与AD凭证配置示例的ISE管理门户访问

目录

<u>简介</u> <u>先决条件</u> <u>Componenets使用了</u> <u>配置</u> <u>加入ISE对AD</u> <u>选择目录组</u> <u>启用AD的管理访问</u> 配置Admin group对AD组映射 设置Admin group的RBAC权限 访问与AD凭证的ISE 验证 <u>故障排除</u> 相关信息

简介

本文描述配置示例为使用Microsoft Active Directory (AD)作为管理访问的外部标识存储对思科身份 服务引擎(ISE)管理GUI。

<u>先决条件</u>

Cisco 建议您了解以下主题:

- Cisco ISE版本1.1.x或以上的配置
- Microsoft AD

Componenets使用了

本文档中的信息基于以下软件和硬件版本:

- Cisco ISE版本1.1.x
- Windows服务器2008版本2

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。

配置

请使用此部分为了配置为使用Microsoft AD作为管理访问的外部标识存储对思科ISE管理GUI。

加入ISE对AD

- 1. 导航对Administration >身份管理>外部标识来源>活动目录。
- 2. 输入AD域名和标识存储名称,并且点击加入。
- 3. 进入能添加和做对计算机对象的变动AD帐户的凭证,并且点击保存配置。

🛕 Home Operations 🔻	Policy 🔻 Admit	itstration 🔹 😶 Task Naviga
🔆 System 🛛 😤 Identity	Management 🔛	Network Resources 📧 Web Portal Management
Identities Groups Ext	ernal Identity Sources	Identity Source Sequences Settings
External Identity Sources		Active Directory > AD1
⊕- ≣ '≣	- -	Connection Advanced Settings Groups Attributes
🚞 Certificate Authentication Pro	afile 🔿	* Domain Name Domian.local
2 Active Directory		* Identity Store Name AD1
EDAP LDAP	۲	One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin.
🚞 RADDUS Token	۲	Belectione hode for fest Connection
E RSA SecurID	۲	Car Con Carlos Connector *
		ISE Node ISE Node Role Status
		✓ ISE-JKATYAL STANDALONE Z Connected to windomain.local

选择目录组

- 1. 导航对Administration >身份管理>外部标识来源>活动目录> Groups >Add >挑选组表目录。
- 2. 导入您的管理员属于至少的一AD组。

🛕 Home Operations 🔻 Policy 🔻	Administration 💌	👓 Task Navigator 👻 🚷
🔆 System 🛛 👰 Identity Management	The Network Resources 😰 Web Portal Management	
Identities Groups External Identity 8	ources Identity Source Sequences Settings	
External Identity Sources	Active Directory > AD1 Connection Advanced Settings Groups Attributes	_
Active Directory	Name	
EDAP	Domain.local /Users/Domain Admins S	
RSA SecurID		

启用AD的管理访问

完成这些步骤为了启用AD的基于密码的验证:

- 1. 导航对管理>System > Admin访问>验证。
- 2. 从**认证方法**选项卡,请选择**根据的密码**选项。
- 3. 选择从标识来源下拉菜单的AD。
- 4. 点击Save Changes。

🛕 Home Operations 🕶 Policy 💌 Administ	ration 🔻	👓 Task Navigator + 😣
🔆 System 🖉 Identity Management 🔛 N	letwork Resources 🛛 😹 Web Portal Management	
Deployment Licensing Certificates Logging	Nantenance Admin Access Settings	
Admin Access	Authentication Method Password Policy	
4•≡ 1	Authentication Type	
Authentication Authentication Authentication Authentication	Password Based * Identity Source A0:A01 *	
🕨 🧱 Settings	O Clent Certificate Based	

配置Admin group对AD组映射

定义思科ISE Admin group并且映射它给AD组。这允许授权确定角色根据组成员的管理员的基于访问控制(RBAC)权限在AD。

- 1. 导航给管理>System > Admin访问>管理员> Admin组。
- 2. 单击添加在表报头为了查看新的Admin group配置窗格。
- 3. 输入名称对于新的Admin group。
- 4. 在Type字段,请检查**外部**复选框。
- 5. 从**外部组**下拉菜单,请选择您希望此Admin group映射的AD组,如对挑选目录组部分定义。
- 6. 点击Save Changes。

🍐 Home Operations 🔻 Policy 🔻	Administration •	👓 Task Navigator 🔻 🙆
🔆 System 🙀 Identity Management	🖬 Network Resources 🛛 🙀 Web Portal Management	
Deployment Licensing Certificates	Logging Maintenance Admin Access Settings	
Admin Access	Admin Group > 15E-Administration_AD1 Admin Group * Name ISE-Administration_AD1 Description Type Internal External External Identity Source NameAD1	
Re Hulpdusk Admin Re Identity Admin Re ISE-Administration_AD1 Re Pini Admin Re Network Device Admin	External Groups " Domain.local/Users/Domain Adn 4 Save Reset	
R Pokcy Admin R RBAC Admin R Super Admin R System Admin F Settings	e a e a	

设置Admin group的RBAC权限

完成这些步骤为了分配RBAC权限到在前面部分创建的Admin组:

- 1. 导航对管理>System > Admin访问>授权>Policy。
- 2. 从在右边的操作下拉菜单,请选择插入下面新建的策略为了添加一项新的策略。
- 3. 创建呼叫ISE_administration_AD的新规则,映射它与在AD部分的Enable (event)管理访问定义 的Admin group,并且分配它权限。Note:在本例中,呼叫**特级Admin的**Admin group分配,与 标准的管理帐户是等同的。

4. 点击保存更改,并且保存的更改的确认显示在GUI的右下角。

🛕 Home Operations 🔹 Policy 🔻	Administration 🔹	🗝 Task Navigator 👻 🌔
🔆 System 🛛 👙 Identity Management	Retwork Resources 😹 Web Portal Management	
Deployment Licensing Certificates	Logging Maintenance Admin Access Settings	
Admin Access	Create Role Dased Access Control policies by configuring rules based on Admin groups, Menu Access permissions (nenu items), Data Access permissions are not allowed on a single policy. You can copy the default provide the value of the subjects permissions will be the apprepare of all permissions from each applicable policy. Permit overrides Deny. (The polyheducial order of the policy name). Reac Policies	emissions (identity group data polices shown below, then inwising, all applicable policies lides are displayed in
T Authentication	Rule Name Admin Groups Permissions	
Pelcy	Helpdesk Admin Policy If Helpdesk Admin 🚸 then Helpdesk Admin Manu Access 🔶	쯡 Actions ▼
Admin there Admin Croups	Identity Admin Policy If Identity Admin 🔷 then	🔆 Actions 👻
8 Helpdesk Admin 8 Identity Admin	Image: Notice and the indexes and ind	출 Actions *

与AD凭证的访问ISE

完成这些步骤为了访问与AD凭证的ISE :

- 1. 管理GUI的注销。
- 2. 从标识来源下拉菜单的挑选AD1。
- 3. 输入从AD数据库和登录的用户名和密码。

	Identity Services Engine Username iseadmin Password Identity Source AD1 Identity Source Cogin Remember username Problem logging in?	
© 2012 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco System and/or its affiliates in the U.S and certain other countries.	ns logo are registered trademarks of Cisco Systems, Inc.	-ili-ili- cisco

Note:对内部用户存储的ISE默认,在AD是不可得到的情况下或者使用的帐户凭证在AD不存在。这实现快速登录,如果使用内部存储,当AD为管理访问时配置。



为了确认您的配置适当地工作,请验证认证的用户名在ISE GUI的角的。



<u>故障排除</u>

目前没有针对此配置的故障排除信息。

相关信息

- <u>思科身份服务引擎用户指南,版本1.1 -管理Indentities和Admin访问</u>
- <u>技术支持和文档 Cisco Systems</u>