



Red Hat IDM

Marc Skinner
Principal Solutions Architect

What is IDM?

IDM = Identity Management

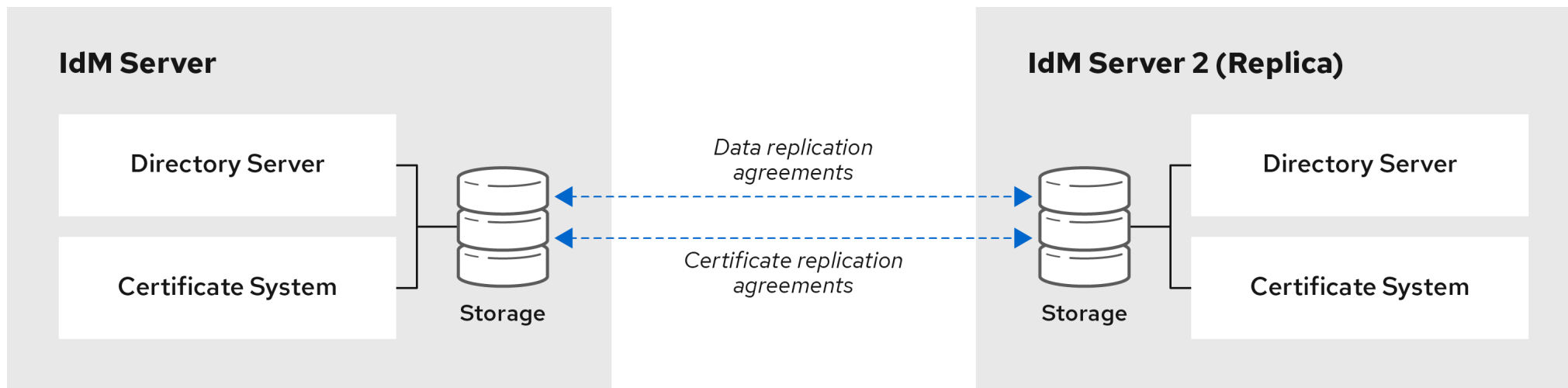
- IDM and IPA will be used interchangeably
- IPA = Identity, Policy and Audit

Top 5 Reasons to use IDM

- IDM is included in your RHEL subscription
 - Centralize / Secure / Comply
- IDM can act as a Domain Controller for RHEL servers
 - Trusted Identity Store
- IDM can integrate with your Microsoft environment
 - Single Source of Trust
- IDM can utilize MFA (Multi-Factor Authentication) for extra security
 - Hardware tokens / Smart Cards / Authentication Types
- IDM can leverage Policy Management
 - HBAC / RBAC / Delegation / Custom SUDO rules

IDM Architecture

IdM Architecture



64_RHEL_0120

IDM Installation

Preparation and Recommendations

- IPv6 protocol must be enabled in the kernel
- IPv6 does not need to be configured / enabled on the network
- Requires System-Wide cryptographic policy DEFAULT

```
# update-crypto-policies --show
```

```
# update-crypto-policies --set DEFAULT
```

- IDM can be installed with FIPS mode enabled
- RAM size matters!
 - 10k users and 100 groups requires 4 GB RAM
 - 100k users and 50k groups requires 16 GB RAM

Preparation and Recommendations

- Time is critical – make sure chronyd is running and time is accurate
- Ensure only 1 reverse DNS (PTR) record is associated with the IDM server
- IDM required firewall ports
 - HTTP/HTTPS : 80/443 : TCP
 - LDAP/LDAPS : 389/636 : TCP
 - Kerberos : 88/464 : TCP/UDP
 - DNS : 53 : TCP/UDP

Installation

- Configure firewalld

```
# firewall-cmd --permanent --add-port={80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp}
```

```
# firewall-cmd --permanent --add-service={freeipa-4,dns}
```

```
# firewall-cmd --reload
```

- Enable correct repositories

```
# subscription-manager repos --enable=rhel-9-for-x86_64-baseos-rpms
```

```
# subscription-manager repos --enable=rhel-9-for-x86_64-appstream-rpms
```

Pick your poison!



- **Installing an IdM server: With integrated DNS, with an integrated CA as the root CA**
- Installing an IdM server: With integrated DNS, with an external CA as the root CA
- Installing an IdM server: With integrated DNS, without a CA
- Installing an IdM server: Without integrated DNS, with an integrated CA as the root CA
- Installing an IdM server: Without integrated DNS, with an external CA as the root CA
- Installing an IdM server or replica with custom database settings from an LDIF file

Installation



- **Install IDM with integrated DNS**
dnf install ipa-server ipa-server-dns
- **Install IDM without integrated DNS**
dnf install ipa-server
- **Install IDM with AD trust integration**
dnf install ipa-server ipa-server-trust-ad samba-client
- **Display and ensure umask for root user is set to 0022 for all install methods**
umask
umask 0022

Integrated DNS with integrated CA as the root CA

```
# ipa-server-install
```

```
# ipa-server-install [ ... options ]
```

```
[root@idm1 ~]# ipa-server-install

The log file for this installation can be found in /var/log/ipaserver-install.log
=====
This program will set up the IPA Server.
Version 4.11.0

This includes:
  * Configure a stand-alone CA (dogtag) for certificate management
  * Configure the NTP client (chronyd)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)
  * Configure SID generation
  * Configure the KDC to enable PKINIT

To accept the default shown in brackets, press the Enter key.

Do you want to configure integrated DNS (BIND)? [no]: yes
```

```
Enter the fully qualified domain name of the computer
on which you're setting up server software. Using the form
<hostname>.<domainname>
Example: master.example.com
```

```
Server host name [idm1.rhlab.skinnerlabs.com]: idm1.idm.skinnerlabs.com
```

```
Warning: skipping DNS resolution of host idm1.idm.skinnerlabs.com
The domain name has been determined based on the host name.
```

```
Please confirm the domain name [idm.skinnerlabs.com]:
```

```
The kerberos protocol requires a Realm name to be defined.
This is typically the domain name converted to uppercase.
```

```
Please provide a realm name [IDM.SKINNERLABS.COM]:
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and has full access
to the Directory for system management tasks and will be added to the
instance of directory server created for IPA.
The password must be at least 8 characters long.
```

```
Directory Manager password:
Password (confirm):
```

```
The IPA server requires an administrative user, named 'admin'.
This user is a regular system account used for IPA server administration.
```

```
IPA admin password:
Password (confirm):
```

```
Checking DNS domain idm.skinnerlabs.com., please wait ...
Please provide the IP address to be used for this host name: 192.168.40.201
```

```
Do you want to configure DNS forwarders? [yes]:
Following DNS servers are configured in /etc/resolv.conf: 192.168.33.31, 192.168.33.32
Do you want to configure these servers as DNS forwarders? [yes]:
All detected DNS servers were added. You can enter additional addresses now:
Enter an IP address for a DNS forwarder, or press Enter to skip:
DNS forwarders: 192.168.33.31, 192.168.33.32
Checking DNS forwarders, please wait ...
Do you want to search for missing reverse zones? [yes]:
Reverse record for IP address 192.168.40.201 already exists
Trust is configured but no NetBIOS domain name found, setting it now.
Enter the NetBIOS name for the IPA domain.
Only up to 15 uppercase ASCII letters, digits and dashes are allowed.
Example: EXAMPLE.

NetBIOS domain name [IDM]:

Do you want to configure chrony with NTP server or pool address? [no]:

The IPA Master Server will be configured with:
Hostname:      idm1.idm.skinnerlabs.com
IP address(es): 192.168.40.201
Domain name:   idm.skinnerlabs.com
Realm name:    IDM.SKINNERLABS.COM

The CA will be configured with:
Subject DN:    CN=Certificate Authority,O=IDM.SKINNERLABS.COM
Subject base:  O=IDM.SKINNERLABS.COM
Chaining:     self-signed

BIND DNS server will be configured to serve IPA domain with:
Forwarders:    192.168.33.31, 192.168.33.32
Forward policy: only
Reverse zone(s): No reverse zone

Continue to configure the system with these values? [no]: yes
```



```
=====
```

```
Setup complete
```

```
Next steps:
```

1. You must make sure these network ports are open:

```
TCP Ports:
```

- * 80, 443: HTTP/HTTPS
- * 389, 636: LDAP/LDAPS
- * 88, 464: kerberos
- * 53: bind

```
UDP Ports:
```

- * 88, 464: kerberos
- * 53: bind
- * 123: ntp

2. You can now obtain a kerberos ticket using the command: 'kinit admin'
This ticket will allow you to use the IPA tools (e.g., ipa user-add)
and the web user interface.

```
Be sure to back up the CA certificates stored in /root/cacert.p12  
These files are required to create replicas. The password for these  
files is the Directory Manager password  
The ipa-server-install command was successful  
[root@idm1 ~]#
```

Installation Log Files

/var/log/ipaserver-install.log

/var/log/httpd/error_log

/var/log/dirsrv/slapd-INSTANCE-NAME/access

/var/log/dirsrv/slapd-INSTANCE-NAME/errors

/var/log/pki/pki-ca-spawn.\$TIME_OF_INSTALLATION.log

/var/log/pki/pki-tomcat/ca/debug.\$DATE.log

/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit

Upgrades

```
# dnf upgrade ipa-*
```

- When updating multiple IDM servers, wait 10 minutes between servers, so post-upgrade data/replication can finish successfully

NOTE : all servers will receive any schema updates after first IDM server is updated

Uninstall

```
# ipa-server-install --uninstall
```

IDM Client Installation

Supported RHEL Versions

- RHEL 7, 8

```
# yum install ipa-client
```

- RHEL 9

```
# dnf install ipa-client
```

- Interactive Install using admin account

```
# dnf install ipa-client
```

```
# ipa-client-install --enable-dns-updates --mkhomedir
```

```
[root@rhel9-1 ~]# ipa-client-install --enable-dns-updates --mkhomedir
This program will set up IPA client.
Version 4.11.0

Discovery was successful!
Do you want to configure chrony with NTP server or pool address? [no]:
Client hostname: rhel9-1.idm.skinnerlabs.com
Realm: IDM.SKINNERLABS.COM
DNS Domain: idm.skinnerlabs.com
IPA Server: idm1.idm.skinnerlabs.com
BaseDN: dc=idm,dc=skinnerlabs,dc=com

Continue to configure the system with these values? [no]: yes
```

```
Synchronizing time
No SRV records of NTP servers found and no NTP server or pool address was provided.
Using default chrony configuration.
Attempting to sync time with chronyc.
Time synchronization was successful.
User authorized to enroll computers: admin
Password for admin@IDM.SKINNERLABS.COM:
Successfully retrieved CA cert
    Subject:      CN=Certificate Authority,0=IDM.SKINNERLABS.COM
    Issuer:       CN=Certificate Authority,0=IDM.SKINNERLABS.COM
    Valid From:   2024-05-16 18:27:17+00:00
    Valid Until:  2044-05-16 18:27:17+00:00

Enrolled in IPA realm IDM.SKINNERLABS.COM
Created /etc/ipa/default.conf
Configured /etc/sss/sss.conf
Systemwide CA database updated.
Hostname (rhel9-1.idm.skinnerlabs.com) does not have A/AAAA record.
Incorrect reverse record(s):
192.168.40.96 is pointing to rhel9-1.rhlab.skinnerlabs.com. instead of rhel9-1.idm.skinnerlabs.com.
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config.d/04-ipa.conf
Configuring idm.skinnerlabs.com as NIS domain.
Configured /etc/krb5.conf for IPA realm IDM.SKINNERLABS.COM
Client configuration complete.
The ipa-client-install command was successful
[root@rhel9-1 ~]#
```


- Interactive Install using one-time password
- On IDM Server request admin Kerberose Ticket to provide access for command line changes

```
# kinit admin
```

```
# klist
```

- On IDM Server add host and set one-time password

```
# ipa host-add rhel-2.idm.skinnerlabs.com --random
```



```
[root@idm1 ~]# ipa host-add rhel9-2.idm.skinnerlabs.com --random
-----
Added host "rhel9-2.idm.skinnerlabs.com"
-----
Host name: rhel9-2.idm.skinnerlabs.com
Random password: 3Ys0mUm0uhGEk2efj4an4pn
Password: True
Keytab: False
Managed by: rhel9-2.idm.skinnerlabs.com
```

- Host appears in IDM but NOT Enrolled

Hosts

Search 

 Refresh  Delete

<input type="checkbox"/>	Host name	Description	Enrolled
<input type="checkbox"/>	idm1.idm.skinnerlabs.com		True
<input type="checkbox"/>	rhel9-1.idm.skinnerlabs.com		True
<input type="checkbox"/>	rhel9-2.idm.skinnerlabs.com		

Showing 1 to 3 of 3 entries.



- Interactive Install using one-time password

```
# dnf install ipa-client
```

```
# ipa-client-install --enable-dns-updates --mkhomedir --password "3YsOmUmOuhGEk2efj4an4pn"
```

```
[root@rhel9-2 ~]# ipa-client-install --enable-dns-updates --mkhomedir --password "3Ys0mUm0uhGEk2efj4an4pn"
This program will set up IPA client.
Version 4.11.0


Discovery was successful!
Do you want to configure chrony with NTP server or pool address? [no]:
Client hostname: rhel9-2.idm.skinnerlabs.com
Realm: IDM.SKINNERLABS.COM
DNS Domain: idm.skinnerlabs.com
IPA Server: idm1.idm.skinnerlabs.com
BaseDN: dc=idm,dc=skinnerlabs,dc=com



Continue to configure the system with these values? [no]: yes
Synchronizing time
No SRV records of NTP servers found and no NTP server or pool address was provided.
Using default chrony configuration.
Attempting to sync time with chronyc.
Time synchronization was successful.
Do you want to download the CA cert from http://idm1.idm.skinnerlabs.com/ipa/config/ca.crt ?
(this is INSECURE) [no]: yes
Successfully retrieved CA cert
    Subject:      CN=Certificate Authority,0=IDM.SKINNERLABS.COM
    Issuer:       CN=Certificate Authority,0=IDM.SKINNERLABS.COM
    Valid From:   2024-05-16 18:27:17+00:00
    Valid Until:  2044-05-16 18:27:17+00:00

Enrolled in IPA realm IDM.SKINNERLABS.COM
Created /etc/ipa/default.conf
Configured /etc/sss/sss.conf
Systemwide CA database updated.
Incorrect reverse record(s):
192.168.40.97 is pointing to rhel9-2.rhlab.skinnerlabs.com. instead of rhel9-2.idm.skinnerlabs.com.
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Principal is not set when enrolling with OTP or PKINIT; using principal 'admin@idm.skinnerlabs.com' for 'getent passwd'.
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config.d/04-ipa.conf
Configuring idm.skinnerlabs.com as NIS domain.
Configured /etc/krb5.conf for IPA realm IDM.SKINNERLABS.COM
Client configuration complete.
The ipa-client-install command was successful
```

- Host appears in IDM and is NOW Enrolled


Hosts

Search 

 Refresh  Delete

<input type="checkbox"/>	Host name	Description	Enrolled
<input type="checkbox"/>	idm1.idm.skinnerlabs.com		True
<input type="checkbox"/>	rhel9-1.idm.skinnerlabs.com		True
<input type="checkbox"/>	rhel9-2.idm.skinnerlabs.com		True

Showing 1 to 3 of 3 entries.



Kickstart Support

- On IDM Server request admin Kerberose Ticket to provide access for command line changes

```
# kinit admin
```

```
# klist
```

- On IDM Server add host and set password

```
# ipa host-add server-name.idm.skinnerlabs.com --password=MYSECRET
```

Kickstart Support

- Add “ipa-client” under Kickstart %packages section
- Add following snippet into Kickstart Post section:

```
%post --log=/root/ks-post.log
```

```
# Generate SSH keys; ipa-client-install uploads them to the IdM server by default
```

```
/usr/libexec/openssh/sshd-keygen rsa
```

```
/usr/sbin/ipa-client-install --hostname=client.example.com --domain=EXAMPLE.COM --  
enable-dns-updates --mkhomedir -w secret --realm=EXAMPLE.COM --  
server=server.example.com --unattended --password=MYSECRET
```

IDM Client Uninstall

- Client Side

```
# ipa-client-install --uninstall
```

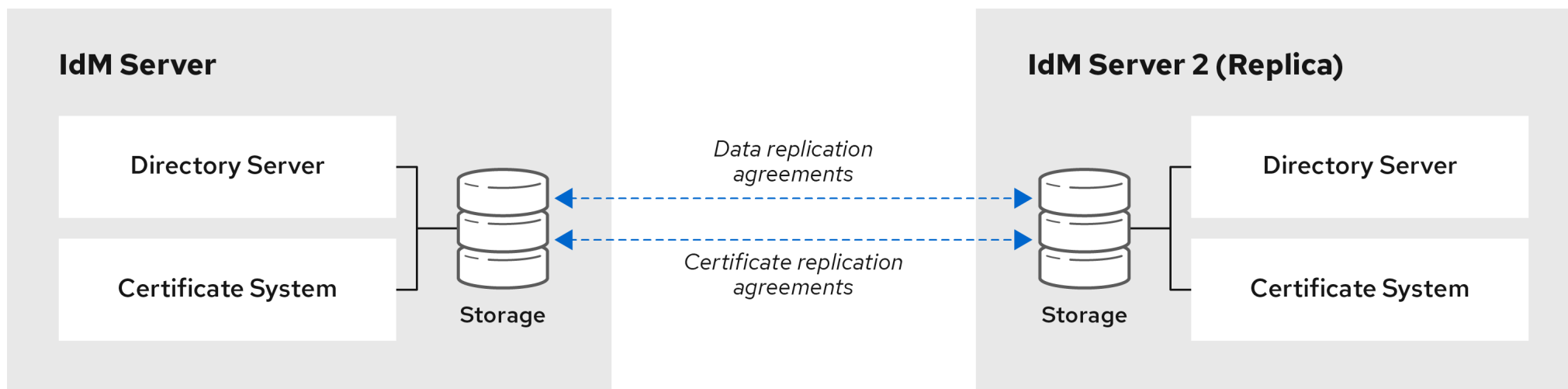
- IDM Server Side

```
# ipa dnsrecord-del
```

```
# ipa host-del CLIENT.FQDN.COM
```

IDM Replica Install

IDM Topology – game plan



64_RHEL_0120

NOTE: Red Hat supports up to 60 replicas

Pick your poison, again!

- Installing an IdM replica: With integrated DNS, with an integrated CA as the root CA
- Installing an IdM replica: With integrated DNS, with an external CA as the root CA
- Installing an IdM replica: With integrated DNS, without a CA
- Installing an IdM replica: Without integrated DNS, with an integrated CA as the root CA
- Installing an IdM replica: Without integrated DNS, with an external CA as the root CA

IDM Replica Preparation

- Enroll new host as IDM Client

```
# ipa-client-install --enable-dns-updates --mkhomedir
```

- Configure firewalld

```
# firewall-cmd --permanent --add-port={80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp}
```

```
# firewall-cmd --permanent --add-service={freeipa-4,dns}
```

```
# firewall-cmd --reload
```

● Install Replica

```
# ipa-replica-install --setup-dns --forwarder 192.168.40.201 --setup-ca
```

```
Configuring SID generation
 [1/7]: adding RID bases
RID bases already set, nothing to do
 [2/7]: creating samba domain object
Samba domain object already exists
 [3/7]: adding admin(group) SIDs
Admin SID already set, nothing to do
Admin group SID already set, nothing to do
 [4/7]: updating Kerberos config
'dns_lookup_kdc' already set to 'true', nothing to do.
 [5/7]: activating sidgen task
 [6/7]: restarting Directory Server to take MS PAC and LDAP plugins changes into account
 [7/7]: adding fallback group
Fallback group already set, nothing to do
Done.
```

IDM Replica Testing

- Test Replica by adding a user from IDM2 Server [replica]

```
# ipa user-add dvader
```

```
[root@idm2 ~]# kinit admin
Password for admin@IDM.SKINNERLABS.COM:
[root@idm2 ~]# ipa user-add dvader
First name: Darth
Last name: Vader
-----
Added user "dvader"
-----
User login: dvader
First name: Darth
Last name: Vader
Full name: Darth Vader
Display name: Darth Vader
Initials: DV
Home directory: /home/dvader
GECOS: Darth Vader
Login shell: /bin/sh
Principal name: dvader@IDM.SKINNERLABS.COM
Principal alias: dvader@IDM.SKINNERLABS.COM
Email address: dvader@idm.skinnerlabs.com
UID: 487500500
GID: 487500500
Password: False
Member of groups: ipausers
Kerberos keys available: False
```

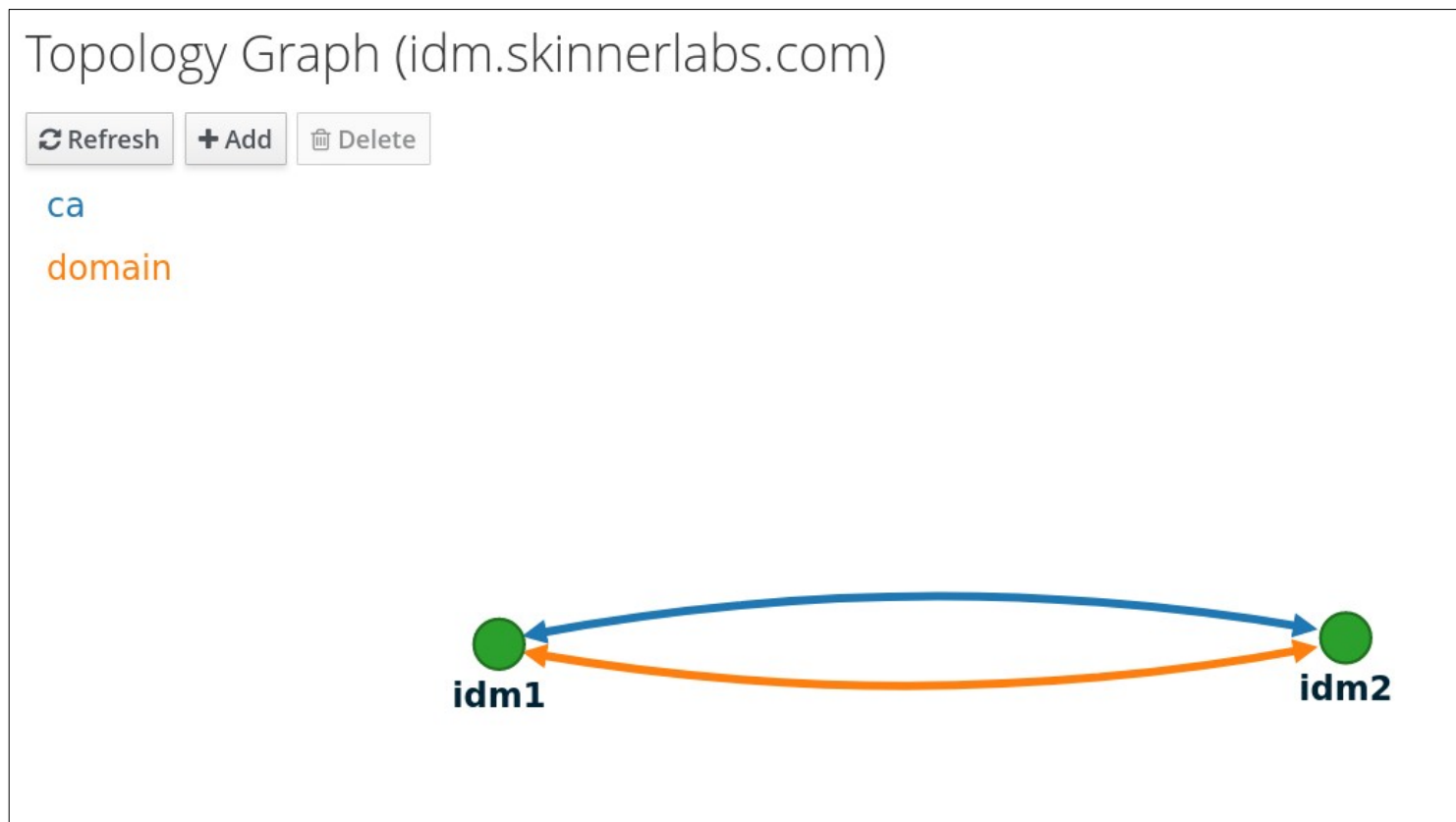
IDM Replica Testing

- Test Replica by listing a user from IDM1 Server

```
# ipa user-show dvader
```

```
[root@idm1 etc]# ipa user-show dvader
User login: dvader
First name: Darth
Last name: Vader
Home directory: /home/dvader
Login shell: /bin/sh
Principal name: dvader@IDM.SKINNERLABS.COM
Principal alias: dvader@IDM.SKINNERLABS.COM
Email address: dvader@idm.skinnerlabs.com
UID: 487500500
GID: 487500500
Account disabled: False
Password: False
Member of groups: ipausers
Kerberos keys available: False
```

IDM Topology – we did it!



IDM Client Resilience



- SSSD configured
- ipa_server is auto-configured for DNS lookup
- Requests SRV record for IDM server

```
[root@rhel9-1 ~]# cat /etc/sss/sss.conf
[domain/idm.skinnerlabs.com]

id_provider = ipa
ipa_server = _srv_, idm1.idm.skinnerlabs.com
ipa_domain = idm.skinnerlabs.com
ipa_hostname = rhel9-1.idm.skinnerlabs.com
auth_provider = ipa
chpass_provider = ipa
access_provider = ipa
cache_credentials = True
ldap_tls_cacert = /etc/ipa/ca.crt
dyndns_update = True
dyndns_iface = enp1s0
krb5_store_password_if_offline = True

[sss]
domains = idm.skinnerlabs.com
config_file_version = 2
services = nss, pam, ssh, sudo
[ssh]

[sudo]

[nss]
homedir_substring = /home

[pam]
```

IDM Healthcheck

IDM Healthcheck Tool

- Run Check on IDM1 and IDM2

```
# ipa-healthcheck --failures-only
```

```
[root@idm2 ~]# ipa-healthcheck --failures-only
[
  {
    "source": "ipahealthcheck.ipa.idns",
    "check": "IPADNSSystemRecordsCheck",
    "result": "WARNING",
    "uuid": "94b20af5-8675-455e-b5b3-504316dc22f6",
    "when": "20240517184946Z",
    "duration": "0.284013",
    "kw": {
      "key": "ipa_ca_missing_idm1.idm.skinnerlabs.com",
      "server": "idm1.idm.skinnerlabs.com",
      "msg": "missing IP address for ipa-ca server {server}"
    }
  },
  {
    "source": "ipahealthcheck.ipa.idns",
    "check": "IPADNSSystemRecordsCheck",
    "result": "WARNING",
    "uuid": "bdd574b2-f54c-4c84-bacc-8562f72e7cf9",
    "when": "20240517184946Z",
    "duration": "0.284034",
    "kw": {
      "key": "ipa_ca_missing_idm2.idm.skinnerlabs.com",
      "server": "idm2.idm.skinnerlabs.com",
      "msg": "missing IP address for ipa-ca server {server}"
    }
  }
]
```

IDM Backups

IDM Backup and Restore

- Create an IDM backup

```
# ipa-backup
```

- Backup defaults to offline and saves backup data into `/var/lib/ipa/backup/`

- Restore

```
# ipa-restore /var/lib/ipa/backup/ipa-full-2024-05-17-15-08-27
```

IDM and Ansible

IDM and Ansible

- Install FreeIPA Ansible Roles (NOT part of RHEL System Roles)

```
# dnf install ansible-freeipa
```

- Ansible Roles [ipaclient / ipareplica / ipaserver]

```
/usr/share/ansible/roles/
```

- Documentation and Playbooks

```
/usr/share/doc/ansible-freeipa/
```

```
/usr/share/doc/ansible-freeipa/playbooks/
```

IDM and Web UI

IDM Web UI

- Web browser to <http://idm1.idm.skinnerlabs.com>

The screenshot shows the login interface for Red Hat Identity Management. At the top, it reads "RED HAT® IDENTITY MANAGEMENT". Below this, there are two input fields: "Username" with a placeholder "Username" and "Password" with a placeholder "Password or Password+One-Time Password". At the bottom right, there are three options: "Log In Using Certificate", "Sync OTP Token", and a blue "Log in" button.

IDM Web UI : Identity : Users

Identity Policy Authentication Network Services IPA Server

Users Hosts Services Groups ID Views Automember ▾ Subordinate IDs ▾


User categories







Active users >

Stage users

Preserved users

Active users

Search 

 Refresh  Delete  Add  Disable  Enable  Actions ▾

<input type="checkbox"/>	User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
<input type="checkbox"/>	admin		Administrator	✓ Enabled	487400000			
<input type="checkbox"/>	dvader	Darth	Vader	✓ Enabled	487500500	dvader@idm.skinnerlabs.com		

Showing 1 to 2 of 2 entries.

IDM Web UI : Identity : Hosts

- Identity
 - Policy
 - Authentication
 - Network Services
 - IPA Server
- Users
 - Hosts**
 - Services
 - Groups
 - ID Views
 - Automember ▾
 - Subordinate IDs ▾

Hosts

Refresh Delete Add Actions ▾

<input type="checkbox"/>	Host name	Description	Enrolled
<input type="checkbox"/>	idm1.idm.skinnerlabs.com		True
<input type="checkbox"/>	idm2.idm.skinnerlabs.com		True
<input type="checkbox"/>	rhel9-1.idm.skinnerlabs.com		True
<input type="checkbox"/>	rhel9-2.idm.skinnerlabs.com		True

Showing 1 to 4 of 4 entries.

IDM Web UI : Identity : Groups : Users


Identity Policy Authentication Network Services IPA Server




Users Hosts Services **Groups** ID Views Automember ▾ Subordinate IDs ▾

Group categories

- User Groups >
- Host Groups
- Netgroups

User Groups

Search 

 Refresh  Delete  Add

<input type="checkbox"/>	Group name	GID	Description
<input type="checkbox"/>	admins	487400000	Account administrators group
<input type="checkbox"/>	editors	487400002	Limited admins who can edit other users
<input type="checkbox"/>	ipausers		Default group for all users
<input type="checkbox"/>	trust admins		Trusts administrators group

Showing 1 to 4 of 4 entries.

IDM Web UI : Identity : Groups : Host

Identity Policy Authentication Network Services IPA Server

Users Hosts Services **Groups** ID Views Automember Subordinate IDs

Group categories

User Groups

Host Groups >

Netgroups

Host Groups

Search

Refresh Delete Add

<input type="checkbox"/>	Host-group	Description
<input type="checkbox"/>	ipaservers	IPA server hosts
<input type="checkbox"/>	rhel9_servers	All RHEL9 Servers

Showing 1 to 2 of 2 entries.

IDM Web UI : Policy : HBAC

[Identity](#)[Policy](#)[Authentication](#)[Network Services](#)[IPA Server](#)[Host-Based Access Control](#) ▾[Sudo](#) ▾[SELinux User Maps](#)[Password Policies](#)[Kerberos Ticket Policy](#)[Passkey Configuration](#)

HBAC Rules

[Refresh](#)[Delete](#)[+ Add](#)[- Disable](#)[✓ Enable](#)

<input type="checkbox"/>	Rule name	Status	Description
<input type="checkbox"/>	allow_all	✓ Enabled	Allow admin to access any host from any host
<input type="checkbox"/>	allow_systemd-user	✓ Enabled	Allow pam_systemd to run user@.service to create a system user session
<input type="checkbox"/>	allow_users	✓ Enabled	Allow all users of group ipausers to access only rhel9-1 and rhel9-2 hosts

Showing 1 to 3 of 3 entries.

HBAC : Edit allow_all

- Reconfigure allow_all HBAC Rule to only allow admin user
- Change “Who” from Anyone to Specific Users and Groups

✓ HBAC Rule: allow_all

Settings

Refresh Revert Save Actions

General

Rule name allow_all

Description Allow admin to access any host from any host

Who

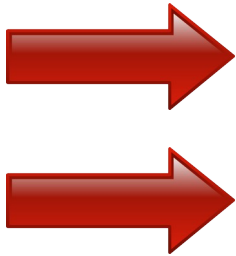
User category the rule applies to: Anyone Specified Users and Groups

- Users Delete Add
- admin
- User Groups Delete Add

Accessing

Host category the rule applies to: Any Host Specified Hosts and Groups

- Hosts Delete Add
- Host Groups Delete Add



HBAC : Create allow_users

- Create new HBAC rule to only allow Specified Users and Groups to access Specified Hosts and Groups
- Add ipausers Users Group to “Who”
- Add rhel9_server Host Group to “Accessing”

✓ HBAC Rule: allow_users

Settings

[Refresh](#) [Revert](#) [Save](#) [Actions](#) ▾

General

Rule name allow_users

Description Allow all users of group ipausers to access only rhel9-1 and rhel9-2 hosts

Who

User category the rule applies to: Anyone Specified Users and Groups

- Users Delete + Add
- User Groups Delete + Add
 - ipausers



Accessing

Host category the rule applies to: Any Host Specified Hosts and Groups

- Hosts Delete + Add
- Host Groups Delete + Add
 - rhel9_servers



IDM Web UI : Policy : Sudo

Identity Policy Authentication Network Services IPA Server

Host-Based Access Control **Sudo** SELinux User Maps Password Policies Kerberos Ticket Policy

Passkey Configuration

- Sudo Rules
- Sudo Commands
- Sudo Command Groups

Sudo Rules

Refresh Delete Add Disable Enable

<input type="checkbox"/>	Rule name	Sudo order	Status	Description
<input type="checkbox"/>	Allow_Reboot_RHEL9		✓ Enabled	




Showing 1 to 1 of 1 entries.

IDM Web UI : Policy : Sudo Commands

- Identity
- Policy**
 - Host-Based Access Control ▾
 - Sudo ▾
 - SELinux User Maps
 - Password Policies
 - Kerberos Ticket Policy
- Authentication
- Network Services
- IPA Server
- Passkey Configuration

Sudo Commands

 Refresh  Delete  Add

<input type="checkbox"/>	Sudo Command	Description
<input type="checkbox"/>	/usr/sbin/reboot	
<input type="checkbox"/>	/usr/sbin/shutdown -h now	

Showing 1 to 2 of 2 entries.

IDM Web UI : Policy : Sudo Rules

Add sudo rule ✕

Rule name *

* Required field

Who

User category the rule applies to: Anyone Specified Users and Groups

<input type="checkbox"/>	Users	External	 Delete + Add
<input type="checkbox"/>	User Groups		 Delete + Add
<input type="checkbox"/>	ipusers		

Access this host

Host category the rule applies to: Any Host Specified Hosts and Groups

<input type="checkbox"/>	Hosts	External	 Delete + Add
<input type="checkbox"/>	Host Groups		 Delete + Add
<input type="checkbox"/>	rhel9_servers		

Run Commands

Command category the rule applies to: Any Command Specified Commands and Groups

Allow

<input type="checkbox"/>	Sudo Allow Commands		 Delete + Add
<input type="checkbox"/>	/usr/sbin/shutdown -h now		

IDM Web UI : Policy : Sudo

```
[dvader@rhel9-1 ~]$ sudo -l
First Factor:
Second Factor:
Matching Defaults entries for dvader on rhel9-1:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS
DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS
LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User dvader may run the following commands on rhel9-1:
    (root) /usr/sbin/shutdown -h now
    (root) /usr/sbin/reboot
```

IDM Web UI : Policy : Password Policies

Identity

Policy

Authentication

Network Services

IPA Server

Host-Based Access Control ▾

Sudo ▾

SELinux User Maps

Password Policies

Kerberos Ticket Policy

Passkey Configuration

Password Policies

Search



Refresh

Delete

Add

<input type="checkbox"/>	Group	Priority
<input type="checkbox"/>	global_policy	

Showing 1 to 1 of 1 entries.

IDM Web UI : Policy :

Password Policies :

global_policy

Password Policy: global_policy

Settings

Refresh

Revert

Save

Password Policy



Group	global_policy
Max lifetime (days)	<input type="text" value="90"/>
Min lifetime (hours)	<input type="text" value="1"/>
History size (number of passwords)	<input type="text" value="0"/>
Character classes	<input type="text" value="0"/>
Min length	<input type="text" value="8"/>
Max failures	<input type="text" value="6"/>
Failure reset interval (seconds)	<input type="text" value="60"/>
Lockout duration (seconds)	<input type="text" value="600"/>
Priority	
Grace login limit	<input type="text" value="-1"/>

IDM Web UI : Authentication : OTP Tokens

- Identity
 - Policy
 - Authentication**
 - Network Services
 - IPA Server
- Certificates
 - OTP Tokens**
 - RADIUS Servers
 - Identity Provider references
 - Certificate Identity Mapping Rules ▾

OTP Tokens

-  Refresh
-  Delete
- +** Add
- Disable
-  Enable

<input type="checkbox"/>	Unique ID	Owner	Status	Description
<input type="checkbox"/>	4b61ca82-1562-468b-97a2-0184a6e10195	dvader	✓ Enabled	

Showing 1 to 1 of 1 entries.

IDM Web UI : Authentication : OTP Tokens : SETUP



Add OTP token

Type Time-based (TOTP) Counter-based (HOTP)

Unique ID

Description

Owner

Validity start : UTC

Validity end : UTC

Vendor

Model

Serial

Key

Algorithm sha1 sha256 sha384 sha512

Digits 6 8


Clock interval (seconds)

* Required field

IDM Web UI : Authentication : OTP Tokens : SETUP

Configure your token



 Configure your token by scanning the QR code below. Click on the QR code if you see this on the device you want to configure.

 You can use [FreeOTP](#) as a software OTP token application.



[Show configuration uri](#)

OK

User Authentication Types

- To enable OTP for user dvader
- Select “Two factor authentication (password + OTP)”

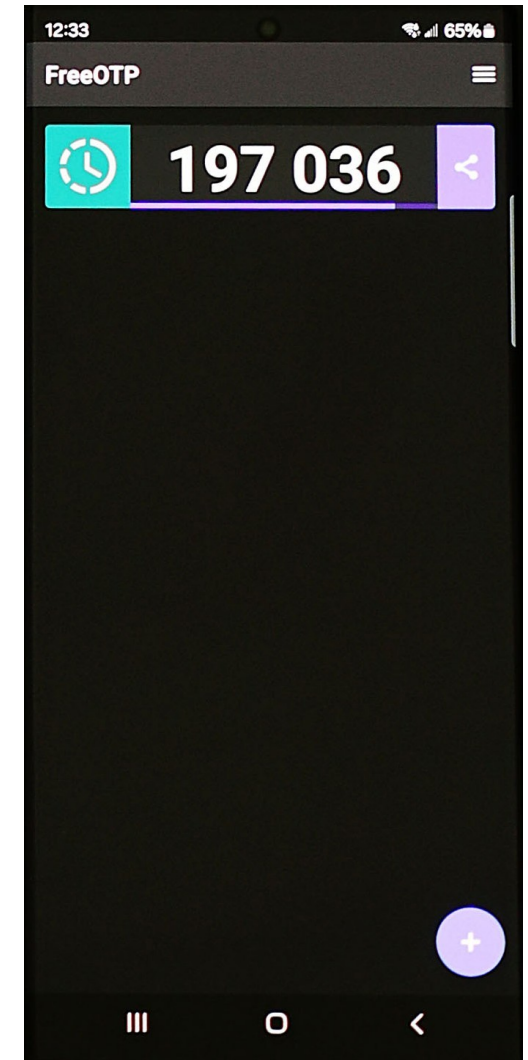
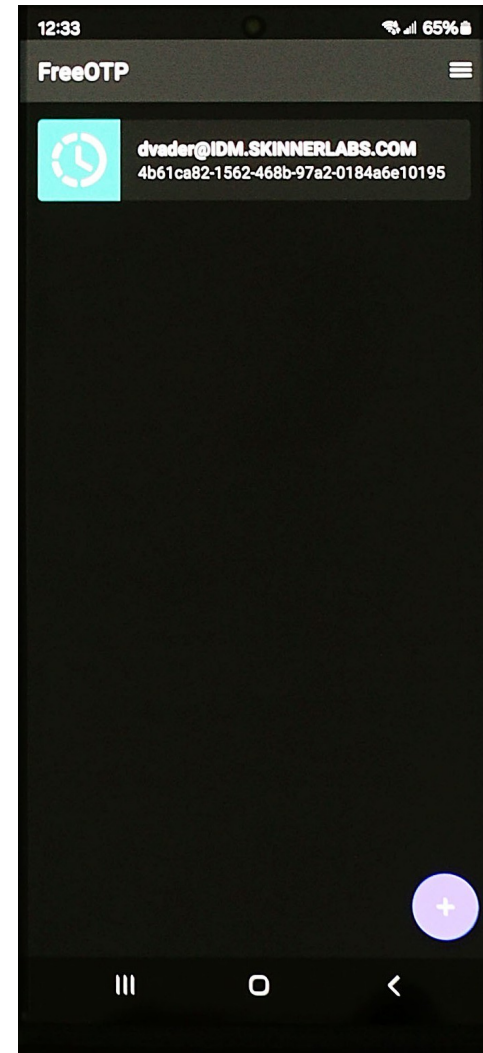
First name *	<input type="text" value="Darth"/>	Password	*****
Last name *	<input type="text" value="Vader"/>	Password expiration	2024-08-15 19:23:58Z
Full name *	<input type="text" value="Darth Vader"/>	UID	<input type="text" value="487500500"/>
Display name	<input type="text" value="Darth Vader"/>	GID	<input type="text" value="487500500"/>
Initials	<input type="text" value="DV"/>	Principal alias	<input type="text" value="dvader@IDM.SKINNERLABS.COM"/> <input type="button" value="Delete"/>
GECOS	<input type="text" value="Darth Vader"/>		<input type="button" value="Add"/>
Class	<input type="text"/>	Kerberos principal expiration	<input type="text" value="YYYY-MM-DD"/> <input type="text" value="hh"/> : <input type="text" value="mn"/> UTC
		Login shell	<input type="text" value="/bin/sh"/>
		Home directory	<input type="text" value="/home/dvader"/>
		SSH public keys	<input type="button" value="Add"/>
		Passkey mapping ⓘ	<input type="button" value="Add"/>
		Certificates	<input type="button" value="Add"/>
		Certificate mapping data ⓘ	<input type="button" value="Add"/>
		User authentication types ⓘ	<input type="checkbox"/> Password <input type="checkbox"/> RADIUS <input checked="" type="checkbox"/> Two factor authentication (password + OTP) <input type="checkbox"/> PKINIT <input type="checkbox"/> Hardened Password (by SPAKE or FAST) <input type="checkbox"/> External Identity Provider <input type="checkbox"/> Passkey



SSH with MFA / OTP



FreeOTP



```
[root@idm1 ~]# ssh dvader@rhel9-1.idm.skinnerlabs.com
(dvader@rhel9-1.idm.skinnerlabs.com) First Factor:
(dvader@rhel9-1.idm.skinnerlabs.com) Second Factor:
Last login: Tue May 21 12:58:20 2024 from 192.168.33.13
[dvader@rhel9-1 ~]$
```

IDM Web UI : Network Services : Automount

Identity Policy Authentication **Network Services** IPA Server

Automount DNS ▾

Automount Locations

 Refresh  Delete  Add

<input type="checkbox"/>	Location
<input type="checkbox"/>	default

Showing 1 to 1 of 1 entries.

IDM Web UI : Network Services : DNS

Identity Policy Authentication **Network Services** IPA Server

Automount **DNS** ▾

DNS Zones

- DNS Zones**
- DNS Forward Zones
- DNS Servers
- DNS Global Configuration

Refresh Delete + Add - Disable ✓ Enable

<input type="checkbox"/>	Zone name	Status
<input type="checkbox"/>	idm.skinnerlabs.com.	✓ Enabled

Showing 1 to 1 of 1 entries.

IDM Web UI : IPA Server : Roles

Identity Policy Authentication Network Services **IPA Server** Configuration

Role-Based Access Control ▾ ID Ranges Realm Domains Trusts ▾ Topology API Browser

Roles

Privileges

Permissions

Self Service Permissions

Delegations

Refresh

Delete

+ Add

	Description
<input type="checkbox"/> Enrollment Administrator	Enrollment Administrator responsible for client(host) enrollment
<input type="checkbox"/> IT Security Specialist	IT Security Specialist
<input type="checkbox"/> IT Specialist	IT Specialist
<input type="checkbox"/> Security Architect	Security Architect
<input type="checkbox"/> Subordinate ID Selfservice User	User that can self-request subordinate ids
<input type="checkbox"/> User Administrator	Responsible for creating Users and Groups

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHat