Active Directory as AFS’ KDC

Derrick Brashear
June 14, 2006
Step 1: Active Directory

- Become an admin in your Active Directory domain.
- Manage users.
Managing Your Server Roles

Use the tools and information found here to add or remove roles and perform your daily administrative tasks.

Your server has been configured with the following roles:

**Domain Controller (Active Directory)**

Domain controllers use Active Directory to manage network resources such as users, computers, and applications.

- Add or remove a role
- Read about server roles
- Read about remote administration
- Manage users and computers in Active Directory
- Manage domains and trusts
- Manage sites and services

**60 days left for activation**

To activate Windows now, click here
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>User</td>
<td>Built-in account for admin...</td>
</tr>
<tr>
<td>Cert Publishers</td>
<td>Security Group</td>
<td>Members of this group are...</td>
</tr>
<tr>
<td>Domain Admins</td>
<td>Security Group</td>
<td>Designated administrators...</td>
</tr>
<tr>
<td>Domain Comp...</td>
<td>Security Group</td>
<td>All workstations and serve...</td>
</tr>
<tr>
<td>Domain Contr...</td>
<td>Security Group</td>
<td>All domain controllers in the...</td>
</tr>
<tr>
<td>Domain Guests</td>
<td>Security Group</td>
<td>All domain guests</td>
</tr>
<tr>
<td>Domain Users</td>
<td>Security Group</td>
<td>All domain users</td>
</tr>
<tr>
<td>Enterprise Ad...</td>
<td>Security Group</td>
<td>Designated administrators...</td>
</tr>
<tr>
<td>Group Policy</td>
<td>Security Group</td>
<td>Members in this group can...</td>
</tr>
<tr>
<td>Guest</td>
<td>User</td>
<td>Built-in account for guest ...</td>
</tr>
<tr>
<td>HelpServices...</td>
<td>Security Group</td>
<td>Group for the Help and Support...</td>
</tr>
<tr>
<td>RAS and IAS</td>
<td>Security Group</td>
<td>Servers in this group can...</td>
</tr>
<tr>
<td>Schema Admins</td>
<td>Security Group</td>
<td>Designated administrators...</td>
</tr>
<tr>
<td>SUPPORT_38...</td>
<td>User</td>
<td>This is a vendor’s account ...</td>
</tr>
<tr>
<td>TelnetClients</td>
<td>Security Group</td>
<td>Members of this group have...</td>
</tr>
</tbody>
</table>
Make users

- Here, I created myself.
And services

- Now, create AFS.
- You will be remapping to a principal later, so don’t worry about the name you use here.
When you click Finish, the following object will be created:

Full name: afs
User logon name: afs-adtest@ad.dementia.org
Bind and Export

- Bind a Kerberos principal name
- Export a keytab
- `ktpass` is in the Support Tools directory on your Windows 2003 media.
ktpass.exe

C:\Documents and Settings\Administrator\Desktop>ktpass -princ afs/atest.dementia.org@AD.DEMENTIA.ORG -mapuser afs -pass * -crypto DES-CBC-MD5 -out afs-keytab
Targeting domain controller: win2003.ad.dementia.org
Using legacy password setting method
Successfully mapped afs/atest.dementia.org to afs-atest.
Type the password for afs/atest.dementia.org:
Type the password again to confirm:
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to afs-keytab:
Keytab version: 0x502
keysize 66 afs/atest.dementia.org@AD.DEMENTIA.ORG ptype 0 (KR5_NT_UNKNOWN) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0x374585bc6d5e9783)
C:\Documents and Settings\Administrator\Desktop>
Try It

- Make sure your new realm is in krb5.conf on client(s).
- kinit as a client and see what happens.
default_domain = xp.win.cmu.edu

AD.CMU.EDU = {
    kdc = nt-ad2.ad.cmu.edu
    kdc = nt-ad3.ad.cmu.edu
    admin_server = nt-ad2.ad.cmu.edu
    default_domain = ad.cmu.edu
}

ANDREW.AD.CMU.EDU = {
    kdc = andrew-ad1.andrew.ad.cmu.edu
    kdc = andrew-ad2.andrew.ad.cmu.edu
    admin_server = andrew-ad2.andrew.ad.cmu.edu
    default_domain = andrew.ad.cmu.edu
}

AD.DEMENTIA.ORG = {
    kdc = 10.0.1.60
    default_domain = ad.dementia.org
}

[v4 realms]

ATHENA/MIT.EDU = {
    kdc = kerberos.mit.edu
Resolving www.dementia.org... 128.2.120.184
Connecting to www.dementia.org!128.2.120.184!80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8,003 (7.8K) [text/plain]

100%[================================================]=> 8,003 12.35K/s

10:21:45 (12.34 KB/s) - `edu.mit.Kerberos' saved [8003/8003]

[valdev08:/Library/Preferences] root# vi edu.mit.Kerberos
[valdev08:/Library/Preferences] root# exit
exit
[valdev08:/Library/Preferences] shadow% kinit shadow@AD.DEMENTIA.ORG
Please enter the password for shadow@AD.DEMENTIA.ORG:
[valdev08:/Library/Preferences] shadow% klist
Kerberos 5 ticket cache: 'API:Initial default cache'
Default principal: shadow@AD.DEMENTIA.ORG

Valid Starting Expires Service Principal
06/14/06 10:23:38 06/14/06 10:48:38 krbtgt/AD.DEMENTIA.ORG@AD.DEMENTIA.ORG
renew until 06/21/06 10:23:38

klist: No Kerberos 4 tickets in credentials cache
[valdev08:/Library/Preferences] shadow%
Add to Keyfile

- Copy the keytab you got with ktpass to the AFS server.
- Use asetkey to add the key.
[valdev08:/usr/afs/bin] root# asetkey add 3 '~/afs-keytab afs/adtest.dementia.org @AD,DEMENTIA.ORG
[valdev08:/usr/afs/bin] root# bos listkeys localhost
bos: no such entry (getting tickets)
bos: running unauthenticated
key 3 has checksum 2284460697
All done.
[valdev08:/usr/afs/bin] root#
At this point, tokens you get with aklog are all you need.
```
[va1dev08:~] shadow% kinit shadow@AD.DEMENTIA.ORG
Please enter the password for shadow@AD.DEMENTIA.ORG:
[va1dev08:~] shadow% aklog adtest.dementia.org -k AD.DEMENTIA.ORG
[va1dev08:~] shadow% tokens

Tokens held by the Cache Manager:

User's (AFS ID 100) tokens for afs@adtest.dementia.org [Expires Jun 14 12:41]
--End of list--
[va1dev08:~] shadow%  
```
Consider disabling PACs

• http://support.microsoft.com/kb/832572/en-us
Active Directory as AFS’ KDC

Questions?
shadow@openafs.org