

## Setting up TAS 7.0/7.1 to use Active Directory (AD)

### I) Overview

Starting with version 7.0, TAS can be set up to use Active Directory as an authentication server. TAS accepts CIFS file service tickets generated by AD's Key Distribution Center (KDC).

The purpose of this document is to describe steps necessary to configure TAS to work with AD as its authentication server.

### II) Configuration Steps

The following steps are necessary to configure TAS CIFS file service to use AD as authentication server:

#### 1) DNS configuration.

If Active Directory server and UNIX server where TAS is running use the same DNS server, no DNS adjustment needs to be made. If their DNS server is not the same, modify /etc/hosts file on UNIX server so the Unix server can find the AD server. This is only necessary if the two DNS domain do not match. For example, since our AD server here uses itself (i.e: superdude) as its DNS server and our Unix server uses wiggum. Since superdude's DNS and wiggum's DNS are two different domain, we need to setup an entry on our Unix server so TAS can find the AD server. We added the following entry to our /etc/hosts file:

```
147.145.205.170 superdude.fwtest.wa.lsil.com
```

#### 2) Synchronize system clocks.

Kerberos tickets only valid for 5 minutes, so the difference between Kerberos server's, TAS server's, and workstation's clock should be within 5 minutes. Otherwise, kerberos authentication will fail due to clock skew error.

#### 3) Configuring TAS CIFS service and creating TAS computer accounts on AD server.

When TAS CIFS service is configured to use AD, each CIFS service represents an AD computer account. A password must be set for each AD computer account and the Kerberos key generated from that password must be stored locally on the TAS host-system.

There are several ways to configure and create TAS CIFS service to work with AD.

##### ***a) Active Directory File Service Configuration I***

The easiest way to configure TAS to use AD is by creating a computer account and configure local TAS at same time thru TNAS.

To create, modify, delete, or view a TAS CIFS service as AD service,

follow these steps:

- o Log on to TNAS as root or TAS administrator
- o TAS Sphere -> CIFS Realm -> Manage CIFS File Services -> Select a File Service -> Authentication Options
- o Determine whether or not to restrict authentication for this file service to the AD service exclusively by clicking the Restrict Authentication to Active Directory Only radio button. TAS can combine other forms of authentication with AD authentication if this radio button is left unmarked.
- o Check the Use Active Directory checkbox and click the Configure action button. In the form that appears, type the Domain name in the text entry area, or select a domain from the pull-down menu. The name of the domain is the same as that for the AD's Kerberos realm.
- o Choose generate a workstation account by selecting the radio button associated with the option. Provide information for the following attributes:
  - Container - provide the name of the container for the account. Usually the value is cn=Computers;
  - Administrator - provide the Kerberos principal name for the AD administrative account.
  - Password - password associated with the AD administrative account.
- o Click Done.
- o Click submit.

TAS CIFS file service is now configured to use AD as authentication server.

#### ***b) Active Directory File Service Configuration II***

This configuration method is divided into two parts. The first part is to configure TAS file service and kerberos key file on TAS host server using TNAS. The second part is to create and set TAS CIFS service as computer account on AD server using AD tools provided by Microsoft.

Part 1, use TNAS to setup TAS CIFS service to use AD:

- o Log on TNAS as root or TAS administrator
- o Click TAS Sphere -> CIFS Realm -> Manage CIFS File Services -> Select a File Service -> Authentication Options
- o Determine whether or not to restrict authentication for this file service to the AD service exclusively by clicking the Restrict Authentication to Active Directory Only radio button. TAS can combine other forms of authentication with AD authentication if this radio button is left unmarked.
- o To create an Active Directory service, check the Use Active Directory checkbox and click the Configure action button.

- o In the form that appears, type the Domain name in the text entry area, or select a domain from the pull-down menu. The name of the domain is the same as that for the AD's Kerberos realm.
- o Choose to use an existing account by selecting the radio button associated with the option.
- o Provide the Account Password associated with the account in the text entry area provided. Using this option assumes that the administrator has set up the account in Active Directory manually, and the password provided here is the one that was created during the manual creation of the account.
- o Click Done then click submit.

Part II: Use AD service management tool from Microsoft to create computer and user accounts for the file service and user security principals logging into the Windows 2000 Kerberos domain.

- o Logon AD server as administrator.
- o Go to administration tools to Select the computer folder, right-click and select New, then choose computer. type the name of the TAS file service. The account should be created in any computer container.
- o Use Ktpass to set up the account for the TAS file service. Example:

```
C:> Ktpass -Cprinc HOST/hostname@NT-DNS-REALM-NAME -Cmapuser account$ -pass password
```

where:

- hostname is the host DNS name; for example: superdude.
- NT-DNS-REALM-NAME is the uppercase name of the Windows 2000 domain; for example: FWTEST.WA.LSIL.COM.
- account is the computer account for the computer.
- password is a complex password for the account.

Note: Domain name and password should be carefully type in. It is case sensitive. Uppercase or lowercase mistype may cause a wrong key to be generated.

### ***c) Active Directory File Service Configuration III***

This process is similar to item a), but instead of TNAS, this uses TAS command-line utilities. The user has to be comfortable with Unix command-line utility to use this configuration method.

- o Create an authentication base by using tnauthdb. Example:
 

```
tnauthdb -A -m my_fwtest.wa.lsil.com -a type=actdir \  
-a actdir-account-container=cn=computers \  
-a actdir-domain=fwtest.wa.lsil.com
```
- o Modify TAS CIFS service to use the new authentication base. Example:
 

```
tnservice -M -r NB -s c_account_cm:file \  
-a extended-authent-bases=my_fwtest.wa.lsil.com
```
- o Set krbkey for this service by using tnadkey.

Example:

```
tnadkey -A -s c_account_cm:file -a my_fwtest.wa.lsil.com \  
-p administrator
```

- o Create a computer account by using tnadaccount.

```
tnadaccount -A -s c_account_cm:file -a my_fwtest.wa.lsil.com  
This command will ask for AD server's principal and password.
```

- o The file service is configured.

These TAS commands that are used to set up TAS CIFS file services to use AD authentication:

```
tnauthdb, tnservice, tnadkey, tnadaccount, tnaddir, tnadcheck,  
and tnadservice.
```

### III) Configuration Testing and Checking.

- 1) Connecting to TAS CIFS file service from client.

Client should be Windows NT, Windows 2000 or Windows XP.

User need to logon on active directory domain or use domain user (like fwtest\testuser) to connect the service.

- 2) Check computer account attributes on Active Directory Server.

Run the following command from Unix server to check computer account attributes, where superdude is the AD server and superdudevidal is the CIFS file service.

```
# /opt/totalnet/sbin/ldapsearch -x -h superdude \  
-D "cn=administrator,cn=users,dc=fwtest,dc=wa,dc=lsil,dc=com" \  
-w administrator -b "dc=fwtest,dc=wa,dc=lsil,dc=com " \  
"samaccountname=superdudevidal$"
```

This should return computer account information that looks like this:

```
#  
# filter: samaccountname=manna$  
# requesting: ALL  
#  
# manna, Computers, FWTEST, wa, lsil, com  
dn: CN=manna,CN=Computers,DC=FWTEST,DC=wa,DC=lsil,DC=com  
accountExpires: 9223372036854775807  
badPasswordTime: 0  
badPwdCount: 0  
codePage: 0  
cn: manna  
countryCode: 0  
instanceType: 4  
isCriticalSystemObject: FALSE  
lastLogoff: 0  
lastLogon: 0  
logonCount: 0  
distinguishedName: CN=manna,CN=Computers,DC=FWTEST,DC=wa,DC=lsil,DC=com  
objectCategory: CN=Computer,CN=Schema,CN=Configuration,DC=FWTEST,DC=wa,DC=lsil,  
,DC=com  
objectClass: top  
objectClass: person  
objectClass: organizationalPerson  
objectClass: user  
objectClass: computer
```

```
objectGUID:: t0jhs3TkbEGPZuz3UebvcA==
objectSid:: AQUAAAAAAAAUVAAAA/XexVhUlr0dDFwoySQYAAA==
operatingSystem:: U29sYXJpcyAgICA=
operatingSystemVersion: 2.6
primaryGroupID: 515
pwdLastSet: 126581900123119280
name: manna
sAMAccountName: MANNA$
sAMAccountType: 805306369
servicePrincipalName: HOST/manna
userAccountControl: 2691072
userPrincipalName: HOST/manna@FWTEST.WA.LSIL.COM
uSNChanged: 8762
uSNCreated: 8539
whenChanged: 20020214225212.0Z
whenCreated: 20020213215116.0Z
```

```
# search reference
```

```
ref: ldap://FWTEST.wa.lsil.com/CN=Configuration,DC=FWTEST,DC=wa,DC=lsil,DC=com
```

```
# search result
```

```
search: 2
```

```
result: 0 Success
```

```
# numResponses: 3
```

```
# numEntries: 1
```

```
# numReferences: 1
```

```
# exit
```

```
# exit
```

```
script done on Tue Apr 09 16:31:37 2002
```

### 3) Common problems during AD service configuration

a) Can not find KDC.

Solution: Check DNS configuration.

b) System clock did not synchronize.

Solution: Check time on AD server, TAS server, and workstation.

c) Object can not be found,

Solution: Check domain name, containers, etc.

d) Cannot authenticate.

Solution: Check to make sure that TAS CIFS service isn't set up as NT logon server. For AD to work, Windows server will have to be the NT logon server.