Authentication of Ezeelogin gateway users using Public keys fetched from Active Directory server

407 Riya Francis July 31, 2024 Features & Functionalities, Technical 5615

Authentication of SSH users using Public keys fetched from the Active Directory server

Overview: This article describes the process for extending the Active Directory schema to add SSH key attributes on Windows Server 2012 and 2016, including schema updates, attribute and class creation, user association, and integrating with Ezeelogin for SSH key retrieval.

- Extending the Active Directory schema to add SSH key attributes in Windows Server 2012 and 2016.
- 1. Launch a cmd prompt then spin up an Administrator cmd by running the following script.

C:UsersAdministrator> runas /user:DOMAINAdministrator cmd

• You'll get the following terminal after running the above command on cmd.



2. To open the Registry Editor run the following command on Administrator cmd.

C:windowssystem32>	regedit

3. Enabling Schema updates in Registry Editor Browse to **HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesNTDSParameters** and add a new DWORD key named **Schema Update Allowed.**

📑 R	egistry	Editor						
File	Edit	View	Favorit	es Help				
		:	∑ - <mark>_</mark> n	psvctrig	^	Name	Туре	Data
			> - n	si siproxy		ab (Default)	REG_SZ	(value not set)
		•	 N 	TDS		ab Configuration NC ab Database backu	REG_SZ REG_SZ	CN=Configuration,DC=Ezeelogin,DC=com C:\Windows\NTDS\dsadata.bak
				Diagnostics Parameters		ab Database log fil	REG_SZ	C:\Windows\NTDS
				Performance		ab Database loggin	REG_SZ	ON
				RID Values		ab DS Drive Mappi	REG_MULTI_SZ	c:\=\\?e2cd9ffb-0000-0000-0000-501f000
				Security		Big DSA Database E	REG_DWORD	0x00001922 (6434)
			> - 📊 N	tFrs		b DSA Database file	REG_SZ	C:\Windows\NTDS\ntds.dit
			> - N	TFS		DSA Working Di	REG_SZ	C:\Windows\NTDS
			N	ull		ab DsaOptions	REG_SZ	1
				vraid		🔀 Global Catalog	REG_DWORD	0x00000001 (1)
			> - <mark>- n</mark>	vstor		🔀 Hierarchy Table	REG_DWORD	0x000002d0 (720)
			> <mark></mark> O	neSyncSvc		🕮 lsClone	REG_DWORD	0x00000000 (0)
			> <mark></mark> O	neSyncSvc_ff869		👪 Idapserverintegr	REG_DWORD	0x00000001 (1)
			Pa	arport		ab Machine DN Na	REG_SZ	CN=NTDS Settings, CN=WIN-KC4AJFLCLGR, CN=S
			≥ - <mark>p</mark> a	artmgr		ab Root Domain	REG_SZ	DC=Ezeelogin,DC=com
			> - <mark>-</mark> Po	caSvc		🔀 Schema Version	REG_DWORD	0x00000057 (87)
			≥ - <mark>_</mark> p	ci		ab ServiceDII	REG_EXPAND_SZ	%systemroot%\system32\ntdsa.dll
			<u>></u>	ciide		Strict Replicatio	REG_DWORD	0x00000001 (1)
			} • <mark></mark> p	cmcia		System Schema	REG_DWORD	0xR0000057 (87)
			p	cw			-	6
			p	dc				
			> PI	EAUTH				

• Add Dword with value name Schema Update Allowed and value data 1.

reby Table PEG DMOPD	0-00000240 (720)	
Edit DWORD (32-bit) Value		×
Value name:		VIN
Schema Update Allowed		
Value data:	Base	
1	Hexadecimal	\nt
	 Decimal 	
	OK Cance	
	Value name: Schema Update Allowed Value data:	Value name: Schema Update Allowed Value data: I I Occurrent OK Cancel

4. Run the following in the Administrator command prompt to enable the schema editor snap-in.

c:Windowssystem32> regsvr32 schmmgmt.dll



5. Run **mmc** in the Administrator command prompt to open the Management console. Click on Ctrl + M and add Active Directory Schema as follows.

Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.



6. Creating a new attribute in Active Directory.

Right Click on Attributes and click 'Create New Attribute'. Provide the Common Name and LDAP Display Name as **sshPublicKeys**, 'Unique X500 Object ID' as **1.3.6.1.4.1.24552.1.13**, Syntax, select **IA5-String**, finally select the **Mutli-Valued** box, and click **Okay**.

 \times

Create New Attribute	\times				
Create a New Attribute Object Identification Common Name:					
LDAP Display Name: sshPublicKeys Unique X500 Object ID: 1.3.6.1.4.1.24552.1.1.1.13					
Syntax and Range					
Minimum:					
Multi-Valued OK Cancel Help					

7. Create a new class for the attribute.

Right-click on Classes and click '**Create class**'. Add 'Common Name' and 'LDAP Display Name', as **IdapPublicKey**, 'Unique X500 Object ID' as **1.3.6.1.4.1.24552.500.1.1.2.0**, Parent Class as '**top**', and for Class Type select '**Auxiliary**'. After providing the necessary fields click on the **Next** button.

Create New Schema Class

common Name:	
LDAP Display Nam	ie: IdapPublicKey
Jnique X500 Objec	ct ID: 1.3.6.1.4.1.24552.500.1.1.2.0
Description:	
nheritance and Ty	ре
Parent Class:	top
Class Type:	Auxiliary ~

×

• Add **sshPublicKeys** under Optional as follows.

Mandatory:			Add Remove	2
Optional:	sshPublicKeys		Add Remove	2
	< Back	Finish	Cancel	Help

 \times

8. Associating that class to user objects.

Expand the Classes and right-click on User then select **properties.** Click on the **Relationship** tab then click **Add Class** under **Auxiliary class.**

Finally, Add IdapPublicKey and click 'Apply'.

user Properties		?	×		
General Relations	nip Attributes	Default Security	1		
■T <mark>■</mark>	user				_
Parent Class:	organizational	Person			
Auxiliary Classes:	Idap Public Key mail Recipient msDS-Cloud E posixAccount securityPrincin	xtensions	• •	Add Class Remove	; ;
Possible Superior:	builtinDomain domainDNS organizational	Unit		Add Superio	or
C	С	iancel /	Apply	He	lp

9. Close all other windows open Active Directory Users and Computers(ADUC) and enable the **Advanced feature** as follows.



10. Browse to the user and add public keys under **Extensions** >> **Attribute Editor** >> **sshPublicKeys**.



11. Creating script on Ezeelogin server to fetch SSH key from AD

• Create the following script on your Ezeelogin server under /usr/local/fetchsshkeys.

Note: Replace the Basedn, Hostname_or_IP, Binddn, and Password with your Active Directory credentials.

#!/bin/bash

Idapsearch -x '(&(objectClass=*)(sAMAccountName='"\$1"'))' 'sshPublicKeys' -b "Base DN" -H Idap://Hostname_or_IP -D "Bind_RDN" -w 'password' | sed -n '/^ /{H;d};/sshPublicKeys:/x;\$g;s/n *//g;s/sshPublicKeys: //gp'

12. Add the following lines on the gateway server to your sshd_config file to point to the script

AuthorizedKeysCommand /usr/local/fetchsshkeys
AuthorizedKeysCommandUser root

• Now, the user "rhea" will be authenticated using the public key fetched from the Active Directory server.

♪ amadmin@ADMOD-LAPHP-01: /mnt/c/windows/system32	_	×
amadmin@ADMOD-LAPHP-01:/mnt/c/windows/system32\$ ssh rhea@192.168.1.10 Enter passphrase for key '/home/amadmin/.ssh/id_rsa':		^

Troubleshooting steps:

1. Ensure that the ssh public key is fetched for the user rhea from the OpenIdap server by running the following command:

root@jumpserver:~# ldapsearch -x '(&(objectClass=*)(sAMAccountName=""rhea""))' 'sshPublicKeys' -b "OU=EzAdmin,DC=Ezeelogin,DC=com" -H ldap://192.168.1.7 -D "cn=Administrator,cn=Users,dc=Ezeelogin,dc=com" -w 'zaQ!23edc123' | sed -n '/^ /{H;d};/sshPublicKeys:/x;\$g;s/n *//g;s/sshPublicKeys: //gp'

2. Ensure that the ssh public key is fetched for the user rhea from Ezeelogin installed server by

running the script:

root@jumpserver:~#/usr/local/fetchsshkeys rhea

Related Articles:

Install and set up an active Directory.

Integrate SAML Authentication with Ezeelogin.

Online URL:

https://www.ezeelogin.com/kb/article/authentication-of-ezeelogin-gateway-users-using-public-keys-fetched-from-active-directory-server-407.html