

Novell Kerberos KDC

1.5

www.novell.com

QUICK START

June 12, 2007



Novell®

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. Please refer to 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.

Copyright © 2005 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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 at <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

Novell Kerberos KDC Quick Start
[July 18, 2005](#)

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

eDirectory is a registered trademark of Novell, Inc.

NMAS is a registered trademark of Novell, Inc.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Directory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries.

SUSE is a registered trademark of Novell, Inc., in the United States and other countries.

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Copyright © 1985-2002 by the Massachusetts Institute of Technology. Export of software employing encryption from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

The implementation of the Yarrow pseudo-random number generator in src/lib/crypto/yarrow has the following copyright:

Copyright 2000 by Zero-Knowledge Systems, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Zero-Knowledge Systems, Inc. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Zero-Knowledge Systems, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

ZERO-KNOWLEDGE SYSTEMS, INC. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL ZERO-KNOWLEDGE SYSTEMS, INC. BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTUOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Kerberos V5 includes documentation and software developed at the University of California at Berkeley, which includes this copyright notice:

Copyright © 1983 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Permission is granted to make and distribute verbatim copies of this manual provided the copyright notices and this permission notice are preserved on all copies.

Permission is granted to copy and distribute modified versions of this manual under the conditions for verbatim copying, provided also that the entire resulting derived work is distributed under the terms of a permission notice identical to this one.

Permission is granted to copy and distribute translations of this manual into another language, under the above conditions for modified versions.

Contents

About This Guide	7
1 Installing and Configuring Novell Kerberos KDC using YaST	9
Prerequisites	9
Installing Novell Kerberos KDC.	9
Installing iManager Plug-ins	11
2 Configuring Novell Kerberos KDC using Administrative Utilities	13
Configuring eDirectory for Novell Kerberos KDC.	13
Modifying the Novell Kerberos KDC Configuration File.	14
Configuring Novell Kerberos KDC Services	15
Starting the Servers	16
Viewing the Log Files.	16
Configuring Kerberos Authentication	17
3 Deconfiguring and Uninstalling Novell Kerberos KDC components	19
Destroying the Kerberos Services	19
Destroying the Realm.	19
Unloading the Kerberos Password Agent	19
Clearing LDAP Kerberos Extension Information	20
Uninstalling Kerberos Components.	20
A Sample krb5.conf File	23

About This Guide

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

The guide is intended for Novell eDirectory™ or Kerberos administrators and is divided into the following chapters:

- ♦ Chapter 1, “Installing and Configuring Novell Kerberos KDC using YaST,” on page 9
- ♦ Chapter 2, “Configuring Novell Kerberos KDC using Administrative Utilities,” on page 13
- ♦ Chapter 3, “Deconfiguring and Uninstalling Novell Kerberos KDC components,” on page 19
- ♦ Appendix A, “Sample krb5.conf File,” on page 23

Documentation Updates

You can find the latest version of this documentation at the [Novell Documentation Website \(http://www.novell.com/documentation/kdc/index.html\)](http://www.novell.com/documentation/kdc/index.html).

Additional Documentation

- ♦ [Novell eDirectory 8.7.3 Documentation \(http://www.novell.com/documentation/edir873/index.html\)](http://www.novell.com/documentation/edir873/index.html)
- ♦ [Novell eDirectory 8.8 Documentation \(http://www.novell.com/documentation/beta/edir88/index.html\)](http://www.novell.com/documentation/beta/edir88/index.html)
- ♦ [Kerberos Documentation \(http://web.mit.edu/kerberos/www/\)](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.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment 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.

1

Installing and Configuring Novell Kerberos KDC using YaST

Novell® Kerberos KDC integrates Kerberos Authentication, Administration, and Password Servers with eDirectory™. Novell Kerberos KDC is derived from [MIT implementation of Kerberos](http://web.mit.edu/kerberos) (<http://web.mit.edu/kerberos>) .

This chapter describes how to install Novell Kerberos KDC and consists of the following sections:

- ♦ “Prerequisites” on page 9
- ♦ “Installing Novell Kerberos KDC” on page 9
- ♦ “Installing iManager Plug-ins” on page 11

Prerequisites

☐ Open Enterprise Server (OES) 2.

☐ Novell eDirectory™ 8.8 or later on Linux

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

☐ Root privileges to install Novell Kerberos KDC through YaST.

☐ Synchronized network server time

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

For information on synchronizing network time, refer to the *Open Enterprise Server Planning and Implementation Guide* (http://www.novell.com/documentation/oes2/oes_implement_lx_nw/index.html?page=/documentation/oes2/oes_implement_lx_nw/data/time.html#time-implement).

For installing iManager plug-ins:

☐ iManager 2.7 installed.

For installation information, refer to the *Novell iManager 2.7 Installation Guide* (<http://www.novell.com/documentation/beta/imanager27/index.html>).

☐ Trusted root certificate imported into the Keystore.

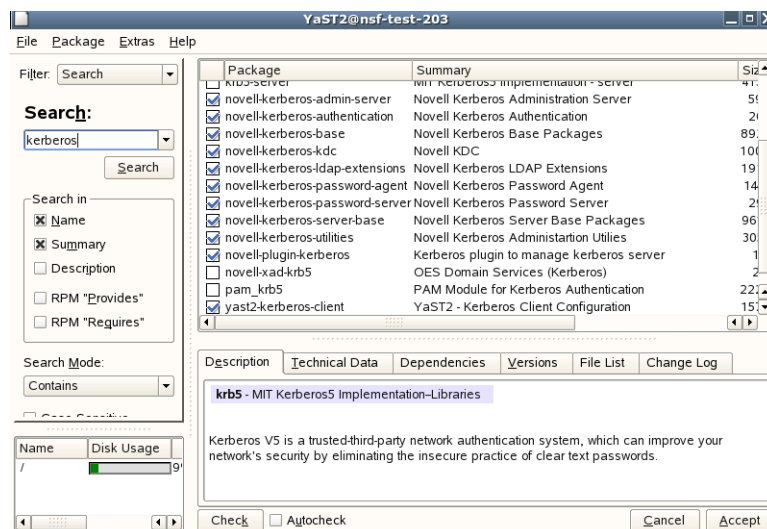
For more information, refer to the *Novell iManager 2.5 Administration Guide* (<http://www.novell.com/documentation/lg/imanager20/imanager20/data/am4ajce.html>).

Installing Novell Kerberos KDC

- 1 Select the following packages in YaST:

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, Administration server, and Password server.
novell-kerberos-kdc	Contains the Key Distribution Center (KDC) server. It 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: <ul style="list-style-type: none"> ♦ kdb5_ldap_util ♦ kadmin.local
Kerberos LDAP Extension and Password Agent	
novell-kerberos-ldap-extension	Contains the Kerberos LDAP extensions. This services requests for storing and retrieving various Kerberos specific keys from eDirectory.
novell-kerberos-password-agent	Contains the Kerberos Password Agent. This synchronizes the Kerberos passwords or keys with a universal password.

Figure 1 Novell KDC Packages



- 2** Click *Accept* to install Novell Key Distribution Centre.

Installing iManager Plug-ins

Novell iManager lets you manage the directory and users, and the access rights and network resources within the directory, from a Web browser and a variety of handheld devices. The Novell Kerberos KDC plug-ins help you perform various tasks such as creating and modifying realms, services, policies, and principals.

- 1** Ensure that you have met the **prerequisites** before proceeding with the installation.
- 2** Download the Novell Kerberos KDC iManager plug-ins.

The Novell Kerberos KDC iManager plug-in file (kerberosPlugin.npm) is present on the Novell Kerberos KDC download Website.

- 3** Install the Novell Kerberos KDC iManager plug-ins.

For information, refer to the *Novell iManager 2.5 Installation Guide* (http://www.novell.com/documentation/imanager25/imanager_install_25/data/alw39eb.html).

2

Configuring Novell Kerberos KDC using Administrative Utilities

After installing Novell® Kerberos KDC, you need to configure it. This chapter guides you to configuring Novell Kerberos KDC.

Novell Kerberos KDC configuration primarily consists of the following steps:

1. [Configuring eDirectory for Novell Kerberos KDC \(page 13\)](#)

In this step, import the trusted root certificate from Novell eDirectory™ and extend the eDirectory schema.

2. [Modifying the Novell Kerberos KDC Configuration File \(page 14\)](#)

In this step, change the Novell Kerberos KDC configuration file (krb5.conf) to include the configuration details such as, the realm name, DNs of the KDC and admin service objects, and path of the stashed passwords file for service objects.

3. [Configuring Novell Kerberos KDC Services \(page 15\)](#)

In this step, create a realm, server objects, and the kadm5.acl file.

4. [Starting the Servers \(page 16\)](#)

After completing the configuration, start the KDC, Administration, and Password servers.

5. [Viewing the Log Files \(page 16\)](#)

The messages from the KDC, Administration, and Password servers are by default logged into these files.

6. [Configuring Kerberos Authentication \(page 17\)](#)

Use kerberos authentication configuration script, krbauthconfig to create the host service principal (**host/hostname@realm**) for Novell Kerberized applications.

Configuring eDirectory for Novell Kerberos KDC

- 1 Export 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 server
-p port -f kerberos.ldif -e trusted_root_certificate -c
```

For example,

```
/opt/novell/eDirectory/bin/ldapmodify -D cn=admin,o=mit -W -h
kerberos.mit.edu -p 636 -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 Ensure that the Kerberos LDAP extensions are installed on the machine where eDirectory is installed.

The kdc-install utility installs libkrbpdw.so in /usr/lib/nds-modules.

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

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

For example:

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

Ensure that you run this command on the machine where KDC is installed.

3c Restart nldap.

To restart nldap, you need to first unload and then load nldap.

♦ **eDirectory 8.8:**

Unload nldap as: `/opt/novell/eDirectory/sbin/nldap -u`

Load nldap as: `/opt/novell/eDirectory/sbin/nldap -l`

4 Configure Kerberos Password Agent on the eDirectory server:

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

4a Start the Kerberos Password Agent as follows:

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

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/Kerberos* directory to */etc*.

While configuring Novell Kerberos KDC, if you do not specify a mandatory parameter, it will be taken from the krb5.conf file.

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

Figure 2 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
  }

[kdcdefaults]
num_threads = 10

[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/kpasswd.log

[dbdefaults]
database_module = ldapconf

[dbmodules]
db_module_dir = /opt/novell/kerberos/lib/
  ldapconf = {
    db_library = kldap
    ldap_ssl_port = 636
    ldap_kdc_dn = "cn=KDC Server - kerberos.mit.edu,o=mit"
    ldap_kadmind_dn = "cn=Admin Server - kerberos.mit.edu,o=mit"
    ldap_kpasswd_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
    realm_read_refresh_interval = 300
    ldap_servers = ldap-server1.mit.edu ldap-server2.mit.edu:1636
    ldap_conns_per_server = 5
  }

```

Diagram annotations:

- Realm Configuration:** Points to the `[realms]` section.
- Number of Threads:** Points to `num_threads = 10`.
- Path of Log Files:** Points to the `[logging]` section.
- Database Module:** Points to `database_module = ldapconf`.
- Path of kldap library:** Points to `db_module_dir = /opt/novell/kerberos/lib/`.
- Library Name:** Points to `db_library = kldap`.
- LDAP Port:** Points to `ldap_ssl_port = 636`.
- DNs of KDC, Administration, and Password Service Objects:** Points to the three `ldap_*_dn` entries.
- Path of Trusted Root Certificate:** Points to `ldap_root_certificate_file`.
- Path of Service Password Stashed File:** Points to `ldap_service_password_file`.
- LDAP Server List:** Points to `ldap_servers`.
- LDAP Connection Pool:** Points to `ldap_conns_per_server`.

Configuring Novell Kerberos KDC Services

Configure the KDC server as follows:


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

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

For example,

```
kdb5_ldap_util -D cn=admin,o=mit create -subtree 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 for all the screens in iManager.

The realm gets created under the `cn=kerberos` container.

- 2 Create the KDC, Administration, and Password service objects in eDirectory 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} -r
realm_list [-randpw|-fileonly] -f filename servicedn
```

The key file 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 -r ATHENA.MIT.EDU
-randpw -f /opt/novell/kerberos/keyfile "cn=kdc-service,o=mit"
```

Similarly, create the Administration and Password service object.

If you are creating the service objects using iManager, then, 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"
```

NOTE: The service passwords are encrypted with NCI keys, so the keyfile cannot be moved to other hosts and used from there. As the encryption keys are specific to the hosts and are not accessible from browsers, iManager does not provide an option to stash 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 mentioning `"* *` 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 \(http://www.novell.com/documentation/kdc/index.html\)](http://www.novell.com/documentation/kdc/index.html).

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/kpasswd start
```

NOTE: If you are not using the scripts to start the servers, you need to export the `LD_LIBRARY_PATH` as follows:

```
export LD_LIBRARY_PATH=/opt/novell/kerberos/lib:/opt/novell/lib:$LD_LIBRARY_PATH
```

Viewing the Log Files

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

Table 1 **Log File Paths**

Services	Log File Name (as in configuration file)
KDC	/var/log/krb5kdc.log
Administration	/var/log/kadmind.log
Password	/var/log/kpasswd.log

You can change the path of the log files by specifying the new path in the krb5.conf file. For more information, refer [Figure 2, “Sample Configuration File,” on page 15](#).

Configuring Kerberos Authentication

You can use kerberos authentication configuration script, `krbauthconfig` to create the host service principal (**host/hostname@realm**) for Novell Kerberized applications.

This script creates the service principal for the host and stashes the principal keys.

If the eDirectory is installed on the machine, it can optionally create a ldap service principal (`ldap/hostname@realm`) for LDAP SASL GSSAPI method.

3

Deconfiguring and Uninstalling Novell Kerberos KDC components

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

- 1 Destroying the Kerberos Services (page 19)
- 2 Destroying the Realm (page 19)
- 3 Unloading the Kerberos Password Agent (page 19)
- 4 Clearing LDAP Kerberos Extension Information (page 20)
- 5 Uninstalling Kerberos Components (page 20)

Destroying the Kerberos Services

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

- 1 Stop the daemon (krb5kdc, kadmind, or kpasswd)
- 2 Destroy the service object as follows:

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

For example:

```
kdb5_ldap_util -D cn=admin,o=mit destroy_service -f /usr/local/var/  
krb5kdc/servicepasswd cn=kdc-service,o=mit
```

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

Destroying the Realm

- 1 Destroy the realm using kdb5_ldap_util as follows:

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

For example:

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

Unloading the Kerberos Password Agent

- 1 Unload the Kerberos Password Agent as follows:

```
kpa -u
```

Clearing LDAP Kerberos Extension Information

Clear LDAP Kerberos Extension information from the LDAP server object:

- 1 Clear the extensionInfo using `kdb5_ldap_util`

```
kdb5_ldap_util [-D user_dn] [-H ldapuri] [-p ldap_port] [-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:

```
nldap -u
```

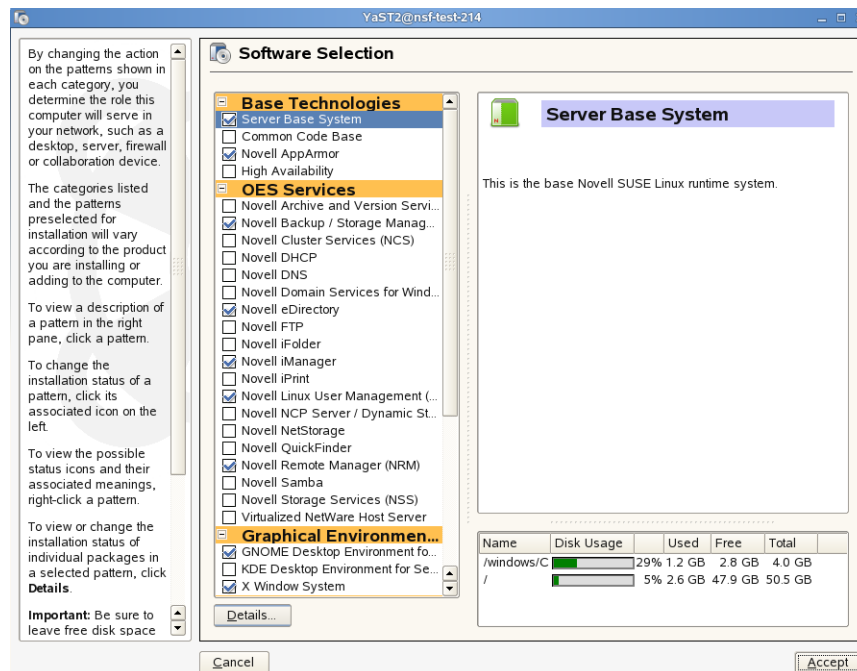
```
nldap -l
```

Uninstalling Kerberos Components

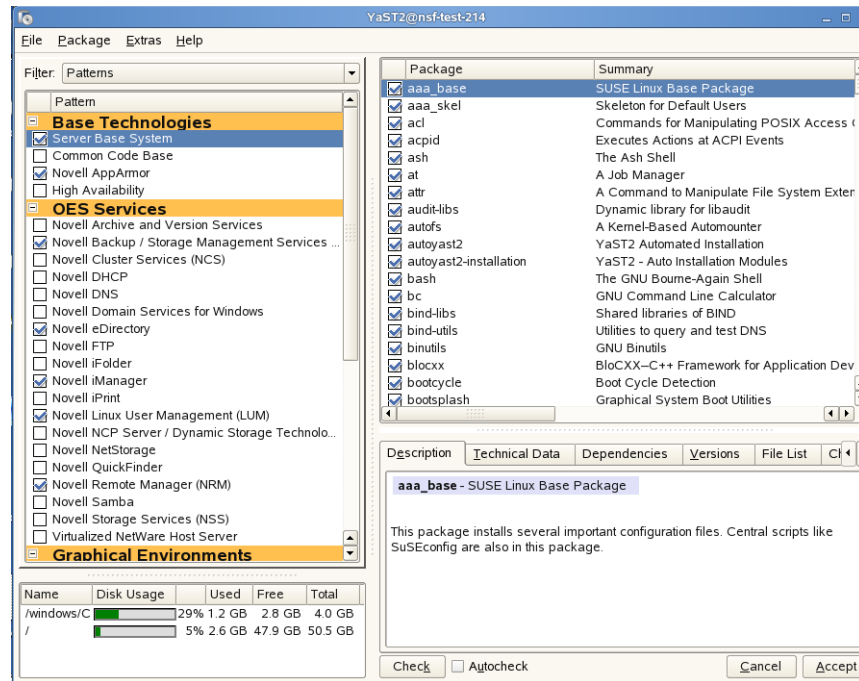
You must stop the eDirectory server before uninstalling `ldap` extension and `passwd` agent package

- 1 Open Yast and Click *Open Enterprise Server*, and then click *OES Install and Configuration*.
- 2 Click *Details* from the below screen.

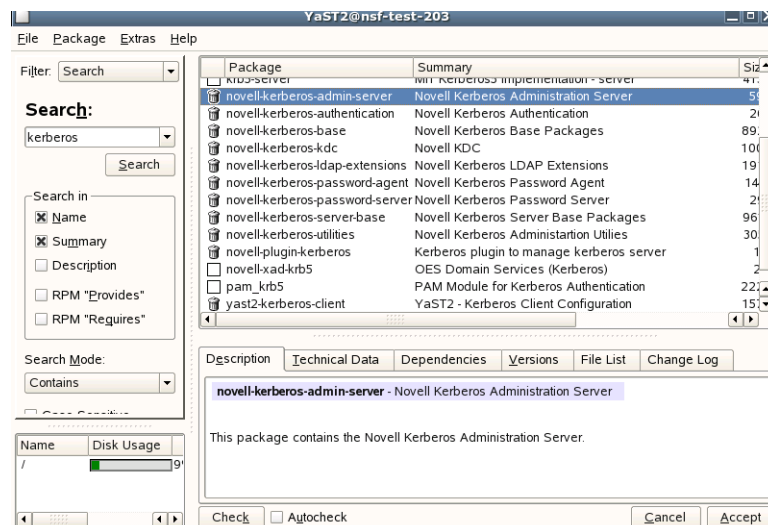
Figure 3 Software Selection



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

Figure 4 OES Services and Packages

- 4** Right click on the package you want to delete, and then click *Delete*. Click *Accept* to uninstall. Refer [Installed Kerberos Packages](#)

Figure 5 Uninstalling Kerberos Component

A

Sample krb5.conf File

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, when you do not specify any of the mandatory parameters, the values are taken from the /etc/krb5.conf file. 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
    }

[kdcdefaults]
num_threads = 10

[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/Certs/TrustedRoot-
            ldap-server1.mit.edu.der /opt/novell/kerberos/Certs/TrustedRoot-ldap-
            -server2.mit.edu.der
        ldap_service_password_file = /opt/novell/kerberos/Keys/keyfile
        realm_read_refresh_interval = 300
    }
```

```
    ldap_servers = ldaps://ldap-server1.mit.edu ldaps://ldap-server2.mit.edu:1636
    ldap_conns_per_server = 5
}
```