使用ACS的安全经理集成

目录

简介

本文档介绍如何将思科安全管理器与思科安全访问控制服务器(ACS)集成。

思科安全ACS为使用管理应用（如思科安全管理器）以配置受管网络设备的用户提供命令授权。对命令授权的支持由包含一组权限的唯一命令授权集类型（在思科安全管理器中称为角色）提供。这些权限（也称为权限）确定具有特定角色的用户可以在思科安全管理器内执行的操作。

思科安全ACS使用TACACS+与管理应用通信。要使思科安全管理器与思科安全ACS通信，您必须将思科安全ACS中的CiscoWorks服务器配置为使用TACACS+的AAA客户端。此外，您必须为CiscoWorks服务器提供您登录Cisco Secure ACS时使用的管理员名称和密码。当您满足这些要求时，它可确保思科安全管理器和思科安全ACS之间通信的有效性。

当思科安全管理器最初与思科安全ACS通信时，它指示思科ACS创建默认角色，这些角色显示在思科安全ACS HTML界面的共享配置文件组件部分。它还规定自定义服务由TACACS+授权。此自定义服务显示在HTML界面的Interface Configuration部分的TACACS+(Cisco IOS®)页面上。然后，您可以修改每个思科安全管理器角色中包含的权限，并将这些角色应用于用户和用户组。

注意：由于不支持CSM，因此无法将CSM与ACS 5.2集成。

先决条件

要求

要使用Cisco Secure ACS，请确保：

- 您定义的角色包括在思科安全管理器中执行必要功能所需的命令。
- 网络访问限制(NAR)包括要管理的设备组（或设备）（如果将NAR应用到配置文件）。
- 受管设备名称在Cisco Secure ACS和Cisco Security Manager中拼写和大写。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全管理器3.0版
- 思科安全ACS版本3.3

注意：确保在网络环境中安装之前选择兼容的CSM和ACS版本。例如，思科测试了仅带CSM 3.0的ACS 3.3，并停止用于更高的CSM版本。因此，建议您将CSM 3.0与ACS 3.3配合使用。有关各种软件版本的详细信息，请参阅兼容性矩阵表。

思科安全管理器版本	CS ACS版本已测试
3.0.0 3.0.0 SP1	Windows 3.3(3)和4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	解决方案引擎4.0(1)Windows 4.0(1)
3.1.0 3.0.2	解决方案引擎4.0(1)Windows 4.1(1)和4.1(3)
3.1.1 3.0.2 SP1 3.0.2 SP2	解决方案引擎v4.0(1)Windows 4.1(2)、4.1(3)和4.1(4)
3.1.1 SP1	解决方案引擎4.0(1)Windows 4.1(4)
3.1.1 SP2	解决方案引擎4.0(1)Windows 4.1(4)和4.2(0)
3.2.0	解决方案引擎4.1(4)Windows 4.1(4)和4.2(0)
3.2.1	解决方案引擎4.1(4)Windows 4.2(0)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

将思科安全管理器与思科安全ACS集成

本节介绍将思科安全管理器与思科安全ACS集成所需的步骤。某些步骤包含几个子步骤。必须按顺序执行这些步骤和子步骤。本节还包含对用于执行每个步骤的特定过程的引用。

请完成以下步骤：

1. **规划您的管理身份验证和授权模式。**在使用思科安全管理器之前，必须确定您的管理模式。这包括您计划使用的管理角色和帐户的定义。**提示：**在定义潜在管理员的角色和权限时，还要考虑是否启用工作流。此选择会影响您限制访问的方式。
2. **安装Cisco Secure ACS、Cisco Security Manager和CiscoWorks Common Services。**在Windows 2000/2003服务器上安装Cisco Secure ACS 3.3版。在不同的Windows 2000/Windows 2003服务器上安装CiscoWorks Common Services和Cisco Security Manager。有关详细信息，请参阅以下文档：思科安全管理器3.0安装指南Cisco Secure ACS for Windows 3.3 安装指南**注：在**选择CSM和ACS软件版本之前，请参阅兼容性矩阵表以了解详细信息。
3. **在思科安全ACS中执行集成过程。**将思科安全管理器用户定义为ACS用户，并根据其规划的角色将其分配给用户组，将所有受管设备（以及CiscoWorks/安全管理器服务器）添加为AAA客户端，并创建管理控制用户。有关详细信息，请参阅在Cisco Secure ACS中执行的集成过程。
4. **在CiscoWorks Common Services中执行集成过程。**配置与Cisco Secure ACS中定义的管理员匹配的本地用户，为系统身份设置定义同一用户，并将ACS配置为AAA设置模式。有关详细信息，请参阅CiscoWorks中执行的集成过程。
5. **在Cisco Secure ACS中为用户组分配角色。**为在Cisco Secure ACS中配置的每个用户组分配角色。您使用的步骤取决于您是否配置了网络设备组(NDG)。有关详细信息，请参阅在Cisco Secure ACS中为用户组分配角色。

在Cisco Secure ACS中执行的集成过程

本节介绍在Cisco Secure ACS中必须完成的步骤，以便将其与Cisco Security Manager集成：

1. 在Cisco Secure ACS中定义用户和用户组
2. 在思科安全ACS中将受管设备添加为AAA客户端
3. 在Cisco Secure ACS中创建管理控制用户

在Cisco Secure ACS中定义用户和用户组

思科安全管理器的所有用户必须在思科安全ACS中定义，并分配与其工作职能相适应的角色。最简单的方法是根据ACS中可用的每个默认角色将用户划分为不同的组。例如，将所有系统管理员分配给一个组，将所有网络操作员分配给另一个组，依此类推。有关ACS中默认角色的详细信息，请参阅Cisco Secure ACS默认角色。

此外，您必须创建一个额外用户，该用户被分配了具有完全权限的系统管理员角色。为此用户建立的凭证稍后会在CiscoWorks的“系统身份设置”(System Identity Setup)页面上使用。有关详细信息，请参阅定义系统身份用户。

请注意，在此阶段，您只是将用户分配给不同的组。在CiscoWorks、思科安全管理器和任何其他应用注册到思科安全ACS后，将稍后执行这些组的实际角色分配。

提示：在继续之前，请在一台Windows 2000/2003服务器上安装CiscoWorks Common Services和Cisco Security Manager。在其他Windows 2000/2003服务器上安装Cisco Secure ACS。

1. 登录Cisco Secure ACS。
2. 配置具有完全权限的用户：单击导**航栏上**的“用户设置”。在“用户设置”(User Setup)页面上，输入新用户的名称，然后单击“添**加/编辑”(Add/Edit**)。从User Setup下的Password Authentication列表中选择身份验证方法。输入并确认新用户的密码。选**择组**1作为用户分配到的组。单击**Submit**以创建用户帐户。
3. 对每个思科安全管理器用户重复步骤2。思科建议您根据每个用户所分配的角色将用户划分为多个组：组1 — 系统管理员组2 — 安全管理员组3 — 安全审批人组4 — 网络管理员组5 — 审批人组6 — 网络运营商第7组 — 帮助台有关与每个角色关联的默认权限的详细信息，请参阅表。有关自定义用户角色的详细信息，请参阅自定义Cisco Secure ACS角色。**注：在**此阶段，组本身是没有任何角色定义的用户的集合。在完成集成过程后，可以为每个组分配角色。有关详细信息，请参阅在Cisco Secure ACS中为用户组分配角色。
4. 创建其他用户并将此用户分配给系统管理员组。为此用户建立的凭证稍后会在CiscoWorks的“系统身份设置”(System Identity Setup)页面上使用。有关详细信息，请参阅定义系统身份用户。
5. 继续在Cisco Secure ACS中将受管设备添加为AAA客户端。

在思科安全ACS中将受管设备添加为AAA客户端

在开始将设备导入思科安全管理器之前，必须先将每台设备配置为思科安全ACS中的AAA客户端。此外，您必须将CiscoWorks/Security Manager服务器配置为AAA客户端。

如果思科安全管理器管理在防火墙设备上配置的安全情景（包括在Catalyst 6500/7600设备的FWSM上配置的安全情景），则必须将每个情景单独添加到思科安全ACS。

用于添加受管设备的方法取决于是否要限制用户使用网络设备组(NDG)管理特定设备集。 请参阅以下部分之一：

- 如果希望用户能够访问所有设备，请按照添加设备(Add Devices as AAA Clients Without NDGs)中所述添加设备。
- 如果希望用户只能访问某些NDG，请按照配置网络设备组以在安全管理器中使用中所述添加设备。

将设备添加为AAA客户端（无NDG）

此过程介绍如何将设备添加为Cisco Secure ACS的AAA客户端。有关所有可用*选项的完整信*息，请参阅网络配置的AAA客户端配置部分。

注意：切记将CiscoWorks/安全管理器服务器添加为AAA客户端。

1. 单击**Cisco Secure ACS导航栏**上的**Network Configuration**。
2. 单击**AAA Clients表**下方的Add Entry。
3. 在Add AAA Client页面上输入AAA客户端主机名（最多32个字符）。AAA客户端的主机名必须与您计划用于思科安全管理器中设备的显示名称相匹配。例如，如果要在思科安全管理器中的设备名称后附加域名，则ACS中的AAA客户端主机名必须为**<device_name>.<domain_name>**。当您命名CiscoWorks服务器时，建议使用完全限定的主机名。请务必正确拼写主机名。主机名不区分大小写。在命名安全情景时，请将情景名称(**_<context_name>**)附加到设备名称。对于FWSM，以下是命名约定：FWSM刀片**- <机箱名称>_FW_<插槽编号>**安全情**景 — <chassis_name>_FW_<slot_number>_<context_name>**
4. 在AAA Client IP Address字段中输入网络设备的IP地址。

5. 在密钥字段中输入共享密钥。
6. 从“**Authenticate Using”（使用验证）列**表中选择TACACS+(Cisco IOS)。
7. 单击**Submit**以保存更改。您添加的设备将显示在AAA客户端表中。
8. 重复步骤1至7以添加其他设备。
9. 添加所有设备后，单击**Submit + Restart**。
10. 继续在Cisco Secure ACS中创建管理控制用户。

配置网络设备组以在安全管理器中使用

Cisco Secure ACS使您能够配置包含要管理的特定设备的网络设备组(NDG)。例如，您可以为每个地理区域或与组织结构匹配的NDG创建NDG。与思科安全管理器配合使用时，NDG使您能够根据用户需要管理的设备为用户提供不同级别的权限。例如，使用NDG，您可以为位于欧洲的设备分配用户A系统管理员权限，为位于亚洲的设备分配帮助台权限。然后，您可以将相反的权限分配给用户B。

NDG不直接分配给用户。相反，NDG会分配给您为每个用户组定义的角色。每个NDG只能分配给一个角色，但每个角色可以包含多个NDG。这些定义将作为所选用户组配置的一部分保存。

以下主题概述配置NDG所需的基本步骤：

- 激活NDG功能
- 创建NDG
- 将NDG和角色与用户组关联

激活NDG功能

必须先激活NDG功能，然后才能创建NDG并使用设备填充它们。

1. 单击**Cisco Secure ACS导航栏**上的**Interface Configuration**。
2. 单击“**Advanced Options(高级选项**)”。
3. 向下滚动，然后选中**Network Device Groups**复选框。
4. 单击“Submit”。
5. 继续执行Create NDGs。

创建NDG

此过程介绍如何创建NDG并使用设备填充它们。每台设备只能属于一个NDG。

注意：思科建议您创建包含CiscoWorks/Security Manager服务器的特殊NDG。

1. 单击导航栏上的**Network Configuration**。所有设备最初都置于“未分配”(Not Assigned)下，它保存所有未置于NDG中的设备。请记住，“未分配”不是NDG。
2. 创建NDG:单击**Add Entry**。在New Network Device Group页面上输入NDG的名称。最大长度为24个字符。允许空格。**当使用4.0或更高版本时为可选：**输入NDG中所有设备使用的密钥。如果为NDG定义密钥，它将覆盖为NDG中的单个设备定义的任何密钥。单击**Submit**以保存NDG。重复步骤a至d以创建更多NDG。
3. 使用设备填充NDG:在Network Device Groups区域中点击NDG的名称。在AAA Clients区**域中单击Add Entry**。定义要添加到NDG的设备的详细信息，然后单击**Submit**。有关详细信息，请参阅将设备添加为AAA Clients Without NDGs。重复步骤b和c，将其余设备添加到NDG。在

Not Assigned类别中，唯一可以保留的设备是默认AAA服务器。在配置最后一台设备后，单击**Submit + Restart**。

4. 继续在Cisco Secure ACS中创建管理控制用户。

在Cisco Secure ACS中创建管理控制用户

使用Cisco Secure ACS中的Administration Control页可定义在CiscoWorks Common Services中定义AAA设置模式时使用的管理员帐户。有关详细信息，请参阅在CiscoWorks中配置AAA设置模式。

1. 在Cisco Secure ACS导航栏上单击**Administration Control**。
2. 单击“**Add Administrator**”。
3. 在“添加管理员”(Add Administrator)页面上，输入管理员的名称和密码。
4. 单击**Administrator Privileges**区域中的**Grant All**，以向此管理员提供完全管理权限。
5. 单击**Submit**以创建管理员。

注意：有关配置管理员时可用选项的详细信息，请参阅管理员和管理策略。

在CiscoWorks中执行的集成过程

本节介绍在CiscoWorks公共服务中完成的步骤，以便将其与Cisco Security Manager集成：

- 在CiscoWorks中创建本地用户
- 定义系统身份用户
- 在CiscoWorks中配置AAA设置模式

完成在Cisco Secure ACS中执行的集成过程后，请完成以下步骤。Common Services将任何已安装应用（如思科安全管理器、自动更新服务器和IPS管理器）的实际注册到思科安全ACS。

在CiscoWorks中创建本地用户

使用CiscoWorks Common Services中的Local User Setup页面创建与您之前在Cisco Secure ACS中创建的管理员重复的本地用户帐户。此本地用户帐户稍后用于系统身份设置。有关详细信息，请参阅。

注意：在继续之前，请在Cisco Secure ACS中创建管理员。有关说明，请参阅在Cisco Secure ACS中定义用户和用户组。

1. 使用默认管理员用户帐**户登**录CiscoWorks。
2. 选择**Server > Security from Common Services**，然后从TOC中选**择Local User Setup**。
3. 单击 **Add**。
4. 输入您在Cisco Secure ACS中创建管理员时输入的相同名称和密码。请参阅在Cisco Secure ACS中定义用户和用户组中的步骤4。
5. 选中“角色”(Roles)下的所有复选框（导出数据除外）。
6. 单击**OK**以创建用户。

定义系统身份用户

使用CiscoWorks公共服务中的“系统身份设置”页可以创建信任用户（称为系统身份用户），该用户允许属于同一域的服务器与位于同一服务器上的应用程序进程之间的通信。应用程序使用系统身份用户对本地或远程CiscoWorks服务器上的进程进行身份验证。当应用程序必须在任何用户登录之前

进行同步时，这尤其有用。

此外，当主任务已经为登录用户授权时，通常使用系统身份用户来执行子任务。例如，要在思科安全管理器中编辑设备，思科安全管理器和公共服务DCR之间需要应用间通信。授权用户执行编辑任务后，使用系统身份用户来调用DCR。

您在此处配置的系统身份用户必须与您在ACS中配置的具有管理（完全）权限的用户相同。否则，将无法查看在思科安全管理器中配置的所有设备和策略。

注意：在继续之前，请在CiscoWorks Common Services中创建与此管理员具有相同名称和密码的本地用户。有关说明，请参阅在CiscoWorks中创建本地用户。

1. 选择**Server > Security**，然后从**TOC中选择Multi-Server Trust Management > System Identity Setup**。
2. 输入您为Cisco Secure ACS创建的管理员的名称。请参阅在Cisco Secure ACS中定义用户和用户组中的步骤4。
3. 输入并验证此用户的密码。
4. 单击 **Apply**。

在CiscoWorks中配置AAA设置模式

使用CiscoWorks公共服务中的AAA设置模式页面将Cisco Secure ACS定义为AAA服务器，包括所需的端口和共享密钥。此外，您最多可以定义两台备份服务器。

这些步骤将CiscoWorks、Cisco Security Manager、IPS Manager（或者，自动更新服务器）实际注册到Cisco Secure ACS中。

1. 选择**Server > Security**，然后从TOC**中选择AAA Mode Setup**。
2. 选中Available Login Module**s下**的TACACS+复选框。
3. 选择**ACS**作为AAA类型。
4. 在Server Details（服务器详细信息）区域中输入最多三台Cisco Secure ACS服务器的IP地址。在主服务器发生故障时，辅助和第三服务器充当备份。**注意：**如果所有已配置的TACACS+服务器都无法响应，您必须使用管理员CiscoWorks本地帐户登录，然后将AAA模式更改回Non-ACS/CiscoWorks Local。在TACACS+服务器恢复服务后，必须将AAA模式更改回ACS。
5. 在Login区域，输入您在Cisco Secure ACS的Administration Control页面上定义的管理员的名称。有关详细信息，请参阅在Cisco Secure ACS中创建管理控制用户。
6. 输入并验证此管理员的密码。
7. 输入并验证在将安全管理器服务器添加为思科安全ACS的AAA客户端时输入的共享密钥。请参阅将设备添加为不带NDG的AAA客户端中的步骤5。
8. 选中**Register all installed applications with ACS(注册所有已安装的应用**与ACS)复选框，以便将Cisco Security Manager和任何其他已安装的应用与Cisco Secure ACS一起注册。
9. 单击 **Apply 以保存设置。**进度条显示注册进度。注册完成时，会显示一条消息。
10. 如果将思科安全管理器与任何ACS版本集成，请重新启动思科安全管理器守护程序管理器服务。有关说明，请参阅重新启动守护程序管理器。**注意：**在CSM 3.0.0之后，思科不再使用ACS 3.3(x)进行测试，因为它已进行大量修补，并且已宣布其寿命终止(EOL)。因此，您需要为CSM 3.0.1版及更高版本使用相应的ACS版本。有关详细信息，请参阅兼容性矩阵表。
11. 重新登录Cisco Secure ACS，以便为每个用户组分配角色。有关说明，请参阅为Cisco Secure ACS中的用户组分配角色。**注意：如**果卸载CiscoWorks Common Services或Cisco

Security Manager，此处配置的AAA设置不会保留。此外，重新安装后无法备份和恢复此配置。因此，如果升级到任一应用的新版本，则必须重新配置AAA设置模式并向ACS重新注册Cisco Security Manager。增量更新不需要此流程。如果在CiscoWorks上安装其他应用（如AUS），则必须重新注册新应用和思科安全管理器。

重新启动守护程序管理器

此过程介绍如何重新启动思科安全管理器服务器的守护程序管理器。您必须执行此操作，才能使您配置的AAA设置生效。然后，您可以使用在Cisco Secure ACS中定义的凭证重新登录CiscoWorks。

1. 登录安装思科安全管理器服务器的计算机。
2. 选择**开始>程序>管理工具>服**务以打开“服务”窗口。
3. 从右侧窗格中显示的服务列表中，选择**Cisco Security Manager Daemon Manager**。
4. 单击工**具栏上**的重新启动服务按钮。
5. 继续执行Assign Roles to User Groups in Cisco Secure ACS。

在Cisco Secure ACS中为用户组分配角色

在您将CiscoWorks、Cisco Security Manager和其他已安装的应用注册到Cisco Secure ACS后，您可以为之前在Cisco Secure ACS中配置的每个用户组分配角色。这些角色确定允许每个组中的用户在思科安全管理器中执行的操作。

您为向用户组分配角色而使用的过程取决于是否使用NDG:

- 将角色分配给没有NDG的用户组
- 将NDG和角色与用户组关联

将角色分配给没有NDG的用户组

此过程介绍如何在未定义NDG时将默认角色分配给用户组。有关详细信息，请参阅Cisco Secure ACS默认角色。

注意：在继续之前：

- 为每个默认角色创建用户组。有关说明，请参阅在Cisco Secure ACS中定义用户和用户组。
- 完成在Cisco Secure ACS中执行的集成过程和在CiscoWorks中执行的集成过程中描述的过程。

请完成以下步骤：

1. 登录Cisco Secure ACS。
2. 单击导**航栏上**的组设置。
3. 从列表中选择系统管理员的用户组。请参阅在Cisco Secure ACS中定义用户和用户组的第2步，然后单击编辑**设置**。

将NDG和角色与用户组关联

将NDG与角色关联以在思科安全管理器中使用时，必须在“组设置”(Group Setup)页面的两个位置创建定义：

- CiscoWorks区域
- 思科安全管理器区域

每个区域的定义必须尽可能地匹配。当您关联CiscoWorks Common Services中不存在的自定义角色或ACS角色时，请尝试根据分配给该角色的权限尽可能定义一个等效项。

您必须为每个用户组创建关联，以便与思科安全管理器一起使用。例如，如果您的用户组包含西部地区的支持人员，则可以选择该用户组，然后将包含该地区设备的NDG与帮助台角色关联。

注意：在继续之前，激活NDG功能并创建NDG。有关详细信息，请参阅配置网络设备组以在安全管理器中使用。

1. 单击导**航栏上**的组设置。
2. 从“组”列表中选择用户组，然后单击“编辑**设置”**。
3. 映射NDG和角色以在CiscoWorks中使用：在“组设置”(Group Setup)页面上，向下滚动到“TACACS+设置”(TACACS+ Settings)下的CiscoWorks区域。选**择Assign a CiscoWorks on a Network Device Group Basis**。从设备组列表中选择NDG。从第二个列表中选择此NDG要关联到的角色。单击“**添加关联**”。关联显示在Device Group框中。重复步骤c到e以创建其他关联。**注意**：要删除关联，请从设备组中选择它，然后点击删除关联。
4. 向下滚动到思科安全管理器区域，创建尽可能与步骤3中定义的关联紧密匹配的关联。**注意**：在Cisco Secure ACS中选择安全审批人或安全管理员角色时，建议选择网络管理员作为最接近的等效CiscoWorks角色。
5. 单击**Submit**以保存设置。
6. 重复步骤2至5，为其余用户组定义NDG。
7. 将NDG和角色与每个用户组关联后，单击“提**交+重新启动**”。

故障排除

1. 在开始将设备导入思科安全管理器之前，必须先将每台设备配置为思科安全ACS中的AAA客户端。此外，您必须将CiscoWorks/Security Manager服务器配置为AAA客户端。
2. 如果收到失败的尝试日志，Cisco Secure ACS中的作者失败并出现错误。
   ```
   "service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*Test
   Devices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switches
   authorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers authoriz"
   ```
   要解决此问题，请确保ACS中设备的名称必须是完全限定的域名。

相关信息

- 思科Windows安全访问控制服务器支持页
- Cisco Security Manager支持页面
- 用于 Windows 的 Cisco 安全访问控制服务器
- Cisco Secure ACS 4.1 配置指南
- Cisco Secure ACS 联机故障排除指南 4.1
- 安全产品现场通知（包括CiscoSecure ACS for Windows）
- 技术支持和文档 - Cisco Systems