Integrating Sun Kerberos and Microsoft Active Directory Kerberos

Purpose:

This document is designed to guide a Sun Solaris administrator through the process of configuring Solaris 9 clients to use the Microsoft's Windows 2003 Active Directory (AD) Kerberos implementation. Active Directory has two pieces to it, an LDAP piece and a Kerberos piece. This guide leverages integration of the Kerberos piece and not the LDAP piece. Configuration of Active Directory as a naming service via LDAP is beyond the scope of this guide.

Prerequisites:

In order for any kerberized network to be available, both DNS and NTP must be configured for all servers and clients. This guide uses a Solaris server for NTP and an AD server for DNS. This is a matter of convenience as configuring NTP on Solaris is very easy and straightforward. Due to the complexity of SRV and TXT record entries for DNS, the AD server was chosen as a DNS server. This guide does not cover setup of either DNS or NTP as it is expected that the reader already possesses these skills. Here are references to setting up servers for those services:

Network Time Protocol for Solaris 9:
http://docs.sun.com/app/docs/doc/816-4882/6mb2ipq4o?a=view

Active Directory/DNS:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/6bdadfc1-4a8e-4b55-8844-7f784d7ff20b.mspx

Sample host, user, and network information:

DNS Domain: **`exmaple.com`**
Kerberos Realm: **`EXAMPLE.COM`**
AD/DNS Server: **`win2003.example.com`**
Solaris Client: **`solaris.example.com`**
NTP Server: **`ntp.example.com`**
UNIX user: **`darren`**
UNIX user principal: **`darren@EXAMPLE.COM`**

I. Configuring Network Time Protocol for Active Directory

1) Open a command prompt. Click **`Start`**, click **`Run`**..., type **`cmd`**, and click **`OK`**.

2) Using the Windows command shell prompt, sync the AD server to the Solaris server:

```
> net time /setsntp:ntp.example.com
```

3) Test to make sure that the AD has the appropriate NTP server,

```
> net time /querysntp
```

II. Installing Active Directory Kerberos Utilities

The **`ktpass`** command is needed to create a **`keytab`** for the Solaris client. This utility is located on the Windows

2003 Server CD as part of the "Support Tools" kit. There is no option during the install of Windows 2003 Server to install these tools. It must be done after the install of Windows 2003 Server.

1) Open a command prompt. Click **Start** and click **Run**....

2) In the **Run**... window, type the following path: **D:\SUPPORT\TOOLS\SUPTOOLS.MSI**

3) Accept all the default installations for the installation of the tools.

III. Setting Up a UNIX user and Active Directory Kerberos Principal.

Just like standard UNIX based Kerberos server and Unix Posix account, two accounts must be setup in both the AD and on the Solaris client. The username and password must be exactly identical in order for this to work.

On the Solaris client:

Create a new user called **darren**. The default naming service for Solaris is local files and it will be used for this example.

```
# mkdir -p /export/home
# useradd -d /export/home/darren -m -s /usr/bin/bash darren
# passwd darren
New Password: darren2212
Re-enter new Password: darren2212
passwd: passwd successfully changed for darren
```

On the AD server:

1) Click on Start, Programs, Administrative Tools, Active Directory Users and Computers.

2) Click on Action, New, User and start the New user wizard.

3) Fill out all of the information for the user darren. Be sure that the AD username and password match that of the Solaris username and password.

User Login Name: **darren@example.com**
User Password: **darren2212**

III. Configuring the Solaris Client

On the AD Server:

A **keytab** file must be generated for the Solaris client. Since the standard **kadmin** interface to a Unix KDC is unavailable, the AD must create the **keytab** on the Solaris client's behalf. This is done through a command line utility in AD called **ktpass**. This command will create a **keytab** file which must be copied over to the Solaris Client.

1) Open a command prompt. Click **Start**, click **Run**..., type **cmd**, and click **OK**.

2) Use the ktpass command to create the Solaris **keytab** file:

```
> ktpass -princ host/solaris.example.com@EXAMPLE.COM -mapuser solaris -pass solaris9919
-out krb5.keytab
```

Both the "**-mapuser**" and "**-pass**" commands are needed as AD creates one merged identity instead of a unique instance of a user and a principal. In other words, the principal **host/solaris.example.com@EXAMPLE.COM** must be mapped to a username. It can't exist by itself nor could the **ktpass** command just create it by itself.

3) Using whatever means available (**sftp/scp**, USB removable device), copy the **krb5.keytab** over to the Solaris client's **/tmp** directory.

On the Solaris client:

1) As the user root, backup any previous **keytab** files:

```
# cd /etc/krb5
# mv krb5.keytab krb5.keytab.old
# mv /tmp/krb5.keytab /etc/krb5
```

2) Edit the **/etc/krb5/krb5.conf** file to point to the AD server.

```
# vi /etc/krb5/krb5.conf
[libdefaults]
default_realm  =  EXAMPLE.COM
default_tkt_enctypes = des-cbc-md5 ; or des-cbc-crc
default_tgs_enctypes = des-cbc-md5 ; or des-cbc-crc

[realms]
EXAMPLE.COM = {
kdc = win2003.example.com:88
}

[domain_realm]
        example.com = EXAMPLE.COM
        .example.com = EXAMPLE.COM

[logging]
        default = FILE:/var/krb5/kdc.log
        kdc = FILE:/var/krb5/kdc.log

[appdefaults]
        gkadmin = {
                help_url = http://docs.sun.com/app/docs/doc/816-4557/6maosrjk8?a=view
                }
```

3) Edit the **/etc/pam.conf** and uncomment the Kerberos authentication entries.

```
# vi /etc/pam.conf
<<output omitted>>
#
# Support for Kerberos V5 authentication (uncomment to use Kerberos)
#
rlogin          auth optional           pam_krb5.so.1 try_first_pass
login           auth optional           pam_krb5.so.1 try_first_pass
other           auth optional           pam_krb5.so.1 try_first_pass
cron            account optional        pam_krb5.so.1
other           account optional        pam_krb5.so.1
other           session optional        pam_krb5.so.1
other           password optional       pam_krb5.so.1 try_first_pass
```

```
ktelnet auth    required        pam_krb5.so.1   acceptor
krlogin auth    required        pam_krb5.so.1   acceptor
krsh    auth    required        pam_krb5.so.1   acceptor
```

IV. Test the Configuration

The Solaris client should be setup to authenticate and acquire it's Ticket Granting Ticket (TGT). Using the **ssh** command from a remote host, attempt to connect to **solaris.example.com.**

```
bash-3.00# ssh darren@solaris.example.com
darren@solaris.example.com's password:
Last login: Fri Apr 22 12:44:07 2005 from 10.16.200.22
Sun Microsystems Inc.   SunOS 5.9       Generic May 2002
Welcome to Sol9_FCS on solaris.example.com
```

Using **klist**, verify that the user **darren** has received Kerberos credentials from the AD server.

```
-> klist
Ticket cache: /tmp/krb5cc_101
Default principal: darren@EXAMPLE.COM

Valid starting                  Expires                     Service principal
Fri Apr 22 12:44:43 2005  Fri Apr 22 22:44:43 2005  krbtgt/EXAMPLE.COM@EXAMPLE.COM
Fri Apr 22 12:44:43 2005  Fri Apr 22 22:44:43 2005  host/server1.example.com@EXAMPLE.COM
```