Geïntegreerde AD voor ISE GUI en CLIaanmelding

Inhoud

Inleiding **Voorwaarden** Gebruikte componenten **Configureren** Meld u aan bij ISE-to-AD **Directory-groepen selecteren** Administratieve toegang voor AD inschakelen De beheergroep configureren voor toewijzing van AD-groepen RBAC-toegangsrechten instellen voor de Admin-groep ISE GUI-toegang met AD-referenties **ISE-CLI-toegang met AD-referenties ISE CLI** Verifiëren Problemen oplossen Problemen samenvoegen Aanmeldingsproblemen

Inleiding

Dit document beschrijft de configuratie van Microsoft AD als externe identiteitsopslag voor administratieve toegang tot de Cisco ISE-beheerGUI en CLI.

Voorwaarden

Cisco raadt kennis van deze onderwerpen aan:

- Configuratie van Cisco ISE versie 3.0
- Microsoft AD

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 3.0
- Windows Server 2016

Dit document beschrijft de configuratie van Microsoft Active Directory (AD) als extern identiteitsarchief voor administratieve toegang tot Cisco Identity Services Engine (ISE) beheer-GUI en CLI.

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Gebruik deze sectie om het gebruik van Microsoft AD als extern identiteitsarchief voor administratieve toegang tot de Cisco ISE-beheerGUI te configureren.

Deze poorten worden gebruikt tussen ISE-knooppunt en AD voor deze communicatie:

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

Opmerking: zorg ervoor dat de AD-account alle vereiste rechten heeft.

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:
 Search Active Directory (to see if a Cisco ISE machine account already exists) Create Cisco ISE machine account to domain (if the machine account does not already exist) Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname) It is not mandatory to be a domain administrator to perform a join operation. 	 Search Active Directory (to see if a Cisco ISE machine account already exists) Remove Cisco ISE machine account from domain If you perform a force leave (leave without the password), it will not remove the machine account from the domain. 	 Ability to change own password Read the user/machine objects corresponding to users/machines being authenticated Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.) Ability to read tokenGroups attribute 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. If multiple join operations are performed, multiple machine accounts are maintained inside Cisco ISE, one for each join.

Meld u aan bij ISE-to-AD

- 1. Naar navigeren Administration > Identity Management > External Identity Sources > Active Directory .
- 2. Voer de nieuwe naam van het toetredingspunt en het AD-domein in.
- 3. Voer de referenties in van de AD-account waarmee u computerobjecten kunt toevoegen en wijzigen en klik op **OK**.

Cisco ISE	Administration • Identity Management	A Evaluation Mode 8
ntities Groups E	xternal Identity Sources Identity Source Sequences Settings	×
xternal Identity Sources	Join Domain Please specify the credentials required to Join ISE node(s) to the Active Directory	vanced Se
 Certificate Authent Active Directory Isha.AD 	AD User Name Administrator Password	_
LDAP ODBC RADIUS Token	Specify Organizational Unit Store Credentials Cancel Cancel	OK ONTROLLER
RSA SecuriD		

Join Operation Status

Status Summary: Successful

ISE Node	^	Node Status	
ise30-1.Isha.global		Completed.	
			Close
			01030

Directory-groepen selecteren

- 1. Naar navigeren Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory .
- 2. Importeer ten minste één AD Group waartoe uw beheerder behoort.



Administratieve toegang voor AD inschakelen

Voltooi deze stappen om wachtwoordgebaseerde verificatie voor AD in te schakelen:

- 1. Naar navigeren Administration > System > Admin Access > Authentication .
- 2. Van de Authentication Method tabblad kiest u de Password Based Optie.
- 3. Selecteer AD in het veld Identity Source (Functie).
- 4. Klik Save Changes .

 \times

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health (Checks
Authentication		Authenticatio	n Method	Password Policy	Account Disab	ble Policy	Lock/Susp
Authorization	>	Authenticat	ion Type				
Administrators	>						
Settings	>	Password	Based				
		* Identity Sour	се				
		AD:Isha.AD		~			
		O Client Cert	ificate Based				

De beheergroep configureren voor toewijzing van AD-groepen

Een Cisco ISE-lijnkaart definiëren Admin Group en in kaart te brengen aan een AD-groep. Dit maakt het mogelijk om de Role Based Access Control (RBAC) toestemmingen voor de beheerder op basis van groepslidmaatschap in AD.

- 1. Naar navigeren Administration > System > Admin Access > Administrators > Admin Groups .
- 2. Klik Add in de kop van de tabel om de nieuwe Admin Group configuratievenster.
- 3. Voer de naam in voor de nieuwe Admin-groep.
- 4. In het Type veld controleert u het External vink het vakje aan.
- 5. Van de External Groups Kies de AD-groep waaraan u deze Admin-groep wilt toewijzen, zoals gedefinieerd in de Select Directory Groups doorsnede.
- 6. Klik Save Changes .

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access
Authentication		Admin Groups >	New Admin Grou	qu				
Authorization	>	Admin Grou	ıp					
Administrators Admin Users	~	* Name	ISE_Admi	n	_			
Admin Groups		Description					11	
		Туре	External	I				
Settings	>	External Identity Name : Isha.AD	Source					
		✓ External	l Groups ha.global/Users	:/Domain User: 🗸	+			

RBAC-toegangsrechten instellen voor de Admin-groep

Voltooi deze stappen om RBAC-rechten toe te wijzen aan de Admin-groepen die in de vorige sectie zijn gemaakt:

1. Naar navigeren Administration > System > Admin Access > Authorization > Policy .

- 2. Van de Actions vervolgkeuzelijst aan de rechterkant, kies Insert New Policy een nieuw beleid toevoegen.
- 3. Maak een nieuwe regel met de naam AD_Administrator, wijst u deze toe aan de Admin Group die is gedefinieerd in de Enable Administrative Access voor AD sectie, en toewijzen het toestemmingen. **Opmerking**: in dit voorbeeld wordt de Admin Group **Super Admin** toegewezen, wat overeenkomt met de standaard admin-account.
- 4. Klik Save Changes . De bevestiging van de opgeslagen wijzigingen wordt weergegeven in de rechterbenedenhoek van de GUI.

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks		Backup & Restore	Admi	n Acc	ess	Se
Authentication		~	ERS Trustsec Policy	If ERS	Trustsec	+ ti	hen	Super Admin Data Access	+	•	ctions \sim	
Authorization	~	~	Helpdesk Admin Policy	If Hel	pdesk Admin	+ t	hen	Helpdesk Admin Menu Acces	s +	A	ctions ~	
Permissions		~ ~	Identity Admin Policy	If Ide	ntity Admin	+ ti	hen	Identity Admin Menu Access.	+	A	ctions \sim	
Menu Access	Ŭ.	2 ~	MnT Admin Policy	lf Mn	ſ Admin	+ ti	hen	MnT Admin Menu Access	+	A	ctions ~	
Data Access		~	AD_Administrator	If ISE	_Admin	+ ti	hen	Helpdesk Admin Menu Acce.	. >	A	ctions \sim	
RBAC Policy		2 ×	Network Device Policy	If Net	work Device Admi	n + ti	hen	Super Admin Menu A	cess	\sim	+	
		~ ~	Policy Admin Policy	If Poli	cy Admin	+ ti	hen					
Administrators	>	~ ~	RBAC Admin Policy	If RB/	AC Admin	+ ti	hen	Super Admin Data Ac	cess	~	٥	

ISE GUI-toegang met AD-referenties

Voltooi de volgende stappen om toegang te krijgen tot de ISE GUI met AD-referenties:

- 1. Uitloggen op de administratieve GUI.
- 2. Selecteer AD in het veld Identity Source (Functie).
- 3. Voer de gebruikersnaam en het wachtwoord in uit de AD-database en log in.

Opmerking: ISE-standaardwaarden voor de interne gebruikersopslag als AD onbereikbaar is of de gebruikte accountreferenties niet in AD bestaan. Dit vergemakkelijkt snel inloggen als u de interne winkel gebruikt terwijl AD is geconfigureerd voor beheertoegang.

	.1 1.1 1. CISCO	
	Identity Services Engine	
1 1 1	Username ad_admin	
	Password	
	Identity Source Isha.AD	_
	Internal	-
	Isha.AD	

Server Information

Username:	ad_admin
Host:	ise30-1
Personas:	Administration, Monitoring, Policy
	Service (SESSION, PROFILER)
Role:	STANDALONE
System Time:	May 08 2021 10:13:22 PM
	Asia/Kolkata
FIPS Mode:	Disabled
Version:	3.0.0.458
Patch Information:	none
	ок

ISE-CLI-toegang met AD-referenties

Verificatie met een externe identiteitsbron is veiliger dan met de interne database. RBAC voor CLI Administrators ondersteunt een extern identiteitsarchief.

Opmerking: ISE versie 2.6 en hoger ondersteunt verificatie van CLI-beheerders door externe identiteitsbronnen, zoals AD.

Beheer één bron voor wachtwoorden zonder dat u meerdere wachtwoordbeleidsregels hoeft te beheren en interne gebruikers binnen ISE dient te beheren, wat resulteert in minder tijd en moeite.

Voorwaarden

U moet de Admin-gebruiker gedefinieerd hebben en deze toegevoegd hebben aan een beheerdersgroep. De beheerder moet een **Super Admin**.

Define the User's Attributes in the AD User Directory

Op de Windows-server die wordt uitgevoerd Active Directory Wijzig de kenmerken voor elke gebruiker die u als CLI-beheerder wilt configureren.

1. Open de Server Manager Window en naar Server Manager > Roles > Active Directory Domain Services > Active

×

Directory Users and Computers > [ad.adserver]

2. Inschakelen Advanced Features onder het menu Beeld zodat u de eigenschappen van een gebruiker kunt bewerken.

Act	tive Direct	ory Us	ers and Com	puters						-	٥	×
File	Action	View	нер				_					
(Add/Remove	Columns								
📄 Ac	tive Direc	I	Large Icons				n					
> 🖺	Saved Q		Small Icons									
× 🕯	Isha.glo	1	List				count for ad					
>	Built		Detail				n this group c					
>	Com		Detail				of this group					
2	Eore	ļ	Users, Contac	ts, Groups, and Com	puters as container	s	of this group t					
	Kevs	~ 1	Advanced Fei	atures			ount manage					
Ś	Lost	F	Filter Options	hð			n this group c					
5	📑 Man	-	Customine				nistrators Gro					
>	Prog	(Customize	11			s who are per					
>	📋 Syste	m		Bomain Ad	Security Group	Designate	d administrato					
	📋 User			Bomain Co	Security Group	All workst	tations and ser					
>	NTD	S Quot	as	Bomain Con	Security Group	All domai	n controllers i					
>	🗎 TPM	Device	es	Bomain Gue	Security Group	All domai	in guests					
				B Domain Users	Security Group	All domai	in users					
				Enterprise A	Security Group	Designate	d administrato					
				Enterprise K	Security Group	Members	of this group					
				Enterprise R	Security Group	Members	of this group					
				Group Polic	Security Group	Members	in this group c					
				Guest	User	Built-in ad	ccount for gue					
				Key Admins	Security Group	Members	of this group					
				a krbtgt	User	Key Distri	bution Center					
				Reprotected Us	Security Group	Members	of this group					
				RAS and IAS	Security Group	Servers in	this group can					
				Read-only D	Security Group	Members	of this group					
				Schema Ad	Security Group	Designate	d administrato					
1												

- 3. Navigeer naar de AD-groep die de Admin-gebruiker bevat en zoek die gebruiker.
- 4. Dubbelklik op de gebruiker om het menu te openen Properties venster en kies de Attribute Editor
- 5. Klik op een kenmerk en voer gid om het kenmerk te vinden gidNumber . Als u de gidNumber kenmerk klikt u op het Filter knop en uitvink. Alleen eigenschappen met waarden tonen.
- 6. Dubbelklik op de naam van het kenmerk om elk kenmerk te bewerken. Voor elke gebruiker: toewijzen uidNumber groter dan 60000, en zorg ervoor dat het nummer uniek is.toewijzen gidNumber als 110 of 111.GidNumber 110 duidt een beheerder aan, terwijl 111 een alleenlezen gebruiker aanduidt.Wijzig de uidNumber na toewijzing.Als u de gidNumber, wacht minstens vijf minuten voordat u een SSH-verbinding maakt.

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: Com and tribute editor Attribute Value Image: Com and tribute editor uid Image: Com and tribute Image: Com and tribute editor uid Image: Com and tribute Image: Com and tribute editor uid Image: Com and tribute Image: Com and tribute editor unixUserPassword Image: Com and tribute editor Image: Com and tribute editor userCent Image: Com and tribute editor Image: Com and tribute editor userCent Image: Com and tribute editor Image: Com and tribute editor userCent Image: Com and tribute editor Image: Com and tribute editor userParameters Image: Com and tribute editor Image: Com and tribute editor userPrincipalName Image: Com and tribute editor Image: Com and tribute editor Image: Com and tribute editor Image: Com and tribute editor Image: Com and tribute editor userPrincipalName Image: Com and tribute editor Image: Com and tribute editor Image: Com and tribute editor Image: Com and tribute	Published Certificates	Member Of	Passwor	d Replicat	ion	Dial-in	Object
General Address Account Profile Telephones Organization Remote Desktop Services Profile COM+ Attribute Editor Attributes: Attribute Value Image: Common and the editor Attribute Value Value Image: Common and the editor uid Image: Common and the editor Image: Common and the editor Attribute Value Image: Common and the editor uid Image: Common and the editor Image: Common and the editor uid Image: Common and the editor Image: Common and the editor unixUserPassword Image: Common and the editor Image: Common and the editor unixUserPassword Image: Common and the editor Image: Common and the editor userCent Image: Common and the editor Image: Common and the editor userParameters Image: Common and the editor Image: Common and the editor userPhanedFolder Image: Common and the editor Image: Common and the editor userSharedFolder Image: Common and the editor Image: Common and the editor Image: Common and the editor Image: Common and the editor Image: Common and the editor user	Security E	nvironment	Sess	sions	Re	mote ca	ontrol
Remote Desktop Services Profile COM+ Attribute Editor Attributes: Attribute Value and set> and set>	General Address	Account	Profile	Telepho	ones	Orga	nization
Attributes:	Remote Desktop S	ervices Profile	C	:OM+	A	tribute B	ditor
Attribute Value ^ uid <not set=""> unicodePwd <not set=""> unixUserPassword <not set=""> unixUserPassword <not set=""> unixUserPassword <not set=""> unixUserPassword <not set=""> userAccountControl 0x200 = (NORMAL_ACCOUNT) userCertificate <not set=""> userParameters <not set=""> userParameters <not set=""> userPhrcS12 <not set=""> userSharedFolder <not set=""></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=""> unixUserPassword <not set=""> unixUserPassword <not set=""> userAccountControl 0x200 = (NORMAL_ACCOUNT) userCert <not set=""> userParameters <not set=""> userParameters <not set=""> userPKCS12 <not set=""> userSharedFolder <not set=""> verSharedFolder <not set=""></not></not></not></not></not></not></not></not></not></not></not></not>	Attribute	Value					^
uddNumber 60001 unicodePwd <not set=""> unixHomeDirectory <not set=""> unixUserPassword <not set=""> unixUserPassword <not set=""> unixUserPassword <not set=""> userAccountControl 0x200 = (NORMAL_ACCOUNT) userCert <not set=""> userCertficate <not set=""> userParameters <not set=""> userPAcS12 <not set=""> userPrincipalName ad_admin@lsha.global userSharedFolder <not set=""></not></not></not></not></not></not></not></not></not></not>	uid	<not set=""></not>					
unicodePwd v (not set> unixHomeDirectory (not set> unixUserPassword (not set> unixUserPassword (not set> userAccountControl 0x200 = (NORMAL_ACCOUNT) userCert (not set> userCertficate (not set> userParameters (not set> userPassword (not set> userPAssword (not set> userPKCS12 (not set> userPrincipalName ad_admin@lsha.global userSharedFolder (not set> ////////////////////////////////////	uidNumber	60001					
unixHomeDirectory <not set=""> unixUserPassword <not set=""> unixUserPassword <not set=""> userAccountControl 0x200 = (NORMAL_ACCOUNT) userCert <not set=""> userCertficate <not set=""> userParameters <not set=""> userPassword <not set=""> userPAssword <not set=""> userPKCS12 <not set=""> userSharedFolder <not set=""></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=""> userCertficate <not set=""> userParameters <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></not></not>	unixHomeDirectory	<not set=""></not>					
url <not set=""> userAccountControl 0x200 = (NORMAL_ACCOUNT) userCert <not set=""> userCertficate <not set=""> userParameters <not set=""> userPassword <not set=""> userPKCS12 <not set=""> userPhrincipalName ad_admin@lsha.global userSharedFolder</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=""> userPrincipalName ad_admin@lsha.global userSharedFolder <not set=""> <</not></not></not></not></not></not>	url	<not set=""></not>					
userCert <not set=""> 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></not>	userAccountContro	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>					
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	@lsha.gl	obal			
< >	userSharedFolder	<not set=""></not>					~
	<					>	
	F -14					Filter	1

Lid worden van de beheerder CLI-gebruiker naar het AD-domein

Verbinding maken met de Cisco ISE-CLI, voer de identity-store opdracht geven en de beheerder toewijzen aan het ID-archief.

Als u bijvoorbeeld de CLI-beheerder wilt toewijzen aan de Active Directory die in ISE is gedefinieerd als isha.global, voert u deze opdracht uit:

identity-store active-directory domain-name

Wanneer de koppeling is voltooid, maakt u verbinding met de Cisco ISE-CLI en logt u in als de beheerder-CLI-gebruiker om uw configuratie te verifiëren.

Als het domein dat u gebruikt in deze opdracht eerder was aangesloten bij de ISE-knooppunt, sluit u zich dan opnieuw aan bij het domein in de beheerdersconsole.

- 1. Klik in de Cisco ISE GUI op de Menu pictogram en navigeer naar Administration > Identity Management > External Identity Sources .
- 2. Kies in het linker deelvenster Active Directory en kies uw AD-naam.
- 3. In het rechter deelvenster wordt mogelijk de status van uw AD-verbinding gelezen **operational** . Er zijn fouten als u de verbinding met Test Gebruiker met of MS-RPC of Kerberos test.
- 4. Controleer of u nog steeds kunt inloggen op de Cisco ISE-CLI als de Admin CLI-gebruiker.

ISE CLI

- 1. Log in op de ISE-CLI: ise30-1/admin# configure terminal Enter configuration commands, one per line. End with CNTL/Z. ise30-1/admin(config)#
- 2. Sluit je aan bij het domein: ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator

Als het domein isha.global is al aangesloten via UI, dan moet u opnieuw toetreden tot het

domein isha.global van UI na deze configuratie. Totdat de herkoppeling gebeurt, worden

verificaties uitgevoerd op isha.global faalt.

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

Lid geworden van de domein sha.global succesvolOpmerkingen:

- Als het domein al is aangesloten via GUI, sluit u zich dan opnieuw aan bij het knooppunt

van GUI, anders blijven de verificaties tegen AD mislukken.

- Alle knooppunten moeten individueel via CLI worden aangesloten. Verifiëren Er is

momenteel geen verificatieprocedure beschikbaar voor deze configuratie. Problemen

OplossenProblemen samenvoegenProblemen tijdens het samenvoegen en de

bijbehorende logs kunnen worden weergegeven onder "/var/log/message file".Opdracht: show

logging system messages WerksCenario2021-07-19T21:15:01.457723+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 realmNiet-werkend

scenarioDoe mee aan een mislukking vanwege een onjuist wachtwoord: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 Aanmeldingsproblemen Problemen tijdens het inloggen en de bijbehorende

logbestanden zijn te zien onder /var/log/secure .Opdracht: show logging system secure Succesvolle

authenticatie: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

Verificatiefout vanwege onjuist wachtwoord: 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 ssh2Verificatiefout vanwege ongeldige gebruiker: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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.