数据中心部署指南

智能业务平台

修订版：2012年上半年

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人员：

- 需要实施解决方案时的标准规范的系统工程师
- 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 指南作为工程师之间技术交流、项目实施经验分享的统一指导文件，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。

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“2011 年 8 月系列”。

您可以在以下网址查看最新的IBA指南系列：
客户访问：http://www.cisco.com/go/cn/iba
合作伙伴访问：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

如需要了解更多有关思科 IBA 智能业务平台的信息，请访问
http://www.cisco.com/go/cn/iba

如需要注册快速报价工具（QPT），请访问
http://www.cisco.com/go/qpt

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

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，确保能够实现无缝协作。IBA 采用的组件式方法简化了在采用多种技术时通常需要进行的系统集成工作，使您可以随意选择能够满足企业需求的解决方案，而不必担心技术复杂性方面的问题。

了解更多信息，请参阅《思科 IBA 使用入门》文档：
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

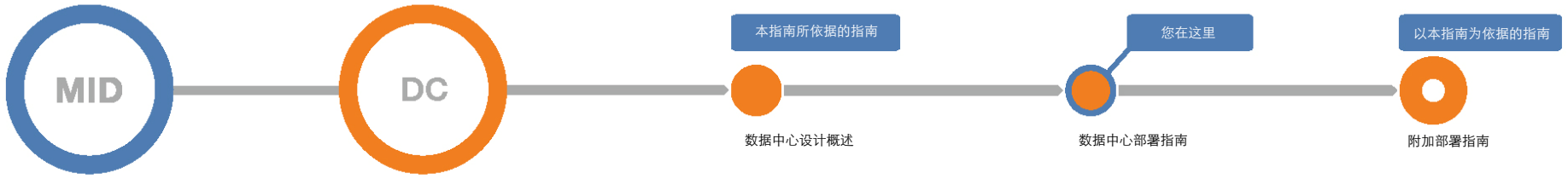
关于本指南

本**基础部署指南**包含多个章节，每个章节又分为以下几个部分：

- **业务概述**——您的企业所面临的挑战。业务决策者可通过本部分内容来了解介绍的解决方案与其企业运营的相关性。
- **技术概述**——思科如何应对上述挑战。技术决策者可以利用此部分内容来了解解决方案的工作原理。
- **部署详情**——解决方案的具体实施步骤介绍。系统工程师可以在这些步骤的指导下快速可靠地配置和启用解决方案。

如欲了解本指南在之前系列指南的基础上所做的变更，请参见附录 B：变更。

本指南假定您已经阅读了本指南所依据的基础设计概述，如以下成功部署路线图中所示。



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——即上面路线图中本指南左侧的所有指南。所有以本指南为依据的指南都在右侧。

如需要了解更多有关思科 IBA 智能业务平台的信息，请访问：http://www.cisco.com/go/cn/iba

如需要注册快速报价工具（QPT），请访问：http://www.cisco.com/go/qpt

简介

面向中小企业数据中心基础的思科 IBA 智能业务平台是一个全面的网络设计，最多能够支持 2500 名用户。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。面向中小企业数据中心的架构以《面向中小企业的思科 IBA 智能业务平台——无边界网络基础部署指南》中所述的服务器空间部署为基础。

面向中小企业数据中心基础的思科 IBA 智能业务平台结合采用了以太网、存储网、计算、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

本指南包括以下模块：

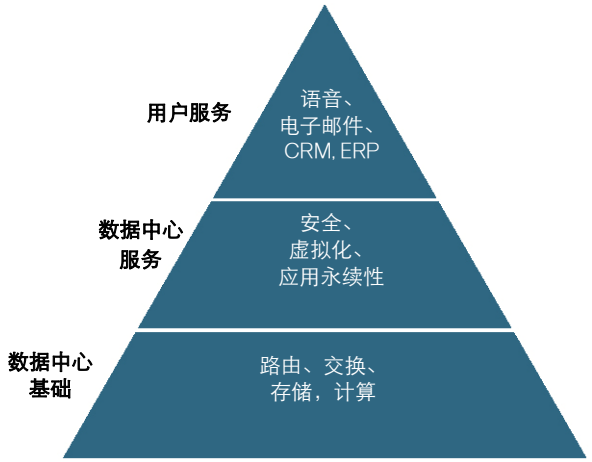
- 第一个模块涵盖有关物理环境的数据中心设计要素，列出了电源、冷却、安装机架和所需空间方面的概要信息，以便您在进行数据中心设计时考虑。
- 本部分侧重于为支持企业及其相关服务的应用服务器建立一个集中连接点。以太网模块说明了如何在数据中心配置第二层和第三层连接，以及到企业其他部分的通信路径。
- 存储网络模块显示了基础以太网设计如何支持面向网络连接存储（NAS）的基于 IP 的网络存储。存储网络模块深入介绍了如何通过使用 Cisco Nexus 5500UP 交换机作为 SAN 核心，来部署光纤通道存储域网络（SAN）。
- 计算连接模块说明了可在数据中心内使用的各种主机连接方案。该模块介绍了双宿主和单宿主服务器，以及到网络的刀片服务器系统连接。
- 网络安全性模块侧重于部署防火墙，以保护贵企业的关键和敏感信息资产。入侵防御系统(IPS)模块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。
- 应用永续性模块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。
- 附录部分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本指南主要变更的列表。

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架构分层服务。

图 1. 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符合此类规模的企业的预算标准。
- **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

中小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，中小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。

面向中小企业的思科 IBA 智能业务平台数据中心架构是基本服务器机房基础设施的自然演进。中小企业数据中心旨在解决以下四大业务挑战：

- 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

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，在存储配置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

在中小企业的发展过程中，通常会为各个应用配备专用的服务器，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。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。

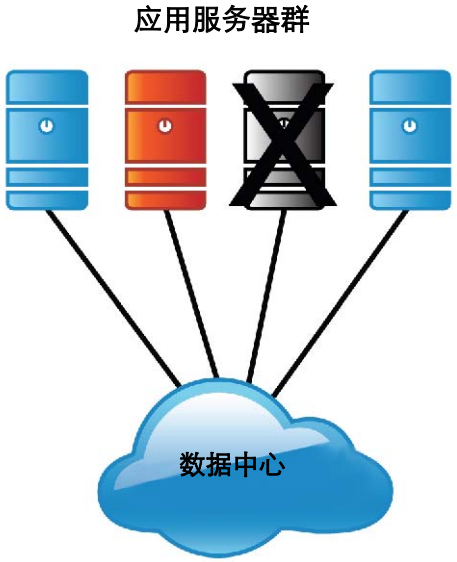
实际上，对于企业数据的威胁常常来自于内部网络。这些威胁可能来自于进入企业办公现场的供应商、受到感染的员工笔记本电脑，或者是已遭到入侵、可能被用来当作攻击平台的服务器。由于企业一般是在数据中心内集中存储最为重要的数据，所以在完整的数据中心架构计划中，安全不再是可选组件，而是必备组成部分。

思科 IBA 智能业务平台中小企业数据中心架构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



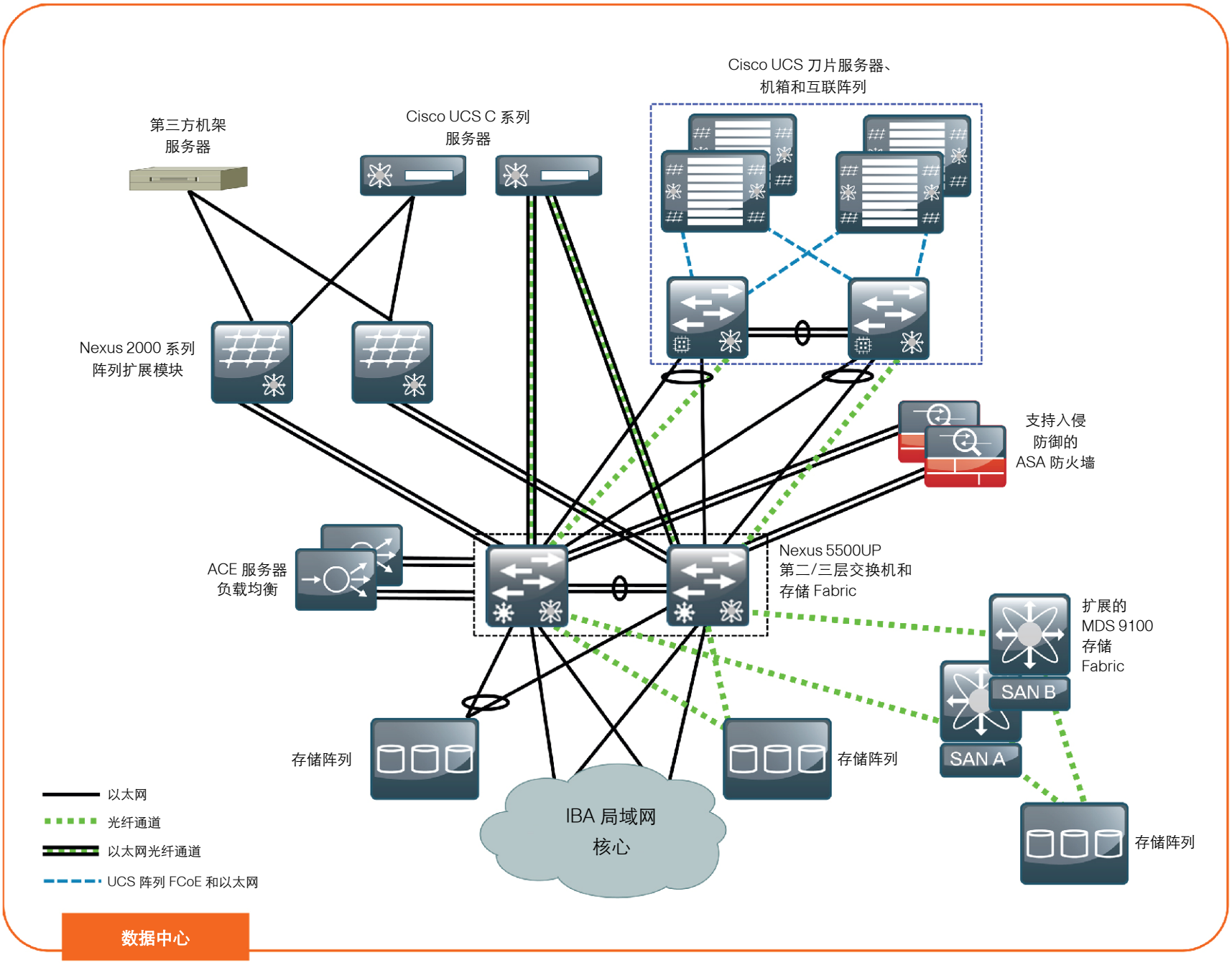
应用可用性决定着生产力和客户满意度，而这对于企业的成功至关重要。IT 部门除了要能够监测简单的服务器可用性，而且还要能够监测应用可用性，并需要能够快速、透明地向应用服务器群添加更多服务器。

技术概述

IBA 中小企业数据中心架构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。

备注

图 3. 思科 IBA 中小企业数据中心架构



正如《面向中小企业的思科 IBA 智能业务平台——无边界网络基础设计概述》中所述，IBA 智能业务平台中小企业数据中心架构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 智能业务平台第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第二层和第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 智能业务平台中小企业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第三层子卡时，能够支持第二层和第三层交换。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技术，可提供一种无回路方法来扩建中小企业数据中心，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。

存储网络

存储网络是解决数据存储日益增长问题的关键，而这一问题是中小企业必须要面对的。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。IBA 智能业务平台中小企业数据中心设计使用 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、光纤通道和以太网光纤通道（FCoE）。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，以满足更大的光纤通道要求。本部署模块包括了在 Cisco Nexus 5500UP 系列与支持光纤通道 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，以支持以太网和光纤通道传输。本模块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和 FCoE 将多个以太网 NIC 和光纤通道主机总线适配器（HBA）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 拓扑的光纤通道连接。该模块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/热备份永续性，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 4710s 可扩展至多千兆位运营，并可作为主动/热备份对进行部署，以防止由于设备故障或维护而中断运行。

借助该架构，中小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。本指南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，但本指南采用了模块化方式，使您可以通过选择率先部署的特定架构组件，来逐步升级。

本指南的后面部分详细介绍了组成该架构的各种技术。

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、交换机室甚至是中小企业数据中心时，您必须要考虑以下三个方面：电源、散热和机架安装。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

面向中小企业数据中心的思科 IBA 智能业务平台架构采用冗余平台和链路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。

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，需要不间断电源（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 200-240 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 110 伏的插座或配电盘。

散热

在用电的同时必将产生热量。也就是说，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，标准的建筑物通风就已经足够。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），建筑物通风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、活动地板间层制冷和墙壁安装式制冷。

设备机架

将设备放置在什么样的机架上是一个不容您忽视的细节问题。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。

备注

以太网基础设施

业务概述

随着中小企业的不断发展，面向中小企业的 IBA 智能业务平台基础架构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 智能业务平台中小企业数据中心架构中，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 智能业务平台中小企业数据中心架构旨在支持将服务器和服务从原始服务器群轻松迁移到能够随着企业的增长而扩展的数据中心。

具备通用端口能力的 Nexus 5500UP 交换机可在单一平台上支持以太网、以太网光纤通道（FCoE）和光纤通道（FC）端口。Nexus 5500UP 能够作为光纤通道 SAN 支持中小企业数据中心，并连接到现有光纤通道 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 智能业务平台中小企业数据中心架构可充分利用 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第二层和第三层交换架构，进而为大多数中小企业数据中心提供可扩展性：

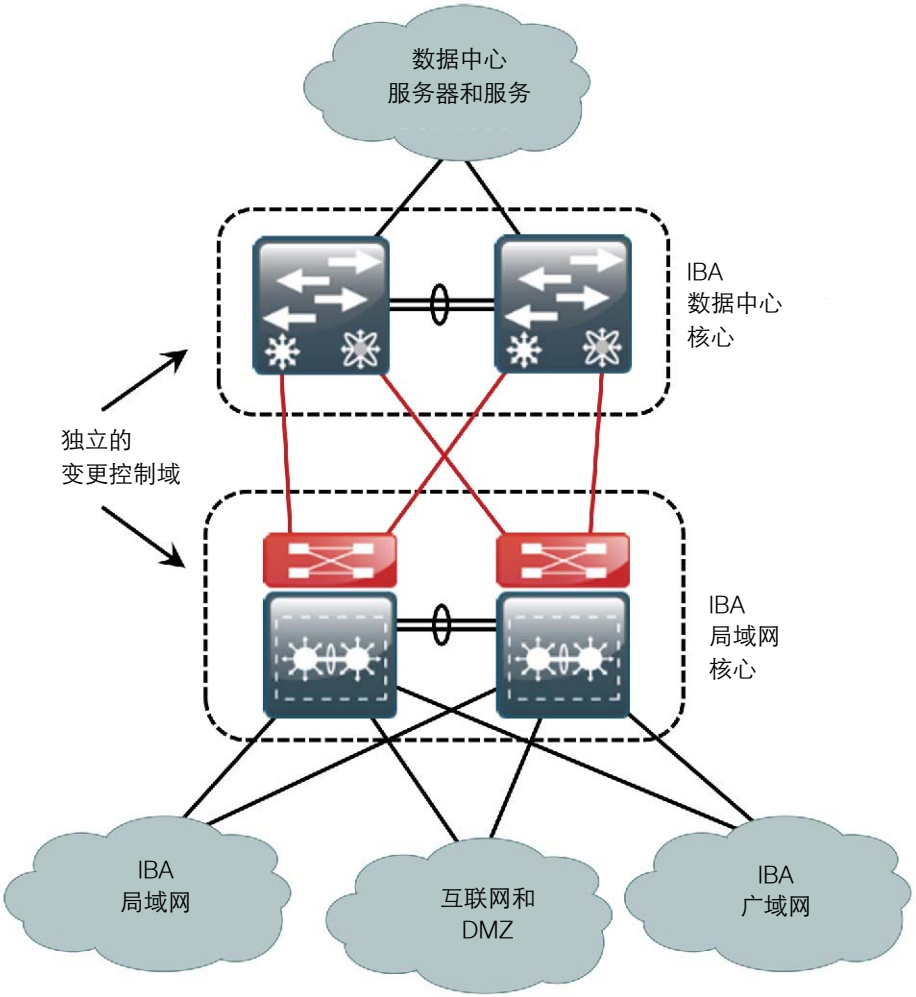
- 第三层路由表最多能支持 8000 个路由。
- 第三层引擎能够为第二层域支持多达 8000 个邻接地址或 MAC 地址。
- 该解决方案在推荐的虚拟端口通道模式下运行时，可提供多达 1000 个 IP 组播组。

读者提示

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

图 4 中显示，第三层数据中心核心层与《面向中小企业的思科 IBA 智能业务平台——无边界网络基础部署指南》中设计的第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



使用第三层互联两个核心层的结果如下：

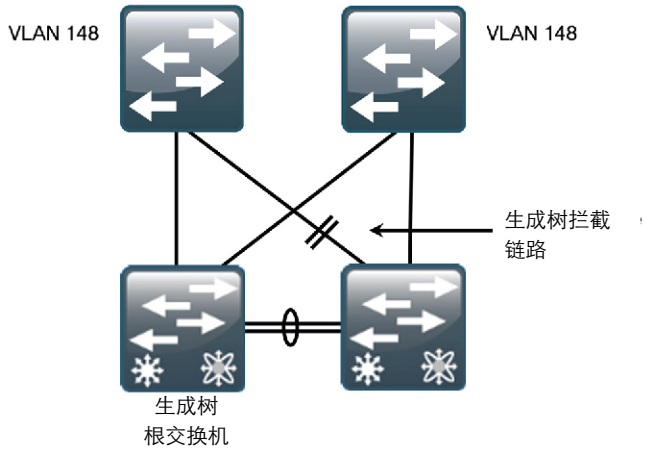
- 形成一条永续第三层互联，支持迅速的故障切换
- 两个核心网络的变更控制在逻辑上是相互独立的。
- 局域网核心层为局域网、广域网和互联网边缘提供了可扩展互联。
- 数据中心核心层为所有数据中心服务器和服务提供了互联。
- 在服务器和设备间传输的数据中心内部第二层和第三层流量在数据中心核心层进行本地交换。
- 数据中心有一个迁移到远程位置的逻辑分隔点，且无需重新设计，仍能提供核心层服务。

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第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

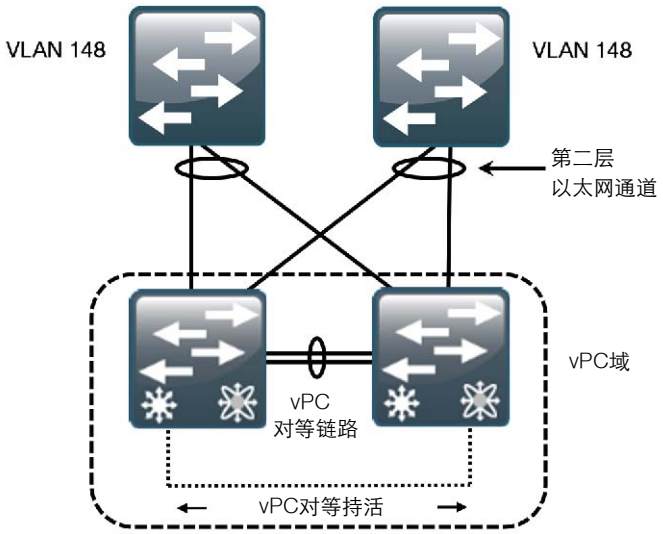


Cisco Nexus 5500UP 系列交换机对采用虚拟端口通道（vPC）特性配置而成，可为思科 IBA 智能业务平台中小企业数据中心架构提供中央以太网交换架构。vPC 支持以物理方式连接到两个不同 Cisco Nexus 交换机的链路向第三方下游设备显示为来自一个设备，并作为单个以太网端口通道的一部分。这个第三方设备可以是服务器、交换机，或其它任何支持 IEEE 802.3ad 端口通道的设备。这一功能允许使用两个数据中心核心层交换机来构建永续、无环路的第二层拓扑结构，通过所有相连链路转发流量，而无需借助生成树协议拦截来防止环路。

数据中心设计中使用的 Cisco NX-OS Software vPC，以及《面向中小企业的思科 IBA 智能业务平台——无边界网络基础设计概述》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第二层端口通道。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 在中小企业数据中心扩展，并保持永续架构。

vPCs 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 智能业务平台中小企业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

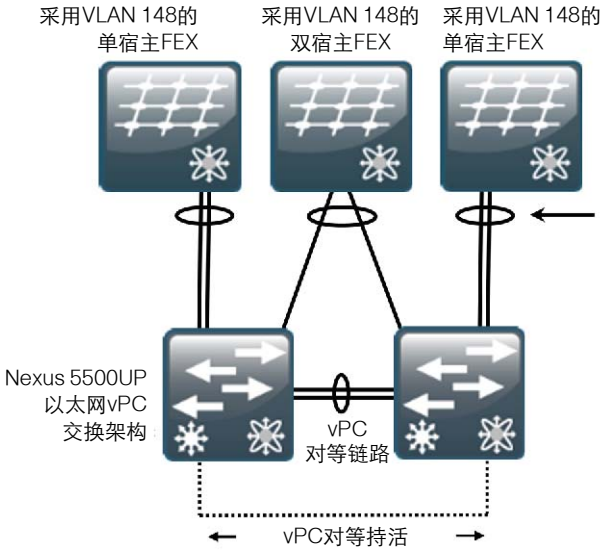
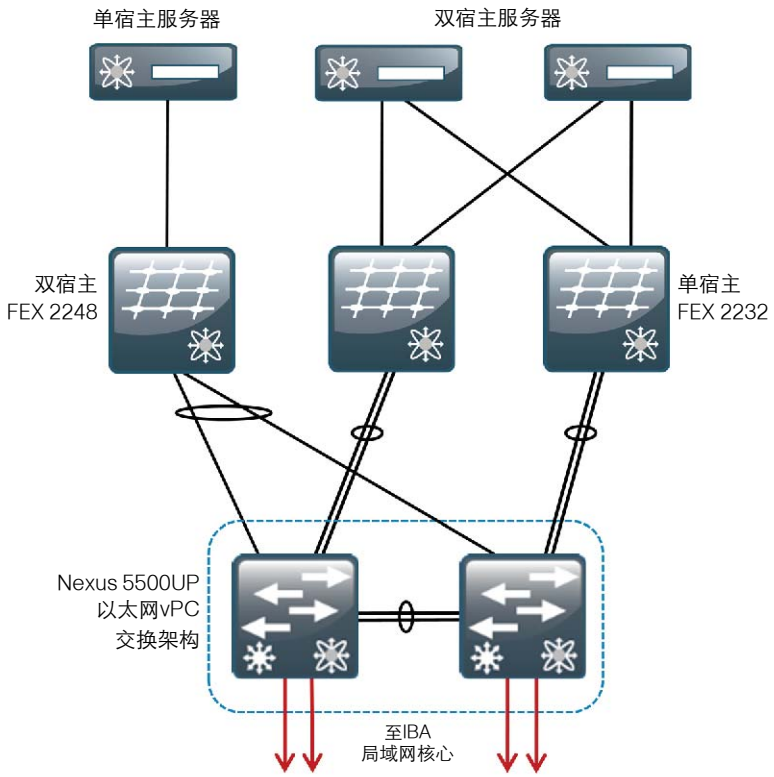


图 8 中的参考架构示例阐述了采用互联服务器的单宿主和双宿主 Cisco FEX 配置。每个 Cisco FEX 均包括专用阵列上行链路端口，设计用于连接上游 Cisco Nexus 5500UP 系列交换机，支持数据通信和管理。Cisco Nexus 5500UP 交换机上的任何万兆以太网端口均可用于 Cisco FEX 连接。

技术提示

当 Cisco Nexus 5500UP 系列交换机配置用于第三层运行时，它们可支持多达 8 个互联 Cisco FEX（要求使用 NX-OS 5.1(3)N1 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



部署详情

为思科 IBA 中小企业数据中心架构配置以太网交换架构时需遵循以下配置步骤。

流程

配置带外管理

1. 应用平台特定的配置
2. 应用全局配置
3. 配置到第三层核心的链路
4. 配置访问端口

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。典型的中小企业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，我们使用固定配置第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。

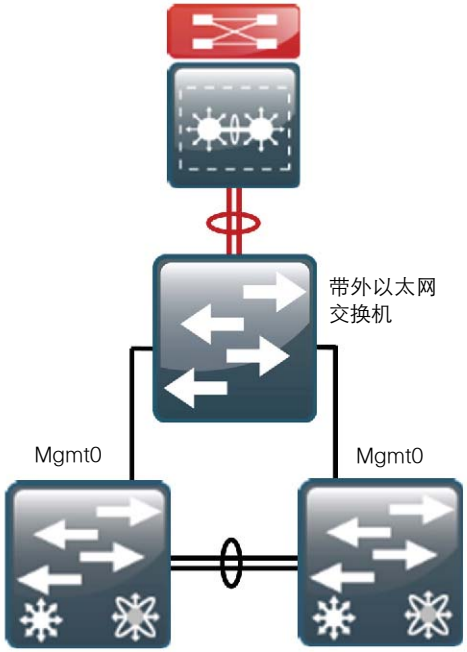
带外网络可提供：

- 第二层路径，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虚拟端口通道持活数据包。
- 用于通过管理接口实现 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

第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 管理人员提供访问这些设备的能力。提供 IP 连接的选项取决于您数据中心的位置。

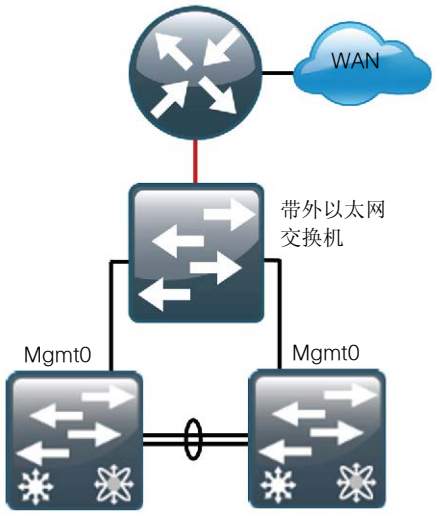
如果您的数据中心与总部局域网处于同一位置，那么核心局域网交换机可提供到数据中心管理子网的第三层连接。

图 9. 提供第三层连接的核心局域网交换机



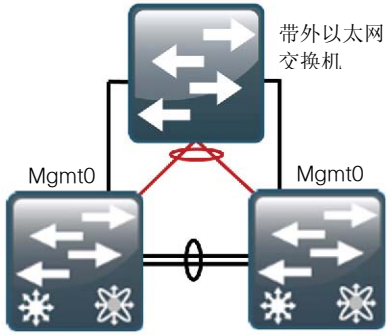
如果您的数据中心位于与大型局域网不同的设施，则广域网路由器可提供到数据中心管理子网的第三层连接。

图 10. 提供第三层连接的广域网路由器



提供到数据中心管理子网的第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。我们将在本指南中配置此连接选项。

图 11. 通过使用核心 Cisco Nexus 5500UP 交换机提供第三层连接



技术提示

当使用数据中心核心 Cisco Nexus 5500UP 交换机支持第三层连接时，用于 vPC 持活数据包的第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路径（vrf），而不是 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，因此它们不需要第三层交换机来支持数据中心核心交换机之间的数据包。第三层交换虚拟接口将为数据中心之外的访问提供连接。

程序 1　应用平台特定的配置

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，将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 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。

程序 2　应用全局配置

带外局域网管理交换机需要基本全局配置。

步骤 1：应用《面向中小企业的思科 IBA 智能业务平台——无边界网络基础部署指南》“全局配置模块”部分中描述的配置。这可支持诸如管理访问和网络时间配置等基础设施要求。

步骤 2：配置设备永续性特性

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，就带外管理网络而言，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
```

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。

虽然此架构没有任何第二层环路，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第二层环路。

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

单向链路检测(UDLD)是一个第二层协议，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时更是如此。

```
udld enable
```

步骤 3：在此设计中，我们广泛使用了 EtherChannel，因为它们具有出色的永续性。如果您希望将 EtherChannel 成员链路间流量负载共享的方法规范化，应将所有管理交换机上行链路设置为在计算通过哪条链路发送流量时使用流量源和目的地 IP 地址。

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

步骤 4：为交换机配置一个 IP 地址，以便能够通过带内连接对其进行管理。

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

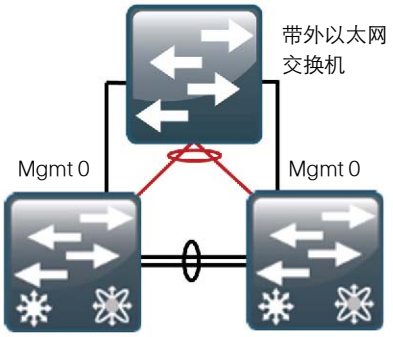
步骤 5：配置管理 VLAN

带外管理网络将使用单一 VLAN 即 VLAN 163 进行设备连接。

```
vlan [163]
name DC-Management
```

程序 3　配置到第三层核心的链路

正如之前所描述的，可通过多种方法连接到第三层，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 range [interface type] [port 1], [interface type] [port 2]
  channel-protocol lacp
  channel-group 1 mode active
```

步骤 2：配置中继。

802.1Q 中继用于连接此上游设备，以支持该设备为服务器机房交换机上定义的所有 VLAN 提供第三层服务。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。

```
interface Port-channel1
switchport trunk allowed vlan [management vlan]
switchport mode trunk
no shutdown
```

读者提示

用于支持到带外管理网络的第三层连接的数据中心核心 Cisco Nexus 5500UP 交换机上的配置，将在本指南程序 9“配置管理交换机连接”中进行介绍。

程序 4　配置访问端口

步骤 1：配置交换机接口，以支持管理控制台端口。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：通过将交换端口设置为主机模式，缩短端口进入转发状态所需的时间。

```
switchport host
```

步骤 3：（可选）保存您的管理交换机配置。

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

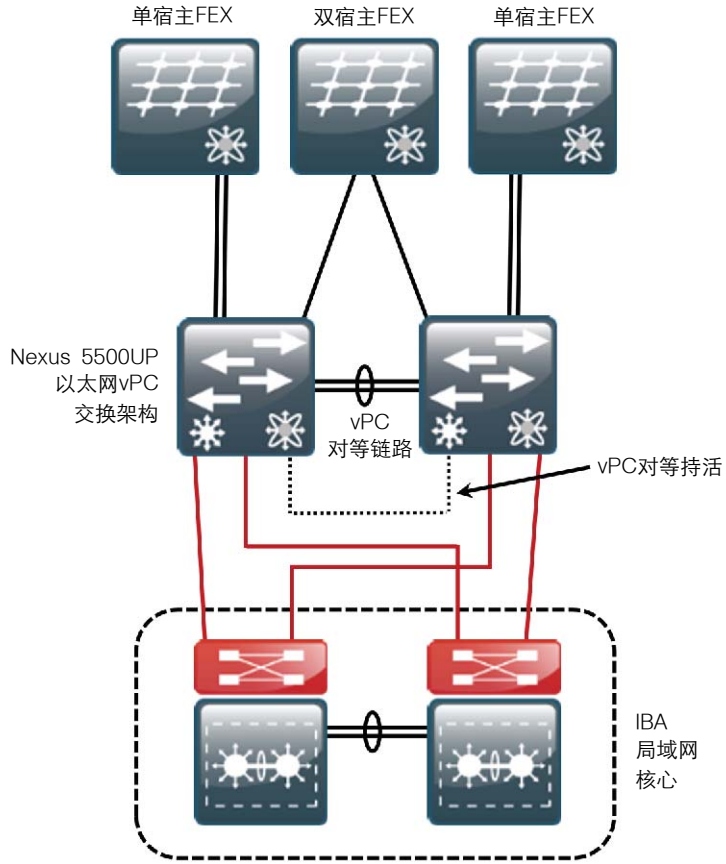
流程

配置数据中心核心

1. 建立物理连接
2. 进行初始设备配置
3. 配置虚拟端口通道
4. 配置全球数据中心核心全局
5. 配置 IP 路由协议
6. 为 VLAN 配置 IP 路由
7. 配置 IP 组播路由
8. 配置到 IBA 智能业务平台核心的连接
9. 配置管理交换机连接
10. 配置阵列扩展模块连接
11. 配置终端节点端口

程序 1　建立物理连接

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。

技术提示

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。

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 5500s 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　进行初始设备配置

软件许可证使用前提

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。数据中心核心层以第三层配置为特征，因此 Cisco Nexus 5500UP 系列交换机需要第三层许可，以支持全部的增强型内部网关路由（EIGRP）功能。当运行本机光纤通道或以太网光纤通道（FCoE）时，需要光纤通道许可证。

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
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]: y
    Mgmt0 IPv4 address : 10.10.63.10
    Mgmt0 IPv4 netmask : 255.255.255.128
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : 10.10.63.1
  Enable the telnet service? (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
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 ad : 10.10.48.17
  Enter basic FC configurations (yes/no) [n]: n
The following configuration will be applied:
  switchname dc5548ax
interface mgmt0
ip address 10.10.63.10 255.255.255.128
no shutdown
exit
vrf context management
ip route 0.0.0.0/0 10.10.63.1
exit
  no telnet server enable
  ssh key rsa 2048 force
  ssh server enable
  ntp server 10.10.48.17 use-vrf management
Would you like to edit the configuration? (yes/no) [n]: n
Use this configuration and save it? (yes/no) [y]: y
[########################################] 100%
dc5548ax login:
```

第二个 Cisco Nexus 5500UP 交换机设置脚本的唯一变化是系统名称和 Mgmt0 地址（将为 10.10.63.11）。

步骤 3：启用系统特性。

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第三层操作、光纤通道存储协议和 FCoE 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》。

在 NXOS 软件中配置通常需要的特性。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
```

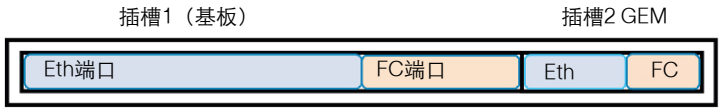
技术提示

虽然本设计中没有使用，但如果您的网络需要光纤通道特定特性 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。它应在对交换机应用任何其它配置之前启用。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：配置端口操作模式。在本例中，在 Cisco Nexus 5548UP 交换机上启用端口 28 至 32 作为光纤通道端口。

```
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 或光纤通道。所有交换机端口均默认启用，支持以太网运行。光纤通道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(1) 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 5：启用巨型帧支持。巨型帧可在 Cisco Nexus 5500UP 上基于每服务类别（CoS）启用。本示例显示了默认 CoS 上启用的巨型帧操作。

```
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9216
system qos
  service-policy type network-qos jumbo
```

技术提示

巨型帧能够提高数据中心内关键终端节点之间的数据吞吐率，这些节点能够承载尺寸较大的数据包，如基于 iSCSI 的存储系统及其相关的服务器。如果您的 iSCSI 流量在子网间路由，您也可在第三层接口上将 mtu 增加至 9216。

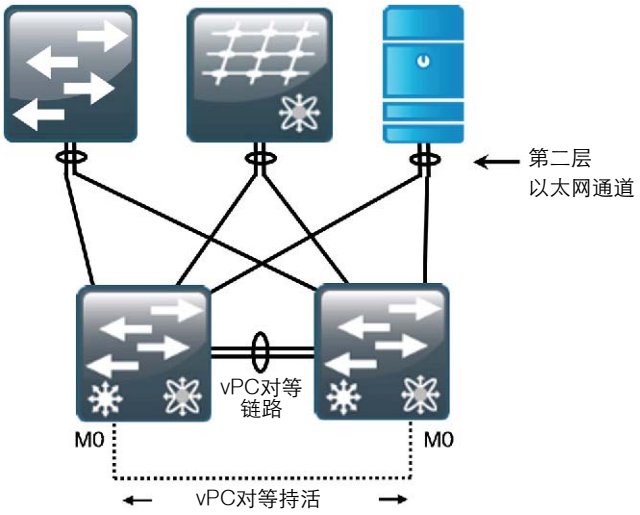
步骤 6：（可选）保存您的配置，然后重新加载交换机。由于 Nexus 交换机需要重启才能识别为支持光纤通道运行而配置的端口，因此这是重新加载交换机的好时机。

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

步骤 7：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。请为 mgmt0 接口设定独一无二的设备名称(dc5548bx)和 IP 地址(10.10.63.11)。其他所有配置详情都是相同的。

程序 3　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，以在单一第二层 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 32667。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 5500s 上配置 vPC 对等持活：

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

```
peer-keepalive destination 10.10.63.11 source 10.10.63.10
```

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

```
peer-keepalive destination 10.10.63.10 source 10.10.63.11
```

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 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
```

技术提示

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： 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-tree port type network
```

步骤 6：配置物理接口，将两个 Cisco Nexus 5500s 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。

技术提示

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：在第二个 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 4　配置全球数据中心核心全局

数据中心核心需要超越设置脚本的基本核心运行配置。

IP 子网和 VLAN 分配

IP 子网和 VLAN 分配均遵循《面向中小企业的思科 IBA 智能业务平台——无边界网络基础部署指南》中的指导。在您查看配置指南时，您可能注意到了第二个 8 位字节的差异。第二个 8 位字节的地址是根据该配置所属的设计来分配的：

- 8 和 9 属于中小企业 – 1000 设计
- 10 和 11 属于中小企业 – 2500 设计

第三个 8 位字节在不同设计间保持相同。 例如，10.x.48.0 子网是服务器群或数据中心子网。对于局域网网段，将 VLAN 编号与 IP 子网匹配对应，能够简化 VLAN 配置。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 1. 数据中心 VLAN

VLAN 编号	用途	中小企业-2500	中小企业-1000
148	Servers_1	10.10.48.0/24	10.8.48.0/24
149	Servers_2	10.10.49.0/24	10.8.49.0/24
150	Servers_3	10.10.50.0/24	10.8.50.0/24
153	FW_Outside	10.10.53.0/24	10.8.53.0/24
154	FW_Inside_1	10.10.54.0/24	10.8.54.0/24
155	FW_Inside_2	10.10.55.0/24	10.8.55.0/24
156	PEERING_VLAN	10.10.56.0/24	10.8.56.0/24
159	1kv-Packet		
160	1kv-Control		
161	VMotion		
162	iSCSI		
163	DC-Management	10.10.63.0/25	10.8.63.0/25

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第二层环路，但向核心交换机分配生成树根是一个很好的实践。

- 将主用 Cisco Nexus 5500UP 配置为生成树根。

```
spanning-tree vlan 148-151,153-157,159-163 root primary
```

- 将第二个 Cisco Nexus 5500UP 配置为备用生成树。

```
Spanning-tree vlan 148-151,153-157,159-163 root secondary
```

步骤 3： 采用该网络的 DNS 服务器的 IP 地址，配置命名服务器命令。在思科 IOS 设备的命令行，如果能够输入一个域名而不是 IP 地址，将会很有帮助。

```
ip name-server 10.10.48.10
```

步骤 4： 为设备所在地设置本地时区。网络时间协议(NTP)用于同步网络中所有设备上的时间，以便进行故障排除。在初始设置脚本中，您可设置 NTP 服务器地址。现在为设备所在地设置本地时间。

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

步骤 5： 定义一个只读和一个读写 SNMP 团体字符串，用于网络管理。在本示例中，只读团体字符串为“cisco”，读写团体字符串为“cisco123”。

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

步骤 6： 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 1
ip address 10.10.63.254/32
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。第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 的回环接口将为 10.10.63.253/32。

步骤 7： 配置 EtherChannel 端口通道，以使用第三层 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 交换机中第三层路由引擎的吞吐率。

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

程序 5　配置 IP 路由协议

步骤 1： 将 EIGRP 配置为 IP 路由协议。

```
router eigrp 1
  router-id 10.10.63.254
```

第二个 Cisco Nexus 5500UP 的路由器 id 将为 10.10.63.253/32。

EIGRP 是中小企业数据中心使用的 IP 路由协议，可兼容中小企业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 1 IP 地址。

步骤 2： 在第三层接口上配置 EIGRP。

```
interface loopback 1
ip router eigrp 1
```

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。如果第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： 配置核心层第三层对等链路。

```
Interface Vlan 156
  ip address 10.10.56.1/30
  ip router eigrp 1
  ip pim sparse-mode
  no shutdown
```

要在路由对等体间传递 EIGRP 路由更新，EIGRP 必须在第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 10.10.56.2/30。

程序 6　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第三层可达性的 VLAN，都需要第三层交换虚拟接口（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： 在接口上配置 EIGRP 进程号。这可向 EIGRP 通告子网。

```
ip router eigrp [router process + number]
```

步骤 4： 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 [router process + number]
```

步骤 5：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 进程号与 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 [process number]
priority [priority]
ip [ip address of 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 10.10.48.2/24
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 148
    priority 110
    ip 10.10.48.1
  no shutdown
  description Servers_1
```

- 这是对等 Nexus 5500UP 交换机的配置示例。

```
interface Vlan148
  no ip redirects
  ip address 10.10.48.3/24
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 148
    ip 10.10.48.1
  no shutdown
  description Servers_1
```

程序 7　配置 IP 组播路由

思科 IBA 智能业务平台中小企业基础网络支持使用 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《面向中小企业的思科 IBA 智能业务平台——无边界网络基础部署指南》中找到。

步骤 1：将网络的 IP 组播汇聚点（RP）配置为 rp-address，并采用 group-list 配置它所服务的 IP 组播子网。

```
ip pim rp-address 10.10.15.252 group-list 239.1.0.0/16
```

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
```

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。

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。

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

步骤 4：采用 pim sparse-mode 命令，为 IP 组播操作配置所有第三层接口。

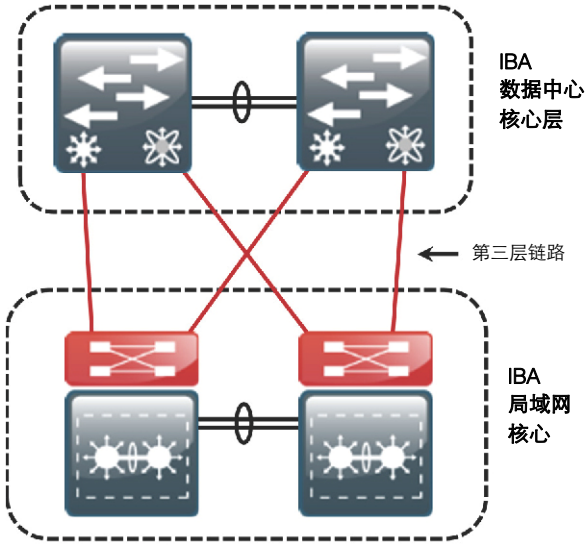
```
ip pim sparse-mode
```

不必在管理 VLAN 接口（接口 vlan 163）上配置 ip 组播。

程序 8　配置到 IBA 智能业务平台核心的连接

虚拟端口通道不支持跨 vPC 与另一个第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第三层接口，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。

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，配置两个点对点第三层接口。

```
interface Ethernet1/19
  description Core Ten1/4/6
  no switchport
  ip address 10.10.24.2/30
  ip router eigrp 1
  ip pim sparse-mode

interface Ethernet1/20
  description Core Ten2/4/6
  no switchport
  ip address 10.10.24.6/30
  ip router eigrp 1
  ip pim sparse-mode
```

步骤 2：在第二个数据中心核心 Cisco Nexus 5500UP 交换机上，配置两个点对点第三层接口。

```
interface Ethernet1/19
  description Core Ten1/4/8
  no switchport
  ip address 10.10.24.10/30
  ip router eigrp 1
  ip pim sparse-mode

interface Ethernet1/20
  description Core Ten2/4/8
  no switchport
  ip address 10.10.24.14/30
  ip router eigrp 1
  ip pim sparse-mode
```

步骤 3：在思科 IBA 智能业务平台中小企业核心 6500 VSS 交换机上，配置四个相应的点对点第三层链路。

```
interface TenGigabitEthernet1/4/6
 description DC5548a Eth1/19
 no switchport
 ip address 10.10.24.1 255.255.255.252
```

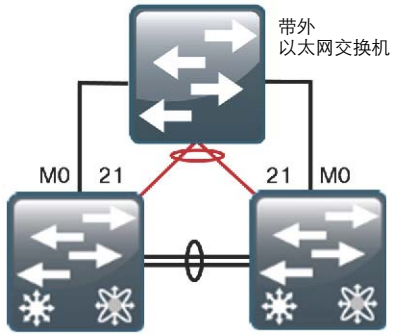
```
 ip pim sparse-mode
 mls qos trust dscp

interface TenGigabitEthernet2/4/6
 description DC5548a Eth1/20
 no switchport
 ip address 10.10.24.5 255.255.255.252
 ip pim sparse-mode
 mls qos trust dscp

interface TenGigabitEthernet1/4/8
 description DC5548b Eth1/19
 no switchport
 ip address 10.10.24.9 255.255.255.252
 ip pim sparse-mode
 mls qos trust dscp

interface TenGigabitEthernet2/4/8
 description DC5548b Eth1/20
 no switchport
 ip address 10.10.24.13 255.255.255.252
 ip pim sparse-mode
 mls qos trust dscp
```

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路由。

程序 9　配置管理交换机连接

以太网基础设施模块的第一个流程涵盖部署带外以太网管理交换机。在该部分，我们配置了支持第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 第三层访问的一个选项，以支持数据中心之外的访问。如果您选择了这一方法来提供带外以太网 VLAN 访问，那么请遵循这一程序来对上行链路和 Cisco Nexus 5500UP 交换机上的第三层 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。



在每个数据中心核心 Cisco Nexus 5500UP 交换机上配置以下步骤。

步骤 1： 配置到以太网管理交换机的 vPC 端口通道。

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

步骤 2： 配置属于端口通道的物理端口。

```
interface Ethernet1/21
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
  channel-group 21 mode active
```

步骤 3： 配置 VLAN 163 的 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 10.10.63.2/25
  ip router eigrp 1
```

```
  ip passive-interface eigrp 1
  hsrp 163
    priority 110
    ip 10.10.63.1
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 10.10.63.3/25
  ip router eigrp 1
  ip passive-interface eigrp 1
  hsrp 163
    ip 10.10.63.1
no shutdown
```

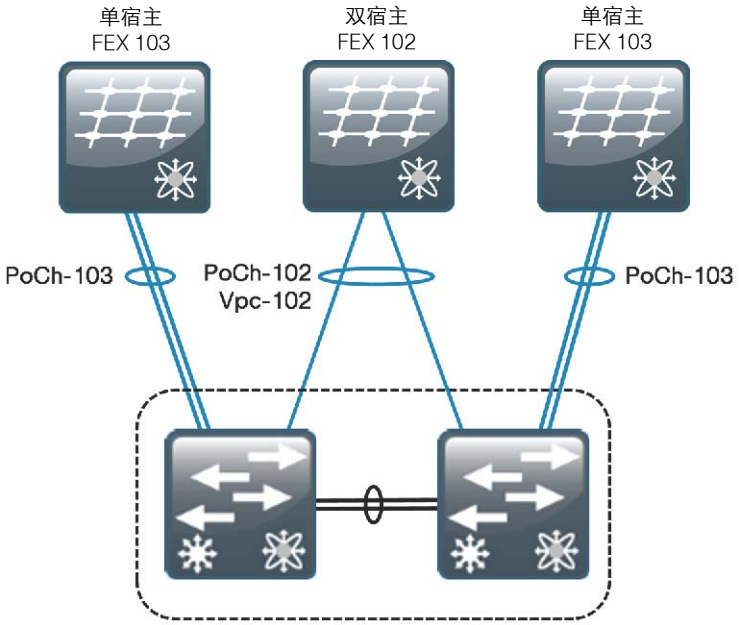
程序 10　配置阵列扩展模块连接

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**支持到第 3 层路由端口的连接（路由协议在此处与第三层核心进行交换），它们仅用于第二层连接的终端主机或设备。
- 运行第三层路由的 Cisco Nexus 5500UP 在一个交换机上最多支持 8 个连接的 Cisco FEX。

此外：

- 思科阵列扩展模块连接也可配置为 Cisco Nexus 5500 系列交换机上的端口通道连接。
- 如果要将 Cisco FEX 以单宿主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 以双宿主方式连接到 vPC 交换机对中的两个成员，以支持单宿主服务器，可将其配置为一个 vPC 端口通道。



技术提示

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。

步骤 1：将物理接口分配到支持 Cisco FEX 连接的端口通道。

```
interface Ethernet1/13
  channel-group 102

interface Ethernet1/25
  channel-group 103

interface Ethernet1/26
  channel-group 103
```

步骤 2：配置端口通道接口来支持 Cisco 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 dual-homed 2248
  switchport mode fex-fabric
  vpc 102
  fex associate 102

interface port-channel103
  description single-homed 2232
  switchport mode fex-fabric
  fex associate 103
```

步骤 3：在完成这些配置步骤之后，您可以利用 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
103       FEX0103     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 11　配置终端节点端口

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边缘之后，端口能够在一个新设备接入后立即为其提供连接。

示例

```
interface Ethernet102/1/1
  switchport access vlan 163
  spanning-tree port type edge
```

技术提示

鉴于主机在一个双宿主 Cisco FEX 上，是双宿主主机，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。

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中继接入，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边缘之后，端口能够在一个新设备接入后立即为其提供连接。

示例

```
interface Ethernet102/1/2
  switchport mode trunk
  switchport trunk allowed vlan 148-151,154-163
  spanning-tree port type edge trunk
```

步骤 3：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。由于该服务器是使用 vPC EtherChannel 的双宿主，该配置必须在两个 Cisco Nexus 5500UP 数据中心核心交换机上完成。

示例

```
interface ethernet103/1/1
  switchport mode trunk
  switchport trunk allowed vlan 148-151,154-163
  spanning-tree port type edge trunk
  channel-group 600
  no shutdown
interface port-channel 600
  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。

总结

利用本章节提供的配置步骤，您可以为自己的中小企业数据中心环境部署一个具有永续性的以太网交换架构，从而立即获益于 Cisco Nexus 5500UP 和 2000 系列产品的高性能、低延迟和高可用性特性。如果了解更多数据中心配置高级特性，请登录 cisco.com 查阅 Cisco Nexus 5500 系列配置指南。

备注

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

IP 存储方案

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)或网络文件系统(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。

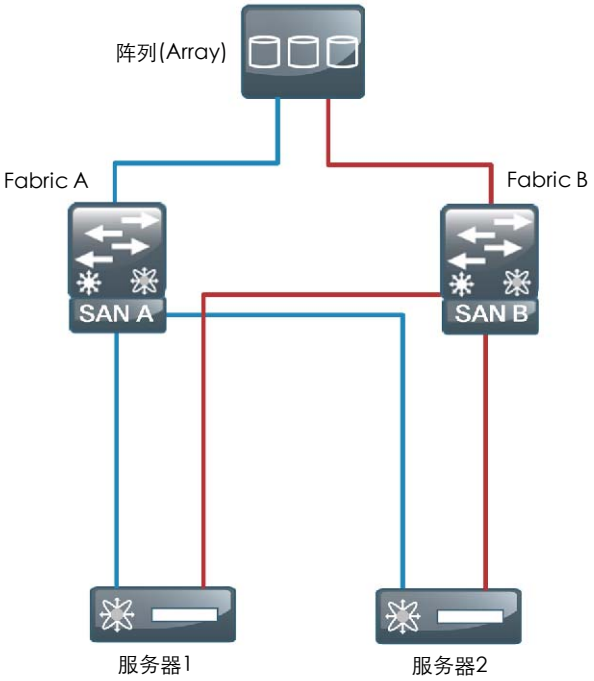
光纤通道存储

光纤通道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 智能业务平台中小企业数据中心架构使用 Cisco Nexus 5500UP 系列交换机作为核心，提供光纤通道和以太网光纤通道（FCoE）SAN 交换。Cisco Nexus 5500UP 通过支持光纤通道和 FCoE 服务器与存储阵列，可提供紧缩的光纤通道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 个光纤通道端口的大型 SAN 阵列的理想选择，提供 48 个线速 8-Gbps 光纤通道端口，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 的光纤通道等选项，支持更长距离的 SAN 扩展。

在 SAN 中，阵列由与光纤通道交换机相连的服务器和存储组成（参见图 12）。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。每个阵列上的光纤通道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 12. 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，连接到光纤通道交换机。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”）。

使用能够简化启动器和目标识别工作的命名惯例。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™ FAS3140。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 网络以支持基于光纤通道的存储。
- Cisco MDS SAN 交换机的配置可支持更大规模的光纤通道环境。
- 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

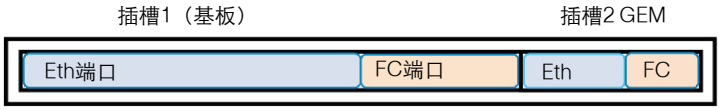
完成以下每个程序，以在数据中心核心 Cisco Nexus 5500UP 交换机上配置光纤通道 SAN。

程序 1　配置光纤通道操作

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 或光纤通道。所有交换机端口均默认启用，支持以太网运行。光纤通道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部署指南之前的以太网部分进行了概要介绍。如果您已配置了用于光纤通道操作的端口，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 作为光纤通道端口。

步骤 1：为光纤通道配置通用端口模式。

```
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(1)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，这可同时启用本机光纤通道和 FCoE 操作。

```
feature fcoe
```

读者提示

在本部署指南以前的以太网章节，我们显示了启用特性 fcoe。

步骤 4: 启用 san 端口通道中继操作和光纤通道 N 端口接口虚拟化，以连接到 Cisco UCS 互联阵列。

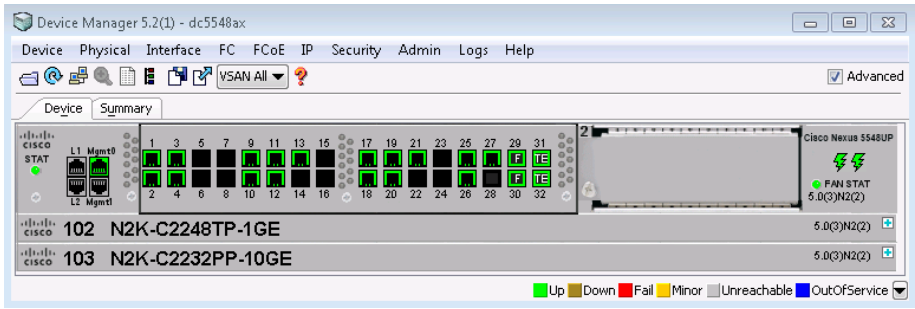
```
feature npiv
feature fport-channel-trunk
```

如需了解有关连接到支持光纤通道操作的 Cisco UCS B 系列互联阵列的更详细信息，请参阅《面向中小企业的思科 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

Cisco MDS 设备管理器可提供一个图形界面，以配置支持光纤通道交换的 Cisco Nexus 交换机或 Cisco MDS 9100 系列交换机。要访问设备管理器，应通过 HTTP 连接至管理地址，或通过思科阵列管理器直接访问。

也可使用 CLI 来配置光纤通道操作。



技术提示

运行思科阵列管理器和设备管理器需要 Java 运行时环境（JRE），用户应在使用任一应用之前先在桌面上安装这一环境。

面向 SAN Essentials Edition 的 Cisco DCNM 是一款免费应用，可从 Cisco.com 上下载，来配置 SAN 设备。同时管理多台交换机需要许可版本。

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。

光纤通道以“SAN A”和“SAN B”方法运行，在那里您可创建两个单独的 SAN 阵列。光纤通道主机和目标连接到两个阵列，以实现冗余。SAN 阵列并行运行。

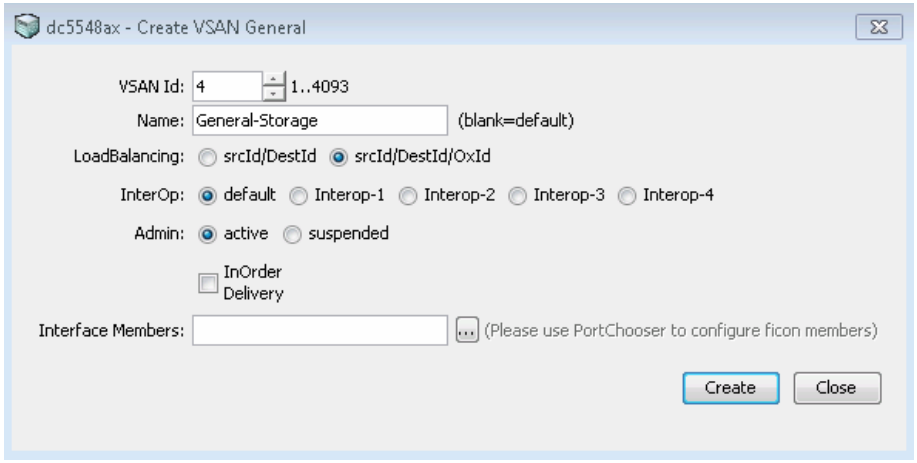
以下示例中创建了两个 VSAN，每个数据中心核心 Nexus 5500UP 交换机上一个。

您可使用命令行界面（CLI）或设备管理器来创建 VSAN。

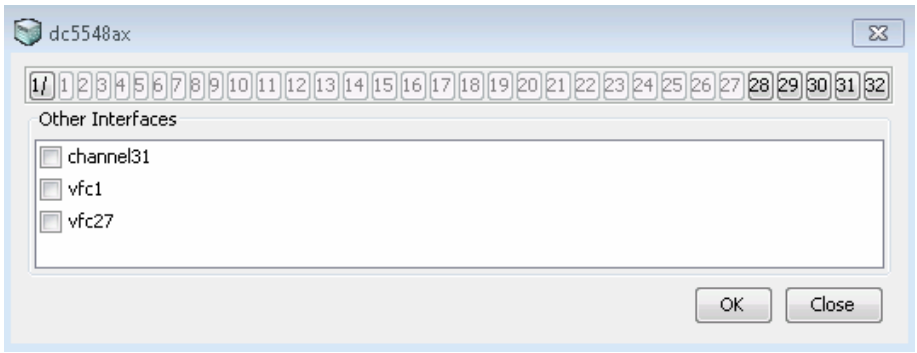
步骤 1：使用 Device Manager（设备管理器），点击 **FC>VSANS**。之后"Create VSAN General（创建 VSAN 常规）"窗口出现。

步骤 2：将 VSAN id 设定为 **4**，名称设定为 **General-Storage**。

步骤 3：在 Interface Members（接口成员）框的旁边，点击省略号（…）按钮。



步骤 4：通过点击您所需的端口编号，选择接口成员。



步骤 5：点击 **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 中应用以下配置。

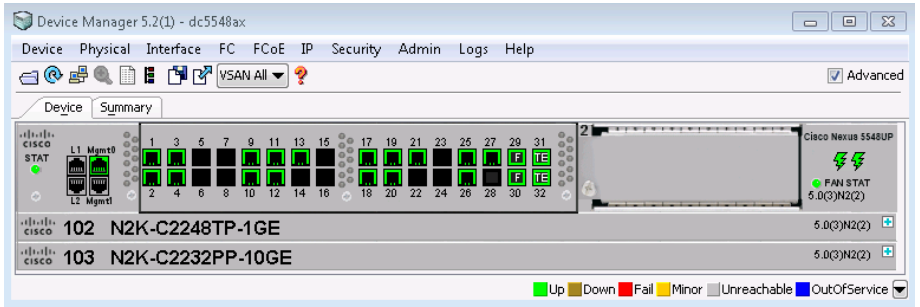
```
vsan database
vsan 4 name “General-Storage”
vsan 4 interface fc1/28
```

步骤 6：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。

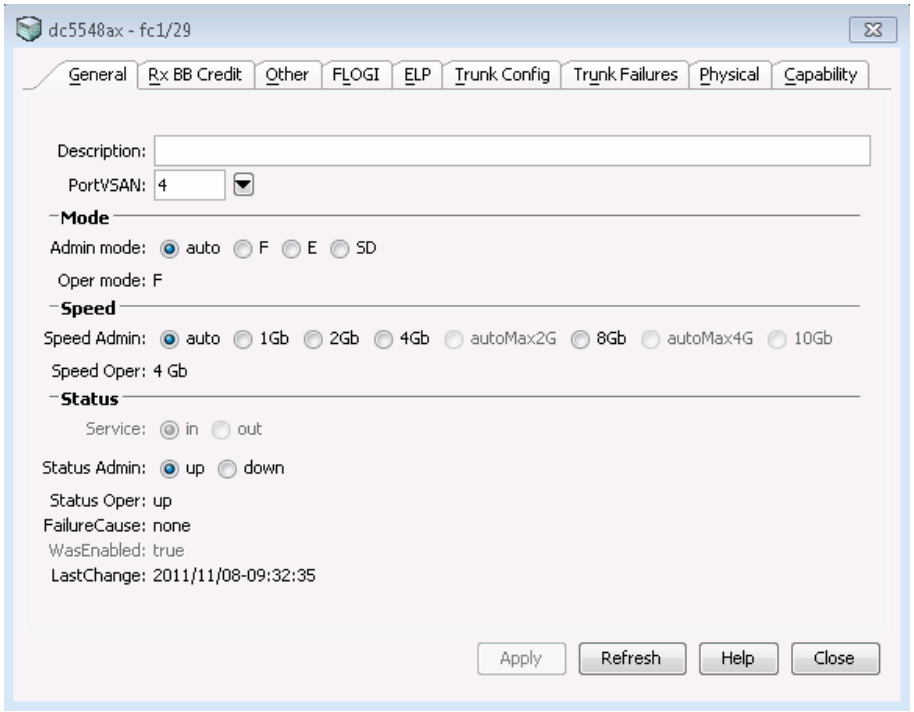
程序 3　配置光纤通道端口

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：点击 Status Admin（状态管理）为 up，启用此端口。

步骤 3：在下拉菜单中向端口分配 VSAN 4 或 VSAN 5，具体取决于您正在使用哪个交换机，然后点击 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，类似于之前的配置 VSAN 程序中的步骤 3。如果您已创建了 vsan，这是向 vsan 分配端口的另一途径。

步骤 4：将光纤通道设备连接到端口。

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光纤通道网络的更多信息，请参阅《面向中小企业的思科 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。

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主机总线适配器插入光纤通道端口上的交换机内，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.
```

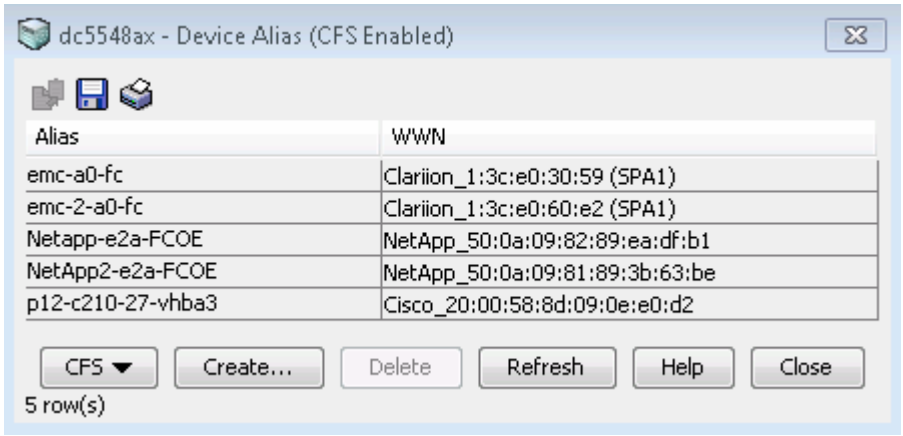
程序 4　配置设备别名

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。

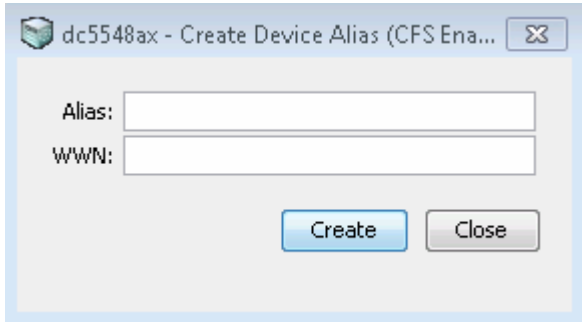
您可以通过设备管理器或 CLI 配置设备别名。

选项 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，通过转至 **FC > Advanced（高级）> Device Alias（设备别名）**，访问设备别名（Device Alias）窗口。



步骤 2：点击 **Create（创建）**。



步骤 3：输入设备别名名称，粘贴或输入主机的 WWN，然后点击 **Create（创建）**。

步骤 4：一旦您创建了设备别名，点击 **CFS > Commit（提交）**。相关变更将被写入数据库。

选项 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：键入 **exit** 。这会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# sh 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：

- 将分区配置为每个分区一个启动器和一个目标。
- 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。

分区可使用 CLI 和阵列管理器进行配置。

选项 1：使用 CLI 配置分区

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。

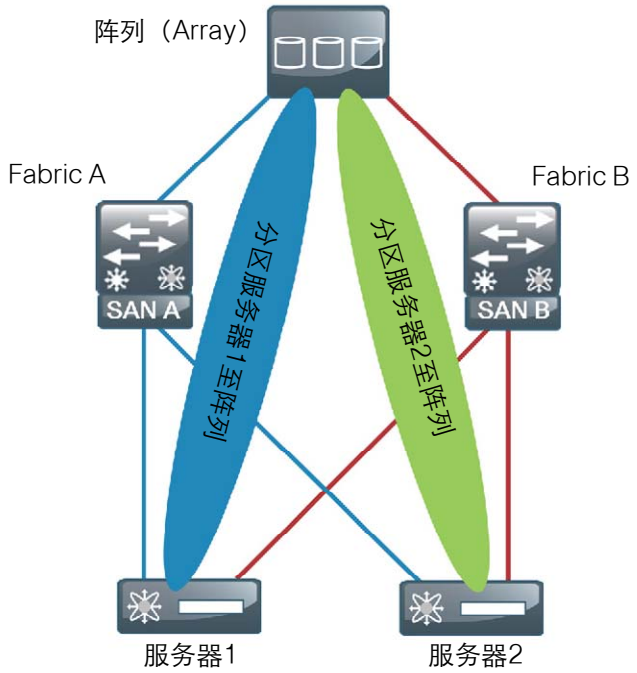
```
member device-alias emc-2-a0-fc
member pwwn 20:00:00:25:b5:77:77:9f
```

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。这可为将您的光纤通道 SAN 扩展到多台交换机做好准备。

```
zoneset distribute full vsan 4
```

选项 2. 通过使用 Data Center Network Manager（数据中心网络管理器），配置分区

步骤 1：安装支持 SAN Essentials 的 Cisco Data Center Network Manager（思科数据中心网络管理器）。

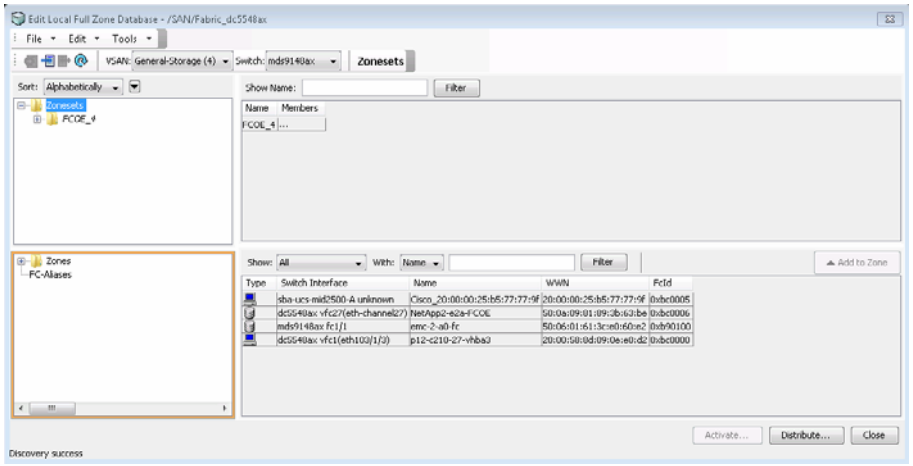
读者提示

Cisco DCNM-SAN Essentials 版本免费提供，用于管理 Cisco Nexus 和 MDS SAN 交换机，可从 http://www.cisco.com 下载。DCNM-SAN Essentials 可替代以前的思科阵列管理器产品。

步骤 2：登录 DCNM-SAN 管理器。默认用户名和密码是 admin/password。

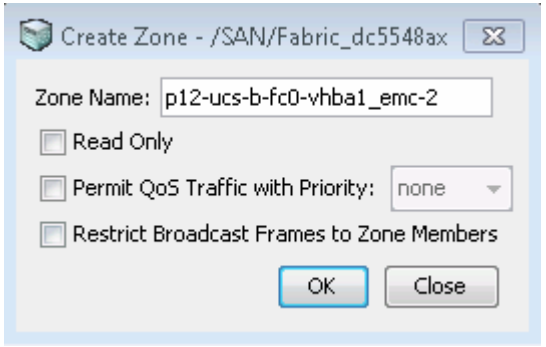
步骤 3：通过输入第一个 Cisco Nexus 5500UP 的 IP 地址（例如 10.10.63.10）选择一个种子交换机，然后从列表中选择 Cisco Nexus 5500UP。

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

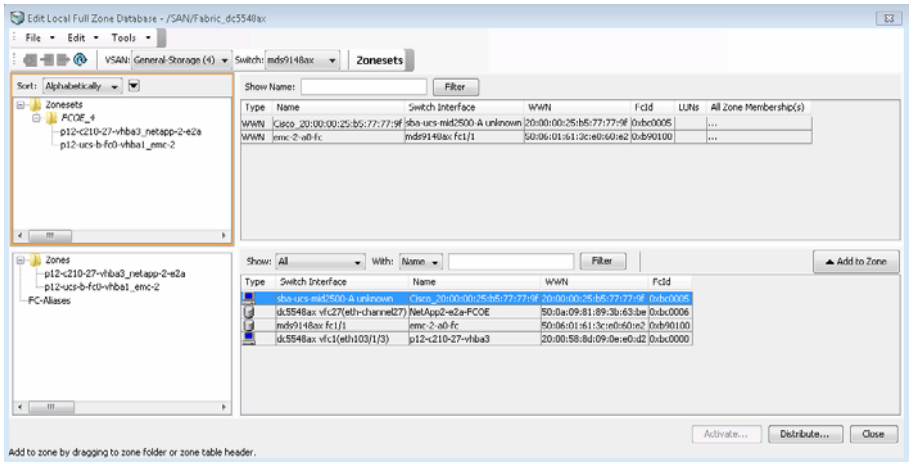


步骤 5：在 Zone Database（分区数据库）窗口的左侧，右击 **Zones（分区）**，然后点击 **Insert（插入）**。这将创建一个新分区。

步骤 6：在 Zone Name（分区名称）框中，键入新分区名称，然后点击 **OK**。



步骤 7：选择新分区，然后从数据库窗口右侧的底部，选择您想加入此分区的启动器或目标。点击 **Add to Zone（添加到分区）**。

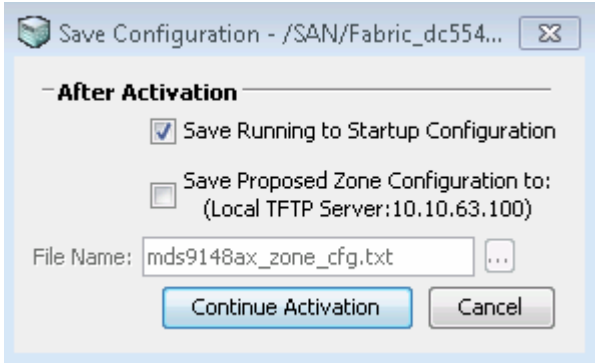


步骤 8：右击 **Zoneset（分区集）**，插入一个新的分区集。

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

步骤 10：点击 **Activate（激活）**。这可激活配置的分区集。

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）**，然后点击 **Continue Activation（继续激活）**。



步骤 12：使用本流程中的程序以相同方式配置 SAN B，以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：验证光纤通道登录。

在光纤通道阵列中，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 命令显示思科光纤通道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 命令测试光纤通道可达性，并使用 fctrace 命令跟踪到主机的路线。

技术提示

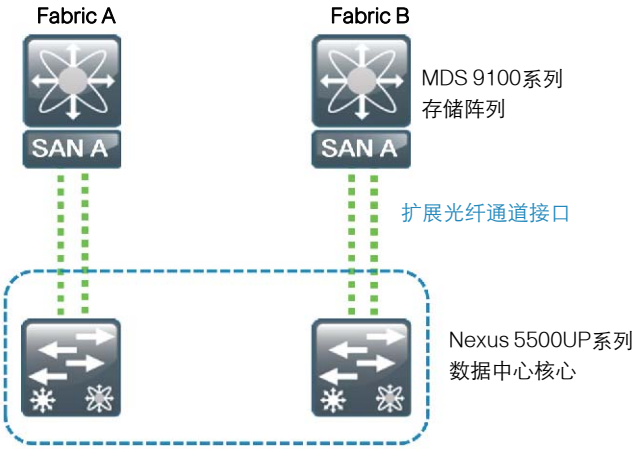
思科创建的这些命令为使用 ping 和 traceroute 的个人提供了熟悉的存储网络故障排除工具。

流程

配置 Cisco MDS 9148 交换机 SAN 扩展

1. 为 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 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 : 10.10.63.12
    Mgmt0 IPv4 netmask : 255.255.255.128
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : 10.10.63.1
  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 : 10.10.48.17
  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 10.10.63.12 255.255.255.128
    no shutdown
  ip default-gateway 10.10.63.1
  ssh key rsa 2048 force
  feature ssh
  no feature telnet
  feature http-server
  ntp server 10.10.48.17
  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

网络时间协议（NTP）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 10.10.63.13，运行第二个 Cisco MDS 9100 交换机的设置脚本。

步骤 3: 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
```

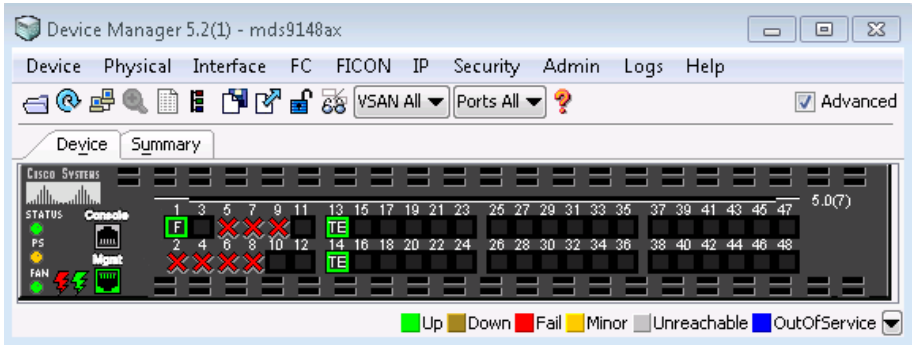
步骤 4: 配置时钟。在设置模式中，您配置了 NTP 服务器地址。在此步骤中，通过配置时钟，使时钟使用 NTP 时间作为参考，并使交换机输出匹配本地时区。

```
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

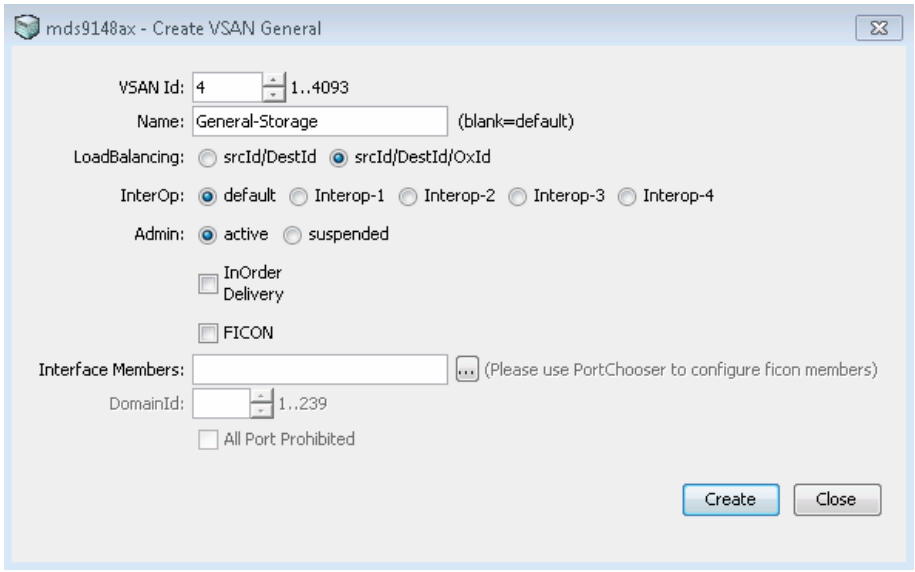
要配置 Cisco MDS 交换机，以扩展您基于 Cisco Nexus 5500UP 交换机构建的光纤通道 SAN，请分别为 SAN A 和 SAN B 使用同一 VSAN 编号。CLI 和 GUI 工具对于 Cisco MDS 和 Cisco Nexus 5500UP 的工作方式相同。

步骤 1：在 Device Manager（设备管理器）中，点击 **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：点击 **Create（创建）**。

上述步骤在 CLI 中应用以下配置。

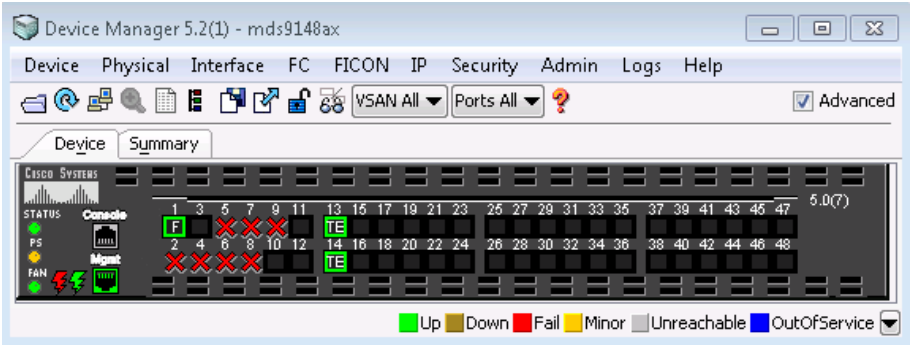
```
vsan database
vsan 4 name “General-Storage”
```

步骤 4：使用上述步骤 1 至步骤 3，采用 vsan **5** 和 vsan 名称 **General-Storage** 配置第二个 MDS SAN 交换机。

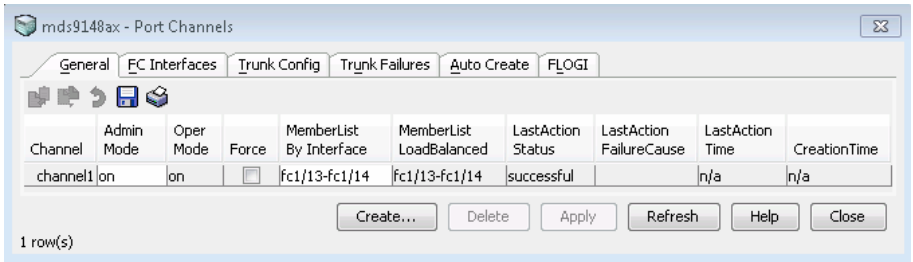
程序 3　为 SAN 互联配置中继

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

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

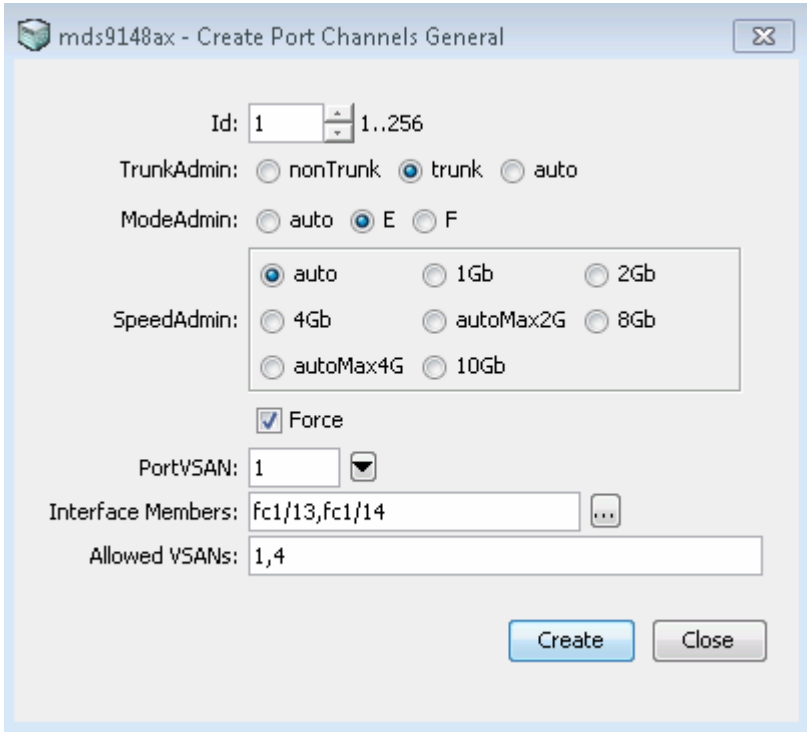


步骤 2：在 Device Manager（设备管理器）屏幕，点击 **Interfaces（接口）> Port Channels（端口通道）**，然后点击 **Create（创建）**在 Cisco MDS 上配置中继端口。

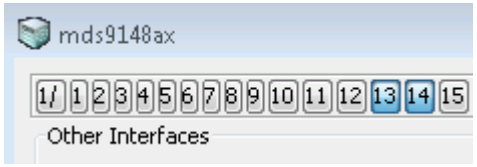


步骤 3：选择端口通道 Id 号，选择 **trunk（中继）**，选择模式 **E**，然后选择 **Force（实施）**。

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，点击…，然后选择将属于此端口通道的 **Interface Members（接口成员）**。



步骤 6：点击 **Create（创建）**。新端口通道创建完成。

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
interface fc1/14
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated
```

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
interface fc1/14
  switchport mode E
  channel-group 1 force
  switchport rate-mode dedicated
```

步骤 7：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
  channel-group 31 force
  no shutdown

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

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

步骤 8：将在 Cisco Nexus 5500UP 交换机上创建的分区数据库分配到新的 MDS 9100 交换机。

针对 SAN-A 配置 Cisco Nexus 5500UP CLI，以向全新 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 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

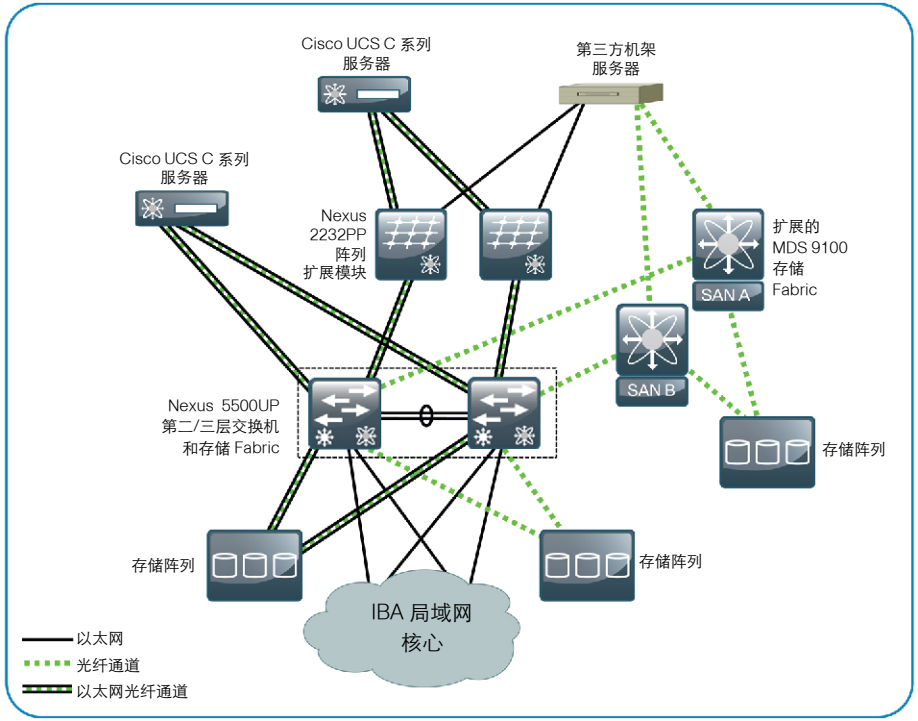
Cisco UCS C 系列机架服务器标配板载 10/100/1000 以太网适配器和一个使用 10/100 以太网端口的思科集成管理控制器（CIMC）。为充分利用机架服务器和最大限度减少 IBA 智能业务平台统一计算架构的布线，Cisco UCS C 系列机架安装式服务器连接至一个统一阵列。用于将 Cisco UCS 5100 系列刀片服务器机箱连接到网络的 Cisco Nexus 5500UP 系列交换机也可用于通过万兆以太网扩展光纤通道流量。Cisco Nexus 5500UP 系列交换机能够将 I/O 整合到一组万兆以太网线缆上，消除冗余适配器、线缆和端口。通过使用以太网光纤通道（FCoE），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

在思科 IBA 智能业务平台中小企业数据中心架构中，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 的服务器需要光纤通道端口许可证。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 的端口提供光纤通道端口许可证。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 上行链路使用光纤通道端口许可证。

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光纤通道连接。下图显示了采用混合统一阵列、标准以太网和光纤通道连接的拓扑结构，以及可选的支持光纤通道扩展的 Cisco MDS 9100 系列。



Cisco UCS C 系列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，您可将思科 IMC 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 Nexus 5500UP 配置

在上述部分，我们启用了 Cisco Nexus 5500UP 系列 FCoE 功能。在本部分，我们将配置以下项目，允许 Cisco C 系列服务器使用 FCoE 进行连接：

- 创建一个虚拟光纤通道接口
- 将 VSAN 分配到虚拟光纤通道接口
- 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：在全局配置模式中键入以下命令，配置 FCoE QoS。

技术提示

系统有四行 QoS 声明，与针对 FCoE 的现有系统 QoS 策略对应。没有这些命令，虚拟光纤通道接口在激活时将不会发挥作用。

```
system qos
service-policy type qos input fcoe-default-in-policy
service-policy type queuing input fcoe-default-in-policy
service-policy type queuing output fcoe-default-out-policy
service-policy type network-qos fcoe-default-nq-policy
```

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。

- 在本例中，VLAN 304 被映射到 VSAN 4。VLAN 304 通过面向第一个 Cisco Nexus 5500UP 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 中，VLAN 305 被映射到 VSAN 5。

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

步骤 2：创建支持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 接口映射到光纤通道。

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。

- 在本示例中，在第一个 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 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 Nexus 5500UP 交换机的配置。

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

- 本示例显示了第二个 Nexus 5500UP 交换机的配置。

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

步骤 5：在 C 系列服务器上配置 VSAN。

技术提示

使用 Cisco P81E CNA 的 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，从而连接到光纤通道阵列。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《面向中小企业的思科 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，验证虚拟光纤通道接口的状态。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 交换机上当前的光纤通道登录数据库中。

```
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。光纤通道名称服务器数据库显示 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]
```

现在您可根据先前的光纤通道配置部分来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中小企业数据中心时，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。思科虚拟端口通道和阵列扩展模块技术广泛用于思科 IBA 智能业务平台中小企业数据中心架构中，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，来配置和管理服务器、网络接口、存储接口、以及其即时连接的网络组件。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，并使中小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。

在将服务器连接到数据中心网络之前，关于 Cisco Nexus 虚拟端口通道和 Cisco Nexus 阵列扩展模块等可增强连接选件的部分特性的说明已经准备就绪。

Cisco Nexus虚拟端口通道

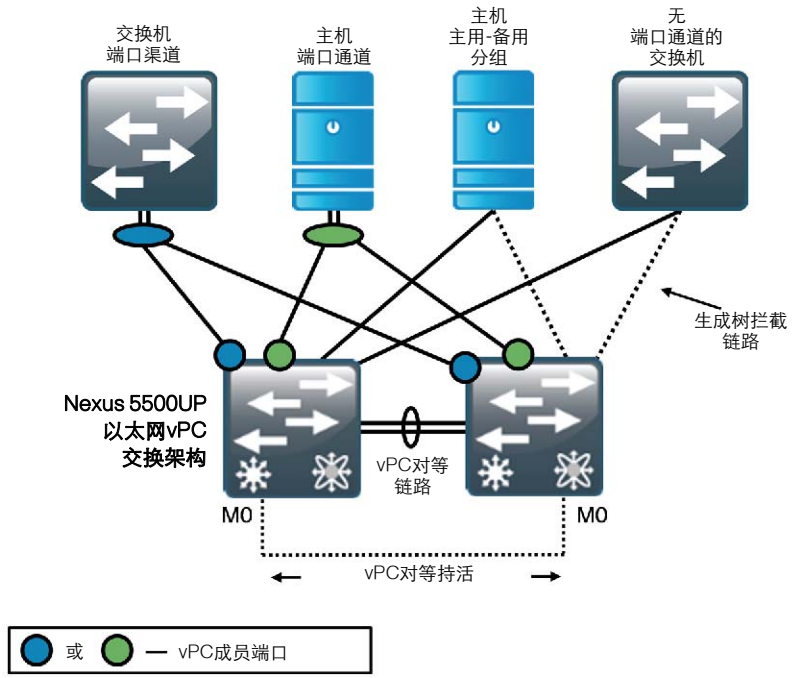
正如以太网基础设施模块中所述，虚拟端口通道（vPC）允许物理连接到两个不同 Cisco Nexus 交换机的链路，针对第三方下游设备显示为来自单一设备，并作为单一以太网端口通道的一部分。这个第三方设备可以是服务器、交换机，或其它任何支持 IEEE 802.3ad 端口通道的设备。对于 Cisco EtherChannel 技术，术语“多机箱 EtherChannel”（MCEC）即指该技术。MCEC 从相连的设备连接到数据中心核心层，提供生成树无环路拓扑结构，允许 VLAN 在中小企业数据中心扩展，并保持永续架构。

vPC 由两个 vPC 对等交换机组成，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。下图阐述了 vPC 端口和孤立端口：

图 13. 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 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。

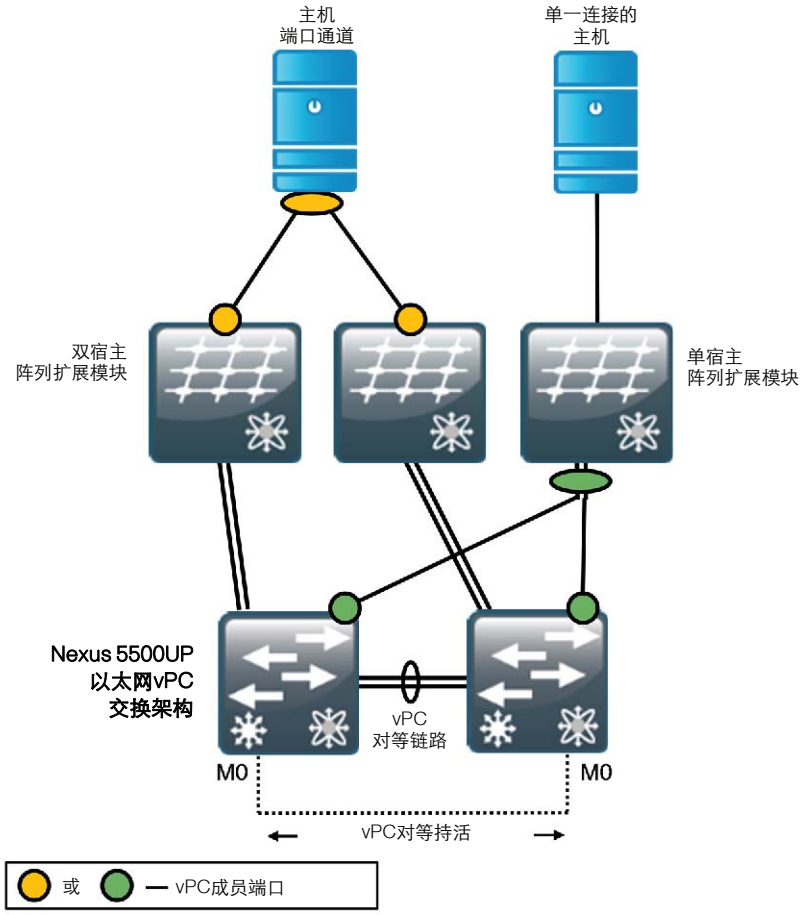
针对 Cisco Nexus 5500UP 交换机进行的全面 vPC 域编程在本文程序 3“ 配置虚拟端口通道（vPC）”中进行详细说明。

Cisco Nexus阵列扩展模块

如本文以太网基础设施模块部分中所述，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 14. 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 4-8 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 4-8 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 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，在本文以太网基础设施模块中进行了详细介绍。

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。

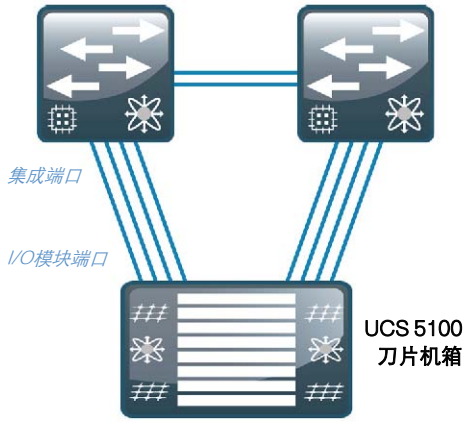
Cisco UCS B 系列刀片机箱系统组件

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 6100 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 2100 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 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 15. Cisco UCS 刀片系统组件连接



Cisco UCS Manager

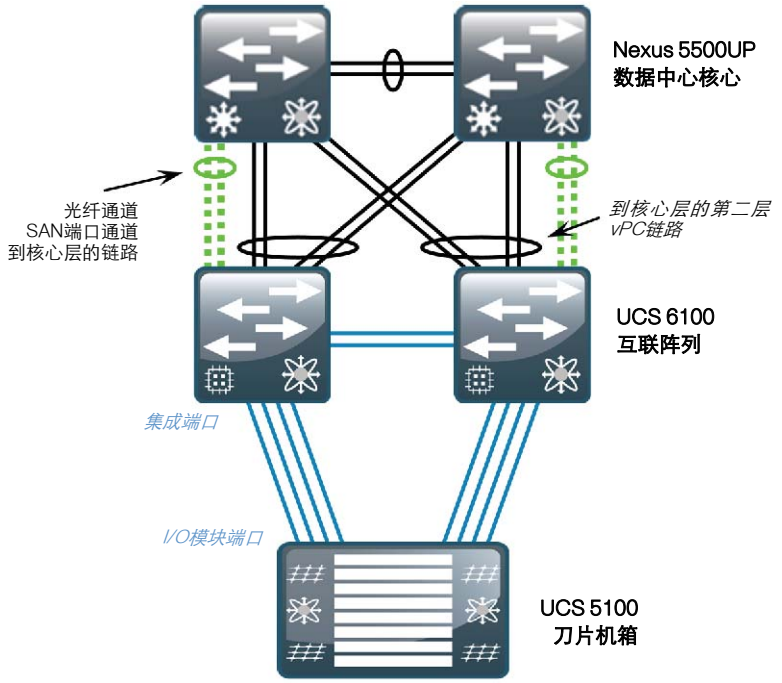
Cisco UCS Manager 是驻留在互联阵列上的嵌入式软件，为 UCS 系统中的所有组件提供了全面的配置和管理功能。该配置信息在两个互联阵列间复制，为这一关键功能提供了一款高度可用的解决方案。访问 Cisco UCS Manager，以完成简单任务的最常用方式就是使用 Web 浏览器打开基于 Java 的 GUI。为支持对系统进行命令行和编程操作，该系统还提供了一个 CLI 和一个 XML API。

Cisco UCS B 系列系统网络连接

Cisco UCS 6100 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，且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 系统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 16 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 16. 到核心的 UCS 互联阵列



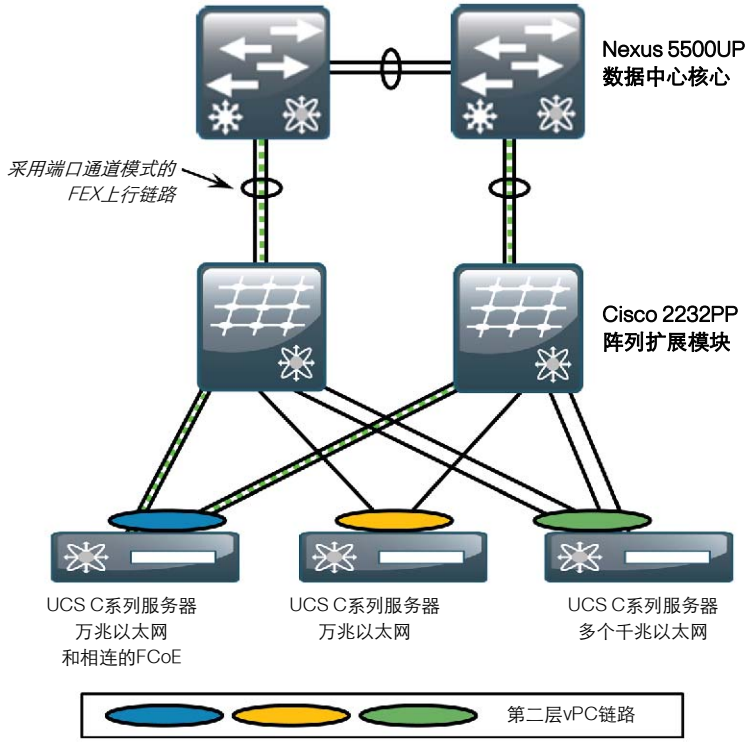
Cisco UCS B 系列部署的详细配置可在《面向中小企业的思科 IBA 智能业务平台——数据中心统一计算系统部署指南》中找到。

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 17 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 17. Cisco UCS C 系列 FEX 连接示例



在以上的图 17 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），以便保持光纤通道传输的误码率（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 和光纤通道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，通常为光纤通道 SAN 流量。

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。

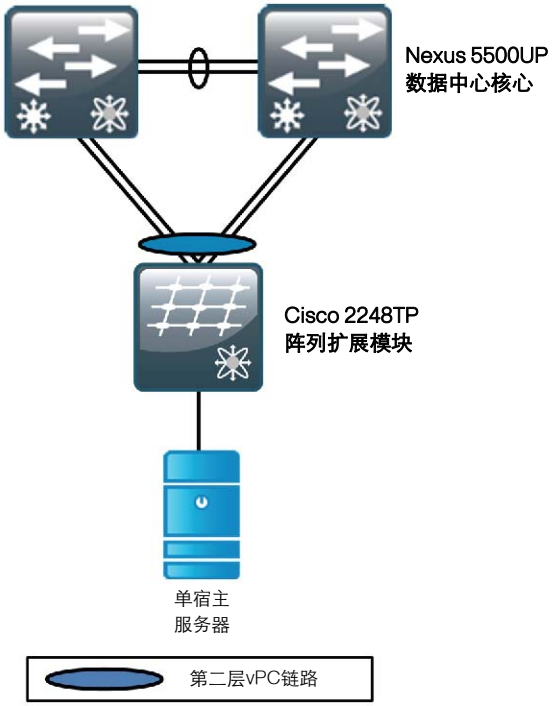
具有多个千兆以太网的 Cisco UCS C 系列服务器使用 vPC 在采用 EtherChannel 的多个链路之间进行流量负载均衡。使用 vPC 并非一项要求。在需要独立服务器接口的非 vPC 服务器连接中，除非服务器操作系统提供永续连接性，否则连接至双宿主 Cisco FEX 可作为提供永续性的首选方式。

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模块中找到。有关 Cisco UCS C 系列部署的详细配置，可在《面向中小企业的思科 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 18. 单宿主服务器与双宿主 Cisco FEX 之间的连接

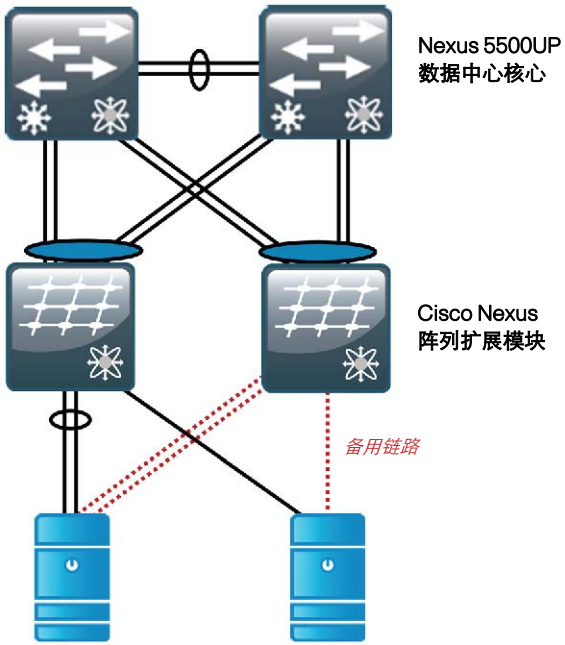


Cisco Nexus 2248TP FEX 的 vPC 连接为连接至相同 Cisco FEX 的服务器提供控制平面和数据平面冗余性。当阵列上行链路或 Nexus 5500UP 核心交换机出现故障时，该拓扑可为相连的服务器提供永续性，但是当 Nexus 2248TP 故障时无法提供冗余性。所有连接至 vPC 双宿主 Cisco FEX 的服务器都采用 vPC 连接，并且必须在每个数据中心核心 Nexus 5500UP 交换机上进行配置。虽然这种方式可以添加永续性，但托管重要应用的单宿主服务器仍应迁移至双宿主连接，以便提供充足的永续性。

具有分组接口连接性的服务器

服务器网络接口卡（NIC）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 UCS C 系列连接性部分中包括的 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 19. 具有主用/备用 NIC 的服务器与 Cisco FEX 之间的连接



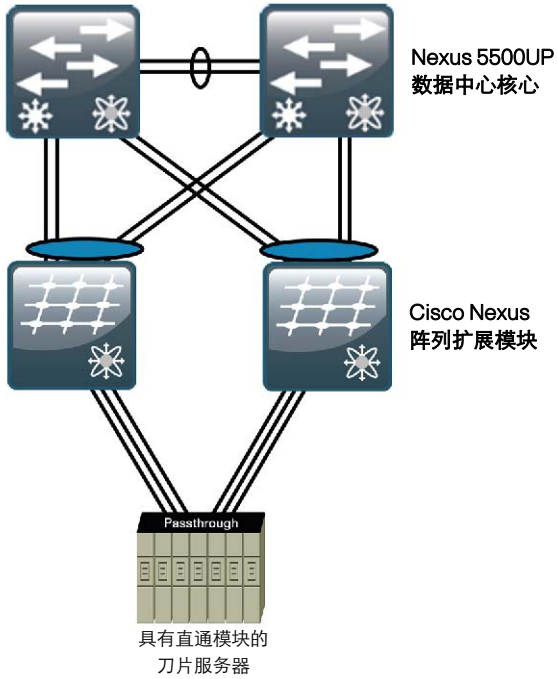
来自 Cisco Nexus 2248TP FEX 的 vPC 连接为连接至每个 Cisco FEX 的服务器提供控制平面和数据平面冗余性。当阵列上行链路或 Nexus 5500UP 核心交换机出现故障时，该拓扑可为相连的服务器提供永续性。当 Cisco FEX 出现故障时，NIC 分组将切换至备用接口。

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 智能业务平台中小企业数据中心架构。

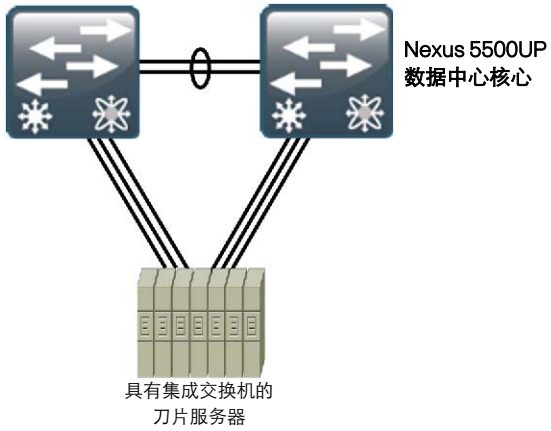
第一个选项是使用具有直通模块的刀片服务器系统，该模块将服务器接口直接扩展至刀片服务器机箱以外，无需在刀片服务器系统中使用内部交换架构。当使用直通模块时，服务器 NIC 连接可以使用 Cisco Nexus 阵列扩展模块来支持高密度端口扇出和永续性连接，如下图所示。

图 20. 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 智能业务平台中小企业数据中心架构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 21 中所示。

图 21. 具有集成交换机的第三方刀片服务器系统



总结

本章节中列出的计算连接选项介绍了思科 IBA 智能业务平台中小企业数据中心基础架构如何与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《面向中小企业的思科 IBA 智能业务平台——数据中心统一计算系统部署指南》。

备注

网络安全性

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。

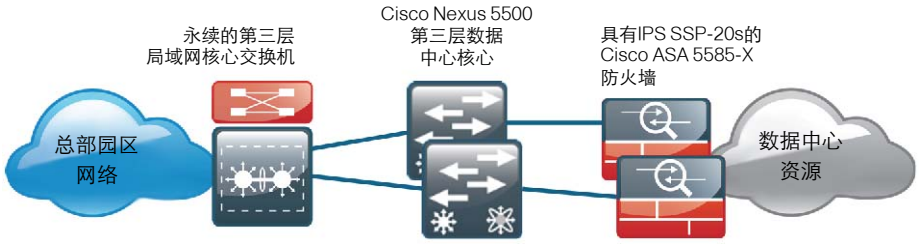
为确保数据中心内重要电子资产的安全，要通过网络安全手段对机构加以保护，防御自动或人为的窃取和篡改，并防止主机遭受消耗大量资源的蠕虫、病毒或僵尸网络的破坏。

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 22. 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
- 远程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。

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 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。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。

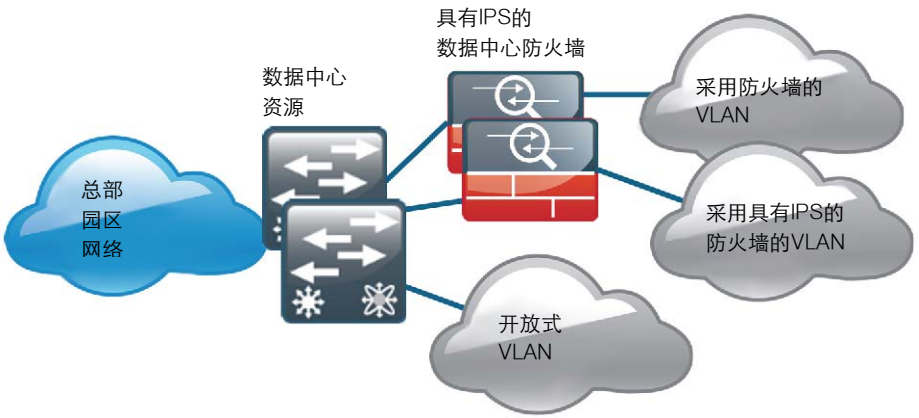
Cisco ASA 以路由模式进行配置；因此，安全网络必须位于一个与客户端子网不同的子网中。如果 Cisco ASA 以透明模式部署，IP 子网分配将会得到简化；但是主机可能会在无意中被连接至错误的 VLAN，而它们仍然能够与网络进行通信，从而导致意外的安全暴露。

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 23. 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 均在逻辑上通过第三层连接至流经 Cisco ASA 的网络的其余部分，因此只能通过穿越 Cisco ASA 抵达。

安全策略制定

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。

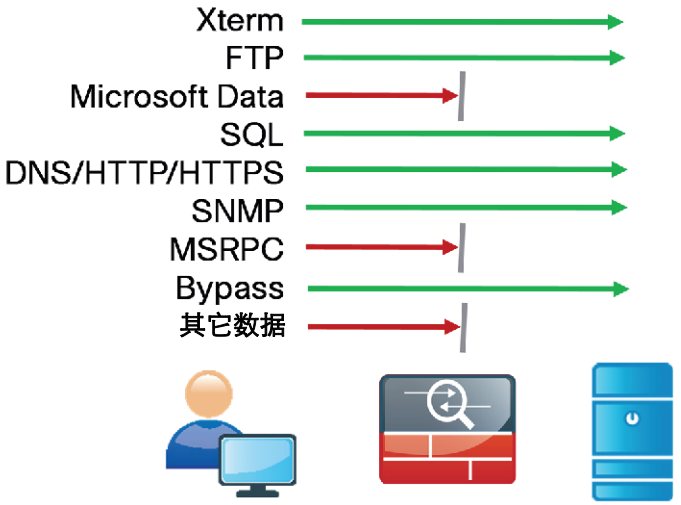
为了在企业网络的各个职能分区间高效地部署安全策略，您应当尽可能获得有关预期网络行为的最详细信息。您掌握的预期网络行为信息越详细，您就越能够出色地定义安全策略，在优化安全性的同时满足企业在应用流量和性能方面的要求。

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。

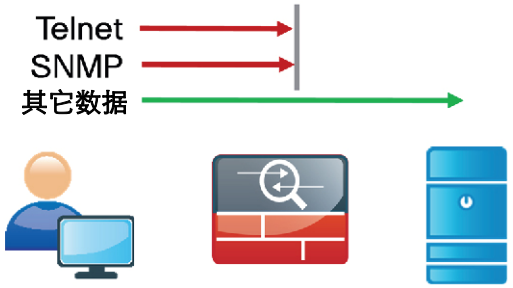
网络安全策略基本可分为两种：“白名单”策略和“黑名单”策略。白名单安全策略提供更加含蓄的安全做法，它会拦截除支持应用所需外的所有流量（在足够精细的级别）。因为只有开展业务所需的流量才会得到许可，因此白名单通常能够更好地满足管制要求。其他流量将被拦截，无需对其进行监控即可确保没有非法活动发生。这将减少将转发至 IDS 或 IPS 的数据量，并能最大限度减少在发生入侵事件或数据丢失时必须浏览的日志条目的数量。

图 24. 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 25. 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。

备注

部署详情

数据中心安全部署通过三个独立的流程来实现：

- Cisco ASA 防火墙连接，在 Cisco ASA 防火墙和 Cisco Nexus 5500UP 数据中心核心层间建立网络连接。
- Cisco ASA 防火墙策略讨论与配置，概括了识别安全策略需求和应用配置以满足要求所需的流程。
- 思科 IPS 连接与策略配置，在一个流程中集成了连接和策略配置。

流程

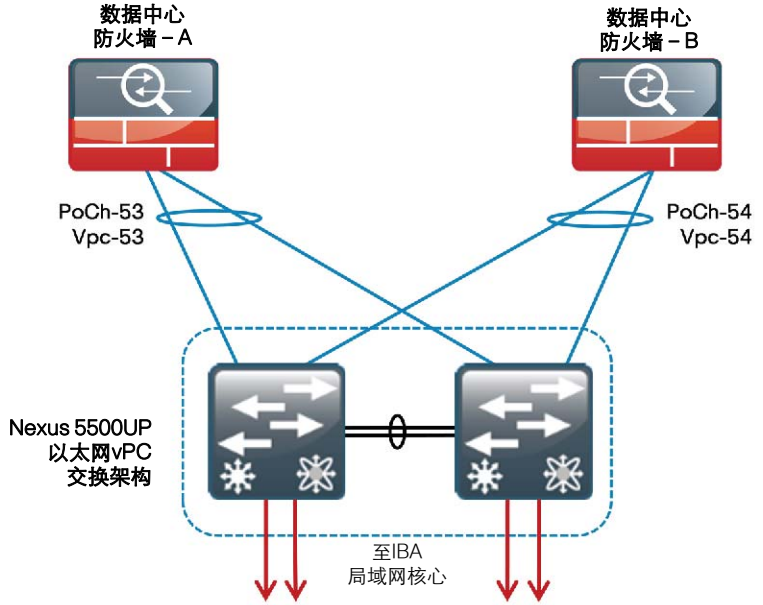
配置 Cisco ASA 防火墙连接

1. 在 Nexus 5500s 上配置端口通道
2. 初始 ASA 配置
3. 配置防火墙连接性
4. 配置路由
5. 配置 Cisco ASA 支持高可用性

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 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 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。

程序 1　在 Nexus 5500s 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：在两个 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。

- 配置第一个 Cisco Nexus 5500UP 交换机。

```
interface Ethernet1/1
  description DC5585a Ten0/8
  channel-group 53 mode active

interface Ethernet1/2
  description DC5585b Ten0/8
  channel-group 54 mode active
```

- 配置第二个 Cisco Nexus 5500UP 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
```

当您向物理接口分配通道组时，会创建将在下一个步骤中配置的逻辑 EtherChannel（端口通道）接口。

步骤 2：为两个数据中心核心交换机配置逻辑端口通道接口。与端口通道绑定的物理接口将继承逻辑端口通道接口的设置。

```
interface port-channel53
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  vpc 53

interface port-channel54
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  vpc 54
```

端口通道将作为 vPC 端口通道创建，因为阵列接口是与两个 Nexus 5500UP 数据中心核心交换机相连的双宿主 EtherChannel。

程序 2　初始 ASA 配置

连接至 Cisco ASA 防火墙控制台，并执行以下全局配置。

步骤 1：配置 Cisco ASA 主机名称，以便于轻松识别。

```
hostname DC5585ax
```

步骤 2：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 3：配置本地用户身份验证。

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

步骤 4：配置启用密码。

```
enable password [password]
```

步骤 5：配置域名。

```
domain-name cisco.local
```

步骤 6：配置管理访问。

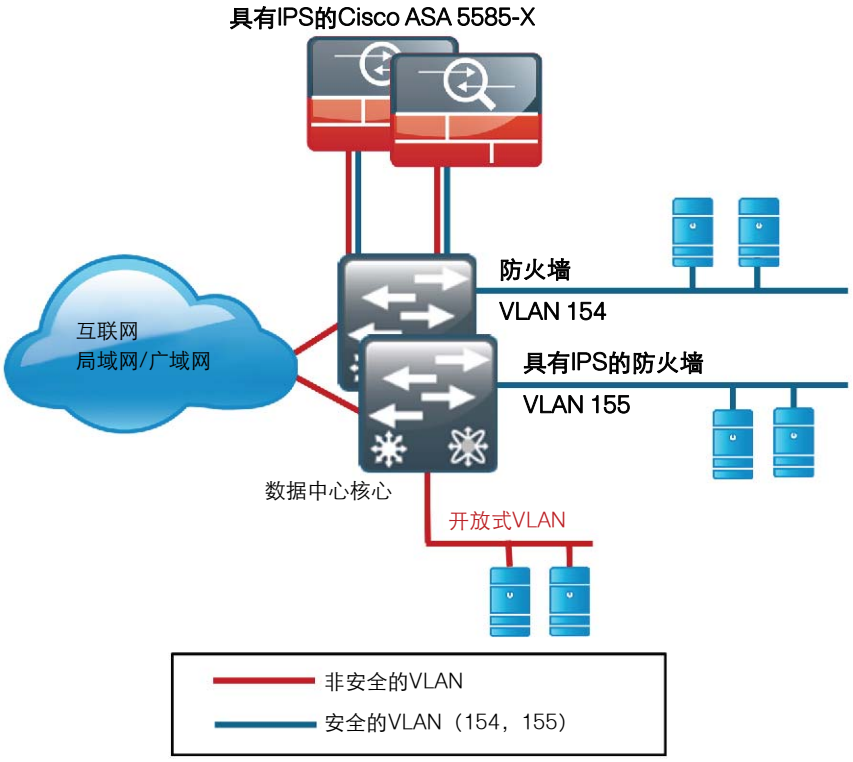
```
http server enable
http 10.0.0.0 255.0.0.0 outside
```

步骤 7：配置网络时间协议(NTP)服务器地址 NTP 用于同步网络中所有设备上的时间，以便进行故障排除。

```
ntp server 10.10.48.17
```

程序 3　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 TenGigx/x/x
 channel-group 10 mode passive
 no shutdown
!
interface TenGigabitEthernet0/9
 description Trunk to DC5548x TenGigx/x/x
 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 VLAN 154 内部，以及具有 IPS VLAN 155 的防火墙内部。

```
interface Port-channel10.153
 description DC VLAN Outside the FW
 vlan 153
 nameif outside
 security-level 0
 ip address 10.10.53.126 255.255.255.128 standby 10.10.53.125
 no shutdown
!
interface Port-channel10.154
 description DC VLAN Inside the Firewall
 vlan 154
 nameif DC-InsideFW
 security-level 75
 ip address 10.10.54.1 255.255.255.0 standby 10.10.54.2
 no shutdown
!
```

```
interface Port-channel10.155
 description DC VLAN Inside the FW w/ IPS
 vlan 155
 nameif DC-InsideIPS
 security-level 75
 ip address 10.10.55.1 255.255.255.0 standby 10.10.55.2
 no shutdown
```

程序 4　配置路由

因为 Cisco ASA 是通往服务器机房安全 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 Nexus 交换机的 HSRP 地址。

在数据中心核心 Cisco Nexus 5500s 上也需要配置静态路由，以便将目的地为安全 VLAN 的流量路由至 Cisco ASA。这些路由还需要注入 EIGRP 中，以便允许其通过网络传播。

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 10.10.53.1 1
```

步骤 2：在数据中心核心 Nexus 5500s 上，配置指向防火墙后安全子网的静态路由，并将子网重新分发至 EIGRP 路由进程。

```
route-map static-to-eigrp permit 10
  match ip address 10.10.54.0/24
route-map static-to-eigrp permit 20
  match ip address 10.10.55.0/24
router eigrp 1
   redistribute static route-map static-to-eigrp
ip route 10.10.54.0/24 Vlan153 10.10.53.126
ip route 10.10.55.0/24 Vlan153 10.10.53.126
```

程序 5　配置 Cisco ASA 支持高可用性

思科 ACE 防火墙经过配置可提供主用—备用高可用性。

步骤 1：定义主用防火墙的故障切换配置。以“failover polltime”开头的两行配置可缩短默认的故障切换时间间隔，实现一秒之内的迅速切换。减少故障切换次数降低了运行中断期间对应用和用户的影响。但是，我们不建议将故障切换时间间隔缩短到这些值以下：

```
interface GigabitEthernet0/1
 description LAN/STATE Failover Interface
 no shutdown
!
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/1
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key [key]
failover replication http
failover link failover GigabitEthernet0/1
failover interface ip failover 10.10.53.130 255.255.255.252
standby 10.10.53.129
```

步骤 2：定义备用防火墙的故障切换配置。故障切换键值必须在配置为主用—备用高可用性对的两台设备上匹配。请注意，这不是设备上存在的配置，但是该配置将应用于未配置的 Cisco ASA，以便使其故障切换至设备对中的备用设备。

```
interface GigabitEthernet0/1
 no shutdown
!
failover
failover lan unit secondary
failover lan interface failover GigabitEthernet0/1
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key [key]
failover replication http
failover link failover GigabitEthernet0/1
failover interface ip failover 10.10.53.130 255.255.255.252
standby 10.10.53.129
```

步骤 3：添加该配置，以便当 DC VLAN 中失去连接时，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
```

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

本节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要求。

- 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。

选项 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：输入以下配置进行访问控制，确保只有特定的主机能够被访问。

```
object network BladeWeb1Secure
 host 10.10.54.100
 object network BladeWeb2Secure
 host 10.10.55.100
object network Secure-Subnets
 subnet 10.10.54.0 255.255.255.0
object network SecureIPS-Subnets
 subnet 10.10.55.0 255.255.255.0
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：您可以指定特定用户（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 10.10.48.224-255 中的管理主机被允许通过 SSH 和 SNMP 访问数据中心子网。

```
object network Mgmt-host-range
 range 10.10.48.224 10.10.48.254
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：（可选）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
```

选项 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；所有其他访问将由上一节中所讨论的旁路规则处理。

步骤 1： 允许针对将分配给 IT 人员的特定地址范围的 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 Mgmt-host-range
 range 10.10.48.224 10.10.48.254
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： 配置旁路规则，允许任何未被明确拒绝的应用流量通过。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 Bypass-Rule log disable
```

步骤 4： 保存您的 Cisco ASA 防火墙配置。

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

流程

部署思科入侵防御系统(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 传感器主要关注获得许可通过防火墙，但意图发起攻击的网络和应用流量。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。

混杂与内嵌（Inline）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性等具体因素。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 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，它能够直接丢弃数据包。这使得 IPS 设备具有较高的实际防御攻击的能力。

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 的安全性以及数据包丢弃能力时，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。

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。一旦这些关键的数据被输入，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一个传感器能在其中路由流量或直接连接管理站的数据中心管理 VLAN 相连。

步骤 1： 在 5585 的前面板上，通过 IPS SSP 模块上的串行控制台连接至 IPS 硅交换处理器(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 模块的命令行界面，通过键入 **Setup** 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。

```
--- 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]:
10.10.63.21/24,10.10.63.1
```

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。对于中小企业—2500 网络，总部子网 (10.10.0.0/16) 中的所有地址将被允许。在空白 Permit: 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: 10.10.0.0/16
```

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]:
```

注意以下几点：

- 全局关联被禁用，直至配置流程的最后环节。
- 对于根据《面向中小企业的思科 IBA 智能业务平台——无边界网络基础部署指南》配置的网络，无需 HTTP 代理服务器地址。
- 您将在传感器的 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>.
```

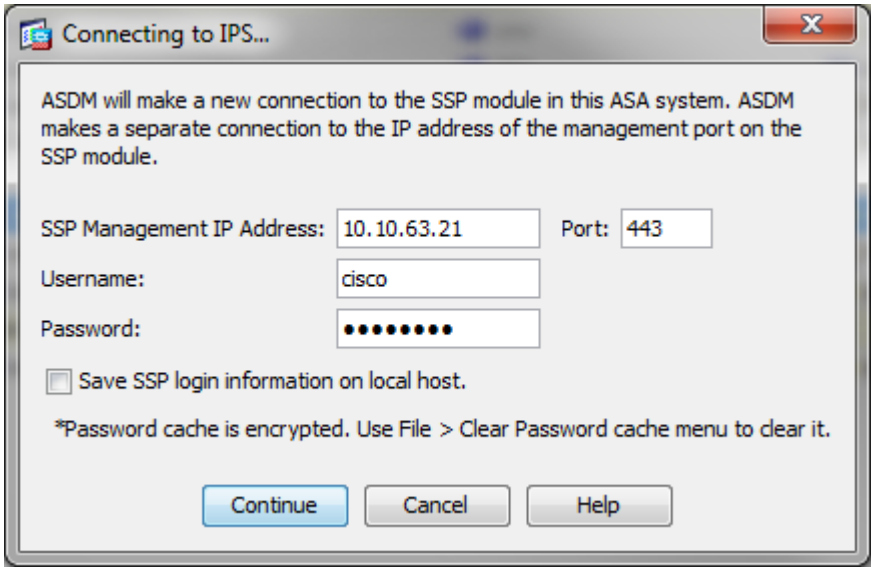
步骤 10：针对在其它 Cisco ASA 机箱中安装的 IPS 传感器，重复程序 1 步骤 1 至步骤 9。确保在另一个传感器的管理接口上使用不同的 IP 地址。

程序 2　完成基本配置

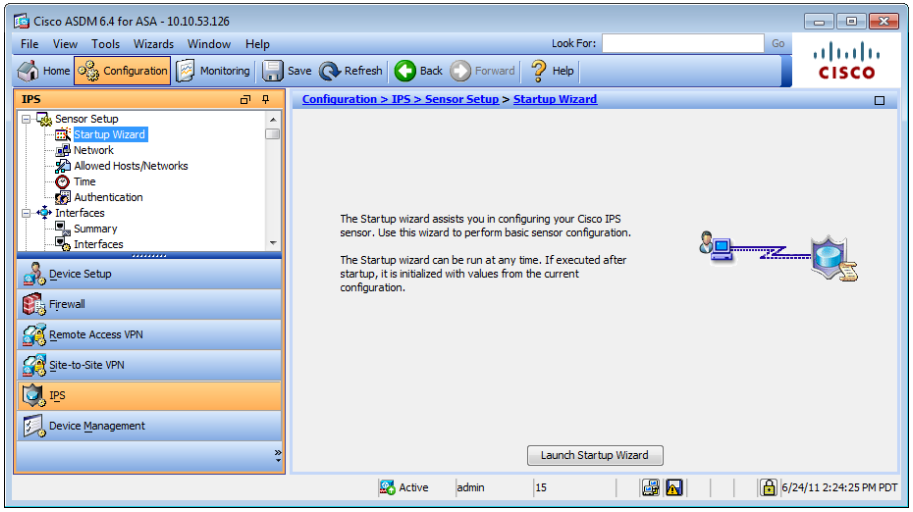
当 System Configuration（系统配置）对话框中的基本设置完成后，您将使用集成管理工具思科自适应安全设备管理器(ASDM)中的启动向导，以便完成剩余任务，进行基本 IDS 配置：

- 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

步骤 1：通过在 Cisco ASDM 中转至 **IPS** 选项卡并输入所需的连接信息，连接传感器。



步骤 2：转至 **Sensor Setup（传感器设置）** > **Startup Wizard（启动向导）**，然后点击 **Launch Startup Wizard（运行启动向导）**。



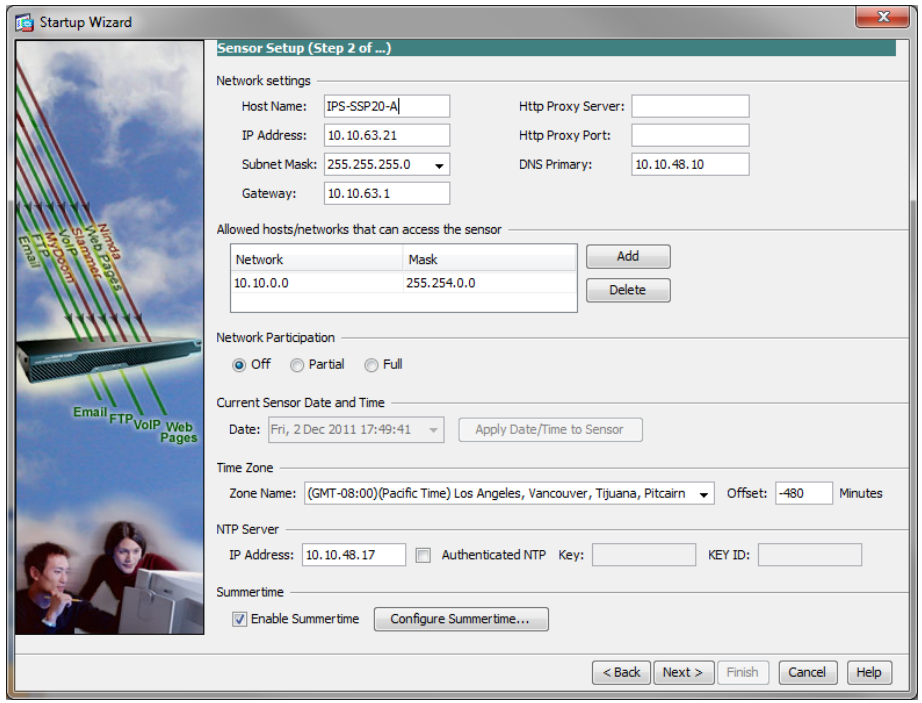
步骤 3：查看 Startup Wizard Introduction（启动向导介绍），然后点击 **Next（下一步）**。

步骤 4：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。

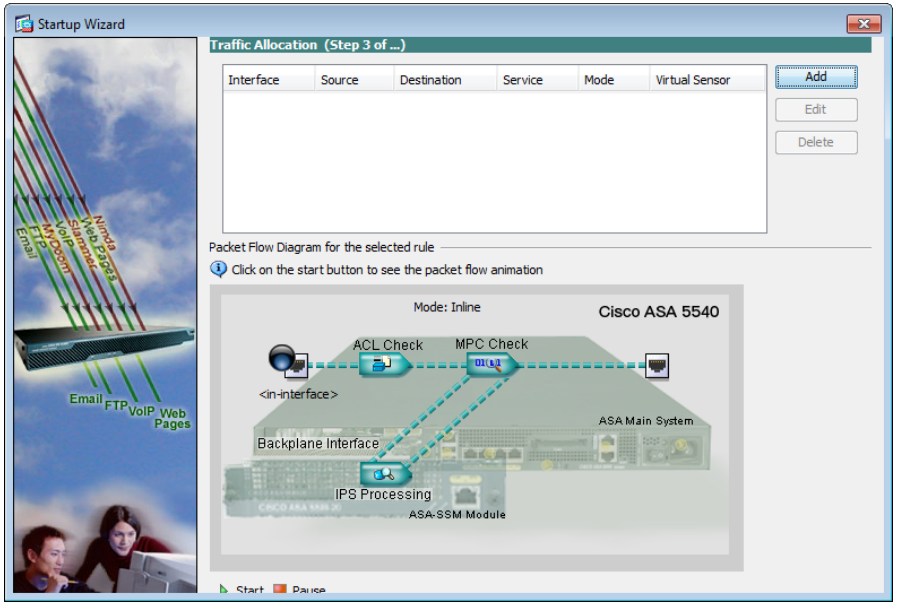
技术提示

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。

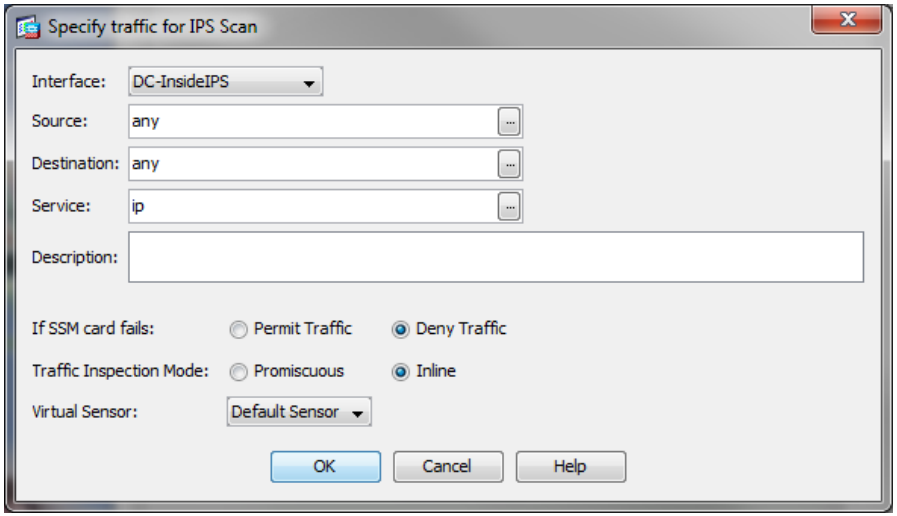
步骤 5：如果您的时区需要，选择 **Enable Summertime（启用夏令时）**。确保没有选择 **Authenticated NTP（身份验证 NTP）**，然后点击 **Next（下一步）**。



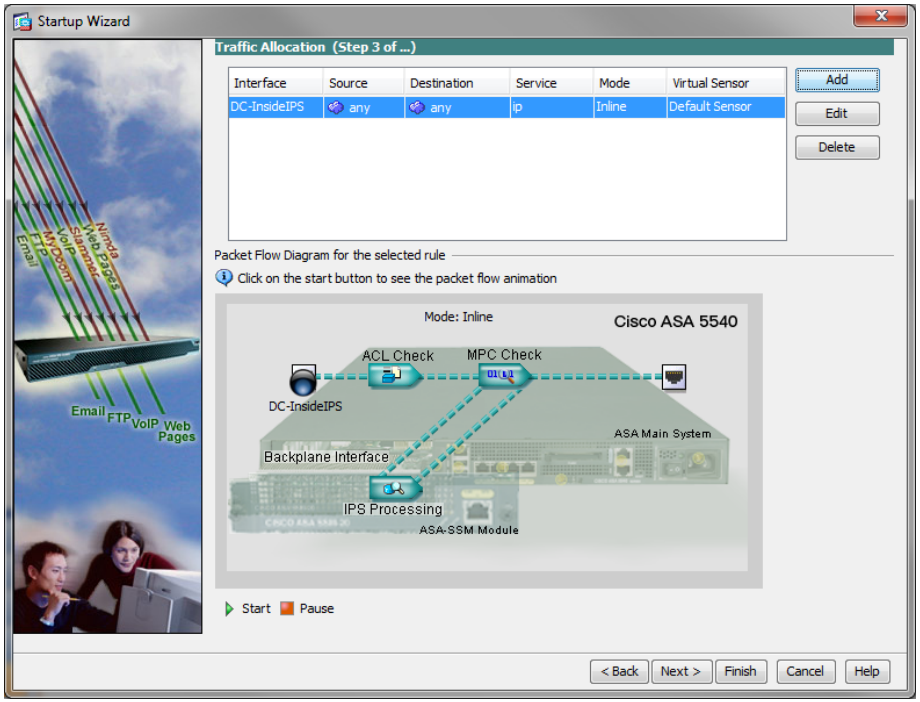
步骤 6：在 Traffic Allocation（流量分配）窗口，点击 **Add（添加）**。



步骤 7：在 **Specify traffic for IPS Scan（指定 IPS 扫描流量）**窗口中，在 **Traffic Inspection Mode（流量检测模式）**旁选择 **Inline（内嵌）**，然后点击 **OK。请注意**，如果 Cisco ASA 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。

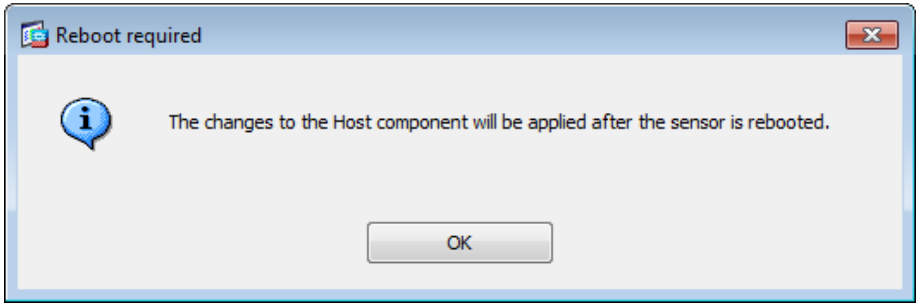


步骤 8：在 Traffic Allocation（流量分配）页，在 **Packet Flow Diagram for the selected Rule（已选规则的数据包流量图）**面板中，通过点击 **Start（开始）**验证流量分配配置。动画将演示数据包被复制到 IPS 模块和出口接口。此动画显示的平台可能并非您正在配置的平台。



步骤 9：在 **Startup Wizard（启动向导）**界面，点击 **Finish（完成）**，然后当提示您是否将更改应用至传感器时点击 **Yes（是）**。

步骤 10：重新启动传感器，并通过点击 **OK** 应用更改。



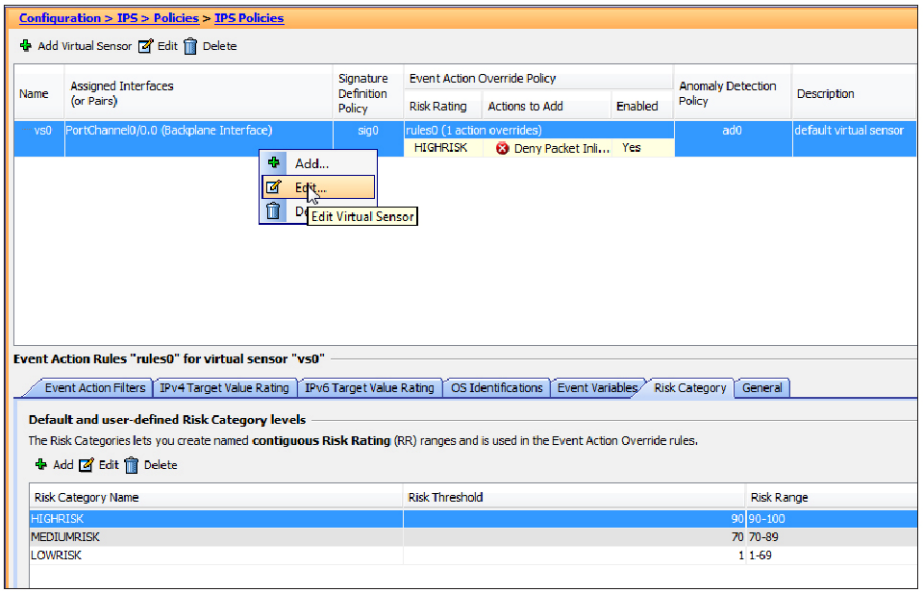
步骤 11：当 IPS 模块重启后，重新连接，并转至 **IPS > Policies（策略）> IPS Policies（IPS 策略）**。

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 12：在主面板中，点击 **Risk Category（风险类别）**了解 High Risk（高风险）表示的信息。

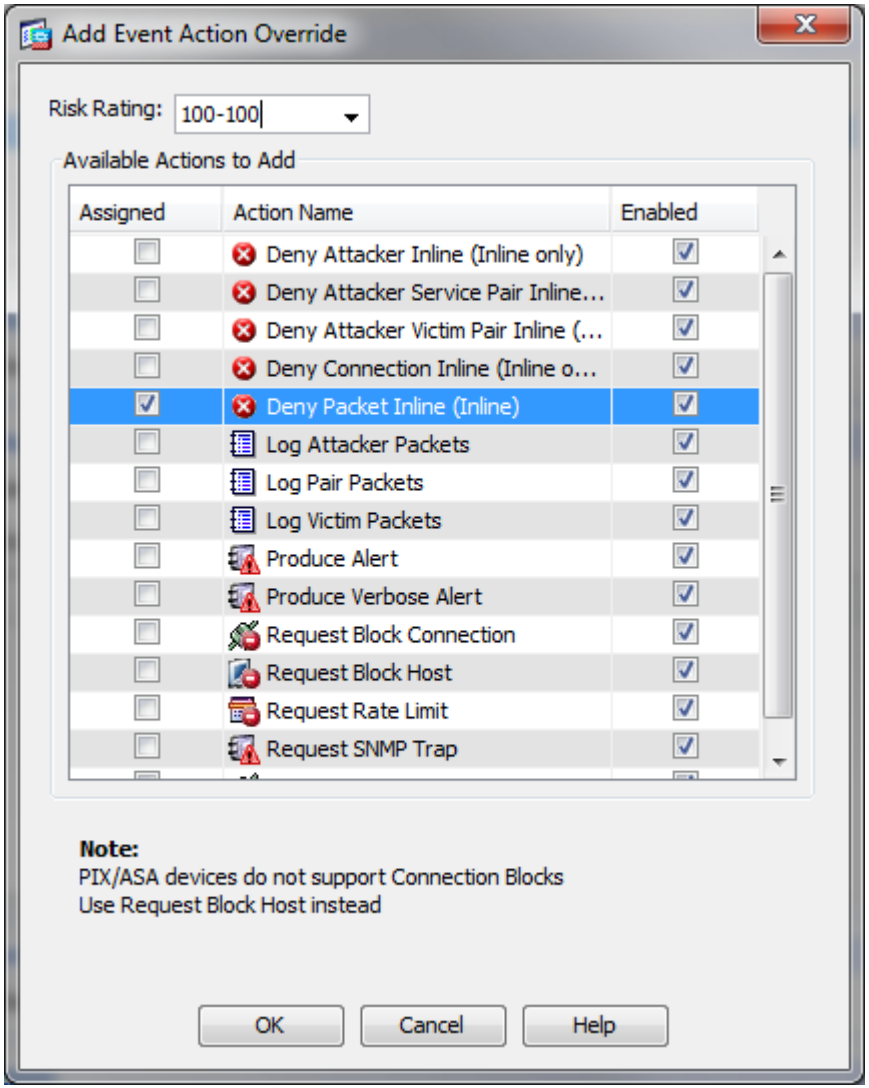
在默认情况下，High Risk 表示事件的风险等级从 90 至 100。为降低丢弃非恶意流量的风险，编辑 Deny Packet（拒绝数据包）操作，使其仅在 Risk Rating（风险等级）为 100 时触发。这意味着传感器现在将仅对 Risk Rating（风险等级）等于 100 的事件使用 Deny Packet（拒绝数据包）操作，即只有当最精确、风险最高的签名防御时才会出现。

步骤 13：在 Virtual Sensor（虚拟传感器）面板中，右击 **vs0** 项，然后选择 **Edit（编辑）**。



步骤 14：点击 **Deny Packet Inline Override（拒绝数据包内嵌覆盖）**，然后点击 **Delete（删除）**。

步骤 15：点击 **Add（添加）**添加新的覆盖，为 Risk Rating（风险等级）输入值 **100-100**，选择 **Deny Packet Inline（拒绝数据包内嵌）**，点击 OK，然后点击 **Apply（应用）**。



步骤 16：针对在其它思科 ASA 机箱中安装的 IPS 传感器，重复这些步骤。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

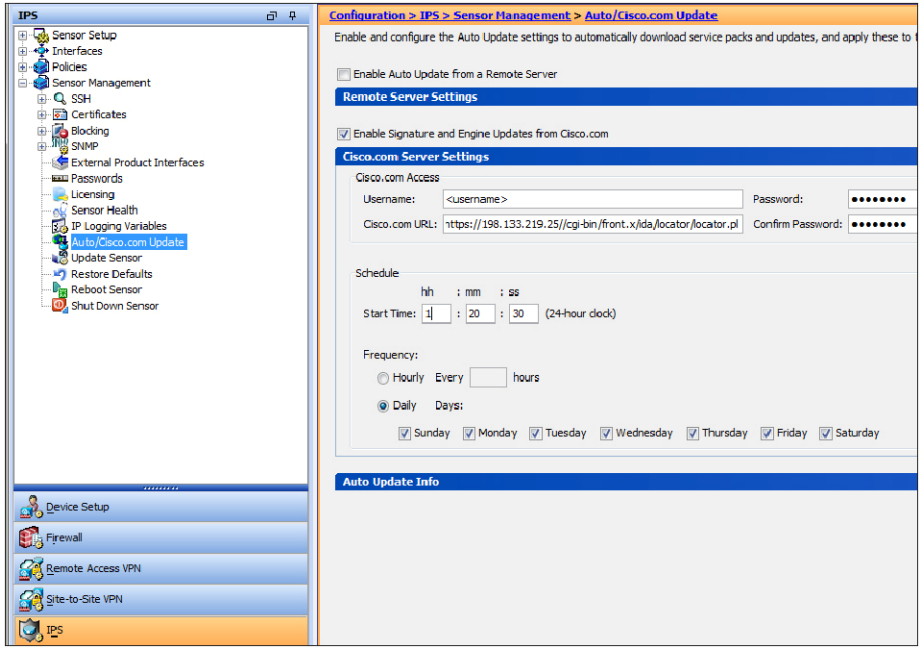
（可选）

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：访问 **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。



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

业务概述

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。

应用基础设施不够灵活

过去，应用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(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、安全套接层(SSL)卸载、压缩和其它各种加速技术。思科 ACE 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。

思科的应用控制引擎是下一代应用交付控制器，具备服务器负载均衡、SSL 卸载和应用加速功能。思科 ACE 提供了四大优势：

- **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。
- **服务器卸载**——思科 ACE 从服务器上卸载了 TCP、SSL 处理和压缩，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%。

为实现最高的可用性，思科 ACE 硬件总是成对部署：一个作为主设备，另一个作为备用设备。如果主用思科 ACE 出现故障，辅助思科 ACE 将取而代之。根据会话状态冗余的配置方式，这一故障切换可能无需中断客户端到服务器连接即可完成。

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，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、流媒体服务器等等。

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。

此外，思科 ACE 还能够将对可缓存内容（如图像文件）的请求，推送到能够比应用服务器相比更经济高效地满足这些请求的缓存。

在 Web 应用服务器上运行 SSL 需要消耗大量服务器资源。通过卸载 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接这些会话，前面讨论的所有持久性选项都可用于安全站点。

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 部署在应用集群的前面。到该应用集群的请求被引导至思科 ACE 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 与第二层/第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第二层/第三层交换机上的策略路由控制。

部署详情

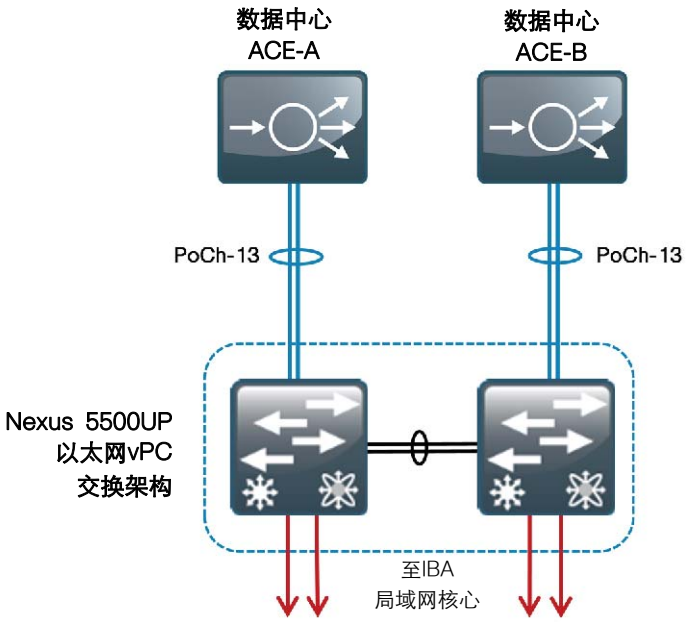
流程

配置到数据中心核心交换机的连接

1. 在 Nexus 5500s 上配置端口通道

程序 1　在 Nexus 5500s 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 端口或 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：按如下所示在两个 Cisco Nexus 5500UP 数据中心核心交换机上配置到端口通道的物理接口。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。**

- 配置第一个 Cisco Nexus 5500UP 交换机。

```
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
```

- 配置第二个 Cisco Nexus 5500UP 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
```

当您向物理接口分配通道组时，它会创建逻辑 EtherChannel（端口通道）接口。在下一个步骤中，在两个数据中心核心交换机上配置逻辑端口通道接口，而与端口通道绑定的物理接口将继承相关设置。

步骤 2： 配置逻辑端口通道接口。

```
interface port-channel13
  switchport mode trunk
  switchport trunk allowed vlan 148,912
  spanning-tree port type edge trunk
```

步骤 3： 在每个 Cisco Nexus 5500UP 交换机上，为思科 ACE 容错 heartbeat VLAN 配置未使用的 VLAN。

```
vlan 912
name ACE-Heartbeat
```

流程

配置思科 ACE 设备网络

1. 执行初始设置
2. 配置高可用性

程序 1　执行初始设置

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：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 3：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 148
  no shutdown
```

该配置调配一个 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 4：在思科 ACE 上配置 VLAN 148 接口用于管理访问和通用网络连接。

```
interface vlan 148
  ip address 10.10.48.119 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown
```

步骤 5：配置默认路由器。

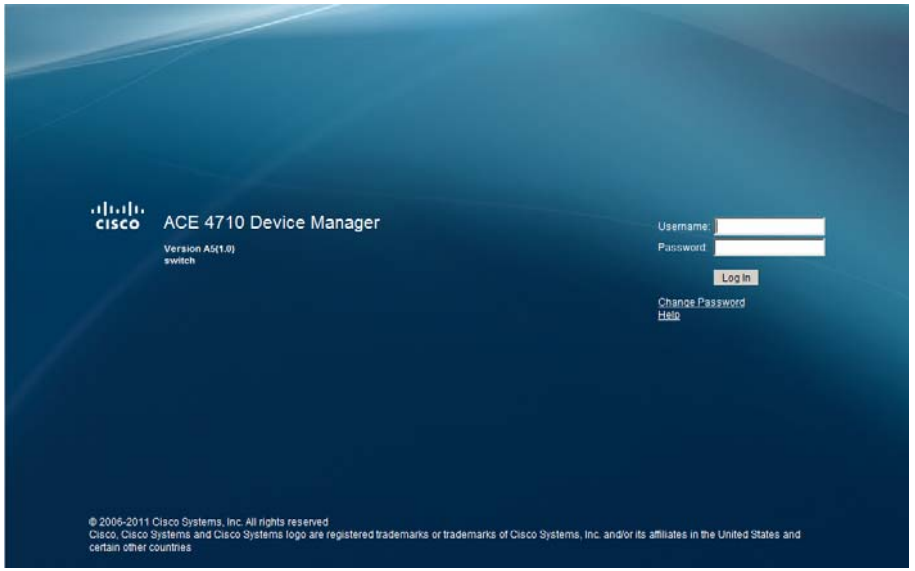
```
ip route 0.0.0.0 0.0.0.0 10.10.48.1
```

思科 ACE 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 5，将步骤 4 中的 IP 地址替换为 10.10.48.120。

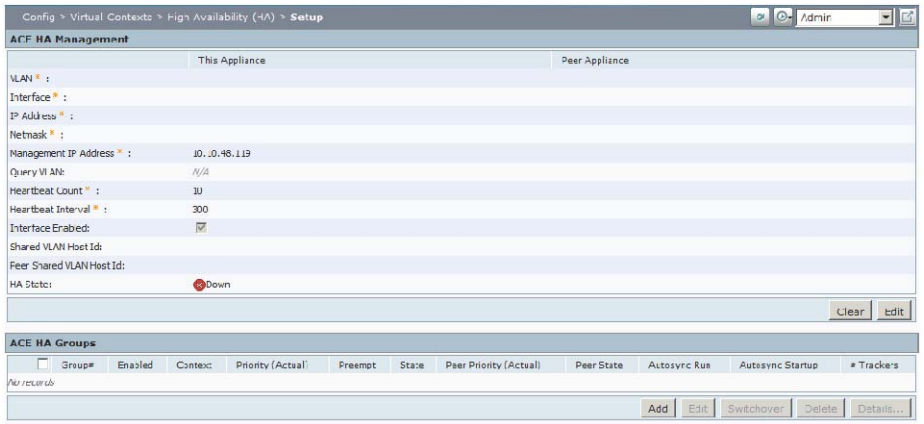
程序 2　配置高可用性

接下来，您要将思科 ACE 设备配置为主用—备用故障切换对。当您配置高可用性时，设备将进行同步，并且仅需在主用思科 ACE 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 10.10.48.119。

步骤 1：要访问思科 ACE GUI，请使用浏览器，转至 https://10.10.48.119，使用在程序 1 步骤 1 中设置的密码以管理员身份登录。

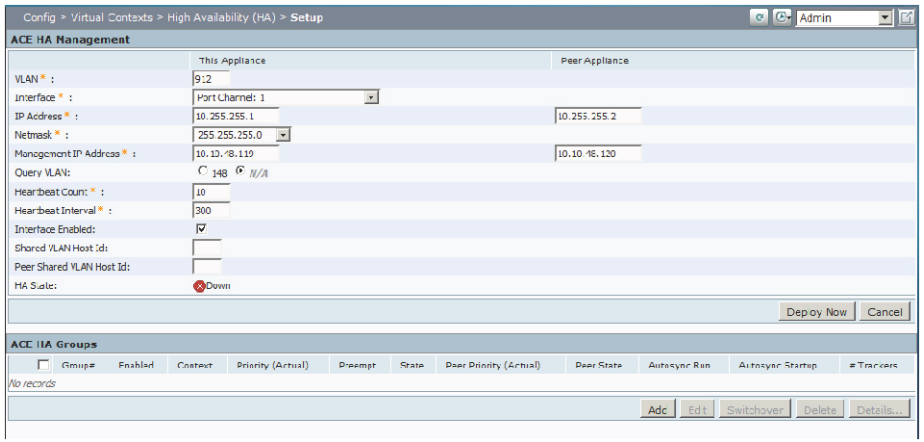


步骤 2：转至 Config（配置）> Virtual Contexts（虚拟上下文）> High Availability (HA)（高可用性(HA)）> Setup（设置），然后点击 Edit（编辑）。



步骤 3：在 ACE HA Management（ACE HA 管理）对话框中，输入以下值，然后点击 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）—10.10.48.119
- Management IP Address Peer Appliance（管理 IP 地址对等设备）—10.10.48.120



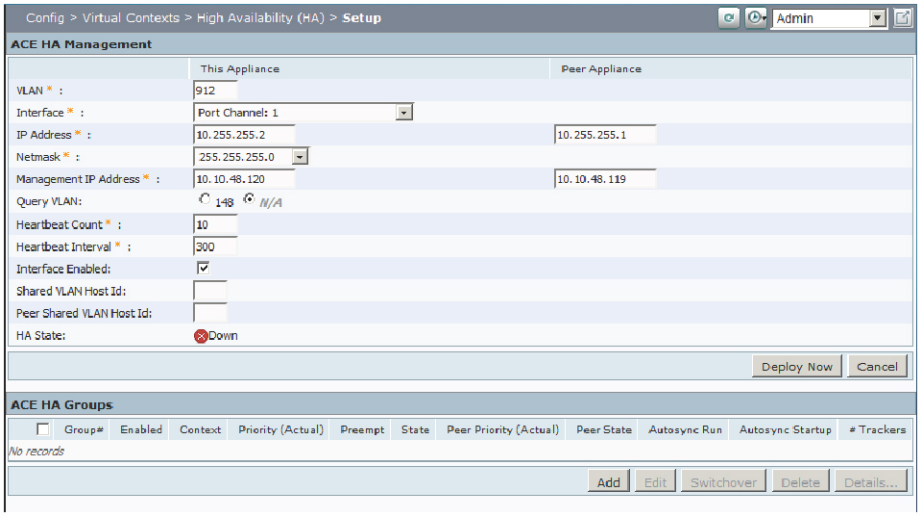
步骤 4：在 ACE HA Groups（ACE HA 组）对话框中，点击 Add（添加）。

步骤 5：将所有值保留为默认值，然后点击 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。对于其余的高可用性配置，您需要登录至备用思科 ACE 设备。

步骤 6：通过转至 HTTPS://10.10.48.120，登录备用思科 ACE 设备。

步骤 7：转至 Config（配置）> Virtual Contexts（虚拟上下文）> High Availability (HA)（高可用性(HA)）> Setup（设置），然后点击 Edit（编辑）。

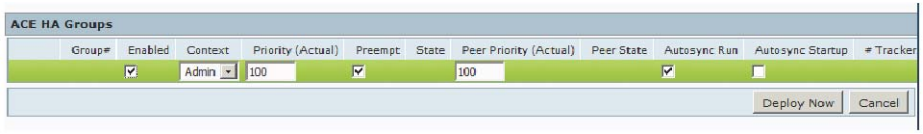


步骤 8: 在 ACE HA Management (ACE HA 管理) 对话框中，输入以下值，然后点击 **Deploy Now（立即部署）**。

- 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）—10.10.48.120
- Management IP Address Peer Appliance（管理 IP 地址对等设备）—10.10.48.119

步骤 9: 在 ACE HA Groups（ACE HA 组）对话框中，点击 **Add（添加）**。

步骤 10: 将所有值保留为默认值，然后点击 **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 10.10.48.119 上进行，任何更改将自动复制到备用思科 ACE。

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 NAT 池
5. 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: 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）**，然后点击+号。

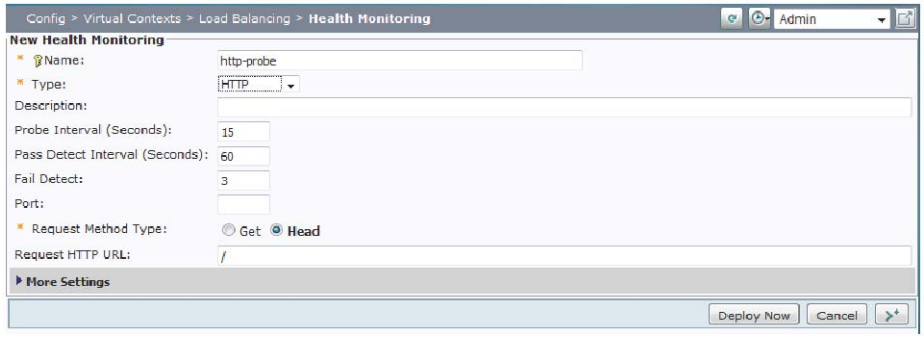
步骤 2: 在 New Health Monitoring（新运行状况监控）对话框中，在 Name（名称）框中，输入 icmp-probe，然后在 Type（类型）列表中选择 **ICMP。**

步骤 3：点击 **Deploy Now（立即部署）**。

步骤 4：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）**，然后点击+号。

步骤 5：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 6：点击 **Deploy Now（立即部署）**。



步骤 7：点击 **Expect Status（预期状态）**选项卡，然后点击+号。

步骤 8：为最大和最小状态代码输入 200，然后点击 **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。

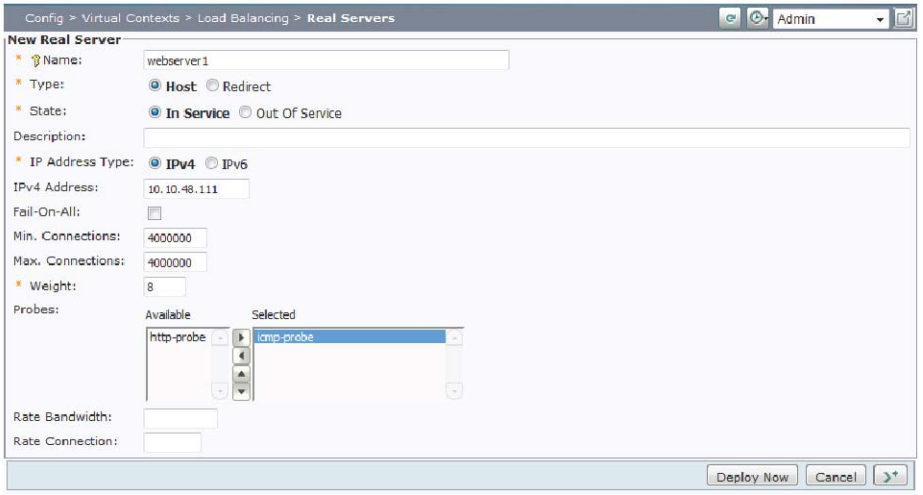
程序 2　配置真实服务器

在本章节中，您将添加真实服务器，在其中思科 ACE 设备将对客户端连接进行负载均衡。

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）**，然后点击 **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，然后点击 **Deploy Now（立即部署）**。

- Name（名称）—webserver1
- IP Address（IP 地址）—10.10.48.111
- 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）**，然后点击 **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，然后点击 **Deploy Now（立即部署）**。

- Name（名称）—webserver2
- IP Address（IP 地址）—10.10.48.112
- 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。

本示例中显示的两个 web 服务器现已配置完成。如果您计划使用其他服务器，您可以按照以上示例中的步骤对其进行配置。

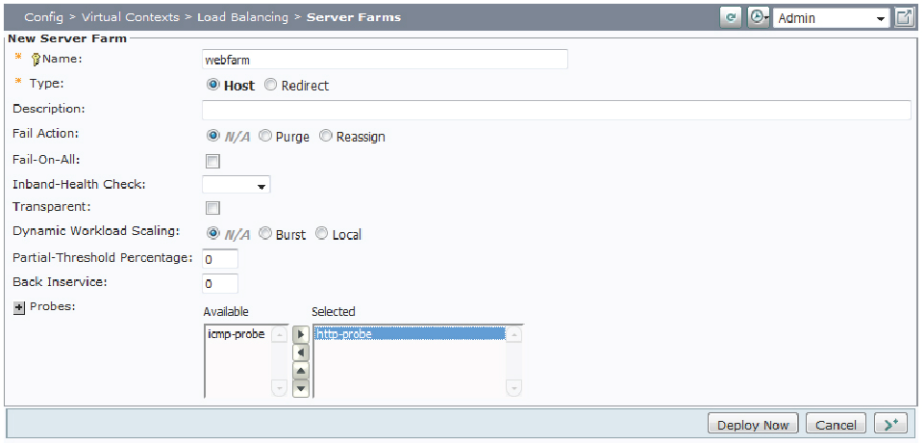
程序 3　配置服务器群

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）**，然后点击 **Add（添加）**。

步骤 2：在 New Server Farm（新服务器群）对话框中，输入以下值，然后点击 **Deploy Now（立即部署）**。

- Name（名称）— webfarm
- Probes（探针）— http-probe



步骤 3：点击 **Real Server（真实服务器）**选项卡，然后点击 **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：点击 **Deploy Now（立即部署）**。

步骤 6：点击 **Real Server（真实服务器）**选项卡，然后点击 **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）框中输入 **80**。

步骤 8：点击 **Deploy Now（立即部署）**。

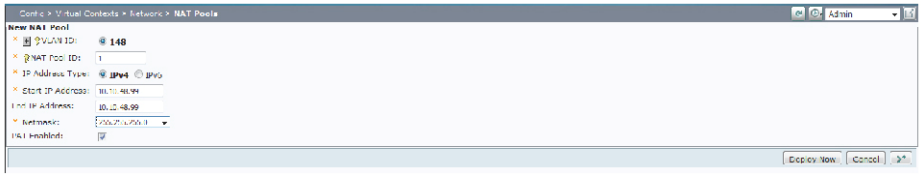
这些步骤创建了服务器群 webfarm，真实服务器成员 webserver1 和 webserver2 用于端口 80 上的 HTTP。http-probe 将监控服务器群中的所有服务器，以确保 HTTP 服务可用。

程序 4　配置 NAT 池

步骤 1：转至 **Config（配置）> Virtual Contexts（虚拟上下文）> Network（网络）> NAT Pools（NAT 池）**，然后点击 **Add（添加）**。

步骤 2：在 New NAT Pool（新 NAT 池）对话框中，输入以下值，然后点击 **Deploy Now（立即部署）**。

- Start IP Address（起始 IP 地址）—10.10.48.99
- End IP Address（结束 IP 地址）—10.10.48.99
- Netmask（子网掩码）—255.255.255.0



程序 5　配置虚拟服务器

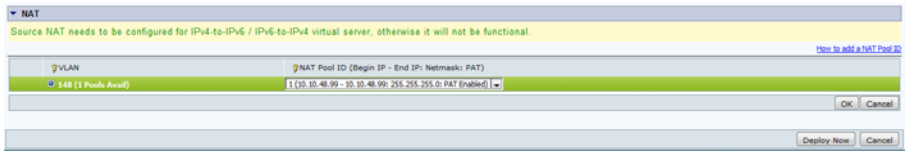
步骤 1：转至 **Config（配置）> Virtual Contexts（虚拟上下文）> Load Balancing（负载均衡）> Virtual Servers（虚拟服务器）**，然后点击 **Add（添加）**。

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）—10.10.48.100
- VLAN—148

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，点击 **Add（添加）**，点击 **OK**，然后点击 **Deploy Now（立即部署）**。



指向端口 80 上的虚拟 IP 10.10.48.100 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 卸载

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

本章节介绍了如何配置一组服务器，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卸载。

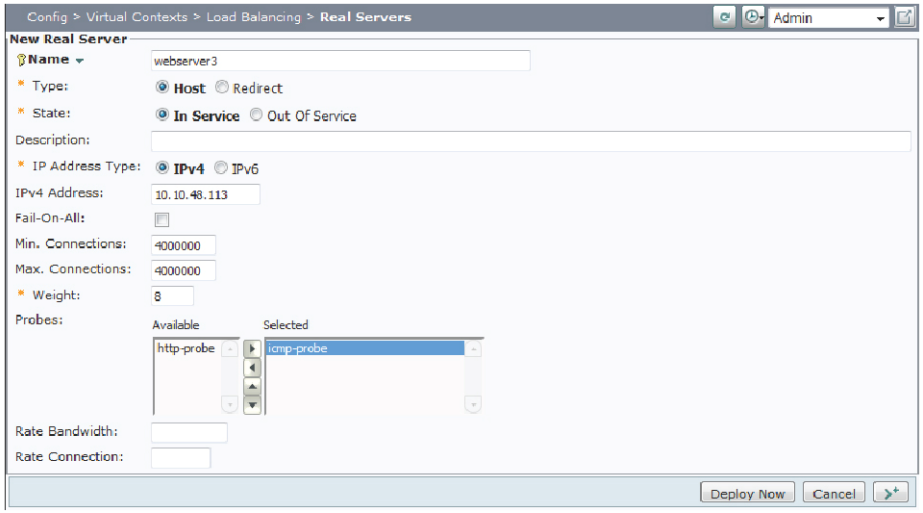
程序 1　配置真实服务器

在本章节中，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：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）**，然后点击 **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，然后点击 **Deploy Now（立即部署）**。

- Name（名称）—webserver3
- IP Address（IP 地址）—10.10.48.113
- 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）**，然后点击 **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，然后点击 **Deploy Now（立即部署）**。

- Name（名称）—webserver4
- IP Address（IP 地址）—10.10.48.114
- 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。

本示例中显示的两个 web 服务器现已配置完成。如果您计划使用其他服务器，您可以按照以上示例中的步骤对其进行配置。

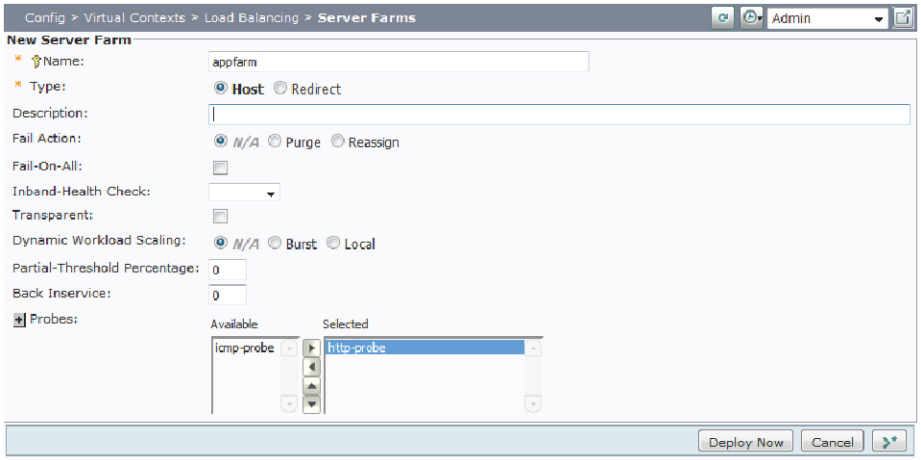
程序 2　配置服务器群

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）**，然后点击 **Add（添加）**。

步骤 2：在 New Server Farm（新服务器群）对话框中，输入以下值，然后点击 **Deploy Now（立即部署）**。

- Name（名称）—appfarm
- Probes（探针）—http-probe



步骤 3：点击 **Real Server（真实服务器）**选项卡，然后点击 **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：点击 **Deploy Now（立即部署）**。

步骤 6：点击 **Real Server（真实服务器）**选项卡，然后点击 **Add（添加）**。

步骤 7：在 New Real Server（新真实服务器）对话框中，在 Name（名称）列表中，选择 **webserver4**，然后在 Port（端口）框中输入 **80**。

步骤 8：点击 **Deploy Now（立即部署）**。

这些步骤创建了服务器群 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。

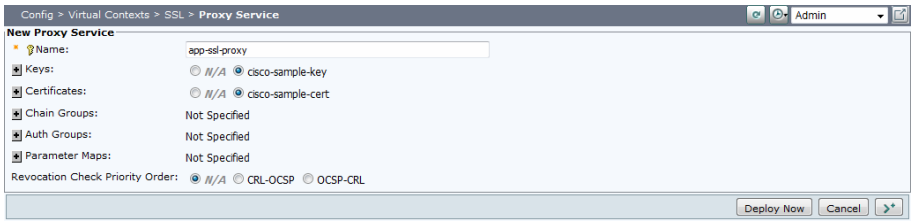
程序 3　配置 SSL 代理服务

为了使思科 ACE 卸载 SSL 处理，您需要配置一个 SSL 代理服务。本示例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）**，然后点击 **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**，然后点击 **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。

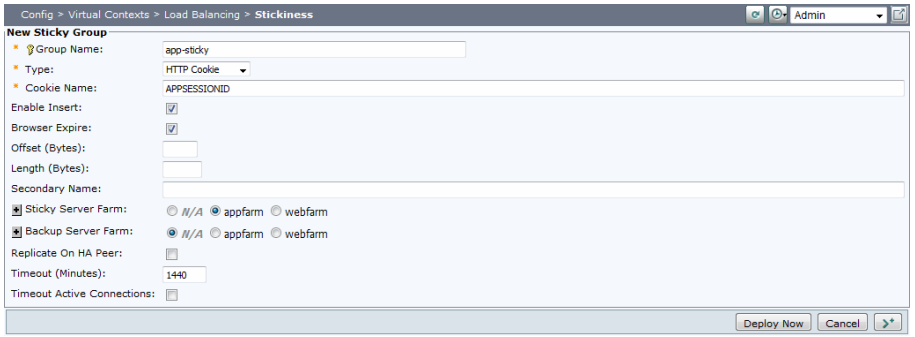
步骤 1：转至 **Config（配置）> Virtual Contexts（虚拟上下文）> Load Balancing（负载均衡）> Stickiness（粘连）**，然后点击 **Add（添加）**。

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**，点击 **Deploy Now（立即部署）**。

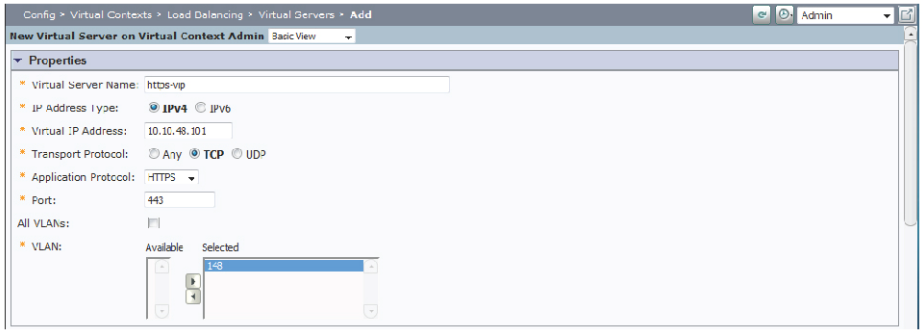


程序 5　配置虚拟服务器

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）**，然后点击 **Add（添加）**。

步骤 2：在 Properties（属性）对话框中，输入以下值。

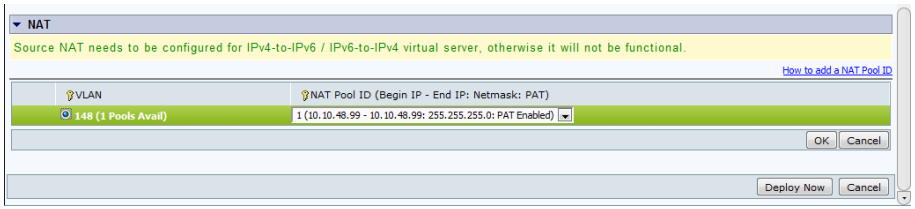
- Virtual Server Name（虚拟服务器名称）—https-vip
- Virtual IP Address（虚拟 IP 地址）—10.10.48.101
- Application Protocol（应用协议）—**HTTPS**
- VLAN—148



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）**，在 Sticky Group（粘连组）列表中，选择 **app-sticky (HTTP Cookie)**，然后选择 **Deflate（收缩）**。

步骤 5：在 NAT 对话框中，点击 **Add（添加）**，点击 **OK**，然后点击 **Deploy Now（立即部署）**。



指向端口 443 上的虚拟 IP 10.10.48.101 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

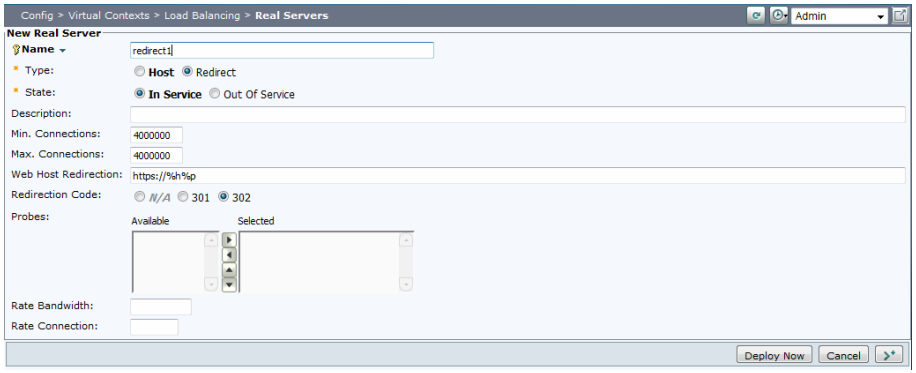
（可选）

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。本示例介绍了如何创建服务，以便将指向 10.10.48.101 的任意 HTTP 流量重定向至在上述步骤中配置的 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）**，然后点击 **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，然后点击 **Deploy Now（立即部署）**。

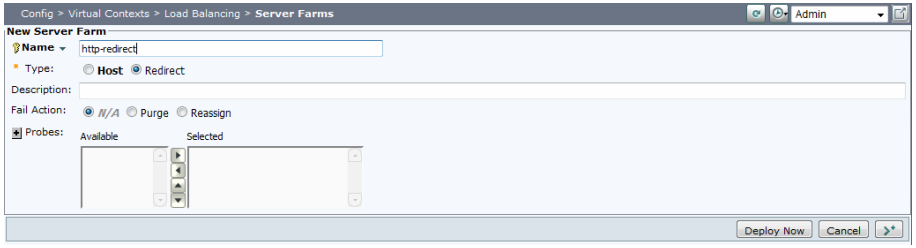
- Name（名称）—redirect1
- Type（类型）—**Redirect**
- Web Host Redirection（Web 主机重定向）—**https://%h%p**
- Redirection Code（重定向代码）—**302**



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）**，然后点击 **Add（添加）**。

步骤 4：在 New Server Farm（新服务器群）对话框中，输入以下值，然后点击 **Deploy Now（立即部署）**。

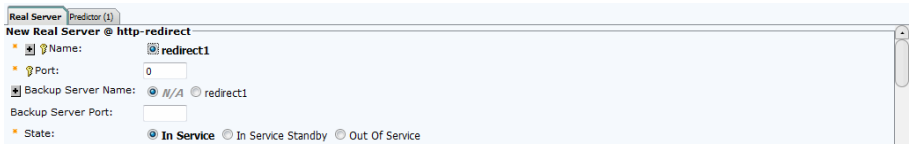
- Name（名称）—http-redirect
- Type（类型）—**Redirect**



步骤 5：点击 **Real Server（真实服务器）**选项卡，然后点击 **Add（添加）**。

步骤 6：在 New Real Server（新真实服务器）对话框中，选择 **redirect1**。

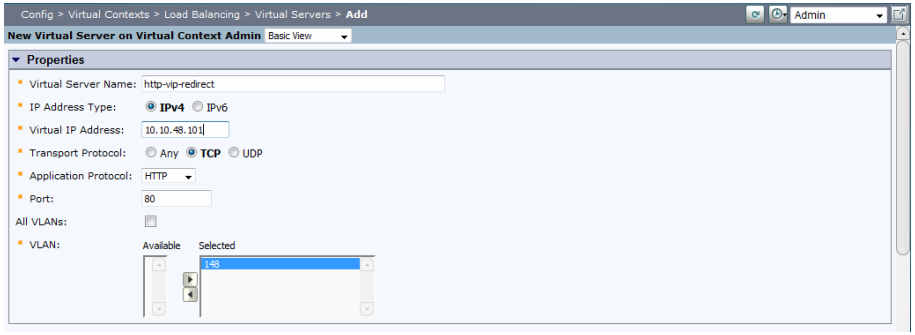
步骤 7：点击 **Deploy Now（立即部署）**。



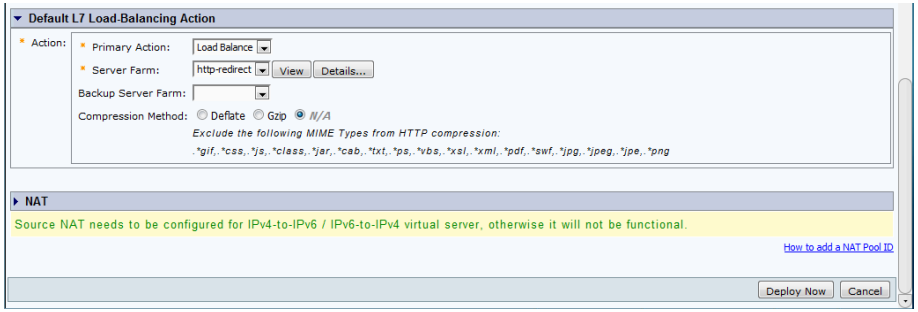
步骤 8：转至 **Config（配置）> Virtual Contexts（虚拟上下文）> Load Balancing（负载均衡）> Virtual Servers（虚拟服务器）**，然后点击 **Add（添加）**。

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）—10.10.48.101
- VLAN—148



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**，然后选择 **Deploy Now（立即部署）**。



附录 A: 产品列表

以下产品与软件版本经验证适用于思科 IBA 智能业务平台：

表 2. 产品

功能区域	产品	产品编号	软件版本
以太网基础设施	Nexus 5548UP Nexus 5548 第三层子卡 Nexus 2248TP Nexus 2232PP	N5K-C5548UP-FA N55-D160L3 N2K-C2248TP-1GE N2K-C2232PP-10GE	NX-OS 5.1(3)N1(1)
存储基础设施	MDS 9148 MDS 9124	DS-C9148D-8G16P-K9 DS-C9124-K9	NX-OS 5.0(7)
网络安全性	ASA 5585-X ASA 5585-X IPS SSP	ASA5585-S40-K9 ASA5585-SSP-IPS20	ASA:8.4.2 IPS:7.1-2-E4
应用永续性	Cisco ACE 4710 设备	ACE-4710-0.5-K9	A5(1.0)

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，本指南所做的变更。

- 我们更新了“以太网基础设施”模块，使用带有第二层和第三层的 Cisco Nexus 5500UP 系列交换机来创建独立的路由数据中心核心。我们还添加了关于以太网带外管理网络的详细信息。
- 我们更新了“存储基础设施”模块，使用 Cisco Nexus 5500UP 系列交换机作为光纤通道 SAN 核心，并通过 MDS 9100 系列部署来满足规模更大的光纤通道 SAN 要求。
- 我们将“计算资源”模块更新成了“计算连接性”，并介绍了将服务器连接至数据中心网络的多种方法。
- 我们更新了“网络安全性”模块，详细介绍了如何迁移数据中心防火墙和集成思科 IPS，以连接至数据中心核心交换机。
- 我们采用更高级的版本更新了“应用永续性”模块，详细介绍了多个运行状况探针和永续性特性的部署。

备注

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

B-0000590-1 2/12