為ISE管理配置證書或基於智慧卡的身份驗證

目錄

簡介 必要條件 需求 採用元件 設定 網路圖表 將ISE加入Active Directory 選擇目錄組 為管理訪問啟用Active Directory基於密碼的身份驗證 將外部身份組對映到管理員組 匯入受信任的證書 配置證書身份驗證配置檔案 啟用基於客戶端證書的身份驗證 驗證 疑難排解

簡介

本文檔介紹如何為身份服務引擎(ISE)管理訪問配置基於客戶端證書的身份驗證。在本示例中 ,ISE管理員根據使用者證書進行身份驗證,以獲得對思科身份服務引擎(ISE)管理GUI的管理員訪 問許可權。

必要條件

需求

思科建議瞭解以下主題:

- •用於密碼和證書身份驗證的ISE配置。
- Microsoft Active Directory(AD)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- •思科身分識別服務引擎(ISE)版本2.6
- Windows Active Directory(AD)Server 2008版本2
- 憑證

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。如果網路處於活動狀態,請確保瞭解任何配置的潛在影響。

設定

使用此部分將客戶端證書或智慧卡配置為外部身份,以便管理訪問思科ISE管理GUI。

網路圖表



將ISE加入Active Directory

- 1. 選擇Administration > 身份管理>外部身份源> Active Directory。
- 2. 在思科ISE中建立具有加入點名稱和AD域的Active Directory例項。
- 3. 按一下「Submit」。

-4[44]>+ CISCO Identity Services Engine Home → Context Visibility	erations + Policy - Administration + Work Centers	License Warning 🔺	O,	0	0	0
System Identity Management Network Resources Device	al Management pxGrid Services + Feed Service + Threat Centric NAC					
Identities Groups External Identity Sources Identity Source Sec	es + Settings					
External Identity Sources Connection			4			
Certificate Authentication Profile Supervised Authentication Profile	AD ()					
Active Directory * Active Directory LDAP	in mydomain.com					
BADIUS Token			~			
RSA SecurID Submit Cancel						
Social Login						

4. 在提示中使用適當的使用者名稱和密碼加入所有節點。

CISCO Identity Services Engine Home	Context Visibility + Operat	tions + Policy -Admin	istration 🔷 Work Ce	nters		License Warning 🔺	্ 😡	0 0
System Identity Management Network	Resources Device Portal M.	anagement pxGrid Services	▶ Feed Service ▶	Threat Centric NAC				
+ Identities Groups External Identity Sources	Identity Source Sequences	 Settings 						
External Identity Sources External Identity Sources Certificate Autoritication Profile Certificate Autoritication Profile AD DoP DOP DOP	Connection Wi * Join Point Name * Active Directory Domain @ Join @ Leave @ Text L	AD mydomain.com Jser	veID Groups	Attributes Advanc	ed Settings			j
RADIUS Token	ise2 mydomain.com	STANDALONE	Constantion al	MIN-58110ETHENIP mydomai	Default First Site Name			
SAML Id Providers		0174107420742	Coperational					_
Social Login		Join Domain Please specify the credentials r * AD User Name * Passw Specify Organizational Unit Store Credentials	equired to Join ISE nod	e(d) to the Active Directory Domain.	Cancel			l

5. 按一下「Save」。

選擇目錄組

1. 建立外部管理員組並將其對映到Active Directory組。

2. 選擇管理>身份管理>外部身份源> Active Directory >組>從目錄選擇組。

3. 至少檢索管理員所屬的一個AD組。

es l	dentity Source Sequences 🕨 Settings			
	Select Directory Groups		×	
	This dialog is used to select groups from the Di	rectory.		
	Demain mydemain com	*		
	Name Filter */CC *			
	Retrieve Groups 2 Groups Pat	sid rinter * Type rinter ALL		
C	Name	Group SID	Group Type	
	wydomain com/ISE-Admin	S.1.5.21.4000324561.3650473562.621564000.1	GLOBAL	
	wydomain.com//scar//SE PO	C 1 5 21 /00022/561 2650/72562 62156/000 11	GLOBAL	
	Mydomain.com/0sels/iSE-RO	5-1-5-21-4009324001-30504/3502-021504990-11	GLOBAL	
ſ				
			OK Cancel	
			Cancer	

4. 按一下「Save」。

為管理訪問啟用Active Directory基於密碼的身份驗證

- 1. 啟用Active Directory例項作為之前加入ISE的基於密碼的身份驗證方法。
- 2. 選擇Administration > System > Admin access > Authentication,如下圖所示。

CISCO Montal Connect Children V Context Visionity V Operations V Pointy Context Visionity	
System > Identity Management > Network Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC	
Deployment Licensing + Certificates + Logging + Maintenance Upgrade + Backup & Restore - Admin Access + Settings	
Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings	
Authorization Authentication Type	
Administrators Password Based Tidentity Source AD:AD T	
• Settings	
O Client Certificate Based	
Save Reset	

3. 按一下「Save」。

附註:啟用基於證書的身份驗證需要基於密碼的身份驗證配置。成功設定基於憑證的驗證後 ,應還原此組態。

將外部身份組對映到管理員組

在本示例中,外部AD組對映到預設的Admin組。

- 1. 選擇Administration > System > Admin Access > Administrators > Admin Groups > Super admin。
- 2. 選中Type as External, 然後在External groups下選擇AD組。

disco Identity Services Engine	Home + Context Visibility + Operations + Policy <a>Administration + Work Centers	License W
▼System → Identity Management	nt Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Deployment Licensing + Certifi	ficates → Logging → Maintenance Upgrade → Backup & Restore ▼Admin Access → Settings	
Authentication + Authorization	Admin Groups > System Admin — Admin Group * Name System Admin	
▼ Administrators	Description Access permission for Operations tab. Includes System and data access permission for Admin Groups.	
Admin Users	Type 🗹 External	
Admin Groups	External Identity Source	
 Settings 	Name : AD	
	🛖 Add 👻 🗶 Delete	
	Status Email Username First Name Last Name	
	No data available	

- 3. 按一下「Save」。
- 4. 選擇Administration > System > Admin Access > Administrators > Admin Groups > Read Only Admin。
- 5. 選中Type as External,然後在External groups下選擇AD組,如下圖所示。

disco Identity Services Engine	Home + Context Vi	sibility + Operations	Policy Administration	♦ Work Cen	iters		License W
▼ System → Identity Management	Network Resources	Device Portal Managemen	nt pxGrid Services 🕨 Fe	ed Service 🕨 T	Fhreat Centric NAC		
Deployment Licensing + Certifi	cates ⊧Logging ⊧M	faintenance Upgrade ⊧	Backup & Restore - Admir	Access + Sett	lings		
Authentication	Admin Groups > Read Admin Group	Only Admin					
· / an on can on	* Name	Read Only Admin					
▼ Administrators	Description	Access Permission for admin v	with read-only functionality			11	
Admin Users	Туре	🗹 External					
Admin Groups	External Identity Sour	ce					
 Settings 	Name : AD						
	▼ External Groups	Ð					
	* mydomain.com	n/Users/ISE-RO 🛛 😔 🕂					
	Member Users Users						
	🐥 Add 👻 🗙 Delete						
	Status	Email	Username	First Name	Last Name		
					No data avai	lable	
	Save						

6. 按一下「Save」。

匯入受信任的證書

- 1. 匯入簽署客戶端證書的證書頒發機構(CA)證書。
- 2. 選擇 Administrator > System > Certificates > Trusted Certificate > Import。
- 3. 按一下「瀏覽」並選擇CA證書。
- 4. 勾選「Trust for client authentication and Syslog」覈取方塊,如下圖所示。

dially Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers	License Warning 🔺		0	
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC				
Deployment Licensing - Certif	ates → Logging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings				
Cartificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Setti Certificate Authority	Import a new Certificate into the Certificate Store				

5. 按一下Submit(提交)。

配置證書身份驗證配置檔案

- 2. 要為基於客戶端證書的身份驗證建立證書身份驗證配置檔案,請選擇Administration >身份管理 >外部身份源>證書身份驗證配置檔案>新增。
- 2. 新增配置檔名稱。
- 3. 在證書屬性中選擇包含管理員使用者名稱的相應屬性。
- 4. 如果使用者的AD記錄包含使用者的證書,並且希望將從瀏覽器收到的證書與AD中的證書進行 比較,請選中Always perform binary comparison覈取方塊,並選擇之前指定的Active Directory例項名稱。

→ System 🔻 Identity Management → Network Resources → Device Portal Management pxGrid Services → Feed Service → Threat Centric NAC	
Identities Groups External Identity Sources Identity Source Sequences Settings	
Ventile Your Edenal Identity Sources Ventiles List > New Certificate Authentication Profile List > New Certificate Authentication Profile Certificate Authentication Profile Image: Comparison of Comparison Image: Comparison of Comparison of Comparison Image: Comparison of Comparison of Comparison Image: Comparison of Comparison of Comparison	

5. 按一下Submit(提交)。

附註:相同的證書身份驗證配置檔案也可用於基於身份的終端身份驗證。

啟用基於客戶端證書的身份驗證

1. 選擇 Administration > System > Admin Access > Authentication > Authentication Method Client Certificate Based。

disco Identity Services Engine	Home + Context Visibility + Oper	ations + Policy Administration + Work Centers			
▼ System → Identity Management	Network Resources Device Portal N	danagement pxGrid Services + Feed Service + Threat Centric NAC			
Deployment Licensing + Certificates + Logging + Maintenance Enabling Client Certificate-Based Authentication will cause an application server restart on all deployment					
0		nodes. This will result in significant downtime for the system.			
Authentication	Authentication Method				
Authorization	Authentication Type	Cancel			
▼ Administrators	Reserverd Based				
Admin Users		* Identity Source AD:AD T			
Admin Groups					
Settings	 Client Certificate Based 				
	Save Reset				

- 2. 按一下「**OK**」(確定)。
- 3. 選擇之前配置的Certificate Authentication Profile。
- 4. 選擇Active Directory例項名稱。

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers
▼ System → Identity Management	Network Resources Povice Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing + Certific	ates → Logging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings
() Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	Authentication Type
▼ Administrators Admin Users	O Password Based
Admin Groups	Client Certificate Based
• Settings	Certificate Authentication Profile CAC_Login_Profile *
	Save Reset

- 5. 按一下「**Save**」。
- 6. 部署中的所有節點上的ISE服務重新啟動。

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing + Certific	cates + Logging + Maintenance The system will now restart.
9	
Authentication	Authentication Method
Authorization	Authentication Type
▼ Administrators	O Password Based
Admin Users	
Admin Groups	
▶ Settings	Client Certificate Based * Certificate Authentication Profile CAC_Login_Profile T
	* Identity Source AD:AD
	Save Reset

驗證

在應用伺服器服務狀態更改為正在運行後驗證對ISE GUI的訪問。

超級管理員用戶:驗證是否提示使用者選擇證書以登入到ISE GUI,如果證書屬於超級管理員外部 身份組的使用者部分,則授予超級管理員許可權。



← ⊕	P ← A C Ø Identity Services Engine ×	£ €
Home + Context Visibility	Operations Policy Administration Work Centers	License Warning 🔺 🔍 🐵 🔿 🌣 🍃
Summary Endpoints Guests Vulnerability	Threat +	Click here to do visibility setup Do not show this again.
METRICS Total Endpoints 0	Active Endpoints Rejected Endpoints	Anomalous Behavior Anomalous Behavior
Identity Store Identity Group Network Device Failure Reason	III NETWORK DEVICES Image: Control of the second	II ENDPOINTS • E S X
No data available.	No data available.	No data available.
	Ο	Ο
III BYOD ENDPOINTS O B C X	III ALARMS III OCCU Last Occu	I node(s)
No data available.		🗹 📄 ise2

只讀管理員用戶:驗證是否提示使用者選擇證書以登入ISE GUI,如果證書屬於只讀管理員外部身份組的使用者部分,則授予只讀管理員許可權。





附註:如果使用通用訪問卡(CAC),則智慧卡在使用者輸入其有效的超級個人識別碼後向 ISE提供使用者證書。

疑難排解

- 使用application start ise safe命令以安全模式啟動Cisco ISE,該模式允許臨時禁用對管理員門 戶的訪問控制,並使用application stop ise命令,然後使用application start ise命令更正配置並 重新啟動ISE的服務.
- 2. 如果管理員無意中阻止所有使用者訪問Cisco ISE管理員門戶,安全選項提供恢複方法。如果

管理員在Administration > Admin Access > Settings > Access頁面中配置了一個不正確的IP Access清單,則會發生此事件。safe選項還可繞過基於證書的身份驗證,並還原為預設使用者 名稱和密碼身份驗證,以便登入到思科ISE管理員門戶。