ISE 访客帐户 RADIUS/802.1x 认证的配置示例

介绍

本文档介绍了如何在思科身份服务引擎（ISE）上配置基于 RADIUS 认证和基于门户认证的访客帐户。

先决条件

要求

本文需要您了解思科身份服务引擎（ISE）和 IEEE 802.1x 的基本知识。

使用的组件

本文档中的信息基于思科身份服务引擎（ISE）。

本文档中的资料是从一个特定实验室环境中的设备上生成的。本文档中使用的所有设备以缺省（默认）配置开始配置。如果您的网络是正在使用的生产系统，请确保您了解所有命令带来的潜在影响。

背景资料

本文档中描述的该功能在不同的 ISE 版本之间的工作方式不同。

*ISE 1.1.1 版本之前：所有访客帐户在创建时处于非活动状态，通过门户网站进行第一次登录前他们不会被激活。处于非活动状态无法使用 RADIUS 登录。

*ISE 1.1.1 及更高版本：默认组（ActivatedGuest）中的访客帐户在创建后就激活。

配置

所有版本的配置注意事项

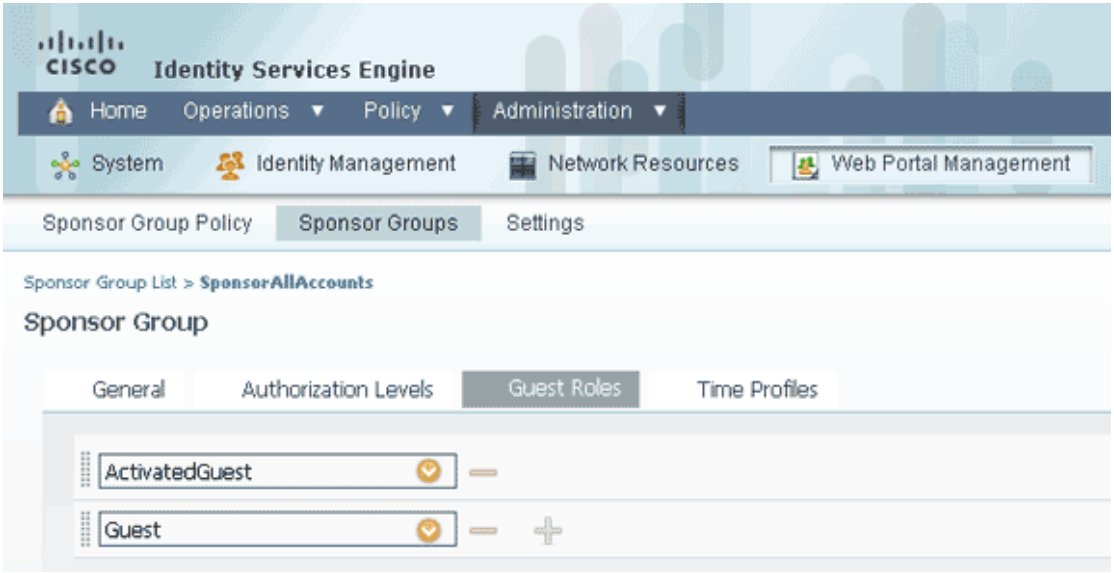
下列注意事项适用于所有版本：

*使用访客帐户的任何认证规则应该有内部用户源。
*任何授权规则序列应符合访客（ISE 1.1.1 版本前）或活动访客（ISE 1.1.1 及以后版本）。
*赞助人门户和自注册门户的配置应该把访客帐户放到正确的组中。对于 ISE 1.1.1，正确的组必须是 ActivatedGuest，以避免通过客户门户进行第一次认证要求。

ISE 1.1.1 和更高版本的配置

完成下列步骤以配置 ISE 1.1.1 及更高版本：

1.配置赞助人组以分配 ActivatedGuest 角色。



2.配置一个授权政策以便允许访问 ActivatedGuest 组。

赞助人用户现在应该能够以 ActivatedGuest 角色创建访客。这里创建的用户应该能够通过内部的身份存储数据库以 802.1x 或任何其他身份验证方法登录。在现场验证日志中，你应该看到下面图像中显示的文字：

Identity Group:	ActivatedGuest
Allowed Protocol Selection Matched Rule:	Default
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Users

注意：身份组是正确的，身份存储数据库为“内部用户”。

原文链接：http://www.cisco.com/en/US/products/ps11640/products_configuration_example09186a0080bec91d.shtml
翻译人：谢清
译于 2013 年 6 月