使用AD憑證的ISE管理門戶訪問配置示例

目錄

<u>簡介</u> <u>必要條件</u> 使用的元件集 設定 <u>將ISE加入AD</u> <u>選擇目錄組</u> <u>啟用AD的管理訪問</u> <u>配置管理組到AD組的對映</u> <u>設定管理員組的RBAC許可權</u> 使用AD憑證訪問ISE <u>驗證</u> <u>疑難排解</u> 相關資訊

簡介

本文檔介紹使用Microsoft Active Directory(AD)作為外部身份庫對思科身份服務引擎(ISE)管理GUI進 行管理訪問的配置示例。

必要條件

思科建議您瞭解以下主題:

- •思科ISE版本1.1.x或更高版本的配置
- Microsoft AD

使用的元件集

本文中的資訊係根據以下軟體和硬體版本:

- Cisco ISE版本1.1.x
- Windows Server 2008版本2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。 使用此部分可以配置使用Microsoft AD作為外部身份庫以管理訪問思科ISE管理GUI。

將ISE加入AD

- 1. 導航到管理>身份管理>外部身份源> Active Directory。
- 2. 輸入AD域名和身份庫名稱,然後按一下加入。
- 3. 輸入可以新增和更改電腦對象的AD帳戶的憑據,然後按一下儲存配置。

🛕 Home Operations 🔻 Pol	cy 🔻 Admit	listration 🔻			🔫 Task Navigal
🔆 System 🛛 👰 Identity Manage	ement 🔳	Network Resources 🛛 🛃 Web Port	al Management		
Identities Groups External Id	entity Sources	Identity Source Sequences Sett	ngs		
External Identity Sources		Active Directory > AD1			
◆ • ■ '≡	- 	Connection Advanced S	ettings Groups	Attributes	
Certificate Authentication Profile		• Do	main Name Domian.local		
Active Directory		* Identity	Store Name AD1		
EDAP LDAP	۲	One or more nodes may be select	ed for Join or Leave operati	ons. If a node is joined then a leave operation	is required before a rejoin.
E RADOUS Token	۲	Select one node for Test Connects	on		
E RSA SecuriD	۲	유럽 Join 유럽 Leave 유럽 Test Co	mechon v		
		ISE Node	 ISE Node Role 	Status	
		ISE-JKATYAL	STANDALONE	Connected to windomain.local	

選擇目錄組

- 1. 導航到Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory。
- 2. 至少匯入管理員所屬的一個AD組。

🛕 Home Operations 🔻 Policy 🔻 Adm	inistration 💌	🗝 Task Navigator 👻 🚷
🔆 System 🛛 👰 Identity Management	Network Resources 🛞 Web Portal Management	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
External Identity Sources	Adve Directory > AD1 Connection Advanced Settings Group: Attributes	
T ACAYE DIRECTORY	Name 🔺	
RADUS Token	Domain.local /Users/Domain Admins	
RSA Securit		

啟用AD的管理訪問

完成以下步驟,為AD啟用基於密碼的身份驗證:

- 1. 導航到Administration > System > Admin Access > Authentication。
- 2. 在Authentication Method頁籤中,選擇Password Based選項。
- 3. 從身份源下拉選單中選擇AD。

4. 按一下Save Changes。

👌 Home Operations 🔻 Policy 💌 Administration 🔻		🕶 Task Navigator + 🙆
🔆 System 🛛 😤 Identity Management 📲 Network Resources 😹 Web Por	tal Management	
Deployment Licensing Certificates Logging Maintenance Admin Access	Settings	
Admin Access	* Identity Source A0:A01 *]

配置管理組到AD組的對映

定義Cisco ISE管理員組並將其對映到AD組。這樣可授權基於AD中的組成員身份確定管理員的基於 角色的訪問控制(RBAC)許可權。

- 1. 導航到Administration > System > Admin Access > Administrators > Admin Groups。
- 2. 在表頭中按一下Add以檢視新的管理員組配置窗格。
- 3. 輸入新管理員組的名稱。
- 4. 在「型別」欄位中,選中External覈取方塊。
- 5. 從External Groups下拉選單中,選擇希望此管理員組對映到的AD組,如「選擇目錄組」部分 中所定義。
- 6. 按一下Save Changes。

💧 Home Operations 🔻 Policy 💌 Admi	nistration 💌	👓 Task Navigator 👻 🙆
🔆 System 😤 Identity Management	Network Resources 🙀 Web Portal Management	
Deployment Licensing Certificates Logg	ing Maintenance Admin Access Settings	
Admin Access	Admin Groups > ISE-Administration_AD1 Admin Group Name ISE-Administration_AD1 Description Type Internal IsExternal External Identity Source Name AD1	
泉 Hulpdusk Admin 泉 Identiky Admin 泉 ISE-Administration_AD1 泉 Mnil Admin 泉 Network Device Admin	External Groups Tomain.local/Users/Domain Adn The Adn	
 Reacy Admin Reacy Admin Super Admin System Admin System Admin Settings 	•	

設定管理員組的RBAC許可權

完成以下步驟,將RBAC許可權分配給在上一節中建立的管理組:

- 1. 導航到Administration > System > Admin Access > Authorization > Policy。
- 2. 從右側的Actions下拉選單中,選擇Insert New Policy Below以新增新策略。
- 3. 建立一個名為ISE_administration_AD的新規則,將其與「啟用AD管理訪問許可權」部分中定

義的管理員組進行對映,然後為其分配許可權。**附註**:在本示例中,分配了名為Super Admin的管理組,該組相當於標準管理員帳戶。

4. 按一下Save Changes, GUI的右下角將顯示對已儲存更改的確認。

🚖 Home Operations 👻 Policy	 Admir 	ristration 🔻					🔫 Task Navigator 👻 🌔
🔆 System 🛛 🙅 Identity Managem	ent 📕	Network Reso	urces 🛛 🔠 Web Portal Manaj	yemen	t		
Deployment Licensing Certificat	es Logg	ing Maintena	ance Admin Access Sett	ings			
Admin Access	٩	Create Role Dat clements) and a modify them as will be evaluate alphabetical on	sed Access Control policies by config other conditions. Note that multiple M needed. Note that system-created a d. The subject's permissions will be ti- lar of the policy name).	uring ru lenu,Da ind def he aggr	les based on Admin groups, Menu A sta Access permissions are not allow auf policies connot be updated, en egate of all permissions from each a	Access permissions (menu itens), Data Ao ved on a single policy. You can copy the d d default policies cernot be deleted. For a applicable policy. Permit overrides Deny. (cess permissions (dentity group data lefault policies shown below, then section making, all applicable policies (The policies are displayed in
Reference in the second	23.4	· RBAC Po	licies				
* Authorization			Rule Name		Admin Groups	Permissions	
🕨 🥝 Perminakana			Helpdesk Admin Policy	1	Helpdesk Admin	then	🔆 Actions *
Selicy		Helpdes	k Admin Menu Access 🛛 🔶				
 Administrators Administrators 			Identity Admin Policy	ľ	Identity Admin	then	🕸 Actions 👻
* 🥵 Admin Groups		Identity Av	dmin Menu Access 🛛 🔶				
🧏 Helpdesk Admin 🕵 Identity Admin			ISE administration_AD	1	ISE-Administration_AD1	⊲> then	횰 Actions *
💫 ISE-Administration_AD1		Super Ad	min Menu Access 🛛 🔶				

使用AD憑證訪問ISE

完成以下步驟,以便使用AD憑證訪問ISE:

- 1. 從管理GUI註銷。
- 2. 從Identity Source下拉選單中選擇AD1。
- 3. 輸入AD資料庫中的使用者名稱和密碼,然後登入。

	Identity S	ervices Engine	
	Username Password Identity Source	iseadmin	

附註:如果AD無法訪問,或者使用的帳戶憑證在AD中不存在,則ISE預設為內部使用者儲存 。如果在為AD配置管理訪問時使用內部儲存,這將有助於快速登入。



為了確認您的配置工作正常,請驗證ISE GUI右上角的身份驗證使用者名稱。



疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 思科身份服務引擎使用手冊,版本1.1 管理身份和管理訪問許可權
- 技術支援與文件 Cisco Systems