AINUX

— TASTE OF LINUX —

WELCOME TO THE WORLD OF LINUX

DAY - 6

CREATED BY : ARYAN M.P

AINUX
TASTE OF LINUX

RedHat Identity Management Services

THE GOAL OF REDHAT IDENTITY MANAGEMENT.

Red Hat Identity Management (IdM) provides a centralized and unified way to manage identity stores, authentication policies, and authorization policies in a Linux-based domain like Microsoft Active Directory.

IdM is one of the few centralized **Identity**, **Policy**, and **Authorization (IPA)** software solutions that support Advanced features of Linux operating system environments Unifying large groups of Linux machines Native integration with Active Directory.

IdM creates a Linux-based and Linux-controlled domain:

IdM servers and clients are Red Hat Enterprise Linux machines. However, even though IdM does not support Windows clients directly, it allows integration with Active Directory environment.

Examples of Benefits Brought by IdM

- Maintain the identities in one central place.
- Apply policies to multiple machines at the same time.
- Set different access levels for users by using host-based access control and other rules.
- Centrally manage privilege escalation rules.
- Reduce the security risk of passwords being written down or stored insecurely.
- Improve usability.
- Integrate the Linux systems with the Windows systems, thus preserving a centralized user store.

AINUX
TASTE OF LINUX

RedHat Identity Management Services

IPA is a combination of 389 Directory Server, Kerberos, HTTP Server, NTP, DNS, Dogtag (certificate system), making it as a single integrated security solution to manage the Identity, Policy, and perform Audit trail.

Identity: (*machine, user, virtual machines, groups, authentication credentials*)
Policy: (*configuration settings, access control information*)
Audit Trail: (*events, logs, analysis*)

Prerequisites

1. Set Host Name

EXP: - # hostnamectl set-hostname srv.iant.com

2. Set Static IP Address

EXP: - # nmcli connection add con-name static type ethernet ifname ens33
nmcli connection modify static ipv4.address 192.168.1.5/24 ipv4.gateway 192.168.1.1 ipv4.dns 192.168.1.1 +ipv4.dns 8.8.8.8
nmcli connection modify static ipv4.method manual

4. Setup a Network based (FTP)YUM server.

5. Add the following services to your firewall list

Ex: - ftp, http, https, ldap, ldaps, kerberos, dns.

AINUX
TASTE OF LINUX

Connecting to Network-Defined Users and Groups

LAB Scenario

Host Name: SRV.IANT.COM
Role: IPA Server
IP Address: 192.168.1.1/24
DNS: 192.168.1.1 / 8.8.8.8

Host Name: CLI-1
Role: IPA Client
IP Address: 192.168.1.2/24
Gateway: 192.168.1.1
DNS: 192.168.1.1 / 8.8.8.8

IPA Server Configuration

yum install ipa-server ipa-server-dns bind bind-dyndb-ldap [Install Packages from YUM Server]

ipa-server-install --setup-dns [install the IPA server]

Note: - Now you have to declare the credentials as follows.

1. Do you want to configure integrated DNS (BIND)? [no]: **yes**
2. Server host name [IPASRV.IANT.COM]: **ipasrv.iant.com**
3. Please confirm the domain name [iant.com]: **iant.com**

AINUX
TASTE OF LINUX

RedHat Identity Management Services

4. Please provide a realm name [IANT.COM]: **iant.com**
5. Do you want to use IANT.COM as realm name? [yes]: **yes**
6. Directory Manager password: **admin123#**
7. Password (confirm): **admin123#**
8. IPA admin password: **admin@123**
9. Password (confirm): **admin@123**
10. Continue to configure the system with these values? [no]: **yes**

Add UDP ports into firewall

```
# firewall-cmd --permanent --add-port=88/udp
# firewall-cmd --permanent --add-port=464/udp
# firewall-cmd --permanent --add-port=123/udp
# firewall-cmd –reload
```

Now check with user admin.

```
# kinit admin
```

Note: - Put the password which you have entered prior.

To display the details of admin user.

```
# ipa user-find admin
```

AINUX
TASTE OF LINUX

RedHat Identity Management Services

To see the status of IPA Server

ipactl status

To add an user in data base of IPA Server

ipa user-add

To set password for user tanima

ipa passwd tanima

To set password for user tanima

ipa user-find tanima

CLIENT CONFIGURATION

Configure Hostname

hostnamectl set-hostname cli1.iant.com

Create a network profile

nmcli connection add con-name lan type ethernet ifname ens33

Set and IP, Gateway and DNS

nmcli connection modify lan ipv4.addresses 192.168.1.6/24 ipv4.gateway 192.168.1.5 ipv4.dns 192.168.1.5 +ipv4.dns 8.8.8.8

nmcli connection modify lan ipv4.method manual

AINUX
TASTE OF LINUX

RedHat Identity Management Services

Configure YUM Client

scp 192.168.1.5:/etc/yum.repos.d/srv.repo /etc/yum.repos.d/client.repo

Install Client packages through YUM server

yum install ipa-client nss-pam-ldapd pam_krb5

Configute IPA client

ipa-client-install

Note: - Now you have to declare the credentials as follows.
Provide the domain name of your IPA server (ex: example.com): iant.com
Provide your IPA server name (ex: ipa.example.com): srv.iant.com

AINUX

TASTE OF LINUX

THANK YOU

CREATED BY : ARYAN M.P