



采用Cloud Volumes ONTAP for Epic 的FlexPod 混合云 FlexPod

NetApp
March 13, 2026

目录

采用Cloud Volumes ONTAP for Epic的FlexPod 混合云	1
TR-4960: 《FlexPod 混合云与适用于Epic的Cloud Volumes ONTAP 》	1
audience	2
解决方案的优势	2
解决方案 拓扑	3
解决方案组件	3
FlexPod	3
EHR	4
NetApp Console	4
控制台代理	4
NetApp Cloud Volumes ONTAP	5
NetApp Active IQ Unified Manager	5
Cisco Intersight	5
VMware vSphere 7.0	6
VMware vCenter Server	6
硬件和软件版本	6
安装和配置	7
NetApp Cloud Volumes ONTAP 部署	7
内部FlexPod 部署	8
内部ONTAP 存储配置	8
将本地FlexPod存储添加到NetApp Console	10
SAN 配置	11
NetApp主机实用程序套件	11
发现ONTAP 存储	11
配置多路径	12
创建物理卷	13
创建卷组	13
创建逻辑卷	14
创建文件系统	14
创建要挂载的文件夹	15
挂载文件系统	15
数据生成	15
在内部ONTAP 和Cloud Volumes ONTAP 之间配置SnapMirror复制	16
解决方案验证	17
应用程序开发和测试(开发/测试)	17
灾难恢复	20
验证生产站点上的数据	23
结论	25
从何处查找追加信息	25

采用Cloud Volumes ONTAP for Epic的FlexPod 混合云

TR-4960: 《FlexPod 混合云与适用于Epic的Cloud Volumes ONTAP》



与以下合作伙伴:

NetApp公司Kamini Singh

实现数字化转型的关键在于利用数据完成更多工作。医院需要生成大量数据、才能有效地运营组织并为患者提供服务。在治疗患者以及管理员工计划和医疗资源时、系统会收集和 处理相关信息。

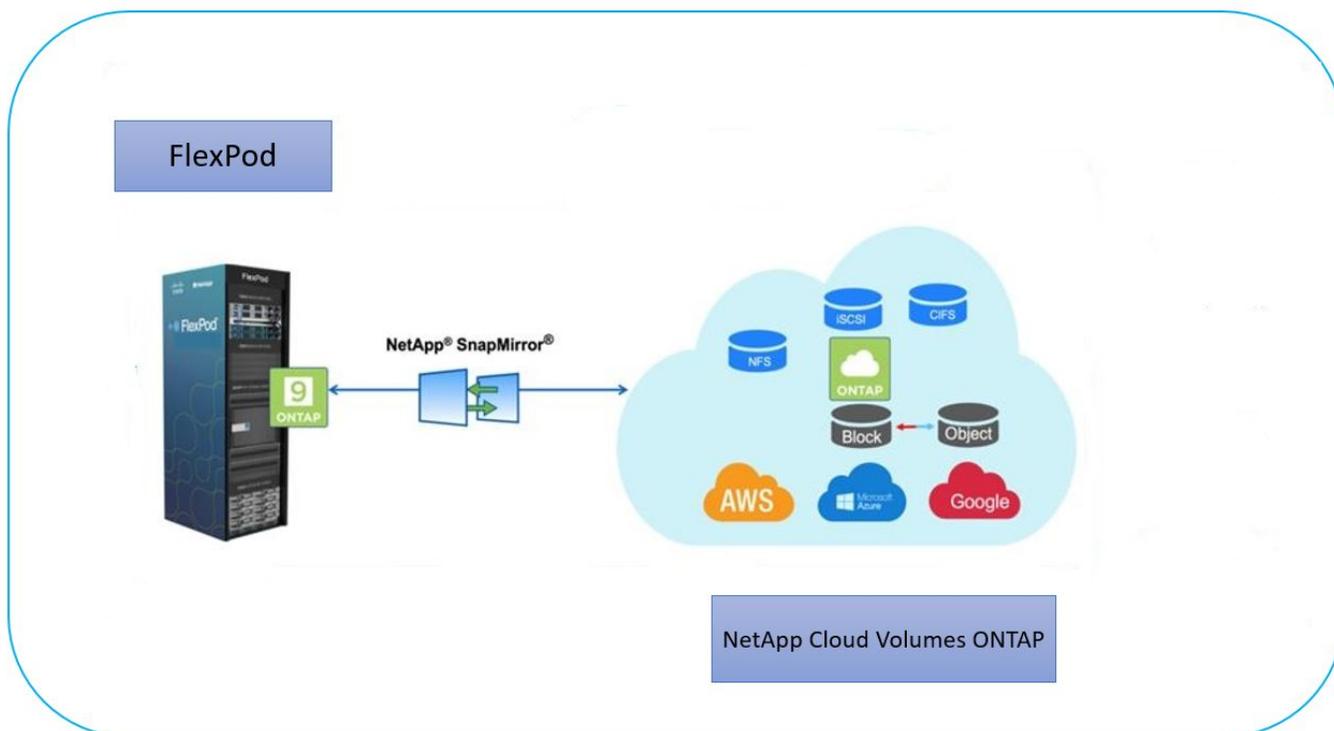
医疗保健数据的规模不断扩大、而且这些数据可以提供宝贵的洞察力、这使得医疗保健数据服务和数据保护变得既重要又具有挑战性。首先、医疗保健数据必须可用且受到保护、才能满足数据恢复、医疗业务连续性或合规性要求。

第二、必须随时提供医疗保健数据以供分析。这种分析通常采用基于人工智能(AI)和机器学习(ML)的方法来帮助 医疗企业改进其解决方案并创造业务价值。

第三、随着医疗业务的增长、数据服务基础架构和数据保护方法必须适应医疗保健数据的增长。此外、由于需要 将数据从创建数据的边缘移动到核心和云、以便使用数据分析或归档所需的资源、数据移动性变得越来越重要。

NetApp为包括医疗保健在内的企业级应用程序提供了一个数据管理解决方案、我们可以指导医院完成数字化转 型之旅。NetApp Cloud Volumes ONTAP 提供了用于医疗保健数据管理的解决方案、可将数据从FlexPod 数据 中心高效复制到AWS等公共云上部署的Cloud Volumes ONTAP。

通过利用经济高效且安全的公共云资源、Cloud Volumes ONTAP 通过高效的数据复制、内置存储效率和简单的 灾难恢复测试增强了基于云的灾难恢复(Disaster Recovery、DR)。这些系统采用统一的控制和简单的拖放操作 进行管理、可提供经济高效的保护、防止出现任何类型的错误、故障或灾难。Cloud Volumes ONTAP 提供 了NetApp SnapMirror技术作为块级数据复制的解决方案、可通过增量更新使目标保持最新。



audience

本文档面向NetApp和合作伙伴解决方案工程师(SE)以及专业服务人员。NetApp假定读者具备以下背景知识：

- 深入了解SAN和NAS概念
- 熟悉NetApp ONTAP 存储系统的技术知识
- 熟悉ONTAP 软件的配置和管理技术

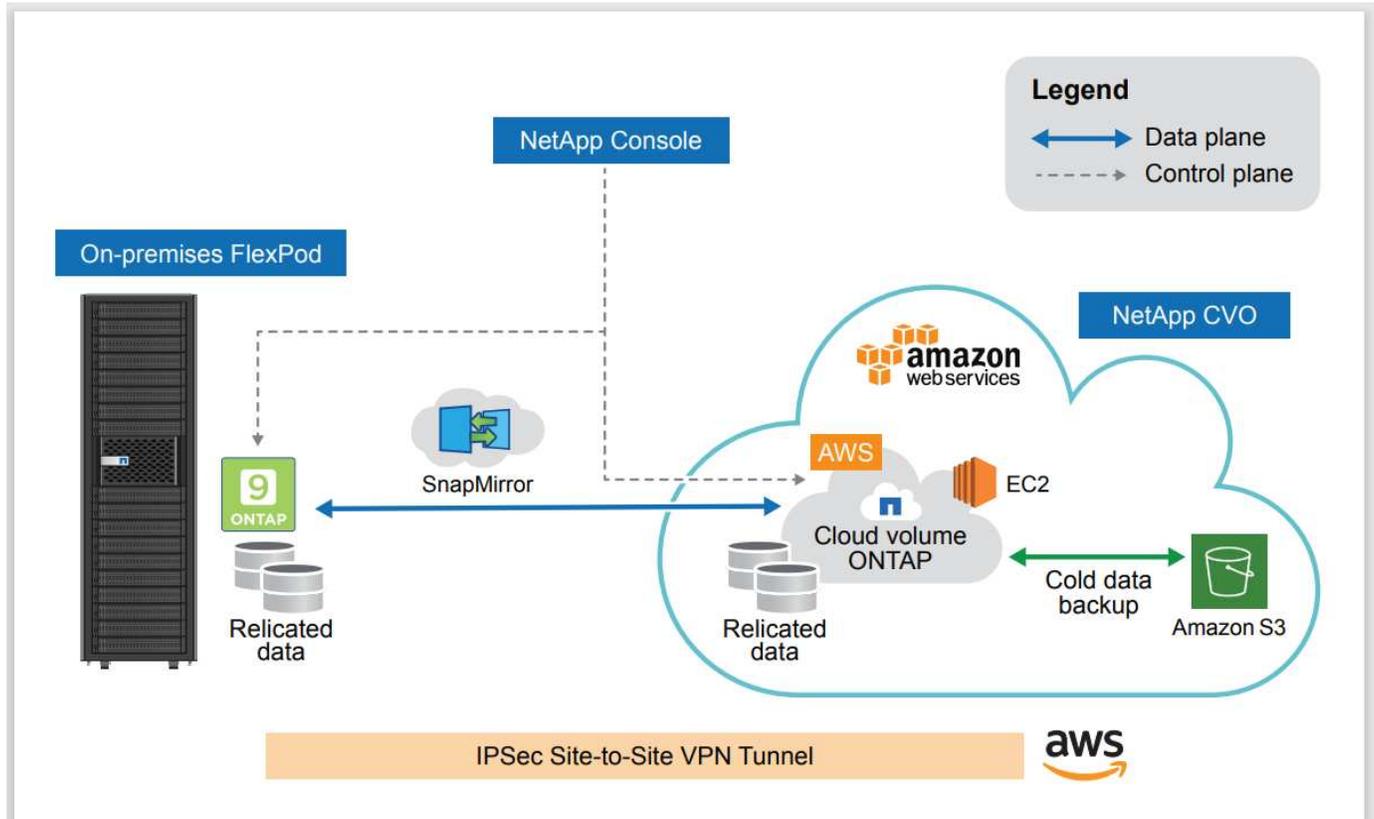
解决方案的优势

与NetApp Cloud Volumes ONTAP 集成的FlexPod 数据中心为医疗保健工作负载提供了以下优势：

- 自定义保护。 Cloud Volumes ONTAP 提供从ONTAP 到云的块级数据复制、通过增量更新使目标保持最新。用户可以指定同步计划来确定何时传输源上的更改。这样可以为各种医疗保健数据提供自定义保护。
- *故障转移和故障恢复。*发生灾难时、存储管理员可以快速为云卷设置故障转移。恢复主站点后、在灾难恢复环境中创建的新数据将同步回源卷、以便重新建立二级数据复制。这样、医疗保健数据便可轻松恢复、而不会造成中断。
- *效率。*二级云副本的存储空间和成本通过数据压缩、精简配置和重复数据删除进行了优化。医疗保健数据以经过压缩和重复数据删除的形式在块级别传输、从而加快传输速度。数据也会自动分层到低成本对象存储、并且只有在访问时才会返回到高性能存储、例如在灾难恢复情形下。这样可以显著降低持续存储成本。
- 勒索软件防护 NetApp Console勒索软件防护功能可扫描本地和云环境中的数据源，检测安全漏洞，并提供其当前的安全状态和风险评分。然后它会提供可操作的建议，您可以进一步调查并遵循这些建议进行补救。这可以帮助您保护关键的医疗保健数据免受勒索软件攻击。

解决方案 拓扑

本节描述解决方案的逻辑拓扑结构。下图表示由FlexPod本地环境、运行在 Amazon Web Services (AWS) 上的NetApp Cloud Volumes ONTAP (CVO) 和NetApp Console SaaS 平台组成的解决方案拓扑。



控制平面和数据平面会在端点之间清晰地指示。通过利用安全的站点到站点VPN连接、数据平面在FlexPod 的纯闪存FAS 上运行的ONTAP 实例与AWS中的NetApp CVO实例之间运行。将医疗保健工作负载数据从内部FlexPod 数据中心复制到NetApp Cloud Volumes ONTAP 时、会通过NetApp SnapMirror复制来处理。此外、此解决方案 还支持将NetApp CVO实例中的冷数据备份和分层到AWS S3。

"接下来：解决方案 组件。"

解决方案组件

"先前版本：解决方案 概述。"

FlexPod

FlexPod 是一组定义的硬件和软件、可为虚拟化和非虚拟化解决方案奠定集成基础。FlexPod 包括NetApp ONTAP 存储、Cisco Nexus网络、Cisco MDS存储网络和Cisco统一计算系统(Cisco UCS)。

医疗保健组织正在寻找解决方案、以简化数字化转型并改善患者体验和结果。借助FlexPod、您可以获得一个安全、可扩展的平台、该平台可提高效率、并使员工能够更快地做出更明智的决策、从而为患者提供更好的护理。

FlexPod 是满足医疗保健工作负载需求的理想平台、因为它具有以下优势：

- 优化操作、更快地获得洞察力并获得更好的患者结果。
- 利用可扩展且可靠的基础架构简化映像应用程序。
- 借助经验证的方法快速高效地部署特定于医疗保健的应用程序、例如EHR。

EHR

电子健康记录(Electronic Health Records、EHRs)为大中型医疗团队、医院和综合医疗保健组织提供软件。客户还包括社区医院、学术机构、儿童组织、安全网络提供商和多医院系统。EHR集成软件涵盖临床、访问和收入功能、并扩展到家庭。

医疗保健提供商组织仍然面临着最大程度地发挥其在行业领先的EHRs上的巨大投资优势的压力。客户在为EHR解决方案和任务关键型应用程序设计数据中心时、通常会为其数据中心架构确定以下目标：

- EHR应用程序的高可用性
- 高性能
- 在数据中心轻松实施EHR
- 灵活性和可扩展性、支持通过新的EHR版本或应用程序实现增长
- 成本效益
- 易管理性，稳定性和易支持性
- 强大的数据保护，备份，恢复和业务连续性

FlexPod已获得 EHR 认证，并支持包含Cisco UCS、Intel Xeon 处理器、Red Hat Enterprise Linux (RHEL) 和 VMware ESXiCisco化的平台。该平台，加上 EHR 对运行ONTAP的NetApp存储的高舒适度评级，使您能够通过FlexPod在完全托管的私有云中运行您的医疗保健应用程序，该私有云还可以连接到任何公共云提供商。

NetApp Console

NetApp Console是一个企业级的、基于 SaaS 的管理平台，它使 IT 专家和云架构师能够使用NetApp云解决方案集中管理其混合多云基础架构。它提供了一个集中式系统，用于查看和管理您的本地和云存储，支持混合云、多云提供商和帐户。有关详细信息，请参阅 "[NetApp Console文档](#)"。

控制台代理

控制台代理实例使控制台能够管理公有云环境中的资源和进程。控制台提供的许多功能都需要控制台代理，它可以部署在云端或本地网络中。

控制台代理在以下位置受支持：

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- 内部部署

["了解有关控制台代理的更多信息"](#)。

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP 是一款软件定义的存储产品、可在云中运行ONTAP 数据管理软件、为文件和块工作负载提供高级数据管理。借助Cloud Volumes ONTAP 、您可以优化云存储成本并提高应用程序性能、同时增强数据保护、安全性和合规性。

主要优势包括：

- **存储效率。** *利用内置的重复数据删除、数据压缩、精简配置和即时克隆功能最大限度地降低存储成本。
- **高可用性。** *在云环境发生故障时提供企业级可靠性和持续运营。
- **数据保护。** Cloud Volumes ONTAP 使用行业领先的NetApp复制技术SnapMirror将内部数据复制到云、以便可以轻松地为多种使用情形提供二级副本。Cloud Volumes ONTAP 还与云备份相集成、提供备份和还原功能、以保护云数据并对其进行长期归档。
- **数据分层。** *按需在高性能和低性能存储池之间切换、而无需使应用程序脱机。
- **应用程序一致性。** *使用NetApp SnapCenter 技术提供NetApp Snapshot副本的一致性。
- **数据安全。** Cloud Volumes ONTAP 支持数据加密、并提供防病毒和勒索软件保护。
- **隐私合规性控制。** *与Cloud Data sense集成有助于您了解数据环境并识别敏感数据。

更多详细信息，请参阅["Cloud Volumes ONTAP"](#)。

NetApp Active IQ Unified Manager

借助NetApp Active IQ Unified Manager 、您可以通过一个经过重新设计的直观界面监控ONTAP 存储集群、从而利用社区智慧和AI分析提供智能。它可以全面洞察存储环境及其运行的虚拟机的运行状况、性能和主动性。当存储基础架构发生问题描述 时、Unified Manager可以通知您问题描述 的详细信息、以帮助识别根发生原因。通过虚拟机信息板、您可以查看虚拟机的性能统计信息、以便调查从vSphere主机向下经过网络并最终到达存储的整个I/O路径。

某些事件还提供了可用于更正问题描述 的补救措施。您可以为事件配置自定义警报、以便在发生问题时、通过电子邮件和SNMP陷阱通知您。通过Active IQ Unified Manager 、您可以通过预测容量和使用趋势来规划用户的存储需求、以便在出现问题之前采取行动、防止做出长期可能导致其他问题的被动短期决策。

有关详细信息，请参阅 ["Active IQ Unified Manager"](#)。

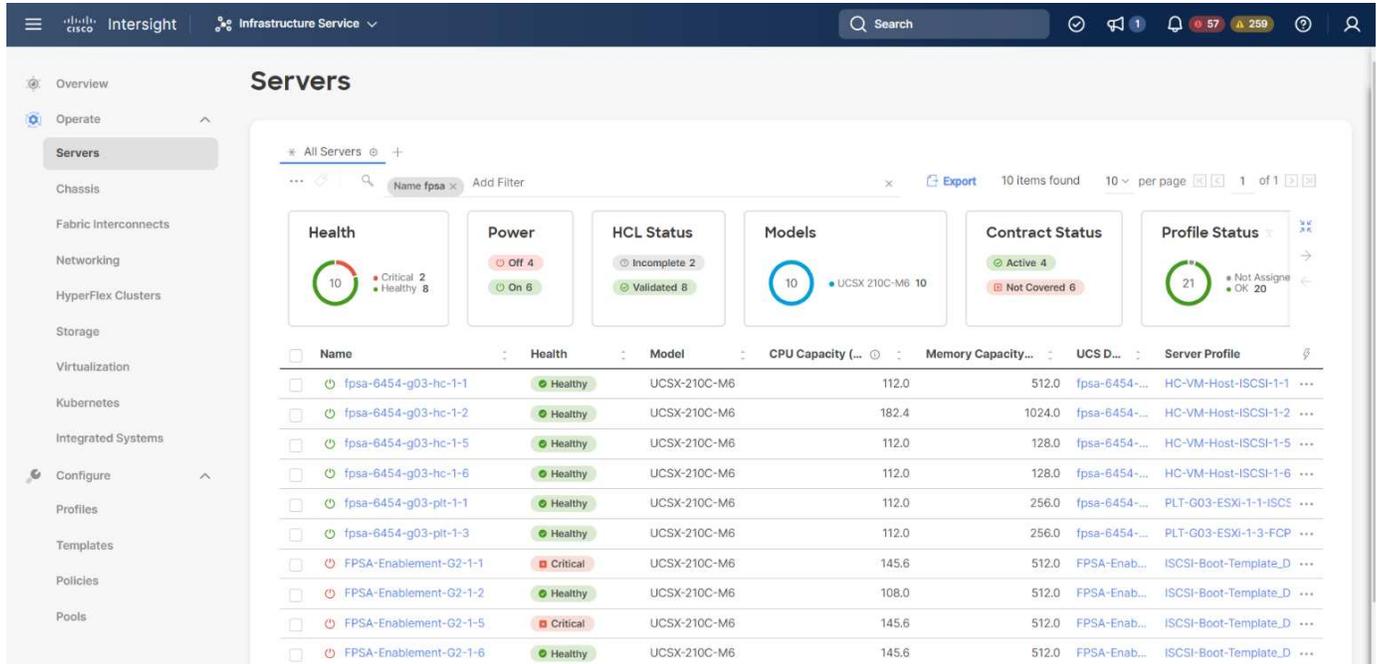
Cisco Intersight

Cisco Intersight是一个SaaS平台、可为传统和云原生应用程序和基础架构提供智能自动化、可观察性和优化功能。该平台有助于推动IT团队的变革、并提供专为混合云设计的运营模式。Cisco Intersight具有以下优势：

- **更快的交付速度。** Intersight通过基于敏捷性的软件开发模式、以云或客户数据中心的服务形式提供、并经常进行更新和持续创新。这样、客户就可以专注于满足关键业务需求。
- **简化操作。** Intersight使用一个安全的SaaS交付工具、该工具具有通用清单、身份验证和API、可在整个堆栈和所有位置运行、从而简化操作、消除团队之间的孤岛。这样、您就可以管理内部、VM、K8s、无服务器、自动化、在内部和公共云中实现优化并控制成本。
- **持续优化。** *您可以利用Cisco Intersight在每一层提供的智能以及Cisco TAC提供的智能来持续优化您的环境。这种智能将转换为建议的可自动化操作、以便您可以实时适应任何变化：从移动工作负载和监控物理服务器的运行状况到为您使用的公共云提供成本降低建议。

Cisco Intersight支持两种管理操作模式：UCSM受管模式(Umm)和Intersight受管模式(IMM)。在初始设置互联阵

列期间、您可以为光纤连接的Cisco UCS系统选择本机UCSM受管模式(Umm)或视间受管模式(IMM)。在此解决方案中、使用原生 IMM。下图显示了Cisco Intersight信息板。



VMware vSphere 7.0

VMware vSphere是一个虚拟化平台、可将大量基础架构(包括CPU、存储和网络)作为一个无缝、多功能且动态的操作环境进行全面管理。与管理单个计算机的传统操作系统不同、VMware vSphere可将整个数据中心的基础架构聚合在一起、从而创建一个具有资源的动力中心、这些资源可以快速动态地分配给任何需要的应用程序。

有关 VMware vSphere 及其组件的更多信息，请参阅["VMware vSphere"](#)。

VMware vCenter Server

VMware vCenter Server可通过一个控制台统一管理所有主机和VM、并对集群、主机和VM进行聚合性能监控。通过VMware vCenter Server、管理员可以深入了解计算集群、主机、虚拟机、存储、子操作系统、虚拟基础架构的其他关键组件。VMware vCenter可管理VMware vSphere环境中提供的丰富功能。

详细信息请参见["VMware vCenter"](#)。

硬件和软件版本

这种混合云解决方案可以扩展到任何运行受支持版本的软件、固件和硬件的FlexPod环境，具体定义见：["NetApp 互操作性表工具"](#)，["UCS硬件和软件兼容性"](#)，和["VMware 兼容性指南"](#)。

下表显示了内部FlexPod 硬件和软件版本。

组件	产品	version
计算	Cisco UCS X210c M6	5.0 (1b)
	Cisco UCS互联阵列6454	4.2 (2a)
网络	Cisco Nexus 9336C-x2 NX-OS	9.3 (9)

组件	产品	version
存储	NetApp AFF A400	ONTAP 9.11.1P2
	适用于 VMware vSphere 的 NetApp ONTAP 工具	9.11
	适用于 VMware VAAI 的 NetApp NFS 插件	2.0
	NetApp Active IQ Unified Manager	9.11P1
软件	VMware vSphere	7.0 (U3)
	VMware ESXi nenic 以太网驱动程序	1.0.35.0
	VMware vCenter设备	7.0.3
	Cisco Intersight Assist虚拟设备	1.0.9-342

下表显示了控制台和Cloud Volumes ONTAP版本。

供应商	产品	version
NetApp	控制台	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"[下一步：安装和配置。](#)"

安装和配置

"[先前版本：解决方案 组件。](#)"

NetApp Cloud Volumes ONTAP 部署

完成以下步骤以配置Cloud Volumes ONTAP 实例：

1. 准备公共云服务提供商环境。

您必须捕获解决方案 配置的公共云服务提供商的环境详细信息。例如、对于Amazon Web Services (AWS) 环境准备、您需要AWS访问密钥、AWS机密密钥以及区域、VPC、子网等其他网络详细信息。

2. 配置VPC端点网关。

要启用VPC与AWS S3服务之间的连接、需要使用VPC端点网关。此操作用于在CVO上启用备份、CVO是网关类型的端点。

3. 访问NetApp Console。

要访问控制台和其他云服务，您需要注册。 "[NetApp Console](#)"。有关在控制台帐户中设置工作区和用户的信息，请参阅 "[NetApp Console设置和管理](#)"。您需要一个具有权限的帐户，才能直接从控制台在您的云提供商处部署控制台代理。要获取所需的权限，请参阅 "[NetApp Console的权限摘要](#)"。

4. 部署控制台代理。

在添加 Cloud Volume ONTAP系统之前，必须先部署控制台代理。如果您尝试在没有安装控制台代理的情况下创建第一个Cloud Volumes ONTAP系统，控制台会提示您。要从控制台在 AWS 中部署控制台代理，请参阅以下内容：["AWS 中的控制台代理安装选项"](#)。

5. 在AWS中启动Cloud Volumes ONTAP。

您可以在单系统配置中或在 AWS 中作为 HA 对启动 Cloud Volumes ONTAP 。["阅读分步说明"](#)。

有关这些步骤的详细信息、请参见 ["AWS中的Cloud Volumes ONTAP 快速入门指南"](#)。

在这个解决方案中，我们在 AWS 上部署了一个单节点Cloud Volumes ONTAP系统。

内部FlexPod 部署

要了解采用UCS X系列的FlexPod 、VMware和NetApp ONTAP 的设计详细信息、请参见 ["采用Cisco UCS X系列的FlexPod 数据中心"](#) 设计指南。本文档提供了在FlexPod 数据中心基础架构中整合Cisco Intersight-managed UCS X系列平台的设计指导。

有关部署内部FlexPod 实例的信息、请参见 ["本部署指南"](#)。

本文档提供了在FlexPod 数据中心基础架构中整合Cisco Intersight-managed UCS X系列平台的部署指导。本文档介绍了成功部署的配置和最佳实践。

FlexPod 既可以部署在UCS托管模式下、也可以部署在Cisco Intersight托管模式(IMM)下。如果要在UCS托管模式下部署FlexPod 、请参见此内容 ["设计指南"](#) 这是 ["部署指南"](#)。

使用Ansible可以通过基础架构作为代码自动部署FlexPod。下面是用于端到端FlexPod 部署的GitHub存储库的链接：

- 可以看到在UCS托管模式、NetApp ONTAP 和VMware vSphere下使用Cisco UCS的FlexPod 的可识别配置 ["此处"](#)。
- 可以看到在IMM、NetApp ONTAP 和VMware vSphere中使用Cisco UCS的FlexPod 的可识别配置 ["此处"](#)。

内部ONTAP 存储配置

本节介绍特定于此解决方案 的一些重要ONTAP 配置步骤。

1. 在运行iSCSI服务的情况下配置SVM。

```
1. vservers create -vservers Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security
-style unix
2. vservers add-protocols -vservers Healthcare_SVM -protocols iscsi
3. vservers iscsi create -vservers Healthcare_SVM
```

To verify:

```
A400-G0312::> vservers iscsi show -vservers Healthcare_SVM
Vserver: Healthcare_SVM
Target Name:
iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
Target Alias: Healthcare_SVM
Administrative Status: up
```

如果在集群配置期间未安装iSCSI许可证、请确保在创建iSCSI服务之前安装此许可证。

2. 创建FlexVol 卷。

```
1. volume create -vservers Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. 添加用于iSCSI访问的接口。

```
1. network interface create -vservers Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vservers Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
3. network interface create -vservers Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
4. network interface create -vservers Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
```

在此解决方案中、我们创建了四个iSCSI逻辑接口(LIF)、每个节点上两个。

在部署了vCenter并向其添加了所有ESXi主机的情况下启动并运行FlexPod 实例后、我们需要部署一个Linux VM、该VM充当连接和访问NetApp ONTAP 存储的服务器。在此解决方案 中、我们已在vCenter中安装CentOS 8实例。

4. 创建LUN。

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1  
-size 200GB -ostype linux -space-reserve disabled
```

对于EHR操作数据库(ODB)、日志和应用程序工作负载、EHR建议将存储作为iSCSI LUN提供给服务器。如果您的AIX和RHEL操作系统版本支持、则NetApp还支持使用FCP和NVMe/FC、从而提高性能。FCP和NVMe/FC可以同时位于同一个网络结构中。

5. 创建igroup。

```
1. igroup create -vserver Healthcare_SVM -igroup ehr -protocol iscsi  
-ostype linux -initiator iqn.1994-05.com.redhat:8e91e9769336
```

igroup用于允许服务器访问LUN。对于Linux主机、可以在文件中找到服务器IQN
/etc/iscsi/initiatorname.iscsi。

6. 将 LUN 映射到 igroup 。

```
1. lun mapping create -vserver Healthcare_SVM -path  
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

将本地FlexPod存储添加到NetApp Console

使用控制台完成以下步骤，将FlexPod存储添加到系统中。

1. 从导航菜单中，选择“存储”>“系统”。
2. 在“系统”页面上，单击“添加系统”，然后选择“本地部署”。
3. 选择*内部部署ONTAP*。单击*下一步*。
4. 在“ONTAP 集群详细信息”页面上，输入管理员用户帐户的集群管理 IP 地址和密码。然后单击*添加*。
5. 在详细信息和凭据页面上、输入工作环境的名称和问题描述、然后单击*执行*。

控制台发现ONTAP集群，并将其作为系统添加到“系统”页面。

有关详细信息、请参见页面 ["发现内部ONTAP 集群"](#)。

["下一步：SAN配置。"](#)

SAN 配置

"先前版本：安装和配置。"

本节介绍EHR为使软件与NetApp存储实现最佳集成而需要的主机端配置。在此部分中、我们将专门讨论Linux操作系统的主机集成。使用 "[NetApp 互操作性表工具 \(IMT\)](#)" 验证所有版本的软件和固件。



以下配置步骤特定于此解决方案 中使用的CentOS 8主机。

NetApp主机实用程序套件

NetApp建议在连接到和访问NetApp存储系统的主机的操作系统上安装NetApp Host Utility Kit (Host Utilities)。支持本机Microsoft多路径I/O (MPIO)。操作系统必须支持多路径的非对称逻辑单元访问(ALUA)。安装Host Utilities 可为NetApp存储配置主机总线适配器(HBA)设置。

可以下载NetApp Host Utilities "[此处](#)"。在此解决方案 中、我们已在主机上安装Linux Host Utilities 7.1。

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-7-1.x86_64.rpm
```

发现ONTAP 存储

确保iSCSI服务在应进行登录时正在运行。要为目标上的特定门户或目标上的所有门户设置登录模式、请使用iscsiadm 命令：

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

现在、您可以使用 `sanlun` 显示有关连接到主机的LUN的信息。确保以root身份登录到主机。

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename adapter protocol size
product
-----
---
Healthcare_SVM                /dev/sdb host33   iSCSI    200g
cDOT
                                /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                /dev/sdc host34   iSCSI    200g
cDOT
                                /vol/hc_iscsi_vol/iscsi_lun1
```

配置多路径

设备映射程序多路径(DM-Multipath)是Linux中的本机多路径实用程序。它可用于实现冗余并提高性能。它可以聚合或组合服务器和存储之间的多个I/O路径、从而在操作系统级别创建一个设备。

1. 在系统上设置DM-Multipath之前、请确保您的系统已更新并包含 device-mapper-multipath 软件包。

```
[root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
device-mapper-multipath-libs-0.8.4-31.el8.x86_64
device-mapper-multipath-0.8.4-31.el8.x86_64
```

2. 配置文件为 /etc/multipath.conf 文件按如下所示更新配置文件。

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
    path_checker      readsector0
    no_path_retry     fail
}
devices {
    device {
        vendor        "NETAPP  "
        product       "LUN.*"
        no_path_retry queue
        path_checker   tur
    }
}
```

3. 启用并启动多路径服务。

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start multipathd.service
```

4. 添加可加载的内核模块 `dm-multipath` 并重新启动多路径服务。最后、检查多路径状态。

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|+- policy='service-time 0' prio=50 status=active
|  `-- 33:0:0:0 sdb 8:16 active ready running
`+- policy='service-time 0' prio=10 status=enabled
  `-- 34:0:0:0 sdc 8:32 active ready running
```



有关这些步骤的详细信息、请参见 ["此处"](#)。

创建物理卷

使用 `pvcreate` 用于初始化块设备以用作物理卷的命令。初始化类似于格式化文件系统。

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

创建卷组

要从一个或多个物理卷创建卷组、请使用 `vgcreate` 命令：此命令将按名称创建一个新卷组、并至少向其中添加一个物理卷。

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

。 `vgdisplay` 命令可用于以固定形式显示卷组属性(例如大小、块区、物理卷数量等)。

```
[root@hc-cloud-secure-1 ~]# vdisplay datavg
--- Volume group ---
VG Name                datavg
System ID
Format                 lvm2
Metadata Areas         1
Metadata Sequence No   1
VG Access              read/write
VG Status              resizable
MAX LV                 0
Cur LV                0
Open LV               0
Max PV                 0
Cur PV                1
Act PV                1
VG Size                <200.00 GiB
PE Size                4.00 MiB
Total PE               51199
Alloc PE / Size        0 / 0
Free PE / Size         51199 / <200.00 GiB
VG UUID                C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

创建逻辑卷

创建逻辑卷时，系统会使用卷组中的物理卷上的可用块区从卷组中划分逻辑卷。

```
[root@hc-cloud-secure-1 ~]# lvcreate -l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

此命令将创建一个名为的逻辑卷 `datalv` 这将使用卷组中的所有未分配空间 `datavg`。

创建文件系统

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv      isize=512    agcount=4, agsize=13106944
blks
        =                          sectsz=4096   attr=2, projid32bit=1
        =                          crc=1       finobt=1, sparse=1, rmapbt=0
        =                          reflink=1   bigtime=0 inobtcount=0
data      =                          bsize=4096  blocks=52427776, imaxpct=25
        =                          sunit=0     swidth=0 blks
naming    =version 2                bsize=4096  ascii-ci=0, ftype=1
log       =internal log             bsize=4096  blocks=25599, version=2
        =                          sectsz=4096  sunit=1 blks, lazy-count=1
realtime  =none                     extsz=4096  blocks=0, rtextents=0
```

创建要挂载的文件夹

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

挂载文件系统

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
```

```
[root@hc-cloud-secure-1 ~]# df -k
```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
devtmpfs	8072804	0	8072804	0%	/dev
tmpfs	8103272	0	8103272	0%	/dev/shm
tmpfs	8103272	9404	8093868	1%	/run
tmpfs	8103272	0	8103272	0%	/sys/fs/cgroup
/dev/mapper/cs-root	45496624	5642104	39854520	13%	/
/dev/sda2	1038336	258712	779624	25%	/boot
/dev/sda1	613184	7416	605768	2%	/boot/efi
tmpfs	1620652	12	1620640	1%	/run/user/42
tmpfs	1620652	0	1620652	0%	/run/user/0
/dev/mapper/datavg-datalv	209608708	1494520	208114188	1%	/file1

有关这些任务的详细信息、请参见页面 ["使用CLI命令管理LVM"](#)。

数据生成

``Dgen.pl`` 是一个用于 EHR I/O 模拟器 (GenerateIO) 的 perl 脚本数据生成器。LUN 内的数据由 EHR 生成。 ``Dgen.pl`` 脚本。该脚本旨在创建与 EHR 数据库中的数据类似的数据。

```

[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                1K-blocks  Used    Available  Use%  Mounted
on
/dev/mapper/datavg-datalv 209608708 178167156 31441552   85%  /file1

```

运行时、Dgen.pl 默认情况下、脚本使用文件系统的85%来生成数据。

在内部ONTAP 和Cloud Volumes ONTAP 之间配置SnapMirror复制

NetApp SnapMirror 可通过 LAN 或 WAN 高速复制数据，从而在虚拟和传统环境中实现高数据可用性和快速数据复制。在将数据复制到 NetApp 存储系统并持续更新二级数据时，您的数据将保持最新，并在需要时保持可用。不需要外部复制服务器。

完成以下步骤以在内部ONTAP 系统和CVO之间配置SnapMirror复制。

1. 从导航菜单中，选择“存储”>“系统”。
2. 在“系统”中，选择包含源卷的系统，将其拖到要将卷复制到的系统，然后选择“复制”。

其余步骤将介绍如何在Cloud Volumes ONTAP 和内部ONTAP 集群之间创建同步关系。

3. *源和目标对等设置。*如果显示此页面、请为集群对等关系选择所有集群间LIF。
4. *源卷选择。*选择要复制的卷。
5. *目标磁盘类型和分层。*如果目标是Cloud Volumes ONTAP 系统、请选择目标磁盘类型、然后选择是否要启用数据分层。
6. *目标卷名称：*指定目标卷名称并选择目标聚合。如果目标是 ONTAP 集群，则还必须指定目标 Storage VM。
7. *最大传输速率。*指定可传输数据的最大速率(以MB/秒为单位)。
8. 复制策略。*选择一个默认策略或单击*其他策略、然后选择一个高级策略。如需帮助， ["了解复制策略"](#)。

9. *计划。*选择一次性副本或重复计划。有多个默认计划可用。如果您需要其他计划、则必须在上创建新计划 destination cluster 使用 System Manager。

10. 查看。*查看您选择的内容、然后单击*执行。

有关这些配置步骤的详细信息、请参见 ["此处"](#)。

控制台启动数据复制过程。在此阶段，您可以看到在本地ONTAP系统和Cloud Volumes ONTAP之间建立的复制服务。

在Cloud Volumes ONTAP 集群中、您可以看到新创建的卷。

您还可以验证是否已在内部卷和云卷之间建立SnapMirror关系。

有关复制任务的详细信息、请参见*复制*选项卡。

["接下来：解决方案验证。"](#)

解决方案验证

["先前版本：SAN配置。"](#)

在本节中、我们将介绍一些解决方案 使用情形。

- SnapMirror的主要使用情形之一是数据备份。通过将数据复制到同一集群或远程目标、可以将SnapMirror用作主备份工具。
- 使用灾难恢复环境运行应用程序开发测试(开发/测试)。
- 灾难恢复。
- 数据分发和远程数据访问。

值得注意的是、此解决方案 中验证的相对较少的使用情形并不代表SnapMirror复制的整个功能。

应用程序开发和测试(开发/测试)

为了加快应用程序开发速度、您可以在灾难恢复站点快速克隆复制的数据并将其用于开发/测试应用程序。灾难恢复和开发/测试环境的主机代管可以显著提高备份或灾难恢复设施的利用率、并且按需开发/测试克隆可以根据需要提供尽可能多的数据副本、以便更快地投入生产。

NetApp FlexClone技术可用于快速创建SnapMirror目标FlexVol 卷的读写副本、以便您可以对二级副本进行读写访问、以确认所有生产数据是否可用。

要使用灾难恢复环境执行应用程序开发/测试、请完成以下步骤：

1. 创建生产数据的副本。为此、请为内部卷执行应用程序快照。应用程序快照创建包括三个步骤： Lock, Snap, 和 Unlock。
 - a. 暂停文件系统、以便暂停I/O并保持应用程序一致性。在步骤C中发出unquiesce命令之前、任何写入文件系统的程序都会保持等待状态步骤a、b和c通过透明的流程或工作流执行、不会影响应用程序SLA。

```
[root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
```

此选项请求在进行新修改时冻结指定的文件系统。任何尝试写入冻结文件系统的进程都会被阻止、直到文件系统被解除冻结为止。

- b. 为内部卷创建快照。

```
A400-G0312::> snapshot create -vserver Healthcare_SVM -volume  
hc_iscsi_vol -snapshot kamini
```

- c. 取消暂停文件系统以重新启动I/O

```
[root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
```

此选项用于取消冻结文件系统并允许操作继续。冻结阻止的任何文件系统修改均不会被阻止、并允许完成。

此外、还可以使用NetApp SnapCenter 执行应用程序一致的快照、NetApp在SnapCenter 中对上述工作流程进行了完整的编排。有关详细信息、请参见 ["此处"](#)。

2. 执行SnapMirror更新操作以使生产系统和灾难恢复系统保持同步。

```
singlecvoaws::> snapmirror update -destination-path  
svm_singlecvoaws:hc_iscsi_vol_copy -source-path  
Healthcare_SVM:hc_iscsi_vol  
  
Operation is queued: snapmirror update of destination  
"svm_singlecvoaws:hc_iscsi_vol_copy".
```

也可以通过NetApp ConsoleGUI 的“复制”选项卡执行SnapMirror更新。

3. 根据先前创建的应用程序快照创建FlexClone实例。

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW  
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy  
-junction-active true -foreground true -parent-snapshot kamini  
  
[Job 996] Job succeeded: Successful
```

对于上一项任务、也可以创建新的快照、但您必须按照上述相同步骤来确保应用程序一致性。

4. 激活FlexClone卷以在云中启动EHR实例。

```

singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver      Path                               Igroup      LUN ID
Protocol
-----
svm_singlecvoaws
                /vol/kamini_clone/iscsi_lun1    ehr-igroup  0    iscsi

```

5. 在云中的EHR实例上执行以下命令以访问数据或文件系统。

a. 发现ONTAP 存储。检查多路径状态。

```

sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/          device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename      adapter protocol size
product
-----
svm_singlecvoaws                      /dev/sda    host2        iSCSI        200g
cDOT
                /vol/kamini_clone/iscsi_lun1

sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running

```

b. 激活卷组。

```

sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active

```

c. 挂载文件系统并显示文件系统信息的摘要。

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used    Available  Use%
Mounted on
/dev/mapper/datavg-datalv 209608708 183987096 25621612   88%
/file1
```

这证明您可以使用灾难恢复环境进行应用程序开发/测试。通过在灾难恢复存储上执行应用程序开发/测试、您可以更多地利用资源、否则这些资源可能会在大部分时间处于闲置状态。

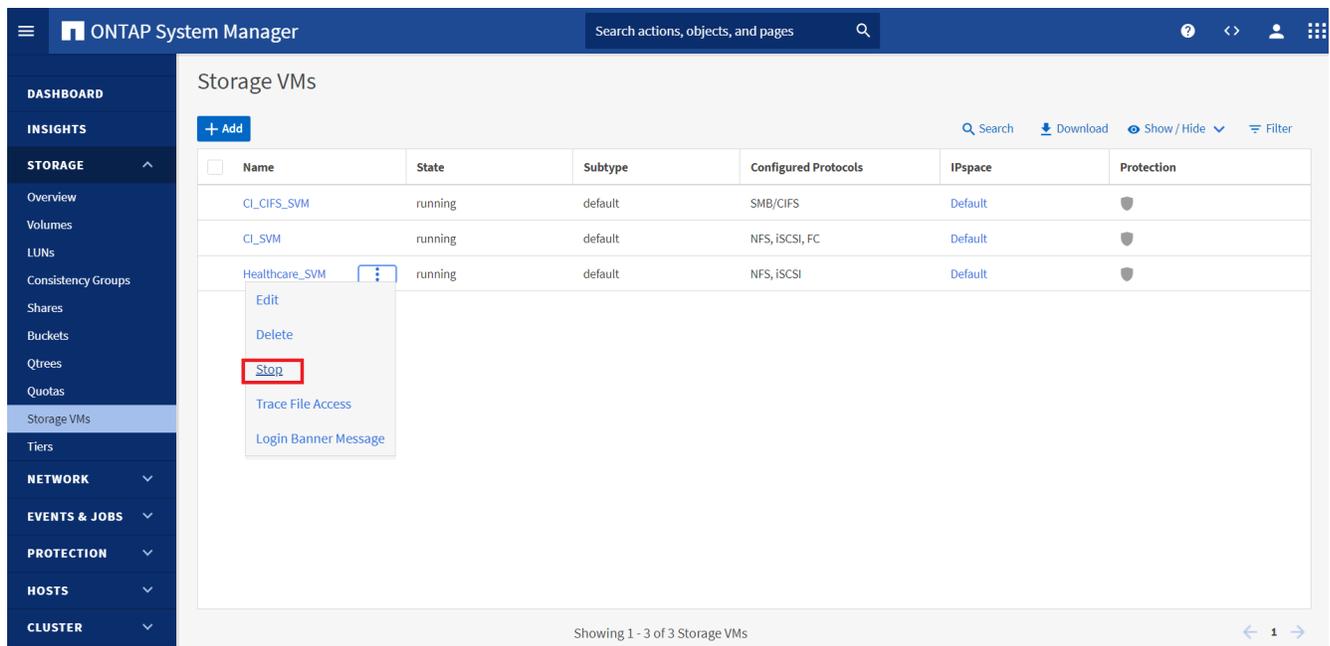
灾难恢复

SnapMirror技术也用作灾难恢复计划的一部分。如果将关键数据复制到其他物理位置、则发生严重灾难时、不必对业务关键型应用程序的数据长时间不可用进行发生原因处理。客户端可以通过网络访问复制的数据、直到生产站点从损坏、意外删除、自然灾害等中恢复为止。

如果要故障恢复到主站点、SnapMirror可提供一种高效的方法来重新同步灾难恢复站点与主站点、只需反转SnapMirror关系、即可仅将更改过的数据或新数据从灾难恢复站点传输回主站点。主生产站点恢复正常应用程序操作后、SnapMirror将继续向灾难恢复站点传输数据、而无需再进行基线传输。

要验证成功的灾难恢复方案、请完成以下步骤：

1. 通过停止托管内部ONTAP 卷的SVM在源(生产)端模拟灾难 (hc_iscsi_vol) 。



The screenshot shows the ONTAP System Manager interface. The main content area displays a table of Storage VMs. The table has columns for Name, State, Subtype, Configured Protocols, IPspace, and Protection. Three rows are visible: CL_CIFS_SVM, CL_SVM, and Healthcare_SVM. A context menu is open over the Healthcare_SVM row, with the 'Stop' option highlighted in red. The left sidebar shows the navigation menu with 'Storage VMs' selected. The top navigation bar includes the ONTAP System Manager logo and a search bar.

Name	State	Subtype	Configured Protocols	IPspace	Protection
CL_CIFS_SVM	running	default	SMB/CIFS	Default	Shield
CL_SVM	running	default	NFS, ISCSI, FC	Default	Shield
Healthcare_SVM	running	default	NFS, ISCSI	Default	Shield

确保已在FlexPod 实例中的内部ONTAP 和AWS中的Cloud Volumes ONTAP 之间设置SnapMirror复制、以

便您可以频繁创建应用程序快照。

SVM停止运行后，`hc_iscsi_vol`控制台中不显示音量。

2. 在CVO中激活灾难恢复。

- a. 中断本地ONTAP 和Cloud Volumes ONTAP 之间的SnapMirror复制关系、并提升CVO目标卷(hc_iscsi_vol_copy)到生产环境。

断开SnapMirror关系后、目标卷类型将从数据保护(DP)更改为读/写(RW)。

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume          type
-----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

- b. 激活Cloud Volumes ONTAP 中的目标卷以在云中的EC2实例上启动EHR实例。

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver      Path                                     Igroup    LUN ID
Protocol
-----
svm_singlecvoaws
          /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0      iscsi
```

- c. 要访问云中EHR实例上的数据和文件系统、请首先发现ONTAP 存储并验证多路径状态。

```

sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/          device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename adapter protocol size
product
-----
-----
svm_singlecvoaws                      /dev/sda  host2      iSCSI      200g
cDOT
                                /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running

```

d. 然后激活卷组。

```

sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active

```

e. 最后、挂载文件系统并显示文件系统信息。

```

sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used    Available  Use%
Mounted on
/dev/mapper/datavg-datalv 209608708 183987096 25621612   88%
/file1

```

此输出显示、用户可以通过网络访问复制的数据、直到生产站点从灾难中恢复为止。

f. 反转SnapMirror关系。此操作将反转源卷和目标卷的角色。

执行此操作时、原始源卷中的内容将被目标卷的内容覆盖。当您要重新激活脱机的源卷时，这非常有用。

现在是CVO卷 (hc_iscsi_vol_copy)将成为源卷、内部卷也将成为源卷 (hc_iscsi_vol)将成为目标卷。

在上次数据复制和源卷禁用之间写入到原始源卷的任何数据都不会保留。

- a. 要验证对CVO卷的写入访问、请在云中的EHR实例上创建一个新文件。

```
cd /file1/  
sudo touch newfile
```

当生产站点关闭时、客户端仍可访问数据、并对Cloud Volumes ONTAP 卷执行写入操作、该卷现在是源卷。

如果要故障恢复到主站点、SnapMirror可提供一种高效的方法来重新同步灾难恢复站点与主站点、只需反转SnapMirror关系、即可仅将更改过的数据或新数据从灾难恢复站点传输回主站点。主生产站点恢复正常应用程序操作后、SnapMirror将继续向灾难恢复站点传输数据、而无需再进行基线传输。

本节说明了在生产站点发生灾难时成功解决灾难恢复方案的方法。现在、数据可以安全地由应用程序使用、这些应用程序现在可以在源站点完成还原期间为客户端提供服务。

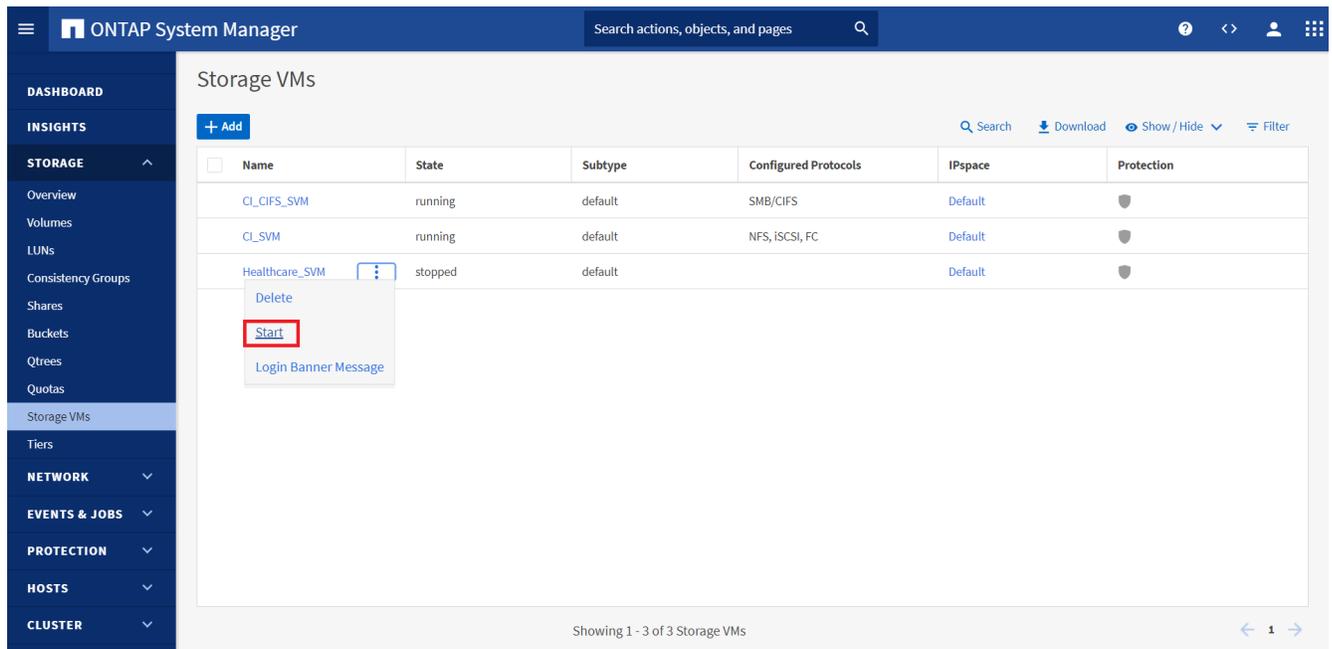
验证生产站点上的数据

恢复生产站点后、您必须确保还原原始配置、并且客户端能够从源站点访问数据。

在本节中、我们将讨论启动源站点、恢复内部ONTAP 和Cloud Volumes ONTAP 之间的SnapMirror关系、并最终对源端执行数据完整性检查

以下操作步骤 可用于验证生产站点上的数据：

1. 确保源站点现在已启动。为此、请启动托管内部ONTAP 卷的SVM (hc_iscsi_vol) 。



2. 中断Cloud Volumes ONTAP 和内部ONTAP 之间的SnapMirror复制关系、并提升内部卷 (hc_iscsi_vol)恢复生产。

断开SnapMirror关系后、内部卷类型将从数据保护(DP)更改为读/写(RW)。

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver          volume          type
-----
Healthcare_SVM hc_iscsi_vol RW
```

3. 反转SnapMirror关系。现在、是内部部署的ONTAP 卷 (hc_iscsi_vol)将成为源卷和之前的源卷、并成为Cloud Volumes ONTAP 卷 (hc_iscsi_vol_copy)将成为目标卷。

通过执行以下步骤、我们已成功还原原始配置。

4. 重新启动内部EHR实例。挂载文件系统并验证 newfile 在生产中断时、您在云中的EHR实例上创建的数据现在也存在。

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01 dir05 dir09 dir13 dir17 dir21 dir25 dir29 dir33 dir37 dir41 dir45 dir49 dir53 dir57 dir61 dir65 dir69 dir73 dir77 kamini
dir02 dir06 dir10 dir14 dir18 dir22 dir26 dir30 dir34 dir38 dir42 dir46 dir50 dir54 dir58 dir62 dir66 dir70 dir74 dir78 latest_file
dir03 dir07 dir11 dir15 dir19 dir23 dir27 dir31 dir35 dir39 dir43 dir47 dir51 dir55 dir59 dir63 dir67 dir71 dir75 dir79 newfile
dir04 dir08 dir12 dir16 dir20 dir24 dir28 dir32 dir36 dir40 dir44 dir48 dir52 dir56 dir60 dir64 dir68 dir72 dir76 dir80
```

我们可以推断、从源到目标的数据复制已成功完成、并且数据完整性已保持不变。这样就完成了对生产站点上数据的验证。

"接下来：总结。"

结论

"先前版本：解决方案 验证。"

构建混合云是大多数医疗保健组织随时提供数据可用性的目标。在此解决方案中、我们实施了采用Cloud Volumes ONTAP 的FlexPod 混合云解决方案、利用NetApp SnapMirror复制技术验证了一些用于备份和恢复医疗保健应用程序和工作负载的用例。

FlexPod 是Cisco和NetApp战略合作伙伴关系中经过严格测试和预先验证的融合基础架构、旨在提供可预测的低延迟系统性能和高可用性。这种方法可为EHR系统用户带来较高的舒适程度、并最终获得最佳响应时间。

借助NetApp、您可以像在内部数据中心运行NetApp存储功能一样、在云中运行EHR生产、灾难恢复、备份或分层。借助NetApp Cloud Volumes ONTAP 、NetApp可提供在云中有效运行EHR所需的企业级功能和性能。NetApp云选项可提供基于iSCSI的块和基于NFS或SMB的文件。

此解决方案 可满足医疗保健组织的需求、并使其能够朝着数字化转型迈进一步。它还可以帮助他们高效地管理应用程序和工作负载。

"下一步：从何处查找追加信息。"

从何处查找追加信息

"上一篇：结论。"

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- FlexPod 主页

["https://www.flexpod.com"](https://www.flexpod.com)

- 适用于FlexPod 的Cisco验证设计和部署指南

["https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"](https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html)

- NetApp Console

["https://console.netapp.com/"](https://console.netapp.com/)

- NetApp Cloud Volumes ONTAP

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html)

- 在 AWS 中快速启动 Cloud Volumes ONTAP

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html)

- SnapMirror 复制

["https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"](https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html)

- TR-3928：《NetApp Epic最佳实践》

<https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf>

- TR-4693 : 《适用于 Epic EHR 的 FlexPod 数据中心部署指南》

["https://www.netapp.com/media/10658-tr-4693.pdf"](https://www.netapp.com/media/10658-tr-4693.pdf)

- 适用于Epic的FlexPod

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html)

- NetApp 互操作性表工具

["http://support.netapp.com/matrix/"](http://support.netapp.com/matrix/)

- Cisco UCS 硬件和软件互操作性工具

["http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"](http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html)

- VMware 兼容性指南

["http://www.vmware.com/resources/compatibility/search.php"](http://www.vmware.com/resources/compatibility/search.php)

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2023年3月	初始版本

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。