Cisco ACS 5.X集成用RSA SecurID令牌服务器

Contents

Introduction

本文描述如何集成Cisco访问控制系统(ACS)版本5.x与RSA SecurID验证技术。

背景信息

Cisco Secure ACS支持RSA SecurID服务器作为外部数据库。

RSA SecurID二要素验证包括用户的personal identification number (PIN)和生成根据时间代码算法的单一用处令牌代码的一个单个注册的RSA SecurID令牌。

一个不同的令牌代码生成在固定的间隔，通常每30或60秒。RSA SecurID服务器验证此动态认证代码。每个RSA SecurID令牌是唯一，并且预测将来令牌的值根据通过令牌是不可能的。

因此，当一个正确的令牌代码与PIN一起被供应，有人是有效用户的高确定程度。所以，
RSA SecurID服务器比常规可再用的密码提供一个更加可靠的认证机制。

您能集成Cisco ACS 5.x与RSA SecurID验证技术用这些方式：

- RSA SecurID代理程序-用户用用户名和密码验证通过本地RSA协议。

- RADIUS协议-用户用用户名和密码验证通过RADIUS协议。

Prerequisites

Requirements

Cisco建议您有这些题目基础知识：

- RSA安全
- 思科安全访问控制系统(ACS)

Components Used

本文档中的信息基于以下软件和硬件版本：

- 思科安全访问控制系统(ACS)版本5.x
- RSA SecurID令牌服务器

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

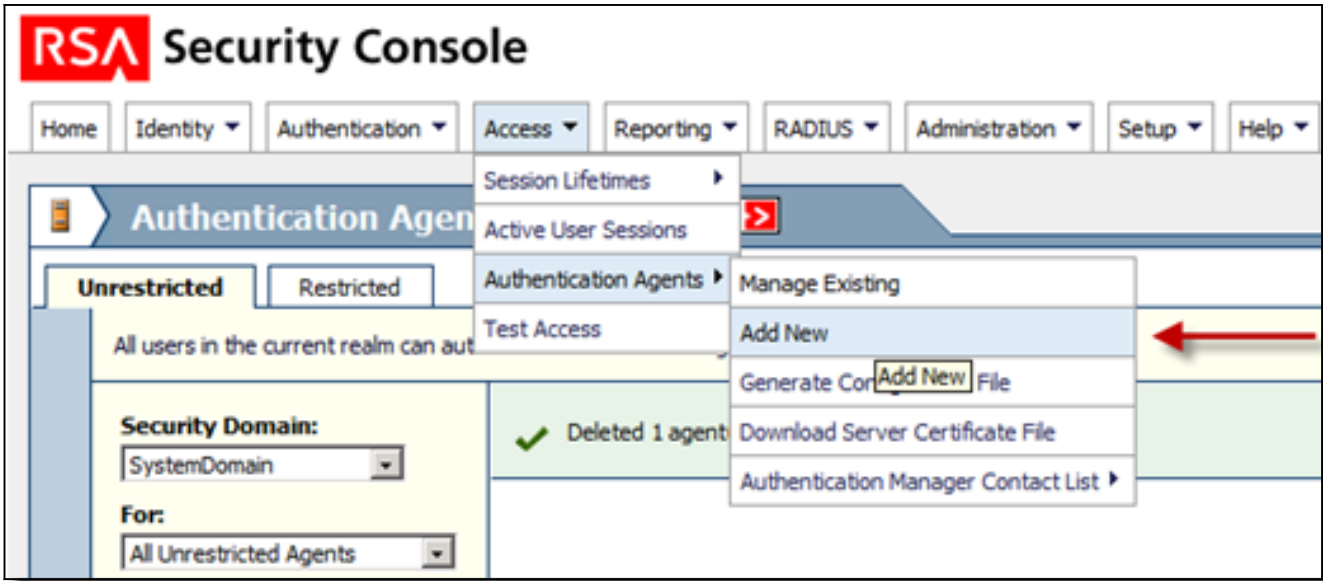
配置

RSA服务器

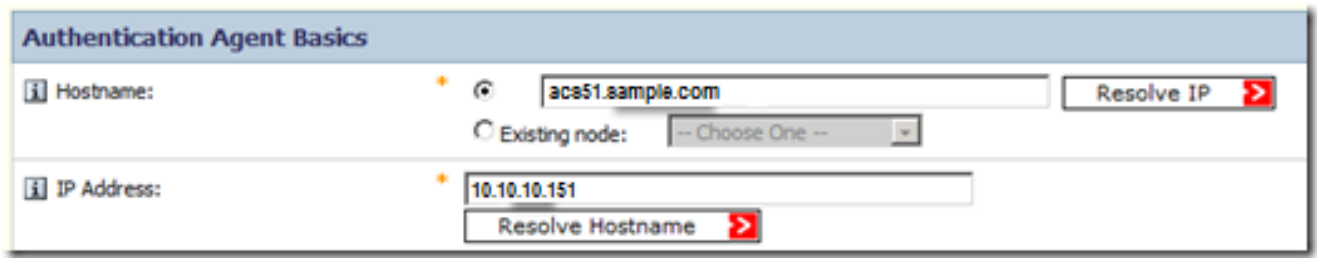
此程序描述RSA SecurID服务器管理员如何创建认证代理程序和一个配置文件。认证代理程序基本上是域名服务器(DNS)名字和有权利访问RSA数据库设备、软件或者服务的IP地址。配置文件基本上描述RSA拓扑和通信。

在本例中，RSA管理员必须创建两个ACS实例的两个代理程序。

1. 在RSA安全控制台中，请连接**访问>认证新代理程序的>**Add ：

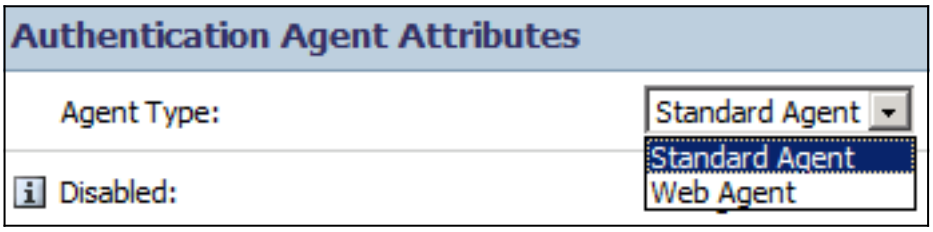


2. 在添加新证书代理窗口，请定义一个主机名和IP地址两个代理程序中的每一个的：

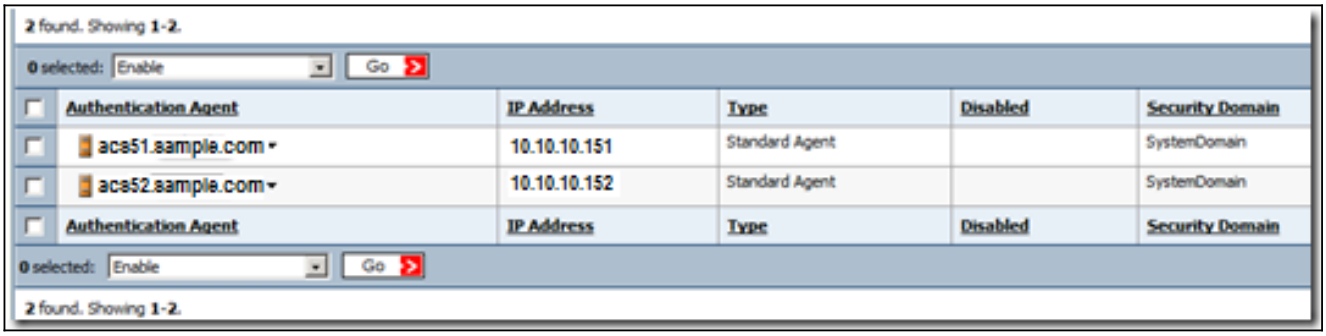


DNS转发，并且ACS代理程序的反向查找应该工作。

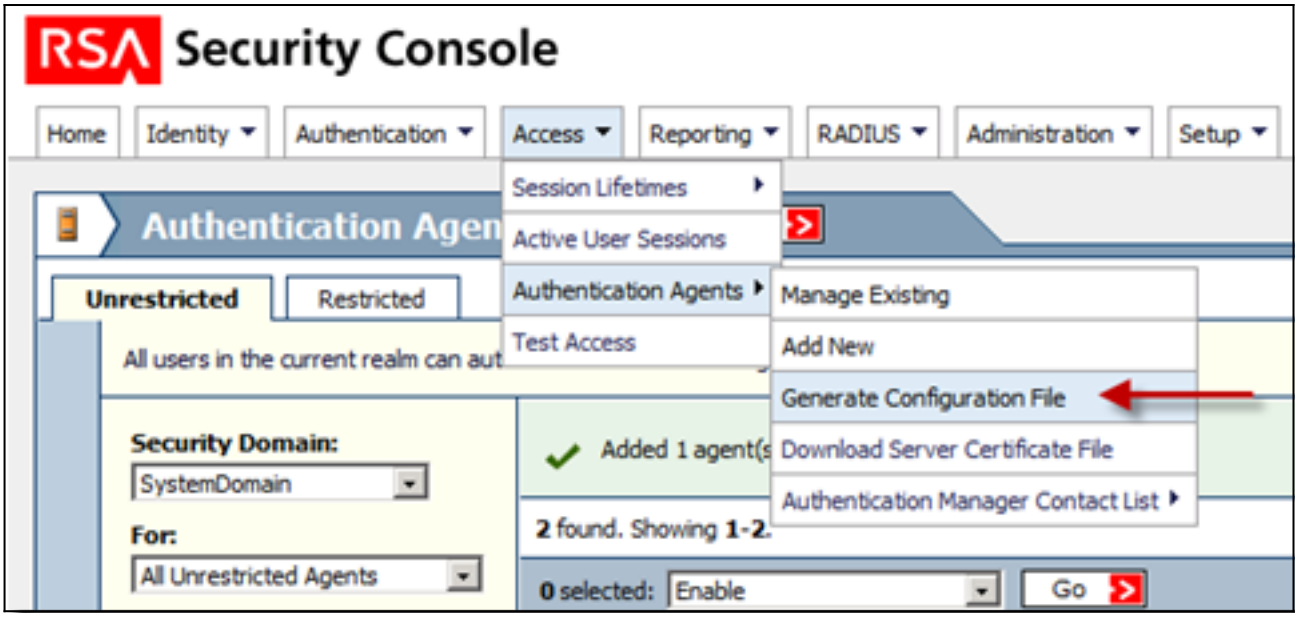
3. 定义代理程序类型成标准的代理程序：



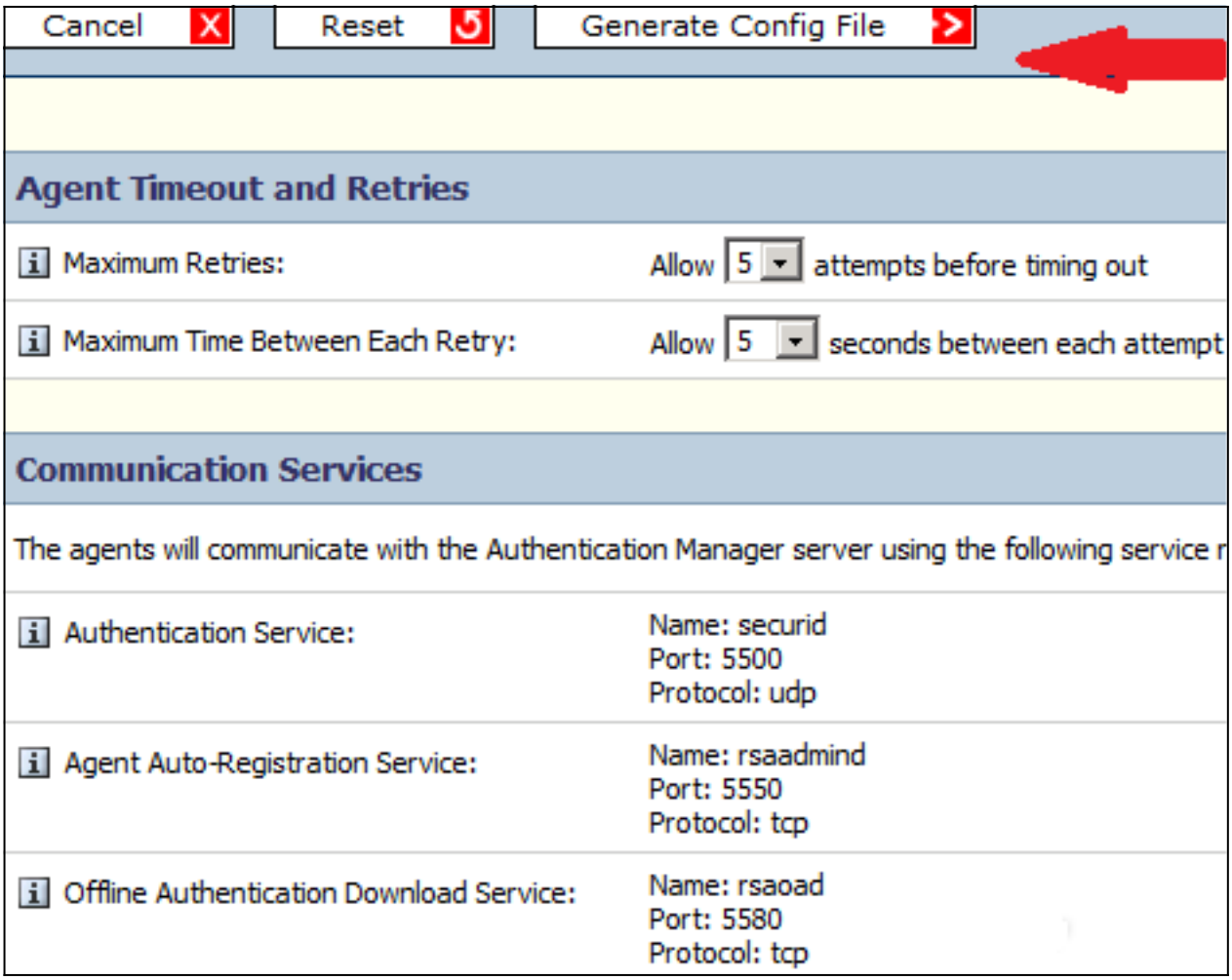
这是您看到信息的示例，一旦代理程序被添加：



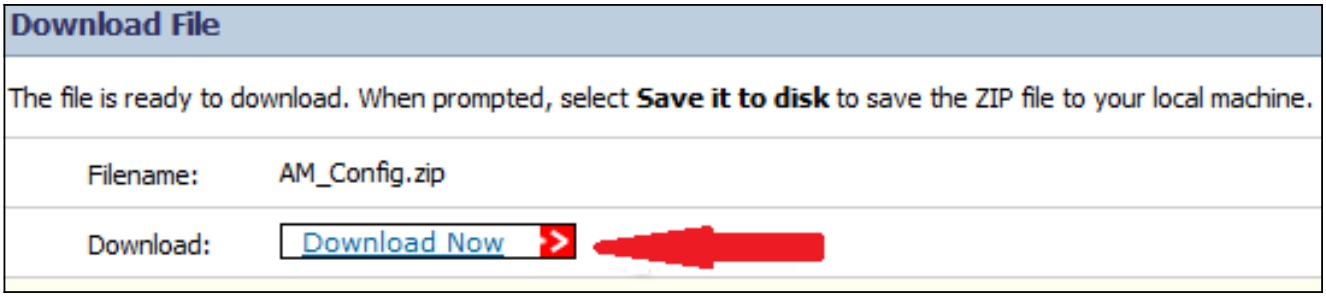
4. 在RSA安全控制台中，请连接**访问>认证代理程序>生成配置文件**为了生成sdconf.rec配置文件：



5. 请使用默认值最大重试次数和每重试次数之间的最大时间：



6. 下载配置文件：

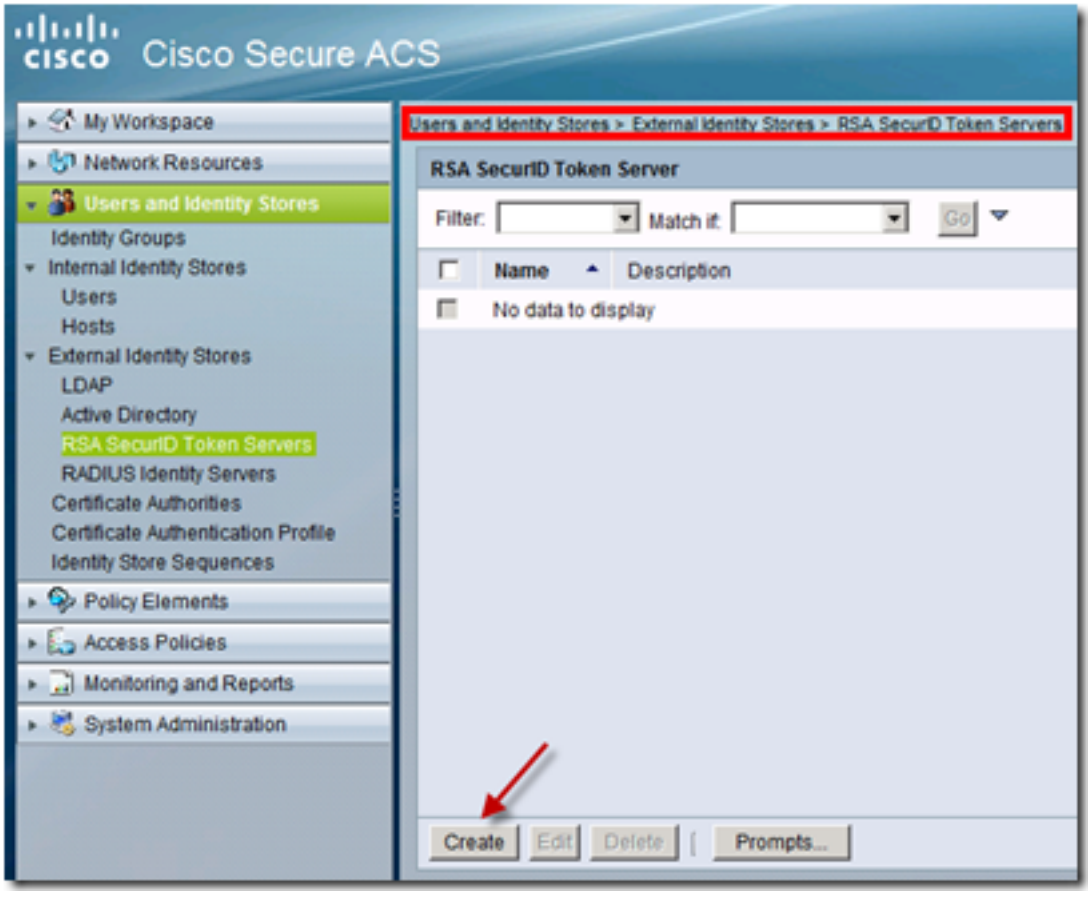


.zip文件包含实际部署sdconf.rec文件， ACS管理员需要为了完整的配置任务。

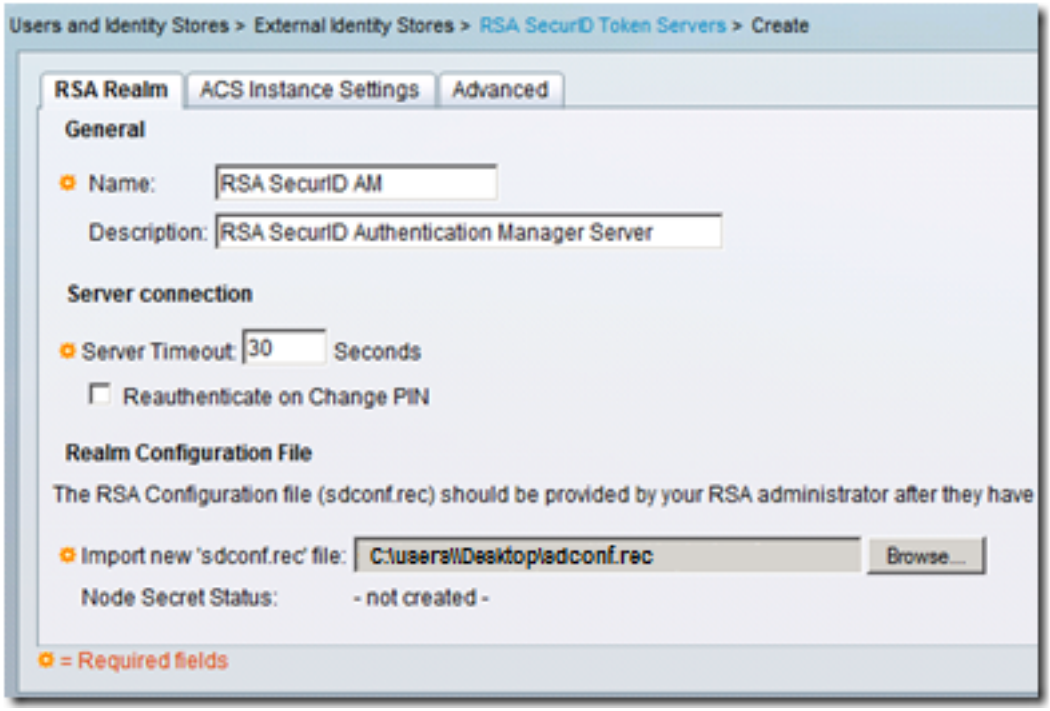
ACS版本5.X服务器

此程序描述ACS管理员如何检索并且提交配置文件。

1. 在Cisco Secure ACS版本5.x控制台中，请连接给**用户，并且身份存储>外部身份存储> RSA SecurID令牌服务器**，并且点击**创建**：



2. 输入RSA服务器的名字，并且访问对从RSA服务器下载的sdconf.rec文件：



3. 选择文件，并且点击**提交**。

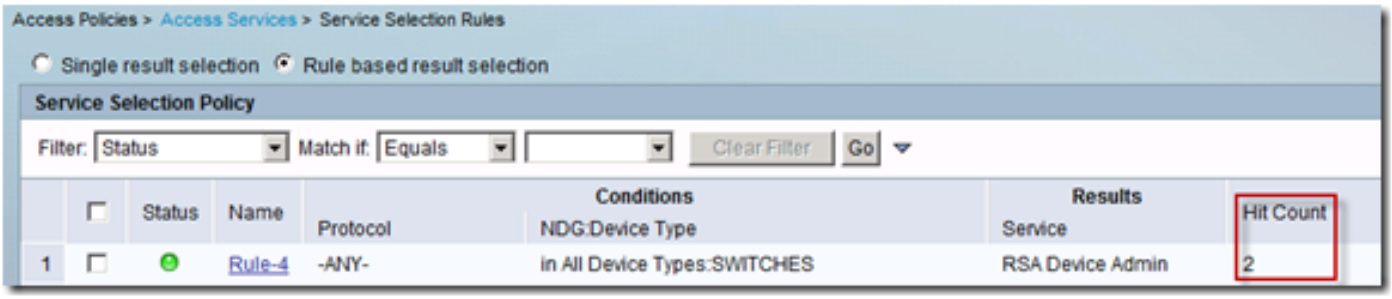
Note:第一次ACS联系令牌服务器，另一个文件，调用了节点秘密文件，为在RSA认证管理器的ACS代理程序被创建和下载到ACS。此文件使用加密的通信。

Verify

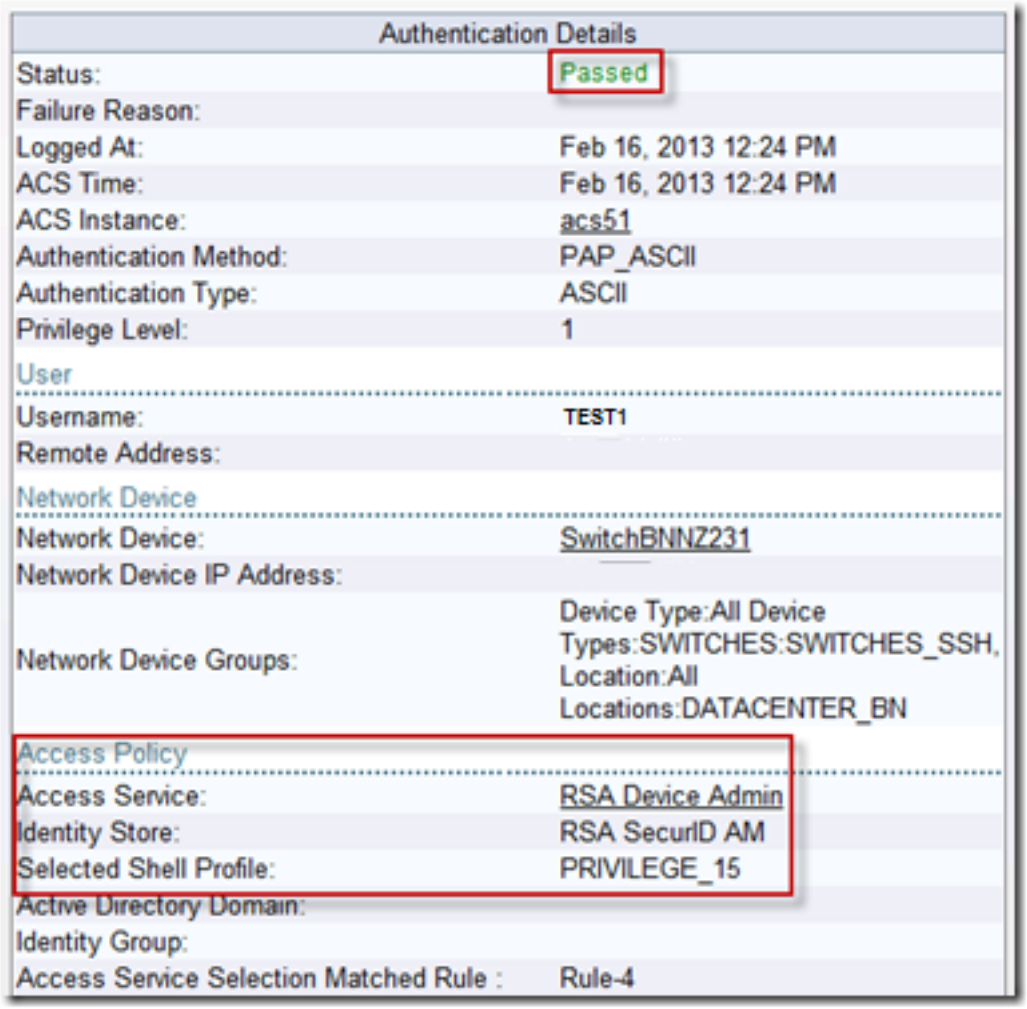
使用本部分可确认配置能否正常运行。

ACS版本5.X服务器

为了验证一个成功的登录，请去ACS控制台，并且查看命中计数：



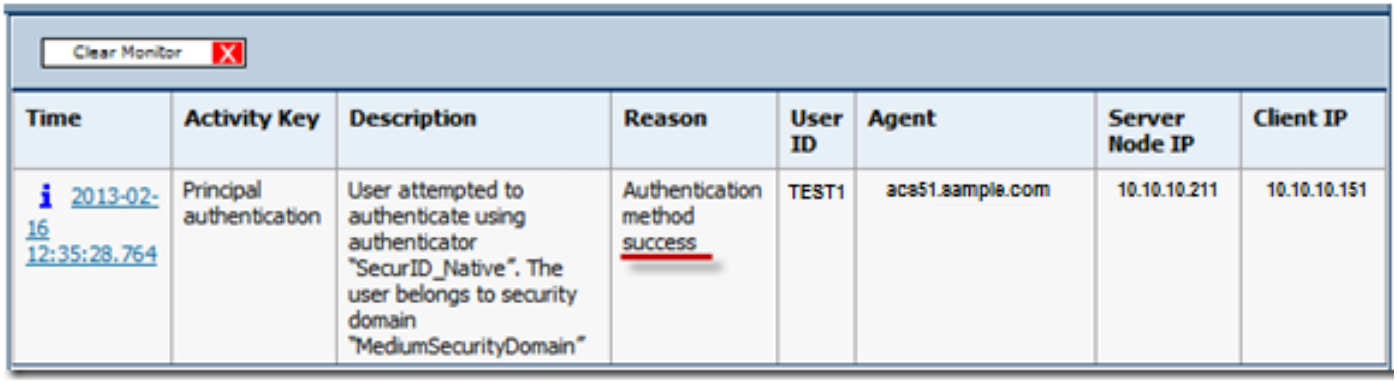
您能也查看从ACS日志的认证详细资料：



Authentication Details	
Status:	Passed
Failure Reason:	
Logged At:	Feb 16, 2013 12:24 PM
ACS Time:	Feb 16, 2013 12:24 PM
ACS Instance:	acs51
Authentication Method:	PAP_ASCII
Authentication Type:	ASCII
Privilege Level:	1
User	
Username:	TEST1
Remote Address:	
Network Device	
Network Device:	SwitchBNNZ231
Network Device IP Address:	
Network Device Groups:	Device Type:All Device Types:SWITCHES:SWITCHES_SSH, Location:All Locations:DATACENTER_BN
Access Policy	
Access Service:	RSA Device Admin
Identity Store:	RSA SecurID AM
Selected Shell Profile:	PRIVILEGE_15
Active Directory Domain:	
Identity Group:	
Access Service Selection Matched Rule :	Rule-4

RSA服务器

为了验证成功的验证，请去RSA控制台，并且检查日志：



Clear Monitor

Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP
2013-02-16 12:35:28.764	Principal authentication	User attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "MediumSecurityDomain"	Authentication method success	TEST1	acs51.sample.com	10.10.10.211	10.10.10.151

Troubleshoot

本部分提供了可用于对配置进行故障排除的信息。

创建座席登录(sdconf.rec)

为了配置在ACS版本5.3的一个RSA SecurID令牌服务器， ACS管理员必须有sdconf.rec文件。sdconf.rec文件是指定的配置记录文件RSA代理程序如何与RSA SecurID服务器领域连通。

为了创建sdconf.rec文件， RSA管理员应该添加ACS主机作为在RSA SecurID服务器的一台代理主机和生成此代理主机的一个配置文件。

重置节点秘密(securid)

在代理程序与RSA SecurID服务器后最初连通，服务器提供代理程序节点秘密文件被呼叫的securid。服务器和代理程序之间的随后的通信依靠节点秘密的交换为了验证其他的真实性。

通常，管理员也许必须重置节点秘密：

1. RSA管理员必须非选定在代理主机记录的节点秘密被创建的复选框在RSA SecurID服务器。
2. ACS管理员必须从ACS删除SECURID文件。

覆盖自动负载均衡

RSA SecurID代理程序自动地均衡在RSA SecurID服务器的被请求的负荷在领域。然而，您有手工均衡的选项负荷。您能指定其中每一台使用的服务器代理主机。您能指定优先级到每个服务器，以便代理主机比其他频繁地指向认证请求到一些服务器。

您在文本文件必须指定优先级设置，保存它作为sdopts.rec和加载它到ACS。

请手工干预删除下来RSA SecurID服务器

当RSA SecurID服务器发生故障时，自动排除机制不迅速总是运作。从ACS删除sdstatus.12文件为了加速此进程。