Integrate Windows AD with CentOS using SSSD

430 Nesvin KN March 27, 2025 Productivity & Efficiency Features 6835

How to integrate Windows AD with Centos 8 using SSSD

Overview: This article provides a comprehensive guide on integrating Windows AD with Ezeelogin and RHEL 8, covering steps for LDAP configuration, authentication setup, and backend integration.

Ensure that the following ports on the RHEL host are open and accessible to the AD domain controllers.

DNS =53, LDAP =389, Kerberos 88 & 464, LDAP Global Catalog 3268 and NTP 123 (UDP)

Verify that the system time on both systems is synchronized. This ensures that Kerberos is able to work correctly.

Refer article to correct server time in Centos, RHEL, Ubuntu, SUSE

Step 1. Login to Ezeelogin Web GUI -> open settings -> Ldap

How to find base DN and bind RDN

Add the details of LDAP configurations.

Only the protoco	I. hostname, and port fields are a	allowed.)					
Ezeelogin		👤 Welcome. Administrator Loc					
t≣ Servers ►	LDAP Settings	•					
📑 Web Portals 🔹 🕨	Name						
1t Users	erad	Name					
		ezad					
Access Control	URI(s) 🤍	URI(s) 💿					
°₀ Settings 🛛 🖤	Idap://ezad.com						
L General	Start TI S @						
Branding							
 Control Panels 							
Data Centers	Bind RDN 🥥	Bind Password 🥹					
► API	CN=Administrator,CN=Users,DC=ezad,DC=com						
LDAP	UID Attribute 🐵	Filter 🐵					
► SAML	sAMAccountName						
► RADIUS	First Name Attribute 😨	Last Name Attribute 🔞					
 Server Fields 	givenName	sn					
🛞 Cluster	Email Attribute @	Group Attribute 📦					
Command Guard	mail						
	Time a fill						
Account		Rank 🥥					
🛇 Help 🕞 🕨	10	10					
License	Active	Windows Active Directory @					
		✓					
	Verify Certificate 😰	Cancel Save					
· · · · ·	- ×						
C ezeelogin.com							

Multiple URIs or a list of URIs can be specified in the format:

• Idaps://host.com:636/ Idaps://host.com:636/

Step 2. Go to Settings -> General -> Authentication -> change Web Panel Authentication to LDAP

Ezeelogin					1 w	elcome, Administrate			
Servers 🕨	General Settings	Authentication	Two Factor Authentication	Security	Defaults	Miscellaneous			
Web Portals 🛛 🕨	Password / Security Code Retries	- · · ·	Login captcha @						
Jsers 🕨	2		Disable	\$					
Access Control	Web Panel Authentication @	Web Panel Authentication 🥹			External SSH Auth 😨				
Settings 🔻	LDAP 🗘		1						
- Seneral	reCAPTCHA Sitekey @ Get reCAPTCHA	reCAPTCHA Sitekey @ Get reCAPTCHA API Key		reCAPTCHA Secret 🧐					
Iranding									
	User Password Lifetime 😨	User Password Lifetime @			Maximum Days Without Login 🐵				
	0		0						
	Allow Browsers To Save Login		Security Code LDA	P 🔞					
	-		Cancel Save						
	and the second se			and the second	S. A.				

Step 3. Select the LDAP users and click on the button to import users into Ezeelogin

Ezeelogin								Welcome	e, Administrator Logout
≣ Servers ►		Users in LDAP	find	All	~				+ >8
🖬 Web Portals	×	□ <u>Username</u> ↓	First Name	Last Name	Email	Status	User Grou	<u>ip LDAP</u>	Notes
🎎 Users 🧹 🔻		alex	alex			New	Dummy	Windows AD	
		🛃 john	john			New	Dummy	Windows AD	
User Groups		sam	sam			New	Dummy	Windows AD	
SSH Log		wick	wick			Exists	Dummy	Windows AD	
 RDP Recording 	1.10								1 - 4 / 4
► SCP Log	0	and the second second		- Contestantes		12 15	and section test	100 million 100 million	and a second
▶ Web Proxy Log		Users not in LD/	AP find	All	~				•
Web Proxy Activity		<u>Username</u> ↓	First Name	Last Name	Email	1	<u>Status</u>	User Group	Actions
Web Activity					No item				
 Shell Activity 		A A A A A A A A A A A A A A A A A A A		and the second second		10 P. 10 P. 10			and the second second
 Server Activity 	· ×						L. L. Con		
Work Summary			-		· *				2 4 S. E. A
► Status			14: 10					and the second	

You can confirm the imported LDAP users were listed in the Users tab in Ezeelogin GUI. You will be able to log in to Ezeelogin GUI with windows user credentials.

Step 4. Enable Security Code LDAP option from Settings > General > Authentication, if the user does not want to login to Ezeelogin GUI to set up a security code.

Ezeelogin		Welcome, Administrator Logout
🗄 Servers 🔻 🕇	General Settings Authentication	Two Factor Authentication Security Defaults Miscellaneous
📲 Web Portals 🕞 🗸	Password / Security Code Retries	Login cantcha
11 Users	2 \$	Disable \$
Access Control	Web Panel Authentication 💿	External SSH Auth 💿
% Settings	Internal \$	×
General	reCAPTCHA Sitekey Get reCAPTCHA API Key	reCAPTCHA Secret
► Branding		Maximum Deur With and Locia
Control Panels	User Password Lifetime	Maximum Days Without Login
Data Centers API		v Saswity Cada IDAD
► LDAP	Allow Browsers To Save Login	Security Code Date
► SAML		Cancel Save
RADIUS Sonrar Fields		
Cluster		
💿 Command Guard		
🐔 Account 🔹 🕨		

Backend configuration to integrate Windows with RHEL 8

Step 1. Install required packages.

root@gateway ~]# yum install realmd sssd oddjob oddjob-mkhomedir adcli samba-common sambacommon-tools krb5-workstation authselect-compat nscd -y

Step 2. Provide Windows IP and Windows domain name in hosts file.

root@gateway ~]# vim /etc/hosts

windows_ip windows_domain_name

Step 3. Provide Windows IP in resolv.conf to resolve and discover AD domain.

```
root@gateway ~]# vim /etc/resolv.conf
```

nameserver windows_ip

Step 4. Check if AD domain discovery is successful. Refer below example with Idapad.com

root@gateway ~]# realm discover ldapad.com

ldapad.com type: kerberos realm-name: LDAPAD.COM domain-name: ldapad.com configured: kerberos-member server-software: active-directory client-software: sssd required-package: oddjob required-package: oddjob-mkhomedir required-package: sssd required-package: adcli required-package: samba-common-tools login-formats: %U@ldapad.com login-policy: allow-realm-logins

Step 5. Join CentOS 8 in Active Directory domain. Replace Administrator with Windows admin account.

root@gateway ~]# realm join ldapad.com -U Administrator

Password for Administrator:

Step 6. Confirm joining successful with realm list. Refer below example.

root@gateway ~]# realm list ldapad.com type: kerberos realm-name: LDAPAD.COM domain-name: ldapad.com configured: kerberos-member server-software: active-directory client-software: sssd required-package: oddjob required-package: oddjob-mkhomedir required-package: sssd required-package: adcli required-package: samba-common-tools login-formats: %U@ldapad.com login-policy: allow-realm-logins **Step 7.** After successful joining you will get below sssd.conf and you need to change use_fully_qualified_names to False and shell to ezsh.

```
root@gateway ~]# vim /etc/sssd/sssd.conf
```

[sssd] domains = ldapad.com config_file_version = 2 services = nss, pam

```
[domain/ldapad.com]
ad_domain = ldapad.com
krb5_realm = LDAPAD.COM
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = ad
```

override_shell = /usr/local/bin/ezsh

Step 8. Restart sssd and nscd using the below commands.

root@gateway ~]# service sssd restart && service nscd restart



root@gateway ~]# id john uid=1701601108(john) gid=1701600513(domain users) groups=1701600513(domain users) root@gateway ~]# getent passwd john

john:*:1701601108:1701600513:john user:/home/john@ldapad.com:/usr/local/bin/ezsh

Note:

Use the below command to clear the cache of the user.

root@gateway ~]# sss_cache -u username

Note:

Verify Certificate feature is only available from **Ezeelogin version 7.35.0**.

Refer article to upgrade Ezeelogin to the latest version

Related Articles

Integrate Windows AD with RHEL 8 using SSSD

Integrate OpenLdap with Centos 8 using SSSD

Integrate Windows AD with Ubuntu using SSSD

Integrate OpenLdap with CentOS using SSSD

Online URL: https://www.ezeelogin.com/kb/article/integrate-windows-ad-with-centos-using-sssd-430.html