Prev Next

12.5. Configuring Kerberos

Kerberos v5 must be deployed on the system to utilize the **GSS-API** mechanism for SASL authentication. Table 12.1, "Supported Kerberos Systems" summarizes the Kerberos applications supported by various platforms. **GSS-API** and Kerberos client libraries must be installed on the Directory Server host to take advantage of Kerberos services.

Operating System	Kerberos Version
Linux	MIT Kerberos version 5
HP-UX 11i	HP Kerberos version 2.1
Sun Solaris	SEAM 1.0.1

Table 12.1. Supported Kerberos Systems

12.5.1. Realms

A *realm* is a set of users and the authentication methods for those users to access the realm. A realm resembles a fully-qualified domain name and can be distributed across either a single server or a single domain across multiple machines. A single server instance can also support multiple realms.

Realms are used by the server to associate the DN of the client in the following form, which looks like an LDAP DN:

```
uid=user_name/[server_instance],cn=realm,cn=mechanism,cn=auth
```

> **NOTE**
>
> Kerberos systems treat the Kerberos realm as the default realm; other systems default to the server.

Mike Connors in the **engineering** realm of the European division of **example.com** would have the following association if he tried to access a different server, such as **cyclops**:

```
uid=mconnors/cn=Europe.example.com,
cn=engineering,cn=gssapi,cn=auth
```

Babara Jensen in the **accounting** realm of **US.example.com** would not have to specify a realm:

```
uid=bjensen,cn=accounting,cn=gssapi,cn=auth
```

If realms are supported by the mechanism and the default realm was not used, *realm* must be specified; otherwise, it is omitted. Currently, only **GSS-API** supports the concept of realms.

12.5.2. Configuring the KDC Server

To use **GSS-API**, the user first obtains a ticket granting ticket (TGT). In many systems, this TGT is issued when the user first logs into the operating system. There are usually command-line utilities provided with the operating system — **kinit**, **klist**, and **kdestroy** — that can be used to acquire, list, and destroy the TGT. The ticket and the ticket's lifetime are parameters in the Kerberos client and server configuration.

Refer to the operating system documentation for information on installing and configuring a Kerberos server (also called a *key distribution center* or KDC). Configuring a KDC for Directory Server is described in Section 12.5.3, "Example: Configuring an Example KDC Server".

> **NOTE**
>
> On Red Hat Enterprise Linux, the client-side Kerberos configuration is in the **/etc/krb5.conf**.
> On Solaris, the client-side Kerberos configuration is in the **/etc/krb5/krb5.conf**.
> The HP server and client are separate packages with their own configuration. The server stores config files in **/opt/krb5**. The client is classic MIT and uses **/etc/krb5.conf**. Both the server and client must be configured to have a working Kerberos system.

In order to respond to Kerberos operations, the Directory Server requires access to its own cryptographic key. This key is read by the Kerberos libraries that the server calls, through **GSS-API**, and the details of how it is found are implementation-dependent. However, in current releases of the supported Kerberos implementations, the mechanism is the same: the key is read from a file called a *keytab* file. This file is created by the Kerberos administrator by exporting the key from the KDC. Either the system default keytab file (typically **/etc/krb5.keytab**) is used, or a service-specific keytab file determined by the value of the **KRB5_KTNAME** environment variable; this environment variable can be set in the **start-slapd** script, which is recommended because it ensures that the variable is properly set each time Directory Server starts.

The Directory Server uses the service name **ldap**. Its Kerberos principal is **ldap**/*host-fqdn*@*realm*, like **ldap/dap.corp.example.com/EXAMPLE.COM**. The *host-fqdn* must be the fully-qualified host and domain name, which can be resolved by all LDAP and Kerberos clients through both DNS and reverse DNS lookups. A key with this identity must be stored in the server's **keytab** in order for Kerberos to work.

For information on setting up the service key, see the Kerberos documentation.

12.5.3. Example: Configuring an Example KDC Server

This example code shows a KDC server configured with the **company.example.com** realm.

```
[libdefaults]
     ticket_lifetime = 24000
     default_realm = COMPANY.EXAMPLE.COM
     dns_lookup_realm = false
     dns_lookup_kdc = false
     ccache_type = 1
     forwardable = true
     proxiable = true
     default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
     default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
     permitted_enctypes = des3-hmac-sha1 des-cbc-crc
[realms]
```

```
  COMPANY.EXAMPLE.COM = {
     kdc = kdcserver.company.example.com:88
     admin_server =adminserver.company.example.com:749
     default_domain = company.example.com
  }
[appdefaults]
  pam = {
     debug = true
     ticket_lifetime = 36000
     renew_lifetime = 36000
     forwardable = true
     krb4_convert = false
  }
[logging]
  default = FILE:/var/krb5/kdc.log
  kdc = FILE:/var/krb5/kdc.log
  admin_server = FILE:/var/log/kadmind.log
```

12.5.4. Configuring SASL Authentication at Directory Server Startup

SASL GSS-API authentication has to be activated in Directory Server so that Kerberos tickets can be used for authentication. This is done by supplying a system configuration file for the init scripts to use which identifies the variable to set the keytab file location. When the init script runs at Directory Server startup, SASL authentication is then immediately active.

The default configuration file is in **/etc/sysconfig/dirsrv**.

> **NOTE**
>
> The default configuration file on Red Hat Enterprise Linux and HP-UX is in **/etc/sysconfig**. On Solaris, it is in **/etc/default**.

If there are multiple Directory Server instances and not all of them will use SASL authentication, then there can be instance-specific configuration files created in that directory named **dirsrv-***instance*. For example, **dirsrv-example**. The default **dirsrv** file can be used for a single instance.

To enable SASL authentication, uncomment the **KRB5_KTNAME** line in the **/etc/sysconfig/dirsrv** (or instance-specific) file, and set the keytab location for the **KRB5_KTNAME** variable. For example:

```
# In order to use SASL/GSSAPI the directory
# server needs to know where to find its keytab
# file - uncomment the following line and set
# the path and filename appropriately
KRB5_KTNAME=/etc/krb5.keytab ; export KRB5_KTNAME
```

For more information on the keytab file, see Section 12.5.2, “Configuring the KDC Server”.