数据中心部署指南

智能业务平台IBA

2012年8月系列

前言

本指南的目标受众

Cisco®智能业务平台(IBA)指南主要面向承担以下职务的读者:

- 需要用标准程序来实施方案时的系统工程师
- 需要撰写思科IBA实施项目工作说明书的项目经理
- 需要销售新技术或撰写实施文档的销售合作伙伴
- 需要课堂讲授或在职培训材料的培训人员

一般来说,您也可以将思科IBA指南作为增加工程师和项目实施统一性的指导文件,或利用它更好地规划项目成本预算和项目工作范围。

版本系列

思科将定期对IBA指南进行更新和修订。在开发新的思科IBA指南系列时,我们将会对 其进行整体评测。为确保思科IBA指南中各个设计之间的兼容性,您应当使用同一系列 中的设计指南文档。

每一个系列的Release Notes (版本说明) 提供了增加和更改内容的总结。

所有思科IBA指南的封面和每页的左下角均标有指南系列的名称。我们以某系列指南发 布时的年份和月份来对该系列命名,如下所示:

年 月 系列

例如,我们把于2011年8月发布的系列指南命名为:
"2012年8月系列"

您可以在以下网址查看最新的IBA指南系列:

http://www.cisco.com/go/cn/iba

如何阅读命令

许多思科IBA指南详细说明了思科网络设备的配置步骤,这些设备运行着Cisco IOS、 Cisco NX-OS或其他需要通过命令行界面(CLI)进行配置的操作系统。下面描述了系 统命令的指定规则,您需要按照这些规则来输入命令:

在CLI中输入的命令如下所示:

```
configure terminal
```

为某个变量指定一个值的命令如下所示:

```
ntp server 10.10.48.17
```

包含您必须定义的变量的命令如下所示:

```
class-map [highest class name]
```

以交互示例形式显示的命令(如脚本和包含提示的命令)如下所示:

```
Router# enable
```

包含自动换行的长命令以下划线表示。应将其作为一个命令进行输入:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

系统输出或设备配置文件中值得注意的部分以高亮方式显示,如下所示:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

问题和评论

如果您需要评论一个指南或者提出问题, 请使用 IBA反馈表。

如果您希望在出现新评论时获得通知,我们可以发送RSS信息。

目录

本IBA指南的内容

关于IBA数据中心

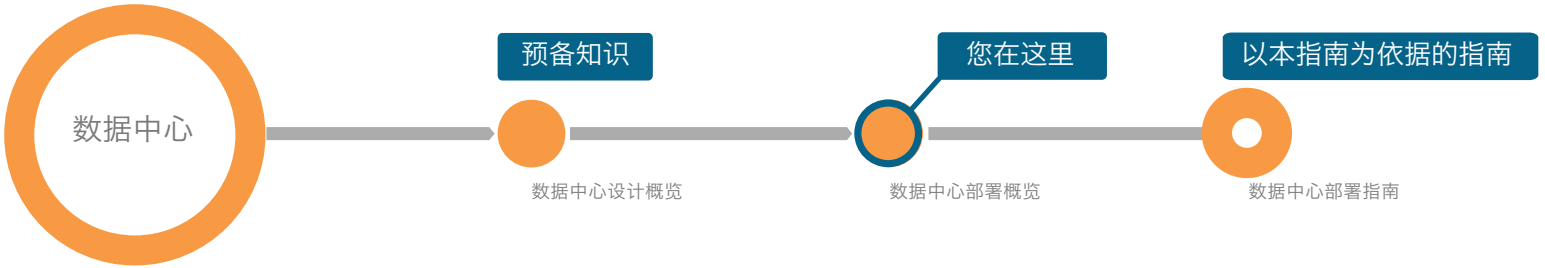
思科IBA能帮助您设计和快速部署一个全服务企业网络。IBA系统是一种规范式设计，即购即用，而且具备出色的可扩展性和灵活性。

思科IBA在一个综合的解决方案中集成了局域网、广域网、无线、安全、数据中心、应用优化和统一通信技术，并对其进行了严格测试，确保能实现无缝协作。IBA采用的模块化分类简化了多技术系统集成的复杂度，使您能够根据需要解决企业需求，而无需担心技术复杂性。

思科IBA数据中心是一个综合的设计，涵盖从机房到数据中心，250到10,000个连接用户的数据中心网络。本设计集成了计算资源、安全、应用永续性以及虚拟化。

成功部署路线图

为确保您能够按照本指南中的设计成功完成部署，您应当阅读本指南所依据的所有相关指南——即如下路线中本指南之前的所有指南。



关于本指南

本部署指南包括一个或多个部署章节，其中包含如下内容：

- **业务概述**——描述本设计的商业用例，业务决策者可通过本章内容来了解解决方案与企业运营的相关性。
- **技术概述**——描述该商业用例的技术设计，包含思科产品如何应对业务挑战。技术决策者可利用本章节理解该设计如何实现。
- **部署详情**——提供解决方案的逐步实施和配置的指导。系统工程师可以在这些步骤的指导下快速和可靠的设计和部署网络。

您可以在以下网址查看最新的IBA指南系列：

http://www.cisco.com/go/cn/iba

简介

思科智能业务平台 (IBA) 数据中心基础是一个综合性的体系结构，设计用以提供数据中心以太网和存储网络，安全性以及混合物理和逻辑服务器，最多支持300个服务器端口的负载平衡。这一即购即用的方法简单、易用、经济，并具有出色的可扩展性和灵活性。Cisco IBA数据中心的架构以《服务器空间部署指南》中所述的服务器空间部署为基础。

思科IBA智能业务平台——《数据中心部署指南》整合了以太网、存储网络、服务器、安全和应用永续性技术，并将它们作为一个解决方案进行了整体测试。这种解决方案级架构构建方式，简化了一般使用多种技术时需要进行的系统集成，允许您挑选能够满足贵企业需求的模块，而不必担心组件匹配和互操作性问题。

在设计思科IBA智能业务平台时，我们竭力使其能够轻松进行配置、部署和管理。该架构：

- 提供了一个强大、坚实的基础平台
- 能够轻松快捷地进行部署
- 能够提高您轻松部署新服务器和其它服务的能力
- 避免随着企业的发展重新对网络进行规划

本指南包括以下章节：

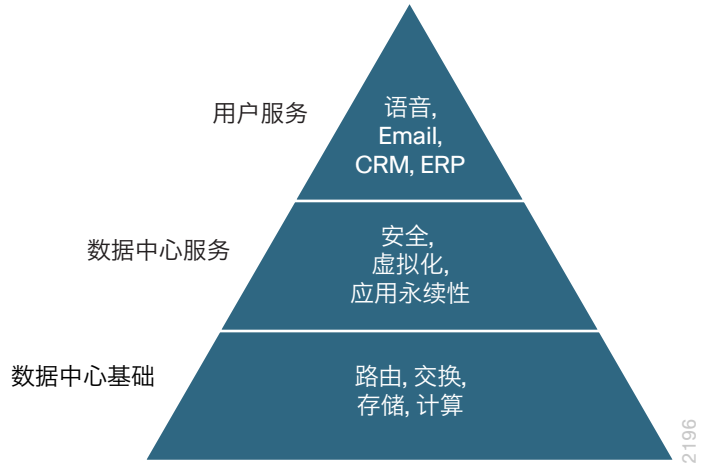
- 第一章节涵盖有关物理环境的数据中心设计要素，列出了电源、冷却、安装机架和所需空间方面的概要信息，以便您在进行数据中心设计时考虑。
- “以太网基础设施”章节为您的数据中心网络在发展其超出服务器群容量时建立基础连接。本部分侧重于为支持企业及其相关服务的应用服务器建立一个集中连接点。以太网章节说明了如何在数据中心配置二层和三层连接，以及到企业其他部分的通信路径。
- “存储基础设施”章节介绍了基础以太网设计如何支持面向网络连接存储 (NAS) 的基于IP的网络存储。存储基础设施章节深入介绍了如何通过使用Cisco Nexus 5500UP交换机作为SAN核心，来部署FC (光纤通道) 存储域网络 (SAN) 。
- “计算连接”章节说明了可在数据中心内使用的各种主机连接方案。该章节介绍了双宿主和单宿主服务器，以及到网络的刀片服务器系统连接。
- “网络安全性”章节则重于部署防火墙，以保护贵企业的关键和敏感信息资产。入侵防御系统 (IPS) 部分说明了如何部署思科IPS，来监控您的网络是否遭到了入侵和攻击。
- “应用永续性”章节描述了如何使用服务器负载平衡来快速扩展服务器应用群，监控服务器和应用运行情况，以及平衡多个服务器间的负载，以实现更高性能。
- 附录提供了本架构实验室测试中所用产品的完整列表，以及各产品所用的软件版本和最近发布的本指南主要变更列表。

为加强您对本架构的理解，我们还提供大量补充指南，介绍可能对解决您的业务问题十分重要的思科及思科合作伙伴功能、技术或特性。

设计目标

思科IBA智能业务平台采用统一的设计流程，在多个服务层基础上构建网络。主要构建模块是所有其他服务所依赖的基础层。数据中心基础必须永续、可扩展、灵活，能够支持数据中心服务，以提高价值、性能和可靠性。此设计的最终目标是支持用户服务，推动企业实现成功。图 1显示了思科IBA智能业务平台数据中心设计分层服务。

图 1 - 思科IBA智能业务平台数据中心的服务层金字塔



思科IBA智能业务平台部署指南采用了模块化概念来扩建网络。每个模块均着眼

于以下原则:

- **易于使用**——开发设计方案时的一个首要要求就是最大限度地减少部署时所需的配置工作和第二天的管理工作。
- **经济高效**——在选择产品时的另一项关键要求是配合数据中心扩展的需求，最多可以扩展至300个服务器端口。
- **灵活性与可扩展性**——随着企业的发展，基础设施也必须随之扩展。因此所选择的产品需要具备可扩展性或能够在架构中进行重新定位。
- **重复使用**——我们的目标是在各种模块中尽可能重复使用相同的产品，以减少所需的备件产品数目。

业务概述

企业在扩展其信息处理能力，以满足不断增长的需求方面面临着许多挑战。在一个新成立的企业中，一小组服务器资源可能就足以支持必要的应用，如文件共享、电子邮件、数据库应用和Web服务等。但随着时间的推移，对于更高处理能力、存储容量和分别控制特定服务器的运营等需求会导致服务器数量激增，我们通常称之为服务器蔓延。此时，企业应使用部分大型企业所使用的数据中心技术，在保持较低投资和运营开支的同时，满足不断扩展的业务需求。本部署指南提供了一个参考架构，使用常用的最佳实践配置，来支持迅速部署这些数据中心技术。

思科IBA智能业务平台数据中心是基本服务器机房基础设施的自然演进。思科IBA数据中心旨在解决以下五大业务挑战:

- 支持应用的迅速增长
- 管理不断提高的数据存储需求
- 优化在服务器处理资源方面的投资
- 保护企业的重要数据
- 提高应用程序的可用性

支持应用的迅速发展

随着应用不断扩展，以支持更多用户，或部署新应用，用于满足企业需求的服务器的数目也在不断增加。当企业现有服务器机房网络的容量无法再满足其需求时，往往就会触发服务器机房演进的第一阶段。许多因素都会限制当前服务器机房网络的容量，如机架空间、供电、通风、交换机吞吐率，以及用以连接新服务器的基本网络端口数目等。本指南中介绍的架构允许企业随业务需求的发展，平稳扩展服务器环境和网络拓扑结构的规模。

管理日益增长的数据存储需求

随着应用需求的增长，对于更高数据存储能力的需要也不断增加。当对于特定服务器的存储需求超出了该服务器硬件平台的物理容量时，就会引发问题。因此，随着企业的不断发展，转而采用集中存储模式，能够最为高效地管理在增加存储容量方面的投资。集中存储系统能为多个应用和服务器提供磁盘容量，在存储供应方面提供更高可扩展性和灵活性。

除原始磁盘容量外，一个专用存储系统还具有多方面的优势。集中存储系统能提高磁盘存储的可靠性，从而改进应用可用性。这种存储系统无需将新设备与一台服务器实际相连，就能通过网络向此服务器提供更高容量。而且，集中存储系统采用了更为先进的备份和数据复制技术，有助于保护企业免遭数据丢失和应用中断的威胁。

优化在服务器处理资源方面的投资

在企业的发展过程中，通常会为各个应用配备专用的物理服务器，以提高稳定性，简化故障排除。但是，这些服务器在一天中的大多数时间无法以较高的处理器利用率运行。服务器处理资源使用率低下，意味着企业并未充分利用这些已有投资来发挥其全部潜力。

服务器虚拟化技术支持单一物理服务器运行访客操作系统的多个虚拟实例，创建虚拟机(VM)。在服务器硬件上运行多个VM有助于更为充分地利用企业在处理资源上的投资，且同时从安全、配置和故障排除角度，都能独立查看每个VM。

服务器虚拟化和集中存储技术相互配合，能够迅速部署新服务器，并在发生服务器硬件故障时缩短停运时间。VMs（虚拟机）能够完全存储在集中存储系统中，这消除了虚拟机与任何物理服务器的关联。因此，企业在部署新应用或升级服务器硬件时能够拥有极高灵活性。

本指南中定义的架构能够加速、简化服务器虚拟化部署，同时支持现有设备。本系列中包括补充指南，着重介绍服务器虚拟化。

保护企业的重要数据

鉴于当今世界上的通信和商务活动越来越依赖于互联网，网络安全很快就成为了成长型企业的一个主要顾虑。通常来说，企业的安全保护范围始于其互联网边缘连接，并将其内部网络视为一个可信的实体。但是，互联网防火墙只是构成网络基础设施安全的一个组件而已。

实际上，对于企业数据的威胁常常来自于内部网络。这些威胁可能来自于进入企业办公现场的供应商、受到感染的员工笔记本电脑，或者是已遭到入侵、可能被

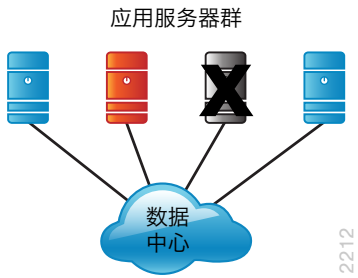
用来当作攻击平台的服务器。由于企业一般是在数据中心内集中存储最为重要的数据，所以在完整的数据中心架构计划中，安全不再是可选组件，而是必备组成部分。

思科IBA智能业务平台数据中心设计说明了如何出色地集成网络安全功能，如防火墙和入侵防御等，以保护网络中的关键服务器资源和存储资源。该架构能够灵活地保护数据中心的特定部分，或者根据企业的安全策略，在多层应用之间插入防火墙功能。

提高应用程序的可用性

鉴于企业不断扩展的全球业务以及全天候运营需求，支持业务的关键应用必须随时可供工作人员使用。应用的可用性会受到过载服务器以及服务器或应用故障的威胁。不平衡的使用会导致对一些用户的响应时间不可接受，而针对另一些用户的运行体验却令人满意，这使得IT团队很难进行诊断。

图 2 - 各种运行状态下的应用服务器群

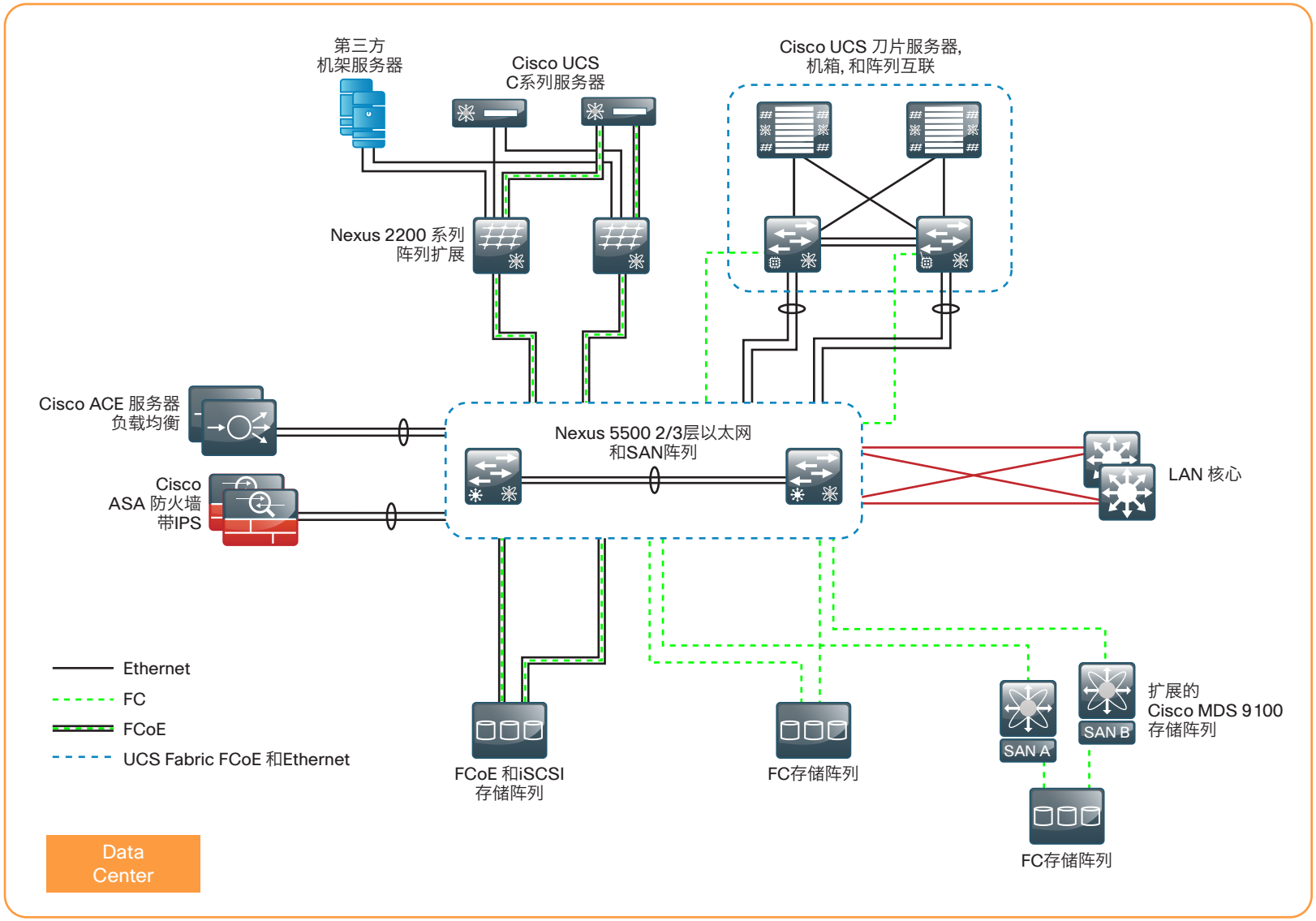


应用可用性决定着生产力和客户满意度，而这对于企业的成功至关重要。IT部门除了要能够监测简单的服务器可用性，而且还要能够监测应用可用性，并需要能够快速、透明地向应用服务器群添加更多服务器。

技术概述

思科IBA数据中心设计旨在帮助企业将现有服务器机房环境提升到更高的性能、灵活性和安全性水平。图 3提供了这一架构的详细介绍。

图 3 - 思科IBA数据中心设计



正如思科IBA智能业务平台——《无边界网络局域网设计概述》中所述，思科IBA智能业务平台数据中心设计是设计用于当部署于异地设施中时保持独立，或连接到任一款IBA智能业务平台三层以太网核心层解决方案。本参考架构中采用了以下技术。

以太网基础设施

以太网基础设施为数据中心内永续的二层和三层通信奠定了基础。这一层支持从您的原始服务器群迁移到一个可扩展的架构，采用模块化方法为数百台服务器提供快速以太网、千兆以太网和万兆以太网连接。

思科IBA智能业务平台数据中心的核心构建在Cisco Nexus 5500UP系列交换机之上。Cisco Nexus 5500UP系列是一款高速交换机，当使用在本设计中测试的三层子卡时，能够支持二层和三层交换。Cisco Nexus 5500UP系列有48端口和96端口两种型号，本设计中使用了48端口型号，96端口型号用于满足更高密度要求。Cisco Nexus 5500UP支持阵列扩展模块（FEX）技术，该技术可提供一种远程线路卡方法，用于从服务器连接到机架顶，以满足快速以太网、千兆以太网和万兆以太网要求。Cisco FEX上的物理接口在Cisco Nexus 5500UP交换机上进行了编程，通过减少部署服务器端口所需使用的设备数量，简化了配置任务。

Cisco Nexus 5500UP系列采用虚拟端口通道（vPC）技术，可提供一种无回路方法来扩建企业数据中心，其中任何VLAN均能够出现在该拓扑结构的任意端口上，而无需生成树环路或拦截链路。数据中心核心交换机通过亚秒级故障切换支持冗余，因此设备故障或维护不会防碍网络运营。

存储基础设施

存储网络是解决数据存储日益增长问题的关键，而这一问题是企业必须要面对的。集中存储减少了单个服务器平台占用的磁盘空间，简化了提供备份以避免数据丢失的任务。思科IBA智能业务平台数据中心设计使用Cisco Nexus 5500UP系列交换机作为网络的核心。该型号交换机的重要性在于，它拥有通用端口（UP）能力。通用端口能够在任意端口上支持以太网、FC（光纤通道）和FCoE（以太网光纤通道）。这使得数据中心核心能够在单一平台类型上支持多种存储网络技术，如光纤通道存储域网络（SAN）、互联网小型计算机系统接口（iSCSI）以及网络连接存储（NAS）。这不仅可减少网络部署成本，而且还节省了昂贵的数据中心托管环境的机架空间。

Cisco Nexus 5500UP光纤通道功能基于Cisco NX-OS操作系统之上，能够与Cisco MDS系列SAN交换机无缝互操作，以满足更高容量的光纤通道要求。本部署章节包括了在Cisco Nexus 5500UP系列与支持FC（光纤通道）SAN的Cisco MDS系列之间进行互联的程序。Cisco MDS系列能够为FC（光纤通道）SAN环境提供一系列高级服务，这一环境可能需要高速加密、VSAN间路由、磁带服务或基于IP的光纤通道扩展。

计算连接性

服务器可通过多种途径连接到数据中心网络，以支持以太网和FC传输。本章节概括介绍了从单宿主以太网服务器到双宿主阵列扩展模块的连接，以及可能使用主动/被动网络接口卡（NIC）分组或EtherChannel支持永续性的双宿主服务器。使用万兆以太网的服务器能够通过融合网络适配器（CNAs）和FCoE将多个以太网NIC和FC主机总线适配器（HBAs）整合到单一线路上。采用FCoE的双宿主万兆以太网服务器可提供永续以太网传输和到SAN-A/SAN-B拓扑的FC连接。该章节还概括介绍了思科统一计算系统（UCS）刀片服务器系统集成连接如何工作，以及将非思科刀片服务器系统连接到网络的考虑事项。

网络安全性

数据中心设计中有许多要求和机会，以便更有效地保护客户机密信息和企业的关键及敏感应用。数据中心设计采用Cisco ASA 5500系列防火墙进行了测试。Cisco ASA 5500为防火墙规则设置提供了高速处理，并采用多个万兆以太网端口提供了高带宽连接，以支持到数据中心核心交换机的永续连接。Cisco ASA 5500还有一个插槽用于提供服务，并在本设计中提供了一个IPS模块，可检查应用层数据、检测攻击和窥探、以及基于数据包内容或发件人声誉阻止恶意流量。采用IPS模块的Cisco ASA 5500防火墙成对部署，可提供主动/备份永续性，防止在出现故障或进行平台维护时停机。

应用永续性

应用性能和可用性会直接影响员工的生产效率和客户满意度，进而影响企业的盈利能力。随着企业日渐开始在24x7全天候全球可用环境中开展业务，确保关键应用以最高性能运行变得越来越重要。

本架构包括思科应用控制引擎（ACE），可为第四层至第七层交换和服务器负载均衡（SLB）提供最新技术。服务器负载均衡器能够在多台服务器间分散应用的负载，并主动探测服务器和应用的负载和运行状况，以防止过载和应用故障。思科ACE还可提供TCP处理卸载、安全套接层（SSL）卸载、压缩以及多种其它加速技术。本架构中使用的Cisco ACE 4710应用可扩展至多千兆位运营，并可作为主动/备份对进行部署，以防止由于设备故障或维护而中断运行。

借助该架构，企业能够在控制设备成本和运营成本的同时，使其网络作好支持未来发展的准备。本章节中记录的部署流程为完成该架构组件的基本配置提供了精确的逐步说明，以使您的网络能够顺利建成并投入运行。这种方法既允许您受益于超大型企业的数据中心所使用的部分最新技术，而且IT人员也不必经历漫长的学习过程。尽管该架构的设计和验证是作为整体进行的，但本章节采用了模块化方式，使您可以通过选择率先部署的特定架构组件，来逐步升级。

备注

物理环境

业务概述

在搭建或改造一个网络时，您必须谨慎考虑设备的安装位置。在搭建服务器机房、交换机机柜甚至是数据中心时，您必须要考虑以下三个方面：电源、散热和机架。在考虑这些因素的基础上，充分了解您的具体情况，将能够最大限度降低意外，以及日后的设备迁移成本。

技术概述

思科IBA数据中心设计提供了一种永续的环境，然而这并不能保护您的数据中心避免由于完全断电或失去冷却而导致的全面故障。在设计数据中心时，您必须考虑需要多少电量，如果提供商断电如何提供备用电力，以及在备用电力情况下能够维持多久等问题。您数据中心中的服务器、网络设备和装置在运行时会散热，这需要适当的冷却设计，包括设备机架位置等，以防止热点。您还需要考虑在您的数据中心，服务器，网络设备和电器由于运行带来的散热问题，这需要您开发一个适当的散热设计，包括定位设备机架，以防止热点。

电源

了解这个区域将安装什么设备。如果您不知道将要安装什么设备，就无法规划供电线路和相关工作。有些设备要求使用标准的110V插座，室内可能已经配备这种插座。而有些设备则可能要求使用更高功率的电源。

电源需要一直保持在开通状态吗？如果室内安装了服务器和存储设备，在多数情况下必须始终保持供电状态。当电源关闭时，应用将无法做出及时响应。为了防止断电，您需要一个不间断电源（UPS）。在电源中断期间，UPS将把电流负荷切换到一组内部或外部电池上。有些UPS是联机的，意味着电源在供电时要经过电池；有些UPS则是切换式的，只在断电时才使用电池。各种UPS所支持的负荷和运行时间各不相同，因此必须进行精心的规划，以确保购买和安装适用的UPS，同时对其进行妥当的管理。多数UPS都提供远程监控功能，而且在UPS电池即将耗尽时能够从容关闭关键任务服务器。

通过为设备配电也可以改变供电要求。从插座或UPS向设备分配电力的方式有很多。举例来说，我们可以利用一个垂直安放在机柜中的配电盘来分配电力，这种配电盘通常带有一个L6-30输入端和输出电压在200-240V之间的C13/C19插座。应当为这些配电盘配备一个电表，以防止电路过载。电表将显示电路的当前负荷量，这一点非常重要，因为由电路过载而导致的电路断路器跳脱会在没有预警的情况下使所有与其连接的设备突然停运，导致业务系统停机，还有可能造成数据损失。为实现全面的远程控制，可以针对配电盘从一个网络浏览器对每个插座进行全方位的远程控制。借助这些垂直配电盘，用户还能够对电源线进行适当的线缆管理。可以使用较短的C13/C14和C19/C20电源线来代替较长的电源线，并将其连接到多个110V的插座或配电盘。

散热

在用电的同时必将产生热量。简单来说就是电力消耗意味着热量的输出。如果只需为一两台服务器和一个交换机提供散热，标准的建筑物空调就已经足够。但是如果有多台服务器和刀片服务器（此外还有存储器和交换机等），建筑物空调则不足以保证适当的散热。请务必与您的设施团队一起讨论当前和未来有哪些可利用的散热方案并进行适当的规划。可供选择的方案有很多，包括行间制冷、天花板制冷、活动地板间上下地板层制冷和墙壁安装式制冷。

设备机架

计划将设备放置在哪儿是十分重要的。正确的安置和规划有利于支持未来的容量增长。在对供电和散热要求进行正确评估之后，下一步就需要安装机架或机柜。多数服务器的深度较大，如果再加上网络连接和电源连接线，整个服务器占用的空间更大。大多数服务器可安放在一个42英寸深的机柜中，深度更大的机柜则可以提供更多空间，让相关人员能够灵活地在机柜中进行线缆和电源管理。请注意您的服务器对导轨有何要求。如今，大多数服务器都带有机架配件，这些配件使用方孔形的垂直机柜导轨。如果没有合适的导轨，必须使用适配器或支架，但是在这种情况下，如果不移除其他设备或牺牲空间很难对服务器和设备进行维护和管理。数据中心机架应使用机柜的方形导轨安装件。可以利用卡式螺母来对路由器、交换机、支架等设备进行线性紧固。

总结

在部署数据中心时，必须对数据中心的物理环境要求进行精细的规划，以高效利用空间，保证未来可扩展性以及维护操作的简便性。部署思科IBA智能业务平台，即使您最初只从一个规模较小的系统起步，您也能够在为数据中心规划物理空间时同时兼顾未来将会安装的其他设备。如需更多关于数据中心供电、散热和设备机架方面的信息，请联系思科在数据中心环境产品领域的合作伙伴，如Panduit和APC。

以太网基础设施

业务概述

随着企业的不断发展，思科IBA——数据中心设计概览中所介绍的基本服务器机房以太网交换堆叠可能无法满足您的需要。另外，为服务器硬件从千兆以太网连接过渡到万兆以太网做好准备，也十分重要。多层应用常常将基于浏览器的客户端服务、业务逻辑和数据库层划分到多个服务器中，增加了服务器间流量，提高了性能要求。随着安放企业服务器的物理环境发展到多个机架，对于将服务器连接到网络所需的布线的管理难度也在加大。使用万兆以太网连接有助于提高网络整体性能，并减少提供带宽所需的物理链路数量。

在有些企业中，数据中心可能位于工厂而不在总部大楼中。有些企业将其数据中心安置在偏远的工厂中，那里的电源或冷却更适合安置数据中心，另一些企业可能向通信服务提供商租赁占地空间、机架和电源，以降低资本成本。要在多个不同位置安置数据中心，要求数据中心架构能够灵活适应不同位置，同时仍可提供该架构的核心要素。

技术概述

在思科IBA智能业务平台数据中心，以太网的基础是一对永续运行的Cisco Nexus 5500UP系列交换机。这些交换机为构建一个可扩展、高性能的数据中心提供了理想平台，既支持通过万兆以太网相连的服务器，也支持通过千兆以太网相连的服务器。思科IBA智能业务平台数据中心设计旨在支持将服务器和服务从原来机房轻松迁移到能够随着企业的增长而扩展的数据中心。

具备通用端口（UP）能力的CiscoNexus 5500UP交换机可在单一平台上支持以太网、FCoE（以太网光纤通道）和FC（光纤通道）端口。Nexus 5500UP能够作为FC（光纤通道）SAN支持企业数据中心，并连接到现有FC（光纤通道）SAN。Cisco Nexus 5000系列还支持Cisco Nexus 2000系列阵列扩展模块。阵列扩展模块能够以物理方式扩展永续交换机对的交换架构，在多个机架顶部提供端口汇聚功能，减少服务器环境扩展时的电缆管理问题。

思科IBA智能业务平台数据中心设计可充分利用Cisco Nexus 5500UP系列交换机系列的许多高级特性，为数据中心环境提供中心二层和三层交换架构：

- 三层路由表最多能支持8000个路由。
- 三层引擎能够为二层域支持多达8000个邻接地址或MAC地址。
- 该解决方案在推荐的虚拟端口通道（vPC）模式下运行时，可提供多达1000个IP组播组。

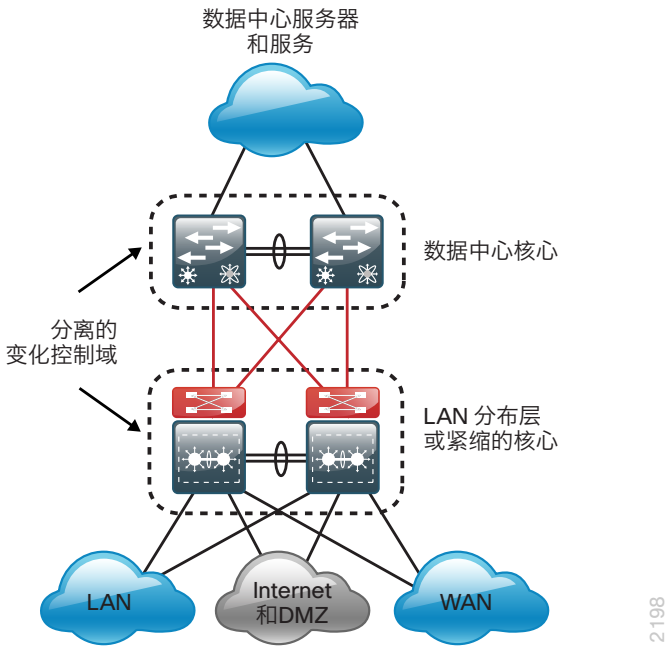
Cisco Nexus5548和5596交换机的第二代3层引擎现在已可使用。第二代硬件的3层模块在使用现有的思科NX-OS软件时与如上的参数相同，并且在使用将来的Cisco NX-OS软件中提供两倍的邻接地址和路由数。

读者提示

如需了解更为详细的Cisco Nexus 5500系列平台可扩展性设计数据，请访问：http://www.cisco.com/en/US/customer/docs/switches/datacenter/nexus5000/sw/configuration_limits/limits_513/nexus_5000_config_limits_513.html#wp328407

图 4中显示，三层数据中心核心层与思科IBA智能业务平台——《无边界网络局域网部署指南》中设计的三层局域网核心层相连。

图 4 - 数据中心核心与局域网核心变更控制相分离



使用三层互联两个核心层的结果如下:

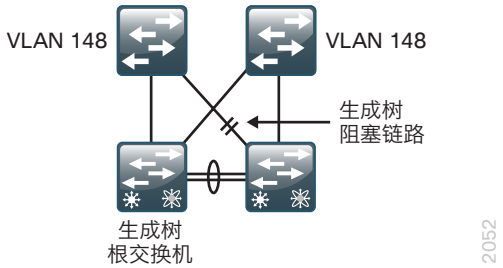
- 形成一条永续三层互联, 支持迅速的故障切换。
- 两个核心网络的变更控制在逻辑上是相互独立的。
- 局域网核心层为局域网、广域网和互联网边缘提供了可扩展互联。
- 数据中心核心层为所有数据中心服务器和服务提供了互联。
- 在服务器和设备间传输的数据中心内部二层和三层流量在数据中心核心层进行本地交换。
- 数据中心有一个迁移到远程位置的逻辑分隔点, 且无需重新设计, 仍能提供核心层服务。

本章概述了在这一拓扑中使用的主要特性, 并对适用于“部署细节”章节中所示的配置示例的具体物理连接进行了具体说明。

永续数据中心核心层

数据中心需要提供一个拓扑结构, 其中任意数据中心VLAN都能扩展到环境中的任意服务器, 无需中断运行就能支持新安装, 且能将一个服务器的负载移至数据中心的其它任意物理服务器。采用局域网交换机的传统二层设计使用生成树, 当VLAN扩展到多个接入层交换机时, 这会形成环路。生成树协议拦截链路, 防止环路, 如图 5所示。

图 5 - 采用生成树拦截链路的传统设计

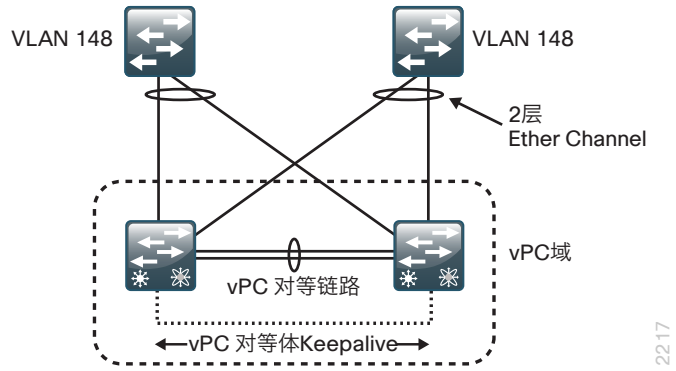


Cisco Nexus 5500UP系列交换机对采用虚拟端口通道 (vPC) 特性配置而成, 可为思科IBA智能业务平台数据中心提供中央以太网交换架构。vPC支持以物理方式连接到两个不同Cisco Nexus交换机的链路向第三方下游设备显示为来自一个设备, 并作为单个以太网端口通道的一部分。这个第三方设备可以是服务器、交换机, 或其它任何支持IEEE 802.3ad端口通道的设备。这一功能允许使用两个数据中心核心层交换机来构建永续、无环路的二层拓扑结构, 通过所有相连链路转发流量, 而无需借助生成树协议拦截来防止环路。

数据中心设计中使用的Cisco NX-OS Software vPC, 以及思科IBA智能业务平台——《无边界网络局域网设计概览》中使用的Cisco Catalyst虚拟交换系统 (VSS) 是类似的技术, 它们都允许创建跨越两个交换机的二层端口通道。对于Cisco EtherChannel技术, 术语“多机箱EtherChannel” (MCEC) 称为技术互换。MCEC使用vPC从相连的设备连接到数据中心核心层, 并提供生成树无环路拓扑结构, 允许VLAN在数据中心扩展, 并保持永续架构。

vPC由两个vPC对等交换机组成, 通过一个对等链路相连。在vPC对等中, 一个是主用, 另一个是备用。由这些交换机构成的系统称为vPC域。

图 6 - Cisco NX-OS vPC设计



该特性增强了易用性，简化了数据中心交换环境的配置。

读者提示

如需了解有关vPC技术和设计的更多信息，请参阅文档“Cisco NX-OS软件虚拟端口通道基础概念”和“面向Cisco NX-OS软件和虚拟端口通道的生成树设计指南”，网址为：www.cisco.com.

思科IBA智能业务平台数据中心设计使用热备份路由器协议（HSRP），为数据中心VLAN提供IP默认网关永续性。当结合使用HSRP和vPC时，无需积极的HSRP计时器来改进收敛，因为两个网关始终处于活跃状态，而且到任一数据中心核心的流量将在本地交换，以提高性能和永续性。

以太网阵列扩展

Cisco Nexus 2000系列阵列扩展模块(FEX)提供了经济高效、高度可扩展的千兆以太网和万兆以太网环境。阵列扩展允许您在每个服务器机架顶部汇聚一组物理交换机端口，而无需将这些端口作为一个独立逻辑交换机进行管理。Cisco FEX作为到Cisco Nexus 5500UP交换机的远程线路卡。Cisco FEX互联服务器的所有配置均在数据中心核心交换机上完成，这些交换机可提供一个集中点来配置所有连接，简单易用。由于Cisco FEX充当Cisco Nexus 5500UP交换机上的线路卡，将VLAN扩展到不同Cisco FEX上的服务器端口不会在整个数据中心创建生成树环路。

通过以双宿主方式将服务器连接到两个独立的阵列扩展模块，每个阵列扩展模块以单宿主方式连接到Cisco Nexus 5500UP系列交换机对的一个成员，您可以提供出色的网络永续性。为了向仅支持单宿主网络连接的服务器提供高可用性，Cisco FEX本身可能须使用vPC双归属到数据中心核心交换机对的两个成员。单宿主和双宿主拓扑均可提供出色的灵活性，在任意端口上部署VLAN，而无需环路或生成树拦截链路。

图 7 - Cisco FEX与vPC 组合

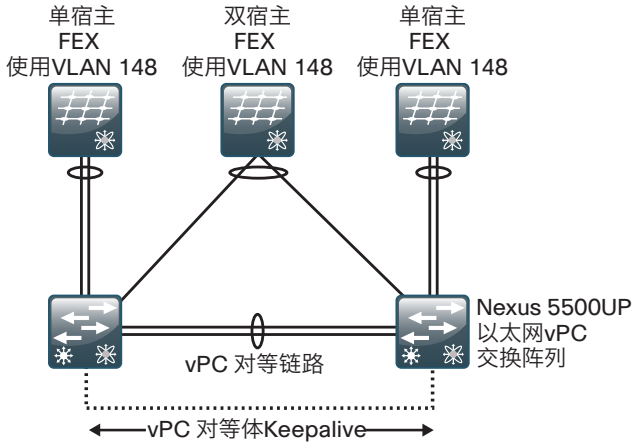
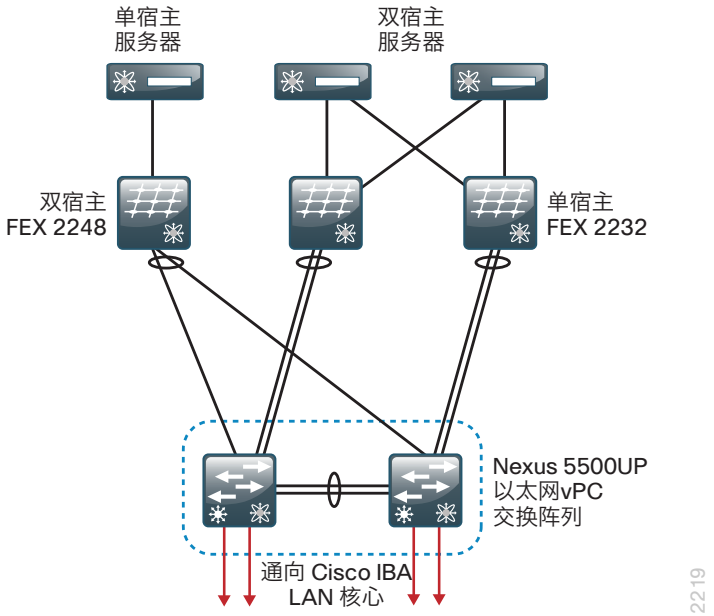


图 8中的参考架构示例阐述了采用互联服务器的单宿主和双宿主Cisco FEX配置。每个Cisco FEX均包括专用阵列上行链路端口，设计用于连接上游Cisco Nexus 5500UP系列交换机，支持数据通信和管理。Cisco Nexus 5500UP交换机上的任何万兆以太网端口均可用于Cisco FEX连接。

技术提示

当Cisco Nexus 5500UP系列交换机配置用于三层运行时，它们可支持多达16个互联Cisco FEX（要求使用CiscoNX-OS 5.1(3)N1(1a)版本）。Cisco FEX将支持多达4个或8个到Cisco Nexus 5500UP父交换机的上行链路，具体取决于使用的Cisco FEX型号，以及您希望在设计中实现的超额开通水平。如果可能，建议配置最大数量的阵列上行链路，充分利用twinax（CX-1）布线或Fabric Extender Transceiver（FET）和OM3多模光纤。为实现最低的永续性，建议至少配置两个到数据中心核心的Cisco FEX上行链路。

图 8 - 以太网交换架构物理连接



QoS服务质量

为了支持FCoE无损数据的要求，Nexus5500交换机和Nexus2000阵列扩展作器做为一个系统使用数据中心的QoS。大部分系统中分类和标记的QoS是通过使用IEEE802.1Q Priority Code Point（优先级代码点）来构建的，也就是来自支持FCoE或支持trunk主机的2层帧头CoS字段。IP流量到达思科Nexus5500系列交换机上的以太端口时也可以被三层的差分服务代码点（DSCP）位与IP访问控制列表（ACL）归类。

流量分类用于映射流量到6个硬件队列中的1个。其中1个队列预定义为默认流量，另一个硬件队列分配为使用无损FCoE流量。剩余的4个队列可供其余流量使用。例如，可以为数据中心的jitter-intolerant（不容忍抖动）多媒体服务定义一个优先级队列。

由于不能保证非FCoE设备进入FEX的包都能带上符合应用要求的CoS标记，思科IBA数据中心部署遵从以下QoS方法：

- FCoE流量，由数据中心桥接交换（DCBX）与主机谈判决定，在数据中心内给予优先级和终端到终端的无损处理对待。
- 没有的CoS分类的非FCoE流量，在思科Nexus5500交换机的入向可用链路上给予默认对待，以避免oversubscription（带宽超额）的情况。在相反的方向，指向到FEX的流量使用思科Nexus5500交换机的QoS出口策略。
- 对于进入到Cisco Nexus5500交换机上的IP三层流量，不论是直接来自FEX或穿越FEX的三层连接，在入向接口配置了DSCP分类。这种分类是为了将流量映射到默认队列或4个非FCoE的内部队列，提供一个合适的QoS每跳行为。
- 为了确保一致的策略部署，通过CoS标记的流量，也和三层引擎的处理一样，适用于每一个思科Nexus5500的内部队列。CoS标记用于分类的流量进入到3层引擎，使系统的应用进行策略排队。

非FCoE的设备，相对于连接思科FEX端口时被采用默认的上连，他们要求连向思科Nexus 5500交换机的流量基于DSCP分类。

QoS策略支持按类配置巨型帧（jumbo frame）。每CoS的最大传输单元（MTU）要求FCoE全系统内一致，而不是数据中心以外典型设备上的基于端口的MTU配置。增加MTU大小，可以提高大数据传输的性能。

部署详情

为思科IBA数据中心设计配置以太网交换架构时需遵循以下配置步骤。

流程

配置以太网带外管理

1、配置平台特定交换机设置

2、配置交换机通用设置

3、应用交换机全局配置

4、配置交换机访问端口

5、配置交换机到第三层核心链路

数量不断增长的交换平台、设备和服务器使用不同的管理端口，设置、监视和保持活跃的进程。典型的中间层数据中心是以太网带外管理网络的理想位置，因为设备通常包含在少数几个机架中，不需要光纤互联来到达位于较远距离的平台。

在此设计中，我们使用固定配置二层交换机来支持带外以太网管理网络。诸如Cisco Catalyst 3560X等交换机是实现这一目的的理想交换机，它有双电源可实现永续性。

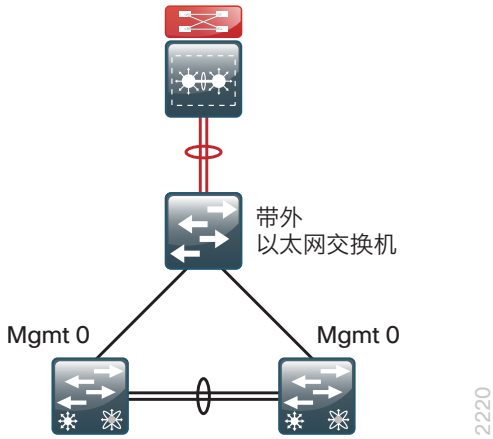
带外网络可提供：

- 二层路径，独立于Cisco Nexus 5500UP数据中心核心交换机的数据路径，支持在管理接口上运行的vPC（虚拟端口通道）持活数据包
- 用于通过管理接口实现Cisco Nexus 5500UP交换机间配置同步的路径。
- 用于数据中心设备管理接口（如防火墙和负载均衡器）的通用连接点
- 用于服务器上“lights out”管理端口的连接点

尽管二层交换机不为数据中心内的数据包提供通用互联，但它需要为数据中心外的IT管理人员提供访问数据中心设备的能力。提供IP连接的选项取决于您数据中心的位置。

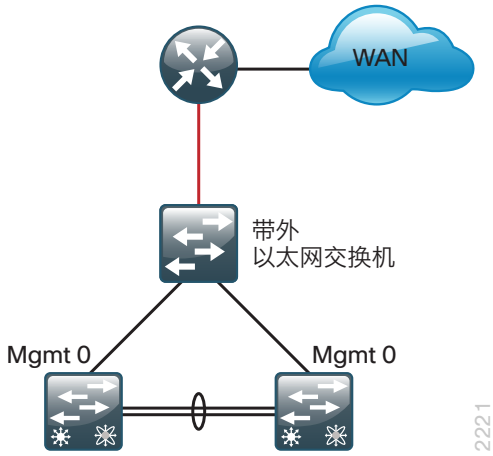
如果您的数据中心与总部局域网处于同一位置，那么核心局域网交换机可提供到数据中心管理子网的三层连接。

图 9 - 提供三层连接的核心局域网交换机



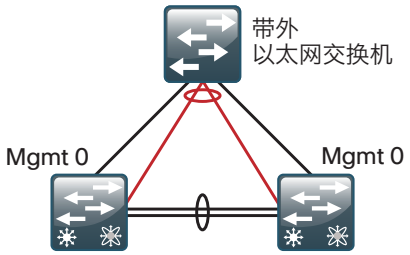
如果您的数据中心位于与大型局域网不同的设施，则广域网路由器可提供到数据中心管理子网的三层连接。

图 10 - 提供三层连接的广域网路由器



提供到数据中心管理子网的三层连接的第三个选项是使用数据中心核心Cisco Nexus 5500UP交换机，如图 11所示。这是本指南中描述的配置。

图 11 - 通过使用核心Cisco Nexus 5500UP 交换机提供三层连接



技术提示

当使您使用数据中心核心Cisco Nexus 5500UP交换机支持三层连接时，用于vPC持活 (keepalive) 数据包的二层路径将使用以太网带外交换机，因为Nexus 5500UP管理端口位于一个单独的管理虚拟路由和转发 (VRF) 路径，而不是Cisco Nexus 5500UP交换机的全局分组交换中。此外，管理端口位于同一IP子网内，因此它们不需要三层交换机来支持数据中心核心交换机之间的数据包。三层交换虚拟接口 (SVI) 将为数据中心之外的访问提供连接。

程序 1　配置平台特定交换机设置

步骤 1： 配置Catalyst 2960-S和3750-X平台。

```
switch [switch number] priority 15
```

当一个堆叠中配置了多个Cisco Catalyst 2960-S或Cisco Catalyst 3750-X系列交换机时，其中一个交换机控制整个堆叠的运行，称为堆叠主交换机。

当堆叠中配置了三个或更多交换机时，选择一个未配置上行链路的交换机配置为堆叠主交换机。

步骤 2： 确保原始主MAC地址在故障后保留堆叠MAC地址。

```
stack-mac persistent timer 0
```

当堆叠主交换机发生故障，默认行为是为新近处于活动状态的堆叠主交换机分配一个新的堆叠MAC地址。由于Link Aggregation Control Protocol (LACP) (链路聚合控制协议 (LACP)) 和其他许多协议均使用堆叠MAC地址且必须重启，这个分配的新MAC地址会使网络不得不重新收敛。因此，应使用**stack-mac persistent timer 0**命令，确保故障后，原来的主MAC地址仍是堆叠MAC地址。

由于AutoQoS 可能没有被配置在此设备上，您需要定义一个宏来手动配置全局QoS设置，您会在后面的程序中使用其应用至平台特定的QoS配置。

Option 1. 为Cisco Catalyst 3750-X和3560-X 配置QoS

步骤 1： 定义一个宏，您可以在后面使用它为Cisco Catalyst 3750-X和3560-X交换机应用平台特定QoS配置。

```
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40
41 42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
```

```
41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38
39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11
13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
macro name EgressQoS
 mls qos trust dscp
 queue-set 1
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
@
!
```

Option 2. 为Cisco Catalyst 2960-S 配置QoS

步骤 1: 定义一个宏, 您可以在后面使用它为Cisco Catalyst 2940-S交换机应用平台特定的QoS配置。

```
mls qos map policed-dscp 0 10 18 24 46 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38
39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11
13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
macro name EgressQoS
 mls qos trust dscp
 queue-set 1
 srr-queue bandwidth share 1 30 35 5
```

```
 priority-queue out
@
!
```

程序 2　配置交换机通用设置

此程序将配置系统设置以方便安全的管理交换机。在本案例中提供的值和实际设置将取决于您实际的网络配置。

表 1 - 用于部署示例的常见网络服务

服务	地址
域名	cisco.local
活动目录，域名系统 (DNS)，动态主机配置协议 (DHCP) 服务器	10.4.48.10
思科访问控制系统 (ACS) 服务器	10.4.48.15
网络时间协议 (NTP) 服务器	10.4.48.17

步骤 1: 配置设备主机名以方便识别此设备。

```
hostname [hostname]
```

步骤 2: 配置VLAN Trunking Protocol (VTP)透明模式。此部署使用VTP透明模式，因为选择其他模式有可能会因操作失误而带来潜在危险。

虚拟中继协议(VTP)允许网络管理员在网络中的某个位置配置VLAN，并将此配置动态传播到其他网络设备。然而，在大多数情况下，VLAN只在交换机设置期间定义一次，之后几乎不进行修改。

```
vtp mode transparent
```

步骤 3: 开启快速每VLAN生成树 (PVST+)。PVST+提供了每VLAN RSTP (802.1w) 的实例。与传统的生成树 (802.1D) 相比，快速PVST+大大提高了检测间接故障或链接恢复事件的能力。

虽然此架构没有任何二层环路，但仍必须启用生成树。启用生成树能够确保如果意外配置了任何物理或逻辑环路，在实际拓扑中也不会出现二层环路。

```
spanning-tree mode rapid-pvst
```

步骤 4: 开启单向链路检测 (UDLD) 协议。UDLD是一个二层协议，使通过光纤或双绞线以太网电缆相连的设备能够监控电缆的物理配置，并检测是否存在单向链路。当UDLD发现单向链路时，它会禁用受影响的接口并向您报警。单向链路会导致一系列问题的发生，包括生成树环路、黑洞和其他不确定性数据包转发等。此外，UDLD能更快检测出链路故障，并支持接口中继的快速重新收敛，特别是采用易于发生单向故障的光纤电缆时更是如此。

```
udld enable
```

步骤 5: 设置EtherChannels (以太网通道) 使用流量源和目的地IP地址。将EtherChannel成员链路间流量负载共享的方法规范化。在此设计中，我们广泛使用了EtherChannel，因为它们对于网络具有出色的永续性。

```
port-channel load-balance src-dst-ip
```

步骤 6: 为主机查找配置DNS。

在Cisco IOS设备的命令行，对于目的地键入一个域名来代替IP地址是有帮助的。

```
ip name-server 10.4.48.10
```

步骤 7: 配置设备管理协议。

Secure HTTP （HTTPS) 和Secure Shell （SSH) 协议是HTTP和Telnet的更安全的替代协议。它们使用Secure Sockets Layer （SSL) 和Transport Layer Security (TLS) 提供设备身份认证和数据加密。

SSH 和HTTPS 协议开启局域网设备的安全管理。这两个协议都为隐私加密，同时关闭不安全协议——Telnet 和HTTP。在vty行指定**transport preferred none**命令来防止从CLI提示错误的连接尝试。如没有这个命令，当IP名称服务器不可到达，长期超时延迟可能会导致输入错误命令。

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
  transport preferred none
```

步骤 8: 开启简单网络管理协议 (SNMP) 以允许一个网络管理系统 (NMS) 来管理网络基础设施设备，然后同时为只读和读写团体字符串配置SNMPv2c 。

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

步骤 9: 如果在您的网络中网络运维管理是集中化的，您可以借助一个访问列表来限制网络中对您设备的访问以提高网络安全性。在本例中，只有在10.4.48.0/24网络上的设备可以通过SSH或者SNMP来访问设备。

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

技术提示

如果您在vty接口配置一个访问列表，您可能无法使用SSH从一台路由器登录到下一台以进行逐跳的排错。

步骤 10: 配置本地登录和密码。

本地登录帐户和密码为具有有限操作权限的交换机提供基本的接入认证。启用密码使进入设备配置模式更安全。通过启用密码加密，防止在查看配置文件时泄露明文密码。

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

默认情况下，HTTPS 访问交换机将启用密码进行身份验证。

步骤 11: 如果您想要减少每个设备的操作任务，配置集中式用户身份验证，通过使用TACACS+协议，在基础设施设备上进行身份验证管理登录至AAA服务器。

随着网络及需要维护设备数量的增长，在每个设备上的本地用户的维护成本也在相应增加。一个集中的AAA服务，为每台设备减少日常操作的同时，也提供偶尔关于用户访问安全合规性和根源分析的审计日志。当为访问控制启用AAA，所有的网络基础设施设备的管理访问（SSH和HTTPS）都由AAA控制。

读者提示

在此架构中使用AAA服务器是Cisco ACS。如需更多关于Cisco ACS 相关配置详情，请参考Cisco IBA——《使用ACS的无边界网络设备管理部署指南》。

TACACS+是在设备上用于验证管理登录到AAA服务器的主要协议。在每个网络设备上一个本地AAA用户数据库同样在步骤 10中被定义，它提供了备用身份验证源，以防集中TACACS+服务不可用的情况。

```
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

步骤 12: 配置网络设备时钟同步到网络中的本地NTP服务器。本地NTP服务器通常参考一个来自外部源的更精确的时钟。配置控制台消息，日志和调试输出，在输出中提供时间戳，允许在网络事件上进行交叉参考。

```
ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

程序 3　应用交换机全局配置

步骤 1: 配置VLAN管理。

带外管理网络将使用一个单独的VLAN, VLAN **163**。

```
vlan [vlan number]
name DC_ManagementVLAN
```

步骤 2: 配置交换机IP地址以使它可以通过带内连接管理，并为其分配一个IP默认网关。

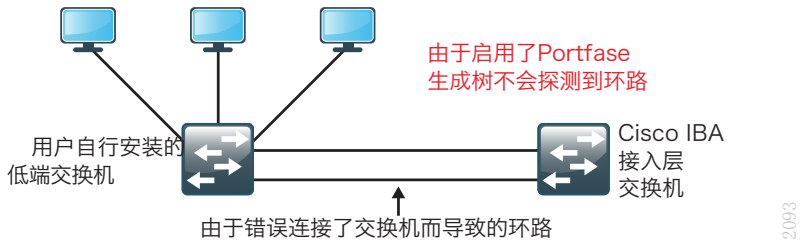
```
interface vlan [management vlan]
ip address [ip address] [mask]
no shutdown
ip default-gateway [default router]
```

步骤 3: 全局配置BPDU Guard (BPDU保护)，以保护PortFast-enabled (启用PortFast) 接口。

BPDU Guard防止用户把交换机插入到接入端口，这可能会导致灾难性的且不易被察觉的生成树环路。

如果一个PortFast-enabled 端口收到了BPDU报文，一个异常的错误一定存在，比如当一个未授权的设备连接时。在一个Portfast端口收到BPDU报文的时候，BPDU Guard特性将一个非干道接口转到errdisable (出错禁止) 状态，从而保护环路。

图 12 - BPDU保护功能保护的场景



如果插入另一台交换机的端口，关闭接口。

```
spanning-tree portfast bpduguard default
```

程序 4　配置交换机访问端口

为了简化配置，在交换机上使用**interface range**命令让相同的配置应用到多个接口上。这个命令允许您用一次命令在同一时间把它应用于多个接口，这可以节省很多时间，因为大多数接口在接入层配置是相同的。例如，下面的命令可以让您同时在所有24个接口 (Gig 0/1至Gig 0/24) 上输入命令。

```
interface range Gigabitethernet 1/0/1-24
```

步骤 1: 配置交换机接口，以支持管理接口。该主机接口配置支持管理端口连接。

```
interface range [interface type] [port number]-[port number]
switchport access vlan [163]
switchport mode access
```

步骤 2: 为主机模式配置交换机端口。因为以太网管理端口只针对终端设备连接，开启PortFast，关闭802.1Q trunking和channel group以缩短其接口进入转发状态时间。

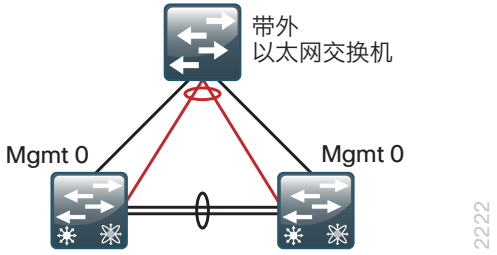
```
switchport host
```

示例: 程序 3和4

```
vlan 163
  name DC_ManagementVLAN
!
interface vlan 163
  description in-band management
  ip address 10.4.63.5 255.255.255.0
  no shutdown
!
ip default-gateway 10.4.63.1
!
spanning-tree portfast bpduguard default
!
interface range GigabitEthernet 1/0/1-22
  switchport access vlan 163
  switchport mode access
  switchport host
```

程序 5　配置交换机到三层核心链路

正如之前所描述的，可通过多种方法连接到三层，实现到数据中心带外管理网络的连接。以下步骤描述了如何配置EtherChannel以连接到数据中心核心Cisco Nexus 5500UP交换机。



步骤 1: 配置两个或多个物理接口作为EtherChannel的成员，并设定链路汇聚控制协议 (LACP) 在链路两端均保持**活跃状态**。这可确保建立适当的EtherChannel，同时不会引起任何问题。

```
interface [interface type] [port 1]
  description Link to DC Core port 1
interface [interface type] [port 2]
  description Link to DC Core port 2
interface range [interface type] [port 1], [interface type]
[port 2]
  channel-protocol lacp
  channel-group 1 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

步骤 2: 配置中继。

802.1Q中继用于连接这里的上游设备，以支持该设备为管理交换机上定义的所有VLAN提供三层服务。该中继上所支持的VLAN仅限于服务器机房交换机上活动的VLAN。

Catalyst 2960-S 不需要**switchport trunk encapsulation dot1q**命令。

```
interface Port-channel1
  description Etherchannel Link to DC Core for Layer 3
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan [management vlan]
  switchport mode trunk
  logging event link-status
  no shutdown
```

读者提示

用于支持到带外管理网络三层连接的数据中心核心Cisco Nexus 5500UP交换机配置，将在本程序 10 “配置管理交换机连接”中稍后的章节“配置数据中心核心”流程中进行介绍。

步骤 3: 保存您的管理交换机配置。

```
copy running-config startup-config
```

示例

```
interface range GigabitEthernet 1/0/23-24
  description Links to DC Core for Layer 3
  channel-protocol lacp
  channel-group 1 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
!
interface Port-channel 1
  description Etherchannel to DC Core for Layer 3
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 163
  switchport mode trunk
  logging event link-status
  no shutdown
```

流程

配置数据中心核心

1、完成物理连接

2、执行初始设备配置

3、配置QoS策略

4、配置虚拟端口通道

5、配置数据中心核心全局设置

6、配置IP路由协议

7、为VLAN配置IP路由

8、配置IP组播路由

9、配置到IBA智能业务平台局域网核心的连接

10、配置管理交换机连接

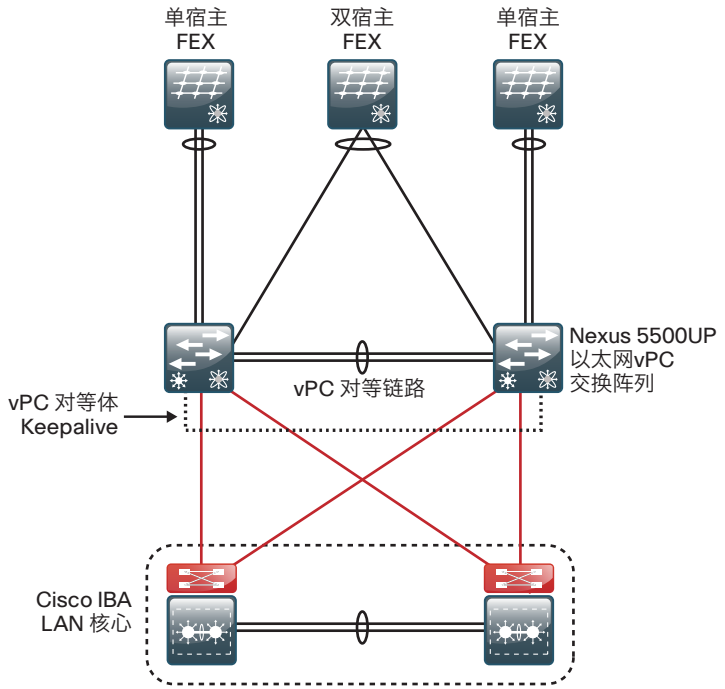
11、配置阵列扩展模块连接

12、配置终端节点端口

Cisco Nexus 5500UP系列提供了一个基于软件许可证的简单软件管理机制。这些许可证在每交换机的基础上运行，支持全套功能。数据中心核心层以三层配置为特征，因此Cisco Nexus 5500UP系列交换机需要三层许可，以支持全部的EIGRP功能。当运行本机FC（光纤通道）或FCoE（以太网光纤通道）时，需要光纤通道许可证。

程序 1　完成物理连接

根据以下阐述完成Cisco Nexus 5500UP系列交换机对的物理连接。



步骤 1： 连接两个Cisco Nexus 5500UP系列交换机间的可用以太网端口。

这些端口将用于建立vPC对等链路，它允许建立对等连接，并支持在某一个vPC端口通道的部分链路发生故障时，继续在交换机之间传输流量。建议使用至少两个链路以实现vPC对等链路永续性，您也可以添加更多链路来支持更高的交换机间流量。

步骤 2： 将每个Cisco Nexus 5500UP系列交换机上的两个可用以太网端口连接到IBA智能业务平台核心。

四个万兆以太网连接将提供到IBA智能业务平台局域网核心的永续连接，以40 Gbps的总吞吐量向企业其余部分传输数据。

步骤 3: 连接到双宿主FEX。

要利用单宿主服务器支持双宿主FEX，可将Cisco FEX上的阵列上行链路端口1和端口2连接到可用的以太网端口（每个Cisco Nexus 5500UP系列交换机上一个）。这些端口将作为一个端口通道运行，以支持双宿主Cisco FEX配置。

根据所使用的Cisco FEX型号，最多可连接4个或8个端口，以从Cisco FEX向核心交换机提供更多吞吐量。

步骤 4: 连接到单宿主FEX 。

通过将每个FEX上的阵列上行链路端口1和端口2连接到Cisco Nexus 5500UP系列交换机对仅一个成员上的两个可用以太网端口，可支持单宿主FEX连接。这些端口将形成一个端口通道，但不会被配置为vPC端口通道，因为它们的物理端口只与交换机对的一个成员相连接。

根据所使用的Cisco FEX型号，可以从Cisco FEX向核心交换机最多连接4个或8个端口，以提供更多吞吐量。

步骤 5: 连接到带外管理交换机。

在该设计中，我们将使用物理上独立的交换机来连接Cisco Nexus 5500交换机的管理端口。该管理端口将为vPC对等持活数据包提供带外管理访问和传输。vPC持活数据包是vPC运行保护机制的一部分。

程序 2 执行初始设备配置

本程序对系统设置进行配置使管理方案简化与安全。本例中使用的值和实际设置取决于您实际的网络配置。

表 2 - 用于部署示例的常用网络服务

服务	地址
域名	cisco.local
活动目录，DNS，DHCP服务器	10.4.48.10
Cisco ACS 服务器	10.4.48.15
NTP 服务器	10.4.48.17
EIGRP Autonomous System (AS)	100

步骤 1: 将一个终端线缆连接到第一个Cisco Nexus 5500UP系列交换机的控制台端口，然后对系统加电以进入初始配置对话框，从而连接到交换机控制台接口。

步骤 2: 运行设置脚本并遵循Basic System Configuration（基本系统配置）对话框，进行第一个Cisco Nexus 5500UP系列交换机的初始设备配置。该脚本将设置系统登录密码、安全外壳（SSH）登录以及管理接口地址。一些设置步骤将略过，在后面的配置步骤中介绍。

```
Do you want to enforce secure password standard (yes/no): y

  Enter the password for "admin":
  Confirm the password for "admin":

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic
configuration of
 the system. Setup configures only enough connectivity for
management
 of the system.

Please register Cisco Nexus 5000 Family devices promptly with
your
supplier. Failure to register may affect response times for
initial
service calls. Nexus devices must be registered to receive
entitled
support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/
no): y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
```

```
  Enter the switch name : dc5548ax
  Enable license grace period? (yes/no) [n]: y
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]: y
    Mgmt0 IPv4 address : 10.4.63.10
    Mgmt0 IPv4 netmask : 255.255.255.0
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : 10.4.63.1
  Configure advanced IP options? (yes/no) [n]:n  Enable the
ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) : rsa
    Number of  key bits <768-2048> : 2048
  Enable the telnet service? (yes/no) [n]: n
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : 10.4.48.17
  Configure default interface layer (L3/L2) [L3]: L2
  Configure default switchport interface state (shut/noshut)
[shut]:shut
  Configure best practices CoPP profile (strict/moderate/
lenient/none) [strict]: moderate
  Configure default switchport trunk mode (on/off/auto) [on]:
auto
  Configure default switchport port mode F (yes/no) [n]:n
  Configure default zone policy (permit/deny) [deny]:y
  Enable full zoneset distribution? (yes/no) [n]: y
  Configure default zone mode (basic/enhanced) [basic]:
The following configuration will be applied:
password strength-check
switchname dc5548ax
license grace-period
interface mgmt0
ip address 10.4.63.10 255.255.255.0
no shutdown
ip route 0.0.0.0/0 10.4.63.1
  ssh key rsa 2048 force
  feature ssh
  no feature telnet
  no feature http-server
  ntp server 10.4.48.17 use-vrf management
  system default switchport
  system default switchport shutdown
  system default switchport trunk mode auto
  system default zone default-zone permit
  system default zone distribute full
  no system default zone mode enhanced
  policy-map type control-plane copp-system-policy

Would you like to edit the configuration? (yes/no) [n]: n
Use this configuration and save it? (yes/no) [y]: y
[########################################] 100%
dc5548ax login:
```

步骤 3: 启用并配置系统特性。

鉴于Cisco NX-OS的模块化特性，只有在启用功能时，进程才启动。因此，当功能启用后，命令和命令链才会显示。针对许可特性，只有在安装了适当的许可证时，才能使用feature-name命令。Cisco Nexus 5500UP系列需要许可证来支持三层操作、FC存储协议和FCoE N-Port Virtualization (NPV) (FCoE N端口虚拟化 (NPV)) 操作。如需了解有关许可的更多信息，请访问www.cisco.com查看《Cisco NX-OS许可指南》。

本指南中的配置示例使用了以下特性:

```
feature udld
feature interface-vlan
feature lacp
feature vpc
feature eigrp
feature fex
feature hsrp
feature pim
feature fcoe
```

技术提示

虽然本设计中没有使用，但如果您的网络需要FC特定特性N端口虚拟化（NPV），则应在对交换机应用任何其它配置之前启用NPV。NPV特性是唯一在启用或禁用时，会擦除您的配置并重启交换机的特性，它要求您对交换机重新应用任何现有的配置命令。

步骤 4: 使用DNS服务器的IP地址为网络配置名称服务器命令。在Cisco IOS命令行，如果可以用域名取代输入IP地址会更加的便利。

```
ip name-server 10.4.48.10
```

步骤 5: 为设备设置本地时区。NTP为故障排错同步同一个网络中的所有设备的时间。在初始设置脚本，您已设置NTP服务器地址。现在为设备设置本地时间。

```
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00
60
```

步骤 6: 为网络管理定义一个只读和读写SNMP community属性。

```
snmp-server community cisco group network-operator
snmp-server community cisco123 group network-admin
```

步骤 7: 如果您想要减少每个设备的操作任务，通过使用TACACS+协议配置集中式用户身份验证，在基础设施设备上进行身份验证管理登录至AAA服务器。

随着网络及需要维护设备数量的增长，在每个设备上的本地用户的维护成本也在相应增加。一个集中的AAA服务，为每台设备减少日常操作的同时，也提供偶尔关于用户访问安全合规性和根源分析的审计日志。当为访问控制启用AAA，所有的网络基础设施设备的管理访问（SSH和HTTPS）都由AAA控制。

TACACS+是在基础设施设备上用于验证管理登录AAA服务器的主要协议。在每个网络基础设施设备上一个本地AAA用户数据库在每台Cisco Nexus 5500交换机设置脚本中被定义，它提供备用身份验证源以防集中TACACS+服务不可用的情况。

```
feature tacacs+
tacacs-server host 10.4.48.15 key SecretKey
aaa group server tacacs+ tacacs
  server 10.4.48.15
  use-vrf default
  source-interface loopback 0
aaa authentication login default group tacacs
```

步骤 8: 如果您的网络是集中式的运营支持，您可以使用一个访问列表限制网络中对您设备的访问来提高安全性。在此示例中，只有在10.4.48.0/24网络中的设备可以通过SSH或者SNMP访问设备。

```
ip access-list vty-acl-in
 permit tcp 10.4.48.0/24 any eq 22
line vty
 ip access-class vty-acl-in in
!
ip access-list snmp-acl
 permit udp 10.4.48.0/24 any eq snmp
snmp-server community cisco use-acl snmp-acl
snmp-server community cisco123 use-acl snmp-acl
```

技术提示

如果您在vty接口配置一个访问列表，您可能无法使用SSH从一台路由器登录到下一台以进行逐跳的排错。

步骤 9: 配置端口操作模式。在本例中，您在Cisco Nexus 5548UP 交换机上开启端口28至32作为FC端口。

```
slot 1
  port 28-32 type fc
```

Cisco Nexus 5500UP交换机拥有通用端口，能够在每个端口上运行以太网+FCoE或FC。所有交换机端口均默认启用，支持以太网运行。FC端口必须在一个连续范围内启用，且必须是交换机基板的高编号端口和/或通用端口扩展模块

的高编号端口。

技术提示

将端口类型更改为FC需要重启Cisco Nexus 5500UP NX-OS 版本5.1(3)N1(1a)软件，以识别新的端口操作。这可能会在以后的软件版本中变更。如果您不在之前步骤 3中启用特性FCoE，端口将不会在此配置中显示为FC端口。

将端口类型更改为FC需要重启Cisco Nexus 5500UP NX-OS 版本5.1(3)N1(1a)软件，以识别新的端口操作。这可能会在以后的软件版本中变更。如果您不在之前步骤 3中启用特性FCoE，端口将不会在此配置中显示为FC端口。

步骤 10: 保存您的配置，然后重新加载交换机。由于Cisco Nexus交换机需要重启才能识别为支持FC运行而配置的端口，因此这是重新加载交换机的好时机。如果您不启用FC端口操作，您就不需要在这里重新加载交换机。

```
copy running-config startup-config
reload
```

步骤 11: 在第二台Cisco Nexus 5500UP系列交换机上，重复本程序（程序 2）的所有步骤。在步骤 2中，请为mgmt0接口设定独一无二的设备名称（**dc5548bx**）和IP地址（**10.4.63.11**）。其他所有配置详情都是相同的。

程序 3 配置QoS策略

思科IBA数据中心已创建了QoS策略以匹配在思科IBA局域网和广域网的QoS配置，它们用来保护穿过数据中心的多媒体数据流，控制流量和FCoE流量。基准是在需要时您可以自定义环境。我们建议数据中心至少配置QoS FCoE，提供无丢失的数据保护。

在本程序中为Cisco Nexus 5500和2200系统全局配置QoS策略，然后定义分配给以太网端口和以太网port-channel。Cisco Nexus FEX 端口可以使用2层CoS标记队列。Cisco Nexus 5500端口可以使用2层CoS或者3层DSCP数据包标记队列分类。

系统默认的FCoE策略纳入整体思科IBA的策略以确保让FCoE设备不用更多的配置就可以整合到数据中心中来。如果未来没有在数据中心部署FCoE的需求，也可使用标准的FCoE QOS组。

创建以下配置：

- 通过**class-map type qos**和**policy-map type qos**配置进行整体系统分类，分类基于CoS关联流量关联到系统内部qos组。
- 接口分类将基于三层的DSCP值，通过**class-map type qos**和**policy-map type qos**配置将特定的IP流量关联到相应的内部的QoS组。
- 基于匹配qos组的系统队列通过**class-map type network qos**和**policy-map type network-qos**来设置2层MTU、缓冲queue-limit（队列限制）和CoS映射（到3层子卡）。
- 基于qos组的系统队列调度通过**class-map type queuing**和**policy-map type queuing**来设置对于抖动敏感的多媒体业务优先级队列，和将带宽应用到加权循环队列。分配给FCoE队列的带宽应按照保证端到端无损传输的部署要求进行分配。例如，重新分配带宽，允许FCoE分配**bandwidth percent 40**（带宽的40%），对于在10Gbps以太网中有4Gbps的FC流量连接到服务器或存储阵列这种情况下，更加合适。
- 在全系统部署QoS **service-policy**。
- 定义接口下的QoS **service-policy**，为稍后配置以太终端连接作准备。

步骤 1: 全局配置**class-map type qos**分类，匹配特定CoS位。现有系统中的class-default将自动匹配任何未标记的数据包，未匹配的CoS值，和标记为0的CoS数据包。FCoE的class-map **type qos class-fcoe**类是预先定义的，将被用于在FCoE的policy map中。

```
class-map type qos match-any PRIORITY-COS
  match cos 5
class-map type qos match-any CONTROL-COS
  match cos 4
class-map type qos match-any TRANSACTIONAL-COS
  match cos 2
class-map type qos match-any BULK-COS
  match cos 1
```

步骤 2: 全局配置**policy-map type qos**策略，创建CoS-to-internal-qos-group 映射。system-defined qos-group 0 是自动创建的，不需要任何定义。

```
policy-map type qos DC-FCOE+1P4Q_GLOBAL-COS-QOS
  class type qos PRIORITY-COS
    set qos-group 5
  class type qos CONTROL-COS
    set qos-group 4
  class type qos class-fcoe
    set qos-group 1
  class type qos TRANSACTIONAL-COS
    set qos-group 2
  class type qos BULK-COS
    set qos-group 3
```

步骤 3: 为以太接口定义 **class-map type qos** 分类，映射IP DSCP到思科Nexus 5500交换机的内部qos组。**match cos**命令用于匹配入向的带有2层CoS的流量，也一样映射到思科5500交换机3层引擎上。所有未被匹配的流量将被系统的class-default 队列处理。

```
class-map type qos match-any PRIORITY-QUEUE
   match dscp ef
   match dscp cs5 cs4
   match dscp af41
   match cos 5
class-map type qos match-any CONTROL-QUEUE
   match dscp cs3
   match cos 4
class-map type qos match-any TRANSACTIONAL-QUEUE
   match dscp af21 af22 af23
   match cos 2
class-map type qos match-any BULK-QUEUE
   match dscp af11 af12 af13
   match cos 1
```

步骤 4: 配置用于接口的 **policy-map type qos**策略，映射DSCP分类到内部qos组。接口策略是非port-channel组成员的以太接口创建的。该策略也被应用到虚拟port-channel接口上，但不是物理口上。

```
policy-map type qos DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  class PRIORITY-QUEUE
    set qos-group 5
  class CONTROL-QUEUE
    set qos-group 4
  class TRANSACTIONAL-QUEUE
    set qos-group 2
  class BULK-QUEUE
    set qos-group 3
```

步骤 5: 配置全局下的 **class-map type queuing** 分类，匹配特定的内部qos组来设定队列属性。有5个内部的qos组可以被分配，加上一个系统自动创建的qos-group 0 处理默认的CoS流量。内部qos组号不用和CoS值匹配。FCoE class-map中的**type queuing class-fcoe** 是预定义的，将用于FCoE流量的policy map。

```
class-map type queuing PRIORITY-GROUP
  match qos-group 5
class-map type queuing CONTROL-GROUP
  match qos-group 4
class-map type queuing TRANSACTIONAL-GROUP
  match qos-group 2
class-map type queuing BULK-GROUP
  match qos-group 3
```

步骤 6: 配置全局下的 **policy-map type queuing** 策略来创建适当的全系统qos组属性，包括带宽、优先级、权重和FCoE丢包scheduling（调度）。

```
policy-map type queuing DC-FCOE+1P4Q_GLOBAL-GROUP-QUEUING
  class type queuing PRIORITY-GROUP
    priority
  class type queuing CONTROL-GROUP
    bandwidth percent 10
  class type queuing class-fcoe
    bandwidth percent 20
  class type queuing TRANSACTIONAL-GROUP
    bandwidth percent 25
  class type queuing BULK-GROUP
    bandwidth percent 20
  class type queuing class-default
    bandwidth percent 25
```

步骤 7: 配置全局下的 **class-map type network-qos**，匹配全系统的队列调度。**type network-qos** 的class-map可以使用5个内部组中的一个，当然也可以使用系统创建的qos group 0。内部qos组号不用和CoS值匹配。FCoE class-map中的**type queuing class-fcoe** 是预定义的，将用于FCoE流量的policy map。

```
class-map type network-qos PRIORITY-SYSTEM
  match qos-group 5
class-map type network-qos CONTROL-SYSTEM
  match qos-group 4
class-map type network-qos TRANSACTIONAL-SYSTEM
  match qos-group 2
class-map type network-qos BULK-SYSTEM
  match qos-group 3
```

步骤 8: 配置全局下的**policy-map type network-qos** 策略来应用系统的队列调度属性。FCoE队列行为已经被配置推荐值：MTU 2158，无丢包，默认缓存79,360字节。其余的队列使用默认的queue-limit 22,720字节，MTU 1500，但有两个例外：BULK-SYSTEM 队列为iSCSI和大型数据传输分配了更多的缓存空间和巨型的MTU 9216，class-default被分配了剩余的缓存空间。

3层路由引擎要求在入向和出向设置CoS位。设置CoS保证了子网间流量处理的连续性，network-qos就是系统qos-group完成CoS标记的地方。

```
policy-map type network-qos DC-FCOE+1P4Q_GLOBAL-SYSTEM-NETWORK-QOS
  class type network-qos PRIORITY-SYSTEM
   set cos 5
  class type network-qos CONTROL-SYSTEM
    set cos 4
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos TRANSACTIONAL-SYSTEM
    set cos 2
  class type network-qos BULK-SYSTEM
     mtu 9216
    queue-limit 128000 bytes
   set cos 1
  class type network-qos class-default
    multicast-optimize
    set cos 0
```

步骤 9: 应用创建的全局策略。

```
system qos
  service-policy type qos input DC-FCOE+1P4Q_GLOBAL-COS-QOS
  service-policy type queuing input DC-FCOE+1P4Q_GLOBAL-GROUP-QUEUING
  service-policy type queuing output DC-FCOE+1P4Q_GLOBAL-GROUP-QUEUING
  service-policy type network-qos DC-FCOE+1P4Q_GLOBAL-SYSTEM-NETWORK-QOS
```

出向output的队列被**system qos** 定义如何在思科Nexus5500和FEX接口中的不同的队列中共享带宽，同时也定义了如何在思科Nexus5500 3层引擎上共享带宽。

步骤 10: 如果使用了 iSCSI，为了大数据的传输，映射iSCSI到合适的队列，可以再分类和队列中加入额外的配置。分类iSCSI流量可以用ACL的TCP端口号来实现。iSCSI的流量可以加入到现有的policy map中，将流量加入到正确的qos组。

```
ip access-list ISCSI
```

```
  10 permit tcp any eq 860 any
  20 permit tcp any eq 3260 any
  30 permit tcp any any eq 860
  40 permit tcp any any eq 3260
!
class-map type qos match-all ISCSI-QUEUE
  match access-group name ISCSI
policy-map type qos DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  class ISCSI-QUEUE
    set qos-group 3
```

技术提示

在思科Nexus 5500中，只用ACL中**permit** 来匹配QoS策略中的流量。对于更多思科Nexus 5500配置QoS策略的信息，请参考：http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/qos/513_n1_1/b_cisco_nexus_5000_qos_config_gd_513_n1_1_chapter_011.html#task_1135158

使用**show queuing interface** 命令来显示 QoS 队列状态信息 。

在步骤 4中创建的端口QoS service-policy DC-FCOE+1P4Q_INTERFACE-DSCP-QOS将在本指南稍后部分应用在:

- 思科Nexus 5500的非FEX以太端口。

  例子:

```
interface Ethernet1/1-27
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

- 思科Nexus 5500的以太port-channel端口。port-channel的成员，物理链路上并不需要policy，因为他们会从逻辑的port-channel 口继承policy。这个service policy也不需要再连接到FEX的上行链路上配置。

  例子:

```
interface port-channel 2-3 , port-channel 5 , port-channel 9
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

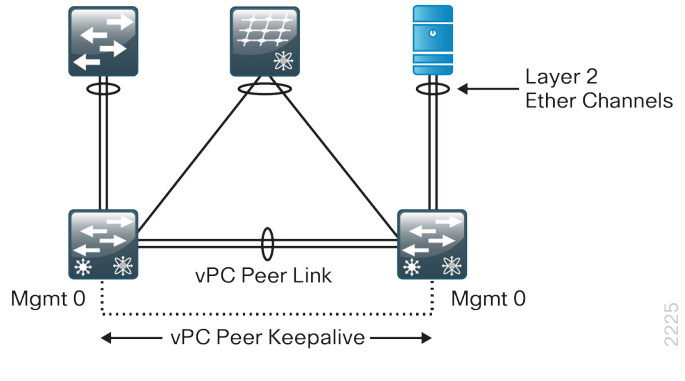
- FEX 主机端口以太接口，同时也不是port-channel的成员。

  例子:

```
interface Ethernet102/1/1-48 , interface Ethernet104/1/1-32 ,
interface Ethernet105/1/1-32
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

程序 4　配置虚拟端口通道

您必须首先在两个Cisco Nexus 5500UP系列交换机之间建立基本的vPC对等关系，然后才能在虚拟端口通道(vPC)模式下将端口通道添加到交换机。vPC对等链路在数据中心核心交换机间提供了一条通信路径，允许设备连接到每个核心交换机，以在单一的二层EtherChannel上实现永续性。



步骤 1: 设定一个vPC域号码，以方便识别成对交换机所共用的vPC域。

```
vpc domain 10
```

步骤 2: 为vPC主用交换机定义一个较低的角色优先级。

```
role priority 16000
```

vPC备用交换机将使用默认值32,667。具有较低优先级的交换机将被选作vPC主用交换机。如果vPC主用交换机在运行，而vPC对等链路中断，vPC备用交换机将暂时关闭其vPC成员端口，以防止发生环路，而vPC主用交换机的所有vPC成员端口仍将保持运行。如果对等链路发生故障，vPC对等体将通过vPC对等持活链路检测对等交换机的故障。

步骤 3: 在两个Cisco Nexus 5500交换机上配置vPC对等持活。

- 在第一个Cisco Nexus 5500UP交换机上，配置对等持活目的地地址和源地址。

```
peer-keepalive destination 10.4.63.11 source 10.4.63.10
```

- 更改目的地地址和源地址，并在第二个Cisco Nexus 5500UP交换机上进行相应配置。

```
peer-keepalive destination 10.4.63.10 source 10.4.63.11
```

对等持活链路是两个运行vPC的Cisco Nexus 5500UP交换机之间的一条理想的替代性物理路径，其作用是确保即使在主要对等链路发生故障的情况下，两个交换机也能清楚地知道对方的运行状态。对等持活源IP地址应为当前所配置交换机的mgmt0接口上使用的地址。目的地地址为vPC对等体上的mgmt0接口。

步骤 4: 在第一台Cisco Nexus 5500UP 交换机上，在vPC域配置模式下配置以下vPC命令。这将可提高永续性，优化性能和减少vPC运行的中断。

```
delay restore 360
auto-recovery
graceful consistency-check
peer-gateway
ip arp synchronize
```

auto-recovery命令拥有240秒的默认计时器。通过添加重新加载延迟变量（时间以秒计），可延长这一时间。vPC恢复的自动恢复特性可代替对原始peer-config-check-bypass特性的需求。

步骤 5: 在第一台Cisco Nexus 5500UP交换机上，创建一个端口通道接口，用作两个vPC交换机之间的对等链路。此对等链路是主要的通信链路，在需要时也用于向对等交换机转发数据流量。

```
interface port-channel 10
switchport mode trunk
vpc peer-link
spanning-treeport type network
```

步骤 6: 在第一台Cisco Nexus 5500UP交换机上，配置物理接口，将两个Cisco Nexus 5500交换机一起连接到端口通道。我们建议至少添加两个物理接口，以实现链路永续性。通道组号必须与在先前步骤中所使用的端口通道号匹配。您可以用其他的万兆以太网端口（根据您的具体部署要求）来代替示例中使用的接口。

```
interface Ethernet1/17
  description vpc peer link
  switchport mode trunk
  channel-group 10 mode active

interface Ethernet1/18
  description vpc peer link
  switchport mode trunk
  channel-group 10 mode active
```

步骤 7: 在第二台Cisco Nexus 5500UP 交换机上，重复步骤 4至步骤 6。

步骤 8: 使用**show vpc**命令，确保vPC对等关系已成功建立。

```
dc5548ax# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC
peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 55
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled

vPC Peer-link status
---------------------------------------------------------------
```

```
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------
1    Po10   up     1
```

步骤 9: 通过确保对等邻接的对等状态成功建立，且对等体的持活状态活跃，确认配置成功。如果状态显示配置未成功，请重复检查为持活源和目的地端口分配的IP地址，以及物理连接。

技术提示

如果此时命令输出界面的顶部出现“(*) - local vPC is down, forwarding via vPC peer-link”（“(*) - 本地vPC中断，将通过vPC对等链路发送流量”）语句，请不用担心。一旦您定义了vPC端口通道，如果其成员链路之一中断或尚未配置，此信息将变为图例，显示列表中您端口通道旁边的星号的含义。

程序 5 配置数据中心核心全局设置

数据中心核心需要超越设置脚本的基本核心配置。

IP子网和VLAN的分配均遵循《服务器机房部署指南》。在您查看配置指南时，您可能注意到

- IP地址字首的10.8用于Cisco IBA服务器机房设计
- IP地址字首的10.4用于Cisco IBA数据中心设计

在此部署指南中，为便于参照，我们使用了IP地址中的第三个8位字节并添加了100来确定VLAN编号。添加100可防止VLAN编号为1或0（这会导致某些设备出现问题），同时使VLAN ID易于记忆。

表 3 - Cisco IBA数据中心VLAN

VLAN	VLAN 名称	IP地址	评论
148	Servers_1	10.4.48.0/24	通用网络服务器使用
149	Servers_2	10.4.49.0/24	在“应用程序永续性”章节使用的服务器负载平衡VLAN
150	Servers_3	10.4.50.0/24	通用服务器使用
153	FW_Outside	10.4.53.0/25	用于防火墙外部接口的路由
154	FW_Inside_1	10.4.54.0/24	在“网络安全”章节中使用的防火墙保护服务器
155	FW_Inside_2	10.4.55.0/24	在“网络安全”章节中使用的防火墙IPS保护服务器
156	PEERING_VLAN	10.4.56.0/30	Cisco Nexus 5500数据中心内的三层对等链接
161	VMotion	10.4.61.0/24	为VMware VMotion流量将来使用保留
162	iSCSI	10.4.62.0/24	为iSCSI存储流量保留
163	DC-Management	10.4.63.0/24	带外数据中心管理VLAN

步骤 1: 为数据中心运行创建必要的VLAN。

```
vlan [vlan number]
 name [vlan name]
```

步骤 2: 配置生成树。

快速每VLAN生成树(PVST+)提供了每VLAN RSTP (802.1w)的实例。与传统的生成树(802.1D)相比，快速PVST+大大提高了检测间接故障或链接恢复事件的能力。Cisco Nexus 5500UP默认运行快速PVST+。

虽然此架构的构建无需任何二层环路，但向核心交换机分配生成树根是一个很好的实践。这种设计为VLAN的一个范围指定生成树的根，其可以被包含在数据中心。

- 将主用Cisco Nexus 5500UP交换机配置为生成树根。

```
spanning-tree vlan 1-400 root primary
```

- 将第二个Cisco Nexus 5500UP交换机配置为备用生成树。

```
Spanning-tree vlan 1-400 root secondary
```

步骤 3: 配置带内管理接口。本示例使用带有32位地址（主机）掩码的数据中心核心寻址之外的IP地址。

```
interface loopback 0
ip address 10.4.56.254/32
ip pim sparse-mode
```

回环接口是一个逻辑接口，只要设备通电且IP接口能接入网络，它就始终可连接。由于这一能力，回环地址是管理交换机带内的最佳方式，可向带外管理接口提供额外的管理点。三层进程和功能也捆绑于此回环接口，以确保进程永续性。

第二个Cisco Nexus 5500UP交换机的回环接口将为**10.4.56.253/32**。

步骤 4: 配置EtherChannel端口通道，以使用三层IP地址和第四层端口号进行负载均衡哈希计算。这可优化EtherChannel链路上的负载均衡，并提高到Cisco Nexus 5500UP交换机中三层路由引擎的吞吐率。

```
port-channel load-balance ethernet source-dest-port
```

程序 6 配置IP路由协议

步骤 1: 将EIGRP配置为IP路由协议。

```
router eigrp 100
  router-id 10.4.56.254
```

第二个Cisco Nexus 5500UP交换机的路由器ID将为**10.4.56.253/32**。

EIGRP是数据中心使用的IP路由协议，可兼容Cisco IBA基础局域网核心和广域网。本示例采用同一路由进程ID，以便能够与局域网核心交换路由。

在此配置中，唯一在EIGRP进程(router eigrp 1)中配置的参数是路由器ID。EIGRP路由器ID使用回环**0** IP地址。

步骤 2: 在三层接口上配置EIGRP。

```
interface loopback 0
ip router eigrp 100
```

Cisco NX-OS路由配置采用以接口为中心的模式。EIGRP需要逐个接口启用，而非添加网络，通过网络声明进行广播。如果三层接口连接有一个需要通过EIGRP进行广播的网络，则需要使用**ip router eigrp**声明。

步骤 3: 配置核心层三层对等链路。

```
Interface Vlan 156
  ip address 10.4.56.1/30
  ip router eigrp 100
  ip pim sparse-mode
  no shutdown
```

要在路由对等体间传递EIGRP路由更新，EIGRP必须在三层链路的每一端启用。为了避免跨所有数据中心VLAN交换虚拟接口的核心数据中心交换机间的不必要EIGRP对等，一条链路将用于支持数据中心核心内的活动EIGRP对等。

对等Cisco Nexus 5500UP交换机将使用IP地址**10.4.56.2/30**。

程序 7 为VLAN配置IP路由

每个需要VLAN之间或者VLAN与网络其余部分之间的三层可达性的VLAN，都需要三层交换虚拟接口（SVI），以从/向VLAN路由数据包。

步骤 1: 配置SVI。

```
interface Vlan [vlan number]
```

步骤 2: 为SVI接口配置IP地址。

```
ip address [ip address]/mask
```

步骤 3: 在SVI上禁用IP redirect （IP重定向）。我们建议在vPC环境下，在SVI上禁用ICMP IP redirect。

```
no ip redirects
```

步骤 4: 在接口上配置EIGRP进程号。这可向EIGRP通告子网。

```
ip router eigrp 100
```

步骤 5: 配置被动模式EIGRP操作。为了避免不必要的EIGRP对等处理，服务器VLAN为被动配置。

```
ip passive-interface eigrp 100
```

步骤 6: 配置热备份路由协议（HSRP）。Nexus 5500UP交换机使用HSRP在vPC环境中提供永续的默认网关。为了便于使用，使HSRP组号与SVI VLAN编号保持一致。为主用HSRP对等体配置大于100的优先级，使第二个交换机保持100的默认优先级。

```
hsrp [group number]
priority [priority]
ip [ip address of hsrp default gateway]
```

技术提示

两个数据中心核心Cisco Nexus 5500UP交换机均能够为其SVI的指定ip地址和HSRP地址处理数据包。在vPC环境中，到任一指向默认网关（HSRP）地址的交换机的数据包会在本地进行切换，无需调节积极的HSRP计时器来改进收敛时间。

- 以下是第一个Nexus 5500UP交换机的配置示例。

```
interface Vlan148
  no ip redirects
  ip address 10.4.48.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 148
    priority 110
    ip 10.4.48.1
  no shutdown
  description Servers_1
```

- 以下是对等Nexus 5500UP交换机的配置示例。

```
interface Vlan148
  no ip redirects
  ip address 10.4.48.3/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 148
    ip 10.4.48.1
  no shutdown
  description Servers_1
```

程序 8　配置IP组播路由

思科IBA智能业务平台基础局域网网络支持使用**pim sparse-mode（pim稀疏模式）**操作为企业实现IP组播路由。该网络其余部分的IP组播配置可在思科IBA智能业务平台——《无边界网络局域网部署指南》中找到。

步骤 1: 配置数据中心核心交换机，从Cisco IBA 局域网核心发现IP组播汇聚点（RP）。每个三层交换机和路由器必须被配置用来发现IP组播RP。**ip pim auto-rp forward listen**命令允许通过**ip pim sparse-mode**链接来发现。

```
ip pim auto-rp forward listen
```

步骤 2: 为核心Cisco Nexus 5500UP交换机间的IP组播复制同步配置一个未使用的VLAN。

```
vpc bind-vrf default vlan 900
```

步骤 3: 当有一个vPC的孤立端口时，将IP组播配置为仅在vPC对等链路上进行复制。

技术提示

用于IP组播**bind-vrf**的VLAN不会出现在Cisco Nexus 5500UP交换机配置中的任何其它地方。它不能在VLAN数据库命令中进行定义，也不能包括在针对vPC核心的VLAN允许列表中。它将在需要时跨整个vPC对等链路主干自动安排数据包复制。

```
no ip igmp snooping mrouter vpc-peer-link
```

步骤 4: 采用**pim sparse-mode**命令，为IP组播操作配置所有三层接口。

```
ip pim sparse-mode
```

不必在管理VLAN接口（接口vlan 163）上配置ip组播。

程序 9　配置到IBA智能业务平台局域网核心的连接

虚拟端口通道不支持跨vPC与另一个三层路由器建立对等关系。本设计将在每个数据中心核心Cisco Nexus 5500UP交换机与每个Cisco Catalyst 6500 VSS核心局域网交换机之间使用双宿主点对点三层接口，以支持在数据中心和网络其余部分之间传输的数据。如果您的设计拥有单一的永续Cisco Catalyst 4500、冗余管理程序和冗余线路卡，您将可连接每个数据中心Cisco Nexus 5500UP交换机到每个冗余线路卡。

表 4 - 数据中心到独立Catalyst 6500交换机的局域网核心的示例

数据中心核心			局域网核心		
交换机	端口	IP地址	IP地址	C6500-1	C6500-2
dc5548a	e1/19	10.4.40.50	10.4.40.49	Te 4/7	—
	e1/20	10.4.40.58	10.4.40.57	—	Te4/7
dc5548b	e1/19	10.4.40.54	10.4.40.53	Te4/8	—
	e1/20	10.4.40.62	10.4.40.61	—	Te4/7

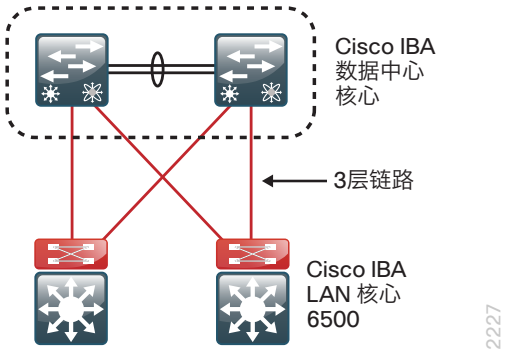
表 5 - 数据中心到Catalyst 6500 VSS对的紧缩局域网核心示例

数据中心核心			局域网核心	
交换机	端口	IP地址	IP地址	C6500VSS
dc5548a	e1/19	10.4.40.50	10.4.40.49	Te1/4/6
	e1/20	10.4.40.58	10.4.40.57	Te2/4/6
dc5548b	e1/19	10.4.40.54	10.4.40.53	Te1/4/8
	e1/20	10.4.40.62	10.4.40.61	Te2/4/8

表 6 - 数据中心到Catalyst 4500的紧缩局域网核心示例

数据中心核心			局域网核心	
交换机	端口	IP地址	IP地址	C4500
dc5548a	e1/19	10.4.40.50	10.4.40.49	Te1/4
	e1/20	10.4.40.58	10.4.40.57	Te2/4
dc5548b	e1/19	10.4.40.54	10.4.40.53	Te1/7
	e1/20	10.4.40.62	10.4.40.61	Te2/7

建议您至少将每个交换机的两个物理接口连接到网络核心，以建立包含四个永续的物理万兆以太网链路的端口通道，并实现40Gbps的吞吐率。



步骤 1: 在第一个数据中心核心Cisco Nexus 5500UP上，配置两个点对点三层接口。

```
interface Ethernet1/19
  description Core-1 Ten4/7
  no switchport
  ip address 10.4.40.50/30
  ip router eigrp 100
  ip pim sparse-mode

interface Ethernet1/20
  description Core-2 Ten4/7
  no switchport
  ip address 10.4.40.58/30
```

```
 ip router eigrp 100
 ip pim sparse-mode
```

步骤 2: 在第二个数据中心核心Cisco Nexus 5500UP交换机上，配置两个点对点三层接口。

```
interface Ethernet1/19
  description Core-1 Ten4/8
  no switchport
  ip address 10.4.40.54/30
  ip router eigrp 100
  ip pim sparse-mode

interface Ethernet1/20
  description Core-2 Ten4/8
  no switchport
  ip address 10.4.40.62/30
  ip router eigrp 100
  ip pim sparse-mode
```

步骤 3: 在思科IBA智能业务平台局域网核心6500交换机上，配置四个相应的点对点三层链路。

- 在第一个Cisco Catalyst 局域网核心交换机上，配置两个链接。

```
interface TenGigabitEthernet4/7
 description DC5548a Eth1/19
 no switchport
 ip address 10.4.40.49 255.255.255.252
 ip pim sparse-mode
 macro apply EgressQoS

interface TenGigabitEthernet4/8
 description DC5548b Eth1/19
 no switchport
 ip address 10.4.40.53 255.255.255.252
 ip pim sparse-mode
 macro apply EgressQoS
```

- 在第二个Cisco Catalyst 局域网核心交换机上，配置两个链接。

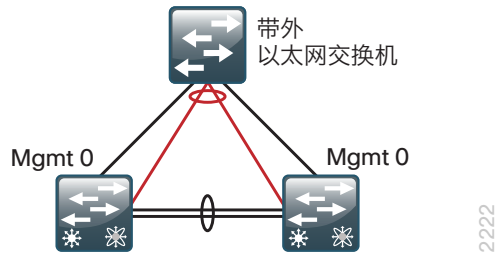
```
interface TenGigabitEthernet4/7
 description DC5548a Eth1/20
 no switchport
 ip address 10.4.40.57 255.255.255.252
 ip pim sparse-mode
 macro apply EgressQoS

interface TenGigabitEthernet4/8
 description DC5548b Eth1/20
 no switchport
 ip address 10.4.40.61 255.255.255.252
 ip pim sparse-mode
 macro apply EgressQoS
```

此时，您应能够在核心Cisco Nexus 5500UP交换机上看到来自网络其余部分的IP路由。

程序 10　配置管理交换机连接

“以太网基础设施”章节的第一个程序涵盖部署带外以太网管理交换机。在那个程序中，您配置了支持二层操作的交换机以及到数据中心核心的上行链路，作为提供管理VLAN三层访问的一个选项，以支持数据中心之外的访问。如果您选择了这一操作来提供三层对带外以太网VLAN访问，那么请遵循这一程序来对上行链路和Cisco Nexus 5500UP交换机上的三层SVI进行编程。

为实现永续性，以太网带外管理交换机将使用vPC端口通道，与每个数据中心核心交换机建立双宿主连接。



步骤 1: 配置以太网带外管理VLAN。您将在每个数据中心核心Cisco Nexus 5500UP交换机上配置相同的值。

```
vlan 163
```

```
  name DC_Management
```

步骤 2: 配置到以太网管理交换机的vPC端口通道。您将在每个数据中心核心Cisco Nexus 5500UP交换机上配置相同的值。

```
interface port-channel21
  description Link to Management Switch for VL163
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
  vpc 21
```

步骤 3: 配置属于端口通道的物理端口。您将在每个数据中心核心Cisco Nexus 5500UP交换机上配置相同的值。

```
interface Ethernet1/21
  description Link to Management Switch for VL163
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
```

步骤 4: channel-group 21 mode active为VLAN163配置一个SVI接口。

- 配置第一个数据中心核心Cisco Nexus 5500UP交换机。

```
interface Vlan163
  description DC-Management
  no ip redirects
  ip address 10.4.63.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  hsrp 163
    priority 110
    ip 10.4.63.1
no shutdown
```

- 配置第二个数据中心核心Cisco Nexus 5500UP交换机。

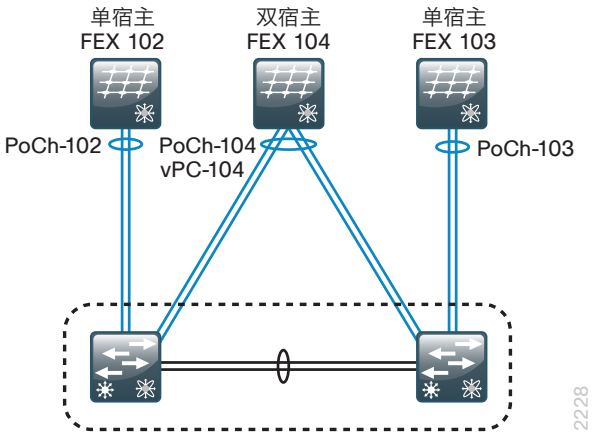
```
interface Vlan163
  description DC-Management
  no ip redirects
  ip address 10.4.63.3/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  hsrp 163
    ip 10.4.63.1
no shutdown
```

程序 11 配置阵列扩展模块连接

Cisco Fabric Extender (FEX) (思科阵列扩展模块 (FEX)) 端口设计用于支持终端主机连接。在将设备连接到Cisco FEX端口时, 需要注意一些设计规则:

- Cisco FEX端口不支持持到产生生成树网桥协议数据单元 (BPDU) 数据包的局域网交换机的连接。如果一个Cisco FEX端口接收到BPDU数据包, 它将以Error Disable状态关闭。
- Cisco FEX端口不支持到三层路由端口的连接 (路由协议在此处与三层核心进行交换) , 它们仅用于二层连接的终端主机或设备。
- 运行三层路由的Cisco Nexus 5500UP交换机在一个交换机上最多支持8个连接的Cisco FEX。
- 思科阵列扩展模块连接也可配置为Cisco Nexus 5500系列交换机上上行链路的永续性和负载共享的端口通道连接。
- 如果要将Cisco FEX以单归属方式连接到交换机对中的一个成员, 可将其配置为一个标准端口通道。
- 如果要将Cisco FEX以双归属方式连接到vPC交换机对中的两个成员以支持单归属服务器或为了增加永续性, 可将其配置为一个vPC port channel。每一个连接到双归属FEX的终端节点或服务器在逻辑上是双归属到Cisco Nexus 5500核心交换机的, 且有一个系统自动生成的vPC针对以太网FEX

边缘端口。



在为Cisco FEX分配编号时，您可以使用与某些其他标识符相对应的编号方法（与示例不同的方法），比如您的环境所使用的机架号码。

Option 1. 配置单宿主FEX

一个单宿主FEX需要在已连接的Cisco Nexus 5500交换机上配置FEX和上行链路。

步骤 1: 在已连接的Cisco Nexus 5500交换机上将物理接口分配到支持Cisco FEX连接的端口通道。这些以太网接口形成已连接的FEX上行端口通道。

```
interface Ethernet1/13
channel-group 102
!
interface Ethernet1/14
  channel-group 102
```

步骤 2: 配置端口通道接口来支持单宿主 FEX连接。**switchport mode fex-fabric**命令将告知Cisco Nexus 5500UP系列交换机：一个阵列扩展模块应该位于此链路的另一端。

```
interface port-channel102
description single-homed 2248
switchport mode fex-fabric
fex associate 102
```

步骤 3: 配置第二个单宿主至第二个Cisco Nexus 5500交换机。

```
interface Ethernet1/13
channel-group 103
!
interface Ethernet1/14
  channel-group 103
!
interface port-channel103
description single-homed 2248
switchport mode fex-fabric
fex associate 103
```

Option 2. 配置双宿主FEX

一个单宿主FEX需要同时在已连接的两个Cisco Nexus 5500交换机上配置FEX和上行链路。

步骤 1: 在第一个已连接的Cisco Nexus 5500交换机上将物理接口分配到支持Cisco FEX连接的端口通道。这些以太网接口形成已连接的FEX上行端口通道。

```
interface Ethernet1/25
  channel-group 104
!
interface Ethernet1/26
  channel-group 104
```

步骤 2: 在第一个已连接的Cisco Nexus 5500交换机上配置端口通道接口来支持双宿主 FEX连接。**switchport mode fex-fabric**命令将告知Cisco Nexus 5500UP系列交换机：一个阵列扩展模块应该位于此链路的另一端。**vpc**命令为双宿主FEX创建一个双宿主端口通道。

```
interface port-channel104
description dual-homed 2232
switchport mode fex-fabric
fex associate104
  vpc 104
```

步骤 3: 在第二个已连接的Cisco Nexus 5500交换机上重复此配置。

```
interface Ethernet1/25
  channel-group 104
!
interface Ethernet1/26
  channel-group 104
!
interface port-channel104
  description dual-homed 2232
  switchport mode fex-fabric
  fex associate 104
  vpc 104
```

在为FEX连接模式完成这些配置之后，您可以重启FEX并利用**show fex**命令查看阵列扩展模块的状态，看看每个组件是否都处在联机状态。

```
dc5548ax# show fex
FEX     FEX         FEX                       FEX
Number  Description State   Model             Serial
------------------------------------------------------
102     FEX0102     Online  N2K-C2248TP-1GE   SSI14140643
104     FEX0104     Online  N2K-C2232PP-10GE  SSI142602QL
```

技术提示

编程后Cisco FEX联机可能需要几分钟时间，因为Cisco FEX在初始化启动时需要从相连的Cisco Nexus交换机上下载操作代码。

程序 12　配置终端节点端口

当为服务器或者设备连接配置Cisco Nexus FEX 以太网端口时，您必须在一个或同时在两个Cisco Nexus 5500UP 核心交换机上配置端口，这取决于FEX连接是单宿主还是双宿主。

Option 1. 单宿主服务器连接双宿主FEX

由于服务器被连接到一个双宿主FEX，因此配置必须在两个Cisco Nexus 5500UP数据中心核心交换机上完成。spanning-tree模式，VLAN列表，和其他特征的以太网端口在每个Cisco Nexus 5500UP交换机上应使用相同的编程。

步骤 1: 将单宿主服务器连接到双宿主Cisco FEX时，分配物理接口以支持属于单一VLAN的服务器或设备作为访问端口。将生成树端口类型设定为**edge**，允许端口能够在一个新设备接入后立即为其提供连接。为已连接的服务器或者在程序 3 “配置QoS策略”中定义的终端节点开启QoS分类。

例子

```
interface Ethernet103/1/1
switchport access vlan 163
spanning-tree port type edge
service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

技术提示

鉴于主机在一个双宿主Cisco FEX上，那主机也是双宿主的，您必须在两个数据中心核心Cisco Nexus 5500UP交换机上分配以太网接口配置。如果在Nexus 5500交换机上未能配置相应的VLAN端口，以太网接口就无法被激活。

步骤 2: 将单宿主服务器连接到双宿主Cisco FEX时，分配物理接口以支持需要VLAN中继接口来与多个VLAN进行通信的服务器或设备。多数虚拟化服务器要求配备trunk接入以支持管理访问和多个虚拟机的用户数据。将生成树端口类型设定为**edge**，允许端口能够在一个新设备接入后立即为其提供连接。为已连接的服务器或者在程序 3 “配置QoS策略”中定义的终端节点开启QoS分类。

由于服务器被连接到一个双宿主FEX，因此配置必须同时在两个Cisco Nexus 5500UP 数据中心核心交换机上完成。

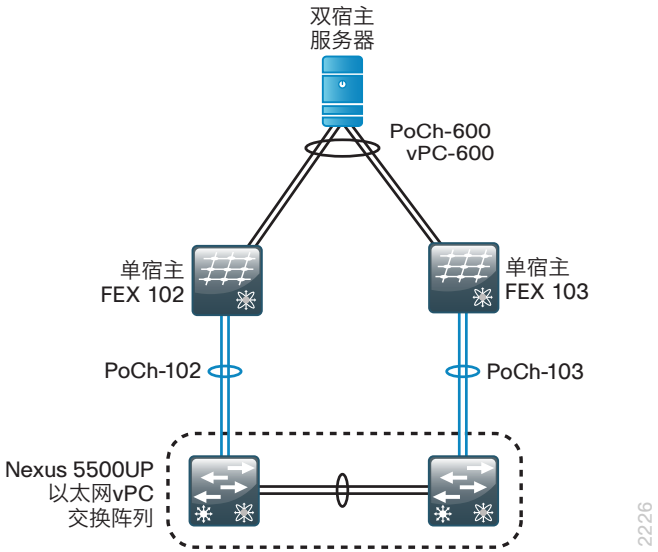
例子

```
interface Ethernet103/1/2
switchport mode trunk
switchport trunk allowed vlan 148-163
```

```
spanning-tree port type edge trunk
service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

Option 2. 使用以太网通道连接两个单宿主FEX的双宿主服务器

由于服务器是双宿主的且使用vPC以太网通道，因此配置必须同时在两个Cisco Nexus 5500UP 数据中心核心交换机上完成。



在将使用IEEE 802.3ad EtherChannel的双宿主服务器从服务器连接到一对单宿主Cisco FEX时，您必须在Cisco FEX上配置以太网接口作为一个端口通道，并分配一个vPC接口以便与连接的服务器进行EtherChannel通信。

例子

步骤 1: 在第一个Cisco Nexus 5500交换机上。

```
interface ethernet102/1/1
switchport mode trunk
switchport trunk allowed vlan 148-163
spanning-tree port type edge trunk
  channel-group 600
  no shutdown
interface port-channel 600
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 600
  no shutdown
```

步骤 2: 在第二个Cisco Nexus 5500交换机上。

```
interface ethernet103/1/1
switchport mode trunk
switchport trunk allowed vlan 148-163
spanning-tree port type edge trunk
  channel-group 600
  no shutdown
interface port-channel 600
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
  vpc 600
  no shutdown
```

技术提示

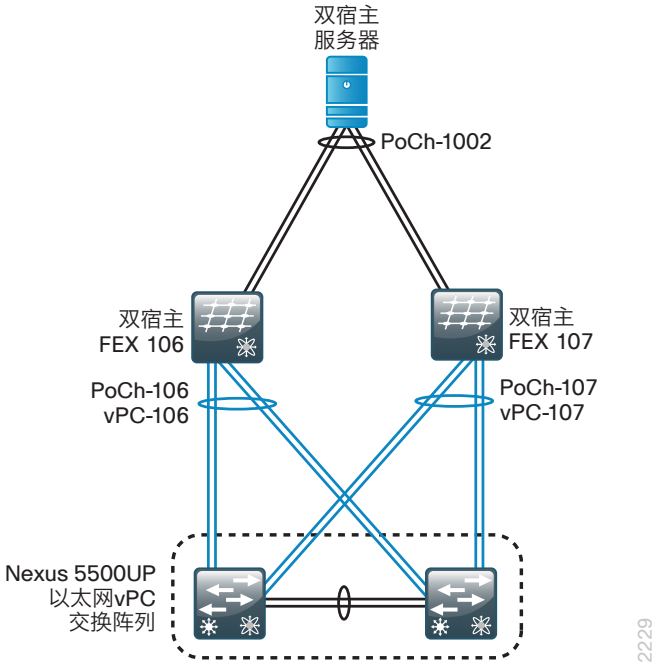
当通过vPC连接端口时，Cisco NX-OS会执行一致性检查，以确保构成vPC的每个交换机上配置的各端口之间的VLAN列表、生成树模式及其它特征相匹配。如果每个端口的配置与另一个不相同，该端口将无法使用。

Option 3. 双宿主服务器使用EtherChannel连接到两个双宿主FEX

本选项，称为增强的vPC，需要思科Nexus 5500交换机NX-OS release 5.1(3)N1(1)或更新版本。双宿主服务器使用EtherChannel连接到双宿主FEX并不在老版本的思科Nexus 5500上支持。

当连接一个使用IEEE 802.3ad EtherChannel的双宿主服务器到一对双宿主的思科FEX时，您必须配置以太网接口的每个思科FEX接口为port channel，

而不是vPC。思科 Nexus 5500会会自动创建一个vPC来追踪双归属的port channel。



在这个配置选项，您使用FEX数字106和107。两个FEX都应该配置为双宿主，连接至Cisco Nexus 5500数据中心核心交换机，正如选项2“配置双宿主FEX”中定义的。

步骤 1: 在第一个核心Cisco Nexus 5500交换机上为一个到服务器的端口通道配置第一个双宿主FEX以太网接口。

```
interface ethernet106/1/3-4
  channel-group 1002
```

步骤 2: 在第一个核心Cisco Nexus 5500交换机上为一个到服务器的端口通道配置第二个双宿主FEX以太网接口。

```
interface ethernet107/1/3-4
  channel-group 1002
```

步骤 3: 配置支持VLAN的端口通道。

```
interface port-channel 1002
  switchport mode trunk
  switchport trunk allowed vlan 148-163
  spanning-tree port type edge trunk
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

步骤 4: 对具有相同设置的第二个核心Cisco Nexus 5500交换机重复此命令，因为服务器和FEX都是双宿主的。

```
interface ethernet106/1/3-4
  channel-group 1002
!
interface ethernet107/1/3-4
  channel-group 1002
!
interface port-channel 1002
switchport mode trunk
switchport trunk allowed vlan 148-163
spanning-tree port type edge trunk
service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

存储基础设施

业务概述

当今企业对存储的需求是永无止境的。用于服务器的存储能够以物理方式直接连接到服务器或经由网络与之相连。直接连接存储(DAS)与单一服务器物理连接，由于它只能由与其相连的主机使用，所以使用效率较低。存储区域网络(SAN)允许多个服务器通过FC（光纤通道）或以太网网络共享一个存储池。这种能力使存储管理员可以轻松扩展支持数据密集型应用的服务器的容量。

技术概述

基于IP的存储选项

许多存储系统都提供了在以太网上使用IP访问存储的选项。利用这种方式，发展中企业能够受益于集中存储的优势，而无需部署和管理一个独立的FC（光纤通道）网络。基于IP的存储连接选项包括互联网小型计算机系统接口（iSCSI）和网络连接存储（NAS）。

iSCSI是一个支持服务器通过IP链路连接到存储的协议，它能够替代FC（光纤通道）且成本较低。因为服务器上的iSCSI服务必须与其他网络应用一起争用CPU和带宽，所以您需要确保服务器的处理能力和性能适用于特定应用。iSCSI目前已成为大多数服务器、存储和应用厂商支持的存储技术。iSCSI提供对原始磁盘资源的区块级存储访问，类似于FC（光纤通道）。网卡也能将iSCSI卸载到一个独立处理器，以提高性能。

网络连接存储（NAS）是一个广义术语，指一组通用文件访问协议，最常见的即是使用通用互联网文件系统（CIFS）或网络文件服务器（NFS）。CIFS最初起源于微软网络环境，是一个通用桌面文件共享协议。NFS则是一个源自UNIX环境的多平台协议，它可用于共享管理程序存储。这两个NAS协议都提供对于共享存储资源的文件级访问。

大多数企业都拥有大量应用，须通过多种存储访问技术访问。例如，通过FC（光纤通道）访问高性能数据库和生产服务器，通过NAS访问桌面存储等。

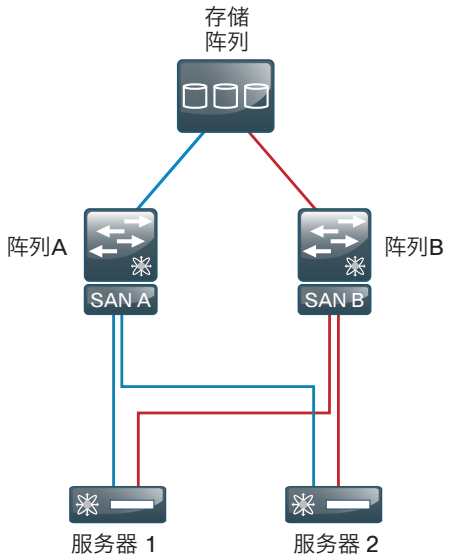
FC（光纤通道）存储

FC可支持服务器通过基于IP的光纤通道跨光纤网络、数据中心甚或广域网与存储相连。多台服务器能够共享一个存储阵列。

思科IBA智能业务平台数据中心设计使用Cisco Nexus 5500UP系列交换机作为核心，提供FC（光纤通道）和FCoE（以太网光纤通道）SAN交换。Cisco Nexus 5500UP通过支持FC和FCoE服务器与存储阵列，可提供紧缩的FC连接要求所需的密度。Cisco MDS 9148多层阵列交换机是构建具有多达48个FC端口的大型SAN阵列的理想选择，提供48个线速8-GbpsFC端口，以及经济高效的可扩展性。思科多层SAN阵列交换机的MDS系列还可提供诸如基于硬件的加密服务、磁带加速和基于IP的FC等选项，支持更长距离的SAN扩展。

在SAN中，阵列由与FC交换机相连的服务器和存储组成（参见图 13）。SAN中的标准做法是，创建两个完全独立的物理阵列，提供两条与存储相连的不同路径。每个阵列上的FC阵列服务都独立运行，以便当服务器需要永续连接到一个存储阵列时，它与两个独立阵列相连。这种设计能够防止一个阵列中的故障或误配置影响另一个阵列。

图 13 - 采用单一磁盘阵列的双阵列SAN



SAN上的每个服务器或主机都通过一条来自主机总线适配器（HBA）的多模光纤电缆，连接到FC交换机。为实现永续连接，每个主机通过一个端口与每个阵列相连。

每个端口都有一个端口全局名称（pWWN），代表了该端口在网络上的唯一识别地址。pWWN的一个示例如下：10:00:00:00:c9:87:be:1c。在数据网络中，这一地址类似于以太网适配器的MAC地址。

虚拟存储区域网络

虚拟存储区域网络(VSAN)是思科根据以太网中虚拟局域网（VLAN）概念创造的一项技术。它能够支持在单台Cisco MDS 9100系列交换机上创建多个逻辑SAN阵列。每个VSAN均有其各自的一组服务和地址空间，可防止一个VSAN中发生的问题影响到其它VSAN。过去，企业通常的做法是为生产、备份、实验室和部门环境构建物理上相独立的阵列。VSAN支持在单台物理交换机上创建所有这些阵列，同时能够提供与使用独立交换机完全相同的保护水平。

分区

术语目标(target)和启动器(initiator)将贯穿于本部分。目标指磁盘或磁带设备。启动器指对磁盘或磁带进行访问的服务器或设备。

分区为限制连接到SAN的设备之间的可见性和连接性提供了一种途径。通过使用分区服务，管理员能够控制启动器可以看到的目标。这一服务在阵列中非常常见，任意对于分区配置的变更均会对整个互联阵列造成破坏。

基于启动器的分区通过使用最终主机的全局名称（WWN），能够让分区摆脱对于端口的依赖。当主机线缆被移动到一个不同的端口时，如果该端口仍属同一VSAN的成员，主机将能够继续工作。

设备别名

当在Cisco MDS 9000系列交换机上配置诸如分区、服务质量（QoS）和端口安全性等特性时，必须指定WWN。WWN命名格式非常繁琐，人工输入WWN很容易出现错误。设备别名为SAN阵列中的WWN提供了一种简单易用的命名格式（例如：使用“p3-c210-1-hba0-a”而非“10:00:00:00:c9:87:be:1c”）。

使用一个方便的命名，使启动器和目标识别容易。例子如下所示，p3-c210-1-hba0-a在本设置中代表：

- 机架位置：p3
- 主机类型：c210
- 主机编号：1
- HBA编号：hba0
- HBA上的端口：a

测试的存储阵列

在本部署指南的测试与验证中使用的存储阵列为EMC CX4-120和NetApp FAS3200。这一特定的存储阵列配置可能发生变化。请参阅相关存储厂商的安装说明。如需了解面向FC（光纤通道）主机总线适配器和存储阵列的思科互操作性支持矩阵，可访问：http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/interoperability/matrix/intmatrx.html

技术提示

具体接口、地址和设备别名均为实验室示例。您的WWN地址、接口和设备别名可能有所差异。

部署详情

本节包含的部署示例包括:

- 配置基于Cisco Nexus 5500UP的SAN网络以支持基于FC (光纤通道) 的存储。
- Cisco MDS SAN交换机的配置可支持高密度FC (光纤通道) 环境。
- FCoE使用Cisco Nexus 5500访问Cisco UCS C系列服务器的存储。

流程

在Cisco Nexus 5500UP交换机上配置光纤通道SAN

1、配置光纤通道操作

2、配置VSAN

3、配置光纤通道端口

4、配置设备别名

5、配置分区

6、验证配置

完成以下每个程序, 以在数据中心核心Cisco Nexus 5500UP交换机上配置FC (光纤通道) SAN。

程序 1　配置FC (光纤通道) 操作

Cisco Nexus 5500UP交换机拥有通用端口, 能够基于每个端口运行以太网+FCoE或FC。所有交换机端口均默认启用, 支持以太网运行。FC端口必须在一个连续范围内启用, 且必须是交换机基板的高编号端口和/或通用端口扩展模块的高编号端口。

读者提示

此程序的第一部分已在本指南中程序 2, "配置数据中心核心" 流程, "以太网基础设施" 章节概述过。如果您已配置了用于FC操作的端口, 那么您可以略过此程序的步骤 1至步骤 3。

在本设计中, 我们将在Cisco Nexus 5548UP交换机上启用端口28至32作为FC端口。

步骤 1: 为FC配置通用端口模式。

```
slot 1
  port 28-32 type fc
```

技术提示

将端口类型更改为**fc**需要重启Cisco Nexus 5500UP版本5.1(3)N1(1a)软件, 以识别新的端口操作。这可能会在以后的软件版本中变更。如果您不在以前的步骤中启用特性FCoE, 端口将不会在此配置中显示为 "fc" 端口。

步骤 2: 如果您此次更改了端口类型, 则保存您的配置并重启交换机, 以便该交换机能够识别出新的 "**fc**" 端口类型操作。如果您已完成这一操作, 则无需重启。

步骤 3: 如果您尚未完成这一操作，则启用FCOE操作，这可同时启用本机FC和FCoE操作。

```
feature fcoe
```

步骤 4: 启用SAN端口通道中继操作和FC（光纤通道）N端口ID虚拟化，以连接到Cisco UCS互联阵列。

```
feature npiv
feature fport-channel-trunk
```

读者提示

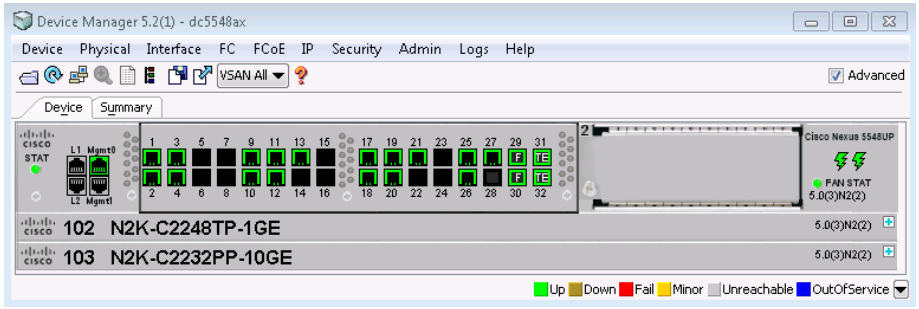
如需了解有关连接到支持FC（光纤通道）操作的Cisco UCS B系列互联阵列的更详细信息，请参阅思科IBA智能业务平台—《数据中心统一计算系统部署指南》。

程序 2 配置VSAN

针对SAN Essentials Edition 的思科数据中心网络管理器（DCNM）是一个免费应用，可用来配置和管理Cisco MDS及Cisco Nexus SAN交换机，您可以从以下位置下载：http://www.cisco.com。针对SAN Essentials的DCNM包括Cisco MDS设备管理器和Cisco SAN 阵列管理器。如果需要在同时管理一个以上的交换机则要求使用授权版本。

使用CiscoDCNM设备管理器管理交换机需要连接交换机的管理IP地址。CLI可以用来配置FC操作。

运行Cisco DCNM阵列管理器和设备管理器需要Java运行环境（JRE），用户应当在使用任一应用之前在桌面上安装这一环境。



默认情况下，交换机初始化时会将所有端口分配给VSAN 1。最佳实践是为生产环境创建一个独立VSAN，并将VSAN 1用于未使用的端口。通过不使用VSAN 1，在组合其它可能设置为VSAN 1的现有交换机时，您可以避免未来合并VSAN的相关问题。

FC以SAN-A和SAN-B方法运行，在那里您可创建两个单独的SAN阵列。FC主机和目标连接到两个阵列，以实现冗余。SAN阵列并行运行。

以下示例中创建了两个VSAN，每个数据中心核心CiscoNexus 5500UP交换机上一个。

您可使用CLI或设备管理器来创建VSAN。

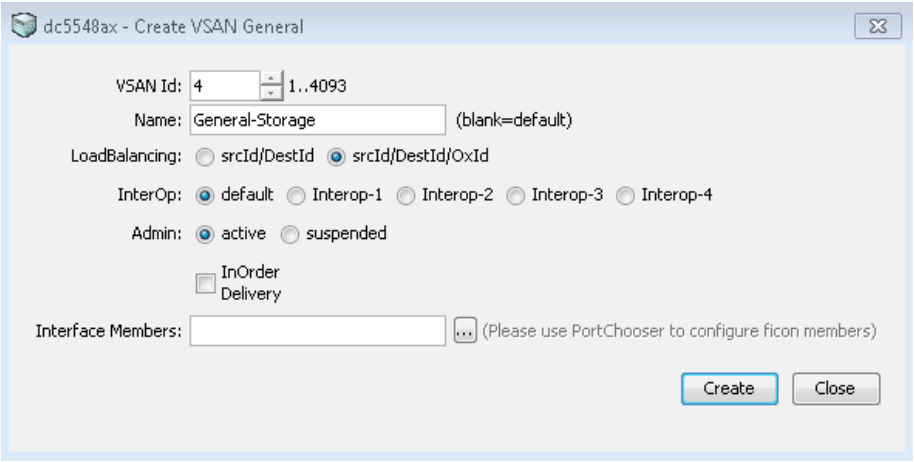
步骤 1: 为SAN Essentiasl安装Cisco DCNM。

步骤 2: 使用DCNM 设备管理器，连接至第一个Cisco Nexus 数据中心核心交换机IP地址（`10.4.63.10`）。

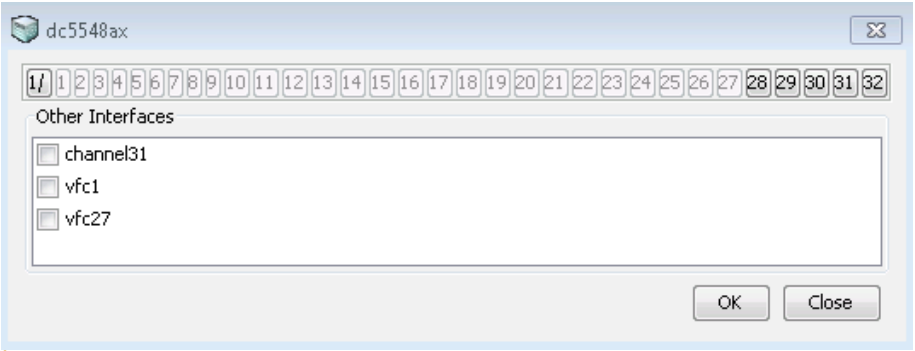
步骤 3: 使用Device Manager（设备管理器），单击**FC>VSANS**。之后“Create VSAN General（创建VSAN常规）”窗口出现。

步骤 4: 在**VSAN id**列表，选择**4**，并在名称框内输入`General-Storage`。

步骤 5: 在Interface Members (接口成员) 框的旁边, 单击省略号 (…) 按钮。



步骤 6: 通过单击您所需的端口编号, 选择接口成员。



步骤 7: 单击**Create (创建)**。VSAN已成功创建。您可以在主VSAN窗口的Membership (成员) 选项卡中添加更多VSAN成员。

上述步骤在CLI上应用以下配置。

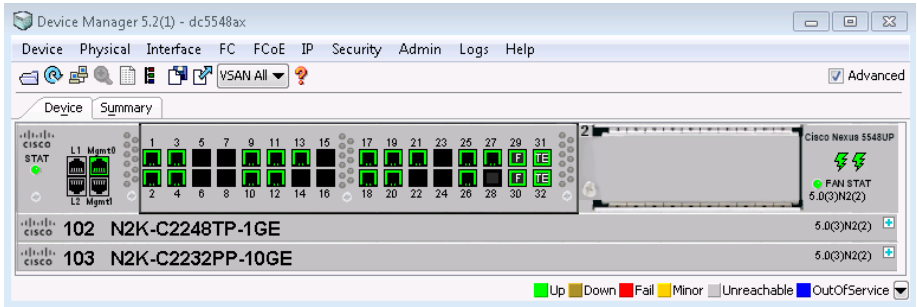
```
vsan database
vsan 4 name "General-Storage"
vsan 4 interface fc1/28
```

步骤 8: 在第二个Cisco Nexus 5500UP交换机上重复本程序中的步骤, 以创建VSAN 5。使用相同的VSAN名称。

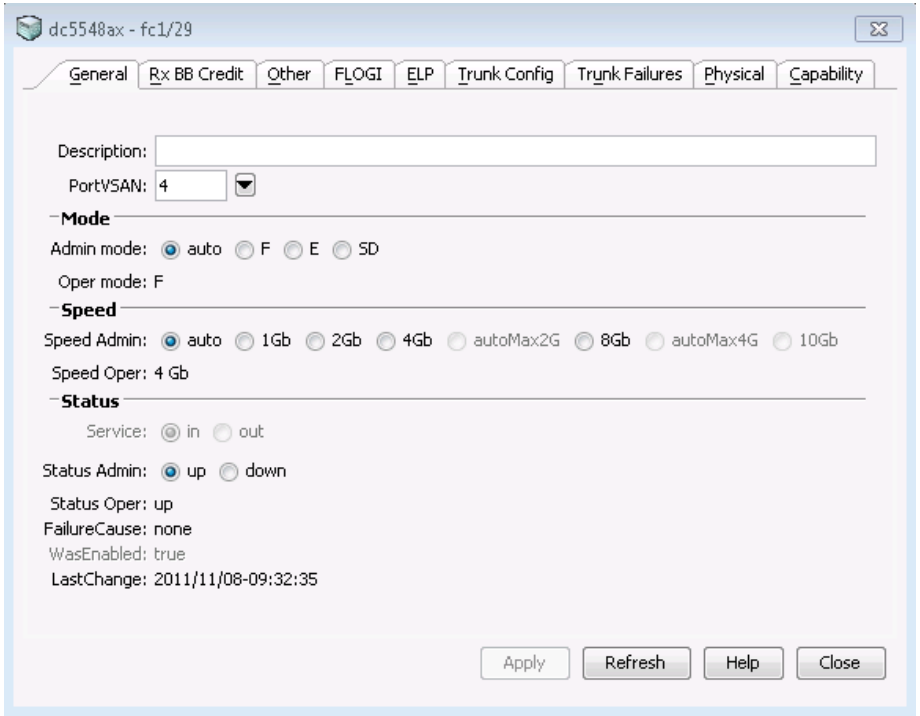
程序 3 配置FC (光纤通道) 端口

默认情况下, 端口被配置为端口模式**Auto (自动)**。对于连接到阵列的大多数设备而言, 无需对这一设置进行修改。然而, 您将需要为端口分配一个VSAN。

步骤 1: 如果您想通过Device Manager (设备管理器) 更改端口模式, 右键单击要配置的端口。



General (常规) 选项卡显示。



在此图中您会看到, PortVSAN分配列于General (常规) 面板的左上侧。

步骤 2: 在Status Admin (状态管理) 旁边, 选择**up**。启用此端口。

步骤 3: 在PortVSAN的下拉列表中, 选择**4**或**5**, 具体取决于您正在使用哪个交换机, 然后单击**Apply (应用)**。更改VSAN并激活端口。

上述步骤在CLI中应用以下配置。

```
vsan database
   vsan 4 interface fc1/28
```

这一步骤可向VSAN分配端口, 类似于之前的程序 "配置VSAN" 中的步骤 5。如果您已创建了VSAN, 这是向VSAN分配端口的另一途径。

步骤 4: 将FC设备连接到端口。

读者提示

如需了解有关准备思科UCS B系列和C系列服务器以连接到FC网络的更多信息, 请参阅思科IBA智能业务平台——《数据中心统一计算系统部署指南》。

步骤 5: 通过在交换机CLI上输入**show flogi database**, 显示阵列登录 (FLOGI)。

技术提示

当启动器或目标插入或启动时, 它将会自动登录阵列。登录后, 接口将会获知启动器或目标WWN。直到您的存储阵列或服务器上有活跃的HBA (主机总线适配器) 插入FC端口上的交换机内, 您才能看到FLOGI数据库中的条目。

示例

```
dc5548ax# show flogi database
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME
NODE NAME
--------------------------------------------------------------------------------
fc1/29           4     0xbc0002  20:41:00:05:73:a2:b2:40
20:04:00:05:73:a2:b2:41
fc1/29           4     0xbc0005  20:00:00:25:b5:77:77:9f
20:00:00:25:b5:00:77:9f
fc1/30           4     0xbc0004  20:42:00:05:73:a2:b2:40
20:04:00:05:73:a2:b2:41
vfc1             4     0xbc0000  20:00:58:8d:09:0e:e0:d2
```

```
10:00:58:8d:09:0e:e0:d2
vfc27             4     0xbc0006  50:0a:09:81:89:3b:63:be
50:0a:09:80:89:3b:63:be

Total number of flogi = 5.
```

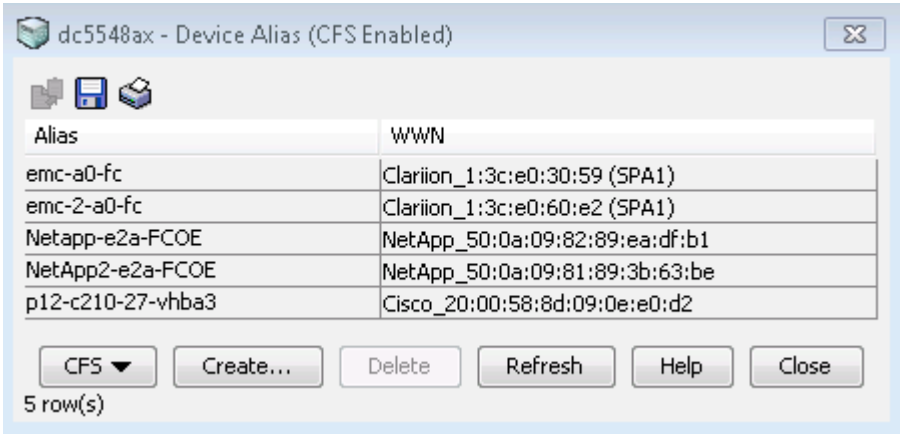
程序 4　配置设备别名

设备别名对应冗长的WWN，以便更轻松地进行分区和识别启动器与目标。不正确的设备名称可能导致意想不到的后果。设备别名可用于分区、端口安全、QoS和**show**命令。

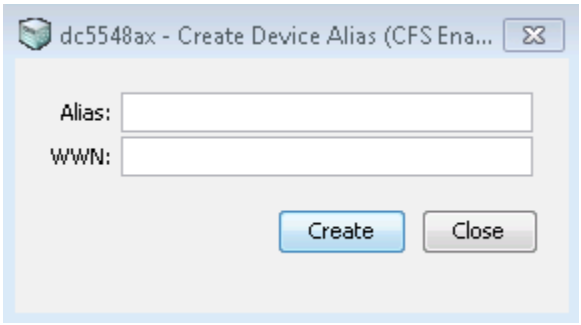
您可以通过设备管理器或CLI配置设备别名。

Option 1. 使用设备管理器配置设备别名

步骤 1: 在Device Manager（设备管理器）中，转至**FC > Advanced（高级）> Device Alias（设备别名）**，进入设备别名（Device Alias）窗口。



步骤 2: 单击**Create（创建）**。



步骤 3: 在Alias（别名）框内，输入一个名称，并且在**WWN**框内，粘贴或输入主机的WWN，然后单击**Create（创建）**。

步骤 4: 在您创建了设备别名后，单击**CFS > Commit（提交）**。相关变更将被写入数据库。

Option 2. 使用CLI配置设备别名

步骤 1: 输入设备别名数据库配置模式。

```
device-alias database
```

步骤 2: 输入设备别名名称，从以上FLOGI数据库映射到PWWN。例如：

```
device-alias name emc-a0-fc pwwn 50:06:01:61:3c:e0:30:59
device-alias name emc-2-a0-fc pwwn 50:06:01:61:3c:e0:60:e2
device-alias name Netapp-e2a-FCOE pwwn 50:0a:09:82:89:ea:df:b1
device-alias name NetApp2-e2a-FCOE pwwn
50:0a:09:81:89:3b:63:be
device-alias name p12-c210-27-vhba3 pwwn
20:00:58:8d:09:0e:e0:d2
```

步骤 3: 退出设备别名配置模式。

```
exit
```

步骤 4: 执行更改。

```
device-alias commit
```

步骤 5: 输入**show flogi database**命令。别名现在可见。

```
dc5548ax# show flogi database
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME
NODE NAME
--------------------------------------------------------------------------------
fc1/29           4     0xbc0002  20:41:00:05:73:a2:b2:40
20:04:00:05:73:a2:b2:41
fc1/29           4     0xbc0005  20:00:00:25:b5:77:77:9f
20:00:00:25:b5:00:77:9f
fc1/30           4     0xbc0004  20:42:00:05:73:a2:b2:40
20:04:00:05:73:a2:b2:41
vfc1             4     0xbc0000  20:00:58:8d:09:0e:e0:d2
10:00:58:8d:09:0e:e0:d2
[p12-c210-27-vhba3]
vfc27            4     0xbc0006  50:0a:09:81:89:3b:63:be
50:0a:09:80:89:3b:63:be
[NetApp2-e2a-FCOE]
```

程序 5　配置分区

分区主要实践包括:

- 在每个分区的一个启动器和一个目标之间配置分区。
- 一个启动器也可配置为与同一分区内的多个目标相连。
- 分区命名应遵循简单的命名惯例: initiator_x_target_x:
  - p12-ucs-b-fc0-vhba1_emc-2
- 将分区限制为拥有一个或多个目标的单个启动器可以帮助避免磁盘崩溃或数据丢失情况。

从CLI和Cisco DCNM配置SAN Fabric Manager (SAN阵列管理器) 分区。

Option 1. 使用CLI配置一个分区

步骤 1: 在配置模式中, 输入分区名称和VSAN编号。

```
zone name p12-ucs-b-fc0-vhba1_emc-2 vsan 4
```

步骤 2: 通过WWN或设备别名, 指定设备成员。

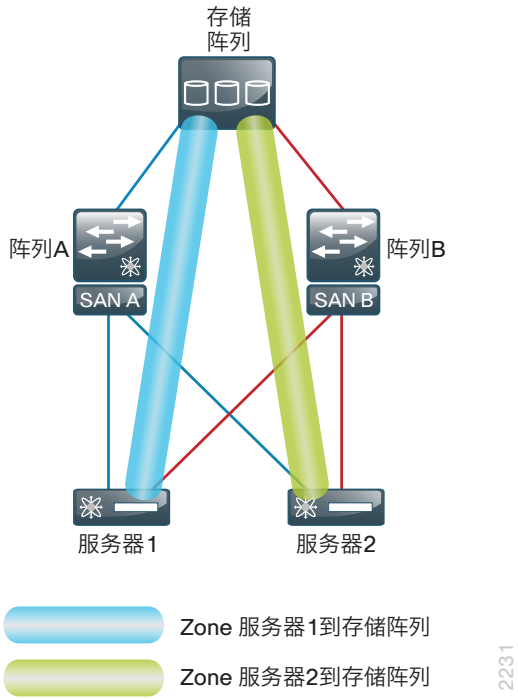
```
member device-alias emc-2-a0-fc
member pwwn 20:00:00:25:b5:77:77:9f
```

步骤 3: 创建和激活分区集。

```
zoneset name FCOE_4 vsan 4
```

技术提示

分区集由一系列分区组成。分区是分区集的成员。将所有分区添加为成员后, 您必须激活分区集。每个VSAN只允许有一个活动的分区集。



步骤 4: 添加成员到分区集。

```
member p12-ucs-b-fc0-vhba1_emc-2
member p12-c210-27-vhba3_netapp-2-e2a
```

步骤 5: 当为VSAN 4创建了所有分区，并添加到分区集后，激活配置。

```
zoneset activate name FCOE_4 vsan 4
```

步骤 6: 向SAN中的其它交换机分配分区数据库。这可为将您的FC（光纤通道）SAN扩展到多台交换机做好准备。

```
zoneset distribute full vsan 4
```

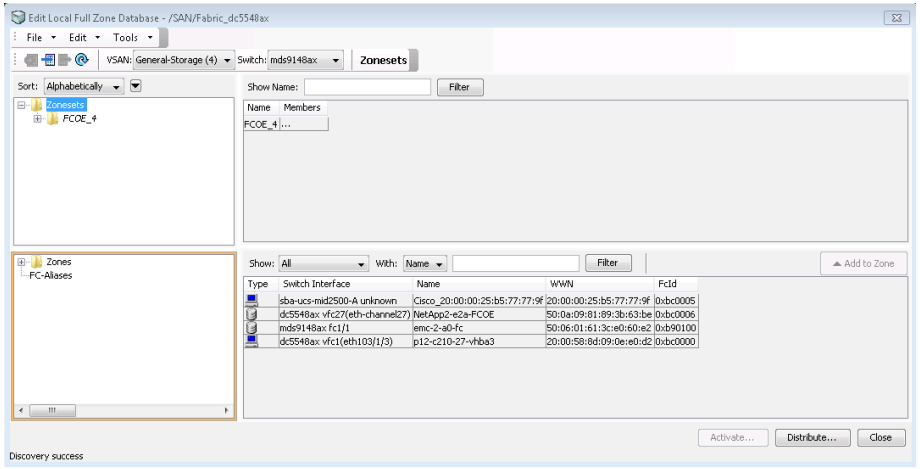
Option 2. 使用Cisco DCNM配置一个分区

步骤 1: 为SAN Fabric Manager（SAN阵列管理器）启动Cisco DCNM，其已在程序“配置VSAN”中的步骤 1中安装。

步骤 2: 登录DCNM-SAN管理器。默认用户名是**admin**以及密码是**password**。

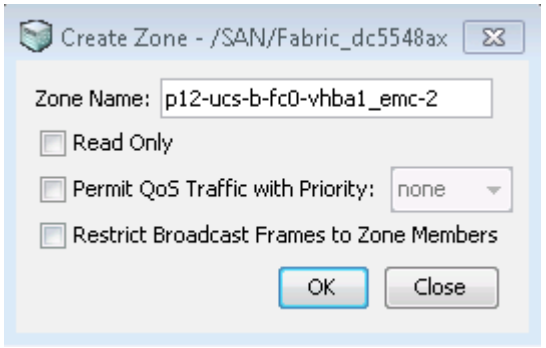
步骤 3: 输入第一个Cisco Nexus 5500UP交换机的IP地址（例如，10.4.63.10），选择一个子交换机，然后从列表里选择Cisco Nexus 5500UP。

步骤 4: 从DCNM-SAN菜单，选择**Zone（分区）**，然后单击**Edit Local Full Zone Database（编辑本地全区数据库）**。

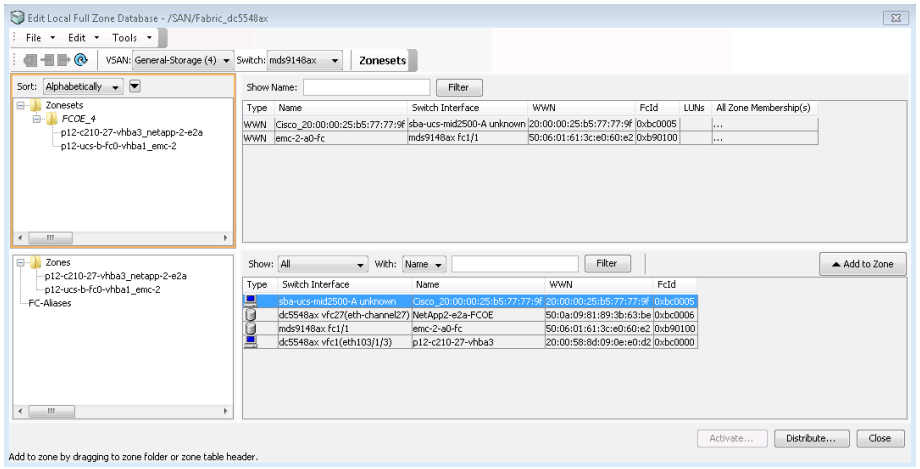


步骤 5: 在Zone Database（分区数据库）窗口，在左窗格中，右键单击**Zones（分区）**，然后单击**Insert（插入）**。

步骤 6: 在**Zone Name（分区名称）**框内，输入新分区的名称，然后单击**OK**。



步骤 7: 选择新的分区，然后，从数据库窗口的右侧的底部，选择您想添加到区域中的启动器或目标，然后单击**Add to Zone（添加到分区）**。

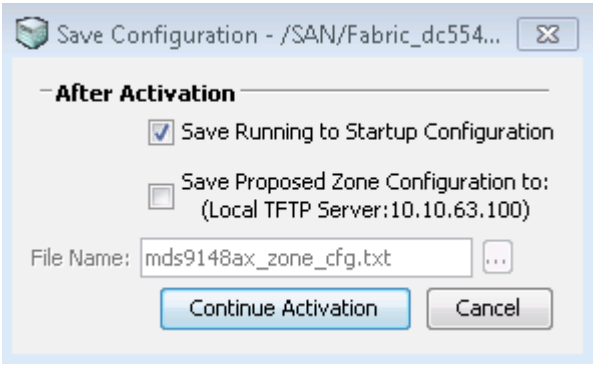


步骤 8: 右键单击**Zoneset（分区集）**以插入一个新的分区集。

步骤 9: 将刚刚创建的分区从zone box（分区箱）拖拽到您创建的分区集文件夹中。

步骤 10: 单击**Activate（激活）**。这将激活已配置的分区集。

步骤 11: 在Save Configuration（保存配置）对话框，选择**Save Running to Startup Configuration（保存运行至启动配置）**，然后单击**Continue Activation（继续激活）**。



步骤 12: 用本程序中的流程以同样方式配置SAN B，在第二个数据中心核心Cisco Nexus 5500UP交换机上创建VSAN 5。

程序 6 验证配置

步骤 1: 验证FC（光纤通道）登录。

在FC阵列中，每个主机或磁盘都需要一个光纤通道ID（FC ID）。当收到来自于设备的阵列登录（FLOGI）时，阵列将指派这一ID。如果所需的设备显示在FLOGI表中，则表示阵列登录成功完成。

```
dc5548ax# show flogi database
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME
NODE NAME
--------------------------------------------------------------------------------
fc1/29           4     0xbc0002  20:41:00:05:73:a2:b2:40
20:04:00:05:73:a2:b2:41
fc1/29           4     0xbc0005  20:00:00:25:b5:77:77:9f
20:00:00:25:b5:00:77:9f
fc1/30           4     0xbc0004  20:42:00:05:73:a2:b2:40
20:04:00:05:73:a2:b2:41
vfc1             4     0xbc0000  20:00:58:8d:09:0e:e0:d2
10:00:58:8d:09:0e:e0:d2
                                 [p12-c210-27-vhba3]
vfc27            4     0xbc0006  50:0a:09:81:89:3b:63:be
50:0a:09:80:89:3b:63:be
                                 [NetApp2-e2a-FCOE]

Total number of flogi = 5.
```

步骤 2: 验证光纤通道名称服务器（FCNS）属性。

FCNS数据库显示相同的PWWN登录以及厂商特定属性和特性。检查确保您的启动器和目标已登录，并如下高亮显示**FC4-TYPE:FEATURE**属性。如果特性属性没有显示，则终端主机或存储设备上的部分配置可能配置错误或存在设备驱动程序问题。

```
dc5548ax# show fcns database

VSAN 4:
-----------------------------------------------------------------
---------
FCID        TYPE  PWWN                    (VENDOR)        FC4-
TYPE:FEATURE
-----------------------------------------------------------------
---------
0xb90100    N     50:06:01:61:3c:e0:60:e2 (Clariion)      scsi-
fcp:target
                  [emc-2-a0-fc]
0xbc0000    N     20:00:58:8d:09:0e:e0:d2                 scsi-
fcp:init fc-gs
                  [p12-c210-27-vhba3]
0xbc0002    N     20:41:00:05:73:a2:b2:40 (Cisco)         npv
0xbc0004    N     20:42:00:05:73:a2:b2:40 (Cisco)         npv
0xbc0005    N     20:00:00:25:b5:77:77:9f                 scsi-
fcp:init fc-gs
0xbc0006    N     50:0a:09:81:89:3b:63:be (NetApp)        scsi-
fcp:target
                  [NetApp2-e2a-FCOE]

Total number of entries = 6
```

步骤 3: 验证活动分区集。

使用可显示活动分区集的**show zoneset active**命令，检查阵列配置以确保正确分区。属于活动分区集成员的每一个分区在左侧以星号 (*) 表示。如果左侧没有星号，主机或者关闭，或者未登录到阵列，或者端口VSAN或分区配置有误。使用**show zone**命令显示思科FC交换机上所有配置的分区。

```
dc5548ax# show zoneset active
zoneset name FCOE_4 vsan 4
  zone name p12-ucs-b-fc0-vhba1_emc-2 vsan 4
  * fcid 0xb90100 [pwwn 50:06:01:61:3c:e0:60:e2] [emc-2-a0-fc]
  * fcid 0xbc0005 [pwwn 20:00:00:25:b5:77:77:9f]

  zone name p12-c210-27-vhba3_netapp-2-e2a vsan 4
  * fcid 0xbc0006 [pwwn 50:0a:09:81:89:3b:63:be] [NetApp2-e2a-
FCOE]
  * fcid 0xbc0000 [pwwn 20:00:58:8d:09:0e:e0:d2] [p12-c210-27-
vhba3]
```

步骤 4: 使用**fcping**命令测试FC（光纤通道）可达性，并使用**fctrace**命令跟踪到主机的路线。思科创建的这些命令为使用ping和traceroute的个人提供了熟悉的存储网络故障排除工具。

流程

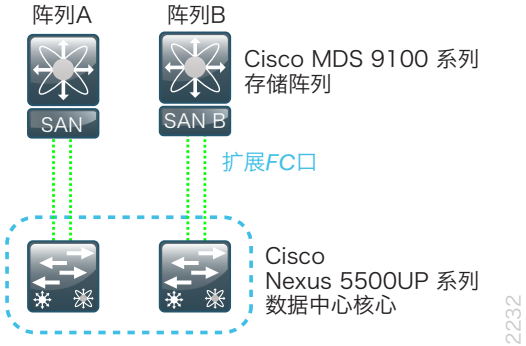
配置Cisco MDS 9148交换机SAN扩展

1、为Cisco MDS交换机执行初始设置

2、配置VSAN

3、为SAN互联配置中继

如果您的FC（光纤通道）SAN环境要求更高的光纤通道端口连接密度，您可以选择使用Cisco MDS 9100系列SAN交换机。



以下程序描述了如何部署Cisco MDS 9124或9148 SAN交换机，以连接到数据中心核心Cisco Nexus 5500UP交换机。

程序 1　为Cisco MDS交换机执行初始设置

完成这一程序需要以下要素：

- 设置管理IP地址
- 配置控制台访问
- 配置安全密码

最初加电后，当通过控制台进行访问时，全新Cisco MDS 9148交换机会启动一个设置脚本。

步骤 1： 按照设置脚本的提示配置登录帐户、带外管理、SSH、网络时间协议、交换机端口模式、以及默认分区策略。

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:
y
  Enter the password for "admin":
  Confirm the password for "admin":
         ---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic
configuration of
the system. Setup configures only enough connectivity for
management
of the system.
*Note: setup is mainly used for configuring the system
initially,
when no configuration is present. So setup always assumes
system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/
no): y
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : mds9148ax
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]: y
    Mgmt0 IPv4 address : 10.4.63.12
    Mgmt0 IPv4 netmask : 255.255.255.0
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : 10.4.63.1
  Configure advanced IP options? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa)
```

```
[rsa]: rsa
    Number of rsa key bits <768-2048> [1024]: 2048
  Enable the telnet service? (yes/no) [n]: n
  Enable the http-server? (yes/no) [y]:
 Configure clock? (yes/no) [n]:
 Configure timezone? (yes/no) [n]:
 Configure summertime? (yes/no) [n]:
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : 10.4.48.17
  Configure default switchport interface state (shut/noshut)
[shut]: noshut
  Configure default switchport trunk mode (on/off/auto) [on]:
  Configure default switchport port mode F (yes/no) [n]: n
  Configure default zone policy (permit/deny) [deny]:
  Enable full zoneset distribution? (yes/no) [n]: y
  Configure default zone mode (basic/enhanced) [basic]:
The following configuration will be applied:
  password strength-check
  switchname mds9148ax
  interface mgmt0
    ip address 10.4.63.12 255.255.255.0
    no shutdown
  ip default-gateway 10.4.63.1
  ssh key rsa 2048 force
  feature ssh
  no feature telnet
  feature http-server
  ntp server 10.4.48.17
  no system default switchport shutdown
  system default switchport trunk mode on
  no system default zone default-zone permit
  system default zone distribute full
  no system default zone mode enhanced

Would you like to edit the configuration? (yes/no) [n]: n
Use this configuration and save it? (yes/no) [y]: y
[########################################] 100%
```

技术提示

NTP（网络时间协议）对于故障排除工作至关重要，不应被忽视。

步骤 2: 使用唯一的交换机名称和Mgmt0 IPv4地址**10.4.63.13**，运行第二个Cisco MDS 9100交换机的设置脚本。

步骤 3: 如果您想要减少每个设备的操作任务，通过使用TACACS+协议配置集中式用户身份验证，在基础设施设备上进行身份验证管理登录至AAA服务器。

随着网络及需要维护设备数量的增长，在每个设备上的本地用户的维护成本也在相应增加。一个集中的AAA服务，为每台设备减少日常操作的同时，也提供偶尔关于用户访问安全合规性和根源分析的审计日志。当为访问控制启用AAA，所有的网络基础设施设备的管理访问（SSH和HTTPS）都由AAA控制。

TACACS+是在设备上用于验证管理登录到AAA服务器的主要协议。在每个Nexus 5500交换机上，一个本地AAA用户数据库同样中被定义到设置脚本中，它提供了备用身份验证源，以防集中TACACS+服务不可用的情况。

```
feature tacacs+
tacacs-server host 10.4.48.15 key SecretKey
aaa group server tacacs+ tacacs
  server 10.4.48.15
aaa authentication login default group tacacs
```

读者提示

在此架构中使用AAA服务器是Cisco ACS。如需更多关于Cisco ACS 相关配置详情，请参考Cisco IBA——《使用ACS的无边界网络设备管理部署指南》。

步骤 4: 设置SNMP字符串，以支持采用设备管理器管理MDS交换机。设置只读（**network-operator**）和读写（**network-admin**）SNMP字符串：

```
snmp-server community cisco group network-operator
snmp-server community cisco123 group network-admin
```

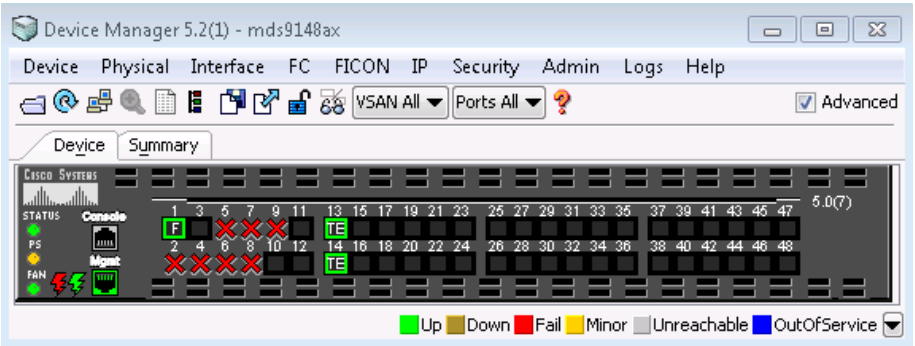
步骤 5: 配置时钟。在设置模式中，您配置了NTP服务器地址。在此步骤中，通过配置时钟，使时钟使用NTP时间作为参考，并使交换机输出匹配本地时区。

```
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00
60
```

程序 2 配置VSAN

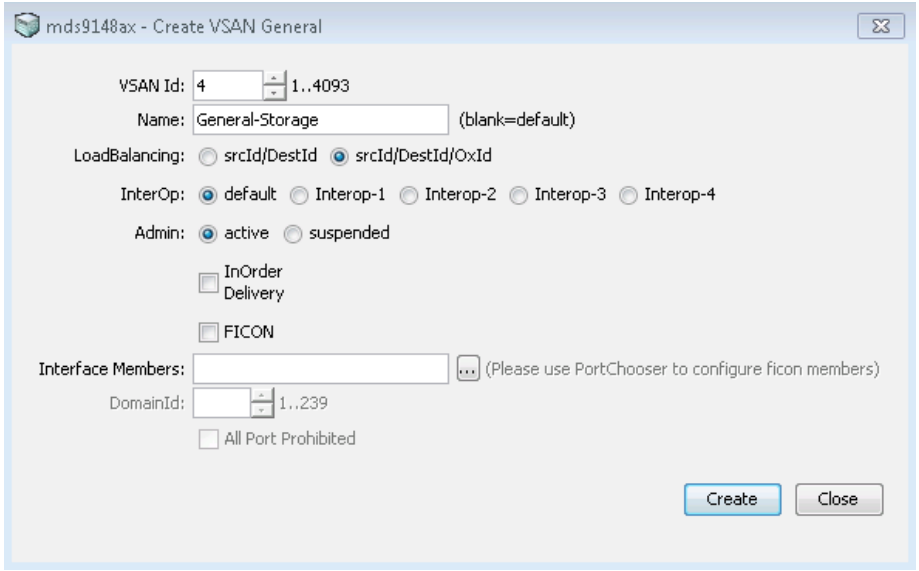
要配置Cisco MDS交换机，以扩展您基于Cisco Nexus 5500UP交换机构建的FC（光纤通道）SAN，请分别为SAN A和SAN B使用同一VSAN编号。CLI和GUI工具对于Cisco MDS和Cisco Nexus 5500UP的工作方式相同。

步骤 1: 在Device Manager（设备管理器）中，登录第一台Cisco MDS SAN交换机，然后单击**FC >VSANS**。



Create VSAN General（创建VSAN常规）窗口出现。

步骤 2: 在VSAN id列表中，选择**4**，然后在**Name（名称）**框中，输入**General-Storage**。



步骤 3: 单击**Create（创建）**。

上述步骤在CLI中应用以下配置。

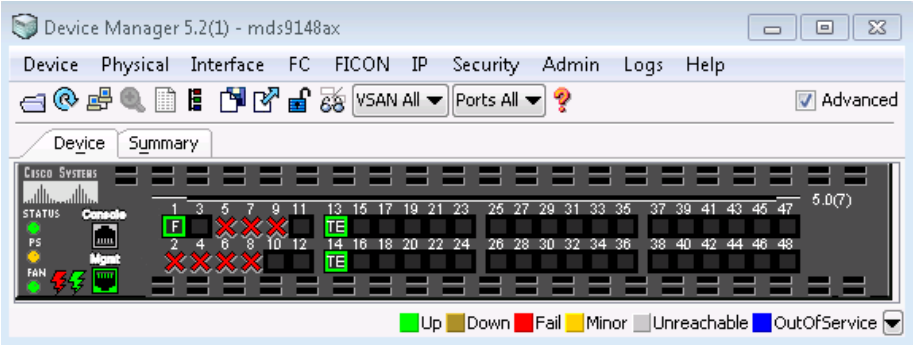
```
vsan database
vsan 4 name "General-Storage"
```

步骤 4: 使用本程序步骤 1至步骤 3，配置第二个交换机的VSAN**5**和VSAN名称为**General-Storage**。

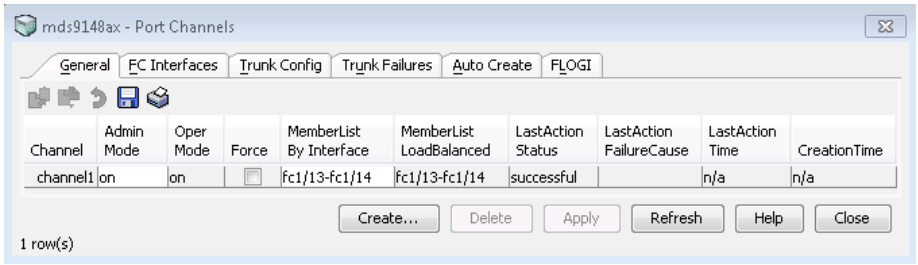
程序 3 为SAN互联配置中继

将Cisco MDS交换机连接到现有Cisco Nexus 5500UP核心FC（光纤通道）SAN。

步骤 1: 在Device Manager (设备管理器) 中, 转至Cisco MDS交换机。

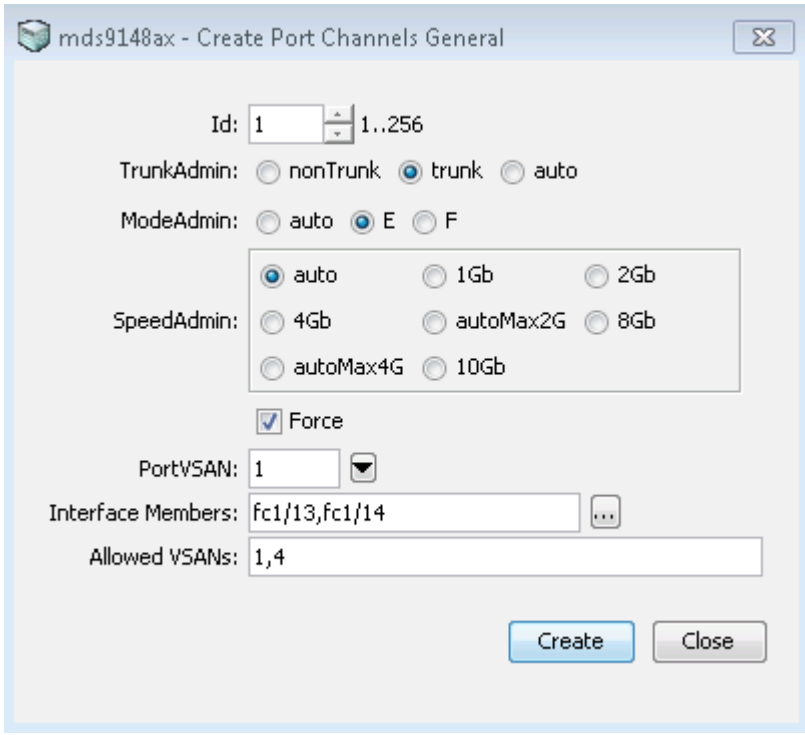


步骤 2: 在Device Manager (设备管理器) 界面, 单击**Interfaces (接口) > Port Channels (端口通道)**, 然后单击**Create (创建)**。接下来在Cisco MDS上配置中继端口。

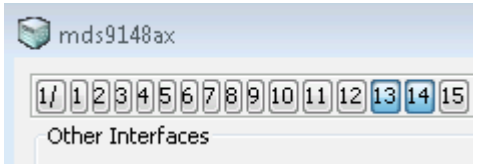


步骤 3: 选择端口通道Id号, 选择**trunk (中继)**, 选择模式**E**, 然后选择**Force (实施)**。

步骤 4: 在Allowed VSANs (允许的VSAN) 框中, 键入**1**, **4**。对于面向SAN阵列B的Cisco MDS交换机, 要键入的VSAN将为**1**和**5**。



步骤 5: 在Interface Members (接口成员) 框右侧, 单击省略号 (…) 按钮, 然后选择将属于此端口通道的Interface Members (接口成员)。



步骤 6: 单击**Create (创建)**。新端口通道创建完成。

步骤 7: 右键单击用于port channel的FC (光纤通道) 端口, 然后选择**enable (开启)**。

上述步骤可将此Cisco MDS 9100配置应用于MDS SAN-A交换机。

```
interface port-channel 1
```

```
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 4
  switchport rate-mode dedicated

interface fc1/13
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated
  no shutdown
interface fc1/14
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated
  no shutdown
```

上述步骤可将此Cisco MDS 9100配置应用于MDS SAN-B交换机。

```
interface port-channel 1
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 5
  switchport rate-mode dedicated

interface fc1/13
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated
  no shutdown
interface fc1/14
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated
  no shutdown
```

步骤 8: 按照此程序 (程序 3) 中的上述步骤, 创建相应的SAN端口通道, 连接到支持Cisco Nexus 5500UP的Cisco MDS交换机。

用于该SAN端口通道的Cisco Nexus 5500UP CLI也将用于SAN-A交换机。

```
interface san-port-channel 31
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 4

interface fc1/31
  switchport description Link to dcmds9148ax port fc-1/13
  switchport mode E
  channel-group 31 force
  no shutdown

interface fc1/32
  switchport description Link to dcmds9148ax port fc1/14
  switchport mode E
  channel-group 31 force
  no shutdown
```

用于该SAN端口通道的Cisco Nexus 5500UP CLI也将用于SAN-B交换机。

```
interface san-port-channel 31
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 5

interface fc1/31
  switchport description Link to dcmds9148bx port fc-1/13
  switchport mode E
  channel-group 31 force
  no shutdown

interface fc1/32
  switchport description Link to dcmds9148bx port fc1/14
  switchport mode E
  channel-group 31 force
  no shutdown
```

步骤 9: 将在Cisco Nexus 5500UP交换机上创建的分区数据库分配到新的Cisco MDS9100交换机。

针对SAN-A配置Cisco Nexus 5500UP CLI, 以向全新Cisco MDS9100交换机分配分区数据库。

```
zoneset distribute full vsan 4
```

针对SAN-B配置Cisco Nexus 5500UP CLI，以向全新Cisco MDS9100交换机分配分区数据库。

```
zoneset distribute full vsan 5
```

流程

配置FCoE主机连接

1、配置FCoE QoS

2、配置面向主机的FCoE端口

3、验证FCoE 连接

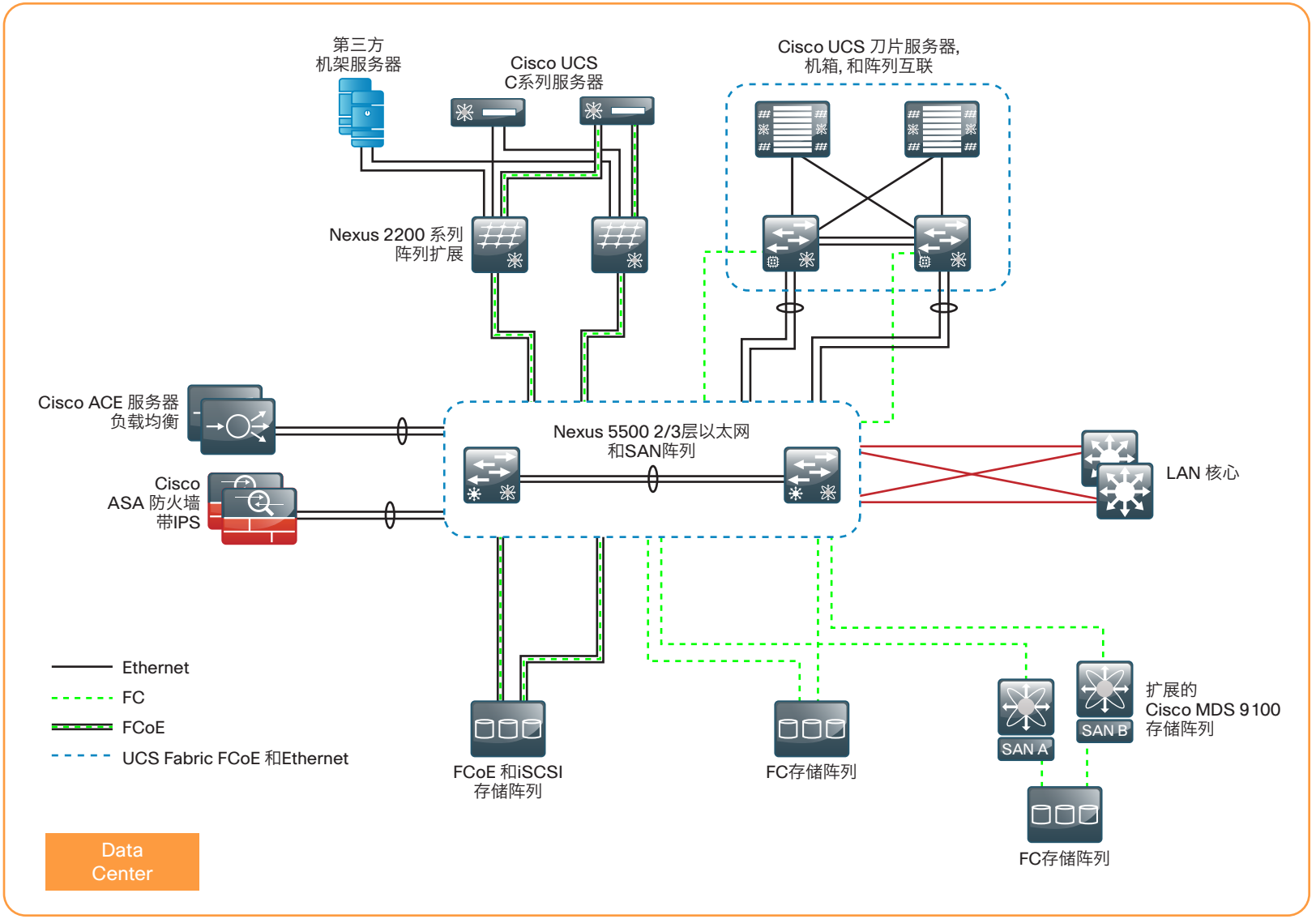
Cisco UCS C系列机柜安装式服务器标配板载10/100/1000以太网适配器和一个使用10/100以太网端口的思科集成管理控制器（CIMC）。为充分利用机架服务器和最大限度减少Cisco IBA智能业务平台统一计算架构的布线，Cisco UCS C系列机架安装式服务器连接至一个统一阵列。用于将Cisco UCS 5100系列刀片服务器机箱连接到网络的Cisco Nexus 5500UP系列交换机也可用于通过万兆以太网扩展FC（光纤通道）流量。Cisco Nexus 5500UP系列交换机能够将I/O整合到一组万兆以太网线缆上，消除冗余适配器、线缆和端口。通过使用光纤通道（FCoE），单一融合网络适配器（CNA）卡和线缆集可将服务器连接到以太网和光纤通道网络。FcoE和CNA还允许在服务器机架中使用单一布线基础设施。

在思科IBA智能业务平台数据中心，Cisco UCS C系列机架安装式服务器配置有双端口CNA。将Cisco UCS C系列服务器与CNA相连可以将线缆数量减少为三条，CNA和CIMC连接上的每个端口一条。

技术提示

连接到运行FCoE的Cisco Nexus 5500UP的服务器需要FC端口许可证。如果您正将FCoE连接服务器连接到Cisco FEX型号2232PP，那么仅连接Cisco FEX的5500UP端口需要为每个连接Cisco FEX的端口提供FC端口许可证。这样，您可将多达32台FCoE服务器连接到Cisco FEX 2232PP，并且仅针对Cisco FEX上行链路使用FC端口许可证。

不具备CNA的标准服务器拥有少量以太网连接以及多个以太网和FC连接。下图显示了采用混合统一阵列、标准以太网和FC连接的拓扑结构，以及可选的支持FC扩展的Cisco MDS 9100系列。


第三方
机架服务器
Cisco UCS
C系列服务器
Cisco UCS 刀片服务器,
机箱, 和阵列互联
Nexus 2200 系列
阵列扩展
Cisco ACE 服务器
负载均衡
Cisco
ASA 防火墙
带IPS
Nexus 5500 2/3层以太网
和SAN阵列
LAN 核心
Ethernet
FC
FCoE
UCS Fabric FCoE 和Ethernet
FCoE 和iSCSI
存储阵列
FC存储阵列
SAN A
SAN B
扩展的
Cisco MDS 9100
存储阵列
FC存储阵列
Data
Center
2216

Cisco UCS C系列服务器使用双轴电缆或光纤电缆从CNA连接至两台Cisco Nexus 5500UP系列交换机。运行FCoE的Cisco UCS服务器还能够连接到单宿主Cisco FEX型号2232PP。

技术提示

此时，FCoE连接主机仅能够通过万兆以太网连接，并且必须使用光纤或双轴电缆连接。

推荐的方法是将CIMC 10/100管理端口连接到带外管理交换机上的一个以太网端口。或者，您可将CIMC管理端口连接到管理VLAN (**163**) 中的Cisco Nexus 2248阵列扩展模块端口。

面向FCoE的CiscoNexus 5500UP配置

在之前程序，我们启用了Cisco Nexus 5500UP系列FCoE功能。在本程序，您将执行以下任务，允许Cisco C系列服务器使用FCoE进行连接：

- 创建一个虚拟通道接口
- 将VSAN分配到虚拟FC接口
- 配置以太网端口和中继

程序 1　配置FCoE QoS

两个Cisco Nexus 5500UP系列交换机的配置相同，但为SAN阵列A和为SAN阵列B配置的VSAN例外。

与Cisco Nexus 5010不同，Cisco Nexus 5500UP并未针对FCoE流量预配置QoS。

步骤 1: 确保Cisco Nexus 5500UP 数据中心核心交换机已被编入Cisco Nexus 5500UP 策略支持无损FCoE传输。针对数据中心核心Nexus 5500UP 交换机的QoS 策略已在程序 3 “配置QoS策略”中被定义。

技术提示

在Cisco Nexus 5500UP 交换机上必须针对FCoE流量配置QoS策略保证无损传输。

程序 2　配置面向主机的FCoE端口

在Cisco Nexus 5500UP交换机上，配置连接到双宿主主机中CNA的以太网端口。

步骤 1: 创建将FCoE流量传输到主机的VLAN。

- 在下面，VLAN 304被映射到VSAN 4。VLAN 304通过面向第一个Cisco Nexus 5500UP交换机的中继将所有VSAN 4流量传输到CNA。

```
vlan 304
fcoe vsan 4
exit
```

- 在第二个Cisco Nexus 5500UP交换机中，VLAN 305被映射到VSAN 5。

```
vlan 305
fcoe vsan 5
exit
```

步骤 2: 创建支持FC (光纤通道) 流量的虚拟光纤通道 (vfc) 接口，然后将它与相应的主机以太网接口绑定。您必须这样做，以便能够将FCoE接口映射到FC。

本示例显示绑定了一个Cisco FEX 2232PP以太网接口。此命令在两个Cisco Nexus 5500UP交换机上相同。

```
interface vfc1
bind interface Ethernet 103/1/3
no shutdown
exit
```

步骤 3: 将vfc接口添加到VSAN数据库。

- 在第一个Cisco Nexus 5500UP交换机上，vfc被映射到VSAN 4。

```
vsan database
vsan 4 interface vfc 1
exit
```

- 在第二个Cisco Nexus 5500UP交换机中，vfc被映射到VSAN 5。

```
vsan database
vsan 5 interface vfc 1
exit
```

步骤 4: 将以太网接口配置为在中继模式下运行，采用FCoE VSAN和该主机所需的任意数据VLAN配置此接口，并将生成树端口类型配置为**中继边缘**。

- 本示例显示了第一个Cisco Nexus 5500UP交换机的配置。

```
interface Ethernet 103/1/3
switchport mode trunk
switchport trunk allowed vlan 148-162,304
spanning-tree port type edge trunk
no shut
```

- 本示例显示了第二个Cisco Nexus 5500UP交换机的配置。

```
interface Ethernet 103/1/3
switchport mode trunk
switchport trunk allowed vlan 148-162,305
spanning-tree port type edge trunk
no shut
```

步骤 5: 在Cisco UCS C系列服务器上配置VSAN。

技术提示

使用Cisco P81E CNA的Cisco UCS C系列服务器必须配置FCoE VSAN，来支持虚拟主机总线适配器（vHBA）操作，从而连接到FC阵列。如需了解有关针对FCoE连接配置C系列服务器的更多信息，请参阅思科IBA智能业务平台——《数据中心统一计算系统部署指南》。

程序 3 验证FCoE 连接

步骤 1: 在Cisco Nexus 5500UP交换机上，使用**show interface**命令，验证虚拟FC接口的状态。如果主机配置正确可支持CNA，则该接口现在应正常工作，如下所示。

读者提示

主机配置超出了本指南的讨论范畴。请查看CNA文档，了解具体的主机驱动程序和配置。

```
dc5548ax# show interface vfc1
vfc1 is trunking (Not all VSANs UP on the trunk)
    Bound interface is Ethernet103/1/3
    Hardware is Virtual Fibre Channel
    Port WWN is 20:00:54:7f:ee:17:cf:3f
    Admin port mode is F, trunk mode is on
    snmp link state traps are enabled
    Port mode is TF
    Port vsan is 4
    Trunk vsans (admin allowed and active)  (1,4)
    Trunk vsans (up)                        (4)
    Trunk vsans (isolated)                  ()
```

```
    Trunk vsans (initializing)              (1)
    1 minute input rate 1672 bits/sec, 209 bytes/sec, 0
frames/sec
    1 minute output rate 320 bits/sec, 40 bytes/sec, 0 frames/
sec
      117038 frames input, 39607100 bytes
        0 discards, 0 errors
      128950 frames output, 33264140 bytes
        0 discards, 0 errors
    last clearing of "show interface" counters never
    Interface last changed at Tue Nov  8 11:11:29 2011
```

步骤 2: 在Cisco Nexus 5500UP交换机上，显示FCoE地址。

```
dc5548ax# show fcoe database

------------------------------------------------------------------
--------------
INTERFACE       FCID            PORT NAME               MAC
ADDRESS
------------------------------------------------------------------
--------------
vfc1            0xbc0000        20:00:58:8d:09:0e:e0:d2
58:8d:09:0e:e0:d2
```

步骤 3: 显示支持FCoE登录的FLOGI数据库。vfc1地址显示在Nexus 5500交换机上当前的FLOGI数据库中。

```
dc5548ax# show flogi database
------------------------------------------------------------------
---------------
INTERFACE        VSAN    FCID           PORT NAME
NODE NAME
------------------------------------------------------------------
---------------
vfc1             4     0xbc0000  20:00:58:8d:09:0e:e0:d2
10:00:58:8d:09:0e:e0:d2
                         [p12-c210-27-vhba3]
```

步骤 4: 显示支持FCoE登录的FCNS数据库。FCNS数据库显示FCoE主机已登录和FC-4 TYPE:FEATURE信息。

```
dc5548ax# show fcns database

VSAN 4:
------------------------------------------------------------------
---------
FCID        TYPE  PWWN                    (VENDOR)        FC4-
TYPE:FEATURE
------------------------------------------------------------------
---------
0xbc0000    N     20:00:58:8d:09:0e:e0:d2                 scsi-
fcp:init fc-gs
                  [p12-c210-27-vhba3]
```

现在您可根据本章节前面部分的程序“在Cisco Nexus 5500UP上配置FC SAN”中的流程配置分区和设备别名。

技术提示

大部分Cisco Nexus 5500UP系列交换机的配置也可在设备管理器中完成；然而，设备管理器不能用于在Cisco Nexus 5500UP系列交换机上配置VLAN或以太网中继。

计算连接性

业务概述

随着中小企业不断成长，完成企业信息处理任务所需的服务器数目和类型也将不断增加。这会带来一些挑战：

- 数据中心占地面积和机架空间有所增加
- 电源和冷却消耗增多，特别是在每一代新CPU的功耗都会随着内核速度的增长而增加的情况下，更是如此
- 数据网络电缆设备的复杂性增加，以便为日益增加的服务器数量提供足够的容量和能力
- 用于购买服务器平台和备件的硬件资本支出提高，用于管理和维护不同硬件及操作系统平台的运营支出增加
- 从现有服务器和应用迁移到新平台和连接方法，需要能同时支持传统和新型服务器及应用的灵活架构
- 永续性和迁移路径方面的挑战增大，因为以设备或服务器为中心的应用平台趋向于以平台为中心，可能无法实现出色的负载均衡或迁移到不同的平台

企业经常需要优化对服务器资源投资的利用，以便在从小型服务器机房环境迁移到数据中心时，能够增加新应用并控制成本。

采用传统服务器、网络设备和存储资源扩展数据中心，会为不断增长的企业带来严峻的挑战。必须集成多种硬件平台和技术，才能提供应用最终用户预期的性能和可用性。数据中心内的这些组件还需要进行管理和维护，通常这需要采用基于不同接口和方法的多种管理工具集实现。

技术概述

服务器虚拟化支持在一个通用硬件平台上运行多个应用服务器，使企业专注于提高数据中心的应用性能，并尽可能降低成本。可通过以下多个方面来提高能力和降低成本：

- 多个应用能结合在单一硬件机箱中，减少了数据中心必须支持的机箱数目
- 由于需要运行的线缆减少，可以根据需要更灵活地向主机分配网络连接，因而简化了线缆管理
- 管理程序支持跨多个平台的工作负载永续性和负载共享，即使在地理位置分散的地点也是如此，从而提高了永续性和应用便携性
- 部署于标准化硬件平台上的应用，可减少平台管理控制台，并最大限度地减少硬件备件库存挑战
- 因为负载较轻、闲置浪费昂贵电量的机箱减少了，由此缩减了机箱数目，降低了供电和制冷要求

采用构建虚拟机(VM)的管理程序(Hypervisor)技术来虚拟化服务器平台，以处理多个操作系统和应用，由此企业可将更多应用整合到更少的物理服务器上，降低资本成本和运营成本。管理程序技术还能够将多个虚拟机集合到一个域中，并在此处协调工作负载以在整个数据中心移动，从而提供永续性和负载均衡，并使新应用能够在数小时内部署完成，而不必花费几天或几周时间。

无论是机箱系统中的刀片服务器还是独立的机架安装式服务器，将虚拟机或应用负载从一台服务器移至另一台服务器的能力，都要求网络灵活、可扩展，进而支持任意VLAN出现在数据中心内的任何地方。思科虚拟端口通道 (vPC) 和阵列扩展模块 (FEX) 技术广泛用于思科IBA智能业务平台数据中心中，以可扩展和永续的方式，为分布于整个数据中心的VLAN提供灵活的以太网连接。

简化服务器硬件的管理及其与网络和存储设备间的交互，是有效利用这一投资的另一个重要手段。思科提供了一个简化的参考模型，用于随着小型服务器机房发展为全功能数据中心，对其进行有效管理。此模型得益于思科统一计算系统（UCS）带来的易用性。Cisco UCS提供了单一的图形管理工具，来供应和管理服务器、网络接口、存储接口、以及其直接连接的网络组件。Cisco UCS将所有这些组件视作一个紧密结合的系统，可简化这些复杂的交互，并使企业能够部署与大型企业一样高效的技术，同时无需太长的学习曲线。

思科IBA智能业务平台统一计算参考架构中主要采用的计算平台是Cisco UCS B系列刀片服务器和Cisco UCS C系列机架安装式服务器。Cisco UCS Manager的图形界面易于使用，与思科IBA智能业务平台的目标相一致。当与思科IBA智能业务平台数据中心网络基础一起部署时，该环境可提供出色灵活性，支持同时使用Cisco UCS B系列刀片服务器、Cisco UCS C系列机架安装式服务器、以及连接到千兆和万兆以太网连接的第三方服务器。

以下部分描述在数据中心中增强连接性选项的功能。

Cisco Nexus虚拟端口通道

正如“以太网基础设施”章节中所述，虚拟端口通道 (vPC) 允许物理连接到两个

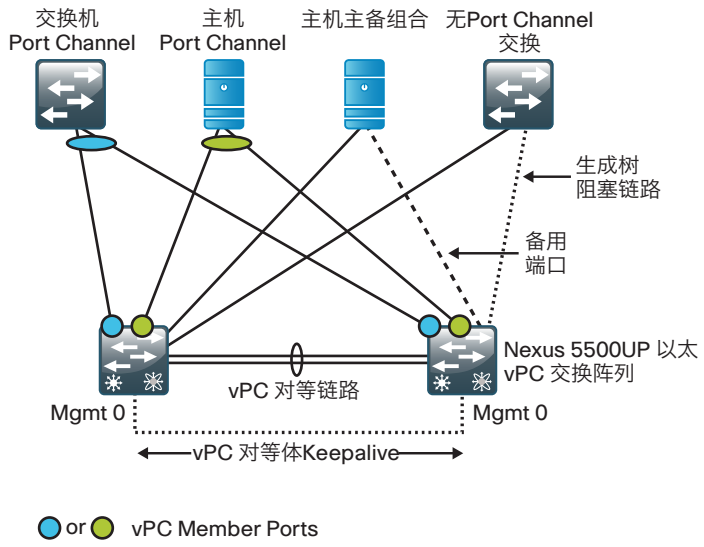
不同Cisco Nexus交换机的链路，针对第三方下游设备显示为来自单一设备，并作为单一以太网端口通道的一部分。这个第三方设备可以是服务器、交换机，或其它任何支持IEEE 802.3ad端口通道的设备。对于Cisco EtherChannel技术，术语“多机箱EtherChannel”（MCEC）即指该技术。MCEC从相连的设备连接到数据中心核心层，提供生成树无环路拓扑结构，允许VLAN在企业数据中心扩展，并保持永续架构。

一个vPC域由两个vPC对等交换机组成，由一个对等链路相连。在vPC对等中，一个是主用，另一个是备用。由这些交换机构成的系统称为vPC域。两个Cisco Nexus交换机间的vPC对等链路是该系统中最重要的连接组件。该链路用于在两个交换机间营造单一控制平台的假象，负责在设备因设计或EtherChannel链路故障而成为单宿主设备时，传送关键控制平面数据包及其它数据包。对于要在vPC上转发的VLAN，该VLAN必须存在于对等链路和两个vPC对等交换机上。

vPC对等持活链路用于解决对等链路连接丢失的双主用情况。如果vPC对等链路连接丢失，备用vPC对等将关闭所有vPC成员链路，主用vPC交换机将继续转发数据包，提供永续的架构。

vPC端口是分配到vPC通道组的一个端口。构成虚拟端口通道的端口在vPC对等体间分开，其在两个vPC交换机上的定义必须完全相同，被称为vPC成员端口。非vPC端口，也称为孤立端口，是属于VLAN的端口，此VLAN是vPC的一部分，但不能设定为vPC成员。下图说明了vPC端口和孤立端口。主机的活动-待机组合接口也被认为是vPC孤立端口。

图 14 - vPC成员和非成员端口



关于vPC孤立端口需要记住的重要一点是，如果vPC对等链路丢失且备用vPC关闭vPC端口，则它不会关闭vPC孤立端口，除非在交换机接口上采用**vpc orphan-port suspend**命令安排如此操作。

示例

```
interface Ethernet103/1/2
  description to_teamed_adapter
  switchport mode access
  switchport access vlan 50
  vpc orphan-port suspend

interface Ethernet104/1/2
  description to_teamed_adapter
  switchport mode access
  switchport access vlan 50
  vpc orphan-port suspend
```

读者提示

vPC的基本概念在http://www.cisco.com/上题为《Cisco NX-OS虚拟端口通道：采用NXOS 5.0的基本设计概念》的白皮书中进行了详细描述。

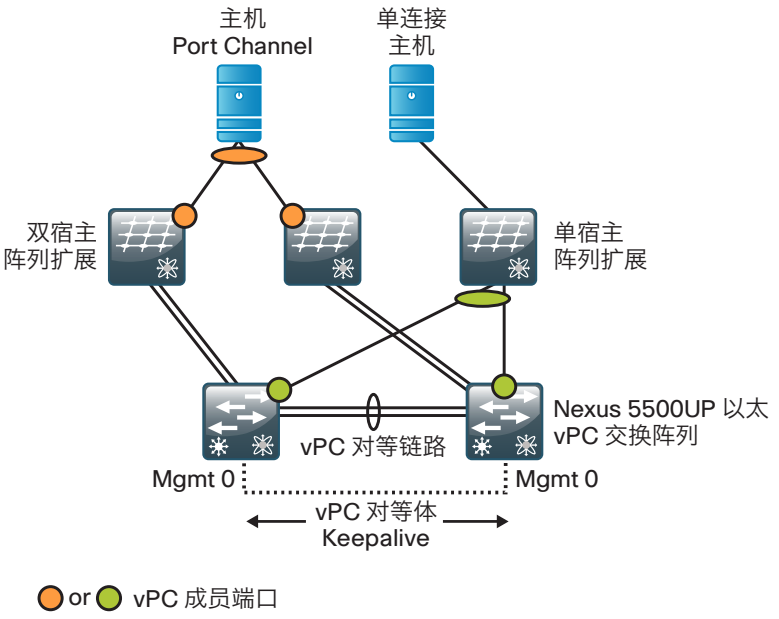
针对Cisco Nexus 5500UP交换机进行的全面vPC域编程在本指南前面的程序 4“配置虚拟端口通道 (vPC) ”中进行详细说明。

Cisco Nexus阵列扩展模块

如本文“以太网基础设施”章节中所述，思科阵列扩展模块 (FEX) 作为到它所连接的Cisco Nexus 5500UP交换机的远程线路卡。这可支持在数据中心核心交换机上集中配置所有交换机端口，并分散连接到更高密度的快速以太网、千兆以太网和万兆以太网，从而支持架顶式服务器连接。由于Cisco FEX充当Cisco Nexus 5500UP交换机上的线路卡，将VLAN扩展到不同Cisco FEX上的服务器端口不会在整个数据中心创建生成树环路。

Cisco FEX可以是针对数据中心核心交换机的单宿主设备 (也称为直通模式)，或是使用vPC的双宿主设备 (也称为主动/主动模式)。

图 15 - 到数据中心核心的Cisco Nexus FEX连接



双宿主 (主动/主动) Cisco FEX使用vPC提供到两个数据中心核心交换机的永续连接，以支持一台相连的主机服务器。每个主机均被视作通过相关连接与vPC双宿主Cisco FEX相连的vPC。Cisco FEX到核心连接包含4至8个上行链路，具体取决于所使用的Cisco FEX类型，并且Cisco FEX上行链路还能够配置为端口通道。

与一对单宿主Cisco FEX相连的主机能够配置用于端口通道操作，以通过到每个Cisco FEX的连接，提供到两个数据中心核心交换机的永续连接。Cisco FEX到核心连接包含4至8个上行链路，具体取决于所使用的Cisco FEX类型，并且Cisco FEX上行链路通常还能够配置为端口通道。

技术提示

诸如局域网交换机等能够产生生成树网桥协议数据单元 (BPDU) 的设备，不应连接到Cisco FEX。Cisco FEX设计用于主机连接，将可禁用出现错误的BPDU数据包接收端口。

对于Cisco Nexus 5500UP数据中心核心交换机和支持服务器连接的以太网端口配置的完整Cisco FEX连接编程，在本指南较早的“以太网基础设施”章节中进行了详细介绍。

Cisco UCS系统网络连接

Cisco UCS B系列刀片服务器和C系列机架安装式服务器都能无缝集成到思科IBA智能业务平台中小企业数据中心架构中。Cisco Nexus 5500UP数据中心核心可在单一平台中提供千兆以太网、万兆以太网和FC（光纤通道）SAN连接。

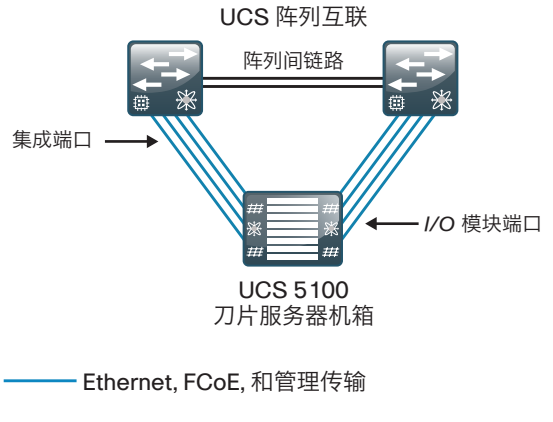
Cisco UCS B系列刀片机箱系统组件

Cisco UCS刀片机箱系统拥有独特架构，可将计算、数据网络访问和存储网络访问集成到单一管理平台接口下的一套通用组件中。该架构中包括的主要组件如下：

- **Cisco UCS 6200系列互联阵列**——为系统中的其它组件提供网络连接和管理功能。
- **Cisco UCS 2200系列阵列扩展模块**——从逻辑角度将互联阵列扩展到用于以太网、FCoE和管理用途的每个机箱中。
- **Cisco UCS 5100系列刀片服务器机箱**——该机箱能够部署多达八个半高或四个全高刀片服务器、与它们相关联的阵列扩展模块，以及四个电源，以实现系统永续性。
- **Cisco UCS B系列刀片服务器**——具有半宽和全宽型号，以及多种高性能处理器和内存架构，可支持客户定制计算资源来满足最关键应用的特定需求。
- **Cisco UCS B系列网络适配器**——支持多种扩展适配器卡，使交换架构能够为服务器提供多个接口。

下图给出了一个Cisco UCS刀片机箱系统中，为在互联阵列和单一刀片机箱间建立连接而需要的物理连接的示例。刀片机箱和互联阵列之间的链路承载着所有服务器数据流量、中央存储流量，以及Cisco UCS Manager生成的管理流量的传输。

图 16 - Cisco UCS刀片机箱系统组件连接



Cisco UCS管理器

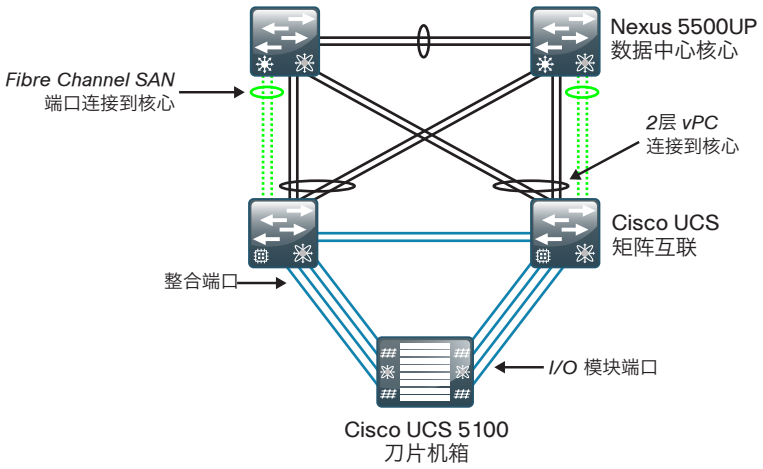
Cisco UCS Manager是驻留在互联阵列上的嵌入式软件，为Cisco UCS的所有组件提供了全面的配置和管理功能。该配置信息在两个互联阵列间复制，为这一关键功能提供了一款高度可用的解决方案。访问Cisco UCS Manager，以完成简单任务的最常用方式就是使用Web浏览器打开基于Java的GUI。为支持对系统进行命令行和编程操作，该系统还提供了一个CLI和一个XML API。

Cisco UCS B系列系统网络连接

Cisco UCS 6200系列互联阵列为Cisco UCS刀片服务器系统提供了连接。下图是一个互联阵列和Cisco Nexus 5500UP系列数据中心核心间连接的详细示例。

互联阵列的默认和建议配置为终端主机模式，这意味着它们不作为全局域网交换机运行，而是它们的运行依赖于上游数据中心交换架构。这样，对网络而言，Cisco UCS就是一个带多个物理连接的虚拟化计算集群。各服务器的流量只传输到特定接口，当主链路发生故障时故障切换功能将启动。图 17中显示的来自互联阵列的以太网流量使用到数据中心核心的vPC链路，提供永续性和流量负载共享。到核心的FC（光纤通道）链路也使用SAN端口通道支持负载共享和永续性。

图 17 - 到核心的CiscoUCS阵列互联



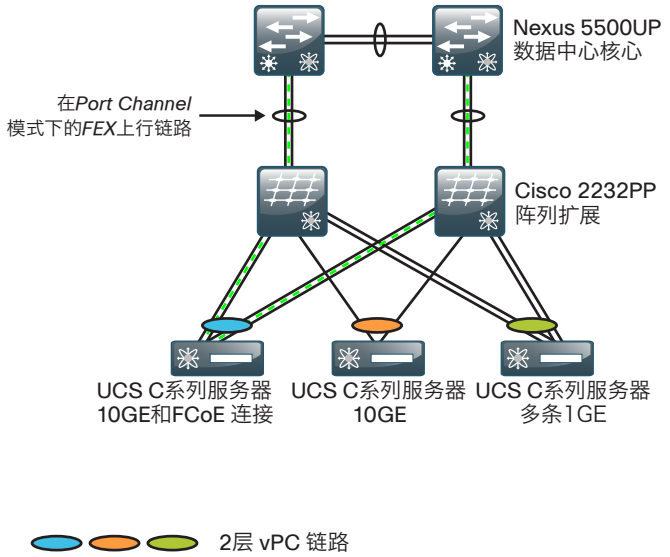
Cisco UCS B系列部署的详细配置可在思科IBA智能业务平台——《数据中心统一计算系统部署指南》中找到。

Cisco UCS C系列网络连接

Cisco UCS C系列机架安装式服务器在简单性、性能和密度之间实现了有效平衡，能够支持生产级虚拟化、Web基础设施和数据中心工作负载。Cisco UCS C系列服务器将统一计算的创新技术和优势扩展到了机架安装式服务器。

Cisco Nexus交换交换可为Cisco UCS C系列服务提供千兆或万兆以太网连接，具体取决于所使用的应用或虚拟机的吞吐量要求以及每台服务器上安装的网络接口卡数量。图 18显示了一些从Cisco UCS C系列服务器到提供千兆和万兆以太网连接的单宿主Cisco FEX的双宿主连接示例。能够支持以太网和FCoE的万兆以太网连接可通过Cisco Nexus 2232PP阵列扩展模块提供，或通过直接在Cisco Nexus 5500UP系列交换机对上使用万兆端口来提供。支持快速以太网或千兆以太网的连接也可使用Cisco Nexus 2248TP阵列扩展模块。

图 18 - Cisco UCS C系列FEX连接示例



在以上的图 18中，Cisco UCS C系列服务器与Cisco FEX选项之间的连接性都使用vPC连接，通过利用从主机至单宿主Cisco Nexus 2232PP FEX之间的IEEE 802.3ad EtherChannel实现。当使用vPC进行服务器连接时，在每个数据中心核心Cisco Nexus 5500UP交换机上，每个服务器接口都必须采用相同的方式配置。Cisco FEX到数据中心核心的上行链路使用端口信道在多条链路上对服务器连接进行负载均衡，并提供了更多冗余性。

具有万兆以太网和FCoE连接的Cisco UCS C系列服务器在服务器中使用融合网络适配器(CNA)，并且必须连接至Cisco Nexus 2232PP FEX，或直接连接至Cisco Nexus 5500UP交换机（就像FCoE上行链路必须使用光纤或双轴连接一样），以便保持FC传输的误码率（BER）阈值。目前，思科仅在万兆以太网上支持FCoE。如果使用vPC，以太网流量将跨服务器链路进行负载均衡，EtherChannel和FC流量从每个链路向上传输至核心，一个链路上的SAN-A流量传输至相连的Cisco FEX和数据中心核心交换机，另一个链路上的SAN-B流量传输至相连的Cisco FEX和数据中心核心交换机，通常为FC SAN流量。

示例

- 下面示例为在第一个Cisco Nexus 5500UP交换机上配置FEX 接口。

```
interface Ethernet103/1/3
```

```
  description Dual-homed server FCoE link to SAN-A VSAN 304
  switchport mode trunk
  switchport trunk allowed vlan 148-163,304
  spanning-tree port type edge trunk
  no shut
```

- 下面示例为在第二个Cisco Nexus 5500UP交换机上配置FEX 接口。

```
interface Ethernet 104/1/3
  description Dual-homed server FCoE link to SAN-B VSAN 305
  switchport mode trunk
  switchport trunk allowed vlan 148-163,305
  spanning-tree port type edge trunk
  no shut
```

具有万兆以太网但没有FCoE的Cisco UCS C系列服务器可以连接至Cisco Nexus 2232 FEX，或直接连接至Cisco Nexus 5500UP交换机。这些服务器连接可以是光纤、铜缆或双轴，取决于使用的Cisco FEX和服务器组合。如果使用vPC，以太网流量在采用EtherChannel的服务器链路之间进行负载均衡。

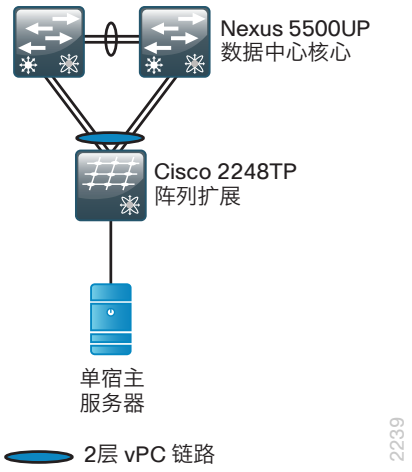
具有多个千兆以太网的Cisco UCS C系列服务器使用vPC在采用EtherChannel的多个链路之间进行流量负载均衡。使用vPC并非一项要求。在需要独立服务器接口的非vPC服务器连接中，除非服务器操作系统提供永续连接性，否则您可能要连接至双宿主Cisco FEX作为提供永续性的首选方式。

有关Cisco Nexus FEX至Cisco Nexus 5500UP交换机连接的详细配置，可在本指南之前的“以太网基础设施”章节中找到。有关Cisco UCS C系列部署的详细配置，可在思科IBA智能业务平台——《数据中心统一计算系统部署指南》中找到。

单宿主服务器连接

随着企业机构的发展，许多具有单一高速以太网或千兆以太网的传统服务器和设备可能需要在数据中心中具有连接性。为了给这些服务器提供更多永续性，建议将使用vPC的双宿主Cisco FEX用于Cisco FEX与数据中心之间的连接，如下图所示。

图 19 - 单宿主服务器与双宿主Cisco FEX之间的连接

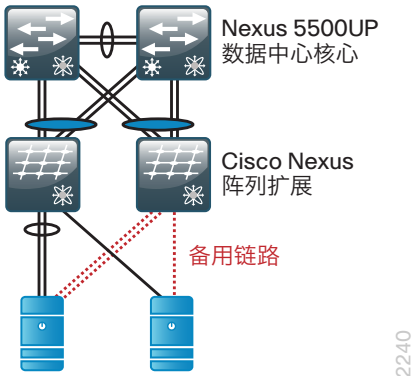


Cisco Nexus 2248TP FEX的vPC连接为连接至相同Cisco FEX的服务器提供控制平面和数据平面冗余性。当阵列上行链路或Cisco Nexus 5500UP核心交换机出现故障时，该拓扑可为相连的服务器提供永续性，但是当Cisco Nexus 2248TP故障时无法提供冗余性。所有连接至vPC双宿主Cisco FEX的服务器都采用vPC连接，并且必须在每个数据中心核心CiscoNexus 5500UP交换机上进行配置。虽然这种方式可以添加永续性，但托管重要应用的单宿主服务器仍应迁移至双宿主连接，以便提供充足的永续性。

具有分组接口连接性的服务器

服务器NIC（网络接口卡）分组具有多种选项和特性。能够在服务器和Cisco FEX之间使用IEEE 802.3ad EtherChannel的NIC适配器和操作系统，将使用在本章节较早的部分“Cisco UCS C系列连接性”中包括的vPC选项。对于使用主用/备用方法连接至Cisco FEX的NIC适配器和操作系统，双宿主Cisco FEX可提供最好的服务，如下图所示。

图 20 - 具有主用/备用NIC的服务器与Cisco FEX之间的连接



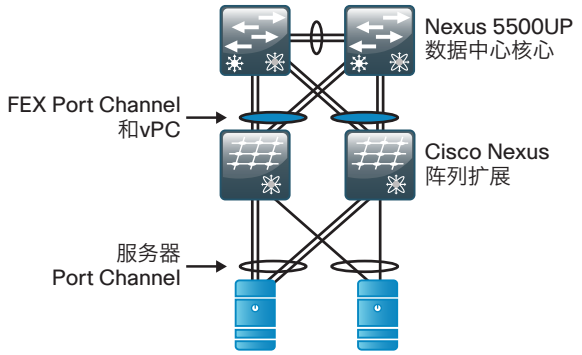
来自Cisco Nexus 2248TP FEX的vPC连接为连接至每个Cisco FEX的服务器提供控制平面和数据平面冗余性。当阵列上行链路或Cisco Nexus 5500UP核心交换机出现故障时，该拓扑可为相连的服务器提供永续性。当Cisco FEX出现故障时，NIC分组将切换至备用接口。

增强的阵列互联和服务器连接性

双宿主的思科Nexus阵列扩展通过同时连接到核心交换机提高了系统的可靠性。有了双宿主的FEX，在一个数据中心的核心思科Nexus5500UP交换机失去服务时，FEX上行链路的流量可以通过剩下的数据中心核心交换机继续转发。直到最近，双宿主的FEX连接也无法支持一个单一的EtherChannel连接到两个双归属FEX。这也意味着，您可能需要一个混合的单宿主FEX和双宿主FEX的数据中心，以支持不同的服务器的连接要求。

然而，从思科Nexus 5500系列交换机的思科NX-OS release 5.1(3)N1(1)版本开始支持port-channel连接到2个双宿主的FEX，如图 21所示。这一新功能被称为增强型vPC。思科5000交换机不支持增强型vPC。

图 21 - 增强型vPC

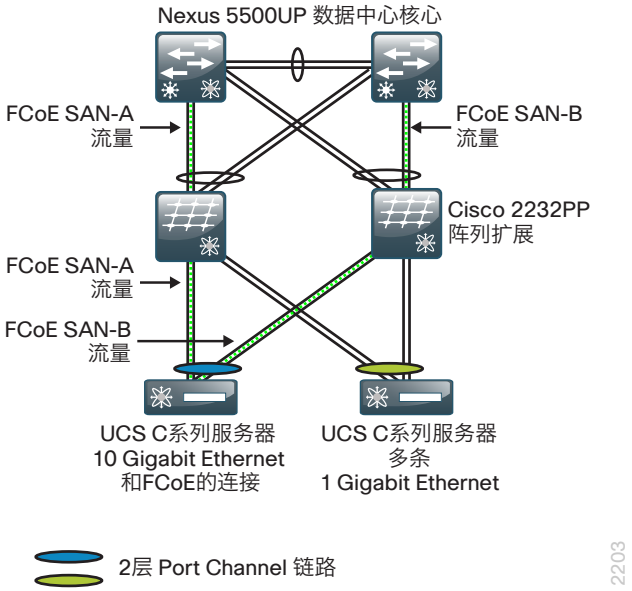


2202

在增强型vPC中，双归属FEX的连接到数据中心核心的上行链路与服务器的port channel进行程序连接。思科Nexus5500交换机自动创建一个vPC使服务器port channel连接到双宿主的一对FEX通道。其结果是一个更灵活，更简化的的数据中心FEX部署，不管服务器是否支持EtherChannel，都可以支持单宿主或双宿主的服务器。

增强型vPC还支持双宿主服务器与EtherChannel运行FCoE。然而，这可能不适合于一个高带宽的FCoE环境，因为FCoE流量只能使用FEX上行链路的一个子集，如在图 22中所示。流量只能使用FEX到思科Nexus 5500的上行链路上的左边或右边，而SAN的流量必须保持SAN-A和SAN-B隔离和因此无法同时连接到两个数据中心的核心交换机。非FCoE的以太网通信（例如，IP连接）的双宿主FEX可以利用所有FEX到-数据中心的的核心上行链路，最大限度地提高流量负载均衡和带宽。

图 22 - 增强型vPC和FCoE流量

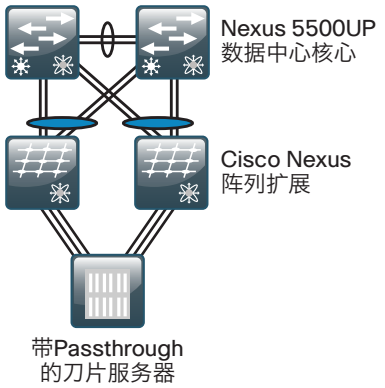


第三方刀片服务器系统连接性

刀片服务器系统可以由思科以外的制造商提供。当您具有非思科刀片服务器系统连接至数据中心时，有多个选项可以连接至您的思科IBA智能业务平台数据中心设计。

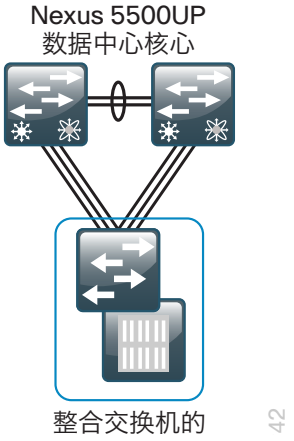
第一个选项是使用具有直通模块的刀片服务器系统，该模块将服务器接口直接扩展至刀片服务器机箱以外，无需在刀片服务器系统中使用内部交换架构。当使用直通模块时，服务器NIC连接可以使用Cisco Nexus阵列扩展模块来支持高密度端口扇出和永续性连接，如下图所示。

图 23 - 具有直通模块的第三方刀片服务器系统



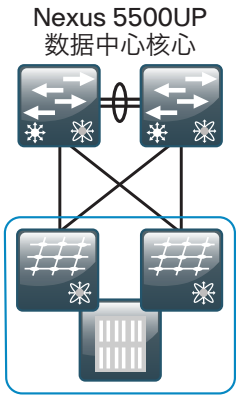
将非思科刀片服务器系统连接至思科IBA智能业务平台数据中心的第二个选项涉及具有集成以太网交换机的刀片服务器系统。在该场景中，刀片服务器机箱中的集成交换机中将产生生成树BPDU，因此无法连接至阵列扩展模块。另一个考虑因素是，建议具有集成交换机的刀片服务器使用多个高速万兆以太网上行链路，从而直接连接至Cisco Nexus 5500UP交换机核心，如图 24中所示。

图 24 - 具有集成交换机的第三方刀片服务器系统



第三个选项是嵌入思科Nexus阵列扩展到非思科的刀片服务器系统中，以连接到思科IBA数据中心核心，如图 25所示。虽然这个选项还未在思科IBA《数据中心部署指南》测试和记录，但对于许多企业它已被证明是一个理想的连接选项。

图 25 - 具有嵌入式Cisco Nexus阵列扩展的非思科刀片服务器系统



总结

本章节中列出的计算连接选项介绍了思科IBA智能业务平台数据中心基础设计如何与Cisco UCS（思科统一计算系统）相集成，以构建一个灵活且可扩展的计算连接。数据中心架构还支持永续的非思科服务器和刀片系统连接。如需进一步了解部署Cisco UCS Server系统的详情，请参见思科IBA智能业务平台——《数据中心统一计算系统部署指南》。

备注

网络安全

业务概述

在今天的商业环境中，一个企业部分最重要的资产往往保存在数据中心内。客户和个人记录、财务数据、电子邮件和知识产权等都必须保存在一个安全环境中，以确保保密性和可用性。此外，在特定行业中，网络的某些部分必须遵从行业或政府法规，强制实施特定的安全控制措施，以保护客户信息。

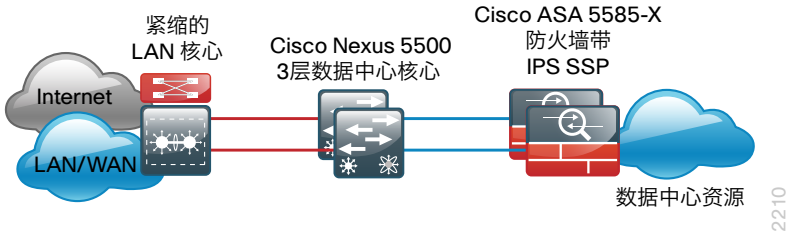
为确保数据中心内重要电子资产的安全，要通过网络安全手段对机构加以保护，防御自动或人为的窃取和篡改，并防止主机遭受消耗大量资源的蠕虫、病毒或僵尸网络的破坏。

虽然蠕虫、病毒及僵尸网络对中央数据造成巨大威胁，尤其是严重危及主机性能和可用性，但与此同时，还必须防止员工窃取和非法访问服务器上的数据。一直以来，统计数据都表明，大部分数据丢失和网络破坏的情况都是企业网络内部人为活动（故意或意外）的结果。

技术概述

为最大限度降低恶意网络入侵的影响，应该在客户端和中央数据资源之间部署防火墙及入侵防御系统（IPS）。

图 26 - 部署内嵌(inline)的防火墙以保护数据资源



因为在托管数据中心资源的受保护VLAN外部，处处都可能存在威胁，所以，与保护这些资源相关的安全策略应考虑到以下潜在威胁因素。

数据中心威胁情况：

- 互联网
- 远端接入和远程工作人员VPN主机
- 远程办公室/分支机构网络
- 业务合作伙伴连接
- 园区网络
- 无保护数据中心网络
- 其它受保护数据中心网络

数据中心安全设计采用一对思科自适应安全设备（ASA）5585-X，并安装了SSP-20防火墙模块及相应的IPS安全服务处理器（SSP）。此配置可提供高达10Gbps的防火墙吞吐率。IPS和防火墙SSP可提供3Gbps的并发吞吐率。我们一系列带有IPS防火墙的Cisco ASA 5585-X以满足您的处理要求。

Cisco ASA机箱中安装的模块上的所有端口都可用于防火墙SSP，由此提供了极其灵活的配置。Cisco ASA防火墙使用两条万兆以太网链路双归属到数据中心核心层Cisco Nexus 5500UP交换机，以提供永续性。每个Cisco ASA上的链路对配置为一条EtherChannel，提供负载均衡以及快速透明的故障恢复。Cisco Nexus 5500UP数据中心核心交换机的Cisco NX-OS虚拟端口通道(vPC)功能，允许防火墙EtherChannel跨越两个数据中心核心交换机（多机箱EhterChannel），却显示为连接到单一的上游交换机。该EtherChannel链路配置为VLAN中继，以支持对于数据中心内多个安全VLAN的访问。数据中心核心层上的一个VLAN作为面向防火墙的外部VLAN，而驻留在该VLAN内的任意主机或服务器处于防火墙之外，因此无法获得Cisco ASA的保护，从而防御来自企业网络任意其它地方的攻击。EtherChannel中继上的其它VLAN被指定为防御所有其它的数据中心威胁向量，或是结合其它IPS服务进行防御。

这对Cisco ASA通过配置，可提供防火墙主用－备用高可用性运行，确保将软件维护或硬件故障造成的停运对数据中心访问的影响降至最低。当Cisco ASA设备以主用—备用模式进行配置时，备用设备不处理流量，因此必须确保主用设备拥有足够高的吞吐率，能够满足核心层和数据中心之间的连接需求。尽管IPS模块不会主动交换状态流量，但它们可以通过将其状态报告给防火墙状态监控器的方式参与防火墙设备的主用/备用状态。如果Cisco ASA本身遇到问题或IPS模块不可用，将进行防火墙故障切换。

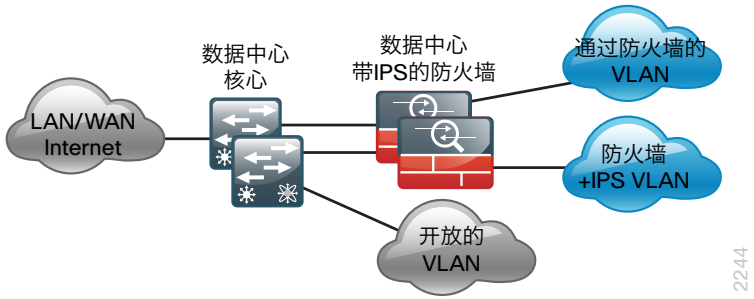
Cisco ASA以路由模式进行配置；因此，安全网络必须位于一个与客户端子网不同的子网中。如果Cisco ASA以透明模式部署，IP子网分配将会得到简化；但是主机可能会在无意中被连接至错误的VLAN，而它们仍然能够与网络进行通信，从而导致意外的安全暴露。

数据中心IPS能够监控和遏制得到Cisco ASA安全策略许可的流量中所包含的潜在恶意行为。IPS传感器以混杂入侵检测系统(IDS)模式部署，因此它们仅监控和报告异常流量。IPS模块可以在IPS模式中以内嵌的方式部署，以便充分利用其入侵防御功能，在恶意流量抵达目的地之前将其阻止。选择传感器是否丢弃流量受多个因素影响：对于出现安全事件的风险容忍，对于不经意丢弃有效流量的风险规避，以及IPS法规遵从要求等其他可能的外部推动原因。由于可以配置以IDS模式还是IPS模式运行，所以在满足特定安全策略方面提供了最高灵活性。

安全拓扑设计

思科IBA智能业务平台安全数据中心设计在数据中心中提供了两个安全的VLAN。安全VLAN的数量可自行确定。本设计示例显示了如何为需要进行隔离的主机服务创建多个安全网络。诸如企业资源规划和客户关系管理等重要应用可能需要与其他应用进行隔离，使用自己的VLAN。

图 27 - 采用安全VLAN的设计示例



在另一个示例中，间接暴露给互联网的服务（通过web服务器或互联网隔离区中的其它应用服务器）应尽可能与其他服务隔离，以避免部分服务器上的互联网威胁蔓延到其他未暴露的服务。除非安全策略规定了服务隔离，否则VLAN间的流量应保持最低。保持VLAN内服务器间的流量将可以改进性能，并减少网络设备的负载。

在本部署中，未应用任何安全策略的开放式VLAN在数据中心核心交换机上进行物理和逻辑配置。对于需要访问策略的设备，它们将在防火墙后的VLAN中部署。需要访问策略和IPS流量检测的设备将在Cisco ASA后逻辑上不同的VLAN中部署。因为Cisco ASA仅物理连接至数据中心核心Nexus交换机，所以这些受保护的VLAN也将在数据中心核心交换机的第二层中存在。所有受保护的VLAN均在逻辑上通过三层连接至流经Cisco ASA的网络的其余部分，因此只能通过穿越Cisco ASA抵达。

安全策略部署

企业在制定IT安全策略时，应首先从定义防火墙策略入手。如果没有公司级的安全策略，那么企业很难在维护安全的计算环境的同时定义一个有效的策略。

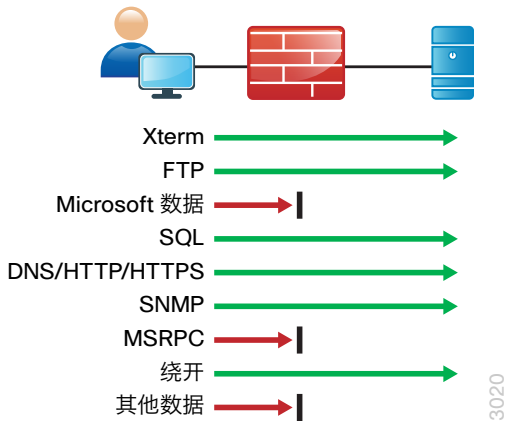
为了在企业网络的各个职能分区间高效地部署安全策略，您应当尽可能获得有关预期网络行为的最详细信息。您掌握的预期网络行为信息越详细，您就越能够出色地定义安全策略，在优化安全性的同时满足企业在应用流量和性能方面的要求。

读者提示

对法规遵从注意事项进行详细阐述超出了本文档的范围，您应在网络安全设计中将行业法规考虑在内。不符合法规要求可能会导致罚金或商业活动暂缓等规管惩罚。

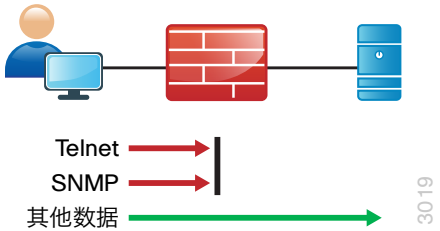
网络安全策略基本可分为两种：“白名单”策略和“黑名单”策略。白名单安全策略提供更加含蓄的安全做法，它会拦截除支持应用所需外的所有流量（在足够精细的级别）。因为只有开展业务所需的流量才会得到许可，因此白名单通常能够更好地满足管制要求。其他流量将被拦截，无需对其进行监控即可确保没有非法活动发生。这将减少将转发至IDS或IPS的数据量，并能最大限度减少在发生入侵事件或数据丢失时必须浏览的日志条目的数量。

图 28 - 白名单策略示例



与白名单相反，黑名单策略只拒绝那些明确会给集中式数据资源带来最大风险的流量。黑名单策略在维护方面更为简单，干扰网络应用的可能性也更低。如果您有机会确定网络的具体要求并调整安全策略来避免所需的网络活动受到干扰，那么白名单策略不失为最佳的方案。

图 29 - 黑名单策略示例



Cisco ASA防火墙隐含地以一个拒绝所有 (deny-all) 规则来结束访问列表。黑名单策略在隐含的拒绝所有规则之前，包括一条明确的规则，可允许任何未被明确许可或拒绝的流量通过。

不管您是选择采用白名单还是黑名单策略基础，都应该考虑部署IDS或IPS，来控制针对可信应用流量的恶意活动。至少，IDS或IPS可以协助进行取证，从而确定数据外泄的原由。理想状态下，IPS可以在攻击发生时进行检测和阻止，并提供详细信息来跟踪恶意活动的来源。IDS或IPS还可能是网络所遵从的法规监察的明确要求 (例如PCI 2.0) 。

在对网络的应用活动进行详细研究不切实际，或者如果网络可用性要求禁止进行应用故障排除的情况下，阻止高风险流量的黑名单策略提供了一个影响较小但是安全性也较低的选项 (与白名单策略相比) 。如果识别所有应用要求不切实际，那么您可以实施启用了日志功能的黑名单策略，以便生成该策略详细的历史记录。在掌握了网络行为的详细信息后，制定白名单策略的工作将会大大简化，效率也会进一步提升。

部署详情

数据中心安全部署通过5个独立的流程来实现：

- “配置Cisco ASA防火墙连接”，在Cisco Nexus 5500UP数据中心核心配置Cisco ASA防火墙网络连接。
- “配置数据中心防火墙”，配置Cisco ASA 初始设置以及与数据中心核心的连接。
- “配置防火墙的高可用性”，针对防火墙对配置高可用性的主用/备用状态。
- “评估和部署防火墙安全策略”，确定安全策略的需求以及应用配置以满足需求的程序概述。
- “部署Cisco IPS”，集成连通性和策略配置在一个程序中。

流程

配置Cisco ASA防火墙连接

1、配置Nexus 5500s上的防火墙

2、在核心交换机上配置端口通道

完成以下程序，来配置Cisco ASA机箱与核心层之间的连接。请注意，在本设计介绍的配置中，Cisco ASA防火墙通过使用EtherChannel中的一对万兆以太网接口连接至Nexus 5500UP数据中心核心交换机。Cisco ASA防火墙将在数据中心核心路由接口和同样驻留在交换机中的受保护VLAN之间连接。

连接主Cisco ASA防火墙与第1个Cisco Nexus 5500数据中心核心交换机的接口，再连接第1个Cisco ASA防火墙与第2个Cisco Nexus 5500数据中心核心交换机的接口。Cisco ASA网络端口的连接如下：

- 万兆以太网0/8连接Cisco Nexus 5500UP 交换机以太网1/1
- 万兆以太网0/9连接Cisco Nexus 5500UP 交换机以太网1/2
- 千兆以太网0/1通过交叉或直通以太网电缆连接到其他由于故障切换链路的防火墙

表 7 - 数据中心防火墙VLAN

VLAN	IP地址	信任状态	使用
153	10.4.53.1 /25	不被信任	数据中心核心路由防火墙
154	10.4.54.X /24	被信任	防火墙保护的VLAN
155	10.4.55.X /24	被信任	防火墙和IPS保护的VLAN

程序 1　配置Nexus 5500s上的防火墙

步骤 1: 在第1个Cisco Nexus 5500UP 数据中心核心交换机上配置outside (untrusted) 和inside (trusted) VLAN。

```
vlan 153
name FW_Outside
vlan 154
  name FW_Inside_1
vlan 155
  name FW_Inside_2
```

步骤 2: 在第1个Cisco Nexus 5500UP 数据中心核心交换机上为VLAN153配置3层SVI。为默认网关设置HSRP地址为10.4.53.1以及为此交换机设置HSRP优先级为110。

```
interface Vlan153
  no shutdown
  description FW_Outside
  no ip redirects
  ip address 10.4.53.2/25
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 153
    priority 110
    ip 10.4.53.1
```

步骤 3: 在第1个Cisco Nexus 5500UP数据中心核心交换机上配置静态路由指向Cisco ASA防火墙后的受信子网。

```
ip route 10.4.54.0/24 Vlan153 10.4.53.126
ip route 10.4.55.0/24 Vlan153 10.4.53.126
```

步骤 4: 在第1个Cisco Nexus 5500UP数据中心核心交换机上将受信子网重分布到现存的EIGRP路由进程。此设计使用route map来控制将被重分布的静态路由。

```
route-map static-to-eigrp permit 10
  match ip address 10.4.54.0/24
route-map static-to-eigrp permit 20
  match ip address 10.4.55.0/24
!
router eigrp 100
  redistribute static route-map static-to-eigrp
```

步骤 5: 在第2个Cisco Nexus 5500UP 数据中心核心交换机上配置outside (不受信的) 和inside (受信的) VLAN。

```
vlan 153
  name FW_Outside
vlan 154
  name FW_Inside_1
vlan 155
  name FW_Inside_2
```

步骤 6: 在第2个Cisco Nexus 5500UP 数据中心核心交换机上为VLAN153配置3层SVI。为默认网关设置HSRP地址为10.4.53.1以及为此交换机设置HSRP优先级为默认值。

```
interface Vlan153
  no shutdown
  description FW_Outside
  no ip redirects
  ip address 10.4.53.3/25
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 153
    ip 10.4.53.1
```

步骤 7: 在第2个Cisco Nexus 5500UP数据中心核心交换机上配置静态路由指向Cisco ASA防火墙后面的受信子网。

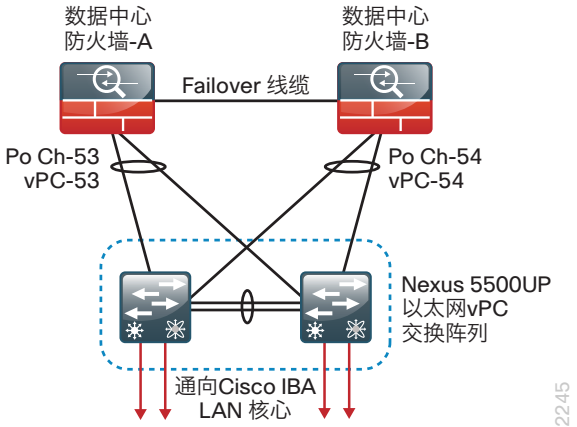
```
ip route 10.4.54.0/24 Vlan 153 10.4.53.126
ip route 10.4.55.0/24 Vlan 153 10.4.53.126
```

步骤 8: 在第2个Cisco Nexus 5500UP数据中心核心交换机上将受信子网重分布到现存的EIGRP路由进程。此设计使用route map来控制将被重分布的静态路由。

```
route-map static-to-eigrp permit 10
  match ip address 10.4.54.0/24
route-map static-to-eigrp permit 20
  match ip address 10.4.55.0/24
!
router eigrp 100
   redistribute static route-map static-to-eigrp
```

程序 2　在核心交换机上配置端口通道

在数据中心内保护应用和服务器的Cisco ASA防火墙将通过EtherChannel链路双归属连接至每个数据中心核心Cisco Nexus 5500UP交换机。



双宿主或多机箱EtherChannel使用vPC连接至Cisco Nexus 5500UP交换机，允许Cisco ASA通过一个逻辑EtherChannel连接至两个数据中心核心交换机。

步骤 1: 在第一个Cisco Nexus 5500UP数据中心核心交换机上配置将组成端口通道的物理接口。

```
interface Ethernet1/1
  description DC5585a Ten0/8
  channel-group 53 mode active
!
interface Ethernet1/2
  description DC5585b Ten0/8
  channel-group 54 mode active
```

当您分配通道组到一个物理接口时，这将创建一个逻辑EtherChannel接口，我们将在下一步骤中配置它。

步骤 2: 在第一个数据中心核心交换机上配置逻辑port-channel接口。绑在port channel下的物理口将从逻辑的port-channel端口继承配置。将在程序3 “配置QoS策略”中创建的QoS策略分配给port channel接口。

```
interface port-channel53
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-
QOS
  vpc 53
!
interface port-channel54
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-
QOS
  vpc 54
```

该port channel也被创建为vPC port channel，因为阵列接口都是双宿主EtherChannel到Nexus 5500UP数据中心核心交换机。

步骤 3: 应用以下配置到第2个Cisco Nexus 5500UP数据中心核心交换机。

```
interface Ethernet1/1
  description DC5585a Ten0/9
  channel-group 53 mode active
!
interface Ethernet1/2
```

```
  description DC5585b Ten0/9
  channel-group 54 mode active
!
interface port-channel53
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-
QOS
  vpc 53
!
interface port-channel54
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-
QOS
  vpc 54
```

流程

配置数据中心防火墙

1、配置初始Cisco ASA 设置

2、配置防火墙连接性

3、配置防火墙到核心层的静态路由

4、配置用户认证

5、配置时间同步和登录

6、配置设备管理协议

这部分的配置用命令在一对高可用的思科ASA防火墙的console端口上进行配置这个程序的配置。备用防火墙会自动从主用防火墙同步配置，在下一个程序 “配置防火墙高可用性”会完成这个高可用的配置。

Enable mode的出厂默认密码是<CR>。

表 8 - Cisco ASA 5500X防火墙和IPS模块地址

ASA防火墙故障切换状态	Firewall IP地址	IPS模块IP地址
主用	10.4.53.126 /25	10.4.63.21 /24
备用	10.4.53.125 /25	10.4.63.23 /24

表 9 - 用于部署的常用网络服务器示例

服务	地址
域名	cisco.local
活动目录, DNS, DHCP服务器	10.4.48.10
Cisco ACS服务器	10.4.48.15
NTP服务器	10.4.48.17

程序 1　配置初始Cisco ASA 设置

连接Cisco ASA 防火墙控制台并执行以下全局配置。

步骤 1: 选择匿名监控属性。当您进入未配置设备的配置模式，系统会提示您一个匿名报告。您可以选择是否开启给思科错误和建康信息的匿名报告。请根据您的企业安全策略选择合适的选项。

```
************************** NOTICE **************************

Help to improve the ASA platform by enabling anonymous
reporting,
which allows Cisco to securely receive minimal error and
health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help
improve
the product? [Y]es, [N]o, [A]sk later:N
```

步骤 2: 配置Cisco ASA防火墙的主机名以便轻松识别。

```
hostname DC5585ax
```

步骤 3: 禁用专用管理端口。本设计未使用专用管理端口。

```
interface Management0/0
  shutdown
```

步骤 4: 配置本地用户身份验证。

```
Username [username] password [password]
```

技术提示

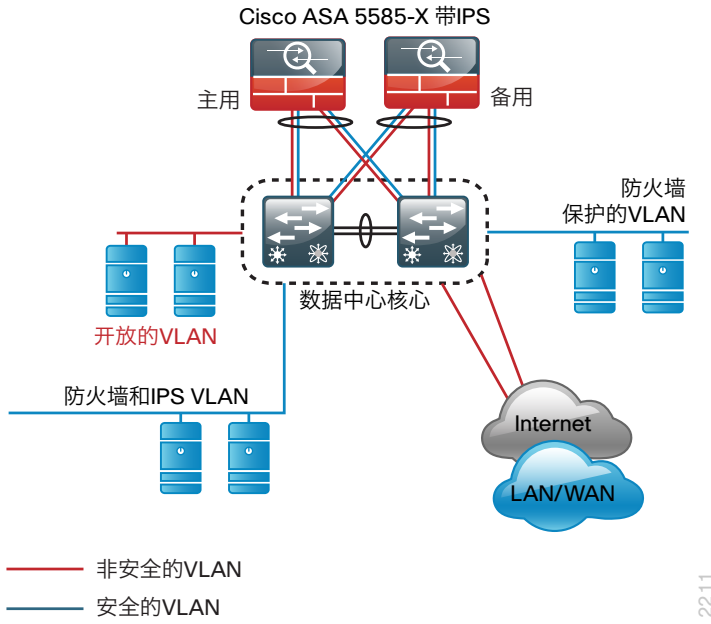
本文档的所有密码只是用于举例，请不要用于产品配置。请遵从您公司的策略，如果没有现成的策略，请创建一个至少八位字符并结合大小写字母和数字的密码。

步骤 5: 配置enable密码。

```
enable password [password]
```

程序 2　配置防火墙连接性

两个万兆以太网链路将每个Cisco ASA机箱连接至两个核心Cisco Nexus交换机。两个接口在端口通道组中组对。在用于外部VLAN 153和所有受保护VLAN内部 (154和155) 的端口通道中创建子接口。创建的每个接口都将分配正确的VLAN、适当的名称、安全级别、IP地址和子网掩码。



Cisco ASA上的所有接口都有一个安全级别设置。编号数字越大，表明该接口

相对于其他接口越可信。内部接口默认分配最高安全级别100。外部接口获得的编号为0。在默认状态下，流量能从高安全级别接口传输到较低安全级别接口。也就是说，来自内部网的流量可以传输到外部网，而反之则不可以。

步骤 1: 使用两个万兆以太网接口配置端口通道组。

```
interface Port-channel10
description ECLB Trunk to 5548 Switches
 no shutdown
!
interface TenGigabitEthernet0/8
 description Trunk to DC5548x eth1/1
 channel-group 10 mode passive
 no shutdown
!
interface TenGigabitEthernet0/9
 description Trunk to DC5548x eth1/2
 channel-group 10 mode passive
 no shutdown
```

步骤 2: 为3个VLAN配置子接口: 外部VLAN 153，防火墙内部VLAN 154，以及具有IPS 防火墙内部VLAN 155。Configure the subinterfaces for the three VLANs:VLAN 153outside, VLAN 154inside the firewall, and VLAN 155inside the firewall with IPS.

```
interface Port-channel10.153
 description DC VLAN Outside the FW
 vlan 153
 nameif outside
 security-level 0
 ip address 10.4.53.126 255.255.255.128 standby 10.4.53.125
 no shutdown
!
interface Port-channel10.154
 description DC VLAN Inside the Firewall
 vlan 154
 nameif DC-InsideFW
 security-level 75
 ip address 10.4.54.1 255.255.255.0 standby 10.4.54.2
 no shutdown
!
interface Port-channel10.155
 description DC VLAN Inside the FW w/ IPS
 vlan 155
 nameif DC-InsideIPS
 security-level 75
 ip address 10.4.55.1 255.255.255.0 standby 10.4.55.2
no shutdown
```

程序 3 配置防火墙到核心层的静态路由

因为Cisco ASA是通往数据中心安全VLAN的网关，所以Cisco ASA对配置为使用静态路由连接至外部VLAN 153上的Cisco Nexus交换机的HSRP地址。

步骤 1: 在Cisco ASA对上配置指向数据中心核心HSRP地址的静态路由。

```
route outside 0.0.0.0 0.0.0.0 10.4.53.1 1
```

程序 4 配置用户认证

(可选)

如果您想要减少每个设备的操作任务，配置集中式用户身份验证，通过使用TACACS+协议，在基础设施设备上进行身份验证管理登录至AAA服务器。

随着网络及需要维护设备数量的增长，在每个设备上的本地用户的维护成本也在相应增加。一个集中的AAA服务，为每台设备减少运营任务，并提供关于用户访问安全合规性和根源分析的审计日志。当为访问控制启用AAA，所有的网络基础设施设备的管理访问 (SSH和HTTPS) 都由AAA控制。

读者提示

用于此架构的AAA服务器是Cisco Secure Access Control Server(ACS)（思科安全访问控制服务器（ACS））。配置Cisco Secure ACS 请参考Cisco IBA——《使用ACS的无边界网络设备管理部署指南》。

TACACS+是在基础设施设备上用于验证管理登录AAA服务器的主协议。在每个网络基础设施设备上，一个本地AAA用户数据库已被定义，它提供备用身份认证源以防集中TACACS+服务不可用的情况。

步骤 1: 配置TACACS+服务器。

```
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (outside) host 10.4.48.15 SecretKey
```

步骤 2: 首先用TACACS+服务器配置设备的管理认证，如果TACACS+服务器不可用则使用本地用户数据库。

```
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
```

步骤 3: 配置设备使用AAA授权管理用户。

```
aaa authorization exec authentication-server
```

技术提示

在Cisco ASA 防火墙的用户授权不像Cisco IOS 设备，不会自动为用户开启enable提示即便用户有15级的权限。

程序 5 配置时间同步和登录

记录和监控是网络安全设备支持故障排除和安全审计的关键环节。

NTP用来在一个网络内同步设备时间。NTP网络通常从一个权威时间源获得时间，例如电台时间或者时间服务器里的原子时钟。NTP通过企业网络分配这些时间。

网络设备应被命令同步到在网络中的一个本地NTP服务器。本地NTP服务器通常参考一个来自外部源反馈的更精确时钟。

有一系列的细节可以被记录在设备上。Informational-level（信息级别）的日志在详细内容和日志信息量之间达到一个平衡。较低的日志级别产生较少的消息，但它们不会产生足够的细节来有效地审计网络活动。较高的日志级别产生更大的信息量，但并不增加更多的价值。

步骤 1: 配置NTP服务器IP地址。

```
ntp server 10.4.48.17
```

步骤 2: 配置时间区域。

```
clock timezone PST -8 0
clock summer-time PDT recurring
```

步骤 3: 配置在设备上存储哪个日志。

```
logging enable
logging buffered informational
```

程序 6 配置设备管理协议

思科自适应安全设备管理器（ASDM）要求设备的HTTPS服务器是可用的。确保配置使得包括行政人员通过思科ASDM可以访问到设备；设备可以提供一个控制Cisco ASDM 访问的单一地址或者管理子网（在本例中是10.4.48.0/24）。

HTTPS和SSH是 HTTP和Telnet协议更安全的替代品。它们使用SSL和TLS以提供设备认证和数据同步。

使用SSH和HTTPS来更安全地管理设备。两种协议都为隐私加密，而不安全的协议——Telnet 和HTTP则被关闭。

开启SNMP以允许网络基础设施设备被NMS管理。SNMPv2c 被配置为只读团体字符。

步骤 1: 允许内部管理员通过HTTPS和SSH远程管理设备。

```
domain-name cisco.local
http server enable
http 10.4.48.0 255.255.255.0 outside
ssh 10.4.48.0 255.255.255.0 outside
ssh version 2
```

步骤 2: 配置设备以允许来自NMS的SNMP轮询。

```
snmp-server host outside 10.4.48.35 community [cisco]
snmp-server community [cisco]
```

流程

配置防火墙高可用性

1、为HA配置主用设备

2、为HA配置备用Cisco ASA

Cisco ASA被设置为高可用性主用/被用对。它使用主用/备用模式，而不是主用/备用配置，因为这样允许相同的设备用于防火墙和VPN服务器（在设备上主动/主动配置的VPN功能默认被禁用）。如果主用设备失效或者需要停机维修，则备用设备会承担所有防火墙和IPS功能。在主用/备用模式时，只有一台设备在同一时间通过流量；因此，2台Cisco ASA的任何一台必须能够处理整个流量负载。

这一对ASA必须是同一型号，具有相同特性许可证和IPS（如果已安装此模块）。开启故障切换，备用ASA需要上电并用电缆连接到同一网络。

将每个设备的一个接口配置为state-synchronization（状态-同步）接口，设备使用该接口共享配置更新，确定设备在高可用性对中优先级，并交换活跃的连接状态信息。该failover接口接受状态同步信息。所有会话状态通过这个接口从主用设备复制到备用设备。这会产生大量的数据，所以建议其为专用接口。

默认情况下，设备可以花费2至25秒从故障中恢复。调整故障切换轮询时间可以减少到0.5至5秒。在一个合适的设备，轮询时间可以调整降低而对设备性能没有影响，最大限度的减少故障切换过程中停机时间所破坏的用户体验。在本指南中我们不建议将故障切换计时器的时间间隔缩短到上述值以下。

程序 1　为HA配置主用设备

步骤 1: 在主用设备上开启failover（故障切换），然后分配其为主用unit（单元）。

```
failover
failover lan unit primary
```

步骤 2: 配置failover接口。为故障切换输入一个配对密钥，稍后您将在备用设备上使用它来配对。

```
failover lan interface failover GigabitEthernet0/1
failover key [key]
failover replication http
failover link failover GigabitEthernet0/1
```

步骤 3: 如果您想要在设备或链接失败时加速故障切换，您可以调整故障切换计时器。默认设置取决于故障状况，Cisco ASA 使用2至25秒从故障切换到备用单元。调整故障切换轮询时间可以降低到0.5至5秒，这也取决于故障状况。

在低负载设备至平均负载设备上，轮询时间可以调整低的同时对性能没有影响。

```
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
```

步骤 4: 配置failover接口IP地址。

```
failover interface ip failover 10.4.53.130 255.255.255.252
standby 10.4.53.129
```

步骤 5: 开启failover接口。

```
interface GigabitEthernet0/1
 no shutdown
```

步骤 6: 配置failover监控inside和outside接口，如果在数据中心VLAN丢失连接，主用防火墙将切换至备用防火墙。

```
monitor-interface outside
monitor-interface DC-InsideFW
monitor-interface DC-InsideIPS
```

程序 2　为HA配置备用Cisco ASA

步骤 1: 在备用Cisco ASA 上，开启failover并分配其作为备用单元。

```
failover
failover lan unit secondary
```

步骤 2: 配置failover接口。

```
failover lan interface failover GigabitEthernet0/1
failover key [key]
failover replication http
failover link failover GigabitEthernet0/1
```

步骤 3: 配置failover接口IP地址。

```
failover interface ip failover 10.4.53.130 255.255.255.252
standby 10.4.53.129
```

步骤 4: 开启failover接口。

```
interface GigabitEthernet0/1
 no shutdown
```

步骤 5: 验证Cisco ASA 设备之间高可用性同步信息。在主用设备的CLI上，输入**show failover state**命令。

```
DC5585ax# show failover state

               State          Last Failure Reason      Date/
Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  None
15:18:12 UTC May 25 2012

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

流程

评估和部署防火墙安全策略

1、评估安全策略要求

2、部署相应的安全策略

本流程描述了评估哪类策略满足企业的数据中心安全要求所需的步骤，并提供了应用这些策略的必要程序。

程序 1　评估安全策略要求

步骤 1： 通过回答以下问题来评估安全策略需求：

- 安全数据中心将提供哪些应用？
- 能否在协议级别描绘应用流量的特征？
- 如果安全策略干扰了应用，能否提供详细的应用行为描述，来加速故障排除？
- 网络对于网络可控部分与不可控部分之间的基准性能期望是什么？
- 您期望安全控件处理的最高吞吐率是多少，包括工作站备份或将数据传输至辅助数据复制站点等带宽密集型活动？

步骤 2： 针对每个数据中心VLAN，确定用于满足应用要求的安全策略。每个需要防火墙的VLAN都将需要部署一个许可性（黑名单）或限制性（白名单）安全策略。

程序 2　部署相应的安全策略

网络安全策略的配置完全取决于企业组织的策略和管理要求。因此，此处的示例仅供您在进行安全策略配置时参考之用。

Option 1. 部署白名单安全策略

可应用基本的白名单数据服务策略，来支持各种常见的商务服务，如HTTP、HTTPS、DNS和其他Microsoft架构网络中常见的服务。

步骤 1： 控制访问确保只有特定的主机能够被访问。

```
object network BladeWeb1Secure
 host 10.4.54.100
 object network BladeWeb2Secure
 host 10.4.55.100
!
object-group network Application-Servers
 description HTTP, HTTPS, DNS, MSExchange
 network-object object BladeWeb1Secure
 network-object object BladeWeb2Secure
!
object-group service MS-App-Services
 service-object tcp destination eq domain
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq netbios-ssn
 service-object udp destination eq domain
 service-object udp destination eq nameserver
 service-object udp destination eq netbios-dgm
 service-object udp destination eq netbios-ns
!
 access-list global_access extended permit object-group MS-
App-Services any object-group Application-Servers
```

步骤 2： 指定特定用户（例如，IT管理人员或网络用户）可以使用的资源，以便于访问管理资源。在本例中，处于IP地址范围10.4.48.224-255中的管理主机被允许通过SSH和SNMP访问数据中心子网。

```
object network Secure-Subnets
 subnet 10.4.54.0 255.255.255.0
object network SecureIPS-Subnets
 subnet 10.4.55.0 255.255.255.0
!
object network Mgmt-host-range
range 10.4.48.224 10.4.48.254
object-group network DC_Secure_Subnet_List
```

```
network-object object Secure-Subnets
network-object object SecureIPS-Subnets
object-group service Mgmt-Traffic
service-object tcp destination eq ssh
service-object udp destination eq snmp
access-list global_access extended permit object-group Mgmt-
Traffic object Mgmt-host-range object-group DC_Secure_Subnet_
List
```

步骤 3: 如果您想允许针对防火墙策略故障排除访问应用程序，配置旁路规则。旁路规则允许对已添加到适当网络对象组中的主机进行广泛访问。必须谨慎地定义旁路规则，以避免对那些必须拦截的主机或服务进行开放式访问。在白名单策略中，旁路规则通常被禁用，只有在防火墙策略故障排除需要访问应用时才启用。

以下策略定义了两个主机，并将它们应用到了旁路规则。

```
object-group network Bypass-Rule
description Open Policy for Server Access
network-object object BladeWeb1Secure
network-object object BladeWeb2Secure
access-list global_access extended permit ip any object-group
Bypass-Rule
```

这会禁用旁路规则：

```
access-list global_access extended permit ip any object-group
Bypass-Rule  inactive
```

技术提示

旁路规则组有助于故障排除，或提供对于那些必须打开以支持维护或服务迁移的主机服务的临时访问。除非用于故障排除，否则它通常会被禁用。

步骤 4: 保存您的Cisco ASA防火墙配置。

```
copy running-config startup-config
```

Option 2. 部署黑名单安全策略

如果一家企业没有意愿或资源来维持细粒度的限制性策略，从而控制集中式数据和用户社区之间的访问，那么他们可以实施更简单且易于部署的安全策略来仅限制那些最高风险流量的传输。这种策略通常会配置为仅拦截特定服务的访问；所有其他流量将被允许。

步骤 1: 允许分配给IT人员的来自特定地址范围的SNMP查询和SSH请求。网络管理用户可能需要从台式机发出SNMP查询请求，以监控网络活动和连接至设备的SSH。

```
object network Secure-Subnets
subnet 10.4.54.0 255.255.255.0
object network SecureIPS-Subnets
 subnet 10.4.55.0 255.255.255.0
!
object network Mgmt-host-range
 range 10.4.48.224 10.4.48.254
object-group network DC_Secure_Subnet_List
 network-object object Secure-Subnets
 network-object object SecureIPS-Subnets
object-group service Mgmt-Traffic
 service-object tcp destination eq ssh
 service-object udp destination eq snmp
access-list global_access extended permit object-group Mgmt-
Traffic object Mgmt-host-range object-group DC_Secure_Subnet_
List
```

步骤 2: 拦截到所有其它主机的Telnet、SSH和SNMP。

```
access-list global_access extended deny object-group Mgmt-
Traffic any any
```

步骤 3: 配置一条规则，通过步骤 2中的黑名单，允许任何未被明确拒绝的应用流量在安全服务器子网通过服务器。请注意，此策略禁止了日志功能，以防止防火墙不得不记录所有对于服务器网络的访问。

```
access-list global_access extended permit ip any object-group
DC_Secure_Subnet_List log disable
```

步骤 4: 保存您的Cisco ASA防火墙配置。

```
copy running-config startup-config
```

流程

部署Cisco IPS

1、应用初始配置

2、完成基本配置

3、配置签名更新

从安全的角度来看，入侵检测系统(IDS)和入侵防御系统(IPS)是防火墙的补充，因为防火墙是通用访问控制设备，专门为阻止对应用或主机的访问而构建。通过这种方式，防火墙能拒绝对于大量应用端口的访问，从而减少服务器威胁。IDS和IPS传感器主要搜寻获得许可通过防火墙，但意图在网络和应用流量中的攻击。如果检测到攻击，IDS传感器会生成一个告警，通知企业有关此活动的情况。IPS的作用方式与IDS因为恶意活动而生成告警类似，另外，它可以采取措施在攻击抵达目的地之前将其拦截。

混杂模式对比内嵌模式

当使用IPS传感器时有两种主要部署模式：混杂（promiscuous）（IDS）或内嵌（inline）（IPS）。选择哪种部署模式取决于风险承受能力和容错能力等具体因素。

- 在混杂模式中（IDS），传感器仅检查数据包的副本，因此当它发现恶意数据包时也无法阻止它的传输。
- IDS传感器必须利用另一个内嵌执行设备来阻止恶意流量。这意味着，对于诸如单数据包攻击（例如，基于用户数据报协议[UDP]的slammer蠕虫）等活动，IDS传感器不能阻止攻击的发生。但在识别和清理受感染主机方面，IDS传感器具有巨大价值。
- 在内嵌IPS部署中，由于数据包流通过传感器发送并返回到Cisco ASA，因此传感器会检测实际数据包。
- IPS模式的优势是，如果传感器发现了恶意行为，它能够直接丢弃恶意数据包。这使得IPS设备具有较高的实际防御攻击的能力。

部署注意事项

如果您不想影响网络可用性或引发延迟问题，则使用IDS。如果您需要高于IDS所能提供的安全性以及恶意数据包丢弃能力时，则使用IPS。

安全的数据中心设计使用具有IPS的Cisco ASA 5585-X，为IPS实施一个策略，它将所有流量内嵌 (inline) 发送至IPS模块。

您的企业能够根据法规和应用需求，选择IPS或IDS部署。在初始部署时可以先从IDS或混杂设计入手，然后在了解了网络中的流量和性能状况，且您确信不会影响到生产流量后，再选择IPS。

程序 1　应用初始配置

使用传感器的CLI (命令行界面) 以设置基本网络信息，包括IP地址、网关地址和允许远程访问的访问列表。这些关键的数据被输入后，其余配置将通过使用嵌入式GUI控制台—IPS设备管理器(IDM)完成。与思科IBA智能业务平台设计中的Cisco ASA防火墙不同，IPS模块使用一条带外管理连接来进行配置和监控。传感器的管理端口与在本指南较早程序 4 “配置交换机访问端口”中配置的数据中心管理VLAN相连，使这个传感器能路由至或直接到达管理站。

步骤 1: 在Cisco ASA 5585-X防火墙的前面板上，通过IPS SSP模块上的串行控制台连接至IPS SSP控制台。

技术提示

您也可以通过在Cisco ASA SSP的CLI中使用**session 1**命令来访问IPS SSP上的控制台。

步骤 2: 登录到IPS设备。默认用户名和密码都是cisco。系统将会提示您更改 “cisco” 用户的登录密码。

步骤 3: 在IPS模块的CLI，启动System Configuration (系统配置) 对话。

```
sensor# setup
```

IPS模块进入交互式设置。

步骤 4: 定义IPS模块的主机名。请注意，不像Cisco IOS设备，即刻修改主机名CLI会显示新的主机名，IPS将在下次登录传感器时CLI才会提示显示新的主机名。

```
--- Basic Setup ---
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Current time: Mon Oct 12 23:31:38 2009
Setup Configuration last modified: Mon Oct 12 23:22:27 2009
Enter host name [sensor]: IPS-SSP20-A
```

步骤 5: 定义IPS模块外部管理端口的IP地址和网关地址。

```
Enter IP interface [192.168.1.62/24,192.168.1.250]:
10.4.63.21/24,10.4.63.1
```

步骤 6: 定义访问列表，然后按**Enter**键。该操作可控制对于IPS模块的管理访问。对于此网络，总部子网 (10.4.0.0/16) 中的所有地址将被允许。在空白许可提示符后按**Enter**键进入下一个步骤。

```
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.4.0.0/16
```

步骤 7: 针对之后三个问题接受默认回答 (no)。

```
Use DNS server for Global Correlation? [no]:
Use HTTP proxy server for Global Correlation? [no]:
Modify system clock settings?[no]:
```

请注意以下几点:

- 全局关联被禁用，直至配置流程的最后环节。
- 您将在IPS模块的GUI控制台中配置时间详细信息。

步骤 8: 针对该选项接受默认回答 (off)，加入SensorBase网络。

```
Participation in the SensorBase Network allows Cisco to
collect aggregated statistics about traffic sent to your IPS.
SensorBase Network Participation level? [off]:
```

IPS SSP显示您的配置和拥有四个选项的简要菜单。

步骤 9: 在System Configuration (系统配置) 对话框中, 保存您的配置, 然后通过输入**2**退出设置。

```
The following configuration was entered.
[removed for brevity]
exit
[0] Go to the command prompt without saving this
configuration.
[1] Return to setup without saving this configuration.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
Enter your selection [3]: 2
Warning: DNS or HTTP proxy is required for global correlation
inspection and reputation filtering, but no DNS or proxy
servers are defined.
--- Configuration Saved ---
Complete the advanced setup using CLI or IDM.
To use IDM, point your web browser at https://<sensor-ip-
address>.
```

步骤 10: 针对在其它Cisco ASA机箱中安装的IPS传感器, 重复本程序。在步骤 4中, 确保使用不同的主机名 (**IPS-SSP20-B**), 并且在步骤 5中, 确保在另一个传感器的管理接口上使用不同的IP地址 (**10.4.63.23**)。

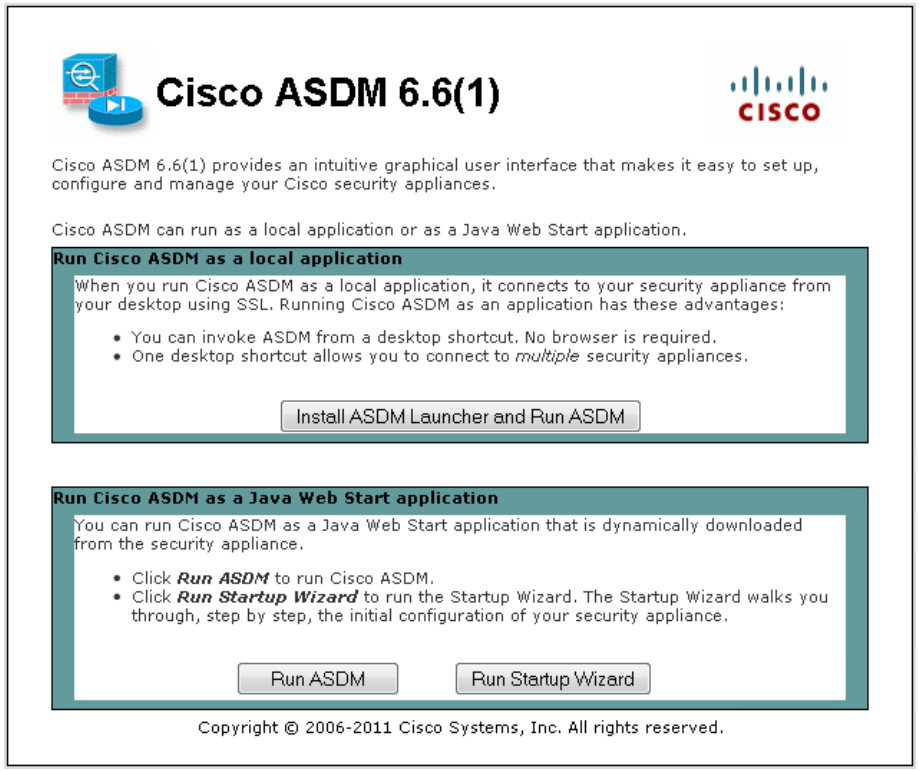
程序 2 完成基本配置

当System Configuration (系统配置) 对话框中的基本设置完成后, 您将使用集成管理工具Cisco ASDM的启动向导, 以便完成剩余任务, 进行基本设置:

- 配置时间设置
- 配置DNS和NTP服务器
- 定义基本的IDS配置
- 配置检测服务规则策略
- 向虚拟传感器分配接口

使用ASDM配置IPS模块, 允许您设置从防火墙到IPS模块的通讯路径, 同时配置IPS模块设置。

转至在“配置防火墙连接性”程序中的步骤 2设置过的防火墙外部接口, 连接传感器, 使用一个安全HTTP会话 (https://10.4.53.126)。接下来, 单击**Run ASDM (运行ASDM)** , 从Java Web Start (JWS) 应用程序运行ASDM; 另外, 您可以选择**Install ASDM Launcher and Run ASDM (安装ASDM启动器并运行ASDM)**, 以允许您连接至多个安全设备。

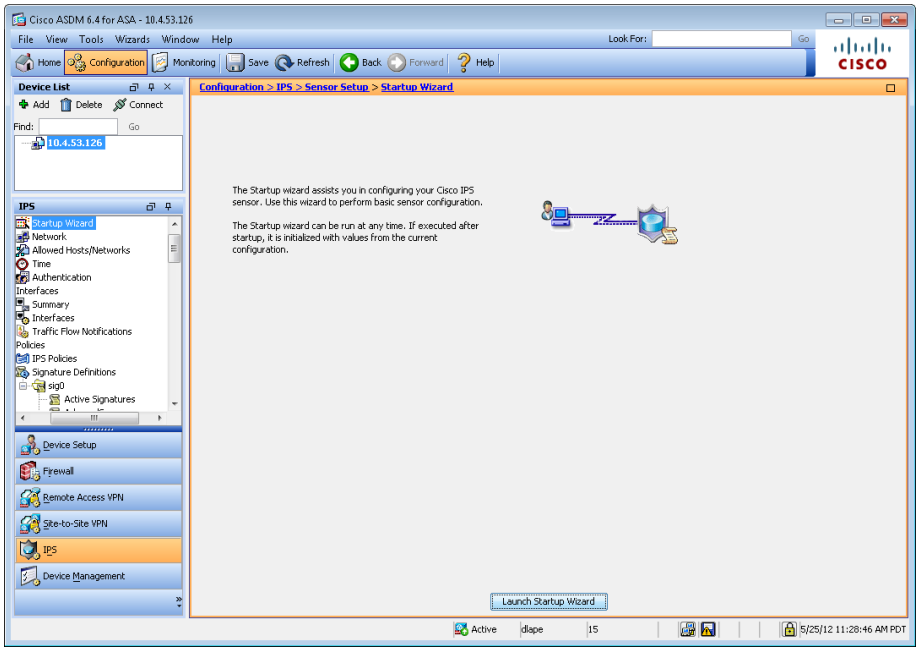


步骤 1: 输入为Cisco ASA 防火墙在流程“配置初始Cisco ASA设置”中的步骤 4配置的用户名和密码。

步骤 2: 在Cisco ASDM 中转至**Intrusion Prevention (入侵防御)** 选项卡, 输入针对**IPS-SSP20-A**访问需求的连接信息, 然后单击**Continue (继续)**。

ASDM将从IPS-SSP20-A 设备下载IPS信息。

步骤 3: 单击**Configuration (配置)**, 转至**IPS**选项卡, 然后单击**Launch Startup Wizard (运行启动向导)**。



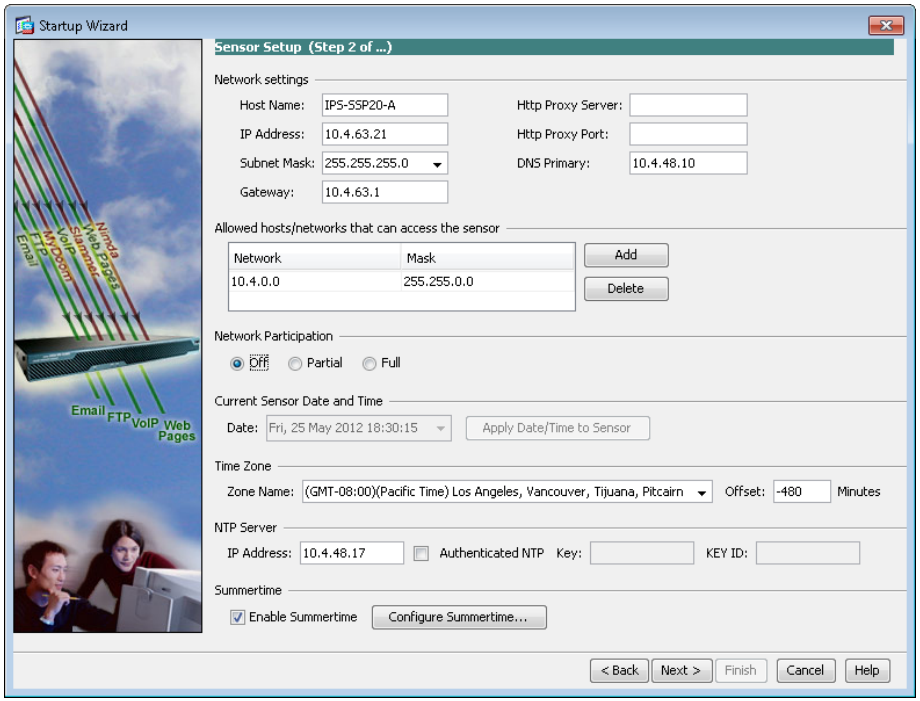
步骤 4: 查看Startup Wizard Introduction (启动向导介绍), 然后单击**Next (下一步)**。

步骤 5: 在Sensor Setup (传感器设置) 页面, 配置DNS服务器地址、时区和NTP服务器地址。

技术提示

如果您使用一款安全事件信息管理器产品来监视网络上的安全活动, 则NTP对于安全事件关联特别重要。

步骤 6: 如果您的时区需要，选择**Enable Summertime（启用夏令时）**。确保没有选择**AuthenticatedNTP（身份认证NTP）**，然后单击**Next（下一步）**。

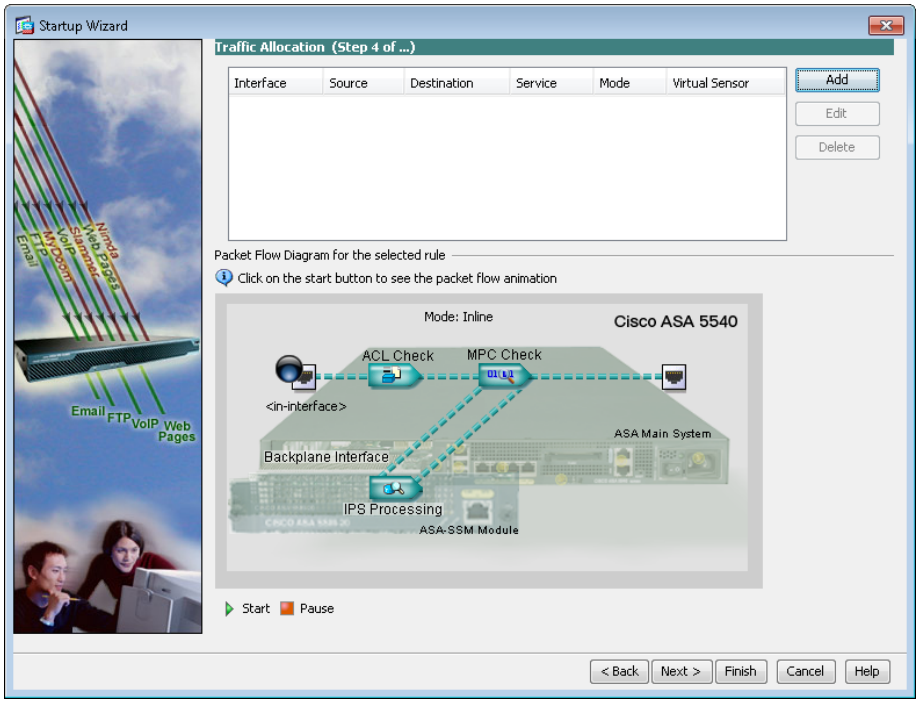


现在您必须决定传感器模式。在IPS模式中，传感器是内嵌在流量路径中的。在此模式中，传感器可以检查并丢弃恶意流量。在另一种IDS模式中，流量副本被动的被发送到传感器，并由传感器检查并发送关于恶意流量的报警。IPS模式对于来自互联网的威胁提供了更多的保护并且，当它使用了可信的技术，在网络上这个点降低了在阻塞重要流量的风险。您可以部署IDS模式作为一个临时的解决办法，看看在网络上IPS会有什么样的影响以及中止什么样的流量。在了解对您网络性能的影响并且执行任何必要的调整后，您可以轻松地更改传感器为IPS模式。

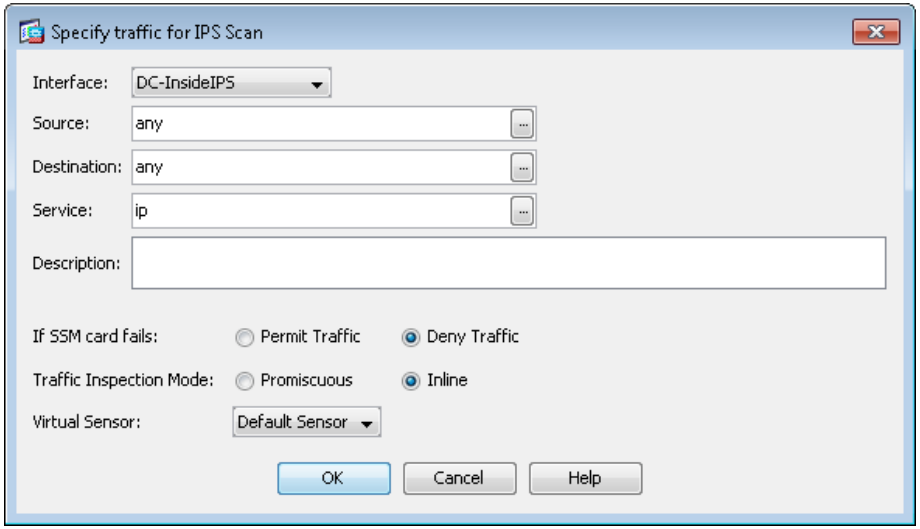
此程序分配IPS模式。

步骤 7: 在启动向导上：Virtual Sensors（虚拟传感器）页面，单击**Next（下一步）**。

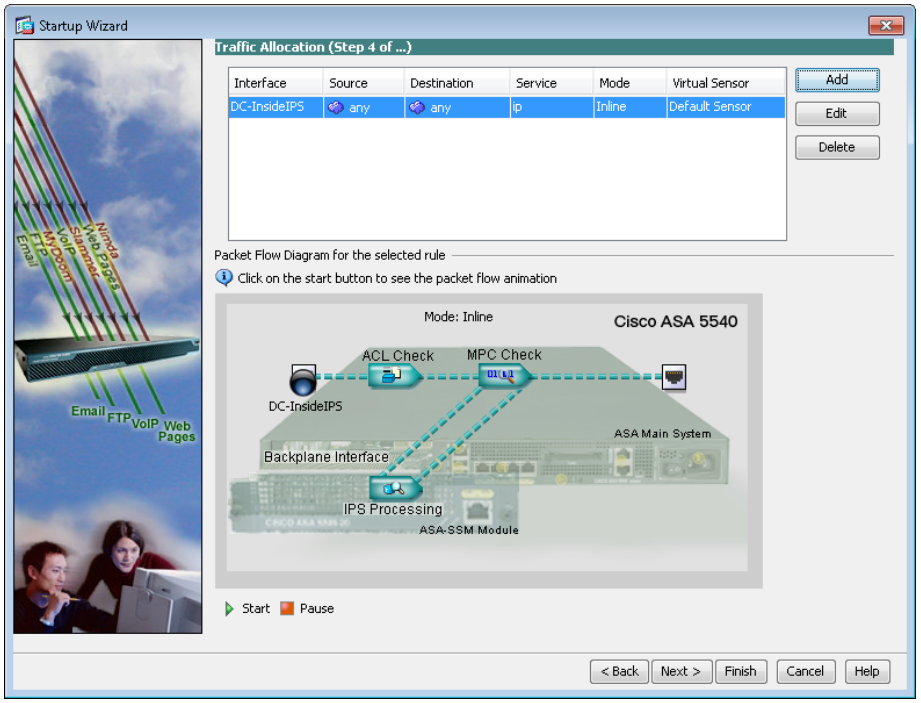
步骤 8: 在启动向导上：Traffic Allocation（流量分配）页面，单击**Add（添加）**。



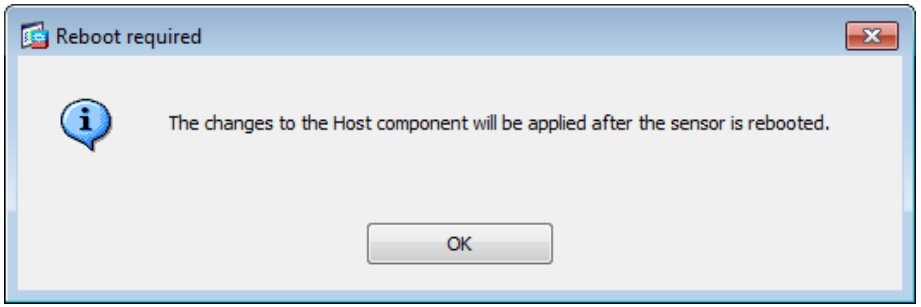
步骤 9: 在Specify traffic for IPS Scan (指定IPS扫描流量) 窗口中, 在Interface (接口) 列表, 选择**DC-InsideIPS**, 并且在Traffic Inspection Mode (流量检测模式) 旁边, 选择**Inline (内嵌)**, 然后单击**OK**。请注意, 如果Cisco ASA防火墙已经具有默认Traffic Allocation (流量分配) 策略, IDM将显示警告 "The Service Rule Policy you are trying to create already exists (您正在试图创建的服务规则策略已经存在)"。如果您收到该告警, 您可以取消该窗口并继续下一步。



步骤 10: 在Traffic Allocation (流量分配) 页面, 在Packet Flow Diagram for the selected Rule (已选规则的数据包流量图) 面板中, 通过单击**Start (开始)** 验证流量分配配置。动画将演示数据包被复制到IPS模块和出口接口。此动画显示的平台可能并非您正在配置的平台。



步骤 11: 在Startup Wizard (启动向导) 页面, 单击**Finish (完成)**, 然后当提示您是否将更改应用至传感器时单击**Yes (是)**。

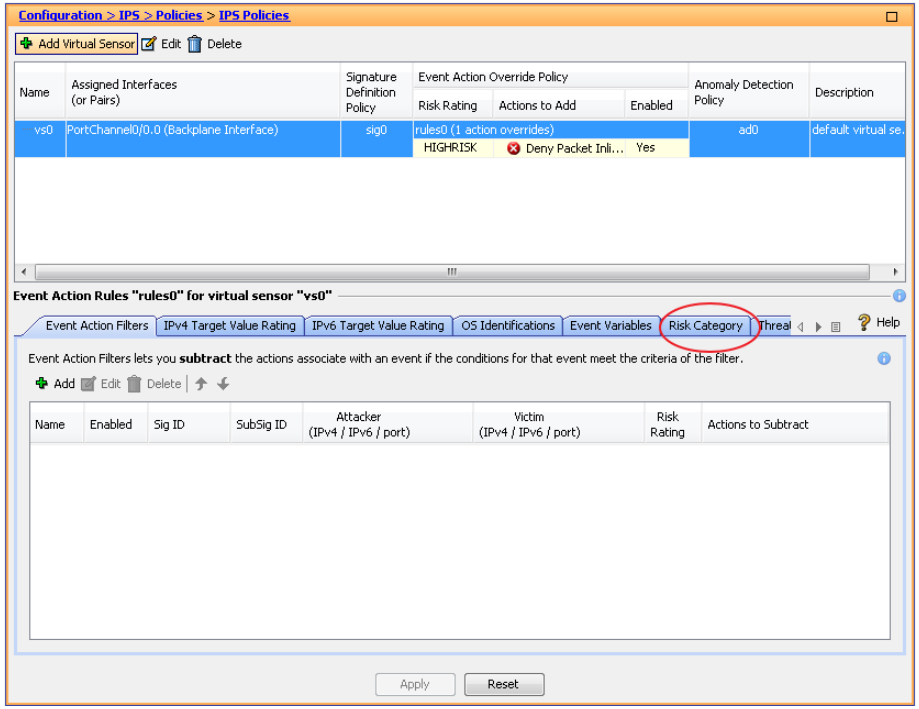


系统提示您IPS传感器需要重启以应用新配置。单击**OK**, 进入到下一步骤, 直到结束本程序再重启。

步骤 12: 转至**Policies (策略) > IPS Policies (IPS策略)**。

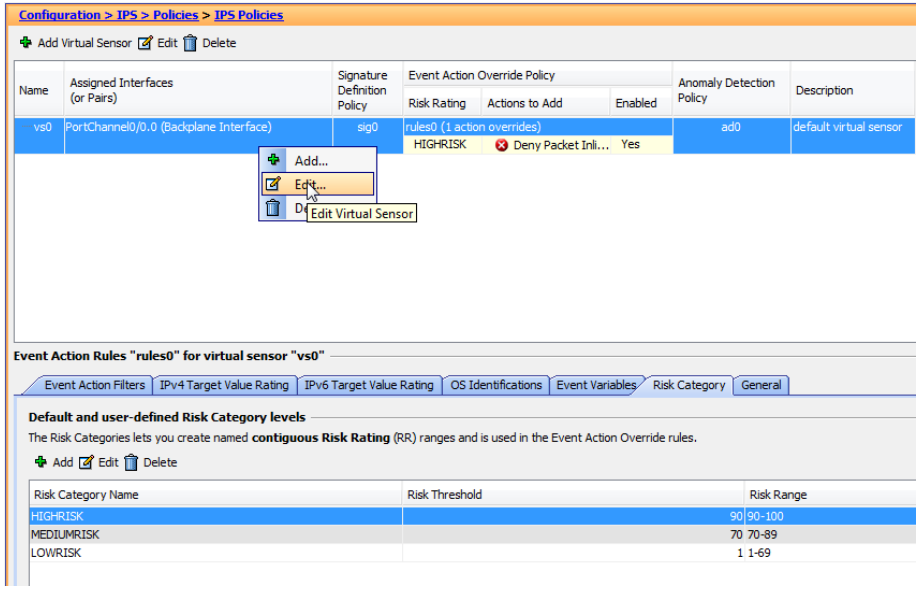
在主面板中, 请注意有Event Action Override (事件操作覆盖), 以便为所有High Risk (高风险) 事件Deny Packet Inline (拒绝数据包内嵌)。

步骤 13: 如果您想要查看高风险意味着什么的相关信息, 在主面板中, 单击**Risk Category (风险类别)**。



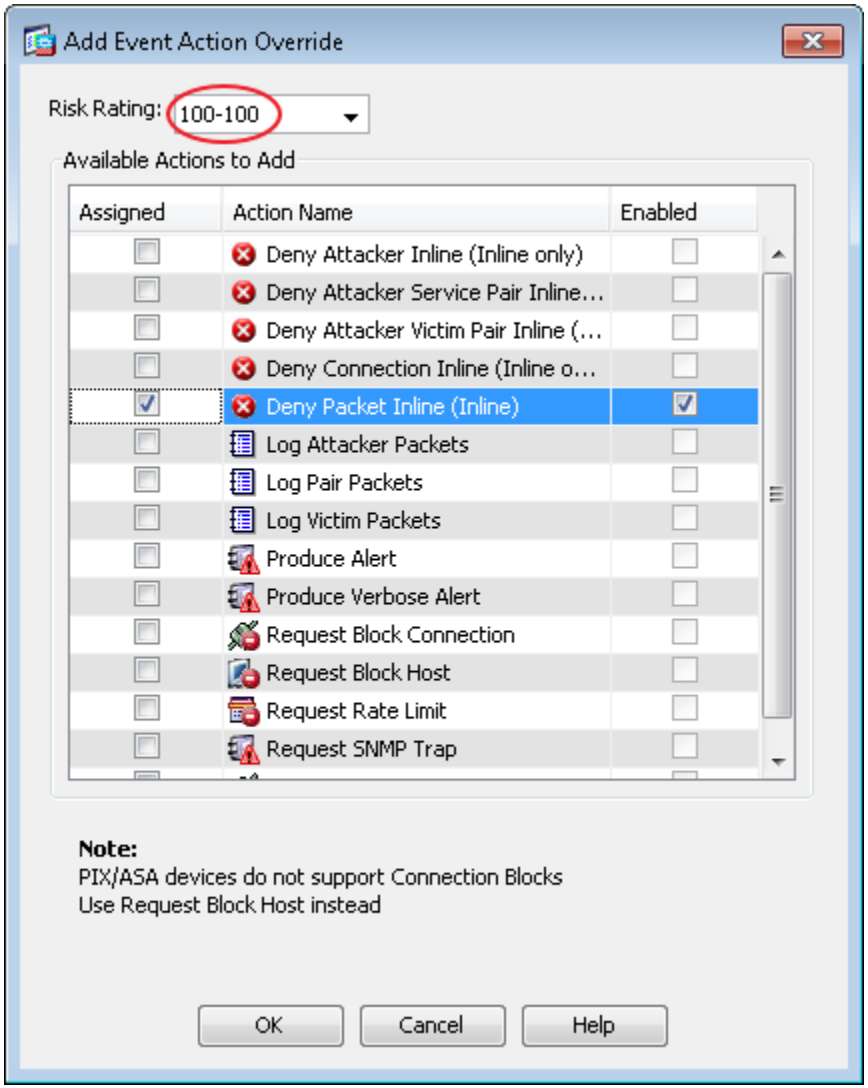
在默认情况下, High Risk表示事件的风险等级从90至100。在本部署中, 通过编辑Deny Packet (拒绝数据包) 操作您降低丢弃非恶意流量的风险, 使其仅在Risk Rating (风险等级) 为100时触发。这意味着传感器现在将仅对Risk Rating (风险等级) 等于100的事件使用Deny Packet (拒绝数据包) 操作, 即只有当最精确、风险最高的签名防御时才会出现。

步骤 14: 在Virtual Sensor (虚拟传感器) 面板中, 右键单击**vs0**项, 然后单击**Edit (编辑)**。

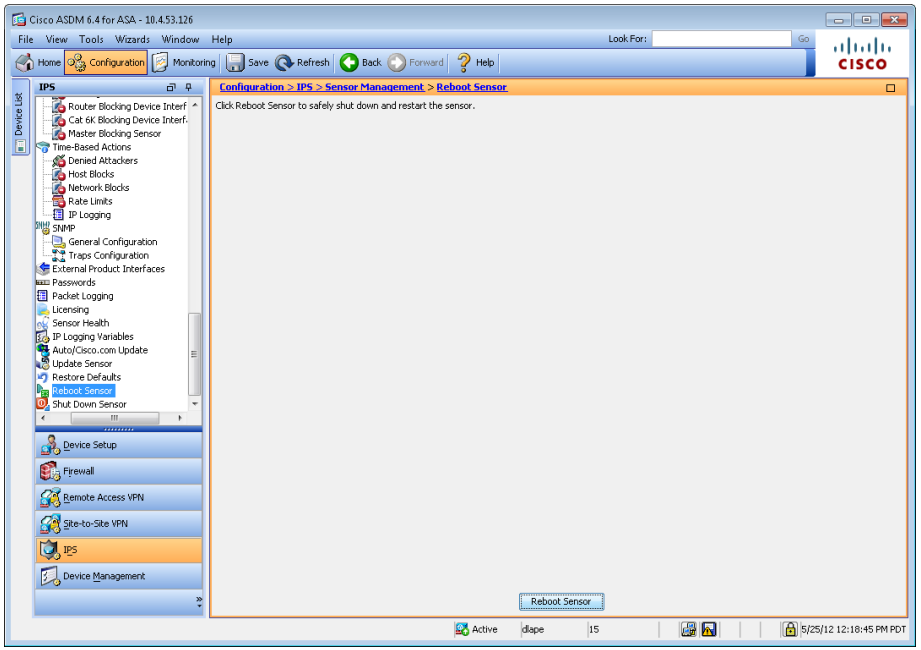


步骤 15: 在Event Action Rule (事件操作规则) 工作面板, 选择**Deny Packet Inline Override (拒绝数据包内嵌覆盖)**, 然后单击**Delete (删除)**。

步骤 16: 单击**Add (添加)**，在Risk Rating (风险等级) 下拉框中高亮并删除HIGHRISK (高风险) 值，再输入值**100-100**，选择**Deny Packet Inline (拒绝数据包内嵌)**，单击**OK**，然后单击**Apply (应用)**。



步骤 17: 转至**IPS > Reboot Sensor (重启传感器)**，单击**Reboot Sensor (重启传感器)**，然后再次单击**OK**。



GUI控制台将从IPS会话断开连接并要求您在Cisco ASA 防火墙再次登陆到ASDM会话。主用防火墙现在将转至备用状态，因为其在主应用中与IPS模块丢失连接。

步骤 18: 使用相同于您在本程序步骤 1中使用的IP地址和证书在防火墙登录ASDM会话。您现在登录至备用的活跃防火墙和IPS模块对。重复步骤 11至步骤 27，使用`IPS SSP20-B`模块名称和`10.4.63.23` IP地址，在其它Cisco ASA 机箱中安装IPS模块。

在这两个传感器之间没有配置同步。

读者提示

Cisco IME是一个独立应用，可以配置和监控最多10个传感器的活动（自IME 7.1.1起）。Cisco IME在Cisco.com上免费提供，网址与思科IPS软件更新和升级相同。

程序 3　配置签名更新

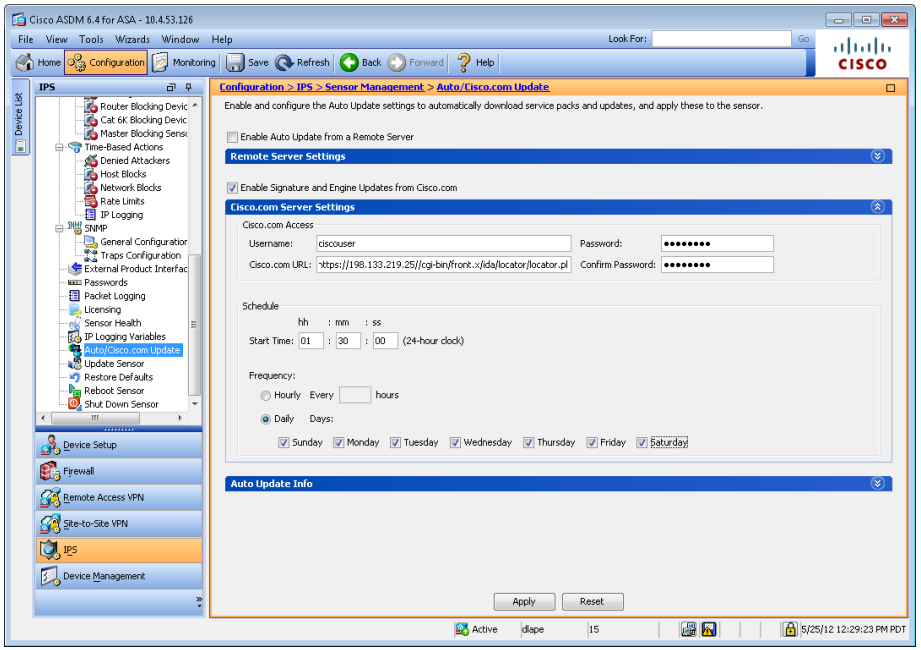
（可选）

IDS和IPS设备的表现通常取决于其获得的最新更新，所以确保传感器不断更新是十分重要的。为此，配置每个传感器的最简单的解决方案是直接从Cisco.com中检索签名更新。使用Cisco ASDM执行以下步骤。

步骤 1: 单击**Configuration（配置）**，单击**IPS**，转至**Configuration（配置）> IPS > Sensor Management（传感器管理）> Auto/Cisco.com Update（自动/Cisco.com更新）**，选择**Enable Signature and Engine Updates from Cisco.com（从Cisco.com中启用签名和引擎更新）**，然后展开**Cisco.com Server Settings（Cisco.com服务器设置）**面板。

步骤 2: 提供一个有权下载IPS软件更新的有效cisco.com用户名和密码。

步骤 3: 选择**Daily（每天）**，输入一个12:00 a.m.至4:00 a.m.之间的时间作为**Start Time（开始时间）**，然后选择每天，并单击**Apply（应用）**。



技术提示

使用Cisco.com的自动更新功能，将只更新传感器的引擎文件和签名文件。主要和次要代码版本以及服务包并不随之更新。

应用永续性

网络对于企业的成功日趋重要。企业资源规划、电子商务、电子邮件和门户等重要应用必须全天候可用，提供不间断的业务服务。但是，这些应用的可用性常常受到网络过载以及服务器和应用故障的威胁。此外，资源利用的不均衡导致低性能资源的请求过载，而高性能资源却闲置。应用性能和可用性直接影响着员工生产率和公司的盈利。随着越来越多的用户需要在更多的时间里使用关键企业应用，解决应用可用性和性能问题对于确保业务流程和目标的顺利实现日益重要。

以下几个因素使得应用很难通过网络进行高效部署和交付，包括：

- **应用基础设施不够灵活**——过去，应用基础设施设计一直是逐个应用进行的。这意味着用于某个特定应用的基础设施常常仅适用于该应用。此种设计将应用和基础设施紧紧地捆绑在一起，灵活性很低。由于应用和基础设施紧密捆绑，很难划分资源和控制级别，来满足不断变化的业务需求。
- **服务器可用性和负载**——应用的关键任务特性对于服务器可用性提出了较高要求。尽管服务器虚拟化技术有一定优势，但随着新应用的部署，物理服务器的数量仍在不断增加，从而导致电力和冷却要求也日益提高。
- **应用安全性和法规遵从**——网络安全所面临的许多新威胁都来自于会危及应用性能和可用性的应用及文档嵌入式攻击。此类攻击也可能会导致重要应用数据丢失，而网络和服务器不受影响。

提高应用性能和可用性的解决方法之一是完全重写应用，使之针对网络进行优化。但是，这要求应用开发人员对于不同应用如何响应带宽限制、延迟、抖动和其它网络状况的变化有深入了解。此外，开发人员还需准确预测最终用户的访问方法。显然这并非对于每个企业应用都可行，特别是那些花费了数年编写及定制的传统应用。

技术概述

提高应用性能的概念源自数据中心。互联网的繁荣带动了服务器负载均衡器（SLB）的发展。SLB对服务器组中的负载进行均衡，以提高响应客户端请求的能力，此外它们也已不断发展，承担了更多责任，如应用代理和完成第四层到第七层应用交换等。

思科应用控制引擎（Cisco ACE）是思科最新推出的SLB产品。 其主要作用是提供第四到七层交换，此外思科ACE还提供了一系列加速和服务器卸载功能，包括TCP处理卸载、SSL（安全套接层）处理卸载，和压缩。思科ACE设备部署在数据中心中，位于应用服务器的前面，通过多种服务来最大限度提高服务器和应用可用性、安全性，以及非对称（从服务器到客户端浏览器）应用加速。在此基础之上，思科ACE使IT部门能够更有力地控制应用和服务器基础设施，更轻松地管理和保护应用服务，同时提高性能。

Cisco ACE 提供了一下优势：

- **可扩展性**——思科ACE通过在组成服务器群的多个服务器间分发客户端请求，能够有效扩展如Web服务器等服务器程序的性能。随着流量的增多，它还支持在群中增加更多服务器。而服务器虚拟化技术的面世，则使应用服务器能够分阶段部署，根据容量需求的变化，灵活、动态地添加。
- **高可用性**——思科ACE能够自动检测出某个服务器的故障，并只需几秒即可在剩余的服务器中重新划分客户端流量，从而可提供出色可用性，确保用户能够获得持续服务。
- **应用加速**——思科ACE提高了应用性能，缩短了响应时间，无论是内部还是外部最终用户，它均能够最大限度地减少任意HTTP应用的延迟并压缩数据传输量。
- **服务器offload（减压）**——思科ACE从服务器上减轻了TCP处理、SSL处理和压缩的压力，从而无需增加服务器数量便能够服务更多用户和处理更多请求，将带宽需求缩减了90%。在Web应用服务器上运行SSL需要消耗大量服务器资源。通过offload SSL处理，这些资源可用于执行传统的Web应用功能。同时，由于内容交换机使用的持久性信息位于HTTP报头中，这一信息在SSL会话中传输时不再可见。通过在应用内容交换决策前端处理这些会话，前面讨论的所有持续性的选项都可用于安全站点。
- **灵活的授权许可**———思科ACE根据您购买的许可证种类提供多种性能选项，吞吐量从500 Mbps到4 Gbps。您可以为您的Cisco ACE设备购买一个1Gbps许可证，然后，根据您对性能需求的增长，用新的许可证在相同的硬件条件下升级至4Gbps。
- **健康监测**——思科ACE同时采用了主动和被动方法来监控服务器状态。通过定期探测服务器并监测从实际服务器返回的流量，Cisco ACE可以迅速检测服务器故障并将连接快速重路由到可用的服务器。ACE支持多种运行状况检查特性，包括验证Web服务器、SSL服务器、应用服务器、数据库、FTP服务器、和流媒体服务器。
- **有效的内容分配**——思科ACE还能够将对可缓存内容的请求，如图像文件，推送到能够提供比应用服务器更经济高效的服务缓存中去。

- 思科ACE能够将单一Web应用的组件划分到多个应用服务器集群中。例如：即使域名相同，www.mycompany.com/quotes/getquote.jsp和www.mycompany.com/trades/order.jsp这两个URL也能位于两个不同的服务器集群上。这一划分功能使应用开发人员不必修改大量代码，就能轻松地将应用扩展到多个服务器。同时，通过将针对相同页面的请求保留在同一服务器上，它还能够最大限度地改进服务器缓存的一致性。

目前有多种方法可将思科ACE集成到数据中心网络。从逻辑上来说，思科ACE设备部署在应用集群的前面。到该应用集群的请求被引导至设备上配置的一个虚拟IP地址(VIP)。思科ACE接收连接和HTTP请求，然后根据所配置的策略，将它们路由到相应的应用服务器。

从物理角度而言，网络拓扑结构可采取多种形式。单臂模式是最简单的部署方法，其中思科ACE与二层/三层基础设施的一端相连。它并不直接位于流量的传输路径当中，只接收专门以ACE为目的地的流量。需要传输到ACE的流量由精心设计的VLAN、虚拟服务器地址、服务器默认网关选择或二层/三层交换机上的策略路由控制。

部署详情

Cisco ACE 4710 硬件总是成对部署，一主一备以实现高可用性。如果主用Cisco ACE设备失效，则使用备用设备控制。根据如何配置冗余会话状态，failover可以不用干扰客户到服务器的连接。

每个Cisco ACE 都有一个port channel连接至交换机以扩展其性能。在此设计中，设备使用两条链路提供了2Gbps的可用吞吐量，但还留有额外两个千兆端口可用。通过使用四个端口，Cisco ACE 设备可以扩展至4Gbps。Cisco ACE运行在主备模式，在有设备失效时提供永续性。所有的链接从每台Cisco ACE设备仅连接至一个单一的交换机。这可以防止Cisco ACE 同时连接两个交换机，当一个交换机出现故障时回切断一半的可用带宽。

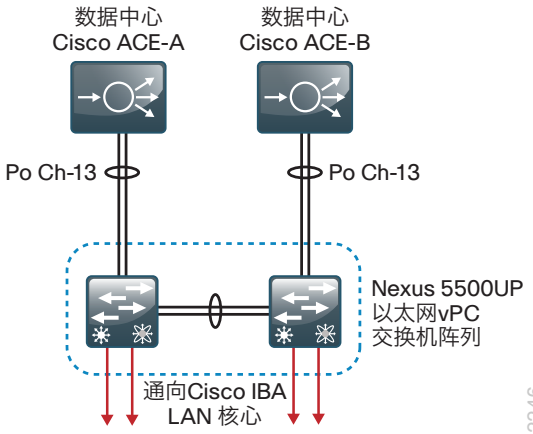
流程

配置到数据中心核心交换机的连接

1、在核心交换机上配置端口通道

程序 1　在核心交换机上配置端口通道

在数据中心服务于应用和服务器的每个思科ACE负载均衡器将通过EtherChannel链路连接至其中一个数据中心核心Cisco Nexus 5500UP交换机。



将EtherChannel链路用于与核心之间的连接性可提供永续的连接，链路流量负载均衡，并简化未来的带宽添加工作。

数据中心核心Cisco Nexus 5500UP交换机针对许多双宿主EtherChannel设备使用虚拟端口通道(vPC)。如果数据中心核心交换机之间的vPC对等链路故障，其中一个交换机将进入错误恢复模式，并切断与作为vPC连接一部分的VLAN关联的接口，以防止在基础设施中出现任何环路。因为思科ACE与每个数据中心核心交换机之间采用单宿主连接，并且未使用vPC进行连接，而是使用作为其它vPC连接一部分的VLAN，所以它们是非vPC端口也叫做vPC孤立端口。当数据中心核心交换机与进入错误恢复模式的交换机之间的vPC对等链路中断

时，在每个交换机上使用**vpc orphan-port suspend**命令关闭到相连思科ACE的EtherChannel接口。交换机上仍在使用中的活跃思科ACE将继续运行，并在设计中提供永续性。

思科ACE支持EtherChannel，但不支持链路汇聚控制协议（LACP）。因此，将强制进入**channel-group mode（通道组模式）**。

步骤 1： 在第一个Cisco Nexus 5500UP数据中心核心交换机上配置到port channel的物理接口。使用**speed 1000**命令从万兆以太网至千兆以太网的默认值中设置连接到思科ACE的端口。

技术提示

当配置接口时，**vpc orphan-port suspend**命令必须在**channel-group**命令之前输入。如果您首先在接口上输入**channel-group**命令，交换机将不会允许您在接口上输入**vpc orphan-port suspend**命令。

您必须给端口通道的所有物理接口成员输入**vpc orphan-port suspend**命令，以确保一致正确的操作。

```
interface Ethernet1/3
  description ACE 1 Gig 1/1
  speed 1000
  vpc orphan-port suspend
  channel-group 13 mode on
!
interface Ethernet1/4
  description ACE 1 Gig 1/2
  speed 1000
  vpc orphan-port suspend
  channel-group 13 mode on
```

当您分配channel group（通道组）到物理接口时，将创建一个逻辑EtherChannel（port-channel）接口。在下一步骤中，为两个数据中心核心交换机配置逻辑端口通道接口。捆绑物理接口的端口通道将继承这些设置。

步骤 2： 配置逻辑端口通道接口。为端口通道接口分配在程序 3 “配置QoS策略”中创建的QoS。

```
interface port-channel13
  switchport mode trunk
  switchport trunk allowed vlan 149,912
  spanning-tree port type edge trunk
service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

步骤 3： 为Cisco ACEfault-tolerant heartbeat VLAN（Cisco ACE容错心跳VLAN）配置一个未使用的VLAN。

```
vlan 912
name ACE-Heartbeat
```

步骤 4： 将以下配置应用至第2个Cisco Nexus 5500UP 数据中心核心交换机。

```
interface Ethernet1/3
  description ACE 2 Gig 1/1
  speed 1000
  vpc orphan-port suspend
  channel-group 13 mode on
!
interface Ethernet1/4
  description ACE 2 Gig 1/2
  speed 1000
  vpc orphan-port suspend
  channel-group 13 mode on
!
interface port-channel13
  switchport mode trunk
  switchport trunk allowed vlan 149,912
  spanning-tree port type edge trunkservice-policy type qos
input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS

!
vlan 912
name ACE-Heartbeat
```

流程

配置Cisco ACE网络

1、执行初始Cisco ACE设置

2、配置高可用性

程序 1　执行初始Cisco ACE设置

步骤 1: 通过控制台连接至思科ACE设备，执行初始配置，在出现提示时从初始配置对话框中退出。

```
switch login: admin
Password: admin
Admin user is allowed to log in only from console until the
default password is changed.
www user is allowed to log in only after the default password
is changed.
Enter the new password for user "admin": password
Confirm the new password for user "admin": password
admin user password successfully changed.
Enter the new password for user "www": password
Confirm the new password for user "www": password
www user password successfully changed.
<text wall removed>
ACE>Would you like to enter the basic configuration dialog
(yes/no) [y]: n
switch/Admin#
```

步骤 2: 在配置模式，设置系统主机名称。

```
hostname ACE4710-A
```

步骤 3: 设置基本网络安全策略。此操作允许对思科ACE进行管理访问。

```
access-list ALL line 8 extended permit ip any any
class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any
policy-map type management first-match remote_mgmt_allow_
policy
  class remote_access
    permit
```

步骤 4: 在千兆以太网接口上配置端口通道和中继。

```
interface gigabitEthernet 1/1
  channel-group 1
  no shutdown
interface gigabitEthernet 1/2
  channel-group 1
  no shutdown
interface port-channel 1
  switchport trunk native vlan 1
  switchport trunk allowed vlan 149
  no shutdown
```

该配置提供一个2-Gbps端口通道，足以支持具有高达2-Gbps许可证的Cisco ACE 4710。如果使用4-Gbps许可证，将包括总吞吐量达4Gbps的千兆以太网端口1/3和1/4。

步骤 5: 在思科ACE上配置VLAN 149接口用于管理访问和通用网络连接。

```
interface vlan 149
  ip address 10.4.49.119 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown
```

步骤 6: 配置默认路由器。

```
ip route 0.0.0.0 0.0.0.0 10.4.49.1
```

步骤 7: 配置NTP。

```
ntp server 10.4.48.17
```

步骤 8: 配置SNMP。

```
snmp-server community cisco ro
```

思科ACE设备现在应可以通过网络抵达。在第二个思科ACE上重复步骤 1至步骤 8，将步骤 5中的IP地址替换为**10.4.49.120**。

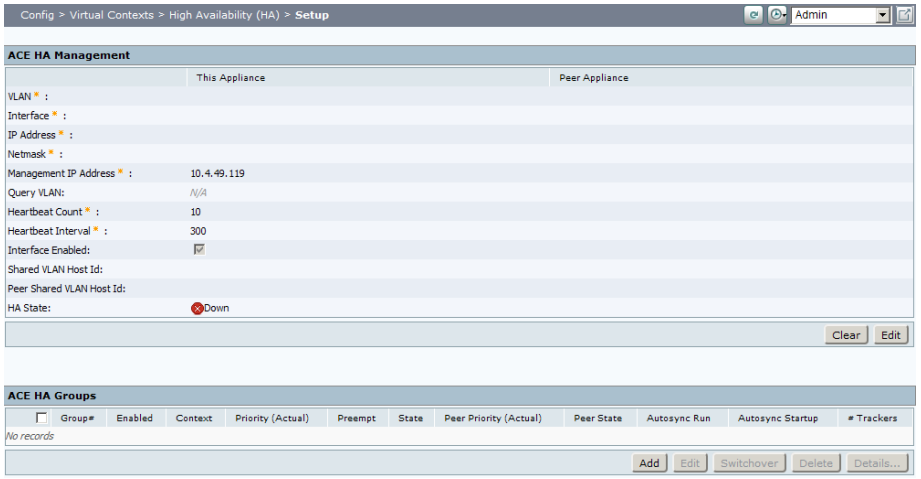
程序 2 配置高可用性

接下来，您要将思科ACE设备配置为主用—备用故障切换对。在您配置高可用性后，设备将进行同步，并且仅需在主用思科ACE设备上做进一步配置。从您希望作为主用设备的思科ACE设备开始。在本示例中，主用设备是10.4.49.119。

步骤 1: 打开浏览器窗口并在地址字段输入**https://10.4.49.119**。打开Cisco ACE GUI。

步骤 2: 在**Username (用户名)** 框内，输入**admin**，在**Password (密码)** 框内，输入您在程序 1，步骤 1中配置的密码，然后单击**Log In (登录)** 。

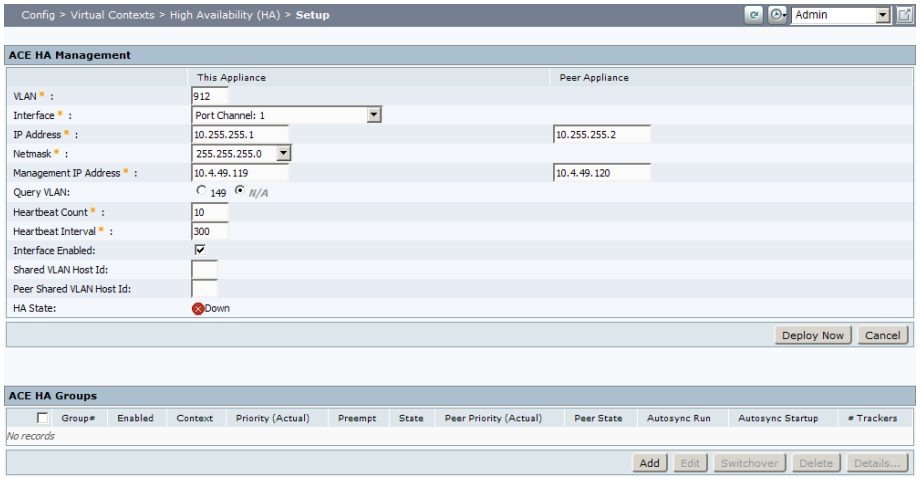
步骤 3: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > High Availability (HA) (高可用性(HA)) > Setup (设置)**，然后单击**Edit (编辑)**。



步骤 4: 在ACE HA Management (ACE HA管理) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

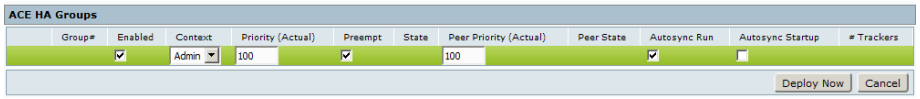
- VLAN—**912**
- Interface (接口) —**Port Channel 1**
- IP Address (IP地址) —**10.255.255.1**
- IP Address Peer Appliance (IP地址对等设备) —**10.255.255.2**
- Netmask (子网掩码) —**255.255.255.0**
- Management IP Address (管理IP地址) —**10.4.49.119**
- Management IP Address Peer Appliance (管理IP地址对等设

备）—**10.4.49.120**



步骤 5: 在ACE HA Groups (ACE HA组) 对话框中, 单击**Add (添加)**。

步骤 6: 将所有值保留为默认值, 然后单击**Deploy Now (立即部署)**。

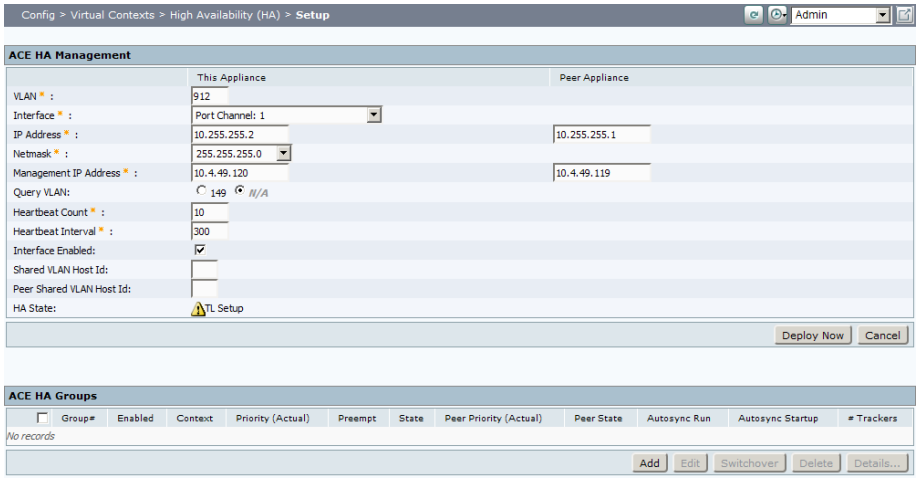


现在, 高可用性已在主用思科ACE设备上配置完成。对于备用设备的高可用性配置, 您必须登录至备用思科ACE设备。

步骤 7: 打开浏览器窗口并在地址字段输入**https://10.4.49.120**。打开Cisco ACE GUI。

步骤 8: 在**Username (用户名)** 框内, 输入**admin**, 在**Password (密码)** 框内, 输入您在程序 1, 步骤 1中配置的密码, 然后单击**Log In (登录)**。

步骤 9: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > High Availability (HA) (高可用性 (HA)) > Setup (设置)**, 然后单击**Edit (编辑)**。

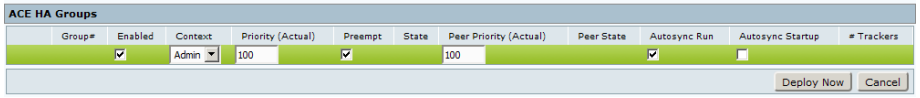


步骤 10: 在ACE HA Management (ACE HA管理) 对话框中, 输入以下值, 然后单击**Deploy Now (立即部署)**。

- VLAN—**912**
- Interface (接口) —**Port Channel 1**
- IP Address (IP地址) —**10.255.255.2**
- IP Address Peer Appliance (IP地址对等设备) —**10.255.255.1**
- Netmask (子网掩码) —**255.255.255.0**
- Management IP Address (管理IP地址) —**10.4.49.120**
- Management IP Address Peer Appliance (管理IP地址对等设备) —**10.4.49.119**

步骤 11: 在ACE HA Groups (ACE HA组) 对话框, 单击**Add (添加)**。

步骤 12: 将所有值保留为默认值, 然后单击**Deploy Now (立即部署)**。



两个思科ACE设备应保持通信, 并且应建立并激活高可用性。您刚刚完成配置的

设备应显示为“Standby Hot（热备份）”状态，其对等设备应为“Active（活动）”状态，如以下ACE HA Groups（ACE HA组）对话框中所示。

其他配置将在主用思科ACE设备10.4.49.119上进行，所有更改将自动复制到备用思科ACE设备10.4.49.120。

流程

为HTTP服务器设置负载均衡

1、配置运行状况探针

2、配置真实服务器

3、配置服务器群

4、配置Inband-Health（带内健康状况）检查

5、配置NAT池

6、配置虚拟服务器

程序 1　配置运行状况探针

运行状况探针将对服务器或应用进行轮询，以确保服务器或服务可用，并允许系统移除故障设备。针对本配置，您将构建互联网控制消息协议(ICMP)和HTTP探针。

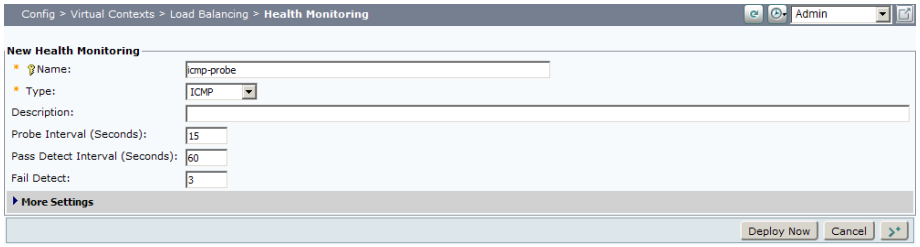
步骤 1： 打开浏览器窗口并在地址字段输入**`https://10.4.49.119`**。打开Cisco ACE GUI。

步骤 2： 在**Username（用户名）**框内，输入**`admin`**，在**Password（密码）**框内，输入您在程序 1，步骤 1中配置的密码，然后单击**Log In（登录）**。

步骤 3： 转至**Config（配置）> Virtual Contexts（虚拟上下文）> Load Balancing（负载均衡）> Health Monitoring（运行状况监控）**，然后单击**Add（添加）**。

步骤 4： 在New Health Monitoring（新运行状况监控）对话框中，在Name（名称）框中，输入**`icmp-probe`**，然后在Type（类型）列表中选择**ICMP**。

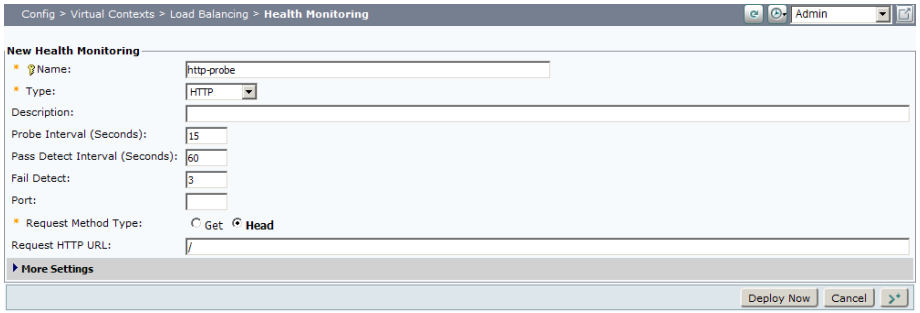
步骤 5: 单击**Deploy Now (立即部署)**。



步骤 6: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Health Monitoring (运行状况监控)**，然后单击**Add (添加)**。

步骤 7: 在New Health Monitoring (新运行状况监控) 对话框中，在**Name (名称)** 框中，输入**http-probe**，然后在Type (类型) 列表中，选择**HTTP**。

步骤 8: 单击**Deploy Now (立即部署)**。



步骤 9: 单击**Expect Status (预期状态)** 选项卡，然后单击**Add (添加)**。

步骤 10: 为最大和最小状态代码输入**200**，然后单击**Deploy Now (立即部署)**。

现在您已经创建ICMP和HTTP探针，您可以使用它们在负载均衡服务器群中监控真实和虚拟服务器。

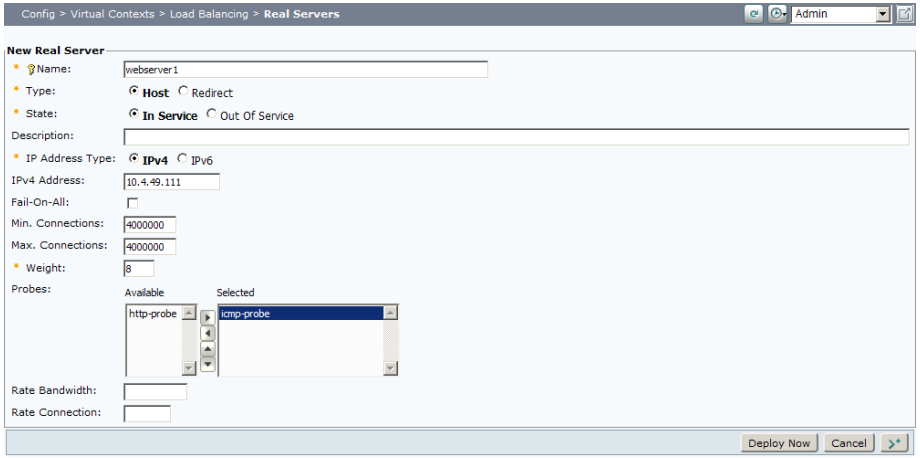
程序 2 配置真实服务器

在本程序中，您将添加真实服务器，在其中进行思科ACE负载均衡客户端连接。

步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Real Servers (真实服务器)**，然后单击**Add (添加)**。

步骤 2: 在New Real Server (新真实服务器) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

- Name (名称) —**webserver1**
- IP Address (IP地址) —**10.4.49.111**
- Probes (探针) —**icmp-probe**



步骤 3: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Real Servers (真实服务器)**，然后单击**Add (添加)**。

步骤 4: 在New Real Server (新真实服务器) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

- Name (名称) —**webserver2**
- IP Address (IP地址) —**10.4.49.112**

- Probes (探针) —**icmp-probe**

本示例使用ICMP探针监控在本例中配置的真实服务器，由此确保对服务器而不是特定服务进行监控。这是最灵活的配置，允许在单个物理或虚拟服务器上对多个服务进行负载均衡。

您现在已配置完成这两个web服务器。如果您计划使用其他服务器，您可以重复程序 2对其进行配置。

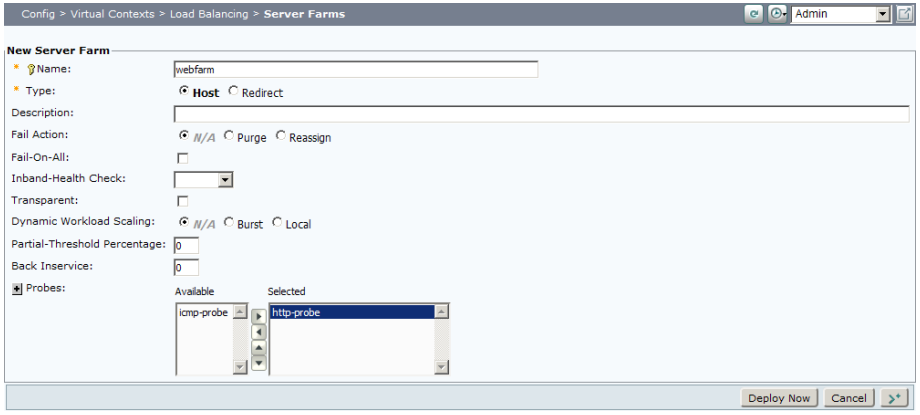
程序 3　配置服务器群

思科ACE上的服务器群是一个真实服务器池，您可以使用它连接至虚拟IP地址，客户端将使用该地址连接至HTTP服务。

步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Server Farms (服务器群)**，然后单击**Add (添加)**。

步骤 2: 在New Server Farm (新服务器群) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

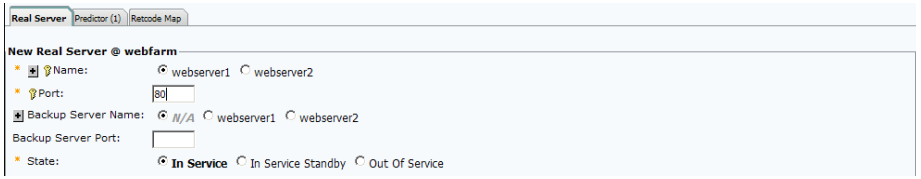
- Name (名称) —**webfarm**
- Probes (探针) —**http-probe**



步骤 3: 单击**Real Server (真实服务器)** 选项卡，然后单击**Add (添加)**。

步骤 4: 在New Real Server (新真实服务器) 对话框中，在Name (名称) 旁边，选择**webserver1**，然后在Port (端口) 框中，为HTTP输入**80**。

步骤 5: 单击**Deploy Now (立即部署)**。



步骤 6: 单击**Real Server (真实服务器)** 选项卡，然后单击**Add (添加)**。

步骤 7: 在New Real Server (新真实服务器) 对话框中，在Name (名称) 旁边，选择**webserver2**，然后在Port (端口) 框中，为HTTP输入**80**。

步骤 8: 单击**Deploy Now (立即部署)**。

步骤 9: 在Edit Server Farm (编辑服务器群) 对话框中，单击**Deploy Now (立即部署)**。

您刚刚已经创建了服务器群webfarm，真实服务器成员webserver1和webserver2用于端口80上的HTTP。http-probe将监控服务器群中的所有服务器，以确保HTTP服务可用。

程序 4　配置Inband-Health (带内健康状况) 检查

Cisco ACE的Inband-health (带内健康状况) 检查监控返回的流量并寻找实时的服务器到客户端的故障。当服务器有问题时，相比有源探针可以更快得到确认。当检测到故障时，可用以下模式：

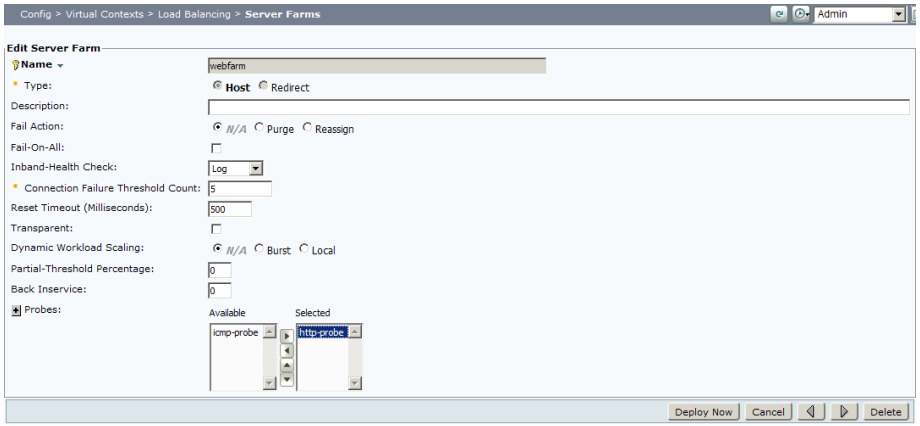
- **计数**——Cisco ACE 对故障进行本地记录，允许您从CLI查看服务器问题。
- **日志**——触发系统日志消息发送到网络管理系统 (NMS)，同时保持日志留在本地CiscoACE。
- **移除**——触发一个日志并使服务器停止服务。

在本程序中，使用Log (日志) 模式。这是因为少量错误在服务器上是常见的，在没有更多服务器群信息的情况下，使用Remove (移除) 模式显得门槛过低并会带来不必要的系统停用，或者门槛过高而不能使出现故障的服务器停止使用。Log (日志) 模式允许您查看错误并确认是哪个服务器存在问题。

步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Server Farms (服务器群)**，选择**webfarm**，然后单击**View/Edit (查看/编辑)**。

步骤 2: 在Edit Server Farm (编辑服务器群) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

- Inband-Health Check (带内健康状况检查) —**Log**
- Connection Failure Threshold Count (连接故障阈值计数) —**5**
- Reset Timeout (Milliseconds) (复位超时 (毫秒)) —**500**

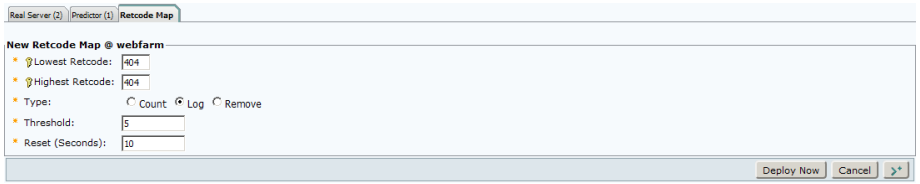


现在我们可以监控webfarm中服务器 的TCP错误。如果每500ms周期内出现五个错误，一个系统日志消息将被发送至NMS。如果在网络上没有系统日志服务器可用，我们可以设置带内健康状况检查模式为Count (计数) 模式，本地统计数据将被保存在Cisco ACE 并且可以从CLI调用。

步骤 3: 在Server Farm (服务器群) 对话框底部，单击**Retcode Map (Retcode地图)** 选项卡，然后单击**Add (添加)**。

步骤 4: 在New Retcode Map (新建Retcode地图) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

- Lowest Retcode (最低Retcode) —**404**
- Highest Retcode (最高Retcode) —**404**
- Type (类型) —**Log**
- Threshold (阈值) —**5**
- Reset (重置) —**10**



如果webfarm 中的一个服务器响应带HTTP的客户端，在10秒内返回5次代码404，一条系统日志消息将被发送至NMS。

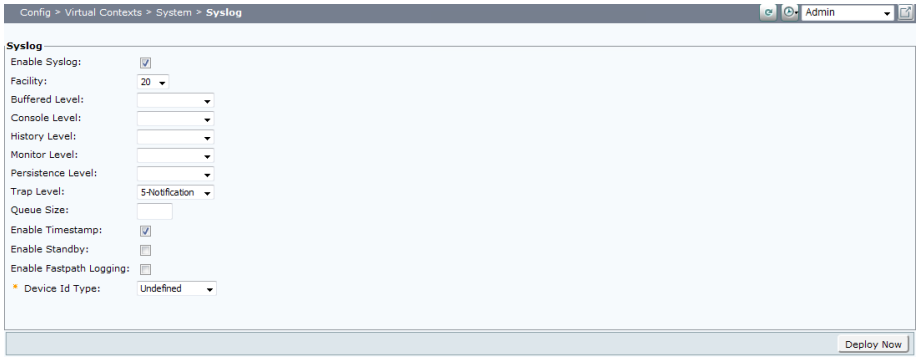
步骤 5: 在Server Farm (服务器群) 对话框的底部，单击**Retcode Map (Retcode地图)** 选项卡，然后单击**Add (新建)**。

步骤 6: 在Retcode Map (Retcode地图) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

- Lowest Retcode (最低Retcode) —**500**
- Highest Retcode (最高Retcode) —**505**
- Type (类型) —**Log**
- Threshold (阈值) —**5**
- Reset (重置) —**10**

如果在10秒周期内，webfarm 中的一台服务器响应一个带有HTTP的客户端5次，返回代码在500至505范围，一条系统日志将被发送至NMS。

步骤 7: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > System (系统) > Syslog (系统日志)**，并选择**Enable Syslog (开启系统日志)**。



步骤 8: 在Log Host (日志主机) 选项卡, 单击**Add (添加)**，输入**10.4.48.35**，然后单击**Deploy Now (立即部署)**。

步骤 9: 在Syslog (系统日志) 对话框中, 单击**Deploy Now (立即部署)**。

通过带内健康状况检查触发的系统日志消息现在会发送到系统日志服务器10.4.48.35上。

程序 5 配置NAT池

步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Network (网络) > NAT Pools (NAT池)**，然后单击**Add (添加)**。

步骤 2: 在New NAT Pool (新NAT池) 对话框中, 输入以下值, 然后单击**Deploy Now (立即部署)**。

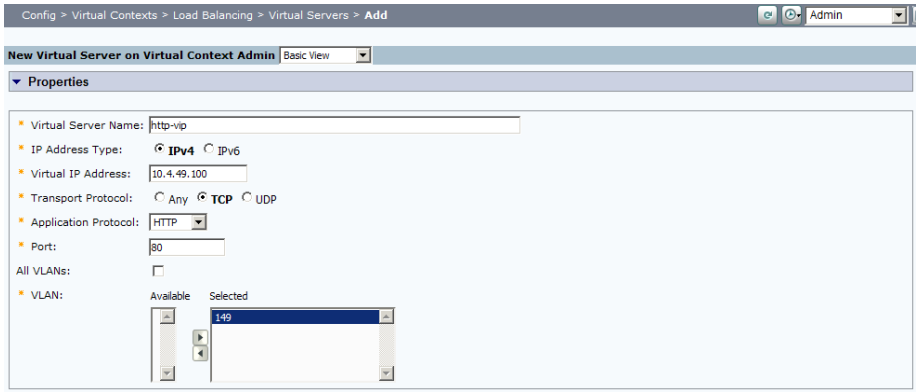
- Start IP Address (起始地址) —**10.4.49.99**
- End IP Address (结束地址) —**10.4.49.99**
- Netmask (子网掩码) —**255.255.255.0**

程序 6 配置虚拟服务器

步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Virtual Servers (虚拟服务器)**，然后单击**Add (添加)**。

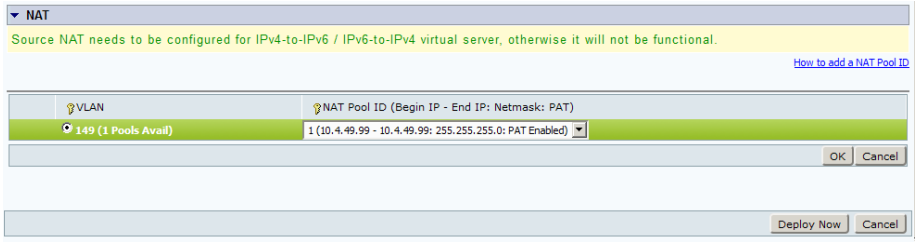
步骤 2: 在Properties (属性) 对话框中, 输入以下值:

- Virtual Server Name (虚拟服务器名称) —**http-vip**
- Virtual IP Address (虚拟IP地址) —**10.4.49.100**
- VLAN—**149**



步骤 3: 在Default L7 Load-Balancing Action (默认L7负载均衡操作) 对话框中, 在**Server Farm (服务器群)** 列表中, 选择**webfarm**, 然后选择**Deflate (收缩)** 。

步骤 4: 在NAT对话框中, 单击**Add (添加)** , 单击**OK**, 然后单击**Deploy Now (立即部署)** 。



指向端口80上的虚拟IP 10.4.49.100的客户端将在服务器群webfarm中的真实服务器webserver1和webserver2之间进行负载均衡。

流程

面向HTTPS服务器的负载均衡和SSL Offloading (减压)

1、配置真实服务器

2、配置服务器群

3、配置SSL代理服务

4、配置HTTP cookie粘连 (sticky) 服务

5、配置虚拟服务器

6、配置HTTP至HTTPS重定向

您可以配置一组服务器, 以便对执行所有SSL处理的思科ACE设备进行负载均衡, 从而将其从服务器中减压。

程序 1　配置真实服务器

在本程序中, 您将添加真实服务器, 在其中思科ACE设备将对客户端SSL连接进行负载均衡。

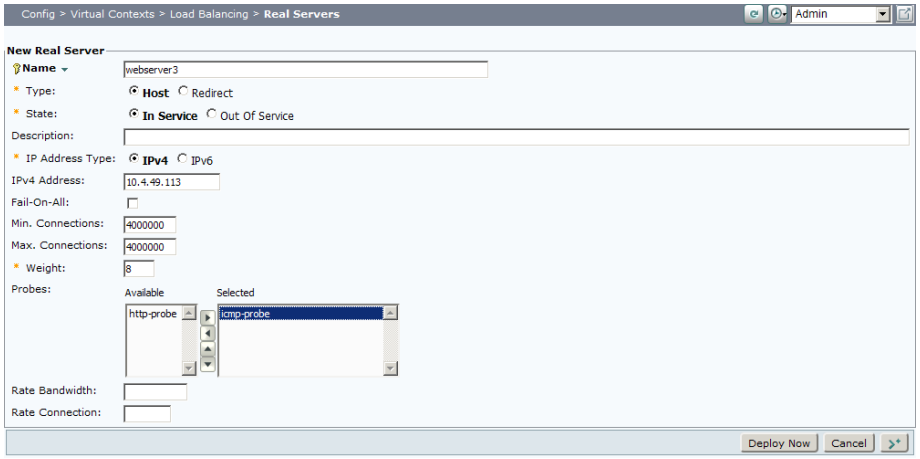
步骤 1: 打开浏览器窗口并在地址字段输入**`https://10.4.49.119`**。打开Cisco ACE GUI。

步骤 2: 在**Username (用户名)** 框内, 输入**`admin`**, 在**Password (密码)** 框内, 输入您在程序 1, 步骤 1中配置的密码, 然后单击**Log In (登录)** 。

步骤 3: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Real Servers (真实服务器)** , 然后单击**Add (添加)** 。

步骤 4: 在New Real Server (新真实服务器) 对话框中, 输入以下值, 然后单击**Deploy Now (立即部署)** 。

- Name (名称) —**webserver3**
- IP Address (IP地址) —**10.4.49.113**
- Probes (探针) —**icmp-probe**



步骤 5: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Real Servers (真实服务器)**，然后单击**Add (添加)**。

步骤 6: 在New Real Server (新真实服务器) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

- Name (名称) —**webserver4**
- IP Address (IP地址) —**10.4.49.114**
- Probes (探针) —**icmp-probe**

本示例中， ICMP探针监控真实服务器，由此确保对服务器而不是特定服务进行监控。这是最灵活的配置，允许在单个物理或虚拟服务器上对多个服务进行负载均衡。

您刚刚完成配置两个web服务器。如果您计划使用其他服务器，您可以重复程序1对其进行配置。

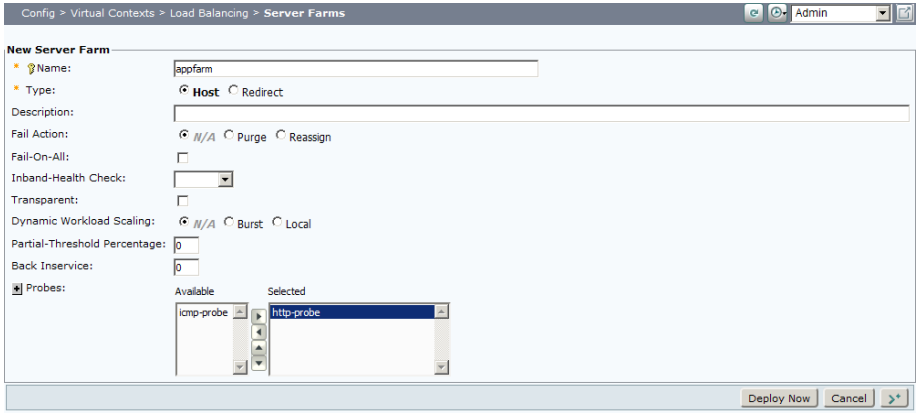
程序 2 配置服务器群

服务器群是一个真实服务器池，您可以使用它连接至vIP (虚拟IP) 地址，客户端将使用该地址连接至HTTP服务。

步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Server Farms (服务器群)**，然后单击**Add (添加)**。

步骤 2: 在New Server Farm (新服务器群) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

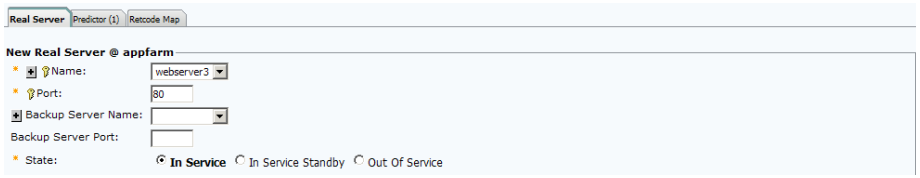
- Name (名称) —**appfarm**
- Probes (探针) —**http-probe**



步骤 3: 单击Real Server (真实服务器) 选项卡，单击**Add (添加)**。

步骤 4: 在New Real Server (新真实服务器) 对话框中，在**Name (名称)** 列表中，选择**webserver3**，然后在**Port (端口)** 框中，为HTTP输入**80**。

步骤 5: 单击**Deploy Now (立即部署)**。



步骤 6: 为新创建的serverfarm 单击**Deploy Now (立即部署)**。这将保存您的更改。

步骤 7: 在**Real Server (真实服务器)** 选项卡, 单击**Add (添加)**。

步骤 8: 在New Real Server (新真实服务器) 对话框中, 在**Name (名称)** 列表中, 选择**webserver4**, 然后在**Port (端口)** 框中输入**80**。

步骤 9: 单击**Deploy Now (立即部署)**。

步骤 10: 在Edit Server Farm (编辑服务器群) 对话框中, 单击**Deploy Now (立即部署)**。

您刚刚创建了服务器群appfarm, 真实服务器成员webserver3和webserver4用于端口80上的HTTP。思科ACE设备将执行所有SSL处理, 因此即便客户端将通过HTTPS访问这些服务器上的应用, 思科ACE与服务器之间的流量将通过端口80传输。http-probe将监控服务器群中的所有服务器, 以确保HTTP服务可用。

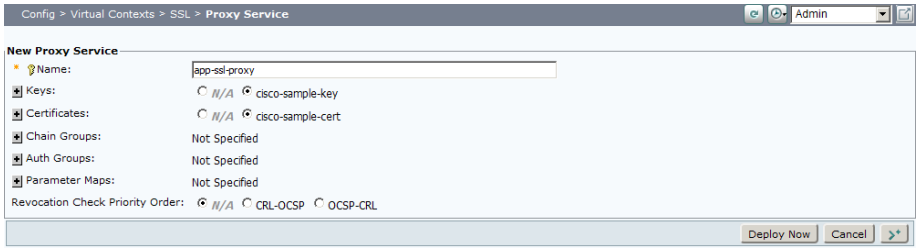
程序 3 配置SSL代理服务

为了使思科ACE卸载SSL处理, 您需要配置一个SSL代理服务。在本指南中, 我们使用思科样本密钥和证书。但是, 在产品部署中, 您将很可能从可信的证书颁发机构 (CA) 处购买证书。

步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > SSL> Proxy Service (代理服务)**, 然后单击**Add (添加)**。

步骤 2: 在New Proxy Service (新代理服务) 对话框中, 在**Name (名称)** 框中, 输入**app-ssl-proxy**。

步骤 3: 选择**cisco-sample-key**和**cisco-sample-cert**, 然后单击**Deploy Now (立即部署)**。



程序 4 配置HTTP cookie粘连 (sticky) 服务

HTTP cookie sticky服务可保持从客户端到单一真实服务器的流量。如果客户端连接在多个服务器之间进行均衡, 这对于状态可能丢失的应用非常有用。

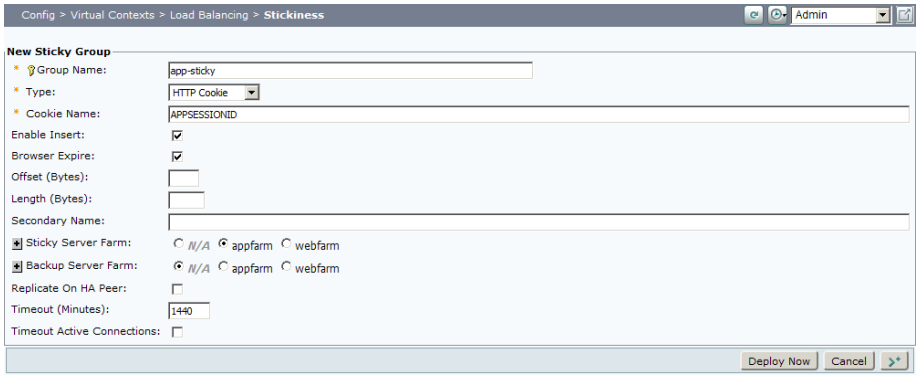
步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Stickiness (粘连)**, 然后单击**Add (添加)**。

步骤 2: 在New Sticky Group (新粘连组) 对话框中, 在**Group Name (组名称)** 框中, 输入**app-sticky**。

步骤 3: 在Type (类型) 列表中, 选择**HTTP Cookie**, 然后在**Cookie Name (Cookie名称)** 框中, 输入**APPSESSIONID**。

步骤 4: 选择**Enable Insert (启用插入)** 和**Browser Expire (浏览器过期)**。

步骤 5: 在Sticky Server Farm (粘连服务器群) 旁边, 选择**appfarm**, 然后单击**Deploy Now (立即部署)** 。

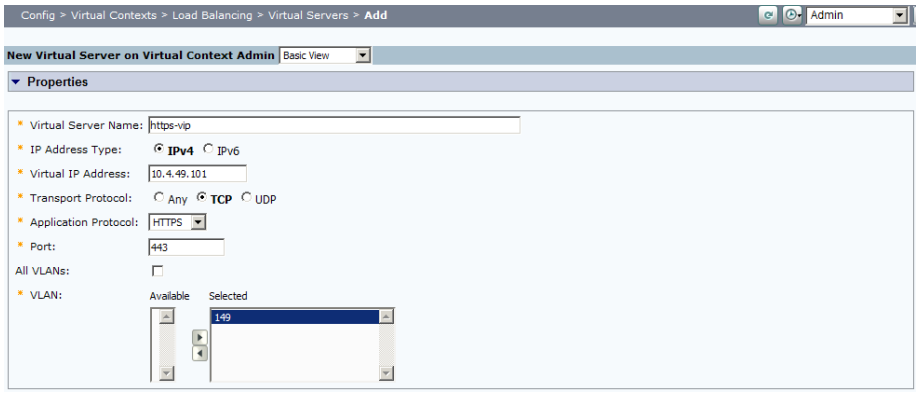


程序 5 配置虚拟服务器

步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Virtual Servers (虚拟服务器)** , 然后单击**Add (添加)** 。

步骤 2: 在Properties (属性) 对话框中, 输入以下值:

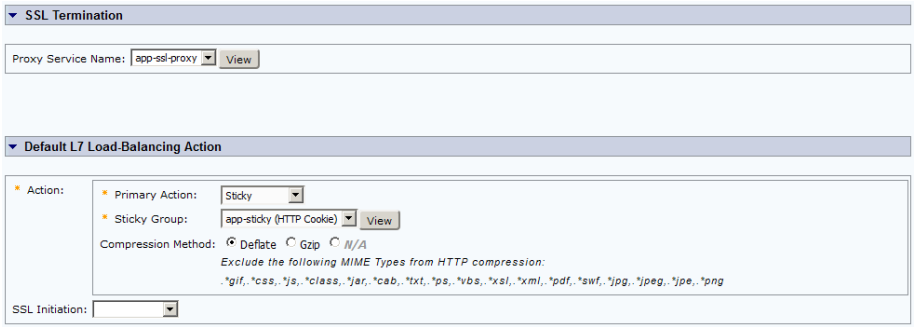
- Virtual Server Name (虚拟服务器名称) —**https-vip**
- Virtual IP Address (虚拟IP地址) —**10.4.49.101**
- Application Protocol (应用协议) —**HTTPS**
- VLAN—**149**



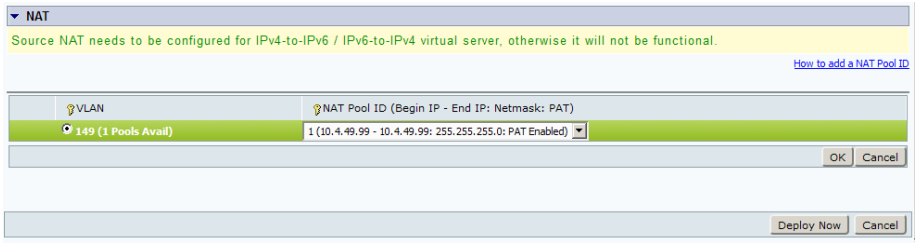
步骤 3: 在SSL Termination (SSL终止) 对话框中, 在**Proxy Service Name (代理服务名称)** 列表中, 选择**app-ssl-proxy**。

步骤 4: 在Default L7 Load-Balancing Action (默认L7负载均衡操作) 对话框中, 在Primary **Action (主操作)** 列表中, 选择**Sticky (粘连)** 。

步骤 5: 在**Sticky Group (粘连组)** 列表中, 选择**app-sticky (HTTP Cookie)** , 然后选择**Deflate (收缩)** 。



步骤 6: 在NAT对话框中, 单击**Add (添加)** , 单击**OK**, 然后单击**Deploy Now (立即部署)** 。



指向端口443上的虚拟IP 10.4.49.101的客户端将在服务器群appfarm中的真实服务器webserver3和webserver4之间进行负载均衡。思科ACE将终止SSL会话, 并在TCP端口80上通过标准HTTP对到真实服务器的连接进行负载均衡。

程序 6 配置HTTP至HTTPS重定向

(可选)

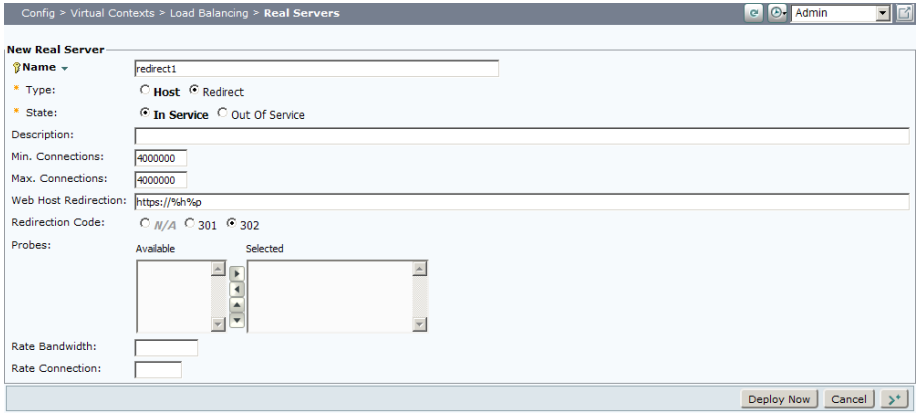
通常, 首选方式是使HTTP流量重定向至HTTPS, 以确保到该服务的连接已加

密。通过以下程序，您可以创建服务，以便将指向10.4.49.101的任意HTTP流量重定向至在上述HTTPS服务。

步骤 1: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Real Servers (真实服务器)**，然后单击**Add (添加)**。

步骤 2: 在New Real Server (新真实服务器) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

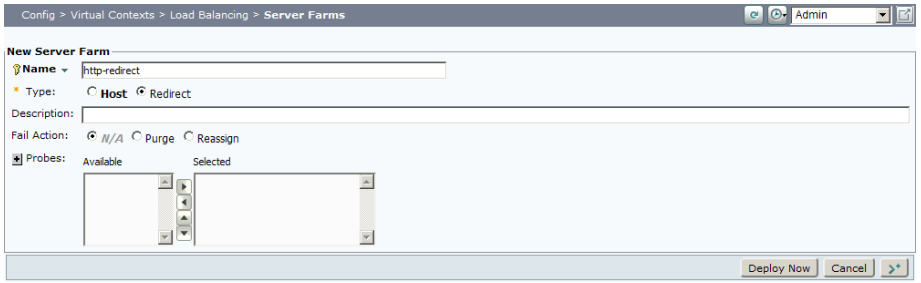
- Name (名称) —**redirect1**
- Type (类型) —**Redirect**
- Web Host Redirection (Web主机重定向) —**https://%h%p**
- Redirection Code (重定向代码) —**302**



步骤 3: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Server Farms (服务器群)**，然后单击**Add (添加)**。

步骤 4: 在New Server Farm (新服务器群) 对话框中，输入以下值，然后单击**Deploy Now (立即部署)**。

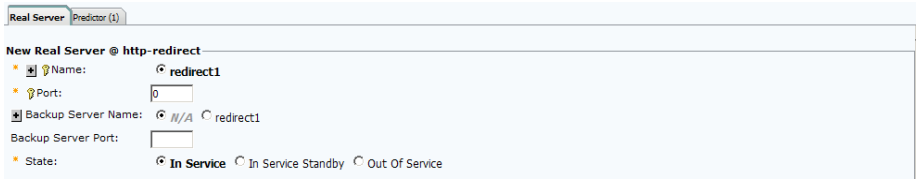
- Name (名称) —**http-redirect**
- Type (类型) —**Redirect**



步骤 5: 单击**Real Server (真实服务器)** 选项卡，然后单击**Add (添加)**。

步骤 6: 在New Real Server (新真实服务器) 对话框中，选择**redirect1**，然后单击**Deploy Now (立即部署)**。

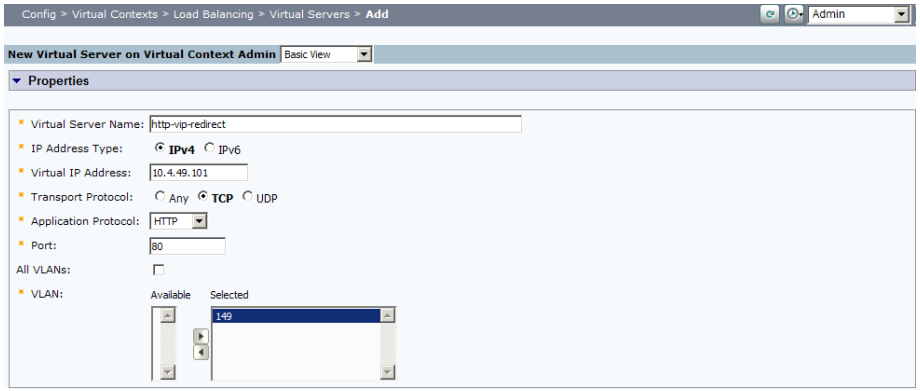
步骤 7: 在Edit Server Farm (编辑服务器群) 对话框中，单击**Deploy Now (立即部署)**。



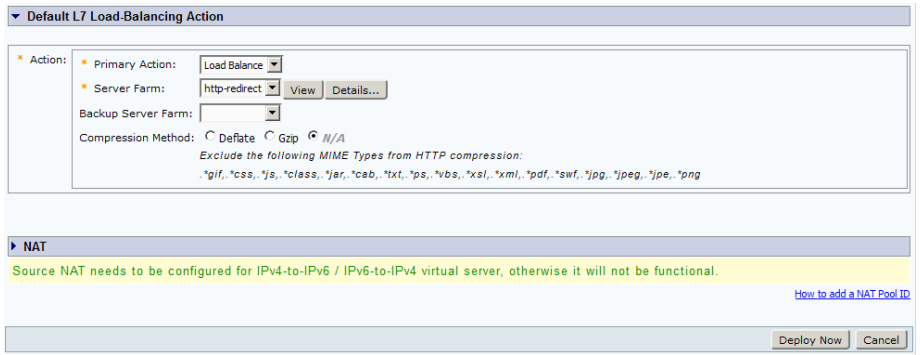
步骤 8: 转至**Config (配置) > Virtual Contexts (虚拟上下文) > Load Balancing (负载均衡) > Virtual Servers (虚拟服务器)**，然后**单击Add (添加)**。

步骤 9: 在Properties (属性) 对话框中，输入以下值：

- Virtual Server Name (虚拟服务器名称) —**http-vip-redirect**
- Virtual IP Address (虚拟IP地址) —**10.4.49.101**



步骤 10: 在Default L7 Load-Balancing Action (默认L7负载均衡操作) 对话框中, 在**Server Farm (服务器群)** 列表中, 选择**http-redirect**, 然后单击**Deploy Now (立即部署)**。



备注

附录A: 产品列表

数据中心核心

功能领域	产品描述	产品编号	软件版本
核心交换机	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.1(3) N1(1a)
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	Layer 3 License
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
以太网扩展	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

数据中心服务

功能领域	产品描述	产品编号	软件版本
应用永续性	Cisco ACE 4710 Application Control Engine 2Gbps	ACE-4710-02-K9	A5(1.2)
	Cisco ACE 4710 Application Control Engine 1Gbps	ACE-4710-01-K9	
	Cisco ACE 4710 Application Control Engine 1Gbps 2-Pack	ACE-4710-2PAK	
	Cisco ACE 4710 Application Control Engine 500 Mbps	ACE-4710-0.5-K9	
防火墙	Cisco ASA 5585-X Security Plus IPS Edition SSP-40 and IPS SSP-40 bundle	ASA5585-S40P40-K9	ASA 8.4.3, IPS 7.1(4) E4
	Cisco ASA 5585-X Security Plus IPS Edition SSP-20 and IPS SSP-20 bundle	ASA5585-S20P20X-K9	
	Cisco ASA 5585-X Security Plus IPS Edition SSP-10 and IPS SSP-10 bundle	ASA5585-S10P10XK9	

存储网络扩展

功能领域	产品描述	产品编号	软件版本
FC交换机	Cisco MDS 9148 Multilayer Fibre Channel Switch	DS-C9148D-8G16P-K9	NX-OS 5.0(7)
	Cisco MDS 9124 Multilayer Fibre Channel Switch	DS-C9124-K9	

计算资源

功能领域	产品描述	产品编号	软件版本
UCS 阵列互联	Cisco UCS up to 48-port Fabric Interconnect	UCS-FI-6248UP	2.0(2q)
	Cisco UCS 20-port Fabric Interconnect	N10-S6100	Cisco UCS Release
	Cisco UCS 6100 6-port Fibre Channel Expansion Module	N10-E0060	
UCS B系列刀片式服务器	Cisco UCS Blade Server Chassis	N20-C6508	2.0(2q)
	Cisco UCS 8-port 10GbE Fabric Extender	UCS-IOM2208XP	Cisco UCS Release
	Cisco UCS 4-port 10GbE Fabric Extender	UCS-IOM2204XP	
	Cisco UCS 4-port 10GbE First Generation Fabric Extender	N20-I6584	
	Cisco UCS B200 M2 Blade Server	N20-B6625-1	
	Cisco UCS B250 M2 Blade Server	N20-B6625-2	
	Cisco UCS M81KR Virtual Interface Card	N20-AC0002	
UCS C系列机架式服务器	Cisco UCS C200 M2 Rack Mount Server	R200-1120402W	1.4.1e
	Cisco UCS C210 M2 Rack Mount Server	R210-2121605W	Cisco UCS CIMC Release
	Cisco UCS C250 M2 Rack Mount Server	R250-2480805W	

附录B: 变更

本附录总结了相比先前的思科IBA智能业务平台系列，本指南所做的变更。

- 我们更新了“以太网基础设施”章节，关于QoS保护多媒体，控制，和存储传输流量的程序。更新还包括为Cisco Nexus FEX连接使用增强vPC的部署指导。
- Computing Resources （计算资源）模块现在叫做“计算机连接性”，并且更新了将服务器连接到数据中心网络的各种方法。
- “应用程序永续性”章节现在包括带内健康状况检查程序，以创建更强大的服务器状态检查，能够更快地检测到故障。

备注

反馈

点击 这里 提供反馈到IBA

美国总部
Cisco Systems, Inc.
San Jose, CA

亚太总部
Cisco Systems (USA) Pte. Ltd.
Singapore

欧洲总部
Cisco Systems International BV Amsterdam,
The Netherlands

思科在全球拥有超过200家办公室。地址，电话号码和传真在思科网站中列出： www.cisco.com/go/offices。