VEC-MZ-LDAP-Configuration on Non-Windows servers.



**Table of Contents**

[Document Information](#page3) [3](#page3)

[Information](#page4) [4](#page4)

[Procedure](#page7) [6](#page7)

[High Level](#page8) [6](#page8)

[Detailed](#page9) [7](#page9)

[Rollback Procedure](#page12) [1](#page12)8

[Detailed](#page13) [1](#page13)8

**Information**

|  |  |  |
| --- | --- | --- |
| Published Date (for Change  Management Team use only): | Title: **Install security Patches\updates on Windows & Non-Windows servers.** | |
| Document (Office Use) #  KB00xxxxx | Prepared By:  **Siddaling Akkalkot** | Date of Prepared:  **2019- 09-10** |
| Revision #: **1.1 2019- 07-02** | Peer Reviewed by: | Date Peer Reviewed: |
| Procedure (Please select):  **Standard** | Manager Reviewed by:  **Joseph Fasano** | Date Manager Reviewed: |
| Service(s) this procedure is  assigned to:  VEC Vulnerability / Compliance Remediation | SRB Approved by: | Date SRB Approved:  **2019-xx-xx** |
| Did Customer Approved Down time: N/A |  | Change Window Hours:  2**4x7(Requiring Customer Approval)** |

**Description**

This change is to configure the all A001 non-Windows servers includes Redhat, CentOS and Ubuntu servers.

**Purpose**

The purpose of the change is to make server comply with audit requirement also to server purpose of universal authentication policy for all users.

**Scope**

RedHat, CentOS and Ubuntu VM’s that are running in Management zones.

**Accountable Teams**

Compute ICOE and Global Vulnerability / Compliance Remediation

**Risk Analysis**

Risk: Low

**Impact**

No expected impact if SOP followed correctly



**Definitions and Acronyms**

AKA: also known as

C/R: Change Request “ticket”

CAB: Change Approval Board

Change Control: A change to an existing process that requires CAB and CRB approvals.

MOP: Method of Procedure

PM: Project Manager

PPE: Personal Protective Equipment (safety practices and procedures for DCs)

Requestor: Individual or Team submitting a request to DC OPS. (This can include internal Virtustream customers and/or and external Virtustream DC customers.)

S/R: Service Request “ticket”

SRF: Service Request Form

SOW: Statement of Work

USDC: US Datacenter,

VS: Virtustream

**Procedure**

**High Level**

**Pre-checks**

1. Server should have repo access so that it can able to download and install the required packages.
2. Ensure Change Implementer have Root\Administrator level access.
3. Should check that, VM shouldn’t be join to any other domain.
4. Ensure inform to server owners about joining server domain.
5. Ensure sever can connect to Domain Controller servers.

Command to check:

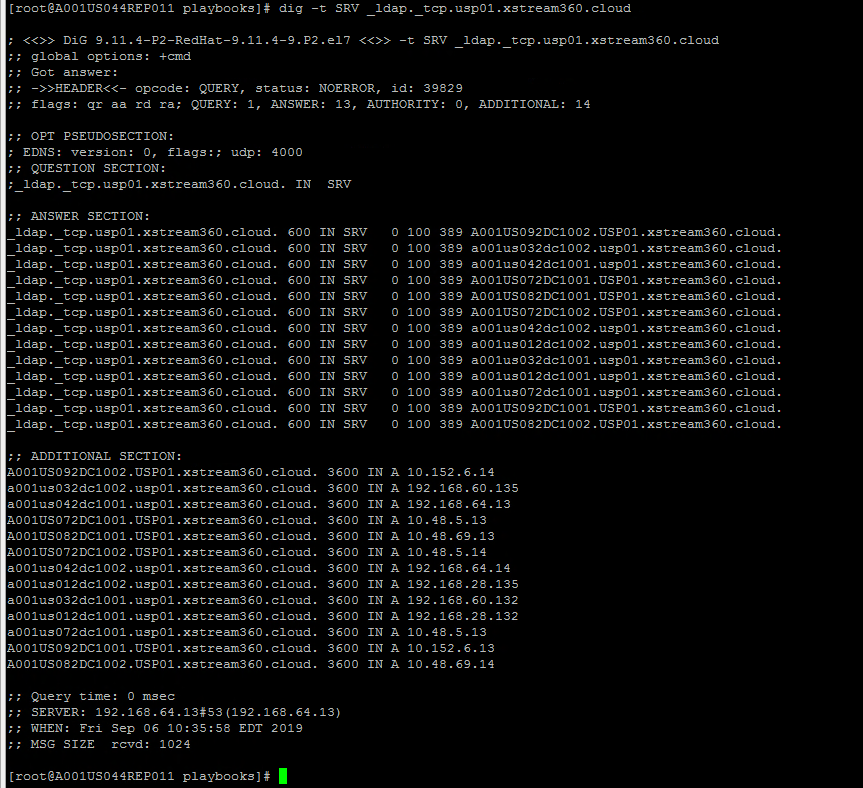
**USP01.XSTREAM360.COM:**

dig -t SRV \_ldap.\_tcp.usp01.xstream360.cloud

if dig command not found then install below package.

#yum install bind-utils -y

It should provide the below output:



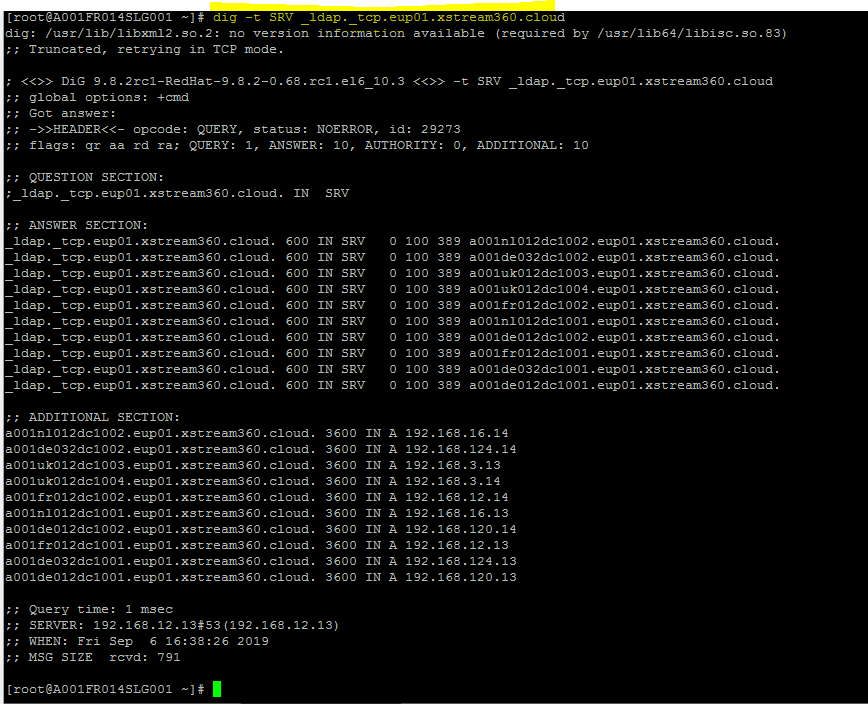
**EUP01.XSTREAM360.CLOUD:**

dig -t SRV \_ldap.\_tcp.eup01.xstream360.cloud

if dig command not found then install below package.

#yum install bind-utils -y

It should provide the below output:



**Implementation Procedure**

1. Login to the server using Putty
2. Install required packages based on the version and flavor of OS.
3. Take backup of all configuration files.
4. Edit the Kerberos ( krb5.conf) file and add the respective DC kdc entries
5. Initiate token to domain controller server.
6. Edit samba file (/etc/samba/smb.conf) and all the realm information.
7. Edit and change the permission of sssd file (/etc/sssd/sssd.conf) and add the all domain server options.
8. Join server to domain using ( net ads join -k )
9. Add sssd.so library authentication to pam files
10. Start the sssd service.
11. Check user details.

**Post-checks**

1. Login to the server using domain id and should allow to login.
2. Also, login to server using local account or root account and should able to login.

**Detailed Implementation Steps:**

**RedHat and CentOS 6/7 Version servers:  
  
Install the following packages:**

Redhat/CentOS 7:

#yum install krb5-workstation samba-common-tools sssd-ad –y

Redhat/CentOS 6:

#yum -y install authconfig krb5-workstation pam\_krb5 samba-common samba-common-tools sssd-ad

**Take backup of all configuration files:**

# cp /etc/krb5.conf /etc/krb5.conf.bak

# cp /etc/samba/smb.conf /etc/samba/smb.conf.bak

# tar -cvzf /tmp/pam.d.tgz /etc/pam.d/

# authconfig --savebackup=sssdDDMMYYYY Ex: authconfig --savebackup=sssd06092019

**Edit Kerberos file and add the kdc entries:**

**USP01.XSTREAM360.COM – kdc values**

[root@A001US034SLG001 Domain\_files]# 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 = USP01.XSTREAM360.CLOUD

dns\_lookup\_realm = true

dns\_lookup\_kdc = true

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = true

rdns = false

default\_ccache\_name = KEYRING:persistent:%{uid}

[realms]

USP01.XCLOUD360.CLOUD = {

kdc = 192.168.60.135

kdc = 192.168.64.14

kdc = 192.168.32.132

kdc = 192.168.60.132

kdc = 192.168.28.132

kdc = 192.168.28.135

kdc = 192.168.64.13

kdc = 10.48.5.13

kdc = 10.48.5.14

kdc = 10.48.69.13

kdc = 10.48.69.14

kdc = 10.152.6.13

kdc = 10.152.6.14

}

[domain\_realm]

usp01.xcloud360.cloud = USP01.XCLOUD360.CLOUD

.usp01.xcloud360.cloud = USP01.XCLOUD360.CLOUD

**EUP01.XSTREAM360.COM – kdc values**

[root@A001FR014SLG001 RHEL\_CENTOS\_6]# 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 = EUP01.XSTREAM360.CLOUD

dns\_lookup\_realm = true

dns\_lookup\_kdc = true

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = true

rdns = false

default\_ccache\_name = KEYRING:persistent:%{uid}

[realms]

EUP01.XCLOUD360.CLOUD = {

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.13

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

}

[domain\_realm]

eup01.xcloud360.cloud = EUP01.XCLOUD360.CLOUD

.eup01.xcloud360.cloud = EUP01.XCLOUD360.CLOUD

**Initiate token to domain controller server:**

#kinit <your\_domain\_id> Ex: kinit akkalkots (USP01 id for US servers or EUP01 id for EMEA servers)



**Edit samba file (/etc/samba/smb.conf) and all the realm information.**

**USP01.XSTREAM360.COM – realm values**

[root@A001US034SLG001 ~] # cat /etc/samba/smb.conf

[global]

workgroup = USP01

password server = 192.168.60.135 192.168.64.14 192.168.32.132 192.168.60.132 192.168.28.132 192.168.28.135 192.168.64.13 10.48.5.13 10.48.5.14 10.48.69.13 10.48.69.14 10.152.6.13 10.152.6.14

realm = USP01.XSTREAM360.CLOUD

security = ads

kerberos method = secrets and keytab

idmap config \* : range = 16777216-33554431

template homedir = /home/%U

template shell = /bin/bash

winbind use default domain = true

winbind offline logon = false

server signing = mandatory

guest account = nobody

restrict anonymous = 1

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

max log size = 50

;security = ads

netbios name = A001US024MLX003 <Change this to VM host name >

;realm = usp01.xstream360.cloud

;password server = 192.168.60.135 192.168.64.14 192.168.32.132 192.168.60.132 192.168.28.132 192.168.28.135 192.168.64.13 10.48.5.13 10.48.5.14 10.48.69.13 10.48.69.14 10.152.6.13 10.152.6.14

;workgroup = USP01

passdb backend = tdbsam

encrypt passwords = yes

;idmap uid = 10000-500000

;idmap gid = 10000-500000

winbind enum users = no

winbind enum groups = no

;winbind use default domain = yes

winbind nested groups = yes

;template homedir = /home/%U

;template shell = /bin/bash

client use spnego = yes

;domain master = no

client signing = mandatory

**EUP01.XSTREAM360.COM – realm values**

[global]

workgroup = EUP01

password server = 192.168.3.13 192.168.3.14

realm = EUP01.XSTREAM360.CLOUD

security = ads

kerberos method = secrets and keytab

idmap config \* : range = 16777216-33554431

template homedir = /home/%U

template shell = /bin/bash

winbind use default domain = true

winbind offline logon = false

server signing = mandatory

guest account = nobody

restrict anonymous = 1

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

max log size = 50

;security = ads

netbios name = A001UK034XWS001 <Change\_value\_to\_host\_name\_or\_DNS\_Name>

;realm = eup01.xstream360.cloud

;password server = 192.168.3.13 192.168.3.14

;workgroup = EUP01

passdb backend = tdbsam

encrypt passwords = yes

;idmap uid = 10000-500000

;idmap gid = 10000-500000

winbind enum users = no

winbind enum groups = no

;winbind use default domain = yes

winbind nested groups = yes

;template homedir = /home/%U

;template shell = /bin/bash

client use spnego = yes

;domain master = no

client signing = mandatory

**Edit and change the permission of sssd file (/etc/sssd/sssd.conf) and add the all domain server options:**

**USP01.XSTREAM360.COM**

# cat /etc/sssd/sssd.conf

[sssd]

domains = usp01.xstream360.cloud

config\_file\_version = 2

services = nss, pam

[domain/usp01.xstream360.cloud]

ad\_domain = usp01.xstream360.cloud

krb5\_realm = USP01.XSTREAM360.CLOUD

realmd\_tags = manages-system joined-with-samba

cache\_credentials = True

id\_provider = ad

krb5\_store\_password\_if\_offline = True

default\_shell = /bin/bash

ldap\_id\_mapping = True

use\_fully\_qualified\_names = False

fallback\_homedir = /home/%u

access\_provider = ad

[pam]

**EUP01.XSTREAM360.COM**

#cat /etc/sssd/sssd/conf

[sssd]

domains = eup01.xstream360.cloud

config\_file\_version = 2

services = nss, pam

[domain/eup01.xstream360.cloud]

ad\_domain = eup01.xstream360.cloud

krb5\_realm = EUP01.XSTREAM360.CLOUD

realmd\_tags = manages-system joined-with-samba

cache\_credentials = True

id\_provider = ad

krb5\_store\_password\_if\_offline = True

default\_shell = /bin/bash

ldap\_id\_mapping = True

use\_fully\_qualified\_names = False

fallback\_homedir = /home/%u

access\_provider = ad

[pam]

Permission change to 0600:

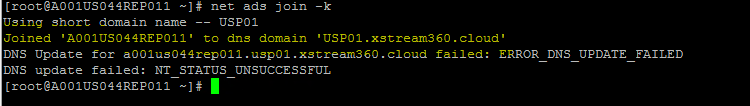
#chmod 0600 /etc/sssd/sssd.conf

#ls -l /etc/sssd/sssd.conf

-rw-------. 1 root root 453 Sep 20 2018 /etc/sssd/sssd.conf

**Join server to domain.**

Use below command to join server to domain.



Can ignore the DNS update Error

**Add sssd.so library authentication to pam files:**

Using below command we can allow the AD users to authenticate to login.

# authconfig --update --enablesssd --enablesssdauth --enablemkhomedir

**Start the sssd service:**

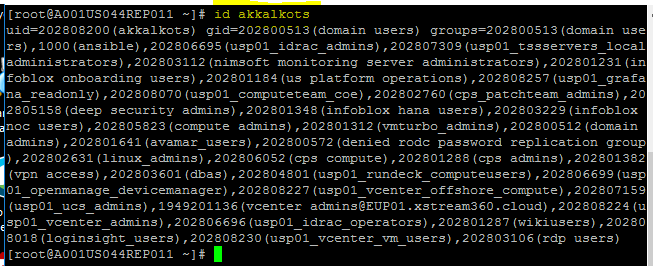
#systemctl start sssd (RedHat 7 or CentOS 7)

OR

#service sssd start (RedHat 6 or CentOS 6)

**Check user details:**

#id <domain\_id> Ex: #id akkalkots



**Ubuntu 14 and 16.04 servers:**

**Install the following packages:**

# apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user

If you get below screen then enter domain name as per VM DC location. ( US VM’s – USP01.XSTREAM360.COM EMEA VM’s - EUP01.XSTREAM360.COM)

Machine generated alternative text:
Pa c kage 
When 
con f i gu rat on 
users attempt to use Kerberos and specify a principal or user name 
without specifying what administrative Kerberos realm that principal 
belongs to, the 
also be used as 
machine . Often, 
DNS domain 
Default Kerberos 
system appends the default realm. The default realm may 
the realm of a Kerberos service running on the local 
the default realm is the uppercase version of the local 
S realm: 

**Setup Kerberos authentication:**

**USP01.XSTREAM360.COM – kdc values**

#cp/etc/krb5.conf /etc/krb5.conf\_bak

[root@A001US034SLG001 Domain\_files]# 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 = USP01.XSTREAM360.CLOUD

dns\_lookup\_realm = true

dns\_lookup\_kdc = true

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = true

rdns = false

default\_ccache\_name = KEYRING:persistent:%{uid}

[realms]

USP01.XCLOUD360.CLOUD = {

kdc = 192.168.60.135

kdc = 192.168.64.14

kdc = 192.168.32.132

kdc = 192.168.60.132

kdc = 192.168.28.132

kdc = 192.168.28.135

kdc = 192.168.64.13

kdc = 10.48.5.13

kdc = 10.48.5.14

kdc = 10.48.69.13

kdc = 10.48.69.14

kdc = 10.152.6.13

kdc = 10.152.6.14

}

[domain\_realm]

usp01.xcloud360.cloud = USP01.XCLOUD360.CLOUD

.usp01.xcloud360.cloud = USP01.XCLOUD360.CLOUD

**EUP01.XSTREAM360.COM – kdc values**

#cp/etc/krb5.conf /etc/krb5.conf\_bak

[root@A001FR014SLG001 RHEL\_CENTOS\_6]# 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 = EUP01.XSTREAM360.CLOUD

dns\_lookup\_realm = true

dns\_lookup\_kdc = true

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = true

rdns = false

default\_ccache\_name = KEYRING:persistent:%{uid}

[realms]

EUP01.XCLOUD360.CLOUD = {

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.13

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

kdc = 192.168.3.13

kdc = 192.168.3.14

}

[domain\_realm]

eup01.xcloud360.cloud = EUP01.XCLOUD360.CLOUD

.eup01.xcloud360.cloud = EUP01.XCLOUD360.CLOUD

Capitalization matters! The realm name is just your domain controller's address in all caps.

**Kerbs authentication**:

# kinit akkalkots <Domain\_id>

Password for akkalkots@ USP01.XSTREAM360.CLOUD:

# klist

Ticket cache: KEYRING:persistent:0:0

Default principal: adye@ USP01.XSTREAM360.CLOUD

Valid starting Expires Service principal

04/13/2018 14:57:43 04/14/2018 00:57:43 krbtgt/ USP01.XSTREAM360.CLOUD @EUP01.X STREAM360.CLOUD

renew until 04/20/2018 14:57:26

**winbind setup**

**USP01.XSTREAM360.COM – realm values**

#cp /etc/samba/smb.conf /etc/samba/smb.conf\_bak

[root@A001US034SLG001 ~]# cat /etc/samba/smb.conf

[global]

workgroup = USP01

password server = 192.168.60.135 192.168.64.14 192.168.32.132 192.168.60.132 192.168.28.132 192.168.28.135 192.168.64.13 10.48.5.13 10.48.5.14 10.48.69.13 10.48.69.14 10.152.6.13 10.152.6.14

realm = USP01.XSTREAM360.CLOUD

security = ads

kerberos method = secrets and keytab

idmap config \* : range = 16777216-33554431

template homedir = /home/%U

template shell = /bin/bash

winbind use default domain = true

winbind offline logon = false

server signing = mandatory

guest account = nobody

restrict anonymous = 1

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

max log size = 50

;security = ads

netbios name = A001US024MLX003 <Change this to VM host name >

;realm = usp01.xstream360.cloud

;password server = 192.168.60.135 192.168.64.14 192.168.32.132 192.168.60.132 192.168.28.132 192.168.28.135 192.168.64.13 10.48.5.13 10.48.5.14 10.48.69.13 10.48.69.14 10.152.6.13 10.152.6.14

;workgroup = USP01

passdb backend = tdbsam

encrypt passwords = yes

;idmap uid = 10000-500000

;idmap gid = 10000-500000

winbind enum users = no

winbind enum groups = no

;winbind use default domain = yes

winbind nested groups = yes

;template homedir = /home/%U

;template shell = /bin/bash

client use spnego = yes

;domain master = no

client signing = mandatory

**EUP01.XSTREAM360.COM – realm values**

#cp /etc/samba/smb.conf /etc/samba/smb.conf\_bak

#cat /etc/samba/smb.conf

[global]

workgroup = EUP01

password server = 192.168.3.13 192.168.3.14

realm = EUP01.XSTREAM360.CLOUD

security = ads

kerberos method = secrets and keytab

idmap config \* : range = 16777216-33554431

template homedir = /home/%U

template shell = /bin/bash

winbind use default domain = true

winbind offline logon = false

server signing = mandatory

guest account = nobody

restrict anonymous = 1

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

max log size = 50

;security = ads

netbios name = A001UK034XWS001 <Change\_value\_to\_host\_name\_or\_DNS\_Name>

;realm = eup01.xstream360.cloud

;password server = 192.168.3.13 192.168.3.14

;workgroup = EUP01

passdb backend = tdbsam

encrypt passwords = yes

;idmap uid = 10000-500000

;idmap gid = 10000-500000

winbind enum users = no

winbind enum groups = no

;winbind use default domain = yes

winbind nested groups = yes

;template homedir = /home/%U

;template shell = /bin/bash

client use spnego = yes

;domain master = no

client signing = mandatory

**Configure nss to make domain accounts locally available.**

Take backup of below file and edit as per here.

#cp /etc/nsswitch.conf /etc/nsswitch.conf.bak

# cat /etc/nsswitch.conf

# /etc/nsswitch.conf

#

# Example configuration of GNU Name Service Switch functionality.

# If you have the `glibc-doc-reference' and `info' packages installed, try:

# `info libc "Name Service Switch"' for information about this file.

passwd: files winbind

group: files winbind

shadow: files

hosts: files dns mdns4\_minimal [NOTFOUND=return]

networks: files

protocols: db files

services: db files

ethers: db files

rpc: db files

netgroup: nis

sudoers: files

**Joining the domain.**

#net ads join -U <domain\_id> Ex: #net ads join -U akkalkots

**Once joined, start or restart the following three services with this command:**

# service winbind restart; service nmbd restart; service smbd restart

stop: Unknown instance:

winbind start/running, process 12083

nmbd stop/waiting

nmbd start/running, process 12103

smbd stop/waiting

smbd start/running, process 12115

**Testing winbind setup**

# wbinfo -u

# wbinfo -g

# wbinfo -i adye

# getent passwd

# getend group

**PAM integration.**

ensure the Winbind NT/Active Directory authentication box is checked

# pam-auth-update

**Rollback Procedure**

**Rollback Procedure Time Estimate:**

15 minutes per VM.

**Steps**

1. Login to server through putty using local/root credentials.
2. Stop the sssd service

#systemctl stop sssd

OR

#service sssd stop

1. Destroy authentication token from domain servers.

#kdestroy

1. Delete server from domain controller.

#net ads leave -U <domain\_id> or #net ads leave -U akkalkots

1. Restore the pam files.

#cp /tmp/pam.d/password-auth-ac\_bak /etc/pam.d/password-auth-ac

#cp /tmp/pam.d/system-auth-ac\_bak /etc/pam.d/system-auth-ac

1. Check the local account/root login.

#kdestory