

Boston, MA June 23-26, 2015

Red Hat Summit 2015 **Red Hat Enterprise Linux Identity Management**

Diaa Radwan





Table of Contents

Lab Overview	3
Background	3
Red Hat Enterprise Linux Identity Management Overview Red Hat Enterprise Linux Identity Management Benefits: Enhances Security Provides eSSO (enterprise Single Sign-on)	3 4 4 4
Centralizes Administration and Control	4
Reduces costs	4 4 4
IdM Lab Environment Details	5
IdM Lab objectives	5
Lab 1: Server Installation	6
Lab 2: Users and Password Policies	9
Lab 3: Two Factor Authentication	11
Lab 4: Client Installation	14
Lab 5: User Groups and Host Groups Management	16
Lab 6: Integrating IdM with Active Directory	20
Lab 7: Host Based Access Control – HBAC	28
Lab 8: IdM Roles Management	32
Lab 9: IdM Replication	37
Lab 10: Services and Keytabs	38

Lab Overview

This lab guide assumes that you're following instructor-led training and that this lab guide is will try to simulate real life tasks and scenarios. It goes through a number of labs that will enable your to create full functional environment using Red Hat Enterprise Linux IdM. Also you will explore IdM features such as users, groups, policies and access control rules management. The purpose is to give you a basic hands-on overview of Red Hat Enterprise Linux Identity Management and how the components are fit together. It will use a combination of command-line tools and the IdM web interface. This lab is prepared to run on environment, the setup is descried in this document on Lab Environment Section.

Your instructor will provide you with any additional information that you will require, primarily the lab setup and required scenarios.

Background

Red Hat Enterprise Linux Identity Management Overview

Red Hat Enterprise Linux IdM is a way to create identity stores, centralized authentication, domain control for Kerberos and DNS services, and authorization policies — all on Linux systems, using native Linux tools. It is also supports Linux/Unix domains.



Red Hat Enterprise Linux Identity Management Benefits:

Enhances Security

Centralizes authentication, authorization and fine-grained access control for UNIX/Linux environments.

Provides eSSO (enterprise Single Sign-on)

Enables users to access many different enterprise resources after their initial log-in without having to type user name and password again and again.

Centralizes Administration and Control

Allows administrators to easily consolidate and manage identity servers in a UNIX/Linux environment; with the option to interoperate with Active Directory.

Implements Standards-Based, Integrated Components

Integrates the capabilities of Kerberos, LDAP, DNS and x.509 certificates into a simple identity management solution.

Reduces costs

Can replace third-party user directories or Identity Management Solutions

IdM Features

- Integrated, native user, host, and service authentication and access control.
- Consistent and manageable identity management for Linux and Unix systems.
- Interoperability with Microsoft Active Directory domains.
- Standards-based, trusted technologies.
- Easier and clearer to implement, maintain, and understand authentication and access control policies.
- Flexible access control rules based on sudo rules, host-based rules, and other criteria.
- Consistent and universal password policies for users.
- Integrate established Linux/Unix services like NFS, automount, NIS, NTP, Kerberos, and DNS into a single management domain.
- Smooth migration paths from NIS and LDAP services.
- Scalable operations with up to 20 servers and replicas and an unlimited number of clients in a single domain.



IdM Lab Environment Details

Element	URL	Username	Password
IdM Server	http://idm-server.example.com	admin	password
IdM Server	ssh: idm-server.example.com	root	redhat
IdM client	ssh: idm-client.example.com	root	redhat
IdM access evaluation	ssh: idm-access.example.com	root	redhat
IdM Replication	ssh idm-replica.example.com	root	redhat
Windows Active Directory	Virtual Machine Console	administrator	Secret123

IdM Lab objectives

Deploy both client and server centralized and high available authentication using Red Hat Enterprise Linux Identity Management (IdM) and provide a working central authentication server, implement additional access controls and sudo rules for client and access machines.

Note: Make sure that all virtual machines starting with "**IdM-***" are running. After finishing Lab1, you can start the Windows-DC machine which is running the Active Directory

Lab 1: Server Installation

Target server: idm-server.example.com Access: ssh root@idm-server.example.com

- Log into idm-server.example.com, via ssh.
- Make sure that hosts file is properly configured, you should find this line:

cat /etc/hosts | grep idm 192.168.10.10 idm-server.example.com idm-server

Install the IdM packages:

yum -y install bind-dyndb-ldap ipa-server

Run as root:

```
[root@idm-server ~]# ipa-server-install --setup-dns --ssh-trust-dns \
    --mkhomedir
```

When you prompt for these questions use the respective answers:

```
Existing BIND configuration detected, overwrite? [no]: <Yes>
Server host name [idm-server.example.com]: <Press Enter>
Please confirm the domain name [example.com]: <Press Enter>
Please provide a realm name [EXAMPLE.COM]: <Press Enter>
Directory Manager password: <Use "password">
Password (confirm): <Use Password>
IPA admin password: <Use Password>
Password (confirm): <Use Password>
Do you want to configure DNS forwarders? [yes]: Yes
Enter IP address for a DNS forwarder: 192.168.10.254
Enter IP address for a DNS forwarder: <Press Enter>
Do you want to configure the reverse zone? [yes]: Yes
Continue to configure the system with these values? [no]: Yes
Domain name: example.com
```

You should get the same information at end of the dialog:

The IPA Master Server will be configured with: Hostname: idm-server.example.com IP address: 192.168.10.10

Domain name: example.com Realm name: EXAMPLE.COM BIND DNS server will be configured to serve IPA domain with: Forwarders: 8.8.8.8 Reverse zone: 10.168.192.in-addr.arpa.

After installation: Check the IdM web interface via idmserver.example.com, use the admin username and password.

				Mozilla Firefox				
🖉 🕅 🕅	entity Management	× 🕒						
	https://idm-server. e :	xample.com/ipa/ui/		▼ C Search	☆ 自	↓ ☆		⊜ ≡
	RED HAT	DENTITY MANAGEMENT				ا	ed ha	it.
/	Username Password	Username Password or Password+One-Time-Pas	ssword Sync OTP Token Login	 To login with username and pa To login with Kerberos, please r configured the browser correctly, 	sssword, enter them in the c make sure you have valid tic then click Login.	orresponding kets (obtainabl	ields, then e via kinit) i	click Login. and

- Check main IPA configuration: /etc/ipa/default.conf base DN, realm.
- Obtain a kerberos ticket:

kinit admin klist

Check automatically created DNS records (A, SRV):

```
ipa dnszone-find
ipa dnsrecord-find --name=idm-server -all
Zone name: example.com
Active zone: TRUE
Authoritative nameserver: idm-server.example.com.
Administrator e-mail address: hostmaster.example.com.
SOA serial: 1434449021
SOA refresh: 3600
SOA retry: 900
```

Check IdM server defaults:

```
ipa config-show
ipa config-mod --defaultshell=/bin/bash
```

• Then on the idm-server check the logs (Just to know where to start debugging, not needed):

```
/var/log/pki-ca/debug
/var/log/pki-ca-install.log
/var/log/dirsrv/ (permissions!)
/var/log/messages
```

- Common install issues:
 - Broken DNS, bad /ect/hosts configuration.
 - Files and certificates remains after the last unsuccessful install.
 - Time synchronization issues.

Lab 2: Users and Password Policies

Target server: idm-server.example.com **Access:** ssh root@idm-server.example.com

1. Add new users (create a username with your preferences in the prompt mode), then run the other commands:

```
ipa user-add
ipa user-add --first=John --last=Smith jsmith
ipa user-add --first=Matt --last=Well --manager=jsmith \
--email=mwell@example.com --homedir=/home/mwell mwell
```

2. Modify User attributes:

```
ipa user-mod jsmith --addattr=departmentnumber=101
ipa user-show jsmith --all
ipa user-mod mwell --title="System Engineer"
```

Modify Users password as admin:

```
ipa user-mod mwell --password
ipa user-mod jsmith --password
```

4. Check if the system recognize the users:

```
id jsmith
getent group mwell
```

5. Check the default Password Polices:

```
ipa help pwpolicy
ipa pwpolicy-show
ipa pwpolicy-mod --maxlife=60
```

6. As jsmith **login** via ssh to idm-server, you will be prompted to change the password for first time. Then Change password with:

```
[root@idm-server ~]# ssh jsmith@localhost
ipa passwd
```

It will fail because of min life policy.

7. As Admin:

```
ipa pwpolicy-mod --minlife=0 --maxfail=3
ipa pwpolicy-show
```

- 8. As mwell, login to the idm-server, change the 1st time password and then, change password with "ipa passwd ", it will succeed as we changed the minimum lifetime of users password.
- 9. On the Web UI check the following:
 - Add a user.
 - Check password expiry.
 - Edit user details.

Reference:

Red Hat Documentation : Managing User Groups

Lab 3: Two Factor Authentication

Two-factor authentication is a security process in which the user provides two means of identification, the user will be asked to provide the authentication system two elements or parts, first part is something the user know and the second one is something the user have. If you didn't finish this lab it will not impact the rest of the workshop.

Target server: idm-server.example.com

2FA soft token: Install FreeOTP on your smartphone, you can find the application on App Store or Google Play

Open http://idm-server.example.com then Login as admin, The navigate to **IPA Server** tab. Then access the "**Configuration**" subtab.

You will find the authentication "**Default user authentication types**" Choose make the "**Two factor authentication (password + OTP)**" then click update:

🔗 Identity Management 🗙 💭			
😵 🗞 🔀 🕼 🗠 🖉 😵 🖉			★ =
RED HAT IDENTITY MANAGEMENT		Red Hat Access	Administrator 🖌 🔒
Identity Policy Authentication Network Services 🚽 IPA Server			
Role Based Access Control ~ ID Ranges ID Views Realm Domains C	onfiguration		
Configuration			
CRefresh DReset Update			
Search Options	User Options		
Search size limit * 100	User search fields *	uid,givenname,sn,telephonenumber,ou,title	
Search time limit * 2	Default e-mail	example.com	
	Default users group *	ipausers	
	Home directory base *	/home	
	Default shell *	/bin/sh	
	Maximum username *	32	
	length		
	Password Expiration * Notification (days)	4	
	Beenvered advertee		
	features	KDC:Disable Last Success	
		C KDC:Disable Lockout	
	Default user	✓ Password	
	authentication	Radius	
	types 🕑 🙎	Two factor authentication (password + OTP)	
		Undo	•

Log out from the admin session, login with jsmith, then navigate to **OTP Tokens** then click on Add. In the Add OTP token, make sure that you fill the required filled as the figure below:

👔 Identity Management 🗙 📃				8 – o ×
💮 🗞 🕃 🕼 🚱	ver.example.com/ipa/	/ui/#/e/otptoken/search		* =
RED HAT IDENTITY MANAGEMENT			Red Hat Access	🛓 John Smith 🔪
Users OTP Tokens	Add OTP Token		×	
OTP Tokens Search Q Unique ID No entries.	Type Description * Required field	Time-based (TOTP) O Counter-based (HOTP) jsmith-token Add Add and Add Another Add and Edit Cance	ete + Add = Disable	▼ Enable

After adding the token, the a QR code will show, scan this QR through FreeOTP or any other Soft token (FreeOTP is recommended):



••••∘ du 奈 Edit	2:59 AM FreeOTP	* 25% □ +	•••••• du 奈 Edit	2:59 AM FreeOTP	* 25% □ →+	••••• du 奈 Edit	3:07 AM FreeOTP	* 33% 🗩 +
				jsmith@EXAMP	LE.COM		28385 jsmith@EXAMP	57 LE.COM

the QR Code Sign, then token for jsmith: scan the OR code

On the smartphone, After scanning the the Click open FreeOTP, click on QR Code you see new

on the new created id to generate a new token.

Now logout user jsmith and try to login using the token. The password will be the original jsmith password+ the generated number. So if the password was "redhat" the login password should be "redhat283857".

Please note that "redhat" as password will still be able to authenticate jsmith because we selected 2 authentication methods in the global IdM configuration.

Lab 4: Client Installation

Target server: idm-client.example.com and idm-access.example.com **Access:** ssh root@idm-client.example.com

• Check in both servers resolv.conf point to IdM server (192.168.10.10):

```
echo 'nameserver 192.168.10.10' > /etc/resolv.conf
cat /etc/resolv.conf
nameserver 192.168.10.10
```

Verify that idm-client/idm-access resolvers arepointing to idm-server

```
dig example.com
example.com. 3600 IN SOA idm-server.example.com. hostmaster.example.com. 1396857706
3600 900 1209600 3600
```

Install the IdM client (sssd):

yum install ipa-client

 on IdM server, make sure that PRT records are created/updated in new client installations:

ipa dnszone-mod --allow-sync-ptr=TRUE
Zone name: example.com

Client installation:

ipa-client-install --enable-dns-updates --mkhomedir --ssh-trust-dns
User authorized to enroll computers: <admin>
Password for admin@EXAMPLE.COM: <password>

Additional options to automate the installation:

```
ipa-client-install --mkhomedir --enable-dns-updates --ssh-trust-dns \
--server=idm-server.example.com --domain=example.com -p admin -w password \
--fixed-primary -U
```

• Some adjustment.

The default shell for new users is /bin/sh, which should probably be changed if you are using Linux only, On idm-server:

[root@idm-server ~]# ipa config-mod --defaultshell=/bin/bash

- Perform all the above steps on idm-access.example.com, to install the client on idm-access.
- Try to access both machines with the above created users from idmclient.example.com.

ssh jsmith@idm-access.example.com
Creating home directory for jsmith.

 Ssh back to idm-client.example.com, you should login without any passwords:

ssh jsmith@idm-client.example.com

Note: make sure that you have domainname and hostname in your hosts file. Example: in idm-access.example.com:

192.168.10.12 idm-access.example.com idm-access

Lab 5: User Groups and Host Groups Management

Target server: idm-server.example.com **Access:** ssh root@idm-server.example.com

Activities for lab 4:

- Create users group (Either through command line or Web UI).
- Adding Group Members.
- Deleting users group.
- Explore IdM group management through command line, a new group named 'servers' will be added, then user 'mwell' will be member of servers, adding other group named 'clients' and finally adding jsmith to 'clients' group:

```
ipa group-add --desc='users server group' servers
ipa group-add-member servers --users=mwell
ipa group-add --desc='users client group' clients
ipa group-add-member clients --users=jsmith
ipa group-find
ipa group-del <group name>
ipa help group
```

On the Web UI check the following:

- The group that you just created through the command line.
- Default User and Groups Settings, 3 default groups:
 - ipausers.
 - admins.
 - editors.
- Check the created groups on the web interface, check also the created users.
- Create two host groups:
 - restricted.
 - access.

Through the web interface follow Identity ► Host groups ► Add. Visit the Host Groups sub tab:

Identity Managemer	ıt – Mozilla Firefox			
🔊 Identity Management 🛛 🗴 🚱				
A https://idm-server.example.com/ipa/ui/#/e/hostgroup/search	▼ C Search	☆ 🖻	↓ ⋒ ∢	□
RED HAT IDENTITY MANAGEMENT			Red Hat Access	🛓 Administrator 🗸
Identity Policy Authentication Network Services IPA Ser	ver			
Users User Groups Hosts Host Groups Netgroups	Services Automember ~			
Host Groups				
Search Q			C Refresh	Delete + Add
□ Host-group	Description			
No entries.				
https://idm-server.example.com/ipa/ul/#identity/nostgroup				

Then find "**Add**" button to add new Host Group:

EED HAT IDENTITY MANAGEMENT Red Hat Access Administrat dentity Policy Authentication Network Services IPA Server	RED HAT IDENTITY MANAGEMENT Identity Policy Authentication Network Services IPA Server Users User Groups Hosts Host Groups Netgroups Services Automember ~ Host Groups Search Q Description No entries.	Administrato
No entries Red Hat Access ▲ Administrate	Red Hat IDENTITY MANAGEMENT Red Hat Access Identity Policy Authentication Network Services IPA Server Users User Groups Hosts Hosts Groups Services Automember ~ Host Groups e e e e Search Q Description e No entries. No entries.	🛓 Administrato
Policy Authentication Network Services IPA Server Isers User Groups Hosts Host Groups Netgroups Services Automember ✓ Host Groups Image: Comparise services Image: Comparise services Image: Comparise services Automember ✓	Identity Policy Authentication Network Services IPA Server Users User Groups Hosts Host Groups Netgroups Services Automember ~ Host Groups Q Refresh Image: Comparison of the services Description No entries. Image: Comparison of the services Image: Comparison of the services Image: Comparison of the services	
lsers User Groups Hosts Host Groups Netgroups Services Automember ∽ HOST Groups Search Q	User Groups Hosts Host Groups Netgroups Services Automember > Host Groups Search Q Image: Refresh Image: R	
Host Groups	Host Groups Search Q Image: Comparison of the second of t	
Search Q CRefresh Delete +Add	Search Q Description No entries.	
Search Q CRefresh Delete + Add	Search Q CRefresh CRE	
Host-group Description	Host-group Description No entries.	Delete + Add
No entries	No entries.	
No citales:		6

As required create new group called "restricted" and "access":

Red Hat loeNtity Policy Authentics Identity Policy Authentics Users User Groups Hosts Host-group* restricted Description This host group is created to restrict users from accessing idm-client.example.com No entries. * Required field	https://idm-server.example.com	/ipa/ui/#/e/hostgroup/sea	rch 🔻 🤁 🔍 Search	☆	Ê	₽.	⋒			9
Identity Policy Authentic Users User Groups Host Host-group Host-group * restricted Description This host group is created to restrict users from accessing Idm-client example.com * Required field * Required field Add Add and Add Another Add and Edit Cancel	RED HAT IDENTITY MANAGEMENT					Red I	Hat Acce	255	🚢 Adr	ninistra
Users User Groups Hosts Host-group * restricted Description This host group is created to restrict users from accessing Idm-client,example.com * Required field * Required field Add and Add Another Add and Edit Cancel	Identity Policy Authentica	Add Host Group		x						
Host-group * restricted Description This host group is created to restrict users from accessing idm-client example.com * Required field Add Add and Add Another Add and Edit Cancel	Users User Groups Hosts									
Search Q Description This host group is created to restrict users from accessing idm-client.example.com * Required field Add Add and Add Another Add and Edit Cancel Add	Host Groups	Host-group *	restricted							
* Required field Add Add and Add Another Add and Edit Cancel	Search Q Host-group No entries.	Description	This host group is created to restrict users from accessing idm-client.example.com			2F	Refresh		elete	+ Ad
Add Add and Add Another Add and Edit Cancel		* Required field								
Add			Add Add and Add Another Add and Edit Car	ncel						
_			Add							

Now the host group is created, click on "**restricted**" to add the hosts

🥖 📦 Ide	entity Management	× 🕒										
(+)	https://idm-serve	r.example.com	/ipa/ui/#/e/hostg	roup/search	▼ (Search		☆ 自	↓ 俞 ·		Ø	≡
RED HA	AT IDENTITY MANAGEMEI	NT							Red Hat Access	🚢 Ac	Iministra	ator ~
Identit	y Policy A	uthentication	Network Se	ervices IPA S	erver							
Users	User Groups	Hosts	Host Groups	Netgroups	Services	Automember \sim						
Hos	t Groups											
Saarch									@ Pofrosh	n Doloto	+ ^/	dd
Search	۷								C Refresh	iii Delete	TAC	uu
	Host-group	Description										
	restricted	This host gro	oup is created to re	strict users from acce	essing idm-client.	example.com						
Showi	ing 1 to 1 of 1 entries.						×					

Then you will find a created host group named "**restricted**", click on the "**restricted**" then "**Add**".

👔 Identity Management 🗙 📃			a - 0x
📀 🛷 🕃 🕼 🗠 🚱 🚱 🚱	/#/e/hostgroup/member_host/restricted		★ =
RED HAT IDENTITY MANAGEMENT			Red Hat Access 🔷 Administrator 🔨
Identity Policy Authentication Network Ser	Add Hosts into Host Group restricted	×	
Users User Groups Hosts Host Groups Host Groups > restricted Host Group: restricted restricted members: Refresh @ Delete	Filter available Hosts Available Host name Hos	Filter Prospective Host name idm-client.example.com Add Cancel	Show Results Direct Membership Indirect Membership

- Both **idm-client** and **idm-server** should be in restricted group.
- Create other host group following the same steps, name this group "access".
- The **idm-access** machines should be in "**access**" group, follow the same steps in creating and adding machines to restricted group.

Reference: Red Hat Documentation : Managing User Groups

Lab 6: Integrating IdM with Active Directory

Target server: idm-server.example.com, idm-client.example.com and winad.example.com

Access: ssh root@idm-server.example.com, ssh root@idmclient.example.com and console access to winad.example.com

One of the available machines is running Windows Active Directory, the machine is ready with AD. Make sure that you have access to the Windows machine using username "administrator" and the password is "Secret123". Also we will install the AD trust and winbind clients.

The IdM integration with Active Directory is sensitive to DNS setup, we want to allow example.com that is hosted on idm-server.example.com to be transferable to the AD

Run on IdM server:

[root@idm-server ~]# yum install -y ipa-server-trust-ad samba-winbind-clients [root@idm-server ~]# ipa dnszone-mod example.com --allow-transfer=192.168.10.253 Zone name: example.com. Active zone: TRUE Authoritative nameserver: idm-server.example.com. Administrator e-mail address: hostmaster.example.com. SOA serial: 1433680513 SOA refresh: 3600 SOA retry: 900 SOA expire: 1209600 SOA minimum: 3600 Allow query: any; Allow transfer: 192.168.10.253;

On winad.example.com:

Open the powershell/cmd and run the following to add the example.com zone:

```
dnscmd 127.0.0.1 /ZoneAdd example.com /Secondary 192.168.10.10
```

Just in case you didn't know how to open PowerShell, here is the icon:



Running the dnscmd command should return the same output:



On the Windows Desktop, You will find DNS icon (shortcut), it will open DNS service on windows, we want to verify the new resources created, double click on DNS icon and follow the DNS tree as shown blow:



The red lines shows that idm-server.example.com is added in the forward lookup zones.

Next configuration will be applying DNS forwarding for queries related to winad.example.com to AD DNS server. On the idm-server.example.com run:

```
[root@idm-server ~]# ipa dnsforwardzone-add winad.example.com \
--forwarder=192.168.10.253 --forward-policy=only
Zone name: winad.example.com.
Active zone: TRUE
Zone forwarders: 192.168.10.253
Forward policy: only
```

Then adding Windows AD A record in the IdM server:

[root@idm-server ~]# ipa dnsrecord-add example.com dc.winad \
--a-ip-address=192.168.10.253
Record name: dc.winad
A record: 192.168.10.253

Also we need to add the NS record for winad (AD domain name)

[root@idm-server ~]# ipa dnsrecord-add example.com winad --ns-hostname=dc.winad Record name: winad NS record: dc.winad

Verify that SRV records are resolvable on IdM server:

```
[root@idm-server ~]# dig SRV _ldap._tcp.winad.example.com
; <<>> DiG 9.9.4-RedHat-9.9.4-18.el7_1.1 <<>> SRV _ldap._tcp.winad.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25329
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;_ldap._tcp.winad.example.com. IN
                                        SRV
;; ANSWER SECTION:
_ldap._tcp.winad.example.com. 468 IN
                                        SRV
                                                0 100 389 dc.winad.example.com.
;; AUTHORITY SECTION:
winad.example.com.
                       86400
                              IN
                                                dc.winad.example.com.
                                        NS
;; ADDITIONAL SECTION:
dc.winad.example.com.
                        3468
                                ΙN
                                        А
                                                192.168.10.253
```

After verifying that IdM server can resolve SRV records of AD, we will verify that SRV records of IdM server are resolvable from AD server (you will type the yellow underlined nslookup commands):

PS C:\Users\Administrator> nslookup.exe Default Server: localhost6.localdomain6 Address: ::1
> <u>set type=srv</u> > <u>_ldaptcp.example.com</u> Server: localhost6.localdomain6 Address: ::1
_ldaptcp.example.com SRU service location:

We can verify that the record it add to the Idap using Idapsearch:

ldapsearch -Y GSSAPI -b cn=dns,dc=example,dc=com idnsname=example.com.

The next configuration required will be installing the AD trust IdM server, it will add all necessary objects and configuration to allow IdM server to create a trust to the Active Directory domain.

ipa-adtrust-install -U --netbios-name="EXAMPLE" --enable-compat -a "password"

Before adding the trust relationship, we need to make sure that both server are in the same timezone, using PowerShell on Windows first command will show the configured timezone and the second command will set it to EST, windows will need to be restarted, reboot the windows machine after running the below commands:

```
PS C:\Users\Administrator> tzutil.exe /g
Eastern Standard TimePS C:\Users\Administrator>
PS C:\Users\Administrator> tzutil.exe /s "Eastern Standard Time"
PS C:\Users\Administrator>
```

On IdM server, run timedatectl to set the timezone to EST:

[root@idm-server ~]# timedatectl set-timezone America/New_York

Then, we can start adding the trust relationship (If IdM and AD are having different timezone it will fail):

ipa trust-add --type=ad winad.example.com --admin Administrator --password Re-established trust to domain "winad.example.com" Realm name: winad.example.com Domain NetBIOS name: WINAD Domain Security Identifier: S-1-5-21-3652195975-17874612-2275940394 SID blacklist incoming: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6, S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-17, S-1-5-16, S-1-5-15, S-1-5-14, SID blacklist outgoing: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6, S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16, S-1-5-15, S-1-5-1, S-1-5-7, S-1-5-6, S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16, S-1-5-15, S-1-5-16, S-1-5-15, S-1-5-14, Trust direction: Two-way trust Trust type: Active Directory domain Trust status: Established and verified

Add AD Admins group to IdM, Create IdM group that will be flagged as external group:

```
[root@idm-server ~]# ipa group-add --desc='ad_domain admins external map' \
ad_admins_external --external
Added group "ad_admins_external"
```

Group name: ad_admins_external
Description: ad_domain admins external map

Create a POSIX compliant group to be linked to the external group:

```
[root@idm-server ~]# ipa group-add --desc='ad_domain admins' ad_admins
Added group "ad_admins"
Group name: ad_admins
Description: ad_domain admins
GID: 1861200012
```

Add members of Domain Admins to the created IdM group:

Adding members from external AD group to IdM POSIX compliant group:

```
[root@idm-server ~]# ipa group-add-member ad_admins --group ad_admins_external
Group name: ad_admins
Description: ad_domain admins
GID: 1861200016
Member groups: ad_admins_external
.....
Number of members added 1
```

The last commands that we need run are to add the AD users to IdM:

```
ipa group-add --desc='ad_domain users external map' ad_users_external --external
ipa group-add --desc='ad_domain users' ad_users
ipa group-add-member ad_users_external --external 'WINAD\Domain Users'
ipa group-add-member ad_users --group ad_users_external
```

Now, this is the testing time; wbinfo will retrieve the SID associated with the username specified:

```
kinit admin
kvno -S HTTP `hostname`
ipa trust-show winad.example.com
kdestroy
klist
kinit Administrator@WINAD.EXAMPLE.COM
klist
kvno -S cifs dc.winad.example.com
wbinfo -n 'WINAD\Domain Admins'
S-1-5-21-66505577-848503339-3105483033-512 SID_DOM_GROUP (2)
```

We can create a shared disk to AD Admins, these commands will create and new directory "/linuxshare" and make it available to AD admins:



The share will be available to Windows Admins, later we can avail users shares if needed, on windows machines open Computer then map the share to a Windows drive following the same procedures:



A new dialog will open as dialog will be opened to define the share it will ask for the user password, use the administrator as user and the password is "Secret123":

🍓 Ma	ap Network D	rive	×						
\bigcirc	😪 Map Network Drive								
	What netwo	rk folder would you like to map? rive letter for the connection and the folder that you want to connect to:							
	Drive: Folder:	Z: Browse \\idm-server.example.com\share Browse Example: \\server\share Reconnect at logon Connect using different credentials Connect to a Web site that you can use to store your documents and pictures.							
		Finish Cancel							

You will find the contens of "/linuxshare" available, the file that we created "IdM-rocks" will be there accessible. You can create folders on Windows and check them back on the idm-server.example.com.

Now, the administrator user can login to Linux machines without passwords, remember that we didn't configure the Host Based Access Control, so all users can login to all servers it is not recommend to run this configuration in the production. Next lab we will have a HBAC configured and it will show how to define new rules and examining the existing rules.

On the Windows Desktop you will find putty (a ssh client) use idmclient.example.com as the Host Name:

🔀 PuTTY Configuration	×
Category:	
- Session - Logging - Terminal - Keyboard - Bel - Features - Window - Appearance - Behaviour - Translation - Selection - Colours - Connection - Data - Proxy - Telnet - Riogin - Serial - Seria	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port idm-client.example.com 22 Connection type: Raw Raw Telnet Rlogin Saved Sessions Default Settings Load Save Delete Save Close window on exit: Always Never Only on clean exit
About	Open Cancel

Then use Administrator@winad.example.com as the login name, you should log in without password request



Reference: Red Hat Documentation : Windows Integration Guide

Lab 7: Host Based Access Control – HBAC

Target server: idm-server.example.com, idm-client.example.com and idmaccess.example.com

Access: ssh root@idm-server.example.com, ssh root@idmclient.example.com and ssh root@idm-client.example.com

In this Lab we will restrict/allow access based on host groups that we defined in the previous labs. By default IdM is having allow access permission to all resources, we could disable it during the installation time through --no_hbac_allow.

Disable the default allow all rule through web interface.

HAT IDENTITY MANAGEMENT			Red Hat Access	Administr
ntity – Policy Authent	cation Network Services	IPA Server		
st Based Access Control ~	Sudo 🗸 SELinux User Maps	Password Policies Kerberos Ticket Policy		
SAC Rules				
			[™] Defecte + Add = Displa	of Engl
Rule name	Status	Description		♥ Ella
allow_all	✓ Enabled	Allow all users to access any host from any host		
owing 1 to 1 of 1 entries.				

RED HAT IDENTITY N	ANAGEMENT				Red Hat Access	Administrator
dentity Polic	cy Auther	ntication	Network Services	IPA Server		
ost Based Acces	s Control 🗸	Sudo 🗸	SELinux User Maps	Password Policies	Kerberos Ticket Policy	
BAC Rules » allow	_all					
✓ HBAC Ru	le: allow_	all				
✓ HBAC RU Settings CRefresh ⑦Res	e: allow_	Actions ~				
 ✓ HBAC Ru Settings CRefresh ORes General 	et L update	Actions ~				
 ✓ HBAC Ru Settings C Refresh ⑦Res General 	et 1 Update Enable Disable 2 Delete	Actions ~				

We want to grant access permissions to users in "servers" group to access all machines considering the following:

- Users in "servers" group can access "restricted" host group servers.
- Users in "clients" group can login into "access" host groups only. •

The HBAC defines who can access within which resources the environment, not the level of access. This is called host-based access control because the rule defines what hosts are allowed to access other hosts within the domain.

Four basic elements to construct HBAC rule:

- Who: The rule applies to.
- Where: Hosts users can access.
- How: What login services can be accessed.
- Setting Host-Based Access control Rules.
 - HBAC Rule with name "access-rule" through the web interface.

📝 📦 Identity Management 🗙 🔲				8 - 0 X
🚱 🗞 🔀 🕼 🚱	mple.com/ipa/ui/#/e/h	bacrule/search		★ =
RED HAT IDENTITY MANAGEMENT				Red Hat Access 💄 Administrator ১
Identity Policy Authentication	Add HBAC Rule		×	
Host Based Access Control - Sudo				
HBAC Rules	Rule name *	access-rule		
Search Q	* Required field			© Delete → Add → Disable → Enable
Rule name State allow_all = 0 Showing 1 to 1 of 1 entries.		Add Add and Add Another Add and Edit Co	ancel	



in 'clients' Group In 'servers' group

Click on the **access-rule** HBAC and add users or users groups that this rule will be applied on.

Settings							
C Refresh D Reset L Update	Actions Add	Jser Groups into HBAC Rule ad	ccess-rule		;	×	
General	Filte	r available User Groups			Filter		
Rule	name Avai	lable		Prosp	ective		
Descr	iption	User Groups	>		User Groups		
		admins			clients		
		editors	<				
		ipausers					
		servers					
W/be		trust admins					
VVIIO							
User category the rule applies to: O An	yone 🤆						
Users					2	-	🛍 Delete 🕈 Add
					Add Cancel	1	1
User Groups					Add	_	🗊 Delete 🛛 🕈 Add

Add "clients" users group to the access-rule in WHO field.

Then add the resources that will have these rules applied either host groups or specific hosts (to access-rule), in this lab the access group should be used, if you didn't create it, you can add host instead of host group, select the idm-access.example.com.

General	Add Host Groups into HBAC Rule a	ccess-rule		3	×	
	Filter available Host Groups			Filter		
	Available		Pros	pective		
	Host Groups	>	0	Host Groups		
	restricted			access		
Vho ier category th		Ľ		_		
VhO per category th Users	e	×.	_	Add Cancel	B Delete •	+ Add
VhO ser category th Users User Gr clients	e suga	×.		2 Add Cancel	B Delete •	+ Add + Add
Who Iser category th Users User Gr clients	napa	×.		2 and Cancel	Delete	+ Ad

Now we want to add the service that will be allowed, select the sshd and login services:

😻 Identity Managemen 🗴							8	
😓 -> 🖏 🕼 🗠 🖉	er.exa	mple.com/ipa/ui/#/e/hbacrul	e/details/acces	s-rule				☆ =
	Add H	HBAC Services into HBAC Rule a	ccess-rule			×		
	Filte	r available HBAC Services				Filter		
Who	Avai	lable		Pros	pective			
User category the rule applies to: ${\sf O}$.		HBAC Services	>		HBAC Services			
Users	0	crond			login		窗 Delete	+ Add
		ftp	<		sshd			
User Groups		gdm					🗑 Delete	+ Add
		gdm-password						
Accessing		gssftp						
Accessing		kdm						
Host category the rule applies to: O		proftpd						
Hosts		pure-ftpd					窗 Delete	+ Add
idm-client.example.com		su						
idm-server.example.com		su-l						
		sudo						
Host Groups		sudo-i						+ Add
		vsftpd						
Via Service								
Service category the rule applies to: (
Services					2 A	d Cancel	1 Delete	+ Add
Service Groups						Á	創 Delete	+ Add

- In previous steps we created the access-rule that will allow "clients" users group to access servers in "Access" host group, Since Access host group doesn't have any other server except idmaccess.example.com; we allowed access to idm-access.example.com or any server that will be added to this host group
- Create additional HBAC with name"restricted-rule" that allows "servers" users group to access servers in "restricted" host group using the previous steps used to create the "allow-rule". So the steps are adding "servers" user group, Accessing "restricted" host group and services via "sshd and login"
- Testing Host-Based Access control Rules:
 - User mwell can ssh to idm-client.example.com successful.
 - User mwell will find access denied message if tried to ssh to "access".
 - User jsmith can login via ssh to access.example.com.

Reference: Red Hat Documentation : Managing Host Based Access Control

Lab 8: IdM Roles Management

IdM Role Management provides rights or permissions that users have been granted to perform operations within IdM on other users or objects:

- Who can perform the operation.
- What can be accessed.
- What type of operation can be performed.
- Existing Predefined Roles.

Role-based access control grants a very different kind of authority to users compared to self-service and delegation access controls. Role-based access controls are fundamentally administrative, with the potential to, for example, add, delete, or significantly modify entries.

In this lab we will provide privileges to mwell or his group to change his/their group membership

Open the "**IPA Server**" tab in the top menu, and select the "**Role Based Access Control**" subtab.

Click the "**Add**" link at the top of the list of role-based ACIs:

Ident	ity Policy Au	uthentication	Network Servio	es IPA	Server	
Role	Based Access Control	 ID Ranges 	ID Views	Realm D	omains)	Conf
Rol	es ^{ch} q			∂ Refresh	Delete	+ Add
	Role name	Description			_	
	IT Security Specialist	IT Security Specia	list			
	IT Specialist	IT Specialist				
	Security Architect	Security Architect	:			

Enter the role name and a description:

Add Role		×
Role name *	Example Role	
Description	For engineers	
* Required field		
	Add and Add Another Add and Edit	Cancel

Click the "Add and Edit" button to save the new role and go to the configuration page.

Click on the Role that you just created, then click on "Add"

🖉 Identity	Management ×					8 - 0 %
@ • 🔊 G	🖹 🖄 bttps://idm-	server.example	com/ipa/ui/#/e	/role/member_u	ser/Example%20r	ole 🔺 🔳
RED HAT ID	ENTITY MANAGEMENT				Red Hat Access	💄 Administrator 🗸
Identity	Policy Aut	hentication	Network Services	IPA Server		
Role Based	l Access Control 🗸	ID Ranges	ID Views	Realm Domains	Configuration	
Role: E Example role Users	xample role	Hosts Host Gro	ups Services	Privileges	Settings	
C Refresh	Telete + Add	-				
No entries.	iogin					

Select the users on the left and use the ">" button to move them to the "**Prospective**" column.

👔 Identity Management 🗙 🔲			8 - 0 X
🚱 🗞 🔀 🏦	er.example.com/ipa/ui/#/e/role/memb	er_user/Example%20role	★ =
RED HAT IDENTITY MANAGEMENT		Red Hat Access	💄 Administrator 💙
Identity Policy Authen	Add Users into Role Example role	×	
Role Based Access Control ~ Roles » Example role	Filter available Users Available	Filter	
Role: Example role	User login	User login	
Example role members: Users User Groups Host Refresh Delete + Add User login No entries.	admin adman jsmith	mwell Add Cancel	

At the top of the "**Privileges**" tab, click "**Add**".

Ident	ity Policy	Authentic	ation N	etwork Service	es IPA Serve	er			
Role	Based Access Cor	ntrol 🗸 🛛 I	D Ranges	ID Views	Realm Domai	ins Configu			
Roles	Roles » Example Role								
Rol	Role: Example Role								
Examp	ole Role members:	ouns Host	s Host Gr	oups Septi	Privileg	as (A) Sattir			
Osers (1) Oser Groups Hosts Host Groups Services Privileges (4) Setting C Refresh Im Delete Im Delete </td									
	Privilege name								
	Automount Administrators								
	Certificate Administrators								
	DNS Administrators								

Select the privileges on the left and use the ">" button to move them to the "**Prospective**" column.

👔 Identity Ma	anagen	nent ×						8 - 0 X
🐨 •≫ ⓒ 🕼 bttps://idm-server.example.com/ipa/ui/#/e/role/memberof_privilege/Example%20 ★ 🚍								
RED HAT IDENTITY MANAGEMENT Red Hat Access Administrator								
Identity	Add R	ole Example role into Privileges					×	
Role Based	Filter	available Privileges					Filter	
Roles » Exai	les » Exa Available			Prospective				
Role: E:		Automember Task Administrator	•	>		Privilege name		
Example role		Automount Administrators				DNS Administrators		
Users (1)		Certificate Administrators		<		DNS Servers		
2 Refresh		Delegation Administrator						
		Group Administrators						
		HBAC Administrator						
No entries.		Host Administrators						
		Host Enrollment						
		Host Group Administrators						
		IPA Masters Readers						
		Kerberos Ticket Policy Readers						
		Modify Group membership						
		Modify Users and Reset passwords						
		Netgroups Administrators						
		PassSync Service	-					
	_		_		_	ZAdd	Cancel	

Click the "Add" button to save.

Log out the admin user, and login with mwell user. Navigate through "**Network Services**", then DNS subtab menu ► then click on example.com. After getting example.com resources; click on "**Add**":

🔞 Identity Management 🗙 🗌								
🗞 🤣 🔀 🕼 الطبحة://idm-server.example.com/ipa/ui/#/e/dnszone/records/example.com.								
RED HAT IDENTITY MANAGEMENT								
Identity Policy Authentication 1 Network Services IPA Server								
Automount 2 DNS v								
DNS Z	Zones » example.com.							
DNS Resource Records: example.com.								
DN	S Resource Record	is: example.co	om.					
DN	S Resource Record	is: example.co	om.					
DN dn	S RESOURCE RECORD	is: example.co	om.					
DN DN Searc	S RESOURCE RECORD	IS: example.co	om.	⊘ Refresh ⊕Delete →Add				
DN bearc	S RESOURCE RECORD	IS: example.co	OM. Data	C Refresh @ Delete Add				
DN bn \$earc	S RESOUICE RECOID IS Resource Records Settin ch Q Record name @	Record Type NS	OM. Data idm-server.example.com.	C Refresh ⓑ Delete → Add				
DN Searce	S RESOUICE RECOID IS Resource Records Settin ch Q Record name @ _kerberos	Record Type NS TXT	OM. Data idm-server.example.com. EXAMPLE.COM	C Refresh @ Delete Add				
DN Searce	S RESOUICE RECOID IS Resource Records Settin ch Q Record name @ _kerberos _kerberos-master_tcp	gs Record Type NS TXT SRV	Data idm-server.example.com. EXAMPLE.COM 0 100 88 idm-server	C Refresh Delete Add				
DN \$earce 0 0 0 0	S RESOUICE RECOID IS Resource Records Settin ch Q Record name @ _kerberos _kerberos-master_tcp _kerberos-master_udp	gs Record Type NS TXT SRV SRV	Data idm-server.example.com. EXAMPLE.COM 0 100 88 idm-server 0 100 88 idm-server	C Refresh @ Delete Add				
	S Resource Records Settin Ch Q Record name C Lerberos Lerberos-master_tcp Lerberos_tcp	Record Type Record Type NS TXT SRV SRV SRV	Data idm-server.example.com. EXAMPLE.COM 0 100 88 idm-server 0 100 88 idm-server 0 100 88 idm-server	CRefresh Delete Add				

We need to test that user "**mwell**" can add new records, create new record "**notify**" TXT record with text data "Important note" :

/ 😻 Identity Managemen ×								
\$	🕅 🕅 🕅 🕅 🕅	-server.example.com/ipa/	ui/#/e/dnszone/records/example.com.			☆ =		
RED HAT IDENTITY MANAGEMENT Red Hat Access								
Ident		×						
Autor	mount DNS 🗸							
DNS Z	ones » example.com.	Record name *	notify					
DNS Resource Re		Record Type	TXT	۲				
DNS Resource Records		Text Data *	Important note					
Search Q		* Required field			C Refresh	lete + Add		
	Record name							
	@							
	_kerberos		Add Add and Add Another Add and Edit	Cancel				
	_kerberos-mastertcp			currect				
	_kerberos-masterudp		SRV 0 100 88 idm-server					

User mwell, will be able to add dns records to example.com domain.

[root@idm-server ~]# dig TXT notify.example.com | grep Important notify.example.com. 86400 IN TXT "Important" "note"

Reference: Red Hat Documentation : Roles Management

Lab 9: IdM Replication

Target server: idm-server.example.com and idm-replica.example.com **Access:** ssh root@idm-server.example.com ssh root@idmreplica.example.com

On the idm-replica.example.com run:

yum install ipa-server bind-dyndb-ldap

On The idm-server.example.com run:

ipa-replica-prepare idm-replica.example.com --ip-address 192.168.10.13

Copy the replication info to the replica:

```
scp /var/lib/ipa/replica-info-idm-replica.example.com.gpg \
root@192.168.10.13:/var
```

On idm-replica.example.com run:

```
ipa-replica-install --no-forwarders --skip-conncheck --setup-dns \
/var/replica-info-idm-replica.example.com.gpg
```

Other options:

```
ipa-replica-install --forwarder=<our forward DNS> --setup-dns <replica
file.gpg>
```

Replication verification.

```
ipa-replica-manage list
ipa-replica-conncheck --replica idm-replica.example.com
```

Reference: Red Hat Documentation Managing the Server-Replica Relationships

Lab 10: Services and Keytabs

Target server: idm-server.example.com or idm-client.example.com **Access:** ssh root@idm-server.example.com ssh root@idmclient.example.com

Log in to idm-access machine:

yum install httpd mod_nss mod_wsgi mod_auth_kerb ipa-admintools

Prepare content for idm-access:

```
cp workshop.conf /etc/httpd/conf.d/workshop.conf
cp workshop.wsgi /var/www/cgi-bin/workshop.wsgi
chmod +x /var/www/cgi-bin/workshop.wsgi
```

Create the IPA service entry for idm-access:

kinit
Password for admin@EXAMPLE.COM:
ipa service-add HTTP/`hostname`
ipa service-show HTTP/`hostname`

Retrieve a keytab for httpd service on idm-access:

```
ipa-getkeytab -p HTTP/`hostname` -k http.keytab -s idm-server.example.com
klist -kt http.keytab
```

Configure idm-access to use the keytab:

mv http.keytab /etc/httpd/conf/ chown apache:apache /etc/httpd/conf/http.keytab chmod 0400 /etc/httpd/conf/http.keytab service httpd restart

Access idm-client and run:

```
yum install firefox xorg-x11-xinit.x86_64
exit
ssh root@ idm-client.example.com -X
firefox
```

In Firefox, access idm-access.example.com/test, when you exit Firefox check:

klist

It might not work as selinux will deny the http-keytab.

```
Cd /root
grep httpd_t /var/log/audit/audit.log | audit2allow -m http-keytab > http-
keytab.te
grep httpd_t /var/log/audit/audit.log | audit2allow -M http-keytab
semodule -i http-keytab.pp
```

Now, check again Firefox, after authentication it should print:

```
Hello!
Received connection from 192.168.10.11
YAY! Kerberos authentication works!
Remote user is admin@EXAMPLE.COM
```

To Allow authentication for this small web application without password:

- In the address bar of Firefox, type 'about:config' to display the list of current configuration options.
- In the Filter field, type negotiate to restrict the list of options.
- Double-click the network.negotiate-auth.trusted-uris entry to display the Enter string value dialog box.
- Enter the name of the domain against which you want to authenticate, for example, example.com.
- Repeat the above procedure for the network.negotiate-auth.delegationuris entry, using the same domain.
- Restart Firefox, you should see the "YAY" message with no user-name and password.