思科美洲台第3层OOB使用数据流隔离的VRF-Lite

目录

简介

此指南描述思科网络准入控制(美洲台)的实施在根据虚拟路由转发的第3层带外(OOB)部署(VRF) -轻。

解决方案概述

此部分给一简要介绍对第3层OOB使用VRF-Lite方法为了实现美洲台体系结构。

执行摘要

思科美洲台强制执行一个组织的网络安全策略在寻找网络访问的所有设备的。思科美洲台只允许兼容并且委托端点设备，例如PCs、服务器和PDA，在网络上。思科美洲台限制固执的设备访问，限制从新兴安全威胁和风险的可能损害。思科美洲台给组织一个强大，基于任务的方法为了防止未经授权的访问和改进网络弹性。

思科美洲台解决方案提供这些商业效益：

- **安全策略标准**—保证终端依照安全策略;保护基础设施和员工生产力;巩固被管理的和不受管理资产;支持内部环境和访客访问;为策略专门制作您的风险级别
- **保护现有投资**—是与第三方管理应用程序兼容;灵活部署选项最小化对基础设施升级的需要
- **缓和从病毒、蠕虫病毒和未授权的访问控制的风险**并且减少大规模基础设施中断;由动态和自动化的进行的移动，添加和更改减少运营费用，因而启用更高的IT效率;集成其他思科自防御网络组件为了提供全面的安全保护

解决方案描述

思科美洲台用于网络基础设施为了强制执行在寻找对网络资源的访问的所有设备的安全策略标准。在他们授权网络访问前，思科美洲台允许网络管理员验证和授权用户和评估和修正他们相关的机器。您能使用几个配置方法完成此任务。本文特别地着重思科美洲台的基于VRF的实施在思科美洲台服务器的第3层OOB部署的(思科Clean Access服务器)在实时IP网关(路由)模式配置。

第3层OOB是其中一美洲台的最普遍的部署方法学。此转移在大众化中根据包括硬件资源的更加好的利用率的几Dynamics。通过部署在第3层OOB方法的思科美洲台，单个Cisco NAC设备能扩展适应更多用户。它也允许思科美洲台在中央查找的伊莱克斯而不是被分配在校园或组织间。所以，第3层OOB部署从大写和操作费用支架是有效两个。

此指南描述思科美洲台的实施在根据VRF-Lite的第3层OOB部署的。

VRF的简单定义

一种方式查看VRF设备虚拟化将等同于它对VLAN出现。VLAN创建虚拟交换机在单个物理交换机外面。VRF扩大该虚拟化通过Layer2边界，并且允许虚拟路由器的创建。虚拟路由器提供从端到端的充分虚拟化网络。

另一个方式查看VRF设计是每个VRF操作正如VPN或通道。被放置到VRF的流量不能通信在VRF(通道)外面直到流量穿过终止通道的设备(目的地VPN路由器)。

注意： 这些定义被认为帮助介绍新概念。这些定义不是确切的表示或VRF的正式定义。

图1显示设备虚拟化的图示与VRF的。每块变色的层在图表中代表一个不同的虚拟路由器或者VRF。VRF方法与能力有多个隔离的数据层面一起提供控制层面和数据层面路径隔离。换句话说，它为一个分开的虚拟路由器提供可能性或网络为在环境预计使用思科美洲台的每流量类型。典型的流量类型是：

- 未认证的用户流量
- 已认证的用户流量
- 承包商流量
- 访客流量

图1 –*设备虚拟化*

解决方案体系结构

思科美洲台服务器最初设计是在波段之内设备。使用思科在Cisco网络基础架构的美洲台伊莱克斯允许您采取设计是在波段之内对所有网络流量的设备，并且部署它与OOB方法。

解决方案体系结构(请参阅图2)识别思科美洲台服务器的关键解决方案组件和集成点。

注意： 在本文中，可互换使用术语“边界交换机”和“接入交换机”。

图2 –*解决方案体系结构*

以下部分描述组成典型的校园体系结构的访问、分配、核心和数据中心层。

接入层

第3层OOB思科美洲台解决方案是可适用的对一个已路由访问园区网设计。在已路由接入模式，第3层交换虚拟接口(SVIs)在接入交换机配置。当图3显示，第3层访问VLAN (例如， VLAN 100)在边界交换机配置，第3层路由从交换机支持到上行分布式交换机或路由器，并且思科美洲台管理器管理接入交换机的端口。

图3 –*接入交换机用对边缘的第3层*

分布层

分布层对第3层接入层交换机的路由和聚合负责。当您在Layer2 OOB设计时的此层能安置思科美洲台服务器，您在第3层OOB设计不找出他们此处。反而，在中央请放置思科美洲台服务器在数据中心服务块，解决方案体系结构显示(图2)。

核心层

核心层使用基于Cisco IOS的路由器。核心层为高速的路由保留，不用任何服务。安置服务在服务交换机在数据中心。

数据中心服务层

数据中心服务分层堆积用途基于Cisco IOS的路由器和交换机在园区网络。思科美洲台管理器和思科美洲台服务器在中央查找在此第3层OOB设计的数据中心服务块。

解决方案组成部分

思科美洲台管理器

思科美洲台管理器是集中所有思科美洲台服务器、用户和策略配置和监视在Cisco NAC设备部署的管理服务器和数据库。对于OOB思科美洲台部署，思科美洲台管理器提供OOB在思科美洲台管理器的域的管理为了添加和控制开关和配置交换机端口。

思科美洲台服务器

思科美洲台服务器是在不信任(管理的)网络和委托(内部)网络之间的实施点。服务器强制执行修正定义在思科美洲台管理器，并且终端与服务器联络在验证时。在此设计，服务器逻辑上分离不信任和可靠网络，并且起集中化实施点作用对于所有访问列表(ACL)和设备的带宽限制在不受信任网络。欲知更多信息，请参阅OOB模式部分。

思科美洲台代理程序

思科美洲台代理程序是思科美洲台解决方案的一个可选组件。当代理程序为您的思科美洲台部署时启用，保证访问您的网络满足系统状态需求您的计算机指定。代理程序只读，易用，在用户机器驻留的斯莫尔覆盖区程序。当用户尝试访问网络时，代理程序检查客户端系统您需要的软件，并且帮助您获取所有缺少更新或软件。请参阅步骤6 ：更新从Cisco.com的策略在思科美洲台管理器欲知更多信息。

设计注意事项

当您考虑一第3层OOB美洲台部署时，请查看几设计注意事项。这些考虑事项在这些小节列出，与

简要论述他们的重要一起。

OOB模式

在Cisco NAC设备OOB部署，美洲台服务器与终端主机仅联络在认证过程中，摆评估和修正姿势。在终端主机被确认后，不与服务器联络。

在OOB模式，思科美洲台管理器使用简单网络管理协议(SNMP)为了控制开关和set vlan分配端口的。当Cisco NAC管理器和服务器为OOB时设置，管理器能控制支持的交换机交换机端口。交换机端口的控制叫作SNMP控制层面。对于所支持的交换机型号列表，参考*交换机支持的OOB支持的交换机*部分Cisco NAC设备的。

OOB模式主要使用有线的部署。当使用时第3层OOB VRF方法，从不信任(坏的) VLAN的所有流量，包括代理程序流量，到达所有实施发生的集中化思科美洲台服务器。在服务器的流量实施是在VRF方法和第3层OOB之间ACL方法的一个关键区别。

注意： 思科美洲台服务器最初设计是一个在波段之内设备。换句话说，服务器设计安排所有流量流经它，将允许服务器是控制点。当您使用第3层OOB时VRF方法，所有未认证的用户流量正确地流经服务器，好象它一在波段之内部署。此通信流允许一个一致，可预测的环境。

终端分类

几个要素造成终端分类，并且包括设备类型和用户角色。设备类型和用户角色影响终端角色。

这些是可能的设备类型：

- 公司设备
- 非公司设备
- 非个人计算机设备

这些是可能的用户角色：

- 员工
- 承包商
- 访客

最初，所有终端分配到未经鉴定的VLAN。对其他角色的访问在标识以后允许，并且状态进程完成。

终端角色

必须最初确定终端的每种类型角色。一典型的校园部署包括几个角色，例如员工、访客、承包商和其他终端例如打印机、无线接入点和IP摄像头。角色被映射到边界交换机VLAN。

注意： 一个另外的角色为所有终端最初属于的验证要求。此角色映射对未经鉴定的“坏的” VLAN。

角色隔离

对于此种美洲台设计，作为“坏”分类的流量必须流到思科美洲台服务器的“不信任”侧。当您设计思科美洲台实施时，请记住此原理。另外，请勿允许“清洗”和“坏的”网络直接地彼此通信。

图4显示，当第3层OOB设计使用VRF时， VRF保证未经鉴定的流量在其自己的虚拟网络依然是隔

离。思科美洲台服务器作为实施点或保证的控制器隔离和安全通信之间“清洗”和“坏的”网络。

图4 –*思科美洲台服务器连接给坏和干净的赛兹*

通信流

当终端连接对一美洲台托管型switchport时，美洲台进程开始。当在“坏的” VRF，作为“坏”或“未经鉴定”分类的流量从网络的其余隔离。此流量隔离并且发送对在思科美洲台服务器的不信任的接口。请参阅图 4。

注意： Cisco NAC设备是忘却的对流量如何被提交对它。换句话说，设备没有首选流量是否通过通用路由封装(GRE)隧道到达或通过基于策略的路由配置， VRF已路由，或者其他重定向方法重定向。

思科美洲台服务器模式

您在这两个模式之一中能部署一个思科美洲台服务器：

- 虚拟网关(网桥)模式
- 实时IP网关(路由)模式

虚拟网关(网桥)模式

典型地使用虚拟网关(网桥)模式，当思科美洲台服务器是Layer2在终端附近时。在此模式，服务器在网络流量的路由决策作为网桥和没有涉及。

注意： 此模式为此特定ACL设计不是可适用的。

雷亚尔德蒙特罗伊IP网关(路由)模式

雷亚尔德蒙特罗伊IP网关(路由)模式是可适用在思科美洲台服务器是远离终端的多层3跳的一设计，例如第3层OOB。当您使用服务器作为雷亚尔德蒙特罗伊IP网关时，请指定其两个接口的IP地址：一委托侧的(服务器管理)和一个不信任(坏的)侧的。双地址必须在不同的子网。不信任的接口IP使用通信与在不信任子网的终端。此指南使用的模式是雷亚尔德蒙特罗伊IP网关。

用户体验(用思科美洲台代理程序)

一般，公司实体有在末端客户端事先被部署的思科美洲台代理程序。在代理程序的发现号主机设置触发将发送的发现信息包对思科美洲台服务器的不信任的接口，通过美洲台进程自动地继续终端。

在一第3层OOB用VRF型号，发现号主机典型地设置是思科美洲台管理器的DNS名或IP地址。管理器在干净的网络存在。默认情况下由于从“坏的”网络的所有流量通过思科美洲台服务器路由，发现信息包自动地流经服务器。描述的通信流此处是其中一个好处对VRF方法。此通信流提供一一致，可预测的体验。欲知更多信息，请参阅思科美洲台进程流。

用户体验(没有思科美洲台代理程序)

能力运行没有思科美洲台代理程序是VRF型号的另一个好处。从“坏的”网络的所有流量通过思科美洲台服务器自然路由。这意味着一计算机的一个用户没有思科美洲台代理程序必须只打开Web浏览器和浏览到所有有效网站。浏览器流量尝试穿过服务器，反过来抓住浏览器会话并且重定向它到俘

虏门户。欲知更多信息，请参阅思科美洲台进程流。

注意： 可能最好的终端用户经验，由最终用户的浏览器委托的使用证书。在思科美洲台服务器和思科美洲台管理器的自生的证书没有为生产环境推荐。

注意： 总是请生成思科美洲台服务器的证书用其不信任的接口的IP地址。

思科美洲台进程流

此部分说明美洲台OOB解决方案的基本流程流程。方案是描述的都有和没有在客户端机器安装的思科美洲台代理程序。此部分显示思科美洲台管理器如何控制交换机端口使用SNMP作为控制介质。这些流程实质上是宏分析，并且仅包含功能决策步骤。进程流不包括发生的每个选项也不跨步和不包括根据终端评估标准的审定决定。

在表6参考进程流流程图关于在表5.的盘旋的步骤。

图5 –*第3层OOB思科美洲台解决方案的美洲台进程流* **图6 –*思科美洲台进程流结构图***

思科美洲台解决方案实施

此部分描述如何实现思科美洲台解决方案。

拓扑

Figure7显示用于此指南的创建的拓扑。内部网络，通过使用全球路由表，包括VLAN 200和210，路由。内部网络没有VRF关联与它。

坏的VRF包含是需要的为了创建所有坏的流量的单个虚拟网络能流到集中化思科美洲台服务器的坏的侧的坏的VLAN和仅相关的转接网络。

访客VRF包含是需要的为了终止从访客来源的所有数据VLAN在独立的子接口在防火墙的访客VLAN和相关的转接网络。三个虚拟网络中的每一个(坏，访客和全局)在同一物理基础设施和提供完整流量和路径隔离运载。

Figure7 –*用于此指南的拓扑*

运算顺序

思科美洲台解决方案的展开的运算顺序容易地是为辩论。在网络准备前，是否配置解决方案的美洲台部分？在您配置思科美洲台设备前，或者，是否准备网络？

为组织的目的，此指南首先着重网络配置。这保证网络为美洲台准备好，然后思科美洲台产品的配置。

网络配置

此指南着重路径隔离的端到端VRF-Lite。请注意您能以GRE隧道使用VRF为了通过一个现有分配和核心层允许路径隔离，没有要求在那些设备的任何配置。关于的更多信息，当和使用GRE隧道与端到端VRF比较为什么请设计时，请参阅延伸在两设备部分之间的VRF。您能也参考美洲台第3层在使用VRF-Lite数据流隔离的波段设计指南外面。

本文是全双工设计指南集中在与GRE方法的VRF-Lite。

另外，全双工标记交换可以在VRF-Lite位置使用在可适用地方。标记交换考虑外范围为本文。

VRF-Lite的重要考虑事项

注意： VRF-Lite是使您支持两个或多个虚拟网络的功能。VRF-Lite也允许在虚拟网络中的交迭的IP地址。然而， IP地址重叠没有为美洲台实施推荐，因为，当基础设施支持重迭的地址时，能创建故障排除复杂性和不正确报告。

使用VRF-Lite，在步骤给的详细信息提供在此部分概述必要步骤为了配置您的路径隔离的网络。到您的网络作为第3层OOB雷亚尔德蒙特罗伊IP网关也提供为插入Cisco NAC设备要求的配置。

VRF-Lite用途输入接口为了区分不同的虚拟网络和表的路由通过关联一个或更多第3层接口分离虚拟路由路线表与每个VRF。在VRF的接口可以是或者物理，例如以太网端口，或者他们可以是或逻辑，例如sub-interface、隧道接口或者VLAN交换机虚拟接口(SVIs)。

注意： 第3层接口不能每次属于超过一个VRF。

注释这些VRF-Lite考虑事项：

- VRF-Lite是仅局部重要的对定义的交换机，并且输入接口取决于VRF会员。不执行任何数据包报头或有效负载处理。
- 有VRF-Lite的一交换机通过多个虚拟网络(安全域)共享，并且所有安全域有他们自己的唯一路由表。
- 所有安全域都必须具有它们自己的 VLAN。
- VRF-Lite不支持所有多协议标签交换(MPLS) - VRF功能例如标签交换，标签转发协议(LDP)也是的邻接或者标记的信息包知道作为标记交换)。
- 第3层三重内容可编址存储器资源共享在所有VRF之间。为了保证所有一个VRF有满足的内容可寻址内存(CAM)空间，请使用**maximum routes命令**。
- 使用VRF-Lite的Catalyst交换机可以支持一个全球网络和64 VRF。支持的路由总数受 TCAM 的大小限制。
- 您能使用多数路由协议例如边界网关协议(BGP)、开放最短路径优先(OSPF)、增强的内部网关路由选择协议(EIGRP)、路由信息协议(RIP)和静态路由在运行VRF-Lite的设备之间。
- 在大多数情况下，那里是没有需要运行BGP以VRF-Lite。
- VRF-Lite 不影响数据包交换速率。
- 您不能同时配置组播和VRF-Lite在同一个第3层接口。
- 当您配置OSPF作为在网络设备之间时的路由协议请使用**功能VRF轻**子命令在router ospf下。

定义VRF

在本例中设计示例，必须为未经鉴定或坏的用户和访客提供路径隔离。其他流量允许使用内部网络。当此配置显示，您必须定义两VRF ：

VRF配置示例

```
!--- This command creates a VRF for the DIRTY virtual
network: ! ip vrf DIRTY ! !--- This command names the
VRF and places you into VRF configuration mode: !
description DIRTY_VRF_FOR_NAC ! !--- Gives the VRF a
user friendly description field for documentation ! rd
```

```
100:3 ! !--- Creates a VRF table by specifying a route
distinguisher. !--- Enter either an AS number and an
arbitrary number (xxx:y) or an IP !--- address and
arbitrary number (A.B.C.D:y). ! !--- This document uses
the Autonomous System number and a unique router-id in
that AS. !--- This example signifies AS 100:Router-ID 3
!
```

注意： 路由辨别器不是VRF-Lite的一必需的配置。然而，认为最佳实践配置路由辨别器为将来，因此无缝地与标记交换一起使用。

```
! -- Here we create a VRF for the GUEST Virtual Network: ! ip vrf GUESTSdescription
GUESTS_VRF_FOR_VISITORSrd 600:3 !
```

将 VLAN 或接口与 VRF 关联

在VRF在第三层交换机或路由器后定义，您必须关联参加与VRF的VRF-Lite配置他们属于的接口。您能关联与VRF的物理或虚拟接口。全部关联与VRF的此部分提供物理接口的示例，一个子接口、交换虚拟接口和隧道接口。

注意： 示例是仅示例和未用于本文拓扑。

物理接口配置示例

```
interface FastEthernet0/1
ip vrf forwarding GUESTS
!--- Associates the interface with the appropriate VRF
defined in Step 1. ip address 192.168.39.1
255.255.255.252
```

子接口配置示例

```
interface FastEthernet3/1.10
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
```

交换虚拟接口配置示例

```
interface Vlan100
ip vrf forwarding DIRTY
ip address 192.168.100.1 255.255.255.0
```

隧道接口配置示例

```
interface Tunnel0
ip vrf forwarding GUESTS
ip address 192.168.38.2 255.255.255.252
tunnel source Loopback0
tunnel destination 192.168.254.1
```

扩大在两个设备之间的VRF设备

有您能使用为了延伸在基础设施之间两个片段的VRF的几可接受方法学。确保您选择的方法根据这些标准：

- 考虑平台的功能。所有当前思科层3有能力企业交换和路由选择平台支持VRF-Lite。这些平台包括，但是没有被限制对， Catalyst 6500， 4500， 3750和3560平台。
- 路由选择平台必须运行适当的IOS。平台包括，但是没有被限制对， 7600， 3900， 3800， 2900， 2800， 1900， 1800和800系列集成服务路由器(ISR)。

- 考虑第3层跳数量在基础设施之间相关片段的。为了确定第3层跳数量，请尽可能简单地保持部署。例如，如果五第3层跳存在主机随路信令(CAS)设备和客户端的基础设施之间，它能创建管理开销。

使用不正确的解决方案：

- Layer2建立中继创建一非常不理想的Layer2拓扑。
- 第3层sub-interface创建许多额外接口配置。配置的更多接口能创建另外的高架管理和潜在的IP寻址问题。假设没有在基础设施的冗余，网络的每块层有一个入口和出口物理接口。子接口数量的计算是然后(VRF 2个*等级编号在网络的*编号)。我们的示例有两VRF，因此公式是(2个*5 * 2)或20 sub-interface。在冗余被添加后，此编号多比加倍。将其与 GRE 扩展进行比较，要得到相同的最终结果，GRE 扩展只需要四个接口。此比较说明GRE如何减少配置影响。

第 2 层中继

Layer2建立中继在接入层设备不支持sub-interface的方案更喜欢。Catalyst 3560， 3750和4500平台不支持sub-interface。

在连接到平台不支持sub-interface到平台的第3层访问型号中，只有使用第2层建立中继在一端的和在另一侧的使用sub-interface。此配置维护第3层壁橱体系结构的所有好处和仍然解决限制没有在一些平台的子接口技术支持。

建立中继在只链路的一端的其中一个配置Layer2主要的优点是生成树没有介绍回到第3层环境。参见3750接入交换机的3750个相关配置示例。哪些不支持GRE或sub-interface，连接到6500分布式交换机。6500分布式交换机支持GRE和sub-interface。

3750相关配置

在此配置中，本地VLAN的默认设置是在快速以太网1/0/1的VLAN1。此配置未进行更改。然而，VLAN1没有允许在链路间建立中继。允许VLAN对是标记为的仅的VLAN被限制。

没有对交换机对交换机中继线协商或VLAN中继协议(VTP)流量的需要在此第3层拓扑方面。所以，也没有需要对于所有未标签的数据流传送在此链路。因为不打开多余的第2层安全孔，此配置增加体系结构的安全状况。

3750个相关配置示例

```
!--- 3750 Switch configuration, related to connecting it
to a !--- sub-interface capable switch (Catalyst 6500):
! ip vrf DIRTY rd 100:1 ! ip vrf GUEST rd 600:1 !
interface GigabitEthernet1/0/48 description Uplink to
Cat6k switchport trunk encapsulation dot1q switchport
trunk allowed vlan 901-903,906 switchport mode trunk
spanning-tree portfast trunk ! !--- Since the 3750 does
not support sub-interfaces, !--- you must configure one
SVI per transit network: ! interface Vlan901 description
DIRTY_TRANSIT ip vrf forwarding DIRTY ip address
172.26.120.2 255.255.255.252 ! interface Vlan902
description GLOBAL_TRANSIT ip address 172.26.120.6
255.255.255.252 ! interface Vlan906 description
GUEST_TRANSIT ip vrf forwarding GUEST ip address
172.26.120.14 255.255.255.252 ! !--- This configuration
uses EIGRP as the routing protocol !--- of choice in
this document. !--- Each VRF is defined as a separate !-
-- Autonomous System under the Global AS. ! router eigrp
26 ! address-family ipv4 vrf DIRTY network 172.26.120.0
0.0.0.255 autonomous-system 100 no auto-summary exit-
```

```
address-family ! address-family ipv4 vrf GUEST
redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family network 172.26.0.0
```

6500相关配置

在此配置中， dot1q封装用于为了用VLAN 901， 902和906标记帧。当您选择时VLAN在sub-interface标记使用，您不能使用在交换机的VLAN数据库已经定义本地的VLAN号。

6500个相关配置示例

```
!--- 6500 Switch configuration, related to connecting it
!--- to a non-sub-interface capable switch (Catalyst
3750): ! ip vrf DIRTY rd 100:26 ! ip vrf GUEST rd 600:26
! interface FastEthernet1/34 description NAC LAB - 3750
no ip address ! interface FastEthernet1/34.901
encapsulation dot1Q 901 ip vrf forwarding DIRTY ip
address 172.26.120.1 255.255.255.252 ! interface
FastEthernet1/34.902 encapsulation dot1Q 902 ip address
172.26.120.5 255.255.255.252 ! interface
FastEthernet1/34.906 encapsulation dot1Q 906 ip vrf
forwarding GUEST ip address 172.26.120.13
255.255.255.252 ! !--- EIGRP is the routing protocol of
choice in this document. !--- Each VRF is defined as a
!--- separate Autonomous System under the Global AS. !--
- See Configure Routing for the VRF for more
information. ! router eigrp 26 network 172.26.0.0
0.0.255.255 no auto-summary passive-interface Vlan1
redistribute static ! address-family ipv4 vrf DIRTY
autonomous-system 100 network 172.26.120.0 0.0.0.3
network 172.26.160.0 0.0.0.255 no auto-summary no
default-information out redistribute static route-map
gw-route exit-address-family ! address-family ipv4 vrf
GUEST redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family !
```

配置VRF的路由

如讨论前在重要使用考虑VRF-Lite部分， VRF-Lite支持BGP、OSPF和EIGRP。在本例中配置示例，EIGRP选择，因为它是思科为在园区网络的实施推荐的路由协议快速收敛哪里要求。

注意： OSPF同样好地与VRF-Lite一起使用，象BGP。

注意： BGP要求，如果设计要求流量“漏”在VRF之间。

VRF的路由与EIGRP配置示例

```
!
!--- This base routing protocol configuration handles
the routing !--- for the Global Routing Table. ! router
eigrp 26 network 172.26.50.0 0.0.0.255 network
172.26.51.0 0.0.0.255 network 172.26.52.0 0.0.0.255
network 172.26.55.0 0.0.0.255 network 172.26.60.0
0.0.0.255 network 172.26.61.0 0.0.0.255 network
172.26.62.0 0.0.0.255 network 172.26.120.4 0.0.0.3
network 172.26.176.0 0.0.0.255 network 172.26.254.1
0.0.0.0 no auto-summary passive-interface Vlan1
```

```
redistribute static ! !--- You must define an address
family for each VRF !--- that is to be routing using the
routing protocol. !--- Routing protocol options such as
auto-summarization, !--- AS number, and router id are
all configured under the !--- address family. EIGRP does
not form a neighbor !--- relationship without the AS
specified under the address family. !--- Also, this AS
number needs to be unique for !--- each VRF and cannot
be the same as the global AS number. ! address-family
ipv4 vrf DIRTY autonomous-system 100 network
172.26.120.0 0.0.0.3 network 172.26.160.0 0.0.0.255 no
auto-summary no default-information out redistribute
static route-map gw-route exit-address-family ! address-
family ipv4 vrf GUEST redistribute static network
172.26.120.0 0.0.0.255 autonomous-system 600 no auto-
summary exit-address-family !
```

在全球路由表和坏的VRF之间的路由流量

根据美洲台部署需求，通过从网络的不信任或坏的侧的流量到委托或清洗网络的侧可能是必要的。例如，修正服务能潜在实际在Cisco NAC设备的委托侧。一旦活动目录单一登录部署，通过流量的一子集到活动目录为了允许交互登录Kerberos票交换，等等是必要的。

无论如何，重要的是非常全球路由表会到达坏的VRF，并且坏的VRF会到达全球路由表，如果任何数据需要通过在两个之间。这由方法在表8.典型地处理。

坏的VRF默认为Cisco NAC设备的不信任或坏的接口。全局仅有静态路由对认为坏的VLAN的子网。那些静态路由点思科美洲台服务器的干净的(委托的)接口作为下一跳。

图8 –*路由流*

在Cisco NAC设备的不信任或坏的侧的第一第3层跳再分布默认路由到路由进程对Cisco NAC设备的该点。在委托的第一第3层跳或清洗Cisco NAC设备的侧再分布属于在接入层的子网的静态路由(在这种情况下172.26.123.0/26)的坏的VLAN。

注意： 在Cisco NAC设备的反面的第一第3层跳可以在同样View (物理设备，但是用不同的VRF。

注意： 在用于本文的拓扑里，思科美洲台服务器的不信任或坏的侧在VRF，而委托或清洗Cisco NAC设备的侧保持在全球路由表里。然而，两个接口连接到同一数据中心交换机。

思科美洲台第3层OOB VRF-Lite配置示例

为了成功部署思科美洲台OOB解决方案，您需要配置美洲台组件为了匹配希望的体系结构。图9是在此部分使用为了显示思科美洲台管理器、思科美洲台服务器和边界交换机相关配置一美洲台第3层OOB的与VRF-Lite部署的第3层思科美洲台OOB逻辑网络图表。

图9 –*思科美洲台第3层OOB逻辑拓扑*

完成在这些部分的步骤为了配置第3层雷亚尔德蒙特罗伊IP OOB VRF思科美洲台部署：

步骤 1：配置边界交换机

这些配置示例显示，请还创建两VLAN (坏和访客)在边界交换机。

现有制作VLAN (VLAN 200)使用所有公司系统。此示例创建VLAN，他们相关的转接网络，并且分

配两个到正确VRF。实施在思科美洲台服务器发生，因此您不需要应用ACL到每个VLAN在交换机。

未经鉴定的角色：VLAN 100，坏的VRF配置示例

```
!--- Define the DIRTY VRF. ip vrf DIRTY rd 100:3 !---
Create the SVI for the DIRTY VLAN. interface Vlan100 ip
vrf forwarding DIRTY ip address 172.26.123.1
255.255.255.224 ip helper-address vrf DIRTY 172.26.51.11
!--- Create the SVI for the DIRTY_TRANSIT_NETWORK.
interface Vlan301 ip vrf forwarding DIRTY ip address
172.26.120.50 255.255.255.252 !--- Set the allowed VLAN
on the trunk. interface FastEthernet1/0/48 switchport
trunk allowed vlan add 301 !--- Set up the routing for
the VRF. router eigrp 26 address-family ipv4 vrf DIRTY
network 172.26.0.0 autonomous-system 100 no auto-summary
exit-address-family
```

访客角色：VLAN 600，访客VRF配置示例

```
!--- Define the GUEST VRF. ip vrf GUEST rd 600:3 !---
Create the SVI for the GUEST VLAN. interface Vlan600 ip
vrf forwarding GUEST ip address 172.26.123.193
255.255.255.224 !--- Create the SVI for the
DIRTY_TRANSIT_NETWORK. interface Vlan306 ip vrf
forwarding GUEST ip address 172.26.120.62
255.255.255.252 !--- Set the allowed VLAN on the trunk.
interface FastEthernet1/0/48 switchport trunk allowed
vlan add 306 !--- Set up the routing for the VRF. router
eigrp 26 address-family ipv4 vrf GUEST network
172.26.0.0 autonomous-system 600 no auto-summary exit-
address-family
```

步骤 2：配置核心交换机

在此部分的配置示例显示Collapse Core的仿真用Catalyst 3750-E交换机。在多数环境，这不是边缘中集集团交换机。然而，交换机在用于本文的实验室环境被建立了。

还创建转接网络的四VLAN，两坏的VLAN的和两访客的VLAN。请参阅图 10。

- 坏的VLANVLAN 301坏从挖出果核的边缘VLAN 901坏从核心到数据中心
- 访客 VLAN从挖出果核的边缘的VLAN 306访客VLAN 906访客从核心到数据中心

转接网络从核心的边缘和核心的一秒钟被建立对数据中心。必须完成转接网络为了坏和访客VRF。如果标记交换启用而不是VRF-Lite，这不是必要的。

注意： 本文着重VRF-Lite，并且标记交换考虑外范围。

图10 –*转接网络*

::

VLAN 301坏从挖出果核的边缘;VLAN 901坏从核心到数据中心配置示例

```
!--- This is the core switch. !--- Define the DIRTY VRF.
ip vrf DIRTY rd 100:1 !--- Create the SVI for the DIRTY
VLANs. interface Vlan301 desc This is the Transit
Network between the Edge & Core ip vrf forwarding DIRTY
ip address 172.26.120.49 255.255.255.252 interface
```

```
Vlan901 desc This is the Transit Network between the
Core and the DC ip vrf forwarding DIRTY ip address
172.26.120.2 255.255.255.252 !--- Set the allowed VLAN
on the trunks. interface GigabitEthernet1/0/3 switchport
trunk allowed vlan add 301 interface
GigabitEthernet1/0/48 switchport trunk allowed vlan add
901 !--- Set up the routing for the VRF. router eigrp 26
address-family ipv4 vrf DIRTY network 172.26.0.0
autonomous-system 100 no auto-summary exit-address-
family exit-address-family
```

从挖出果核的边缘的VLAN 306访客;VLAN 906访客从核心到数据中心配置示例

```
!--- This is the core switch. ! !--- Define the GUEST
VRF. ip vrf GUEST rd 600:1 !--- Create the SVI for the
GUEST VLANS. interface Vlan306 desc This is the transit
network between the Edge & Core ip vrf forwarding GUEST
ip address 172.26.120.61 255.255.255.252 interface
Vlan906 description Transit Network between Core & DC ip
vrf forwarding GUEST ip address 172.26.120.14
255.255.255.252 !--- Set the allowed VLAN on the trunks.
interface GigabitEthernet1/0/3 switchport trunk allowed
vlan add 306 interface GigabitEthernet1/0/48 switchport
trunk allowed vlan add 906 !--- Set up the routing for
the VRF. router eigrp 26 address-family ipv4 vrf GUEST
network 172.26.0.0 autonomous-system 600 no auto-summary
exit-address-family
```

步骤 3：配置数据中心交换机

当配置示例显示，思科美洲台服务器有两个接口连接对同一6500个数据中心交换机。受信接口在VLAN 60，并且不信任的接口在VLAN 160，在坏的VRF。

1. 还创建连接的四VLAN对核心：坏的VLAN (160)干净的VLAN (60)一坏的转接网络(901)一干净的转接网络(906)添加坏的VLAN到坏的VRF。终止该的访客的DMZ (999)访客VRF用途思科ASA防火墙(出于本文的范围)为了联络来宾用户到互联网和执行网络地址转换(NAT)功能。
2. 创建坏和访客传输sub-interface。在数据中心交换机配置示例显示的命令执行这些任务：定义坏和访客VRF。创建思科美洲台服务器的坏和干净的网络。

数据中心交换机配置示例

```
!--- Define the DIRTY and GUEST VRFs. ip vrf DIRTY rd
100:26 ip vrf GUEST rd 600:26 !--- Create the sub-
interface and switched virtual interface (SVI) !--- for
the DIRTY and GUEST VLANs. interface
FastEthernet1/34.901 desc Transit Network from Core to
DC for DIRTY traffic encapsulation dot1Q 901 ip vrf
forwarding DIRTY ip address 172.26.120.1 255.255.255.252
interface FastEthernet1/34.906 desc Transit Network from
Core to DC for GUEST traffic encapsulation dot1Q 906 ip
vrf forwarding GUEST ip address 172.26.120.13
255.255.255.252 interface Vlan60 desc Trusted (CLEAN)
side of the NAC Server ip address 172.26.60.1
255.255.255.0 interface Vlan160 desc Untrusted (DIRTY)
side of the NAC Server ip vrf forwarding DIRTY ip
address 172.26.160.1 255.255.255.0 interface Vlan999
description GUEST VLAN SVI ip vrf forwarding GUEST ip
address 192.168.26.254 255.255.255.0 !--- Set up the
```

```
routing for the VRFs. router eigrp 26 network
172.26.60.0 0.0.0.255 no auto-summary redistribute
static address-family ipv4 vrf DIRTY autonomous-system
100 network 172.26.120.0 0.0.0.3 network 172.26.160.0
0.0.0.255 no auto-summary redistribute static exit-
address-family address-family ipv4 vrf GUEST network
172.26.0.0 network 192.168.26.0 autonomous-system 600 no
auto-summary redistribute static exit-address-family !--
- Set up the static routes for redistribution for the
VRFs. ip route 172.26.123.0 255.255.255.192 172.26.60.2
ip route vrf DIRTY 0.0.0.0 0.0.0.0 172.26.160.2 ip route
vrf GUEST 0.0.0.0 0.0.0.0 192.168.26.1
```

步骤 4：执行Cisco NAC管理器和服务器的初始设置

Cisco NAC管理器和服务器安装通过控制台访问被执行。安装工具指南您通过管理器和服务器的初始配置。去安装Clean Access管理器和Clean Access服务器为了执行初始设置。

步骤 5：应用许可证给思科美洲台管理器

在您通过控制台后执行初始设置，请访问思科美洲台管理器GUI为了持续配置Cisco NAC管理器和服务器。首先请上传用设备来的管理器和服务器许可证。关于如何上传许可证的更多信息，请去*访问安装*Clean Access管理器和Clean Access服务器的*CAM Web控制台*部分。

注意： 所有Cisco NAC管理器和服务器许可证根据管理器的eth0 MAC地址。在故障切换设置，许可证根据主要的和附属思科美洲台管理器eth0 MAC地址。

步骤 6：从Cisco.com的更新策略在思科美洲台管理器

思科美洲台管理器必须配置为了从中央更新服务器获取定期更新查找在思科。Cisco NAC设备支持的AV/AS产品列表是从提供支持的防病毒和antispyware供应商和被使用产品的版本最当前的矩阵配置防病毒或antispyware规则和防病毒或者antispyware定义更新需求状态评估和修正的一个集中化更新服务器分配的versioned XML文件。此列表为防病毒有规律地更新，并且支持和版本每个思科美洲台代理程序antispyware产品发布并且包括新代理人版本的新产品。列表提供仅版本信息。当思科美洲台管理器下载支持的防病毒和antispyware产品列表时，下载关于什么的信息最新的版本是为防病毒和antispyware产品。它不是下载的实际补丁文件或病毒定义文件。凭此信息，代理程序能然后触发本地防病毒或antispyware应用程序为了执行更新。关于更新如何的更多信息获取，请去配置座席登录和客户端状态评估的Cisco NAC设备的*客户端机器*部分的*要求座席登录*。

步骤 7：从一第三方Certificate Authority (CA)的安装证书

在安装时，思科美洲台管理器和思科美洲台服务器的配置工具脚本要求您生成一临时SSL证书。对于实验室环境，您能继续使用自签名证书。然而，他们没有为生产网络推荐。

关于安装在思科美洲台管理器的证书的更多信息从第三方CA，请去管理CAM的*设置系统时期*和*Clean Access服务器直接访问Web控制台*部分。

注意： 如果在实验室环境、思科美洲台管理器和思科美洲台服务器使用赛弗符号证书每需要委托其他的证书。这要求您上传两个的证书作为委托认证机关下面**SSL >信任证书权限**。

步骤 8:复核思科美洲台服务器设置

记住的多数重要事情为一成功的美洲台设计是作为坏分类的流量必须流到美洲台服务器的不信任侧，因为图11显示：

图11 –*思科美洲台服务器部署*

步骤 9：添加思科美洲台服务器到思科美洲台管理器

完成这些步骤为了添加思科美洲台服务器到思科美洲台管理器：

1. 单击**CCA服务器**在设备管理窗格下。请参阅图 12。
2. 点击新的Server选项。
3. 请使用服务器IP地址方框为了添加思科美洲台服务器的受信接口的IP地址。
4. 在服务器位置方框中，请进入**OOB思科美洲台服务器**作为服务器位置。
5. 从服务器类型下拉列表选择**带外雷亚尔德蒙特罗伊IP网关**。
6. 单击**添加Clean Access服务器**。

图12 –*添加思科美洲台服务器到思科美洲台管理器*

注意： 思科美洲台管理器和思科美洲台服务器必须委托彼此的CA为了管理器能成功地添加服务器。

在您添加思科美洲台服务器后，在列表看起来在服务器选项卡下列表。请参阅图 13。

步骤 10：配置思科美洲台服务器

完成这些步骤为了配置思科美洲台服务器：

1. 点击服务器选项卡列表。
2. 点击Manage图标Cisco NAC服务器的为了继续配置。

图13 –*思科美洲台管理器管理的思科美洲台服务器*

在您点击Manage图标后，在图显示的屏幕14上出现。

步骤 11：Enable (event)第3层支持

完成这些步骤为了启用第3层支持：

1. 选择Network选项。
2. 检查**Enable (event) L3支持**复选框。
3. 检查**Enable (event) L3严格模式阻塞有美洲台代理程序**复选框。的**NAT设备**
4. 单击**更新**。
5. 重新启动思科美洲台服务器如提示。

图14 –*思科美洲台服务器网络详细信息*

注意： 总是请生成思科美洲台服务器的证书用其不信任的接口的IP地址。一基于域名的证书，名称需要解决到不信任的接口IP地址。当端点与服务器的不信任的接口联络为了开始美洲台进程时，服务器重定向用户对证书主机名或IP。如果证书指向受信接口，登录过程不正确地作用。

步骤 12：配置静态路由

完成这些步骤为了配置静态路由：

1. 在思科美洲台服务器重新启动，回到服务器并且继续配置后。思科美洲台服务器必须使用不信任的接口为了与在未经鉴定的VLAN的端点联络。
2. 选择**先进>静态路由**为了添加路由到未经鉴定的VLAN。
3. 填写未经鉴定的VLAN的适当的子网。
4. 单击**添加路由**。
5. 选择这些路由的**不信任的接口[eth1]**。

图15 –*添加静态路由到达未经鉴定的用户子网*

步骤 13：交换机的设置配置文件在思科美洲台管理器

完成这些步骤为了设置交换机的配置文件在思科美洲台管理器：

1. 选择**OOB Management> Profiles>设备>** Edit。
2. 填写设备配置文件信息。请使用图16作为指南。每交换机关联与配置文件。添加思科美洲台管理器将管理边界交换机的每种类型的一配置文件。在本例中， 3750交换机被管理。**图16 –*用于的SNMP配置文件管理交换机***
3. 设置SNMP的交换机配置。配置在思科美洲台管理器配置的同样SNMP读/写社区字符串的边界交换机。`snmp-server community Cisco123 RO`
   `snmp-server community Cisco1234 RW`
4. 选择**OOB Management>新建的Profiles> Port>**。请参阅图 17。对于单个端口控制，请配置包括默认未经鉴定的VLAN和默认访问VLAN的端口配置文件在**OOB Management> Profiles>波尔特下**。在访问VLAN部分，请指定用户角色VLAN使用下拉式的访问VLAN。思科美洲台管理器更改未经鉴定的VLAN对根据VLAN VLAN的访问定义在用户属于的角色。定义端口配置文件为了控制端口VLAN根据实现的用户角色和VLAN。验证VLAN是未经鉴定的VLAN (VLAN 17)未经鉴定的设备最初分配。默认访问VLAN是员工VLAN (VLAN14)。此VLAN，如果已认证的用户不安排基于任务的VLAN定义，使用。访问VLAN能改写默认VLAN到用户角色VLAN，定义在用户角色下。关于安装用户角色的更多信息，请参阅步骤17 ：配置用户角色。LDAP映射可以用于为了映射在美洲台的用户角色对LDAP组。欲知更多信息，参考NAC(CCA) 4.x ：某些角色的地图用户使用IDAP配置示例。**图17 –*管理交换机端口的波尔特配置文件*注意**：您能也定义VLAN名称而不是ID。如果定义了VLAN名称，您能有在另外交换机的VLAN ID在校园间。然而，同样VLAN名称附加对一个特定的角色。其它选项是可用的在端口配置文件下为IP版本并且更新选项。把显示的页移下来为了发现这些选项。如果用户是在IP电话后，请不选定**跳动端口，在VLAN是更改的**复选框。后如果这被检查，能可能重新启动IP电话，当端口重新启动时。**图18 –*多种选项可用的下面波尔特配置文件***

步骤 14：配置SNMP接收方设置

除设置读取/写入的SNMP团体字符串之外，您也需要配置思科美洲台管理器为了收到从交换机的SNMP陷阱。当用户从端口时，连接并且断开这些陷阱被发送。当思科美洲台服务器发送一个特定的端点的MAC IP地址信息对管理器时的，管理器能为MAC/IP和交换机端口构件映射表内部地。

1. 挑选**OOB Management> Profiles> SNMP接收方**。
2. 配置SNMP陷阱设置，此图显示：**图19 –*思科美洲台管理器SNMP收集SNMP陷阱的接收方设置和通知***
3. 为了配置SNMP陷阱的交换机设置，请增加默认交换机Clean Access管理器(CAM)冲洗计时器对每思科最佳实践推荐的1个小时美洲台OOB的。CLI示例显示`mac-address-table`参数集到3600。设置对1个小时的计时器使频率MAC通知降低已经发送在连接的设备外面到思科美洲台管理器。请使用**trap命令的来源**为了指定使用派出陷阱的源地址。随意地，请配置联结和链路

中断陷阱为了发送对思科美洲台管理器(没显示在CLI示例)。这些陷阱在终端主机没有在IP电话后连接的部署方案仅使用。**注意：** Snmp inform，因为他们比SNMP陷阱，可靠推荐。并且，请考虑SNMP的服务质量(QoS)在高数据流网络环境。

步骤 15：添加交换机作为在思科美洲台管理器的设备

完成这些步骤为了添加交换机作为在思科美洲台管理器的设备：

1. 选择**OOB Management>设备>设备>**New。请使用创建的交换机配置文件在步骤13为了添加交换机。
2. 在设备配置文件下，请使用您创建的配置文件。当您添加交换机时，请勿更改默认端口配置文件值。**图20 –*添加在思科美洲台管理器的边界交换机通过SNMP控制***
3. 在交换机被添加到思科美洲台管理器后，您能选择您要管理的端口。

步骤 16：配置美洲台能将管理的设备的交换机端口

完成这些步骤为了配置美洲台能将管理的设备的交换机端口。

1. 选择**OOB Management>设备开关[IP address] > Ports>列表**为了看到您能管理的可用的交换机端口。**图21 –*波尔特控制一托管型交换机的选择联机***注意：** 请勿留下默认配置文件作为“未管制”，直到您能静态标记适当的接口作为“未管制”。在上行链路端口和需要保持未管制的所有其他开-关端口以后设置;然后请更改默认对您受控的端口配置文件。失败按此顺序能导致较不比理想结果。
2. 挑选**OOB Management>设备开关[IP address] > Ports>设法**为了立即管理几个端口。

图22 –*管理有加入选项的多个端口*

步骤 17：配置用户角色

在本例中，对应于每个角色的VLAN在边界交换机已经创建。

1. 选择**用户管理>用户角色>** Edit**角色**并且创建雇员角色，此图显示：**图23 –*创建雇员角色并且映射数据VLAN***
2. 选择**用户管理>用户角色>** Edit**角色**并且创建访客角色，此图显示：**图24 –*创建访客角色并且映射访客VLAN***

第 18 步：添加用户并且分配合适用户角色

在园区环境，您将集成外部验证服务器并且映射用户对一个特定的角色通过LDAP属性。此示例以角色使用一个本地用户和关联该本地用户。

第 19 步：定制Web的洛金用户登录页

默认登录页在思科美洲台管理器已经创建。您能或者定制登录页为了更改Web门户的外观。对于美洲台第3层OOB解决方案，您必须下载ActiveX或Java组件到末端客户端为了执行这些任务：

- 拿来客户端机器的MAC地址。
- 执行IP地址版本并且更新。

1. 选择**Administration >用户页**。
2. 编辑页为了启用选项，此图显示：

图25 – ***Web的洛金用户页定位***

第 20 步：定制用户角色的思科美洲台代理程序

完成这些步骤为了定制用户角色的思科美洲台代理程序：

1. 选择**设置的设备管理> Clean Access** >General **>座席登录**。您能配置思科美洲台管理器为了使代理程序必需对于所有用户角色。在本例中，代理程序对于雇员角色是必需的。承包商和访客角色必须使用Web登录。
2. 检查**要求使用代理程序**复选框。

图26 –*为雇员角色要求的座席登录*

步骤21 ：分配思科美洲台代理程序的发现号主机

思科美洲台代理软件分配、安装和配置报道配置座席登录和客户端状态评估的Cisco NAC设备。此示例配置在思科美洲台管理器的发现主机。

选择**设备管理> Clean Access > Clean Access代理程序>安装**：

图27 –*发现思科美洲台代理程序的主机*

如果思科美洲台代理程序从思科美洲台服务器，下载发现号Host Field被事前填充。请参阅图 27。

注意： 在一第3层OOB用VRF型号，发现号主机典型地设置是思科美洲台管理器的DNS名或IP地址，在干净的网络存在。默认情况下由于从“坏的”网络的所有流量通过思科美洲台服务器路由，发现信息包自动地流经服务器。描述的通信流此处是其中一个好处对VRF方法。它提供一一致，可预测的体验。欲知更多信息，请参阅思科美洲台进程流。

步骤 22：Web洛金

完成这些步骤为了通过Web登陆：

1. 连接客户端机器使用思科美洲台管理器控制的其中一个边缘端口。客户端机器在未经鉴定的VLAN安置。确保计算机收到从未经鉴定的VLAN子网的一个IP地址。
2. 打开浏览器为了执行登录。假定是此客户端机器没有已经安装的一个思科美洲台代理程序。如果所有DNS条目重定向对思科美洲台服务器的不信任的接口，对登录页的自动浏览器重定向。如果它不，去特定URL例如guest.nac.local为了执行登录：

图28 – ***Web登录页***

步骤23 ：座席登录

您能分配思科美洲台代理程序正如所有其它软件应用程序对最终用户使用思科美洲台服务器，或您能强制它。

注意： 关于代理程序分配和安装的详细信息是可用的在Cisco NAC设备- Clean Access管理器配置指南。

出现的此图显示屏幕，当代理程序激活时：

图29 –*座席登录*

1. 选择从服务器下拉列表的服务器。
2. 输入用户名。
3. 输入密码。
4. 单击 Login。图30和31显示出现：的屏幕。**图30 –*思科美洲台代理程序执行的IP版本或更新*图31 –*指示全双工网络访问的思科美洲台代理程序在IP刷新以后***
5. 单击 Ok。

附录

高可用性

其中每一个各自的思科美洲台管理器和思科美洲台服务器在解决方案在高性能的模式可以配置，含义有在激活待机配置里操作的两个设备。

美洲台管理器

您能配置有两个美洲台管理器在激活待机配置里操作的高性能的模式的思科美洲台管理器。在管理器的整个配置在数据库存储。暂挂管理器与在活动管理器的数据库同步其数据库。做的所有配置更改对活动管理器立即推送对暂挂管理器。这些关键点提供高性能的管理器操作一高层次摘要：

- 思科美洲台管理器高性能的模式是方面一个暂挂管理器作为备份给一个活动管理器的激活或被动服务器配置在。
- 活动思科美洲台管理器执行系统的所有任务。暂挂管理器监控活动管理器并且保持其数据库同步与活动管理器的数据库。
- 两个思科美洲台管理器共享Eth0受信接口的虚拟服务IP。请使用此服务IP SSL证书。
- 主要的和附属思科美洲台管理器交换UDP心跳信息包每2秒。如果检测信号计时器超时，有状态故障切换发生。
- 为了保证一个活动思科美洲台管理器总是可用的，其受信接口(Eth0)必须是UP。您必须避免管理器是活跃的情况，但是不可取得通过其受信接口。此情况发生，如果暂挂管理器收到从活动管理器的心跳信息包，但是活动管理器的Eth0接口发生故障。当活动管理器的Eth0接口变得不可用时，林克检测机制允许暂挂管理器知道。
- 您能选择“自动地配置”在**Administration > CCA Manager>故障切换**页的Eth1接口。然而，您必须手工配置其他(Eth2或Eth3)高性能的接口用IP地址和网络屏蔽，在您配置在思科美洲台管理器前的高可用性。
- Eth0、Eth1和Eth2/Eth3接口可以用于心跳信息包和数据库同步。另外，所有可用的序列(COM)接口可能也用于心跳信息包。如果使用超过一这些接口，故障切换发生，只有当所有检测信号接口发生故障。

注意： 思科美洲台管理器高性能的对不可能由第3层链路分离。

欲了解更详细的信息，参考思科美洲台管理器文档在配置高可用性。

思科美洲台服务器

为了提供防护单点故障，您能配置在高性能的模式的思科美洲台服务器。思科美洲台服务器的高性能的模式类似于那思科美洲台管理器并且使用激活待机配置。思科美洲台服务器仍然共享一个虚拟IP地址(呼叫服务IP)，但是他们不共享虚拟MAC地址。

这些关键点提供高性能的思科美洲台服务器操作高水平概述：

- 思科美洲台服务器高性能的模式是方面一个暂挂思科美洲台服务器设备作为备份到一个活动思科美洲台服务器的一个主动或被动服务器配置在。
- 活动思科美洲台服务器执行系统的所有任务。由于大多数服务器配置在思科美洲台管理器存储，当服务器故障切换发生时，管理器推送配置到重新激活的服务器。
- 暂挂思科美洲台服务器不转发在其接口之间的任何数据包。
- 暂挂思科美洲台服务器通过检测信号接口(序列和一个或更多UDP接口)监控活动服务器的健康。(如果Eth2或Eth3接口不是可用的)，心跳信息包在serial interfaces、专用的Eth2接口、专用的Eth3接口或者Eth0/Eth1接口可以被发送。
- 主要的和附属思科美洲台服务器交换UDP心跳信息包每两秒。如果检测信号计时器超时，有状态故障切换发生。
- 除基于检测信号的故障切换之外，思科美洲台服务器也提供根据Eth0或Eth1链路故障的基于林克的故障切换。服务器发送ICMP Ping数据包对外部IP地址通过Eth0和Eth1接口。只有当一个思科美洲台服务器能ping外部地址，故障切换发生。

欲了解更详细的信息，参考思科美洲台服务器文档在配置高可用性。

活动目录SingleSignOn (活动目录SSO)

Windows活动目录SSO自动地是Cisco NAC设备的能力给登录用户已经验证对一个后端Kerberos域控制器(激活目录服务器)。在您已经登录域后，此能力排除需要登录思科美洲台服务器。欲了解更详细的信息关于配置在Cisco NAC设备的活动目录SSO，请去配置活动目录单一登录。

Windows域环境考虑事项

为准备美洲台部署，对登录脚本策略的更改可能要求。Windows登录脚本可以分类作为启动或关闭和登录或者注销脚本。Windows在“计算机上下文运行启动和关闭脚本”。运行脚本只作用，如果Cisco NAC设备打开特定的角色的脚本要求的适当的网络资源，当这些脚本被执行在PC启动或关闭时，典型地是未经鉴定的角色。登录和注销脚本在“用户上下文被执行”，含义登录脚本执行，在用户登陆通过Windows姬娜后。登录脚本可以不能执行，如果验证或客户端机器状态评估不完成，并且网络访问没有授权及时。这些脚本可能被思科美洲台代理程序启动的IP地址刷新也中断在OOB登录事件以后。关于对登录脚本的必要的更改的更多信息，请去Windows GPO脚本和思科美洲台互通性。

配置座席登录和客户端状态评估的Cisco NAC设备

思科美洲台代理程序和思科美洲台Web代理程序为客户端机器提供本地状态评估和修正。用户下载并且安装思科美洲台代理程序或思科美洲台Web代理程序(只读客户端软件)，能检查主机注册、进程、应用程序和服务。欲了解更详细的信息关于代理程序和状态评估和修正，请去配置座席登录和客户端状态评估的Cisco NAC设备。

相关信息

- Cisco NAC设备支持页面
- 技术支持和文档 - Cisco Systems