COMPAQ

Contents

Enabling LDAP Authentication on Compaq TaskSmart C-Series Servers

Abstract: This document was created to assist in the enabling of Lightweight Directory Access Protocol (LDAP) authentication on TaskSmart C-Series (TaskSmart C4000 series) servers.

Notice

158E-0701A-WWEN ©2001 Compaq Computer Corporation

Compaq, the Compaq logo and TaskSmart are trademarks of Compaq Information Technologies Group, L.P. Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States and other countries. Inktomi Traffic Engine is a trademark of Inktomi. All other product names mentioned herein may be trademarks of their respective companies.

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

LDAP Authentication on TaskSmart C-Series Servers

LDAP authentication via proxy server is an important security option offered on Compaq *TaskSmart*™ C-Series servers. The administrator of the network can use an existing directory service (for example, users on Microsoft Windows NT domain can sync with a Netscape Directory Server) by supporting asynchronous bind requests to an LDAP server. This process is discussed in the *Compaq TaskSmart C-Series Server Administration Guide* (Powered by Inktomi Traffic Server).

Edit records.config

The file, records.config, is found in the /home/inktomi/*x.x.x*/config directory, where *x.x.x* represents the version of your Traffic Server, and can be modified using a Telnet session to the TaskSmart C-Series server.

To enable LDAP authentication for security on the Traffic Server, the following strings must be modified:

IMPORTANT: Modify strings by using the VI or PICO editors.

- CONFIG proxy.config.ldap.auth.enabled INT 1 (changed from default 0)

- CONFIG proxy.config.ldap.proc.ldap.server.name STRING frank.com (The administrator can place a physical address of LDAP server into this variable, for example, 192.168.1.6.)

- CONFIG proxy.config.ldap.proc.ldap.server.port INT 389 (LDAP port 389)

- CONFIG proxy.config.ldap.base.dn STRING o=CORAL (DN or suffix on Netscape Directory Server; ensure format is correct.)

- CONFIG proxy.config.ldap.uid_filter STRING uid

- CONFIG proxy.config.body_factory.response_suppression_mode INT 0 (defaults to 2, ensure this mode is turned off)

Exit your editor, and then save changes. Stop and restart the Traffic Server service using the following command lines:
/home/inktomi/x.x.x/bin/stop_traffic_server
/home/inktomi/x.x.x/bin/start_traffic_server

Where *x.x.x* represents the version of your Traffic Server.

How to Customize the Authentication Dialogue Box

In the file, records.config, add the following string under the LDAP subtitle and append the following line directory below the uid_filter entry:
CONFIG proxy.config.proxy.authenticate.basic.realm to NULL

Modifications to this file allow the administrator to customize the authentication window. Figure 1 provides an example of the user authentication window which is displayed when the user attempts to open the browser.
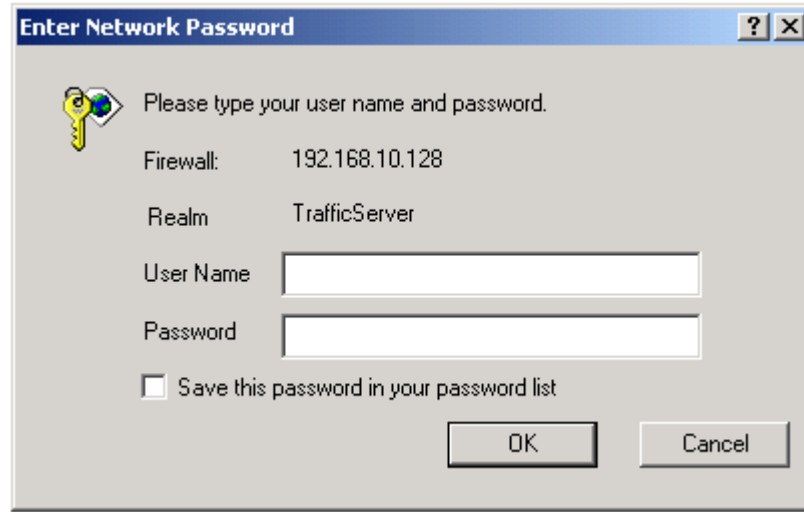

Figure 1: Enter Network Password window

LDAP Servers Supported

Openldap

Linux supports Openldap, a TGZ file format that adds service to a dedicated Linux LDAP authentication server. Currently, version 2.0.11 can be downloaded from

www.openldap.org.

Distinguished Names: As mentioned in the section, "Edit records.config," the DN string must be entered correctly. For more details on DN format, refer to RFC 1779 at

www.cis.ohio-state.edu/cgi-bin/rfc/rfc1779.html

Netscape Directory Server 4.13

Downloads for Netscape Directory Server 4.13 are located at www.iplanet.com. Netscape Directory Server provides a centralized directory service which can be synced with Windows NT Server and other operating systems. Netscape Directory Server supports LDAP versions 2 and 3. An LDAP directory service implementation consists of at least one LDAP server and at least one LDAP client.

Distinguished names are imperative to the authentication handshake. With Netscape Directory Server, suffixes are represented in DN format. The primary suffix represents the directory tree under which directory data is stored. The root entry must have a DN that is identical to a suffix. For example, when the suffix is o=CORAL, then the root entry must have the distinguished name of o=CORAL. The suffix may contain multiple attributes for example, dc=CORAL, dc=com; in which case, the DN of the entry in the directory tree must be dc=CORAL, dc=com.

More examples of DN strings and translations:

CONFIG proxy.config.ldap.base.dn STRING c=US, ou=People, o=CORAL

Translates to: Country = US, Organizational Units = People, Organization = CORAL

Documentation on Netscape Directory Server can be found at

http://developer.netscape.com/docs/manuals/index.html?content=directory.html

Netscape Directory Server SSL

Encrypted LDAP communications using Netscape Directory Server are referred to as LDAPS connections. To use LDAPS, the administrator must configure a security database for the server, and then turn on SSL in the server.

Use the following steps for setup of SSL using Certificate Setup Wizard:

1. Have the following information on a worksheet before proceeding:
    - Your contact information
    - Common name (fully qualified name of the website)
    - Name of your organization
    - Organizational unit
    - City/Location
    - State/Province
    - Country

2. Upon setup of Certificate Wizard, the administrator will be asked if a certificate has already been acquired via Certificate Authority. (www.verisign.com) Select **No,** and then click **Next.**

3. A window presents questions regarding trust relationship. Choose **Trust Does Not Exist,** and then click **Next.**

4. A token is presented and named; for example, **admin-serv-frank.** Add password, and then verify password. Click **Next.**

5. Trust has been created; click **Next.**

6. Generate Certificate request, and then click **Next.**

7. Add the required information marked by an asterisk for the new certificate, and then click **Next.**

8. Copy the certificate, including beginning and ending headers, and then paste into Notepad. Save as a text file.

9. Send to VeriSign Certificate Authority via VeriSign secure server ID. VeriSign turnaround time is approximately three to six hours.

10. After the certificate is received via email, copy the entire certificate including the beginning and ending headers, and then paste the certificate in the dialogue box on Netscape Directory Server. **Assign to this Server** button is enabled.

11. Proceed to server console, and then configure encryption that enables SSL. The drop-down box lists the certificates that were installed on the server. Choose **admin-serv-frank** as the certificate received from VeriSign.

Note: VeriSign trial certificates are protected to prevent fraudulent use of test server IDs. To test the use of trial certificates, the administrator must install a special Test CA Root on each browser that will be used in the test.

Required Equipment

Hardware:

- TaskSmart C4000 server (Model 30, 40, or 50)
- LDAP server (see variants in the introduction of this document)
- L4 or Fast Ethernet Switch
- 1-unlimited clients
- Connection to Internet

Software:

- TaskSmart C-Series server, software version 2.0 or higher
- IE 4.0 or higher browser
- Client operating system Windows NT
- W2000prof

Diagram of Network Configuration (Transparent Proxy, L4 Switch)

Router

Firewall

Netscape Directory Server 4.13; LDAP server

Workstation: WinNT/Win2000prof

L4 switch, Foundry

Fast Ethernet Switch

Workstation

Workstation

TaskSmart C4000 model 30