Novell Kerberos KDC

1.5

April 8, 2008

QUICK START

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

Third-Party Materials

Contents

About This Guide

Kerberos is a standard protocol that provides a means of authenticating entities on a network and is based on a trusted third-party model. It involves shared secrets and uses symmetric key cryptography. Traditional Kerberos implementations store relevant Kerberos information pertaining to a realm in a database. Database propagation between KDCs are handled by vendor-specific protocols.

Novell® Kerberos KDC integrates Kerberos Authentication, Administration, and Password servers with eDirectory as data store. It moves Kerberos-specific data to eDirectory and provides Kerberos services using a KDC that accesses data stored in eDirectory. Novell® Kerberos KDC provides the ease of single point of management for deployments with both Kerberos and Novell eDirectory™, and gives the advantage of eDirectory replication and security capabilities.

This guide describes how to install and configure Novell Kerberos KDC.

Audience

The guide is intended for Novell eDirectory™ or Kerberos administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the Novell Kerberos KDC 1.5 Quick Start, visit http://www.novell.com/documentation/kdc15/index.html (http://www.novell.com/documentation/kdc15/index.html).

Additional Documentation

- Novell eDirectory 8.8 Documentation (http://www.novell.com/documentation/edir88/index.html)
- Kerberos Documentation (http://web.mit.edu/kerberos/www/)

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol ($^{®}$, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Installing Novell Kerberos KDC

1

Novell® Kerberos KDC is a network authentication protocol that uses the Key Distribution Center (KDC) to integrate the Kerberos Authentication, Administration, and Password servers with eDirectory™. Novell Kerberos KDC is derived from the MIT implementation of Kerberos (http://web.mit.edu/kerberos).

This section describes how to install Novell Kerberos KDC and has the following information:

- Section 1.1, "Prerequisites," on page 9
- Section 1.2, "Installing Novell Kerberos KDC by Using YaST," on page 9

1.1 Prerequisites

❑ Open Enterprise Server (OES) 2.0 on Linux.

❑ Novell eDirectory 8.8 SP2 or later on OES 2.0 or SUSE® Linux Enterprise Server (SLES) 10 SP1.

eDirectory and Novell Kerberos KDC can be installed on different machines.

❑ Root privileges to install Novell Kerberos KDC.

❑ Synchronized network server time

You must synchronize the time on eDirectory, KDC, Administration server, Password server, kerberized applications, and the client hosts.

For information on synchronizing network time, refer to the OES 2.0 documentation (http://www.novell.com/documentation/oes2/ oes_implement_lx_nw/index.html?page=/documentation/oes2/oes_implement_lx_nw/data/ time.html#time-implement).

To install iManager plug-ins:

❑ iManager 2.7 installed.

For installation information, refer to the *Novell iManager 2.7 Installation Guide* (http://www.novell.com/documentation/imanager27/imanager_install_27/index.html?page=/documentation/imanager27/imanager_install_27/data/hk42s9ot.html).

❑ Trusted root certificate imported into the keystore.

For more information, refer to the *Novell iManager 2.7 Administration Guide* (http://www.novell.com/documentation/imanager27/imanager_admin_27/index.html?page=/documentation/imanager27/imanager_admin_27/data/hk42s9ot.html).

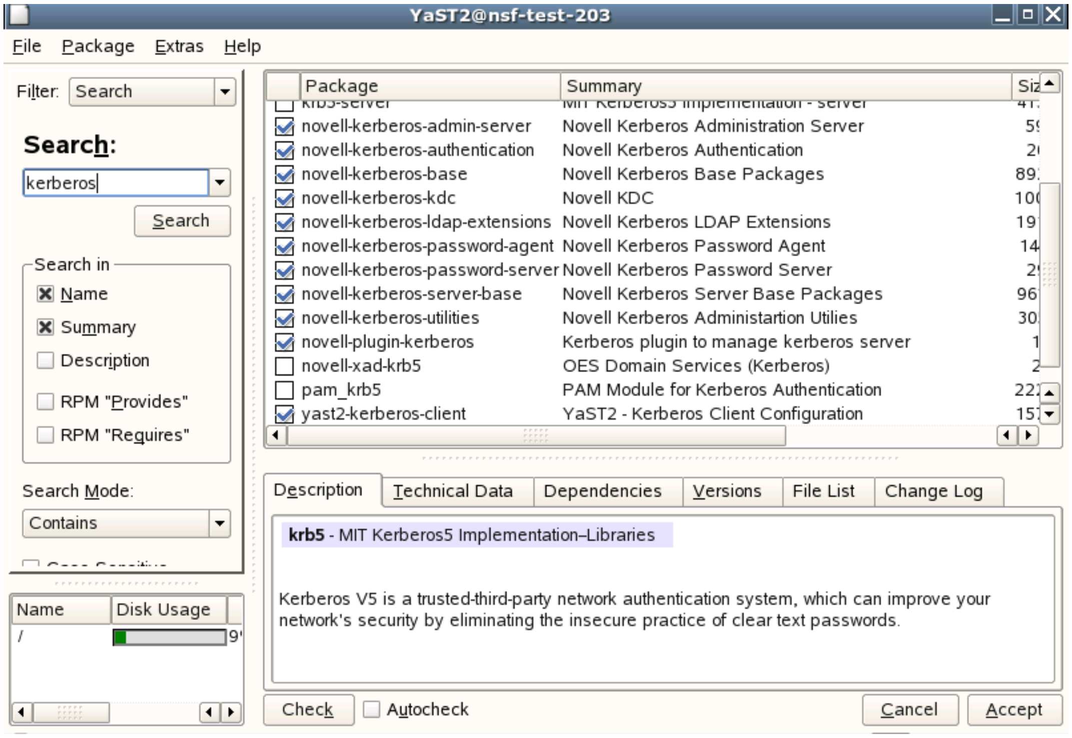
1.2 Installing Novell Kerberos KDC by Using YaST

1 Start *yast2.*

2 Click software > software management.

3 Filter for Kerberos packages, then select the following packages:

Package	Description
NKDC	
novell-kerberos-base	The base package necessary for both servers and clients.
novell-kerberos-server-base	The base package necessary for KDC, the Administration server, and the Password server.
novell-kerberos-kdc	Contains the KDC server, which stores all the principal and realm information in eDirectory.
novell-kerberos-admin-server	Contains the Administration server. This is the server component of the Kerberos Administration solution for maintaining Kerberos principals, policies, and service key tables (keytabs).
novell-kerberos-password-server	Contains the server component of the Kerberos Password utility for changing passwords of Kerberos principals.
novell-kerberos-utilities	Contains the Kerberos utilities, such as: ◆ kdb5_ldap_util ◆ kadmin.local
Kerberos LDAP Extension and Password Agent	
novell-kerberos-ldap-extensions	Contains the Kerberos LDAP extensions, which services requests for storing and retrieving various Kerberos-specific keys from eDirectory.
novell-kerberos-password-agent	Contains the Kerberos Password Agent, which synchronizes the Kerberos passwords or keys with a universal password.



Filter: Search

Search: kerberos

Search in

☒ Name

☒ Summary

☐ Description

☐ RPM "Provides"

☐ RPM "Requires"

Search Mode: Contains

Name	Disk Usage
/	9'

	Package	Summary	Siz
☐	krb5-server	MIT Kerberos5 Implementation - server	41.
☑	novell-kerberos-admin-server	Novell Kerberos Administration Server	5!
☑	novell-kerberos-authentication	Novell Kerberos Authentication	2(
☑	novell-kerberos-base	Novell Kerberos Base Packages	89.
☑	novell-kerberos-kdc	Novell KDC	10(
☑	novell-kerberos-ldap-extensions	Novell Kerberos LDAP Extensions	19
☑	novell-kerberos-password-agent	Novell Kerberos Password Agent	14
☑	novell-kerberos-password-server	Novell Kerberos Password Server	2!
☑	novell-kerberos-server-base	Novell Kerberos Server Base Packages	96
☑	novell-kerberos-utilities	Novell Kerberos Administartion Utilies	30.
☑	novell-plugin-kerberos	Kerberos plugin to manage kerberos server	1
☐	novell-xad-krb5	OES Domain Services (Kerberos)	2
☐	pam_krb5	PAM Module for Kerberos Authentication	22.
☑	yast2-kerberos-client	YaST2 - Kerberos Client Configuration	15.

Description | Technical Data | Dependencies | Versions | File List | Change Log

krb5 - MIT Kerberos5 Implementation–Libraries

Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of clear text passwords.

☐ Autocheck

You can install KDC, the Administration server, the Password server, and eDirectory on different machines.

The Kerberos LDAP Extension must be installed on all the eDirectory servers that will be accessed by the Kerberos services.

The Kerberos Password Agent must be installed on all the eDirectory servers (with writable replicas) that the users will be using for changing their passwords.

If you have installed iManager, the Kerberos plug-in is installed by default. If the Kerberos plug-in is not installed, select the novell-plugin-kerberos package to install it.

4 Click *Accept* to install Novell Key Distribution Center.

Configuring Novell Kerberos KDC 2

After installing Novell® Kerberos KDC, you need to configure it. This section has the following information:

- Section 2.1, "Prerequisites," on page 13
- Section 2.2, "Configuring eDirectory for Novell Kerberos KDC," on page 13
- Section 2.3, "Modifying the Novell Kerberos KDC Configuration File," on page 14
- Section 2.4, "Configuring Novell Kerberos KDC Services," on page 15
- Section 2.5, "Starting the Servers," on page 16
- Section 2.6, "Viewing the Log Files," on page 16

2.1 Prerequisites

Before you proceed with the configuration, make sure of the following:

- The eDirectory server is running on the same machine or on any other machine on the same network.
- All packages for Novell Kerberos KDC are installed.
- The Kerberos LDAP Extension and Kerberos Password Agent (KPA) on the eDirectory™ server are installed.
- The Novell C LDAP SDK is installed on the host. The packages, `novell-NLDAPsdk` and `novell-NLDAPbase` are available in OES2.0.
- The Novell Kerberos KDC configuration file exists in the `/etc` directory. If the file is does not exist, then copy the sample `krb5.conf` file from `/opt/novell/kerberos` to the `/etc` directory.
- The Novell Kerberos KDC is compatible with the MIT Kerberos and you can use the client utilities of MIT Kerberos with the Novell Kerberos KDC.

2.2 Configuring eDirectory for Novell Kerberos KDC

1. Export the trusted root certificate to `/opt/novell/kerberos/Trustedroot.der`
2. Extend the eDirectory schema by extending the `/opt/novell/kerberos/schema/kerberos.ldif` file as follows:

   ```
   /opt/novell/eDirectory/bin/ldapmodify -D admin_dn -W -H ldapuri
   -f /opt/novell/kerberos/schema/kerberos.ldif -e
   trusted_root_certificate -c
   ```

   For example:

   ```
   /opt/novell/eDirectory/bin/ldapmodify -D cn=admin,o=mit -W -H
   ldaps://kerberos.mit.edu -f /opt/novell/kerberos/schema/
   kerberos.ldif -e
   /opt/novell/kerberos/Trustedroot.der -c
   ```

You can also extend the schema through Novell iManager as follows:

2a In Novell iManager, click the *Roles and Tasks* button .

2b Select *Kerberos Management* > *Extend Schema*.

2c Click *OK* to extend the schema.

3 Configure Kerberos LDAP extensions on the eDirectory server.

3a Make sure that the Kerberos LDAP extensions are installed on the machine where eDirectory is installed.

The Kerberos LDAP extensions library `libkrbpwd.so` is installed in `/opt/novell/eDirectory/lib/nds-modules`.

3b Add the Kerberos LDAP extensions to eDirectory as follows:

```
kdb5_ldap_util [-D user_dn] [-w passwd] [-H ldapuri] [-t
trusted_cert] ldapxtn_info -add|-clear
```

For example:

```
kdb5_ldap_util -D cn=admin,o=mit -w novell -H ldaps://
kerberos.mit.edu -t /opt/novell/kerberos/Trustedroot.der
ldapxtn_info -add
```

Make sure that you run this command on the machine where Kerberos client package (novell-kerberos-utilities) is installed.

3c Unload nldap:

```
/opt/novell/eDirectory/sbin/nldap -u
```

3d Load nldap:

```
/opt/novell/eDirectory/sbin/nldap -l
```

4 Configure the Kerberos Password Agent on the eDirectory server:

You need to configure the Kerberos Password Agent if you want to integrate universal password with Novell Kerberos KDC.

4a Make sure that the Password Agent package is installed on the machine where eDirectory is running.

4b Start the Kerberos Password Agent as follows:

```
/opt/novell/kerberos/sbin/kpa -l
```

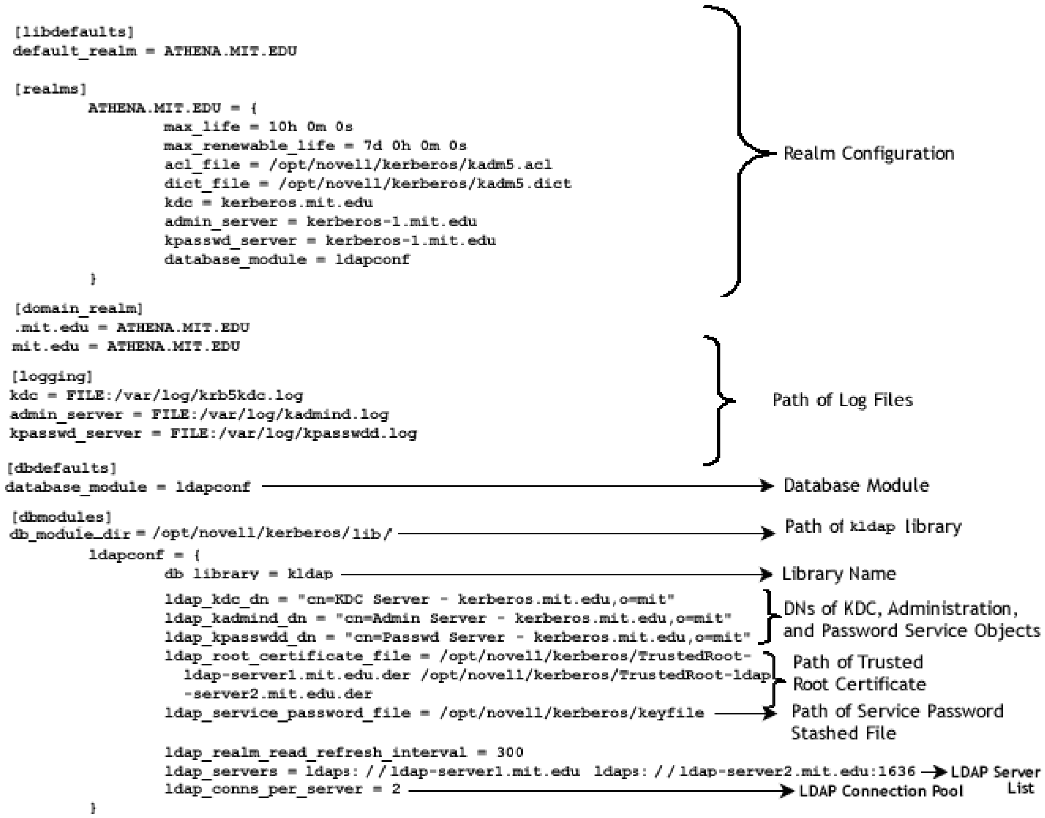
2.3 Modifying the Novell Kerberos KDC Configuration File

We have provided you with a sample `krb5.conf` file. To use it, copy it from the `/opt/novell/krberos` directory to the `/etc` directory.

When you configure Novell Kerberos KDC, if you do not specify a mandatory parameter, it is taken from the `krb5.conf` file.

Modify the `/etc/krb5.conf` file to include the following information:

Figure 2-1 *Sample Configuration file*



```
[libdefaults]
default_realm = ATHENA.MIT.EDU

[realms]
        ATHENA.MIT.EDU = {
                max_life = 10h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                acl_file = /opt/novell/kerberos/kadm5.acl
                dict_file = /opt/novell/kerberos/kadm5.dict
                kdc = kerberos.mit.edu
                admin_server = kerberos-1.mit.edu
                kpasswd_server = kerberos-1.mit.edu
                database_module = ldapconf
        }
[domain_realm]
.mit.edu = ATHENA.MIT.EDU
mit.edu = ATHENA.MIT.EDU

[logging]
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
kpasswd_server = FILE:/var/log/kpasswdd.log

[dbdefaults]
database_module = ldapconf

[dbmodules]
db_module_dir = /opt/novell/kerberos/lib/
        ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=KDC Server - kerberos.mit.edu,o=mit"
                ldap_kadmind_dn = "cn=Admin Server - kerberos.mit.edu,o=mit"
                ldap_kpasswdd_dn = "cn=Passwd Server - kerberos.mit.edu,o=mit"
                ldap_root_certificate_file = /opt/novell/kerberos/TrustedRoot-
                  ldap-server1.mit.edu.der /opt/novell/kerberos/TrustedRoot-ldap
                  -server2.mit.edu.der
                ldap_service_password_file = /opt/novell/kerberos/keyfile

                ldap_realm_read_refresh_interval = 300
                ldap_servers = ldaps: //ldap-server1.mit.edu  ldaps: //ldap-server2.mit.edu:1636
                ldap_conns_per_server = 2
        }
```

Realm Configuration
Path of Log Files
Database Module
Path of kldap library
Library Name
DNs of KDC, Administration, and Password Service Objects
Path of Trusted Root Certificate
Path of Service Password Stashed File
LDAP Server List
LDAP Connection Pool

2.4 Configuring Novell Kerberos KDC Services

Configure the KDC server as follows:

1 Create a realm. From the `/opt/novell/kerberos/sbin/` directory, enter the following:

```
kdb5_ldap_util -D admin_dn -H ldapuri create -subtrees subtree
```

For example:

```
kdb5_ldap_util -D cn=admin,o=mit -H ldaps://kerberos.mit.edu create
-subtrees o=mit
```

You can also create a realm through iManager as follows:

1a In Novell iManager, click the *Roles and Tasks* button .

1b Select *Kerberos Management* > *New Realm*.

For more information, refer to the online help available in iManager.

The realm is created under the cn=kerberos,cn=security container by default.

2 Create the KDC, Administration, and Password service objects in eDirectory by using the kdb5_ldap_util utility. The kdb5_ldap_util utility is present in the `/opt/novell/kerberos/sbin/` directory:

```
kdb5_ldap_util -D admin_dn create_service {-kdc | -admin | -pwd} -
realm realm_list [-randpw|-fileonly] -f filename servicedn
```

The keyfile name for all the services should be the same. It also needs to match the value of the ldap_service_password_file parameter in the `/etc/krb5.conf` file.

For example, to create a KDC server object:

```
kdb5_ldap_util -D cn=admin,o=mit create_service -kdc -realm
ATHENA.MIT.EDU
-randpw -f /opt/novell/kerberos/keyfile "cn=kdc-service,o=mit"
```

Similarly, create the Administration and Password service objects.

If you are creating the service objects with iManager, you must run kdb5_ldap_util to set the passwords as follows:

```
kdb5_ldap_util -D admin_dn setsrvpw [-randpw|-fileonly] [-f
filename] service_dn
```

For example, to set the password of the service objects:

```
kdb5_ldap_util -D cn=admin,o=mit setsrvpw -randpw -f /opt/novell/
kerberos/keyfile "cn=kdc-server,o=mit"
```

The service passwords are encrypted with NICI keys, so the keyfile cannot be moved to other hosts and used from there. Because the encryption keys are specific to the hosts and are not accessible from browsers, iManager does not provide an option to cache the service passwords.

3 Create the `kadm5.acl` file in `/opt/novell/kerberos/kadm5.acl` with "* *" as its content.

Administrative privileges for the Kerberos data are stored in the kadm5.acl file.

IMPORTANT: By using "* *" in the file, you give all privileges to all principals. After creating a principal, you must update this file with appropriate administrative privileges for that principal. For details, refer to the *Novell Kerberos KDC Administration Guide* (http://www.novell.com/documentation/).

2.5 Starting the Servers

1 Start the KDC server:

```
/etc/init.d/krb5kdc start
```

2 Start the Administration server:

```
/etc/init.d/kadmind start
```

3 Start the Password server:

```
/etc/init.d/kpasswdd start
```

2.6 Viewing the Log Files

The messages from the KDC, Administration, and Password servers are logged into the following log files, by default:

***Table 2-1** Log File Paths*

Services	Log File Name
KDC	`/var/log/krb5kdc.log`
Administration	`/var/log/kadmind.log`
Password	`/var/log/kpasswdd.log`

You can change the path of the log files by specifying the new path in the `krb5.conf` file. For more information, see Section 2.3, "Modifying the Novell Kerberos KDC Configuration File," on page 14.

Deconfiguring and Uninstalling Novell Kerberos KDC components

3

To deconfigure and uninstall the Novell® Kerberos KDC components, complete the tasks below:

- Section 3.1, "Destroying the Kerberos Services," on page 19
- Section 3.2, "Destroying the Realm," on page 19
- Section 3.3, "Unloading the Kerberos Password Agent," on page 19
- Section 3.4, "Clearing LDAP Kerberos Extension Information," on page 20
- Section 3.5, "Uninstalling Kerberos Components by Using YaST," on page 20

3.1 Destroying the Kerberos Services

Destroy the Kerberos services (KDC, Administration server, and Password server).

1 Stop the daemon (krb5kdc, kadmind, or kpasswdd)

2 Destroy the service object as follows:

```
kdb5_ldap_util [-D user_dn] [-H ldapuri] [-t trusted_cert]
destroy_service [-f stashfilename] service_dn
```

For example:

```
kdb5_ldap_util -D cn=admin,o=mit destroy_service -f /opt/novell/
kerberos/keyfile cn=kdc-service,o=mit
```

IMPORTANT: If you destroy a Kerberos service without stopping the daemon, the service continues to serve the incoming requests because it has an active connection with the LDAP server.

3.2 Destroying the Realm

1 Destroy the realm by using kdb5_ldap_util as follows:

```
kdb5_ldap_util [-D user_dn] [-H ldapuri] [-t trusted_cert]
destroy [-f] [-r realm]
```

For example:

```
kdb5_ldap_util -D cn=admin,o=mit destroy -r ATHENA.MIT.EDU
```

3.3 Unloading the Kerberos Password Agent

1 Unload the Kerberos Password Agent as follows:

```
/opt/novell/kerberos/sbin/kpa -u
```

3.4 Clearing LDAP Kerberos Extension Information

Clear LDAP Kerberos Extension information from the LDAP server object:

1 Clear the extensionInfo by using kdb5_ldap_util

```
kdb5_ldap_util [-D user_dn] [-H ldapuri] [-t trusted_cert]
ldapxtn_info -clear
```

For example:

```
kdb5_ldap_util -D cn=admin,o=mit ldapxtn_info -clear
```

2 Restart the nldap server as follows:

```
/opt/novell/eDirectory/sbin/nldap -u
```

```
/opt/novell/eDirectory/sbin/nldap -l
```

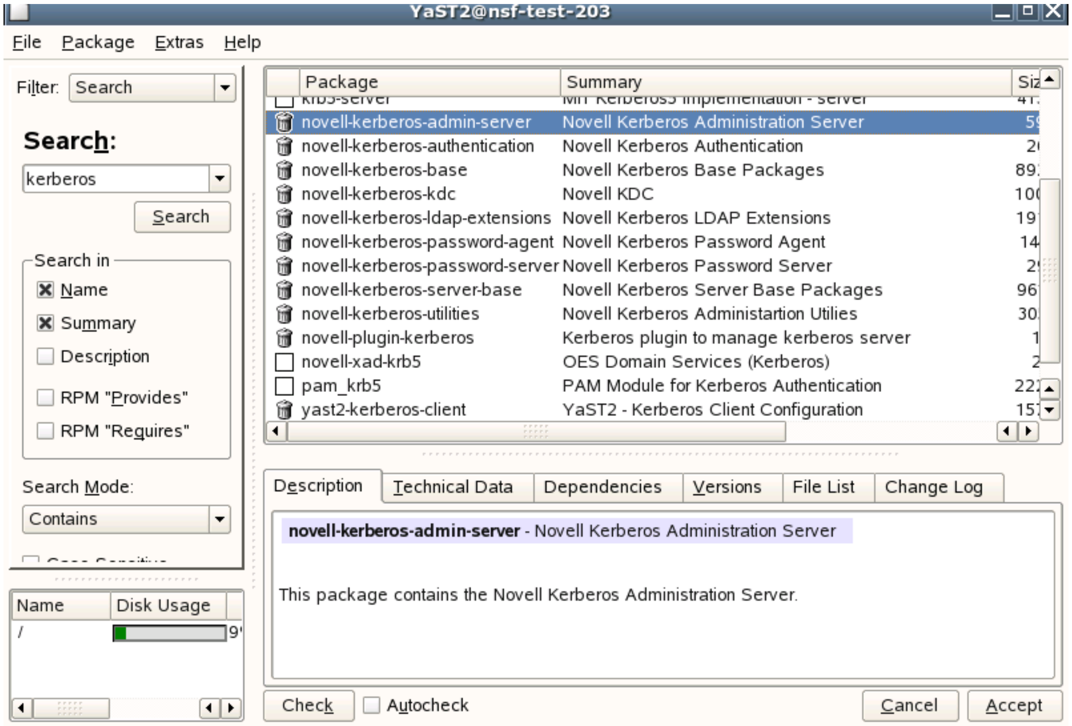
3.5 Uninstalling Kerberos Components by Using YaST

You must stop the eDirectory server before uninstalling the LDAP extension and the Password Agent package

1 Start *yast2*.

2 Click software > software management.

3 Select *Search* from the *Filter* drop-down list, specify `Kerberos` in the *Search Text* box, and click *Search*.



Filter: Search

Search: kerberos

Search in
☒ Name
☒ Summary
☐ Description
☐ RPM "Provides"
☐ RPM "Requires"

Search Mode: Contains

	Package	Summary	Siz
☐	krb5-server	MIT Kerberos5 implementation - server	41
🗑	novell-kerberos-admin-server	Novell Kerberos Administration Server	5
🗑	novell-kerberos-authentication	Novell Kerberos Authentication	2
🗑	novell-kerberos-base	Novell Kerberos Base Packages	89
🗑	novell-kerberos-kdc	Novell KDC	10
🗑	novell-kerberos-ldap-extensions	Novell Kerberos LDAP Extensions	19
🗑	novell-kerberos-password-agent	Novell Kerberos Password Agent	14
🗑	novell-kerberos-password-server	Novell Kerberos Password Server	2
🗑	novell-kerberos-server-base	Novell Kerberos Server Base Packages	96
🗑	novell-kerberos-utilities	Novell Kerberos Administartion Utilies	30
🗑	novell-plugin-kerberos	Kerberos plugin to manage kerberos server	1
☐	novell-xad-krb5	OES Domain Services (Kerberos)	2
☐	pam_krb5	PAM Module for Kerberos Authentication	22
🗑	yast2-kerberos-client	YaST2 - Kerberos Client Configuration	15

Name	Disk Usage
/	🟩 9

novell-kerberos-admin-server - Novell Kerberos Administration Server

This package contains the Novell Kerberos Administration Server.

4. Right-click the package you want to delete, click *Delete*, then click *Accept* to uninstall. For more information see, Chapter 1, “Installing Novell Kerberos KDC,” on page 9.

Sample krb5.conf File

A

A sample krb5.conf file is provided in the /opt/novell/kerberos/ directory. You can use the /etc/krb5.conf configuration file to set the default values. While managing Novell® Kerberos KDC, if you do not specify any of the mandatory parameters, the values specified in /etc/krb5.conf file are used. This file looks similar to the following:

```
[libdefaults]
      default_realm = ATHENA.MIT.EDU

[realms]
        ATHENA.MIT.EDU = {
                max_life = 10h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                acl_file = /opt/novell/kerberos/kadm5.acl
                dict_file = /opt/novell/kerberos/kadm5.dict
                kdc = kerberos.mit.edu
                admin_server = kerberos-1.mit.edu
                kpasswd_server = kerberos-1.mit.edu
                database_module = ldapconf
        }

[domain_realm]
      .mit.edu = ATHENA.MIT.EDU
      mit.edu = ATHENA.MIT.EDU

[logging]
      kdc = FILE:/var/log/krb5kdc.log
      admin_server = FILE:/var/log/kadmind.log
      kpasswd_server = FILE:/var/log/kpasswdd.log

[dbdefaults]
      database_module = ldapconf

[dbmodules]
db_module_dir=/opt/novell/kerberos/lib/
        ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=KDC Server - kerberos.mit.edu,o=mit"
                ldap_kadmind_dn = "cn=Admin Server - 
kerberos.mit.edu,o=mit"
                ldap_kpasswdd_dn = "cn=Passwd Server - 
kerberos.mit.edu,o=mit"
                ldap_root_certificate_file = /opt/novell/kerberos/
Trustedroot.der
                ldap_service_password_file = /opt/novell/kerberos/
keyfile
                realm_read_refresh_interval = 300
                ldap_servers = ldaps://ldap-server1.mit.edu ldaps://
ldap-server2.mit.edu:1636
```

```
          ldap_conns_per_server = 2
}
```