Hitachi HiCommand® Backup Services Manager

Enterprise LDAP / Active Directory Integration Guide

November 2006

Version 6.0

Doc ID: MK-95APT013-01

ALL RIGHTS RESERVED

Copyright © 2003-2006 APTARE, Inc.

TABLE OF CONTENTS

1. INTRODUCTION 3
2. SUPPORTED LDAP AND ACTIVE DIRECTORY SERVICES 3
3. SWITCHING FROM THE DEFAULT HBSM LDAP SERVICE TO AN EXTERNAL AUTHENTICATION SERVICE 3
4. USER ADMINISTRATION USING AN EXTERNAL AUTHENTICATION SERVICE 5

ALL RIGHTS RESERVED
Copyright © 2003-2006 APTARE, Inc.

1. Introduction

Hitachi HiCommand® Backup Services Manager comes bundled with its own LDAP service for managing user login authentication. The standard product installation utilizes this LDAP service by default; however integration to the Enterprise LDAP or Active Directory service is also supported. This document provides instructions for integrating the HBSM Portal to the Enterprise LDAP or Active Directory service. This install guide is valid for HBSM Portal version 6.0 onward.

Separate instructions are provided as necessary for Windows and UNIX.

If you encounter any problems or if you have questions regarding this task, please contact the HDS Technical Support Center which will be happy to assist you:

Technical Support Center Contact Information

Phone:	
Nth & Latin America	1-800-348-4357
Europe	+(44)-175-361-8000
Asia Pacific (call USA GCC)	+(1) 858-547-4765
Email:	support@hds.com

2. Supported LDAP and Active Directory Services

2.1. Supported Configurations

Hitachi HiCommand® Backup Services Manager has been certified to integrate with the following LDAP and Active Directory products:

- SunOne Directory Server 5.2
- OpenLDAP
- Microsoft Active Directory

3. Switching from the default HBSM LDAP service to an external Authentication service

3.1. Update the default Administration login

The standard install creates a user account in the form “admin@yourdomain.com” in the HBSM database. You will need to update this user record in the database to correspond to an existing user account in your Enterprise Authentication directory so you can login to the HBSM Portal application.

3.1.1.

Determine the login attribute in your Enterprise directory that is used for authentication (e.g. employee id, user_id etc. – typically the field you use for login to your other Enterprise systems today.) This field must correspond to the value entered in the <LOGIN_ATTRIBUTE> tag described below. Note the actual value of this login attribute for the HBSM Super User Administration login. For this example let’s assume the login attribute is “employee_id” and the actual value is 0888.

3.1.2.

As the unix user ‘aptare’, or on Windows as a user who is a member of the “ORA_DBA” group, run sqlplus on the HBSM database server to update the existing record:

ALL RIGHTS RESERVED
Copyright © 2003-2006 APTARE, Inc.

```
sqlplus portal/<portal password[1]>

UPDATE ptl_user SET ldap_id = '0888'
WHERE user_id = 100000;
commit;
```

3.2. Update the HBSM portal LDAP configuration settings

The LDAP configuration settings can be found in the file /opt/aptare/portalconf/portalproperties.xml. Make a backup copy and then edit this file. By default the file will contain the following entries:

```
<namingService>
<INIT_CONTEXT>com.sun.jndi.ldap.LdapCtxFactory</INIT_CONTEXT>
<SERVICE_URL>ldap://localhost:389</SERVICE_URL>
<MGR_DN>cn=Manager, dc=aptare, dc=com</MGR_DN>
<MGR_PW>password</MGR_PW>
<SEARCHBASE>dc=aptare, dc=com</SEARCHBASE>
<EXTERNAL_LDAP>false</EXTERNAL_LDAP>
<LOGIN_ATTRIBUTE>uid</LOGIN_ATTRIBUTE>
<KEYSTORE>/opt/aptare/portalconf/portal.keystore</KEYSTORE>
</namingService>
```

Change the following fields:

Field	Value
SERVICE_URL	Set to the host and port of your external authentication service
MGR_DN, MGR_PW	Set to the id and password of a user who has permission to search the searchbase specified below. (This field is only required for Active Directory services which do not allow anonymous binds.)
SEARCHBASE	Location from which the search will be performed to locate users in the authentication directory.
EXTERNAL_LDAP	Set to TRUE if an external Enterprise authentication service will be used. Set to FALSE if using the bundled HBSM LDAP service (default).
LOGIN_ATTRIBUTE	The LDAP / Active Directory attribute used for login authentication (e.g. uid, employee_id, email_address etc.) In the above example this would be “employee_id”
KEYSTORE	Keystore file location if external authentication service uses SSL.

If SSL support is required, you can generate the KEYSTORE file via the following command:

```
/usr/java/bin/keytool –import –file certificate_file  -keystore keystore_file
```

where: *certificate_file* is the path and filename for the X.500 CA certificate
keystore_file is target path and filename for the KEYSTORE file being generated

3.3. Restart the HBSM Portal tomcat service

3.3.1. UNIX

/opt/aptare/bin/tomcat-portal restart

3.3.2. Windows

[1] Default password is portal

ALL RIGHTS RESERVED
Copyright © 2003-2006 APTARE, Inc.

Using the Windows services console, restart the following service:

APTARE Portal Tomcat

3.4. Add new user accounts to the Portal

Once you have configured the HBSM Portal to use your enterprise directory service, you can login using the Admin user account set up above and create new user records that correspond to existing user accounts in the enterprise directory.

4. User Administration using an external Authentication service

4.1. Adding and updating User accounts

When using the default LDAP Service that comes bundled with HBSM, adding a user via the Portal Web GUI will also add the user to the HBSM LDAP directory. Similarly, you can change a user's password via the Portal Web GUI.

However, when using an external authentication service, the user must already exist in the external directory before you can add a record for this user via the HBSM Portal Web GUI. Note too that you will not be able to change a user's password via the HBSM Portal Web GUI.

ALL RIGHTS RESERVED
Copyright © 2003-2006 APTARE, Inc.