添加 ID 存储和创建身份验证策略

安全访问操作指南系列

作者：Hosuk Won

日期：2012 年 8 月

目录

VMware 部署

简介

本操作指南介绍如何使用 VMware 虚拟机 (VM) 上的 ISE 启用设备分析探测功能。本文档还将说明配置混合 VMware 网络以及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，并熟悉所使用的两台 VMware ESX 服务器和其他 VMware 服务器的配置过程。有关为 VMware 部署配置 ISE 的详细信息，请参阅以下网址中的《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：请参阅《HowTo-04-ISE_Bootstrapping 指南》，了解有关启用设备分析探测功能的更多信息。

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，那么妥善配置 VMware 网络就对确保混合接口正常工作十分重要。如果思科 ISE 部署在物理设备中，那么可以直接跳至“配置交换机上的 SPAN 会话”部分。

本程序可用于将 VMware ESX 服务器上的一个专用接口配置和指定为混合接口。如果 ESX 服务器上的物理接口无法专用于 SPAN，请按照本文档后面的程序 2 操作。

注：如果通过 VMware 进行部署，请特别注意以下网址提供的安装指南中列出的规格：http://www.cisco.com/en/US/docs/security/ise/1.0.4/install_guide/ise104_vmware.html。尤其需要注意的是，磁盘容量可能真的会带来问题。如果思科 ISE 在具有许多已记录事件的 VMware 中运行，当磁盘空间耗尽时，会对部署造成灾难性的后果。请始终遵循推荐的 VMware 大小。

步骤 1 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”（图 3）。

步骤 2 系统将启动“Add Network Wizard”向导。在“Connection Types”下，选择“Virtual Machine”，然后点击“Next”（图 4）。

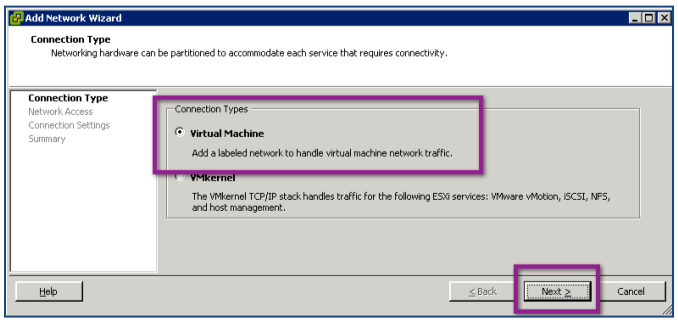


图 1. 添加网络向导

步骤 3 选择要连接至交换机 SPAN 端口的物理接口，然后点击“Next”（图 5）。

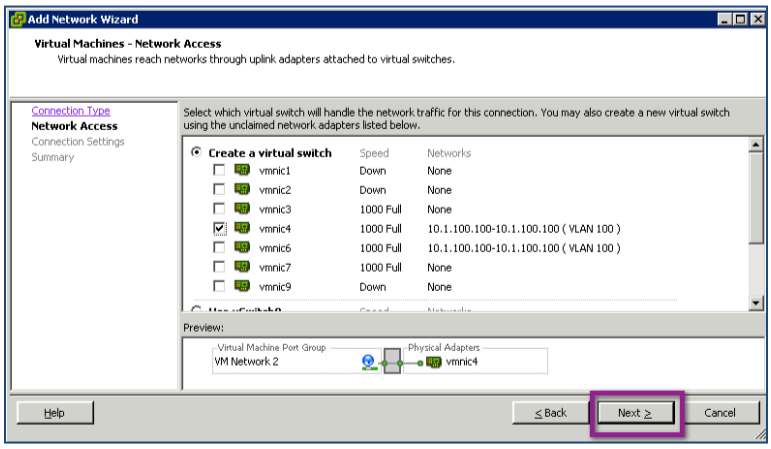


图 2. 选择物理接口

步骤 4 将网络命名为“SPAN_Session”或任何其他逻辑名称（图 6）。

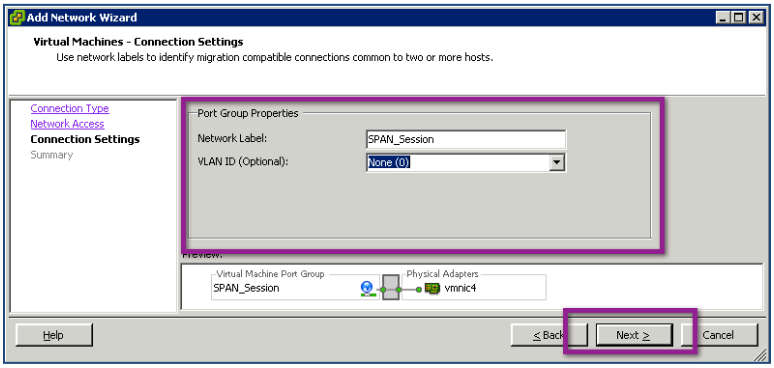
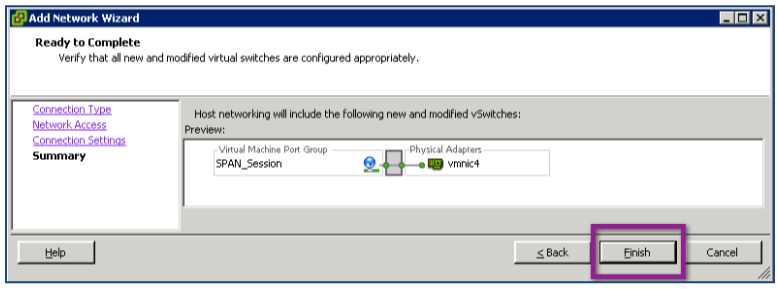


图 3. 为网络命名

步骤 5 选择“Finish”（图 7）。

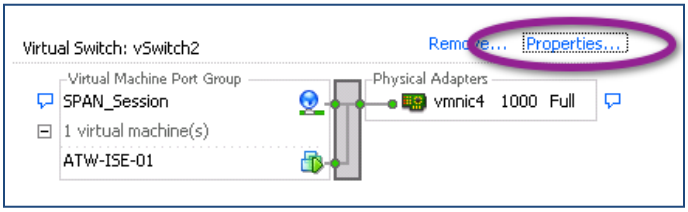
图 7 完成虚拟交换机的配置



步骤 6 要启用在新创建的虚拟交换机上的混合流量，请选择“Properties”（图 8）。

注：默认情况下，所有 VMware 网络均会拒绝混合流量。

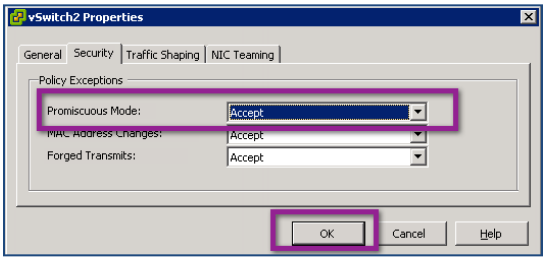
图 8 设置 vSwitch2 属性



步骤 7 突出显示新的虚拟交换机，然后选择“Edit”。

步骤 8 选择“Security”选项卡，然后从“Promiscuous Mode”下拉菜单中选择“Accept”并点击“OK”（图 9）。

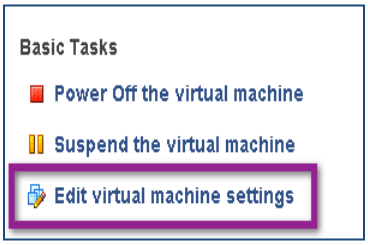
图 9 接受混合模式



步骤 9 关闭 vSwitch 属性窗口。

步骤 10 编辑思科 ISE 虚拟机设置（图 10）。

图 10 编辑虚拟机设置

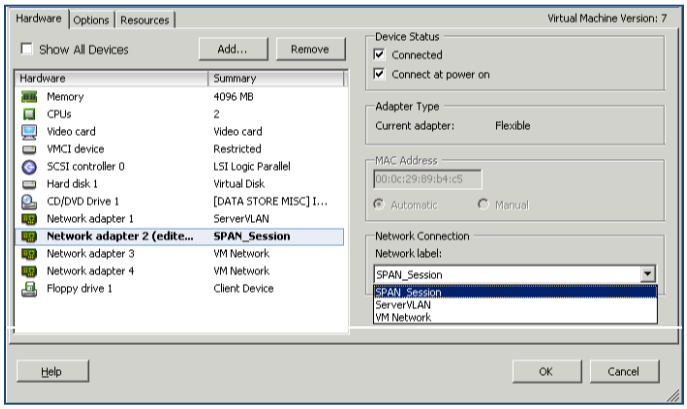


步骤 11 为思科 ISE 选择合适的网络适配器（对于思科 ISE 中的“GigabitEthernet 1”，通常应选择“Network Adaptor 2”）。

步骤 12 确保将“Device Status”设置为“Connected”，并将“Connect at power on”设为启用状态（图 11）。

步骤 13 从“Network Connection”下拉菜单中，选择新创建的 SPAN_Session 网络（图 11）。

图 11 虚拟机设置

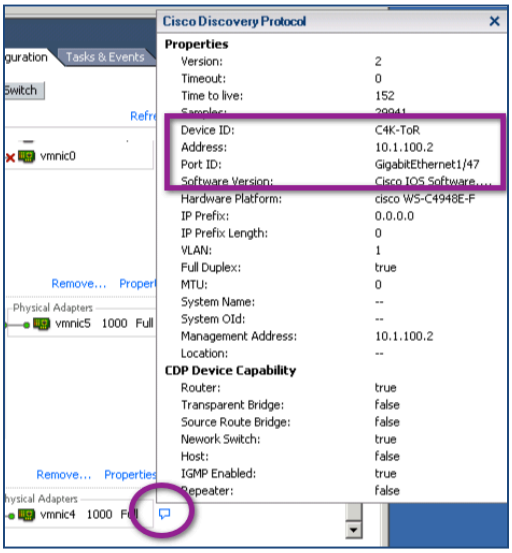


步骤 14 点击“OK”。

步骤 15 记录混合接口所连接的交换机端口，以便下一节使用。

注：VMware ESX 服务器具有体贴用户的特性，可显示其所连接接口的思科发现协议信息。图 12 提供了此显示的示例。

图 12 思科发现协议



配置混合 VMware 端口组（可选）

您也可以通过在现有 vSwitch 上创建混合端口组的方式配置混合 VMware 网络。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。

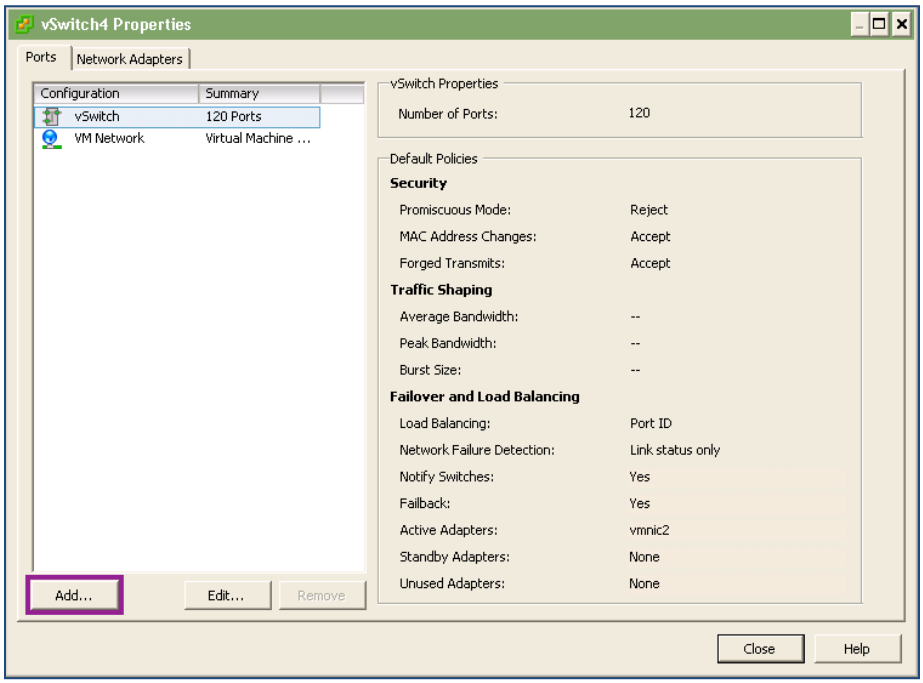
步骤 1 在 VMware VSphere 客户端中选择物理 ESX 服务器。

步骤 2 选择“Configuration”→“Networking”，然后选择您的 vSwitch 并点击“Properties”（图 13）。

图 13 Configuration → Networking

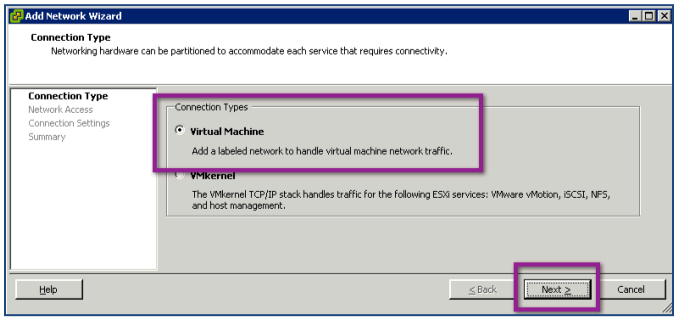
步骤 3 在 vSwitch 属性窗口的“Ports”选项中，点击左下角的“Add”[[是否必须确保选中“vSwitch 120 Ports”？]]（图 14）。

图 14 vSwitch 属性



步骤 4 系统将启动“Add Network Wizard”向导。在“Connection Types”下，选择“Virtual Machine”，然后点击“Next”（图 15）。

图 15 连接类型

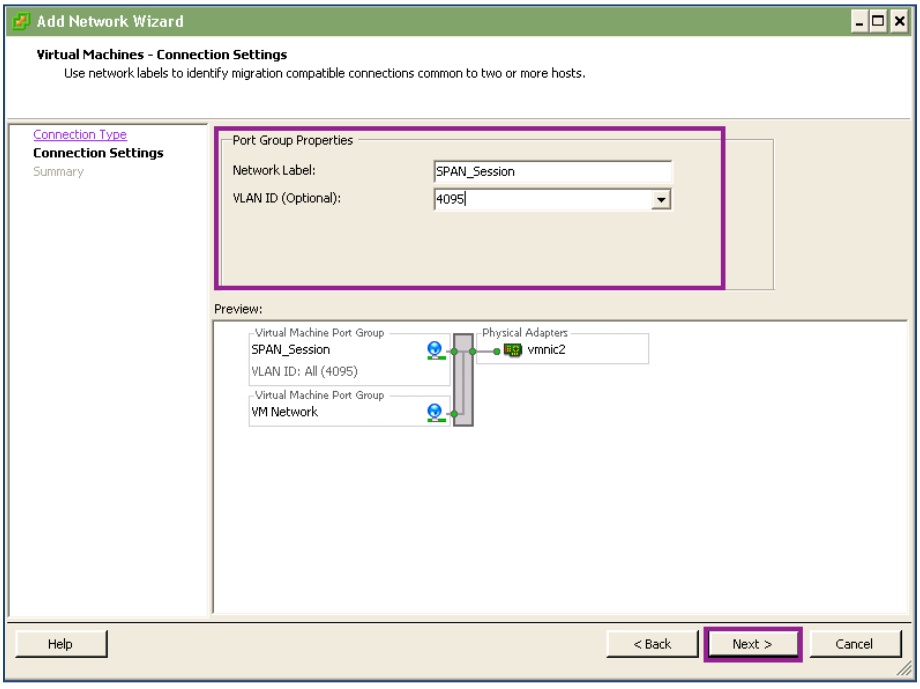


步骤 5 将端口组命名为“**SPAN_Session**”或任何其他逻辑名称。

步骤 6 将“VLAN”设置为 **4095**，然后点击“Next”（图 16）。

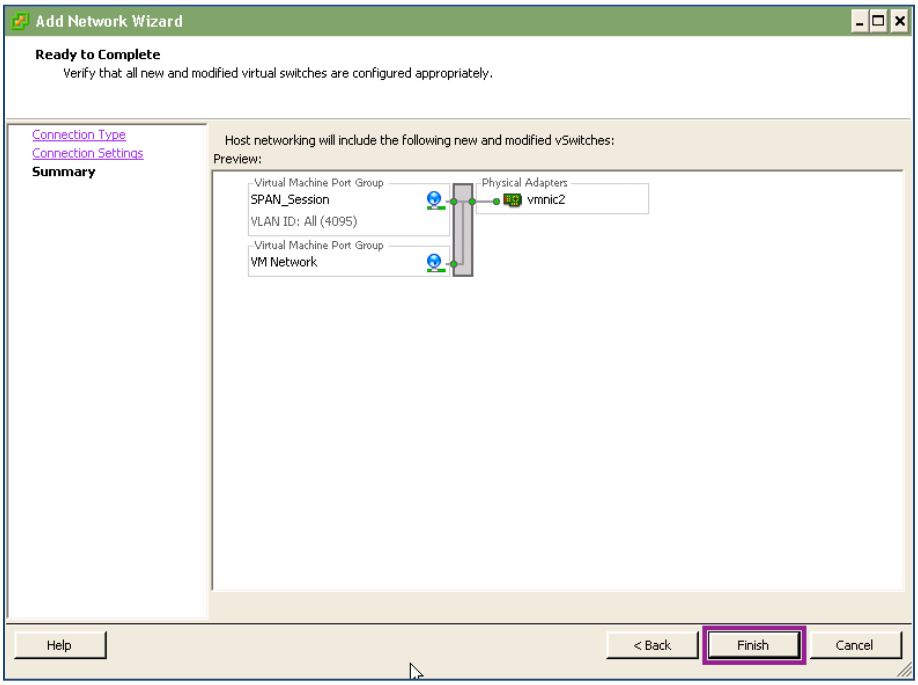
注：此 VLAN 就是侦听该 vSwitch 上所有其他 VLAN 的特殊 VMware VLAN。

图 16 端口组属性



步骤 7 选择“Finish”（图 17）。

图 17 预览



步骤 8 突出显示新端口组。

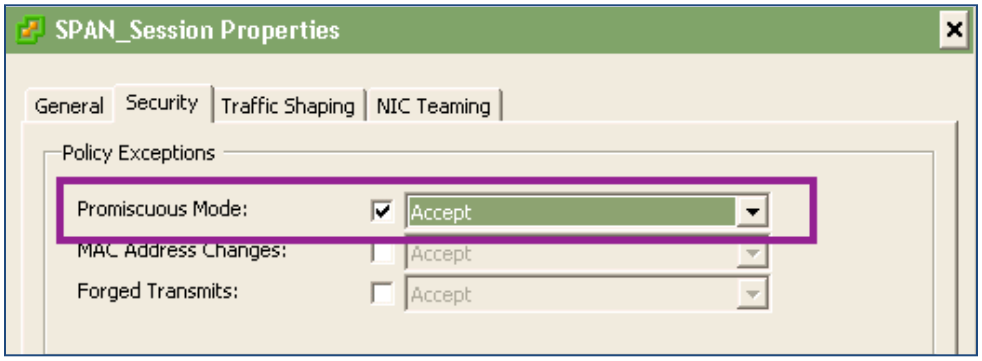
步骤 9 选择“Edit”。

步骤 10 选择“Security”选项卡。

步骤 11 从“Promiscuous Mode”下拉菜单中选择“Accept”。

步骤 12 单击“OK”。

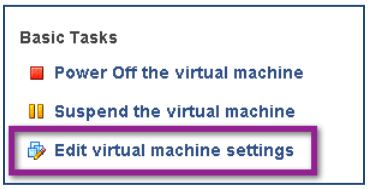
图 18 混合模式



步骤 13 关闭 vSwitch 属性窗口。

步骤 14 编辑思科 ISE 虚拟机设置（图 19）。

图 19 编辑虚拟机设置

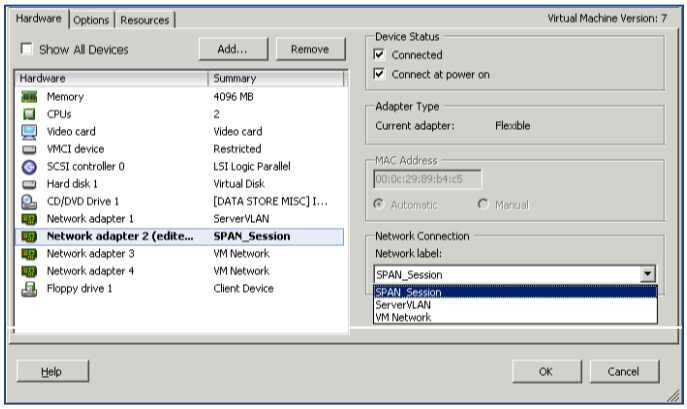


步骤 15 为思科 ISE 选择合适的网络适配器（对于思科 ISE 中的“GigabitEthernet1”，通常应选择“Network Adaptor 2”）。

步骤 16 确保将“Device Status”设置为“Connected”，并将“Connect at power on”设为启用状态。

步骤 17 从“Network Connection”下拉菜单中，选择新创建的 SPAN_Session 网络（图 20）。

图 20 VM 设置



步骤 18 点击 **OK**。

如何配置 SPAN 会话

配置交换机上的 SPAN 会话

步骤 1 进入全局配置。[[位置在哪里？请更明确地加以说明。]]

步骤 2 配置 SPAN 会话源。示例如下：

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

步骤 3 配置 SPAN 会话目标。示例如下：

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

步骤 4 验证端口当前是否处于监控模式。

```
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 探测功能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。这样一来，此节点添加过程除向环境中的生产 DHCP 服务器发送所有 DHCP 请求的副本之外，还会向思科 ISE 发送所有 DHCP 请求的副本。

步骤 1 进入全局配置模式。[[位置在哪里？请更明确地加以说明。]]

步骤 2 进入 Access 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。示例如下：

```
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：

- Cisco Catalyst 2900 系列交换机：
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 3000 系列交换机：
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 3000-X 系列交换机：
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- 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
- 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
- Cisco ASR 1000 系列路由器：
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

思科无线局域网控制器：
http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html