配置UNIX的(Solaris) CSU

目录

简介

用于UNIX的Cisco Secure ACS (CSU)软件帮助保证网络的安全并且跟踪成功连接对网络人的活动。CSU作为TACACS+或RADIUS服务器并且使用验证、授权和统计(AAA)提供网络安全。

CSU支持这些数据库选项存储组和用户配置文件和记帐信息：

- SQLAnywhere (包括与CSU)。Sybase SQLAnywhere此版本没有客户端/服务器支持。然而，它优化进行重要AAA服务与CSU。**警告：** SQLAnywhere数据库选项不支持超出5,000个配置文件信息用户、复制在数据库站点中的或者Cisco Secure分布式会话管理器(DSM)功能的配置文件数据库。
- Oracle或Sybase关系数据库管理系统(RDBMS)。支持Cisco Secure 5,000个或更多用户配置文件数据库、数据库复制或者Cisco Secure DSM功能，您必须事先装配Oracle (版本7.3.2，7.3.3或者8.0.3)或Sybase SQL server (版本11) RDBMS保持您的Cisco Secure配置文件信息。在Cisco Secure安装完成后，数据库复制要求进一步RDBMS配置。
- 现有的数据库的升级从CSU一个上一个(2.x)版本的。如果从Cisco Secure一个初期的2.x版本升级，Cisco Secure安装程序自动地升级配置文件数据库是与UNIX的CSU 2.3兼容。
- 导入一个现有配置文件数据库。您能转换现有免费软件TACACS+或RADIUS配置文件数据库或者展开文件为了用在CSU的此版本上。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据UNIX的Cisco Secure ACS 2.3。

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

CSU配置

使用这些步骤配置CSU。

启动Cisco Secure管理员接口

使用此步骤登陆对Cisco Secure管理员。

1. 从有Web连接的所有工作站对ACS，请启动您的Web浏览器。
2. 输入Cisco Secure管理员网站的这些URL之一：如果在您的浏览器的安全套接字层功能没有启用，请输入：`http://your_server/cs`那里your_server是主机名(或完全合格的域名(FQDN)，如果主机名和FQDN有所不同您安装CSU的) SPARCstation。您能用your_server也替代SPARCstation的IP地址。如果在您的浏览器的安全套接字层功能启用，请指定“https”而不是“http”作为超文本传输协议。输入：`https://your_server/cs`那里your_server是主机名(或FQDN，如果主机名和FQDN有所不同您安装CSU的) SPARCstation。您能用your_server也替代SPARCstation的IP地址。**注意：** URL和服务器名区分大小写。必须正确地键入他们与大写和小写字母如显示。CSU登录页显示。
3. 请输入您的用户名和密码。单击 **submit**。**注意：** 最初的默认用户名是“超级用户”。最初的默认密码是“changeme”。在您的首次登录以后，您需要为最大安全性立即更改用户名和密码。在您登陆后， CSU主页显示与沿顶部的主菜单档。CSU主菜单页显示，只有当用户提供有管理员级别权限的一个名称和密码。如果用户提供有仅用户级权限的一个名称和密码，则一不同的屏幕显示。

启动高级配置程序

启动基于Java的Cisco Secure管理员高级配置程序从任何CSU管理员网页。从CSU Web接口的菜单栏，请点击**先进**，然后单击再**提前**。

Cisco Secure管理员高级配置程序显示。它也许可能花费几分钟装载。

创建组配置文件

请使用Cisco Secure管理员高级配置程序创建和配置组配置文件。思科建议您创建组配置文件配置很大数量相似的用户的详细的AAA需求。在组配置文件定义后，请迅速请使用CSU Add a User网页对添加用户时配置文件对组配置文件。配置的高级需求组的适用于每个成员用户。

使用此步骤创建组配置文件。

1. 在Cisco Secure管理员高级配置程序，请选择**Members选项**。在浏览器窗格，请取消选定**Browse复选框**。Create New Profile图标显示。
2. 在浏览器窗格，请执行这些中的一个：要创建组配置文件没有parent，请找出并且点击[Root]文件夹图标。要创建您的组配置文件作为另一个组配置文件的孩子，请找出您想要作为parent并且点击它的组。如果您希望是parent的组是子组，请点击其父组的文件夹显示它。
3. 单击**创建新配置文件**。New Profile对话框显示。
4. 选择**Group复选框**，键入您要创建组的名称，并且点击OK键。在树的新的组显示。
5. 在您创建组配置文件后，请分配TACACS+或RADIUS属性配置特定AAA属性。

创建在高级配置模式的用户配置文件

请使用Cisco Secure管理员高级配置模式创建和配置用户配置文件。您比对添加可能的每用户页能执行此较详细地定制用户配置文件的授权和记帐相关的属性。

使用此步骤创建用户配置文件：

1. 在Cisco Secure管理员高级配置程序，请选择**Members选项**。在浏览器窗格，请查找并且取消选定**浏览**。Create New Profile图标显示。
2. 在浏览器窗格，请执行这些中的一个：找出并且点击用户属于的组。如果不希望用户属于组，请点击[Root]文件夹图标。
3. 单击**创建配置文件**。New Profile对话框显示。
4. 确保**Group复选框**取消选定。
5. 输入您要创建和点击OK键用户的名称。在树的新用户显示。
6. 在您创建用户配置文件后，请分配特定TACACS+或RADIUS属性配置特定AAA属性：对用户配置文件的分配TACACS+配置文件，参见分配TACACS+属性到组或用户配置文件。对用户配置文件的分配RADIUS配置文件，参见分配RADIUS属性到组或用户配置文件。

适用属性的策略

请使用CSU组配置文件功能和TACACS+和RADIUS属性通过CSU实现网络用户认证和授权。

对组和用户计划属性

CSU的组配置文件功能使您定义很大数量的用户的共同的一套AAA需求。

您能分配一套TACACS+或RADIUS属性值到组配置文件。这些属性值分配到组适用于是成员或被添加作为该组的成员的所有用户。

有效请使用组配置文件功能

要配置CSU管理有复杂AAA需求的大量的和各种类型用户，思科建议您使用Cisco Secure管理员高级配置程序的功能创建和配置组配置文件。

组配置文件需要包含不是特定对用户的所有属性。这通常含义所有属性除了密码。您能然后使用添加Cisco Secure管理员的用户页创建与密码属性的简单用户配置文件和分配这些用户配置文件到适当的组配置文件。为特定组和属性值定义的功能然后适用给其成员用户。

父组和子组

您能创建组层级。在组配置文件内，您能创建子组配置文件。属性值分配到父组配置文件是子组配置文件的默认值。

社团级别管理

Cisco Secure系统管理员能分配单个Cisco Secure用户组管理员状态。组是辅助对他们的组的管理员状态使个人用户管理所有子组配置文件和用户配置文件。然而，他们的组的层级的外部下跌的它不给他们管理任何组或用户。因此，系统管理员分配管理大型网络任务给其他个人，无需授权每一个相等的权限。

为个人用户定义了什么属性？

思科建议您赋予个人用户对用户是唯一，例如属性定义了用户名、密码、密码类型和Web权限的基本认证属性值。赋予基本认证属性值到您的用户通过CSU的Edit a User或添加用户页。

为组配置文件定义了什么属性？

思科建议您定义了鉴定、授权和记帐相关的属性在社团级别。

在本例中，名为“拨入用户的”组配置文件分配属性值对Frame-Protocol=PPP和服务类型=Framed。

什么是绝对属性？

TACACS+的一在CSU的子集和RADIUS属性可以分配在组配置文件级别的绝对状态。为绝对状态启用的属性值在组配置文件级别改写所有冲突的属性值在子组配置文件或成员用户配置文件级别。

在与几个级别的多重网络内组管理员，绝对属性使系统管理员设置分组管理员在较底层不能改写的选定组属性值。

可以分配绝对状态显示在Cisco Secure管理员高级配置程序的属性方框的一个绝对复选框的属性。选择复选框启用绝对状态。

组属性值和用户属性值能否相冲突？

在属性值中的冲突解决分配到父组配置文件，子组配置文件，并且成员用户配置文件取决于属性值是否绝对，并且他们是否是TACACS+或RADIUS属性：

- TACACS+或RADIUS属性值分配到与绝对状态覆盖的一个组配置文件任何冲突的属性值设置在子组或用户配置文件级别。
- 如果TACACS+属性值的绝对状态没有启用在组配置文件级别，由所有冲突的属性值改写设置在

子组或用户配置文件级别。
- 如果RADIUS属性值的绝对状态没有启用在父组级别，则所有冲突的属性值设置在子组导致一种无法预测的结果。当您定义了组和其成员用户的时RADIUS属性值，请避免分配同一个属性到用户和组配置文件。

请使用Prohibit和Permit选项

对于TACACS+，请改写值通过加前缀关键字**禁止**被继承的服务的可用性或**允许**对服务规格。**permit**关键字允许指定的服务。**禁止**关键字禁止指定的服务。使用使用这些关键字一起，您能修建“一切除了”配置。例如，此配置允许从所有服务的访问除了X.25 ：

```
default service = permit
prohibit service = x25
```

分配TACACS+属性到组或用户配置文件

分配特定TACACS+服务和属性对组或用户配置文件，遵从这些步骤：

1. 在Cisco Secure管理员高级配置程序，请选择**Members选项**。在浏览器窗格，请点击TACACS+属性分配的组或用户配置文件的图标。
2. 如果需要，在配置文件窗格，请点击**Profile图标**展开它。包含属性可适用对选定配置文件或服务的列表或对话框在窗口显示在屏幕的右下。在此窗口的信息更改基于哪些配置文件或在配置文件窗格服务您选择。
3. 点击服务或协议您想要添加和单击**应用**。服务被添加到配置文件。
4. 输入或选择在Attribute窗口的必要的文本。有效条目在应用的CSU 2.3的属性选项策略解释UNIX参考指南的。**注意：** 如果分配属性值在组配置文件级别和您指定显示一个**绝对**复选框的属性，精选该复选框分配值绝对状态。赋予的绝对状态值不可能由任何冲突的值改写分配在辅助组配置文件或用户配置文件级别。
5. 为您需要添加的每份其它服务或协议通过重复步骤1。
6. 当所有变动做时，请单击**提交**。

分配RADIUS属性到组或用户配置文件

对组或用户配置文件的分配特定RADIUS属性：

1. 分配RADIUS词典到组配置文件：在Cisco Secure管理员高级配置程序的成员页，请点击**组**或**用户**图标，然后点击在配置文件窗格的**Profile图标**。在属性窗格中，选项菜单显示。在**选项菜单**，请点击您希望组或用户使用RADIUS词典的名称。(例如， RADIUS -思科。)单击 **Apply**。
2. 添加需要的检查项目和回复属性到RADIUS配置文件：**注意：** 检查项目是为验证要求的属性，例如用户ID和密码。回复属性是属性发送对网络接入服务器(NAS)，在配置文件通过认证程序后，例如帧协议。对于检查项目和回复属性的列表和说明，参考RADIUS属性-值对和词典管理在CSU 2.3 UNIX参考指南的。在Profile窗口，请点击RADIUS - dictionaryname文件夹图标。(您很可能需要点击展开RADIUS文件夹的配置文件的+符号。)检查项目和回复属性选项显示在Attribute Group窗口。使用一个或很多这些属性，点击您要使用的属性，然后单击请**应用**。您能每次添加超过一个属性。单击**+** RADIUS的符号- dictionaryname展开文件夹。**注意：** 如果选择RADIUS-Cisco11.3选项，请确保Cisco IOS软件版本11.3.3(T)或以后在您连接的NAS安装并且添加新的命令行到您的NAS配置。参考充分启用在CSU 2.3的RADIUS-Cisco11.3字典UNIX参考指南的。
3. 指定已添加检查项目和回复属性的值：**警告：** 对于RADIUS协议，继承是附加的与分层的相对

。(TACACS+协议使用分层的继承)。例如，如果分配同样回复属性到用户和组配置文件，授权发生故障，因为NAS两次接收属性数量。它不能有意义回复属性。请勿分配同一个检查项目或回复属性到组和用户配置文件。点击**检查项目**或**回复属性**或者点击两个。可适用的检查项目和回复属性值列表在更低右侧的窗口发表。点击+展开文件夹的符号。点击您想要分配的值，然后单击**应用**。关于值的更多信息，参考RADIUS属性-值对和词典管理在CSU 2.3 UNIX参考指南的。**注意：** 如果分配属性值在组配置文件级别和您指定显示一个绝对复选框的属性，精选该复选框分配值绝对状态。分配的值绝对状态不可能由任何冲突的值改写分配在辅助组配置文件或用户配置文件级别。当您完成进行的更改时，请单击**提交**。

4. 使用一个或很多这些属性，点击您要使用的属性，然后单击请**应用**。您能每次适用超过一个属性。

指定访问控制权限级别

超级用户管理员使用Web权限属性分配级别访问控制权限给Cisco Secure用户。

1. 在Cisco Secure管理员高级配置程序，请点击访问控制权限您想要分配，然后点击在配置文件窗格的Profile图标的用户。
2. 在选项菜单，请点击**Web权限**并且选择这些值之一。**0** -拒绝用户包括能力更改用户的Cisco Secure密码的所有访问控制权限。**1** -准许对CSUser网页的用户访问。这允许Cisco Secure用户更改他们的Cisco Secure密码。关于如何更改密码的详情，参考用户级功能(更改密码)在简单用户和ACS管理。**12** -授权用户组管理员权限。**15** -授权用户系统管理员特权。**注意：** 除0之外，如果选择任何Web权限选项，您必须也指定密码。要满足Web权限密码需求，单个空格是至少可接受的。

启动和终止CSU

通常， CSU自动地开始，当您开始或重新启动安装的SPARCstation时。然而，您能手工开始CSU或者关闭它，无需关闭整个SPARCstation。

登陆作为[Root]对您安装CSU的SPARCstation。

要手工开始CSU，请键入：

```
# /etc/rc2.d/S80CiscoSecure
```

要手工终止CSU，请键入：

```
# /etc/rc0.d/K80CiscoSecure
```

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco Secure ACS for UNIX 支持页
- TACACS+ 支持页
- RADIUS 支持页
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems