OpenVMS Enterprise Directory

Release Notes

Revision/Update Information: Version 5.3

This document was prepared using VAX DOCUMENT, Version 3.3-1E.

Contents

1 Before You Start

Note that the product now available as the OpenVMS Enterprise Directory V5.3 was previously available with these names:

Compaq X.500 Directory Service V4.0
Digital X.500 Directory Service V3.1 and earlier

This section documents important information about the Enterprise Directory and about installing and deinstalling the Enterprise Directory software.

1.1 New Functionality in This Release

This kit includes the following new functionality:

- The DSA, DXIM, and applications linked against the supplied XDS library, can now run on systems without DECnet–Plus installed. This has been achieved by three major enhancements:
  - The DSA, DXIM, and applications linked against the supplied XDS library, now contain an implementation of RFC 1006, which specifies a means for providing an ISO Transport Service on top of TCP, thus enabling all communication to be over TCP/IP. For more details see Section 2.1.
  - The hp Administrator of Enterprise Directory has been enhanced so that it can now fully control the DSA, so that NCL commands are no longer required. For more details see the release notes contained in the readme.txt file supplied with the hp Administrator for Enterprise Directory kit.
  - For those customers who have written NCL command procedures to manage the DSA, but who no longer wish to configure DECnet–Plus, a new NCL Emulator has been provided. This NCL Emulator will perform NCL commands to manage the DSA, using exactly the same syntax. For more details see Section 2.2.
- The DSA can now function as a pure LDAP DSA. This has been achieved by removing the need for a presentation address to be set, and instead an LDAP port number can be specified.

- Improvements have been made to the support of the Secure Sockets Layer (see Section 2.6.3). These are:
  - A new DSA Characteristic called PRIVATE KEY PASSPHRASE has been added. This Pass Phrase is used to protect the the DSA's Certificate PEM file and Private Key PEM file. It must be the same as that used to encrypt the Certificate's Private Key when it was created. In the previous release the DSA password had to be used.
  - A new DSA characteristic called LDAP CIPHERSUITES has been added. This attribute allows the Manager to restrict the set of ciphersuites used by the DSA. The syntax and possibilities are specified on the OpenSSL web site at http://www.openssl.org/docs/apps/ciphers.html. If not specified the default used by the SSL implementation will be used.
  - The default SSL protocol type is now SSLv23
  - The SSL negotiations can now use Diffie-Hellman key exchange.
- The schema provided with this version of the Directory Service has been extended to support the storage of OpenVMS authentication information. To take advantage of this, an enhancement to the OpenVMS LOGINOUT procedure is being provided, starting with an Early Adopters' Kit in V7.3-2. For more details see Section 2.3.

1.2 VMS Cluster Support

You can run the Directory Service software on a cluster if you follow these guidelines:

- Run a DSA on only one node in a cluster.

  When installing on a cluster, if you select the Server component, you are asked which node is to be the server node. After installation, configure the DSA on the node where it will run. See *Enterprise Directory for eBusiness — Management* for information about configuring the DSA.
- If the cluster has multiple system disks, you must repeat the installation for each system disk.

  Always specify the same node to be server node.

- You can run applications from any node in the cluster providing the directory information tree files are in a common area.

  You can run the DUA configuration utility on any node in the cluster, but you must specify the node where the DSA runs and not the cluster alias when prompted for the name of the DSA node.

- If you want the DSA to be enabled automatically during cluster startup you must edit the file SYS$STARTUP:DXD$DSA_STARTUP.NCL to remove the comment tags before the NCL ENABLE DSA and NCL CREATE DSA commands.

- Run the startup procedure SYS$STARTUP:DXD$COMMON_STARTUP.COM on all the nodes in the cluster that have directory components installed.

1.3 No Auto Answer Support in Installation

AutoAnswer files can only be used on installations that follow the pattern of previous installations. AutoAnswer files created during a first-time installation (that is, installation on a system that had no Directory previously), are not available during an upgrade. AutoAnswer files created during an upgrade will be available at the time of the next upgrade and any subsequent upgrade.

2 Additional Documentation for Directory Functions

This section deals with new functions added to Enterprise Directory since the last full release of the main documents.

2.1 Running without DECnet–Plus

Prior to this release the Directory Service had a pre-requisite that DECnet–Plus was installed. This restriction has been removed, but for customers who wish to use an OSI Transport, the use of DECnet–Plus is still optionally available.

In order to remove the DECnet–Plus dependency, the DSA and DUAs, now have their own implementation of RFC1006 transport.

Directory User Agent (DUA)

In this section there are references to a DUA, which stands for Directory User Agent. This reference will apply to DXIM and applications linked against the supplied XDS library.

The DSA and DUAs will use their implementation of RFC1006 transport if the DECnet–Plus OSAK library is not available. If the OSAK library is available, then by default the DSA and DUAs will use the OSAK library for transport. This will be the case for the DSA unless the DSA characteristic PROHIBIT DECNET TRANSPORT is set to TRUE. Similarly this will be the case for a DUA unless the logical name DXD$NO_DECNET is defined as TRUE before the DUA is activated.

If DECnet–Plus is installed then there is an issue with the use of standard port numbers. This is described in Section 2.1.1.

2.1.1 Resolving a conflict with Port 102

If you wish to configure an RFC1006 presentation address on a system which has DECnet–Plus installed, then it is recommended that you use the DECnet implementation of RFC1006, which will always use port 102.

If you wish to configure a DSA to have an RFC1006 presentation address on a system which does not have DECnet–Plus installed, then you must use the DSA's and DUAs' private RFC1006 implementation, and it is recommended that in this case you also use port 102 (however, see note 4 below).

If you wish to use the DSA's or a DUA's private RFC1006 implementation on a system which has DECnet–Plus installed, the following section explains why there is a conflict, and how to resolve it.

The RFC1006 specification reserves port 102 for applications using the RFC1006 protocol. The DECnet OSAK library provides CLNS, CONS and RFC1006 transports: its RFC1006 implementation allocates TCP/IP port 102, and then automatically and transparently diverts any incoming requests to the appropriate RFC1006 application (such as the DSA).

Because the DSA's private RFC1006 implementation does not use DECnet, it cannot use port 102 if DECnet–Plus is installed and already using it.

So to use the DSA's private RFC1006 implementation on a system that has DECnet–Plus installed, you need to configure the DSA to listen on a port number other than 102 for incoming RFC1006 connections (and also set the DSA characteristic PROHIBIT DECNET TRANSPORT to TRUE). For example, the RFC1006 address below specifies port 5050:

```
"DSA"/"DSA"/"DSA"/RFC1006+foo.bar.hp.com+5050
```

Note however, that:

1. DECnet–Plus will only ever listen to port 102 for RFC1006 communication. So for a system which has DECnet–Plus installed, a DSA configured with the presentation address shown above and with the DSA characteristic PROHIBIT DECNET TRANSPORT set to FALSE, the port number (5050) will be ignored by DECnet–Plus in favour of port 102. This restriction applies to both OpenVMS and Tru64 UNIX.
2. On OpenVMS, when DECnet–Plus makes outgoing connections to another system using RFC1006 protocol, it always ignores the specified port number and uses port 102. So if you configure a DSA or DUA with the presentation address shown above on a system which does not have DECnet–Plus installed, then it will use port 5050, but no other OpenVMS DSA will be able to communicate with it. This restriction does not apply to Tru64 UNIX.
3. The DSA's and DUAs' implementation of RFC1006 respect the port number specified in presentation addresses for both incoming and outgoing connections.
4. The DSA's implementation of RFC1006 does not have the same arbitration between multiple RFC1006 applications that DECnet–Plus provides. So if you configure the DSA on a system without DECnet to use port 102, this will prevent other applications which also want to use port 102 from being able to run.
5. If an RFC1006 presentation address, that does not have a port number, is set or displayed then the default port number 102 will be used.

2.2 DSA NCL commands

Management of the DSA can now be performed from the hp Administrator for Enterprise Directory program. In previous versions management had to be performed from the Network Control Language (NCL) command line interface, and System Managers may have written command procedures using NCL commands in order to manage the Directory. So that these command procedures may continue to be used on systems where DECnet–Plus is not installed, and hence NCL is not available, version 5.3 of the Enterprise Directory includes an NCL Emulator.

The NCL Emulator accepts commands in exactly the same syntax as NCL, with the restriction that it will only accept NCL commands for the "DSA" entity, that is it can only be used to manage an Enterprise Directory.

To start the NCL Emulator run the program at SYS$SYSTEM:DXD$NCL.EXE.

There are some points to note if the NCL Emulator is used to manage a DSA on another node:

- The NCL Emulator can only be used to manage version V5.3 or later of an Enterprise Directory.

- With the original NCL it was necessary to set up OpenVMS proxies in order to gain the authority to manage a remote DSA running on OpenVMS. These are not required by the NCL Emulator, and instead a new command called AUTHENTICATE is supplied exclusively by the NCL Emulator. The syntax is:

```
AUTHENTICATE NODE <node> DSA [PORT <port>] [PASSWORD <password>]
```

  The AUTHENTICATE directive is used to bind to a remote DSA, in order to issue NCL commands to the remote DSA. An AUTHENTICATE directive must be issued before any remote commands to that DSA are attempted. It remains in force for the duration of the NCL session. The password required is the Management Password required to access the hp Administrator for Enterprise Directory Utility on the remote system. For details on how to set this password see Section 3.3. Note that remote commands require a TCP/IP network to be configured.

2.3 Schema Extensions

New schema objectclasses and attributes have been defined to support hp OpenVMS LDAP SYS$ACM Authentication Agent. This product will be available as an Early Adopters' Kit in OpenVMS V7.3-2, and will enable OpenVMS authentication information to be stored in an LDAP Directory.

In addition the Internet standard inetOrgPerson LDAP Object Class has been added to the schema. This is described in RFC 2798 and is a general purpose object class that holds attributes about people.

2.4 Extended Syntax Support

DXIM will now display passwords as octet strings if they contain non-ISO Latin-1 characters. Octet strings can now be used to enter passwords.

Support has been added for an "approximate match" when comparing attributes that have a syntax of bitstring. An approximate match is true if all the bits set in the assertion are also set in the value, and false if any of the bits set in the assertion are not set in the value.

For example, the following would be considered matches:

'1000'b would match '101100001'b
'111'b would match '1111111'b

The following would not be considered matches:

'1000'b would not match '0100110110'b
'1010'b would not match '1101110'b

Note that bit 0 is the left-most bit.

2.5 Selective Shadowing

This release supports selective shadowing; that is, it is now possible to specify which attributes can and cannot be shadowed to a consumer DSA.

The shadowing filter is controlled by the shadowingAttributeSelection attribute in the shadow agreement subentry. Thus every shadowing agreement has its separate filter. If a shadow agreement subentry does not have the shadowingAttributeSelection attribute then all user attributes are shadowed to the consumer DSA.

The shadowing filter is performed on the supplier DSA. Time stamp and security attributes are always shadowed to the consumer DSA. See X.525 for more information.

The shadowingAttributeSelection attribute is multivalued. Each value is a classAttributeSelection and consists of an object class and either an "include" or "exclude" list of attributes or "all attributes".

The object class in the classAttributeSelection can either be a specific object class or all object classes. In the "exclude" form, attributes not in the exclude list are implicitly included.

A classAttributeSelection is applicable to an entry if allObjectClasses is specified or if the specified object class matches an object class of the entry. If more than one classAttributeSelection filter applies to an entry, an "include" filter takes priority over an "exclude" filter and an "exclude" filter takes priority over "all attributes" and implicitly included attributes. If no

classAttributeSelection is applicable to an entry then only the time stamp and security attributes are shadowed.

The command-line DXIM syntax for the shadowingAttributeSelection value is:

```
<objectclassselection>  ::= "objectClass" "=" <value>   |
                            "allObjectClasses"

<attributefilter>       ::= "include" "=" "{" <attr>, <attr>... "}" |
                            "allAttributes" |
                            "exclude" "=" "{" <attr>, <attr>... "}"

<classAttributeSelection> ::=
                          "[" <objectclassselection> "," <attributefilter> "]"
```

For example:

```
dxim> modify /c=us/o=acme/cn="supplier /c=us/o=acme 3" -
_dxim> add attribute shadowingAttributeSelection = -
_dxim> [objectclass=person, -
_dxim> exclude={description,title,telephone number}]
```

Note

In Section A.1.35 of the V5.0 Management Guide, the attribute shadowingAttributeSelection (together with this new information) replaces shadowingAttributes.

2.6 LDAP Support Enhancements

2.6.1 LDAP Controls

The DSA supports the ManageDSAIT Control, as defined in RFC 3296, to indicate that an operation is intended to manage knowledge information within the DSA Information Tree.

2.6.2 LDAP Extensions

The DSA supports the Start TLS extension to LDAP for use with SSL (Section 2.6.3), as defined in RFC 2830.

2.6.3 Secure Sockets Layer

On OpenVMS the Secure Socket Layer/Transport Layer Security in the Directory relies on the SSL shareables supplied with OpenVMS V7.3-1 or later. These are not installed by default. If they are not installed on a system, the Directory will operate but SSL will not be available. If the shareables are installed after the Directory is installed or started, it is not necessary to reinstall the Directory. You should simply stop and restart the DSA.

The Directory can receive commands over a secure line using LDAPv3 (provided that the client is using the Start_TLS extension). The Directory uses the same LDAP port to receive both secure and unsecured communication.

The Directory supports SSLv23 (the default), SSLv3 and TLSv1 protocols, but only one can be supported at any time. The user can select the protocol by disabling the DSA and setting the protocol using the NCL command:

```
SET DSA LDAP SECURITY PROTOCOL <"SSLv3"/"SSLv23"/"TLSv1">
```

To use this support, you must provide a Certificate file and a Private Key for the DSA. These are stored as (DXD$DIRECTORY:DSA-CERTIFICATE.PEM) and (DXD$DIRECTORY:DSA-PRIVATE-KEY.PEM). The DSA's Pass Phrase must be used as the PEM passphrase. The DSA's Pass Phrase is stored in the DSA Characteristic "PRIVATE KEY PASSPHRASE".

The DSA does not provide a default certificate or private key. For more information on certificates and keys, see http://www.openssl.org.

The Directory can be placed in one of three security states — no security, selectable security or mandatory security. This is chosen by setting the attribute SSL State to OFF, ON, or MANDATORY using the NCL (or NCL Emulator) command "SET DSA SSL State <*state*>", for example SET DSA SSL State ON .

If the SSL State is set to OFF, SSL will not be available. If the SSL State is set to ON, SSL will be available to any LDAP client that can issue an ldap_tls_start request. If the SSL State is set to MANDATORY, LDAP connections will only be accepted from clients that either use anonymous credentials (and therefore have the lowest possible access level), or use SSL to encrypt the connection.

The SSL cipher suites used by the DSA can be specified by setting the characteristic LDAP CIPHERSUITES. If it is not specified then the implementation's default for SSL is used.

3 hp Administrator for Enterprise Directory Management Utility

The hp Administrator for Enterprise Directory GUI has a Utility for controlling certain aspects of the behaviour of a directory server (DSA) over an SSL-secured network connection, that requires TCP/IP. This section deals with the GUI and the Utility.

3.1 Background

For the most part, the hp Administrator for Enterprise Directory GUI communicates directly with the directory server (DSA) that is running in order to manage the DSA. However, there are certain extended management operations (for example, restarting the DSA) which cannot be performed by the DSA itself. In these cases, the GUI communicates with a detached process that runs on the same node as the DSA. This process is the hp Administrator for Enterprise Directory Utility.

3.2 hp Administrator for Enterprise Directory Utility Functions

The GUI communicates with the Utility in order to perform the following operations:

- displaying a list of the available schema files
- creating a new schema file
- editing an existing schema file
- recompiling the schema
- restarting the DSA
- editing the DSA Characteristics

The system manager can decide whether or not the hp Administrator for Enterprise Directory Utility should be enabled on any given server. The GUI only requires that the Utility be available in order to carry out the functions listed above; other administrative operations (such as viewing and updating the contents of the DSA) do not require the Utility to be running.

3.3 Security

As part of the process to configure the hp Administrator for Enterprise Directory Utility, the system manager specifies a management password: this password must be supplied to the Utility by any client attempting to connect to it. This means that users of the GUI do not automatically have the ability to perform extended management operations; they must first supply the Utility's password.

The Utility's password is distinct from any DSA-based password, and should only be disclosed to trusted users.

3.4 Utility Configuration (OpenVMS)

If you install the Utility, a directory will be created beneath DXD$DIRECTORY. This directory will have a name of CAED_NATIVE, and will contain files used by the Utility.

The Utility relies on a configuration file called ADMINISTRATOR.INI which resides in the CAED_NATIVE directory. This file contains an encoded version of the Utility password, as well as information relating to the IP port numbers that it should use.

By default, the GUI expects to use port 389 for LDAP connections to the DSA, and 907 for SSL connections between the GUI and Utility process. You can override these values by editing the configuration file.

To find out what port number is being used for LDAP access to the Enterprise Directory, you can use the NCL utility, for example:

```
ncl> show dsa ldap port

Node 0 DSA
AT 2002-01-01-10:05:02.110+00:00Iinf

Characteristics

    LDAP Port                         = 389
```

If port 907 is already in use by an application on your system, then you will need to choose another port number in the range 1..1023.

3.5 Creating the Configuration File (OpenVMS)

Before starting the Utility for the first time, you need to create this file, which can be done using the command: $ @SYS$STARTUP:DXD$CAED_UTILITY_CONFIGURE

This command procedure will prompt you to provide the password for the Utility, and then create ADMINISTRATOR.INI for you. Initially, the port numbers that will be used are 389 for LDAP connections to the DSA, and 907 for connections between the GUI and the Utility.

Once the command procedure has created the configuration file, it gives you the option of starting the Utility. If you want to change the port numbers that the utility uses, then you can reply NO to this question. In this case, you can edit the configuration file before starting the utility.

3.6 Editing the Configuration File (OpenVMS)

The version of ADMINISTRATOR.INI that is provided the first time you run the configuration command procedure looks like this:

```
[<nodename>]
Ae Title=<nodename>
DSA Entity Name=DSA
Port Number=389
[General]
ServerPort=907
---Do not edit any data below this line---
HashedPassword=<some-value>
```

Where *nodename* will be the name of the server you are using, and *some-value* is a string of digits representing an encoded version of the password that you supplied. Note that the Ae Title field will not necessarily reflect the Ae Title of your DSA. To change either of the port numbers, edit the configuration file and modify the appropriate line(s).

3.7 Changing the Utility Password (OpenVMS)

The Utility's password is stored in the configuration file in an encoded form using a hashing algorithm internal to the daemon. The only way to change this password is to request that the daemon generate a new one, which is what happens when you run the configuration command procedure.

You can run SYS$STARTUP:DXD$CAED_UTILITY_CONFIGURE.COM at any time to change the password (so long as the Utility is not running). When a new password is generated, the other contents of the ADMINISTRATOR.INI file are left unchanged.

3.8 Starting the Utility (OpenVMS)

After running DXD$CAED_UTILITY_CONFIGURE.COM, you have the option of starting the Utility. You can also start the utility using the command $ @sys$startup:dxd$caed_utility_startup

Note that this procedure will fail if you have not created a valid ADMINISTRATOR.INI, or if the Utility is already running.

The file SYS$STARTUP:DXD$COMMON_STARTUP.COM automatically attempts to invoke the Utility startup command procedure if you have installed the Utility on your system. If you do not want the Utility to run on your system then either ensure that no ADMINISTRATOR.INI file exists, or comment out the relevant line from the DXD$COMMON_STARTUP.COM.

3.9 Shutting down the Utility (OpenVMS)

If you wish to shut down the Utility process, use the command $ @sys$startup:dxd$caed_utility_shutdown

The file SYS$STARTUP:DXD$COMMON_SHUTDOWN.COM automatically attempts to invoke the Utility shutdown command procedure if you have installed the Utility on your system.

3.10 Diagnosing problems with the Utility (OpenVMS)

As it runs, the Utility process writes a log file into the CAED_NATIVE directory, called DXD$CAED_UTILITY_STARTUP_OUTPUT.LOG. This log file contains information about requests from any client that attempts to make a connection, as well as messages that may help diagnose problems that occur should the utility fail to start properly.

4 Lightweight Directory Access Protocol

The DSA supports the LDAP V2 and V3 protocols. This allows LDAP clients to access the Directory.

4.1 LDAP String Syntaxes Not Implemented

Enterprise Directory implements both the LDAP protocols (V2 and V3). The following syntaxes are not supported as string syntaxes, but you can use them all as binary syntaxes:

- Teletex Terminal Identifier
- Presentation Address
- Guide (search guide)
- User Certificate
- CA Certificate
- Certificate Revocation List
- Cross Certificate Pair
- Other Mailbox

- Distribution List Submit Permission

4.2 Restrictions on LDAP V3 UTF-8 LDAP Strings

The LDAP V3 implementation only supports UTF-8 characters that can be mapped to T.61 characters.

5 Restrictions in DECnet–Plus

Some restrictions in DECnet–Plus can affect the behaviour of the Enterprise Directory. It is therefore helpful to be aware of DECnet restrictions, as listed in the DECnet–Plus release notes for your system. Particular areas of interest are NCL restrictions and restrictions related to OSI Transport.

The following sections list restrictions in DECnet–Plus that are known to affect the Enterprise Directory. See Section 6 for information about NCL restrictions.

5.1 DSA on OpenVMS Systems Handling of Multiple Bind Requests

On OpenVMS systems, there is a known problem with DECnet which can cause binds to fail if there are already many applications bound to the DSA. The DSA's ability to accept multiple bindings is limited by the BYTLM quota of the DSA account. This quota might be exceeded by a very busy DSA.

If your DSA's binding limit is reached, an additional bind attempt can expose the DECnet problem. All subsequent binds fail, even if the total number of concurrent bindings drops below the limit. To permit the DSA to start receiving more binds, you need to stop and restart the DSA using NCL.

If large numbers of concurrent bindings are likely, you can increase the BYTLM quota specified in the DSA startup procedure DXD$DSA_STARTUP.COM. Amend the /buffer_limit qualifier to increase the quota. Shut down and restart the DSA to use this increased quota. The DSA shutdown procedure is DXD$DSA_SHUTDOWN.COM.

See *Enterprise Directory for eBusiness — Problem Solving* for further information about resource problems.

6 NCL Restrictions

This section describes restrictions on the use of the NCL director to manage the DSA.

6.1 Creating and Deleting the DSA Quickly

If you use the NCL CREATE DSA and DELETE DSA directives repeatedly in quick succession you might see the following error message in response to one of the DELETE DSA directives:

```
No Such Entity Instance exists
```

This occasionally happens even if the preceding CREATE DSA directive appeared to succeed. In fact, the preceding CREATE DSA directive failed, but NCL lost the error response.

Note that this restriction does not apply to the NCL Emulator.

6.2 Restriction on Using Zero Length Passwords

The schema provided with this version of the Directory Service states that the `userPassword` attribute can have a minimum length of zero characters.

However, the NCL commands for the DSA entity and the Accessor entity, which both have Password attributes, do not support zero length passwords. Do not assign a zero length password to a directory entry if you also need to configure the same password in either a DSA or Accessor entity.

6.3 Limited NCL Command Buffer Size

The NCL command input buffer size is 2048 bytes. This limits the number of characters that can be entered in one NCL directive. When you interactively enter a long directive, the NCL command input buffer can overflow, causing the directive to fail.

Note that the NCL Emulator program can accept input commands up to a maximum of 4096 bytes.

6.4 NCL Command Filtering

If you use a filter in an NCL command, the command fails for most of the attributes of the DSA entity. NCL does not fully support filtering for the types of attribute used by the Directory Service.

6.5 Display of DSA Attributes on OpenVMS Systems

The DSA on OpenVMS systems cannot display attributes if you specify a list of different types of attribute. For example, the following NCL directive is mishandled by the DSA because it requests a display of counter attributes and status attributes:

```
NCL> SHOW DSA ALL STATUS, ALL COUNTERS
```

7 DSA Information and Known Problems

7.1 Looping DSA on OpenVMS V7.2-1

If you observe a looping DSA on OpenVMS Alpha 7.2-1 (DSA consuming CPU time with no load), then you need to apply a patch. The patch you need is the OpenVMS patch VMS721_PTHREAD V3.0 or greater.

7.2 Restrictions on Removing Shadowing Agreements

You should remove shadowing agreements in the reverse of the order you used to set them up. That is, the agreement at the end of the shadowing chain should be removed first. If it is not, the DSA will continue to hold shadow naming contexts that are not updated by a shadowing agreement.

For example, if DSA A shadows a naming context to DSA B, which then further shadows the naming context to DSA C, you should remove the last agreement first: remove the consumer access point on DSA B before removing the consumer access point on DSA A.

7.3 Clarification on Updating Shadowing Agreements

The DSA does not update the supplier's agreement shadowingflags relating to the replication strategy when changes are made on the consumer's shadowingFlags. You must change these settings on the supplier.

7.4 Year 2000 Conformance

In Version 3.1, the UTC time matching rules used by the DSA were changed so that dates beyond the year 2000 are recognized by the DSA. Time syntaxes, such as UTC Time, represent the year as a two digit number For example, 10.30am GMT on 5th November 1999 is expressed in UTC Time as 991105103000Z.

With the new time matching rules, a time value with a year that is less than 50 is assumed by the DSA to be after 2000. For example, a time value containing the year 01 is assumed by the DSA to be 2001.

A time value with the year equal to or greater than 50 is assumed by the DSA to be between 1950 and 1999. For example, a time value with the year 99 is assumed by the DSA to be 1999.

7.5 Dereferencing of Search Aliases

There is a known problem with the dereferencing of search aliases.

When a DSA is processing a search, it checks beneath the specified search base for subordinate references that it needs to follow. It is during these checks that the DSA can make an error. The following set of circumstances can cause a DSA to create an incomplete list of subordinate references:

i There are alias entries within the search subtree

ii Those alias entries refer to entries that are held on the same DSA

iii There are subordinate references beneath the entries referred to by the aliases

Those subordinate references are not followed during the search. The search of subtrees beneath aliased entries can therefore be incomplete.

7.6 Memory Exhaustion During Replication Can Cause the DSA to Terminate

If replication fails because of memory exhaustion, the consumer DSA will exit if it is unable to roll back the changes. The DSA exits to avoid corrupting its database. This generates a Resource Exhausted event, with a Reason of Fatal Memory Exhaustion.

Another possible cause for the DSA to run out of memory is as a result of processing many thousands of entry modifications in rapid succession. If the DSA permits volatile modifications, then the last few modifications may be lost. If the DSA does not permit volatile modifications, the last modification may be lost. However, in either case, the vast majority of the modifications are safe. Restarting the DSA increases the virtual memory available to the consumer DSA.

If you need to make a lot of changes to a naming context that is replicated to other DSAs, and you cannot provide more virtual memory, you can use the scheduling attributes of the shadowing agreement to make replication more frequent. For example, you might cause an unscheduled update to occur after a specific number of modifications so that the consumer DSA's memory resources are not overloaded. See *Enterprise Directory for eBusiness — Management* for details of shadowing agreement management.

7.7 DSA Handling of Temporary Files

During normal operation the DSA uses temporary files. When the DSA exits, these temporary files are normally deleted. If the DSA exits abnormally, some temporary files may remain.

If the DSA is not running, you can delete any temporary files that remain. Never delete temporary files while the DSA is still running.

On OpenVMS systems, the temporary files are created in SYS$SCRATCH. The DSA process defines SYS$SCRATCH to be DXD$DIRECTORY by default, and the temporary files have the .TMP file extension.

7.8 Length Constraints on T.61 Strings

When the DSA checks the lengths of T.61 strings, it counts the number of octets in the string rather than the number of characters that those octets represent. Some T.61 characters require more than one octet to represent. This may confuse users who expect the DSA to accept a string of a certain number of characters, but find that the string is rejected.

7.9 Restriction on the Definition of Labels in the Schema

Enterprise Directory for eBusiness — Management states that you can specify schema definitions within your schema text files in any order. However, there is a known exception to this rule. A label can only be specified after the definition for which it provides a label.

7.10 DSA Handling of Referral Loops

DSAs cannot detect referral loops. For example, a DSA can chain to a second DSA and receive a referral to a third DSA. It can then chain to the third DSA and receive a referral back to the second DSA. This type of looping is not covered by the standard loop detection model.

To prevent a DSA from following such referrals indefinitely, the DSA stops after the tenth referral for a given user request, and instead displays the referral to the user.

Looping should not occur if your DSAs are configured correctly.

7.11 Distributed Access Failure Event

If you see the Distributed Access Failure event with the following additional information, then it is possible that the failure was caused by the remote DSA being unable to verify this DSA's password:

```
Reason                 = Communications Failure
Communications Problem = ACSE User Reject. No Reason Specified
```

The remote DSA should have generated an event that indicates a failure to verify this DSA's password. Distributed operations between DSAs will fail if the DSAs are unable to verify each other's passwords. Refer to *Enterprise Directory for eBusiness — Management* for details of replicating information about your DSAs so that they have copies of each other's passwords.

7.12 Database Snapshot Failures

The following three events can mean that the DSA has failed to create a new snapshot file. However, the events do not state explicitly that a snapshot failure has occurred. If you see any of these events without a statement of what operation failed, then you can assume that it was an attempt to create a new snapshot file.

```
Resource Exhausted
Insufficient Disk Space.
```

```
Resource Exhausted
Insufficient Memory.
```

```
Internal Error
Unexpected exception in DbMonitor.
```

7.13 DSA Handling of Presentation Address Protocol Identifiers

If a presentation address specifies that a single network service access point (NSAP) can be used for more than one network protocol, the presentation address is not encoded properly by the DSA when it writes the information to disk. The next time you create the DSA, the presentation address is incorrect.

For example, the following presentation address is specified as having two identical NSAPs, but different protocol identifiers:

```
"DSA"/"DSA"/"DSA"/NS+49002AAA004021,CLNS|NS+49002AAA004021,CONS
```

If you delete the DSA, and then recreate the DSA, and then display the presentation address, it appears as follows:

```
"DSA"/"DSA"/"DSA"/NS+49002AAA004021,CLNS|NS+49002AAA004021,CLNS
```

The CONS protocol identifier has been incorrectly encoded, and is displayed as CLNS.

The same encoding error applies to any presentation address attributes within the database, including those in characteristic attributes of the DSA entity and its subentities, and in any directory entries that contain presentation addresses.

7.14 Displaying Entries that are Part of Your Global Prefix

When you create your DIT, you will probably have a global prefix that connects your organization's DIT to the root of the global DIT. The entries named in the global prefix are not part of your organization's DIT, and may not exist at all, except as placeholders for a future connection to a global DIT.

If you try to display entries that are part of your global prefix, the Directory Service returns an error.

For example, in the example used in *Enterprise Directory for eBusiness — Management*, the Abacus organization has a global prefix that includes the name `/C=US`. The entry called `/C=US` does not exist, so if you try to display it, you get an error.

This problem also affects browsing the DIT using the DXIM Browse window; entries that are part of the global prefix cannot be displayed. *Enterprise Directory for eBusiness — Management* gives details of the global prefix. The immediate subordinates of the browse base must be real entries, not part of the global prefix.

8 DXIM Problems

The information in the following sections applies to both the command line interface and the Motif interface to DXIM.

8.1 Handling of Attributes that Have No Matching Rules

If you modify the schema to define an attribute that has no equality matching rule, directory applications, including DXIM, will have difficulty managing that attribute.

This is because the DSA cannot tell whether the value you specify is already present in an entry. Therefore, if you try to add a value to the attribute, the DSA cannot detect value duplications, and if you try to remove a value, the DSA cannot determine whether the value actually exists. This is particularly true of the DXIM Motif interface, which attempts to add and remove values whenever you edit a value input box on the Modify window.

Refer to *Enterprise Directory for eBusiness — Management* for advice about selecting matching rules for attributes.

8.2 Syntaxes Supported by the Directory Service

HP DSAs support the syntaxes and matching rules documented in *Enterprise Directory for eBusiness — Management* and the DXIM online help.

This section details known restrictions with some of the documented syntaxes and matching rules.

- The following syntaxes are supported by the DSA, but are not supported by the DXIM Motif interface:
  - ACIitem
  - Integer

    Although this syntax is supported, the interface cannot handle the specification of values greater than $2**31 - 1$
- The following syntaxes are supported by the DSA, but are not fully supported by either DXIM interface:
  - Teletex Terminal Identifier

    Teletex Nonbasic parameters are not supported
  - Facsimile Telephone Number

    G3 Facsimile Nonbasic parameters are not supported

Neither DXIM nor the DSA supports Search Guide syntax.

8.3 DXIM Command Line Interface Problems

The following section describes problems and restrictions in the command line interface version of DXIM. If you create any DXIM scripts, you are recommended to keep them, to help diagnose any problems.

8.3.1 Ambiguous Keyword

The keyword BINDING has two meanings in DXIM: it is used in the SHOW BINDING command and to indicate the Binding service control. This ambiguity means that you may see misleading error messages if you specify an incomplete or incorrect command that includes the keyword BINDING. See the DXIM online help information about the SHOW BINDING command and the Binding service control.

8.4 DXIM Motif Interface Restrictions

8.4.1 Problem Deleting Multiple Entries

If you select a large number of entries, and then select the Delete Entry option, DXIM displays a confirmation window, asking you whether you really want to delete the selected entries.

If you select too many entries, the buttons of the window are not visible on your screen. Press RETURN to cancel the operation. Select fewer entries for deletion, so that the window is small enough to fit on the screen.

8.4.2 Handling of User Passwords

The DXIM Motif interface does not support creation or modification of password attributes, even if they are added to the window definition.

8.4.3 Handling of Search Filters

A DXIM Motif interface user can use the Find window to specify details of entries to search for. If the user specifies a detail that is inappropriate for a given filter field, DXIM ignores that detail. For example, if a user specifies an alphabetic string for a field that requires integer values, DXIM ignores that particular field. Only fields that contain appropriate details are processed.

In most cases, this is the user-friendly way to process user input. However, the effect might be that DXIM returns more entries than the user expects to see, including entries that the user thought would be excluded.

8.4.4 Support of the undefinedSyntax

Attribute values that are of `undefinedSyntax` might be displayed in verbatim format, for example:

```
'14 01 c4'v
```

DXIM uses this format if it cannot convert the value into a user-friendly external representation.

DXIM only accepts the verbatim format on input of such values. You need to know how to represent the value in verbatim format. Where possible, do not use the `undefinedSyntax` for attributes.

8.4.5 Online Help

The online help for the DXIM Motif interface does not support the search for keywords option of the Help widget. If you select Search Keywords... from the Help window, DXIM displays an internal error.

8.4.6 Display of the Base Object

The DXIM Browse and Find windows allow you to show the attributes of an entry by selecting the entry and double clicking on it, or by selecting the Show Attributes option from the View menu.

To see the attributes of an entry you have modified, you must collapse and expand the parent entry of the modified entry.

However, this does not work with the base object of the Browse or Find window. The base object is the entry that is displayed at the top of the window, and appears when you invoke the window. Whenever you use the Show Attributes option on that entry, you see the attributes and values that were in the entry when you invoked the window. To see the attributes of this object you must invoke a new Browse or Find window.

8.4.7 Deleting Entries

When you use the DXIM Motif interface to delete an entry, you have to click on Yes to execute the deletion. If you double click on Yes, the deletion succeeds, but DXIM reports an internal error. You must then exit DXIM.

8.4.8 No Support for Auxiliary Object Classes

The DXIM Motif interface does not support auxiliary object classes.

8.4.9 Incorrect Integer Values Not Detected

If you specify a hyphen in an integer value when adding a value to an attribute or creating an attribute, DXIM does not return an error. For example if you try to add the value 1-2-3 to an attribute with integer syntax, no error is displayed. When you subsequently display that attribute, the value displayed is 1.

8.4.10 Usability Problems

The DXIM Motif interface is known to have some usability problems.

- The positioning of new input boxes is faulty.

  If you use the Add Value option, a new input box might be placed partially or completely off the window. To workaround this problem, only add one or two values to an attribute at a time. Click on OK. If you want to add more values, select the Modify Entry option again, and you will be able to display one or two more new input boxes. By this method you can gradually add more values.

- Any modifications made to the Directory using the Create or Modify windows are not automatically reflected in the Browse and Find windows. For example, if you change the name of an entry, the Browse window still displays the old name. Similarly, if you create an entry, DXIM does not display the entry in the Browse window.

If the information in the Browse and Find windows is out of date, use the collapse and expand options to refresh the window.

•

8.5 Application Resources

The DXIM Motif interface does not currently provide an application resource file to define, for example, the colours to use in DXIM windows. You can edit your default resource file to include information that controls the DXIM display. On an OpenVMS system edit the appropriate file in your SYS$LOGIN directory and use the resource name `dxd_mainwin`.

For example, to set the foreground colour to red, edit the appropriate file and add the following line:

```
dxd_mainwin*Foreground: #ffff00000000
```

9 Problems with the Lookup Client

9.1 Lookup Client GUI Help Requires Bookreader

The graphical interface of the Lookup Client requires the Bookreader software. If Bookreader is not installed on the Lookup Client system, then attempts to read the online help will have no effect.

9.2 Lookup Client Display of Modified Entries

Attribute values displayed in Lookup Client displays cannot be guaranteed to have come from master DSAs. This is particularly important when you use the Alter window of the Motif interface. The values displayed in the Alter window may have come from a shadow DSA. After changing an entry, the changes you make might not be visible in the Lookup Client.

This is because the Lookup Client uses a protocol that does not enable applications to specify that master information is required. The only workaround is to make sure that the Lookup Client is connected to the master DSA for the entry you want to change.

10 XDS Problems and Information

10.1 Documentation of Maximum Outstanding Operations Constant

The Directory Service programming documentation states that the value of the DS_MAX_OUTSTANDING_OPERATIONS constant is defined by the DSA implementation. In fact, the value is defined by the XDS API implementation. HP's XDS API defines the constant to be 32. If 32 asynchronous operations are outstanding, XDS will not accept more asynchronous operations.

If you are writing an application that will use another vendor's XDS API implementation, then the constant may have a different value. It may therefore be advisable not to define this constant in your application, because it cannot be set to both values. Instead, your application can detect the Library Error: Too Many Operations if and when the XDS API returns it. If this error is returned, you can use the Receive Result function to reduce the number of outstanding operations.

10.2 Documentation of the Search and Read Functions

Note that the programming documentation is unchanged for this release of Enterprise Directory. *DEC X.500 Directory Service Programming Reference* documents the functions of the XDS API. The discussions of the Search and Read functions, ds_search and ds_read, does not explain how to select the particular attributes that you want returned from the entry or entries to which the function applies. They only explain that you can use the Select-No-Attributes, Select-All-Types, and Select-All-Types-And-Values constants.

If you want to select specific attributes to be returned from these functions, use the Entry Information Selection class. This class is documented in Section 3.12 of *DEC X.500 Directory Service Programming Reference*.

10.3 XDS Example Programs

The API component of the Enterprise Directory includes a set of callable routines that illustrates how to use the XDS and OM routines. You can also use these routines, which are known as the XDSHLI routines, in your application. The set of routines also includes a simple search application, written using the XDSHLI routines. The file SYS$EXAMPLES:[DXD]XDSHLI.H contains details of the XDSHLI routines and related files.

10.4 Primitive Syntax Attributes in Uninitialized Objects

The sequence OM_CREATE with the initialize argument set to FALSE, followed by OM_PUT using INSERT_AT_END, will return the error WRONG_VALUE_NUMBER, for any single valued primitive attributes. To avoid this, use REPLACE_ALL in OM_PUT.

10.5 XDS is not Thread-safe in a Multithreading Environment

If you are using multithreading, you must lock calls to XDS. This version of XDS does not handle threads correctly in all cases.

10.6 XDS Does Not Support Calls at AST-Level on OpenVMS Systems

If you call XDS routines at AST-level, XDS may behave unpredictably.

10.7 No Support for Boolean Attribute Values

XDS does not support attribute values of Boolean syntax. Such values always appear to be FALSE.

10.8 Incorrect Initial Value for Information Type

The initial value for the Information Type attribute of the Entry Information Selection object should be types-and-values, as stated in the documentation and defined in the standard. However, XDS sets the initial value to types-only.

10.9 Primitive Values Incorrect in a Referral

A restriction in this version of XDS and XOM means that primitive values in Referrals always appear to be present. A value that should be absent has a value of 0.