

Tru64 UNIX Best Practice

Configuring a System to Use LDAP for User Authentication Using Internet Express

November 2002

Product Version: Internet Express Version 6.0

This Best Practice describes how to use the Internet Express Administration utility to set up and configure a system running the HP Tru64 UNIX Operating System to use LDAP for user authentication.

**Hewlett-Packard Company
Palo Alto, California**

Contents

Configuring a System to Use LDAP for User Authentication Using Internet Express

Is This Best Practice Right for You?	1
Introduction to LDAP for System Authentication	1
Before You Begin	2
Applying the Best Practice	2
Obtain the Internet Express Kit	3
Install the LDAP Module for System Authentication	3
Configure the LDAP Module for System Authentication ..	4
Import User Data into the LDAP Database	4
Configure Caching Parameters	5
Verifying Success	6
Troubleshooting	6
Comments and Questions	7
Legal Notice	7

Configuring a System to Use LDAP for User Authentication Using Internet Express

This Best Practice describes how to use the Internet Express Administration utility to set up and configure a system running the HP Tru64 UNIX Operating System to use LDAP for user authentication.

See the Tru64 UNIX Best Practices Web page (http://www.tru64unix.compaq.com/docs/best_practices/) for more information about Best Practices documentation.

Is This Best Practice Right for You?

Not all Best Practices apply to all configurations, so you must be sure that it is appropriate for your system and circumstances. To use this Best Practice, you must meet the requirements described in the following table:

Requirement	Description
Operating System	Tru64 UNIX Version 5.0A or higher
Product Version	Internet Express Version 6.0 or higher
Directory Server	OpenLDAP Version 2.0.7 or higher or equivalent directory server. Note that the directory server does not need to be running on the local system.

Introduction to LDAP for System Authentication

The Lightweight Directory Access Protocol (LDAP) is an Internet standard directory service protocol that runs over TCP/IP. An LDAP server manages entries in a directory and makes the information available to users and applications across the network. The server can be used as a central repository of user information to identify and authenticate individuals.

An LDAP server offers the following advantages:

- An LDAP directory can be scaled to handle thousands of users.

- An LDAP directory database can be used as a central management repository of user information to identify and authenticate users.
- You can set up multiple LDAP servers to make the data in the directory highly available. You can ensure that all LDAP servers have identical copies of the directory by replicating the directory.

Internet Express provides a loadable authentication mechanism through the LDAP Module for System Authentication. When you install and enable the LDAP Module for System Authentication, all user and group authentication takes place through the LDAP server without any changes to existing application source code, providing transparent authentication for login (`rlogin`, `ftp`, `telnet`), mail (POP and IMAP), and other applications that identify or authenticate users using standard UNIX library calls.

Before You Begin

Before you apply the Best Practice for Setting Up and Configuring LDAP for User Authentication, you must understand some background information and perform some preliminary tasks.

Internet Express is a collection of popular Open Source and HP software contained on CD-ROM. Using Internet Express, you can install the LDAP Module for System Authentication on your Tru64 UNIX system. You can use the Administration utility provided with Internet Express to modify the default LDAP configuration values.

Before you can set up the LDAP Module for System Authentication, you must have one or more directory servers installed. The Internet Express kit includes the OpenLDAP Directory Server. The OpenLDAP Directory Server is configured for use with the LDAP Module for System Authentication.

For high availability, you should run directory servers on more than one system, and configure each to automatically replicate entries to the other. These directory servers must be configured with the same root distinguished name and password and with the same search base.

Applying the Best Practice

Before you set up and configure your system to use LDAP for user authentication, be sure to follow the recommendations in *Before You Begin*.

The Internet Express CD-ROM labeled "Installation and Documentation" contains the LDAP Module for System Authentication, OpenLDAP, and

directory servers, as well as other Internet software. To configure your system to use LDAP for user authentication, you should:

1. Obtain a copy of the Internet Express kit. See *Obtain the Internet Express Kit*.
2. Install the required components from the Internet Express kit. See *Install the LDAP Module for System Authentication*.
3. Use the Internet Express Administration utility to configure the LDAP Module for System Authentication. See *Configure the LDAP Module for System Authentication*.
4. Import your user information into the LDAP database. See *Import User Data into the LDAP Database*.
5. Configure caching parameters. See *Configure Caching Parameters*.

Obtain the Internet Express Kit

HP includes the Internet Express CD-ROMs with Tru64 UNIX AlphaServer™ systems. If you need the Internet Express CD-ROMs, you can contact your HP representative. The part number for the Internet Express kit is QB-3NCAA-SA.

Install the LDAP Module for System Authentication

Your environment must have a directory server that can be used with the LDAP Module for System Authentication. This directory server can either be one installed on the local system (by Internet Express) or one on a remote system that has already been configured. The directory server can also be installed at the same time as the LDAPSIA module and LDAP runtime. If the directory server is a remote server, the person who installs the LDAPSIA must have the following information:

- root domain name
- password for the rootdn
- the searchbase for user account information

To install the LDAP Module for System Authentication, follow the instructions in the *Internet Express for Tru64 UNIX Installation Guide*.

Ensure that you select the LDAP Module for System Authentication (IAELDAM) subset.

After you install the LDAP Module for System Authentication from the Internet Express kit, the system is set up with default LDAP configuration settings.

Configure the LDAP Module for System Authentication

The LDAP caching daemon uses the `/etc/ldapcd.conf` configuration file. This file provides information on how to connect to the LDAP directory server, the attribute mappings for the password and group entries, and caching parameters. This file must contain a clear text password that allows the utilities to connect to the directory server and should always be read only by root. You should use the Internet Express Administration utility to modify the `/etc/ldapcd.conf` file.

To modify the LDAP configuration parameters, follow these steps:

1. Choose Manage Components from the Administration utility main menu.
2. Under Users, choose LDAP System Authentication.
3. Change the configuration parameters as desired.

For a description of these parameters, see the LDAP Module for System Authentication chapter in *Internet Express Administration Guide*. In the directory server System Name field, multiple directory servers can be entered as a comma-separated list.

To specify multiple directory servers list all the directory servers available in your environment; for example:

```
directory: dir1.hp.com, dir2.hp.com, dir3.hp.com
```

If you intend to use a directory server (other than OpenLDAP) that requires user passwords to be encrypted prior to sending them to the server, you must manually add the following line to the `/etc/ldapcd.conf` file:

```
crypt_passwd: 1
```

Import User Data into the LDAP Database

After you configure the LDAP Module for System Authentication, you must import user data (unless you are using an existing LDAP server).

To import user data and store it in the LDAP database, follow these steps:

1. Identify the user data that you want to put into the LDAP directory.
2. Extract the user data from the `/etc/passwd` file using the `/usr/internet/ldap_tools/passwd_extract` utility. Or, to

import from NIS, use `ypcat` to output the entries to a local file, and remove any entries you do not wish to have in the LDAP database.

3. Store the records (formatted as `passwd(4)` entries) in a file.
4. Import these password records into the LDAP server using the following command:

```
$ ldap_add_user -f input-file
```

Note

For system security reasons, the following users should never be LDAP authenticated: `root`, `nobody`, `nobodyV`, `daemon`, `bin`, `uucp`, `uucpa`, `auth`, `cron`, `lp`, `tcb`, `adm`, `ris`, `wnn`, `pop`, `imap`, `ftp`, and `anonymous`.

For complete instructions, see the LDAP Module for System Authentication chapter in *Internet Express Administration Guide*.

Configure Caching Parameters

When configuring the LDAP Authentication Module, you can further improve performance by adjusting the caching parameters identified in the following table.

Parameter	Description
<code>pw_cachesize</code>	Determines the size of the password cache. Ideally this parameter should be set to the number of users that typically log in to this machine. A higher number will increase the probability of a cache hit, thereby increasing performance. Conversely a lower number will decrease the probability of a cache hit thereby decreasing performance.
<code>pw_expirecache</code>	Determines how long, in seconds, a password entry exists in the cache. A higher number increases the probability of a cache hit over time. However, a higher number also increases the probability that user data removed from the directory will still remain in the cache. If user data is routinely created and deleted, you should use a lower number.

Parameter	Description
gr_cachesize	Determines the size of the group cache. Ideally this parameter should be set to the number of groups that typically exist on this machine. A higher number will increase the probability of a cache hit, thereby increasing performance. Conversely a lower number will decrease the probability of a cache hit, thereby decreasing performance.
gr_expirecache	Determines how long, in seconds, a group entry exists in the cache. A higher number increases the probability of a cache hit over time. However, a higher number also increases the probability that a group removed from the directory will still remain in the cache. Generally groups are not deleted, so you can safely use a higher number.

Verifying Success

After you apply the Best Practice for Setting Up and Configuring LDAP for User Authentication, you can verify whether it was successful:

- You successfully installed the LDAP Module for System Authentication component of the Internet Express.
- You can access the Manage LDAP for System Authentication menu from the Manage System menu of the Administration utility for Internet Express.
- You can log in as a user whose information is in the LDAP server but not in the password file.

The Internet Express software kit includes several utilities that you can use to maintain the extended LDAP directory server shipped with Internet Express . These utilities, are installed in the `/usr/internet/ldap_tools` directory. One of these utilities is `ldap_check`, which verifies that the specified directory servers are running and that connections to the servers can be made.

If the Best Practice was not successful, see *Troubleshooting* for information about identifying and solving problems.

Troubleshooting

If you determine that the Best Practice was not successful, as described in *Verifying Success*, see the chapter LDAP Module for System Authentication in the *Internet Express Administration Guide*.

In addition to other detailed information, this chapter discusses how to use the `ldapcd` command with the `-d` option to check for errors.

You can also use the tool `/usr/internet/ldap_tools/ldap_check`. This tool reports on any problems that it finds that may interfere with the operation of the LDAP Module for System Authentication.

Comments and Questions

We value your comments and questions on the information in this document. Please mail your comments to us at this address:

`best_practices@zk3.dec.com`

Legal Notice

© 2002 Hewlett-Packard Company

Microsoft® and Windows NT® are trademarks of Microsoft Corporation in the U.S. and/or other countries. Intel®, Pentium®, and Intel Inside® are trademarks of Intel Corporation in the U.S. and/or other countries. UNIX® and The Open Group™ are trademarks of The Open Group in the U.S. and/or other countries. All other product names mentioned herein may be the trademarks of their respective companies.

Confidential computer software. Valid license from Compaq Computer Corporation, a wholly owned subsidiary of Hewlett-Packard Company, required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

None of Compaq, HP, or any of their subsidiaries shall be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for HP or Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.