AD für ISE-GUI und CLI integrieren Anmelden

Inhalt

Einleitung Voraussetzungen Verwendete Komponenten Konfigurieren Der ISE zur AD beitreten Verzeichnisgruppen auswählen Administrator-Zugriff für AD aktivieren Konfigurieren der Admin-Gruppe zur AD-Gruppenzuordnung RBAC-Berechtigungen für die Admin-Gruppe festlegen ISE-GUI-Zugriff mit AD-Anmeldeinformationen ISE CLI-Zugriff mit AD-Anmeldeinformationen **ISE-Kommandozeile** Überprüfung Fehlerbehebung Teilnahmeprobleme Anmeldeprobleme

Einleitung

In diesem Dokument wird die Konfiguration von Microsoft AD als externer Identitätsspeicher für den Administratorzugriff auf die Management-GUI und -CLI der Cisco ISE beschrieben.

Voraussetzungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Konfiguration der Cisco ISE Version 3.0
- Microsoft AD

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE Version 3.0
- Windows Server 2016

Dieses Dokument beschreibt die Konfiguration von Microsoft Active Directory (AD) als externer Identitätsspeicher für den Administratorzugriff auf das Cisco Identity Services Engine (ISE) Verwaltungs-GUI und -CLI.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren

In diesem Abschnitt können Sie die Verwendung von Microsoft AD als externen Identitätsspeicher für den Administratorzugriff auf die Cisco ISE-Verwaltungs-GUI konfigurieren.

Diese Ports werden zwischen ISE-Knoten und AD für diese Kommunikation verwendet:

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

Hinweis: Stellen Sie sicher, dass das AD-Konto über alle erforderlichen Berechtigungen verfügt.

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

Der ISE zur AD beitreten

- 1. Navigieren Sie zu Administration > Identity Management > External Identity Sources > Active Directory .
- 2. Geben Sie den neuen Namen des Join-Points und die AD-Domäne ein.
- 3. Geben Sie die Anmeldeinformationen des AD-Kontos ein, das Computerobjekte hinzufügen und ändern kann, und klicken Sie auf **OK**.

Cisco ISE	Administration • Identit	ty Management	Evaluation Mode 8
ntities Groups	External Identity Sources Identity Sou	irce Sequences Settings	
xternal Identity Sources	Join Domain Please specify the credentials required to	o Join ISE node(s) to the Active Directory Doma	vanced Se
 Certificate Authors Active Directory Isha.AD 	• AD User Name () Adm • Password	ninistrator	_
 LDAP ODBC RADIUS Token 	Specify Organizational Unit	Cancel	ontroller
RSA SecuriD			

Join Operation Status

Status Summary: Successful

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

Verzeichnisgruppen auswählen

- 1. Navigieren Sie zu Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory .
- 2. Importieren Sie mindestens eine AD-Gruppe, der Ihr Administrator angehört.



Administrator-Zugriff für AD aktivieren

Führen Sie die folgenden Schritte aus, um die kennwortbasierte Authentifizierung für AD zu aktivieren:

- 1. Navigieren Sie zu Administration > System > Admin Access > Authentication .
- 2. Über die Authentication Method Wählen Sie die Password Based Option.
- 3. Wählen Sie AD aus dem Identity Source aus.
- 4. Klicken Sie auf Save Changes .

 \times

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				

Konfigurieren der Admin-Gruppe zur AD-Gruppenzuordnung

Definieren einer Cisco ISE Admin Group und sie einer AD-Gruppe zuzuordnen. Dies ermöglicht die Autorisierung zur Bestimmung des Role Based Access Control (RBAC) Berechtigungen für den Administrator basierend auf der Gruppenmitgliedschaft in AD.

- 1. Navigieren Sie zu Administration > System > Admin Access > Administrators > Admin Groups .
- 2. Klicken Sie auf Add in der Tabellenkopfzeile, um die neuen Admin Group Konfigurationsbereich.
- 3. Geben Sie den Namen für die neue Admin-Gruppe ein.
- 4. Im Type Feld, überprüfen Sie die External Kontrollkästchen.
- 5. Über die External Groups Wählen Sie die AD-Gruppe aus, der diese Admin-Gruppe zugeordnet werden soll, wie im Select Directory Groups Abschnitt.
- 6. Klicken Sie auf Save Changes .

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access
Authentication		Admin Groups	New Admin Grou	qu				
Authorization	>	Admin Grou	qu					
Administrators Admin Users	~	* Name	ISE_Admi	n	-			
Admin Groups		Description					h	
		Туре	External	1				
Settings	>	External Identity Name : Isha.AD	Source					
		✓ Externa	I Groups ha.global/Users	/Domain User: 🗸	+			

RBAC-Berechtigungen für die Admin-Gruppe festlegen

Gehen Sie wie folgt vor, um den im vorherigen Abschnitt erstellten Admin-Gruppen RBAC-Berechtigungen zuzuweisen:

1. Navigieren Sie zu Administration > System > Admin Access > Authorization > Policy .

- 2. Über die Actions Dropdown-Liste auf der rechten Seite auswählen, Insert New Policy um eine neue Richtlinie hinzuzufügen.
- Erstellen Sie eine neue Regel mit der Bezeichnung AD_Administrator, ordnen Sie sie der Admin-Gruppe zu, die im Enable Administrative Access f
 ür den AD-Abschnitt und weisen Sie ihm Berechtigungen zu. Hinweis: In diesem Beispiel wird die Admin-Gruppe mit dem Namen Super Admin zugewiesen. Dies entspricht dem Standard-Admin-Konto.
- 4. Klicken Sie auf **Save Changes**. Die Bestätigung der gespeicherten Änderungen wird unten rechts in der GUI angezeigt.

Deployment	Licensing	Certificates Logg	aing Maintenance	Upgrade Health	h Checks	Backup & Restore	Admin A	ccess	Se
Authentication		🖌 🗸 ERS Trustse	ec Policy If ERS	Trustsec	+ then	Super Admin Data Access	+	Actions \vee	
Authorization	~	Helpdesk A	dmin Policy If Help	desk Admin	+ then	Helpdesk Admin Menu Acces	s +	Actions $ \!$	
Permissions		🗹 🗸 Identity Adr	min Policy If Ident	tity Admin	+ then	Identity Admin Menu Access.	+	Actions $ \sim $	
Menu Access		MnT Admin	Policy If MnT	Admin	+ then	MnT Admin Menu Access	+	Actions \sim	
Data Access		AD_Admini:	strator If ISE_	Admin	+ then	Helpdesk Admin Menu Acce.	. ×	Actions $ \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! \! $	
RBAC Policy		V Network De	vice Policy If Network	vork Device Admin	+ then	Super Admin Menu A	ccess ~	+	
		🔽 \vee 🛛 Policy Admi	in Policy If Polic	y Admin	+ then				
Administrators	>	RBAC Admi	in Policy If RBAG	C Admin	+ then	Super Admin Data Ac	cess ~	0	

ISE-GUI-Zugriff mit AD-Anmeldeinformationen

Führen Sie die folgenden Schritte aus, um mit AD-Anmeldeinformationen auf die ISE-GUI zuzugreifen:

- 1. Melden Sie sich von der Administrations-GUI ab.
- 2. Wählen Sie AD aus dem Identity Source aus.
- 3. Geben Sie den Benutzernamen und das Kennwort aus der AD-Datenbank ein, und melden Sie sich an.

Hinweis: Die ISE verwendet standardmäßig den internen Benutzerspeicher, wenn AD nicht erreichbar ist oder die verwendeten Kontoanmeldeinformationen in AD nicht vorhanden sind. Dies erleichtert die schnelle Anmeldung, wenn Sie den internen Speicher verwenden, während AD für den Administratorzugriff konfiguriert ist.

	cisco))	- 1
	Identity Servic	es Engine	
	Intuitive network	security	
1-1-	Username ad_admin		1
	Password		
	Identity Source		
	Isha.AD	^	-
and the second se	And the second		

 \times

οк

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

ISE CLI-Zugriff mit AD-Anmeldeinformationen

Die Authentifizierung mit einer externen Identitätsquelle ist sicherer als mit der internen Datenbank. RBAC für CLI Administrators unterstützt einen externen Identitätsspeicher.

Hinweis: ISE Version 2.6 und höher unterstützt die Authentifizierung von CLI-Administratoren über externe Identitätsquellen wie AD.

Verwalten Sie eine einzige Passwortquelle, ohne mehrere Passwortrichtlinien verwalten zu müssen, und verwalten Sie interne Benutzer innerhalb der ISE, was den Zeit- und Arbeitsaufwand verringert.

Voraussetzungen

Sie müssen den Administrator-Benutzer definiert und einer Administratorgruppe hinzugefügt haben. Beim Administrator muss es sich um einen Super Admin .

Define the User's Attributes in the AD User Directory

Auf dem Windows-Server, der Active Directory ändern Sie die Attribute für jeden Benutzer, den Sie als CLI-Administrator konfigurieren möchten.

- 1. Öffnen Sie Server Manager Window , und navigieren Sie zu Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ad.adserver]
- 2. Aktivieren Advanced Features im Menü Ansicht, damit Sie die Attribute eines Benutzers bearbeiten können.

Active Directory	y User	rs and Computers						-	٥	×
File Action V	iew	Help								
🗢 🌩 🖄 🚺	A	dd/Remove Columns								
Active Direc Saved Q Saved Saved Saved Q Saved Q Save	La Sr Li Do Us Fii Cu	arge Icons mall Icons st etail sers, Contacts, Groups, and Com dvanced Features liter Options ustomize	puters as containers Security Group Security Group	; Designate All workst	n n this group c of this group t of this group t ount manage n this group c n this group c s who are per d administrato tations and ser					
> 🦳 NTDS C > 🗂 TPM De	Quota:	s 國Domain Con 國Domain Con 國Domain Gue 國Enterprise A 國Enterprise R 國Group Polic 意Guest 國Krbgt 國Protected Us 國RAS and IAS 國Read-only D 國Schema Ad	Security Group Security Group Security Group Security Group Security Group Security Group User Security Group Security Group Security Group Security Group Security Group	All domai All domai All domai Designate Members Members Built-in ac Members Key Distril Members Servers in Members Designate	in controllers i in guests in users ed administrato of this group of this group c ccount for gue of this group c of this group bution Center of this group an this group can of this group ed administrato					

- 3. Navigieren Sie zur AD-Gruppe, die den Admin-Benutzer enthält, und suchen Sie diesen Benutzer.
- 4. Doppelklicken Sie auf den Benutzer, um das Properties und wählen Sie Attribute Editor .
- 5. Klicken Sie auf ein beliebiges Attribut, und geben Sie ein gid das Attribut suchen gidNumber. Wenn Sie das nicht finden gidNumber -Attribut auf das Filter und deaktivieren Sie. Zeigt nur Attribute an, die Werte haben.
- 6. Doppelklicken Sie auf den Attributnamen, um die einzelnen Attribute zu bearbeiten. Für jeden Benutzer: Zuweisen uidNumber größer als 60000 ist, und stellen Sie sicher, dass die Nummer eindeutig ist.Zuweisen gidNumber als 110 oder 111.GidNumber 110 steht für einen

Administrator, während 111 für einen schreibgeschützten Benutzer steht.Ändern Sie die uidNumber nach der Aufgabe.Wenn Sie die gidNumber, warten Sie mindestens fünf Minuten, bevor Sie eine SSH-Verbindung herstellen.

Published Certificates	Member Of	Password	Replicat	tion Dial-in	Object
Security En	vironment	Sessi	ons	Remote	control
General Address	Account	Profile	Teleph	ones Org	anization
Remote Desktop Se	ervices Profile	CC	+MC	Attribute	Editor
Attributes:					
Attribute	Value				^
garbageCollPeriod	<not set=""></not>				
gecos	<not set=""></not>				
generationQualifier	<not set=""></not>				
gidNumber	110				
givenName	ad_admin				
groupMembershipSA	<pre>M <not set=""></not></pre>				
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>				
info	<not set=""></not>				× *
(
Edit				Filte	r

Security Environment General Address Account Pro Remote Desktop Services Profile Attributes: Attribute Value uid <not set=""> uidNumber 60001 unicodePwd <not set=""></not></not>	Sessions ofile Telepho COM+	Remote co nes Orga Attribute I	ontrol inization Editor
General Address Account Pro Remote Desktop Services Profile Attributes:	COM+	nes Orga Attribute	nization Editor
Remote Desktop Services Profile Attributes: Attribute Value uid <not set=""> uidNumber 60001 unicodePwd <not set=""></not></not>	COM+	Attribute	Editor
Attributes: Attribute Value uid <not set=""> uidNumber 60001 unicodePwd <not set=""></not></not>			
Attribute Value uid <not set=""> uidNumber 60001 unicodePwd <not set=""></not></not>			
uid <not set=""> uidNumber 60001 unicodePwd <not set=""></not></not>			^
uidNumber 60001 unicodePwd <not set=""></not>			
unicodePwd <not set=""></not>			
unixHomeDirectory <not set=""></not>			
unixUserPassword <not set=""></not>			
und <not set=""></not>			
userAccountControl 0x200 = (NO	RMAL_ACCOUN	T)	
userCert <not set=""></not>			
userCertificate <not set=""></not>			
userParameters <not set=""></not>			
userPassword <not set=""></not>			
userPKCS12 <not set=""></not>			
userPrincipalName ad_admin@ls	ha.global		
userSharedFolder <not set=""></not>			~
Edit		Filter	

Beitreten des Admin-CLI-Benutzers zur AD-Domäne

Stellen Sie eine Verbindung zur Cisco ISE CLI her, und starten Sie das identity-store und weisen Sie den Administrator-Benutzer dem ID-Speicher zu.

Führen Sie beispielsweise den folgenden Befehl aus, um den CLI-Administrator-Benutzer dem Active Directory zuzuordnen, das in ISE als isha.global definiert ist:

identity-store active-directory domain-name

Wenn der Join abgeschlossen ist, stellen Sie eine Verbindung mit der Cisco ISE-CLI her, und melden Sie sich als Administrator-CLI-Benutzer an, um Ihre Konfiguration zu überprüfen.

Wenn die Domäne, die Sie in diesem Befehl verwenden, zuvor dem ISE-Knoten hinzugefügt wurde, treten Sie erneut der Domäne in der Administratorkonsole bei.

- 1. Klicken Sie in der Cisco ISE-GUI auf Menu und navigieren Sie zu Administration > Identity Management > External Identity Sources .
- 2. Wählen Sie im linken Fensterbereich Active Directory und wählen Sie Ihren AD-Namen aus.
- 4. Stellen Sie sicher, dass Sie sich weiterhin als Administrator-CLI-Benutzer bei der Cisco ISE CLI anmelden können.

ISE-Kommandozeile

- 1. Melden Sie sich bei der ISE CLI an: ise30-1/admin# configure terminal Enter configuration commands, one per line. End with CNTL/Z. ise30-1/admin(config)#
- 2. Beitreten des Knotens zur Domäne: ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator

Wenn die Domäne isha.global ist bereits über die UI beigetreten, dann müssen Sie erneut der

Domäne beitreten isha.global nach dieser Konfiguration über die Benutzeroberfläche aus. Bis

zur erneuten Anmeldung werden die Authentifizierungen isha.global schlägt fehl.

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

Der Domain isha.global erfolgreich beigetretenHinweise:

- Wenn die Domäne bereits über die GUI beigetreten ist, treten Sie dem Knoten über die GUI

erneut bei. Andernfalls schlägt die Authentifizierung gegen AD weiterhin fehl.

- Alle Knoten müssen einzeln über die CLI verbunden werden. Überprüfung Für diese

Konfiguration ist derzeit kein Überprüfungsverfahren

verfügbar. FehlerbehebungTeilnahmeproblemeProbleme während des Join-

Vorgangs und die dazugehörigen Protokolle sind unter "/var/log/messages file" zu

sehen.Command: show logging system messagesArbeitsszenario2021-07-19T21:15:01.457723+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/realmdsmb-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/realmdsmb-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 realmNicht-

ArbeitsszenarioTeilnahmefehler aufgrund eines falschen Kennworts: 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/realmdsmb-conf.R0SM60 -U Administrator ads join Isha.global 2021-07-19T21:12:52.369726+05:30 ise30-1 realmd: Enter Administrator's password: 2021-07-19T21:12:52.369726+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 Anmeldeprobleme Probleme bei der Anmeldung und die zugehörigen Protokolle

finden Sie unter /var/log/secure .Command: show logging system secure Erfolgreiche

Authentifizierung: 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

Authentifizierungsfehler aufgrund eines falschen Kennworts: 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 ssh2Authentifizierungsfehler aufgrund eines ungültigen Benutzers: 2021-07-19T21:28:08.756228+05:30 ise30-1 sshd[125725]: Invalid user Masked(xxxxx) 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(xxxxx) [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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.