# Integrazione di AD per l'interfaccia grafica ISE e accesso tramite CLI

# Sommario

Introduzione **Prerequisiti** Componenti usati **Configurazione** Iscriviti ad ISE 2008 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 GUI ISE con credenziali AD Accesso CLI ISE con credenziali AD **ISE CLI** Verifica Risoluzione dei problemi Problemi di join Problemi di accesso

# Introduzione

Questo documento descrive la configurazione di Microsoft AD come archivio identità esterno per l'accesso amministrativo alla GUI e alla CLI di Cisco ISE Management.

# Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco ISE versione 3.0
- Microsoft AD

## Componenti usati

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

- Cisco ISE versione 3.0
- Windows Server 2016

Questo documento descrive la configurazione di Microsoft Active Directory (AD) come archivio identità esterno per l'accesso amministrativo a Cisco Identity Services Engine (ISE) GUI e CLI di gestione.

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.

Queste porte vengono usate tra il nodo ISE e AD per questa comunicazione:

Service	Port	Protocol	Notes
DNS	53	UDP and TCP	
LDAP	389	UDP and TCP	
Kerberos	88	UDP and TCP	
Kerberos	464	UDP and TCP	Used by kadmin for setting and changing a password
LDAP Global Catalog	3268	TCP	If the id_provider = ad option is being used
NTP	123	UDP	Optional

Nota: verificare che l'account AD disponga di tutti i privilegi necessari.

#### Active Directory Account Permissions Required for Performing Various Operations

Join Operations	Leave Operations	Cisco ISE Machine Accounts
For the account that is used to perform the join operation, the following permissions are required:	For the account that is used to perform the leave operation, the following permissions are required:	For the newly created Cisco ISE machine account that is used to communicate to the Active Directory connection, the following permissions are required:
<ul> <li>Search Active Directory (to see if a Cisco ISE machine account already exists)</li> <li>Create Cisco ISE machine account to domain (if the machine account does not already exist)</li> <li>Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname)</li> <li>It is not mandatory to be a domain administrator to perform a join operation.</li> </ul>	<ul> <li>Search Active Directory (to see if a Cisco ISE machine account already exists)</li> <li>Remove Cisco ISE machine account from domain</li> <li>If you perform a force leave (leave without the password), it will not remove the machine account from the domain.</li> </ul>	<ul> <li>Ability to change own password</li> <li>Read the user/machine objects corresponding to users/machines being authenticated</li> <li>Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.)</li> <li>Ability to read tokenGroups attribute</li> <li>You can precreate the machine account in Active Directory, and if the SAM name matches the Cisco ISE appliance hostname, it should be located during the join operation and re-used.</li> <li>If multiple join operations are performed, multiple machine accounts are maintained inside Cisco ISE, one</li> </ul>

## Iscriviti ad ISE 2008

- 1. Passa a Administration > Identity Management > External Identity Sources > Active Directory .
- 2. Immettere il nuovo nome del punto di join e il dominio Active Directory.
- 3. Immettere le credenziali dell'account AD che consente di aggiungere e modificare gli oggetti computer e fare clic su **OK**.

Cisco ISE	Administration • Identity Management	A Evaluation Mode 8
ntities Groups I	External Identity Source Sequences Settings	×
xternal Identity Sources	Join Domain	vanced Set
<ul> <li>Certificate Auther</li> <li>Active Directory</li> <li>Isha.AD</li> </ul>	Please specify the credentials required to Join ISE node(s) to the Active Directory Dor nticati  AD User Name  Administrator Password	main.
DDBC	Specify Organizational Unit  Store Credentials	ontroller
RADIUS Token     RSA SecuriD     SAMI, Id Dravideor	Cancel	ок

# Join Operation Status

Status Summary: Successful

ISE Node	^	Node Status	
ise30-1.Isha.global		Completed.	
			Close

#### Seleziona gruppi di directory

- 1. Passa a Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory .
- 2. Importare almeno un gruppo AD a cui appartiene l'amministratore.



#### Abilita accesso amministrativo per AD

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

- 1. Passa a Administration > System > Admin Access > Authentication .
- 2. Dal Authentication Method , Scegliere la scheda Password Based Opzione.
- 3. Scegliere AD dal menu Identity Source elenco a discesa.
- 4. Clic Save Changes .

×

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health (	Checks
Authentication		Authenticatio	n Method	Password Policy	Account Disat	ole Policy	Lock/Susp
Authorization	>	Authentica	tion Type				
Administrators	>						
Settings	>	Password	Based				
		* Identity Sour	rce				
		AD:Isha.AD	Þ	~			
		O Client Cer	tificate Based				

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

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

- 1. Passa a Administration > System > Admin Access > Administrators > Admin Groups .
- 2. Clic Add nell'intestazione della tabella per visualizzare il nuovo Admin Group riquadro di configurazione.
- 3. Immettere il nome del nuovo gruppo Amministratore.
- 4. Nella scheda Type, selezionare il External.
- 5. Dal External Groups dall'elenco a discesa, scegliere il gruppo AD a cui si desidera mappare questo gruppo di amministratori, come definito Select Directory Groups sezione.
- 6. Clic Save Changes .

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access
Authentication		Admin Groups >	New Admin Grou	up				
Authorization	>	Admin Grou	p					
Administrators Admin Users	~	* Name	ISE_Admi	n				
Admin Groups		Description	External	1			li.	
Settings	>	External Identity Name : Isha.AD	Source					
		✓ External	Groups na.global/Users	s/Domain User: 🗸	+			

## Impostare le autorizzazioni RBAC per il gruppo Admin

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

- 1. Passa a Administration > System > Admin Access > Authorization > Policy .
- 2. Dal Actions a destra, scegliere Insert New Policy per aggiungere un nuovo criterio.
- Creare una nuova regola denominata AD\_Administrator, eseguirne il mapping con il gruppo Admin definito nel Enable Administrative Access per la sezione AD e assegnarle le autorizzazioni. Nota: in questo esempio viene assegnato il gruppo amministrativo denominato Super Admin, che equivale all'account amministratore standard.
- 4. Clic Save Changes . La conferma delle modifiche salvate viene visualizzata nell'angolo inferiore destro dell'interfaccia utente.

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks		Backup & Restore	Admir	Access	Se
Authentication		🗹 🗸 ER	S Trustsec Policy	If ERS	Trustsec	+	then	Super Admin Data Access	+	Actions	~
Authorization	~	✓ He	Ipdesk Admin Policy	If Help	desk Admin	+	then	Helpdesk Admin Menu Acces	s +	Actions	~
Permissions		🗹 🗸 Ide	entity Admin Policy	If Ident	ity Admin	+	then	Identity Admin Menu Access.	+	Actions	$\sim$
Menu Access	Ť	🗹 🗸 Mr	nT Admin Policy	If MnT	Admin	+	then	MnT Admin Menu Access	+	Actions	~
Data Access		AD	D_Administrator	If ISE_/	Admin	+	then	Helpdesk Admin Menu Acce.	. ×	Actions	~
RBAC Policy		🗹 🗸 Ne	rtwork Device Policy	If Netw	ork Device Admir	+	then	Super Admin Menu A	ccess	$\sim$	+
		🗹 🗸 Po	licy Admin Policy	If Polic	y Admin	+	then				
Administrators	>	🗹 🗸 RB	AC Admin Policy	If RBAG	C Admin	+	then	Super Admin Data Ac	Cess	~	٥

## Accesso GUI ISE con credenziali AD

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

- 1. Uscire dalla GUI amministrativa.
- 2. Scegliere AD dal menu Identity Source elenco a discesa.
- 3. Immettere il nome utente e la password dal 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.

	cisco		T
	Identity Service	es Engine	- 10.
	Intuitive network s	ecurity	
1 1 -	Username ad_admin		1
	Password		
	Identity Source		-
	Isha.AD	~	
	Internal		
	Isha.AD		

 $\times$ 

οк

# Server Information

ad_admin
ise30-1
Administration, Monitoring, Policy
Service (SESSION, PROFILER)
STANDALONE
May 08 2021 10:13:22 PM
Asia/Kolkata
Disabled
3.0.0.458
none

Accesso CLI ISE con credenziali AD

L'autenticazione con un'origine identità esterna è più sicura rispetto a quella con il database interno. RBAC per CLI Administrators supporta un archivio identità esterno.

**Nota**: ISE versione 2.6 e successive supportano l'autenticazione degli amministratori CLI da origini identità esterne, ad esempio AD.

Gestione di un'unica origine per le password senza la necessità di gestire più policy sulle password e di amministrare gli utenti interni all'interno di ISE, con una conseguente riduzione di tempi e sforzi.

#### Prerequisiti

Ènecessario aver definito l'utente Admin e averlo aggiunto a un gruppo Administrator. L'amministratore deve essere un **super Admin**.

#### Define the User's Attributes in the AD User Directory

Sul server Windows in esecuzione Active Directory modificare gli attributi per ogni utente che si intende configurare come amministratore CLI.

- 1. Aprire il Server Manager Window e passare a Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ ad.adserver ]
- 2. Abilita Advanced Features nel menu Visualizza, in modo da poter modificare gli attributi di un utente.

Active Directory Users and Comp	puters		-	٥	×
🗢 🔿 👔 Add/Remove	Columns				
Active Direc Saved Q Saved Q Saved Q Small Icons Small Icons List Detail Dor Users, Contac Corr C	tts, Groups, and Computers as containers atures Domain Ad Security Group Domain Co Security Group Domain Gue Security Group Domain Gue Security Group Domain Users Security Group Enterprise A Security Group Enterprise K Security Group Enterprise R Security Group Group Polic Security Group Group Polic Security Group Security Group Group Polic Security Group Rest User Protected Us Security Group RAS and IAS Security Group Read-only D Security Group Schema Ad Security Group	count for ad n this group c of this group t out manage n this group c nistrators Gro s who are per Designated administrato All domain controllers i All domain guests All domain users Designated administrato Members of this group Members of this group Members of this group Built-in account for gue Members of this group Servers in this group Servers in this group Members of this group Designated administrato			

- 3. Passare al gruppo AD che contiene l'utente Amministratore e individuare tale utente.
- 4. Fare doppio clic sull'utente per aprire Properties e scegliere il pulsante Attribute Editor .
- 5. Fare clic su un attributo e immettere: gid per individuare l'attributo gidNumber. Se non si trova la gidNumber, fare clic sull'attributo Filter e deselezionare. Mostra solo gli attributi con valori.
- 6. Fare doppio clic sul nome dell'attributo per modificarlo. Per ogni utente: Assegna uidNumber maggiore di 60000 e assicurarsi che il numero sia univoco.Assegna gidNumber come 110 o 111.GidNumber 110 indica un utente amministratore, mentre 111 indica un utente di sola lettura.Non modificare uidNumber dopo l'assegnazione.Se si modifica il gidNumber, attendere almeno cinque minuti prima di stabilire una connessione SSH.

Published Certificates N	Member Of	Passwon	d Replicatio	n Dial-in	Object
Security Envir	onment	Sess	ions	Remote co	ontrol
General Address	Account	Profile	Telephor	nes Orga	nization
Remote Desktop Servi	ces Profile	0	OM+	Attribute I	Editor
Attributes:					
Attribute	Value				^
garbageCollPeriod	<not set=""></not>				
gecos	<not set=""></not>				
generationQualifier	<not set=""></not>				
gidNumber	110				
givenName	ad_admin				
group Membership SAM	<not set=""></not>				
groupPriority	<not set=""></not>				
groupsTolgnore	<not set=""></not>				
homeDirectory	<not set=""></not>				
homeDrive	<not set=""></not>				
homePhone	<not set=""></not>				
homePostalAddress	<not set=""></not>				
houseIdentifier	<not set=""></not>				
into 🧹	<not set=""></not>			>	
Edit				Filter	

Security       Environment       Sessions       Remote control         General       Address       Account       Profile       Telephones       Organization         Remote Desktop Services Profile       COM+       Attribute Editor         Attributes:       Attribute       Value       Image: Common Services       Image: Common Services         Attribute       Value       Image: Common Services       Image: Common Services       Image: Common Services       Image: Common Services         Attributes:       Image: Common Services         Image: Common Services <td< th=""><th>Published Certificates</th><th>Member Of</th><th>Passwor</th><th>d Replicat</th><th>tion</th><th>Dial-in</th><th>Object</th></td<>	Published Certificates	Member Of	Passwor	d Replicat	tion	Dial-in	Object
General       Address       Account       Profile       Telephones       Organization         Remote Desktop Services Profile       COM+       Attribute Editor         Attributes:       Attribute       Value       Image: Comparization         Attribute       Value       Value       Image: Comparization         uid       cnot set>       Image: Comparization       Image: Comparization         uid       cnot set>       Image: Comparization       Image: Comparization         uid       cnot set>       Image: Comparization       Image: Comparization         unix Home Directory       cnot set>       Image: Comparization       Image: Comparization         unix UserPassword       cnot set>       Image: Comparization       Image: Comparization         userAccountControl       0x200 = (NORMAL_ACCOUNT)       Image: Comparization       Image: Comparization         userCentificate       cnot set>       Image: Comparization       Image: Comparization       Image: Comparization         userParameters       cnot set>       Image: Comparization       Image: Comparization       Image: Comparization       Image: Comparization         userPrincipalName       ad_admin@lsha.global       Image: Comparization       Image: Comparization       Image: Comparization       Image: Comparization <t< td=""><td>Security En</td><td>vironment</td><td>Sess</td><td>ions</td><td>Re</td><td>emote co</td><td>ontrol</td></t<>	Security En	vironment	Sess	ions	Re	emote co	ontrol
Remote Desktop Services Profile       COM+       Attribute Editor         Attributes:       Attribute       Value <ul> <li>and set&gt;</li> <li>uid Number</li> <li>G0001</li> <li>unicodePwd</li> <li>and set&gt;</li> <li>unixHomeDirectory</li> <li>and set&gt;</li> <li>unixUserPassword</li> <li>and set&gt;</li> <li>unixUserPassword</li> <li>and set&gt;</li> <li>userAccountControl</li> <li>0x200 = (NORMAL_ACCOUNT)</li> <li>userCertificate</li> <li>and set&gt;</li> <li>userParameters</li> <li>and set&gt;</li> <li>userParameters</li> <li>and set&gt;</li> <li>userPrincipalName</li> <li>ad_admin@lsha.global</li> <li>userSharedFolder</li> <li>and set&gt;</li> </ul>	General Address	Account	Profile	Teleph	ones	Orga	nization
Attribute       Value         uid <not set="">         uidNumber       60001         unicodePwd       <not set="">         unixHomeDirectory       <not set="">         unixUserPassword       <not set="">         unixUserPassword       <not set="">         userAccountControl       0x200 = (NORMAL_ACCOUNT)         userCert       <not set="">         userParameters       <not set="">         userPassword       <not set="">         userParameters       <not set="">         userPassword       <not set="">         userParameters       <not set="">         userParameters       <not set="">         userPrincipalName       ad_admin@lsha.global         userSharedFolder       <not set=""></not></not></not></not></not></not></not></not></not></not></not></not></not>	Remote Desktop Se	rvices Profile	0	OM+	A	ttribute E	ditor
Attribute       Value       *         uid <not set="">       60001         unicodePwd       <not set="">       unixHomeDirectory       <not set="">         unixUserPassword       <not set="">       unixUserPassword       <not set="">         url       <not set="">       unot set&gt;       unixUserPassword       <not set="">         userAccountControl       0x200 = (NORMAL_ACCOUNT)       userCentificate       <not set="">         userCertificate       <not set="">       userParameters       <not set="">         userPassword       <not set="">       userParameters       <not set="">         userPKCS12       <not set="">       userPhincipalName       ad_admin@lsha.global         userSharedFolder       <not set=""></not></not></not></not></not></not></not></not></not></not></not></not></not></not>	Attributes:						
uid <not set="">         uidNumber       60001         unicodePwd       <not set="">         unixHomeDirectory       <not set="">         unixUserPassword       <not set="">         url       <not set="">         userAccountControl       0x200 = (NORMAL_ACCOUNT)         userCert       <not set="">         userCertificate       <not set="">         userParameters       <not set="">         userPKCS12       <not set="">         userSharedFolder       <not set=""></not></not></not></not></not></not></not></not></not></not>	Attribute	Value					^
uidNumber       60001         unicodePwd <not set="">         unixHomeDirectory       <not set="">         unixUserPassword       <not set="">         unixUserPassword       <not set="">         unixUserPassword       <not set="">         unixUserPassword       <not set="">         userAccountControl       0x200 = (NORMAL_ACCOUNT)         userCert       <not set="">         userCertificate       <not set="">         userParameters       <not set="">         userPAssword       <not set="">         userPKCS12       <not set="">         userSharedFolder       <not set=""></not></not></not></not></not></not></not></not></not></not></not></not>	uid	<not set=""></not>					
unicodePwd <pre>     cnot set&gt;     unixHomeDirectory <not set="">     unixUserPassword <not set="">     unixUserPassword <not set="">     unix <pre>     unixUserPassword <not set="">     userAccountControl 0x200 = (NORMAL_ACCOUNT)     userCert <pre>     cnot set&gt;     userCertficate <not set="">     userParameters <not set="">     userPassword <not set="">     userPassword <not set="">     userPAssword <not set="">     userPAssword <not set="">     userPKCS12 <not set="">     userSharedFolder <not set="">     </not></not></not></not></not></not></not></not></pre></not></pre></not></not></not></pre>	uidNumber	60001					
unixHomeDirectory <not set="">         unixUserPassword       <not set="">         url       <not set="">         userAccountControl       0x200 = (NORMAL_ACCOUNT)         userCert       <not set="">         userCertficate       <not set="">         userParameters       <not set="">         userPAccount       <not set="">         userPassword       <not set="">         userPAssword       <not set="">         userPKCS12       <not set="">         userSharedFolder       <not set=""></not></not></not></not></not></not></not></not></not></not></not>	unicodePwd	<not set=""></not>					
unixUserPassword <not set="">         unixUserPassword       <not set="">         userAccountControl       0x200 = (NORMAL_ACCOUNT)         userCert       <not set="">         userCertificate       <not set="">         userParameters       <not set="">         userPassword       <not set="">         userPKCS12       <not set="">         userSharedFolder       <not set=""></not></not></not></not></not></not></not></not>	unixHomeDirectory	<not set=""></not>	-				
und <not set="">         userAccountControl       0x200 = (NORMAL_ACCOUNT)         userCert       <not set="">         userCertficate       <not set="">         userParameters       <not set="">         userPassword       <not set="">         userPKCS12       <not set="">         userSharedFolder       <not set=""></not></not></not></not></not></not></not>	unixUserPassword	<not set=""></not>	-				
userAccountControl       0x200 = (NORMAL_ACCOUNT)         userCert <not set="">         userCertificate       <not set="">         userParameters       <not set="">         userPassword       <not set="">         userPKCS12       <not set="">         userSharedFolder       <not set=""></not></not></not></not></not></not>	url	<not set=""></not>	-				
userCert <pre>cnot set&gt; userCertificate <not set=""> userParameters <not set=""> userPassword <not set=""> userPKCS12 <not set=""> userPrincipalName ad_admin@lsha.global userSharedFolder <not set=""> </not></not></not></not></not></pre>	userAccountControl	0x200 = (	NORMAL	_ACCOU	NT)		
userCertificate <not set=""> userParameters <not set=""> userPassword <not set=""> userPKCS12 <not set=""> userPrincipalName ad_admin@lsha.global userSharedFolder <not set=""></not></not></not></not></not>	userCert	<not set=""></not>					
userParameters <not set=""> userPassword <not set=""> userPKCS12 <not set=""> userPrincipalName ad_admin@lsha.global userSharedFolder <not set=""></not></not></not></not>	userCertificate	<not set=""></not>					
userPassword <not set=""> userPKCS12 <not set=""> userPrincipalName ad_admin@lsha.global userSharedFolder <not set=""></not></not></not>	userParameters	<not set=""></not>	r -				
userPKCS12 <not set=""> userPrincipalName ad_admin@lsha.global userSharedFolder <not set=""></not></not>	userPassword	<not set=""></not>					
userPrincipalName ad_admin@lsha.global userSharedFolder <not set=""></not>	userPKCS12	<not set=""></not>					
userSharedFolder <not set=""></not>	userPrincipalName	ad_admin	n@lsha.glo	bal			
	userSharedFolder	<not set=""></not>					~
	Edit					Filter	
Edit	and the second se						

Aggiunta dell'utente CLI di amministrazione al dominio AD

Collegarsi alla CLI di Cisco ISE, eseguire la identity-store e assegnare l'utente Admin all'archivio ID.

Ad esempio, per mappare l'utente amministratore CLI ad Active Directory definito in ISE come isha.global, eseguire questo comando:

#### identity-store active-directory domain-name

Una volta completato il join, connettersi alla CLI di Cisco ISE e accedere come utente Admin CLI per verificare la configurazione.

Se il dominio usato in questo comando è stato aggiunto in precedenza al nodo ISE, aggiungere nuovamente il dominio nella console Administrators.

1. Nell'interfaccia utente di Cisco ISE, fare clic sul pulsante Menu e passare a Administration >

Identity Management > External Identity Sources .

- 2. Nel riquadro di sinistra, scegliere Active Directory e scegliere il nome dell'annuncio.
- 3. Nel riquadro di destra, lo stato della connessione AD potrebbe essere **operational**. Se si esegue il test della connessione con Test User con MS-RPC o Kerberos, si verificano errori.
- 4. Verificare di poter ancora accedere alla CLI di Cisco ISE come utente Admin CLI.

## **ISE CLI**

- 1. Accedere alla CLI di ISE: ise30-1/admin# configure terminal Enter configuration commands, one per line. End with CNTL/Z. ise30-1/admin(config)#
- 2. Aggiungere il nodo al dominio: ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator

Se il dominio isha.global è già stato aggiunto tramite l'interfaccia utente, quindi è necessario

aggiungere di nuovo il dominio isha.global dall'interfaccia utente dopo questa configurazione.

Fino a quando non si verifica il rejoin, le autenticazioni a isha.global non riesce.

Do you want to proceed? Y/N : Y Password for Administrator:

Aggiunta al dominio isha.global completataNote:

- Se il dominio è già stato aggiunto tramite GUI, aggiungere di nuovo il nodo dalla GUI; in

caso contrario, le autenticazioni di AD continuano a fallire.

- Tutti i nodi devono essere uniti singolarmente tramite la CLI. Verifica Attualmente non è

disponibile una procedura di verifica per questa configurazione. Risoluzione dei

## problemiProblemi di joinI problemi durante l'operazione di unione e i relativi registri

possono essere visualizzati in "/var/log/messages file".Comando: show logging system

```
messagesScenario di lavoro2021-07-19T21:15:01.457723+05:30 ise30-1 dbus[9675]: [system] Activating via
systemd: service name='org.freedesktop.realmd' unit='realmd.service'
2021-07-19T21:15:01.462981+05:30 ise30-1 systemd: Starting Realm and Domain Configuration...
2021-07-19T21:15:01.500846+05:30 ise30-1 dbus[9675]: [system] Successfully activated service 'org.freedesktop.realmd'
2021-07-19T21:15:01.501045+05:30 ise30-1 systemd: Started Realm and Domain Configuration.
2021-07-19T21:15:01.541478+05:30 ise30-1 realmd: * Resolving: _ldap._tcp.isha.global
2021-07-19T21:15:01.544480+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.115
2021-07-19T21:15:01.546254+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.236
2021-07-19T21:15:01.546777+05:30 ise30-1 realmd: * Successfully discovered: Isha.global
2021-07-19T21:15:09.282364+05:30 ise30-1 realmd: * Required files: /usr/sbin/oddjobd, /usr/libexec/oddjob/mkhomedir,
/usr/sbin/sssd, /usr/bin/
2021-07-19T21:15:09.282708+05:30 ise30-1 realmd: * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-
smb-conf.MU0M60 -U Administrator ads join Isha.global
2021-07-19T21:15:12.701071+05:30 ise30-1 realmd: Enter Administrator's password:DNS update failed:
NT_STATUS_INVALID_PARAMETER
2021-07-19T21:15:12.705753+05:30 ise30-1 realmd:
2021-07-19T21:15:12.706142+05:30 ise30-1 realmd: Use short domain name -- ISHA
2021-07-19T21:15:12.706580+05:30 ise30-1 realmd: Joined 'ISE30-1' to dns domain 'Isha.global'
2021-07-19T21:15:12.708781+05:30 ise30-1 realmd: * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-
smb-conf.MU0M60 -U Administrator ads keytab create
2021-07-19T21:15:13.786749+05:30 ise30-1 realmd: Enter Administrator's password:
```

2021-07-19T21:15:13.859916+05:30 ise30-1 realmd: \* /usr/bin/systemctl enable sssd.service 2021-07-19T21:15:13.870511+05:30 ise30-1 systemd: Reloading. 2021-07-19T21:15:13.870724+05:30 ise30-1 realmd: Created symlink from /etc/systemd/system/multiuser.target.wants/sssd.service to /usr/lib/systemd/system/sssd.service. 2021-07-19T21:15:13.943407+05:30 ise30-1 realmd: \* /usr/bin/systemctl restart sssd.service 2021-07-19T21:15:13.956987+05:30 ise30-1 systemd: Starting System Security Services Daemon... 2021-07-19T21:15:14.240764+05:30 ise30-1 sssd: Starting up 2021-07-19T21:15:14.458345+05:30 ise30-1 sssd[be[lsha.global]]: Starting up 2021-07-19T21:15:15.180211+05:30 ise30-1 sssd[nss]: Starting up 2021-07-19T21:15:15.208949+05:30 ise30-1 sssd[pam]: Starting up 2021-07-19T21:15:15.316360+05:30 ise30-1 systemd: Started System Security Services Daemon. 2021-07-19T21:15:15.317846+05:30 ise30-1 realmd: \* /usr/bin/sh -c /usr/sbin/authconfig --update --enablesssd -enablesssdauth --enablemkhomedir --nostart && /usr/bin/systemctl enable oddjobd.service && /usr/bin/systemctl start oddjobd.service 2021-07-19T21:15:15.596220+05:30 ise30-1 systemd: Reloading. 2021-07-19T21:15:15.691786+05:30 ise30-1 systemd: Reloading.

2021-07-19T21:15:15.750889+05:30 ise30-1 realmd: \* Successfully enrolled machine in realm**Scenario non** 

lavorativoErrore di accesso a causa di password errata:2021-07-19T21:12:45.487538+05:30 ise30-1

dbus[9675]: [system] Activating via systemd: service name='org.freedesktop.realmd' unit='realmd.service'

2021-07-19T21:12:45.496066+05:30 ise30-1 systemd: Starting Realm and Domain Configuration...

2021-07-19T21:12:45.531667+05:30 ise30-1 dbus[9675]: [system] Successfully activated service 'org.freedesktop.realmd'

2021-07-19T21:12:45.531950+05:30 ise30-1 systemd: Started Realm and Domain Configuration.

2021-07-19T21:12:45.567816+05:30 ise30-1 realmd: \* Resolving: \_ldap.\_tcp.isha.global

2021-07-19T21:12:45.571092+05:30 ise30-1 realmd: \* Performing LDAP DSE lookup on: 10.127.197.115

2021-07-19T21:12:45.572854+05:30 ise30-1 realmd: \* Performing LDAP DSE lookup on: 10.127.197.236

2021-07-19T21:12:45.573376+05:30 ise30-1 realmd: \* Successfully discovered: Isha.global

2021-07-19T21:12:52.273667+05:30 ise30-1 realmd: \* Required files: /usr/sbin/oddjobd, /usr/libexec/oddjob/mkhomedir, /usr/sbin/sssd, /usr/bin/net

2021-07-19T21:12:52.274730+05:30 ise30-1 realmd: \* LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.R0SM60 -U Administrator ads join Isha.global

2021-07-19T21:12:52.369726+05:30 ise30-1 realmd: Enter Administrator's password:

2021-07-19T21:12:52.370190+05:30 ise30-1 realmd: Failed to join domain: failed to lookup DC info for domain 'Isha.global' over rpc: The attempted logon is invalid. This is either due to a bad username or authentication information.

2021-07-19T21:12:52.372180+05:30 ise30-1 realmd: ! Joining the domain Isha.global failed **Problemi di accessol** 

#### problemi durante l'accesso e i log relativi possono essere visualizzati in /var/log/secure

.Comando: show logging system secure Autenticazione riuscita:2021-07-19T21:25:10.435849+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:auth): unknown option: no\_magic\_root 2021-07-19T21:25:10.438694+05:30 ise30-1 sshd[119435]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin 2021-07-19T21:25:11.365110+05:30 ise30-1 sshd[119435]: pam\_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin 2021-07-19T21:25:11.365156+05:30 ise30-1 sshd[119435]: pam\_sss(sshd:auth): received for user ad\_admin: 12 (Authentication token is no longer valid; new one required) 2021-07-19T21:25:11.368231+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:account): unknown option: reset 2021-07-19T21:25:11.370223+05:30 ise30-1 sshd[119435]: pam\_succeed\_if(sshd:account): 'uid' resolves to '60001' 2021-07-19T21:25:11.370337+05:30 ise30-1 sshd[119435]: Accepted password for ad\_admin from 10.227.243.67 port 61613 ssh2 2021-07-19T21:25:11.371478+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root 2021-07-19T21:25:11.781374+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): reading settings from '/etc/security/limits.conf' 2021-07-19T21:25:11.781445+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): reading settings from '/etc/security/limits.d/20-nproc.conf' 2021-07-19T21:25:11.781462+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): process\_limit: processing soft nproc 4096 for DEFAULT 2021-07-19T21:25:11.781592+05:30 ise30-1 sshd[119435]: pam\_unix(sshd:session): session opened for user ad\_admin by (uid=0) 2021-07-19T21:25:11.784725+05:30 ise30-1 sshd[121474]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root

Errore di autenticazione a causa di una password errata:2021-07-19T21:25:10.435849+05:30 ise30-1

sshd[119435]: pam\_tally2(sshd:auth): unknown option: no\_magic\_root 2021-07-19T21:25:10.438694+05:30 ise30-1 sshd[119435]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin 2021-07-19T21:25:11.365110+05:30 ise30-1 sshd[119435]: pam\_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin 2021-07-19T21:25:11.365156+05:30 ise30-1 sshd[119435]: pam\_sss(sshd:auth): received for user ad\_admin: 12 (Authentication token is no longer valid; new one required) 2021-07-19T21:25:11.368231+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:account): unknown option: reset 2021-07-19T21:25:11.370223+05:30 ise30-1 sshd[119435]: pam\_succeed\_if(sshd:account): 'uid' resolves to '60001' 2021-07-19T21:25:11.370337+05:30 ise30-1 sshd[119435]: Accepted password for ad\_admin from 10.227.243.67 port 61613 ssh2 2021-07-19T21:25:11.371478+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root 2021-07-19T21:25:11.781374+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): reading settings from '/etc/security/limits.conf' 2021-07-19T21:25:11.781445+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): reading settings from '/etc/security/limits.d/20-nproc.conf' 2021-07-19T21:25:11.781462+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): process\_limit: processing soft nproc 4096 for DEFAULT 2021-07-19T21:25:11.781592+05:30 ise30-1 sshd[119435]: pam\_unix(sshd:session): session opened for user ad \_admin by (uid=0)2021-07-19T21:25:11.784725+05:30 ise30-1 sshd[121474]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root 2021-07-19T21:25:56.737559+05:30 ise30-1 sshd[119435]: pam\_unix(sshd:session): session closed for user ad\_admin 2021-07-19T21:25:56.738341+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root 2021-07-19T21:26:21.375211+05:30 ise30-1 sshd[122957]: pam\_tally2(sshd:auth): unknown option: no\_magic\_root 2021-07-19T21:26:21.376387+05:30 ise30-1 sshd[122957]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin 2021-07-19T21:26:21.434442+05:30 ise30-1 sshd[122957]: pam\_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin 2021-07-19T21:26:21.434461+05:30 ise30-1 sshd[122957]: pam\_sss(sshd:auth): received for user ad\_admin: 17 (Failure setting user credentials) 2021-07-19T21:26:21.434480+05:30 ise30-1 sshd[122957]: pam\_nologin(sshd:auth): unknown option: debug 2021-07-19T21:26:22.742663+05:30 ise30-1 sshd[122957]: Failed password for ad\_admin from 10.227.243.67 port 61675

ssh2**Errore di autenticazione a causa di un utente non valido:**2021-07-19T21:28:08.756228+05:30 ise30-1 sshd[125725]: Invalid user Masked(xxxx) from 10.227.243.67 port 61691 2021-07-19T21:28:08.757646+05:30 ise30-1 sshd[125725]: input\_userauth\_request: invalid user Masked(xxxx) [preauth]

2021-07-19T21:28:15.628387+05:30 ise30-1 sshd[125725]: pam\_tally2(sshd:auth): unknown option: no\_magic\_root 2021-07-19T21:28:15.628658+05:30 ise30-1 sshd[125725]: pam\_tally2(sshd:auth): pam\_get\_uid; no such user 2021-07-19T21:28:15.628899+05:30 ise30-1 sshd[125725]: pam\_unix(sshd:auth): check pass; user unknown 2021-07-19T21:28:15.629142+05:30 ise30-1 sshd[125725]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67

2021-07-19T21:28:15.631975+05:30 ise30-1 sshd[125725]: pam\_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=isha

2021-07-19T21:28:15.631987+05:30 ise30-1 sshd[125725]: pam\_sss(sshd:auth): received for user isha: 10 (User not known to the underlying authentication module)

2021-07-19T21:28:15.631993+05:30 ise30-1 sshd[125725]: pam\_nologin(sshd:auth): unknown option: debug 2021-07-19T21:28:17.256541+05:30 ise30-1 sshd[125725]: Failed password for invalid user Masked(xxxxx) from 10.227.243.67 port 61691 ssh2

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).