IBM Vault Registry



# Using the LDAP Directory With IBM Vault Registry

IBM Vault Registry



# Using the LDAP Directory With IBM Vault Registry

# Contents

Chapter 2. Installing and Configuring the LDAP Directory       3         Prerequisites       3         Installing the LDAP Directory Software       3         Preparing the System       3         Preparing the System       4         Modifying the Directory Schema       5         Update Attributes       5         Update Object Classes       5         Starting the LDAP Directory Management System       6         Setting Up Anonymous Access       6         Configuring Directory Entries       8         Add a Country Suffix       9         Add the Vault CA       10         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Prerequisites       3         Installing the LDAP Directory Software       3         Preparing the System       4         Modifying the Directory Schema       5         Update Attributes       5         Update Object Classes       5         Starting the LDAP Directory Management System       6         Setting Up Anonymous Access       6         Configuring Directory Entries       8         Add a Country Suffix       9         Add the Vault CA       10         Add an Organization CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Installing the LDAP Directory Software       3         Preparing the System       4         Modifying the Directory Schema       5         Update Attributes       5         Update Object Classes       5         Starting the LDAP Directory Management System       6         Setting Up Anonymous Access       6         Configuring Directory Entries       8         Add a Country Suffix       9         Add the Vault CA       10         Add an Organization CA       11         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Preparing the System
Modifying the Directory Schema       5         Update Attributes       5         Update Object Classes       5         Starting the LDAP Directory Management System       6         Setting Up Anonymous Access       6         Configuring Directory Entries       8         Add a Country Suffix       9         Add the Vault CA       10         Add an Organization CA       11         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Update Attributes.       5         Update Object Classes       5         Starting the LDAP Directory Management System       6         Setting Up Anonymous Access.       6         Configuring Directory Entries       8         Add a Country Suffix       8         Add a Country Directory Entry       9         Add the Vault CA.       10         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Update Object Classes       5         Starting the LDAP Directory Management System       6         Setting Up Anonymous Access.       6         Configuring Directory Entries       8         Add a Country Suffix       8         Add a Country Directory Entry       9         Add the Vault CA.       10         Add an Organization CA       11         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Starting the LDAP Directory Management System       6         Setting Up Anonymous Access.       6         Configuring Directory Entries       8         Add a Country Suffix       8         Add a Country Directory Entry       9         Add the Vault CA.       10         Add an Organization CA       11         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Setting Up Anonymous Access.       6         Configuring Directory Entries       8         Add a Country Suffix       8         Add a Country Directory Entry       9         Add the Vault CA.       9         Add an Organization CA       10         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Configuring Directory Entries       8         Add a Country Suffix       8         Add a Country Directory Entry       9         Add the Vault CA.       9         Add an Organization CA       10         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Add a Country Suffix       8         Add a Country Directory Entry       9         Add the Vault CA.       10         Add an Organization CA       11         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Add a Country Directory Entry       9         Add the Vault CA.       10         Add an Organization CA       11         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Add the Vault CA.       .
Add an Organization CA       11         Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Add a Directory Administrator for the Vault CA       11         Add a Directory Administrator for an Organization CA       12         Update the ACL for the Vault CA       13
Add a Directory Administrator for an Organization CA
Update the ACL for the Vault CA
Lipdate the ACL for an Organization CA
Clean Lip AIX Environment Variables
Chapter 3. Monitoring the LDAP Directory
Chapter 4. Backing Up and Restoring the LDAP Directory
Using the LDAP Directory Management System To Back Up the Directory 25
Using the LDAP Directory Management System To Restore the Directory 25
Using AIX Line Commands To Back Up the Directory
Using AIX Line Commands To Restore the Directory
Chapter 5. Reinitializing the Directory
Using the LDAP Directory Management System To Reinitialize the Directory 29
Using AIX Line Commands To Reinitialize the Directory

# **Chapter 1. Overview**

In prior releases of IBM<sup>®</sup> Vault Registry, the IBM eNetwork<sup>™</sup> 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, 1dap.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<sup>®</sup> 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<sup>®</sup> Universal Database (UDB) Enterprise Edition for AIX<sup>®</sup> 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 1dapdb2 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 1dapdb2 again.
- Enter the following command to start DB2: db2start
- Enter the following command to create the 1dapdb2 database: db2 create database 1dapdb2
- 7. Use the 1dapcfg 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.

#### 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:

D Introduction	er antz
Server     Suffixes	K Ready
• Replicas           • Database           • Indexing rules           • Directory/Access control           • Access groups           • Access roles           • Error log           • Logoff	Use these forms to gain access to an individual directory entry. This entry will open up a secondary browser window. From this window, you can view the attributes of the entry. If you have the proper authority, you can also manage access control to the entry. If the entry is either an access group or an access role, actions specific to those classes can be performed. If the entry has descendants, those descendants can also be searched for specific conditions. <ul> <li><u>Browse tree</u> - Browse directory tree to locate a desired DN</li> <li><u>Work with DN</u> - Work with a specific DN</li> </ul>

- 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:

LDAP Directory Entry	Work with access control for t
Introduction	cn=localhost
Browse entry     Access control	🖌 Ready
	Use these forms to restrict access to this
	Access Control Lists (ACL) provide a m perform given operations on a portion of
	Entry owners have complete permissions
	<ul> <li><u>Access control list</u> - Work with th</li> <li><u>Owners</u> - Work with the access c</li> </ul>

- 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.

Access control	Keady								
	List	Add		Ed	lit	De	elete	Re	emove all
	Permissions below and c	uck <b>Apply</b> y entries in	y. 1herit th	is access	control list.				
	Descendant directory	uck <b>Apply</b> y entries in	y. 1herit th	is access	control list. Gi	ranted	Rights		
	Descendant directory           Subject           Distinguished Name	y entries in	y. 1herit th <i>Add</i>	is access	control list. Gi <i>Class</i>	ranted I Read	Rights Write	Search	Compare
	permissions below and c         Image: Descendant directory         Subject         Distinguished Name	nck <b>Apply</b> y entries in <i>Type</i>	y. iherit th <i>Add</i>	is access	control list. Gi <i>Class</i> Normal	ranted I Read	Rights Write	Search	Compare
	Permissions below and c Descendant directory Subject Distinguished Name CN=ANYBODY	nck <b>Apply</b> y entries in <i>Type</i> Group	y. nherit th <i>Add</i>	is access	control list. <i>Class</i> Normal Sensitive	ranted I Read	Rights Write	Search V	Compare V

7. Click on the App1y 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"
- "Add a Country Directory Entry" on page 9
- "Add the Vault CA" on page 10
- "Add an Organization CA" on page 11
- "Add a Directory Administrator for the Vault CA" on page 11
- "Add a Directory Administrator for an Organization CA" on page 12
- "Update the ACL for the Vault CA" on page 13
- "Update the ACL for an Organization CA" on page 16

#### 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.
- Select Suffixes from the LDAP Directory Server menu, and then click on Add a suffix. For example:

LDAP Directory Server	Working with server suffixes 0
► Suffixes	K Ready
<ul> <li>Replicas</li> <li>Database</li> </ul>	Use these forms to define and maintain the list of suffixes that this server will support.
Control Provided Field Provided	A suffix is a DN that identifies the top entry in a locally held directory hierarchy. Because of the relative naming scheme used in LDAP, this DN is also the suffix of every other entry within that directory hierarchy. A directory server may have multiple suffixes, each identifying a locally held directory hierarchy.
<ul> <li>☑ Error log</li> <li>☑ Logoff</li> </ul>	<ul> <li><u>List suffixes</u> - List configured suffixes for this server</li> <li><u>Add a suffix</u> - Add a suffix to the configured suffixes for this server</li> <li><u>Delete suffixes</u> - Delete suffixes from those configured for this server</li> </ul>

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

Add a suffix for this server ➔ antz
Kan Ready
To add a new suffix, please type in the suffix distinguished name.
Suffix DN: C=US
Add a new suffix
Related tasks:
<ul> <li><u>List suffixes</u> - List configured suffixes for this server</li> <li><u>Delete suffixes</u> - Delete suffixes from those configured for this server</li> </ul>

The system shows that the suffix was successfully added.

List configured suffixes for ⊛ antz	this server
The suffix was successfully added	You must <u>restart the server</u> for this change to take effect.          Suffixes         C=US         cn=localhost
Related tasks: • <u>Add a suffix</u> - Add a suffix to • <u>Delete suffixes</u> - Delete suffix	the configured suffixes for this server es from those configured for this server

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:

LDAP Directory Server	Working with the backend database 0 ↔ antz	
<ul> <li>C Suffixes</li> </ul>	K Ready	
Replicas     Database     Indexing rules	Use these forms to change the configuration of the backend database for this server and to perform routine maintenance tasks, sur as optimizing, loading and backing up the database.	ch
Directory/Access control     Access groups     Access roles	The LDAP Data Interchange Format (LDIF) is used to represent directory entries in text form. LDIF files provide a convenient means for bulk loading and backing up the database.	
Access roles     Error log     Logoff	<ul> <li><u>Properties</u> - Edit database properties</li> <li><u>Backup</u> - Backup the database to an LDIF file</li> <li><u>Add entries</u> - Add entries to the database from an LDIF file</li> <li><u>Optimize</u> - Optimize database performance</li> <li><u>Configure</u> - Configure new or existing database</li> </ul>	

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.

LDAP Directory Server	Add entries to the database from an LDIF file
<ul> <li>Server</li> <li>Server</li> <li>Suffixes</li> <li>Replicas</li> <li>Database</li> <li>Indexing rules</li> <li>Indexing rules</li> <li>Indexes control</li> <li>Access groups</li> <li>Access roles</li> <li>Error log</li> <li>Logoff</li> </ul>	<ul> <li>Ready</li> <li>To add entries to the database, type the fully qualified name of the file. The file must be in LDIF format to be read.</li> <li>It is highly recommended that you <u>optimize</u> the database after significant database updates.</li> <li>File /tmp/add_country_us.ldif</li> <li>Add entries to database</li> <li>Related tasks:         <ul> <li><u>Properties</u> - Edit database properties</li> <li>Backman - Backman the database to an LDIF file</li> </ul> </li> </ul>
	Optimize - Optimize database performance <u>Configure</u> - Configure new or existing database

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

 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

 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

 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

- 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.

- 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:

<ul> <li>Introduction</li> <li>Server</li> <li>Suffixes</li> <li>Replicas</li> <li>Database</li> <li>Database</li> <li>Database</li> <li>Dindexing rules</li> <li>Bindexing rules</li> <li>Cherry/Access control</li> <li>Access groups</li> <li>Access groups</li> <li>Access roles</li> <li>Browse tree - Browse directory tree to locate a desired DN</li> <li>Work with DN - Work with a specific DN</li> </ul>
---

 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:

LDAP Directory Entry	Work with access control for this entry ₀=iBM,C=US
Access control	K Ready
Search subtree	Use these forms to restrict access to this entry and its data. Access to this entry's descendants can also be restricted.
	Access Control Lists (ACL) provide a means to protect information in an LDAP directory. An ACL grants a subject permission to perform given operations on a portion of the directory, or a specific data entry.
	Entry owners have complete permissions to perform any operation on the entry regardless of the ACL.
	<u>Access control list</u> - Work with the access control list for this entry <u>Owners</u> - Work with the access control owners of this entry

- 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 App1y 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.

LDAP Directory Entry □ Introduction □ Browse entry • □ Access control □ Search subtree	Work with the acco 0=IBM, C=US	ess control list for th	nis entry		?
	List	Add	Edit	Delete	<u>Remove all</u>
	This entry has no access	control list of its own, it is	inherited from the system	n default.	
	Click the <b>Next</b> button to a control list.	copy the system default ac	cess control list to this di	rectory entry and then edit	this entry's new access
	Step 1 of 2				Next >

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

LDAP Directory Entry  Introduction Browse entry Access control	Work with the ac o=IBM,C=US Ready	cess contro	ol list for this e	ntry	?-
Search subtree	List	Add	Edit	<u>Delete</u>	<u>Remove all</u>
	To add a subject to this rights you wish to defin	directory entry e.	r's access control li	st, select the type o	f subject whose
	G	Local user			
	c	Foreign use	r		
	Step 1 of 2				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.

The access control entries were	successfully modif	ied.						
List	Add		<u>Edit</u>		<u>Delete</u>		Res	move all
Subject				0	ranted l	Rights		
Distinguished Mame	Time	Add	Dalata	Class	Poad	Waita	Saarah	Company
Distinguished Name	Type	Add	Delete	Class Normal	Read ✓	Write	Search	Compare V
Distinguished Name	<i>Type</i> Group	Add	Delete	Class Normal Sensitive	Read ✓	Write	Search	Compare ✓
Distinguished Name	<i>Type</i> Group	Add	Delete	Class Normal Sensitive Critical	Read ✓	Write	Search	Compare ✓
Distinguished Name	<i>Type</i> Group	Add	Delete	Class Normal Sensitive Critical Normal	Read           ✓           ✓           ✓	Write	Search	Compare ✓
Distinguished Name CN=ANYBODY O=IBM, C=US	Type Group User	Add	Delete	Class Normal Sensitive Critical Normal Sensitive	Read           ✓           ✓           ✓           ✓           ✓	Write	Search	Compare

- 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).

owse entry cess control	O=IBM,C=US							
arch subtree	List		Add	Edit		<u>Delete</u>		<u>Remove all</u>
	To add an access contro access rights.	ol list subj	ect for a loca	l user, type the relati	ve distingui:	shed name	for the user a	and choose the
	Suffix	c=US						
	Relative DN	CN=Dir	Admin, O=]	BM		A		
		Add	Delete	Access class	Read	Write	Search	Compare
				Normal	V	•	•	<b>v</b>
	Access rights	V	J	Sensitive	•	•	V	•

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.

DAP Directory Entry	Work with the access control O=IBM,C=US	list for thi	s entr	У					
Access control	M The access control entries were succe	essfully modifi	ed.						
	List <u>Add</u>	1		Edit		<u>Delete</u>		Ret	nove all
	Propagate access control list to current o	lescendants:	Yes						
	Subject				c	ranted l	Rights		
	Distinguished Name	Type	Add	Delete	Class	Read	Write	Search	Compare
					Normal	~		~	~
	CN=ANYBODY	Group			Sensitive	~		~	~
					Critical				
					Normal	~	~	~	~
	CN=DIRADMIN, O=IBM, C=US	User	~	~	Sensitive	~	~	~	~
					Critical	~	~	~	~
					Normal	~	~	~	~
	O=IBM, C=US	User	~	~	Sensitive	~	~	~	~
					Critical				

#### 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:

Introduction     Server     Suffixes     Capilicas     Database     Indexing rules     Directory/Access control     Access groups     Access groups     Access of B     Error log     Logoff	<ul> <li>antz</li> <li>Ready</li> <li>Use these forms to gain access to an individual directory entry. This entry will open up a secondary browser window. From this window, you can view the attributes of the entry. If you have the proper authority, you can also manage access control to the entry. If the entry is either an access group or an access role, actions specific to those classes can be performed. If the entry has descendants, those descendants can also be searched for specific conditions.</li> <li><u>Browse tree</u> - Browse directory tree to locate a desired DN</li> <li><u>Work with DN</u> - Work with a specific DN</li> </ul>
--	--

 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:

LDAP Directory Entry	Work with access control for this entry o=IBM1,C=US
<ul> <li>Prowse entry</li> <li>Access control</li> <li>Search subtree</li> </ul>	<ul> <li>Ready</li> <li>Use these forms to restrict access to this entry and its data. Access to this entry's descendants can also be restricted.</li> <li>Access Control Lists (ACL) provide a means to protect information in an LDAP directory. An ACL grants a subject permission to perform given operations on a portion of the directory, or a specific data entry.</li> <li>Entry owners have complete permissions to perform any operation on the entry regardless of the ACL.</li> <li><u>Access control list</u> - Work with the access control list for this entry</li> <li><u>Owners</u> - Work with the access control owners of this entry</li> </ul>

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:

LDAP Directory Entry  Introduction Browse entry CAccess control Search subtree	Work with the acco o=IBM1,C=US Ready	ess control list for th	nis entry		?
	List This entry has no access Click the <b>Next</b> button to a control list.	<u>Add</u> control list of its own, it is copy the system default ac	Edit inherited from the syster cess control list to this dir	Delete n default. rectory entry and then edit t	<u>Remove all</u> his entry's new access
	Step 1 of 2				Next >

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.

LDAP Directory Entry	Work with the access	control lis	t for th	is entry						?
<ul> <li>Browse entry</li> <li>Access control</li> <li>Search subtree</li> </ul>	式 Ready									
	List	Add			lit	D	elete	E	lemove all	
	Descendant directory ent	ries inherit thi	s access	control list.		Granted I	Rights			
	Distinguished Name	Type	Add	Delete	Class	Read	Write	Search	Compare	-
					Normal			ঘ	V	
	CN=ANYBODY	Group			Sensitive			2	V	
					Critical					
	Apply Reset									

7. Click on the **App1y** 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.

ccess control	The access control entries	were success	fully mod	ified.					
earch subtree	List	<u>Add</u>		E	.dit.	D	)elete	E	emove all
	Subject					Granted F	Rights	~ 1	<i></i>
	Distinguished Name	Type	Add	Delete	Class	Read	Write	Sparch	1 2000000
	Distinguished Name	Type	Add	Delete	Class Normal	Read.	Write	Search ✓	⊂ompar ✓
	Distinguished Name	<i>Type</i> Group	Add	Delete	Class Normal Sensitive	Read ✓	Write	Search	⊂ompar ✓

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

LDAP Directory Entry  Introduction Browse entry Access control Description	Work with the O=IBM1,C=US	acce	ess contro	ol list for this	entry		?-
Search subtree	List		Add	Edit	Delete	<u>Remove all</u>	
	To add a subject to rights you wish to d	this dir lefine.	ectory entry	's access control	list, select the type o	of subject whose	
		~	Ecolor abor				
		0	roreign use:	I			
	Step 1 of 2					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).

Introduction   Browse entry   Access control	O=IBM1,C=US <b>≪</b> Ready							
Search subtree	List		Add	Edit		<u>Delete</u>		<u>Remove all</u>
	To add an access o user and choose th	control li e acces c=US	ist subject s rights.	for a local user, 1	type the	relative d	listinguishe	ed name for th
	- Sumr							
	Relative DN	O=IBN	11		<u></u>	<u>- 116 dir</u>		
	Relative DN	O=IBM	11 Delete	Access class	Read	Write	Search	Compare
	Relative DN	O=IBN Add	1 Delete	Access class	Read	Write	Search	Compare
	Relative DN Access rights	O=IBM Add	11 Delete	Access class Normal Sensitive	Read	Write	Search	Compare IZ

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.

Introduction     Browse entry     Access control     Access control list     Owners     Search subtree	0=IBM1,C=US		entry						
	List A	Add ntrol list to current descendants: Y		<u>Edit</u> Yes			<u>Delete</u>		<u>nove all</u>
			1						
	Subject				G	anted l	Rights		
	Subject Distinguished Name	Туре	Add	Delete	G Class	ranted I <i>Read</i>	Rights Write	Search	Compare
	Subject Distinguished Name	Туре	Add	Delete	G Class Normal	Read	Rights Write	Search	Compare ✓
	Subject Distinguished Name CN=ANYBODY	Type	Add	Delete	G Class Normal Sensitive	Read	Rights Write	Search	Compare ✓
	Subject Distinguished Name	<i>Type</i> Group	Add	Delete	G Class Normal Sensitive Critical	Read	Rights Write	Search	Compare ✓
	Subject Distinguished Name CN=ANYBODY	<i>Type</i> Group	Add	Delete	G Class Normal Sensitive Critical Normal	Read	Rights Write	Search	Compare ✓
	Subject Distinguished Name CN=ANYBODY O=IBM1, C=US	Type Group User	Add	Delete	G Class Normal Sensitive Critical Normal Sensitive	Read	Rights Write	Search	Compare

- 12. Click on **Add** in the action bar again to add access control rights for the Organization CA's Directory Administrator.
- 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).

<u>List</u> Fo add an access o Iser and choose th	control 1 e acces	Add ist subject is rights.	<u>Edit</u> for a local user, t	ype the :	<u>Delete</u> relative d	listinguishe	<u>Remove all</u> ed name for the
Suffix Relative DN	C=US	irådmin,	O=IBM1			×	
	Add	Delete	Access class	Read	Write	Search	Compare
			Normal		V	V	
Access rights	V		Sensitive		V	V	
			Critical	9	9	P	
	Fo add an access o iser and choose th Suffix Relative DN Access rights	Fo add an access control l iser and choose the access Suffix c=US Relative DN Access rights	Fo add an access control list subject ser and choose the access rights. Suffix c=US Relative DN Access rights Access rights	Fo add an access control list subject for a local user, t aser and choose the access rights. Suffix c=US Relative DN Access rights Access rights IM IM IM IM IM IM IM IM IM IM	Fo add an access control list subject for a local user, type the sales and choose the access rights. Suffix c=US Relative DN           CN=DirAdmin, O=IBM1           Add         Delete         Access class         Read           Access rights         Image: Critical         Sensitive         Image: Critical         Image: Critical<	Fo add an access control list subject for a local user, type the relative of a ser and choose the access rights.          Suffix       c=US         Relative DN       CN=DirAdmin, O=IBM1         Add       Delete       Access class       Read       Write         Access rights       Image: Compute the sector of the s	Fo add an access control list subject for a local user, type the relative distinguishes ser and choose the access rights. Suffix c=US Relative DN Access rights Add Delete Access class Read Write Search Normal $\overrightarrow{v}$ $\overrightarrow{v}$ Sensitive $\overrightarrow{v}$ $\overrightarrow{v}$ Critical $\overrightarrow{v}$ $\overrightarrow{v}$ $\overrightarrow{v}$

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.

Image: mark with the mark w	Work with the access control list for this entry ○=IBM1,C=∪S										
ntrol Keady control list											
List	<u>Add</u>		Edit		Delete			<u>Remove all</u>			
	Subject				G	anted l	Rights				
Disting	uished Name	Type	Add	Delete	Class	Read	Write	Search	Compar		
					Normal	~		~	~		
CN=ANYBODY		Group			Sensitive	~		~	~		
					Critical						
					Normal	~	~	~	~		
CN=DIRADMIN,	O=IBM1, C=US	User	~	~	Sensitive	~	~	~	~		
					Critical	~	~	~	~		
					Normal	~	~	~	~		
		User	~	~	Sensitive	~	~	~	~		
O=IBM1, C=US		0.001									

# **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.
- If the following entry exists, remove it: DB2INSTANCE=1dapdb2

### **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:

 (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
- (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.
- 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:

LDAP Directory Server	Add entries to the database from an LDIF file	0 ?-
Replicas     Database     Properties     Backup     Add entries     Optimize     Configure	To add entries to the database, type the fully qualified name of the file. The file must be in LDIF format to be read. <ul> <li>It is highly recommended that you <u>optimize</u> the database after significant database updates.</li> </ul> File //tmp/data/my_ibm_backup	
Industry rules     Directory/Access control     Access groups     Access roles     Diror log     Logoff	Add entries to database Related tasks:  • <u>Properties</u> - Edit database properties  • <u>Backup</u> - Backup the database to an LDIF file  • <u>Optimize</u> - Optimize database performance  • <u>Configure</u> - Configure new or existing database	

**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 db21dif 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 db21dif 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 1dif2db 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 1dif2db to add entries to an empty Directory database or to a database that already contains entries. The command syntax for 1dif2db 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:

		_
LDAP Directory Server	Configure database ● antz	) ?.
Carter → Diserver → D	Ready The directory data is stored in a DB2 database. You can either use the default database for the directory server or configure th directory server to use a custom database of your own.	he
Add entries Add entries Optimize Configure	<ul> <li>Use default database</li> <li>Use custom database</li> </ul>	
<ul> <li>Lindexing rules</li> <li>Lindexing rules</li> <li>Control Access groups</li> <li>Access groups</li> <li>Access roles</li> <li>Pirrol rog</li> <li>Logoff</li> </ul>	Step 1 Next >	
	Related tasks:         • Properties         • Backup - Backup the database to an LDIF file         • Add entries - Add entries to the database from an LDIF file         • Optimize         • Optimize	

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

LDAP Directory Server	Configure database	0	?-
Introduction	🗲 antz		
▶ 🔁 Server	A Boody		
▶ 🖸 Suffixes	Neauly		
Replicas	Warning: The existing database will be <i>datated</i> if you proceed with creating a new database. It is strongly recommen	nded that	
Database     Deconstinue	vou backus the current database before proceeding.		
Propenses	······		
Add entries	To backup the database, type the fully qualified name of the file to be created in LDIF format.		
Optimize			
Configure	• File		
Indexing rules	✓ Overwrite if file exists		
Directory/Access control			
Access groups	O Do not backup before deleting		
Error log			<u></u>
	Sten 2 of 3	Nevt >	
	Courter and Courte	NOXE 2	
			_
	Related tasks:		
	<ul> <li><u>Properties</u> - Edit database properties</li> </ul>		
	<ul> <li><u>Backup</u> - Backup the database to an LDIF file</li> </ul>		
	<ul> <li><u>Add entries</u> - Add entries to the database from an LDIF file</li> </ul>		
	<u>Optimize</u> - Optimize database performance		

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:

DAP Directory Server     Introduction     Server     Suffxes     Replicas     Properties     Backup     Add entries     Optimize     Dediffuer	Configure database * antz The database was successfully backed up. The database ontaining the directory entries will be created in the location you specify. For successfully, there must be at least 30 megabytes available. You should also have addition accommodate the growth of the database as entries are added. There are currently 48 me /home/Idapdb2 location.	Or the empty database to be created al disk space available to sgabytes available for the
Configure Confi	Step 3 of 3         Related tasks:         • Properties - Edit database properties         • Backup - Backup the database to an LDIF file         • Add entries - Add entries to the database from an LDIF file         • Ottiming Outpring database and featomene	< Back Finish
Applet com ibm	webexec.herald HeraldApplat running	E 🐝 🖷 🐠 🌮

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 1dapsearch 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 4.1dif:
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.