Esempio di configurazione dell'accesso al portale di amministrazione ISE con credenziali AD

Sommario

Introduzione Prerequisiti Componenti usati Configurazione Partecipa ad ISE e AD Seleziona gruppi di directory Abilita accesso amministrativo per AD Configurare il mapping tra il gruppo di amministratori e il gruppo AD Impostare le autorizzazioni RBAC per il gruppo Admin Accesso ad ISE con credenziali AD Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento descrive un esempio di configurazione per l'utilizzo di Microsoft Active Directory (AD) come archivio identità esterno per l'accesso amministrativo all'interfaccia utente di gestione di Cisco Identity Services Engine (ISE).

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco ISE versione 1.1.x o successive
- Microsoft AD

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Cisco ISE versione 1.1.x

• Windows Server 2008 release 2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Utilizzare questa sezione per configurare l'uso di Microsoft AD come archivio identità esterno per l'accesso amministrativo all'interfaccia utente grafica di gestione di Cisco ISE.

Partecipa ad ISE e AD

- 1. Passare a Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory.
- 2. Immettere il nome del dominio Active Directory e il nome dell'archivio identità e fare clic su **Partecipa**.
- 3. Immettere le credenziali dell'account AD che possono aggiungere e modificare gli oggetti computer e fare clic su **Salva configurazione**.

💧 Home Operations 🔻 Policy	nent 📰 I	Nstration 🔹 💽 ee Task Navigator Network Resources 🚯 Web Portal Management
Identities Groups External Iden	tity Sources	Identity Source Sequences Settings
External Identity Sources	@.	Adve Directory > AD1 Connection Advanced Settings Groups Attributes
Certificate Authentication Profile		* Domain Name Domian.local
- Kane brockry		Identity Store Name AD1
LDAP		One of more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Solicit one and is the Test Comparison.
Carlor Contraction RADOUS Token	۲	
a RSA SecurID	۲	😳 Ion 😳 Leave 😳 Test Connection *
		ISE Node ISE Node Role Status
		ISE-JKATYAL STANDALONE Connected to windomain.local

Seleziona gruppi di directory

- 1. Passare a Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory > Gruppi > Aggiungi > Seleziona gruppi dalla directory.
- 2. Importare almeno un gruppo AD a cui appartiene l'amministratore.

💧 Home Operations 🔻 Policy 🔻 Adminis	n T	👓 Task Navigator 👻 🚷				
🔆 System 🛛 🙀 Identity Management 🖉 N	etwork Resources 🛛 🙀 Yeb Portal Management					
Identities Croups External Identity Sources Identity Source Sequences Settings						
External Identity Sources	Adve Directory > AD1 Connection Advanced Settings Groups Attributes					
Active Directory		_				
EDAP ®	Domain. local /Users/Domain Admins					
RADOUG Token (2) RSA SecurID (2)						

Abilita accesso amministrativo per AD

Completare questa procedura per abilitare l'autenticazione basata su password per AD:

- 1. Selezionare Amministrazione > Sistema > Accesso amministratore > Autenticazione.
- 2. Nella scheda Metodo di autenticazione selezionare l'opzione Basato su password.
- 3. Selezionare AD dal menu a discesa Origine identità.
- 4. Fare clic su Salva modifiche.

🛕 Home Operations 🔻 Policy 💌 Admin	stration 🔻	👓 Task Navigator 👻 🕙
🔆 System 🛛 🖉 Identity Management 🛛 🖷	Network Resources 🛛 😹 Web Portal Management	
Deployment Licensing Certificates Loggi	g Nantenance Admin Access Settings	
Admin Access	Authentication Method Password Policy Authentication Type: Authentication Type: • Password Based * Identity Source • Authenticate Based • Offent Certificate Based	

Configurare il mapping tra il gruppo di amministratori e il gruppo AD

Definire un Cisco ISE Admin Group e mapparlo a un gruppo AD. In questo modo viene concessa l'autorizzazione per determinare le autorizzazioni RBAC (Role Based Access Control) per l'amministratore in base all'appartenenza ai gruppi in Active Directory.

- 1. Passare a Amministrazione > Sistema > Accesso amministratore > Amministratori > Gruppi amministratori.
- 2. Fare clic su **Add** nell'intestazione della tabella per visualizzare il nuovo riquadro di configurazione del gruppo di amministratori.
- 3. Immettere il nome del nuovo gruppo Amministratore.
- 4. Nel campo Tipo selezionare la casella di controllo Esterno.
- 5. Dal menu a discesa **Gruppi esterni**, selezionare il gruppo AD a cui si desidera mappare questo gruppo amministrativo, come definito nella sezione Seleziona gruppi di directory.
- 6. Fare clic su Salva modifiche.

💧 Home Operations 🔻 Policy 💌 Admir	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	
 Administrators Identistrators Admin Users Se Admin Groups 	External Identity Source Name AD1	
Relptusk Admin Statitity Admin Statistics Administration_AD1	Esternal Groups Domain.local/Users/Domain Adn +	
器 Mini Admin 器 Network Device Admin 象 Policy Admin	Save Reset	
💫 REAC Admin 🤐 Super Admin 🧏 System Admin		
🕨 🧰 Settings	*	

Impostare le autorizzazioni RBAC per il gruppo Admin

Completare questi passaggi per assegnare le autorizzazioni RBAC ai gruppi amministrativi creati nella sezione precedente:

- 1. Selezionare Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Criteri.
- 2. Dal menu a discesa **Azioni** a destra, selezionare **Inserisci nuovo criterio sotto** per aggiungere un nuovo criterio.
- 3. Creare una nuova regola denominata **ISE_administration_AD**, mapparla al gruppo Admin definito nella sezione Abilitare l'accesso amministrativo per AD e assegnarle le autorizzazioni.**Nota:** In questo esempio viene assegnato il gruppo Admin denominato **Super Admin**, equivalente all'account admin standard.
- 4. Fare clic su **Save Changes** (Salva modifiche). Nell'angolo inferiore destro dell'interfaccia grafica viene visualizzata la conferma delle modifiche salvate.

🛕 Home Operations 🔹 Policy	- Admi	istration 🔻	🗝 Task Navigator 👻 🛃
🔆 System 🛛 👰 Identity Manageme	nt 📕	Network Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificate	Logg	ing Maintenance Admin Access Settings	
Admin Access	۹ چ	Create Role Dased Access Control policies by configuring rules based on Admin groups, Menu Access permissions (neru items), Data Access ciencers(s) and other conditions. Note that multiple Menu/Data Access permissions are not allowed on a single policy. You can copy the defined modify them as meeded. Note that mystem-created and default policies cannot be updated, and default policies cannot be deleted. For der will be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy. Permit overrides Deny. (Th aphilautical order of the policy name).	s permissions (identity group data uit policies shown below, then ison making, all applicable policies e policies are displayed in
Authentication		REAC Policies Rule Name Admin Groups Permissions	
Permission Permission Permission		Image: State	叠 Actions *
 Administrators Administrators Administrators Administrators Administrators 			🖗 Actions *
器 Helpdesk Admin 象 Identity Admin 象 ISE Administration_AD1		Image: Second station_AD If ISE Administration_AD1 then Super Admin Menu Access	🖗 Actions *

Accesso ad ISE con credenziali AD

Per accedere ad ISE con le credenziali di AD, completare la procedura seguente:

- 1. Uscire dalla GUI amministrativa.
- 2. Selezionare AD1 dal menu a discesa Origine identità.
- 3. Immettere il nome utente e la password del database di Active Directory ed eseguire l'accesso.



Nota: Per impostazione predefinita, ISE utilizza l'archivio utenti interno nel caso in cui AD non sia raggiungibile o le credenziali dell'account utilizzate non esistano in AD. Ciò semplifica l'accesso rapido se si utilizza l'archivio interno mentre AD è configurato per l'accesso amministrativo.

Verifica

Per verificare che la configurazione funzioni correttamente, verificare il nome utente autenticato nell'angolo in alto a destra della GUI di ISE.



Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- <u>Guida dell'utente di Cisco Identity Services Engine, versione 1.1 Gestione delle identità e</u> <u>dell'accesso degli amministratori</u>
- Documentazione e supporto tecnico Cisco Systems