与 VMware 的混合模式
适用于思科身份服务引擎

安全访问操作指南系列

作者：Aaron Woland

日期：2012 年 8 月

目录

VMware 部署

简介

本操作指南解释如何使用 VMware 虚拟机 (VM) 上的 ISE 来启用设备分析探测。本指南将展示配置混合 VMware 网络的步骤和启用交换端口分析器 (SPAN) 会话的步骤。本指南假定您了解在 VMware VM 上安装思科身份服务引擎 (ISE) 的要求，且了解如何配置 VMware ESX 服务器和其他 VMware 服务器。有关如何为 VMware 部署配置 ISE 的详细信息，请参阅 ISE 1.1 硬件安装指南：http://www.cisco.com/en/US/docs/security/ise/1.0.4/install_guide/ise104_vmware.html。

注意：有关启用设备分析探测的更多信息，请参阅 HowTo-04-ISE_Bootstrapping 指南。

如何配置混合 VMware 网络

配置混合 VMware 网络

如果思科 ISE 部署在虚拟环境中，妥善配置 VMware 网络以确保混合接口的正常工作是非常重要的。如果思科 ISE 部署在物理设备上，请跳转到“在交换机上配置 SPAN 会话”部分。

按照此步骤将 VMware ESX 服务器上的一个接口配置为专用的混合接口。如果 ESX 服务器上的物理接口不能专用于 SPAN，请按照本文档稍后将介绍的步骤 2 操作。

注意：如要与 VMware 一起部署，请特别注意以下安装指南中列出的各项规格：http://www.cisco.com/en/US/docs/security/ise/1.0.4/install_guide/ise104_vmware.html。尤其是，需要特别留意磁盘大小。如果思科 ISE 在 VMware 中运行，带有许多事件记录，而磁盘空间已耗尽，这可能对部署造成灾难性的后果。请始终遵循推荐的 VMware 大小。

第 1 步 在 VMware VSphere 客户端中选择物理 ESX 服务器。选择 Configuration → Networking，然后选择 **Add Networking**。

第 2 步 系统将启动添加网络向导。在 Connection Types 下，选择 Virtual Machine，然后点击 **Next**。

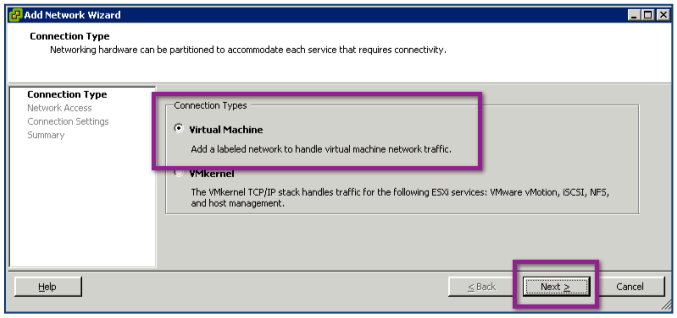

图 1. 添加网络向导

第 3 步 选择要连接至交换机 SPAN 端口的物理接口，然后点击 **Next**。

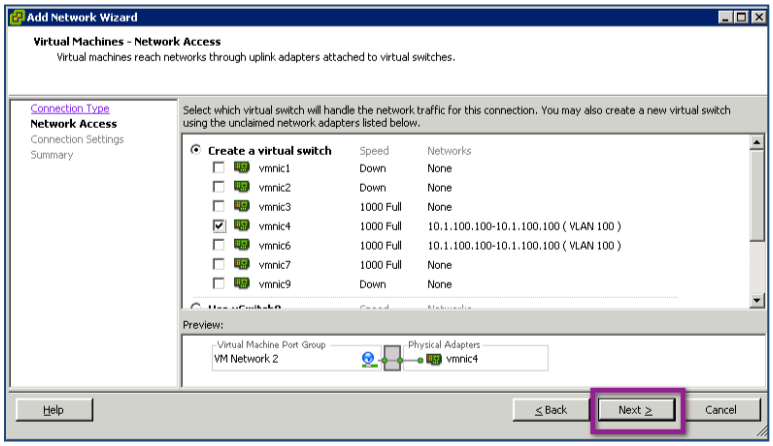

图 2. 选择物理接口

第 4 步 将网络命名为 **SPAN_Session** 或其他任意逻辑名。

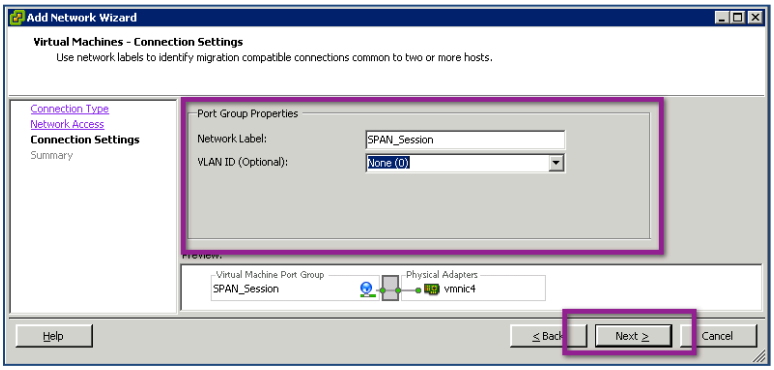

图 3. 为网络命名

第 5 步 选择 **Finish**。

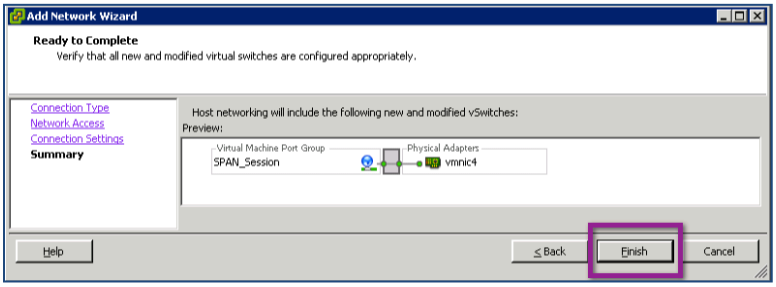

图 4. 完成虚拟交换机的配置

第 6 步 要允许在新创建的虚拟交换机上使用混合流量，请选择 **Properties**。

注意：默认情况下，所有 VMware 网络均会拒绝混合流量。

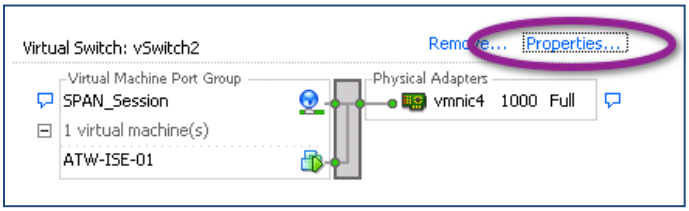

图 5. 设置 vSwitch2 属性

第 7 步 突出显示新的虚拟交换机，然后选择 **Edit**。

第 8 步 选择 Security 选项卡，然后从 Promiscuous Mode 下拉菜单中选择 **Accept** 并点击 **OK**。

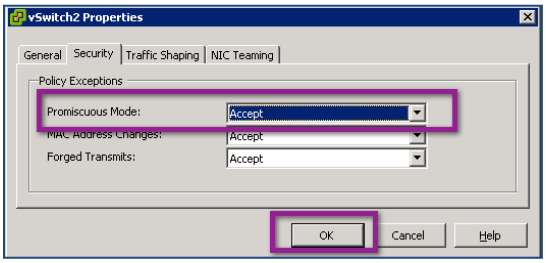

图 6. 接受混合模式

第 9 步 关闭 **vSwitch Properties** 窗口。

第 10 步 修改 **Cisco ISE Virtual Machine** 设置。

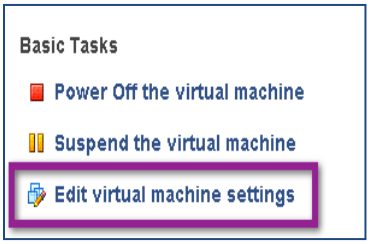

图 7. 修改虚拟机设置

第 11 步 为思科 ISE 选择合适的网络适配器（对思科 ISE 中的 GigabitEthernet 1 来说通常选择 Network Adaptor 2）。

第 12 步 确保 Device Status 已设置为 Connected，且 Connect at power on 已启用。

第 13 步 从 Network Connection 下拉菜单选择新创建的 **SPAN_Session** 网络。

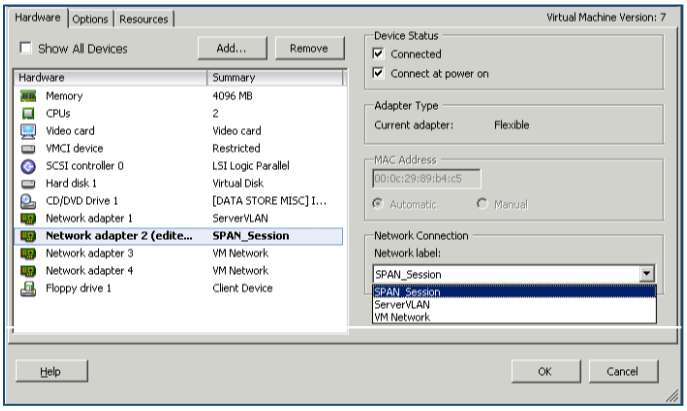

图 8. 虚拟机设置

第 14 步 点击 **OK**。

第 15 步 记录混合接口所连接的交换机端口，以便下一节使用。

注意：VMware ESX 服务器有一项用户友好功能，可显示其已连接接口的思科发现协议信息。图 12 展示了这种情况。

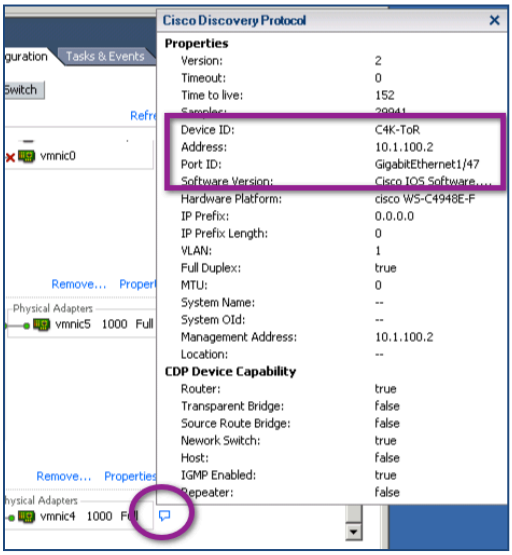

图 9. 思科发现协议

如何配置混合 VMware 端口组

配置混合 VMware 端口组（可选）

配置混合 VMware 网络的第二种方法是在现有 vSwitch 上创建混合端口组。如果物理 SPAN 端口不可能专用于思科 ISE 虚拟机，或者虚拟部署本身不允许从物理交换机复制所有流量而必须从 vSwitch 本身获取，那么这种部署就非常重要。

第 1 步 在 VMware VSphere 客户端中选择物理 ESX 服务器。

第 2 步 选择 Configuration → Networking，然后选择您的 vSwitch 并点击 Properties（图 13）。

图 10. VMware VSphere 客户端

第 3 步 在 vSwitch Properties 窗口中，Ports 选项卡上，点击左下角的 Add [[他们是否需要确认已选中 vSwitch 120 Ports？]]。

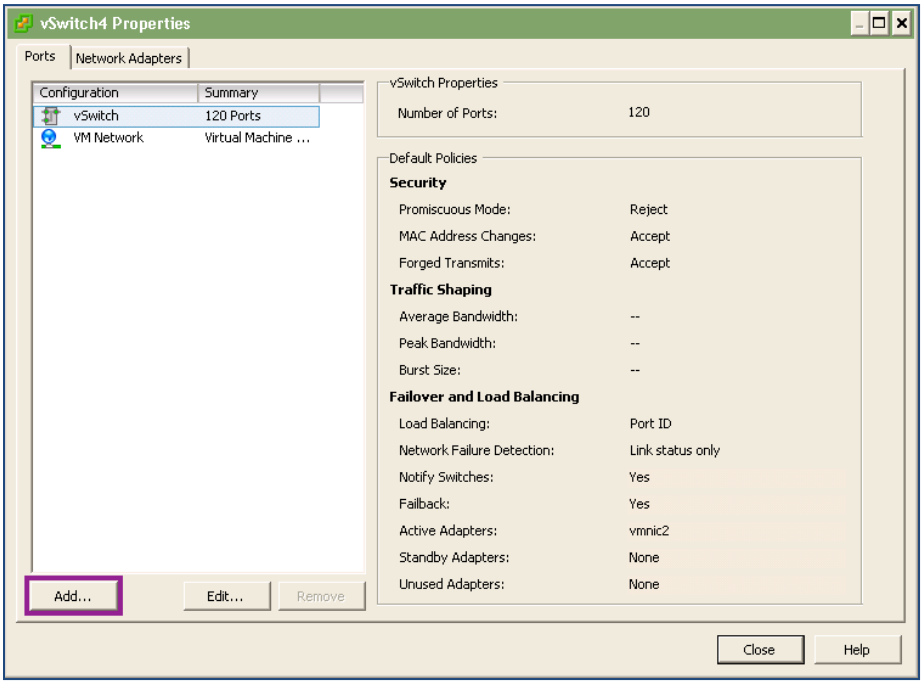

图 11. vSwitch 属性

系统将启动添加网络向导。

第 4 步 在 Connection Types 下，选择 Virtual Machine，然后点击 **Next**。

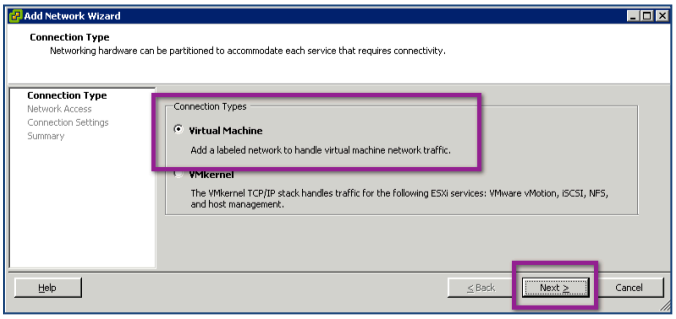

图 12. 连接类型

第 5 步 将端口组命名为 **SPAN_Session** 或其他任意逻辑名。

第 6 步 将 VLAN 设为 **4095** 并点击 **Next**。

注意：这是一个特殊的 VMware VLAN，会侦听 vSwitch 上所有其他 VLAN。

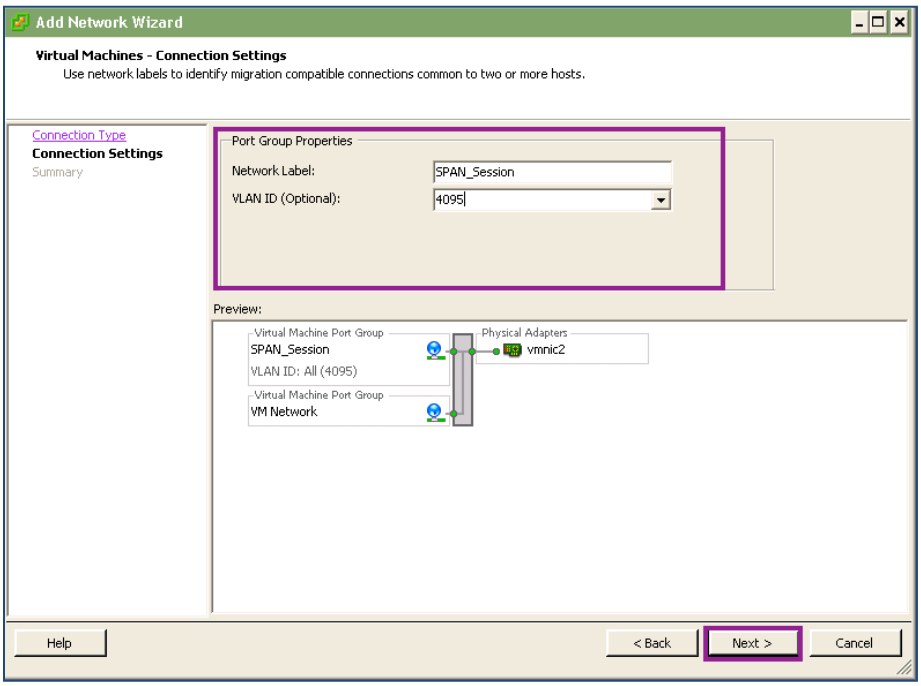

图 13. 端口组属性

第 7 步 选择 **Finish**。

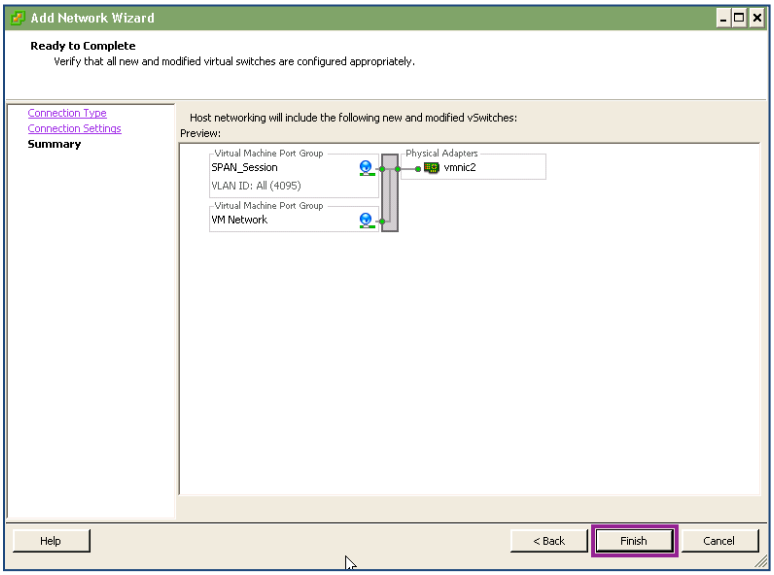

图 14. 预览

第 8 步 突出显示 **new port group**。
第 9 步 选择 **Edit**。
第 10 步 选择 **Security** 选项卡。
第 11 步 从 Promiscuous Mode 下拉菜单中选择 **Accept**。
第 12 步 点击 **OK**。

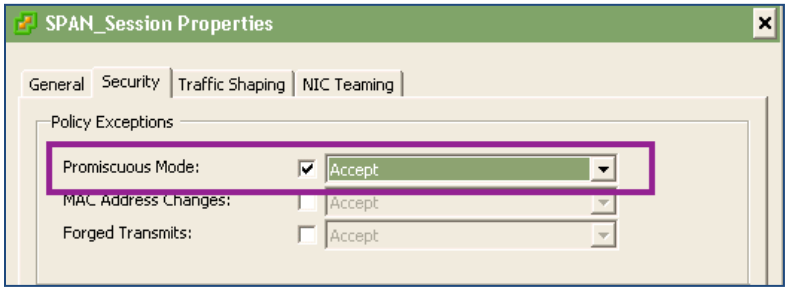

图 15. 混合模式

第 13 步 关闭 **vSwitch Properties** 窗口。
第 14 步 修改思科 ISE 虚拟机设置。

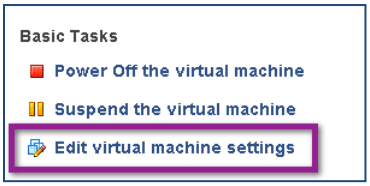

图 16. 修改虚拟机设置

第 15 步 为思科 ISE 选择合适的网络适配器（对思科 ISE 中的 GigabitEthernet1 来说通常选择 Network Adaptor 2）。

第 16 步 确保 Device Status 已设置为 Connected，且 Connect at power on 已启用。

第 17 步 从 Network Connection 下拉菜单选择新创建的 **SPAN_Session** 网络。

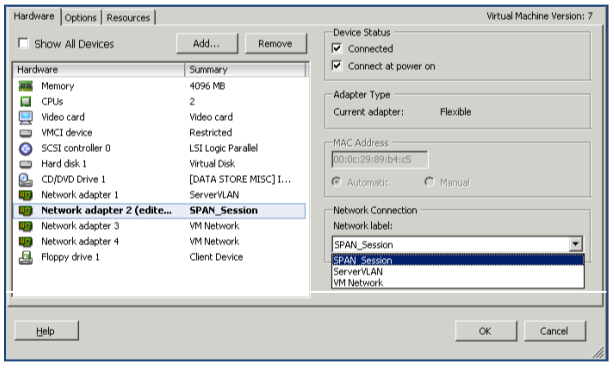

图 17. 虚拟机设置

第 18 步 点击 **OK**。

如何配置 SPAN 会话

配置交换机上的 SPAN 会话

第 1 步 进入全局配置。[[哪里？明确一点。]]

第 2 步 配置 SPAN 会话源。以下是示例：

```
C4K-ToR(config)#monitor session 1 source vlan 100 both
```

第 3 步 配置 SPAN 会话目标。以下是示例：

```
C4K-ToR(config)#monitor session 1 destination interface g 1/47
```

第 4 步 验证端口现在是否处于监控状态。

```
C4K-ToR(config)#do show int status | i 47
Gi1/47 monitoring  1  a-full a-1000 10/100/1000-TX
```

配置 IP HELPER 语句

要与 DHCP 探测配合使用以进行思科 ISE 分析，应该向网络第 3 层接口上的 **ip helper-address** 语句添加思科 ISE 策略节点。此节点添加除了会将所有 DHCP 请求发送到环境中的生产 DHCP 服务器外，还会发送一份副本到思科 ISE。

第 1 步 进入全局配置模式。[[哪里？明确一点。]]

第 2 步 进入接入 VLAN 第 3 层接口的接口配置模式，并将思科 ISE 添加为 **ip helper-address** 的另一个目标。以下是示例：

```
interface Vlan10
 ip address 10.1.10.1 255.255.255.0
 ip helper-address 10.1.100.100  ! - this is the DHCP Server
 ip helper-address 10.1.100.3    ! - this is the ISE Server
```

附录 A：参考

Cisco TrustSec 系统：

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

设备配置指南：

思科身份服务引擎用户指南：
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

有关思科 IOS 软件、思科 IOS XE 软件和思科 NX-OS 软件版本的更多信息，请参阅以下 URL：

- 对于 Cisco Catalyst 2900 系列交换机：
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 3000 系列交换机：
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 3000-X 系列交换机：
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 4500 系列交换机：
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 6500 系列交换机：
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- 对于 Cisco ASR 1000 系列交换机：
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html
- 对于思科无线 LAN 控制器：
  http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html