Novell
Kerberos Login Method for NMAS™

1.0

ADMINISTRATION GUIDE

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.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright© 2004 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.

Patents Pending

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 trademark of Novell, Inc.

NMAS is a trademark of Novell, Inc.

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

Novell Client is a trademark of Novell, Inc.

Third-Party Trademarks

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

Contents

About This Guide

The Kerberos Login Method for NMAS™ supports logging in to Novell® eDirectory™ using Kerberos credentials acquired from a KDC (Key Distribution Centre). This method plugs in to and makes use of the Novell NMAS infrastructure to support this Kerberos-based login.

This guide contains the following sections:

- Chapter 1, "Introduction to the Kerberos Login Method for NMAS," on page 9
- Chapter 2, "Using the Kerberos Login Client Method for NMAS," on page 11
- Chapter 3, "Administering the Kerberos Login Method for NMAS," on page 15
- Chapter 4, "Uninstalling the Kerberos Login Method for NMAS," on page 25
- Chapter 5, "Troubleshooting the Kerberos Login Method for NMAS," on page 27

Documentation Updates

For the most recent version of the Novell Kerberos Login Method for NMAS Administration Guide and Quick Start Card, see the Novell Kerberos Login Method Documentation Web Site (http://www.novell.com/documentation/nmaslm/index.html).

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 (®, TM, 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 UNIX*, should use forward slashes as required by your software.

1 Introduction to the Kerberos Login Method for NMAS

The Kerberos Login Method for Novell Modular Authentication Services™ (NMAS) supports logging in to Novell® eDirectory™ using Kerberos credentials acquired from a KDC (Key Distribution Centre). This method plugs in to and makes use of the Novell NMAS infrastructure to support this Kerberos-based login.

The Kerberos Login Method for NMAS consists of the following components:

- **NMAS Kerberos Login Server Method (Kerberos LSM):** Installed on the eDirectory server that has the NMAS Server already installed.

- **Novell Kerberos LDAP Extensions:** Installed on all the servers that are used for administering the Kerberos Login Method for NMAS.

- **iManager plug-in for NMAS Kerberos:** Lets you manage the Kerberos objects and attributes. For more information, refer to the Kerberos Login Method for NMAS Quick Start Card.

- **NMAS Kerberos Login Client Method (Kerberos LCM):** Installed along with the Novell Client™ and NMAS client on the Windows* workstations. This must be installed on each Windows workstation that will use the Kerberos Login Method for NMAS.

Basic Functionality

In an environment where eDirectory and Kerberos are deployed, users must authenticate both to eDirectory and KDC to access the eDirectory services and the Kerberized services. Users must log in twice, once to eDirectory and once to KDC. The Kerberos Login Method for NMAS solves the problem of authenticating separately to eDirectory and KDC to access eDirectory and Kerberized services. Here, with the Kerberos Login Method for NMAS installed, eDirectory is considered as a Kerberized service and it authenticates the users with their Kerberos tickets obtained from the KDC.

In a typical Kerberos deployment, all users and services (application) are called principals. These principals and KDC together constitute a realm. Each of these principals have their accounts in KDC, and are associated with a unique secret stored in the KDC. As eDirectory is also treated as a Kerberized service, it must have a corresponding service principal created in the KDC.

Since the Kerberos Login Method for NMAS provides access to both the eDirectory and Kerberized services, an eDirectory user object must store the principal names associated with that user. As these principals are present in the realms that are served by third-party (foreign) KDCs, the principal names for a user are stored as foreign principal names.

For an eDirectory user, the NMAS Kerberos LCM helps in acquiring a Kerberos Ticket Granting Ticket (TGT) as a particular user principal and the Service Ticket (ST) to eDirectory from the

KDC. This service ticket is sent to the NMAS Kerberos LSM, which validates it and allows the user to log in to eDirectory.

In order to validate the ST, the NMAS Kerberos LSM requires a keytab of the eDirectory service principal that is created in the Kerberos KDC. Traditionally, the principal keys are created in the Kerberos database and extracted using Kerberos Administration tools. These keys are stored as keys in the local file system. But, in the Kerberos Login Method for NMAS, the principal keys (keytab) are encrypted with a realm-specific master key, securely stored, and read from eDirectory. This can be managed using the iManager plug-in for Kerberos.

Setting Up the Kerberos Login Method for NMAS

You must configure the following in the sequence mentioned below to make the Login Method available for use:

1. "Installing the NMAS Kerberos LSM"

2. "Installing the Kerberos LDAP Extensions"

3. "Installing the iManager Plug-In for NMAS Kerberos"

4. "Installing the NMAS Kerberos LCM"

5. "Creating a Service Principal for eDirectory"

6. "Extracting the Key of the Service Principal for eDirectory"

7. "Configuring the Kerberos Login Method for NMAS"

8. "Creating a Login Sequence"

For information, refer to the Kerberos Login Method for NMAS Quick Start Card.

Supported Features

The Kerberos Login Method for NMAS supports the following features:

- "MIT Kerberos Client Cache" on page 12
- "Microsoft Kerberos Client Cache" on page 13

2 Using the Kerberos Login Client Method for NMAS

This section tells you how to use the Kerberos Login Client Method for NMAS™.

- "Logging In Using the NMAS Client" on page 11
- "Enabling a Single Sign-On" on page 12
- "Locking and Unlocking a Workstation" on page 14

Logging In Using the NMAS Client

1 In the Novell Client™ login screen, go to the NMAS tab and select the Kerberos method.

2 Specify the following:

- eDirectory™ username (not the Kerberos principal name) in the User Name field.
- (Optional) Kerberos password (not the eDirectory password) in the Password field.

  NOTE: Do not specify the Kerberos password in this field if you want to specify the ticket options (as mentioned in step 5).

- Tree
- Context
- Server

3 Click OK.

4 (Conditional) If you have more than one principal identity, all principal names are displayed. Select the principal that you want to log in with.

5 (Conditional) Specify the password if you haven't already specified the password in Step 2.

The user principal, eDirectory service principal, and the realm names are displayed.

Click Options to specify the ticket options:

- **Encryption Type:** Select the supported encryption type for the principal.
- **Lifetime:** You can select maximum lifetime of the ticket, based on weeks, days, hours, and minutes. The minimum request for the lifetime of ticket should be more than 5 minutes. The default lifetime of the ticket is 8 hours.
- **Renewal:** You can select the maximum renewal time of the ticket, based on weeks, days, hours, and minutes.
- **Proxiable:** You can request a Proxiable ticket by selecting this check box.
- **Forwardable:** You can request a Forwardable ticket by selecting this check box.

◆ **Cache Tickets:** For this release, only File Cache is supported. By default, the cache is destroyed immediately after the login. Select this option to store the tickets in the Novell file cache and to use the novl2mit utility to populate the MIT cache. This utility destroys the Novell cache after populating the MIT cache.

IMPORTANT: If you do not run the novl2mit utility, you must manually delete the cache file before logging out.

Enabling a Single Sign-On

MIT Kerberos Client Cache

In an environment where eDirectory and Kerberos deployments co-exist, there is a need for single sign-on. To support this, the NMAS Kerberos LCM provides a feature to populate the MIT client's credential cache with the acquired Kerberos credentials.

After the eDirectory login, run the novl2mit utility to populate the MIT credential cache.

The Novell credential cache must be retained to populate the MIT credential cache. If you haven't selected Retain the Novell Credential Cache option during installation, enable it by editing the registry entry CacheTickets under hkey_local_machine\software\novell\kerberos\1.0\krb5-config to 1 (enable). The novl2mit utility deletes the Novell credential cache after populating the MIT credential cache.

This will allow the other Kerberized applications working with MIT Kerberos client to make use of this TGT for further operations, thereby providing a single sign-on to the user.

If you use the FILE cache option for MIT cache, the novl2mit utility needs Write permissions to the file cache to populate it. You must grant Write permissions to the user because the novl2mit utility runs as a user process.

To populate the MIT cache, MIT libraries (kfw 2.1 or later for Windows) must be installed on the client machines. For more information, refer to the *MIT Kerberos Distribution page* (http://web.mit.edu/kerberos/dist/index.html).

If you do not want to populate the MIT credential cache, disable this option by editing the registry entry CacheTickets under hkey_local_machine\software\novell\kerberos\1.0\krb5-config to 0 (disable).

Using the novl2mit Utility

The novl2mit utility populates only the Ticket Granting Tickets (TGT) to the MIT cache. This utility can be run as part of the start up program or login script. To run it as part of the login script program, you must first add it to the login script.

To add the novl2mit utility to the login script:

1 Log in to eDirectory.

2 Right-click the N from the taskbar, then click User Administration for *Tree* > Edit Login Script.

3 Add @novl2mit to the login script.

4 Click OK.

Microsoft Kerberos Client Cache

Unlike the MIT Kerberos client, the Microsoft* implementation of the Kerberos client does not provide any functions to populate its credential cache. Also, Microsoft applications might not be able to provide the necessary functionality using the tickets acquired from MIT or other KDCs.

The NMAS Kerberos LCM has a configurable option to work with the Microsoft client cache to provide a single sign-on in a mixed environment with Microsoft Kerberized applications.

The NMAS Kerberos LCM retrieves the ticket from Microsoft Kerberos Client Cache and logs in to eDirectory. The Microsoft Cache is typically available to a machine when the machine is part of the Active Directory* domain, and a domain user logs in to the machine.

Microsoft Windows Domain Configuration

For example, create a user *novledir* in the Active Directory. Extract the key of this principal using ktpass.exe. (This utility is part of the Windows 2000 installation and can be installed from the \support\tools\setup.exe of the Windows 2000 installation CD.)

In order to set the password and extract the key, execute the following command:

```
ktpass -princ novledir/MYTREE@MYREALM -mapuser novledirMYTREE -
pass mypassword -out MYTREE.keytab
```

where *MYTREE* is the eDirectory tree name, *MYREALM* is the Windows 2000 domain name, *my-password* is the password for the service principal, and *my-keytab-file* is the keytab file where the key of the service principal is extracted.

Add this Windows 2000 domain realm to eDirectory with the keytab (extracted in the above step) and set Active Directory as the KDC for the realm by following the procedure listed in the Kerberos Login Method for NMAS Quick Start Card.

Client Configuration

On Windows 2000 or later, the Novell Client 4.9 or later must be installed. This machine should be part of the Active Directory domain.

The Windows Login must be set as default before using the Kerberos Login Method for NMAS with MS cache support. This can be done by the following method:

1 Double-click the ChangeDefaultLogin.exe from *extracted_folder/* NMAS_Kerberos_Method_10/Novell/Kerberos/MS Cache Utility, where *extracted_folder* is the directory where you extracted the NMAS_Kerberos_Method_10.zip.

   This will check for the Novell Client version.

2 Based on the default login, do one of the following:

   ◆ If Novell Login is set as the default, click Yes to set the Windows Login as the default and enable the MS cache support for this method.

   ◆ If the Windows Login is set as the default, click Yes to set the Novell Login as the default and disable the MS cache support.

For every user in the AD domain, there is a corresponding Kerberos principal associated for the user. You must associate the Kerberos principal for the domain user to the eDirectory user you want to log in with. For more information, refer to the Kerberos Login Method for NMAS Quick Start Card.

NOTE: The kerberos principal names are case-sensitive. You must use the exact case reported in the AD administration tools.

Logging in to eDirectory using the MS Ticket

1 Log in to the machine as the domain user.

2 Right-click the N from the taskbar to initiate the Novell Login.

3 Specify the eDirectory user that is associated with this domain user, then click OK.

The Login using the MS ticket will go through without prompting for the password.

4 (Conditional) If multiple principals are associated for the same eDirectory user, choose the principal with which you logged in. If you choose other principals, you will be prompted for the password.

Locking and Unlocking a Workstation

If your workstation's initial login screen is the Novell Client login screen (NetWare Graphical Identification and Authentication (NWGINA)), it is invoked when you try to unlock the workstation after it is locked. If you have logged in using the Kerberos Login Method for NMAS, when you unlock the workstation you are prompted for the Kerberos password to acquire a fresh TGT and Service Ticket to log in to eDirectory. If this is successful, the workstation is unlocked.

Every time you lock and unlock the workstation, fresh tickets are obtained from the KDC and validated.

If the Microsoft workstation login (Microsoft Graphical Identification and Authentication (MSGINA)) is the primary workstation login, it is invoked when you attempt to unlock the workstation. This handles the user password validation. In this case, the NMAS Kerberos LCM is not involved in the unlock procedure.

3 Administering the Kerberos Login Method for NMAS

This section tells you how to administer the Kerberos Login Method for NMAS™. It covers the following:

- "Launching iManager" on page 15
- "Extending the Kerberos Schema" on page 16
- "Managing the Kerberos Realm Object" on page 16
- "Managing a KDC Service Object" on page 18
- "Managing a Service Principal" on page 19
- "Editing Foreign Principals" on page 23

Launching iManager

1. Open the browser.

2. Enter the following URL in the address field of the browser window:

   ```
   http://hostname/nps/iManager.html
   ```

   where *hostname* is the server name or IP address of the iManager server where you want to install the iManager plug-in for NMAS Kerberos.

   NOTE: In case of problems, ensure that the Tomcat and Web server are configured properly. For information, refer to *iManager Administration Guide* (http://www.novell.com/documentation/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/bnpta1r.html).

3. Specify the username and password to log in to eDirectory™, then click Login.

Logging in to a Different Tree

1. Click the Login to a different tree [icon] icon in the taskbar and provide the following:
   - Username
   - Password
   - Context
   - Tree

2. Click Login.

Extending the Kerberos Schema

This task allows you to extend your eDirectory™ schema with the Kerberos object class and attribute definitions.

1 In iManager, click Kerberos Management > Extend Schema to open the Extend Schema page.

2 If the schema has not already been extended, click OK to extend the schema.

If the schema has been extended, a message is displayed with the status. Click Close.

NOTE: This will automatically update your eDirectory schema with the Kerberos object classes and attributes defined in the *kereberos.ldif* file located at the *extracted_folder*/NMAS_Kerberos_Method_10/Novell/ Kerberos, where *extracted_folder* is the directory where you extracted the NMAS_Kerberos_Method_10.zip file.

Managing the Kerberos Realm Object

This section discusses the following:

Creating a New Realm Object

1 In iManager, click Kerberos Management > New Realm to open the New Realm page.

2 Specify a name for the Kerberos realm that is to be created.

The realm name must be the same as the one with which you want to configure this Login Method and must conform to the RFC 1510 conventions.

3 Specify a master password for the realm and confirm the password.

4 Select the key type that is to be used for generating the master key for this realm.

The available key types are DES-CBC-CRC, DES-CBC-MD5, and DES3-CBC-MD5.

The default is DES3-CBC-MD5.

5 Select the encryption types for this realm:

5a Select the supported encryption types.

5b Select the default encryption type.

The available encryption types are DES-CBC-CRC, DES-CBC-MD5, and DES3-CBC-MD5.

The default value is DES-CBC-CRC.

NOTE: The selected default encryption type must be present in the Supported Encryption type list.

6 Specify the subtree you want the Kerberos realm to be configured with or use the Object Selector icon to select it.

This is the FDN of the subtree or the container that contains the eDirectory service principals of this realm. This subtree is not applicable to user principals (Foreign Principal names).

If you do not select a subtree or a container, the root of the tree is used as the default.

7 Specify the scope of the subtree search:

◆ One-level: Searches the immediate subordinates of the realm subtree.

◆ Subtree: Searches the entire subtree starting with, and including the realm subtree.

8 Specify the KDC service that serves this realm or use the Object Selector icon to select it.

NOTE: If you have not created a KDC Service Object, leave this field blank. You can create one using "Creating a New KDC Service Object" on page 18 and associate it with this realm. This will automatically update the KDC service entry for this realm.

9 Click OK.

Editing a Realm Object

This task helps you modify the attribute values of the existing Realm object.

1 In iManager, click Kerberos Management > Edit Realm to open the Edit Realm page.

2 Specify a name for the Kerberos realm that is to be edited.

3 Click OK.

4 Select the encryption types for this realm:

4a Select the supported encryption types.

4b Select the default encryption type.

The available encryption types are DES-CBC-CRC, DES-CBC-MD5, and DES3-CBC-MD5.

The default value is DES-CBC-CRC.

NOTE: The selected default encryption type must be present in the Supported Encryption type list.

5 Specify the subtree you want the Kerberos realm to be configured with or use the Object Selector icon to select it.

This is the FDN of the subtree or the container that contains the eDirectory service principals of this realm. This subtree is not applicable to user principals (Foreign Principal names).

If you do not select a subtree or a container, the root of the tree is used as the default.

6 Specify the scope of the subtree search.

◆ One-level: Searches the immediate subordinates of the realm subtree.

◆ Subtree: Searches the entire subtree starting with, and including the realm subtree.

7 Specify the KDC service that serves this realm or use the Object Selector icon to select it.

NOTE: If you have not created a KDC Service Object, you can create using "Creating a New KDC Service Object" on page 18 and associate with this realm. This will automatically update the KDC service entry for this realm.

8 Click OK.

9 (Optional) To edit another realm, click Repeat Task.

Deleting a Realm Object

This task helps you delete existing Kerberos realms.

1 In iManager, click Kerberos Management > Delete Realm to open the Delete Realm page.

2 Select the realms that are to be deleted.

To select multiple realms, press Shift and select the realms or press Shift + Arrow keys.

3 Click OK.

4 Click OK again to confirm the delete operation or click Cancel to cancel the delete operation.

Managing a KDC Service Object

This section discusses the following:

Creating a New KDC Service Object

1 In iManager, click Kerberos Management > New KDC Service to open the New KDC Service page.

2 Specify a name for the KDC service that is to be created.

This will represent the KDC service in eDirectory.

3 Specify the name of the container where the KDC service is to be created or use the Object Selector icon to select it.

4 Specify the host servers.

   4a Click Add to open the Host server entry pop-up window.

   4b Specify the DNS name or IP address of the server that hosts the KDC service.

   4c Specify the port number of the server.

   If it is not specified, the default port 88 is used.

   4d Select the protocol for the host server.

   The default is UDP.

   4e Click OK to add the host server entry.

5 Specify the FDN of the Kerberos realm object or use the Object Selector icon to select it.

6 Click OK.

7 (Optional) To create another KDC Service, click Repeat Task.

Editing a KDC Service Object

This task helps you edit an existing KDC service.

1 In iManager, click Kerberos Management > Edit KDC Service to open the Edit KDC Service page.

2 Specify the name for the KDC service that is to be edited.

3 Click OK.

4 Specify the host servers.

   4a Click Add to open the Host server entry pop-up window.

   4b Specify the DNS name or IP address of the server that hosts the KDC service.

4c Specify the port number of the server.

   If it is not specified, the default port 88 is used.

4d Select the protocol for the host server.

   The default is UDP.

4e Click OK to add the host server entry.

   To delete a host server entry, select the host entry and click Delete ▣

5 Specify the FDN of the Kerberos realm object or use the Object Selector icon to select it.

6 Click OK.

7 (Optional) To edit another KDC Service, click Repeat Task.

Deleting a KDC Service Object

1 In iManager, click eDirectory Administration > Delete Object to open the Delete Objects page.

2 Specify the KDC Service object that is to be deleted or use the Object Selector icon to select it.

3 Click OK.

Managing a Service Principal

This section discusses the following:

Creating a Service Principal for eDirectory

You must create a service principal for eDirectory in the same Kerberos realm as the users that use the Kerberos Login Method for NMAS in order to log in to both eDirectory and KDC (to access the eDirectory services and the Kerberized services). This can be done with the help of your Kerberos administrator.

Use the Kerberos Administration tool that is available with your KDC to create the eDirectory Service principal with the encryption type and salt type as DES-CBC-CRC and Normal respectively.

The name of the principal must be novledir/*TREENAME@REALMNAME*.

NOTE: The *TREENAME* in novledir/*TREENAME@REALMNAME* must be in uppercase.

For example, if you are using MIT KDC, execute the following command:

kadmin:addprinc -e des-cbc-crc:normal novledir/MYTREE@MYREALM

For example, if you are using Heimdal KDC, execute the following command:

```
kadmin -l
kadmin> add --random-key novledir/MYTREE@MYREALM
```

To delete the unsupported encryption types for the service principal, execute the following command:

```
kadmin> del_enctype novledir/MYTREE@MYREALM des-cbc-md4
kadmin> del_enctype novledir/MYTREE@MYREALM des-cbc-md5
kadmin> del_enctype novledir/MYTREE@MYREALM des3-cbc-sha1
```

where *MYTREE* is the treename and *MYREALM* is the Kerberos realm.

Extracting the Key of the Service Principal for eDirectory

Use the Kerberos Administration tool that is available with your KDC to extract the key of the eDirectory service principal created in the "Creating a Service Principal for eDirectory" on page 19 and store it in the local file system. This can be done with the help of your Kerberos administrator.

For example, if you are using an MIT KDC, execute the following command:

```
kadmin: ktadd -k /directory_path/keytabfilename -e des-cbc-
crc:normal novledir/MYTREE@MYREALM
```

For example, if you are using Microsoft KDC, create a user novledirMYTREE in Active Directory and then execute the following command:

```
ktpass -princ novledir/MYTREE@MYREALM -mapuser novledirMYTREE -
pass mypassword -out MYTREE.keytab
```

This command maps the principal (novledir/MYTREE@MYREALM) to the user account (novledirMYTREE), sets the host principal password to mypassword, and extracts the key into the MYTREE.keytab file.

For example, if you are using Heimdal KDC, execute the following command:

```
kadmin> ext_keytab -k /directory_path/keytabfilename novledir/
MYTREE@MYREALM
```

where *keytabfilename* is the name of the file that contains the extracted key, *MYTREE* is the treename, and *MYREALM* is the Kerberos realm.

Creating a Service Principal Object in eDirectory

You must create a Kerberos service principal with the same name (novledir/
TREENAME@REALMNAME) as specified in "Creating a Service Principal for eDirectory" on page 19.

Best Practice

Service principals for eDirectory must be readily accessible to all servers enabled for Kerberos Login Method for NMAS. If these eDirectory service principals are not created under the Kerberos Realm container inside the Security container, we strongly recommend that you create the container that contains these eDirectory service principals as a separate partition, and that the container be widely replicated.

1 In iManager, click Kerberos Management > New Principal to open the New Principal page.

2 Specify the name of the principal that is to be created.

The principal name must be in the format novledir/*TREENAME@REALMNAME*.

3 Specify the name of the container where the principal object is to be created or use the Object Selector icon to select it.

4 Specify the name of the realm.

If you have already specified the realm name in Step 2, leave this field blank.

5 Do either of the following:

◆ Specify the keytab filename or click Browse to select the location where the keytab file is stored.

This is the file that contains the key extracted in .

◆ Specify the password and confirm the password and then select the encryption type and salt type combination.

The password and encryption type/salt type combination must be the same as the those specified while creating the service principal in the KDC database.

6 Click OK.

Viewing the Kerberos Service Principal Keys

This task helps you edit an existing Kerberos foreign principal.

1 In iManager, click Kerberos Management > View Principal Keys to open the View Principal Keys page.

2 Specify the name of the principal key that is to be viewed or use the Object Selector icon to select it.

The following information of the principal keys is displayed:

◆ Principal name

◆ Key Table

 ◆ Number: Specifies the serial number of the key in the key table

 ◆ Version: Specifies the version of the key

 ◆ Key Type: Specifies the type of this principal key

 ◆ Salt Type: Specifies the salt type of this principal key

3 Click OK.

Deleting a Kerberos Service Principal Object

This task helps you delete an existing Kerberos service principal.

You can select a single object, multiple objects, or perform an advanced selection of the principal objects to be deleted.

To delete a single principal object:

1 In iManager, click Kerberos Management > Delete Principal to open the Delete Principal page.

2 Click Select a single object.

3 Specify the name of the principal object that is to be deleted or use the Object Selector icon to select it.

4 Click OK.

5 Click OK again to confirm the delete operation or click Cancel to cancel the delete operation.

To delete multiple principal objects:

1 In iManager, click Kerberos Management > Delete Principal to open the Delete Principal page.

2 Click Select multiple objects.

3 Specify the name of the principal objects that are to be deleted or use the Object Selector icon to select them.

4 Select the principal that must be deleted.

5 Click OK.

6 Click OK again to confirm the delete operation or click Cancel to cancel the delete operation.

To delete a principal using advanced selection:

1 In iManager, click Kerberos Management > Delete Principal to open the Delete Principal page.

2 Click Advanced Selection.

3 Select the object class.

4 Specify the container that contains the principal object or use the Object Selector icon to select it.

5 Click Include sub-containers to include the sub-containers of the container specified in Step 3.

6 Click ![icon] to open the Advanced Selection Criteria window.

7 Select the type of attribute and the operator from the drop-down list and provide the corresponding values.

8 Click Add row ![icon] to include more Logic groups to the selection.

9 Click OK to set the filter.

10 Click Show preview to display the preview of the advanced selection.

11 Click OK.

12 Click OK again to confirm the delete operation or click Cancel to cancel the delete operation.

Setting a Password for the Kerberos Service Principal

This task helps you set the password of an existing Kerberos service principal.

If the eDirectory service principal key has been reset in your KDC, you must update the key for this principal in eDirectory also.

For information on extracting the key, refer to "Extracting the Key of the Service Principal for eDirectory" on page 20.

1 In iManager, click Kerberos Management > Set Principal Password to open the Set Principal Password page.

2 Select the name of the principal object for which an individual password has to be set or use the Object Selector icon to select it.

3 Specify the keytab filename or click Browse to browse the location where the keytab file is stored.

4 Do either of the following:

   ◆ Specify the name of the keytab file that contains the principal key or click Browse to select the location where the keytab file is stored.

   NOTE: For more information on creating service principals and extracting the keys, refer "Creating a Service Principal for eDirectory" on page 19 and "Extracting the Key of the Service Principal for eDirectory" on page 20.

   ◆ Specify the password and confirm the password and then select the encryption type and salt type combination.

5 Click OK to set the password.

6 (Optional) To set the password for another principal, click Repeat Task.

Editing Foreign Principals

You can add Kerberos principal names to the eDirectory users using iManager:

1 In iManager, click Kerberos Management > Edit Foreign Principals to open the Edit Foreign Principals page.

2 Specify the FDN of a valid user object or use the Object Selector icon to select the User object reference.

3 Click OK.

4 Specify the foreign principal names and click Add 🔷.

The principal name must be in the format principalname@*REALMNAME*.

To delete the foreign principal name, select the name and click Delete ➖.

5 Click OK.

4 Uninstalling the Kerberos Login Method for NMAS

This section tells you how to uninstall the NMAS™ Kerberos LCM and the Kerberos LDAP Extensions for the Kerberos Login Method for NMAS.

- "Uninstalling the NMAS Kerberos LCM" on page 25
- "Uninstalling the Kerberos LDAP Extensions on NetWare" on page 25
- "Uninstalling the Kerberos LDAP Extensions on Windows" on page 25
- "Uninstalling the Kerberos LDAP Extensions on Linux/Solaris" on page 25

Uninstalling the NMAS Kerberos LCM

1 From the Control Panel, click Add/Remove Programs.

2 Select NMAS - Kerberos Login Client Method (1.0) > click Change/Remove.

3 Click Yes to proceed with the uninstallation.

Uninstalling the Kerberos LDAP Extensions on NetWare

1 Map the SYS: volume on the remote NetWare machine to a drive on the Windows machine that you are using to uninstall the Kerberos LDAP Extensions.

2 Double-click krbldapx_Uninstall.exe from the *mapped_drive*:/System directory.

3 Follow the on-screen instructions and provide the LDAP authentication information.

Uninstalling the Kerberos LDAP Extensions on Windows

1 Double-click krbldapx_Uninstall.exe from *eDirectory_installation_directory*/NDS.

2 Follow the on-screen instructions and provide the LDAP authentication information.

Uninstalling the Kerberos LDAP Extensions on Linux/Solaris

1 Execute the krbldapx_install script from /usr/sbin by entering:

```
krbldapx_install -u -D bind_fdn [-w bind_fdn_password]
[-h ldap_server] [-p port] [-e trusted_root_file]
```

where

- *bind_fdn* is the FDN of the administrator or the user with administrator-equivalent rights. This must be in the format cn=admin,o=org.

- *bind_fdn_password* is the password of the *bind_fdn*.

- *ldap_server* is the hostname or IP address of the LDAP server.

- *port* is the port that the LDAP server is running on.

- *trusted_root_file* is the trusted root certificate filename for the SSL bind.

5 Troubleshooting the Kerberos Login Method for NMAS

This section discusses the troubleshooting scenarios for the Kerberos Login Method for NMAS™.

Kerberos LCM

Uninstaller setup failed to initialize. You might not be able to uninstall the product.

Explanation: You do not have enough privileges to install the Kerberos Login Method for NMAS.

Possible Cause: You are either not an administrator or a user with administrator-equivalent rights to install the Kerberos Login Method for NMAS.

Action: Make sure that you log in as administrator or a user with administrator-equivalent rights and install the Kerberos Login Method for NMAS.

NMAS Login Failed Return Code: -1642 (0xFFFFF996) Login Failed

There are a number of possible causes for this error.

Possible Cause: The system time between the hosts are not synchronized.

Action: Synchronize the time between the NMAS Client host, the NMAS Server host, and the KDC host.

Possible Cause: The Realm object or the KDC object has not been configured properly.

Action: Configure all the mandatory attributes of the Realm object and the KDC Object with correct values.

Possible Cause: The User object does not contain the Principal name attribute.

Action: Extend the User object with ForeignPrincipalAux class and specify the krbForeignPrincipalName attribute.

Possible Cause: The hostname or address of the KDC Server has changed in Novell® eDirectory™ and has not been updated in the krb.con file. (This file will be present in the Client Installed folder.)

Action: Update the krb.con file or delete it, so that the client can re-create this file with the updated values.

Possible Cause: The key of the service principal has not been extracted with the correct encryption type.

Action: Check the NMAS server log. If the encryption type does not match, extract the service principal's key with "encryption type":"salt" combination "des-cbc-crc":"normal" value.

Possible Cause: The KDC Server's host entry might not be present in DNS.

Action: Update the host entry of the KDC Server in DNS.

User Principal in the Kerberos database has expired

Action: Contact your Kerberos administrator to enable the user principal

eDirectory Service Principal in the Kerberos database has expired

Action: Contact your Kerberos administrator to enable the eDirectory service principal

The specified value in the lifetime field is negative or too short

Action: The specified ticket lifetime must be more than the minimum value set by the Kerberos policy. Contact you Kerberos administrator for the minimum ticket lifetime value.

KDC does not support the specified encryption type

Action: For this release, the Kerberos Login Method for NMAS supports only DES-CBC-CRC, DES-CBC-MD5, and DES3-CBC-MD5 encryption types. Contact your Kerberos administrator.

User Principal not found in the Kerberos database

Action: Contact your Kerberos administrator for creating this principal or find out the correct principal name. Principal names are case-sensitive. Ensure that you specify the principal names with the proper case.

eDirectory Service Principal not found in the Kerberos database

Possible Cause: The specified eDirectory service principal was not found in the Kerberos database.

Action: Contact your Kerberos administrator for creating this principal or find out the correct principal name. Principal names are case-sensitive. Ensure that you specify the principal names with the proper case.

User Principal not yet valid - Try again later

Possible Cause: The Kerberos administrator has not yet enabled the user principal.

Action: Contact your Kerberos administrator for enabling this principal.

eDirectory Service Principal not yet valid - Try again later

Possible Cause: The Kerberos administrator has not yet enabled the eDirectory service principal.

Action: Contact your Kerberos administrator for enabling this principal.

User Principal Password in Kerberos database has expired

Possible Cause: The user principal password in the Kerberos database has expired.

Action: Contact your Kerberos administrator to enable the Kerberos password.

Decrypt Integrity check failed. Password might be wrong

Possible Cause: An invalid password has been specified or the specified encryption type is not supported.

Action: You must have either specified a wrong password or the specified encryption type is not supported by the Kerberos Login Method for NMAS. For this release, only the DES-CBC-CRC, DES-CBC-MD5, and DES3-CBC-MD5 encryption types are supported. Contact your Kerberos administrator.

Clock skew is too high between the Client and KDC

Possible Cause: The clock skew is more than 5 minutes between the eDirectory server being contacted, the client machine, and the KDC.

Action: Synchronize the time between the eDirectory server, the client machine, and the KDC used for obtaining tickets.

Invalid format for KDC hostname

Possible Cause: The format of the hostname that is specified is invalid.

Action: Check whether the KDC hostname format specified in the krbHostServer attribute of the KDC object in eDirectory is correct.

Cannot contact any KDC for the requested realm

Possible Cause: The KDC could not be contacted for the requested realm.

Action: The Kerberos Login Method for NMAS is unable to contact KDC because the KDC server might be down. Contact your Kerberos administrator.

The specified KDC hostname/address does not exist

Action: Check whether the KDC hostname/address specified in the krbHostServer attribute of the KDC object in eDirectory is correct.

NMAS Login Failed Return Code: -1634 (0xFFFFF99E) System Resources

There are a few possible causes for this error:

Possible Cause: The system might be running low in memory.

Action: Make sufficient free memory available on the system.

Possible Cause: The krb.con file is in Read-only mode and the required KDC information is not present.

Action: Update the KDC information in the krb.con file or delete it, so that the client can create it with the appropriate entries.

Kerberos LSM

Directory Services Trace

This section explains the error messages displayed in the *Directory Services Trace (DSTrace)* (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2908733.htm).

NMASKRB: Unable to accept the context from the *eDirectory user FDN*

There are a number of possible causes for this error.

Possible Cause: The replay cache is not found.

Action: This is specific to Windows. Check whether the /tmp/rc directory exists under the directory specified by the hkey_local_machine\software\novell\kerberos\1.0\krb5-config\directory registry key.

If not, manually create it.

Possible Cause: The system time between the hosts are not synchronized.

Action: Synchronize the time between the NMAS Client host, the NMAS Server host, and the KDC host.

Possible Cause: The key, the key version, or the key type of the eDirectory service principal in eDirectory and in the KDC might be different.

Action: Perform the procedure given in "Extracting the Key of the Service Principal for eDirectory" on page 20 and "Setting a Password for the Kerberos Service Principal" on page 22.

NMASKRB: Internal Error

Explanation: The Kerberos Login Method for NMAS failed to acquire the required system resources.

NMASKRB: Insufficient Memory

Possible Cause: The memory available is not sufficient.

Action: Ensure that the other processes running on the system are not consuming excess memory.

NMASKRB: The *realm name* object does not exist

Possible Cause: The Realm object does not exist under the Kerberos Security container.

Action: Create a Realm object for the required realm. For more information, refer to "Creating a New Realm Object" on page 16.

NMASKRB: The *realm name* is not configured properly

Possible Cause: The required attributes are not available for the Realm object.

Action: Add the required attributes to the Realm object. For more information, refer to "Creating a New Realm Object" on page 16.

NMASKRB: Unable to inject credentials for the *eDirectory service principal name*

Possible Cause: The eDirectory service principal key might be corrupted.

Action: Perform the procedure mentioned under "Creating a Service Principal Object in eDirectory" on page 20.

NMASKRB: Unable to acquire credentials for the *eDirectory service principal name*

Possible Cause: The service principal object might not be present in the eDirectory server.

Action: Perform the procedure mentioned under "Creating a Service Principal Object in eDirectory" on page 20.

Possible Cause: The eDirectory service principal key might not be present in the service principal object on the eDirectory server.

Action: Perform the procedure mentioned under "Creating a Service Principal Object in eDirectory" on page 20.

Possible Cause: The eDirectory service principal key might be corrupted.

Action: Perform the procedure mentioned under "Creating a Service Principal Object in eDirectory" on page 20.

Possible Cause: The realm's master key is corrupted.

Action: Delete the realm and create it again with the master password. Ensure that the master password is the same as the one specified previously while creating the realm.

Possible Cause: The treename is specified in lower case in the eDirectory service principal name.

Action: Refer to "Creating a Service Principal for eDirectory" on page 19.

NMASKRB: Failed to create the required registry entry

Possible Cause: The registry entry hkey_local_machine\software\novell\kerberos\1.0\krb5-config\directory registry key is missing.

Action: You must manually create the registry key and its value must be an existing directory. For example: C:\Novell\NDS\

iManager plug-in for NMAS Kerberos

Creation of Secure SSL LDAP context failed

Possible Cause: After you have logged in using the Login to a Different Tree button, you might receive the message like Creation of Secure SSL LDAP context failed when administering a Kerberos Management role.

Action: The Kerberos Management role requires secure LDAP access to function properly. To set up secure access, see Configuring iManager for SSL/TLS Connection to eDirectory section in *iManager Administration Guide* (http://www.novell.com/documentation/lg/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/am4ajce.html#bow4dv4).

Authentication Failed

Possible Cause: The Kerberos Login Method for NMAS requires a secure LDAP access to function properly.

Action: Configure iManager for SSL/TLS Connection to eDirectory. For more information, refer to the *iManager Administration Guide* (http://www.novell.com/documentation/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/am4ajce.html).

IIS File Upload Error During Module Package Install

Action: An "Unexpected end of part" error may be encountered during module package install when running iManager on a Windows IIS Web server with Tomcat. This is due to a known issue with uploading files through the Tomcat redirector for IIS. To successfully run a module package install, connect to iManager directly through Tomcat (for example, through port 8080).

For more information, refer to the *iManager Administration Guide* (http://www.novell.com/documentation/imanager20/index.html).

Service unavailable:

Possible Cause: The specified Fully Distinguished Name (FDN) might be invalid.

Action: Specify the correct FDN of the object.

-1073728824 Server received a corrupted request

Possible Cause: The Kerberos LDAP Extensions client (iManager) does not support the Kerberos LDAP Extensions installed on the eDirectory server.

Action: Upgrade both the Kerberos LDAP Extensions client and the server to the latest version.

-1073728823 The communication channel is not secure

Possible Cause: The connection between the Kerberos LDAP Extensions client (iManager) and the Kerberos LDAP Extensions installed on the eDirectory server is not secure.

Action: Configure iManager for SSL/TLS Connection to eDirectory. For more information, refer to the *iManager Administration Guide* (http://www.novell.com/documentation/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/am4ajce.html).

-1073728822 Unable to process the request. Try after some time

Possible Cause: The resources required for processing the request might not be available. This may be due to many reasons such as insufficient memory, etc.

Action: Try after some time.

-1073728821 The Server does not have enough memory to process the request

Possible Cause: The Server is running low in memory to process the request.

Action: Try after some time.

-1073728820 The request is not supported by this version

Possible Cause: The version of the Kerberos LDAP Extensions that you have does not support the request.

Action: Upgrade to the latest available version.

-1073728819 The protocol version of the client is not supported by the server

Possible Cause: The protocol version of the Kerberos LDAP Extensions client (iManager) does not match with that of the Kerberos LDAP Extensions installed on the eDirectory server.

Action: Upgrade both the Kerberos LDAP Extensions client and the server to the latest version.

-1073728818 Unable to resolve the proper replica type

Possible Cause: The Kerberos LDAP Extensions client (iManager) is unable to resolve to a Writable replica.

Action: If the writable/master replica is down, wait for sometime and try again.

-1073728817 Encryption type requested is not supported

Possible Cause: The requested encryption type is not supported by the Kerberos LDAP Extensions.

Action: Refer "Creating a New Realm Object" on page 16.

-1073728815 Principal key is corrupted

Possible Cause: The principal key information is corrupted and cannot be understood by the Kerberos LDAP Extensions.

Action: Manually delete the principal key and recreate it using the "Setting a Password for the Kerberos Service Principal" on page 22.

-1073728814 Unable to read the master key for the specified realm

Possible Cause: Unable to read the master key from eDirectory for the specified realm.

Action: You might not have enough permissions to read the master key from eDirectory. If this is not the case, recreate the realm object with the master password.

-1073728813 Master key is corrupted

Possible Cause: The master key information is corrupted and cannot be understood by the Kerberos LDAP Extensions.

Action: Recreate the realm object with the master password. Ensure that the master password is the same as the one specified previously while creating the realm. If the master password does not match with the previous one, all the principal keys encrypted with the old master password become unusable.

-1073728812 Requested principal key is not found in eDirectory

Possible Cause: No password options were specified while creating a principal object or the principal key attribute might have been deleted.

Action: Set the principal key using the "Setting a Password for the Kerberos Service Principal" on page 22.

-1073728811 Requested Master key is not found in eDirectory

Possible Cause: No master password was specified while creating the realm object or the master key attribute might have been deleted.

Action: Recreate the realm object with the master password. Ensure that the master password is same as the one specified previously while creating the realm. If the master password does not match with the previous one, all the principal keys encrypted with the old master password become unusable.

-1073728808 Unrecognizable response from Server

Possible Cause: The Kerberos LDAP Extensions Server is malfunctioning or the version of the Kerberos LDAP Extensions client (iManager) and Kerberos LDAP Extensions server do not match.

Action: Upgrade both the Kerberos LDAP Extensions client and the server to the latest version.

-1073728805 An unknown error has occurred

Possible Cause: The specified tree key type is not supported by the Kerberos LDAP Extensions

Action: Report this error to Novell Technical Support (http://support.novell.com).

-1073736929 Decrypt integrity check failed. Encrypted data might have been modified

Possible Cause 1: The encrypted principal key has changed, but the syntax has been maintained

Possible Cause 2: The principal key has not been changed after changing the master key.

Possible Cause 3: The realm object has been recreated with a different master password.

Action: Delete the principal key and create the key again so that the principal key is encrypted with the latest master key.

-1073728810 Principal name exceeds the maximum size limit

-1073728809 Principal key exceeds the maximum size limit

-1073728807 Realm Name exceeds the maximum size limit