# RHEL Clients to AD

**Integrating RHEL clients to Active Directory**

Presenter Dave Sullivan
Sr. TAM, Red Hat
2013-09-03

# Agenda

- Review Dmitri Pal and Simo Sorce Preso
  - Legacy RHEL hook to AD
  - RHEL Direct--->sssd--->AD
  - RHEL IdM/Trust--->sssd--->(FreeIPA/IdM and AD)
- Review Mark Heslin's Reference Architecture
  - Direct AD integration options (excludes IdM/IPA integration)
- Quick walk through on simple direct integration
  - rhel--->sssd--->AD

# Dmitri Pal & Simo Sorce Preso

- **Dmitri Pal (Software Engineering Manager focused on IdM)**
- **Simo Sorce (Principal Software Engineer focused on IdM)**
- **Presentation, “AD Integration Options For Linux Systems”**
  - Dmitri Pal & Simo Sorce - Integrating Linux systems into Active Directory Environment

# Mark Heslin's Reference Architecture

- **Mark Heslin (Principal Software Engineer focused on IdM)**
- **Reference Architecture, “Integrating Enterprise Linux 6 With Active Directory”**
  - How do I authenticate RHEL to Active Directory using sssd?

# Direct RHEL6 integration to AD Walk-through

- **Active Directory Existing**
  - Windows 2k8r2
- **Existing RHEL Client**
  - RHEL6.4+ @base
  - [root@testclient-rhel6-006 ~]# rpm -qa | wc -l

    433
- **System Security Services Daemon (SSSD)**
  - Permits offline authentication
  - Reduces load on identification/authentication servers
  - yum -y install sssd
  - See References [SSSD] for detailed SSSD documentation

# Prerequisites

- **Active Directory Existing**
  - Windows 2k8r2
- **Existing RHEL Client**
  - RHEL6.4+ @base
  - [root@testclient-rhel6-006 ~]# rpm -qa | wc -l

    433
- **System Security Services Daemon (SSSD)**
  - Permits offline authentication
  - Reduces load on identification/authentication servers
  - yum -y install sssd
  - See References [SSSD] for detailed SSSD documentation

# Multiple Ways To Integrate – GUI or CLI

- **GUI**

  1. Run the authconfig-tui tool. Select ldap under the "User Information" section and Kerberos under the "Authentication" Section.
  2. On the ldap Settings step. Leave the use TLS option unselected put the AD servers fully qualified domain name in and the base DN.
  3. On the kerberos Settings page enter the AD servers Realm, also list the AD servers fully qualified domain name for the KDC and Admin Server.

- **CLI**

  - [root@testclient-rhel6-006 ~]# rpm -qa | grep sssd

    sssd-client-1.9.2-82.7.el6_4.x86_64

    sssd-1.9.2-82.7.el6_4.x86_64

  - Utilize authconfig tool

    - Need Windows FQDN, AD basedn
    - Automatically configures nss, pam, sssd.conf, and krb5.conf

      [authconfig --enableldap --enablekrb5 --ldapserver=ldap://win2k8.example.com --ldapbasedn="dc=example,dc=com" --enablerfc2307bis --disablekrb5realmdns --krb5kdc=win2k8.example.com --krb5realm=EXAMPLE.COM --disableforcelegacy --enablelocauthorize --enablemkhomedir --updateall

      [root@testclient-rhel6-006 ~]# echo $?

      0

# Review CLI Configuration

- **NSS**
  - [root@testclient-rhel6-006 ~]# cat /etc/nsswitch.conf | grep sss

    passwd:  files sss

    shadow:  files sss

    group:  files sss

    services:  files sss

    netgroup:  files sss
- **PAM**
  - [root@testclient-rhel6-006 ~]# ls -lrt /etc/pam.d/
  - system-auth-ac, password-auth-ac, smartcard-auth-ac, fingerprint-auth-ac modified

    lrwxrwxrwx. 1 root root  14 Jun 27  2012 system-auth -> system-auth-ac

    lrwxrwxrwx. 1 root root  16 Jun 27  2012 password-auth -> password-auth-ac

    lrwxrwxrwx. 1 root root  19 Jun 27  2012 fingerprint-auth -> fingerprint-auth-ac

    lrwxrwxrwx. 1 root root  17 Jun 27  2012 smartcard-auth -> smartcard-auth-ac

# Review CLI Configuration

- **sssd.conf**
  - [root@testclient-rhel6-006 sssd]# cat /etc/sssd/sssd.conf

    ...

    ldap_schema = rfc2307bis

    ldap_search_base = dc=example,dc=com

    krb5_realm = EXAMPLE.COM

    krb5_server = win2k8.example.com

    id_provider = ldap

    auth_provider = krb5

    chpass_provider = krb5

    ldap_uri = ldap://win2k8.example.com

    krb5_kpasswd = kerberos.example.com

    cache_credentials = True

    ldap_tls_cacertdir = /etc/openldap/cacerts

    [sssd]

    services = nss, pam

    config_file_version = 2

# Review CLI Configuration

- **krb5.conf**
  - [root@testclient-rhel6-006 sssd]# cat /etc/krb5.conf

    ...

    [logging]

     default = FILE:/var/log/krb5libs.log

     kdc = FILE:/var/log/krb5kdc.log

     admin_server = FILE:/var/log/kadmind.log

    [libdefaults]

     default_realm = EXAMPLE.COM

     dns_lookup_realm = false

     dns_lookup_kdc = false

     ticket_lifetime = 24h

     renew_lifetime = 7d

     forwardable = true

# Install oddjob-mkhomedir

- [root@test-rhel6-ad sssd]# yum -y install oddjob-mkhomedir
  - Ensure that user home directories are created with the proper SELinux file and directory contexts
- [root@test-rhel6-ad sssd]# chkconfig oddjobd on;service oddjobd start

  Starting oddjobd: [ OK ]

# Kerberos Binding To AD

- [root@testclient-rhel6-006 sssd]# yum -y install krb5-workstation samba-common
- [root@testclient-rhel6-006 sssd]# kinit Administrator

  Password for Administrator@EXAMPLE.COM:

  kinit: Clock skew too great while getting initial credentials
- [root@testclient-rhel6-006 sssd]# ntpdate win2k8.example.com

  3 Sep 01:11:55 ntpdate[25813]: step time server 192.168.1.78 offset -50400.525691 sec
- [root@testclient-rhel6-006 sssd]# kinit Administrator

  Password for Administrator@EXAMPLE.COM:
- [root@testclient-rhel6-006 sssd]# klist

  Ticket cache: FILE:/tmp/krb5cc_0

  Default principal: Administrator@EXAMPLE.COM

  Valid starting  Expires  Service principal

  09/03/13 01:11:58  09/03/13 11:12:01  krbtgt/EXAMPLE.COM@EXAMPLE.COM

  renew until 09/10/13 01:11:58

# Join To AD Via Samba

- [root@testclient-rhel6-006 sssd]# cat /etc/samba/smb.conf

  [global]

  workgroup = EXAMPLE

  client signing = yes

  client use spnego = yes

  kerberos method = secrets and keytab

  log file = /var/log/samba/%m.log

  realm = EXAMPLE.COM

  security = ads

  #necessary if dns not properly setup

  password server = win2k8.example.com

- [root@testclient-rhel6-006 sssd]# hostname test-rhel6-ad
- [root@testclient-rhel6-006 sssd]# net ads join -k

  Using short domain name -- EXAMPLE

  Joined 'TEST-RHEL6-AD' to dns domain 'EXAMPLE.COM'

  No DNS domain configured for test-rhel6-ad. Unable to perform DNS Update.

  DNS update failed!

# Add Group To AD

- Open Administrative Tools -> Active Directory Users and Computers
- Browse to EXAMPLE.COM, then to Users
- Right click on Users and Create a New Group named unixusers
- Double click on the unixusers group then switch to the UNIX Attributes tab
- Select the NIS Domain created earlier
- Set the GID as appropriate

# Add User To AD

- Open Administrative Tools -> Active Directory Users and Computers
- Browse to EXAMPLE.COM, then to Users
- Right click on Users and Create a New User named aduser
- Make sure User must change password at next logon and Account is disabled are unchecked
- Double click on the aduser group then switch to the UNIX Attributes tab
- Select the NIS Domain created earlier
- Set the UID as appropriate
- Set the Login Shell to /bin/bash
- Set the Home Directory to /home/aduser
- Set Primary Group Name/GID to unixusers

# Can we query AD?

- root@testclient-rhel6-006 sssd]# yum -y install openldap-clients
- [root@testclient-rhel6-006 sssd]# /usr/bin/ldapsearch -H ldap://win2k8.example.com/ -Y GSSAPI -N -b "dc=example,dc=com" "(&(objectClass=user)(sAMAccountName=aduser))"

  ...

  # red hat, Users, EXAMPLE.COM

  dn: CN=red hat,CN=Users,DC=EXAMPLE,DC=COM

  objectClass: top

  objectClass: person

  objectClass: organizationalPerson

  objectClass: user

  cn: red hat

  sn: hat

  givenName: red

  distinguishedName: CN=red hat,CN=Users,DC=EXAMPLE,DC=COM

  InstanceType: 4

  ...

# Test with id command

- [root@testclient-rhel6-006 sssd]# kinit Administrator

  Password for Administrator@EXAMPLE.COM:
- [root@testclient-rhel6-006 sssd]# time id aduser <----first pull takes longer, not cached

  uid=10000(aduser) gid=10000(unixusers) groups=10000(unixusers)

  real 0m21.930s

  user 0m0.000s

  sys 0m0.001s
- [root@testclient-rhel6-006 sssd]# time id aduser <----second time much faster, it's in our sss cache

  uid=10000(aduser) gid=10000(unixusers) groups=10000(unixusers)

  real 0m0.002s

  user 0m0.001s

  sys 0m0.000s

# Test logging in remotely via ssh

- [root@test-rhel6-ad ~]# grep aduser /etc/passwd

  [root@test-rhel6-ad ~]# ifconfig eth0 | grep 192

  inet addr:192.168.1.155  Bcast:192.168.1.255  Mask:255.255.255.0
- [dsulliva@localhost ~]$ ssh aduser@192.168.1.155

  aduser@192.168.1.155's password:

  Last login: Mon Sep  9 05:49:05 2013 from 192.168.1.6
- [aduser@test-rhel6-ad ~]$ pwd

  /home/aduser
- [aduser@test-rhel6-ad ~]$ echo $SHELL

  /bin/bash

# Clear kerberos and sssd cache

- [root@testclient-rhel6-006 sssd]# kdestroy
- [root@testclient-rhel6-006 sssd]# service sssd stop; rm -f /var/lib/sss/db/*; service sssd restart

  Stopping sssd: [ OK ]

  Stopping sssd: cat: /var/run/sssd.pid: No such file or directory

  [FAILED]

  Starting sssd: [ OK ]

# References

- SSSD
  - https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/SSSD-Introduction.html
- Red Hat Presentations
  - How do I authenticate RHEL to Active Directory using sssd?
  - Dmitri Pal & Simo Sorce - Integrating Linux systems into Active Directory Environment

# THOUGHTS?
# QUESTIONS?
# CONCERNS?