Konfigurieren der Authentifizierung für ISE-Administration auf Zertifikats- oder Smartcard-Basis

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Beitritt zur ISE zu Active Directory Verzeichnisgruppen auswählen Aktivieren der auf Active Directory-Kennwörtern basierenden Authentifizierung für den Administratorzugriff Externe Identitätsgruppen Administratorgruppen zuordnen Vertrauenswürdiges Zertifikat importieren Zertifikatauthentifizierungsprofil konfigurieren Clientzertifikatbasierte Authentifizierung aktivieren Überprüfen Fehlerbehebung

Einführung

In diesem Dokument wird beschrieben, wie die Client-Certificate-basierte Authentifizierung für den ISE-Managementzugriff (Identity Services Engine) konfiguriert wird. In diesem Beispiel authentifiziert sich der ISE-Administrator anhand des Benutzerzertifikats, um Administratorzugriff auf die Verwaltungs-GUI der Cisco Identity Services Engine (ISE) zu erhalten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, die folgenden Themen zu kennen:

- ISE-Konfiguration für Passwort und Zertifikatsauthentifizierung.
- Microsoft Active Directory (AD)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Identity Services Engine (ISE) Version 2.6
- Windows Active Directory (AD) Server 2008, Version 2
- Zertifikat

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn das Netzwerk in Betrieb ist, sollten Sie die potenziellen Auswirkungen einer Konfiguration verstehen.

Konfigurieren

In diesem Abschnitt können Sie das Client-Zertifikat oder die Smart Card als externe Identität für den Administratorzugriff auf die Cisco ISE-Verwaltungs-GUI konfigurieren.

Netzwerkdiagramm



Beitritt zur ISE zu Active Directory

- 1. Wählen Sie Administration > Identitätsmanagement > Externe Identitätsquellen > Active Directory.
- 2. Erstellen Sie eine Active Directory-Instanz mit dem Join Point-Namen und der AD-Domäne in der Cisco ISE.
- 3. Klicken Sie auf Senden.



4. Verbinden Sie alle Knoten mit dem entsprechenden **Benutzernamen** und **Kennwort** in der Eingabeaufforderung.

cisco Identity Services Engine Home	Context Visibility → Oper	ations + Policy -Admi	nistration 🔹 Work C	enters		License Warning 🔺	O,	0 c	ø	
System +Identify Management Helwork Resources Horize Portal Management px0/i/d Service + Threat Centric NAC										
+ Identities Groups External Identity Sources	Identity Source Sequences	▶ Settings								
	-									
External Identity Sources	Connection	Whitelisted Domains Pas	siveID Groups	Attributes Advance	ced Settings					
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	* Join Point Name	AD		Ø					Ê	
Active Directory AD	* Active Directory Domain	mydomain.com		Ð						
DDBC	on on Leave 🤦 Test	: User 🛛 👌 Diagnostic Tool 🔗 R	efresh Table							
ADIUS Token	ISE Node	 ISE Node Role 	Status	Domain Controller	Site					
ERSA SecurID	ise2.mydomain.com	STANDALONE	🖸 Operational	WIN-58UQFTHFNIP.mydomai	Default-First-Site-Name					
SAML Id Providers					_					
Social Login		Join Domain		dada da da data Disada a Demaia	×					
		Please specify the credentials	required to Join ISE no	de(s) to the Active Directory Domain	·					
		* AD User Name	e @							
		* Passi	vord							
		Specify Organizational Unit	a a							
		Store Credentials	e @							
				OK	Cancel					

5. Klicken Sie auf Speichern.

Verzeichnisgruppen auswählen

- 1. Erstellen Sie eine externe Administratorgruppe, und ordnen Sie diese der aktiven Verzeichnisgruppe zu.
- 2. Wählen Sie Administration >Identitätsmanagement > Externe Identitätsquellen > Active Directory > Gruppen > Wählen Sie Gruppen aus dem Verzeichnis aus.
- 3. Rufen Sie mindestens eine AD-Gruppe ab, der der Administrator angehört.

es	Identity Source Sequences + Settings		
	Select Directory Groups		×
	This dialog is used to select groups from the Direct	tory.	
	Domain mydomain.com	*	
	Name Filter *ISE-*	D Filter * Type Filter ALL	·
	Retrieve Groups 2 Groups Retriev	ed.	
	V Name	Group SID	Group Type
	mydomain.com/ISE-Admin	S-1-5-21-4009324561-3650473562-621564990-1	GLOBAL
	mydomain.com/Users/ISE-RO	S-1-5-21-4009324561-3650473562-621564990-11	GLOBAL
	1		
			OK Capcel

4. Klicken Sie auf Speichern.

Aktivieren der auf Active Directory-Kennwörtern basierenden Authentifizierung für den Administratorzugriff

- 1. Aktivieren Sie die Active Directory-Instanz als kennwortbasierte Authentifizierungsmethode, die der ISE bereits zuvor beigetreten ist.
- 2. Wählen Sie Administration > System > Admin access > Authentication (Verwaltung > System > Administratorzugriff > Authentifizierung) aus, wie im Bild gezeigt.

disco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
▼ System → Identity Management	Network Resources Povice Portal Management pxGrid Services Peed Service Threat Centric NAC
Deployment Licensing + Certific	cates → Logging → Maintenance Upgrade → Backup & Restore →Admin Access → Settings
Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	Authentication Type
 Administrators 	Password Based
• Settings	* Identity Source AD:AD
	O Client Certificate Based
	Save Reset

3. Klicken Sie auf Speichern.

Hinweis: Zur Aktivierung der zertifikatbasierten Authentifizierung ist eine kennwortbasierte Authentifizierungskonfiguration erforderlich. Diese Konfiguration sollte nach erfolgreicher Konfiguration der zertifikatbasierten Authentifizierung zurückgesetzt werden.

Externe Identitätsgruppen Administratorgruppen zuordnen

In diesem Beispiel wird die externe AD-Gruppe der standardmäßigen Admin-Gruppe zugeordnet.

- 1. Wählen Sie Administration > System >Admin Access >Administrator >Admin Groups > Super Admin.
- 2. Aktivieren Sie Typ als Extern und wählen Sie unter Externe Gruppen die AD-Gruppe aus.

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy	License W
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC	
Deployment Licensing + Certifi	cates → Logging → Maintenance Upgrade → Backup & Restore <mark>→</mark> Admin Access → Settings	
Authentication Authorization	Admin Groups > System Admin Admin Group	
▼ Administrators	Description Access permission for Operations tab. Includes System and data access permission for Admin Groups.	
Admin Users	Type V External	
Admin Groups	External Identity Source	
Settings	Name : AD	
	* Imydomain.com/ISE-Admin O + Member Users	
	Status Email Username First Name Last Name	
	Ro data avaliabie	

- 3. Klicken Sie auf Speichern.
- 4. Wählen Sie Administration > System > Admin Access > Administrator Groups > Read Only Admin (Nur Lesezugriff) aus.
- 5. Aktivieren Sie Type as **External** und wählen Sie unter **External groups** die AD-Gruppe aus, wie im Bild gezeigt.

-4(++1)- cisco Identity Services Engine Home →	Context Visibility + Operations + Policy - Administration + Work Centers License W
▼System → Identity Management → Network F	Resources
Deployment Licensing + Certificates + Log	ging → Maintenance Upgrade → Backup & Restore <mark>▼</mark> Admin Access → Settings
Authentication Admin Grou Authorization Admin Grou	րբ » Read Only Admin ՏԱՌ * Name – Read Only Admin
▼ Administrators D	escription Access Permission for admin with read-only functionality
Admin Users	Type 🗸 External
Admin Groups External Id	entity Source
Settings Name : AD	
▼ Extern	al Groups 🕧
× my	domain.com/Users/ISE-RO 🛛 😳 🕂
Member I Users	Jsers
🕂 Add 👻	X Delete
Status	Email Username First Name Last Name
	No data available
Save	leset

6. Klicken Sie auf Speichern.

Vertrauenswürdiges Zertifikat importieren

- 1. Importieren Sie das Zertifikat der Zertifizierungsstelle (Certificate Authority, CA), das das Clientzertifikat signiert.
- 2. Auswählen Administrator > System > Certificates > Trusted Certificate > Import.
- 3. Klicken Sie auf Durchsuchen, und wählen Sie das Zertifizierungsstellenzertifikat aus.
- 4. Aktivieren Sie das Kontrollkästchen Vertrauenswürdig für Client-Authentifizierung und Syslog, wie im Bild gezeigt.

dentity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers	License Warning	<u>ه</u>	θ	• •
▼ System	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC				
Deployment Licensing • Certif	sates → Logging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings				
Certificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests	Import a new Certificate into the Certificate Store * Certificate File Choose File DCcomDCmymainW.pem Friendly Name Trusted For: ① Trusted For: ① Trust for authentication within ISE				
Certificate Authority	Trust for client authentication and Syslog Trust for authentication of Cisco Services Validate Certificate Extensions				
	Description Cancel				

5. Klicken Sie auf Senden.

Zertifikatauthentifizierungsprofil konfigurieren

1. Um ein Zertifikatauthentifizierungsprofil für die zertifikatbasierte Authentifizierung des Clients

zu erstellen, wählen Sie Administration >Identitätsmanagement > Externe Identitätsquellen > Zertifikatauthentifizierungsprofil > Hinzufügen.

- 2. Profilname hinzufügen
- 3. Wählen Sie das entsprechende Attribut aus, das den Administratorbenutzernamen im Zertifikatattribut enthält.
- 4. Wenn der AD-Datensatz für den Benutzer das Benutzerzertifikat enthält und das vom Browser erhaltene Zertifikat mit dem Zertifikat in AD vergleichen möchte, aktivieren Sie das Kontrollkästchen Immer Binärvergleich durchführen und wählen den zuvor angegebenen Active Directory-Instanznamen aus.

cisco	lder	tity Ser	vices I	Engine	Home	➤ Context Vis	sibility	 Operations 	Policy	▼Adminis	stration	♦ Work	Centers
♦ S3	stem	▼lde	ntity M	anagement	▶ Netwo	rk Resources	▶ Device	e Portal Manag	ement p×G	rid Services	▶ Feed	Service	Threat Centric NAC
⊮ Id	entitie	5 Gro	ups	External Ide	ntity Sourc	es Identity :	Source Se	quences 🕨 S	Settings				
	kterna + 1 C A A B C A A C A A S S S S	I Ident s Gro entificat. AD DAP DBC ADIUS : SA Sect AML Id I cocial Log	ity Sou a Auther rectory Token IrID Provider	External Ide	le Sev	es Identity : Certificat Certifica Certifica Submit	Us bh Client C ifficate In I	quences > S cation Profiles entication Pr * Name Description Identity Store te Identity From ertificate Again dentity Store	AD AD AD AD Any Su Any Su Any Su Any Su Any Su Any Su Any Su Any Su Any Su	rtificate Aut	Subject native Nationary comp	Alternativ me Attribu	e // // // // // // // // // // // // //
						Submit	Cancel		○ Only ④ Alway	to resolve ide	entity amb	iguity arison	

5. Klicken Sie auf Senden.

Hinweis: Das gleiche Zertifikatauthentifizierungsprofil kann auch für die identitätsbasierte Endpunkt-Authentifizierung verwendet werden.

Clientzertifikatbasierte Authentifizierung aktivieren

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

cisco Identity Services Engine		ations				
▼ System → Identity Management	Network Resources Device Portal 1	Management pxGrid Services + Feed Service + Threat Centric NAC				
Deployment Licensing + Certificates + Logging + Maintenance						
0		nodes. This will result in significant downtime for the system.				
Authentication	Authentication Method					
Authorization	Authentication Type	Cancel				
▼ Administrators	O Password Based					
Admin Users		* Identity Source AD:AD *				
Admin Groups						
Settings	Client Certificate Based					
	Save Reset					

- 2. Klicken Sie auf OK.
- 3. Wählen Sie das zuvor konfigurierte Zertifikatauthentifizierungsprofil aus.
- 4. Wählen Sie den Instanznamen der Active Directory-Instanz aus.

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy Administration + Work Centers
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
Deployment Licensing + Certific	cates → Logging → Maintenance Upgrade → Backup & Restore <mark>→</mark> Admin Access → Settings
3 Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	Authentication Type
 Administrators 	O Password Based
Admin Users	
Admin Groups	Client Certificate Based * Certificate Authentication Profile CAC Login Profile *
	* Identity Source AD:AD
	Save Reset

- 5. Klicken Sie auf Speichern.
- 6. ISE-Services auf allen Knoten, die bei der Bereitstellung neu gestartet werden.

cisco Identity Services Engine	Home → Context Visibility → Ope	erations Policy Administration	▶ Work Centers	
▼ System → Identity Management	Network Resources Device Portal	Management pxGrid Services + Feed :	Service	
Deployment Licensing + Certifi	cates → Logging → Maintenance 🔒	The system will now restart.		
0				
Authentication	Authentication Method			
Authorization	Authentication Type		ок	
★ Administrators	O Password Based			
Admin Users				
Admin Groups				
Settings	Client Certificate Based	* Certificate	e Authentioation Profile CAC_Login_Profile *	
			* Identity Source AD:AD *	
	Save Reset			

Überprüfen

Überprüfen Sie den Zugriff auf die ISE-GUI, nachdem sich der Dienststatus des Anwendungsservers in Ausführung geändert hat.

Super Admin User (Super-Admin-Benutzer): Stellen Sie sicher, dass der Benutzer aufgefordert wird, ein Zertifikat für die Anmeldung bei der ISE-GUI auszuwählen, und dass er Super Admin-Berechtigungen erhält, wenn das Zertifikat ein Benutzer der Super Admin External Identity-Gruppe ist.



Schreibgeschützter Admin-Benutzer: Vergewissern Sie sich, dass der Benutzer aufgefordert wird, ein Zertifikat für die Anmeldung bei der ISE-GUI auszuwählen, und dass ihm Schreibschutzberechtigungen gewährt werden, wenn das Zertifikat einem Benutzer angehört, der zur Gruppe "Schreibgeschützt" der externen Administrator-Identität gehört.

() () (https://ise2.mydomain.com/	× - ۵	○ Waiting for ise2.mydomain ×	
ſ			
	Windows Security	×	
	Confirm Certificate		
	Confirm this certificate by clicking OK click Cancel.	. If this is not the correct certificate,	
	Vinodh		
	Issuer: mydomain-WI Valid From: 10/16/201	N-58UQFTHF 9 to 10/15/2020	
	Click here to view cer	tificate prope	
		OK Cancel	

< li>https://ise2.mydomain.com/admin/	🔎 👻 🖴 🖒 🏉 Identity Services Engine 🛛 🛛	☆ 🕸
Home Context Visibility	Operations Policy Administration Work Centers	🚔 Read-Only License Warning 🔺 🔍 🐵 🌣 🖕
Summary Endpoints Guests Vulnerability	Threat 🕂	¢ -
METRICS		- Ø
	Active Endpoints Rejected Endpoints	
Identity Store Identity Group Network Device Failure Reason	III NETWORK DEVICES C C X Device Name Type Location	II ENDPOINTS IV Profile
No data available.	No data available.	No data available.
III BYOD ENDPOINTS O D X	II ALARMS C C X Severity Name Occu Last Occi	II SYSTEM SUMMARY AII - 24HR -
No data available.		M II 1967

Hinweis: Wenn eine Common Access Card (CAC) verwendet wird, legt Smartcard das Benutzerzertifikat der ISE vor, nachdem der Benutzer seinen gültigen Super-Pin eingegeben hat.

Fehlerbehebung

- Verwenden Sie den Befehl application start ise safe, um die Cisco ISE im abgesicherten Modus zu starten, der es ermöglicht, die Zugriffskontrolle für das Admin-Portal vorübergehend zu deaktivieren und die Konfiguration zu korrigieren und die Dienste der ISE mit dem Befehl application stop ise gefolgt von application start ise neu zu starten..
- 2. Die Option "safe" bietet eine Möglichkeit zur Wiederherstellung, wenn ein Administrator versehentlich den Zugriff auf das Cisco ISE-Admin-Portal für alle Benutzer sperrt. Dieses Ereignis kann auftreten, wenn der Administrator auf der Seite Administration > Admin Access > Settings > Access (Administration > Administratorzugriff > Einstellungen > Zugriff) eine falsche IP-Zugriffsliste konfiguriert hat. Die Option "safe" umgeht außerdem die zertifikatsbasierte Authentifizierung und kehrt zur Standard-Benutzernamen- und Kennwortauthentifizierung für die Anmeldung beim Cisco ISE Admin-Portal zurück.