IBM Vault Registry

Using the LDAP Directory With IBM Vault Registry

IBM Vault Registry

Using the LDAP Directory With IBM Vault Registry

Contents

Chapter 1. Overview

In prior releases of IBM® Vault Registry, the IBM eNetwork™ X.500 Directory was required. With Vault Registry version 2.2.2, which is a Directory-neutral product, you can also use the IBM eNetwork LDAP Directory version 2.1. This document discusses how to set up the LDAP Directory server for use in a Vault Registry environment. It also provides guidelines for backing up, restoring, and monitoring the Directory.

Chapter 2. Installing and Configuring the LDAP Directory

Before configuring the Vault Registry system, you must perform the following tasks:

- Ensure that the proper prerequisite programs have been installed and configured.
- Install the LDAP Directory software.
- Install an LDAP Directory software patch (provided with the Vault Registry software).
- Modify the Directory schema.
- Set up the Directory to allow anonymous access.
- Configure Directory entries for Vault Registry.
- Clean up AIX environment variables.

Prerequisites

If you plan to use the LDAP Directory, you must first install the LDAP Directory server that comes with the IBM AIX/6000 version 4.3.2. Then, you must install the version that is provided in the Vault Registry product package. This version, `ldap.server.rte 2.1.0.1`, which contains fixes that are not included with AIX/6000 version 4.3.2, is necessary for the proper operation of the Directory with Vault Registry.

The following list summarizes the prerequisite products that must be installed and configured on the LDAP Directory server before you can use the Directory with Vault Registry. Refer to the LDAP Directory documentation for specific details about system requirements.

- IBM AIX/6000® version 4.3.2
- Java 1.1.6 or higher
- A Web browser that supports the following:
  - Java 1.1.6
  - HTML 3.0 or higher
  - JavaScript 1.2
- IBM DB2® Universal Database (UDB) Enterprise Edition for AIX® version 5.2
- Lotus Domino Go Webserver version 4.6.2 or higher (you should use the version that is distributed with the Vault Registry software)

Installing the LDAP Directory Software

You can install the LDAP Directory software on the same machine where you plan to install the Vault Registry server components or on a separate machine. Regardless of where you install the software, you must ensure that IBM DB2 UDB version 5.2 is also installed on that machine.

To install the LDAP Directory, you must explicitly mount the CD-ROM file system and provide a pointer to the directory containing the LDAP Directory installation images. Use the following procedure to install the LDAP Directory software:

1. Log in to the AIX server as `root`.
2. Install the LDAP Directory that is included on the AIX 4.3.2 CD-ROM (`ldap.client ALL` and `ldap.server ALL`).
3. Place the *IBM Vault Registry Code for AIX* disc in the CD-ROM drive.

4. Enter the following commands:

```
# mount           /cdrom
# installp -a -d  /cdrom/ldap2101 -g ldap.server.rte 2.1.0.1
# umount          /cdrom
```

Preparing the System

The following steps summarize the procedures you should follow to set up the LDAP Directory in AIX before you configure it for use with Vault Registry. Refer to the following document for detailed information on how to configure the LDAP server:

`/usr/share/man/info/en_US/ldap/config/asvcfg.htm`

1. In AIX, make sure that:
   - The group `dbsysadm` is created. This group should contain users `root` and `ldapdb2`.
   - The user `ldapdb2` is created. Its primary group is `dbsysadm`.
2. Create the following DB2 instance (depending on your server, this may take a few minutes to create):

   /usr/lpp/db2_05_00/instance/db2icrt -u ldapdb2 ldapdb2
3. Log on as user `ldapdb2` and add the following line to the `.profile` file if it is not already there:

   . /home/ldapdb2/sqllib/db2profile
4. Exit and then log on as user `ldapdb2` again.
5. Enter the following command to start DB2:

   db2start
6. Enter the following command to create the `ldapdb2` database:

   db2 create database ldapdb2
7. Use the `ldapcfg` tool to define the LDAP administrator DN and password. For example:

   ldapcfg -u "cn=root,o=IBM,c=US" -p Secure98

   Note: You may want to make a note of this DN and password. You will need to log in as this user when setting up the Directory for Vault Registry.
8. Perform the following steps to prepare and start the Web server. These steps assume that you installed the Lotus Domino Go Webserver.
   - Enter the following command to make a copy of the Web server configuration file:

     cp -p /etc/httpd.conf /etc/httpd.ldapdb2.conf
   - Edit the `httpd.ldapdb2.conf` file, and change the **Port** directive from **80** to another unused port, such as **8000**.
   - Enter the following command to configure the Directory to use the Lotus Domino Go Webserver:

     ldapcfg -s dominogo -f /etc/httpd.ldapdb2.conf
   - Enter the following command to start the Web server with the new configuration values:

     /usr/sbin/httpd -r /etc/httpd.ldapdb2.conf

For additional information, see the HTML documentation provided in the following directories. The `config` directory contains information about the LDAP Directory and its prerequisite components.

```
/usr/share/man/info/en_US/ldap/config
/usr/share/man/info/en_US/ldap/program
```

Modifying the Directory Schema

For the LDAP Directory to work correctly with Vault Registry, you must modify the Directory schema files. The following sections discuss the changes you must make to certain schema attributes and object classes before using the Directory with Vault Registry.

- “Update Attributes”.
- “Update Object Classes”.

Update Attributes

To modify schema attributes, edit the `/etc/slapd.at.conf` file.

Update the schema attributes as shown below:

```
attribute sn s surname               cis  sn                128     normal
attribute comment                    bin  comment           5000    normal
attribute email emailAddress         cis  emailAddress      128     normal
attribute attributeCertificate       bin  attributeCertific 250000  sensitive
attribute userCertificate            bin  userCertificate   250000  sensitive
attribute cACertificate              bin  cACertificate     250000  sensitive
attribute authorityRevocationList    bin  authRevocationLst 250000  sensitive
attribute certificateRevocationList  bin  certRevocationLst 250000  sensitive
attribute deltaRevocationList        bin  deltRevocationLst 250000  sensitive
attribute crossCertificatePair       bin  crossCertPair     250000  sensitive
```

Update Object Classes

To modify object classes, edit the `/etc/slapd.oc.conf` file.

You must update the following existing object classes:

- Add `comment` to the list of allowed attributes (`allows`) under the `organizationalPerson` object class. You can optionally add the `comment` attribute to the `organization`, `organizationalUnit`, `locality`, and `device` object classes.
- Add `serialNumber` and `emailAddress` to the list of allowed attributes (`allows`) under the `organizationalPerson` object class.

You must also add two object classes, `entrustUser` and `entrustCA`, and define attributes for them as shown below:

```
objectClass entrustUser
        requires
                objectClass
        allows
                userCertificate

objectClass entrustCA
        requires
                objectClass
        allows
                cACertificate,
                certificateRevocationList,
                authorityRevocationList,
                crossCertificatePair,
                attributeCertificate
```

Starting the LDAP Directory Management System

To configure the LDAP Directory, you must start the LDAP management system and log in as the LDAP administrator.

1. Launch a Web browser.
2. Access the LDAP management system at the following URL, where *hostname.domain:port* identifies where you installed the Web server on your system:

   `http://`*`hostname.domain:port`*`/ldap`
3. For example:

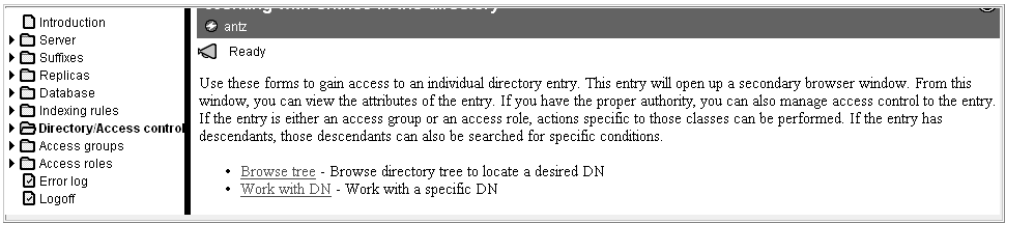
   `http://LDAPServer.ibm.com:8000/ldap`
4. Log in as the LDAP administrator you created in step 7 on page 4 as part of Preparing the System.

   Using the example provided in the procedure, you would log in as user `cn=root,o=ibm,c=us`, and specify the password `Secure98`.
5. The first time that you start the LDAP management system, you must select **`Database`**, and then click on **`Configure database`** to create a default database configuration.

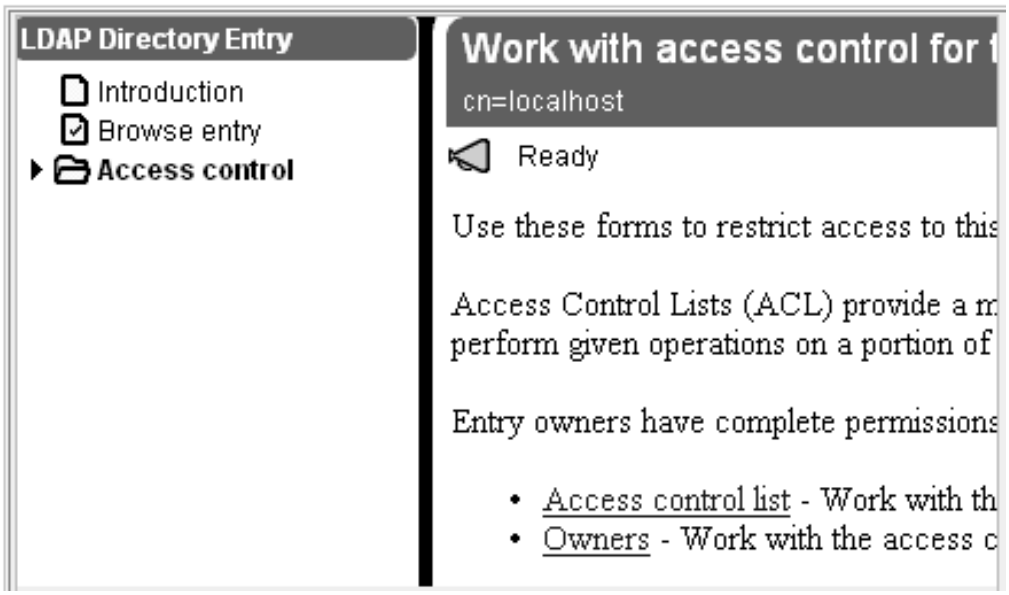
Setting Up Anonymous Access

Use the following procedure to set up anonymous access to the Directory. This allows all users to access the Directory and read, search, or compare entries in it.

1. If necessary, follow the procedure in “Starting the LDAP Directory Management System” and log in as the LDAP administrator.
2. Select **`Directory/Access control`** from the LDAP Directory Server menu, and then click on **`Browse tree`**. For example:

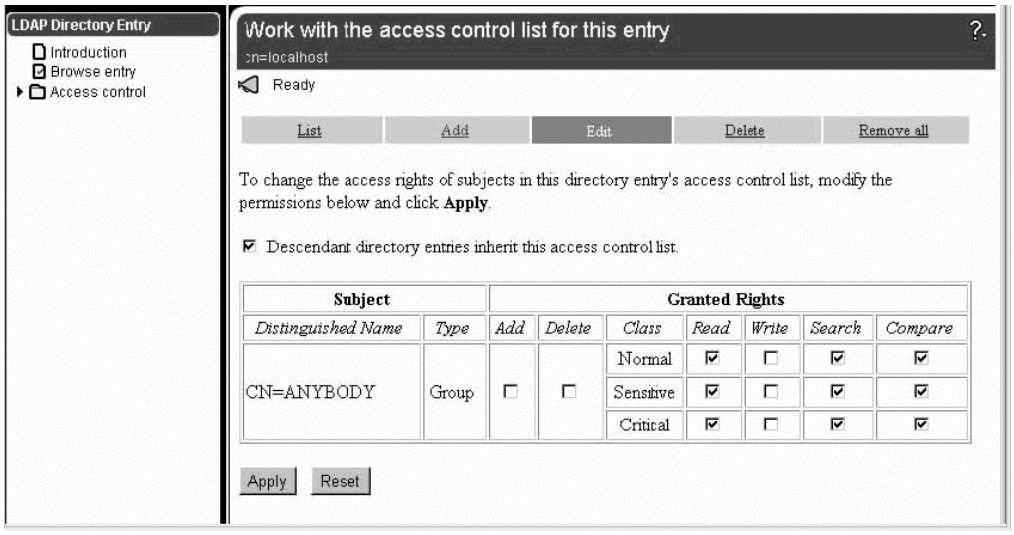


3. Expand the Directory tree and then select the entry **`cn=localhost`**.
4. Select **`Access control`** from the LDAP Directory Entry menu, and then click on **`Access control list`**. For example:



5. Click on **Edit** in the action bar.
6. Using the following figure as a guideline, grant **CN=ANYBODY** the right to **Read**, **Search**, and **Compare** entries in the Directory. Be sure to select all classes (**Normal**, **Sensitive**, and **Critical**) under each category.

   Note that you must also click in the **Descendent directory entries inherit this access control list** checkbox.



7. Click on the **Apply** button to apply the access control settings.

Configuring Directory Entries

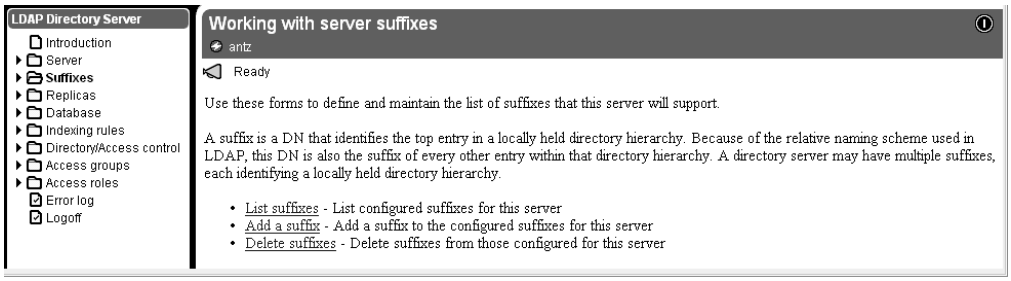
Follow the procedures in this section to set up entries in the LDAP Directory for the Vault Registry certificate management system. You must perform the following tasks to create a distinguished name (DN) for each Vault Registry certificate authority (CA) and its associated Directory Administrator (DirAdmin). You must also update the access control list (ACL) to grant appropriate access rights to each CA and its associated DirAdmin.

Add a Country Suffix

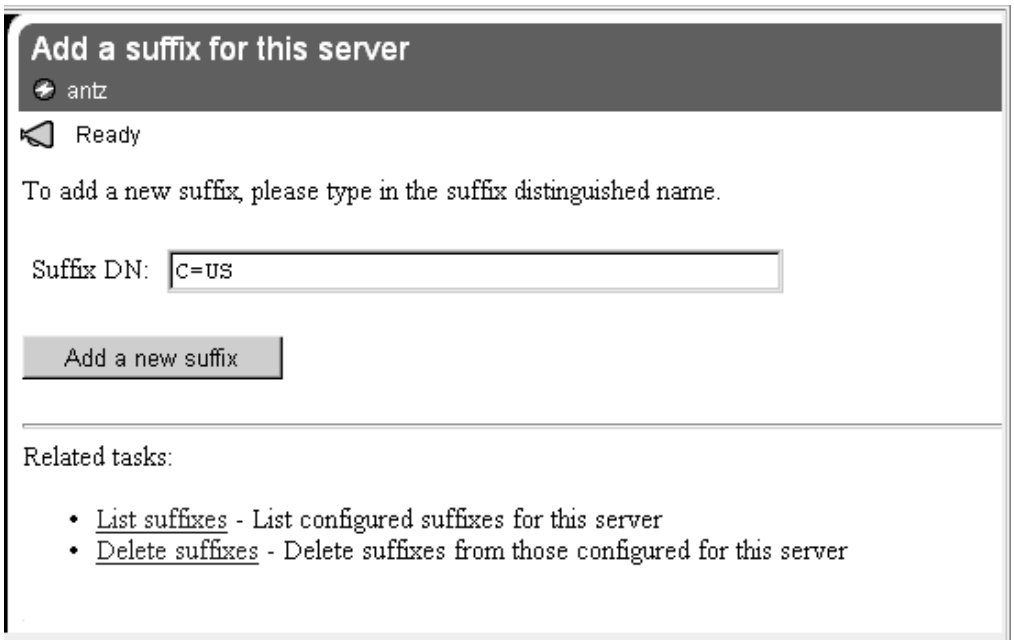
Use this procedure to add a country suffix for the distinguished names that will be created and used by the Vault Registry CAs. In the default Vault Registry configuration, the country suffix is:

c=US

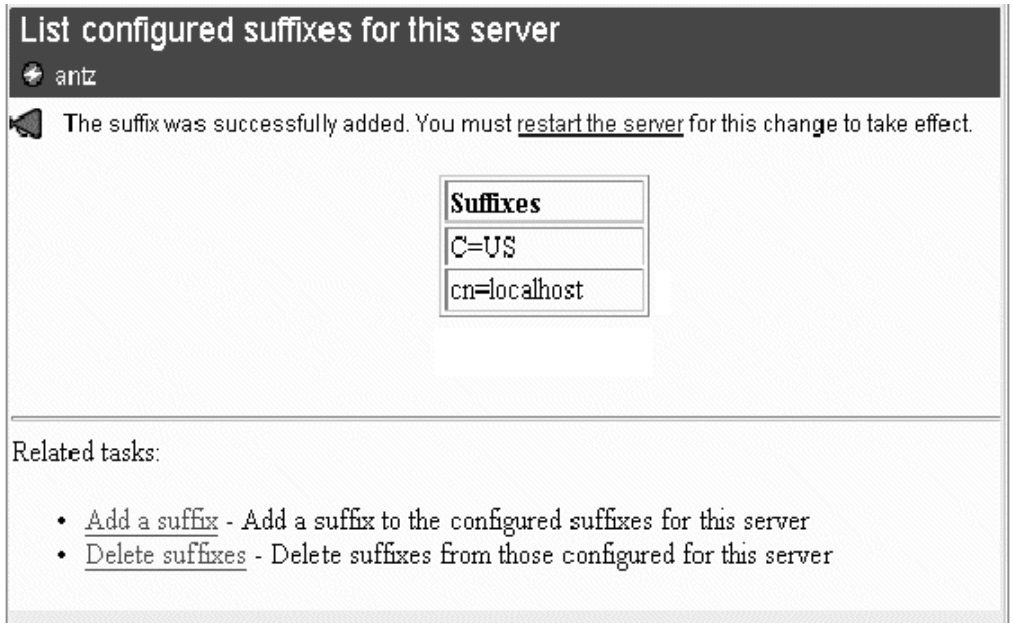
1. If necessary, follow the procedure in "Starting the LDAP Directory Management System" on page 6 and log in as the LDAP administrator.
2. Select **Suffixes** from the LDAP Directory Server menu, and then click on **Add a suffix**. For example:



3. Type the new suffix in the **Suffix DN** field, and then click on the **Add a new suffix** button.



The system shows that the suffix was successfully added.



4. Restart the server by clicking on the highlighted **restart the server** link, or by clicking on the **Restart server** button.

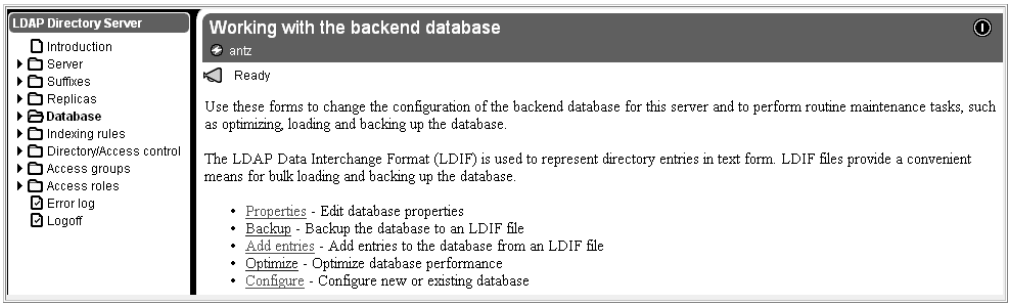
Add a Country Directory Entry

Use this procedure to add a country entry for the distinguished names that will be created and used by the Vault Registry CAs.

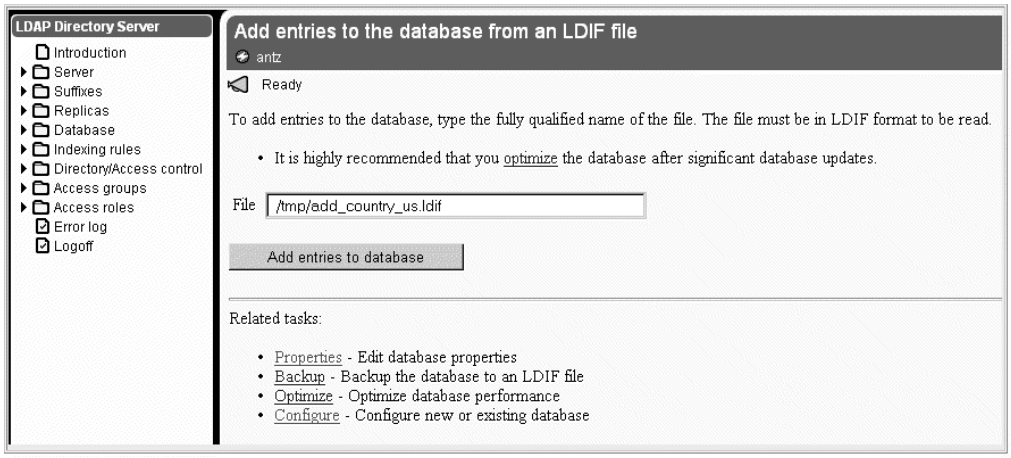
1. Create an LDAP Data Interchange Format (LDIF) ASCII file in the `/tmp` directory named **add_country_us.ldif**. Include the following lines:

```
dn:c=US
countryname:US
objectclass:country
```

2. If necessary, follow the procedure in “Starting the LDAP Directory Management System” on page 6 and log in as the LDAP administrator.
3. Select **Database** from the LDAP Directory Server menu, and then click on **Add entries**. For example:



4. Type the path for the LDIF file you just created in the **File** field, and then click on the **Add entries to database** button.



5. Restart the server by clicking on the highlighted **restart the server** link, or by clicking on the **Restart server** button.

Add the Vault CA

Use this procedure to create a Directory entry for the Vault CA. In the default Vault Registry configuration, the Vault CA’s DN is:

o=IBM, c=US

1. Create an LDIF-formatted ASCII file in the `/tmp` directory named **add_ca_ibm.ldif**.

2. To create the Vault CA at the organization level, as in the default Vault Registry configuration, include the following lines:

   ```
   dn:o=IBM, c=US
   organizationname:IBM
   userpassword:Secure98
   OBJECTCLASS:ORGANIZATION
   OBJECTCLASS:ENTRUSTCA
   ```

3. If you want to create the Vault CA as an organizational unit, include the following additional lines (making sure to leave at least one blank line between the two blocks of lines):

   ```
   dn:ou=OUname, o=IBM, c=US
   userpassword:Secure98
   organizationname:IBM
   organizationalUnit:OUname
   OBJECTCLASS:ORGANIZATIONALUNIT
   OBJECTCLASS:ORGANIZATION
   OBJECTCLASS:ENTRUSTCA
   ```

4. Follow the instructions in Add a Country Directory Entry, beginning with step 2 on page 10, to add the new DN entry to the Directory database.

Add an Organization CA

Use this procedure to create a Directory entry for the first Organization CA. In the default Vault Registry configuration, the first Organization CA's DN is:

o=IBM1, c=US

If you configure additional Organization CAs for Vault Registry, you must repeat this procedure for each CA. Make sure that you define unique LDIF files and DNs for each CA that you configure.

1. Create an LDIF-formatted ASCII file in the `/tmp` directory named **add_ca_ibm1.ldif**.
2. To create the Organization CA at the organization level, as in the default Vault Registry configuration, include the following lines:

   ```
   dn:o=IBM1, c=US
   organizationname:IBM1
   userpassword:Secure98
   OBJECTCLASS:ORGANIZATION
   OBJECTCLASS:ENTRUSTCA
   ```

3. If you want to create the Organization CA as an organizational unit, include the following additional lines (making sure to leave at least one blank line between the two blocks of lines):

   ```
   dn:ou=OUname, o=IBM1, c=US
   userpassword:Secure98
   organizationname:IBM1
   organizationalUnit:OUname
   OBJECTCLASS:ORGANIZATIONALUNIT
   OBJECTCLASS:ORGANIZATION
   OBJECTCLASS:ENTRUSTCA
   ```

4. Follow the instructions in Add a Country Directory Entry, beginning with step 2 on page 10, to add the new DN entry to the Directory database.

Add a Directory Administrator for the Vault CA

Use this procedure to create a Directory entry for the Directory Administrator associated with the Vault CA. In the default Vault Registry configuration, the DN for the Vault CA's DirAdmin entry is:

cn=DirAdmin, o=IBM, c=US

1. Create an LDIF-formatted ASCII file in the /tmp directory named **add_diradmin_ibm.ldif**.
2. If the Vault CA was created at the organization level, include the following lines:

   ```
   dn:cn=DirAdmin, o=IBM, c=US
   cn:DirAdmin
   sn:surname
   userpassword:Secure98
   OBJECTCLASS:ORGANIZATIONALPERSON
   OBJECTCLASS:PERSON
   ```

3. If the Vault CA was created at the organizational unit level, include the following additional lines (making sure to leave at least one blank line between the two blocks of lines):

   ```
   dn:cn=DirAdmin, ou=OUname, o=IBM, c=US
   cn:DirAdmin
   sn:surname
   userpassword:Secure98
   OBJECTCLASS:ORGANIZATIONALPERSON
   OBJECTCLASS:PERSON
   ```

4. Follow the instructions in Add a Country Directory Entry, beginning with step 2 on page 10, to add the new DN entry to the Directory database.

Add a Directory Administrator for an Organization CA

Use this procedure to create a Directory entry for the Directory Administrator associated with the first Organization CA. In the default Vault Registry configuration, the DN for the first Organization CA's DirAdmin entry is:

cn=DirAdmin, o=IBM1, c=US

If you configure additional Organization CAs for Vault Registry, you must repeat this procedure for each unique DirAdmin you want to define (the same DirAdmin can be associated with more than one Organization CA). Make sure that you define unique LDIF files and DNs for each DirAdmin that you configure.

1. Create an LDIF-formatted ASCII file in the /tmp directory named **add_diradmin_ibm1.ldif**.
2. If the Organization CA was created at the organization level, include the following lines:

   ```
   dn:cn=DirAdmin, o=IBM1, c=US
   cn:DirAdmin
   sn:surname
   userpassword:Secure98
   OBJECTCLASS:ORGANIZATIONALPERSON
   OBJECTCLASS:PERSON
   ```

3. If the Organization CA was created at the organizational unit level, include the following additional lines (making sure to leave at least one blank line between the two blocks of lines):

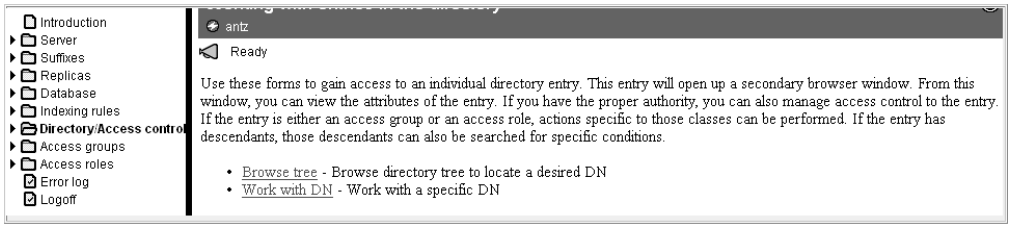
   ```
   dn:cn=DirAdmin, ou=OUname, o=IBM1, c=US
   cn:DirAdmin
   sn:surname
   userpassword:Secure98
   OBJECTCLASS:ORGANIZATIONALPERSON
   OBJECTCLASS:PERSON
   ```

4. Follow the instructions in Add a Country Directory Entry, beginning with step 2 on page 10, to add the new DN entry to the Directory database.

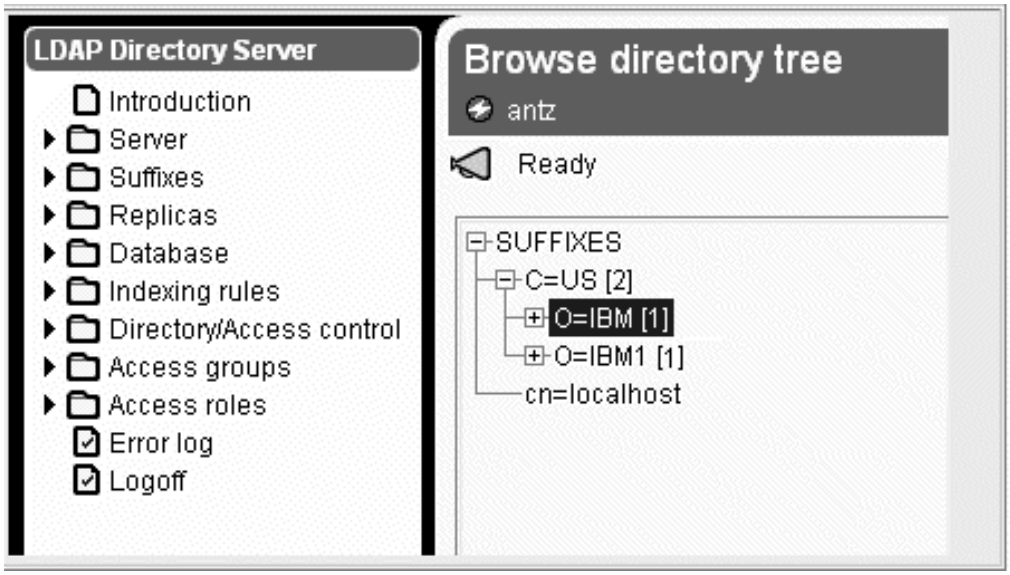
Update the ACL for the Vault CA

Use this procedure to set the appropriate permissions for the Vault CA and its corresponding DirAdmin entry.

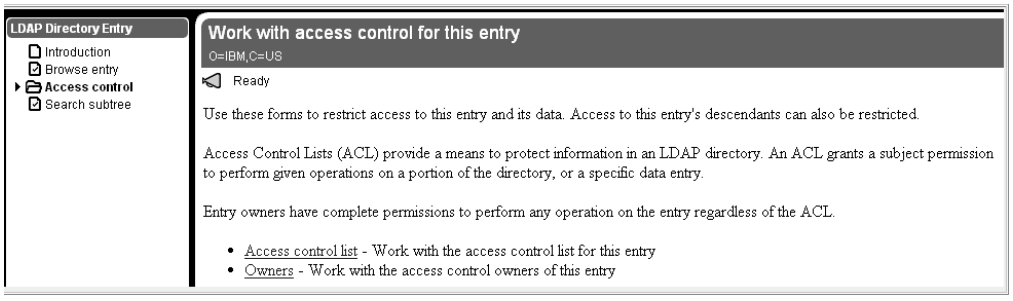
1. If necessary, follow the procedure in “Starting the LDAP Directory Management System” on page 6 and log in as the LDAP administrator.
2. Select **Directory/Access Control** from the LDAP Directory Server menu, and then click on **Browse tree**. For example:



3. Expand the Directory tree and select the entry for the Vault CA. The following example shows the entry used in the default Vault Registry configuration (`o=IBM`).



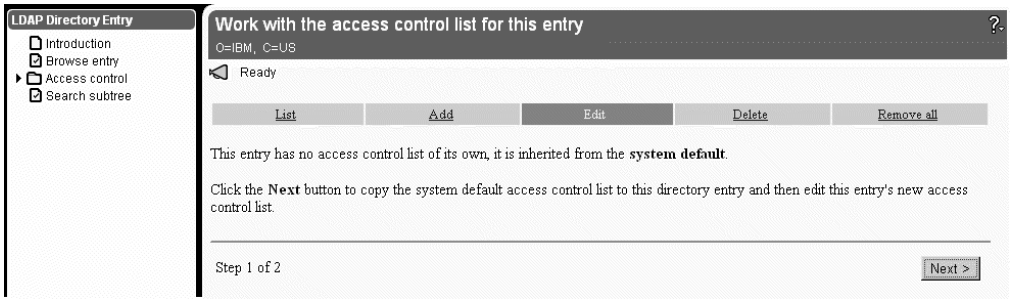
4. Select **Access control** from the LDAP Directory Entry menu, and then click on **Access control list**. For example:



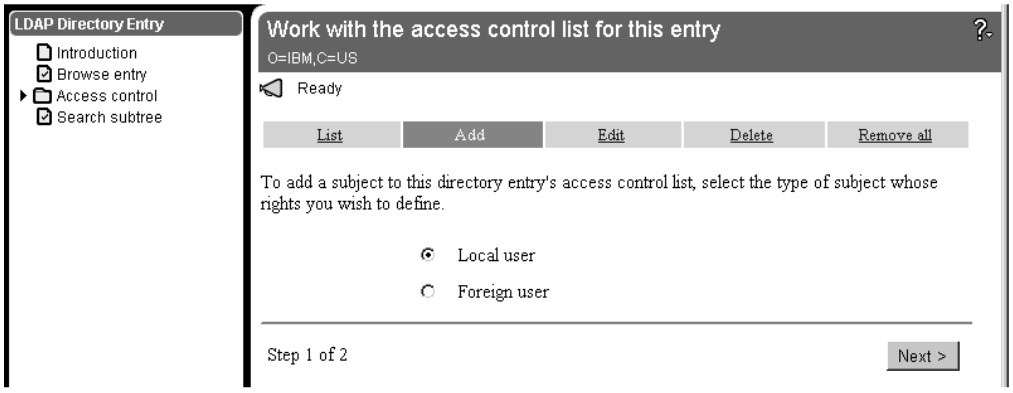
5. Click on **Edit** in the action bar.
6. Using the following figure as a guideline, grant **CN=ANYBODY** the right to **Read**, **Search**, and **Compare** entries in the Directory for only the **Normal** and **Sensitive** classes.

   Note that you must also click in the **Descendent directory entries inherit this access control list** checkbox.

7. Click on the **Apply** button to apply the access control settings.
8. Click on **Add** in the action bar.
9. Make sure your selections match those in the following figure, and then click on **Next**.

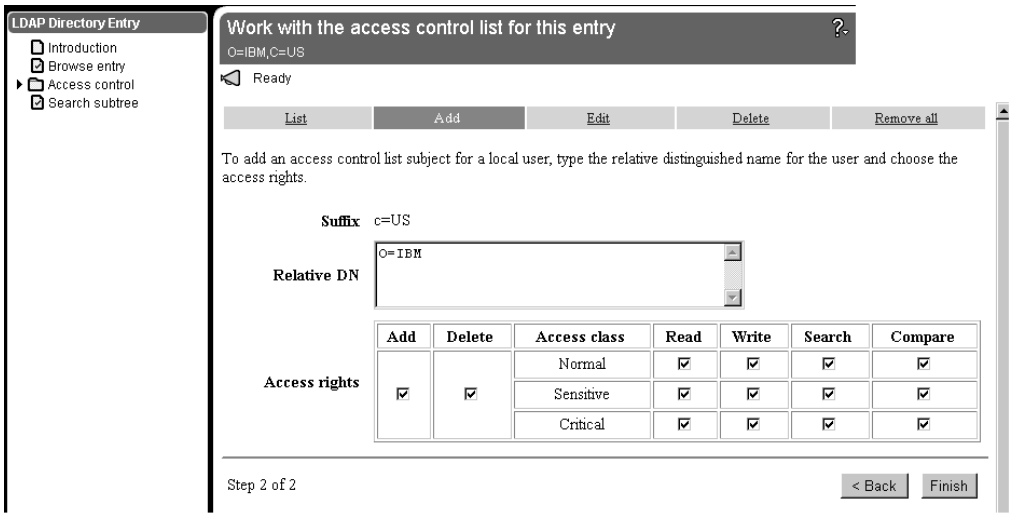


10. Make sure your selections match those in the following figure, and then click on **Next**.



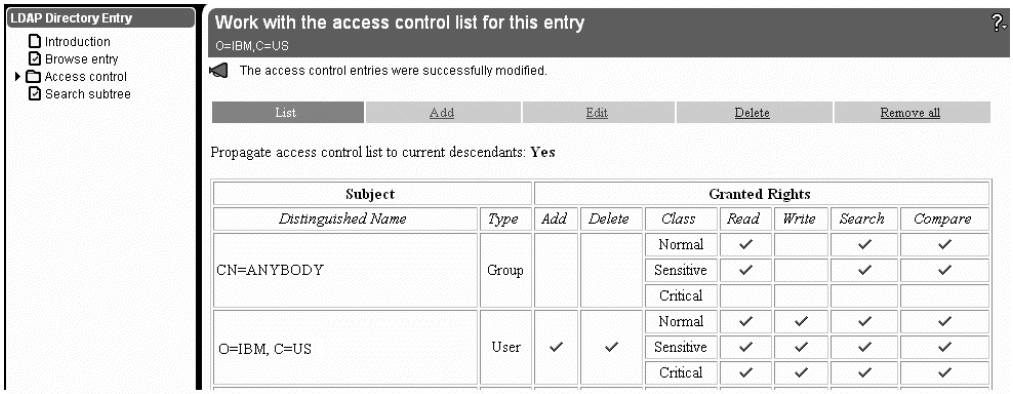
11. Using the following figure as a guideline, type the relative DN for the Vault CA (such as `o=IBM`).

Grant the Vault CA the right to **Add**, **Delete**, **Read**, **Write**, **Search**, and **Compare** entries in the Directory. Make sure that you select all three classes (**Normal**, **Sensitive**, and **Critical**).



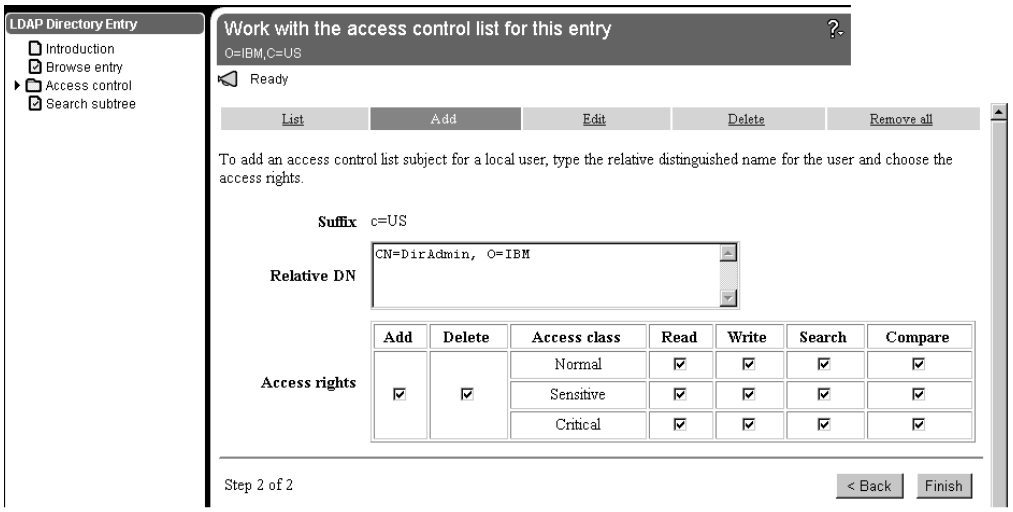
12. Click on the **Finish** button.

    The following figure shows the Vault CA's access control entries as they should appear when the rights have been successfully modified.



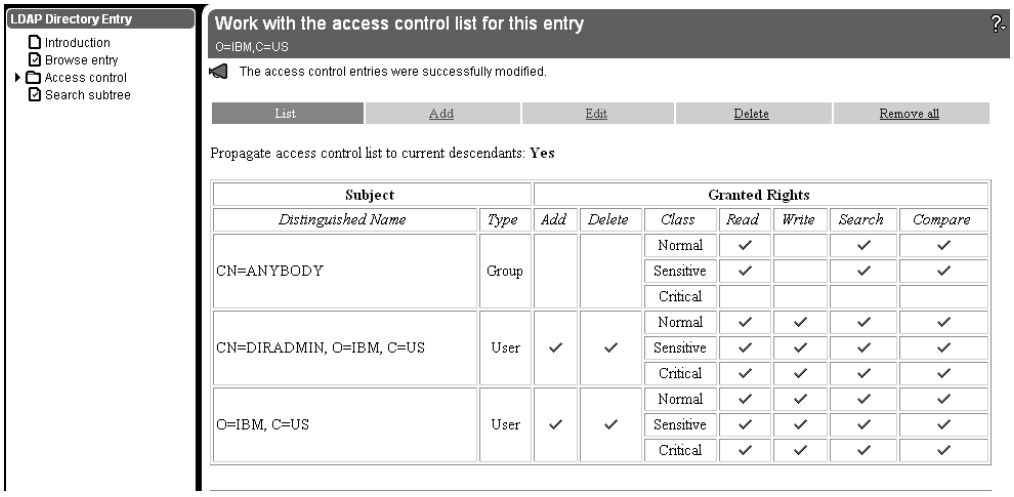
13. Click on **Add** in the action bar again to add access control rights for the Vault CA's Directory Administrator.
14. Using the following figure as a guideline, type the relative DN for the DirAdmin. The entry used in the default Vault Registry configuration is `cn=DirAdmin, o=IBM`.

    Grant the DirAdmin the right to **Add**, **Delete**, **Read**, **Write**, **Search**, and **Compare** entries in the Directory. Make sure that you select all three classes (**Normal**, **Sensitive**, and **Critical**).



15. Click on the **Finish** button again.

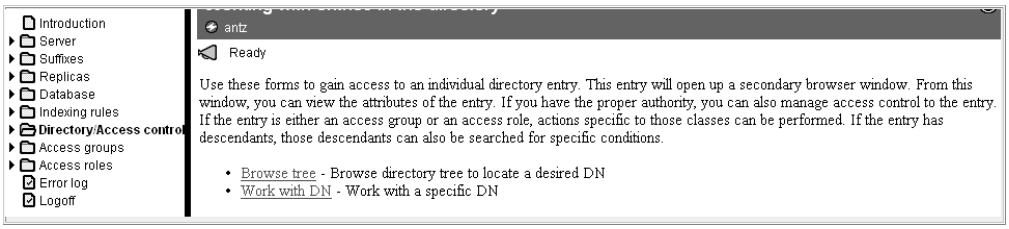
    The following figure shows the Vault CA's DirAdmin access control entries as they should appear when the rights have been successfully modified.



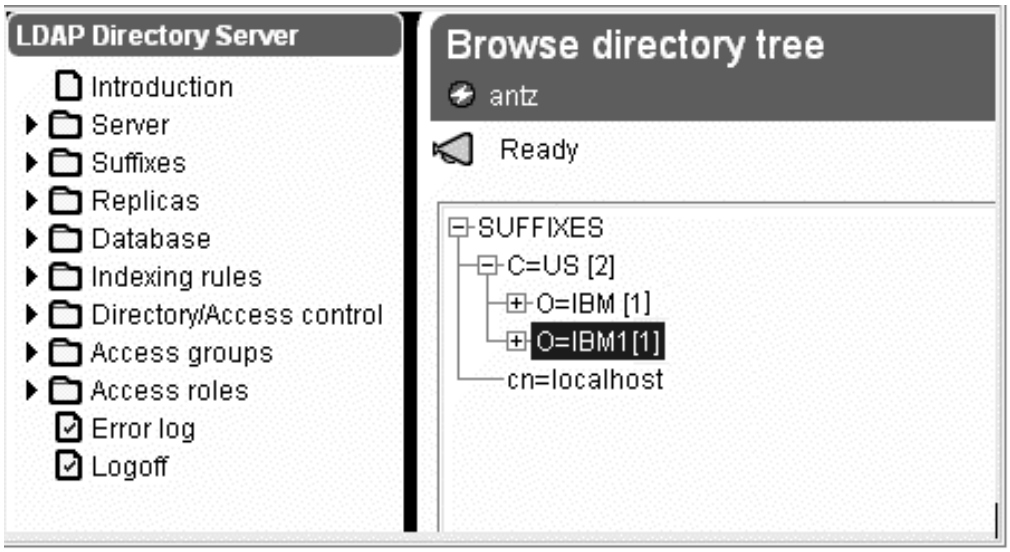
Update the ACL for an Organization CA

Use this procedure to set the appropriate permissions for an Organization CA and its corresponding DirAdmin entry. You must do this procedure for the first Organization CA. If you configure additional Organization CAs for Vault Registry, you must repeat this procedure for each DirAdmin that you configure.

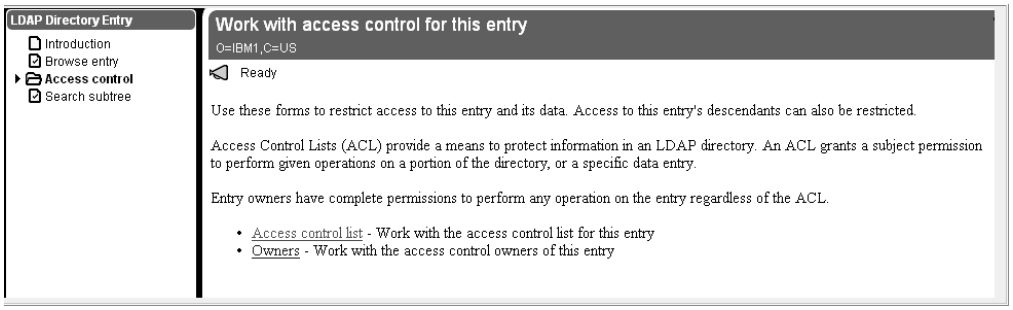
1. If necessary, follow the procedure in "Starting the LDAP Directory Management System" on page 6 and log in as the LDAP administrator.
2. Select **Directory/Access Control** from the LDAP Directory Server menu, and then click on **Browse tree**. For example:



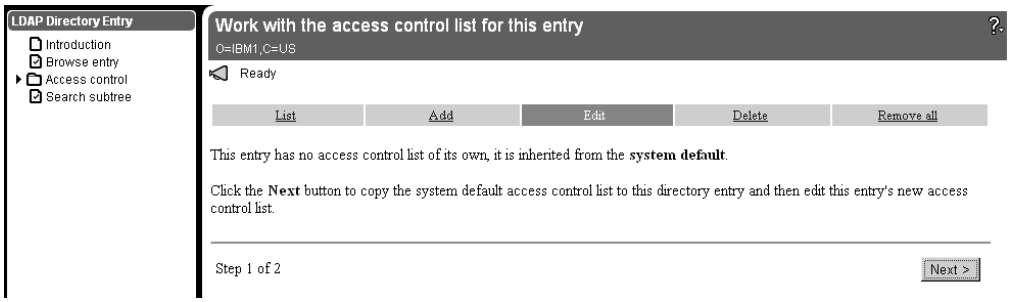
3. Expand the Directory tree and select the entry for the Organization CA. The following example shows the entry used in the default Vault Registry configuration (`o=IBM1`).



4. Select **`Access control`** from the LDAP Directory Entry menu, and then click on **`Access control list`**. For example:

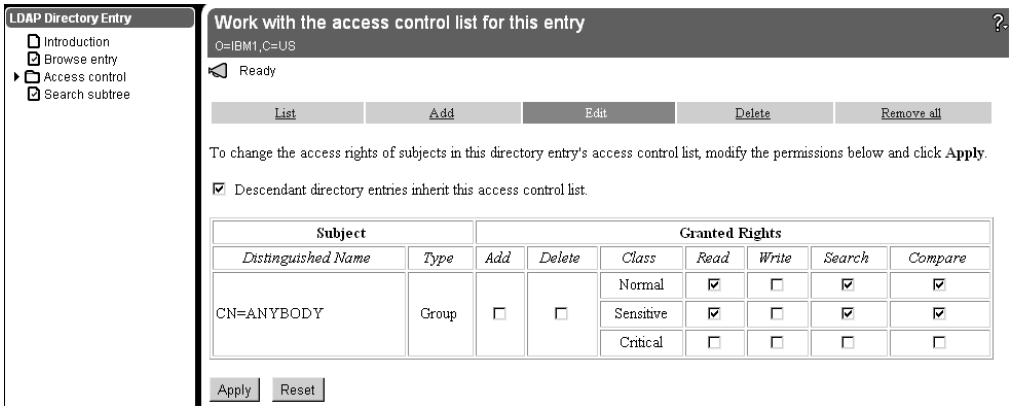


5. Click on **`Edit`** in the action bar, and then click on the **`Next`** button to copy the default access control list to this entry. For example:



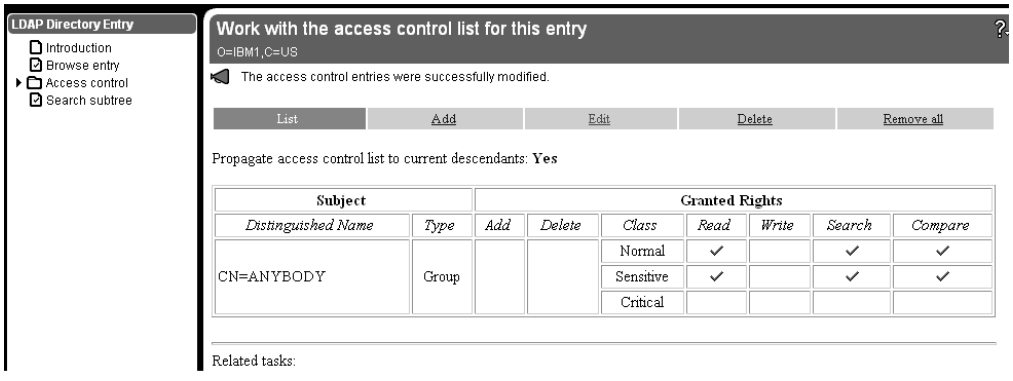
6. Using the following figure as a guideline, grant **CN=ANYBODY** the right to **Read**, **Search**, and **Compare** entries in the Directory for only the **Normal** and **Sensitive** classes.

   Note that you must also click in the **Descendent directory entries inherit this access control list** checkbox.

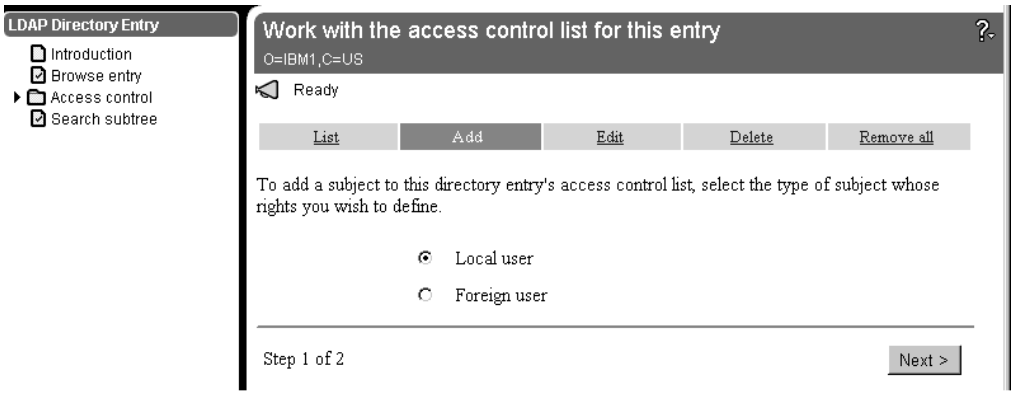


7. Click on the **Apply** button to apply the access control settings.

   The following figure shows the access control entries as they should appear when the rights have been successfully modified.

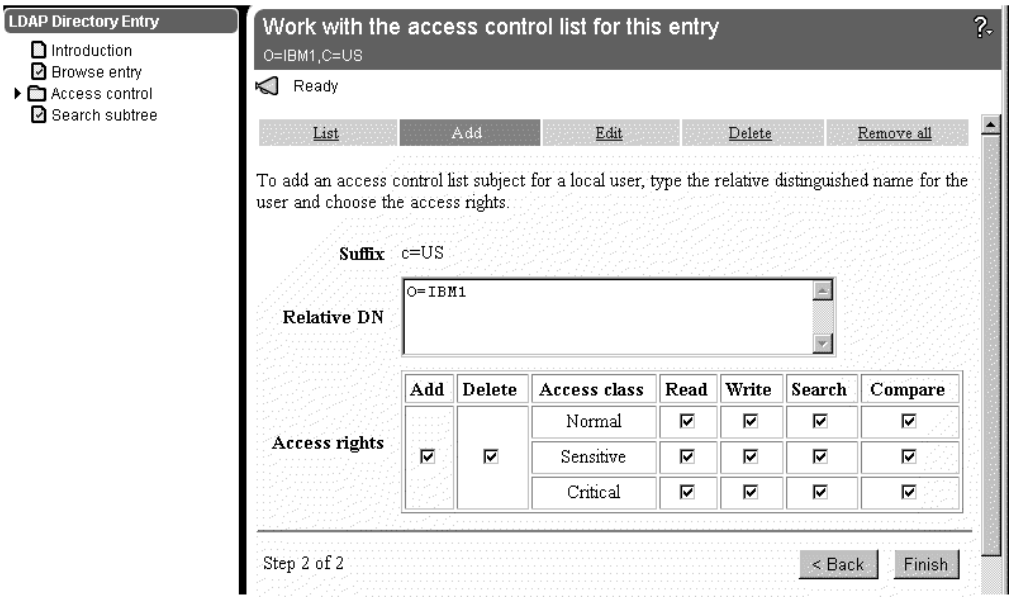


8. Click on **Add** in the action bar.
9. Make sure your selections match those in the following figure, and then click on **Next**.



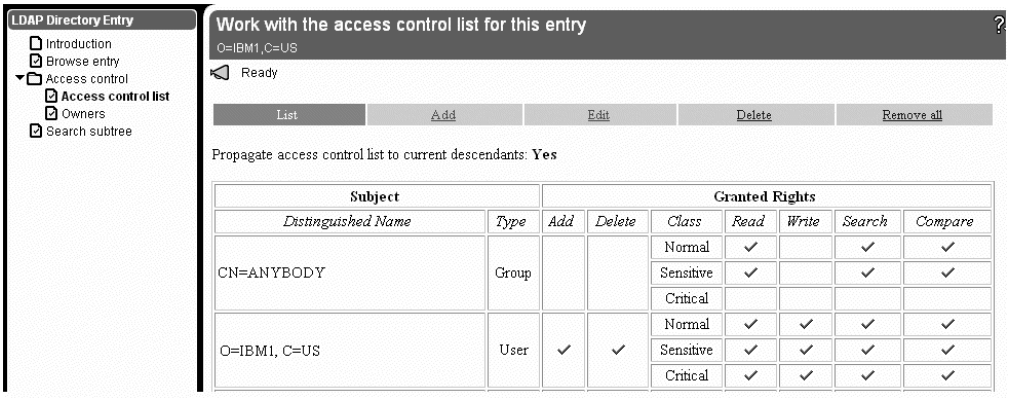
10. Using the following figure as a guideline, type the relative DN for the Organization CA (such as `o=IBM1`).

    Grant this CA the right to **`Add`**, **`Delete`**, **`Read`**, **`Write`**, **`Search`**, and **`Compare`** entries in the Directory. Make sure that you select all three classes (**`Normal`**, **`Sensitive`**, and **`Critical`**).



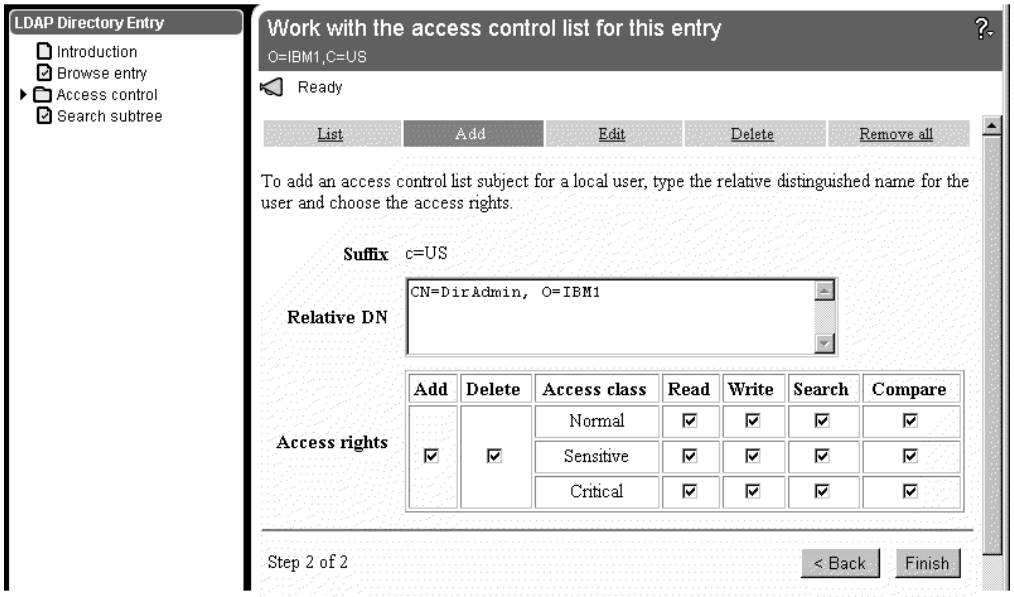
11. Click on the **`Finish`** button.

    The following figure shows the Organization CA's access control entries as they should appear when the rights have been successfully modified.



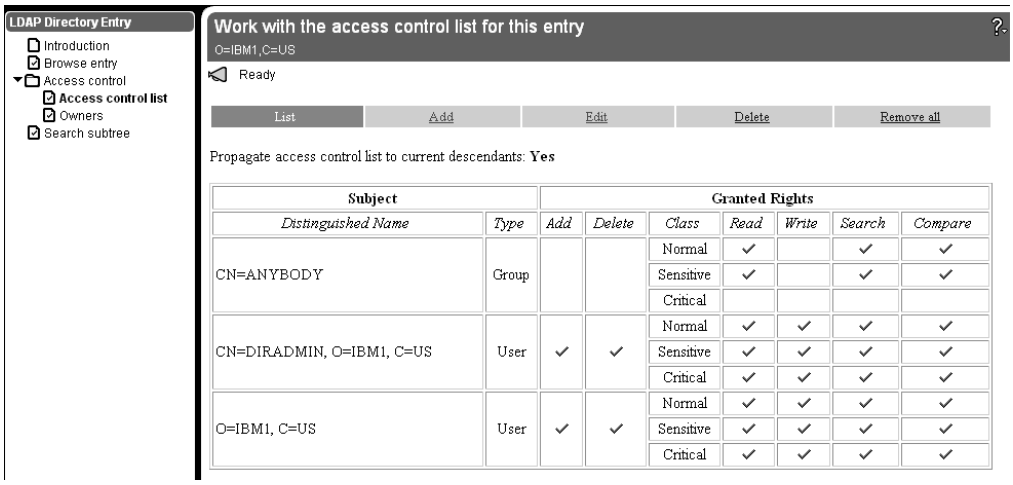
12. Click on **Add** in the action bar again to add access control rights for the Organization CA's Directory Administrator.
13. Using the following figure as a guideline, type the relative DN for the DirAdmin. The entry used in the default Vault Registry configuration is `cn=DirAdmin, o=IBM1`.

    Grant the DirAdmin the right to **Add**, **Delete**, **Read**, **Write**, **Search**, and **Compare** entries in the Directory. Make sure that you select all three classes (**Normal**, **Sensitive**, and **Critical**).



14. Click on the **Finish** button again.

    The following figure shows the Organization CA's DirAdmin access control entries as they should appear when the rights have been successfully modified.



Clean Up AIX Environment Variables

Before you start to configure the Vault Registry system, you must remove LDAP DB2 information from the AIX environment settings. To do so:

1. Examine the `/etc/environment` file.
2. If the following entry exists, remove it:

   `DB2INSTANCE=ldapdb2`

Chapter 3. Monitoring the LDAP Directory

To monitor the Directory, you must set up the `AutoStart` configuration file and run the Directory during configuration time. The following assumptions are that you will:

- Use a single executable to start your Directory.
- Use a single executable to stop your Directory.
- Use a process ID (PID) file to check whether the process is running or not.
- Use standard in (`stdin`) for providing a password.

Use the following procedure to monitor the LDAP Directory server when it is located on either a local or a remote machine. During the pause after the first stage of the Vault Registry configuration process when you receive the message `Please configure the directory (if required) and resume the rest of the configuration`, follow these steps:

1. (Perform this step only if your LDAP Directory is on a remote machine.) Copy the following files to the remote machine from the Vault Registry server machine:

   ```
   /usr/lpp/irg/admin/CLmonitor
   /usr/lpp/irg/admin/CLautoStartConfig
   /usr/lpp/irg/bin/vsSU
   /usr/lpp/irg/bin/monitor
   /usr/lpp/irg/cfg/AutoStart.tpl
   ```

2. Log in as `root`.
3. Change directories by entering this command:

   ```
   cd  /usr/lpp/irg/cfg
   ```

4. Copy the `AutoStart` template file to the `AutoStart` configuration file by entering this command:

   ```
   cp AutoStart.tpl AutoStart.cfg
   ```

5. Change directories by entering this command:

   ```
   cd  /usr/lpp/irg/admin
   ```

6. Set up the `start` command in the `AutoStart` configuration file by entering:

   ```
   /usr/lpp/irg/admin/CLautoStartConfig -a /usr/lpp/irg/cfg/AutoStart.cfg
        -o A -t T -c G -w /bin -e /bin/slapd -u root -f /etc/slapd.pid -i
   ```

7. Set up the `stop` command in the `AutoStart` configuration file by entering:

   ```
   /usr/lpp/irg/admin/CLautoStartConfig -a /usr/lpp/irg/cfg/AutoStart.cfg
        -o A -t P -c G -w /bin -e /bin/slapd -u root -f /etc/slapd.pid -i
   ```

8. (Perform this step only if your LDAP Directory is on a remote machine.) Enter this command:

   ```
   /usr/lpp/irg/admin/CLmonitor -a /usr/lpp/irg/cfg/AutoStart.cfg
        -p defaultpw -o T -t S -u root -e /bin/slapd -l -h
   ```

Note: The *defaultpw* is the Web Server Key Ring password.

Chapter 4. Backing Up and Restoring the LDAP Directory

You can use one of two methods for backing up and restoring the LDAP Directory.

- Using the LDAP Directory Management System

  Use this method if you prefer using a graphical user interface (GUI) and if you plan to back up the entire Directory tree.

- Using AIX line commands

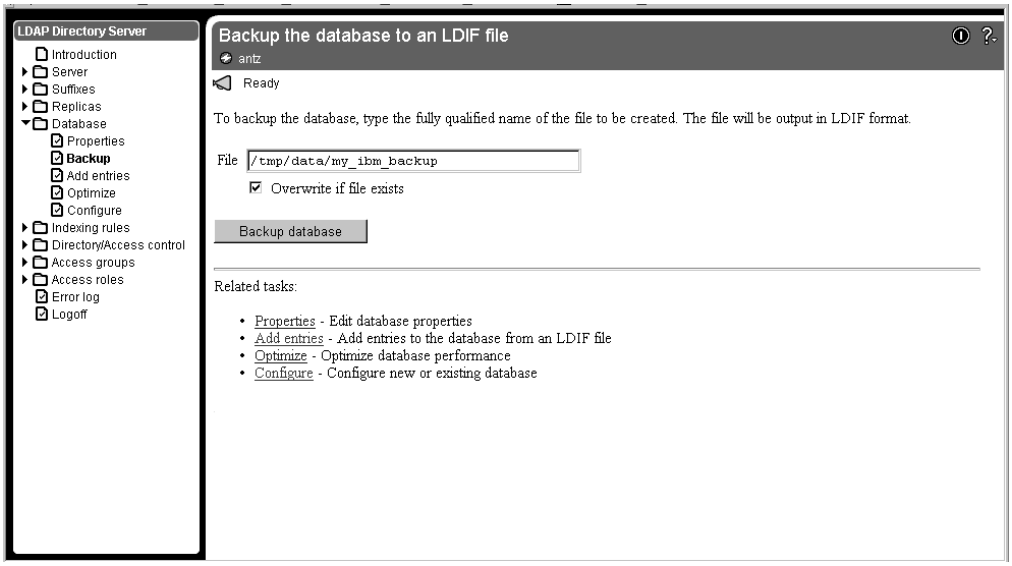
  This manual approach is for the experienced user and it allows you to back up only selected subtrees of the Directory.

Note: Vault Registry has a single point of entry into the Directory cloud (network of Directory servers). If you are using replication, make sure that the Master Directory server and the Directory servers holding the replicas are synchronized before you begin the backup and restore procedures.

Using the LDAP Directory Management System To Back Up the Directory

Follow this procedure to back up the Directory using the LDAP Directory Management System:

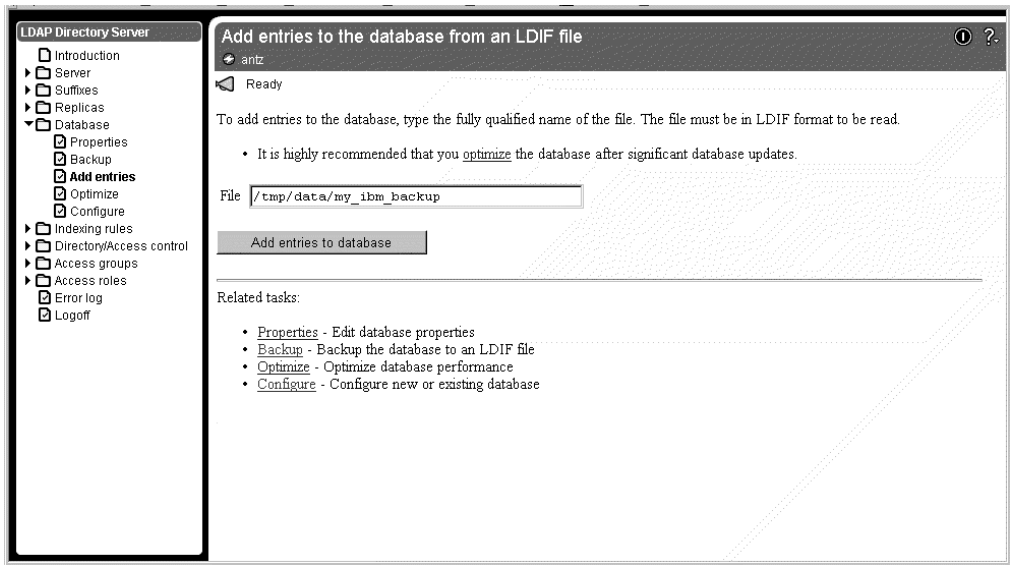
1. If necessary, follow the procedure in “Starting the LDAP Directory Management System” on page 6 and log in as the LDAP administrator.
2. Select **Database** from the LDAP Directory Server menu and then click on **Backup**.
3. In the `File` field, specify the file location to which you are backing up the data and then click on the **Backup database** button. For example:



Using the LDAP Directory Management System To Restore the Directory

Follow this procedure to restore the Directory using the LDAP Directory Management System:

1. If necessary, follow the procedure in “Starting the LDAP Directory Management System” on page 6 and log in as the LDAP administrator.
2. Select **Database** from the LDAP Directory Server menu and then click on **Add entries**.
3. In the `File` field, specify the backup directory filename and click on the **Add entries to database** button. For example:



Note: Be sure to optimize the Directory database periodically or after significant database updates. To optimize the Directory for better performance, click on the **Optimize** link.

Using AIX Line Commands To Back Up the Directory

This section discusses two programs for backing up and restoring the LDAP Directory repositories. They are:

- `db2ldif`
- `ldif2db`

Use the `db2ldif` tool for performing an online backup of the Directory server. This program dumps entries from a Directory stored in a relational database into a text file in LDAP Directory Interchange Format (LDIF). The command syntax for `db2ldif` is:

`db2ldif -o` *`output_file`* `[-s` *`subtree`*`]`

Where:

-o *output_file*
: Specifies the output file to contain the Directory entries in LDIF. All entries from the specified subtree are written in LDIF to the output file. If the file is not in the current directory, you must specify a full path and file name. This option is required.

-s *subtree*
: Specifies the subtree DN identifying the top entry of the subtree that is to be dumped to the LDIF output file. This entry, plus all the entries below it in the Directory hierarchy, are written out. If you do not specify this option, all

Directory entries stored in the database are written to the output file based on the suffixes in the configuration file (/etc/slapd.cnf).

For example, to perform an online backup of the Directory subtree o=IBM, c=US, and write it to the my_ibm_backup output file, enter the following command:

```
db2ldif -o my_ibm_backup -s "o=IBM, c=US"
```

Note: All options are case-sensitive.

Using AIX Line Commands To Restore the Directory

Use the ldif2db program for performing an online restore of the LDAP Directory server. This program loads entries specified in text LDAP Directory Interchange Format (LDIF) into a Directory stored in an existing relational database. You can use ldif2db to add entries to an empty Directory database or to a database that already contains entries. The command syntax for ldif2db is:

```
ldif2db -i input_file
```

Where:

-i *input_file*
Specifies the input file containing the Directory entries in LDIF. If the file is not in the current Directory, a full path and file name must be specified. This option is required.

For example, to perform an online restore of the subtree shown in the previous example, enter the following command:

```
ldif2db -i my_ibm_backup
```

Note: All options are case-sensitive.

Chapter 5. Reinitializing the Directory

In certain cases, for example testing of the system, where the Directory data is no longer valid, you should clean up or reinitialize the Directory. To eliminate invalid data and prepare the Directory for production, you can use one of the following two methods:

- Using the LDAP Directory Management System

  This approach removes everything from the Directory database. Using this method is preferable if you are not absolutely sure which Directory entries to remove and which you can leave.

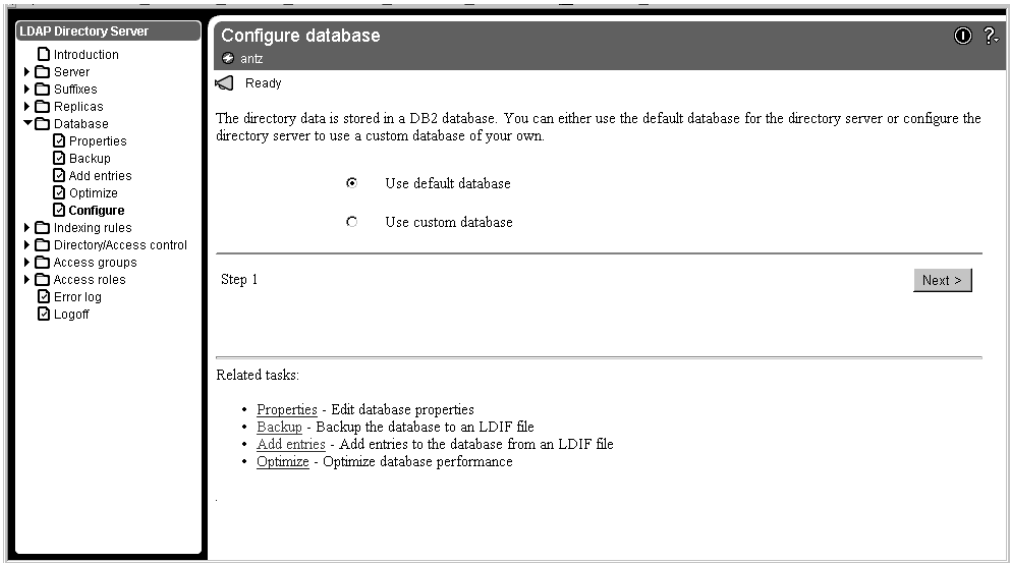
- Using AIX line commands

  This manual approach is for the experienced user and allows you to remove Directory entries selectively.

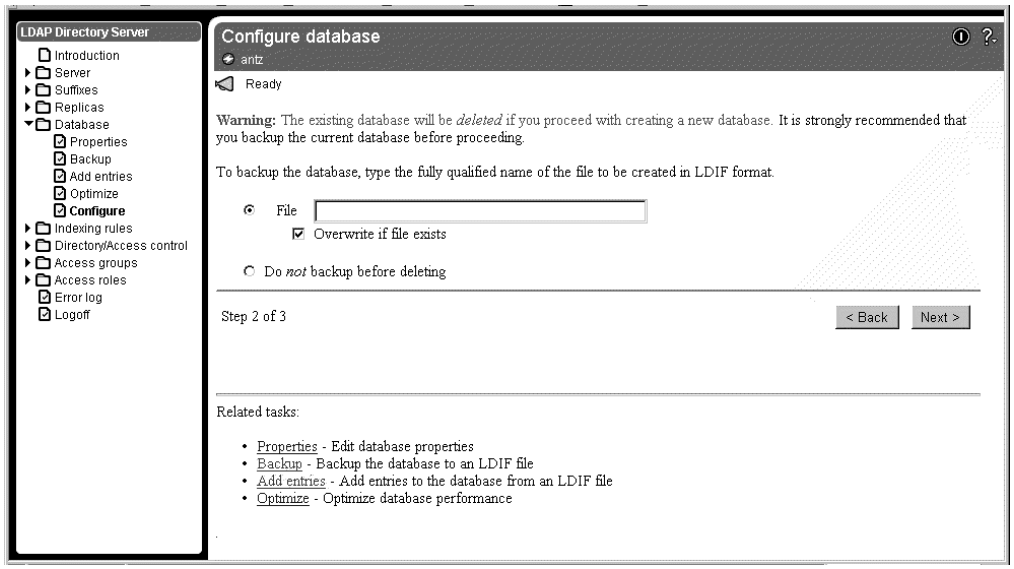
Using the LDAP Directory Management System To Reinitialize the Directory

Follow this procedure to clean up the Directory using the LDAP Directory Management System:

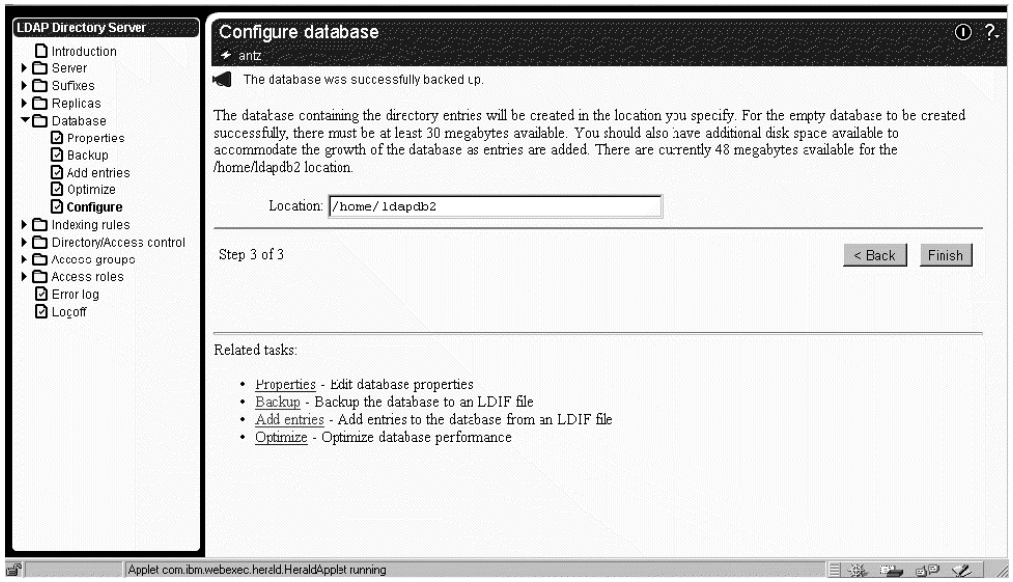
1. If necessary, follow the procedure in “Starting the LDAP Directory Management System” on page 6 and log in as the LDAP administrator.
2. Select **Database** from the LDAP Directory Server menu and then click on **Configure**. For example:



3. Click on **Backup** from the Configure database window to back up data and then select **Next**. For example:



4. Specify the location to which you are backing up the data if it is different from the default directory and then select **Finish**. For example:



5. When you have completed the previous tasks, follow the instructions in “Setting Up Anonymous Access” on page 6 and “Configuring Directory Entries” on page 8 to add the required Directory entries and update the ACL.

Using AIX Line Commands To Reinitialize the Directory

Follow this procedure to clean the Directory of all entries except the required ones specified in “Setting Up Anonymous Access” on page 6 and “Configuring Directory Entries” on page 8 using AIX line commands:

1. In AIX, use `ldapsearch` to locate all entries and save them to a file. For example:

```
ldapsearch -L -b "c=us" "objectClass=*" "cn"> /tmp/data.ldif
```

2. Using an editor such as vi, do the following:
   a. Delete all entries with the exception of the Vault and Organization CAs and their associated DirAdmins that were added in “Setting Up Anonymous Access” on page 6 and “Configuring Directory Entries” on page 8.
   b. Remove the ″dn:″ preceding each entry.
   c. Once the preceding step is completed, use `ldapdelete` to remove these entries from the Directory. For example:

      ```
      ldapdelete -D "cn=root,o=ibm,c=us" -w password -f /tmp/data.ldif
      ```

3. Remove the `cacertificate` and `attributecertificate` entries for both the Vault and the Organization CAs. To do this, follow these steps:
   a. Create four files that specify the DN, the change type and the type of entry to delete. For example:

      ```
      file_1.ldif:
      dn: OU=VR, O=IBM, C=US
      changetype: modify
      delete: cacertificate

      file_2.ldif:
      dn: OU=VR, O=IBM, C=US
      changetype: modify
      delete: attributecertificate

      file_3.ldif:
      dn: OU=VR1, O=IBM1, C=US
      changetype: modify
      delete: cacertificate

      file_4.ldif:
      dn: OU=VR1, O=IBM1, C=US
      changetype: modify
      delete: attributecertificate
      ```

   b. For each of the files listed, enter the following command, where *file_x.ldif* is the name of each file:

      ```
      ldapmodify -D "cn=root,o=ibm,c=us" -w password -f /tmp/file_x.ldif
      ```

For more information about `ldapsearch` and `ldapdelete`, go to the following Web site:

`http://www.umich.edu/~dirsvcs/ldap/`

Program Number: 5648–B28

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.