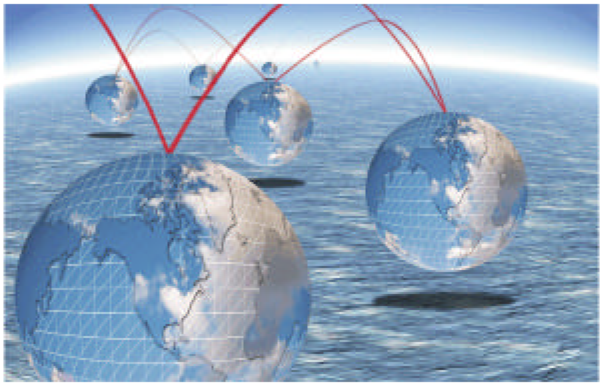
Using PMDF



to Leverage LDAP Servers

PMDF can use LDAP in many ways to build and maintain a large-scale secure mail environment. PMDF allows you to leverage your existing LDAP database to simplify mail administration and authenticate users' e-mail access. In addition, mail administrators can use the LDAP v2 or v3 compliant LDAP server of their choice, because PMDF is not tied to any particular LDAP vendor's solution.

Here is why you should leverage your LDAP database using PMDF.

Reliable Message Delivery
The most common use of LDAP with PMDF is to store user address mapping information. Local user mailbox addresses (such as smith@process.com) can be mapped to corporate standard Internet addresses (such as joe.smith@process.com) stored in an LDAP database. This is accomplished by using the PMDF Directory channel.

One advantage of using LDAP to map user mailbox names to corporate Internet addresses is increased reliability of message delivery. Without this feature, e-mail messages may bounce back to a sender if he or she misspells an e-mail address, a common occurrence when the sender may not know the exact address of the intended message recipient. With PMDF's Directory channel configured to do LDAP lookups, a mail message could be addressed to j.smith@process.com, joe.smith@process.com or smithj@process.com and be delivered to smith@process.com.This is possible because the Directory channel will try various LDAP lookups based on what appears to the left of the "@"-sign in the address. Compare this to the PMDF Alias Database which allows only an exact mapping between mail addresses and mail recipients.

Another advantage to using PMDF with an LDAP database is that PMDF provides the ability to return helpful information to the message sender in the event that the directory channel found that it could not match the specified destination address. The mail administrator can configure the directory channel so that in the event an input destination address produces multiple matches (e.g. a search for j.smith@process.com matches 5 entries in the LDAP directory), it will return a message to the sender indicating that the address was ambiguous, together with a list of the addresses that matched. This option should only be set-up for internal corporate use so that corporate employee addresses are not exposed to potential hackers and spammers. A separate directory channel can be set-up for communication outside the company that provides the sender with a simple "ambiguous address" response which does not list the internal addresses, should an attempt to send an e-mail message from outside the corporation fail.

Server Access Controls

PMDF with an LDAP database can provide remote user authentication when accessing an organization's SMTP, POP, or IMAP mail service. This is achieved by PMDF allowing the incoming username and password to be verified against an LDAP database. For example, a remote employee dialing into the corporate PMDF mail server at Company A would be required to enter a username and password before he or she can access their mail account (See Figure 1). Company A's PMDF mail server would perform an LDAP lookup prior to allowing e-mail to be sent from the remote employee. Once the username and password has been authenticated, the remote employee from Company A could send an e-mail message to an employee at Company B.

This feature protects users from potentially having their e-mail forged by another user. A hacker could send inappropriate e-mail messages to a corporation and alter the e-mail from: field so that it appears as if it was coming from someone else. For example, a hacker could send a "get rich quick" e-mail message to the CEO of Process Software and make it appear as if it was coming from smith@process.com, a Process Software employee.

In addition, mail administration in a multi-mail system environment can be simplified through the use of a centralized LDAP repository for usernames and passwords. There is also an option in PMDF that allows the mail administrator to indicate whether the username and password will be encoded or in plain text and whether the LDAP server is LDAPv2 or LDAPv3 compliant.

Authenticating mail using PMDF and LDAP

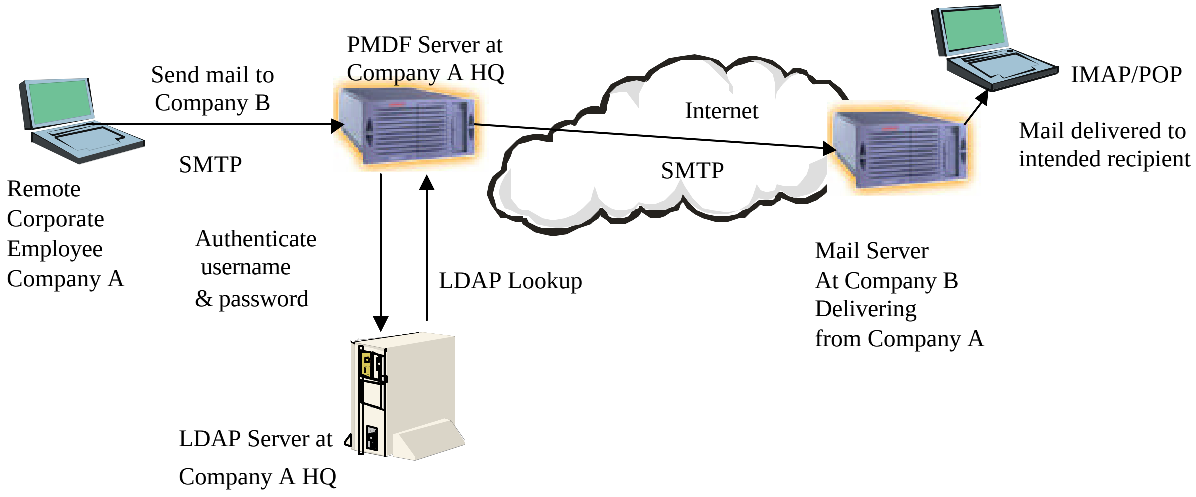


Figure 1

Ease Mail Administration

Using PMDF and LDAP can ease mail administration in several ways, including managing multiple mail servers and updating mailing lists.

Multiple mail servers

In multiple mail server environments, LDAP can be used in conjunction with PMDF to minimize the amount of updates that need to be made by the mail administrator, thus creating a more reliable mail delivery system. PMDF rewrite rule substitutions can be stored in an LDAP database, allowing two or more PMDF mail servers to query one set of rewrite rules. Storing the rewrite rules in an LDAP database allows an administrator to make changes to the configuration once, versus having to update the rewrite rules in each PMDF system. For example, an ISP adds and removes customers on a regular basis, hence the list of domains that PMDF will accept needs to be updated every time this occurs. Assume that this ISP uses a directory database for each domain. One method of making updates is to assign a rewrite rule per domain, which represents a specific customer. Each rewrite rule is hard coded into the configuration file. However, every time the ISP adds or loses a customer, the configuration file must be updated on each system, and the SMTP services will have to be restarted on each system. Using the LDAP database to verify the domain in question instead of the configuration file allows the ISP to make the changes once for all systems, and avoids the requirement of restarting the SMTP services. In order to accomplish this, a "wildcard" rewrite rule is used in PMDF, which performs an LDAP lookup for the domain name attributes that match the mail address. In Figure 2, mail sent to webmaster@yoyodyne.com, would have the following rewrite rule in the ISP mail server configuration file:

```
*    $U%$]<ldap:///ou=customers,dc=isp,mdc=com?domainName?sub?domainName=$D[
     @DIRECTORY-DAEMON
```

This rule allows PMDF to perform an LDAP search for entries with a 'domainName' attribute matching the domain name used in the mail address. The LDAP database entry would find the domain name yoyodyne.com and PMDF would deliver the mail to webmaster@yoyodyne.com.

With PMDF's configuration data stored in a central LDAP database, one mail system could be set-up to failover to a second system should one of the mail servers become unavailable. Mail services will not be interrupted because the LDAP database contains a centralized PMDF configuration repository.

A similar benefit also applies to mail administrators using PMDF and HP's (formerly Compaq/DEC) All-In-1. Both products can perform LDAP lookups so that a list of users does not have to be coordinated between the two products. LDAP queries from the VMS MAIL Utility (or PMDF MAIL) can also be performed.

PMDF LDAP Rewrite Rules

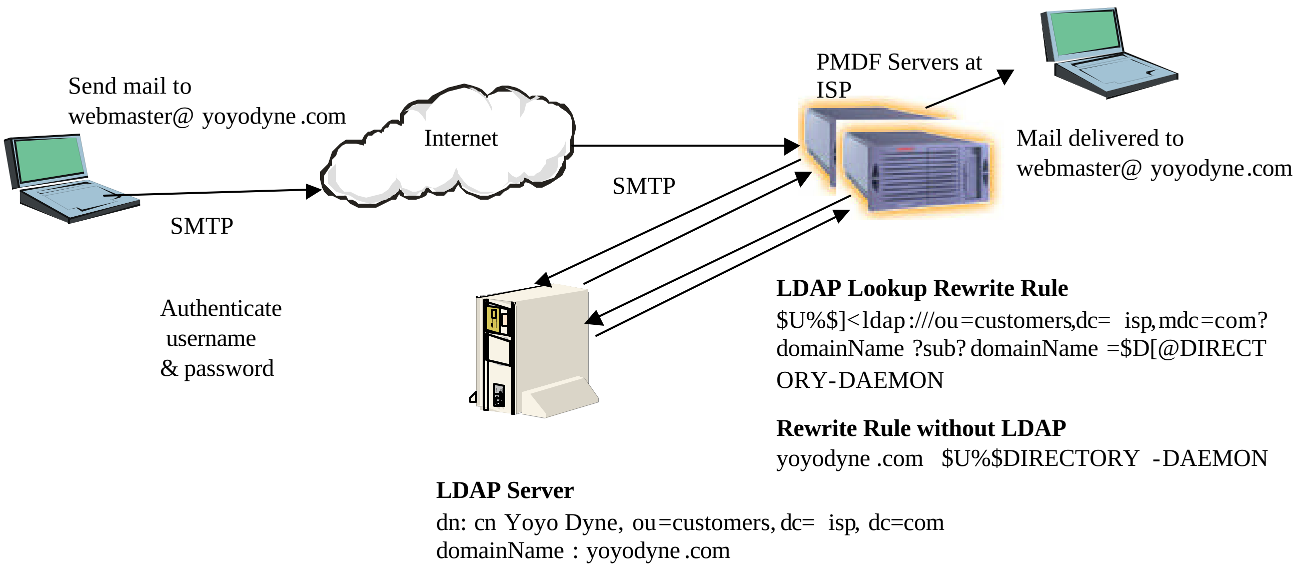

Send mail to
webmaster@ yoyodyne .com
SMTP
Internet
SMTP
PMDF Servers at
ISP
Mail delivered to
webmaster@ yoyodyne.com
Authenticate
username
& password
LDAP Lookup Rewrite Rule
$U%$]<ldap :///ou =customers,dc= isp,mdc=com?
domainName ?sub? domainName =$D[@DIRECT
ORY-DAEMON
Rewrite Rule without LDAP
yoyodyne .com $U%$DIRECTORY -DAEMON
LDAP Server
dn: cn Yoyo Dyne, ou=customers, dc= isp, dc=com
domainName : yoyodyne .com

Figure 2

Mail list maintenance
A mail administrator can reduce mailing list maintenance for users that belong to multiple mailing lists. For example, DECUS Australia maintains approximately 20 mailing lists, including the master list of all members as well as lists associated with each Special Interest Group and Local User Group. Membership and mailing list subscription information is stored in an LDAP database, which PMDF uses to build distribution lists based on the user group information stored in the LDAP database. When an individual joins DECUS or changes his or her particulars, the mail administrator simply needs to update a single entry in the database instead of having to edit 20 lists.

Improve Performance

An organization often uses a standard uniform address scheme for external addresses. Address reversal is a method by which local e-mail addresses are mapped to external addresses. PMDF can use information stored in an LDAP directory to perform address reversal. However, this can sometimes cause performance issues so some sites run a nightly procedure to extract the necessary information into a local on-disk database file.

The current shipping version of PMDF, version 6.2, released in November 2002, includes an LDAP upgrade. The PMDF implementation has been upgraded to the most current version of OpenLDAP, which provides compatibility with Windows 2000, and increases performance by reducing the amount of overhead required to perform an LDAP lookup. Thus some sites may find it is no longer necessary to perform regular LDAP extracts to local disk files, with the benefit that local users will be able to send mail as soon as they are registered in the LDAP directory instead of having to wait until the on-disk file is rebuilt.

References

To implement some of these PMDF and LDAP techniques as described in this overview, please see the following documentation:

Topic	PMDF Documentation
LDAP URLs in Rewrite Rules	System Manager's Guide Chapter 2.2.6.4
LDAP URLs for Forwarding Mail	System Manager's Guide Chapter 3.1
Forwarding with the ALIAS_URLn Options	System Manager's Guide Chapter 3.1.1
LDAP Lookups for Address Reversal	System Manager's Guide Chapter 3.3
LDAP URLs in Mappings	System Manager's Guide Chapter 5.3.2.7
LDAP Lookups from VMS & PMDF Mail	System Manager's Guide Chapter 21.3
Mailing Lists	System Manager's Guide Chapter 4

Summary

Process Software is committed to develop and support standards-based mail initiatives in PMDF, such as LDAP. For more information on PMDF 6.2 and its OpenLDAP support, see the Process Software Web page, www.process.com.

PROCESS™
SOFTWARE
A Platinum Equity Company

Process Software • 959 Concord Street • Framingham, MA 01701

Telephone: U.S./Canada (800)722-7770; International (508)879-6994

Fax: (508)879-0042 • Web: www.process.com • E-mail: info@process.com

November, 2002. The information contained in this document is subject to change without notice. Process Software assumes no responsibility for any errors that may appear in this document. © Process Software, November 2002. TCPware and MultiNet and PMDF are registered trademarks of Process Software. The Process Software name and logo are trademarks of Process Software. All other trademarks are property of their respective owners.