节点，直到满足以下条件为止：

- 所有数据都会完全复制到节点
- 已解决所有阻止的集群故障
- 此节点上托管的卷的所有临时备用节点分配均已取消激活

满足这些条件后，节点将过渡到维护模式之外。如果在一小时内未满足这些条件，则节点将无法过渡到维护模式之外。

您可以使用 Element API 查看使用维护模式时的维护模式操作状态：

- * 已禁用 * ： 未请求任何维护。
- * 故障转移至恢复 * ： 节点无法从维护中恢复。
- * 重新覆盖 FromMaintenance* ： 节点正在从维护中恢复。
- * 准备维护 * ： 正在执行操作以允许节点执行维护。
- * 就绪 ForMaintenance* ： 节点已准备好执行维护。

了解更多信息

- "SolidFire和Element文档中心"

卷

存储在 NetApp Element 系统中配置为卷。卷是指使用 iSCSI 或光纤通道客户端通过网络访问的块设备。

通过适用于 vCenter Server 的 NetApp Element 插件，您可以创建，查看，编辑，删除，克隆， 为用户帐户备份或还原卷。您还可以管理集群上的每个卷，以及在卷访问组中添加或删除卷。

永久性卷

通过永久性卷，可以将管理节点配置数据存储在指定的存储集群上，而不是本地 VM 上，以便在管理节点丢失或删除时可以保留这些数据。永久性卷是一种可选的管理节点配置，但建议使用此配置。

如果使用 NetApp 部署引擎为 NetApp HCI 部署管理节点，则会自动启用并配置永久性卷。

部署新管理节点时，安装和升级脚本中包含一个启用永久性卷的选项。永久性卷是指基于 Element 软件的存储集群上的卷，其中包含主机管理节点虚拟机的管理节点配置信息，这些信息会在虚拟机生命周期结束后持续存在。如果管理节点丢失，替代管理节点 VM 可以重新连接到丢失的 VM 并恢复其配置数据。

如果在安装或升级期间启用了永久性卷功能，则会自动创建多个卷，并在分配的集群上预先指定 NetApp-HCI-名称 。与任何基于 Element 软件的卷一样，这些卷可以使用 Element 软件 Web UI ，适用于 vCenter Server 的 NetApp Element 插件或 API 进行查看，具体取决于您的首选项和安装。永久性卷必须已启动且正在运行，并与管理节点建立 iSCSI 连接，以维护可用于恢复的当前配置数据。

> 与管理服务关联的永久性卷会在安装或升级期间创建并分配给新帐户。如果您使用的是永久性卷，请勿修改或删除这些卷或其关联帐户。

了解更多信息

- "管理卷"
- "适用于 vCenter Server 的 NetApp Element 插件"
- "SolidFire 和 Element 软件文档中心"

卷访问组

卷访问组是用户可以使用 iSCSI 或光纤通道启动程序访问的一组卷。

通过创建和使用卷访问组，您可以控制对一组卷的访问。将一组卷和一组启动程序与一个卷访问组相关联时，访问组会授予这些启动程序对该组卷的访问权限。

卷访问组具有以下限制：

- 每个卷访问组最多 128 个启动程序。
- 每个卷最多 64 个访问组。
- 一个访问组最多可由 2000 个卷组成。
- IQN 或 WWPN 只能属于一个卷访问组。

了解更多信息

- "管理卷访问组"
- "适用于 vCenter Server 的 NetApp Element 插件"
- "SolidFire 和 Element 软件文档中心"

启动程序

通过启动程序，外部客户端可以访问集群中的卷，从而充当客户端和卷之间通信的入口点。您可以使用启动程序对存储卷进行基于 CHAP 的访问，而不是基于帐户的访问。添加到卷访问组时，单个启动程序允许卷访问组成员访问添加到组中的所有存储卷，而无需身份验证。一个启动程序只能属于一个访问组。

了解更多信息

- "管理启动程序"
- "卷访问组"
- "管理卷访问组"
- "适用于 vCenter Server 的 NetApp Element 插件"
- "SolidFire 和 Element 软件文档中心"

NetApp HCI 许可

使用 NetApp HCI 时，您可能需要其他许可证，具体取决于所使用的内容。

NetApp HCI 和 VMware vSphere 许可

VMware vSphere 许可取决于您的配置：

网络选项	许可
选项 A ： 使用两根缆线连接使用 VLAN 标记的计算节点（所有计算节点）	需要使用 vSphere 分布式交换机，这需要 VMware vSphere Enterprise Plus 许可。
选项 B ： 使用带标记 VLAN 的计算节点（ H410C 2RU 4 节点计算节点）使用六根缆线	此配置使用 vSphere 标准交换机作为默认配置。要选择使用 vSphere 分布式交换机，需要获得 VMware Enterprise Plus 许可。
选项 C ： 为使用原生和标记 VLAN 的计算节点（ H410C ， 2RU 4 节点计算节点）使用六根缆线	此配置使用 vSphere 标准交换机作为默认配置。要选择使用 vSphere 分布式交换机，需要获得 VMware Enterprise Plus 许可。

NetApp HCI 和 ONTAP Select 许可

如果您获得的 ONTAP Select 版本可与购买的 NetApp HCI 系统结合使用，则需遵守以下附加限制：

- ONTAP Select 许可证与 NetApp HCI 系统销售捆绑在一起，只能与 NetApp HCI 计算节点结合使用。
- 这些 ONTAP Select 实例的存储只能位于 NetApp HCI 存储节点上。
- 禁止使用第三方计算节点或第三方存储节点。

了解更多信息

- "适用于 vCenter Server 的 NetApp Element 插件"
- "SolidFire 和 Element 软件文档中心"

NetApp Hybrid Cloud Control 配置上限

NetApp HCI 包含 NetApp 混合云控制功能，可简化计算生命周期和存储管理。它支持在 NetApp HCI 和 NetApp SolidFire 存储集群的存储节点上升级 Element 软件，以及在 NetApp HCI 中升级 NetApp HCI 计算节点的固件。默认情况下，此选项在 NetApp HCI 的管理节点上可用。

除了在 NetApp HCI 安装中传达 NetApp 提供的硬件和软件组件之外， NetApp 混合云控制还与客户环境中的第三方组件（例如 VMware vCenter ）进行交互。NetApp 对 NetApp Hybrid Cloud Control 的功能及其在客户环境中与这些第三方组件的交互进行了限定，并可达到一定的规模。为了获得 NetApp Hybrid Cloud Control 的最佳使用体验， NetApp 建议保持在配置上限范围内。

如果超过这些测试上限，则可能会遇到 NetApp Hybrid Cloud Control 问题，例如用户界面速度较慢， API 响应或功能不可用。如果您在配置超出配置上限的环境中联系 NetApp 为 NetApp 提供 NetApp Hybrid Cloud Control 的产品支持， NetApp 支持部门会要求您将配置更改为记录的配置上限以内。

配置最大值

NetApp混合云控制支持包含多达100个ESXi主机和1000个虚拟机的VMware vSphere环境(相当于小型vCenter Server设备配置)。

NetApp HCI 安全性

使用 NetApp HCI 时，您的数据会受到行业标准安全协议的保护。

存储节点的空闲加密

使用 NetApp HCI 可以对存储集群上存储的所有数据进行加密。

存储节点中支持加密的所有驱动器都在驱动器级别使用 AES 256 位加密。每个驱动器都有自己的加密密钥，该密钥是在首次初始化驱动器时创建的。启用加密功能后，系统将创建一个存储集群范围的密码，然后将该密码块分发到集群中的所有节点。没有一个节点存储整个密码。然后，使用此密码对所有驱动器访问进行密码保护。您需要使用密码来解锁驱动器，由于驱动器正在对所有数据进行加密，因此您的数据始终是安全的。

启用空闲加密后，存储集群的性能和效率不受影响。此外，如果使用 Element API 或 Element UI 从存储集群中删除启用了加密的驱动器或节点，则驱动器上会禁用空闲加密，并且驱动器会安全擦除，从而保护先前存储在这些驱动器上的数据。删除驱动器后、您可以使用API方法安全地擦除此驱动器 `SecureEraseDrives`。如果您强制从存储集群中删除某个驱动器或节点，则数据仍受集群范围密码和驱动器的各个加密密钥的保护。

有关启用和禁用空闲加密的信息、请参见 "为集群启用和禁用加密"SolidFire和Element文档中心中的。

空闲软件加密

通过软件空闲加密，可以对写入存储集群中 SSD 的所有数据进行加密。这样可以在 SolidFire 企业 SDS 节点中提供一个主加密层，其中不包括自加密驱动器（ SED ）。

外部密钥管理

您可以将 Element 软件配置为使用符合 KMIP 的第三方密钥管理服务（ Key Management Service ， KMS ）来管理存储集群加密密钥。启用此功能后，存储集群的集群范围驱动器访问密码加密密钥将由您指定的 KMS 管理。Element 可以使用以下密钥管理服务：

- Gemalto SafeNet KeySecure
- KeySecure 上的 SafeNet
- HyTrust KeyControl
- Vormetric Data Security Manager
- IBM 安全密钥生命周期管理器

有关配置外部密钥管理的详细信息、请参见 "外部密钥管理入门"SolidFire和Element文档中心中的。

多因素身份验证

通过多因素身份验证（ Multi-Factor Authentication ， MFA ），您可以要求用户在登录时提供多种类型的证据，以便通过 NetApp Element Web UI 或存储节点 UI 进行身份验证。您可以将 Element 配置为仅接受与现有用户管理系统和身份提供程序集成的登录的多因素身份验证。您可以将 Element 配置为与现有 SAML 2.0 身份提供程序集成，此身份提供程序可强制实施多种身份验证方案，例如密码和文本消息，密码和电子邮件消息或其他方法。

您可以将多因素身份验证与通用 SAML 2.0 兼容身份提供程序（ IdP ）配对，例如 Microsoft Active Directory 联合身份验证服务（ Active Directory Federation Services ， ADFS ）和 Shibboleth 。

要配置MFA、请参见 "启用多因素身份验证"SolidFire和Element文档中心中的。

用于 **HTTPS** 和空闲数据加密的 **FIPS 140-2**

NetApp SolidFire 存储集群和 NetApp HCI 系统支持符合联邦信息处理标准（ FIPS ） 140-2 加密模块要求的加密。您可以在 NetApp HCI 或 SolidFire 集群上为 HTTPS 通信和驱动器加密启用 FIPS 140-2 合规性。

在集群上启用 FIPS 140-2 操作模式后，集群将激活 NetApp 加密安全模块（ NetApp Cryptographic Security Module ， NCSM ），并利用 FIPS 140-2 1 级认证加密通过 HTTPS 与 NetApp Element UI 和 API 进行所有通信。您可以将Element API与参数结合 `fips`使用 `EnableFeature`来启用`FIPS 140-2 HTTPS`加密。在使用`FIPS`兼容硬件的存储集群上、您还可以使用`Element API`和 `FipsDrives`参数为空闲数据启用`FIPS`驱动器加密 `EnableFeature`。

有关为FIPS 140-2加密准备新存储集群的详细信息，请参见 "创建支持 FIPS 驱动器的集群"。

有关在已准备好的现有集群上启用FIPS 140-2的详细信息，请参见 "EnableFeature Element API"。

性能和服务质量

SolidFire 存储集群能够按卷提供服务质量（ QoS ）参数。您可以使用以下三个可配置参数来定义 QoS ，以保证集群性能（以每秒输入和输出数（ IOPS ）为单位）：最小 IOPS ，最大 IOPS 和突发 IOPS 。

SolidFire Active IQ 提供了一个 QoS 建议页面，可提供有关最佳配置和设置 QoS 设置的建议。

服务质量参数

IOPS 参数的定义方式如下：

- * 最小 IOPS* —存储集群为卷提供的最小可持续每秒输入输出数（ IOPS ）。为卷配置的最小 IOPS 是卷性能的保证级别。性能不会低于此级别。
- * 最大 IOPS* —存储集群为卷提供的最大可持续 IOPS 。如果集群 IOPS 级别非常高，则不会超过此 IOPS 性能级别。
- * 突发 IOPS* —在短时突发情况下允许的最大 IOPS 数。如果卷运行的 IOPS 低于最大 IOPS ，则会累积突发额度。如果性能级别变得非常高并被推送到最大级别，则允许在卷上短时突发 IOPS 。

  当集群在集群 IOPS 利用率较低的状态下运行时， Element 软件将使用突发 IOPS 。

  单个卷可以累积突发IOPS、并使用这些额度在设置的"突发期间"突发IOPS、使其高于其最大IOPS、直至达到突发IOPS级别。如果集群具有容纳此突发的容量，则卷的突发时间可长达 60 秒。卷在其最大 IOPS 限制下运行的每秒累积一秒突发额度（最多 60 秒）。

  突发 IOPS 有两种限制：

  - 卷可以在数秒内突发超过其最大 IOPS ，该秒数等于卷累积的突发额度数。

- 当卷突发到其最大 IOPS 设置以上时，它将受到其突发 IOPS 设置的限制。因此，突发 IOPS 不会超过卷的突发 IOPS 设置。

- * 有效最大带宽 * —最大带宽是通过将 IOPS 数（基于 QoS 曲线）乘以 IO 大小计算得出的。

  示例： 100 min IOPS ， 1000 Max IOPS 和 1500 Burst IOPS 的 QoS 参数设置会对性能质量产生以下影响：

  - 工作负载可以达到并保持最大 IOPS 1000 ，直到集群上明显出现工作负载争用 IOPS 的情况为止。然后， IOPS 会逐渐减少，直到所有卷上的 IOPS 都在指定的 QoS 范围内，并缓解对性能的争用。
  - 所有卷上的性能都将推向最小 IOPS 100 。此级别不会低于最小 IOPS 设置，但在缓解工作负载争用后，此级别仍可能高于 100 IOPS 。
  - 在一段持续时间内，性能不会超过 1000 IOPS 或低于 100 IOPS 。允许性能达到 1500 IOPS （突发 IOPS ），但仅适用于通过低于最大 IOPS 而累积突发额度的卷，并且仅允许短时间内运行。突发级别永远不会持续。

QoS 值限制

下面列出了 QoS 的可能最小值和最大值。

参数	最小值	默认	**4 4 KB**	**5 8 KB**	**6 16 KB**	**262 KB**
最小 IOPS	50	50	15,000	9,375*	5556 *	385 *
最大 IOPS	100	15,000	20 万 *	125,000	74,074	5128
突发 IOPS	100	15,000	20 万 *	125,000	74.074	5128

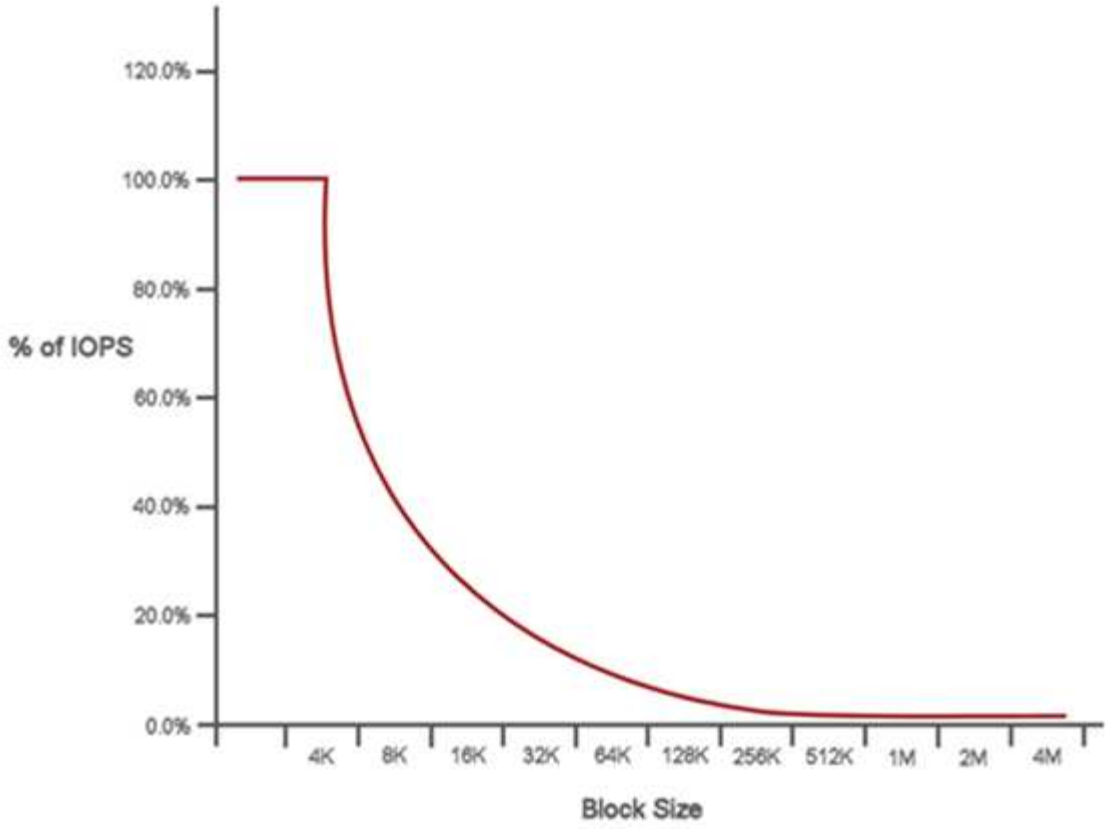
- 这些估计值为近似值。"Max IOPS" 和 "Burst IOPS" 可以设置为高达 200 ， 000 ；但是，只有在有效地取消卷性能上限时，才允许使用此设置。卷的实际最高性能受集群使用情况和每个节点性能的限制。

QoS 性能

QoS 性能曲线显示了块大小与 IOPS 百分比之间的关系。

块大小和带宽会直接影响应用程序可获取的 IOPS 数量。Element 软件会将所接收的块大小规范化为 4k ，从而将其考虑在内。根据工作负载，系统可能会增加块大小。随着块大小的增加，系统会将带宽增加到处理较大块大小所需的级别。随着带宽的增加，系统能够达到的 IOPS 数量也会减少。

QoS 性能曲线显示了块大小增加与 IOPS 百分比降低之间的关系：



例如，如果块大小为 4 k ，带宽为 4000 KBps ，则 IOPS 为 1000 。如果块大小增加到 8k ，则带宽将增加到 5000 KBps ，而 IOPS 将减少到 625 。通过考虑块大小，系统可确保使用较高块大小的较低优先级工作负载（例如备份和虚拟机管理程序活动）不会占用较小块大小的较高优先级流量所需的太多性能。

QoS 策略

通过 QoS 策略，您可以创建并保存可应用于多个卷的标准化服务质量设置。

QoS 策略最适合服务环境，例如数据库，应用程序或基础架构服务器，这些服务器很少重新启动，需要对存储的持续等量访问。单个卷 QoS 最适合日常或每天多次重新启动，启动或关闭的轻型 VM ，例如虚拟桌面或专用自助服务终端类型的 VM 。

QoS 和 QoS 策略不应一起使用。如果使用的是 QoS 策略，请勿对卷使用自定义 QoS 。自定义 QoS 将覆盖和调整卷 QoS 设置的 QoS 策略值。

要使用 QoS 策略，选定集群必须为 Element 10.0 或更高版本；否则， QoS 策略功能将不可用。

了解更多信息

- "适用于 vCenter Server 的 NetApp Element 插件"
- "NetApp HCI 资源页面"