mod05_ex01: Touring FreeIPA

The purpose of this exercise is to tour FreeIPA. IPA is a web UI combining many of the common Linux directory services. FreeIPA provides services for Identity Management, MIT Kerberos, Certificates, Domain Services, Network File System, and more. FreeIPA deploys a client to every host; this client is based on System Security Services Daemon (SSSD).

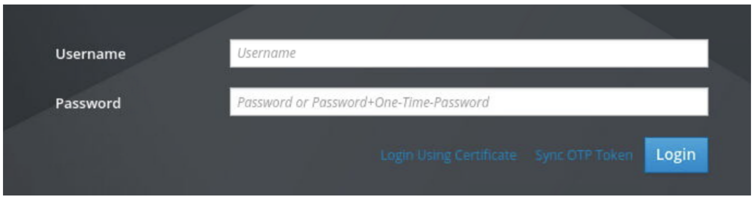
FreeIPA is the public source version of Redhat's IdM tool. It is designed and built from the ground up to support Linux based systems. It is used in this course due to the ease of use and ease of access.

Reference Information

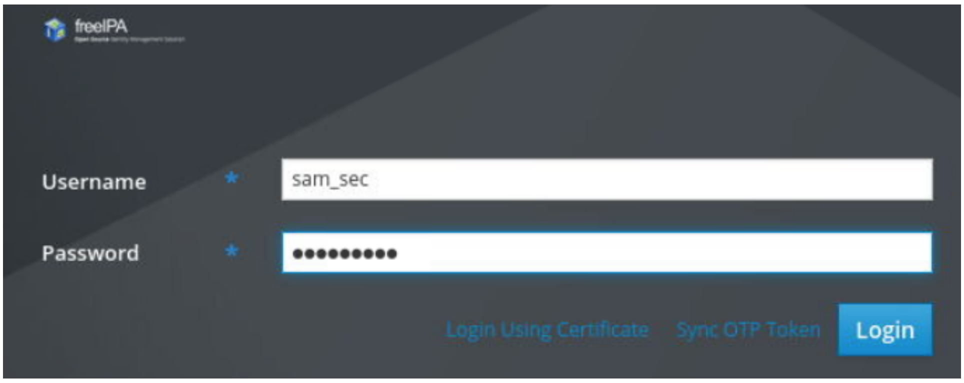
- TBD

1. Login into IPA as the security administrative user, sam_sec.

1.1 Select workspace 2. Open Firefox. On the Firefox bookmark toolbar select Identity Management. The IPA login screen will open.



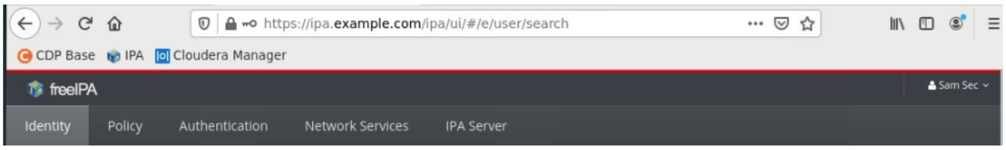
1.2 Login with the security administrative user, sam_sec, and password <password>. Click Login.



Username * sam_sec

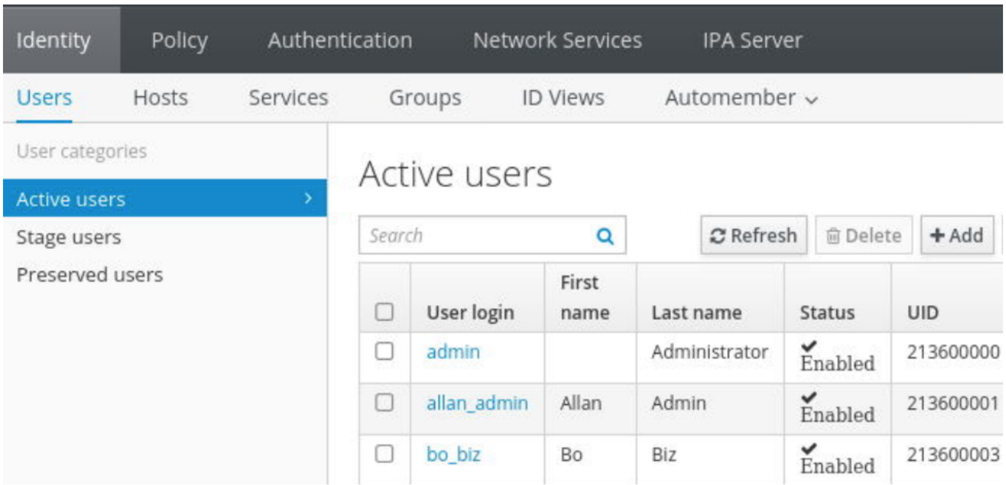
Password * ●●●●●●●●●●

1.3 The IPA tool bar has five tabs: Identity, Policy, Authentication, Network Services, and IPA Server.



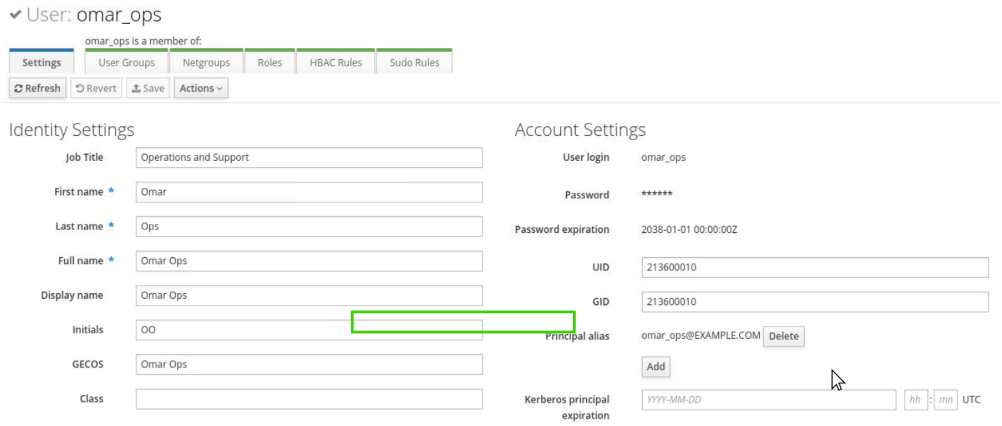
2. Tour Identity.

2.1 By default IPA opens to the list of users in Identity. The Identity tab manages users and groups. Review the list of users and groups, you will use several of them in future exercises. Select the user omar_ops.



□	User login	First name	Last name	Status	UID
□	admin		Administrator	✓ Enabled	213600000
□	allan_admin	Allan	Admin	✓ Enabled	213600001
□	bo_biz	Bo	Biz	✓ Enabled	213600003

2.2 IPA allows you to change many fields for a user. You cannot change the User Login. Notice the Principal alias for Kerberos is automatically created. Select Actions > Reset Password. Change the password to <password>. Click Reset Password.



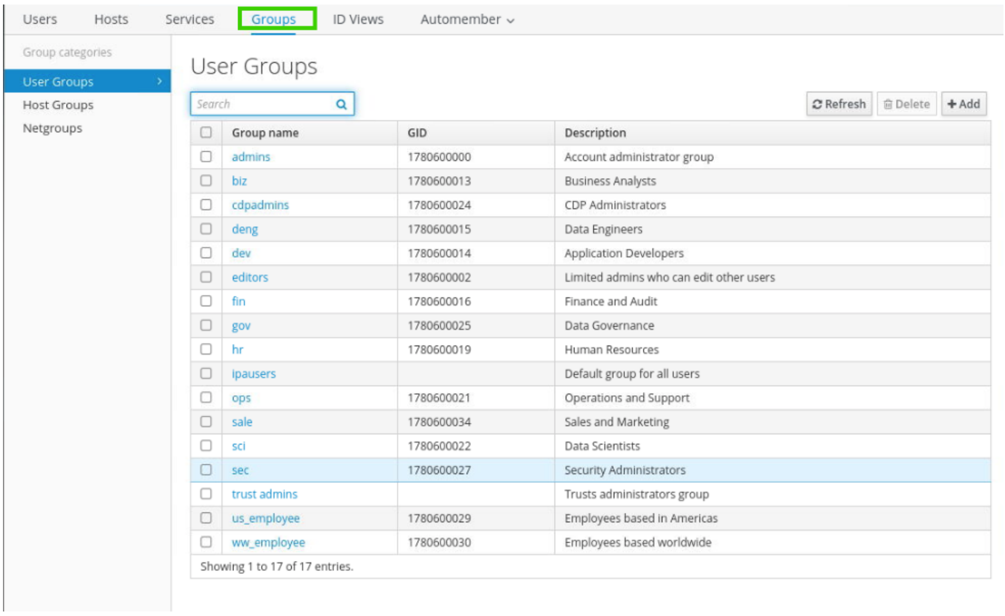
Identity Settings

Job Title	Operations and Support
First name *	Omar
Last name *	Ops
Full name *	Omar Ops
Display name	Omar Ops
Initials	OO
GECOS	Omar Ops
Class	

Account Settings

User login	omar_ops
Password	******
Password expiration	2038-01-01 00:00:00Z
UID	213600010
GID	213600010
Principal alias	omar_ops@EXAMPLE.COM Delete Add
Kerberos principal expiration	YYYY-MM-DD hh : mn UTC

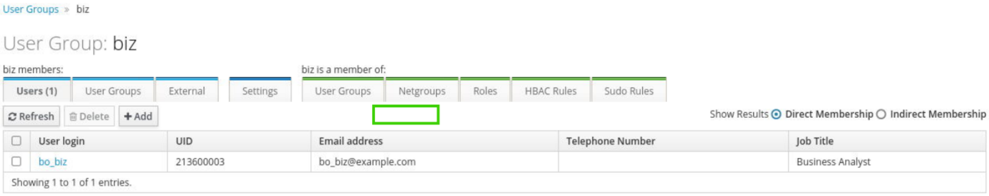
2.3 Select Groups. Select the group biz.



☐	Group name	GID	Description
☐	admins	1780600000	Account administrator group
☐	biz	1780600013	Business Analysts
☐	cdpadmins	1780600024	CDP Administrators
☐	deng	1780600015	Data Engineers
☐	dev	1780600014	Application Developers
☐	editors	1780600002	Limited admins who can edit other users
☐	fin	1780600016	Finance and Audit
☐	gov	1780600025	Data Governance
☐	hr	1780600019	Human Resources
☐	ipausers		Default group for all users
☐	ops	1780600021	Operations and Support
☐	sale	1780600034	Sales and Marketing
☐	sci	1780600022	Data Scientists
☐	sec	1780600027	Security Administrators
☐	trust admins		Trusts administrators group
☐	us_employee	1780600029	Employees based in Americas
☐	ww_employee	1780600030	Employees based worldwide

Showing 1 to 17 of 17 entries.

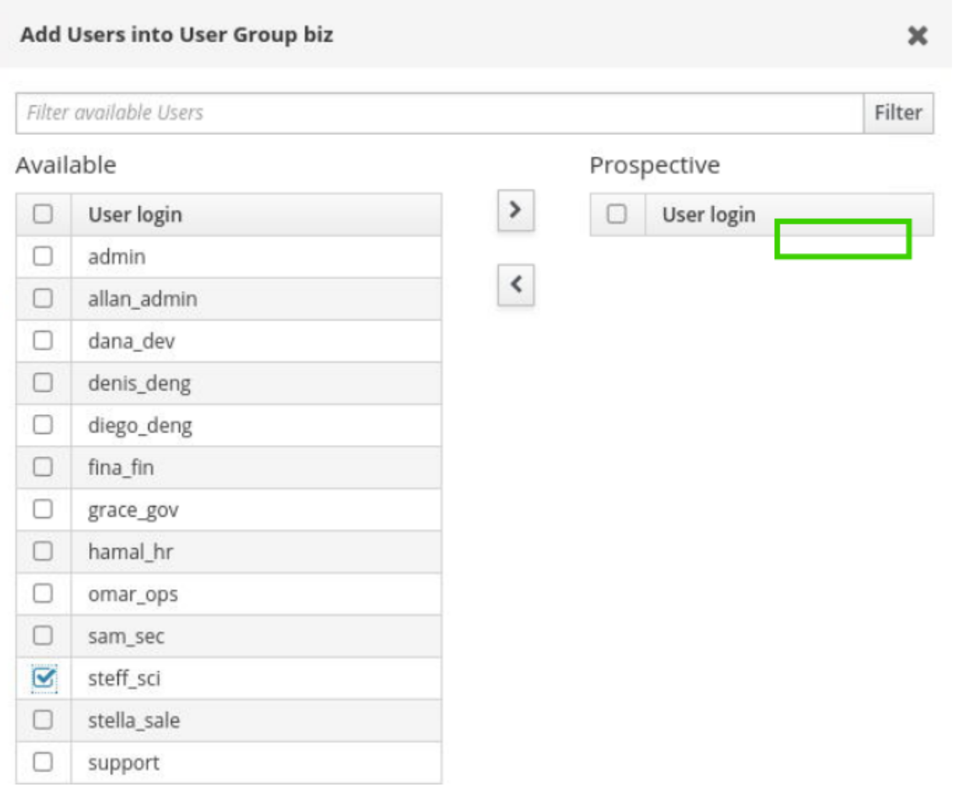
2.4 You will see the list of users assigned to the biz group.



☐	User login	UID	Email address	Telephone Number	Job Title
☐	bo_biz	213600003	bo_biz@example.com		Business Analyst

Showing 1 to 1 of 1 entries.

2.5 Click +Add. Click steff_sci. Click >. Click Add. The user steff_sci is now a member of the biz group.



Add Users into User Group biz

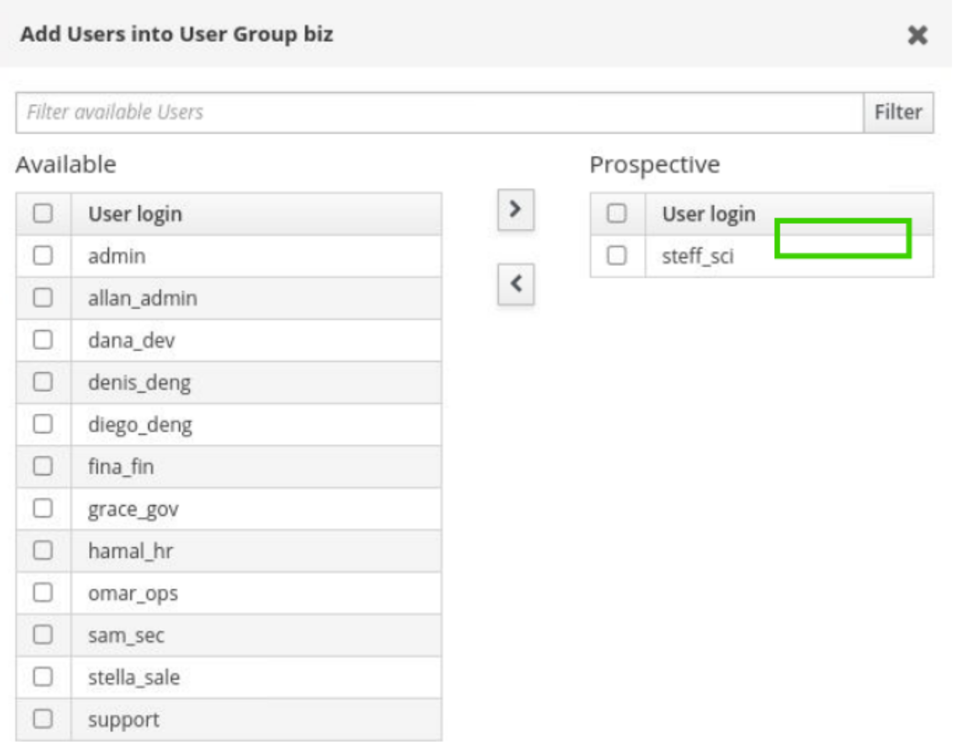
Available

□	User login
□	admin
□	allan_admin
□	dana_dev
□	denis_deng
□	diego_deng
□	fina_fin
□	grace_gov
□	hamal_hr
□	omar_ops
□	sam_sec
☑	steff_sci
□	stella_sale
□	support

Prospective

□	User login

2.6 Click Add. The user steff_sci is now a member of the biz group.



Add Users into User Group biz

Available

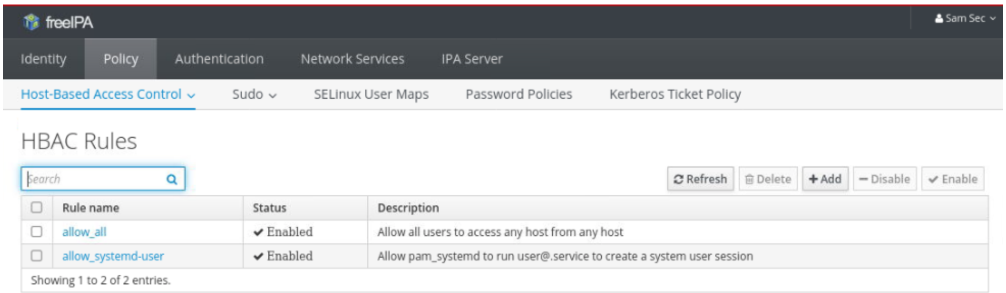
□	User login
□	admin
□	allan_admin
□	dana_dev
□	denis_deng
□	diego_deng
□	fina_fin
□	grace_gov
□	hamal_hr
□	omar_ops
□	sam_sec
□	stella_sale
□	support

Prospective

□	User login
□	steff_sci

3. Tour Policy.

3.1 On the IPA menu select Policy. The Policy tabs are Host-Based Access Control, Sudo, SELinux User Maps, Password Policy, and Kerberos Ticket Policy.

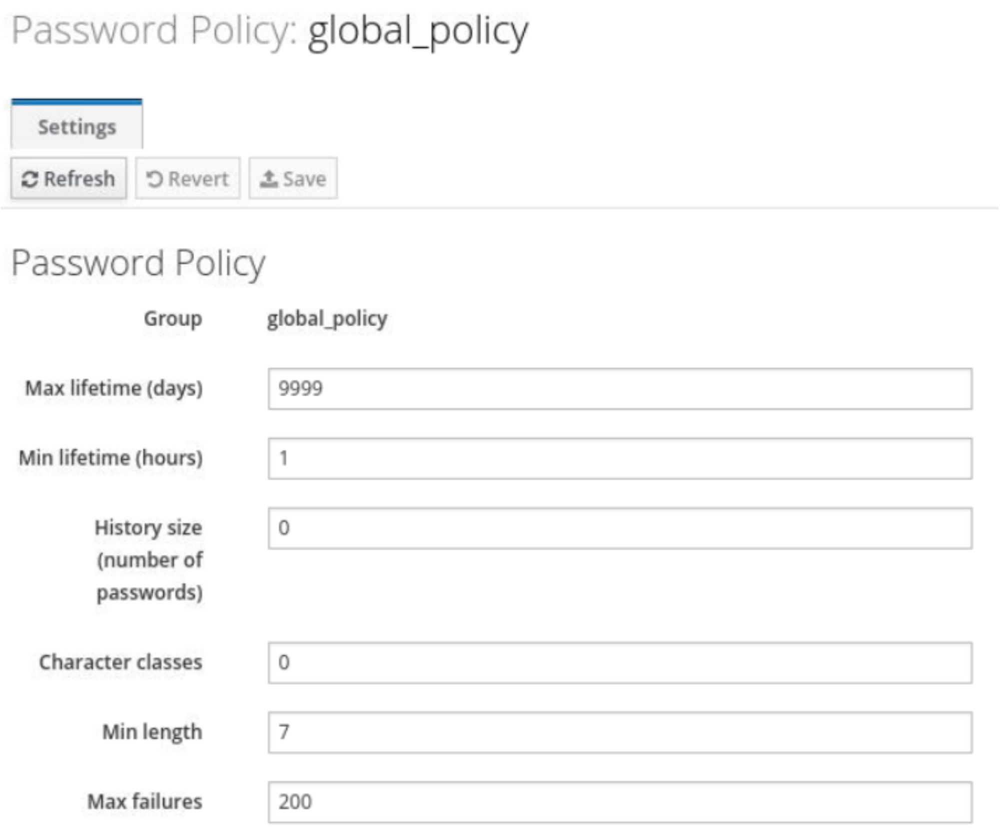


HBAC Rules

□	Rule name	Status	Description
□	allow_all	✓ Enabled	Allow all users to access any host from any host
□	allow_systemd-user	✓ Enabled	Allow pam_systemd to run user@.service to create a system user session

Showing 1 to 2 of 2 entries.

3.2 Click on the Password Policy tab. Click on global_policy. Review the properties for passwords. Do not make any changes.



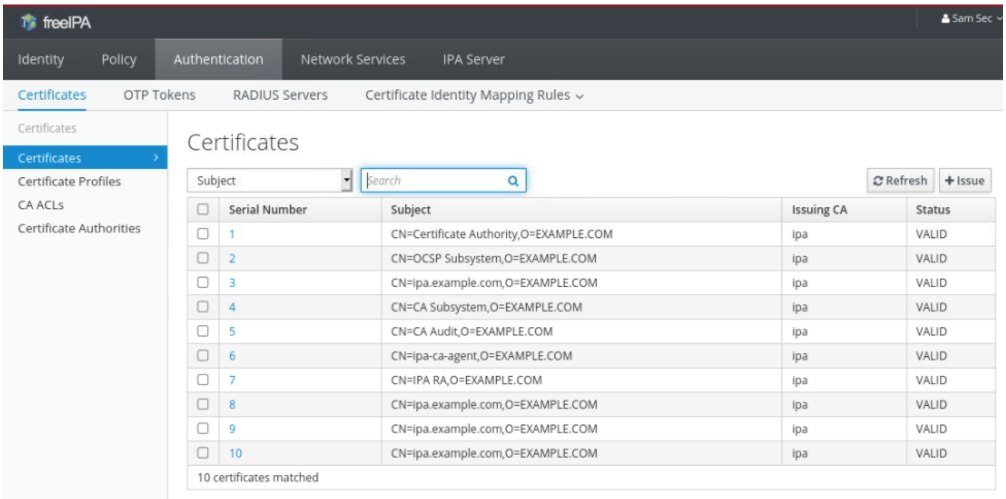
Password Policy: global_policy

Password Policy

Group	global_policy
Max lifetime (days)	9999
Min lifetime (hours)	1
History size (number of passwords)	0
Character classes	0
Min length	7
Max failures	200

4. Tour Authentication

4.1 On the IPA menu select Authentication. FreeIPA can act as a Certificate Authority. This pages lists the current certificates.



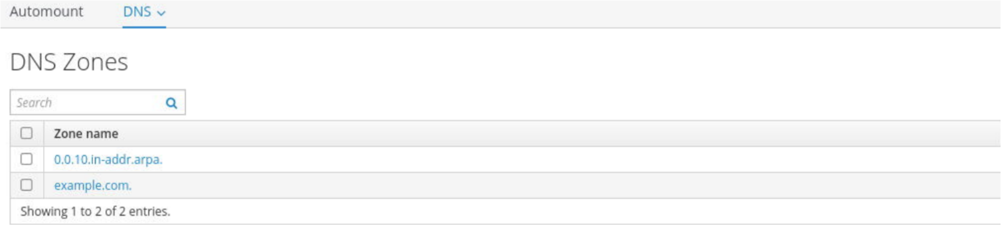
Certificates

□	Serial Number	Subject	Issuing CA	Status
□	1	CN=Certificate Authority,O=EXAMPLE.COM	ipa	VALID
□	2	CN=OCSP Subsystem,O=EXAMPLE.COM	ipa	VALID
□	3	CN=ipa.example.com,O=EXAMPLE.COM	ipa	VALID
□	4	CN=CA Subsystem,O=EXAMPLE.COM	ipa	VALID
□	5	CN=CA Audit,O=EXAMPLE.COM	ipa	VALID
□	6	CN=ipa-ca-agent,O=EXAMPLE.COM	ipa	VALID
□	7	CN=IPA RA,O=EXAMPLE.COM	ipa	VALID
□	8	CN=ipa.example.com,O=EXAMPLE.COM	ipa	VALID
□	9	CN=ipa.example.com,O=EXAMPLE.COM	ipa	VALID
□	10	CN=ipa.example.com,O=EXAMPLE.COM	ipa	VALID

10 certificates matched

5. Tour Network Services.

5.1 On the IPA menu select Network Services. IPA acts as our DNS server. DNS services are configured from this page. Select DNS > DNS Zones.

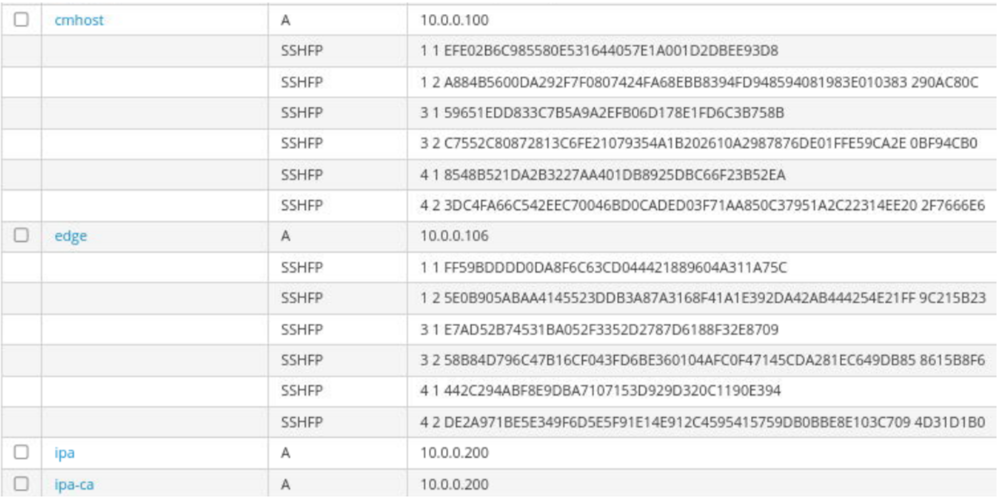


DNS Zones

□	Zone name
□	0.0.10.in-addr.arpa.
□	example.com.

Showing 1 to 2 of 2 entries.

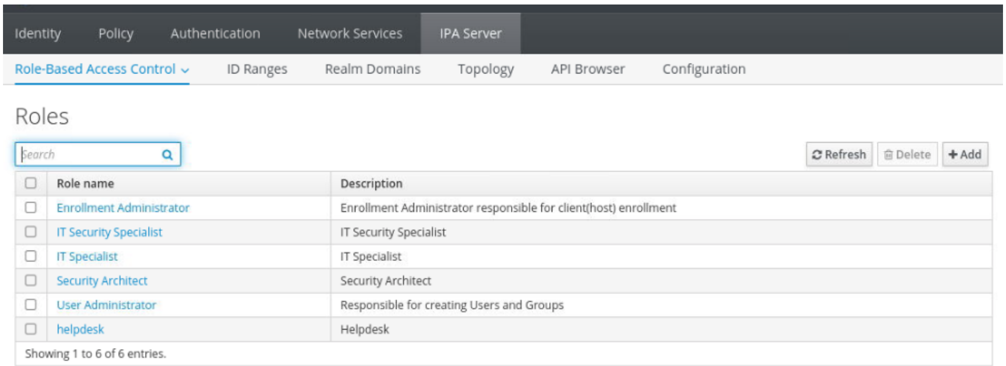
5.2 Select example.com. Review the list of records. Notice both the A records and the SSHFP records.



□	cmhost	A	10.0.0.100
		SSHFP	1 1 EFE02B6C985580E531644057E1A001D2DBEE93D8
		SSHFP	1 2 A884B5600DA292F7F0807424FA68EBB8394FD948594081983E010383 290AC80C
		SSHFP	3 1 59651EDD833C7B5A9A2EFB06D178E1FD6C3B758B
		SSHFP	3 2 C7552C80872813C6FE21079354A1B202610A2987876DE01FFE59CA2E 0BF94CB0
		SSHFP	4 1 8548B521DA2B3227AA401DB8925DBC66F23B52EA
		SSHFP	4 2 3DC4FA66C542EEC70046BD0CADED03F71AA850C37951A2C22314EE20 2F7666E6
□	edge	A	10.0.0.106
		SSHFP	1 1 FF59BDDDD0DA8F6C63CD044421889604A311A75C
		SSHFP	1 2 5E0B905ABAA4145523DDB3A87A3168F41A1E392DA42AB444254E21FF 9C215B23
		SSHFP	3 1 E7AD52B74531BA052F3352D2787D6188F32E8709
		SSHFP	3 2 58B84D796C47B16CF043FD6BE360104AFC0F47145CDA281EC649DB85 8615B8F6
		SSHFP	4 1 442C294ABF8E9DBA7107153D929D320C1190E394
		SSHFP	4 2 DE2A971BE5E349F6D5E5F91E14E912C4595415759DB0BBE8E103C709 4D31D1B0
□	ipa	A	10.0.0.200
□	ipa-ca	A	10.0.0.200

6. Tour IPA Server.

6.1 On the IPA menu select IPA Server. One unique capability for IPA is Role-Based Access Controls. Review the list of default roles. Select IT Specialist.

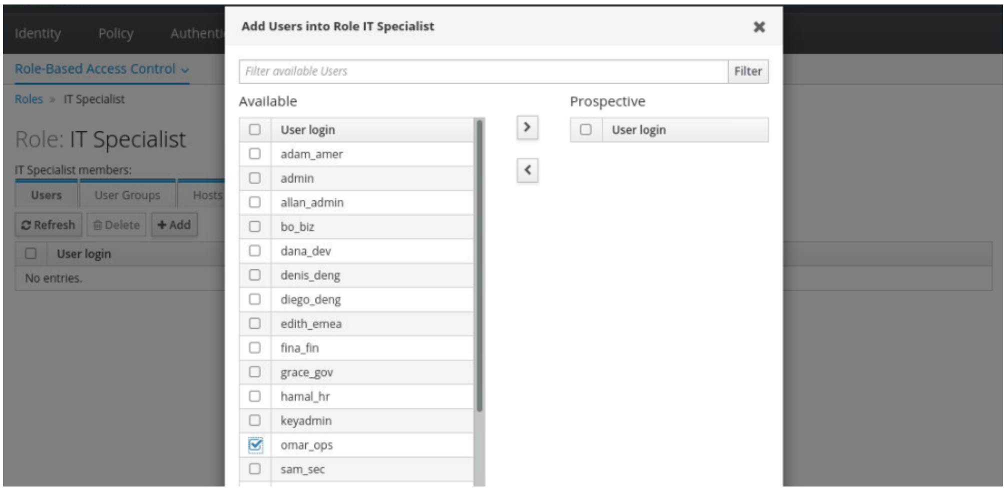


Roles

□	Role name	Description
□	Enrollment Administrator	Enrollment Administrator responsible for client(host) enrollment
□	IT Security Specialist	IT Security Specialist
□	IT Specialist	IT Specialist
□	Security Architect	Security Architect
□	User Administrator	Responsible for creating Users and Groups
□	helpdesk	Helpdesk

Showing 1 to 6 of 6 entries.

6.2 Assign a user to the role IT Specialist. Click + Add. Select omar_ops. Click >. Click Add.



□	User login
No entries.	

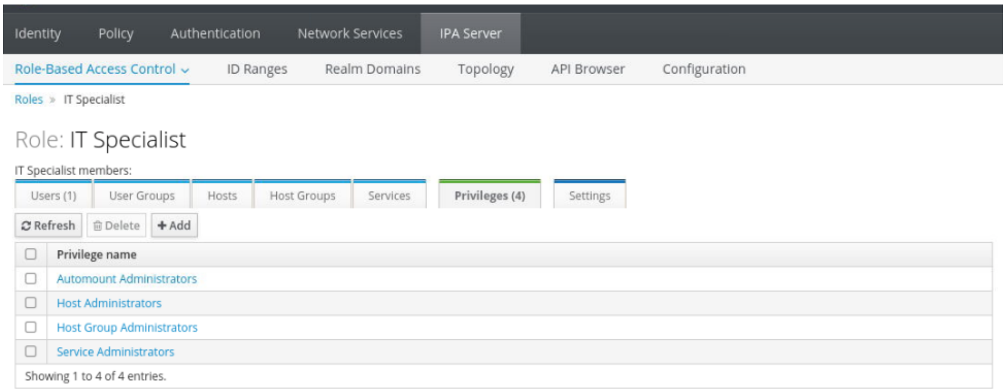
Available

□	User login
□	adam_amer
□	admin
□	allan_admin
□	bo_biz
□	dana_dev
□	denis_deng
□	diego_deng
□	edith_emea
□	fina_fin
□	grace_gov
□	hamal_hr
□	keyadmin
☑	omar_ops
□	sam_sec

Prospective

□	User login

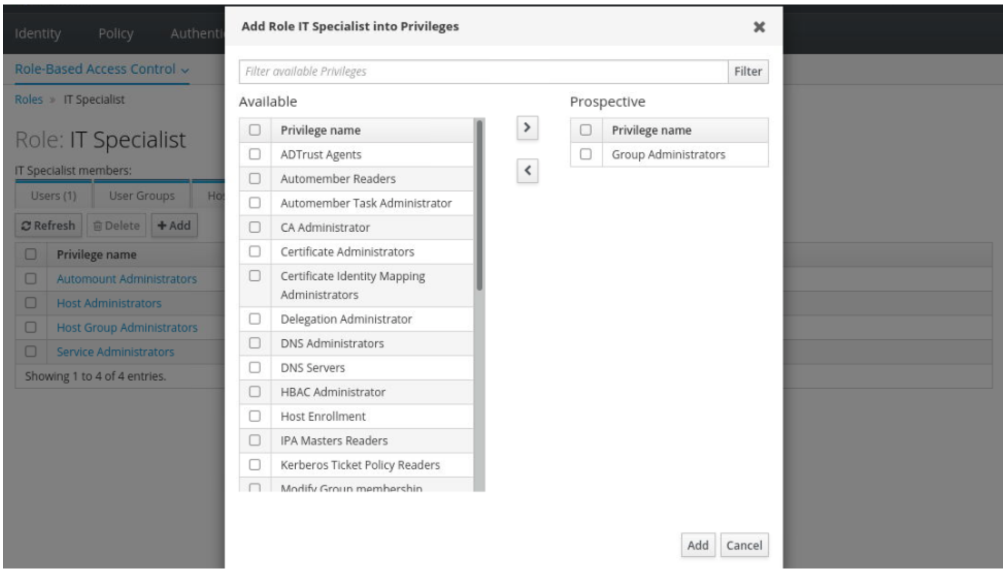
6.3 Select Privileges (4). Review the list of privileges assigned to the role IT Specialist. The IT Specialist is able to log into IPA to administrator hosts and groups.



□	Privilege name
□	Automount Administrators
□	Host Administrators
□	Host Group Administrators
□	Service Administrators

Showing 1 to 4 of 4 entries.

6.4 Click + Add. Review the list of all of the privileges. Add a new privilege to the IT specalist role. Select Group Administrators. Click >. Click Add.



Add Role IT Specialist into Privileges ✖

Filter available Privileges [Filter]

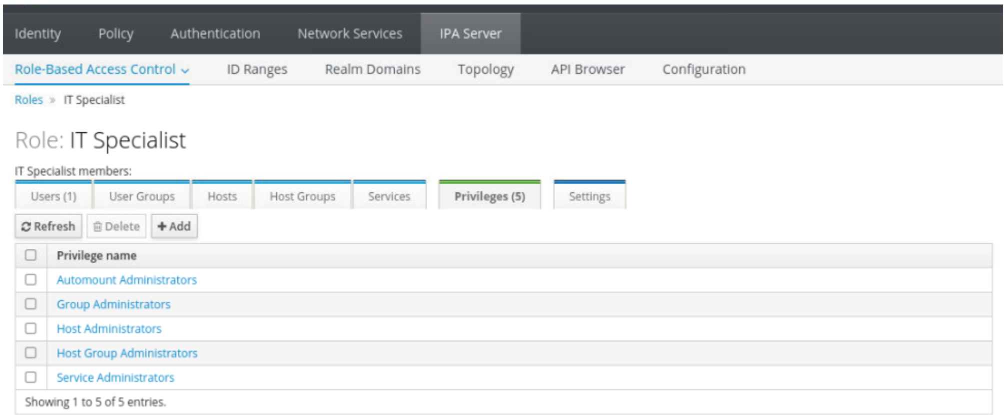
Available

□	Privilege name
□	ADTrust Agents
□	Automember Readers
□	Automember Task Administrator
□	CA Administrator
□	Certificate Administrators
□	Certificate Identity Mapping Administrators
□	Delegation Administrator
□	DNS Administrators
□	DNS Servers
□	HBAC Administrator
□	Host Enrollment
□	IPA Masters Readers
□	Kerberos Ticket Policy Readers
□	Modify Group membership

Prospective

□	Privilege name
□	Group Administrators

6.5 Review the list of privileges. Validate Host Group Administrators is now added to the role IT Specialist.



Role: IT Specialist

IT Specialist members:

□	Privilege name
□	Automount Administrators
□	Group Administrators
□	Host Administrators
□	Host Group Administrators
□	Service Administrators

Showing 1 to 5 of 5 entries.

7. In the upper right corner of IPA select the security administrative user, sam_sec. Select Logout.