Mac OS X Server v10.5 or later: Rebuilding the KDC while maintaining LDAP and PasswordServer databases

Last Modified: January 07, 2010
Article: HT3655

Summary

In certain cases, it may be desirable to rebuild the Kerberos Key Distribution Center (KDC) on a Mac OS X Server v10.5 or later server in a manner that retains the existing databases for LDAP and PasswordServer. The steps outlined in this article will accomplish this.

Note: You must have at least one of the "Recoverable Authentication Methods" (WebDAV-Digest and/or APOP) checked in the Policy tab under Settings for the Open Directory service in Server Admin, otherwise passwords will not be recreated properly.

Important: You should back up the files mentioned in the steps below prior to editing or deleting them.

Products Affected

Mac OS X Server 10.5, Mac OS X Server 10.6

1. If a KDC is currently running on the server, stop the process by entering the following commands in Terminal:
   Mac OS X Server v10.5 commands:

```
sudo -s
launchctl unload /System/Library/LaunchDaemons/com.apple.kdcmond.plist 2>/dev/null
launchctl unload /System/Library/LaunchDaemons/edu.mit.kadmind.plist 2>/dev/null
```

   Mac OS X Server v10.6 commands:

```
sudo -s
launchctl unload /System/Library/LaunchDaemons/edu.mit.Kerberos.krb5kdc.plist 2>/dev/null
launchctl unload /System/Library/LaunchDaemons/edu.mit.Kerberos.kadmind.plist 2>/dev/null
```

2. In Terminal, navigate to the /var/db/krb5kdc/ directory and remove Kerberos principal files:

```
# cd /var/db/krb5kdc
```

   Remove all files prefixed with principal.<REALMNAME> (for example, principal.SERVER1.APPLE.COM). Do NOT remove the files prefixed with principal.LKDC.

```
# rm principal.<REALMNAME>*
```

3. While still in the /var/db/krb5kdc/ folder, edit the kdc.conf file using a command-line text editor (such as VI or nano) and remove the server realm information from the file. For example, a file that looks like this:

```
## This file autogenerated by KDCSetup from (null) ##
[libdefaults]
        default_realm = SERVER1.APPLE.COM

[kdcdefaults]
        kdc_ports = 88
        kdc_tcp_ports = 88

[realms]
        SERVER1.APPLE.COM = {
                kadmind_port = 749
                max_life = 10h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                master_key_type = des3-hmac-sha1
                supported_enctypes = des3-hmac-sha1:normal arcfour-hmac-md5:normal des-cbc-crc:normal des-cbc-crc:v4
                acl_file = /var/db/krb5kdc/kadm5.acl
                admin_keytab = /var/db/krb5kdc/kadm5.keytab
                database_name = /var/db/krb5kdc/principal.SERVER1.APPLE.COM
                key_stash_file = /var/db/krb5kdc/.k5.SERVER1.APPLE.COM
        }
```

```
                LKDC:SHA1.D9778E7719119E1359ABC67ACDDE16DDA1E3378C = {
                        kadmind_port = 749
                        max_life = 10h 0m 0s
                        max_renewable_life = 7d 0h 0m 0s
                        master_key_type = des3-hmac-sha1
                        supported_enctypes = des3-hmac-sha1:normal arcfour-hmac-md5:normal des-cbc-crc:normal des-cbc-crc:v4
                        acl_file = /var/db/krb5kdc/kadm5.acl
                        admin_keytab = /var/db/krb5kdc/kadm5.keytab
                        database_name = /var/db/krb5kdc/principal.LKDC:SHA1.D9778E7719119E1359ABC67ACDDE16DDA1E3378C
                        key_stash_file = /var/db/krb5kdc/.k5.LKDC:SHA1.D9778E7719119E1359ABC67ACDDE16DDA1E3378C
                }
        [logging]
                kdc = FILE:/var/log/krb5kdc/kdc.log
                admin_server = FILE:/var/log/krb5kdc/kadmin.log
```

should be edited to look like this:

```
        ## This file autogenerated by KDCSetup from (null) ##
        [libdefaults]
                default_realm =

        [kdcdefaults]
                kdc_ports = 88
                kdc_tcp_ports = 88

        [realms]
                LKDC:SHA1.D9778E7719119E1359ABC67ACDDE16DDA1E3378C = {
                        kadmind_port = 749
                        max_life = 10h 0m 0s
                        max_renewable_life = 7d 0h 0m 0s
                        master_key_type = des3-hmac-sha1
                        supported_enctypes = des3-hmac-sha1:normal arcfour-hmac-md5:normal des-cbc-crc:normal des-cbc-crc:v4
                        acl_file = /var/db/krb5kdc/kadm5.acl
                        admin_keytab = /var/db/krb5kdc/kadm5.keytab
                        database_name = /var/db/krb5kdc/principal.LKDC:SHA1.D9778E7719119E1359ABC67ACDDE16DDA1E3378C
                        key_stash_file = /var/db/krb5kdc/.k5.LKDC:SHA1.D9778E7719119E1359ABC67ACDDE16DDA1E3378C
                }
        [logging]
                kdc = FILE:/var/log/krb5kdc/kdc.log
                admin_server = FILE:/var/log/krb5kdc/kadmin.log
```

4. Remove the KerberosClient and KerberosKDC records from the LDAP node. Substitute the name of your OD directory administrator for USERNAME:

```
dscl -u USERNAME /LDAPv3/127.0.0.1 rm /Config/KerberosClient
dscl -u USERNAME /LDAPv3/127.0.0.1 rm /Config/KerberosKDC
```

5. Restart the KDC:
   Mac OS X Server v10.5 commands:

```
launchctl load /System/Library/LaunchDaemons/com.apple.kdcmond.plist
launchctl load /System/Library/LaunchDaemons/edu.mit.kadmind.plist
```

   Mac OS X Server v10.6 commands:

```
launchctl load /System/Library/LaunchDaemons/edu.mit.Kerberos.krb5kdc.plist
launchctl load /System/Library/LaunchDaemons/edu.mit.Kerberos.kadmind.plist
```

6. Type the following command to re-Kerberize the server. Substitute the name of your OD directory administrator for USERNAME and the name of your realm (for example, SERVER1.APPLE.COM) for REALMNAME:

```
# slapconfig -kerberize -f --allow_local_realm USERNAME REALMNAME
```

   Note: This final command outputs its progress to the terminal. If you see lines such as the following, you can disregard them:

```
WARNING: no policy specified for server1.apple.com@SERVER1.APPLE.COM; defaulting to no policy
add_principal: Principal or policy already exists while creating "server1.apple.com$@SERVER1.APPLE.COM".
WARNING: no policy specified for root@SERVER1.APPLE.COM; defaulting to no policy
add_principal: Principal or policy already exists while creating "root@SERVER1.APPLE.COM".
```