eDirectory Field Guide

Rick Killpack

Apress®

eDirectory Field Guide

ISBN (pbk): 1-59059-553-X

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Lead Editor: Jim Sumser
Technical Reviewer: Kevin Fenn
Editorial Board: Steve Anglin, Dan Appleman, Ewan Buckingham, Gary Cornell, Tony Davis, Jason Gilmore, Jonathan Hassell, Chris Mills, Dominic Shakeshaft, Jim Sumser
Associate Publisher: Grace Wong
Project Manager: Sofia Marchant
Copy Edit Manager: Nicole LeClerc
Copy Editor: Bill McManus
Assistant Production Director: Kari Brooks-Copony
Compositor: Dina Quan
Proofreader: Dan Shaw
Indexer: Valerie Perry
Artist: Kari Brooks-Copony
Cover Designer: Kurt Krames
Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax 201-348-4505, e-mail `orders-ny@springer-sbm.com`, or visit `http://www.springeronline.com`.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail `info@apress.com`, or visit `http://www.apress.com`.

CHAPTER 5

Backup and Restore Operations

The following topics are covered in this chapter:

- Types of backup options
  - Hot continuous backup (Backup eMTool)
  - Directory backup and restore in NWCONFIG
  - DIB backup through DSREPAIR
  - NDSBackup
  - TSA backup
  - File copy
  - DIBClone
- Backup and restore strategies
- Using hot continuous backup
  - The backup file header
  - Roll-forward logging
  - Using iManager to configure and perform backup and restore
- Backing up the security infrastructure

eDirectory has built-in fault tolerance. Because eDirectory is a multi-master directory, any read/write replica can become the master replica and distribute replicas to other servers. So, if a server fails because of a hardware problem or for any other reason, the eDirectory information can be re-sent from another server that holds a replica of the same data to the failed server after the failure has been resolved.

Even though eDirectory has built-in fault tolerance, it is a good idea to back up the eDirectory database on each server, especially if the server

contains replicas of very large partitions. With large partitions, or a large number of objects broken up into many partitions, it will take a while to replicate all of the objects back to the server that failed. If you have made a backup of the local database, the backup can be restored fairly quickly, leading to less down time.

Types of Backup Options

There are several ways to back up the eDirectory database. Some of the methods are platform specific. This section covers the different backup methods and makes recommendations on which one to use and when to use it.

Hot Continuous Backup (Backup eMTool)

The Novell eDirectory Backup eMTool (hot continuous backup) is designed to give you a complete backup and restore solution of the database and associated files on an individual server. The eMTool will verify the state of other servers in the tree that hold replicas of the same partitions that the "bad" server held and will restore the replicas to the current state on the server that went down. The eMTool does this by restoring the last full backup and incremental backups taken and then re-executing any transactions that occurred after the last backup.

Advantages

- Same tool is used for all platforms.
- Backs up the database with the directory agent still running.
- Restores very quickly, for minimal down time.
- Provides remote task-management support, so you don't have to be at the server to use it.
- Supports unattended backups through scripts.
- Maintains partition boundary information.

■ **Note** For detailed information on the eMBox Backup tool, see "Backing Up and Restoring Novell eDirectory" in the *Novell eDirectory 8.7.3 Administration Guide,* at `http://www.novell.com/documentation/edir873/edir873/data/a2n4mb6.html`.

Disadvantages

- It is not very useful for a multiple-server outage. The exception to this is that if the whole tree is wiped out, one box can be restored with the entire tree and then eDirectory replication can be used to rebuild the other servers.
- Does not back up file system information.
- Roll-forward logs (RFLs) store all of the updated transactions, which can take up a lot of disk space.
- Does not support single-object backup or restore.

Directory Backup and Restore in NWCONFIG

This option is used for hardware upgrades. The migration utility in NetWare uses this method to back up an eDirectory database and move it to another server during the migration process.

Advantages

- Quick and efficient way to back up the database for hardware upgrades.

■ **Note** For more information on backup and restore options in NWCONFIG, see `http://support.novell.com/cgi-bin/search/searchtid.cgi?/10014282.htm`.

- Built into the eDirectory agent. No additional configuration is required.

Disadvantages

- Only available on NetWare.
- Does not back up the file system.
- Very rigid on restore. It is important that nothing is changed in the existing tree between backup and restore.
- Will lock the current database.

DIB Backup Through DSREPAIR

DSREPAIR has an option to back up the eDirectory database (creating an eDirectory archive).

Advantages

- Is quick and efficient.
- Can be automated.

Disadvantages

- Does not back up file system information.
- Only available on NetWare.
- No restore option is available through the product. Novell NTS must be used to restore the database.
- Most of the time, after the database is restored, all replicas must be removed and re-added to ensure data integrity across all replicas of the given partitions.
- Does not back up file system information.

NDSBackup

NDSBackup is a *nix (Linux, Solaris, HP-UX, AIX) solution. It is a powerful tool that allows the backup of a database with the NDSD process active or inactive.

■ **Note** For more information about NDSBackup, see `http://www.novell.com/documentation/edir873/edir873/data/a2n4mbo.html#advslf6`.

Advantages

- Allows for selective backup and restore.
- Can be scripted to run in unattended mode.

Disadvantages

- Only available on *nix platforms.
- Does not save partition information.

- If restoring, all other copies of the objects being restored must be removed from the other servers. The reason for this is that the object information is saved but the EntryIDs are not. On restore, a new object with the same name and information is created. If other copies of the old object are still present, collision renames will occur because you will have two objects with the same name but different creation time stamps.
- Does not back up file system information.

TSA Backup

Novell eDirectory provides APIs that will allow a TSA-enabled backup vendor to capture eDirectory data and store it on tape.

Advantages

- File system–specific data can be backed up.
- It allows for selective backup and restore.
- It can be scripted to run in unattended mode.

Disadvantages

- Only available for Windows and NetWare.
- Does not save partition information.
- If restoring, all other copies of the objects being restored must be removed from the other servers. The reason for this is that the object information is saved but the EntryIDs are not. On restore, a new object with the same name and information is created. If other copies of the old object are still present, collision renames will occur because you will have two objects with the same name but different creation time stamps.
- Requires a third-party TSA backup application.

File Copy

The Novell eDirectory database files can be copied to another server or directory for redundancy. If a server goes down, they can be copied back to the default location as a restore option.

Advantages

- Is quick and efficient.
- Can be automated.

Disadvantages

- Does not back up file system information.
- If a server fails, when new hardware is put in place, make sure that the server maintains the same name and addresses as it did before the crash.
- Most of the time, after the database is restored, all replicas must be removed and re-added to ensure data integrity across all replicas of the given partitions.

■ **Important** Do not restore the database unless you have experience doing so. You can create conditions where the entire partition with all of its replicas will no longer synchronize. It is highly recommended that you contact Novell NTS before executing this restore procedure.

DIBClone

DIBClone enables you to replicate an entire server with all of its partitions to another server. You do this simply by adding the new server's NCP server object into eDirectory and adding the new server to the replica ring and transitive vectors. The DIB from the original server is copied to the target server. The target server makes some modifications on bootup so that the DIB belongs to the target server rather than the source server. The result is that you now have two servers with the same partitions without having to replicate the objects over the wire.

Advantages

- Very fast way to replicate a server.
- Great for large-scale environments.

Disadvantages

- Must have another server with all of the partitions to make a copy.
- Only restores the NCP server object, so it is not a completely fault-tolerant solution. You would need to reinstall all the components, such as SAS, HTTP, LDAP, NMAS, etc.

Backup and Restore Strategies

The reason that there are several backup and restore options for eDirectory is that the disaster-recovery requirements change in each business environment. Your task is to determine which solution works best for you. To help you make that determination, this section provides some points of consideration and describes which backup and restore solution works best for each business case scenario. Review the different areas of interest and determine the best backup strategy for your environment.

The following are some backup and restore considerations, each of which is described in turn in the sections that follow:

- Automated backups
- No data loss
- Remote capabilities
- No additional configuration requirements after restore
- Size of the DIB in eDirectory
- Partitioning considerations
- Selective restore requirements
- File system considerations
- Multiple-server restore strategies

Automated Backup

If you want to automate your backups, the following options are available:

- *Partition replication*: By default, eDirectory replicates all data to all servers in a given replica ring. It is important in these cases to make sure that there are adequate copies of the partition. You should have at least three copies of any partition. Furthermore, one of those copies should be located at a different site in case of a loss of an entire site.
- *Hot continuous backup*: The Backup eMBox tool allows you to run backups in batch mode. Depending on the operating system, you can write a script with the command-line options. Also depending on the operating system, you can use automated applications like CRON to launch the script at different times of the day, week, month, or year.

Tip See `http://www.novell.com/documentation/edir873/edir873/data/agatd4y.html` for more information on backup options with the eMBox client.

- *DIB Backup through DSREPAIR*: DSREPAIR has command-line options in NetWare. Running the DSREPAIR –RC command will automatically execute a backup of the eDirectory database. This command can be written to an NCF file and executed in intervals using CRON.
- *NDSBackup*: NDSBackup is a command-line utility for Linux/Unix platforms. For more information on the available options, see the man pages for NDSBackup (type **man ndsbackup** from a Linux or Unix console). You can write a script with the desired options for NDSBackup. You can then automate execution of the script with applications like CRON.
- *TSA backup*: This option is vendor specific. Many TSA backup vendors provide automated procedures for backing up eDirectory.

No Data Loss

The sensitivity of lost data must be considered. If preventing data loss is extremely important to you because of the uniqueness or sensitivity of the data, you should put in place additional measures to prevent data loss. In the case of high data availability, the following backup and restore options are recommended:

- *Partition replication*: By default, eDirectory replicates all data to all servers in a given replica ring. It is important in these cases to make sure that there are adequate copies of the partition. You should have at least three copies of any partition. Furthermore, one of those copies should be located at a different site in case of a loss of an entire site.
- *Hot continuous backup*: Make sure that roll-forward logging is turned on so that all data is recovered.

■ **Tip** For more information on roll-forward logging, please see `http://www.novell.com/documentation/edir873/edir873/data/agavcur.html`.

- *File system trustee backup*: If file system trustees are critical, they should be backed up separately.
- *Security infrastructure backup*: If user certificates, trusted root containers, SSL connections, etc. are being used and are critical, you should back up the Certificate Authority Container object and the W0 object. For more information, see the following Novell resources:

- *Server keys*: See `http://support.novell.com/cgi-bin/search/searchtid.cgi?/10066559.htm` for information on and the location of NICI files for each platform.
- *Certificate Authority object*: See `http://support.novell.com/cgi-bin/search/searchtid.cgi?/10065921.htm` for information on the Certificate Authority object.
- *Tree key information*: See `http://support.novell.com/cgi-bin/search/searchtid.cgi?/10064202.htm` for information on how to manage the tree key.

Remote Capabilities

The following backup and restore options are available remotely:

- *Hot continuous backup*: Novell iManager enables you to execute the backup and restore options remotely. For more information, see `http://www.novell.com/documentation/edir873/edir873/data/af37xzc.html`.
- *TSA backup*: Depending on the vendor, the TSA backup option will allow you to do remote backup and restore operations.

No Additional Configuration Requirements After Restore

The following backup option should be used if you do not require additional configuration after the restore of the eDirectory database:

- *Hot continuous backup*: Hot continuous backup enables you to restore a server to the exact state it was in before it went down. The exception to this would be file system trustee assignments.

Size of the DIB in eDirectory

If the size of the DIB is large—2 to 3GB or greater—some backup and restore operations can take a while. Partition replication, TSA backup, etc. may not be the best options. The following is recommended in these cases:

- *Hot continuous backup*: This option is highly scalable. Novell testing has shown isolated cases where a 20GB database can be backed up in 10 minutes and restored in 15 minutes.

■ **Important** Because many variables will affect performance, your testing results may vary from those reported in the tests conducted by Novell.

- *DIBClone*: DIBClone was designed to duplicate a very large database quickly. In testing conducted by Novell, a 100-million-object tree was cloned on a second server in just a few hours.
- *NDSBackup*: This option could be a good solution if only part of the database is critical. A selective backup and restore could be performed using NDSBackup to save only the critical, irreplaceable data.

Partitioning Considerations

If your tree has extensive partitioning, TSA backup and NDSBackup are probably not good options. The reason for this is that those options do not save partition configurations. After a restore with TSA backup or NDS-Backup, all partitioning would have to be reconfigured, which could be very time consuming and costly. The following options should be considered if partitioning is a factor:

- Hot continuous backup
- DIBClone
- DIB backup through DSREPAIR

Selective Restore Requirements

The following options allow for selective restore:

- NDSBackup
- TSA backup (dependent on the third-party TSA solution)

File System Considerations

Most of the backup options do not back up the file system–specific information. The following options are available:

- TSA backup (dependent on the third-party TSA solution)
- File system trustee backup

Multiple-Server Restore Strategies

If multiple servers fail, typical backup and restore options may not apply. The purpose of this section is to recommend some disaster-recovery options to consider:

- *Hot continuous backup*: This option was designed to restore a single-server failure. The nature of this restore is to re-execute all changes made to eDirectory on the given server since the last backup of the database. If multiple servers are involved with the same changes, determining which server to restore first and how to synchronize the data can become very complex. If multiple servers fail at the same time and you are using hot continuous backup, Novell recommends restoring without verification a server that holds common replicas and restoring all other servers as external reference objects. For more information on these procedures, see `http://www.novell.com/documentation/edir873/edir873/data/agm7hq7.html`.
- *TSA backup*: This is a good option for a treewide disaster recovery. The TSA backup software allows the whole tree to be backed up to tape. The entire tree would be restored to one server. eDirectory partitions would be removed from all other servers in the tree. Partition boundaries would be re-established and then replicated to all servers in the tree.
- *NDSBackup*: With NDSBackup, a procedure similar to the one described in the preceding TSA backup option would be used.

Best Practice Recommendations

It is wise to use multiple backup strategies to ensure minimal data loss in case of hardware failure. It is also wise to ensure proper tree design and partition replication as the default method of backup and restore.

■ **Tip** For more information on Novell eDirectory replication, see `http://www.novell.com/documentation/edir873/edir873/data/a2iiie1.html`.

Secondarily, hot continuous backup is a great option for server-to-server backup and restore. It enables you to back up and restore a server to its exact state before the failure.

Although hot continuous backup is a great option, a wise administrator would not be satisfied with a potential single point of failure. There is always a chance that the hot continuous backup information could also be lost. For that reason, it is wise to also keep a reasonably current snapshot of the

database. The frequency of this will vary, depending on the amount of changes that are taking place in the tree and the criticality of the data. Use options like the following to make sure a reasonably current version of the database is maintained:

- DIB backup through DSREPAIR
- File copy
- Export to an LDIF file
- NDSBackup

These backups should be stored off of the server on secondary media and possibly even offsite to ensure high availability in the case of a disaster.

Using Hot Continuous Backup

eDirectory ships with a Java-based toolbox called eDirectory Management Toolbox (eMBox). This Java client can access tools called eMTools. A very powerful and flexible eMTool called Backup is included. The Backup eMTool can be used to perform hot continuous backup. In most cases, it is recommended to use the hot continuous backup solution over the other backup solutions described in this chapter. Therefore, I will spend some time talking about how to configure and use the Backup eMTool.

■ **Note** For an exhaustive description of how to use this tool, please refer to the *eDirectory Administration Guide* at `http://www.novell.com/documentation`.

The following files are the primary files used for hot continuous backup solutions:

- *backuptl*: This file provides the user interfaces. It connects into the library backupcr. This file can be accessed by the eMBox Client by calling "backup" or by using the iManager eDirectory Maintenance backup and restore plug-in.
- *backupcr*: This is the core library that performs the actual backup and restore. It is called through the backuptl interface.

The Backup eMTool backs up the entire eDirectory database and stores it in an encrypted file. The filename is specified when you initiate the backup. eDirectory also provides a feature called *roll-forward logging* (see the section "Roll-Forward Logging" later in the chapter). This is a true

database transactional backup. All modifications to the directory are stored in roll-forward logs (RFLs). The Backup eMTool has the ability to restore the backup, which is a snapshot in time, and then re-execute all of the modification transactions that are stored in the RFLs, putting the DIB back into the exact state before the failure that triggered the need to restore the database.

The Backup File Header

The backup file that is created is stored in an XML format. The Document Type Definition (DTD) is included at the beginning of the backup file. There is a lot of good information stored in the DTD that you can use to determine which backup file you are looking at. Refer to Table 5-1 for information about the data stored in the DTD.

Table 5-1. *The DTD*

Field	Description
backup version	Identifies the version of the backup tool that was used to perform the backup.
backup_type	Specifies whether the backup was incremental or a full backup.
idtag	Identifies the ID of the backup. The ID is a GUID that is based off of the time stamp when the backup was taken.
time	Stores the date and time when the backup was taken.
srvname	Identifies the Distinguished Name (DN) of the server that was backed up.
dsversion	Indicates the eDirectory version of the server that was backed up.
compression	Specifies whether or not the backup was compressed.
os	Records the operating system that eDirectory is running on. It is recommended that you restore the backup on the same operating system that it was backed up from.
current_log	Specifies the first RFL that the backup is expecting. This field helps you to identify which RFLs you need to restore a complete backup.
number_of_files	Indicates the number of files in this backup set. This value will only be set on the first file. One of the variables you can set is the backup file size. If you choose this option, you could potentially have more than one backup file.

Continued

Table 5-1. *Continued*

Field	Description
backup_file	Provides the full path and name of the backup file. If your backup spans multiple files, this field contains the name as well as a number indicating its order in the backup file set.
incremental_file_id	Identifies the file ID if the backup is incremental.
next_inc_file_id	Indicates the file ID of the next backup file if the backup is an incremental backup.
replica_partition_DN	Specifies the DN of each partition root entry that resides on this server. This is helpful to identify which partitions reside on this server.
modification_time	Lists the Transitive Vector value for this server at the time of the backup. This value is used by the restore process to ensure replication consistency after a restore. The values are stored in hexadecimal. The Transitive Vector value contains the number of seconds since January 1, 1970, as well as the replica number and event; for example, CB708641_r1_e1.
replica_type	Lists the replica type for each value in the replica_partition_DN field.
replica_state	Lists the replica state for each value in the replica_partition_DN field.
file_size	Indicates the file size of any files that are user files included in the backup.
file_name	Specifies the name and location of any user-included files.
file_encoding	Lists the algorithm used to encode the specified user-included file.
file_type	Lists the type of file included by the user.

Listing 5-1 includes a sample backup.log file and output.

Listing 5-1. *Sample backup.log File*

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE backup [
<!ELEMENT backup (file|replica)*>
<!ELEMENT file (#PCDATA)>
<!ELEMENT replica EMPTY>
<!ATTLIST backup version CDATA #REQUIRED
     backup_type (full|incremental) #REQUIRED
     idtag CDATA #REQUIRED
     srvname CDATA #REQUIRED
```

```
     dsversion CDATA #REQUIRED
     compression CDATA "none"
     os CDATA #REQUIRED
     current_log CDATA #REQUIRED
     number_of_files CDATA #IMPLIED
     backup_file CDATA #REQUIRED
     incremental_file_ID CDATA #IMPLIED
     next_inc_file_ID CDATA #IMPLIED>
<!ATTLIST file size CDATA #REQUIRED
     name CDATA #REQUIRED
     encoding CDATA "base64"
     type (user|nici) #REQUIRED>
<!ATTLIST replica partition_DN CDATA #REQUIRED
     modification_time CDATA #REQUIRED
     replica_type (MASTER|SECONDARY|READONLY|SUBREF ➥
|SPARSE_WRITE|SPARSE_READ|Unknown) #REQUIRED
     replica_state (ON|NEW_REPLICA|DYING_REPLICA|LOCKED ➥
||CRT_0|CRT_1|TRANSITION_ON|DEAD_REPLICA ➥
||BEGIN_ADD|MASTER_START|MASTER_DONE|FEDERATED|SS_0|SS_1|JS_0 ➥
||JS_1|MS_0|MS_1|Unknown) #REQUIRED>
]>
<backup version="2" backup_type="full" idtag="425AB288" ➥
| time="2005-4-11'T11:23:20" srvname="\T=RK_TREE\O=User\CN=rklinux"➥
dsversion="1055260" compression="none" os="windows" ➥
|current_log="00000001.log" next_inc_file_ID="1" ➥
number_of_files="000001" backup_file="backup.bak">
<replica partition_DN="\T=RK_TREE\O=User\OU=DK" ➥
|modification_time="s425AB216_r3_e2" replica_type="SUBREF" ➥
|replica_state="ON" />
<replica partition_DN="\T=RK_TREE\O=User\OU=obit" ➥
|modification_time="s425AB0C0_r3_e2" replica_type="SUBREF" ➥
|replica_state="ON" />
```

```
|==================DSBackup Log: Backup================|
Backup type: Full
Log file name: backup.log
Backup started: 2005-4-11'T11:23:20
Backup file name: backup.bak
Server name: \T=RK_TREE\O=abendme\CN=rklinux
Current Roll Forward Log: 00000001.log
DS Version: 1055260
Backup ID: 425AB288
```

```
Starting database backup...
Database backup finished
Completion time 00:00:02
Backup completed successfully
```

Roll-Forward Logging

Roll-forward logging enables eDirectory to be a true journaling database. Each modification made to eDirectory is stored in the roll-forward logs (RFLs). eDirectory enables you to specify where the RFLs are stored. The only requirement is that the RFLs must be stored on a local drive.

By default, roll-forward logging is configured to overwrite the existing log when the size limit is exceeded. This implies that there could potentially be modifications that are lost if a database restore is required. If you use the Backup eMTool, it is recommended that you configure roll-forward logging to not overwrite the existing log when the size limit is hit. Configure the roll-forward logging to create a new file and continue logging. While performing a restore, the Backup eMTool will allow you to specify which RFLs to use and will re-execute all the transactions in those RFLs to bring the database back to the exact state before the database went down, causing the restore in the first place.

To allow roll-forward logging to create new files, you can use the eMBox Client. The procedure provided in Task 5-1 will enable roll-forward logging.

■ **Note** To use eMBox, Role-Based Services (RBS) must be set up in iManager. For more information on how to use eMBox, see Novell's documentation at `http://www.novell.com/documentation`.

Task 5-1. Enabling Roll-Forward Logging

1. Launch eMBox in interactive mode by typing **edirutil –i**.

■ **Note** On Windows, edirutil.exe is located in the directory where dhost.exe resides. By default, this is c:\novell\nds.

2. Log in to eMBox by typing the following at the eMBox Client prompt (if going nonsecure, you must specify the –n option):

```
login -s <server address> -p <http port i.e. 8008, 8028> ➥
| -u <user DN i.e. admin.novell> -w <password> -n
```

   To determine the HTTP port, perform the following based on your operating system:

   - *Netware*: The port is hard-coded to 8008 for nonsecure and to 8009 for secure.
   - *Windows*: In NDSCons, click the Transports tab and then choose HTTP ➤ Bound Transports for nonsecure or HTTPS ➤ Bound Transports for secure.
   - **nix*: At a terminal, type **ndsconfig get | grep http.**

3. Turn on logging by typing the following (the –s option starts a new file):

```
backup.setconfig -L(turns on logging) ➥
| -T(starts logging of streams files) -r<RFL directory> ➥
| -n<minimum size of RFLs> -m<max size of files> ➥
| -s
```

■ **Note** To see all of the options, type **list –t backup**.

When using roll-forward logging, you should address the following issues:

- Create a new partition on your disk for roll-forward logging. The RFLs are stored in the same directory as the eDirectory DIB. If, by mistake, you forget to remove the logs before you run out of space, you may create a condition in which eDirectory cannot open because it is out of disk space.
- Remove RFLs periodically and store them on an external storage device, such as a tape drive.
- Do not change the name of the RFLs.
- Removing eDirectory from a server will also remove the RFLs. Make sure the logs have been copied to another drive before you remove eDirectory when performing disaster recovery.
- During a restore, all RFLs must be located in the same directory.

Using iManager to Configure and Perform Backup and Restore

You can also use iManager to configure and perform eMBox backups. To access the tools from iManager, choose eDirectory Maintenance ➤ Backup Configuration, as shown in Figure 5-1. After you configure the backup, as shown in Figure 5-1, click Start to save your changes.

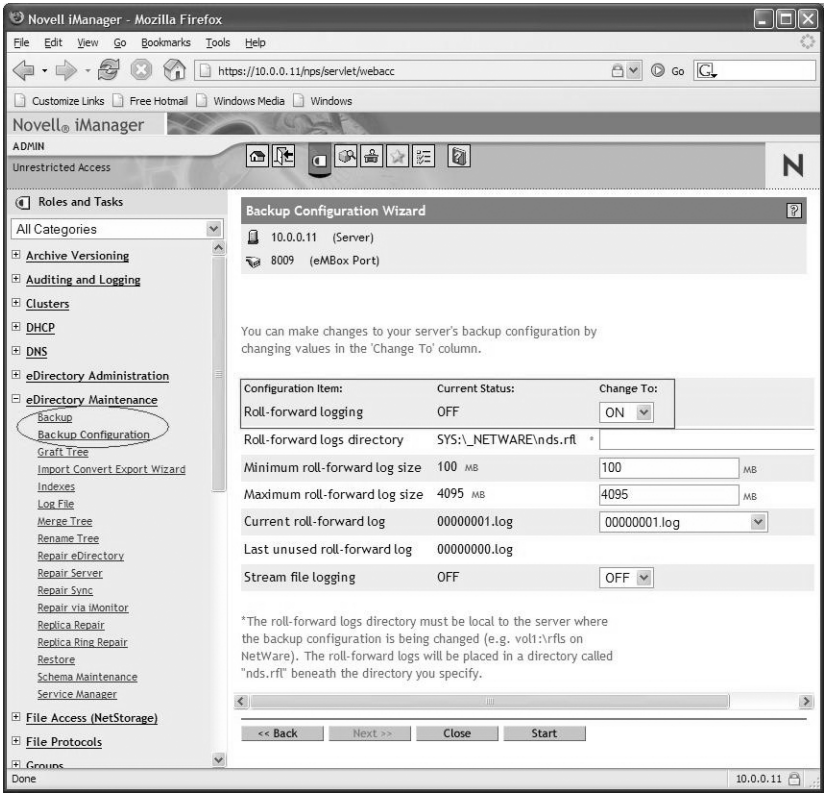

Figure 5-1. *Configuring the backup*

To initiate a backup through iManager, use the same eDirectory Maintenance role but use the Backup task instead, as shown in Figure 5-2.

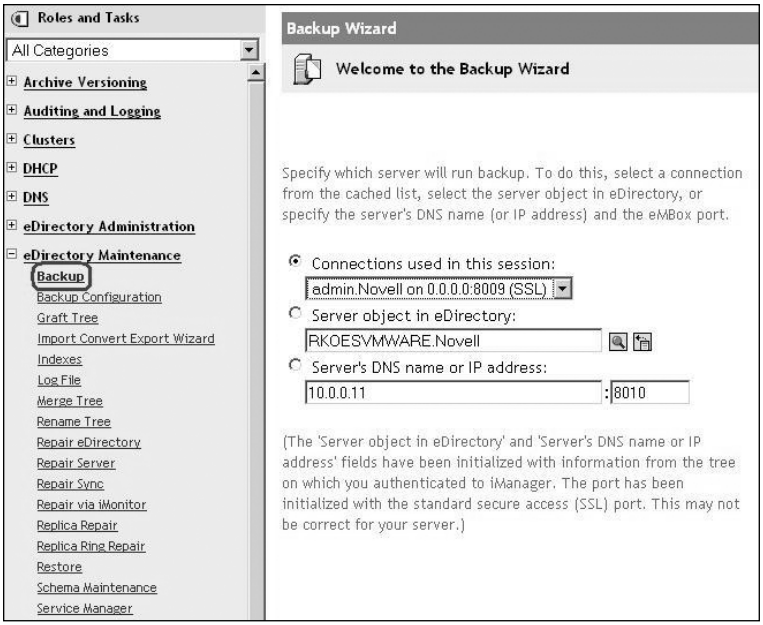

Figure 5-2. *Initiating a backup*

When creating a backup, you must specify, at a minimum, the names of the backup file and log file, similar to what is shown in Figure 5-3. You should specify the explicit directory as well.

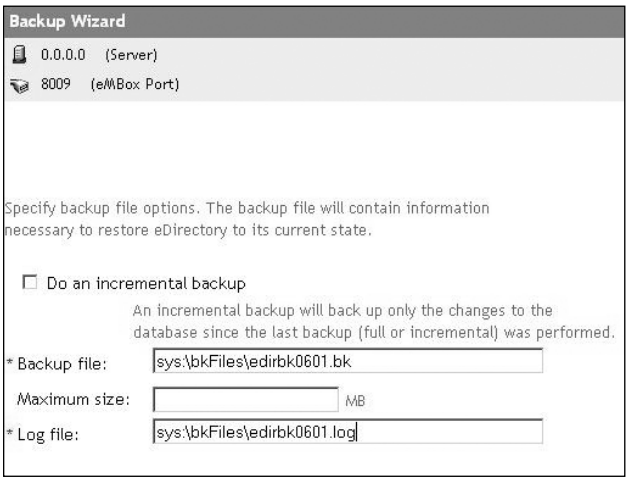

Figure 5-3. *Specifying the backup file and log file*

Click Next to finish configuring your backup options. When you are ready to begin, click Start.

■ **Note** Prior to the backup, you must create the directory in which the backup file and backup log will be stored. If the directory does not exist, an Error –2 will be returned and the backup will fail.

Backing Up the Security Infrastructure

You should also consider the security infrastructure when evaluating your backup needs. In general, the backup options described thus far do not back up file system information. Much of the security infrastructure is dependent on objects within Novell eDirectory as well as on the file system. It is important that the file system information also be backed up for disaster-recovery purposes. The following are some areas to consider:

- *Server keys*: Server keys are the core component of eDirectory's security infrastructure. If these keys are lost, all data that was encrypted directly or indirectly using the server keys will be lost. For more information on backing up the server keys, see `http://support.novell.com/cgi-bin/search/searchtid.cgi?/10066559.htm`.
- *Certificate Authority object*: The CA object has the trusted root information in it. If the CA object is lost, for whatever reason, all user certificates and server certificates will have to be reissued. For more information about backing up the CA object, see `http://support.novell.com/cgi-bin/search/searchtid.cgi?/10065921.htm`.
- *Tree key*: The tree key is used to encrypt user secrets. NMAS uses this extensively. Typically, all servers in the tree have a copy of the tree key, so it is not extremely critical if one server loses the key. It can by synchronized back. However, if all servers lose the tree key, all data (e.g., users' passwords) will be lost. For more information about backing up the tree key, please see `http://support.novell.com/cgi-bin/search/searchtid.cgi?/10064202.htm`.