Deployment Example 1: Access Manager 7.0 Load Balancing, Distributed Authentication UI, and Session Failover

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–6258–40
October 2007

071106@19028

Contents

PART I

About This Deployment Example

◆ ◆ ◆ CHAPTER 1

Key Features and Constraints

This document provides instructions for installing and configuring a common Sun Java System Access Manager 7 2005Q4 solution that incorporates load-balancing, distributed authentication UI, and policy agents.

1.1 Key Features of This Deployment Example

- All components such as Directory Servers, Access Manager Servers, Distributed Authentication UI servers, and Policy Agents are redundant to achieve high availability.
- Both Web Policy Agents and J2EE Policy Agents are used to protect resources in the environment.
- All components use load-balancing for system failover and for high availability.
- Each Directory Server contains three instances: one named `ds-config` for storing Directory Server configuration, one named `am-config` for storing Access Manager configuration, and one named `am-users` for storing Access Manager users. The `am-users` instance serves as the LDAPv3 user data store.
- The environment includes one service access interface for external users and agents, and a separate service access interface for internal administrators.
- Actual firewalls were not used in this deployment. However, critical components such as Access Manager and Directory Server can be protected by three firewalls as illustrated in Figure 1–1. In this illustration, only simple components and interfaces are exposed to the Internet in a minimally-secured zone known as the DMZ.
- Access Manager servers are reconfigured to run as non-root users.
- The environment is configured for system failover capability. System failover ensures that when one Access Manager server goes down, requests are redirected to a second Access Manager server. It is important to note that system failover, by itself, does not ensure Access Manager session failover.

- The environment is configured for session failover capability. Session failover ensures that when the Access Manager server *where the user's session was created* is stopped, the user's session token can still be retrieved from a backend session database. The user is continuously authenticated, and does not have to log into the system again unless the session is invalidated. For example, a session is invalidated when the logout occurs or when the session expires.
- An existing LDAPv3 user data store is integrated into the environment.
- SSL is terminated at the load balancer for Access Manager servers and at the load balancer for Access Manager Distributed Authentication UI servers. In this deployment example, communication to each of these load balancers is in SSL, and communication between the load balancer and the server is non-SSL.
- Each policy agent in the deployment is configured with a unique agent profile used by the agent to authenticate itself to Access Manager.
- The Distributed Authentication UI servers use a custom user profile to authenticate to Access Manager instead of a default of `amadmin` or `UrlAccessManager`.

1.2 System Environment and Architecture

The following components comprise the system environment and architecture described in this document:

Network Connectivity

Although firewalls were not actually implemented when setting up this deployment example, in this environment the best practice is to use three firewalls which form three distinct security zones as illustrated in Figure 1–1. One zone would be completely secured, protected by all three firewalls, and would used for internal traffic only. Two minimally-secured zones, also known as DMZs, would be protected by only two firewalls. One minimally-secured zone would be used for internal traffic only, and the second minimally-secured would be used for external traffic. Direct access to individual Access Manager servers would be allowed for internal administrators only if permitted by firewall rules. For more information on specific firewall rules, see the section "2.4 Firewall Rules" on page 27 in this document.

Distributed Authentication UI servers

The Distributed Authentication UI servers provide a thin presentation layer for user authentication. The purpose of the Distributed Authentication UI servers is to protect the Access Manager servers from exposure in the minimally-secured DMZ. During user authentication, a Distributed Authentication Module passes the user's credential to the Access Manager server for verification. The user does not have direct network access to Access Manager servers.

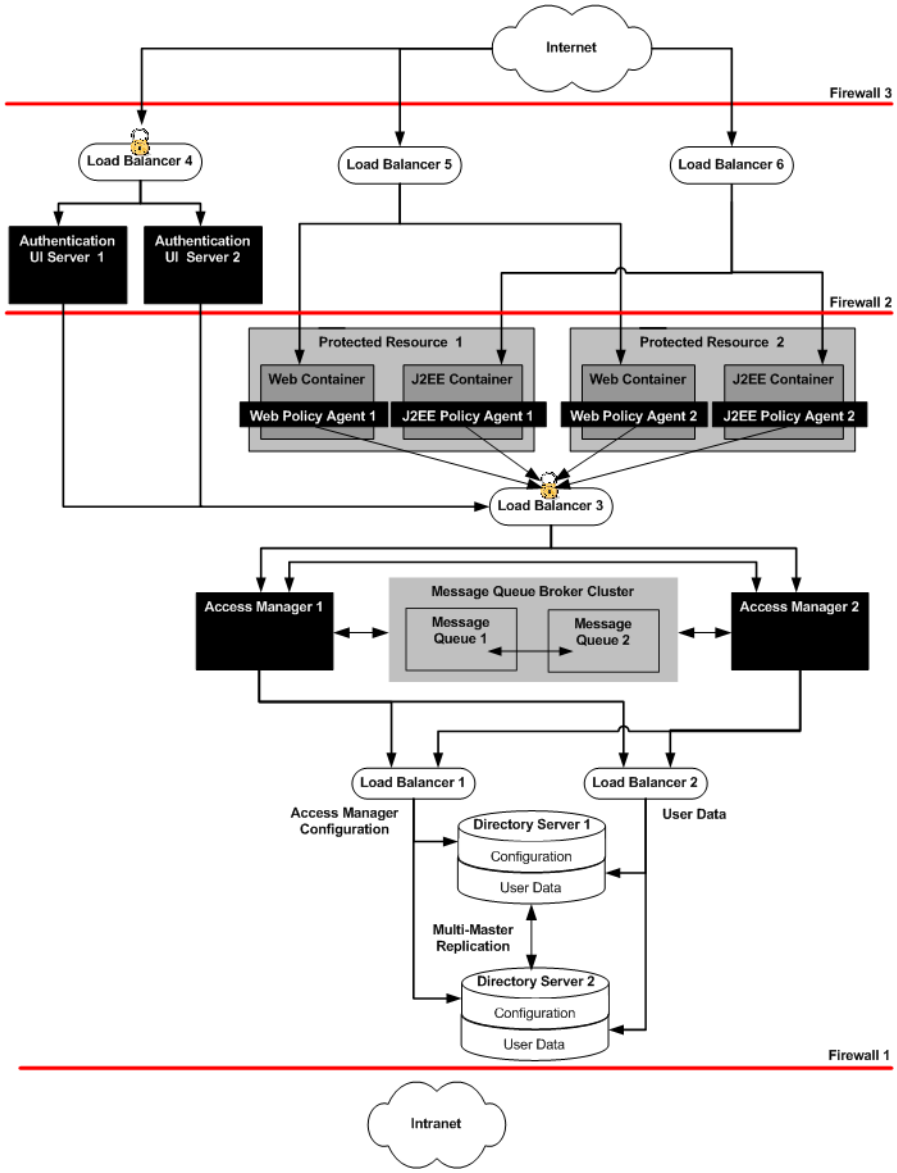

FIGURE 1–1 System Architecture

Protected Resources

Protected resources are the Web Servers or Application Servers to which you want to restrict access. For example, your Human Resources Department might use Applications Servers to host applications and Web Servers to host content. Some of the hosted information must be made available to external benefits administration vendors. External vendors might include

health care providers or stock administrators who must access employee information in order to coordinate benefits. The external vendors access the protected resources through an external-facing load balancer. Other information must be restricted to only internal Human Resources administrators. Internal administrators access the protected resources through an internal-facing load balancer.

J2EE Policy Agents and Web Policy Agents

Policy agents restrict access to content or applications hosted on the protected resources. The policy agents intercept HTTP requests from external users, then communicate with the Access Manager servers. If the user presents proper credentials and can be authenticated by the Access Manager server, Access Manager allows the user to access the protected resource. The policy agents are deployed with a load balancer in front of them.

Access Manager Servers

Two separate Access Manager servers provide core Access Manager functionality. Both servers share the same configuration. Both servers store their configuration through a single load balancer deployed in front of the two Directory Servers.

The Access Manager servers are hosted behind the internal firewall and outside the DMZ. The load balancer and two Access Manager servers together provide high data availability within the infrastructure.

Directory Servers

Two Directory Server instances provide the storage for Access Manager configuration information. This includes information about services, policies, and more. Both Directory Server data instances are master replicas that engage in multi-master replication (MMR). MMR allows data to be synchronized in real time between two directories. This synchronization provides high availability to the Access Manager layer.

Load Balancers

Load balancers in this environment enable system failover and high server availability for optimized performance. Multiple virtual load balancers in this deployment example were aggregated into a single unit of load balancing hardware.

Distributed Authentication UI Load Balancer

This external-facing load balancer exposes the remote, web-based Access Manager interface for user authentication, self-registration, and policy agent authentication.

Policy Agents Load Balancers

Policy agents are deployed with external-facing load balancers in front of them. The policy agents then communicate with Access Manager servers through an internal-facing load balancer.

Access Manager Load Balancer

This internal-facing load balancer exposes the web-based Access Manager administration console to internal administrators. Alternatively, internal administrators can also bypass the internal-facing load balancer and log in directly to an Access Manager administration console.

Directory Server Load Balancer
The load balancer in front of the Directory Servers provides round-robin load balancing for Directory Server access, and detects individual Directory Server failures and recovery. Failed servers are taken out of the load balancer list. The load balancer also provides a single virtual Directory Server host name to the Access Manager servers.

Message Queue Broker Cluster
In this deployment example, Access Manages uses two Message Queue instances to form a cluster. The cluster acts as a communications broker, and uses the Berkeley DB by Sleepycat Software, Inc. as the session store database. When session failover is enabled, and an Access Manager server goes down, the available Access Manager server can retrieve the user's session token from one of the Message Queues in the cluster. This ensures that the user remains continuously authenticated, and allows the user to access to the Protected Resources without having to re-authenticate.

1.3 System Behaviors

The following sequence describes the interaction between the various components in this Deployment Example. These interactions are also illustrated in the following pages. The numbered steps here correspond to the numbers in the figures on the following pages.

1. A user attempts to access the J2EE application hosted by Protected Resource 1 and by Protected Resource 2 through Load Balancer 6. Load Balancer 6 redirects the user to Protected Resource 1.
2. The J2EE Policy Agent intercepts the request and checks for the Access Manager cookie.
3. If the Access Manager cookie is not found, the J2EE Policy Agent redirects the user to Load Balancer 4, the load balancer for the Distributed Authentication UI servers.
4. Load Balancer 4 routes the user request to Authentication UI Server 2.
5. Authentication UI Server 2 displays a login page to the user.
6. The user enters credentials on the login page.
7. Authentication UI Server 2 passes the credentials to Load Balancer 3.
8. Load Balancer 3 routes the Authentication UI 2 request to Access Manager 1 for validation.
9. Access Manager 1 sends the Authentication UI 2 request to Load Balancer 2. Load Balancer 2 handles Directory Server requests for user data.
10. Load Balancer 2 routes the Authentication UI 2 request to Directory Server 2 where validation takes place.
11. After successful authentication, Access Manager 1 sends the Authentication UI 2 request back to the J2EE Policy Agent. The J2EE Policy Agent receives the request and checks for the Access Manger cookie.
12. When a cookie is found, the J2EE Policy Agent sends a session validation request to the Access Manager Load Balancer 3.

13. The Access Manager Load Balancer 3 forwards the request to the Access Manager 1 where the session originated. Cookie-based persistency and routing enables Access Manager to route the request properly.
14. Access Manager 1 sends a response back to the J2EE Policy Agent.
15. If the session is not valid, the J2EE Policy Agent would redirect the user to the Distributed Authentication UI server.
16. In this example, J2EE Policy Agent receives the response back as a valid session. When the session is valid, the J2EE Policy Agent sends a policy request to Access Manager servers' Load Balancer 3.
17. Access Manager 1 conducts the policy evaluation.
18. Based on the policy evaluation, the J2EE Policy Agent either allows access to the resource or denies access to the resource. In this example, the user is allowed access to the Application Server.

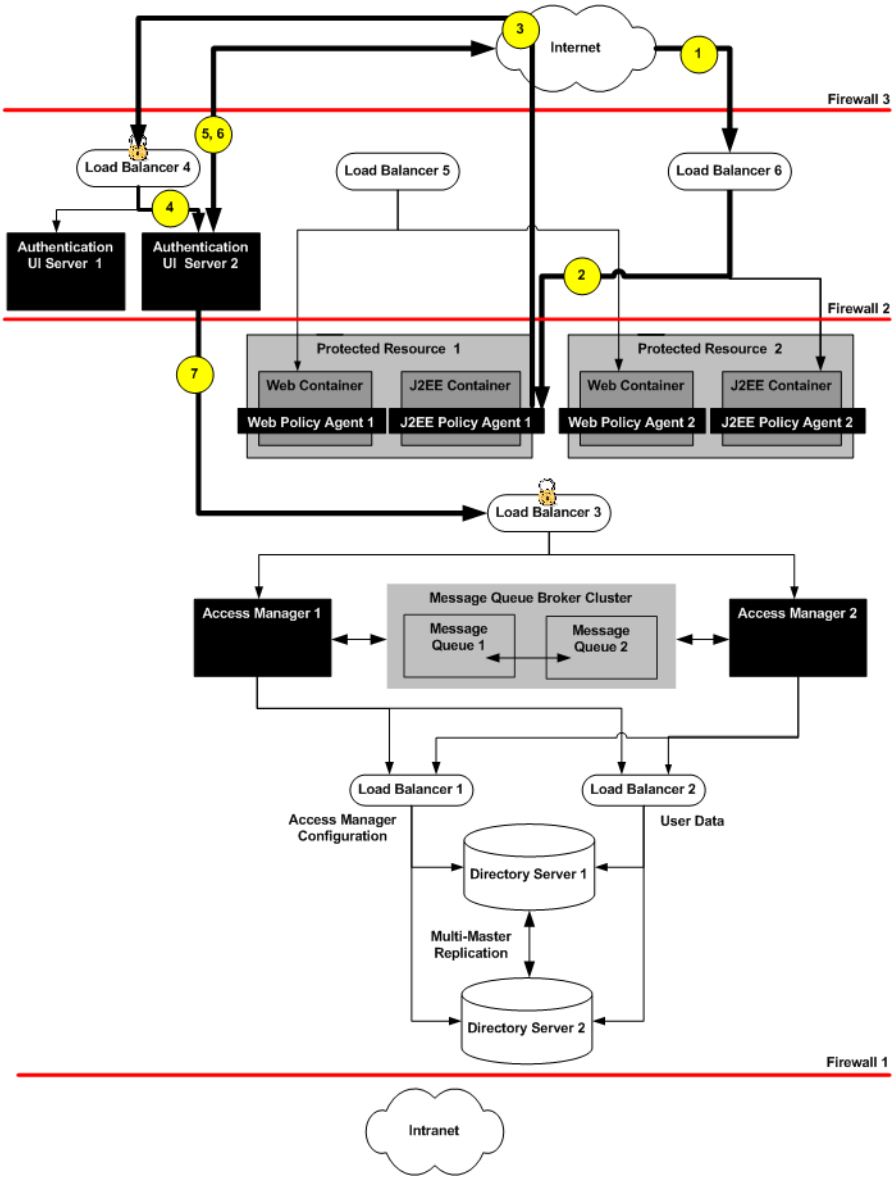

FIGURE 1–2 Request for Access

In this figure, a user attempts to access a protected application. The J2EE Policy Agent intercepts the access request. The Authentication UI is invoked. The Authentication UI server displays a login page to the user.

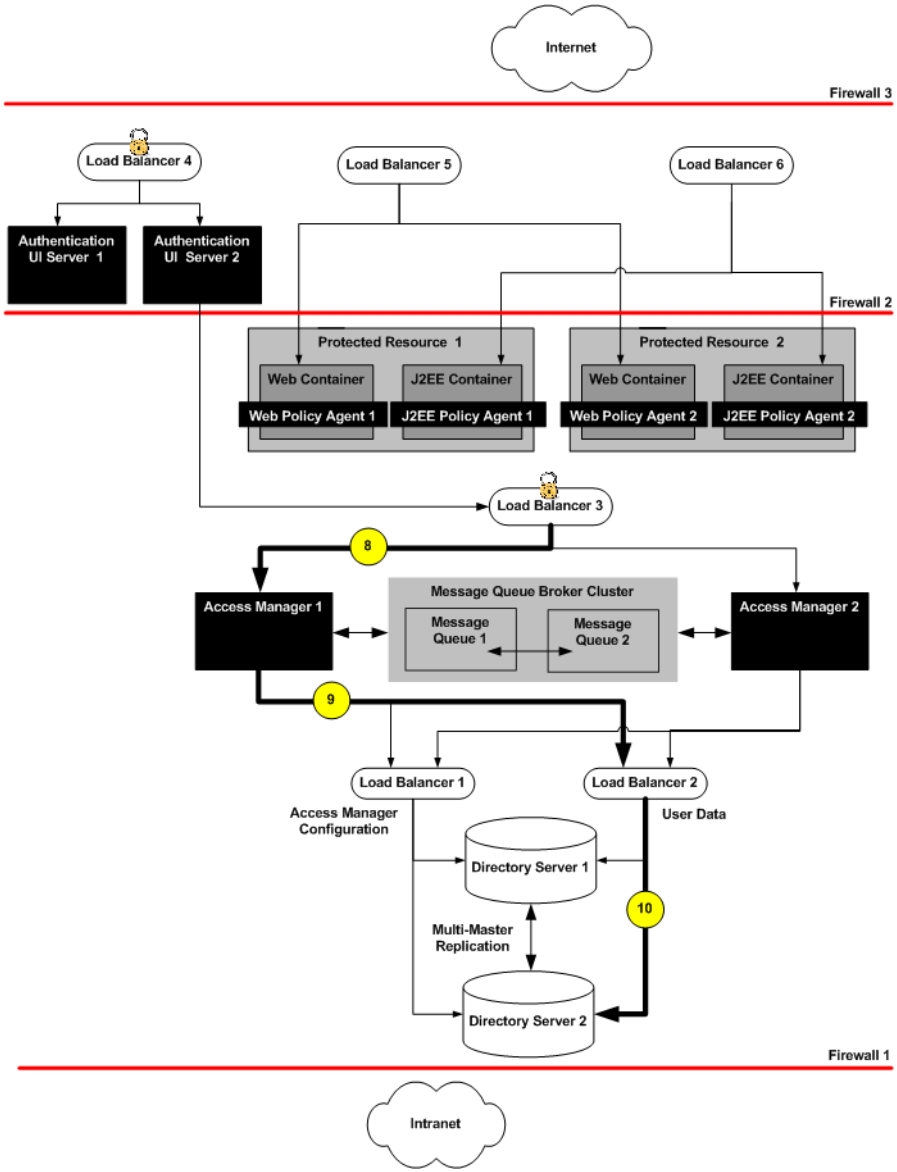

FIGURE 1–3 Authentication

In this figure, the user credentials are passed to Access Manager 1. Access Manager 1 checks the user credentials against Directory Server.

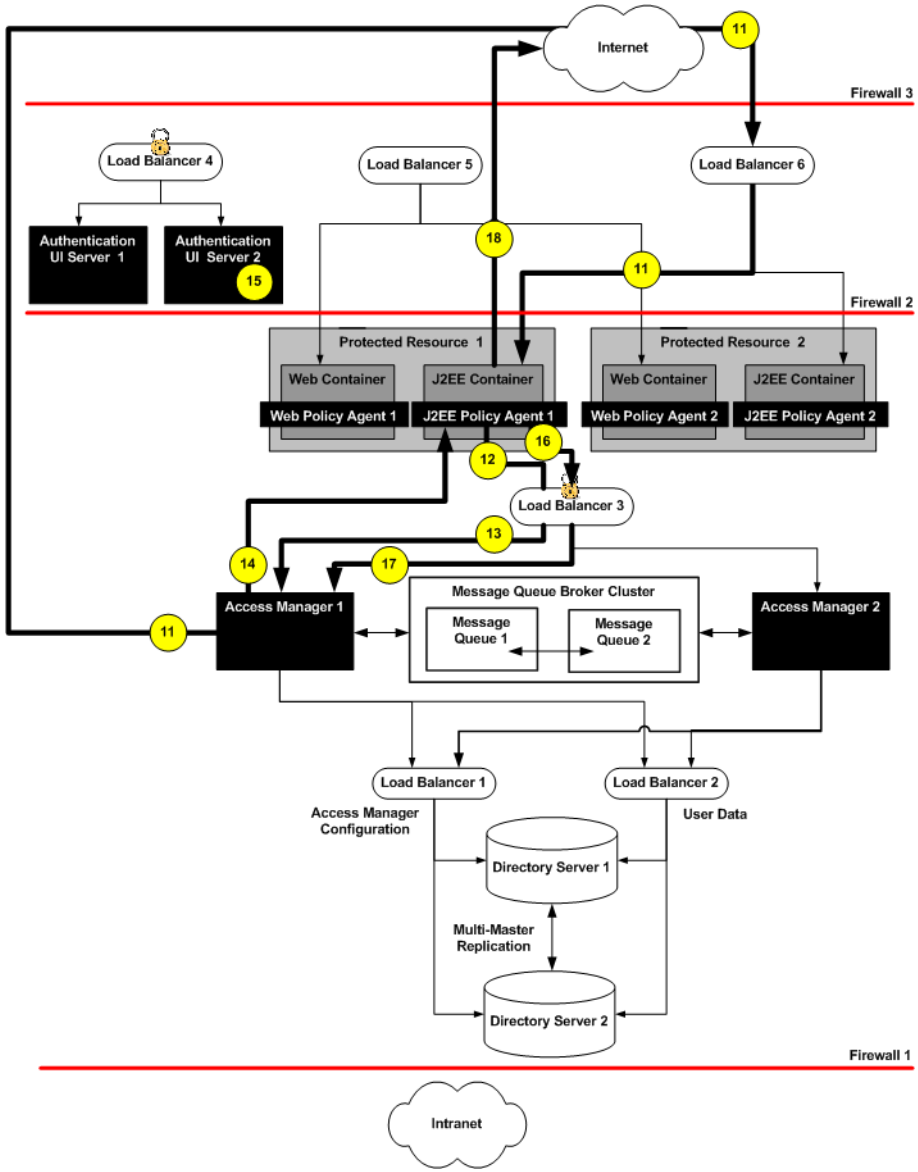

FIGURE 1–4 Access Granted

Access Manager authenticates the user, and the J2EE Policy Agent determines that the user's session is valid. The J2EE Policy Agent sends a second request to Access Manager for policy evaluation. Based on the results of the policy evaluation, the J2EE Policy Agent allows access to the application server. Access Manager continues to manage the session until the user logs out.

◆ ◆ ◆ CHAPTER 2

Technical Overview

This chapter contains the following topics:

2.1 Software Used in this Environment

The following table lists the software used in this deployment.

TABLE 2–1 Software Versions and Download Locations

Product	Version	Download Location
Sun Java Web Server	6.1SP5 (JES 2005Q4)	http://www.sun.com/download
Sun Java Directory Server	5.2_Patch_4 (JES 2005Q4)	http://www.sun.com/download
Sun Java Access Manager	7.0 (JES 2005Q4)	http://www.sun.com/download
Sun Java Access Manager Patch	7.0_Patch_5 120954-05 (sparc), 120955-05 (x86)	http://sunsolve.sun.com/ (`http://www.sun.com/download`)
BEA Weblogic Application Server	9.1	See the BEA website http://www.bea.com (`http://www.bea.com`)
Web Policy Agent (for Sun Java WebServer v6.1)	2.2_HotPatch_5	http://www.sun.com/download (`http://www.sun.com/download`)

TABLE 2–1 Software Versions and Download Locations *(Continued)*

Product	Version	Download Location
J2EE Policy Agent (for BEA Weblogic Application Server v9.1)	2.2_HotPatch_3	http://www.sun.com/download (http://www.sun.com/download)
Java (for Access Manager, Web Agent, J2EE Agent)	1.5.0_04	Automatically installed with Java Enterprise System, and BEA Application Server.
Big-IP Load Balancer		See the F5 Networks website http://www.f5.com (http://www.f5.com)

2.2 Host Names and Main Service URLs Used in Examples

The following table summarizes naming conventions used in this guide. For detailed configuration information, see Part IIIin this guide.

TABLE 2–2 Host Names and Service URLs

Host or Component	Main Service URL
Directory Servers	
DirectoryServer–1	ldap://DirectoryServer-1.example.com:1389
DirectoryServer-1 User Data Store	ldap://DirectoryServer-1.example.com:1489
DirectoryServer–2	ldap://DirectoryServer-2.example.com:1389
DirectoryServer-1 User Data Store	ldap://DirectoryServer-2.example.com:1489
LoadBalancer–1	http://LoadBalancer-1.example.com:389 (Access Manager configuration)
LoadBalancer–2	http://LoadBalancer-2.example.com:489 (User data store)
Access Manager Servers	
AccessManager–1	http://AccessManager-1. example.com:1080/amserver/console
AccessManager–2	http://AccessManager-2. example.com:1080/amserver/console

TABLE 2–2 Host Names and Service URLs *(Continued)*

Host or Component	Main Service URL
LoadBalancer–3	http://LoadBalancer-3.example.com:90 (for Intranet users) https://LoadBalancer-3.example.com:9443 (for Internet users)
Message Queue Broker Cluster	
MessageQueue–1	http://MessageQueue-1.example.com:7777
MessageQueue–2	http://MessageQueue-2.example.com:7777
Distributed Authentication UI Modules	
AuthenticationUI–1	http://AuthenticationUI-1. example.com:1080/distAuth/UI/Login
AuthenticationUI–2	http://AuthenticationUI-2. example.com:1080/distAuth/UI/Login
LoadBalancer–4	https://LoadBalancer-4.example.com:9443
Protected Resources and Policy Agents	
ProtectedResource–1	http://ProtectedResource-1.example.com:8888 (Sun Java System Web Server)
Web Agent 1	http://ProtectedResource-1.example.com:1080
ProtectedResource–1	http://ProtectedResource-1.example.com:7001/console (WebLogic Application Server)
J2EE Policy Agent 1	http://ProtectedResource-1.example.com:1081
ProtectedResource–2	http://ProtectedResource-2.example.com:8888 (Sun Java System Web Server)
Web Agent 2	http://ProtectedResource-2.example.com:1080
ProtectedResource–2	http://ProtectedResource-2.example.com:7001/console (WebLogic Application Server)
J2EE Policy Agent 2	http://ProtectedResource-2.example.com:1081
LoadBalancer–5	http://LoadBalancer-5.example.com:90 (Web Policy Agents)
LoadBalancer–6	http://LoadBalancer-6.example.com:91 (J2EE Policy Agents)

2.3 Intercomponent Communication

The following table provides an overview of the types of communication that take place between server, load balancers, and other components in the deployment example.

TABLE 2–3 Summary of Intercomponent Communication

Entity A	Entity B	Bi-Directional	Port	Protocol	Traffic Type
Intranet Users	LoadBalancer-5		90	HTTP	Application Traffic
Internet Users	LoadBalancer-6		91	HTTP	Application Traffic
Internet Users	LoadBalancer-4		9443	HTTPS	Internet User Authentication
Intranet Users	LoadBalancer-3		90	HTTP	Intranet User Authentication
LoadBalancer-4	AuthenticationUI-1		1080	HTTP	Internet User Authentication
LoadBalancer-4	AuthenticationUI-2		1080	HTTP	Internet User Authentication
LoadBalancer-5	ProtectedResource-1		1080	HTTP	Application Traffic
LoadBalancer-5	ProtectedResource-2		1080	HTTP	Application Traffic
LoadBalancer-6	ProtectedResource-1		1081	HTTP	Application Traffic
LoadBalancer-6	ProtectedResource-2		1081	HTTP	Application Traffic
AuthUIServer-1	LoadBalancer-3		9443	HTTPS	Internet User Authentication
AuthUIServer-2	LoadBalancer-3		9443	HTTPS	Internet User Authentication
ProtectedResource-1	LoadBalancer-3		9443	HTTPS	Agent-AM communication
ProtectedResource-2	LoadBalancer-3		9443	HTTPS	Agent-AM communication
LoadBalancer-3	AccessManager-1		1080	HTTP	User Authentication Agent-AM communication
LoadBalancer-3	AccessManager-2		1080	HTTP	User Authentication Agent-AM communication
AccessManager-1	AccessManager-2	Yes	1080	HTTP	AM Back-channel communication
AccessManager-1	MessageQueue-1	Yes	7777	HTTP	Session communication
AccessManager-2	MessageQueue-2	Yes	7777	HTTP	Session communication
MessageQueue-1	MessageQueue-2	Yes	7777	HTTP	Session communication
MessageQueue-2	MessageQueue-1	Yes	7777	HTTP	Session communication
AccessManager-1	LoadBalancer-1		389	LDAP	AM Configuration communication

TABLE 2–3 Summary of Intercomponent Communication *(Continued)*

Entity A	Entity B	Bi-Directional	Port	Protocol	Traffic Type
AccessManager-1	LoadBalancer-2		489	LDAP	User profile communication User Authentication
AccessManager-2	LoadBalancer-1		389	LDAP	AM Configuration communication
AccessManager-2	LoadBalancer-2		489	LDAP	User profile communication User Authentication
LoadBalancer-1	DirectoryServer-1		1389	LDAP	AM Configuration communication
LoadBalancer-1	DirectoryServer-2		1389	LDAP	AM Configuration communication
LoadBalancer-2	DirectoryServer-1		1489	LDAP	User profile communication User Authentication
LoadBalancer-2	DirectoryServer-2		1489	LDAP	User profile communication User Authentication
DirectoryServer-1	DirectoryServer-2	Yes	1389	LDAP	Data replication communication
DirectoryServer-1	DirectoryServer-2	Yes	1489	LDAP	Data replication communication

2.4 Firewall Rules

Set up firewalls to allow traffic to flow as described in the following table.

TABLE 2–4 Summary of Firewall Rules

From	To	Port #	Protocol	Traffic Type
Internet users	LoadBalancer-4	9443	HTTPS	User authentication
Internet users	LoadBalancer-5	90	HTTP	Application access by internet user
Internet user	LoadBalancer-6	90	HTTP	Application access by internet user
AuthenticationUI-1	LoadBalancer-3	9443	HTTPS	User authentication
AuthenticationUI-2	LoadBalancer-3	9443	HTTPS	User authentication
LoadBalancer-5	ProtectedResource-1	1080	HTTP	Application access by user
LoadBalancer-6	ProtectedResource-2	1081	HTTP	Application access by user
Intranet User	LoadBalancer-3	9443	HTTPS	User authentication and various Access Manager services

PART II

Building the Environment

◆ ◆ ◆ CHAPTER 3

Before You Begin

This chapter contains the following topics:

3.1 About This Guide

This guide provides instructions for building an environment for this Deployment Example. These instructions were used to build, deploy and test this Deployment Example in a lab facility. When using this guide, you'll obtain the best results if you perform the tasks in the exact sequence in which they are presented. Use the Table of Contents as a master task list. Tasks are numbered for your convenience.

The last step in each task is a verification procedure. Be sure to verify the success of each task before moving on to the next task in the sequence.

This guide is designed to demonstrate just one way to deploy Access Manager with load-balancers to optimize performance and high availability. Although these instructions incorporate many recommended or "best practices," and may be suitable in many different scenarios, this is not the only way to achieve the same results.

Caution – If you do plan to deviate from the task sequence or details described in this guide, you should refer to the relevant product documentation for information on differences in platforms, software versions or other requirement constraints.

3.1.1 Naming Conventions

See "2.2 Host Names and Main Service URLs Used in Examples" on page 24 for a quick reference of server names and component names used in this deployment example. See Part III for more detailed information.

3.1.2 Typographical Conventions

The following table describes the typographic conventions that are used in this deployment example.

TABLE 3–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

3.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer

Installation as described in this document includes the installation and basic configuration of a Java Enterprise System (Java ES) solution. Installation, as used in this document, means using the Java ES 2004Q5 installer to copy the files for Java ES components to computer systems. You can download and unpack the installer zip files onto one host computer system, and then mount the cd image on any remote host computer systems where you must install Directory Server, Access Manager, or Web Server.

▼ To Download and Mount the Java Enterprise System 2005Q4 Installer

1 **Download the Java ES installer zip files.**

   a. **Start a browser, and go to http://www.sun.com/software/solaris/get.jsp (`http://www.sun.com/software/solaris/get.jsp`).**

   b. **Choose Java Enterprise System.**

   Follow the instructions for downloading two zip files that together will form the CD image.

2 **Log in as a root user to a host computer system where you want to run the installer.**

3 **Copy the Java Enterprise System installer zip files to this host computer system.**

4 **Unzip each zipped file. Example:**

```
#ls
java_es_05Q4-ga-solaris-sparc-1-iso.zip
java_es_05Q4-ga-solaris-sparc-2-iso.zip
# unzip java_es_05Q4-ga-solaris-sparc-1-iso.zip
inflating: java_es_05Q4-ga-solaris-sparc-1.iso...

# unzip java_es_05Q4-ga-solaris-sparc-2-iso.zip
inflating: java_es_05Q4-ga-solaris-sparc-2.iso...
```

5 **Create three directories for mounting the `.iso` files. Example:**

```
# mkdir /mnt
# mkdir /mnt2
# mkdir /jes-complete
```

6 **Mount the `.iso` files.**

In the following examples, replace */download-directory/* with the path to your `.iso` file:

```
# lofiadm -a /download-directory/java_es_05Q4-ga-solaris-sparc-1.iso /dev/lofi/1
 # mount -F hsfs -o ro /dev/lofi/1 /mnt
```

Tip – If the `/dev/lofi/1` device is already in use, run this command:

```
# lofiadm –d /dev/lofi/1
```

and then retry using the `lofiad -a` command.

To mount the second iso file:

```
# lofiadm -a /download-directory/java_es_05Q4-ga-solaris-sparc-2.iso /dev/lofi/2
# mount -F hsfs -o ro /dev/lofi/2 /mnt2
# lofiadm
Block Device             File
dev/lofi/1              /export/temp/java_es_05Q4-ga-solaris-sparc-1.iso
/dev/lofi/2             /export/temp/java_es_05Q4-ga-solaris-sparc-2.iso
```

7 Copy both mounted `.iso` files to the same directory.

The two `.iso` files together form the complete JES package, so you must copy both files into the same directory. As an alternative, you can burn each ISO onto a CD, and then run the installer from a CD drive.

```
# cd /mnt1
# cp -r * /jes-complete
# cd /mnt2
# cp -r * /jes-complete
```

Next Steps After you mount the `.iso` files and copy them to the same directory, the installer is located in the here:

```
/jes-complete/Solaris_sparc
```

In this Deployment Example, you start the installer with the `-nodisplay` option:

```
# /jes-complete/Solaris_sparc/installer –nodisplay
```

3.3 Setting Up a Load Balancer

You will need load balancing hardware and software to replicate this deployment environment. The load balancer hardware and software used in the lab facility for this deployment is BIG-IP® manufactured by F5 Networks. If you are using different load balancer software, see the documentation that comes with that product for detailed settings information.

The following tasks require load-balancing hardware and software:

- "4.3 Configuring the Directory Servers Load Balancer" on page 54
- "5.4 Configuring the Access Manager Load Balancer" on page 86
- "6.2 Configuring the Distributed Authentication UI Servers Load Balancer" on page 121
- "7.3 Configuring the User Data Stores Load Balancer" on page 146
- "9.1 Configuring the Web Policy Agents Load Balancer" on page 241
- "9.2 Configuring the J2EE Policy Agents Load Balancer" on page 249

3.4 Obtaining Secure Socket Layer (SSL) Certificates

You will need to obtain root certificate authority (CA) certificates and server SSL certificates to enable SSL in this deployment environment. The certificate issuer used in this deployment is a test CA certificate from OpenSSL. You can obtain a root CA certificate from a commercial certificate issuer such as Verisign. For more information, see the documentation provided by your certificate authority.

The following tasks require SSL certificates:

- "To Request an SSL Certificate for the Access Manager Load Balancer" on page 95
- "To Install an SSL Certificate on the Access Manager Load Balancer" on page 96
- "To Install a Root CA Certificate on the Access Manager Load Balancer" on page 96
- "To Import the Root CA Certificate for the Access Manager Load Balancer into Authentication UI Server 1" on page 118
- "To Import the Root CA Certificate for the Access Manager Load Balancer into Authentication UI Server 2" on page 119

3.5 Resolving Host Names

There are many ways to resolve host names used in this deployment. For example, you can us a DNS naming service, or you can include entries in a DNS database. For this particular deployment, the following entries were added to the local `host` file on all Unix hosts. The entries were also added to equivalent files on Windows hosts, and on client machines for where browsers are used.

```
xxx.xx.72.122        DirectoryServer-1    DirectoryServer-1.example.com
xxx.xx.72.121        DirectoryServer-2    DirectoryServer-2.example.com
xxx.xx.72.84     AccessManager-1    AccessManager-1.example.com
xxx.xx.72.85     AccessManager-2     AccessManager-2.example.com
xxx.xx.72.120     AuthenticationUI-1        AuthenticationUI-1.example.com
xxx.xx.72.73     AuthenticationUI-2        AuthenticationUI-2.example.com
xxx.xx.72.151   ProtectedResource-1        ProtectedResource-1.example.com
xxx.xx.72.152   ProtectedResource-2        ProtectedResource-2.example.com
xxx.xx.69.246     MessageQueue-1        MessageQueue-1.example.com
xxx.xx.69.247     MessageQueue-2        MessageQueue-2.example.com
xxx.xx.69.14    LoadBalancer-1        LoadBalancer-1.example.com
LoadBalancer-3     LoadBalancer-3.example.com     LoadBalancer-2
LoadBalancer-2.example.com
xxx.xx.69.17     LoadBalancer-4        LoadBalancer-4.example.com
xxx.xx.69.16     LoadBalancer-5        LoadBalancer-5.example.com
LoadBalancer-6     LoadBalancer-6.example.com
```

3.6 Known Issues and Limitations

See Appendix H, "Known Issues and Limitations" for descriptions of problems encountered when implementing the deployment examples. The list will be updated as new information becomes available.

◆ ◆ ◆ CHAPTER 4

Installing and Configuring the Directory Servers

This chapter contains detailed instructions for the following tasks:

4.1 Installing Two Directory Servers

Use the following as your checklist for installing the Directory Servers:

1. Install Directory Server 1.
2. Install Directory Server 2.
3. Create a New Data Instance in Directory Server 1.
4. Create a New Data Instance in Directory Server 2.

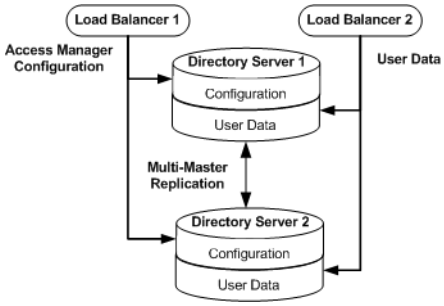

FIGURE 4–1 Directory Servers Configured for Multi-Master Replication

The Java ES installer must be mounted on the host computer system where you will install Directory Server. See the section "To Download and Unpack the Java Enterprise System 2005Q4 Installer""3.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer" on page 32 in this document.

▼ To Install Directory Server 1

1 As a root user, log in to the host DirectoryServer–1.

2 Start the installer with the `nodisplay` option. Example:

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

3 When prompted, provided the following information:

`Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>`	Press Enter.
`<Press ENTER to display the Software License Agreement>`	Press Enter.
`Have you read, and do you accept, all of the terms of the preceding Software License Agreement?`	Enter **`y`**.
`Please enter a comma separated list of languages you would like supported with this installation`	Enter **`8`** to select "English only."
`Enter a comma separated list of products to install, or press R to refresh the list.`	Enter **`6,20`**. Be sure you've specified Sun Java System Administration Server 5 2005Q4 and Sun Java System Directory Server 5 2005Q4.
`Press "Enter" to Continue or Enter a comma separatedlist of products to deselect.`	Press Enter.
`Enter 1 to upgrade these shared components and 2 to cancel.`	If upgrades are required, enter **`1`** to upgrade shared components.
`Enter the name of the target installation directory for each product:`	Accept the default value for each product.
`System ready for installation...`	Enter **`1`** to continue.
`Select Type of Configuration`	Enter **`1`** to configure now.
`Enter Host Name [DirectoryServer-1]`	Accept the default value.
`Enter DNS Domain Name [example.com]`	Accept the default value.
`Enter IP Address [10.5.82.207]`	Accept the default value.
`Enter Server admin User ID [admin]`	Accept the default value.

`Enter Admin User's Password (Password cannot be less than 8 characters)`	For this example, enter **`d1r4dmin`**.
`Confirm Admin User's Password []`	Enter the same password again.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Enter Server Admin ID [admin]`	Accept the default value.
`Enter Admin User's Password (At least 8 characters long)`	For this example, enter **`d1r4dmin`**.
`Retype Password []`	Enter the same password again.
`Enter Directory Manager DN [cn=Directory Manager]`	Accept the default value.
`Enter Directory Manager's Password (At least 8 characters long)`	For this example, enter **`d1rm4n4ger`**.
`Retype Password []`	Enter the same password again.
`Directory Server Root [/var/opt/mps/serverroot]`	Accept the default value.
`Enter Server Identifier [DirectoryServer-1]`	Enter **`ds-config`**.
`Enter Server Port [390]`	Enter **`1390`**.
`Enter a valid Suffix [example.com]`	Enter `dc=example,dc=com`.
`Enter Administration Domain [example.com]`	Accept the default value.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`This server's configuration can be stored in this new directory server or in another previously prepared configuration server.`	Enter **`1`** to choose "The new instance will be the configuration directory server."
`This server can store its own user data and group data, or it can access user data and group data from another instance of directory server.`	Enter **`1`** to store data in the new directory server.
`The new directory server can be populated with sample or real data.`	Enter **`4`** to choose "Populate with no data."
`Do you wish to disable Schema Checking when importing data?`	Enter **`n`**.

`Enter the Server Root [/var/opt/mps/serverroot]`	Accept the default value.
`Enter the Administration Port [390]`	Enter `1391`.
`Enter the Administration Domain [example.com]`	Accept the default value.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Enter Administration ID for Configuration Server Administration ID[admin]`	Accept the default value.
`Enter the admin Password []`	For this example, enter **`d1r4dmin`**.
`Enter the Configuration Directory Host [DirectoryServer-1.example.com]`	Accept the default value.
`Enter the Configuration Directory Port [1390]`	Accept the default value.
`Ready to Install. The following components will be installed: Directory Server Preparation Tool Directory Server 5 Administration Server`	Enter **`1`** to install now.

4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:

```
# cd /var/sadm/install/logs
```

```
# tail –f Java_Enterprise_System_install.B xxxxxx
```

5 Upon successful installation, enter `!` to exit.

6 Verify that Directory Server was successfully installed.

a. As a root user, log into the host DirectoryServer–1.

b. Start the Directory Server.

```
# cd /var/opt/mps/serverroot/slapd-ds-config
# ./stop-slapd; ./start-slapd
```

c. Use the `tail` command to monitor the Directory Server error log and see that the server successfully starts up.

```
# tail -50 logs/errors
```

d. Use the `netstat` command to verify that the Directory Server port is open and listening.

```
# netstat -an | grep 1390
* 1390            *.*            0            0 49152            0 LISTEN
```

e. Start the Administration Server that manages Directory Server.

```
 cd /var/opt/mps/serverroot
./stop-admin; ./start-admin
```

Installation is successful if the Administration Server displays a start-up message.

f. Use the `netstat` command to verify that the Administration Server port is open and listening.

```
# netstat -an | grep 1391
* 1391            *.*            0            0 49152            0 LISTEN
```

▼ To Install Directory Server 2

1 As a root user, log in to the host DirectoryServer–2.

2 Start the installer with the `nodisplay` option. Example:

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

3 When prompted, provided the following information:

`Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>`	Press Enter.
`<Press ENTER to display the Software License Agreement>`	Press Enter.
`Have you read, and do you accept, all of the terms of the preceding Software License Agreement?`	Enter **`y`**.
`Please enter a comma separated list of languages you would like supported with this installation`	Enter **`8`** to select "English only."
`Enter a comma separated list of products to install, or press R to refresh the list.`	Enter **`6,20`**. Be sure you've specified Sun Java System Administration Server 5 2005Q4 and Sun Java System Directory Server 5 2005Q4.

`Press "Enter" to Continue or Enter a comma separatedlist of products to deselect.`	Press Enter.
`Enter 1 to upgrade these shared components and 2 to cancel.`	If upgrades are required, enter **`1`** to upgrade shared components.
`Enter the name of the target installation directory for each product:`	Accept the default value for each product.
`System ready for installation...`	Enter **`1`** to continue.
`Select Type of Configuration`	Enter **`1`** to configure now.
`Enter Host Name [DirectoryServer-2]`	Accept the default value.
`Enter DNS Domain Name [example.com]`	Accept the default value.
`Enter IP Address [10.5.82.207]`	Accept the default value.
`Enter Server admin User ID [admin]`	Accept the default value.
`Enter Admin User's Password (Password cannot be less than 8 characters)`	For this example, enter **`d1r4dmin`**.
`Confirm Admin User's Password []`	Enter the same password again.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Enter Server Admin ID [admin]`	Accept the default value.
`Enter Admin User's Password (At least 8 characters long)`	For this example, enter **`d1r4dmin`**.
`Retype Password []`	Enter the same password again.
`Enter Directory Manager DN [cn=Directory Manager]`	Accept the default value.
`Enter Directory Manager's Password (At least 8 characters long)`	For this example, enter **`d1rm4n4ger`**.
`Retype Password []`	Enter the same password again.
`Directory Server Root [/var/opt/mps/serverroot]`	Accept the default value.
`Enter Server Identifier [DirectoryServer-2]`	Enter **`ds-config`**.
`Enter Server Port [390]`	Enter **`1390`**.
`Enter a valid Suffix [example.com]`	Enter `dc=example,dc=com`.

`Enter Administration Domain [example.com]`	Accept the default value.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`This server's configuration can be stored in this new directory server or in another previously prepared configuration server.`	Enter **1** to choose "The new instance will be the configuration directory server."
`This server can store its own user data and group data, or it can access user data and group data from another instance of directory server.`	Enter **1** to store data in the new directory server.
`The new directory server can be populated with sample or real data.`	Enter **4** to choose "Populate with no data."
`Do you wish to disable Schema Checking when importing data?`	Enter **n**.
`Enter the Server Root [/var/opt/mps/serverroot]`	Accept the default value.
`Enter the Administration Port [390]`	Enter `1391`.
`Enter the Administration Domain [example.com]`	Accept the default value.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Enter Administration ID for Configuration Server Administration ID[admin]`	Accept the default value.
`Enter the admin Password []`	For this example, enter **`d1r4dmin`**.
`Enter the Configuration Directory Host [DirectoryServer-2.example.com]`	Accept the default value.
`Enter the Configuration Directory Port [1390]`	Accept the default value.

`Ready to Install.`
`The following components will be installed:`
`Directory Server Preparation Tool`
`Directory Server 5`
`Administration Server`
	Enter **1** to install now.

4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:

```
# cd /var/sadm/install/logs
```

```
# tail –f Java_Enterprise_System_install.B xxxxxx
```

5 Upon successful installation, enter ! to exit.

6 Verify that Directory Server was successfully installed.

a. Log in as a root user to DirectoryServer–2.

b. Start the Directory Server.

```
# cd /var/opt/mps/serverroot/slapd-ds-config
# ./stop-slapd; ./start-slapd
```

c. Use the `tail` command to monitor the Directory Server error log and verify that the server successfully starts up.

```
# tail -50 logs/errors
```

d. Use the `netstat` command to verify that the Directory Server port is open and listening.

```
# netstat -an | grep 1390
* 1390            *.*            0            0 49152            0 LISTEN
```

e. Start the Administration Server that manages Directory Server.

```
 cd /var/opt/mps/serverroot
./stop-admin; ./start-admin
```

Installation is successful if the Administration Server displays a start-up message.

f. Use the `netstat` command to verify that the Administration Server port is open and listening.

```
# netstat -an | grep 1391
* 1391            *.*            0            0 49152            0 LISTEN
```

▼ To Create a New Data Instance in Directory Server 1

Create a new data instance for storing the Access Manager configuration data. This ensures that if you ever have to uninstall or restore Access Manager configuration, the Directory Server configuration remains untouched and will not have to be restored.

1 As a root user, log in to host DirectoryServer-1.

Set the X window display variable, and start the Directory Server console.

```
# cd /var/opt/mps/serverroot/
# export DISPLAY=DirectoryServer-1.example.com:1
# ./startconsole &
```

2. **Log in to the Directory Server 1 console using the following information:**

Username	**cn=Directory Manager**
Password	**d1rm4n4ger**
Administration URL	**http://DirectoryServer-1.example.com:1391**

3. **In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.**

4. **Right-click on Server Group, and choose "Create an instance of Sun Directory Server."**

5. **In the Create New Instance dialog box, provide the following information:**

Server identifier:	Enter **am-config**.
Network port:	Enter **1389**.
Base suffix:	Enter **o=example.com**.
Directory Manager DN:	Enter **cn=Directory Manager**
Password:	For this example, enter **d1rm4n4ger**.
Confirm Password:	Enter the same password to confirm it.
Server Runtime (UNIX) user ID:	Enter **nobody**.

6. **Click OK, and then close the status window.**

7. **Verify that the new Directory Server instance named `am-config` successfully starts up .**

   a. **Log in as a root user to DirectoryServer-1.**

   b. **Start the new data Directory Server instance.**

```
# cd /var/opt/mps/serverroot/slapd-am-config
# ./stop-slapd; ./start-slapd
```

   c. **Use the `tail` command to monitor the Directory Server error log and see that the server starts up successfully.**

```
# tail –f logs/errors
```

▼ To Create a New Data Instance in Directory Server 2

1 **As a root user, log into host DirectoryServer–2.**

Set the X window display variable, and start the Directory Server console.

```
# cd /var/opt/mps/serverroot/
# export DISPLAY=DirectoryServer-2.example.com:1
# ./startconsole &
```

2 **Log in to the Directory Server 2 console using the following information:**

Username	**cn=Directory Manager**
Password	**d1rm4n4ger**
Administration URL	**http://DirectoryServer-2.example.com:1391**

3 **In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see Server Group item.**

4 **Right-click on Server Group, and choose "Create an instance of Sun Directory Server."**

5 **In the Create New Instance dialog box, provide the following information:**

Server identifier:	Enter **am-config**.
Network port:	Enter **1389**.
Base suffix:	Enter **o=example.com**.
Directory Manager DN:	Enter **cn=Directory Manager**
Password:	For this example, enter **d1rm4n4ger**.
Confirm Password:	Enter the same password to confirm it.
Server Runtime (UNIX) user ID:	Enter **root**.

6 **Click OK, and then close the status window.**

7 **Verify that the new Directory Server instance named** `am-config` **successfully starts up .**

a. **As a root user, log into host DirectoryServer–2.**

b. **Start the new data Directory Server instance.**

```
# cd /var/opt/mps/serverroot/slapd-am-config
# ./stop-slapd; ./start-slapd
```

c. Use the `tail` command to monitor the Directory Server error log and see that the server starts up successfully.

```
# tail –f logs/errors
```

4.2 Enabling Multi-Master Replication

In this procedure you enable multi-master replication (MMR) between two directory masters. Then you use the data and schema from the first directory master to initialize the second directory master. When you're finished, you will have two Directory Servers, and each will contain two instances. The instance named `ds-config` stores Directory Server administration configuration. The instance named `am-config` stores the user data and Access Manager configuration.

On each Directory Server, the `ds-config` instance is a local configuration instance. Do *not* replicate this instance to other host systems. On each Directory Server, the `am-config` instance is the directory data instance. You enable the `am-config` instance for MMR with its counterpart on the other Directory Server host.

Use the following as your checklist for enabling multi-master replication:

1. Enable Multi-Master Replication on Directory Server 1.
2. Enable Multi-Master Replication on Directory Server 2.
3. Create Replication Agreements on Directory Server 1.
4. Create Replication Agreements on Directory Server 2.
5. Initialize the Master Replica

▼ To Enable Multi-Master Replication on Directory Server 1

1 On Directory Server 1, start the Directory Server console.

```
# cd /var/opt/mps/serverroot/
# ./startconsole &
```

2 Log in to the Directory Server 1 console using the following information:

Username	**`cn=Directory Manager`**
Password	**`d1rm4n4ger`**
Administration URL	**`http://DirectoryServer-1.example.com:1391`**

3. **In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.**

4. **Click to expand the Server Group.**

   You should see three items: an Administration Server, a Directory Server (`am-config`), and a Directory Server (`ds-config`).

5. **Double-click the instance name `Directory Server (am-config)` to display the console for managing the instance `am-config`.**

6. **Click the Configuration tab and navigate to the Replication pane.**

   a. **Expand the Data node.**

   b. **Expand the node for the suffix you want to be a master replica.**

      In this example, double-click the suffix `o=example.com`.

   c. **Click Replication.**

7. **Click the "Enable replication" button to start the Replication Wizard.**

8. **Select Master Replica, and then click Next to continue.**

9. **Enter a Replica ID, and then click Next.**

   For this example, when enabling replication on DirectoryServer-1, assign the number 11.

10. **If you have not already been prompted to select the change log file, you are prompted to select one now.**

    The default change log file is shown in the text field. If you do not wish to use the default, type in a filename for the change log, or click Browse to display a file selector. If the change log has already been enabled, the wizard will skip this step.

11. **If you have not already been prompted to enter and confirm a password for the default replication manager, you are prompted now.**

    The replication manager is not used in the case of single-master replication, but you must still enter a password to proceed. For this example, enter **`replm4n4ger`**.

    a. **Click Next.**

    The Replication Wizard displays a status message while updating the replication configuration.

12. **Click Close when replication is finished.**

▼ To Enable Multi-Master Replication on Directory Server 2

1 **On Directory Server 2, start the Directory Server console.**

```
# cd /var/opt/mps/serverroot/
# ./startconsole &
```

2 **Log in to the Directory Server 2 console using the following information:**

Username	**`cn=Directory Manager`**
Password	**`d1rm4n4ger`**
Administration URL	**`http://DirectoryServer-2.example.com:1391`**

3 **In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.**

4 **Click to expand the Server Group.**

You should see three items: an Administration Server, a Directory Server (`am-config`), and a Directory Server (`ds-config`).

5 **Double-click the instance name `Directory Server (am-config)` to display the console for managing the instance `am-config`.**

6 **Click the Configuration tab and navigate to the Replication pane.**

a. **Expand the Data node.**

b. **Expand the node for the suffix you want to be a master replica.**

In this example, double-click the suffix `o=example.com`.

c. **Click Replication.**

7 **Click the "Enable replication" button to start the Replication Wizard.**

8 **Select Master Replica, and then click Next to continue.**

9 **Enter a Replica ID, and then click Next.**

For this example, when enabling replication on DirectoryServer-2, assign the number 22.

10 **If you have not already been prompted to select the change log file, you are prompted to select one now.**

The default change log file is shown in the text field. If you do not wish to use the default, type in a filename for the change log, or click Browse to display a file selector. If the change log has already been enabled, the wizard will skip this step.

11 **If you have not already been prompted to enter and confirm a password for the default replication manager, you are prompted now.**

The replication manager is not used in the case of single-master replication, but you must still enter a password to proceed. For this example, enter **`replm4n4ger`** .

a. **Click Next.**

The Replication Wizard displays a status message while updating the replication configuration.

12 **Click Close when replication is finished.**

▼ To Create Replication Agreements on Directory Server 1

1 **On DirectoryServer-1, in the Directory Server console, display the general properties for the Directory Server instance named** `am-config` **.**

Navigate through the tree in the left panel to find the Directory Server instance named `am-config`, and click on the instance name to display its general properties.

2 **Click the Open button to display the console for managing the** `am-config` **instance.**

3 **Click the Configuration tab and navigate to the Replication pane.**

a. **Expand the Data node.**

b. **Expand the node for the suffix you want to be a master replica.**

In this example, double-click the suffix `o=example.com`.

c. **Click Replication.**

4 **Click the New button.**

5 **In the Replication Agreement dialog box, click the Other button.**

6 **In the Remote Server dialog box, provide the following information, and then click OK.**

Host	`DirectoryServer-2.example.com`
Port	`1389`
Secure Port	Leave this box unmarked.

7. **In the Replication Agreement dialog, for the distinguished name (DN) of the replication manager entry on the consumer server, accept the default value.**

   By default, the DN is that of the default replication manager.

8. **For the password of the replication manager, enter `replm4n4ger`.**

9. **(Optional) Provide a description string for this agreement.**

   For this example, enter **`Replication from DirectoryServer-1 to DirectoryServer-2`**.

10. **Click OK when done.**

11. **In the confirmation dialog, click Yes to test the connection to the server and port number.**

    Use the given replication manager and password **`replm4n4ger`**.

    If the connection fails, you will still have the option of using this agreement. For example, the parameters are correct but the server is offline. When you have finished, the agreement appears in the list of replication agreements for this master replica.

▼ To Create Replication Agreements on Directory Server 2

1. **On DirectoryServer-2, in the Directory Server console, display the general properties for the Directory Server instance named `am-config`.**

   Navigate through the tree in the left panel to find the Directory Server instance named `am-config`, and click on the instance name to display its general properties.

2. **Click the Open button to display the console for managing the `am-config` instance.**

3. **Click the Configuration tab and navigate to the Replication pane.**

   a. **Expand the Data node.**

   b. **Expand the node for the suffix you want to be a master replica.**

      In this example, double-click the suffix `o=example.com`.

   c. **Click Replication.**

4 **Click the New button.**

5 **In the Replication Agreement dialog box, click the Other button.**

6 **In the Remote Server dialog box, provide the following information, and then click OK.**

Host	`DirectoryServer-1.example.com`
Port	`1389`
Secure Port	Leave this box unmarked.

7 **In the Replication Agreement dialog, for the distinguished name (DN) of the replication manager entry on the consumer server, accept the default value.**

By default, the DN is that of the default replication manager.

8 **For the password of the replication manager, enter `replm4n4ger`.**

9 **(Optional) Provide a description string for this agreement.**

For this example, enter **`Replication from DirectoryServer-2 to DirectoryServer-1`**.

10 **Click OK when done.**

11 **In the confirmation dialog, click Yes to test the connection to the server and port number.**

Use the given replication manager and password.

If the connection fails, you will still have the option of using this agreement. For example, the parameters are correct but the server is offline. When you have finished, the agreement appears in the list of replication agreements for this master replica.

▼ To Initialize the Master Replica

1 **On DirectoryServer–1, in the Directory Server console, navigate through the tree in the left panel to find the Directory Server instance named `am-config`, and click on the instance name to display its general properties.**

2 **Double-click the instance name `Directory Server (am-config)` in the tree to display the console for managing the data.**

3 **Click the Configuration tab and navigate to the Replication pane.**

   a. **Expand the Data node.**

b. Expand the node for the suffix you want to be a master replica.

In this example, double-click the suffix `o=example.com`.

c. Click Replication.

4 In the list of defined agreements, select the replication agreement corresponding to DirectoryServer-2, the consumer you want to initialize.

5 Click Action > Initialize remote replica.

A confirmation message warns you that any information already stored in the replica on the consumer will be removed.

6 In the Confirmation dialog, click Yes.

Online consumer initialization begins immediately. The icon of the replication agreement shows a red gear to indicate the status of the initialization process.

7 Click Refresh > Continuous Refresh to follow the status of the consumer initialization.

Any messages for the highlighted agreement will appear in the text box below the list.

8 Verify that replication is working properly.

a. Log in to both Directory Server hosts as a root user, and start both Directory Server consoles.

b. Log in to each Directory Server console.

c. In each Directory Server console, enable the audit log on both Directory Server instances.

Go to Configuration > Logs > Audit Log. Check Enable Logging, and then click Save.

d. In separate terminal windows , use the `tail -f` command to watch the audit log files change.

e. On DirectoryServer-1, in the Directory Server console, create a new user entry.

- Go to the Directory tab, and right-click the suffix `o=example`. Then click New > Group. Name the new group People, and then click OK.
- Click People, and then right-click to choose New > User.
- In the Create New User dialog, enter a first name and last name, an then click OK.

Note the user entry is created in the instance audit log. Check to be sure the same entry is also created in on DirectoryServer-2 in the Directory Server instance audit log

f. On DirectoryServer-2, in the Directory Server console, create a new user entry.

- Go to the Directory tab, and right—click the suffix `o=example.com`Click People, and then right-click to choose New > User.
- In the Create New User dialog, enter a first name and last name, an then click OK.

  Note the user entry is created in the instance audit log. Check to be sure the same entry is also created in on DirectoryServer-1 in the Directory Server instance audit log

g. Delete both new user entries in the Directory Server 2 console.

Look in the Directory Server 1 console to verify that both users have been deleted.

4.3 Configuring the Directory Servers Load Balancer

In the following procedures, you configure the load balancer in front of the two Directory Servers. Then you configure the load balancer for simple persistence. When the load balancer is configured for simple persistence, all Access Manager requests sent *within a specified interval* are sent to the same Directory Server for processing. Simple persistence ensures that within the specified interval, no errors or delays occur due to replication time or redirects when retrieving data.

When a request requires information to be written to Directory Server 1, that information is also replicated in Directory Server 2. But the replication takes time to complete. During that time, if a related request is directed by the load balancer to Directory Server 2, the request may fail.

For example, when simple persistence is not configured properly, creating a realm from the Access Manager administration console could fail in the following way. A request for the parent entry creation is routed to Directory Server 1, and a second request to create the subentry is routed to Directory Server 2. But if the parent entry request is not yet fully replicated to Directory Server 2, the subentry request fails. The result is a partially created realm which may not contain all its subentries such as realm administration roles. Simple persistence eliminates this type of error. When persistence is properly configured, both the parent entry request and the subentry request are routed to Directory Server 1. The requests are processed in consecutive order. The parent entry is fully created before the subentry request begins processing.

▼ To Configure Load Balancer 1

Before You Begin

- Contact your network administrator to obtain an available virtual IP address for the load balancer you want to configure.

  You must also know the IP address of the load balancer hardware, the URL for the load balancer login page, and a username and password for logging in to the load balancer application.

Note – The load balancer hardware and software used in the lab facility for this deployment is BIG-IP® manufactured by F5 Networks. If you are using different load balancer software, see the documentation that comes with that product for detailed settings information.

- You must also have ready the IP addresses for Directory Server 1 and Directory Server 2.

  To obtain these IP addresses, on each Directory Server host, run the following command:

  ```
  ifconfig –a
  ```

1 Create a Pool.

A pool contains all the backend server instances.

a. Go to URL for the Big IP load balancer login page.

b. Open the Configuration Utility.

Click "Configure your BIG-IP (R) using the Configuration Utility."

c. In the left pane, click Pools.

d. On the Pools tab, click the Add button.

e. In the Add Pool dialog, provide the following information:

Pool Name	Example: `directoryserver-pool`
Load Balancing Method	Round Robin
Resources	Add the IP address of both Directory Server hosts. In this case, add the IP address and port number for `DirectoryServer-1:1389` and for `DirectoryServer-2:1389`.

f. Click the Done button.

2 Add a Virtual Server.

If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

a. In the left frame, Click Virtual Servers.

b. On the Virtual Servers tab, click the Add button.

c. In the Add a Virtual Server dialog box, provide the following information:

Address xxx.xx.69.14 (for `LoadBalancer-1.example.com`)

Service	`389`
Pool	`directoryserver-pool`

d. Continue to click Next until you reach the Pool Selection dialog box.

e. In the Pool Selection dialog box, assign the Pool (DirectoryServer-POOL) that you have just created.

f. Click the Done button.

3 Add Monitors

Monitors are required for the load balancer to detect the backend server failures.

a. In the left frame, click Monitors.

b. Click the Basic Associations tab.

c. Add an LDAP monitor for the Directory Server 1 node.

Three columns exist on this page: Node, Node Address, and Service. In the Node column, locate the IP address and port number `DirectoryServer–1:1389`. Select the Add checkbox.

d. Add an LDAP monitor for the Directory Server 2 node.

In the Node column, locate the IP address and port number for `DirectoryServer–2:1389` . Select the Add checkbox.

e. At the top of the Node column, in the drop-down list, choose `ldap-tcp` .

f. Click Apply.

4 Configure the load balancer for simple persistence.

Simple persistence returns a client to the same node to which it connected previously. Simple persistence tracks connections based only on the client IP address.

a. In the left frame, click Pools.

b. Click the name of the pool you want to configure.

In this example, directoryserver-pool.

c. Click the Persistence tab.

d. On the Persistence tab, under Persistence Type, select the Simple.

e. Set the timeout interval.

In the Timeout field, enter 300 seconds.

f. Click Apply.

5 Verify the Directory Server load-balancer configuration.

a. Log in as a root user to the host of each Directory Server.

b. On each Directory Server host, use the `tail` command to monitor the Directory Server access log.

```
# cd /var/opt/mps/serverroot/slapd-am-config/logs

# tail -f access
```

You should see connections to the load balancer IP address opening and closing. Example:

```
[12/Oct/2006:13:10:20-0700] conn=54 op=-1 msgId=-1 –
fd=22 slot=22 LDAP connection from xxx.xx.69.18 to xxx.xx.72.33

[12/Oct/2006:13:10:20-0700] conn=54 op=-1 msgId=-1 – closing – B1

[12/Oct/2006:13:10:20-0700] conn=54 op=-1 msgId=-1 – closed.
```

c. Execute the following LDAP search multiple times against the Directory Server load balancer:

```
# cd /var/opt/mps/serverroot/shared/bin/
# ./ldapsearch -h LoadBalancer-1.example.com -p 389 -b "o=example.com"
-D "cn=directory manager" -w d1rm4n4ger "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Make sure the LDAP search operations display in the same Directory Server access log.

d. Stop Directory Server 1, and again perform the following LDAP search against the Directory Server load balancer:

```
# cd /var/opt/mps/serverroot/slapd-am-config
# ./stop
# cd /var/opt/mps/serverroot/shared/bin/
# ./ldapsearch -h LoadBalancer-1.example.com -p 389 -b "o=example.com"
-D "cn=directory manager" -w d1rm4n4ger "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Verify that the Directory Server access entries display in only one Directory Server access log.

You may encounter the following error message:

```
# ./ldapsearch –h LoadBalancer-1.example.com –p 1389 –b “o=example.com“
–D “cn=Directory Manager” –w d1rm4n4ger

ldap_simple_bind: Cant’ connect to the LDAP
server – Connection refused
```

The load balancer may not fully detect that Directory Server 1 is stopped. Or you may have started the search too soon based on the polling interval setting. For example, if the polling interval is set to 10 seconds, you can wait ten seconds to start the search again. Or you can reset the timeout properties to a lower value.

i. Click the Monitors tab, and click the ldap-tcp monitor name.

ii. In the Interval field, set the value to 5.

This tells the load balancer to poll the server every 5 seconds.

iii. In the Timeout field, set the value to 16.

The default is 16 seconds. You can change this number to any value. In this deployment example, the BigIP documentation recommends the value should be at least three times the interval number of seconds plus one second.

iv. Click Apply.

Repeat the LDAP search.

e. Restart the stopped Directory Server 1, and then stop Directory Server 2.

Confirm that the requests are forwarded to the running Directory Server 2.

f. Perform the following LDAP search against the Directory Server load balancer.

```
# cd /var/opt/mps/serverroot/shared/bin/
# ./ldapsearch -h LoadBalancer-1.example.com -p 389 -b "o=example.com"
-D "cn=Directory Manager" -w d1rm4n4ger "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Make sure the directory access entries display in only the one Directory Server access log.

◆ ◆ ◆ CHAPTER 5

Installing and Configuring the Access Manager Servers

This chapter contains detailed instructions for the following tasks:

5.1 Installing Two Access Manager Servers

Use the following as your checklist for installing the Access Manager servers:

1. Install Access Manager 1.
2. Install Access Manager 2.
3. Configure the Access Manager infrastructure to work with multiple instances.
4. Back up the Access Manager configuration in Directory Server.

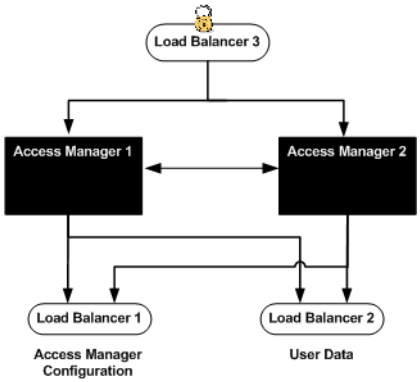

FIGURE 5–1 Two Access Manager Servers and Load Balancer

You must have a CD image of the Sun Java Enterprise System product mounted on the host computer system where you are installing Access Manger. For information on obtaining and mounting the Sun Java Enterprise System, see "3.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer" on page 32 in this document.

▼ To Install Access Manager 1

1 **As a root user, log into host AccessManager-1.**

2 **Unzip the two zip files that comprise the Java Enterprise System installer binaries.**

3 **Start the installer with the `-nodisplay` option.**

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

4 **When prompted, provide the following information:**

`Welcome to the Sun Java(TM) Enterprise System;`
`serious software made simple...`
`<Press ENTER to Continue>`
	Press Enter.

`<Press ENTER to display the Software` `License Agreement>`	Press Enter.
`<--[40%]--[ENTER To Continue]--` `[n To Finish]-->n`	Enter **n**.

`Have you read, and do you accept, all of the terms of the preceding Software License Agreement[No] ?`	Enter **`y`**.
`Please enter a comma separated list of languages you would like supported with this installation [8]`	Enter **`8`** for "English only."
`The following component products are detected on this system. They will appear disabled, "* *", in the following Component Selection Main Menu...`	Press ENTER to continue.
`Enter a comma separated list of products to install, or press R to refresh the list[]:`	Enter **`3,9,12`** to select Web Server, Access Manager, and Message Queue. The Message Queue packages you install now will be used when you implement session failover later in the deployment.
`"Enter" to Continue or Enter a comma separated list of products to deselect... [1]`	Enter **`-20`** to deselect Directory Server.

`Based on product dependencies for your selections, the installer will install:`
`[X] 3. Sun Java(TM) System Web Server 6.1 SP5 2005Q4 (64.61 MB)`
`[X] 9. Sun Java(TM) System Access Manager 7 2005Q4 (27.80 MB)`
`Press "Enter" to Continue...[1]`
	Press Enter.

`[X] 1. Identity Management and Policy Services Core`
`[X] 2. Access Manager Admiistration Console`
`[X] 3. Common Domain Services for Federation Management`
`[X] 4. Access Manager SDK`
 	
`Enter a comma separated list of components to install (or D to install all )[D]`
	Enter **`D`**.

`[X] 1. Identity Management and Policy Services Core`
`[X] 2. Access Manager Admiistration Console`
`[X] 3. Common Domain Services for Federation Management`
`[X] 4. Access Manager SDK`
 	
`Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]`
	Press Enter.

`Warnings - Product Dependency Checks`
 	
`1. Install Sun Java(TM) System Directory Server 5 2005Q4 locally`
`2. Use Sun Java(TM) System Directory Server 5 2005Q4 installed on a remote machine`
 	
`These products can be installed locally or remotely, please choose your option [1]:`
	Enter **2**.

`J2SE(TM) Software Development Kit Upgrade Required`
 	
`1. Automatically update with version on installer disk (recommended)`
 	
`2. Manually upgrade with downloaded version from Sun web site: http://java.sun.comAfter installation, the link /usr/jdk/entsys-j2se refers to the version of J2SE SDK that is compatible with Java Enterprise System.`
 	
`Enter 1 or 2 [1]:`
	Enter **1**.

`The shared components listed below are currently installed. They will be upgraded for compatibility with the products you chose to install...`
 	
`Enter 1 to upgrade these shared components and 2 to cancel [1]`
	Enter **1**.

`Enter the name of the target installation directory for each product:` `Access Manager [/opt] :`	Accept the default value.
`Web Server[/opt/SUNWwbsvr]:`	Accept the default value.
`System ready for installation` `Enter 1 to continue [1]`	Accept the default value.

`1. Configure Now - Selectively override defaults or express through`
`2. Configure Later - Manually configure following installation`
`Select Type of Configuration[1]`
	Enter **1** to configure now.

`The following settings apply to all installed component products.` `Enter Host Name [AccessManager-1]`	Accept the default value.

`Enter DNS Domain Name [example.com]`	Accept the default value.
`Enter IP Address [10.5.82.208]`	Accept the default value.
`Enter Server admin User ID [admin]`	Accept the default value.
`Enter Admin User's Password` `(Password cannot be less than 8characters)`	For this example, enter **`web4dmin`**.
`Confirm Admin User's Password []`	Enter the same password again.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Web Server: Administration` `Enter  Server Admin User ID [admin]`	Accept the default value.
`Enter Admin User's Password []`	For this example, enter **`web4dmin`**.
`Retype Password []`	Enter the same password again.
`Enter Host Name [AccessManager-1.example.com]`	Accept the default value.
`Enter Administration Port [8888]`	Accept the default value.
`Enter Administration Server User ID [root]`	Accept the default value.
`Enter System User ID [webservd]`	Enter **`root`**.
`Enter System Group [webservd]`	Enter **`root`**.
`Enter HTTP Port [80]`	Enter **`1080`**.
`Enter content Root [/opt/SUNWwbsvr/docs]`	Accept the default value.
`Do you want to automatically start Web` `Server when system re-starts.(Y/N)[N]`	Accept the default value.
`Access Manager: Administration` `Administrator User ID: amAdmin`	Accept the default value.
`Administrator Password [] :`	For this example, enter **`4m4dmin1`**.
`Retype Password [] :`	Enter the same password again.
`LDAP User ID: amldapuser`	Accept the default value.
`LDAP Password [] :`	For this example, enter **`4mld4puser`**. Much later in the deployment, in a subsequent task, you use this password as the Web Policy Agent "shared secret."
`Retype Password [] :`	Enter the same password again.

`Password Encryption Key [EWDwdXCHs3CZkYs1CfqxTkQfKtORCFCS]:`	Accept the default value and make note of this key string. You will need it when you install Access Manager 2.
`Install type (Realm/Legacy) Mode [Legacy] : realm`	Enter **`Realm`**.
`Access Manager: Web Container 1. Sun Java System Application Server 2. Sun Java System Web Server Select the container to deploy the component and hit enter key [2]`	Enter **`2`**.
`Access Manager: Sun Java System Web Server Host Name [AccessManager-1.example.com] :`	Accept the default value.
`Web Server Instance Directory [/opt/SUNWwbsvr/https-AccessManager-1.example.com]:`	Accept the default value.
`Web Server Port [1080] :`	Accept the default value.
`Document Root Directory [/opt/SUNWwbsvr/docs] :`	Accept the default value.
`Secure Server Instance Port [No] :`	Accept the default value.
`Host Name [AccessManager-1.example.com] :`	Accept the default value.
`Services Deployment URI [amserver] :`	Accept the default value.
`Common Domain Deployment URI [amcommon] :`	Accept the default value.
`Cookie Domain (Assure it is not a top level domain) [.example.com] :`	Accept the default value.
`Password Deployment URI [ampassword] :`	Accept the default value.
`Access Manager: Directory Server Information Directory Server Host [] :`	Enter **`DirectoryServer-1.example.com`**.
`Directory Server Port [] :`	Enter **`1389`**. This is the port number you entered for the data instance of Directory Server.
`Directory Root Suffix [dc=example,dc=com] :`	Enter **`o=example.com`**
`Directory Manager DN [cn=Directory Manager]: <`	Accept the default value.

`Directory Manager Password [] :`	For this example, enter **`d1rm4n4ger`**.
`Is Directory Server provisioned with user data [No] :`	Accept the default value `No`.

`1. Install`
`2. Start Over`
`3. Exit Installation`
`What would you like to do [1] ?`
	First, see the next numbered (Optional) step.
	When you're ready to install, enter **`1`** to start the installation.

5 (Optional) During installation, you can monitor the log to watch for installation errors. Example:

```
# cd /var/sadm/install/logs
```

```
# tail –f Java_Enterprise_System_install.B xxxxxx
```

6 Upon successful installation, enter `!` to exit.

7 Start the Access Manager Web Server.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com
```

```
# ./stop; # ./start
```

8 Verify that Access Manager has been installed successfully.

a. Go to the Access Manager login URL:

`http://AccessManager-1.example.com:1080/amserver/console`

b. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

You should be able to log in successfully and to navigate to various areas of the console with no error messages.

Troubleshooting If you have configured everything so far according to these instructions, and the following error message is displayed "No such Organization found," it is probably due to the mixed— case Access Manager host names used in this deployment example. For example, the host name `AccessManager-1.example.com` includes both upper and lower case letters. For more detailed information, see Appendix H, "Known Issues and Limitations".

▼ To Install Access Manager 2

Before You Begin You must have a CD image of the Sun Java Enterprise System product mounted on the host computer system where you are installing Access Manger. For information on obtaining and mounting the Sun Java Enterprise System, see "3.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer" on page 32 in this document.

1 As a root user, log in to host AccessManager-2.

2 Unzip the two zip files that comprise the Java Enterprise System installer binaries.

3 Start the installer with the `-nodisplay` option.

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

4 When prompted, provide the following information:

`Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>`	Press Enter.
`<Press ENTER to display the Software License Agreement>`	Press Enter.
`<-[40%]-[ENTER To Continue]-- [n To Finish]-->n`	Enter **`n`**.
`Have you read, and do you accept, all of the terms of the preceding Software License Agreement[No] ?`	Enter **`yes`**.
`Please enter a comma separated list of languages you would like supported with this installation [8]`	Enter **`8`** for "English only."
`The following component products are detected on this system. They will appear disabled, "* *", in the following Component Selection Main Menu...`	Press ENTER to continue.
`Enter a comma separated list of products to install, or press R to refresh the list[]:`	Enter **`3,9, 12`** to select Web Server, and Access Manager, and Message Queue. The Message Queue packages you install now will be used when you implement session failover later in the deployment.

Press"Enter" to Continue or Enter a comma separated list of products to deselect... [1]	Enter **-20** to deselect Directory Server.
Based on product dependencies for your selections, the installer will install: [X] 3. Sun Java(TM) System Web Server 6.1 SP5 2005Q4 (64.61 MB) [X] 9. Sun Java(TM) System Access Manager 7 2005Q4 (27.80 MB) Press "Enter" to Continue...[1]	Press Enter.
[X] 1. Identity Management and Policy Services Core [X] 2. Access Manager Admiistration Console [X] 3. Common Domain Services for Federation Management [X] 4. Access Manager SDK Enter a comma separated list of components to install (or D to install all)[D]	Enter **D**.
[X] 1. Identity Management and Policy Services Core [X] 2. Access Manager Admiistration Console [X] 3. Common Domain Services for Federation Management [X] 4. Access Manager SDK Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]	Press Enter.
Warnings - Product Dependency Checks 1. Install Sun Java(TM) System Directory Server 5 2005Q4 locally 2. Use Sun Java(TM) System Directory Server 5 2005Q4 installed on a remote machine These products can be installed locally or remotely, please choose your option [1]:	Enter **2**.

J2SE(TM) Software Development Kit Upgrade Required 1. Automatically update with version on installer disk (recommended) 2. Manually upgrade with downloaded version from Sun web site: http://java.sun. comAfter installation, the link /usr/jdk/entsys-j2se refers to the version of J2SE SDK that is compatible with Java Enterprise System. Enter 1 or 2 [1]:	Enter **1**.
The shared components listed below are currently installed. They will be upgraded for compatibility with the products you chose to install... Enter 1 to upgrade these shared components and 2 to cancel [1]	Enter **1**.
Enter the name of the target installation directory for each product: Access Manager [/opt] :	Accept the default value.
Web Server[/opt/SUNWwbsvr]:	Accept the default value.
System ready for installation Enter 1 to continue [1]	Accept the default value.
1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration[1]	Enter **1** to configure now.
The following settings apply to all installed component products. Enter Host Name [AccessManager-2]	Accept the default value.
Enter DNS Domain Name [example.com]	Accept the default value.
Enter IP Address [10.5.82.208]	Accept the default value.
Enter Server admin User ID [admin]	Accept the default value.
Enter Admin User's Password (Password cannot be less than 8 characters)	For this example, enter **web4dmin**.

`Confirm Admin User's Password []`	Enter the same password again.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Web Server: Administration` `Enter  Server Admin User ID [admin]`	Accept the default value.
`Enter Admin User's Password []`	For this example, enter **`web4dmin`**.
`Retype Password []`	Enter the same password again.
`Enter Host Name [AccessManager-2.example.com]`	Accept the default value.
`Enter Administration Port [8888]`	Accept the default value.
`Enter Administration Server User ID [root]`	Accept the default value.
`Enter System User ID [webservd]`	Enter **`root`**.
`Enter System Group [webservd]`	Enter **`root`**.
`Enter HTTP Port [80]`	Enter **`1080`**.
`Enter content Root [/opt/SUNWwbsvr/docs]`	Accept the default value.
`Do you want to automatically start Web` `Server when system re-starts.(Y/N)[N]`	Accept the default value.
`Access Manager: Administration` `Administrator User ID: amAdmin`	Accept the default value.
`Administrator Password [] :`	For this example, enter **`4m4dmin1`**.
`Retype Password [] :`	Enter the same password again.
`LDAP User ID: amldapuser`	Accept the default value.
`LDAP Password [] :`	For this example, enter **`4mld4puser`**. Much later in the deployment, in a subsequent task, you use this password as the Web Policy Agent "shared secret."
`Retype Password [] :`	Enter the same password again.
`Password Encryption Key` `[JSIodCIOSxks3CHISjs4CHYpw0ejfk]:`	This password encryption key must be identical to the key that was generated and entered when you installed Access Manager 1. In this deployment example, the string is `EWDwdXCHs3CZkYs1CfqxTkQfKtORCFCS`

`Install type (Realm/Legacy) Mode` `[Legacy] : realm`	Enter **`Realm`**.

`Access Manager: Web Container`
`1. Sun Java System Application Server`
`2. Sun Java System Web Server`
 	
`Select the container to deploy the component`
`and hit enter key [2]`
	Enter **`2`**.

`Access Manager: Sun Java System`
`Web Server Host Name`
`[AccessManager-2.example.com] :`
	Accept the default value.

`Web Server Instance Directory` `[/opt/SUNWwbsvr/https-AccessManager-2.example.com]:`	Accept the default value.
`Web Server Port [1080] :`	Accept the default value.
`Document Root Directory` `[/opt/SUNWwbsvr/docs] :`	Accept the default value.
`Secure Server Instance Port [No] :`	Accept the default value.
`Host Name [AccessManager-2.example.com] :`	Accept the default value.
`Services Deployment URI [amserver] :`	Accept the default value.
`Common Domain Deployment URI [amcommon] :`	Accept the default value.
`Cookie Domain (Assure it is not a top` `level domain) [.example.com] :`	Accept the default value.
`Password Deployment URI [ampassword] :`	Accept the default value.

`Access Manager: Directory Server`
`Information`
 	
`Directory Server Host [] :`
	Enter **`DirectoryServer-2.example.com`**.

`Directory Server Port [] :`	Enter **`1389`**. This is the port number you entered for the data instance of Directory Server.
`Directory Root Suffix` `[dc=example,dc=com] :`	Enter **`o=example.com`**
`Directory Manager DN` `[cn=Directory Manager]: <`	Accept the default value.
`Directory Manager Password [] :`	For this example, enter **`d1rm4n4ger`**.

`Is Directory Server provisioned with user data [No] :`	Accept the default value `No`.

`1. Install`
`2. Start Over`
`3. Exit Installation`
`What would you like to do [1] ?`
	First, see the next numbered (Optional) step.
	When you're ready to install, enter **`1`** to start the installation.

5 (Optional) During installation, you can monitor the log to watch for installation errors. Example:

```
# cd /var/sadm/install/logs
# tail –f Java_Enterprise_System_install.Bxxxxxx
```

6 Upon successful installation, enter `!` to exit.

7 Start the Access Manager Web Server.

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com
# ./stop
# ./start
```

8 Add the lowercase host name `accessmanager-2.example.com` to the Realm alias list.

This eliminates the need to enter the full path to the user's organization each time you want to log in to Access Manager.

a. Go to the following URL:

`http://AccessManager-1.example.com:1080/amserver/UI/Login?org=example.com`

b. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

c. On the Access Control tab, under Realms, click the `example.com` realm name.

d. On the General tab, under Realm Attributes, in the Add field enter the name `accessmanager-2.example.com` (all lowercase).

e. Click Add, and then click Save.

f. Click "Log Out."

9 **Verify that Access Manager has been installed successfully.**

a. **Go to the Access Manager login URL:**

`http://AccessManager-2.example.com:1080/amserver/console`

b. **Log in to the Access Manager console using the following information:**

Username **`amadmin`**

Password **`4m4dmin1`**

You should be able to log in successfully and to navigate to various areas of the console with no error messages.

Next Steps

Caution – Do not try to log in to the second Access Manager server because the instance is not fully configured to be used yet. Access Manager 2 is enabled in the following procedure.

▼ To Configure the Access Manager Infrastructure to Work with Multiple Instances

In this procedure, you configure both Access Manager 1 and Access Manager 2 to operate as two instances of a single server. All configuration takes place on the Access Manager 1 host. There is no need to repeat the steps on the Access Manager 2 host.

1 **On AccessManager-1, start a new browser, and go to the URL for the Access Manager console.**

Example: `http://AccessManager-1.example.com:1080/amserver/console`

2 **Log in to the Access Manager console using the following information:**

User Name **`amadmin`**

Password **`4m4dmin1`**

3 **On the Access Control tab, under Realm Name, click the top-level realm.**

In this example, the top-level realm is `example`.

4 **On the General tab, under Realm Attributes, add `AccessManager–2.example.com` to the Realms/DNS Aliases list.**

a. **In the Add text field, provide a fully qualified domain name for Access Manager 2.**

Example: `AccessManager-2.example.com`

b. **Click Add.**

c. **In the Add text field, provide the Access Manager 2 host name using all lowercase.**
Example: `accessmanager-2.example.com`

d. **Click Add.**

e. **Click Save.**

5 **Go to Realms > Configuration.**

6 **On the Configuration tab, click System Properties > Platform.**

7 **On the Platform page, add a new instance name.**

a. **Under Instance Name, click New.**

b. **In the New Server Instance page, provide the following information:**
Server **`http://AccessManager-2.example.com:1080`** .
Instance Name **`02`**.

c. **Click OK.**
On the Platform page, you see a new instance created in the Instance Name list.

d. **Click Save.**

8 **Click the Log Out button to log out of the console.**

9 **Verify that both Access Manager servers are configured properly.**

a. **As a root user, log in to host AccessManager-1.**

b. **Restart the Access Manager server by restarting the Web Server.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com
# ./stop; ./start
```

Check for errors on the start-up screen and in the Web Server error log as the server restarts.

c. **As a root user, log in to host AccessManager-2.**

d. **Restart the Access Manager server by restarting the Web Server.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com
# ./stop; ./start
```

Check for errors on the start-up screen and in the Web Server error log as the server restarts.

e. Start a new browser and to go the URL for the other Access Manager server.

Example: `http://AccessManager-2.example.com:1080/amserver/console`

f. Log in as to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

g. If you can log in successfully, close the browser.

If you cannot log in successfully, restart Access Manager 2. Be sure that the Access Manager 2 host can access the Directory Server 1 host.

h. Log out of the Access Manager console.

Troubleshooting When you cannot log in successfully, one way to troubleshoot is to log in using the fully qualified name for the user `amadmin` . If you can authenticate using the fully qualified name, you can focus on issues other than authentication and log in. In the file `/etc/opt/SUNWam/config/AMConfig.properties`, look for the following entry:

```
com.sun.identity.authentication.super.user=uid=amAdmin,ou=People,o=example.com
```

Use the fully qualified User Name `uid=amAdmin,ou=People,o=example.com` to log in.

▼ To Back Up the Access Manager Configuration in Directory Server

Backing up your Access Manager configuration ensures that if you run into problems later in the deployment, you can revert to this configuration without having to re-install Access Manager.

1 On Directory Server 1, in the `slapd-am-config` directory, run the `db2ldif` script.

```
# cd /var/opt/mps/serverroot/slapd-am-config/
# ./stop
# ./db2ldif -n userroot
ldiffile: /var/opt/mps/serverroot/slapd-am-config/ldif/2006_03_14_111537.ldif
[14/Mar/2006:11:15:40 -0800] - export userRoot: Processed 112 entries (31%).
[14/Mar/2006:11:15:41 -0800] - export userRoot: Processed 224 entries (62%).
[14/Mar/2006:11:15:42 -0800] - export userRoot: Processed 338 entries (94%).
[14/Mar/2006:11:15:42 -0800] - export userRoot: Processed 360 entries (100%).
```

2 (Optional) You can create a readme file that describes the contents of the new ldif file.

```
# cd /var/opt/mps/serverroot/slapd-am-config/ldif
# ls
2006_03_14_111537.ldif    Example-Plugin.ldif    Example.ldif
European.ldif    Example-roles.ldif
# cat > README
2006_03_14_111537.ldif: backup after post-am install,
pre-patch application
^D
# ls -l
2006_03_14_111537.ldif  Example-Plugin.ldif
Example.ldif  European.ldif    Example-roles.ldif  README
```

5.2 Applying Service Patch 5

The Access Manager 7 2005Q4 SP5 patch must be copied to the Access Manager host computer system. Patches are available for systems that use the Solaris™ Operating System (Solaris OS) or Linux operation system. You can download the following patches for from SunSolve Online (http://sunsolve.sun.com/).

Solaris OS on SPARC® based systems	http://sunsolve.sun.com/search/document.do?assetkey=1-21-120954-03
Solaris OS on x86 platforms	http://sunsolve.sun.com/search/document.do?assetkey=1-21-120955-03
Linux systems	http://sunsolve.sun.com/search/document.do?assetkey=1-21-120956-03 **Note –** No Linux systems were used in this deployment. For Linux detailed patch instructions, see the Readme file that comes with the patch.

Use the following as your checklist for applying Service Patch 5:

1. Apply Service Patch 5 to Access Manager Server 1.
2. Apply Service Patch 5 to Access Manager Server 2.

▼ To Apply Service Patch 5 to Access Manager Server 1

1 As a root user, log in to host AccessManager-1.

2 Unzip the patch file. Example:

```
# cd /temp
# ls
```

```
120954-05.zip
# unzip 120954-03.zip
```

3 Run the `patchadd` command.

(On Solaris 10) `# patchadd -G /temp/120954-05`

For other platforms, see the Readme file that comes with the patch.

After successful installation ,a draft `amsilent` file is created in `/opt/SUNWam`directory. This `amsilent` is based on `/opt/SUNWam/bin/amsamplesilent` , but with some required parameters set according to the AM config files on this system.

4 Redeploy the Access Manager applications.

For detailed information about the following substeps, see the Release Notes (`120954-05/rel_notes.html`) that come with the patch.

a. In the `amsilent` file, use a text editor to uncomment and modify the value of each password parameter, and verify the accuracy of other parameters in this file.

In the following example, the entries in **`bold`** have been uncommented and modified.

```
# cd opt/SUNWam

# vi amsilent

...
# The following entries contain sample values!
# These should be modified for your specific installation
# and then uncommented (remove the # from the line)
#
SERVER_NAME=AccessManager-1
SEVER_HOST=AccessManager-1.example.com
SERVER_PORT=1080

ADMIN_PORT=8888
DS_HOST=DirectoryServer-1.example.com

DS_DIRMGRPASSWD=d1rm4n4ger
ROOT_SUFFIX="o=example.com"

ADMINPASSWD=4m4dmin1
AMLDAPUSERPASSWD=4mld4puser
COOKIE_DOMAIN=example.com
AM_ENC_PWD=13MRBS4UH1fXNnfp3i/44elABip5CTnk
NEW_OWNER=rootNEW_GROUP=otherPAM_SERVICE_NAME=other
WEB_CONTAINER=WS6
...
```

```
DIRECTORY_MODE=5
DS_PORT=1389
...
```

b. Run the following `amconfig` command:

```
# cd /opt/SUNWam/bin

# ./amconfig -s /opt/SUNWam/amsilent
```

5 Update the Access Manager schema.

a. In the directory where you unzipped the patch files, run the `updateschema.sh` command.

Provide information when prompted. See the following example:

```
# cd /tmp/120954-05
# ./udpateschema.sh
Executing updateschema.sh, the lof file is
/var/opt/SUNWam/logs/AM70Patch.upgrade.schema.03080833
Directory Server fully-qualified hostname (LoadBalancer-1.example.com):
DirectoryServer-1.example.com
Directory manager dn (cn=Directory Manager):
Directory manager password:
Top-Level Administrator DN (uid=amAdmin,ou=People,o=example.com):
Top-Level Adminsitrator password:
loading /etc/opt/SUNWam/accountLockout.ldif.....
modifying entry cn=schema

updateschema.sh done!
```

b. Restart Directory Server 1.

```
# cd /var/opt/mps/serverroot/slapd-am-config
# ./stop; start
```

Check the error log to be sure there are no startup errors.

c. Restart Directory Server 2.

```
# cd /var/opt/mps/serverroot/slapd-am-config
# ./stop; start
```

Check the error log to be sure there are no startup errors.

6 Change the Server Name to Load Balancer 1 in the `serverconfig.xml` file.

This step is necessary because a load balancer is used between the two Access Manager servers.

```
# cd /etc/opt/SUNWam/config
# vi serverconfig.xml
<iPlanetDataAccessLayer>
        <ServerGroup name="default" minConnPool="1" maxConnPool="10">
```

```
                <Server name="Server1" host="LoadBalancer-1.example.com"
                  port="389" type="SIMPLE" />
                <User name="User1" type="proxy">
                        <DirDN>
                                cn=puser,ou=DSAME Users,o=example.com
                        </DirDN>
                        <DirPassword>
                                AQICMvvJ0xQN1lpFwZ9IjTPISL2TOx1yX2N8
                        </DirPassword>
                </User>
                <User name="User2" type="admin">
                        <DirDN>
                                cn=dsameuser,ou=DSAME Users,o=example.com
                        </DirDN>
                        <DirPassword>
                                AQICMvvJ0xQN1lpFwZ9IjTPISL2TOx1yX2N8
                        </DirPassword>
                </User>
                <BaseDN>
                        o=example.com
                </BaseDN>
   </ServerGroup>
</iPlanetDataAccessLayer>
```

Save the file.

7 Verify that the patch was successfully installed.

a. Restart the Access Manager 1 Web Server.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com
# ./stop; ./start
```

b. Use the `version` command to display installed patches.

```
# cd /opt/SUNWam/bin
# ./amadmin --version
Sun Java System Access Manager 7 2005Q4 patch 120954-05
```

c. On AccessManager-1, start a new browser and go to the URL of Access Manager 1.

```
http://AccessManager-1:1080/amserver/console
```

d. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

If you can log in successfully, close the browser.

▼ To Apply Service Patch 5 to Access Manager Server 2

1 As a root user, log in to host AccessManager-2.

2 Unzip the patch file. Example:

```
# cd /temp
# ls
120954-05.zip
# unzip 120954-03.zip
```

3 Run the `patchadd` command.

(On Solaris 10) `# patchadd -G /temp/120954-05`

For other platforms, see the Readme file that comes with the patch.

After successful installation ,a draft `amsilent` file is created in `/opt/SUNWam`directory. This `amsilent` is based on `/opt/SUNWam/bin/amsamplesilent` , but with some required parameters set according to the AM config files on this system.

4 Redploy the Access Manager applications.

For detailed information about the following substeps, see the Release Notes (`120954-05/rel_notes.html`) that come with the patch.

a. In the `amsilent` file, use a text editor to uncomment and modify the value of each password parameter, and verify the accuracy of other parameters in this file.

In the following example, the entries in **`bold`** have been uncommented and modified.

```
# cd opt/SUNWam

# vi amsilent

...
# The following entries contain sample values!
# These should be modified for your specific installation
# and then uncommented (remove the # from the line)
#
SERVER_NAME=AccessManager-2
SEVER_HOST=AccessManager-2.example.com
SERVER_PORT=1080

ADMIN_PORT=8888
DS_HOST=DirectoryServer-2.example.com

DS_DIRMGRPASSWD=d1rm4n4ger
ROOT_SUFFIX="o=example.com"
```

```
ADMINPASSWD=4m4dmin1
AMLDAPUSERPASSWD=4mld4puser
COOKIE_DOMAIN=example.com
AM_ENC_PWD=13MRBS4UH1fXNnfp3i/44elABip5CTnk
NEW_OWNER=rootNEW_GROUP=otherPAM_SERVICE_NAME=other
WEB_CONTAINER=WS6
...
DIRECTORY_MODE=5
DS_PORT=1389
...
```

b. Run the `amconfig` command:

```
# cd /opt/SUNWam/bin

# ./amconfig -s /opt/SUNWam/amsilent
```

5 Update the Access Manager schema.

a. In the directory where you unzipped the patch files, run the `updateschema.sh` command.

Provide information when prompted. See the following example:

```
# cd /tmp/120954-05
# ./udpateschema.sh
Executing updateschema.sh, the lof file is
/var/opt/SUNWam/logs/AM70Patch.upgrade.schema.03080833
Directory Server fully-qualified hostname (LoadBalancer-1.example.com):
DirectoryServer-2.example.com
Directory manager dn (cn=Directory Manager):
Directory manager password:
Top-Level Administrator DN (uid=amAdmin,ou=People,o=example.com):
Top-Level Adminsitrator password:
loading /etc/opt/SUNWam/accountLockout.ldif.....
modifying entry cn=schema

updateschema.sh done!
```

b. Restart Directory Server 1.

```
# cd /var/opt/mps/serverroot/slapd-am-config
# ./stop; start
```

Check the error log to be sure there are no startup errors.

c. Restart Directory Server 2.

```
# cd /var/opt/mps/serverroot/slapd-am-config
# ./stop; start
```

Check the error log to be sure there are no startup errors.

6 Change the Server Name to Load Balancer 1 in the `serverconfig.xml` file.

This step is necessary because a load balancer is used between the two Access Manager servers.

```
# cd /etc/opt/SUNWam/config
# vi serverconfig.xml
<iPlanetDataAccessLayer>
        <ServerGroup name="default" minConnPool="1" maxConnPool="10">
            <Server name="Server1" host="LoadBalancer-1.example.com"
              port="389" type="SIMPLE" />
            <User name="User1" type="proxy">
                    <DirDN>
                            cn=puser,ou=DSAME Users,o=example.com
                    </DirDN>
                    <DirPassword>
                            AQICMvvJ0xQN1lpFwZ9IjTPISL2TOx1yX2N8
                    </DirPassword>
            </User>
            <User name="User2" type="admin">
                    <DirDN>
                            cn=dsameuser,ou=DSAME Users,o=example.com
                    </DirDN>
                    <DirPassword>
                            AQICMvvJ0xQN1lpFwZ9IjTPISL2TOx1yX2N8
                    </DirPassword>
            </User>
            <BaseDN>
                    o=example.com
            </BaseDN>
   </ServerGroup>
</iPlanetDataAccessLayer>
```

Save the file.

7 Verify that the patch was successfully installed.

a. Restart the Access Manager 2 Web Server.

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com
# ./stop; ./start
```

b. Use the `version` command to display installed patches.

```
# cd /opt/SUNWam/bin
# ./amadmin --version
Sun Java System Access Manager 7 2005Q4 patch 120954-05
```

c. On AccessManager-2, start a new browser and go to the URL of Access Manager 2.

```
http://AccessManager-1:1080/amserver/console
```

d. Log in to the Access Manager console using the following information:

Username **amadmin**

Password **4m4dmin1**

If you can log in successfully, close the browser.

5.3 Configuring the Access Manager Servers to Run as Non-Root Users

During the Access Manager installation, the installer requires that Access Manager run as a root user. If you want administrators who don't have root permissions to perform any administration tasks on Access Manager, you must reconfigure Access Manager to run as a non-root user.

1. Reconfigure Access Manager 1 to run as a non-root user.
2. Reconfigure Access Manager 2 to run as a non-root user.
3. Reconfigure the Web Server Administration Servers to run as non-root users.

Caution – You must use a port number higher than 1024. If the Web Server port is below 1024, then even after configuring the Access Manager server to run as a non-root user, you still must start Access Manager Web Server in a root shell.

▼ To Reconfigure Access Manager 1 to Run as a Non-Root User

1 As a root user, log into host AccessManager-1.

2 Stop Access Manager 1.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com/
# ./stop
```

3 Stop the Web Server administration server.

```
# cd /opt/SUNWwbsvr/https-admserv/
# ./stop
```

4 Change the "runs as" user ID from `root` to `nobody`.

```
# cd /opt/SUNWwbsvr/
# chown -R nobody:nobody https-AccessManager-1.example.com/* httpacl alias \
/var/opt/SUNWam /etc/opt/SUNWam
# rm  -rf /tmp/https-*
```

5 Edit the magnus.conf file.

It is a good practice to make a backup of this or any other configuration file before making changes to the file.

```
# vi https-AccessManager-1.example.com/config/magnus.conf
```

Change the User property value from `root` to `nobody`.

6 Verify that Access Manager successfully runs as a non-root user.

a. Log in as a root user to the Access Manager host.

b. Start the Access Manager server.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com/
# ./start
```

c. Confirm that the Web Server start process actually runs as `nobody`.

```
# ps -ef | grep SUNWwbsvr
```

d. Start a new browser and go to the Access Manager URL.

Example: `http://AccessManager-1.example.com:1080/amserver/console`

Close the browser if successful.

e. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

If you can log in successfully, close the browser.

▼ To Reconfigure Access Manager 2 to Run as a Non-Root User

1 As a root user, log into host AccessManager-2.

2 Stop Access Manager 2.

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com/
# ./stop
```

3 Stop the Web Server administration server.

```
# cd /opt/SUNWwbsvr/https-admserv/
# ./stop
```

4 Change the "runs as" user ID from `root` to `nobody`.

```
# cd /opt/SUNWwbsvr/
# chown -R nobody:nobody https-AccessManager-2.example.cm/* httpacl alias
/var/opt/SUNWam /etc/opt/SUNWam
# rm  -rf /tmp/https-*
```

5 Edit the magnus.conf file.

```
# vi https-AccessManager-2.example.com/config/magnus.conf
```

Change the User property value from `root` to `nobody`.

6 Verify that Access Manager 2 successfully runs as a non-root user.

a. As a root user, log into host AccessManager-2.

b. Start the Access Manager server.

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com/
# ./start
```

c. Confirm that the Web Server start process actually runs as `nobody`.

```
ps -ef | grep SUNWwbsvr
```

d. Start a new browser and go to the Access Manager URL.

Example: `http://AccessManager-2.example.com:1080/amserver/console` Close the browser if successful.

e. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **4m4dmin1**

If you can log in successfully, close the browser.

To Reconfigure the Web Server Administration Servers to Run as Non-Root Users

In this procedure, you reconfigure the administration server for each of the Web Servers that contain Access Manager. Although this is not required, it's a good practice to run the Access Manager Web Servers and their administration servers as the same non-root user ID. This eliminates permissions problems. For example, if the Access Manager Web Server runs as a non-root user, and its administration server runs as a root user, then files created by the administration server may not be readable by the Access Manager Web Server.

1. **As a root user, log into host AccessManager-1.**

2. **Stop the Web Server administration server by issuing the commands:**

```
# cd /opt/SUNWwbsvr/https-admserv
# ./stop
```

3. **Change the "runs as" user ID from `root` to `nobody`.**

```
# cd /opt/SUNWwbsvr/
# chown -R nobody:nobody https-admserv/* httpacl/ alias
# rm -rf /tmp/https-admserv
```

4. **Edit the `magnus.conf` file.**

   Make a backup of this file before making changes to the file.

```
# vi https-admserv/config/magnus.conf
```

   Change the User property value from `root` to `nobody`.

5. **Verify that the Web Server administration server successfully runs as a non–root user.**

   a. **As a root user, log into host AccessManager-1.**

   b. **Start the Access Manager server:**

```
# cd /opt/SUNWwbsvr/https-admserv/

# ./start
```

   c. **Use `ps` command to confirm the started Web Server process indeed runs as `nobody`.**

```
# ps -ef | grep admserv
```

6. **As a root user, log into host AccessManager-2.**

7. **Stop the Web Server administration server by issuing the commands:**

```
# cd /opt/SUNWwbsvr/https-admserv
# ./stop
```

8. **Change the "runs as" user ID from `root` to `nobody`.**

```
# cd /opt/SUNWwbsvr/
# chown -R nobody:nobody https-admserv/* httpacl/ alias
# rm -rf /tmp/https-admserv
```

9. **Edit the `magnus.conf` file.**

```
# vi https-admserv/config/magnus.conf
```

Change the User property value from `root` to `nobody`.

10. **Verify that the Web Server administration server successfully runs as a non–root user.**

    a. **As a root user, log into host AccessManager-2.**

    b. **Start the Access Manager server:**

```
# cd /opt/SUNWwbsvr/https-admserv/

# ./start
```

    c. **Use `ps` command to confirm the started Web Server process indeed runs as `nobody`.**

```
# ps -ef | grep admserv
```

5.4 Configuring the Access Manager Load Balancer

In this procedure, you configure the Access Manager servers to access the Directory Server through the load balancer. All configuration changes you implement through the Access Manager 1 console will be replicated to Access Manager 2, so there is no need to repeat these steps on the Access Manager 2 console. However, you must also edit XML files in this task. You must manually edit the XML files on Access Manager 1 and on Access Manager 2.

Note – The load balancer hardware and software used in the lab facility for this deployment is BIG-IP® manufactured by F5 Networks. If you are using different load balancer software, see the documentation that comes with that product for detailed settings information.

Use the following as your checklist for configuring the Access Manager load balancer:

1. Configure the Access Manager servers to access the Directory Server load balancer.
2. Verify successful Directory Server load balancing and system failover.
3. Configure the Access Manager load balancer.
4. Verify that the Access Manager load balancer is configured properly.
5. Request an SSL certificate for the Access Manager load balancer.
6. Install a root CA certificate on the Access Manager load balancer.
7. Install an SSL certificate on the Access Manager load balancer.
8. Configure SSL termination on the Access Manager load balancer.

▼ To Configure the Access Manager Servers to Access the Directory Server Load Balancer

1 Go to the Access Manager URL.

`http://AccessManager-1.example.com:1080/amserver/console`

2 Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

3 Click the Configuration tab.

4 Under Authentication, edit the following service configurations. Edit the service configurations to reflect the LDAP server name and port number `LoadBalancer-1.example.com:1389`

Under Authentication, for the following services, change the Primary LDAP server name and port to the load-balancer name and port. In this example, the new name is `LoadBalancer-1.example.com:389` .

a. Under Authentication, click LDAP.

In the Primary LDAP Server list, Add `LoadBalancer-1.example.com:389` and delete the default server from the list. Click Save, and the return to the Configuration tab.

b. Under Authentication, click Membership.

In the Primary LDAP Server list, Add `LoadBalancer-1.example.com:389` and delete the default server from the list. Click Save, and the return to the Configuration tab.

c. Under Authentication, click MSISDN.

In the Primary LDAP Server list, Add `LoadBalancer-1.example.com:389` and delete the default server from the list. Click Save, and the return to the Configuration tab.

d. Under Global Properties, click Policy Configuration.

In the Primary LDAP Server, add `LoadBalancer-1.example.com:389` and delete the default server from the list. Click Save, and the return to the Configuration tab.

5 Edit the following property files on AccessManager–1.

a. Still logged in to the Access Manager server as a root user, use an editor to modify the file `/etc/opt/SUNWam/config/serverconfig.xml.`

Change LDAP serer host name and port number to the fully-qualified name and port number for Load Balancer 1 Example:

```
<iPlanetDataAccessLayer>
                <ServerGroup name="default" miConnPool="1" maxConnPool="10">
                        <Server name="Server1"
                                host="LoadBalancer-1.example.com" port="389"
 type="SIMPLE"/>
...
```

b. Use an editor to modify the file `/etc/opt/SUNWam/config/AMConfig.properties.`

Set the following properties:

- `com.iplanet.am.directory.port=389`
- `com.iplanet.am.directory.host=LoadBalancer-1.example.com`
- `com.sun.am.event.connection.idle.timeout=3`

The connection idle time out value is set to 3 minutes. This value is less than the value for the Firewall 3–to-Load Balancer 1 connection timeout which is 5 minutes in this example. By setting this value to be 3 minutes, the Access Manager server will assume its persistent search connections may be silently dropped by Firewall 3–to-Load Balancer 1. The Access Manager server will re-establish the persistent search connections every 3 minutes. Otherwise, the Access Manager server may forever block on the persistent search because it is not made aware that the TCP connection is dropped silently.

6 **Edit the following property files on AccessManager–2.**

a. **Still logged in to the Access Manager server as a root user, use an editor to modify the file** `/etc/opt/SUNWam/config/serverconfig.xml`.

Change LDAP serer host name and port number to the fully-qualified name and port number for Load Balancer 1. Example:

```
<iPlanetDataAccessLayer>
                <ServerGroup name="default" miConnPool="1" maxConnPool="10">
                        <Server name="Server1"
                                host="LoadBalancer-1.example.com" port="389"
 type="SIMPLE"/>
...
```

b. **Use an editor to modify the file** `/etc/opt/SUNWam/config/AMConfig.properties`.

Set the following properties:

- `com.iplanet.am.directory.port=389`
- `com.iplanet.am.directory.host=LoadBalancer-1.example.com`
- `com.sun.am.event.connection.idle.timeout=3`

7 **Restart both Access Manager servers in order for the changes to take place.**

▼ To Verify Successful Directory Server Load Balancing and System Failover

For each of the Access Manager servers, perform the following steps to confirm its directory accesses are all directed to one and only one Directory Server instance, and that system failover and recover work properly. The following section describes how to perform the sanity check for the first Access Manager instance. Substitute the console URL with that of the second Access Manager instance when you perform the task for the second Access Manager instance.

1 **Confirm that the load balancer is properly configured for simple persistence.**

a. **As a root user, log into host DirectoryServer-1 and host DirectoryServer-2.**

b. **For each server, use the tail command to watch the Directory Server access log.**

```
# tail-f logs/access
```

c. **Start a new browser and go to the Access Manager 1 URL.**

Example: `http://AccessManager-1.example.com:1080/amserver/console`

d. **Log in to the Access Manager console using the following information:**

Username **amadmin**

Password **4m4dmin1**

e. Navigate inside the Access Manager console while paying attention to the Directory Server access log.

In the access log, you should see all directory accesses are directed to one Directory Server instance only, excluding the health check probing from the load balancer device. The navigation should not have any errors. Logout and close the browser if successful.

2 Confirm that Directory Server failover works properly.

a. Shut down Directory Server 1.

b. Start a new browser and go to the Access Manager URL.

Example: `http://AccessManager-1.example.com:1080/amserver/console`

c. Log in to the Access Manager console using the following information:

Username **amadmin**

Password **4m4dmin1**

d. Navigate inside the Access Manager console while paying attention to the Directory Server access logs.

```
# cd /var/opt/mps/serverroot/slapd-data/logs
```

In the access logs, you should see all directory accesses are directed only to Directory Server 2. The navigation should not have any errors. Log out and close the browser if successful.

e. Restart Directory Server 1, and stop Directory Server 2.

f. Start a new browser go to the Access Manager URL.

Example: `http://AccessManager-1.example.com:1080/amserver/console`

g. Log in to the Access Manager console using the following information:

Username **amadmin**

Password **4m4dmin1**

h. Navigate inside the Access Manager console,

Watch the access logs of both Directory Server instances. You should see all directory accesses (excluding health checks by load balancer) are directed to only Directory Server 1. The navigation should not have any errors.

i. Log out and close the browser if successful.

3 Restart Directory Server 2.

Confirm that both Directory Servers are restarted and running.

▼ To Configure the Access Manager Load Balancer

Users internal to your company will access the Access Manager servers through the internal-facing load balancer. The internal-facing load balancer is optional, and enables you to customize an internal-facing login page that is different from the external-facing login page. Users external to your company will first access the Distributed Authentication UI servers, which in turn route requests to the external-facing load balancer. Internal users will access port 90 while External users will access port 9443.

Load Balancer 3 sends the user and agent requests to the server where the session originated. SSL is terminated at Load Balancer 3 before a request is forwarded to the Access Manager Servers. Otherwise the load balancer cannot inspect the traffic for proper routing.

Load Balancer 3 is capable of the following types of load balancing:

Cookie-based	The load balancer makes decisions based on client's cookies. The load balancer looks at the request and detects the presence of a cookie by a specific name. If the cookie is detected in the request, the load balancer routes the request to the specific server to which the cookie has been assigned. If the cookie is not detected in the request, the load balancer balances client requests among the available servers.
IP-based	This is similar to cookie-based load balancing, but the decision is based on the IP address of the client. The load balancer sends requests from a specific client to the same server. So a request from the client will always be processed by the server that last processed the request from that client.
TCP	The load balancer mainstreams session affinity. This means that all requests related to a TCP session, are forwarded to the same server. In this deployment example, Load Balancer 3 forwards all requests from a single client to exactly the same server. When the session is started and maintained by one client, session affinity is guaranteed. This type of load-balancing is applicable to the TCP-based protocols.

Before You Begin Contact your network administrator to obtain two available virtual IP addresses.

Note – The load balancer hardware and software used in the lab facility for this deployment is BIG-IP® manufactured by F5 Networks. If you are using different load balancer software, see the documentation that comes with that product for detailed settings information.

---

1 Create a Pool.

A pool contains all the backend server instances.

a. Go to URL for the Big IP load balancer log in.

b. Open the Configuration Utility.

Click "Configure your BIG-IP (R) using the Configuration Utility."

c. In the left pane, click Pools.

d. On the Pools tab, click the Add button.

e. In the Add Pool dialog, provide the following information:

Pool Name	Example: AccessManager-Pool
Load Balancing Method	Round Robin
Resources	Add all the Access Manager servers IP addresses. In this example, add the IP address and port number for `AccessManager-1:1080` and for `AccessManager-2:1080`.

f. Click the Done button.

2 Configure the load balancer for persistence.

a. In the left pane click Pools.

b. Click the name of the pool you want to configure.

c. Click the Persistence tab.

d. On the Persistence tab, under Persistence Type, select Cookie Hash and set the following Hash Values:

Cookie Name:	**`amlbcookie`**
Offset:	1
Length:	1

e. Click Apply.

3 Add a Virtual Server.

If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

a. In the left frame, Click Virtual Servers.

b. On the Virtual Servers tab, click the Add button.

c. In the Add a Virtual Server dialog box, provide the following information:

Address	`xxx.xx.69.13` (for `LoadBalancer-3.example.com`)
Service	`90`
Pool	`AccessManager-Pool`

d. Continue to click Next until you reach the Pool Selection dialog box.

e. In the Pool Selection dialog box, assign the Pool (AccessManager-Pool) that you have just created.

f. Click the Done button.

4 Add Monitors.

The load balancer has a built-in HTTP monitor that probes the Access Manager TCP port periodically. Successive probing failure indicates the server is down. However, this probing does not address the case where the Access Manager server responds to a TCP connection request, but fails to process any further Access Manager requests because of internal errors such as deadlocks. Access Manager comes with a JSP file `/amserver/isAlive.jsp` to address this challenge. In the following steps, you create a custom monitor that periodically accesses the JSP. If a success response can be obtained, it means not only that Access Manager is responding to TCP connection request, but also that free threads exist to process the request.

a. Click the Monitors tab, and then the click Add button.

In the Add Monitor dialog, provide the following information:

Name:	**`AccessManager-http`**
Inherits From:	Choose **`http`**.

b. Click Next.

In the Configure Basic Properties page, click Next.

c. In the "Configure ECV HTTP Monitor" dialog, in the Send String field, enter the following:

`GET /amserver/isAlive.jsp`

d. In the Destination Address and Service (Alias) page, click Done.

On the Monitors tab, the monitor you just added is now contained in the list of monitors.

e. Click the Basic Associations tab.

Look for the IP address for `AccessManager-1:1080` and `AccessManager-2:1080`.

f. Mark the Add checkbox for AccessManager-1 and AccessManager-2.

g. At the top of the Node column, choose the monitor that you just added, `AccessManager-http`.

h. Click Apply.

▼ To Verify that the Access Manager Load Balancer is Configured Properly

1 Log in as root to the host AccessManager–1.

2 Run the tail command to view the access log.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com/logs
# tail -f access
```

If you see frequent entries similar to this one:

```
xxx.xx.69.18--[12/Oct/2006:13:10:20-0700]
"GET/amserver/isAlive.jsp" 200 118
```

then the custom monitor is configured properly. If you do not see "`GET /amserver/isAlive.jsp`" then you must troubleshoot the load balancer configuration.

3 Log in as root to the host AccessManager-2.

4 Run the tail command to view the access log.

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com/logs
# tail -f access
```

If you see frequent entries similar to this one:

```
xxx.xx.69.18--[12/Oct/2006:13:10:20-0700]
"GET /amserver/isAlive.jsp" 200 118
```

then the custom monitor is configured properly. If you do not see "`GET /amserver/isAlive.jsp`" then you must troubleshoot the load balancer configuration.

5 **Start a new browser and go to the internal-facing load balancer URL.**

Example: `http://LoadBalancer-2.example.com:90/` . Do not supply the `amserver` prefix.

If the browser successfully renders the default Sun Web Server default document root page, close the browser.

▼ To Request an SSL Certificate for the Access Manager Load Balancer

1 **Open a browser, go to the BIG-IP URL:**

`https://is-F5.example.com`

2 **Log in to the BIG-IP console using the following information:**

Username **`username`**

Password **`password`**

3 **Click "Configure your BIG-IP (R) using the Configuration Utility."**

4 **In the left pane, click Proxies.**

5 **Click the Cert-Admin tab.**

6 **On the SSL Certificate Administration page, click the button named "Generate New Key Pair/Certificate Request."**

7 **In the Create Certificate Request page, provide the following information:**

Key Identifier: **`LoadBalancer-3.example.com`**

Organizational Unit Name: **`Deployment`**

Domain Name: **`LoadBalancer-3.example.com`**

Challenge Password: **`password`**

Retype Password: **`password`**

8 **Click the button "Generate Key Pair/Certificate Request."**

On the SSL Certificate Request page, the request is generated in the Certificate Request field.

9 **Copy all the text contained in the Certificate Request field.**

Save the text in a text file to keep it handy for later use.

10 **Send the text of the certificate request to a Certificate Authority of your choice.**

A Certificate Authority is an entity that issues certified digital certificates. VersiSign, Thawte , Entrust, and GoDaddy are just a few examples of Certificate Authority companies. In this deployment example, CA certificates were obtained from OpenSSL. Follow the instructions provided by the Certificate Authority for submitting a certificate request.

▼ To Install a Root CA Certificate on the Access Manager Load Balancer

The root Certificate Authority certificate proves that a Certificate Authority such as VeriSign or Entrus actually issued the digital server certificate you received. You install the root certificate on Load Balancer 3 to ensure that the link between the Load Balancer 3 SSL certificate can be maintained with the issuing company.

1 **In the BIG-IP load balancer console, click Proxies.**

2 **Click the Cert-Admin tab.**

3 **Click the Import link.**

4 **In the Import Type field, choose Certificate, and then click Continue.**

5 **In the Install SSL Certificate page, in the Certificate File field, click Browse.**

6 **In the Choose File dialog, choose Browser.**

Navigate to the file that includes the root CA Certificate, and click Open.

7 **In the Certificate Identifier field, enter `OpenSSL_CA_cert`.**

8 **Click Install Certificate.**

9 **In the Certificate OpenSSL_CA_Cert page, click Return to Certificate Administration.**

The new certificate OpenSSL_CA_Cert is now included in the Certificate ID list.

▼ To Install an SSL Certificate on the Access Manager Load Balancer

1 **Once you've received the SSL certificate from a Certificate Authority, in the BIG-IP load balancer console, click Proxies.**

2 **Click the Cert-Admin tab.**

The key `LoadBalancer-3.example.com` is in the Key List. This was generated in a previous step when you generated a key pair and a certificate request.

3 **In the Certificate ID column, click the Install button for `LoadBalancer-3.example.com`.**

4 **In the Certificate File field, click Browse.**

In the Choose File dialog, navigate to the text file in which you saved the certificate text sent to you by the certificate issuer, and then click Open.

5 **Click Install Certificate.**

6 **In the Certificate LoadBalancer-3.example.com page, click Return to Certificate Administration Information link.**

In the SSL Certificate Administration page, verify that the Certificate ID indicates `LoadBalancer-3.example.com`.

▼ To Configure SSL Termination on the Access Manager Load Balancer

In this deployment example, Secure Socket Layer (SSL) termination at Load Balancer 3 increases the performance at the server level, and simplifies SSL certificate management. Clients will access Load Balancer 3 using SSL-encrypted data. Load Balancer 3 decrypts the data and then sends the unencrypted data on to the Access Manager server. The Access Manager server or Authentication UI server does not have to perform decryption, and the burden on its processor is relieved. Load Balancer 3 then load-balances the decrypted traffic to the appropriate Access Manager server. Finally, Load Balancer 3 encrypts the responses from server, and sends encrypted responses to the client.

Load Balancer 3 sends the user and agent requests to the server where the session originated. SSL is terminated at Load Balancer 3 before a request is forwarded to the Access Manager Servers. Otherwise the load balancer cannot inspect the traffic for proper routing.

In this deployment example, you set up a proxy server using BIG-IP™ hardware and software.

1 **Configure the new proxy service.**

a. **Log in to the BIG-IP load balancer using the following information:**

Username **`username`**

Password **`password`**

b. Click the link "Configure your BIG-IP using the Configuration Utility."

c. In the load balancer console, in the left pane, click Proxies.

d. On the Proxies tab, click Add.

e. In the Add Proxy dialog, provide the following information:

Proxy Type:	Check the SSL checkbox.
Proxy Address:	**`xxx.xx.69.14`** (The IP address of Load Balancer 3, the Access Manager server load balancer.)
Proxy Service:	**`9443`** (The port number of the new proxy you are setting up.)
Destination Address:	**`xxx.xx.69.14`**
Destination Service:	**`90`**
Destination Target:	Choose **`Local Virtual Server`**.
SSL Certificate:	Choose **`LoadBalancer-3.example.com`**.
SSL Key:	Choose **`LoadBalancer-3.example.com`**.
Enable ARP:	Check this checkbox.

f. Click Next.

g. In the Rewrite Redirects field, choose `Matching`.

h. Click Done.

The new proxy server is now added to the Proxy Server list.

2 Verify that you can access the Access Manager server using the new proxy server port number.

a. Open a browser, and go to the following URL:

```
https://LoadBalancer-3.example.com:9443/index.html
```

Tip – A message may be displayed indicating that the Access Manager server doesn't recognize the certificate issuer. When this happens, install the root Certificate Authority certificate in the browser so that the browser recognizes the certificate issuer. See your browser's online help system for information on installing a root CA certificate.

---

i. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **4m4dmin1**

If you can successfully log in to Access Manager 1, then the SSL certificate is installed properly and proxy service is configured properly.

b. Log out of Access Manager, and close the browser.

5.5 Importing the Root CA Certificate into the Access Manager Web Servers

Use the following as your checklist for importing the root CA certificate into the Access Manager Web Servers:

1. Import the root CA certificate into the Access Manager 1 Web Server.
2. Modify the `AMConfig.properties` file.
3. Import the root CA certificate into the Access Manager 2 Web Server.
4. Modify the `AMConfig.properties` file.

▼ To Import the Root CA Certificate into the Access Manager 1 Web Server

1 To to the Web Server administration URL:

`http://AccessManager-1.example.com:8888/https-admserv/bin/index`

2 Log in to the Web Server console using the following information:

User name: **admin**

Password: **web4d4min**

3 On the Servers tab, select the server `AccessManager-1.example.com`, and then click Manage.

4 Click on the Security tab, and then initialize the Trust Database by providing the following information:

Database Password: password

Password (again): password

Click OK.

5 In the left frame, click Install Certificate. In the Install a Server Certificate page, provide the following information:

Certificate for:	Choose Trusted Certificate Authority (CA)
Message text (with headers):	Choose this option, and then paste into the text box the root certificate you received from the CA. "To Request an SSL Certificate for the Distributed Authentication UI Load Balancer" on page 127. The root certificate will look similar to this:

```
-----BEGIN CERTIFICATE-----
UbM77e50M63v1Z2A/5O5MA0GCSqGSIb3DQEOBAU
AMF8xCzAJBgNVBAYTAlVTMSAwHgYDVQQKExdSU0
EgRGF0YSBTZWN1cml0eSwgSW5jLjEuMCwGA1UEC
xMlU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAeFw0wMTA4MDIwMDAwMDBaFw0
wMzA4MDIyMzU5NTlaMIGQMQswCQYDVQQGEwJVUz
ERMA8GA1UECBMIVmlyZ2luaWExETAPBgNVBAcUC
FJpY2htb25kMSAwHgYDVQQKFBdDYXZhbGllciBU
ZWxlcGhvYm9uZGluZy5jYXZ0ZWwuY29tMIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8x/1dxo
2YnblilQLmpiEziOqb7ArVfI1ymXo/MKcbKjnY2
-----END CERTIFICATE REQUEST-----
```

Click OK.

6 On the "Add Trusted CA Certificate page," click "Add Server Certificate."

7 In the left frame, click Manage Certificates.

In the list of certificates, you will see the certificate you just added. In this deployment example, the certificate name OpenSSLTestCA-Sun is displayed in the list.

Close the browser.

8 As a root user, log into the Access Manager 1 host.

9 To verify that the certificate was imported properly, go to the following directory:

```
/opt/SUNWwbsvr/alias
```

In a directory listing, notice that certificate filename is formed by joining the prefix `https-AccessManager-1.example.com` and database file name `cert8.db`.

```
#ls
https-AccessManager-1.example.com-AccessManager-1-cert8.db
https-AccessManager-1.example.com-AccessManager-1-key3.db
https-AccessManager-1.example.com-cert8.db
https-AccessManager-1.example.com-key3.db
secmod.db
```

10 **Run the `certutil list` command, specifying the prefix from certificate filename:**

```
# cd /opt/SUNWwbsvr/bin/https/admin/bin
# ./certutil -L -d /opt/SUNWwbsvr/alias/ -P "https-AccessManager-1.example.com-"
OpenSSLTestCA - Sun
```

The `OpenSSLTestCA – Sun` certificate you imported is displayed.

▼ To Modify the `AMConfig.properties` File

1 **As a root user, log in to the Access Manager 1 host.**

2 **Go to the following directory:**

```
/etc/opt/SUNWam/config
```

Make a backup of the `AMConfig.properties` file before making any changes to the file.

3 **In the `AMConfig.properties` file, verify that the certificate database directory is specified correctly as in this example:**

```
com.iplanet.am.admin.cli.certdb.dir=/opt/SUNWWwbsvr/alias
```

4 **For the value of the following property, add the prefix from the certificate filename as in this example:**

```
com.iplanet.am.admin.cli.certdb.prefix=https-AccessManager-1.example.com-
```

5 **Notice that the following property points to a file `wtpass` which doesn't exist yet:**

```
com.iplanet.am.admin.cli.certdb.
```

You will create this file in the next step.

Save the file.

6 **Create the `wtpass` file.**

In the file, enter the name of the password you used to create the certificate database. Example:

```
# cd /etc/opt/SUNWam/config
# vi .wtpass
password
```

Save the file.

7 **Verify that the file was created properly.**

```
# cat .wtpass
password
```

8 **Restart the Web Server.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com
# ./stop; ./start
```

▼ To Import the Root CA Certificate into the Access Manager 2 Web Server

1 **To to the Web Server administration URL:**

`http://AccessManager-2.example.com:8888/https-admserv/bin/index`

2 **Log in to the Web Server console using the following information:**

User name: **`admin`**

Password: **`web4d4min`**

3 **On the Servers tab, select the server `AccessManager-2.example.com`, and then click Manage.**

4 **Click on the Security tab, and then initialize the Trust Database by providing the following information:**

Database Password: password

Password (again): password

Click OK.

5 **In the left frame, click Install Certificate. In the Install a Server Certificate page, provide the following information:**

Certificate for: Choose Trusted Certificate Authority (CA)

Message text (with headers): Choose this option, and then paste into the text box the root certificate you received from the CA. "To Request an SSL Certificate for the Distributed Authentication UI Load Balancer" on page 127. The root certificate will look similar to this:

```
-----BEGIN CERTIFICATE-----
UbM77e50M63v1Z2A/5O5MA0GCSqGSIb3DQEOBAU
AMF8xCzAJBgNVBAYTAlVTMSAwHgYDVQQKExdSU0
EgRGF0YSBTZWN1cml0eSwgSW5jLjEuMCwGA1UEC
xMlU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAeFw0wMTA4MDIwMDAwMDBaFw0
wMzA4MDIyMzU5NTlaMIGQMQswCQYDVQQGEwJVUz
ERMA8GA1UECBMIVmlyZ2luaWExETAPBgNVBAcUC
```

```
FJpY2htb25kMSAwHgYDVQQKFBdDYXZhbGllciBU
ZWxlcGhvYm9uZGluZy5jYXZ0ZWwuY29tMIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8x/1dxo
2YnblilQLmpiEziOqb7ArVfI1ymXo/MKcbKjnY2
-----END CERTIFICATE REQUEST-----
```

Click OK.

6 **On the "Add Trusted CA Certificate page," click "Add Server Certificate."**

7 **In the left frame, click Manage Certificates.**

In the list of certificates, you will see the certificate you just added. In this deployment example, the certificate name OpenSSLTestCA-Sun is displayed in the list.

Close the browser.

8 **As a root user, log into the Access Manager 2 host.**

9 **To verify that the certificate was imported properly, go to the following directory:**

```
/opt/SUNWwbsvr/alias
```

In a directory listing, notice that certificate filename is formed by joining the prefix `https-AccessManager-1.example.com` and database file name `cert8.db`.

```
#ls
https-AccessManager-1.example.com-AccessManager-2-cert8.db
https-AccessManager-1.example.com-AccessManager-2-key3.db
https-AccessManager-2.example.com-cert8.db
https-AccessManager-1.example.com-key3.db
secmod.db
```

10 **Run the `certutil list` command, specifying the prefix from certificate filename:**

```
# cd /opt/SUNWwbsvr/bin/https/admin/bin
# ./certutil -L -d /opt/SUNWwbsvr/alias/ -P "https-AccessManager-2.example.com-"
OpenSSLTestCA - Sun
```

The `OpenSSLTestCA – Sun` certificate you imported is displayed.

▼ To Modify the `AMConfig.properties` File

1 **As a root user, log in to the Access Manager 2 host.**

2 **Go to the following directory:**

```
/etc/opt/SUNWam/config
```

Make a backup of the `AMConfig.properties` file before making any changes to the file.

3 **In the `AMConfig.properties` file, verify that the certificate database directory is specified correctly as in this example:**

```
com.iplanet.am.admin.cli.certdb.dir=/opt/SUNWWwbsvr/alias
```

4 **For the value of the following property, add the prefix from the certificate filename as in this example:**

```
com.iplanet.am.admin.cli.certdb.prefix=https-AccessManager-2.example.com-
```

5 **Notice that the following property points to a file `wtpass` which doesn't exist yet:**

```
com.iplanet.am.admin.cli.certdb.
```

You will create this file in the next step.

Save the file.

6 **Create the `wtpass` file.**

In the file, enter the name of the password you used to create the certificate database. Example:

```
# cd /etc/opt/SUNWam/config
# vi .wtpass
password
```

Save the file.

7 **Verify that the file was created properly.**

```
# cat .wtpass
password
```

8 **Restart the Web Server.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com
# ./stop; ./start
```

5.6 Creating an Access Manager Site

Access Manager 7 2005Q4 introduces the *site* concept which provides centralized configuration management for an Access Manager deployment. In this example, you configure two Access Manager servers to work as a single site. Once configured as a site, all client requests always go through a load balancer. In this example, requests go through either the internal or external load balancer. This flow simplifies the deployment by resolving firewall issues between the client and the back-end Access Manager servers.

Use the following as your checklist for creating an Access Manager site:

1. Create an Access Manager site.
2. Verify that the site was configured properly.

To Create an Access Manager Site

Complete the following steps on the Access Manager 1 host. It is not necessary to repeat the steps on the Access Manager 2 host.

1 Start a browser, and access the Access Manager 1 server.

`http://AccessManager-1:1080/amserver/console`

2 Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

3 In the Access Manager console, click the Access Control tab, and then click the top-level Realm Name `example`.

4 In the Realm/DNS Aliases field, add the name of the internal load balancer.

For this example, enter `LoadBalancer-3.example.com:90`, and then click Add.

Note – Do not remove the host names AccessManager-1 and AccessManager-2 from the alias list. These allow administrators to log in to the console directly in the event of a load balancer failure.

---

5 For this deployment example, add an entry for the same host name using all lowercase.

Example: `loadbalancer-3.example.com:90`

6 Click Save.

7 In the Access Manager console, click the Realms link, and then navigate through the following:

Configuration > System Properties > Platform >

8 Under Site Name, click New, and enter the following values for the external load balancer:

Server: **`https://loadbalancer-3.example.com:9443`**

Site Name: **`11`**

9 Click OK, and then click Save.

10 **Under Site Name, click New. Enter the following values for the internal load balancer:**

Server: **`http://loadbalanacer-3.example.com:90`**

Site Name: **`12`**

11 **Click OK, and then click Save.**

12 **On the same Platform page, under Instance Name, click AccessManager-1.**

Change the site ID from `01` to `01|11|12`.

```
http://AccessManager-1.example.com:1080:01|11|12
```

13 **Click OK, and then click Save.**

14 **On the Platform page, under Instance Name, click AccessManager-2.**

Change the site ID from `02` to `02|11|12`.

```
http://AccessManager-2.example.com:1080:02|11|12
```

15 **Click OK, and then click Save.**

16 **Restart AccessManager-1 and AccessManager-2 for the changes to take effect.**

a. **Log in as a root user to the Access Manager 1 host.**

```
#cd /opt/SUNWwbsvr/https-AccessManager-1
# ./stop; ./start
```

b. **Log in as a root user to the Access Manager 2 host.**

```
#cd /opt/SUNWwbsvr/https-AccessManager-2
# ./stop; ./start
```

▼ To Verify that the Site was Configured Properly

1 **Go to the Access Manager Site URL:**

```
http://LoadBalancer-3.example.com:90/amserver/UI/Login
```

If an error message is displayed indicating that the browser cannot connect to either `AccessManager- 1.example.com` or `AccessManager-2.example.com`, then the site configuration is not correct. If the site configuration is correct, all browser interactions will always occur with the Site URL.

2. **If the Access Manager login page is displayed, verify that the browser URL still contains the Site URL.**

   If it does not contain the Site URL, then the site configuration is incorrect. If the site configuration is correct, all browser interactions will always occur with the Site URL

3. **If the Access Manager login page is displayed, and the browser URL contains the Site URL, log in to the Access Manager console using the following information:**

   User Name: **`amadmin`**

   Password: **`4m4dmin1`**

4. **Verify that you can successfully login to the Access Manager console.**

5. **Log out of the Access Manager console.**

◆ ◆ ◆ CHAPTER 6

Installing and Configuring the Distributed Authentication UI Servers

This chapter contains detailed instructions for the following tasks:

6.1 Installing and Deploying the Distributed Authentication UI Servers

Use the following as your checklist for installing and Deploying the Distributed Authentication UI servers:

1. Install a container for Distributed Authentication UI Server 1.
2. Build and deploy Distributed Authentication UI Server 1.
3. Install a container for Distributed Authentication UI Server 2.
4. Build and deploy Distributed Authentication UI Server 2.
5. Import the root CA certificate for the Access Manager load balancer into Authentication UI Server 1.
6. Verify that authentication through Authentication UI Server 1 is successful.
7. Import the root CA certificate for the Access Manager load balancer into Authentication UI Server 2.
8. Verify that authentication through Authentication UI Server 2 is successful.

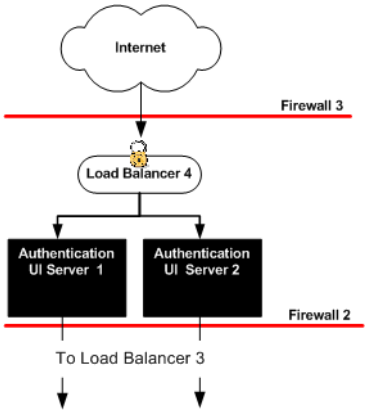

FIGURE 6–1 Distributed Authentication

The Java ES installer must be mounted on the host AuthenticationUI-1 where you will install Web Server. See the section "To Download and Unpack the Java Enterprise System 2005Q4 Installer""3.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer" on page 32 in this document.

▼ To Install a Container for Distributed Authentication UI Server 1

1 **As a root user, log in to host Authentication UI-1.**

2 **Start the Java Enterprise System installer with the `-nodisplay` option.**

```
# /mnt/Solaris_sparc
# ./installer -nodisplay
```

3 **When prompted, provide the following information:**

`Welcome to the Sun Java(TM) Enterprise System;`
`serious software made  simple...`
`<Press ENTER to Continue>`
	Press Enter.

`<Press ENTER to display the Software` `License Agreement>`	Press Enter.

`Have you read, and do you accept, all of`
`the termsof the preceding Software`
`License Agreement [No]`
	Enter **y**.

`Please enter a comma separated list of languages you would like supported with this installation [8]`	Enter 8 for "English only."
`Enter a comma separated list of products to install,or press R to refresh the list []`	Enter **3** to select Web Server.
`Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]`	Press Enter.
`Enter 1 to upgrade these shared components and 2 to cancel [1]`	You are prompted to upgrade shared components only if the installer detects that an upgrade is required. Enter **1** to upgrade shared components.
`Enter the name of the target installation directory for each product: Web Server [/opt/SUNWwbsvr] :`	Accept the default value.
`System ready for installation Enter 1 to continue [1]`	Enter **1**.
`1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]`	Enter **1**.
`Common Server Settings Enter Host Name [AuthenticationUI-1]`	Accept the default value.
`Enter DNS Domain Name [example.com]`	Accept the default value.
`Enter IP Address [xxx.xx.87.180]`	Accept the default value.
`Enter Server admin User ID [admin]`	Enter **admin**.
`Enter Admin User's Password (Password cannot be less than 8 characters) []`	For this example, enter **web4dmin**.
`Confirm Admin User's Password []`	Enter the same password to confirm it.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Enter Server Admin User ID [admin]`	Enter **admin**.
`Enter Admin User's Password []`	For this example, enter **web4dmin**.
`Enter Host Name [AuthenticationUI-1.example.com]`	Accept the default value.

`Enter Administration Port [8888]`	Accept the default value.
`Enter Administration Server User ID [root]`	Accept the default value.
`Enter System User ID [webservd]`	Enter **`root`**.
`Enter System Group [webservd]`	Enter **`root`**.
`Enter HTTP Port [80]`	Enter **`1080`**.
`Enter content Root [/opt/SUNWwbsvr/docs]`	Accept the default value.
`Do you want to automatically start Web Serverwhen system re-starts.(Y/N) [N]`	Accept the default value.
`Ready to Install 1. Install 2. Start Over 3. Exit Installation What would you like to do [1]`	When ready to install, enter **`1`**.

▼ To Build and Deploy Distributed Authentication UI Server 1

1 Log in as a root user to AccessManager-1.

For this example, log into AccessManager-1.

2 Copy the Distributed Authentication UI files to another workspace on the AccessManager-1.

```
# cd /opt/SUNWcomm/SUNWam
# cp README.distAuthUI amauthistui.war Makefile.distAuthUI /opt/SUNWam
```

3 Edit the `Makefile.distAuthUI` file and set the following properties:

```
JAVA_HOME=/usr/jdk/entsys-j2se/
SERVER_PROTOCOL=http
SERVER_HOSTNAME=LoadBalancer-3.example.com
SERVER_PORT=90
SERVER_DEPLOY_URI=amserver
DISTAUTH_PROTOCOL=http
DISTAUTH_HOSTNAME=AuthenticationUI-1.example.com
DISTAUTH_PORT=1080
DISTAUTH_DEPLOY_URI=/distAuth
APPLICATION_USERNAME=amadmin
APPLICATION_PASSWORD=4m4dmin1
NOTIFICATION_URL=http://AuthenticationUI-1.example.com:1080/
        distAuth/notificationservice
DEBUG_LEVEL=message
DEBUG_DIR=/tmp/distAuth
```

```
COOKIE_ENCODE=false
DISTAUTH_VERSION=7.0
```

4 **Create the war file by issuing the following command**

```
# /usr/sfw/bin/gmake -f Makefile.distAuthUI
```

This creates a war file named `distAuthUI.war` .

5 **Rename the generated file.**

```
# mv distAuthUI.war distAuth_AccessManager-1.war
```

6 **Copy `distAuth_AccessManager-1.war` from the local host where you built the Distributed Authentication UI server (AccessManager–1) to the remote host where the Distributed Authentication UI server will be deployed (AuthenticationUI-1).**

In this deployment example, the desintation directory is `/tmp`.

7 **Log in as a root user to the Authentication UI-1 Web Server.**

8 **Start the Authentication UI-1 Web Server.**

```
# cd /opt/SUNWwbserver
# #cd https-AuthenticationUI-1.example.com
# # ./start
```

9 **Deploy the Distributed Authentication UI WAR file.**

On the host AuthenticationUI-1, in the directory where you copied the `distAuth_AuthenticationUI-1.war` file, run the `wdeploy` command using the following form:

`wdeploy deploy -u` *uri_path* `-i` *instance* `-v` *vs_id*

`[ [-V` *verboseLevel* `]| [-q] ] [-n] [-d` *directory*`]` *war_file*

For example, in this Deployment Example:

```
# cd /opt/SUNWwbsvr/bin/https/bin
# ./wdeploy deploy -u /distAuth -i https-AuthenticationUI-1.example.com
-v https-AuthenticationUI-1.example.com
-d /opt/SUNWwbsvr/https-AuthenticationUI-1.example.com/webapps/distAuth
/tmp/distAuth_AuthenticationUI-1.war
```

10 **Restart Web Server.**

```
# cd /opt/SUNWwbserver
# cd https-AuthenticationUI-1.example.com
# ./stop; ./start
server has been shutdown
# Sun ONE Web Server 6.1SP5 B06/23/2005 18:00
info: CORE3016: daemon is running as super-user
info: CORE5076: Using [Java HotSpot(TM) Server VM,
```

```
Version 1.5.0_04] from [Sun Microsystems Inc.]
#
info: WEB0100: Loading web module in virtual server
[https-AuthenticationUI-1.example.com] at [/distAuth]
info: WEB0100: Loading web module in virtual server
[https-AuthenticationUI-1.example.com] at [/search]
info: HTTP3072: [LS ls1] http://AuthenticationUI-1.example.com:8080
ready to accept requests
startup: server started successfully
```

Next Steps The web module is loaded in the following directory:

```
/opt/SUNWwbsvr/https-AuthenticationUI-1.example.com/webapps/distAuth
```

▼ To Install a Container for Distributed Authentication UI Server 2

1. **As a root user, log in to host AuthenticationUI-2.**
2. **Start the Java Enterprise System installer with the `-nodisplay` option.**

```
# /mnt/Solaris_sparc
# ./installer -nodisplay
```

3. **When prompted, provide the following information:**

`Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>`	Press Enter.
`<Press ENTER to display the Software License Agreement>`	Press Enter.
`Have you read, and do you accept, all of the termsof the preceding Software License Agreement [No]`	Enter **y**.
`Please enter a comma separated list of languages you would like supported with this installation [8]`	Enter 8 for “English only.”
`Enter a comma separated list of products to install,or press R to refresh the list []`	Enter **3** to select Web Server.

`Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]`	Press Enter.
`Enter 1 to upgrade these shared components and 2 to cancel [1]`	You are prompted to upgrade shared components only if the installer detects that an upgrade is required. Enter **1** to upgrade shared components.
`Enter the name of the target installation directory for each product: Web Server [/opt/SUNWwbsvr] :`	Accept the default value.
`System ready for installation Enter 1 to continue [1]`	Enter **1**.
`1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]`	Enter **1**.
`Common Server Settings Enter Host Name [AuthenticationUI-2]`	Accept the default value.
`Enter DNS Domain Name [example.com]`	Accept the default value.
`Enter IP Address [xxx.xx.87.180]`	Accept the default value.
`Enter Server admin User ID [admin]`	Enter **admin**.
`Enter Admin User's Password (Password cannot be less than 8 characters) []`	For this example, enter **web4dmin**.
`Confirm Admin User's Password []`	Enter the same password to confirm it.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Enter Server Admin User ID [admin]`	Enter **admin**.
`Enter Admin User's Password []`	For this example, enter **web4dmin**.
`Enter Host Name [AuthenticationUI-2.example.com]`	Accept the default value.
`Enter Administration Port [8888]`	Enter **1080**.
`Enter Administration Server User ID [root]`	Accept the default value.
`Enter System User ID [webservd]`	Enter **root**.

`Enter System Group [webservd]`	Enter **`root`**.
`Enter HTTP Port [80]`	Enter **`8888`**.
`Enter content Root [/opt/SUNWwbsvr/docs]`	Accept the default value.
`Do you want to automatically start Web Serverwhen system re-starts.(Y/N)[N]`	Accept the default value.
`Ready to Install 1. Install 2. Start Over 3. Exit Installation What would you like to do [1]`	When ready to install, enter **`1`**.

▼ To Build and Deploy Distributed Authentication UI Server 2

1 Log in as a root user to an Access Manager host.

For this example, log into AccessManager-2.

2 Copy the Distributed Authentication UI files to another workspace on the same (local) host.

```
cd /opt/SUNWcomm/SUNWam
cp README.distAuthUI amauthistui.war Makefile.distAuthUI /opt/SUNWam
```

3 Edit the `Makefile.distAuthUI` file and set the following properties:

```
JAVA_HOME=/usr/jdk/entsys-j2se/
SERVER_PROTOCOL=http
SERVER_HOSTNAME=LoadBalancer-3.example.com
SERVER_PORT=90
SERVER_DEPLOY_URI=amserver
DISTAUTH_PROTOCOL=http
DISTAUTH_HOSTNAME=AuthenticationUI-2.example.com
DISTAUTH_PORT=1080
DISTAUTH_DEPLOY_URI=/distAuth
APPLICATION_USERNAME=amadmin
APPLICATION_PASSWORD=4m4dmin1
NOTIFICATION_URL=http://AuthenticationUI-2.example.com:1080/
        distAuth/notificationservice
DEBUG_LEVEL=message
DEBUG_DIR=/tmp/distAuth
COOKIE_ENCODE=false
DISTAUTH_VERSION=7.0
```

4 Create the war file by issuing the following command

```
gmake -f Makefile.distAuthUI.war
```

This creates a war file named `distAuth_deploy.war`.

5 Rename the generated file.

```
mv distAuthUI.war distAuth_AccessManager-2.war
```

6 Copy `distAuth_AccessManager-2.war` from the local host where you built the Distributed Authentication UI (AccessManager—2) to the remote host where the Distributed Authentication UI will be deployed (AuthetnicationUI-2).

```
# cp distAuth_AccessManager-2.war /net/AuthenticationUI-2/
tmp/distAuth_ AuthenticationUI-2.war
```

7 Deploy the Distributed Authentication UI WAR file.

On the host AuthenticationUI-2, in the directory where you copied the `distAuth_ AuthenticationUI-2.war` file, run the `wdeploy` command using the following form:

`wdeploy deploy -u` *uri_path* `-i` *instance* `-v` *vs_id*

`[ [-V` *verboseLevel* `]| [-q] ] [-n] [-d` *directory*`]` *war_file*

For example, in this Deployment Example:

```
# ./wdeploy deploy -u /distAuth -i https-AuthenticationUI-2.example.com
-v https-AuthenticationUI-2.example.com
-d /opt/SUNWwbsvr/https-AuthenticationUI-2.example.com/webapps/distAuth
/tmp/distAuth_ AuthenticationUI-2.war
```

8 Restart Web Server.

```
# cd /opt/SUNWwbserver
# cd https-AuthenticationUI-2.example.com
# ./stop; ./start
server has been shutdown
# Sun ONE Web Server 6.1SP5 B06/23/2005 18:00
info: CORE3016: daemon is running as super-user
info: CORE5076: Using [Java HotSpot(TM) Server VM,
Version 1.5.0_04] from [Sun Microsystems Inc.]
#
info: WEB0100: Loading web module in virtual server
[https-AuthenticationUI-2.example.com] at [/distAuth]
info: WEB0100: Loading web module in virtual server
[https-AuthenticationUI-2.example.com] at [/search]
info: HTTP3072: [LS ls1] http://AuthenticationUI-2.example.com:8080
ready to accept requests
startup: server started successfully
```

Next Steps The web module is loaded in the following directory:

```
/opt/SUNWwbsvr/https-AuthenticationUI-2.example.com/webapps/distAuth/distAuth
```

▼ To Import the Root CA Certificate for the Access Manager Load Balancer into Authentication UI Server 1

In this procedure, you import a Certificate Authority (CA) certificate. The certificate enables the Authentication UI server to trust the certificate from the Access Manager load balancer (Load Balancer 3), and to establish trust with the certificate chain that is formed from the CA to the certificate.

1 Log in as root to Authentication UI Server 2.

2 Copy the root CA certificate into a directory.

After the certificate authority (CA) sends you the certificate, copy the certificate text into a file. In this example, the file is `/export/software/ca.cer`.

3 Import the root CA certificate into the Java certificate store.

```
# /usr/jdk/entsys-j2se/jre/bin/keytool -import -trustcacerts
 -alias OpenSSLTestCA -file /export/software/ca.cer -keystore
/usr/jdk/entsys-j2se/jre/lib/security/cacerts -storepass changeit
Owner: EMAILADDRESS=nobody@nowhere.com, CN=OpenSSLTestCA, OU=Sun,
O=Sun,L=Santa Clara, ST=California C=US
Issuer: EMAILADDRESS=nobody@nowhere.com, CN=OpenSSLTestCA, OU=Sun,
O=Sun,L=Santa Clara, ST=California C=US
Serial number: 97dba0aa26db6386
Valid from: Tue Apr 18 07:66:19 PDT 2006 until: Tue Jan 13 06:55:19
PST 2009
Certificate fingerprints:
               MD5: 9f:57:ED:B2:F2:88:B6:E8:0F:1E:08:72:CF:70:32:06
     SHA1: 31:26:46:15:C5:12:5D:29:46:2A:60:A1:E5:9E:26:64:36:80:E4:70
Trust this certificate: [no] yes
Certificate was added to keystore.
```

4 Verify that the root CA certificate was imported into the keystore.

```
# /usr/jdk/entsys-j2se/jre/bin/keytool -list -keystore ./cacerts
-storepass changeit | grep -i open
openssltestca, Nov 8, 2006, trustedCertEntry
```

5 Restart AuthenticationUI-1.

```
# cd /opt/SUNWwwbsvr/https-AuthenticationUI-1.example.com
# ./stop
server has been shutdown
#./start
Sun ONE Web Server 6.1SP5 B06/23/2005 18:00
info: CORE3016: daemon is running as super-user
```

```
info: CORE5076: Using [Java HotSpot(TM) Server VM,
version 1.5.0_04 ] from [Sun Microsystems Inc.]
info: WEB0100: Loading web module in virtual server
https-AuthenticationUI-1.example.com]
at [/distAuth]
info: WEB0100: Loading web module in virtual server
https-AuthenticationUI-1.example.com] at [/search]
info: HTTP3072: [LS is 1] http://AuthenticationUI-1.example.com:1080
ready to accept requests
startup: server started successfully
```

▼ To Verify that Authentication Through Authentication UI Server 1 is Successful

Find a host that has direct network connectivity to both Authentication UI servers and the external facing load balancer of the Access Manager servers. One natural place is the Distributed Authentication UI server host itself.

1 Open a web browser and go to the following URL:

```
http://AuthenticationUI-1.example.com:1080/distAuth/UI/Login?goto=
http://LoadBalancer-3.example.com:90
```

2 Log in to the Access Manager console using the following information:

Username **amadmin**

Password **4m4dmin1**

After successful authentication, you should be redirected to the index page for Access Manager's Web Server.

3 Log out of the Access Manager console.

▼ To Import the Root CA Certificate for the Access Manager Load Balancer into Authentication UI Server 2

In this procedure, you import a Certificate Authority (CA) certificate. The certificate enables the Authentication UI server to trust the certificate from the Access Manager load balancer (Load Balancer 3), and to establish trust with the certificate chain that is formed form the CA to the certificate.

1 Log in as a root user to Authentication UI Server 2.

2 Copy the root CA certificate into a directory.

After the certificate authority (CA) sends you the certificate, copy the certificate text into a file. In this example, the file is `/export/software/ca.cer`.

3 Import the root CA certificate into the Java certificate store.

```
# /usr/jdk/entsys-j2se/jre/bin/keytool -import -trustcacerts
 -alias OpenSSLTestCA -file /export/software/ca.cer -keystore
/usr/jdk/entsys-j2se/jre/lib/security/cacerts -storepass changeit
Owner: EMAILADDRESS=nobody@nowhere.com, CN=OpenSSLTestCA, OU=Sun,
O=Sun,L=Santa Clara, ST=California C=US
Issuer: EMAILADDRESS=nobody@nowhere.com, CN=OpenSSLTestCA, OU=Sun,
O=Sun,L=Santa Clara, ST=California C=US
Serial number: 97dba0aa26db6386
Valid from: Tue Apr 18 07:66:19 PDT 2006 until: Tue Jan 13 06:55:19
PST 2009
Certificate fingerprints:
               MD5: 9f:57:ED:B2:F2:88:B6:E8:0F:1E:08:72:CF:70:32:06
     SHA1: 31:26:46:15:C5:12:5D:29:46:2A:60:A1:E5:9E:26:64:36:80:E4:70
Trust this certificate: [no] yes
Certificate was added to keystore.
```

4 Verify that the root CA certificate was imported into the keystore.

```
# /usr/jdk/entsys-j2se/jre/bin/keytool -list -keystore ./cacerts
-storepass changeit | grep -i open
openssltestca, Nov 8, 2006, trustedCertEntry
```

5 Restart AuthenticationUI-2.

```
# cd /opt/SUNWwwbsvr/https-AuthenticationUI-2.example.com
# ./stop
server has been shutdown
#./start
Sun ONE Web Server 6.1SP5 B06/23/2005 18:00
info: CORE3016: daemon is running as super-user
info: CORE5076: Using [Java HotSpot(TM) Server VM,
version 1.5.0_04 ] from [Sun Microsystems Inc.]
info: WEB0100: Loading web module in virtual server
[https-AuthenticationUI-2.example.com]
at [/distAuth]
info: WEB0100: Loading web module in virtual server
[https-AuthenticationUI-2.example.com]
at [/search]
info: HTTP3072: [LS is 1] http://AuthenticationUI-2.example.com:1080
ready to accept requests
startup: server started successfully
```

▼ To Verify that Authentication Through Authentication UI Server 2 is Successful

Find a host that has direct network connectivity to both Authentication UI servers and the external facing load balancer of the Access Manager servers. One natural place is the Distributed Authentication UI server host itself.

1 **Open a web browser and go to the following URL:**

```
http://AuthenticationUI-2.example.com:1080/distAuth/UI/Login?goto=
http://LoadBalancer-3.example.com:90
```

2 **Log in to the Access Manager console using the following information:**

Username **amadmin**

Password **4m4dmin1**

After successful authentication, you should be redirected to the index page for Access Manager's Web Server.

6.2 Configuring the Distributed Authentication UI Servers Load Balancer

1. Configure the Distributed Authentication UI servers load balancer.
2. Configure Distributed Authentication UI servers to authenticate to Access Manager as a custom user.
3. Configure the load balancer cookies for the Distributed Authentication UI servers.
4. Request an SSL certificate for the Distributed Authentication UI load balancer.
5. Install a root CA certificate on the Distributed Authentication UI load balancer.
6. Install an SSL certificate on the Distributed Authentication UI load balancer.
7. Configure SSL termination on the Distributed Authentication UI load balancer.

▼ To Configure the Distributed Authentication UI Servers Load Balancer

Before You Begin Contact your network administrator to obtain an available virtual IP address.

Note – The load balancer hardware and software used in the lab facility for this deployment is BIG-IP® manufactured by F5 Networks. If you are using different load balancer software, see the documentation that comes with that product for detailed settings information.

1 Create a Pool.

A pool contains all the backend server instances.

a. Go to URL for the Big IP load balancer and log in.

b. Open the Configuration Utility.

Click "Configure your BIG-IP (R) using the Configuration Utility."

c. In the left pane, click Pools.

d. On the Pools tab, click the Add button.

e. In the Add Pool dialog, provide the following information:

Pool Name	Example: AuthenticationUI-Pool
Load Balancing Method	Round Robin
Resources	Add IP addresses for the Distributed Authentication UI server hosts. For this example, add AuthenticationUI-1:1080 and AuthenticationUI-2:1080.

f. Click the Done button.

2 Configure the load balancer for persistence.

a. In the left frame, click Pools.

b. Click the DistributedUI-Pool link.

c. Click the Persistence tab.

d. Under Persistence Type, choose Passive HTTP Cookie, and then click Apply.

3 Add a Virtual Server.

a. In the left frame, Click Virtual Servers.

b. On the Virtual Servers tab, click the Add button.

c. In the Add Virtual Server wizard, enter the virtual server IP address and port number.

In this example, enter the IP address for Load Balancer 4, and enter the port number 90.

d. Continue to click Next until you reach the Pool Selection dialog box.

e. In the Pool Selection dialog box, assign the AuthenticationUI-Pool that you have just created.

f. Click the Done button.

4 Add monitors.

Monitors are necessary for the load balancer to detect any backend server failures that may occur.

a. In the left frame, click Monitors.

b. Click the Basic Associations tab.

c. Add an HTTP monitor to each Web Server node.

In the Node list, locate the *IPaddress:port* of the node for which you are creating the monitor. Select the Add checkbox.

d. Click Apply.

5 Verify that the Distributed Authentication UI server load balancer is configured properly.

Start a new browser and go to the Distributed Authentication UI load balancer URL. Example:

`http://LoadBalancer-4.example.com:90/`.

If the browser successfully renders the default Sun Web Server default document root page, close the browser.

▼ To Configure Distributed Authentication UI Servers to Authenticate to Access Manager as a Custom User

1 Set up a custom user.

a. Open a browser and go to the Access Manager login URL.

`https://LoadBalancer-3.example.com:9443/amserver/UI/Login`

b. Log in to the Access Manager console using the following information:

Username **amadmin**

Password **4m4dmin1**

c. **On the Access Control tab, click the top-level realm** `example.com`**.**

d. **Click the Subjects tab.**

e. **Click the Agents tab.**

f. **On the Agents tab, click the New button.**

g. **In the New Agent page, provide the following information, and then click Create.**

ID **authuiadmin**

Password **4uthu14dmin**

h. **On the Agent tab, in the list of Agent names, click on** `authuiadmin`**.**

i. **On the General tab, copy the UniversalID value, and save it where you can use it later.**

i. **Log out of the console.**

2 **Define** `authuiadmin` **as a special user in Access Manager 1.**

a. **As a root user, log in to host AccessManager–1.**

b. **Locate the** `/etc/opt/SUNWam/config/AMConfig.properties` **file.**

Make a backup of this file before you modify it.

c. **In the file, locate the following property:**

```
com.sun.identity.authentication.special.users
```

d. **At end of the list of values, add the UniversalID that you obtained and saved from the Agents list:**

```
|uid=authuiadmin,ou=agents,o=example.com
```

This step authorizes the user to authenticate remote applications to the Access Manager server using the Access Manager Client SDK.

3 **Define** `authuiadmin` **as a special user in Access Manager 2.**

a. **As a root user, log into host AccessManager–2.**

b. Locate the `/etc/opt/SUNWam/config/AMConfig.properties` file.

Make a backup of this file before you modify it.

c. In the file, locate the following property:

```
com.sun.identity.authentication.special.users
```

d. At end of the list of values, add the UniversalID that you obtained and saved from the Agents list:

```
|uid=authuiadmin,ou=agents,o=example.com
```

This step authorizes the user to authenticate remote applications to the Access Manager server using the Access Manager Client SDK.

4 Restart both Access Manager 1 server and Access Manager 2 server.

5 Log out of Access Manager 1 and log out of Access Manager 2.

6 Define the custom user as a special user on the Authentication UI 1 server.

a. As a root user log into host AuthenticationUI— 1.

b. Locate the following file:

```
opt/SUNWwbsvr/https-AuthenticationUI-1.example.com/
webapps/distAuth/WEB-INF/classes/AMConfig.properties
```

Make a backup of this file before you modify it.

c. In the file, set the following properties:

```
com.sun.identity.agents.app.username=authuiadmin
```

```
com.iplanet.am.service.password=4uthu14dmin
```

7 Define the custom user as a special user on the Authentication UI 2 server.

a. As a root user, log into host AuthenticationUI–2.

b. Locate the following file:

```
opt/SUNWwbsvr/https-AuthenticationUI-2.example.com/
webapps/distAuth/WEB-INF/classes
```

Make a backup of this file before you modify it.

c. In the file, set the following properies:

```
com.sun.identity.agents.app.username=authuiadmin
```

```
com.iplanet.am.service.password=4uthu14dmin
```

8 Restart Authentication UI 1 server and Authentication UI 2 server.

```
# cd /opt/SUNWwbsvr/https-AuthenticationUI-1.example.com
# ./stop ; ./start
# cd /opt/SUNWwbsvr/https-AuthenticationUI-2.example.com
# ./stop ; ./start
```

9 Log out of Authentication UI 1 server and log out of Authentication UI 2 server.

10 Verify that everything works.

a. On Directory Server 1 and Directory Server 2, go to logs directory and run the `tail` command.

```
# cd /var/opt/mps/serverroot/slapd-am-config/logs
# tail -f access | grep authuiadmin
```

b. In a browser, go to following URL to open the Access Manager login page.

```
https://LoadBalancer-4.example.com:9443/distAuth/UI/Login?
goto=https://LoadBalancer-3.example.com:9443/amserver/UI/Login
```

Using this URL, you will be able to view entries for the Authentication UI server binding to the Directory Server as the special user `authuiadmin`.

c. In the logs, look for entries similar to this:

```
[12/Jul/2006:21:08:33 -0700] conn=43430 op=0 msgId=1059 -
BIND dn="uid=authuiadmin,ou=agents,o=example.com" method=128 version=3
[12/Jul/2006:21:08:33 -0700] conn=43430 op=0 msgId=1059 -
RESULT err=0 tag=97 nentries=0 etime=0 dn="uid=authuiadmin,ou=agents,o=example.com"
```

When you see `err=0` in either log, you know that the Authentication UI server successfully logged into the Access Manager server. If the `err` value is anything other an 0, you must troubleshoot the configuration.

d. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

If you can successfully log in, you know that authentication worked successfully

11 Log out of the console.

▼ To Configure the Load Balancer Cookies for the Distributed Authentication UI Servers

1. **Log in as a root user to Authentication UI 1 host.**
2. **Go to the following directory:**

   ```
   # cd /webapps/distAuth/WEB-INF/classes
   ```

3. **Modify the `AMconfig.properties` file.**

   Make a backup of this file.

   At the end of the file, uncomment the last two lines and set the following values:

   ```
   com.iplanet.am.lbcookie.name=AuthenticationUILBCookie
   com.iplanet.am.lbcookie.value=AuthenticationUI-1
   ```

4. **Restart the Authentication UI 1 host.**
5. **As a root user log into host AuthenticationUI–2 .**
6. **Go to the following directory:**

   ```
   # cd /webapps/distAuth/WEB-INF/classes
   ```

7. **Modify the `AMconfig.properties` file.**

   Make a backup of this file.

   At the end of the file, uncomment the last two lines and set the following values:

   ```
   com.iplanet.am.lbcookie.name=AuthenticationUILBCookie
   com.iplanet.am.lbcookie.value=AuthenticationUI-2
   ```

8. **Restart the Distributed Authentication UI 1 server.**

▼ To Request an SSL Certificate for the Distributed Authentication UI Load Balancer

1. **Open a browser, go to the BIG-IP URL:**

   ```
   https://is-F5.example.com
   ```

2. **Log in to the BIG-IP console using the following information:**

   User Name: **`username`**

Password: **password**

3. **Click "Configure your BIG-IP (R) using the Configuration Utility."**

4. **In the left pane, click Proxies.**

5. **Click the Cert-Admin tab.**

6. **On the SSL Certificate Administration page, click the button named "Generate New Key Pair/Certificate Request."**

7. **In the Create Certificate Request page, provide the following information:**

   Key Identifier: **LoadBalancer-4.example.com**

   Organizational Unit Name: **Deployment**

   Domain Name: **LoadBalancer-4.example.com**

   Challenge Password: **password**

   Retype Password: **password**

8. **Click the button "Generate Key Pair/Certificate Request."**

   On the SSL Certificate Request page, the request is generated in the Certificate Request field.

9. **Copy all the text contained in the Certificate Request field.**

   Save the text in a text file to keep it handy for later use.

10. **Send the text of the certificate request to a Certificate Authority of your choice.**

    A Certificate Authority is an entity that issues certified digital certificates. VersiSign, Thawte , Entrust, and GoDaddy are just a few examples of Certificate Authority companies. In this deployment example, CA certificates were obtained from OpenSSL. Follow the instructions provided by the Certificate Authority for submitting a certificate request.

▼ To Install a Root CA Certificate on the Distributed Authentication UI Load Balancer

The root Certificate Authority certificate proves that a Certificate Authority such as VeriSign or Entrus actually issued the digital server certificate you received. You install the root certificate on Load Balancer 3 to ensure that the link between the Load Balancer 3 SSL certificate can be maintained with the issuing company.

1. **In the BIG-IP load balancer console, click Proxies.**

2. **Click the Cert-Admin tab.**
3. **Click the Import link.**
4. **In the Import Type field, choose Certificate, and then click Continue.**
5. **In the Install SSL Certificate page, in the Certificate File field, click Browse.**
6. **In the Choose File dialog, choose Browser.**
   Navigate to the file that includes the root CA Certificate, and click Open.
7. **In the Certificate Identifier field, enter `OpenSSL_CA_cert`.**
8. **Click Install Certificate.**
9. **In the Certificate OpenSSL_CA_Cert page, click Return to Certificate Administration.**
   The new certificate OpenSSL_CA_Cert is now included in the Certificate ID list.

▼ To Install an SSL Certificate on the Distributed Authentication UI Load Balancer

1. **Once you've received the SSL certificate from a Certificate Authority, in the BIG-IP load balancer console, click Proxies.**
2. **Click the Cert-Admin tab.**
   The key `LoadBalancer-4.example.com` is in the Key List. This was generated in a previous step when you generated a key pair and a certificate request.
3. **In the Certificate ID column, click the Install button for `LoadBalancer-4.example.com`.**
4. **In the Certificate File field, click Browse.**
   In the Choose File dialog, navigate to the text file in which you saved the certificate text sent to you by the certificate issuer, and then click Open.
5. **Click Install Certificate.**
6. **In the Certificate LoadBalancer-3.example.com page, click Return to Certificate Information link.**
   In the SSL Certificate Administration page, verify that the Certificate ID indicates `LoadBalancer-4.example.com`.

▼ To Configure SSL Termination on the Distributed Authentication UI Load Balancer

In this deployment example, Secure Socket Layer (SSL) termination at Load Balancer 4 increases the performance at the server level, and simplifies SSL certificate management. Clients will access Load Balancer 4 using SSL-encrypted data. Load Balancer 4 decrypts the data and then sends the unencrypted data on to the Access Manager server. The Access Manager server or Authentication UI server does not have to perform decryption, and the burden on its processor is relieved. Load Balancer 3 then load-balances the decrypted traffic to the appropriate Access Manager server. Finally, Load Balancer 34encrypts the responses from server, and sends encrypted responses to the client.

In this deployment example, an SSL certificate is required only at the Load Balancer 4, and not required for each Access Manager server. This simplifies SSL certificate management. Load Balancer 4 can intelligently load-balance a request based on unencrypted cookies. This would not be possible with SSL-encrypted cookies because Load Balancer 4 cannot read SSL-encrypted cookies.

In this deployment example, you set up a proxy server using BIG-IP™ hardware and software.

1 Configure the new proxy service.

a. Log in to the BIG-IP load balancer using the following information:

Username **`username`**

Password **`password`**

b. Click the link "Configure your BIG-IP using the Configuration Utility."

c. In the load balancer console, in the left pane, click Proxies.

d. On the Proxies tab, click Add.

e. In the Add Proxy dialog, provide the following information:

Proxy Type:	Check the SSL checkbox.
Proxy Address:	**`xxx.xx.69.14`** (The IP address of Load Balancer 3, the Access Manager server load balancer.)
Proxy Service:	**`9443`** (The port number of the new proxy you are setting up.)
Destination Address:	**`xxx.xx.69.14`**
Destination Service:	**`90`**
Destination Target:	Choose **`Local Virtual Server`**.

SSL Certificate:	Choose **`LoadBalancer-4.example.com`**.
SSL Key:	Choose **`LoadBalancer-4.example.com`**.
Enable ARP:	Check this checkbox.

f. Click Next.

g. In the Rewrite Redirects field, choose `All`.

h. Click Done.

The new proxy server is now added to the Proxy Server list.

2 Verify that you can access the Access Manager server using the new proxy server port number.

a. Open a browser, and go to the following URL:

```
https://LoadBalancer-4.example.com:9443/distAuth/UI/Login?goto=
https://LoadBalancer-3.example.com:9443/amserver/UI/Login
```

Tip – You may see a message indicating that the Access Manager server doesn't recognize the certificate issuer. When this happens, install the root Certificate Authority certificate in the browser so that the browser recognizes the certificate issuer. See your browser's online help system for information on installing a root CA certificate.

---

i. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

If you can successfully log in to Access Manager 1, then the SSL certificate is installed properly and proxy service is configured properly.

b. Log out of Access Manager, and close the browser.

◆ ◆ ◆ CHAPTER 7

Integrating an Existing User Data Store

This chapter contains detailed instructions for the following tasks:

7.1 Creating and Configuring a New User Data Store

1. Create a user data store instance on Directory Server 1.
2. Create a user data store instance on Directory Server 2.
3. Create a new branch in the user data store.
4. Import users into the user data store.

In this deployment example, the new user data store is created within the same Directory Servers as the Access Manager configuration store. In most cases, the new data store would be created in a different Directory Server.

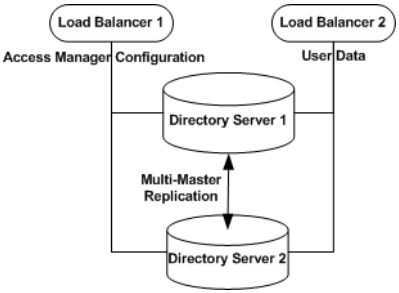

FIGURE 7–1 Directory Servers with User Data and Access Manager Configuration

▼ To Create a User Data Store Instance on Directory Server 1

1 As a root user log in to the Directory Server 1 host.

2 Run the `netstat` command to be sure the that the Directory Server administration port is open.

```
# cd /var/opt/mps/serverroot

# netstat –an | grep 1391
* 1390           *.*           0           0 49152           0 LISTEN
```

If the administration server is not running, start it now:

```
# ./start-admin
```

3 Start the Directory Server console.

```
# ./startconsole &
```

4 Log in to the Directory Server console using the following information:

Username	**`cn=Directory Manager`**
Password	**`d1rm4n4ger`**
Administration URL	**`http://DirectoryServer-1.example.com:1391`**

5 Expand the `example.com` domain, the `DirectoryServer-1.example.com` node, and the Server Group object.

You should see three Directory Server objects: an Administration Server, Directory Server (`ds-config`), and Directory Server (`am-config`).

6 Right-click the Server Group object, and choose "Create Instance Of."

Choose Sun Java™ System Directory Server.

7 **In the Create New Instance dialog, provide the following information and then click OK:**

Server Identifier:	**am-users**
Network port:	**1489**
Base suffix:	**dc=company,dc=com**
Directory Manager DN:	**cn=Directory Manager**
Directory Manager Password:	**d1rm4n4ger**
Confirm password:	**d1rm4n4ger**
Server Runtime (UNIX) user ID:	**nobody**

In the navigation tree, the new instance `Directory Server (am-users)` is added to the Server Group list.

8 **In the navigation tree, click the `Directory Server (am-users)` to open its console.**

Verify that the Server status indicates "Started."

9 **Click Open, then click the Directory tab.**

In the `DirectoryServer-1.example.com:1489` node, you should see the new user data store base suffix `dc=company,dc=com`.

▼ To Create a User Data Store Instance on Directory Server 2

1 **As a root user log in to the Directory Server 2 host.**

2 **Run the `netstat` command to be sure the that the Directory Server administration port is open.**

```
# cd /var/opt/mps/serverroot

# netstat –an | grep 1391
* 1390           *.*           0           0 49152           0 LISTEN
```

If the administration server is not running, start it now:

```
# ./start-admin
```

3 **Start the Directory Server console.**

```
# ./startconsole &
```

4 **Log in to the Directory Server console using the following information:**

Username	**cn=Directory Manager**

Password	**d1rm4n4ger**
Administration URL	**http://DirectoryServer-2.example.com:1391**

5 **Expand the** `example.com` **domain, the** `DirectoryServer-2.example.com` **node, and the Server Group object.**

You should see three Directory Server objects: an Administration Server, Directory Server (`ds-config`), and Directory Server (`am-config`).

6 **Right-click the Server Group object, and choose "Create Instance Of."**

Choose Sun Java System Directory Server.

7 **In the Create New Instance dialog, provide the following information and then click OK:**

Server Identifier:	**am-users**
Network port:	**1489**
Base suffix:	**dc=company,dc=com**
Directory Manager DN:	**cn=Directory Manager**
Directory Manager Password:	**d1rm4n4ger**
Confirm password:	**d1rm4n4ger**
Server Runtime (UNIX) user ID:	**nobody**

In the navigation tree, the new instance `Directory Server (am-users)` is added to the Server Group list.

8 **In the navigation tree, click the** `Directory Server (am-users)` **to open its console.**

Verify that the Server status indicates "Started."

9 **Click Open, then click the Directory tab.**

In the `DirectoryServer-2.example.com:1489` node, you should see the new user data store base suffix `dc=company,dc=com`.

▼ To Create a New Branch in the User Data Store

You only have to perform these steps on Directory Server 1. With multi-master replication enabled, all changes to the directory are automatically replicated to Directory Server 2.

1 **Log in to the Directory Server 1 console using the following information.**

Username	**cn=Directory Manager**

Password	**d1rm4n4ger**
Administration URL	**http://DirectoryServer-1.example.com:1391**

2. **In the navigation pane, expand the example.com suffix, and expand the Server Group objects.**
3. **Under Server Group, click the** `am-users` **instance.**
   In the `am-users` console properties page, click Open.
4. **Click the Directory tab,**
5. **Select New Instance, and then open the new instance.**
6. **Click the Directory tab.**
7. **Right click the** `dc=company, dc=com` **suffix, and choose "Create a new Organization Unit."**
8. **In the Create New Organizational Unit dialog, in the Name field, enter** `users`**, and then click OK.**
   On the Directory tab, click the `dc=company,dc=com` suffix. You should see the new `users` instance in the list.

▼ To Import Users into the User Data Store

In this procedure, you create four special accounts for the following users:

- The user `userdbadmin` will be used by the AccessManager servers to connect to the user data store for data management purposes.
- The user `userdbauthadmin` will be used by the AccessManager servers to authenticate users to the user data store.
- The user `testuser1` will be used to verify that the Policy Agent is configured properly.
- The user `testuser2` will be used to verify the working of the Policy Agent.

1. **Create an LDIF file named** `/tmp/am-users.ldif`**.**
   The file should contain the following users:

```
dn: uid=userdbadmin,ou=users,dc=company,dc=com
uid: userdbadmin
givenName: UserDB
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
```

```
sn: Admin
cn: UserDB Admin
userPassword: 4serd84dmin

dn: uid=userdbauthadmin,ou=users,dc=company,dc=com
uid: userdbauthadmin
givenName: UserDB
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: AuthAdmin
cn: UserDB AuthAdmin
userPassword: 4serd84uth4dmin

dn: uid=testuser1,ou=users,dc=company,dc=com
uid: testuser1
givenName: Test
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: User1
cn: Test User1
userPassword: password

dn: uid=testuser2,ou=users,dc=company,dc=com
uid: testuser2
givenName: Test
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: User2
cn: Test User2
userPassword: password
```

2 Import the LDIF file into the Directory Server-1 server.

```
# cd /var/opt/mps/serverroot/shared/bin
# ./ldapmodify -h DirectoryServer-1.example.com -p 1489 -D "cn=Directory Manager"
 -w d1rm4n4ger -a -f /tmp/am-users.ldif
adding new entry uid=userdbadmin,ou=users,dc=company,dc=com
adding new entry uid=userdbauthadmin,ou=users,dc=company,dc=com
```

3 **Verify that the new users were imported to Directory Server 1 with no errors.**

a. **In the Directory Server console,**

Expand Directory Server 1, expand the Server Group, click `am-users`, and then click Open.

Click Directory tab, expand the `dc=company, dc=com` suffix, and then click the `users` branch

b. **Verify that you can see four new users .**

7.2 Enabling Multi-Master Replication

In this procedure you enable multi-master replication (MMR) between two directory masters. Then you use the data and schema from the first directory master to initialize the second directory master. When you're finished, you will have two Directory Servers, and each will contain two instances. The instance named `ds-config` stores Directory Server administration configuration. The instance named `am-config` stores the user data and Access Manager configuration.

On each Directory Server, the `ds-config` instance is a local configuration instance. Do *not* replicate this instance to other host systems. On each Directory Server, the `am-config` instance is the directory data instance. You enable the `am-config` instance for MMR with its counterpart on the other Directory Server host.

Use the following as your checklist for enabling multi-master replication:

1. Enable multi-master replication on Directory Server 1.
2. Enable multi-master replication on Directory Server 2.
3. Create replication agreements on Directory Server 1.
4. Create replication agreements on Directory Server 2.
5. Initialize the master replica.

▼ To Enable Multi-Master Replication on Directory Server 1

1 **On Directory Server 1, start the Directory Server console.**

```
# cd /var/opt/mps/serverroot/
# ./startconsole &
```

2 **Log in to the Directory Server 1 console using the following information:**

Username **`cn=Directory Manager`**

Password	**d1rm4n4ger**
Administration URL	**http://DirectoryServer-1.example.com:1391**

3 In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.

4 Click to expand the Server Group.

You should see the following items: an Administration Server, a Directory Server (`am-config`), a Directory Server (`ds-config`), and a Directory Server (`am-users`).

5 Double-click the instance name `Directory Server (am-users)` to display the console for managing the instance `am-users`.

6 Click the Configuration tab and navigate to the Replication pane.

a. Expand the Data node.

b. Expand the node for the suffix you want to be a master replica.

In this example, double-click the suffix `dc=company,dc=com`.

c. Click Replication.

7 Click the "Enable replication" button to start the Replication Wizard.

8 Select Master Replica, and then click Next to continue.

9 Enter a Replica ID, and then click Next.

For this example, when enabling replication on DirectoryServer-1, assign the number 11.

10 If you have not already been prompted to select the change log file, you are prompted to select one now.

The default change log file is shown in the text field. If you do not wish to use the default, type in a filename for the change log, or click Browse to display a file selector. If the change log has already been enabled, the wizard will skip this step.

11 If you have not already been prompted to enter and confirm a password for the default replication manager, you are prompted now.

The replication manager is not used in the case of single-master replication, but you must still enter a password to proceed. For this example, enter **`replm4n4ger`**.

a. Click Next.

The Replication Wizard displays a status message while updating the replication configuration.

12 **Click Close when replication is finished.**

▼ To Enable Multi-Master Replication on Directory Server 2

1 **On Directory Server 2, start the Directory Server console.**

```
# cd /var/opt/mps/serverroot/
# ./startconsole &
```

2 **Log in to the Directory Server 2 console using the following information:**

Username	**`cn=Directory Manager`**
Password	**`d1rm4n4ger`**
Administration URL	**`http://DirectoryServer-2.example.com:1391`**

3 **In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.**

4 **Click to expand the Server Group.**

You should see the following items: an Administration Server, a Directory Server (`am-config`), a Directory Server (`ds-config`), and a Directory Server (`am-users`).

5 **Double-click the instance name `Directory Server (am-users)` to display the console for managing the instance `am-config`.**

6 **Click the Configuration tab and navigate to the Replication pane.**

a. **Expand the Data node.**

b. **Expand the node for the suffix you want to be a master replica.**

In this example, double-click the suffix `dc=company, dc=com`.

c. **Click Replication.**

7 **Click the "Enable replication" button to start the Replication Wizard.**

8 **Select Master Replica, and then click Next to continue.**

9. **Enter a Replica ID, and then click Next.**

   For this example, when enabling replication on DirectoryServer-2, assign the number 22.

10. **If you have not already been prompted to select the change log file, you are prompted to select one now.**

    The default change log file is shown in the text field. If you do not wish to use the default, type in a filename for the change log, or click Browse to display a file selector. If the change log has already been enabled, the wizard will skip this step.

11. **If you have not already been prompted to enter and confirm a password for the default replication manager, you are prompted now.**

    The replication manager is not used in the case of single-master replication, but you must still enter a password to proceed. For this example, enter **`replm4n4ger`**.

    a. **Click Next.**

    The Replication Wizard displays a status message while updating the replication configuration.

12. **Click Close when replication is finished.**

▼ To Create Replication Agreements on Directory Server 1

1. **On DirectoryServer-1, in the Directory Server console, display the general properties for the Directory Server instance named `am-users`.**

   Navigate through the tree in the left panel to find the Directory Server instance named `am-users`, and click on the instance name to display its general properties.

2. **Click the Open button to display the console for managing the `am-users` instance.**

3. **Click the Configuration tab and navigate to the Replication pane.**

   a. **Expand the Data node.**

   b. **Expand the node for the suffix you want to be a master replica.**

      In this example, double-click the suffix `dc=company,dc=com`.

   c. **Click Replication.**

4. **Click the New button.**

5. **In the Replication Agreement dialog box, click the Other button.**

6. **In the Remote Server dialog box, provide the following information, and then click OK.**

Host	`DirectoryServer-2.example.com`
Port	`1489`
Secure Port	Leave this box unmarked.

7. **In the Replication Agreement dialog, for the distinguished name (DN) of the replication manager entry on the consumer server, accept the default value.**

   By default, the DN is that of the default replication manager.

8. **For the password of the replication manager, enter `replm4n4ger`.**

9. **(Optional) Provide a description string for this agreement.**

   For this example, enter **`Replication from DirectoryServer-1 to DirectoryServer-2`**.

10. **Click OK when done.**

11. **In the confirmation dialog, click Yes to test the connection to the server and port number.**

    Use the given replication manager and password **`replm4n4ger`**.

    If the connection fails, you will still have the option of using this agreement. For example, the parameters are correct but the server is offline. When you have finished, the agreement appears in the list of replication agreements for this master replica.

▼ To Create Replication Agreements on Directory Server 2

1. **On DirectoryServer-2, in the Directory Server console, display the general properties for the Directory Server instance named `am-users`.**

   Navigate through the tree in the left panel to find the Directory Server instance named `am-users`, and click on the instance name to display its general properties.

2. **Click the Open button to display the console for managing the `am-users` instance.**

3. **Click the Configuration tab and navigate to the Replication pane.**

   a. **Expand the Data node.**

b. Expand the node for the suffix you want to be a master replica.

In this example, double-click the suffix `dc=company,dc=com`.

c. Click Replication.

4 Click the New button.

5 In the Replication Agreement dialog box, click the Other button.

6 In the Remote Server dialog box, provide the following information, and then click OK.

Host	`DirectoryServer-1.example.com`
Port	`1489`
Secure Port	Leave this box unmarked.

7 In the Replication Agreement dialog, for the distinguished name (DN) of the replication manager entry on the consumer server, accept the default value.

By default, the DN is that of the default replication manager.

8 For the password of the replication manager, enter `replm4n4ger`.

9 (Optional) Provide a description string for this agreement.

For this example, enter **`Replication from DirectoryServer-2 to DirectoryServer-1`**.

10 Click OK when done.

11 In the confirmation dialog, click Yes to test the connection to the server and port number.

Use the given replication manager and password.

If the connection fails, you will still have the option of using this agreement. For example, the parameters are correct but the server is offline. When you have finished, the agreement appears in the list of replication agreements for this master replica.

▼ To Initialize the Master Replica

1 On DirectoryServer–1, in the Directory Server console, navigate through the tree in the left panel to find the Directory Server instance named `am-users`, and click on the instance name to display its general properties.

2 Double-click the instance name `Directory Server (am-users)` in the tree to display the console for managing the data.

3. **Click the Configuration tab and navigate to the Replication pane.**

   a. **Expand the Data node.**

   b. **Expand the node for the suffix you want to be a master replica.**
      In this example, double-click the suffix `dc=company,dc=com`.

   c. **Click Replication.**

4. **In the list of defined agreements, select the replication agreement corresponding to DirectoryServer-2, the consumer you want to initialize.**

5. **Click Action > Initialize remote replica.**
   A confirmation message warns you that any information already stored in the replica on the consumer will be removed.

6. **In the Confirmation dialog, click Yes.**
   Online consumer initialization begins immediately. The icon of the replication agreement shows a red gear to indicate the status of the initialization process.

7. **Click Refresh > Continuous Refresh to follow the status of the consumer initialization.**
   Any messages for the highlighted agreement will appear in the text box below the list.

8. **Verify that replication is working properly.**

   a. **Log in to both Directory Server hosts as a root user, and start both Directory Server consoles.**

   b. **Log in to each Directory Server console.**

   c. **In each Directory Server console, enable the audit log on both Directory Server instances.**
      Go to Configuration > Logs > Audit Log. Check Enable Logging, and then click Save.

   d. **In separate terminal windows , use the `tail -f` command to watch the audit log files change.**

   e. **On DirectoryServer-1, in the Directory Server console, create a new user entry.**

      - Go to the Directory tab, and expand the suffix `dc=company,dc=com`.
      - Right-click `users`, and then choose New > User.
      - In the Create New User dialog, enter a first name and last name, an then click OK.

      Note the user entry is created in the instance audit log. Check to be sure the same entry is also created in on DirectoryServer-2 in the Directory Server instance audit log

f. On DirectoryServer-2, in the Directory Server console, create a new user entry.

- Go to the Directory tab, and expand the suffix `dc=company,dc=com`.
- Right-click `users`, and then choose New > User.
- In the Create New User dialog, enter a first name and last name, an then click OK.

  Note the user entry is created in the instance audit log. Check to be sure the same entry is also created in on DirectoryServer-1 in the Directory Server instance audit log

g. Delete both new user entries in the Directory Server 2 console.

Look in the Directory Server 1 console to verify that both users have been deleted.

7.3 Configuring the User Data Stores Load Balancer

- Contact your network administrator to obtain an available virtual IP address for the load balancer you want to configure.

  You must also know the IP address of the load balancer hardware, the URL for the load balancer login page, and a username and password for logging in to the load balancer application.

Note – The load balancer hardware and software used in the lab facility for this deployment is BIG-IP® manufactured by F5 Networks. If you are using different load balancer software, see the documentation that comes with that product for detailed settings information.

- You must also have ready the IP addresses for Directory Server 1 and Directory Server 2.

  To obtain these IP addresses, on each Directory Server host, run the following command:

  ```
  ifconfig –a
  ```

▼ To Configure the User Data Stores Load Balancer

1 Create a Pool.

A pool contains all the backend server instances.

a. Go to URL for the Big IP load balancer login page.

b. Open the Configuration Utility.

Click “Configure your BIG-IP (R) using the Configuration Utility.”

c. In the left pane, click Pools.

d. On the Pools tab, click the Add button.

e. In the Add Pool dialog, provide the following information:

Pool Name	Example: `DirectoryServer-UserData-Pool`
Load Balancing Method	Round Robin
Resources	Add the IP address of both Directory Server hosts. In this case, add the IP address and port number for `DirectoryServer-1:1489` and for `DirectoryServer-2:1489`.

f. Click the Done button.

2 Add a Virtual Server.

If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

a. In the left frame, Click Virtual Servers.

b. On the Virtual Servers tab, click the Add button.

c. In the Add a Virtual Server dialog box, provide the following information:

Address	xxx.xx.69.14 (for `LoadBalancer-2.example.com`)
Service	`489`
Pool	`DirectoryServer-UserData-Pool`

d. Continue to click Next until you reach the Pool Selection dialog box.

e. In the Pool Selection dialog box, assign the Pool (DirectoryServer-POOL) that you have just created.

f. Click the Done button.

3 Add Monitors

Monitors are required for the load balancer to detect the backend server failures.

a. In the left frame, click Monitors.

b. Click the Basic Associations tab.

c. Add an LDAP monitor for the Directory Server 1 node.

Three columns exist on this page: Node, Node Address, and Service. In the Node column, locate the IP address and port number `DirectoryServer-1:1489` . Select the Add checkbox.

d. Add an LDAP monitor for the Directory Server 2 node.

In the Node column, locate the IP address and port number for `DirectoryServer–2:1489`. Select the Add checkbox.

e. At the top of the Node column, in the drop-down list, choose `ldap-tcp`.

f. Click Apply.

4 Configure the load balancer for persistence.

a. In the left frame, click Pools.

b. Click the name of the pool you want to configure.

In this example, `DirectoryServer-UserData-Pool`.

c. Click the Persistence tab.

d. On the Persistence tab, under Persistence Type, select None.

e. Click Apply.

5 Verify the Directory Server load balancer configuration.

a. Log in as a root user to the host of each Directory Server.

b. On each Directory Server host, use the `tail` command to monitor the Directory Server access log.

```
# cd /var/opt/mps/serverroot/slapd-am-users/logs

# tail -f access
```

You should see connections to the load balancer IP address opening and closing. Example:

```
[12/Oct/2006:13:10:20-0700] conn=54 op=-1 msgId=-1 –
fd=22 slot=22 LDAP connection from xxx.xx.69.18 to xxx.xx.72.33

[12/Oct/2006:13:10:20-0700] conn=54 op=-1 msgId=-1 – closing – B1

[12/Oct/2006:13:10:20-0700] conn=54 op=-1 msgId=-1 – closed.
```

c. Execute the following LDAP search against the Directory Server load balancer:

```
# cd /var/opt/mps/serverroot/shared/bin/
# ./ldapsearch -h LoadBalancer-2.example.com -p 1489 -b "dc=company,dc=com"
-D "cn=directory manager" -w d1rm4n4ger "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Make sure the directory access entries display in only one Directory Server access log.

d. Stop Directory Server 1, and again perform the following LDAP search against the Directory Server load balancer:

```
# cd /var/opt/mps/serverroot/slapd-am-config
# ./stop
# cd /var/opt/mps/serverroot/shared/bin/
# ./ldapsearch -h LoadBalancer-2.example.com -p 1489 -b "dc=company,dc=com"
-D "cn=directory manager" -w d1rm4n4ger "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Verify that the Directory Server access entries display in only one Directory Server access log.

You may encounter the following error message:

```
ldap_simple_bind: Cant' connect to the LDAP
server – Connection refused
```

In the Load Balancer configuration page, reset the timeout properties to lower values.

- **Click the Monitors tab, and click the ldap-tcp monitor name.**
- **In the Interval field, set the value to** `5`**.**
- **In the Timeout field, set the value to** `16`**.**

  The default is 16 seconds. You can change this number to any value. In this deployment example, the BigIP documentation recommends the value should be at least three times the interval number of seconds plus one second.

- **Click Apply.**

Repeat the LDAP search.

e. Restart the stopped Directory Server 1, and then stop Directory Server 2.

Confirm that the requests are forwarded to the running Directory Server 1.

f. Perform the following LDAP search against the Directory Server load balancer.

```
# cd /var/opt/mps/serverroot/shared/bin/
# ./ldapsearch -h LoadBalancer-2.example.com -p 1489 -b "dc=company,dc=com"
-D "cn=Directory Manager" - w d1rm4n4ger "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Make sure the directory access entries display in only the one Directory Server access log.

7.4 Configuring a User Realm

Create a new realm that you can use to authenticate against only the existing Directory Server. The two Access Manager servers share configuration, so you configure the new realm on just one Access Manager server.

Use the following as your checklist for creating a user realm:

1. Create a new realm.
2. Configure a realm alias .
3. Configure the realm authentication.
4. Configure Access Manager to use roles from the user data store.
5. Configure the user data stores.

▼ To Create a New Realm

1 Start a new browser and log in to the first Access Manager server.

Go to the URL `http://AccessManager-1.example.com:1080/amserver/console`

2 Log in as a root user to the Access Manager console using the following information:

User Name: **`amadmin`**

Password: **`4m4dmin1`**

3 Click the Access Control tab, and then click New.

4 In the New Realm page, in the Name field, enter `users` .

5 Click OK.

▼ To Configure a Realm Alias

1 On the Access Control tab, under Realms, click the Realm Name `users`.

2 On the General tab for users-Properties, add `users` to the Realm/DNS/Aliases list.

In the Add field enter **`users`**, and then click Add.

3 **Click Save.**

▼ To Configure the Realm Authentication

1 **Modify the User Profile.**

a. **Click Realms.**

b. **On the Access Control tab, under Realms, select the new realm** `users`**.**

c. **Click the Authentication tab.**

d. **In the General section, click Advanced Properties.**

e. **In the Core page, in the Realm Attributes section, change the User Profile attribute to** `Ignored`**.**

Access Manager is configured to use only the existing Directory Server for authentication, and a full User Profile may not exist. That's why the attribute is set to `Ignored` in this example.

f. **Click Save.**

The changes are saved, and the Core > Realm Attributes page is displayed.

2 **Create a new authentication module.**

a. **Click Edit Realm to return to the** `users – Authentication` **page.**

b. **In the Module Instances section, click New.**

c. **In the New Module Instance page set the following attributes:**

Name Enter `usersLDAP`.

Type Choose LDAP.

d. **Click Create.**

The new module is created, and the `users – Authentication` page is displayed.

3 **Configure the new realm.**

a. **In the** `users – Authentication` **page, in the New Module Instances section, click the New Instance named** `usersLDAP`**.**

b. In the LDAP > Realm Attributes page, set the following attributes:

Primary LDAP Server	a. In the Add field, enter the hostname and port number for the load balancer for the user data store:`LoadBalancer-2.example.com:489`. b. In the server listbox, select the default server, then click Remove.
DN to Start User Search	a. In the Add field, enter `dc=company,dc=com` and then click Add. b. Select the default entry `o=example.com`, and then click Remove.
DN for Root User Bind	`uid=userdbauthadmin,ou=users,dc=company,dc=com`
Password for Root User Bind	`4serd84uth4dmin`
Password for Root User Bind (confirm)	`4serd84uth4dmin`

These values were imported into the user data store in a previous task. See "To Import Users into the User Data Store" on page 137.

c. Click Save.

The changes are saved, and the `users` — Authentication page is displayed.

4 Configure the default `ldapService` chain to use the new authentication module.

a. In the Authentication Chaining section, click on the default `ldapService` chain to configure it.

b. On the `ldapService` - Edit Authentication Chain page, in the Instance column, choose `usersLDAP`.

c. In the Criteria column, set the attribute to `Required`.

d. Click Save.

5 **Remove the LDAP authentication module.**

This module is automatically inherited from the default realm and it authenticates against the Access Manager configuration directory. The module is no longer needed now that the `usersLDAP` module will be used for authentication.

a. **Click Edit Realm >** `users`**.**

b. **Under Module Instances section, mark the checkbox for the existing realm named LDAP.**

c. **Click Delete.**

The LDAP authentication module is deleted, and the `users` — Authentication page is displayed.

6 **On the** `users` **— Authentication page, click Save.**

Changes you made in the previous steps are saved.

▼ To Configure Access Manager to Use Roles from the User Data Store

This procedure is not required to make Access Manager work in all scenarios because not all scenarios require role support. The procedure is required in this deployment example because policies are created in later procedures, and the policies will refer to roles.

1 **On the Access Control tab, under Realms, click the** `users` **link.**

2 **Click the Data Stores tab, and then click the** `usersLDAP` **link.**

3 **On the Edit Data Store page, in the section "LDAPv3 Plugin Supported Types and Operations," in the Add field, enter** `role=read,create,edit,delete`**, and then click Add.**

4 **In the section, "LDAP User Attributes," in the Add field, enter** `nsrole`**, and then click Add.**

5 **In the Add field, enter** `nsroledn`**, and then click Add.**

6 **Click Save.**

7 **Edit the Top-Level Realm.**

Click Edit Realm.

a. **Click Subjects > Role.**

Two roles `employee` and `manager` are in the Roles list.

b. Click the Users tab, and then click the `testuser1` link.

c. Click on the Role tab.

Verify that `testuser1` is added to the `manager` role. The role `manager` is displayed in the list of selected roles.

d. Click Edit Realm —users, and then click the `testuser2` link.

e. Click on the Role tab.

Verify that `testuser2` is added to the `employee` role. The role `employee` is displayed in the list of selected roles.

f. Click Edit Realm —users, and then click the `testuser2` link.

▼ To Configure the User Data Stores

1 Delete the default data store.

a. In the sub-realm `users` Authentication page, click the Data Stores tab.

b. In the sub-realm `users` Data Stores page, mark the checkbox for `amSDK1`, the default data store.

c. Click Delete.

2 Create a new data store.

a. Click New .

b. In the "Step 1 of 2: Select Type of Data Store" page, set the following attributes:

Name Enter **`usersLDAP`**.

Type Choose "LDAPv3 Repository Plug-In."

c. Click Next.

d. In the "Step 2 of 2: New Data Store" page, set the following attributes:

Primary LDAP Server	a. In the Add field, enter the hostname and port number for the existing directory. Use the form `LoadBalancer-2.example.com:489` b. Select the default `DirectoryServer-1.example.com:1389`, and then click Remove.
LDAP Bind DN	Enter **`uid=userdbadmin,ou=users,dc=company,dc=com`**.
Password for Root User Bind	`4serd84dmin`
Password for Root User Bind (confirm)	`4serd84dmin`
LDAP Organization DN	Enter **`dc=company,dc=com`**.
LDAP People Container Value	`users` When this field is empty, the search for users will start from the root suffix.
Persistent Search Base DN	Enter **`dc=company,dc=com`**.

These values were imported into the user data store in a previous task. See "To Import Users into the User Data Store" on page 137.

e. Click Finish and log out of the Access Manager console.

3 Restart each Access Manager server for the changes to take place.

Log in to each Access Manager host system, and restart the Web Server on each host system.

4 Verify that in the Access Manager console you can see the users in the external user data store.

a. Go to the Access Manager URL.

`http://AccessManager-1.example.com:1080/amserver/UI/Login`

b. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

c. Click on Users Realm.

d. Click on Subjects tab.

You should see three new users: `authuiadmin`, `userdbadmin`, and `userdbauthadmin`.

5 Verify that a user can successfully authenticate against the new realm.

a. Start a new browser session and log in to Access Manager.

Go to the following URL:

```
http://AccessManager-1.example.com:1080/amserver/UI/Login?realm=users
```

The parameter `realm=users` specifies the new realm to use for authentication. Without the parameter, the default realm is used.

b. On the login page, provide a user login and password from the existing directory.

User Name: **`authuiadmin`**

Password: **`4uthu14dmin`**

You should be able to log in successfully.

If the login is not successful, watch the existing Directory Server access log to troubleshoot the problem.

At this point, a user can log in against the existing Directory Server if he invokes the *realm=users* parameter. If such a parameter is absent, the default realm is used.

Administrators who want to access the Access Manager console should log in to the default realm.

7.5 (Optional) Enabling Access Manager to Manage Users in the Existing User Data Store

You can user the Access Manager console to create, edit, and delete user profiles in your existing data store. The procedures in this section are optional.

Access Manager typically is used more for policy management than for user management. In most cases, the user repository is a different repository than the one used by Access Manager to store its configuration. Administrators usually prefer to manage the user repository separately or differently from the Access Manager repository. However, at some times administrators find it necessary to manage the assignment of Access Manager services to users or roles. For convenience, administrators can to do this through the Access Manager console. The relevant AM objectclasses must be imported into the user repository so that Access Manager can read and write Access Manager service properties into the relevant entries in the user repository.

Use the following as your checklist for enabling Access Manager to manage users in the existing data store:

1. Configure Access Manager to manage users in an existing user data store.
2. Verify that user management with the existing data store works properly.

▼ To Configure Access Manager to Manage Users in an Existing User Data Store

1 Copy Access Manager schema to Directory Server 1.

a. As a root user log into host DirectoryServer–1.

b. At the command line, run the following `copy` command:

```
# cp /var/opt/mps/serverroot/slapd-am-config/config/schema/99user.ldif
/var/opt/mps/serverroot/slapd-am-users/config/schema/98am-schema.ldif
```

2 Copy Access Manager schema to Directory Server 2.

a. As a root user, log into host DirectoryServer–2.

b. At the command line, run the following `copy` command:

```
# cp /var/opt/mps/serverroot/slapd-am-config/config/schema/99user.ldif
/var/opt/mps/serverroot/slapd-am-users/config/schema/98am-schema.ldif
```

3 Start the Directory Server 1 console.

```
# cd /var/opt/mps/serverroot
# ./startconsole &
```

4 Log in to the Directory Server 1 console using the following information:

Username	**`cn=Directory Manager`**
Password	**`d1rm4n4ger`**
Administration URL	**`http://DirectoryServer-1.example.com:1391`**

5 Create a new Access Control Instruction (ACI).

a. In the Directory Server console, in the navigation tree, expand the Server Group object and then click on the `am-users` instance.

b. On the Directory Server page for am-users, click Open.

c. **Click the Directory tab.**

d. **In the navigation tree, click the** `dc=company, dc=com` **suffix.**

e. **Double-click the Directory Administrators group.**

f. **On the Edit Entry page for Directory Administrators, click Members.**

g. **On the Static Group page, click Add.**

h. **In the Search dialog, click Search.**

i. **In the results list, click the User ID** `userdbadmin`**.**

The Member User ID `userdbadmin` is now added to the Static Group list.

Click OK.

6 **Set access permissions.**

a. **On the Directory tab, in the navigation tree, right— click the** `dc=company, dc=com` **suffix, and the select Set Access Permissions.**

b. **In the Manage Access Control dialog, click New.**

c. **In the Edit ACI dialog, in the ACI name field, enter** `Directory Administrators`**.**

d. **In the list of Users/Groups, select All Users, and then click Remove.**

e. **Click Add.**

f. **In the Add Users and Groups, click Search.**

g. **In the Search results list, select Directory Administrators, and then click Add.**

h. **Click OK.**

The group Directory Administrators group is now displayed in the list of Users/Groups who have access permission.

i. **Click the Target tab.**

j. **In the "Target directory entry," click This Entry.**

The `dc=company,dc=com suffix` is displayed.

k. Click OK.

The Directory Administrators group is displayed in the Manage Access Control dialog.

l. Click OK, and then log out of Directory Server 1.

7 Restart both Directory Server 1 and Directory Server 2.

a. Log in as a root user to the Directory Server 1 host.

```
# cd /var/opt/mps/serverroot
# ./restart
```

b. Log in as a root user to the Directory Server 2 host.

```
# cd /var/opt/mps/serverroot
# ./restart
```

Tip – If you see errors such as the following on the command line:

```
[13/Oct/2006:12:43:39 -0700] - ERROR<5895> - Schema  -
conn=-1 op=-1 msgId=-1 -
User error:  Entry "cn=schema", single-valued attribute
"modifyTimestamp" has multiple values
```

then run the following commands:

```
# cd config/schema # edit file 98am-schema.ldif
# remove the entries:
        modifiersName: cn=directory manager
        modifyTimestamp: 20060913190551Z
# cd ../..
# ./restart-slapd
```

---

8 Restart both Access Manager 1 and Access Manager 2.

a. Log in as a root user to the AccessManager-1 host.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1
# ./stop; ./start
```

b. Log in as a root user to the AccessManager-2 host.

```
# cd /opt/SUNWwbsvr/https-AccessManager-2
# ./stop; ./start
```

▼ To Verify that User Management with the Existing Data Store Works Properly

1 **In a browser, go to the following Access Manager URL:**

`https://loadbalancer-3.example.com:9443/amserver/UI/Login`

2 **Log in to the Access Manager console using the following information:**

Username **amadmin**

Password **4m4dmin1**

3 **Add a new user.**

a. **On the Realms page, click the** `users` **link.**

b. **Click the Subjects tab.**

c. **On the User page, under User, click New.**

d. **On the New User page, provide the following information, and then click Create:**

ID: **johndoe**

First Name: **John**

Last Name: **Doe**

Full Name: **John Doe**

Password: **password**

Password Confirm: **password**

John Doe is now displayed in the list of Users. This indicates the user created in Access Manager was also created in Directory Server. Changes to the user profile were updated in Directory Server.

e. **Modify the John Doe entry.**

i. **Click the UserID for** `johndoe`**.**

ii. **In the Edit User dialog, in the Full Name field, enter** `John Michael Doe`**, and then click Save.**

You can see changes reflected in Access Manager. Changes to the user profile were also updated in Directory Server.

4 Log in as a root user to the host DirectoryServer-1.

a. Start the Directory Server console:

```
# cd /var/opt/mps/serverroot
# ./startconsole &
```

b. Log in to the Directory Server console using the following information:

Username	**cn=Directory Manager**
Password	**d1rm4n4ger**
Administration URL	**http://DirectoryServer-1.example.com:1391**

c. In the navigation tree, expand the DirectoryServer-1 node, and expand the Server Group.

d. Click the `am-users` instance.

e. On the Directory Server page for `am-users`, click Open.

f. Click the Directory tab.

g. Click the `dc=company,dc=com` suffix, and then click the `users` group.

h. In the list of users, double-click the `johndoe`entry.

In the Edit User page, verify that the information is the same as the information you entered through the Access Manager console in the previous steps.

Leave the Directory Server console open.

5 In the Access Manager console, create a new role and add John Doe to the role.

a. In the Realms page for `users`, click the Subjects tab.

b. Click the Role tab.

c. Under Roles, click New Role.

d. In the Role page, in the Name field, enter testRole.

e. Click Create.

The new role `testRole` is now displayed in the list of roles.

f. Click the `testRole` link.

g. **Click the User tab.**

h. **In the Edit Role page for** `testRole`**, in the Available list, select** `johndoe`**.**

i. **Click Add.**
The user `johndoe` is added to the Selected list.

j. **Click Save.**
John Doe is now added to the `testRole` role.

6 **Verify that the new user and role are created in Directory Server.**

a. **In the** `am-users` **instance, on the Directory tab, click the** `dc=company,dc=com` `suffix`**.**
The role `testRole` is included in the right pane.

b. **Double-click** `testRole`**.**

c. **In the Edit Role dialog, click Members.**
Verify that John Michael Doe is included in the list of members.

◆ ◆ ◆ CHAPTER 8

Installing and Configuring the Protected Resources with Policy Agents

This chapter contains detailed instructions for the following tasks:

8.1 Installing Web Server 1 and Web Policy Agent 1

Use the following as your checklist for installing Web Server 1 and Web Policy Agent 1:

1. Install Web Server 1 on Protected Resource 1.
2. Install Web Policy Agent 1.
3. Verify that Web Policy Agent 1 works properly.
4. Import the root CA certificate into the Web Server 1 key store.
5. Verify that the Web Policy Agent is working properly.
6. Create an agent profile on Access Manager.
7. Configure the Web Policy Agent to use the new agent profile.
8. Verify that the Web Policy Agent is working properly.

For this part of the deployment, you must have the JES 5 installer and Web Policy Agent installer mounted on the host Protected Resource 1. See "3.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer" on page 32 at the beginning of this manual.

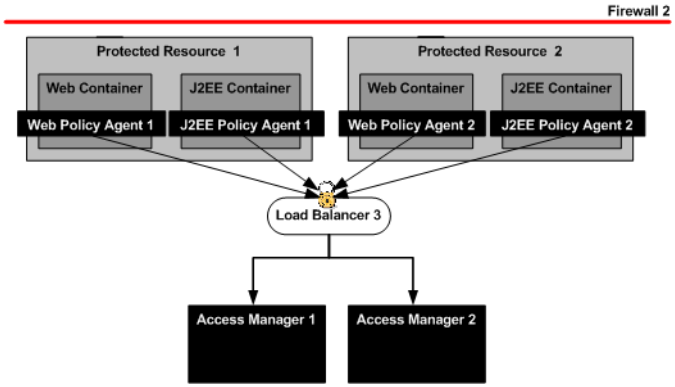

FIGURE 8–1 Protected Resources and Policy Agents

▼ To Install Web Server 1 on Protected Resource 1

1 As a root user, log into host ProtectedResource-1.

2 Start the Java Enterprise System installer with the `-nodisplay` option.

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

3 When prompted, provide the following information:

`Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>`	Press Enter.
`<Press ENTER to display the Software License Agreement>`	Press Enter.
`Have you read, and do you accept, all of the termsof the preceding Software License Agreement [No]`	Enter **y**.
`Please enter a comma separated list of languages you would like supported with this installation [8]`	Enter 8 for "English only."
`Enter a comma separated list of products to install,or press R to refresh the list []`	Enter **3** to select Web Server.
`Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]`	Press Enter.

`Enter 1 to upgrade these shared components and 2 to cancel [1]`	You are prompted to upgrade shared components only if the installer detects that an upgrade is required. Enter **1** to upgrade shared components.
`Enter the name of the target installation directory for each product: Web Server [/opt/SUNWwbsvr] :`	Accept the default value.
`System ready for installation Enter 1 to continue [1]`	Enter **1**.
`1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]`	Enter **1**.
`Common Server Settings Enter Host Name [ProtectedResource-1]`	Accept the default value.
`Enter DNS Domain Name [example.com]`	Accept the default value.
`Enter IP Address [xxx.xx.87.180]`	Accept the default value.
`Enter Server admin User ID [admin]`	Enter **admin**.
`Enter Admin User's Password (Password cannot be less than 8 characters) []`	For this example, enter **web4dmin**.
`Confirm Admin User's Password []`	Enter the same password to confirm it.
`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Enter Server Admin User ID [admin]`	Accept the default value.
`Enter Admin User's Password []`	For this example, enter **web4dmin**.
`Enter Host Name [ProtectedResource-1.example.com]`	Accept the default value.
`Enter Administration Port [8888]`	Accept the default value.
`Enter Administration Server User ID [root]`	Accept the default value.
`Enter System User ID [webservd]`	Enter **root**.
`Enter System Group [webservd]`	Enter **root**.

`Enter HTTP Port [80]`	Enter **`1080`**.
`Enter content Root [/opt/SUNWwbsvr/docs]`	Accept the default value.
`Do you want to automatically start Web Serverwhen system re-starts.(Y/N) [N]`	Accept the default value.
`Ready to Install 1. Install 2. Start Over 3. Exit Installation What would you like to do [1]`	First, see the next numbered (Optional) step. When ready to install, enter **`1`**.

4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:

```
# cd /var/sadm/install/logs

# tail –f Java_Enterprise_System_install.B xxxxxx
```

5 Upon successful installation, enter `!` to exit.

6 Verify that the Web Server is installed properly.

a. Start the Web Server administration server to verify it starts with no errors.

```
# cd /opt/SUNWwbsvr/https-admserv

# ./stop; ./start
```

b. Run the `netstat` command to verify that the Web Server ports are open and listening.

```
# netstat -an | grep 8888
  *.8888           *.*           0        0    49152        0    LISTEN
```

c. Go to the Web Server URL.

`http://ProtectedResource-1.example.com:8888`

d. Log in to the Web Server using the following information:

Username **`admin`**

Password **`web4dmin`**

You should be able to see the Web Server console. You can log out of the console now.

e. Start the Protected Resource 1 instance.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-1.example.com
# ./stop; ./start
```

f. Run the `netstat` command to verify that the Web Server ports are open and listening.

```
# netstat -an | grep 1080
  *.1080           *.*           0        0    49152        0    LISTEN
```

g. Go to the instance URL.

```
http://ProtectedResource-1.example.com:1080
```

You should see the default Web Server index page.

▼ To Install Web Policy Agent 1

Before You Begin

Caution – Due to a known problem with this version of the Web Policy Agent, you must start an X-display session on the server host using a program such as Reflections X or VNC, even though you use the command-line installer. For more information about this known problem, see `http://docs.sun.com/app/docs/doc/819-2796/6n52flfoq?a=view#adtcd`.

1 As a root user, log into to host ProtectedResource–1.

2 Download the Java System Web Policy Agents 2.2 package from the following website:

`http://www.sun.com/download`

3 Unpack the downloaded package.

In this example, the package was downloaded into the directory `/temp`.

```
# cd /temp
# gunzip sun-one-policy-agent-2.2-es6-solaris_sparc.tar.gz
# tar –xvof sun-one-policy-agent-2.2-es6-solaris_sparc.tar
```

4 Start the Web Policy Agents installer.

```
# ./setup -nodisplay
```

5 When prompted, provide the following information:

`When you are ready, press Enter to continue.` `<Press ENTER to Continue>`	Press Enter.
`Press ENTER to display the Sun Software` `License Agreement`	Press Enter.

`Have you read, and do you accept, all of`
`the terms of the preceding Software License`
`Agreement [no] y`
	Enter **y**.

`Install the Sun Java(tm) System Access Manager` `Policy Agent in this directory [/opt] :`	Accept the default value.

`Enter information about the server instance this agent will protect.` `Host Name [ProtectedResource-2.example.com]:`	Accept the default value.
`Web Server Instance Directory []:`	Enter **`/opt/SUNWwbsvr/https-ProtectedResource-1.example.com`**
`Web Server Port [80]:  :`	Enter **`1080`**.
`Web Server Protocol [http]`	Accept the default value.
`Agent Deployment URI [/amagent]:`	Accept the default value.
`Enter the Sun Java(tm) System Access Manager Information for this Agent.` `Primary Server Host [ProtectedResource-2.example.com] :`	For this example, enter the external-facing load balancer host name. Example: **`LoadBalancer-3.example.com`**
`Primary Server Port [1080]`	Enter the load balancer HTTP port number. For this example, enter **`90`**.
`Primary Server Protocol [http]:`	Accept the default value.
`Primary Server Deployment URI [/amserver]:`	Accept the default value.
`Primary Console Deployment URI [/amconsole] :`	Accept the default value.
`Failover Server Host [] :`	Accept the default value.
`Agent-Access Manager Shared Secret:`	Enter the `amldapuser` password that was entered when Access Manager was installed. For this example, enter **`4mld4puser`** .
`Re-enter Shared Secret:`	Enter the **`4mld4puser`** password again to confirm it.
`CDSSO Enabled [false]:`	Accept the default value.
`Press "Enter" when you are ready to continue.`	First, see the next (Optional) numbered step. When you are ready to start installation, press Enter.

6 (Optional) During installation, you can monitor the log to watch for installation errors. Example:

```
# cd /var/sadm/install/logs
# tail –f var/sadm/install/logs/
Sun_Java_tm__System_Access_Manager_Policy_Agent_install.B<xxxxxxxx>
```

7 Modify the `AMAgent.properties` file.

```
# cd /etc/opt/SUNWam/agents/es6/
config/_opt_SUNWwbsvr_https-ProtectedResource-1.example.com
```

Make a backup of `AMAgent.properties` before setting the following property:

```
com.sun.am.policy.am.login.url =
https://LoadBalancer-4.example.com:9443/distAuth/UI/Login?realm=users
```

8 Restart the Web Server.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-1.example.com
# ./stop; ./start
```

Examine the Web Server log for startup errors.

```
# /opt/SUNWwbsvr/https-ProtectedResource-1.example.com/logs
# vi errors
```

▼ To Verify that Web Policy Agent 1 Works Properly

1 Start a new browser and go to the Access Manager URL.

Example: `https://loadbalancer-3.example.com:9443/amserver/console`

2 Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

3 Create a referral policy in the top-level realm.

a. On the Access Control tab, under Realms, click `example.com`.

b. Click the Policies tab.

c. On the Policies tab for example.com-Policies, click New Referral.

d. In the New Policy page, provide the following information:

Name: Referral URL Policy for users realm.

Active: Mark the Yes checkbox.

e. On the same page, in the Rules section, click New.

f. Select a Service Type.

On the page "Step 1 of 2: Select Service Type for the Rule," select URL Policy Agent (with resource name)

g. Click Next.

h. On the page "Step 2 of 2: New Rule," provide the following information:

Name: **`URL Rule for ProtectedResource-1`**

Resource Name: **`http://ProtectedResource-1.example.com:1080/*`**

i. Click Finish.

j. On the same page, in the Referrals section, click New.

k. In the New Referral — Sub Realm page, provide the following information:

Name: Sub-Realm users

Filter: Type an asterisk (*), and then click Search.

Value: In the list, choose `users`.

l. Click Finish.

m. On the New Policy page, click Create.

In the Policies tab for example.com — Policies, you should see the policy named "Referral URL Policy for users realm."

4 Create a policy in the `users` realm.

a. Click Realms.

b. On the Access Control tab, under Realms, click the Realm Name `users`.

c. Click the Policies tab.

d. On the Policies tab for users-Policies, click New Policy.

e. In the New Policy page, provide the following information:

Name: **`URL Policy for ProtectedResource-1`**

Active: Mark the Yes checkbox.

f. On the same page, in the Rules section, click New.

g. On the page "Step 1 of 2: Select Service Type for the Rule," click Next.

The Service Type "URL Policy Agent (with resource name) is the only choice.

h. On the page "Step 2 of 2: New Rule," provide the following information:

Name: **`URL Rule for ProtectedResource-1`**

Resource Name:	Click the URL listed in the Parent Resource Name list: `http://ProtectedResource-1.example.com:1080/*` The URL is automatically added to the Resource Name field.
GET:	Mark this checkbox, and select the Allow value.
POST:	Mark this checkbox, and select the Allow value.

i. Click Finish.

5 Create a new subject.

On the New Policy page, in the Subjects section, click New.

a. Select the subject type and then click Next.

On the page "Step 1 of 2: Select Subject Type," select the "Access Manager Identity Subject" type.

b. On the page "Step 2 of 2: New Subject — Access Manager Identity Subject," provide the following information:

Name:	Enter **`Test Subject`**.
Filter:	Choose `User`, and then click Search. Four users are added to the Available list.
Available:	In the list, select`testuser1`, and then click Add. The user `testuser1` is added to the Selected list.

c. Click Finish.

6 In the New Policy page, click Create.

On the Policies tab for users-Policies, the new policy "URL Policy for ProtectedResource-1" is now in the Policies list.

7 Log out of the console.

8 Verify that an authorized user can access the Web Server 1.

a. Go to the following URL:

`http://ProtectedResource-1.example.com:1080`

b. Log in to Access Manager using the following information:

Username	**`testuser1`**
Password	**`password`**

You should see the default `index.html` page for Web Server 1.

The user `testuser1` was configured in the test policy to be allowed to access Protected Resource 1.

9 Verify that an unauthorized user cannot access the Web Server 1.

a. Go to the following URL:

`http://ProtectedResource-1.example.com:1080`

b. Log in to Access Manager using the following information:

Username **`testuser2`**

Password **`password`**

You should see the message, "You're not authorized to view this page."

The user `testuser2` was not included in the test policy tat allows access to Protected Resource 1.

▼ To Import the Root CA Certificate into the Web Server 1 Key Store

The Web Policy Agent on Protected Resource 1 connects to Access Manager servers through Load Balancer 3. The load balancer is SSL-enabled, so the agent must be able to trust the load balancer SSL certificate in order to establish the SSL connection. To do this, import the root CA certificate that issued the Load Balancer 3 SSL server certificate into the Web Policy Agent certificate store.

Before You Begin Obtain the root CA certificate, and copy it to ProtectedResource-1.

1 Copy the root CA certificate to Protected Resource 1.

2 Open a browser, and go to the Web Server 1 administration console.

`http://ProtectedResource-1.example.com:8888`

3 Log in to the Web Server 2 console using the following information:

User Name: **`admin`**

Password: **`web4dmin`**

4 In the Select a Server field, select `ProtectedResource-1.example.com`, and then click Manage.

Tip – If a "Configuration files have not been loaded" message is displayed, it may be that the administration server has never been accessed, and so the configuration files have never been loaded. First click Apply, and then click Apply Changes. The configuration files are read, and the server is stopped and restarted.

5 **Click the Security tab.**

6 **On the Initialize Trust Database page, enter a Database Password.**

Enter the password again to confirm it, and then click OK.

7 **In the left frame, click Install Certificate and provide the following information, and then click OK:**

Certificate For:	Choose **`Trusted Certificate Authority (CA)`**.
Key Pair File Password:	**`password`**
Certificate Name:	**`OpenSSL_CA_Cert`**
Message in this File:	**`/export/software/ca.cert`**

8 **Click Add Server Certificate.**

9 **Click Manage Certificates.**

The root CA Certificate name `OpenSSL_CA_Cert` is included in the list of certificates.

10 **Click the Preferences tab.**

11 **Restart Web Server 2.**

On the Server On/Off page, click Server Off. When the server indicates that the administration server is off, click Server On.

12 **Configure the Web Policy Agent 1 to point to the Access Manager SSL port.**

a. **Edit the `AMAgent.properties` file.**

```
# cd /opt/SUNWam/agents/es5/config/
_optSUNWwbsvr_https=ProtectedResource-1.example.com
```

Make a backup of the `AMAgent.properties` file before setting the following property:

```
# com.sun.am.naming.url =
https://LoadBalancer-3.example.com:9443/amserver/namingservice
```

b. **Save the file.**

13 Restart Web Server 1.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-1.example.com
# ./stop; ./start
```

▼ To Verify that the Web Policy Agent is Working Properly

1 Verify that an authorized user can access the Web Server 1.

a. Go to the following URL:

`http://ProtectedResource-1.example.com:1080`

b. Log in to Access Manager using the following information:

Username **`testuser1`**

Password **`password`**

You should see the default `index.html` page for Web Server 1.

The user `testuser1` was configured in the test policy to be allowed to access Protected Resource 1.

2 Verify that an unauthorized user cannot access the Web Server 1.

a. Go to the following URL:

`http://ProtectedResource-1.example.com:1080`

b. Log in to Access Manager using the following information:

Username **`testuser2`**

Password **`password`**

You should see the message, "You're not authorized to view this page."

The user `testuser2` was not included in the test policy tat allows access to Protected Resource 1.

▼ To Create an Agent Profile on Access Manager

The web agent will, by default, use the account with the `uid` `UrlAccessAgent` to authenticate to Access Manager. Creating an agent profile is not a requirement for Web Policy Agents. You can use the default values and never change the Web Policy Agent user name. However, in certain

cases, you might want to change these default values. For example, if you want to audit the interactions between multiple agents and the Access Manager server, you want be able to distinguish one agent from another. This would not be possible if all the agents used the same default agent user account. For more information, see the *Sun Java System Access Manager Policy Agent 2.2 User's Guide*.

- **Create an agent profile on Access Manager.**

  This new account will be used by Web Policy Agent 1 to access the Access Manager server.

  a. **Go to Access Manage load balancer URL:**

     `https://LoadBalancer-3.example.com:9443/amserver/UI/Login`

  b. **Log in to the Access Manager console using the following information:**

     Username **`amadmin`**

     Password **`4m4dmin1`**

  c. **On the Access Control tab, under Realms, click the realm name** `example.com`**.**

  d. **Click the Subjects tab.**

  e. **Click the Agents tab.**

  f. **On the Agent page, click New.**

  g. **On the New Agent page, provide the following information:**

     ID: **`webagent-1`**

     Password: **`web4gent1`**

     Password Confirm: **`web4gent1`**

     Device State: Choose **`Active`**.

  h. **Click Create.**

     The new agent `webagent–1` is now display in the list of Agent Users.

▼ To Configure the Web Policy Agent to Use the New Agent Profile

1 **Log in to as a root user to Protected Resource 1.**

2 **Run the `cypt_util` utility.**

The utility encrypts the password.

```
# cd /opt/SUNWam/agents/bin
# ./crypt_util web4gent1
BXxzBswD+PZdMRDRMXQQA==
```

Copy the encrypted password, and save it in a text file.

3 **Edit the `AMAgent.properties` file.**

```
# cd /etc/opt/SUNWam/agents/es6/
config/_opt_SUNWwbsvr_https-ProtectedResource-1.example.com
```

Make a backup of `AMAgent.properties` you make the following change in the file:

```
com.sun.am.policy.am.password = webagent-1
com.sun.am.policy.am.password = BXxzBswD+PZdMRDRMXQQA==
```

Use the encrypted password obtained in the previous step.

Save the file.

4 **Restart Web Server 1.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-1.example.com
 # ./stop; ./start
```

▼ To Verify that the Web Policy Agent is Working Properly

1 **Verify that an authorized user can access the Web Server 1.**

a. **Go to the following URL:**

`http://ProtectedResource-1.example.com:1080`

b. **Log in to Access Manager using the following information:**

Username **`testuser1`**

Password **`password`**

You should see the default `index.html` page for Web Server 1.

The user `testuser1` was configured in the test policy to be allowed to access Protected Resource 1.

2 Verify that an unauthorized user cannot access the Web Server 1.

a. Go to the following URL:

`http://ProtectedResource-1.example.com:1080`

b. Log in to Access Manager using the following information:

Username **`testuser2`**

Password **`password`**

You should see the message, "You're not authorized to view this page."

The user `testuser2` was not included in the test policy tat allows access to Protected Resource 1.

8.2 Installing Application Server 1 and J2EE Policy Agent 1

You must have the WebLogic Application Server installer and the Sun J2EE Policy Agent installer mounted on Protected Resource 1.

Use the following as your checklist for installing Application Server 1 and the J2EE Policy Agent 1:

1. Install Application Server 1 on Protected Resource 1.
2. Create an agent profile on Access Manager.
3. Run the J2EE Policy Agent installer on Application Server 1.

▼ To Install Application Server 1 on Protected Resource 1

1 Obtain the Application Server installer from the BEA .

2 Start the installer.

```
# /download_directory/export/weblogic/server910_solaris32.bin
```

3 Provide the following information when prompted:

`Welcome...`
`You may quit the installer at any time by`
`typing "Exit."`
`Enter [Exit][Next]`
	Enter **`Next`**.

`Select Option:`
`1. Yes, I agree with the terms of`
`the license.`
`2. No, I do not agree with the terms`
`of the license.`
	Enter **`1`**.

`Choose BEA Home Directory [/usr/local/bea]:`	Press Enter to accept the default value and continue.

`Choose Install Type :`
`->1|Complete`
`  2|Custom`
	Enter **`2`**.

`Release 9.1.0.0`
`        WebLogic Server [1]`
`            Server [1.1]`
`            Server Examples [1.2]`
`            Web Server Plug-ins [1.3]`
 	
`Choose Componenets to install:`
	Press Enter to continue.

`Choose Product Directory [/usr/local/bea/weblogic91]:`	Press Enter to accept the default value and continue.

`Choose Product Directory`
`[Yes, use this product directory]:`
`->|Yes`
`  |No`
	Press Enter to confirm the default value and continue.

`Installation Complete` `Press [Enter] to continue...`	Press Enter.

4 Create a new domain.

a. Start the BEA WebLogic Configuration Wizard.

```
# cd /usr/local/bea/weblogic91/common/bin
# ./config.sh
```

b. Provide the following information:

`Welcome...`
 	
`->1| Create a new WebLogic domain.`
`  2| Extend an existing WebLogic domain.`
	Press Enter to accept the default value 1.

`Select Domain Source:`
`->1| Choose WebLogic Platform components`
`  2| Choose custom template`
	Press Enter to accept the default value 1.

`Application Template Selection:`
`Avaliable Templates`
`  WebLogic Server (Required)x`
`  Appache Behive [2]`
	Press Enter to accept the default value and continue.

`Configure Administrator Username and Password:`
`Select Option:`
`1- Modify "user name"`
`2- Modify "user password"`
`3- Modify "Confirm user password"`
`4- Modify "Description'`
`5- Discard changes`
	Enter **2** to modify the user password.

`Input User password :`	Enter **w3bl0g1c**.

`Configure Adminstrator Username and Password:`
`1- *User name:  weblogic`
`2- *User password:  ********`
`3- *Confirm user password:  ******`
`4- Description:  This user is the`
`default administrator`
 	
`Select Option:`
`1- Modify "user name"`
`2- Modify "user password"`
`3- Modify "Confirm user password"`
`4- Modify "Description'`
`5- Discard changes`
	Enter **3** to confirm user password.

`Confirm user password:`	Enter **w3bl0g1c**.

`Configure Adminstrator Username and Password:`
`1- *User name:  weblogic`
`2- *User password:  ********`
`3- *Confirm user password:  ********`
`4- Description:  This user is the`
`default administrator`
 	
`Select Option:`
`1- Modify "user name"`
`2- Modify "user password"`
`3- Modify "Confirm user password"`
`4- Modify "Description'`
`5- Discard changes`
	Press Enter to accept the values and continue.

`Domain Mode Configuration:`
`->1| Development Mode`
`  2| Production Mode`
	Enter **2** to select Production Mode.

`Java SDK Selection:`
`->1| Sun SDK 1.5.0_04 @ /usr/local/bea/jdk150_04`
`  2| Other Java SDK`
	Press Enter to accept the default value and continue.

`Choose Configuration Option:`
`  1|Yes`
`->2|No`
	Enter **1** .

`Configure the Adminstration Server:`
 	
`Select Option:`
`1- *Name:    AdminServer`
`2- Listen address:        All Local Addresses`
`3- Listen port:    7001`
`4- SSL listen port    :  N/A`
`5- SSl enabled:    false`
 	
`Select Option:`
`1- Modify "Name"`
`2- Modify "Listen address"`
`3- Modify "Listen port"`
`4- Modify "SSL enabled"`
	Press Enter to Continue.

`Configure Managed Servers:`
`Add or delete configuration information for`
`Managed Servers...`
 	
`Enter name for a new...`
	Enter **ApplicationServer-1**.

`Configure Managed Servers:`
`Add or delete configuration information for`
`Managed Servers...`
`Name:  ApplicationServer-1`
`Listen address:  All Local Addresses`
`Listen port:  7001`
`SSL listen port:  N/A`
`SSL enabled:  false`
 	
`Select Option:`
`1- Modify "Name"`
`2- Modify "Listen address"`
`3- Modify "Listen port"`
`4- Modify "SSL enabled"`
`5- Done`
	Enter **3** to modify the Listen port.

`Modify “Listen port.”`	Enter **1081**.

Configure Managed Servers: Add or delete configuration information for Managed Servers... Name: ApplicationServer-1 Listen address: All Local Addresses Listen port: 1081 SSL listen port: N/A SSL enabled: false Select Option: 1- Modify "Name" 2- Modify "Listen address" 3- Modify "Listen port" 4- Modify "SSL enabled" 5- Done	Press Enter to continue.
Configure Clusters: Enter name for a new Cluster	Press Enter to continue.
Configure Machines: Enter name for a new Machine	Press Enter to continue.
Configure Unix Machines: Enter name for a new Unix Machine	Enter **ProtectedResource-1**.
Configure Unix Machines: Add or delete configuration information for machines: 1- Name: ProtectedResource-1 2- Post bind GID enabled: false 3- Post bind GID: nobody 4- Post bind UID enabled: false 5- Post bind UID: nobody 6- Node manager listen address: localhost 7- Node manager listen port: 5556	Press Enter to accept these values.
Configure Unix machines: Name: ProtectedResource-1 Select Option: 1- Add Unix machine 2- Modify Unix machine 3- Delete unix machine 4- Discar Changes	Enter **1** to add a Unix machine.
Enter name for a new Unix Machine.	Enter **ProtectedResource-2**.

`Configure Unix Machines:`
`1- Name:  ProtectedResource-2`
`2- Post bind GID enbled:  false`
`2- Post bind GID:  nobody`
`4- Post bind UID enabled:  false`
`5- Post bind UID:  nobody`
`6-     Node manager listen address:  localhost`
`7- Node manager listen port:  5556`
	Press Enter to accept these values.

`Assign Servers to Machines:`
 	
`Machine`
`            Unix Machine`
`                        ProtectedResource-1 [1.1]`
`                        ProtectedResource-2    [1.2]`
	Press Enter to continue.

`Select the target domain directory for this domain:`	Press Enter to continue.
`Edit Domain Information:` `Enter value for "Name."`	Enter **`ProtectedResource-1`**.

`Edit Domain Information:`
`1- Name:    ProtectedResource-1`
 	
`Select Option:`
`1- Modify "Name"`
`2- Discard Changes`
	Press Enter to continue.

`Installation Complete` `Press [Enter] to continue...`	Press Enter.

5 Create two files necessary to automate Application Server 1 startup.

Create one file in the directory for the Application Server 1 administration server, and create one file in the Application Server 1 instance directory. The administrative user and password are stored in each file. Application Server 1 uses this information during server start-up. Without these files, Application Server 1 will fail to start. Application Server 1 encrypts the file, so there is no security risk even though you enter the user name and password in clear text.

```
# cd /usr/local/bea/user_projects/domains/
ProtectedResource-1/servers/AdminServer
# mkdir security
# cd security/
# cat > boot.properties
username=weblogic
password=w3bl0g1c
^D

# cd /usr/local/bea/user_projects/domains/
ProtectedResource-1/servers/ApplicationServer-1/
# mkdir security
```

```
# cd security/
# cat > boot.properties
username=weblogic
password=w3bl0g1c
^D
```

6 Start the servers.

```
# cd /usr/local/bea/user_projects/domains/
ProtectedResource-1/bin/
# nohup ./startWebLogic.sh &
#tail -f nohup.out

...
# netstat -an | grep 7001
xxx.xx.72.151.7001        *.*        0        0 49152        0 LISTEN
127.0.0.1.7001         *.*        0        0 49152        0 LISTEN
#
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin/
# nohup ./startManagedWebLogic.sh ApplicationServer-1
http://ProtectedResource-1.example.com:7001 &

# cd /usr/local/bea/user_projects/domains/
ProtectedResource-1/bin/
# netstat -an | grep    1081
xxx.xx.72.151.1081        *.*        0        0 49152        0 LISTEN
127.0.0.1.1081          *.*        0        0 49152        0 LISTEN
xxx.xx.72.151.33425  xxx.xx.72.151.1081    49152    0 49152
0 ESTABLISHED
xxx.xx.72.151.1081    xxx.xx.72.151.33425    49152    0 49152
0 ESTABLISHED
```

7 Verify that Application Server 1 is up and running.

a. Go to the following URL:

`http://ProtectedResource-1.example.com:7001/console`

b. Log in to the Application Server 1 console using the following information:

Username **`weblogic`**

Password **`w3bl0g1c`**

Verify that you can successfully log into the console.

c. Under Domain Structure , expand the Environment object

d. Click Servers.

On the Summary of Servers page, verify that both `AdminServer(admin)` and `ApplicationServer-1` are running and OK.

▼ To Create an Agent Profile on Access Manager

This new account will be used by J2EE Policy Agent 1 to authenticate to the Access Manager server.

1 Go to Access Manage load balancer URL:

`https://LoadBalancer-3.example.com:9443/amserver/UI/Login`

2 Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

3 On the Access Control tab, under Realms, click the realm name `example.com`.

4 Click the Subjects tab.

5 Click the Agents tab.

6 On the Agent page, click New.

7 On the New Agent page, provide the following information:

ID: **`j2eeagent-1`**

Password: **`j2ee4gent1`**

Password Confirm: **`j2ee4gent1`**

Device State: Choose **`Active`**.

8 Click Create.

The new agent `j2eeagent–1` is now display in the list of Agent Users.

9 Log out of the Access Manager console.

10 Create a text file, and add the Agent Profile password to the file.

The J2EE Policy Agent installer requires this file for installation.

```
# cd /opt/j2ee_agents/amwl9_agent
# cat > agent_pwd
```

```
j2ee4gent1
^D
```

▼ To Run the J2EE Policy Agent Installer on Application Server 1

Before You Begin Application Server 1 must be stopped when you install J2EE Policy Agent 1.

You must stop both the Application Server 1 instance and the administration server before installing J2EE Policy Agent 1.

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin/
# ./stopManagedWebLogic.sh ApplicationServer-1  t3://localhost:7001
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
# ./stopWebLogic.sh
```

1 Unpack the J2EE Policy Agent bits.

```
# cd /opt
# /usr/sfw/bin/gtar -xvf /export/software/SJS_Weblogic_9_agent_2.2.tar
```

2 Start the J2EE Policy Agent installer.

```
# cd /opt/j2ee_agents/am_wl9_agent/bin
# ./agentadmin --install
```

3 When prompted, provide the following information:

`Please read the following License Agreement carefully:`	Press Enter to continue. Continue to press Enter until you reach the end of the License Agreement.
`Enter startup script location.`	Enter . **`/usr/local/bea/user_projects/domains/ProtectedResource-1/bin/startwebLogic.sh`**
`Enter the WebLogic Server instance name: [myserver]`	Enter **`ApplicationServer-1`**.
`Access Manager Services Host:`	Enter **`LoadBalancer-3.example.com`**.
`Access Manager Services port: [80]`	Enter **`90`**.
`Access Manager Services Protocol: [http]`	Enter **`http`**.
`Access Manager Services Deployment URI: [/amserver]`	Accept the default value.

`Enter the Agent Host name:`	**`ProtectedResource-1.example.com`**
`Enter the WebLogic home directory: [usr/local/bea/weblogic90]`	Enter **`/usr/loca/bea/weblogic91`**.
`Enter the port number for Application Server instance [80]:`	Enter **`1081`**.
`Enter the Preferred Protocol for Application instance [http]:`	Accept the default value.
`Enter the Deployment URI for the Agent Application [/agentapp]`	Accept the default value.
`Enter the Encryption Key [Q558gNigkno4dGZmPtgGs4K1HL1153QD]:`	Accept the default value.
`Enter the Agent Profile name:`	Enter **`j2eeagent-1`**.
`Enter the path to the password file:`	Enter **`/opt/j2ee_agent/am_w19_agent/agent_pwd`**.
`Are the Agent and Access Manager installed on the same instance of Application Server? [false]:`	Accept the default value.

`Verify your settings and decide from the choices below:`
`1. Continue with Installation`
`2. Back to the last interaction`
`3. Start Over`
`4. Exit`
`Please make your selection [1]:`
	Accept the default value.

The J2EE Policy Agent installer creates a new file in the Application Server `bin` directory:

```
/usr/local/bea/user_projects/domains/ProtectedResource-1/bin/
setAgentEnv_ApplicationServer-1.sh
```

4 Modify the Application Server startup script to reference the new file.

a. As a root user, log into ProtectedResource–1.

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin/
```

b. Make a backup of `setDomainEnv.sh`.

c. In `setDomainEnv.sh`, insert the following line at the end of the file:

```
. /usr/local/bea/user_projects/domains/ProtectedResource-1/
bin/setAgentEnv_ApplicationServer-1.sh
```

This command references the file the installer created in the Application Server `bin` directory.

d. Save the `setDomainEnv.sh`file.

e. Change permissions for the `setAgentEnv_ApplicationServer-1.sh` file:

```
# chmod 755 setAgentEnv_ApplicationServer-1.sh
```

5 Start the Application Server administration server.

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

Watch for startup errors.

8.3 Completing the J2EE Policy Agent 1 Installation

The J2EE Policy Agent is not yet ready to begin working. In the following procedures, you deploy the policy agent application , setup up an authentication provider, and modify the Bypass Principal List. All of these tasks must be completed before the agent can do its job.

Use the following as your checklist for completing the J2EE Policy Agent 1 installation:

1. Modify the Application Server startup file.
2. Deploy the J2EE Policy agent application .
3. Start the agent application.
4. Set Up the agent authentication provider.
5. Edit the AMAgent.properties file.

▼ To Modify the Application Server Startup File

1 Go to the following Protected Resource 1 directory.

The J2EE Policy Agent installer creates a new file in the Application Server bin directory:

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
```

2 Make a backup of the file `setDomainEnv.sh`.

3 In the `setDomainEnv.sh` file, at the end of the file append the following:

```
echo "Setting Policy Agent Env..."  .
/usr/local/bea/user_projects/domains/ProtectedResource-1/bin/
setAgentEnv_ApplicationServer-1.sh
```

This command references the file the installer created in the Application Server `bin` directory.

4 **Save the `setDomainEnv.sh` file.**

5 **Change permissions for the `setAgentEnv_ApplicationServer-1.sh` file:**

```
# cdmod 755 setAgentEnv_ApplicationServer-1.sh
```

6 **Stop Application Server 1.**

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
# ./stopManagedWebLogic.sh ApplicationServer-1 t3://localhost:7001
```

7 **Stop the administration server.**

```
#cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
./stopWebLogic.sh
```

8 **Start the administration server.**

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

Watch for startup errors.

9 **Start Application Server 1.**

```
# nohup ./startManageWebLogic sh ApplicatoinServer-1
http://ProtectedResource-1.example.com:7001 &
tail -f nohup.out
```

10 **Run the `netstat` command to verify that Application Server 1 is up and listening.**

```
# netstat -an | grep 1081
xxx.xx.72.151.1081        *.*        0        0    49152        0    LISTEN
127.0.0.01.1081            *.*        0        0    49152        0    LISTEN
```

▼ To Deploy the J2EE Policy Agent Application

1 **Go to the following Application Server URL:**

`http://ProtectedResource-1.example.com:7001/console`

2 **Log in to the Application Server console using the following information:**

Username **`weblogic`**

Password **`w3bl0g1c`**

3 **In the Application Server console, under Domain Structure, click Deployments.**

4 **On the Summary of Deployments page, in the Change Center, click "Lock & Edit."**

5. **Under Deployments, click Install.**
6. **On the Install Application Assistant page, click the `protectedresource-1.example.com` link.**
7. **In the field named Location: `protectedresource-1.example.com`, click the root directory.**
   Navigate to the application directory: `/opt/j2ee_agents/am_wl9_agent/etc/`
8. **Select `agentapp.war`, and then click Next.**
9. **In the Install Application Assistant page, choose "Install this deployment as an application," and then click Next.**
10. **In the list of Servers, mark the checkbox for ApplicationServer-1, and then click Next.**
11. **In the Optional Settings page, click Next.**
12. **Click Finish.**
13. **On the "Settings for agentapp" page, click Save.**
14. **In the Change Center, click Activate Changes.**

▼ To Start the Agent Application

1. **On the "Settings for agentapp" page, click Deployments.**
2. **On the Summary of Deployments page, mark the `agentapp` checkbox, and then click Start > "Servicing all requests."**
3. **On the Start Deployments page, click Start.**
   You may encounter a Javascript error. The agent application will not start until you start the Application Server.

▼ To Set Up the Agent Authentication Provider

1. **In the console, on the Summary of Deployments page, under Domain Structure, click Security Realms.**
2. **On the Summary of Security Realms page, click "Lock & Edit."**

3. **Click the Realm name `myrealm` link.**
4. **On the "Settings for myrealm" page, click the Providers tab.**
5. **On the Providers tab, under Authentication Providers, click New.**
6. **On the Create a New Authentication Provider page, provide the following information:**

   Name: **`Agent-1`**

   Type: **`AgentAuthenticator`**
7. **Click OK.**

   `Agent-1` is now included in the list of Authentication Providers.
8. **In the list of Authentication Providers, click `Agent-1`.**
9. **In the Settings for Authentication Providers page, verify that the Control Flag is set for OPTIONAL.**
10. **On the Settings for Agent-1 page, in the list of Authentication Providers, click DefaultAuthenticator.**
11. **On the Settings for DefaultAuthenticator page, set the Control Flag to OPTIONAL, and then click Save.**
12. **Return to the Providers page.**

    In the navigation tree near the top of the page, click Providers.
13. **In the Change Center, click Activate Changes.**

▼ To Edit the AMAgent.properties File

1. **Make a backup of the following file:**

   `/opt/j2ee_agents/am_wl9_agent/agent_001/config/AMAgent.properties`
2. **In the `AMAgent.properties` file, set the following property:**

   `com.sun.identity.agents.config.bypass.principal[0] = weblogic`
3. **At end of the file, insert a new property.**

   `com.sun.identity.session.resetLBCookie='true'`

The default value for this property is `false`. You must add this property only if session failover has been configured for Access Manager. If session failover is not configured for Access Manager, and this property is added, it could impact performance negatively. If session failover is enabled for Access Manager, and this property is not added, then Access Manager sessions will still fail over, and the session failover functionality will work properly. However, the stickiness to the Access Manager server will not be maintained after failover occurs. Session stickiness to the Access Manager server helps performance. This property must be added to the `AMConfig.properties` file on the Access Manager servers, as well as to the `AMAgent.properties` for the J2EE Policy Agent servers. This property is not required for the Web Policy Agent servers. The "Access Manager 7 2005Q4 Patch 3" in *Sun Java System Access Manager 7 2005Q4 Release Notes* Release Notes also references this property. See the section"CR# 6440651: Cookie replay requires com.sun.identity.session.resetLBCookie property" in *Sun Java System Access Manager 7 2005Q4 Release Notes*.

4 **Save the file.**

8.4 Setting Up a Test for the J2EE Policy Agent 1

Use the following as your checklist for setting up a test for the J2EE Policy Agent 1:

1. Deploy the sample application.
2. Create roles in the external data store.
3. Create a test referral policy in the base suffix.
4. Create a test policy in the user realm.
5. Configure J2EE properties for the sample application.
6. Verify that J2EE Policy Agent 1 is configured properly.

▼ To Deploy the Sample Application

The BEA Policy Agent comes with a sample application specifically created to help you test your access policies. Locate the sample application file here: `opt/j2ee_agents/am_wl9_agent/sampleapp`. For more information, see the file `/opt/j2ee_agents/am_wl9_agent/sampleapp/readme.txt`.

1 **Go to the Application Server 1 URL:**

`http://ProtectedResource-1.example.com:7001/console`

2 **Log in to the Application Server using the following information:**

Username **`weblogic`**

Password **`w3bl0g1c`**

3. **In the Application Server console, on the Summary of Deployments page, click "Lock & Edit."**
4. **Under Domain Structure, click Deployments.**
5. **Under Deployments, click Install.**
6. **On the Install Application Assistant page, click the** `protectedresource-1.example.com` **link.**
7. **In the list for Location:** `protectedresource-1.example.com`**, click the root directory.**
   Navigate to the application directory: `/opt/j2ee_agents/am_wl9_agent/sampleapp/dist`
8. **Select** `agentsample`**, and then click Next.**
9. **In the Install Application Assistant page, choose "Install this deployment as an application," and then click Next.**
10. **In the list of Servers, mark the checkbox for** `ApplicationServer-1`**, and then click Next.**
11. **On the "Optional Settings" page, click Next to accept the default settings.**
12. **On the Review Your Choices" page, click Finish.**
    The Target Summary section indicates that the module `agentsample` will be installed on the target `ApplicationServer-1`.
13. **In the "Settings for agentsample" page, click Activate Changes.**
14. **Under Domain Structure, click Deployments.**
15. **In the Deployments list, mark the checkbox for** `agentsample`**, and then click Start > Servicing All Requests.**
16. **On the Start Deployments page, click Yes.**
    The state of the deployment changes from Prepared to Active.
17. **Log out of the Application Server 1 console.**

▼ To Create Roles in the External Data Store

You will use these roles to verify that the sample application has been successfully installed and configured.

1. **Start the Directory Server 1 console, and log in:**

Username	**cn=Directory Manager**
Password	**d1rm4n4ger**
Administration URL	**http://DirectoryServer-1.example.com:1391**

2. **In the Directory Server console, expand the** `example.com` **suffix.**
3. **Click Server Group >** `am-users`**, and then click Open.**
4. **Click the Directory tab.**
5. **Right-click** `dc=company, dc=com`**, and then click New > Role.**
6. **In the Create New Role page, in the Role Name field, enter** `manager`**, and then click OK.**
7. **Right-click** `dc=company, dc=com`**, and then click New > Role.**
8. **In the Create New Role page, in the Role Name field, enter** `employee`**, and then click OK.**
   On the Directory Tab, for the suffix `dc=company, dc=com`, you should see the two users you just added: `manager` and `employee`.
9. **Double-click the** `manager` **role.**
10. **In the Edit Role page, click Members and then click Add.**
11. **In the Search Users and Groups dialog, click Search.**
    In the list of results, select Test User 1 and then click OK.
12. **In the Edit Role page, click OK.**
13. **Double-click the** `employee` **role.**
14. **In the Edit Role page, click Members and then click Add.**
15. **In the Search Users and Groups dialog, click Search.**
    In the list of results, select Test User 2 and then click OK.
16. **In the Edit Role page, click OK.**
17. **Log out of the Directory Server console.**

▼ To Create a Test Referral Policy in the Base Suffix

1. **In the Access Manager 1 console, on the Access Control tab, click the `example.com` link.**
2. **Click the Policies tab.**
3. **Under Policies, click the "Referral URL Policy for users realm" link.**
   This is the policy that was created when setting up the Web Policy Agent.
4. **On the Edit Policy page, under Rules, click New.**
5. **On the page "Step 1 of 2: Select Service Type for the Rule," select "URL Policy Agent (with resource name)," and then click Next.**
6. **On the page "Step 2 of 2: New Rule," provide the following information, and then click Next:**
   Name: **`URL Policy for ApplicationServer-1`**
   Resource Name: **`http://ProtectedResource-1.example.com:1081/agentsample/*`**
7. **Click Finish.**

▼ To Create a Test Policy in the User Realm

1. **In the Access Manager 1 console, on the Access Control tab, click the `users` link.**
2. **Click the Policies tab.**
3. **Under Policies, click New Policy.**
4. **In the Name field, enter `URL Policy for ApplicationServer-1`.**
5. **Under Rules, click New.**
6. **On the page "Step 1 of 2: Select Service Type for the Rule," click Next.**
   The default "URL Policy Agent (with resource name)" should be selected.
7. **On the page "Step 2 of 2: New Rule," provide the following information:**
   Name: **`agentsample`**
   Parent Resource Name: In the list, select **`http://ProtectedResource-1.example.com:1081/agentsample/*`**

Resource Name:	The following is automatically entered when you select the Parent Resource Name above:
	`http://ProtectedResource-1.example.com:1081/agentsample/*`
GET	Mark this check box, and verify that the Allow value is selected.
POST	Mark this check box, and verify that the Allow value is selected.

8 **Click Finish.**

The rule `agentsample` is now added to the list of Rules.

9 **Under Subjects, click New.**

10 **On the page "Step 1 of 2: Select Subject Type," select Access Manager Identity Subject, then click Next.**

11 **On the page " Step 2 of 2: New Subject — Access Manager Identity Subject," provide the following information:**

Name: **`agentsampleRoles`**

Filter: Select `role`.

12 **Click Search.**

13 **In the Available list, the select `manager` and `employee` roles, and then click Add.**

The roles are now displayed in the Selected list.

14 **Click Finish.**

15 **Click Create.**

The new policy is included in the list of Policies.

▼ To Configure J2EE Properties for the Sample Application

1 **Log in as a root user to Protected Resource 2.**

```
# cd /opt/j2ee_agents/am_wl9_agent/agent_001/config
```

2 **Make a back up the `AMAgent.properties` file.**

3 In the `AMAgent.properties` file, set the following properties:

```
com.sun.identity.agents.config.notenforced.uri[0] =
   /agentsample/public/*
   com.sun.identity.agents.config.notenforced.uri[1] =
   /agentsample/images/*
   com.sun.identity.agents.config.notenforced.uri[2] =
   /agentsample/styles/*
   com.sun.identity.agents.config.notenforced.uri[3] =
   /agentsample/index.html
   com.sun.identity.agents.config.notenforced.uri[4] =
   /agentsample
   com.sun.identity.agents.config.access.denied.uri =
   /agentsample/authentication/accessdenied.html
   com.sun.identity.agents.config.login.form[0] =
   /agentsample/authentication/login.html
   com.sun.identity.agents.config.login.url[0] =
   http://LoadBalancer-3.example.com:7070/amserver/UI/Login?realm=users
```

4 Save the file.

5 Restart the Application Server 2.

a. Stop Application Server 2 .

```
# cd /usr/local/bea/user_projects/domains/
ProtectedResource-2/bin
# ./stopManagedWebLogic.sh ApplicationsServer-2
t3://localhost:7001
```

b. Stop the administration server.

```
# ./stopWebLogic.sh
```

c. Start the administration server.

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

d. Start Application Server 2.

```
# nohup ./startManagedWebLogic.sh
ApplicationServer-1 http://ProtectedResource-1.example.com:7001 &
```

▼ To Verify that J2EE Policy Agent 1 is Configured Properly

Use these steps to access the agent sample application, and then test policies against that sample application.

1 **Go to the Sample Application URL:**

`http://protectedresource-1.example.com:1081/agentsample/index.html`

The Sample Application welcome page is displayed.

2 **Click J2EE Declarative Security > "Invoke the Protected Servlet"**

The Policy Agent redirects to the Access Manager login page.

3 **Log in to the Access Manager console using the following information:**

Username **`testuser1`**

Password **`password`**

If you can successfully log in as `testuser1`, and the J2EE Policy Agent Sample Application page is displayed, then this part of the test succeeded and authentication is working as expected.

4 **Click the "J2EE Declarative Security" link.**

5 **On the J2EE Declarative Security page, click the "Invoke the Protected Servlet link".**

If the Success Invocation message is displayed, then this part of the test succeeded , and the sample policy for the `manager` role has been enforced as expected.

6 **Click the "J2EE Declarative Security" link to go back.**

7 **Click the "Invoke the Protected EJB via an Unprotected Servlet" link.**

If the Failed Invocation message is displayed, then this part of the test succeeded, and the sample policy for the `employee` role has been enforced as expected.

8 **Close the browser.**

9 **In a new browser session, go to the Sample Application URL:**

`http://protectedresource-1.example.com:1081/agentsample/index.html`

The Sample Application welcome page is displayed.

10 **Click the "J2EE Declarative Security" link.**

11 On the J2EE Declarative Security page, click the "Invoke the Protected EJB via an Unprotected Servlet" link.

The Policy Agent redirects to the Access Manager login page.

12 Log in to the Access Manager console using the following information:

Username `testuser1`

Password `password`

If you can successfully log in as `testuser1`, and the J2EE Policy Agent Sample Application page is displayed, then this part of the test succeeded and authentication is working as expected.

13 Click the "J2EE Declarative Security" link to go back.

14 On the J2EE Declarative Security page, click the "Invoke the Protected EJB via an Uprotected Servlet" link.

The Successful Invocation message is displayed. The sample policy for the employee role has been enforced as expected.

8.5 Configuring Access Manager to Communicate Over SSL

In this section, you configure the policy agent to point to the SSL port for the Access Manager load balancer.

Use the following as your checklist for configuring Access Manager to communicate over SSL:

1. Import the root CA certificate into the Application Server keystore.
2. Configure the J2EE Policy Agent for SSL.
3. Verify that J2EE Policy Agent 1 is configured properly.
4. Configure the Policy Agents to access the Distributed Authentication UI server.

▼ To Import the Root CA Certificate into the Application Server Keystore

In this procedure, you import a Certificate Authority (CA) certificate. The certificate enables the Authentication UI server to trust the certificate from the Access Manager load balancer (Load Balancer 3), and to establish trust with the certificate chain that is formed from the CA to the certificate.

1 Go to the directory where the keystore (the `cacerts` file) is located:

```
#cd /usr/local/bea/jdk150_04/jre/lib/security/
```

2 **Make a backup of the** `cacerts` **file.**

3 **Copy the CA certificate that you obtained from your Certificate Authority into a temporary directory. Example:**

```
/export/software/ca.cer
```

4 **Import the certificate:**

```
# /usr/local/bea/jdk150_04/bin/keytool -import
-trustcacerts -alias OpenSSLTestCA -file /export/software/ca.cer
-keystore /usr/local/bea/jdk150_04/jre/lib/security/cacerts
-storepass changeit

Owner: EMAILADDRESS=nobody@nowhere.com, CN=OpenSSLTestCA, OU=Sun,
O=Sun, L=Santa Clara, ST=California, C=US
Issuer: EMAILADDRESS=nobody@nowhere.com, CN=OpenSSLTestCA, OU=Sun,
O=Sun, L=Santa Clara, ST=California, C=US
Serial number: 97dba0aa26db6386
Valid from: Tue Apr 18 07:55:19 PDT 2006
until: Tue Jan 13 06:55:19 PST 2009
Certificate fingerprints:
                        MD5: 9F:57:ED:B2:F2:88:B6:E8:0F:1E:08:72:CF:70:32:06
                        SHA1: 31:26:46:15:C5:12:5D:29:46:2A:60:A1:E5:9E:28:64:36:
                        80:E4:70
Trust this certificate? [no]: yes Certificate was added to keystore
```

5 **Verify that the certificate was imported successfully:**

```
# /usr/local/bea/jdk150_04/bin/keytool -list
-keystore /usr/local/bea/jdk150_04/jre/lib/security/cacerts
-storepass changeit | grep openssl

openssltestca, Oct 2, 2006, trustedCertEntry,
```

▼ To Configure the J2EE Policy Agent for SSL

1 **As a root user, log into host ProtectedResource–1.**

```
# cd /opt/j2ee_agents/am_wl9_agent/agent_001/config
```

2 **Make a backup of the** `AMAgent.properties` **file.**

3 **In the** `AMAgent.properties`**, set the following properties:**

```
com.sun.identity.agents.config.login.url[0] =
https://LoadBalancer-3.example.com:9443/amserver/UI/Login?realm=users
com.sun.identity.agents.config.cdsso.cdcservlet.url[0] =
```

```
https://LoadBalancer-3.example.com:9443/amserver/cdcservlet
com.sun.identity.agents.config.cdsso.trusted.id.provider[0] =
https://LoadBalancer-3.example.com:9443/amserver/cdcservlet
com.iplanet.am.naming.url=
https://LoadBalancer-3.example.com:9443/amserver/namingservice
com.iplanet.am.server.protocol=https
com.iplanet.am.server.port=9443
```

4 **Save the file.**

5 **Stop Application Server 1 .**

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
# ./stopManagedWebLogic.sh ApplicationsServer-1 t3://localhost:7001
```

6 **Stop the administration server.**

```
# ./stopWebLogic.sh
```

7 **Start the administration server.**

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

8 **Start Application Server 1.**

```
# nohup ./startManagedWebLogic.sh
ApplicationServer-1 http://ProtectedResource-1.example.com:7001 &
```

▼ To Verify that J2EE Policy Agent 1 is Configured Properly

Use these steps to access the agent sample application, and then test policies against that sample application.

1 **Go to the Sample Application URL:**

`http://protectedresource-1.example.com:1081/agentsample/index.html`

The Sample Application welcome page is displayed.

2 **Click J2EE Declarative Security > "Invoke the Protected Servlet"**

The Policy Agent redirects to the Access Manager login page.

3 **Log in to the Access Manager console using the following information:**

Username **`testuser1`**

Password **password**

If you can successfully log in as `testuser1`, and the J2EE Policy Agent Sample Application page is displayed, then this part of the test succeeded and authentication is working as expected.

4 **Click the "J2EE Declarative Security" link.**

5 **On the J2EE Declarative Security page, click the "Invoke the Protected Servlet link".**

If the Success Invocation message is displayed, then this part of the test succeeded , and the sample policy for the `manager` role has been enforced as expected.

6 **Click the "J2EE Declarative Security" link to go back.**

7 **Click the "Invoke the Protected EJB via an Unprotected Servlet" link.**

If the Failed Invocation message is displayed, then this part of the test succeeded, and the sample policy for the `employee` role has been enforced as expected.

8 **Close the browser.**

9 **In a new browser session, go to the Sample Application URL:**

`http://protectedresource-1.example.com:1081/agentsample/index.html`

The Policy Agent redirects to the Access Manager login page.

10 **Log in to the Access Manager console using the following information:**

Username **testuser2**

Password **password**

The Failed Invocation message is displayed.

11 **Click the "J2EE Declarative Security" link.**

12 **On the J2EE Declarative Security page, click the "Invoke the Protected EJB via an Unprotected Servlet" link.**

The Successful Invocation message is displayed. The sample policy for the `employee` role has been enforced as expected.

13 **Click the "J2EE Declarative Security" link to go back.**

14 **Click the "Invoke the Protected Servlet" link.**

If the Access to Requested Resource Denied message is displayed, then this part of the test is successful. The sample policy for the `manager` role has been enforced as expected.

▼ To Configure the Policy Agents to Access the Distributed Authentication UI Server

1 **Log in as a root user to Protected Resource 1.**

```
# cd /opt/j2ee_agents/am_wl9_agent/agent_001/config
```

2 **Make a backup of the file** `AMAgent.properties`**.**

3 **In the** `AMAgent.properties` **file, set the following properties:**

```
com.sun.identity.agents.config.login.url[0] =
https://LoadBalancer-4.example.com:9443/distAuth/UI/Login?realm=users
```

4 **Save the file.**

5 **Restart the Application Server.**

a. **Stop Application Server 1.**

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
# ./stopManagedWebLogic.sh ApplicationServer-1 t3://localhost:7001
```

b. **Stop the administration server.**

```
#cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
./stopWebLogic.sh
```

c. **Start the administration server.**

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

Watch for startup errors.

d. **Start Application Server 1.**

```
# nohup ./startManageWebLogic.sh
ApplicatoinServer-1 http://ProtectedResource-1.example.com:7001 &
tail -f nohup.out
```

6 **Verify that the agents are configured properly.**

a. **Go to the sample application URL:**

```
http://ProtectedResource-1.example.com:1081/agentsample/index.html
```

b. In the left navigation bar, click "Invoke the Protected Servlet."

You are redirected to the Distributed Authentication UI server URL `https://loadbalancer-4.example.com:9443/distAuth/UI/login`. The Access Manager login page is displayed.

c. Double-click the gold lock in the lower left corner of the browser.

In the Properties page, you see certificate for `LoadBalancer–4.example.com`.

d. Log in to the Access Manager console using the following information:

Username **`testuser1`**

Password **`password`**

You are redirected to the protected servlet of the Sample Application, and a success message is displayed. This indicates that authentication through the Distributed Authentication UI server was successful.

8.6 Installing Web Server 2 and Web Policy Agent 2

Use the following as your checklist for installing Web Server 2 and Web Policy Agent 2:

1. Install Web Server 2 on Protected Resource 2.
2. Install Web Policy Agent 2.
3. Verify that Web Policy Agent 2 works properly.
4. Import the root CA certificate into the Web Server 2 key store.
5. Create an agent profile on Access Manager.
6. Configure the Web Policy Agent to use the new agent profile.

▼ To Install Web Server 2 on Protected Resource 2

1 As root, log in to host ProtectedResource-2.

2 Start the Java Enterprise System installer with the `-nodisplay` option.

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

3 When prompted, provide the following information:

`Welcome to the Sun Java(TM) Enterprise System;`
`serious software made  simple...`
`<Press ENTER to Continue>`
	Press Enter.

`<Press ENTER to display the Software` `License Agreement>`	Press Enter.

`Have you read, and do you accept, all of`
`the termsof the preceding Software`
`License Agreement [No]`
	Enter **`y`**.

`Please enter a comma separated list of`
`languages you would like supported with`
`this installation [8]`
	Enter 8 for “English only.”

`Enter a comma separated list of products to` `install,or press R to refresh the list  []`	Enter **`3`** to select Web Server.
`Press "Enter" to Continue or Enter a` `comma separated list of products to deselect... [1]`	Press Enter.
`Enter 1 to upgrade these shared components` `and 2 to cancel  [1]`	You are prompted to upgrade shared components only if the installer detects that an upgrade is required. Enter **`1`** to upgrade shared components.

`Enter the name of the target`
`installation directory for each product:`
`Web Server [/opt/SUNWwbsvr] :`
	Accept the default value.

`System ready for installation` `Enter 1 to continue [1]`	Enter **`1`**.

`1. Configure Now - Selectively override defaults or`
`express through`
`2. Configure Later - Manually configure following`
`installation`
` Select Type of Configuration [1]`
	Enter **`1`**.

`Common Server Settings` `Enter Host Name [ProtectedResource-2]`	Accept the default value.
`Enter DNS Domain Name [example.com]`	Accept the default value.
`Enter IP Address [xxx.xx.87.180]`	Accept the default value.
`Enter Server admin User ID [admin]`	Enter **`admin`**.

`Enter Admin User’s Password`
`(Password cannot be less than 8 characters)`
`[]`
	For this example, enter **`web4dmin`**.

`Confirm Admin User’s Password []`	Enter the same password to confirm it.

`Enter System User [root]`	Accept the default value.
`Enter System Group [root]`	Accept the default value.
`Enter  Server Admin User ID [admin]`	Accept the default value.
`Enter Admin User's Password []`	For this example, enter **`web4dmin`**.
`Enter Host Name [ProtectedResource-2.example.com]`	Accept the default value.
`Enter Administration Port [8888]`	Accept the default value.
`Enter Administration Server User ID [root]`	Accept the default value.
`Enter System User ID [webservd]`	Enter **`root`**.
`Enter System Group [webservd]`	Enter **`root`**.
`Enter HTTP Port [80]`	Enter **`1080`**.
`Enter content Root [/opt/SUNWwbsvr/docs]`	Accept the default value.
`Do you want to automatically start Web Serverwhen system re-starts.(Y/N)  [N]`	Accept the default value.

`Ready to Install`
`1. Install 2. Start Over 3. Exit Installation`
`What would you like to do [1]`
	First, see the next numbered (Optional) step. When ready to install, enter **`1`**.

4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:

```
# cd /var/sadm/install/logs
# tail –f Java_Enterprise_System_install.B xxxxxx
```

5 Upon successful installation, enter `!` to exit.

6 Verify that the Web Server is installed properly.

a. Start the Web Server administration server to verify it starts with no errors.

```
# cd /opt/SUNWwbsvr/https-admserv

# ./stop; ./start
```

b. Run the `netstat` command to verify that the Web Server ports are open and listening.

```
# netstat -an | grep 8888
  *.8888           *.*           0        0    49152        0    LISTEN
```

c. Go to the Web Server URL.

```
http://ProtectedResource-2.example.com:8888
```

d. Log in to the Web Server using the following information:

User Name: **admin**

Password: **web4dmin**

You should be able to see the Web Server console. You can log out of the console now.

e. Start the Protected Resource 2 instance.

```
#cd /opt/SUNWwbsvr/https-ProtectedResource-2.example.com
# ./stop; ./start
```

f. Run the `netstat` command to verify that the Web Server ports are open and listening.

```
# netstat -an | grep 1080
  *.1080           *.*           0        0    49152        0    LISTEN
```

g. Go to the instance URL.

```
http://ProtectedResource-2.example.com:1080
```

You should see the default Web Server index page.

▼ To Install Web Policy Agent 2

Before You Begin The Java System Web Policy Agents 2.2 package must be downloaded to each Protected Resource that will host a Web Policy Agent. You can download the package from the following website: `http://www.sun.com/download`

Caution – Due to a known problem with this version of the Web Policy Agent, you must start an X-display session on the server host using a program such as Reflections X or VNC, even though you use the command-line installer. For more information about this known problem, see `http://docs.sun.com/app/docs/doc/819-2796/6n52flfoq?a=view#adtcd`.

1 Log in as a root user to host ProtectedResource-2.

2 Download the Java System Web Policy Agents 2.2 package from the following website:

`http://www.sun.com/download`

3 Unpack the downloaded package.

In this example, the package was downloaded into the directory `/temp`.

```
# cd /temp
# gunzip sun-one-policy-agent-2.2-es6-solaris_sparc.tar.gz
# tar –xvof sun-one-policy-agent-2.2-es6-solaris_sparc.tar
```

4 Start the Web Policy Agents installer.

```
# ./setup -nodisplay
```

5 When prompted, provide the following information:

`When you are ready, press Enter to continue.` `<Press ENTER to Continue>`	Press Enter.
`Press ENTER to display the Sun Software` `License Agreement`	Press Enter.

`Have you read, and do you accept, all of`
`the terms of the preceding Software License`
`Agreement [no] y`
	Enter **`y`**.

`Install the Sun Java(tm) System Access Manager` `Policy Agent in this directory [/opt] :`	Accept the default value.

`Enter information about the server instance this`
`agent will protect.`
`Host Name [ProtectedResource-2.example.com]:`
	Accept the default value.

`Web Server Instance Directory [] {`	Enter . **`/opt/SUNWwbsvr/`** **`https-ProtectedResource-2.example.com`**
`Web Server Port [80]:    :`	Enter **`1080`**.
`Web Server Protocol [http]`	Accept the default value.
`Agent Deployment URI [/amagent]:`	Accept the default value.

`Enter the Sun Java(tm) System Access Manager`
`Information for this Agent.`
`Primary Server Host [ProtectedResource-1.example.com] :`
	For this example, enter the external-facing load balancer host name. Example:
	`LoadBalancer-3.example.com`

`Primary Server Port [1080]`	Enter the load balancer HTTP port number. For this example, enter **`90`**.
`Primary Server Protocol [http]:`	Accept the default value.
`Primary Server Deployment URI [/amserver]:`	Accept the default value.
`Primary Console Deployment URI [/amconsole] :`	Accept the default value.

`Failover Server Host :`	Accept the default value.
`Agent-Access Manager Shared Secret:`	Enter the `amldapuser` password that was entered when Access Manager was installed. For this example, enter **`4mld4puser`**.
`Re-enter Shared Secret:`	Enter the **`4mld4puser`** password again to confirm it.
`CDSSO Enabled [false]:`	Accept the default value.
`Press "Enter" when you are ready to continue.`	First, see the next (Optional) numbered step. When you are ready to start installation, press Enter.

6 (Optional) During installation, you can monitor the log to watch for installation errors. Example:

```
# cd /var/sadm/install/logs
# tail –f /var/sadm/install/logs/
Sun_Java_tm__System_Access_Manager_Policy_Agent_install.B<xxxxxx>
```

7 Modify the `AMAgent.properties` file.

```
# cd /etc/opt/SUNWam/agents/es6/
config/_opt_SUNWwbsvr_https-ProtectedResource-2.example.com
```

Make a backup of `AMAgent.properties` before setting the following property:

```
com.sun.am.policy.am.login.url =
https://LoadBalancer-4.example.com:9443/distAuth/UI/Login?realm=users
```

8 Restart the Web Server.

Watch for errors as the server starts up.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-2.example.com
```

```
# ./stop; ./start
```

a. Examine the Web Server log for startup errors.

```
# /opt/SUNWwbsvr/https-ProtectedResource-2.example.com/logs
```

```
# vi errors
```

▼ To Verify that Web Policy Agent 2 Works Properly

1 Start a new browser and go to the Access Manager URL.

Example: `https://loadbalancer-3.example.com:9443/amserver/console`

2 Log in to Access Manager using the following information:

Username **amadmin**

Password **4m4dmin1**

3 Create a referral policy in the top-level realm.

a. On the Access Control tab, under Realms, click `example.com`**.**

b. Click the Policies tab.

c. On the Policies tab for example.com-Policies, click the "Referral URL Policy for users realm" link.

d. In the Edit Policy page, under Rules, click New.

e. In the Edit Rule page, provide the following information.

f. On the same page, in the Rules section, click New.

g. Select a Service Type.

On the page "Step 1 of 2: Select Service Type for the Rule," select URL Policy Agent (with resource name)

h. Click Next.

i. On the page "Step 2 of 2: New Rule," provide the following information:

Name: **URL Rule for ProtectedResource-2**

Resource Name: **http://ProtectedResource-2.example.com:1080/***

j. Click Finish.

k. On the Edit Policy page, click Save.

In the Policies tab for example.com — Policies, you should see the policy named Referral URL Policy for users realm.

4 Create a policy in the `users` **realm.**

a. Click Realms.

b. On the Access Control tab, under Realms, click the Realm Name `users`**.**

c. Click the Policies tab.

d. On the Policies tab for users-Policies, click New Policy.

e. In the New Policy page, provide the following information:

Name: **`URL Policy for ProtectedResource-2`**

Active: Verify that the checkbox is marked.

f. On the same page, in the Rules section, click New.

g. On the page "Step 1 of 2: Select Service Type for the Rule," click Next.

The Service Type "URL Policy Agent (with resource name) is the only choice.

h. On the page "Step 2 of 2: New Rule," provide the following information:

Name:	**`URL Rule for ProtectedResource-2`**
Resource Name:	Click the URL listed in the Parent Resource Name list: `http://ProtectedResource-2.example.com:1080/*` The URL is automatically added to the Resource Name field.
GET:	Mark this checkbox, and select the Allow value.
POST:	Mark this checkbox, and select the Allow value.

i. Click Finish.

j. On the Policy page, in the Subjects section, click New.

i. Select the subject type.

On the page "Step 1 of 2: Select Subject Type," select the Access Manager Identity Subject type.

ii. On the page "Step 2 of 2: New Subject — Access Manager Identity Subject," provide the following information:

Name:	**`Test Subject`**
Filter:	Choose `User`, and then click Search. Four users are added to the Available list.
Available:	In the list, select `testuser1`, and then click Add. The user `testuser1` is added to the Selected list.

iii. Click Finish.

k. In the New Policy page, click Create.

On the Policies tab for users-Policies, the new policy "URL Policy for ProtectedResource-2" is now in the Policies list.

5 Verify that the new policy works with Web Policy Agent 2.

a. Verify that an authorized user can access the Web Server 2.

i. Go to the following URL:

`http://ProtectedResource-2.example.com:1080`

ii. Log in to Access Manager using the following information:

Username **`testuser1`**

Password **`password`**

You should see the default `index.html` page for Web Server 2.

b. Verify that an unauthorized user cannot access the Web Server 2.

i. Go to the following URL:

`http://ProtectedResource-2.example.com:1080`

ii. Log in to Access Manager using the following information:

Username **`testuser2`**

Password **`password`**

You should see the message, "You're not authorized to view this page."

▼ To Import the Root CA Certificate into the Web Server 2 Key Store

The Web Policy Agent on Protected Resource 1 connects to Access Manager servers through Load Balancer 3. The load balancer is SSL-enabled, so the agent must be able to trust the load balancer SSL certificate in order to establish the SSL connection. To do this, import the root CA certificate that issued the Load Balancer 3 SSL server certificate into the Web Policy Agent certificate store.

Before You Begin Obtain the root CA certificate, and copy it to ProtectedResource-2.

1 Copy the root CA certificate to Protected Resource 2.

2 **Open a browser, and go to the Web Server 2 administration console.**

`http://ProtectedResource-2.example.com:8888`

3 **Log in to the Web Server 2 console using the following information:**

User Name: **`admin`**

Password: **`web4dmin`**

4 **In the Select a Server field, select `ProtectedResource-2.example.com`, and then click Manage.**

Tip – If a "Configuration files have not been loaded" message is displayed, it may be that the administration server has never been accessed, and so the configuration files have never been loaded. First click Apply, and then click Apply Changes. The configuration files are read, and the server is stopped and restarted.

---

5 **Click the Security tab.**

6 **On the Initialize Trust Database page, enter a Database Password.**

Enter the password again to confirm it, and then click OK.

7 **In the left frame, click Install Certificate and provide the following information, and then click OK:**

Certificate For: Choose **`Trusted Certificate Authority (CA)`**

Key Pair File Password: **`password`**

Certificate Name: **`OpenSSL_CA_Cert`**

Message in this File: **`/export/software/ca.cert`**

8 **Click Add Server Certificate.**

9 **Click Manage Certificates.**

The root CA Certificate name `OpenSSL_CA_Cert` is included in the list of certificates.

10 **Click the Preferences tab.**

11 **Restart Web Server 2.**

On the Server On/Off page, click Server Off. When the server indicates that the administration server is off, click Server On.

12 Configure the Web Policy Agent 2 to point to the Access Manager SSL port.

a. Edit the `AMAgent.properties` file.

```
# cd /opt/SUNWam/agents/es5/config/
_optSUNWwbsvr_https=ProtectedResource-2.example.com
```

Make a backup of the `AMAgent.properties` file before setting the following property:

```
# com.sun.am.naming.url =
https://LoadBalancer-3.example.com:9443/amserver/namingservice
```

b. Save the file.

13 Restart Web Server 2.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-2.example.com
# ./stop; ./start
```

▼ To Create an Agent Profile on Access Manager

This new account will be used by J2EE Policy Agent 2 to access the Access Manager server.

● **Create an agent profile on Access Manager.**

a. Go to Access Manage load balancer URL:

`https://LoadBalancer-3.example.com:9443/amserver/UI/Login`

b. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

c. On the Access Control tab, under Realms, click the realm name `example.com`.

d. Click the Subjects tab.

e. Click the Agents tab.

f. On the Agent page, click New.

g. On the New Agent page, provide the following information:

ID: **`webagent-2`**

Password: **`web4gent2`**

Password Confirm: **web4gent2**

Device State: Choose **Active**.

h. Click Create.

The new agent webagent–2 is now display in the list of Agent Users.

▼ To Configure the Web Policy Agent to Use the New Agent Profile

1 Log in to as a root user to Protected Resource 2.

2 Run the `cypt_util` utility.

The utility encrypts the password.

```
# cd /opt/SUNWam/agents/bin
# ./crypt_util web4gent2
BXxzBswD+PZdMRDRMXQQA==
```

Copy the encrypted password, and save it in a text file.

3 Edit the `AMAgent.properties` file.

```
# cd /etc/opt/SUNWam/agents/es6/
config/_opt_SUNWwbsvr_https-ProtectedResource-2.example.com
```

Make a backup of `AMAgent.properties` you make the following change in the file:

```
com.sun.am.policy.am.password = webagent-2
com.sun.am.policy.am.password = BXxzBswD+PZdMRDRMXQQA==
```

Use the encrypted password obtained in the previous step.

Save the file.

4 Restart Web Server 2.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-2.example.com
 # ./stop; ./start
```

8.7 Installing Application Server 2 and J2EE Policy Agent 2

Use the following as your checklist for installing Application Server 2 and the J2EE Policy Agent 2:

1. Install Application Server 2 on Protected Resource 2.
2. Create an agent profile on Access Manager.
3. Run the J2EE Policy Agent installer on Application Server 2.

▼ To Install Application Server 2 on Protected Resource 2

1 Download the BEA WebLogic Server installer onto Protected Resource 2.

Follow the instructions provided by BEA for obtaining and using the software.

2 Extract the installer files:

```
# /download_directory/export/weblogic/server910_solaris32.bin
```

`Welcome...`
`You may quit the installer at any time by typing "Exit."`
 	
`Enter [Exit][Next]`
	Enter **`Next`**.

`Select Option:`
`1. Yes, I agree with the terms of`
`the license.`
`2. No, I do not agree with the terms`
`of the license.`
	Enter **`1`**.

`Choose BEA Home Directory [/usr/local/bea]:`	Press Enter to accept the default value and continue.
`Choose Install Type [Complete]:`	Enter **`2`** to choose custom install.

`Release 9.1.0.0`
`WebLogic Server [1]`
`Server [1.1]`
`Server Examples [1.2]`
`Web Server Plug-ins [1.3]`
 	
`Choose Componenets to install:`
	Enter **`Next`**.

`Choose Product Directory` `[/usr/local/bea/weblogic91]:`	Press Enter to accept the default value and continue.
`Choose Product Directory [Yes, use this product` `directory]:`	Press Enter to confirm the default value and continue.

`Installation Complete` `Press [Enter} to continue...`	Press Enter.

3 Create a new domain.

a. Start the BEA WebLogic Configuration Wizard.

```
# cd /usr/local/bea/weblogic91/common/bin
# ./config.sh
```

b. Provide the following information:

`Welcome...`
 	
`->1| Create a new WebLogic domain.`
`2| Extend an existing WebLogic domain.`
	Press Enter to accept the default value 1.

`Select Domain Source:`
`->1| Choose WebLogic Platform components`
`2| Choose custom template`
	Press Enter to accept the default value 1.

`Application Template Selection:`
`Avaliable Templates`
`WebLogic Server (Required)x`
`Appache Behive [2]`
	Press Enter to accept the default value and continue.

`Configure Administrator Username and Password:`
`Select Option:`
`1- Modify "user name"`
`2- Modify "user password"`
`3- Modify "Confirm user password"`
`4- Modify "Description'`
`5- Discard changes`
	Enter **2** to modify the user password.

`Input User password :`	Enter **w3bl0g1c**.

Configure Adminstrator Username and Password: 1- *User name: weblogic 2- *User password: ******** 3- *Confirm user password: ****** 4- Description: This user is the default administrator Select Option: 1- Modify "user name" 2- Modify "user password" 3- Modify "Confirm user password" 4- Modify "Description' 5- Discard changes	Enter **3** to confirm user password.
Confirm user password:	Enter **w3bl0g1c**.
Configure Adminstrator Username and Password: 1- *User name: weblogic 2- *User password: ******** 3- *Confirm user password: ******** 4- Description: This user is the default administrator Select Option: 1- Modify "user name" 2- Modify "user password" 3- Modify "Confirm user password" 4- Modify "Description' 5- Discard changes	Press Enter to accept the values and continue.
Domain Mode Configuration: ->1| Development Mode 2|	Enter **2** to select Production Mode.
Java SDK Selection: ->1| Sun SDK 1.5.0_04 @ /usr/local/bea/jdk150_04 2| Other Java SDK	Press Enter to accept the default value and continue.
Choose Configuration Option: 1|Yes ->2| No	Enter **1** .

`Configure the Adminstration Server:`
 	
`Select Option:`
`1- *Name:  AdminServer`
`2- Listen address:  All Local Addresses`
`3- Listen port:  7001`
`4- SSL listen port:  N/A`
`5- SSl enabled:  false`
 	
`Select Option:`
`1- Modify "Name"`
`2- Modify "Listen address"`
`3- Modify "Listen port"`
`4- Modify "SSL enabled"`
	Press Enter to Continue.

`Configure Managed Servers:`
`Add or delete configuration information`
`for Managed Servers...`
 	
`Enter name for a new...`
	Enter **`ApplicationServer-2`**.

`Configure Managed Servers:`
`Add or delete configuration information`
`for Managed Servers...`
`Name:  ApplicationServer-2`
`Listen address:  All Local Addresses`
`Listen port:  7001`
`SSL listen port:  N/A`
`SSL enabled:  false`
 	
`Select Option:`
`1- Modify "Name"`
`2- Modify "Listen address"`
`3- Modify "Listen port"`
`4- Modify "SSL enabled"`
`5- Done`
	Enter **`3`** to modify the Listen port.

`Modify “Listen port.”`	Enter **`1081`**.

`Configure Managed Servers:`
`Add or delete configuration information`
`for Managed Servers...`
`Name:  ApplicationServer-2`
`Listen address:      All Local Addresses`
`Listen port:  1081`
`SSL listen port:  N/A`
`SSL enabled:  false`
 	
`Select Option:`
`1- Modify "Name"`
`2- Modify "Listen address"`
`3- Modify "Listen port"`
`4- Modify "SSL enabled"`
`5- Done`
	Press Enter to continue.

`Configure Clusters:` `Enter name for a new Cluster`	Press Enter to continue.
`Configure Machines:` `Enter name for a new Machine`	Press Enter to continue.
`Configure Unix Machines:` `Enter name for a new Unix Machine`	Enter **`ProtectedResource-2`**.

`Configure Unix Machines:`
`Add or delete configuration information for machines:`
`1- Name:  ProtectedResource-2`
`2- Post bind GID enabled:      false`
`3- Post bind GID:  nobody`
`4- Post bind UID enabled:  false`
`5- Post bind UID:  nobody`
`6- Node manager listen address:  localhost`
`7- Node manager listen port:  5556`
	Press Enter to accept these values.

`Enter name for a new Unix Machine.`	Enter **`ProtectedResource-2`**.

`Configure Unix Machines:`
`1- Name:      ProtectedResource-2`
`2- Post bind GID enbled:  false`
`2- Post bind GID:  nobody`
`4- Post bind UID enabled:      false`
`5- Post bind UID:  nobody`
`6- Node manager listen address:  localhost`
`7- Node manager listen port:      5556`
	Press Enter to accept these values.

`Configure Unix machines:`
`Name:  ProtectedResource-2`
 	
`Select Option:`
`1- Add Unix machine`
`2- Modify Unix machine`
`3- Delete unix machine`
`4- Discar Changes`
	Enter **1** to add a Unix machine.

`Assign Servers to Machines:`
 	
`Machine`
`Unix Machine`
`ProtectedResource-1 [1.1]`
`ProtectedResource-2  [1.2]`
	Press Enter to continue.

`Select the target domain directory for this domain:`	Press Enter to continue.
`Edit Domain Information:` `Enter value for "Name."`	Enter **`ProtectedResource-2`**.

`Edit Domain Information:`
`1- Name:  ProtectedResource-2`
 	
`Select Option:`
`1- Modify "Name"`
`2- Discard Changes`
	Press Enter to continue.

`Installation Complete` `Press [Enter] to continue...`	Press Enter.

4 Create two files necessary to automate Application Server 2 startup.

Create one file in the directory for the Application Server 2 administration server, and create one file in the Application Server 2 instance directory. The administrative user and password are stored in each file. Application Server 2 uses this information during server start-up. Without these files, Application Server 2 will fail to start. Application Server 2 encrypts the file, so there is no security risk even though you enter the user name and password in clear text.

```
# cd /usr/local/bea/user_projects/domains/
ProtectedResource-2/servers/AdminServer
# cat > boot.properties
username=weblogic
password=w3bl0g1c
^D
```

```
# cd /usr/local/bea/user_projects/domains/
ProtectedResource-2/servers/ApplicationServer-2/
# mkdir security
```

```
# cd security/
# cat > boot.properties
username=weblogic
password=w3bl0g1c
^D
```

5 Start the servers.

```
# cd /usr/local/bea/user_projects/
domains/ProtectedResource-2/bin/
# ./startWebLogic.sh &
#
# netstat -an | grep 7001
xxx.xx.72.151.7001        *.*            0            0 49152            0 LISTEN
127.0.0.1.7001                 *.*            0            0 49152            0 LISTEN
#
# cd /usr/local/bea/user_projects/domains/ProtectedResource-2/bin/
# ./startManagedWebLogic.sh ApplicationServer-2
http://ProtectedResource-2.example.com:7001 &

#
# ./startManagedWebLogic.sh ApplicationServer-2
http://ProtectedResource-2.example.com:7001
# cd /usr/local/bea/user_projects/domains/
ProtectedResource-1/bin/
# netstat -an | grep 7001
xxx.xx.72.151.1081        *.*            0            0 49152            0 LISTEN
127.0.0.1.1081                *.*         0            0 49152            0 LISTEN
xxx.xx.72.151.33425  xxx.xx.72.151.1081   49152        0 49152   0 ESTABLISHED
xxx.xx.72.151.1081   xxx.xx.72.151.33425  49152        0 49152   0 ESTABLISHED
```

6 Verify that Application Server 2 is up and running.

a. Go to the following URL:

`http://ProtectedResource-2.example.com:7001/console`

b. Log in to Application Server 2 using the following information:

User Name: **`weblogic`**

Password: **`w3bl0g1c`**

Verify that you can successfully log into the console.

c. Under Domain Structure > ProtectedResource-2, expand the Environment object.

d. Click Servers.

On the Summary of Servers page, verify that both `AdminServer(admin)` and `ApplicationServer-2` are running and OK.

▼ To Create an Agent Profile on Access Manager

This new account will be used by J2EE Policy Agent 2 to authenticate to the Access Manager server.

1 **Go to Access Manage load balancer URL:**

`https://LoadBalancer-3.example.com:9443/amserver/UI/Login`

2 **Log in to the Access Manager console using the following information:**

Username **`amadmin`**

Password **`4m4dmin1`**

3 **On the Access Control tab, under Realms, click the realm name** `example.com`**.**

4 **Click the Subjects tab.**

5 **Click the Agents tab.**

6 **On the Agent page, click New.**

7 **On the New Agent page, provide the following information:**

ID: **`j2eeagent-2`**

Password: **`j2ee4gent2`**

Password Confirm: **`j2ee4gent2`**

Device State: Choose **`Active`**.

8 **Click Create.**

The new agent `j2eeagent–2` is now display in the list of Agent Users.

9 **Log out of the Access Manager console.**

10 **Create a text file, and add the Agent Profile password to the file.**

The J2EE Policy Agent installer requires this file for installation.

```
# cd /opt/j2ee_agents/amwl9_agent
# cat > agent_pwd
j2ee4gent2
^D
```

▼ To Run the J2EE Policy Agent Installer on Application Server 2

Before You Begin Application Server 2 must not be running when you install J2EE Policy Agent 2.

You must stop both the Application Server 2 instance and the administration server before installing J2EE Policy Agent 2.

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-2/bin/
# ./stopManagedWebLogic.sh ApplicationServer-2  t3://localhost:7001
# cd /usr/local/bea/user_projects/domains/ProtectedResource-2/bin
# ./stopWebLogic.sh
```

1 Unpack the J2EE Policy Agent bits.

```
cd /opt
# /usr/sfw/bin/gtar -xvf /export/software/SJS_Weblogic_9_agent_2.2.tar
# gunzip ../SJS_Weblogic_9_agent_2.2.tar.gz
# /usr/sfw/bin/gtar -xvf ../SJS_Weblogic_9_agent_2.2.tar
```

2 Start the J2EE Policy Agent installer.

```
# cd /opt/j2ee_agents/am_wl9_agent/bin
# ./agentadmin --install
```

3 When prompted, provide the following information:

`Please read the following License Agreement carefully:`	Press Enter to continue. Continue to press Enter until you reach the end of the License Agreement.
`Enter startup script location.`	Enter **`/usr/local/bea/user_projects/domains/ProtectedResource-1/bin/startwebLogic.sh`**.
`Enter the WebLogic Server instance name: [myserver]`	Enter **`ApplicationServer-2`**.
`Access Manager Services Host:`	Enter **`LoadBalancer-3.example.com`**.
`Access Manager Services port: [80]`	Enter **`90`**.
`Access Manager Services Protocol: [http]`	Enter **`http`**.
`Access Manager Services Deployment URI: [/amserver]`	Accept the default value.
`Enter the Agent Host name:`	**`ProtectedResource-2.example.com`**

`Enter the WebLogic home directory: [usr/local/bea/weblogic90]`	Enter **`/usr/loca/bea/weblogic91`**.
`Enter the port number for Application Server instance [80]:`	Enter **`1081`**.
`Enter the Preferred Protocol for Application instance [http]:`	Accept the default value.
`Enter the Deployment URI for the Agent Application [/agentapp]`	Accept the default value.
`Enter the Encryption Key [Q558gNigkno4dGZmPtgGs4K1HL1153QD]:`	Accept the default value.
`Enter the Agent Profile name:`	Enter **`j2eeagent-1`**.
`Enter the path to the password file:`	Enter **`/opt/j2ee_agent/am_w19_agent/agent_pwd`**.
`Are the Agent and Access Manager installed on the same instance of Application Server? [false]:`	Accept the default value.

`Verify your settings and decide from the choices below:`
`1. Continue with Installation`
`2. Back to the last interaction`
`3. Start Over`
`4. Exit`
`Please make your selection [1]:`
	Accept the default value.

4 **Check the installation log to make sure there are no problems reported.**

8.8 Completing the J2EE Policy Agent 2 Installation

Use the following as your checklist for completing the J2EE Policy Agent 2 installation:

1. Modify the Application Server startup script.
2. Deploy the agent application.
3. Start the agent application.
4. Set up the agent authentication provider.
5. Edit the AMAgent.properties file.

▼ To Modify the Application Server Startup Script

The J2EE Policy Agent installer creates a new file in the Application Server `bin` directory:

```
/usr/local/bea/user_projects/domains/ProtectedResource-2/
bin/setAgentEnv_ApplicationServer-2.sh
```

1. **Make a backup of** `setDomainEnv.sh`**.**

   ```
   # cd /usr/local/bea/user_projects/domains/ProtectedResource-2/bin/
   ```

2. **In** `setDomainEnv.sh`**, insert the following at the end of the file:**

   ```
   . /usr/local/bea/user_projects/domains/ProtectedResource-2/
   bin/setAgentEnv_ApplicationServer-2.sh
   ```

   This command references the file the installer created in the Application Server `bin` directory.

3. **Save the file.**

4. **Change permissions for the** `setAgentEnv_ApplicationServer-2.sh` **file:**

   ```
   # chmod 755 setAgentEnv_ApplicationServer-2.sh
   ```

5. **Start the Application Server administration server.**

   ```
   # cd /usr/local/bea/user_projects/domains/ProtectedResource-2/bin
   # nohup ./startWebLogic.sh &
   # tail -f nohup.out
   ```

   Watch for startup errors.

▼ To Deploy the Agent Application

1. **Go to the following Application Server URL:**

   `http://ProtectedResource-2.example.com:7001/console`

2. **Log in to the Application Server console using the following information:**

   Username: **`weblogic`**

   Password: **`w3bl0g1c`**

3. **In the Application Server console, under Domain Structure, click Deployments.**

4. **On the Summary of Deployments page, click "Lock & Edit."**

5. **Under Deployments, click Install.**

6. **On the Install Application Assistant page, click the** `protectedresource-2.example.com` **link.**

7 **In the list for Location:** `protectedresource-2.example.com`**, click the root directory.**

Navigate to the application directory: `/opt/j2ee_agents/am_wl9_agent/etc/`

8 **Select** `agentapp.war`**, and then click Next.**

9 **In the Install Application Assistant page, choose "Install this deployment as an application," and then click Next.**

10 **In the list of Servers, mark the checkbox for ApplicationServer-2, and then click Next.**

11 **In the Optional Settings page, click Next.**

12 **On the Summary of Deployments page, click Finish.**

13 **In the Change Center, click Activate Changes.**

▼ To Start the Agent Application

1 **On the "Settings for agentapp" page, under Domain Structure, click Deployments.**

2 **On the Summary of Deployments page, mark the** `agentapp` **checkbox, and then click Start > Servicing All Requests.**

3 **On the Start Deployments page, clickYes.**

You may encounter a Javascript error. The agent application will not start until you start the Application Server.

▼ To Set Up the Agent Authentication Provider

1 **In the console, on the Summary of Deployments page, under Domain Structure, click Security Realms.**

2 **On the Summary of Security Realms page, in the Change Center click "Lock & Edit."**

3 **Click the Realm name** `myrealm` **link.**

4 **On the "Settings for myrealm" page, click the Providers tab.**

5 **On the Providers tab, under Authentication Providers, click New.**

6. **On the Create a New Authentication Provider page, provide the following information:**

   Name: **`Agent-1`**

   Type: **`AgentAuthenticator`**

7. **Click OK.**

   `Agent-1` is now included in the list of Authentication Providers.

8. **In the list of Authentication Providers, click `Agent-1`.**

9. **In the Settings for Authentication Providers page, verify that the Control Flag is set for OPTIONAL.**

10. **On the Settings for Agent-1 page, in the list of Authentication Providers, click DefaultAuthenticator.**

11. **On the Settings for DefaultAuthenticator page, set the Control Flag to OPTIONAL, and then click Save.**

12. **Return to the Providers page.**

    In the navigation tree near the top of the page, click Providers.

13. **Click Activate Changes.**

▼ To Edit the AMAgent.properties File

1. **Make a backup of the following file:**

   `/opt/j2ee_agents/am_wl9_agent/agent_001/config/AMAgent.properties`

2. **In the `AMAgent.properties` file, set the following property:**

   `com.sun.identity.agents.config.bypass.principal[0] = weblogic`

3. **At end of the file, insert a new property.**

   `com.sun.identity.session.resetLBCookie='true'`

   The default value for this property is `false`. You must add this property only if session failover has been configured for Access Manager. If session failover is not configured for Access Manager, and this property is added, it could impact performance negatively. If session failover is enabled for Access Manager, and this property is not added, then Access Manager sessions will still fail over, and the session failover functionality will work properly. However, the stickiness to the Access Manager server will not be maintained after failover occurs. Session

stickiness to the Access Manager server helps performance. This property must be added to the `AMConfig.properties` file on the Access Manager servers, as well as to the `AMAgent.properties` for the J2EE Policy Agent servers. This property is not required for the Web Policy Agent servers. The "Access Manager 7 2005Q4 Patch 3" in *Sun Java System Access Manager 7 2005Q4 Release Notes* Release Notes also references this property. See the section"CR# 6440651: Cookie replay requires com.sun.identity.session.resetLBCookie property" in *Sun Java System Access Manager 7 2005Q4 Release Notes*.

4 **Save the file.**

8.9 Setting Up a Test for the J2EE Policy Agent 2

Use the following as your checklist for setting up a test for the J2EE Policy Agent 2:

1. Deploy the sample application.
2. Restart the Application Server.
3. Create a test referral policy in the base suffix.
4. Create a test policy in the user realm.
5. Configure J2EE properties for the sample application.
6. Verify that J2EE Policy Agent 2 is configured properly.

▼ To Deploy the Sample Application

Deploy the sample application on Application Server 1.

1 **Go to the Application Server 1 URL:**

`http://ProtectedResource-1.example.com:7001/console`

2 **Log in to the Application Server using the following information:**

Username: **`weblogic`**

Password: **`w3bl0g1c`**

3 **In the Application Server console, on the Summary of Deployments page, click "Lock & Edit."**

4 **Under Domain Structure, click Deployments.**

5 **Under Deployments, click Install.**

6 **On the Install Application Assistant page, click the `protectedresource-1.example.com` link.**

7. **In the list for Location:** `protectedresource-2.example.com`**, click the root directory.**
   Navigate to the application directory: `/opt/j2ee_agents/am_wl9_agent/sampleapp/dist`
8. **Select** `agentsample.ear`**, and then click Next.**
9. **In the Install Application Assistant page, choose "Install this deployment as an application," and then click Next.**
10. **In the list of Servers, mark the checkbox for** `ApplicationServer-1`**, and then click Next.**
11. **On the "Optional Settings" page, click Next to accept the default settings.**
12. **On the Review Your Choices" page, click Finish.**
    The Target Summary section indicates that the module `agentsample` will be installed on the target `ApplicationServer-1`.
13. **In the "Settings for agentsample" page, click Activate Changes.**
14. **Under Domain Structure, click Deployments.**
15. **In the Deployments list, mark the checkbox for** `agentsample`**, and then click Start > Servicing All Requests.**
16. **On the Start Deployments page, click Yes.**
    The state of the deployment changes from Prepared to Active.
17. **Log out of the Application Server 1 console.**

▼ To Restart the Application Server

1. **Go to the following Protected Resource 1 directory:**
   `/usr/local/bea/user_projects/domains/ProtectedResource-1/bin`
2. **Stop Application Server 1.**

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
# ./stopManagedWebLogic.sh ApplicationServer-1 t3://localhost:7001
```

3. **Stop the administration server.**

```
#cd /usr/local/bea/user_projects/domains/ProtectedResource-1/bin
./stopWebLogic.sh
```

4 **Start the administration server.**

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

Watch for startup errors.

5 **Start Application Server 1.**

```
# nohup ./startManageWebLogic.sh
ApplicatoinServer-2 http://ProtectedResource-1.example.com:7001 &
tail -f nohup.out
```

6 **Run the `netstat` command to verify that Application Server 1 is up and listening.**

```
# netstat -an | grep 1081
xxx.xx.72.151.1081        *.*        0        0    49152        0    LISTEN
127.0.0.01.1081               *.*        0        0    49152        0    LISTEN
```

▼ To Create a Test Referral Policy in the Base Suffix

1 **In the Access Manager 1 console, on the Access Control tab, click the `example.com` link.**

2 **Click the Policies tab.**

3 **Under Policies, click the "Referral URL Policy for users realm" link.**

This is the policy that was created when setting up the Web Policy Agent.

4 **On the Edit Policy page, under Rules, click New.**

5 **On the page "Step 1 of 2: Select Service Type for the Rule," select "URL Policy Agent (with resource name)," and then click Next.**

6 **On the page "Step 2 of 2: New Rule," provide the following information, and then click Next:**

Name: **`URL Policy for ApplicationServer-2`**

Resource Name: **`http://ProtectedResource-2.example.com:1081/agentsample/*`**

7 **Click Finish.**

▼ To Create a Test Policy in the User Realm

1. **In the Access Manager 1 console, on the Access Control tab, click the `users` link.**
2. **Click the Policies tab.**
3. **Under Policies, click New Policy.**
4. **In the Name field, enter `URL Policy for ApplicationServer-2`.**
5. **Under Rules, click New.**
6. **On the page "Step 1 of 2: Select Service Type for the Rule," click Next.**
   The default "URL Policy Agent (with resource name)" should be selected.
7. **On the page "Step 2 of 2: New Rule," provide the following information:**

Name:	**`agentsample`**
Parent Resource Name:	Choose **`http://ProtectedResource-2.example.com:1081/agentsample/*`**
Resource Name:	The following is automatically entered when you select the Parent Resource Name above: **`http://ProtectedResource-2.example.com:1081/agentsample/*`**
GET	Mark this check box, and verify that the Allow value is selected.
POST	Mark this check box, and verify that the Allow value is selected.

8. **Click Finish.**
   The rule `agentsample` is now added to the list of Rules.
9. **Under Subjects, click New.**
10. **On the page "Step 1 of 2: Select Subject Type," select Access Manager Identity Subject, then click Next.**
11. **On the page " Step 2 of 2: New Subject — Access Manager Identity Subject," provide the following information:**

Name:	**`agentsampleRoles`**
Filter:	Select `role`.

12. **Click Search.**

13 **In the Available list, the select** `manager` **and** `employee` **roles, and then click Add.**

The roles are now displayed in the Selected list.

14 **Click Finish.**

15 **Click Create.**

The new policy is included in the list of Policies.

▼ To Configure J2EE Properties for the Sample Application

1 **Log in as a root user to Protected Resource 2.**

```
# cd /opt/j2ee_agents/am_wl9_agent/agent_001/config
```

2 **Make a back up the AMAgent.properties file.**

3 **Set the following properties:**

```
com.sun.identity.agents.config.notenforced.uri[0] =
   /agentsample/public/*
   com.sun.identity.agents.config.notenforced.uri[1] =
   /agentsample/images/*
   com.sun.identity.agents.config.notenforced.uri[2] =
   /agentsample/styles/*
   com.sun.identity.agents.config.notenforced.uri[3] =
   /agentsample/index.html
   com.sun.identity.agents.config.notenforced.uri[4] =
   /agentsample
   com.sun.identity.agents.config.access.denied.uri =
   /agentsample/authentication/accessdenied.html
   com.sun.identity.agents.config.login.form[0] =
   /agentsample/authentication/login.html
   com.sun.identity.agents.config.login.url[0] =
   http://LoadBalancer-3.example.com:7070/amserver/UI/Login?realm=users
```

4 **Save the file.**

5 **Restart the Application Server 2.**

a. **Stop Application Server 2 .**

```
# cd /usr/local/bea/user_projects/domains/
ProtectedResource-2/bin
```

```
# ./stopManagedWebLogic.sh ApplicationsServer-2
t3://localhost:7001
```

b. Stop the administration server.

```
# ./stopWebLogic.sh
```

c. Start the administration server.

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

d. Start Application Server 2.

```
# nohup ./startManagedWebLogic.sh ApplicationServer-2
http://ProtectedResource-2.example.com:7001 &
```

▼ To Verify that J2EE Policy Agent 2 is Configured Properly

1 Go to the Sample Application URL:

`http://protectedresource-2.example.com:1081/agentsample/index.html`

The Sample Application welcome page is displayed.

2 Click J2EE Declarative Security > "Invoke the Protected Servlet"

The Policy Agent redirects to the Access Manager login page.

3 Log in to the Access Manager console using the following information:

Username **`testuser1`**

Password **`password`**

If you can successfully log in as `testuser1`, and the J2EE Policy Agent Sample Application page is displayed, then this part of the test succeeded and authentication is working as expected.

4 Click the "J2EE Declarative Security" link.

5 On the J2EE Declarative Security page, click the "Invoke the Protected Servlet link".

If the Success Invocation message is displayed, then this part of the test succeeded , and the sample policy for the `manager` role has been enforced as expected.

6 Click the "J2EE Declarative Security" link to go back.

7. **Click the "Invoke the Protected EJB via an Unprotected Servlet" link.**

   If the Failed Invocation message is displayed, then this part of the test succeeded, and the sample policy for the `employee` role has been enforced as expected.

8. **Close the browser.**

9. **In a new browser session, go to the Sample Application URL:**

   `http://protectedresource-2.example.com:1081/agentsample/index.html`

   The Sample Application welcome page is displayed.

10. **Click the "J2EE Declarative Security" link.**

11. **On the J2EE Declarative Security page, click the "Invoke the Protected EJB via an Unprotected Servlet" link.**

    The Policy Agent redirects to the Access Manager login page.

12. **Log in to the Access Manager console using the following information:**

    Username **`testuser2`**

    Password **`password`**

    If you can successfully log in as **`testuser2`**, and the J2EE Policy Agent Sample Application page is displayed, then this part of the test succeeded and authentication is working as expected.

13. **Click the "J2EE Declarative Security" link to go back.**

14. **On the J2EE Declarative Security page, click the "Invoke the Protected EJB via an Uprotected Servlet" link.**

    The Successful Invocation message is displayed. The sample policy for the employee role has been enforced as expected.

8.10 Configuring Access Manager to Communicate Over SSL

Use the following as your checklist for configuring Access Manager to communicate over SSL:

1. Configure the J2EE Policy Agent for SSL.
2. Import a root CA certificate into the Application Server 2 key store.
3. Verify that J2EE Policy Agent 2 is configured properly.
4. Configure the J2EE Policy Agents to access the Distributed Authentication UI server.

▼ To Configure the J2EE Policy Agent for SSL

1 **Log in as a root user to Protected Resource 2.**

```
# cd /opt/j2ee_agents/am_wl9_agent/agent_001/config
```

2 **Make a backup of the `AMAgent.properties` file.**

3 **In the `AMAgent.properties`, set the following properties:**

```
com.sun.identity.agents.config.login.url[0] =
https://LoadBalancer-3.example.com:9443/amserver/UI/Login?realm=users
com.sun.identity.agents.config.cdsso.cdcservlet.url[0] =
https://LoadBalancer-3.example.com:9443/amserver/cdcservlet
com.sun.identity.agents.config.cdsso.trusted.id.provider[0] =
https://LoadBalancer-3.example.com:9443/amserver/cdcservlet
com.iplanet.am.naming.url=
https://LoadBalancer-3.example.com:9443/amserver/namingservice
com.iplanet.am.server.protocol=https
com.iplanet.am.server.port=9443
```

4 **Save the `AMAgent.properties` file.**

▼ To Import a Root CA Certificate into the Application Server 2 Key Store

1 **Log in as a root user to Protected Resource 2 and go to the following directory:**

```
/usr/local/bea/jdk150_04/jre/lib/security/
```

2 **Make a backup of `cacerts`.**

3 **Import the certificate.**

```
# /usr/local/bea/jdk150_04/bin/keytool -import -trustcacerts
-alias OpenSSLTestCA -file /export/software/ca.cer -keystore /
usr/local/bea/jdk150_04/jre/lib/security/cacerts -storepass changeit
Owner: EMAILADDRESS=nobody@nowhere.com, CN=OpenSSLTestCA, OU=Sun,
O=Sun, L=Santa Clara, ST=California, C=US
Issuer: EMAILADDRESS=nobody@nowhere.com, CN=OpenSSLTestCA, OU=Sun,
O=Sun, L=Santa Clara, ST=California, C=US
Serial number: 97dba0aa26db6386
Valid from: Tue Apr 18 07:55:19 PDT 2006 until: Tue Jan 13 06:55:19 PST 2009
Certificate fingerprints:
            MD5:  9F:57:ED:B2:F2:88:B6:E8:0F:1E:08:72:CF:70:32:06
            SHA1: 31:26:46:15:C5:12:5D:29:46:2A:60:A1:E5:9E:28:64:36:80:E4:70
```

```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

4 **Verify the certificate was added to the key store.**

```
# /usr/local/bea/jdk150_04/bin/keytool -list
-keystore /usr/local/bea/jdk150_04/jre/lib/security/cacerts
-storepass changeit | grep i openssl
opensssltestca, Oct 2, 2006, trustedCertEntry,
```

5 **Stop Application Server 2 .**

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-2/bin
# ./stopManagedWebLogic.sh ApplicationServer-2 t3://localhost:7001
```

6 **Stop the administration server.**

```
# ./stopWebLogic.sh
```

7 **Start the administration server.**

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

8 **Start Application Server 2.**

```
# nohup ./startManagedWebLogic.sh ApplicationServer-2
http://ProtectedResource-2.example.com:7001 &
```

▼ To Verify that J2EE Policy Agent 2 is Configured Properly

1 **Go to the Sample Application URL:**

`http://protectedresource-2.example.com:1081/agentsample/index.html`

The Sample Application welcome page is displayed.

2 **Click J2EE Declarative Security > "Invoke the Protected Servlet"**

The Policy Agent redirects to the Access Manager login page.

3 **Log in to the Access Manager console using the following information:**

Username **`testuser1`**

Password **`password`**

If you can successfully log in as `testuser1`, and the J2EE Policy Agent Sample Application page is displayed, then this part of the test succeeded and authentication is working as expected.

4. **Click the "J2EE Declarative Security" link.**

5. **On the J2EE Declarative Security page, click the "Invoke the Protected Servlet link".**

   If the Success Invocation message is displayed, then this part of the test succeeded , and the sample policy for the `manager` role has been enforced as expected.

6. **Click the "J2EE Declarative Security" link to go back.**

7. **Click the "Invoke the Protected EJB via an Unprotected Servlet" link.**

   If the Failed Invocation message is displayed, then this part of the test succeeded, and the sample policy for the `employee` role has been enforced as expected.

8. **Close the browser.**

9. **In a new browser session, go to the Sample Application URL:**

   `http://protectedresource-2.example.com:1081/agentsample/index.html`

   The Policy Agent redirects to the Access Manager login page.

10. **Log in to the Access Manager console using the following information:**

    Username **`testuser2`**

    Password **`password`**

    The Failed Invocation message is displayed.

11. **Click the "J2EE Declarative Security" link.**

12. **On the J2EE Declarative Security page, click the "Invoke the Protected EJB via an Unprotected Servlet" link.**

    The Successful Invocation message is displayed. The sample policy for the `employee` role has been enforced as expected.

13. **Click the "J2EE Declarative Security" link to go back.**

14. **Click the "Invoke the Protected Servlet" link.**

    If the Access to Requested Resource Denied message is displayed, then this part of the test is successful. The sample policy for the `manager` role has been enforced as expected.

▼ To Configure the J2EE Policy Agents to Access the Distributed Authentication UI Server

1 **Log in as a root user to Protected Resource 2.**

```
# cd /opt/j2ee_agents/am_wl9_agent/agent_001/config
```

2 **Make a backup of the file** `AMAgent.properties`**.**

3 **In the** `AMAgent.properties` **file, set the following properties:**

```
com.sun.identity.agents.config.login.url[0] =
https://LoadBalancer-4.example.com:9443/distAuth/UI/Login?realm=users
```

4 **Save the file.**

5 **Restart the Application Server.**

a. **Stop Application Server 2.**

```
# cd /usr/local/bea/user_projects/domains/ProtectedResource-2/bin
# ./stopManagedWebLogic.sh ApplicationServer-2 t3://localhost:7001
```

b. **Stop the administration server.**

```
#cd /usr/local/bea/user_projects/domains/ProtectedResource-2/bin
./stopWebLogic.sh
```

c. **Start the administration server.**

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

Watch for startup errors.

d. **Start Application Server 2.**

```
# nohup ./startManageWebLogic.sh
ApplicatoinServer-2 http://ProtectedResource-2.example.com:7001 &
tail -f nohup.out
```

6 **Verify that the agents are configured properly.**

a. **Go to the sample application URL:**

```
http://ProtectedResource-2.example.com:1081/agentsample/index.html
```

b. In the left navigation bar, click "Invoke the Protected Servlet."

You are redirected to the Distributed Authentication UI server URL `https://loadbalancer-4.example.com:9443/distAuth/UI/login`. The Access Manager login page is displayed.

c. Double-click the gold lock in the lower left corner of the browser.

In the Properties page, you see certificate for `LoadBalancer–4.example.com`.

d. Log in to the Access Manager console using the following information:

Username **`testuser1`**

Password **`password`**

You are redirected to the protected servlet of the Sample Application, and a success message is displayed. This indicates that authentication through the Distributed Authentication UI server was successful.

◆ ◆ ◆ CHAPTER 9

Setting Up Load Balancers for the Policy Agents

This chapter contains detailed instructions for the following tasks:

9.1 Configuring the Web Policy Agents Load Balancer

Load Balancer 5 can be located in a less-secured zone, and handles traffic for the Web Policy Agents.

Load Balancer 5 is configured for simple persistence so that browser requests from the same IP address will always be directed to the same Web Policy Agent instance . This guarantees that the requests from the same user session will always be sent to the same Web Policy Agent instance. This is important from the performance perspective. Each Web Policy Agent must validate the user session and evaluate applicable policies. The results are subsequently cached on the individual Web Policy Agent to improve the performance. If no load balancer persistence is set, and the same user's requests are spread across two agents, then each agent must build up its own cache. To do so, both agents must validate the session and evaluate policies. This effectively doubles the workload on the Access Manager servers, and cuts the overall system capacity by half. The problem becomes even more acute as the number of Web Policy Agents increases further.

As a general rule, in situations where each Web Policy Agent instance is protecting identical resources, some form of load balancer persistence is highly recommended for the performance reasons. The actual type of persistence may vary when a different load balancer is used, as long as it achieves the goal of sending the requests from the same user session to the same Web Policy Agent instance.

Use the following as your checklist for configuring the Web Policy Agents load balancer:

1. Configure the Web Policy Agents load balancer.

2. Configure the Web Policy Agent.
3. Create Policies for the agent resources.
4. Verify that the Web Policy Agents load balancer is working properly.

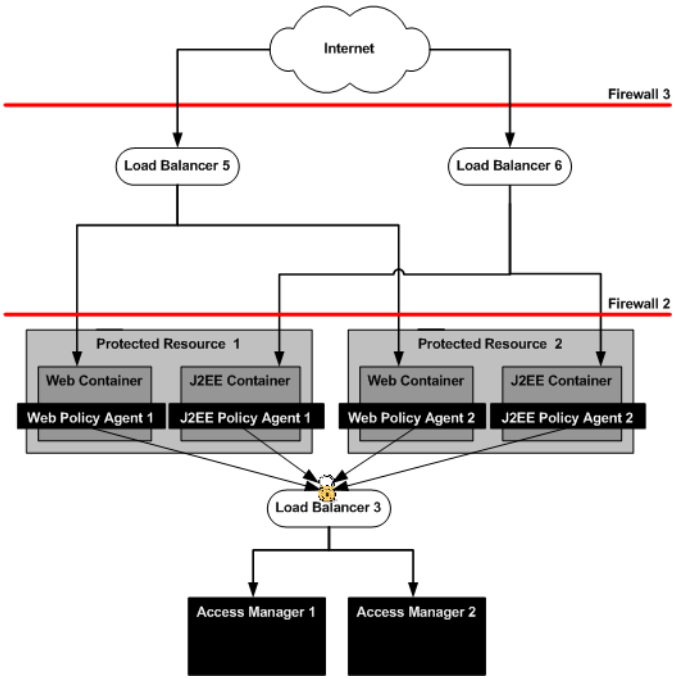

FIGURE 9–1 Policy Agents and Load Balancers

▼ To Configure the Web Policy Agents Load Balancer

1 Go to URL for the Big IP load balancer. login page and log in.

`https://ls-f5.example.com`

2 Log in using the following information:

User name: **`username`**

Password: **`password`**

3 Create a Pool.

A pool contains all the backend server instances.

a. Open the Configuration Utility.

Click "Configure your BIG-IP (R) using the Configuration Utility."

b. In the left pane, click Pools.

c. On the Pools tab, click the Add button.

d. In the Add Pool dialog, provide the following information:

Pool Name	Example: WebAgent-Pool
Load Balancing Method	Round Robin
Resources	Add all the Web Policy Agent IP addresses. In this example, add the IP address and port number for `ProtectedResource-1:1080` and for `ProtectedResource-2:1080`.

e. Click the Done button.

4 Configure the load balancer for simple persistence.

a. In the left frame, click Pools.

b. Click the name of the pool you want to configure.
In this example, WebAgent-Pool.

c. Click the Persistence tab.

d. On the Persistence tab, under Persistence Type, select the Simple.

e. Set the timeout interval.
In the Timeout field, enter 300 seconds.

f. Click Apply.

5 Add a Virtual Server.
If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

a. In the left frame, Click Virtual Servers.

b. On the Virtual Servers tab, click the Add button.

c. In the Add a Virtual Server dialog box, provide the following information:

Address	`xxx.xx.69.14` (for `LoadBalancer-5.example.com`)
Service	`90`

Pool `WebAgent-Pool`

d. Continue to click Next until you reach the Pool Selection dialog box.

e. In the Pool Selection dialog box, assign the Pool (WebAgent-Pool) that you have just created.

f. Click the Done button.

6 Add Monitors.

a. Click the Monitors tab, and then click the Add button.

In the Add Monitor dialog provide the following information:

Name: **`WebAgent-http`**

Inherits From: Choose **`http`**.

b. Click Next.

In the Configure Basic Properties page, click Next.

c. In the Configure ECV HTTP Monitor, in the Send String field, enter the following:

```
GET / launch.html
```

Click Next.

d. In the Destination Address and Service (Alias) page, click Done.

On the Monitors tab, the monitor you just added is now contained in the list of monitors.

e. Click the Basic Associations tab.

Look for the IP addresses for `ProtectedResource-1:1080` and `ProtectedResourece-2:1080`.

f. Mark the Add checkbox for `ProtectedResource-1` and `ProtectedResource-2`.

g. At the top of the Node column, choose the monitor that you just added, `WebAgent-http`.

h. Click Apply.

▼ To Configure the Web Policy Agent

In this procedure you modify the `AMAgent.properties` file. Map Protected Resource 1 and Protected Resource 2 to Load Balancer 5.

1. **Log in as a root user to Protected Resource 1.**

   ```
   # cd /etc/opt/SUNWam/agents/es6/
   config/_opt_SUNWwbsvr_https-ProtectedResource-1.example.com
   ```

2. **Use a text editor to modify the `AMAgent.properties` file.**

   Make a backup of `AMAgent.properties`, and then add the following entry:

   ```
   com.sun.am.policy.agents.config.fqdn.map =
   LoadBalancer-5.example.com|LoadBalancer-5.example.com
   ```

   For this property:

   `com.sun.am.policy.agents.config.notenforced_list`

   append the following to the end of the value string :

   ```
   http://ProtectedResource-1.example.com:1080/launch.html
   http://LoadBalancer-5.example.com:90/launch.html
   ```

3. **Save the file.**

4. **Log in as a root user to Protected Resource 2.**

   ```
   # cd /etc/opt/SUNWam/agents/es6/
   config/_opt_SUNWwbsvr_https-ProtectedResource-2.example.com
   ```

5. **Use a text editor to modify the `AMAgent.properties` file.**

   Make a backup of `AMAgent.properties`, and then add the following entry:

   ```
   com.sun.am.policy.agents.config.fqdn.map =
   LoadBalancer-5.example.com|LoadBalancer-5.example.com
   ```

   For this property:

   `com.sun.am.policy.agents.config.notenforced_list`

   append the following to the end of the value string :

   ```
   http://ProtectedResource-2.example.com:1080/launch.html
   http://LoadBalancer-5.example.com:90/launch.html
   ```

6. **Save the file.**

▼ To Create Policies for the Agent Resources

The policies you create here are used in a the subsequent verification procedure.

1 Create a referral policy for Load Balancer 5.

a. Go to the Access Manager URL:

`https://loadbalancer-3.example.com:9443/amserver/UI/Login`

b. Log in to the Access Manager console using the following information:

Username **`amadmin`**

Password **`4m4dmin1`**

c. On the Access Control tab, click the realm name `example.com`.

d. Click the Policies tab.

e. Click the "Referral URL Policy for users realm" link.

f. In the Edit Policy page, under Rules, click New.

g. In the page "Step 1 of 2: Select Service Type for the Rule," select "URL Policy Agent (with resource name), and then click Next.

h. In the page "Step 2 of 2: New Rule," provide the following information:

Name: **`URL Rule for LoadBalancer-5`**

Resource Name: **`http://LoadBalancer-5.example.com:90/*`**

i. Click Finish, and then click Save.

The new rules you added are now contained in the Rules list.

2 Create a policy in the users realm.

a. In the Edit Policy page, click the Realms link.

b. On the Access Control tab, click the `users` link.

c. Click the Policies tab, and then click New Policy.

In the Name field, enter **`URL Policy for LoadBalancer-5`**.

d. Under Rules, click NEW.

e. In the page "Step 1 of 2: Select Service Type for the Rule," click Next.

f. In the page "Step 2 of 2: New Rule," provide the following information:

Name:	Enter **`LoadBalancer-5`**.
Parent Resource Name:	Click `http://LoadBalancer-5.example.com:90/*` to select it. The Parent Resource Name you selected is now contained in the Resource Name field.
GET	Mark the checkbox, and verify that the Allow option is selected.
POST	Mark the checkbox, and verify that the Allow option is selected.

g. Click Finish.

h. In the New Policy page, in the Subjects section, click New.

i. In the "Step 1 of 2: Select Subject Type" page, be sure that Access Manager Identity Subject is selected, and then click Next.

j. In the "Step 2 of 2: New Subject — Access Manager Identity Subject" page, provide the following information:

Name:	**`LoadBalancer-5_Roles`**
Filter:	In the drop-down list, select Role. Then click Search. The search returns a list of available roles.

k. In the Available: list, select `manager` and `employee`, and then click Add.

The roles `manager` and `employee` are now contained in the Selected List.

l. Click Finish.

m. On the Policy page, click Create.

The policy you just created is now included in the list of Policies.

3 Log out of the Access Manager console and close the browser.

▼ To Verify that the Web Policy Agents Load Balancer is Working Properly

1 **Restart Web Server 1 on Protected Resource 1.**

```
#cd /opt/SUNWwbsvr/https-ProtectedResource-1.example.com
# ./stop; ./start
```

2 **Restart Web Server 2 on Protected Resource 2.**

```
#cd /opt/SUNWwbsvr/https-ProtectedResource-2.example.com
# ./stop; ./start
```

3 **In a browser, go to the following URL:**

`http://loadbalancer-5.example.com:90/index.html`

The load balancer redirects the request to the Access Manager login page.

4 **Log in to the Access Manager console using the following information:**

Username **`testuser1`**

Password **`password`**

If the default Web Server `index.html` page is displayed, then the load balancer is configured properly.

5 **Verify that Load Balancer 5 monitors are monitoring the Web Servers properly.**

a. **Log in as a root user to Protected Resource 1.**

b. **Run the `tail` command.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-1.example.com/logs
# tail -f access
```

If you see frequent entries similar to this one:

```
xxx.xx.69.18 - - [06/Oct/2006:13:53:07 -0700] "GET /launch.html" 200 8526
```

then the custom monitor is configured properly. If you do not see "`GET /launch.html`", then you must troubleshoot the load balancer configuration.

c. **Log in as root to Protected Resource 2.**

d. **Run the `tail` command.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-1.example.com/logs
# tail -f access
```

If you see frequent entries similar to this one:

```
xxx.xx.69.18 - - [06/Oct/2006:13:53:07 -0700] "GET /launch.html" 200 8526
```

then the custom monitor is configured properly. If you do not see "`GET /launch.html`", then you must troubleshoot the load balancer configuration.

9.2 Configuring the J2EE Policy Agents Load Balancer

Load Balancer 6 can be located in a less-secured zone, and handles traffic for the J2EE Policy Agents.

Load Balancer 6 is configured for simple persistence so that browser requests from the same IP address will always be directed to the same J2EE Policy Agent instance . This guarantees that the requests from the same user session will always be sent to the same J2EE Policy Agent instance. This is important from the performance perspective. Each J2EE Policy Agent must validate the user session and evaluate applicable policies. The results are subsequently cached on the individual Web Policy Agent to improve the performance. If no load balancer persistence is set, and the same user's requests are spread across two agents, then each agent must build up its own cache. To do so, both agents must validate the session and evaluate policies. This effectively doubles the workload on the Access Manager servers, and cuts the overall system capacity by half. The problem becomes even more acute as the number of J2EE Policy Agents increases further.

As a general rule, in situations where each J2EE Policy Agent instance is protecting identical resources, some form of load balancer persistence is highly recommended for the performance reasons. The actual type of persistence may vary when a different load balancer is used, as long as it achieves the goal of sending the requests from the same user session to the same J2EE Policy Agent instance.

Use the following as your checklist for configuring the J2EE Policy Agents load balancer:

1. Configure the J2EE Policy Agents load balancer.
2. Configure the Agent.
3. Create Polices for the agent resources.
4. Verify that the J2EE Policy Agents load balancer is working properly.

▼ To Configure the J2EE Policy Agents Load Balancer

1 Go to URL for the Big IP load balancer login page and log in.

`https://ls-f5.example.com`

User name: **`username`**

Password: **password**

2 Create a Pool.

A pool contains all the backend server instances.

a. Open the Configuration Utility.

Click "Configure your BIG-IP (R) using the Configuration Utility."

b. In the left pane, click Pools.

c. On the Pools tab, click the Add button.

d. In the Add Pool dialog, provide the following information:

Pool Name	Example: J2EEAgent-Pool
Load Balancing Method	Round Robin
Resources	Add all the Application Server IP addresses. In this example, add the IP address and port number for `ProtectedResource-1:1081` and for `ProtectedResource-2:1081`.

e. Click the Done button.

f. In the List of Pools, click the name of the pool you just created (J2EEAgent-Pool).

g. Click the Persistence tab, provide the following information, and then click Apply:

Persistence Type:	Choose "Active Http Cookie."
Method:	Choose Insert.

3 Add a Virtual Server.

If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

a. In the left frame, Click Virtual Servers.

b. On the Virtual Servers tab, click the Add button.

c. In the Add a Virtual Server dialog box, provide the following information:

Address	`xxx.xx.69.14` (for `LoadBalancer-6.example.com`)
Services Port	`91`

Pool J2EEAgent-Pool

d. **Continue to click Next until you reach the Pool Selection dialog box.**

e. **In the Pool Selection dialog box, assign the Pool (J2EEAgent-Pool) that you have just created.**

f. **Click the Done button.**

4 **Add Monitors.**

a. **Click the Basic Associations tab.**

Look for the IP addresses for `ProtectedResource-1:1081` and `ProtectedResourece-2:1081`.

b. **Mark the Add checkbox for ProtectedResource-1 and ProtectedResource-2.**

c. **At the top of the Node column, select `tcp`.**

d. **Click Apply.**

▼ To Configure the Agent

In the `AMAgent.properties` file, map Protected Resource 1 and Protected Resource 2 to Load Balancer 6 .

1 **Log in as root to Protected Resource 1.**

2 **Use a text editor to modify the `AMAgent.properties` file.**

```
# cd /opt/j2ee_agents/am_wl9_agent/agent_001/config
```

Make a backup of `AMAgent.properties`, and then set the following property:

```
com.sun.identity.agents.config.fqdn.mapping[LoadBalancer-6.example.com] =
LoadBalancer-6.example.com
```

3 **Save the file.**

4 **Log in as root to Protected Resource 2.**

5 **Use a text editor to modify the `AMAgent.properties` file.**

```
# cd /opt/j2ee_agents/am_wl9_agent/agent_001/config
```

Make a backup of `AMAgent.properties`, and then set the following property:

```
com.sun.identity.agents.config.fqdn.mapping[LoadBalancer-6.example.com] =
LoadBalancer-6.example.com
```

6 Save the file.

▼ To Create Polices for the Agent Resources

The policies you create here are used in a subsequent procedure that verifies that the agents and load balancer work properly.

1 Create a referral policy for Load Balancer 6.

a. Go to the Access Manager URL:

`https://loadbalancer-3.example.com:9443/amserver/UI/Login`

b. Log in to the Access Manager console using the following information:

Username **amadmin**

Password **4m4dmin1**

c. On the Access Control tab, click the realm name `example.com`**.**

d. Click the Policies tab.

e. Click the "Referral URL Policy for users realm" link.

f. In the Edit Policy page, under Rules, click New.

g. In the page "Step 1 of 2: Select Service Type for the Rule," select "URL Policy Agent (with resource name), and then click Next.

h. In the page "Step 2 of 2: New Rule," provide the following information:

Name: **URL Rule for LoadBalancer-6**

Resource Name: **http://LoadBalancer-6.example.com:91/***

i. Click Finish, and then click Save.

The new rules you added are now contained in the rules list.

2 Create a policy for the users realm.

a. In the Edit Policy page, click the Realms link.

b. On the Access Control tab, click the `users` link.

c. Click the Policies tab, and then click New Policy.

In the Name field, enter **`URL Policy for LoadBalancer-6`** .

d. Under Rules, click NEW.

e. In the page "Step 1 of 2: Select Service Type for the Rule," click Next.

f. In the page "Step 2 of 2: New Rule," provide the following information:

Name:	Enter **`LoadBalancer-6`**.
Parent Resource Name:	Click `http://LoadBalancer-6.example.com:91/*` to select it. The Parent Resource Name selected is not contained in the Resource Name field.
GET	Mark the checkbox, and verify that the Allow option is selected.
POST	Mark the checkbox, and verify that the Allow option is selected.

g. Click Finish.

h. In the "Step 1 of 2: Select Subject Type" page, be sure that Access Manager Identity Subject is selected, and then click Next.

i. In the "Step 2 of 2: New Subject — Access Manager Identity Subject" page, provide the following information:

Name:	**`LoadBalancer-6_Roles`**
Filter:	In the drop-down list, select Role. Then click Search. The search returns a list of available roles.

j. In the Available: list, select `manager` and `employee`, and then click Add.

The roles `manager` and `employee` are now contained in the Selected List.

k. Click Finish.

3 Log out of the Access Manager console and close the browser.

▼ To Verify that the J2EE Policy Agents Load Balancer is Working Properly

1 Restart the Application Servers.

a. Stop Application Server 1 .

```
# cd /usr/local/bea/user_projects/
domains/ProtectedResource-1/bin
# ./stopManagedWebLogic.sh ApplicationsServer-1
t3://localhost:7001
```

b. Stop the administration server.

```
# ./stopWebLogic.sh
```

c. Start the administration server.

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

d. Start Application Server 1.

```
# nohup ./startManagedWebLogic.sh
ApplicationServer-1 http://ProtectedResource-1.example.com:7001 &
```

e. Stop Application Server 2 .

```
# cd /usr/local/bea/user_projects/domains/
ProtectedResource-2/bin
# ./stopManagedWebLogic.sh ApplicationsServer-2
t3://localhost:7001
```

f. Stop the administration server.

```
# ./stopWebLogic.sh
```

g. Start the administration server.

```
# nohup ./startWebLogic.sh &
# tail -f nohup.out
```

h. Start Application Server 2.

```
# nohup ./startManagedWebLogic.sh
ApplicationServer-2 http://ProtectedResource-2.example.com:7001 &
```

2 Go to the Sample Application URL:

`http://loadbalancer-6.example.com:91/agentsample/index.html`

The Sample Application welcome page is displayed.

3 **Click J2EE Declarative Security > "Invoke the Protected Servlet"**

The Policy Agent redirects to the Access Manager login page.

4 **Log in to the Access Manager console using the following information:**

Username **testuser1**

Password **password**

If you can successfully log in as `testuser1`, and the J2EE Policy Agent Sample Application page is displayed, then this part of the test succeeded and authentication is working as expected.

5 **Click the "J2EE Declarative Security" link.**

6 **On the J2EE Declarative Security page, click the "Invoke the Protected Servlet link".**

If the Success Invocation message is displayed, then this part of the test succeeded , and the sample policy for the `manager` role has been enforced as expected.

7 **Click the "J2EE Declarative Security" link to go back.**

8 **Click the "Invoke the Protected EJB via an Unprotected Servlet" link.**

If the Failed Invocation message is displayed, then this part of the test succeeded, and the sample policy for the `employee` role has been enforced as expected.

9 **Close the browser.**

10 **In a new browser session, go to the Sample Application URL:**

`http://loadbalancer-6.example.com:91/agentsample/index.html`

The Sample Application welcome page is displayed.

11 **Click the "J2EE Declarative Security" link.**

12 **On the J2EE Declarative Security page, click the "Invoke the Protected EJB via an Unprotected Servlet" link.**

The Policy Agent redirects to the Access Manager login page.

13 **Log in to the Access Manager console using the following information:**

Username **testuser2**

Password **password**

If you can successfully log in as **testuser2**, and the J2EE Policy Agent Sample Application page is displayed, then this part of the test succeeded and authentication is working as expected.

14 Click the "J2EE Declarative Security" link to go back.

15 On the J2EE Declarative Security page, click the "Invoke the Protected EJB via an Uprotected Servlet" link.

The Successful Invocation message is displayed. The sample policy for the employee role has been enforced as expected.

◆ ◆ ◆ CHAPTER 10

Implementing Session Failover

This chapter contains detailed instructions for the following tasks:

10.1 Installing Two Message Queue Instances

When session failover is implemented for Access Manager, session information is replicated in two backend session store databases. This ensures that when one Access Manager fails or stops, the information stored in the backend session databases can be used to keep the user continuously authenticated. If session failover is not implemented, when one Access Manager fails, if the user's session was created in the failed Access Manager server, the next time the user performs an operation that requires a session token, the user will have to use a login page to re-authenticate.

Use the following as your checklist for installing the Message Queue instances:

1. Install Message Queue 1.
2. Install Message Queue 2.

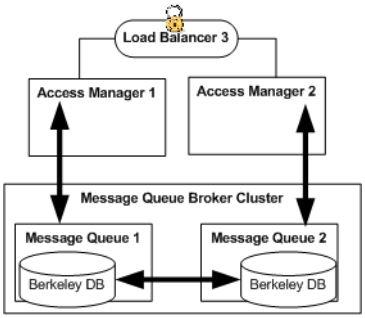

FIGURE 10–1 Session Failover

Access Manager provides a web container-independent session failover feature that uses Sun Java System Message Queue (Message Queue). Message Queue is a messaging middleware product that enables distributed applications to communicate and exchange data by sending and receiving messages. In this Deployment Example, Access Managers uses Message Queue as a communications broker, and uses the Berkeley DB by Sleepycat Software, Inc. for the backend session store databases.

For detailed information about how Access Manager and Message Queue interact, see "Implementing Access Manager Session Failover" in *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide* in the *Access Manager Deployment Planning Guide*.

▼ To Install Message Queue 1

Before You Begin The Java ES installer must be mounted on the host computer system where you will install Message Queue. See the section "To Download and Unpack the Java Enterprise System 2005Q4 Installer""3.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer" on page 32 in this document.

1. **Log in as a root user to the host MessageQueue–1.**

2. **Start the installer with `-nodisplay` option. Example:**

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

3. **When prompted, provide the following information:**

Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>	Press Enter.
Before you install this product, you must read and accept the entire Software License Agreement under which this product is licensed for your use. <Press ENTER to display the Software License Agreement>	Press Enter.
Language Support Please enter a comma separated list of languages you would like supported with this installation [8]	Enter **8** for English.
The following component products are detected on this system. They will appear disabled, "* *", in the following Component Selection Main Menu <Press ENTER to continue>	Press Enter.
Component Selection - Main Menu Enter a comma separated list of products to install, or press R to refresh the list []:	Enter **12** for Message Queue.
Based on product dependencies for your selections,the installer will install: [X] 12. Sun Java(TM) System Message Queue 3 2005Q4 Enterprise Edition (10.06 MB) Press "Enter" to Continue...	Press Enter.
Shared Component Upgrades Required Enter 1 to upgrade these shared components and 2 to cancel [1]:	Accept the default value.
System Ready for Installation. Memory detectionis disabled in a local zone. Enter 1 to continue [1]	Accept the default value.

`Screen for selecting Type of Configuration`
`1. Configure Now - Selectively override defaults or`
`express through  2. Configure Later - Manually configure following installation`
`Select Type of Configuration [1]`
	Enter **1** for Configure Now.

`Sun Java(TM) System Message Queue 3 2005Q4 Enterprise Edition`
`1. Install`
`2. Start Over`
`3. Exit Installation.`
`What would you like to do [1]`
	First, see the following (Optional) Step 4. When you're ready to install, press Enter to accept the default value.

`Installation Complete` `Enter 1 to view installation summary and Enter 2 to view installation logs [1]`	Enter **!** when you're ready to exit the installer program.

4 (Optional) Monitor the log files and watch for installation errors.

```
# cd /var/sadm/install/logs
# tail -f Java_Enterprise_System_install.B10110830
```

▼ To Install Message Queue 2

1 Log in as a root user to the host MessageQueue–2.

2 Start the installer with `-nodisplay` option. Example:

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

3 When prompted, provide the following information:

`Welcome to the Sun Java(TM) Enterprise System;`
`serious software made simple...`
`<Press ENTER to Continue>`
	Press Enter.

`Before you install this product, you must read and accept the entire Software License Agreement under which this product is licensed for your use. <Press ENTER to display the Software License Agreement>`	Press Enter.
`Language Support Please enter a comma separated list of languages you would like supported with this installation [8]`	Enter **8** for English.
`The following component products are detected on this system. They will appear disabled, "* *", in the following Component Selection Main Menu <Press ENTER to continue>`	Press Enter.
`Component Selection - Main Menu Enter a comma separated list of products to install, or press R to refresh the list []:`	Enter **12** for Message Queue.
`Based on product dependencies for your selections,the installer will install: [X] 12. Sun Java(TM) System Message Queue 3 2005Q4 Enterprise Edition (10.06 MB) Press "Enter" to Continue...`	Press Enter.
`Shared Component Upgrades Required Enter 1 to upgrade these shared components and 2 to cancel [1]:`	Accept the default value.
`System Ready for Installation. Memory detectionis disabled in a local zone. Enter 1 to continue [1]`	Accept the default value.
`Screen for selecting Type of Configuration 1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]`	Enter **1** for Configure Now.

`Sun Java(TM) System Message Queue 3 2005Q4 Enterprise Edition`
`1. Install`
`2. Start Over`
`3. Exit Installation.`
`What would you like to do [1]`
	First, see the following (Optional) Step 4. When you're ready to install, press Enter to accept the default value.

`Installation Complete` `Enter 1 to view installation summary and Enter 2 to view installation logs [1]`	Enter `!` when you're ready to exit the installer program.

4 (Optional) Monitor the log files and watch for installation errors.

```
# cd /var/sadm/install/logs
# tail -f Java_Enterprise_System_install.B10110830
```

10.2 Installing the Access Manager Session Failover Components

The Java ES installer and `amconfig` script adds the Access Manager packages or RPMs required for the Berkeley DB client. However, if you want to install the Berkeley DB client on a server where you have not installed Access Manager, you must manually add the following packages or RPMs, depending on your operating system. In this deployment example, for the Solaris OS, you add the following packages using the `pkgadd` command: `SUNWbdb`, `SUNWbdbj`, and `SUNWamsfodb`. In this deployment example, it is not necessary to run the `amsfoconfig` utility.

Use the following as your checklist for installing the Access Manager session failover components:

1. Install Access Manager session failover components on Message Queue 1.
2. Install Access Manager session failover components on Message Queue 2.
3. Edit the Access Manager Web Server configuration files.
4. Verify that Session Failover works properly.

▼ To Install Access Manager Session Failover Components on Message Queue 1

1 **As root, log in to the host MessageQueue-1.**

2 **Use the `pkgadd` command to install the Access Manager session failover component packages.**

a. **Add the BerkeleyDB-Base and BerkeleyDB-Java packages.**

```
# cd /mnt/Solaris_sparc/Product/shared_components/Packages
# pkgadd -d . SUNWbdb SUNWbdbj
```

b. **Add the Access Manager Session Failover DB components.**

```
# cd /mnt2/Solaris_sparc/Product/identity_svr/Packages
# pkgadd -d . SUNWamsfodb
```

3 **Add a new user and password.**

These are the user and password you will use connect to the Message Queue broker on servers where Message Queue is installed. Using this new user ensures that the guest user will not be able to access the other Access Manager server.

a. **Create a new instance named `msgqbroker` by running the following command:**

```
/bin/imqbrokerd -name msgqbroker -port 7777 &
```

Run the `netstat` command to verify that the new Message Queue instance is up and running.

```
# netstat -an | grep 7777
*.7777       *.*           0           0    49152       0    LISTEN
```

b. **Add a new user named `msgquser`.**

For this deployment example, create a specific user who will be used only for session failover purposes. This new user does not assume the privileges of the guest user. It is a good practice to create a custom user for such purposes, and not to rely on the known user accounts or default user accounts. This helps to prevent brute force or DOS attacks.

```
# /bin/imqusermgr add -u msgquser -g admin -p m5gqu5er -i msgqbroker
```

c. **Update the guest user.**

This step effectively disables the guest user.

```
# /bin/imqusermgr update -u guest -a false -i msgqbroker
User repository for broker instance: msgqbroker
Are you sure you want to update user guest? (y/n) y
User guest successfully updated.
```

4 Edit the `/opt/SUNWam/lib/amsfo.conf` file.

Make a backup of the `amsfo.conf` file, and then set the following properties:

```
CLUSTER_LIST=MessageQueue-1.example.com:7777,MessageQueue-2.example.com:7777
BROKER_INSTANCE_NAME=msgqbroker
USER_NAME=msgquser
lbServerPort=9443
lbServerProtocol=https
lbServerHost=LoadBalancer-3.example.com
SiteID=11
```

5 Run the `amsfopassword` command.

This command generates an encrypted password, creates a new file named `.password`, and stores the encrypted password in the new file.

```
# cd /opt/SUNWam/bin

# ./amsfopassword -e m5gqu5er -f /opt/SUNWam/.password
```

To view the encrypted password:

```
# more /opt/SUNWam/.password

M27OGb6U4ufRu+oWAzBdWw==
```

6 Edit the `/opt/SUNWam/bin/amsessiondb` script.

Make a backup of the `/opt/SUNWam/bin/amsessiondb` script before making any changes to the script.

The `amsessiondb` script is called by the `amsfo` script to start the Berkeley DB client (`amsessiondb`), create the database, and set specific database values. The script contains variables that specify various default paths and directories:

```
JAVA_HOME=/usr/jdk/entsys-j2se/
IMQ_JAR_PATH=/usr/share/lib
JMS_JAR_PATH=/usr/share/lib
BDB_JAR_PATH=/usr/share
BDB_SO_PATH=/usr/lib
AM_HOME=/opt/SUNWam
```

If any of these components are not installed in their default directories, edit the `amsessiondb` script and set the variables, as needed, to the correct locations.

7 Edit the `/opt/SUNWam/bin/amsfo`script.

Make a backup of the `/opt/SUNWam/bin/amsfo` script before making any changes to the script. In the following line, add the the parameter –`name $BROKER_INSTANCE_NAME` as follows:

```
$JMQEXECUTABLE -bgnd $BROKER_OPTIONS -vmargs $BROKER_VM_ARGS
           -name $BROKER_INSTANCE_NAME -port $BROKER_PORT
           -cluster $CLUSTER_LIST &
```

```
-jmqpid=$!
echo $_jmqpid > $JMQ_PID_FILE
```

8 Restart the Access Manager session failover components.

a. Stop the Message Queue broker instance.

```
# cd /opt/SUNWam/bin
# ./amsfo stop
```

b. Run the `netstat` command to verify that the Message Queue broker instance is stopped.

```
# netstat -an | grep 7777
```

If `netstat` returns no result, then the Message Queue broker instance is stopped.

Tip – If the Message Queue broker instance is not stopped, run the following commands:

```
# cd /tmp/amsession/logs
# cat *.pid
```

Process IDs are displayed. Example:

```
4940
    4924
```

Kill these Java processes. Example:

```
# kill -9 4940 4924
```

If you don't see the process-ids in that file, and the `netstat` is still listening on port 7777, then it's possible that the `amsfo` script did not stop properly. In this case, run the following command to identify the java processes:

```
# ps -ef | grep java
```

Then kill those identified processes as shown in the `kill` command example above.

Then check with `netstat` again. The port socket should be relinquished before you start up `amsfo` again. Otherwise, session failover problems may occur.

---

c. Restart the Message Queue broker instance.

```
# ./amsfo start
```

d. Run the `netstat` command to verify that the Message Queue port is open and listening.

```
# netstat -an | grep 7777
*.7777           *.*           0           0    49152           0    LISTEN
```

▼ To Install Access Manager Session Failover Components on Message Queue 2

1 As root, log in to the host MessageQueue-2.

2 Use the `pkgadd` command to install the Access Manager session failover component packages.

a. Add the BerkeleyDB-Base and BerkeleyDB-Java packages.

```
# cd /mnt/Solaris_sparc/Product/shared_components/Packages
# pkgadd -d . SUNWbdb SUNWbdbj
```

b. Add the Access Manager Session Failover DB components.

```
# cd /mnt2/Solaris_sparc/Product/identity_svr/Packages
# pkgadd -d . SUNWamsfodb
```

3 Add a new user and password.

This is the user and password you will use connect to the Message Queue broker on servers where Message Queue is installed. Using this new user ensures that the guest user will not be able to access the other Access Manager server.

a. Create a new instance named `msgqbroker` by running the following command:

```
/bin/imqbrokerd -name msgqbroker -port 7777 &
```

Run the `netstat` command to verify that the new Message Queue instance is up and running.

```
# netstat -an | grep 7777
*.7777           *.*               0           0    49152           0    LISTEN
```

b. Add a new user named `msgquser`.

```
# /bin/imqusermgr add -u msgquser -g admin -p m5gqu5er -i msgqbroker
```

c. Update the guest user.

```
# /bin/imqusermgr update -u guest -a false -i msgqbroker
User repository for broker instance: msgqbroker
Are you sure you want to update user guest? (y/n) y
User guest successfully updated.
```

4 Edit the `/opt/SUNWam/lib/amsfo.conf` file.

Make a backup of the `amsfo.conf` file, and then set the following properties:

```
CLUSTER_LIST=MessageQueue-1.example.com:7777,MessageQueue-2.example.com:7777
BROKER_INSTANCE_NAME=msgqbroker
USER_NAME=msgquser
```

```
lbServerPort=9443
lbServerProtocol=https
lbServerHost=LoadBalancer-3.example.com
SiteID=11
```

5 Run the `amsfopassword` command.

This command generates an encrypted password, creates a new file named `.password`, and stores the encrypted password in the new file.

```
# cd /opt/SUNWam/bin

# ./amsfopassword -e m5gqu5er -f /opt/SUNWam/.password
```

To view the encrypted password:

```
# more /opt/SUNWam/.password

M27OGb6U4ufRu+oWAzBdWw==
```

6 Edit the `/opt/SUNWam/bin/amsessiondb` script.

Make a backup of the `/opt/SUNWam/bin/amsessiondb` script before making any changes to the script.

The `amsessiondb` script is called by the `amsfo` script to start the Berkeley DB client (`amsessiondb`), create the database, and set specific database values. The script contains variables that specify various default paths and directories:

```
JAVA_HOME=/usr/jdk/entsys-j2se/
IMQ_JAR_PATH=/usr/share/lib
JMS_JAR_PATH=/usr/share/lib
BDB_JAR_PATH=/usr/share
BDB_SO_PATH=/usr/lib
AM_HOME=/opt/SUNWam
```

If any of these components are not installed in their default directories, edit the `amsessiondb` script and set the variables, as needed, to the correct locations.

7 Edit the `/opt/SUNWam/bin/amsfo` script.

Make a backup of the `/opt/SUNWam/bin/amsfo` script before making any changes to the script. In the following line, add the parameter `–name $BROKER_INSTANCE_NAME` as follows:

```
$JMQEXECUTABLE -bgnd $BROKER_OPTIONS -vmargs $BROKER_VM_ARGS
           -name $BROKER_INSTANCE_NAME -port $BROKER_PORT
           -cluster $CLUSTER_LIST &
           -jmqpid=$!
           echo $_jmqpid > $JMQ_PID_FILE
```

8 Restart the Access Manager session failover components.

a. Stop the Message Queue broker instance.

```
# cd /opt/SUNWam/bin
# ./amsfo stop
```

b. Run the `netstat` command to verify that the Message Queue broker instance is stopped.

```
# netstat -an | grep 7777
```

If `netstat` returns no result, then the Message Queue broker instance is stopped.

Tip – If the Message Queue broker instance is not stopped, run the following commands:

```
# cd /tmp/amsession/logs
# cat *.pid
```

Process IDs are displayed. Example:

```
4940
    4924
```

Kill these Java processes. Example:

```
# kill -9 4940 4924
```

If you don't see the process-ids in that file, and the `netstat` is still listening on port 7777, then it's possible that the `amsfo` script did not stop properly. In this case, run the following command to identify the java processes:

```
# ps -ef | grep java
```

Then kill those identified processes as shown in the `kill` command example above.

Then check with `netstat` again. The port socket should be relinquished before you start up `amsfo` again. Otherwise, session failover problems may occur.

---

c. Restart the Message Queue broker instance.

```
# ./amsfo start
```

d. Run the `netstat` command to verify that the Message Queue port is open and listening.

```
# netstat -an | grep 7777
*.7777           *.*               0           0    49152           0    LISTEN
```

9 Run the `netstat` command to verify that the Message Queue port is open and listening.

```
# netstat -an | grep 7777
*.7777           *.*               0               0    49152        0    LISTEN
```

▼ To Identify The Session Store Components In Access Manager

Create a new secondary configuration instance for the Access Manager load balancer.

1 **Go to the Access Manager URL:**

```
https://LoadBalancer-3.example.com:9443/amserver/UI/Login
```

2 **Log in to the Access Manager console using the following information:**

Username **amadmin**

Password **4m4dmin1**

3 **Click Configuration > Global Properties > Session > Secondary Configuration Instance.**

4 **Click New, and add the following values:**

Name:	Load balancer URL. Example: `https://LoadBalancer-3.example.com:9443`
Session Store User:	**msgquser**
Session Store Password:	**m5gqu5er**
Session Store Password (Confirm):	**m5gqu5er**
Maximum Wait Time:	**5000** (This is the default value.)
Database URL:	Message Queue broker address list. Example: `MessageQueue-1.example.com:7777, MessageQueue-2.example.com:7777`

5 **Click Add, and then click Save.**

▼ To Edit the Access Manager Web Server Configuration Files

1 **Log in as a root user to the host Access Manager 1.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com/config
```

2. **Edit file** `server.xml`**.**

   Make a backup of this file, and then make the following changes:

   a. **In** `server.xml`**, locate this entry:**

      ```
      <JAVA javahome="/usr/jdk/entsys-j2se" serverclasspath=
      ```

   b. **At the end of the** `serverclasspath` **attribute, append these values:**

      ```
      /usr/share/lib/jms.jar:/usr/share/lib/imq.jar:
      ```

   c. **Save the file.**

3. **Edit the file** `sun-web.xml`**.**

   ```
   cd /opt/SUNWwbsvr/https-AccessManager-1.example.com/is-web-apps/services/WEB-INF
   ```

   a. **Make a copy of** `sun-web.xml`**.**

   b. **In the** `<cookie-properties>` **element, add the following property:**

      ```
      <property name="encodeCookies" value="false"/>
      ```

   c. **Save the file.**

4. **Log in as a root user to the host Access Manager 2.**

   ```
   # cd /opt/SUNWwbsvr/https-AccessManager-2.example.com/config
   ```

5. **Edit file** `server.xml`**.**

   Make a backup of this file, and then make the following changes:

   a. **In** `server.xml`**, locate this entry:**

      ```
      <JAVA javahome="/usr/jdk/entsys-j2se" serverclasspath=
      ```

   b. **At the end of the** `serverclasspath` **attribute, append these values:**

      ```
      /usr/share/lib/jms.jar:/usr/share/lib/imq.jar:
      ```

   c. **Save the file.**

6. **Edit the file** `sun-web.xml`**.**

   ```
   cd /opt/SUNWwbsvr/https-AccessManager-2.example.com/is-web-apps/services/WEB-INF
   ```

   a. **Make a copy of** `sun-web.xml`**.**

b. In the `<cookie-properties>` element, add the following property:

```
<property name="encodeCookies" value="false"/>
```

c. Save the file.

7 Restart Access Manager 1 and Access Manager 2.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1
# ./stop; ./start
# cd /opt/SUNWwbsvr/https-AccessManager-2
# ./stop; ./start
```

▼ To Verify that Session Failover Works Properly

Before You Begin Both Access Manager 1 and Access Manager 2 should be up and running before you begin this verification procedure.

1 Stop Access Manager 1.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1
# ./stop
```

2 Open a browser (Browser 1) and go to the following Access Manager load balancer URL:

```
https://LoadBalancer-3.example.com:9443/amserver/UI/Login?realm=users
```

3 Log in to the Access Manager console using the following information:

Username **`testuser1`**

Password **`password`**

The Edit User page for `testuser1` is displayed.

This indicates that although Access Manager 1 was stopped (see step 1), the Access Manager load balancer (LoadBalancer-3) directed your login request to Access Manager 2, and the session for `testuser1` was successfully created in Access Manager 2.

Leave Browser 1 open.

4 On the host AccessManager–1, at the command line, start Access Manager 1.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1
# ./start
```

Both Access Manager 1 and Access Manager 2 are now up and running.

5 **Open a second browser (Browser 2) and go to the following Access Manager URL:**

```
http://accessmanager-1.example.com:1080/amserver/UI/Login
```

6 **Log in to the Access Manager console using the following information:**

Username **amadmin**

Password **4m4dmin1**

7 **On the Realms page, click the Sessions tab.**

a. **In the View: field, select** `Access Manager-2.example.com:1080`**.**
Verify that only one User Id, named `testuser1`, exists in the Sessions list.

b. **In the View: field, select** `Access Manager-1.example.com:1080`
Verify that only one User Id, named `amAdmin`, exists in the Sessions list.

Leave Browser 2 open.

8 **Stop Access Manager 2.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-2
# ./stop
```

Access Manager 1 is still up and running, and Access Manager 2 is now stopped.

9 **In Browser 1, in the Edit User page for** `testuser1`**, modify the user profile.**

In the Full Name field, enter **`NewTestUser1`**, and then click Save.

The message "Profile was updated" is displayed.

10 **In Browser 2, in the Realms page, click the Sessions tab.**

In the View: list, select `AccessManager-1.example.com:1080`.

Verify that now two UserIds, named `amAdmin` and `testuser1`, exist in the Sessions list. This indicates that the session successfully failed over to Access Manager 1.

Close Browser 2.

11 **Start Access Manager 2.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-2
# ./start
```

Both Access Manager 1 and Access Manager 2 are now up and running.

12 Stop Access Manager 1.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1
# ./stop
```

Access Manager now down, and Access Manager 2 is still up and running.

13 In a new browser (Browser 3), go to the following Access Manager URL:

```
http://accessmanager-2.example.com:1080/amserver/UI/Login
```

14 Log in to the Access Manager console using the following information:

Username **amadmin**

Password **4m4dmin1**

Leave the browser open.

a. On the Realms page, click the Sessions tab.

b. In the View field, select `AccessManager-2.example.com:1080`**.**

c. Click the Search button.

Under Sessions, only one UserID named `amAdmin` exists in the Session list.

Leave the Browser 3 open.

15 In Browser 1, in the Edit User page for `testuser1`**, modify the user profile.**

In the Full Name field, change `NewTestUser1` back to `TestUser1`, and then click Save.

The message "Profile is updated" is displayed.

16 In Browser 3, on the Sessions tab, click Search to refresh the page.

Under Sessions, two UserIDs, named `amAdmin` and `testuser1` , are now displayed in the Sessions list. This indicates that the session successfully failed back to Access Manager 2.

PART III

Reference: Summaries of Server and Component Configurations

◆ ◆ ◆ APPENDIX A

Directory Servers

TABLE A–1 Directory Server 1 Configuration

Component	Description	
Host	Computer system that hosts the Directory Server.	
	Host Name	DirectoryServer–1.example.com
Directory Server Administration Instance	Administration server that manages Directory Server and all its instances.	
	Port Number	1391
	Service URL	http://DirectoryServer–1.example.com:1391
	Instance Directory	/var/opt/mps/serverroot/admin-serv
Directory Server Configuration Instance	Instance that stores Directory Server configuration data.	
	Instance name	ds-config
	Port Number	1390
	Service URL	http://DirectoryServer-1.example.com:1390
	Base suffix	dc=example,dc=com
	Super User	cn=Directory Manager
	Super User password	d1rm4n4ger
	Administrative User	admin
	Administrative User Password	d1r4dmin
	Instance Directory	/var/opt/mps/serverroot/slapd-ds-config

TABLE A–1 Directory Server 1 Configuration *(Continued)*

Component	Description	
Access Manager Configuration Instance	Stores Access Manager configuration data.	
	Instance name	am-config
	Port Number	1389
	Service URL	
	Base Suffix	o=example.com
	Replication Manager	cn=replication manager,cn=replication,cn=config
	Replication Manager Password	replm4n4ger
	Instance Directory	/var/opt/mps/serverroot/slapd-am-config
User Data Store	Stores Access Manager user data. In this deployment example, the user data store is located on the same computer system as the Access Manager configuration data store. The user data store could also be installed on a different computer system.	
	Instance Name	am-users
	Port Number	1489
	Service URL	http://DirectoryServer-1.example.com:1489
	Base Suffix	dc=company, dc=com
	Users Suffix	ou=users,dc=company,dc=com
	Replication Manager	cn=replication manager, cn=replication,cn=config
	Replication Manager Password	replm4n4ger
	Instance Directory	/var/opt/mps/serverroot/slapd-am-users

TABLE A–2 Directory Server 2 Configuration

Component	Description	
Host	Computer system that hosts the Directory Server.	
	Host Name	DirectoryServer–2.example.com
Directory Server Administration Instance	Administration server that manages Directory Server and all its instances.	
	Port Number	1391
	Service URL	http://DirectoryServer–2.example.com:1391
	Instance Directory	/var/opt/mps/serverroot/admin-serv
Directory Server Configuration Instance	Instance that stores Directory Server configuration data.	
	Instance name	ds-config
	Port Number	1390
	Service URL	http://DirectoryServer-2.example.com:1390
	Base suffix	dc=example,dc=com
	Super User	cn=Directory Manager
	Super User password	d1rm4n4ger
	Administrative User	admin
	Administrative User Password	d1r4dmin
	Instance Directory	/var/opt/mps/serverroot/slapd-ds-config
Access Manager Configuration Instance	Stores Access Manager configuration data.	
	Instance name	am-config
	Port Number	1389
	Service URL	
	Base Suffix	o=example.com
	Replication Manager	cn=replication manager,cn=replication,cn=config
	Replication Manager Password	replm4n4ger
	Instance Directory	/var/opt/mps/serverroot/slapd-am-config

TABLE A–2 Directory Server 2 Configuration *(Continued)*

Component	Description	
User Data Store	Stores Access Manager user data. In this deployment example, the user data store is located on the same computer system as the Access Manager configuration data store. The user data store could also be installed on a different computer system.	
	Instance Name	am-users
	Port Number	1489
	Service URL	http://DirectoryServer-2.example.com:1489
	Base Suffix	dc=company, dc=com
	Users Suffix	ou=users,dc=company,dc=com
	Replication Manager	cn=replication manager, cn=replication,cn=config
	Replication Manager Password	replm4n4ger
	Instance Directory	/var/opt/mps/serverroot/slapd-am-users

TABLE A–3 User Data Store Accounts

UserID	Description	
userdbadmin	Used by the Access Manager servers to connect to the user data store for data management purposes.	
	Password	4serd84dmin
	DN	uid=userdbadmin,ou=users,dc=company,dc=com
userdbauthadmin	Used by the Access Manager servers to authenticate users to the user data store.	
	Password	4serd84uth4dmin
	DN	uid=userdbauthadmin,ou=users,dc=company,dc=com
testuser1	Used to verify that the policy agents work properly.	
	Password	password
	DN	uid=testuser1,ou=users,dc=company,dc=com
testuser2	Used to verify that the policy agents work properly.	
	Password	password
	DN	uid=testuser2,ou=users,dc=company,dc=com

◆ ◆ ◆ APPENDIX B

Access Manager Servers

TABLE B–1 Access Manager 1 Configuration

Component	Description	
Host	Computer system that hosts the Access Manager server.	
	Host Name	AccessManager-1.example.com
Web Server Administration	Manages the entire Web Server an all its instances.	
	Instance name	admserv
	Port Number	8888
	Service URL	http://AccessManager–1.example.com:8888
	Administrative User	admin
	Administrative User Password	web4dmin
	Instance Directory	/opt/SUNWwbsvr/https-admserv
Access Manager Web Server	Contains the Access Manager applications	
	Instance name	AccessManager-1.example.com
	Port Number	1080
	Service URL	http://AccessManager-1.example.com:1080
	Administrative User	amadmin
	Administrative User Password	4m4dmin1
	amLDAP user	amldapuser

TABLE B–1 Access Manager 1 Configuration *(Continued)*

Component	Description	
	amLDAP user Password	4mld4puser
	Instance Directory	/opt/SUNWwbsvr/https-AccessManager-1.example.com

TABLE B–2 Access Manager 2 Configuration

Component	Description	
Host	Computer system that hosts the Access Manager server.	
	Host Name	AccessManager-2.example.com
Web Server Administration	Manages the entire Web Server an all its instances.	
	Instance name	admserv
	Port Number	8888
	Service URL	http://AccessManager–2.example.com:8888
	Administrative User	admin
	Administrative User Password	web4dmin
	Instance Directory	/opt/SUNWwbsvr/https-admserv
Access Manager Web Server	Contains the Access Manager applications	
	Instance name	AccessManager-2.example.com
	Port Number	1080
	Service URL	http://AccessManager-2.example.com:1080
	Administrative User	amadmin
	Administrative User Password	4m4dmin1
	amLDAP user	amldapuser
	amLDAP user Password	4mld4puser
	Instance Directory	/opt/SUNWwbsvr/https-AccessManager-1.example.com

◆ ◆ ◆ APPENDIX C

Distributed Authentication UI Servers

TABLE C–1 Distributed Authentication UI 1 Configuration

Component	Description	
Host	Computer system that hosts the Access Manager server.	
	Host Name	AuthenticationUI-1.example.com
Web Server Administration	Manages the entire Web Server an all its instances.	
	Instance name	admserv
	Port Number	8888
	Service URL	http://AuthenticationUI-1..example.com:8888
	Administrative User	admin
	Administrative User Password	web4dmin
	Instance Directory	/opt/SUNWwbsvr/https-admserv
Distributed Authentication UI Server	Contains the Distributed Authentication UI module.	
	Instance name	AuthenticationUI-1.example.com
	Port Number	1080
	Service URL	http://AuthenticaitonUI-1.example.com:1080
	Instance Directory	/opt/SUNWwbsvr/https-AuthenticationUI-1.example.com
User Profile	Administrative User	authuiadmin
	Administrative User Password	4uthu14dmin

TABLE C–2 Distributed Authentication UI 2 Configuration

Component	Description	
Host	Computer system that hosts the Access Manager server.	
	Host Name	AuthenticationUI-2.example.com
Web Server Administration	Manages the entire Web Server an all its instances.	
	Instance name	admserv
	Port Number	8888
	Service URL	http://AuthenticationUI-2..example.com:8888
	Administrative User	admin
	Administrative User Password	web4dmin
	Instance Directory	/opt/SUNWwbsvr/https-admserv
Distributed Authentication UI Server	Contains the Distributed Authentication UI module.	
	Instance name	AuthenticationUI-2.example.com
	Port Number	1080
	Service URL	http://AuthenticaitonUI-2.example.com:1080
	Instance Directory	/opt/SUNWwbsvr/https-AuthenticationUI-2.example.com
User Profile	Administrative User	authuiadmin
	Administrative User Password	4uthu14dmin

◆ ◆ ◆ APPENDIX D

Sun Java System Web Servers and Web Policy Agents

TABLE D–1 Protected Resource 1 Web Server and Web Policy Agent 1 Configurations

Component	Description	
Host	Computer system that hosts Web Server 1	
	Host Name	ProtectedResource-1.example.com
Web Server Administration Server	Manages the entire Web Server and all its instancces.	
	Instance Name	admserv
	Port Number	8888
	Administrative User	admin
	Administrative User Password	web4dmin
	Instance Directory	/opt/SUNWwbsvr/https-admserv
Web Policy Agent Instance	Server instance that contains the web server and web policy agent.	
	Instance Name	ProtectedResource-1.example.com
	Port Number	1080
	Instance Directory	/opt/SUNWwbsvr/https-ProtectedResource-1.example.com
Web Agent Profile		
	Administrative User	webagent-1
	Administrative User Password	web4gent1

TABLE D–2 Protected Resource 2 Web Server and Web Policy Agent 2 Configurations

Component	Description	
Host	Computer system that hosts Web Server 2	
	Host Name	ProtectedResource-2.example.com
Web Server Administration Server	Manages the entire Web Server and all its instances.	
	Instance Name	admserv
	Port Number	8888
	Administrative User	admin
	Administrative User Password	web4dmin
	Instance Directory	/opt/SUNWwbsvr/https-admserv
Web Policy Agent Instance	Server instance which contains the web server and web policy agent.	
	Instance Name	ProtectedResource-2.example.com
	Port Number	1080
	Instance Directory	/opt/SUNWwbsvr/https-ProtectedResource-2.example.com
Web Agent Profile		
	Administrative User	admin
	Administrative User Password	web4dmin

◆ ◆ ◆ APPENDIX E

WebLogic Application Servers and J2EE Policy Agents

TABLE E–1 Protected Resource 1 Application Server and J2EE Policy Agent 1 Configurations

Component	Description	
Host	Computer system that hosts Application Server 1	
	Host Name	ProtectedResource-1.example.com
WebLogic Administration Server	Manages the entire Application Server and all its instances	
	Instance Name	AdminServer
	Port Number	7001
	Administrative User	weblogic
	Administrative User Password	w3bl0g1c
	Instance Directory	/usr/local/bea/user_projects/domains/ProtectedResource-1/servers/AdminServer
WebLogic Domain	Stores configuration information for this Application Server instance.	
	Instance Name	ProtectedResource-1
	Instance Directory	/usr/local/bea/user_projects/domains/ProtectedResource-1
J2EE Policy Agent Instance	Server instance which contains the Application Server and J2EE policy agent.	
	Instance Name	ApplicationServer-1
	Port Number	1081
	Instance Directory	/usr/local/bea/user_projects/domains/ProtectedResource-1/servers/ApplicationServer-1
J2EE Policy Agent Profile		

TABLE E–1 Protected Resource 1 Application Server and J2EE Policy Agent 1 Configurations *(Continued)*

Component	Description	
	Administrative User	j2eeagent-1
	Administrative User Password	j2ee4gent1

TABLE E–2 Protected Resource 2 Application Server and J2EE Policy Agent 2 Configurations

Component	Description	
Host	Computer system that hosts Application Server 2	
	Host Name	ProtectedResource-2.example.com
WebLogic Administration Server	Manages the entire Application Server an all its instances.	
	Instance Name	AdminServer
	Port Number	7001
	Administrative User	weblogic
	Administrative User Password	w3bl0g1c
	Instance Directory	/usr/local/bea/user_projects/domains/ProtectedResource-2/servers/AdminServer
WebLogic Domain	Stores configuration information for this Application Server instance.	
	Instance Name	ProtectedResource-2
	Instance Directory	/usr/local/bea/user_projects/domains/ProtectedResource-2
J2EE Policy Agent Instance	Server instances which contains the Application Server and J2EE web policy agent.	
	Instance Name	ApplicationServer-2
	Port Number	1081
	Instance Directory	/usr/local/bea/user_projects/domains/ProtectedResource-2/servers/ApplicationServer-2
J2EE Policy Agent Profile		
	Administrative User	j2eeagent-2
	Administrative User Password	j2ee4gent2

◆ ◆ ◆ APPENDIX F

Load Balancers

TABLE F–1 Load Balancer Configurations

Component	Description	
Host	Computer system that hosts all virtual servers in this deployment example.	
	Host Name	is-f5.example.com
Load Balancer 1	Virtual Service Address for the Access Manager configuration store.	
Access Manager Configuration Stores	Configured for cookie and IP-based stickiness and TCP (HTTP and LDAP) load balancing.	
	Instance Name	LoadBalancer-1
	Port Number	389
	Pool Name	AccessManager-Pool
	Virtual Server and Port Number	LoadBalancer-1.example.com:389
	Monitor	ldap-tcp
Load Balancer 2	Virtual Service Address for the User Data store.	
Directory Server User Data Stores		
	Instance Name	LoadBalancer-2
	Port Number	489
	Pool Name	DirectoryServer-UserData-Pool
	Virtual Server and Port Number	LoadBalancer-2.example.com:489
	Monitor	ldap-tcp

TABLE F–1 Load Balancer Configurations *(Continued)*

Component	Description	
Load Balancer 3	Virtual Service Address for the Access Manager Web Server instances.	
Access Manager Servers	SSL is terminated at this at this load balancer before the request is forwarded to the Access Manager Servers. This load-balancer is the single point-of-failure for Access Manager and can be considered a limitation of this deployment example.	
	Configured for cookie and IP— based stickiness and TCP (HTTP and LDAP) load balancing.	
	External users access port 9443, while internal users will access port 90.	
	Instance Name	LoadBalancer-3
	Port Number	90 and 9443
	Pool Name	AccessManager-Pool
	Virtual Server and Port Number	LoadBalancer-3.example.com:90
	Monitor	AccessManager-http
Load Balancer 4	Virtual Service Address for the Distributed Authentication UI web server instances.	
Distributed Authentication UI Servers	SSL is terminated at this load balancer before the request is forwarded to the Distributed Authentication UI servers.	
	Configured for cookie and IP-based stickiness and TCP (HTTP and LDAP) load balancing.	
	Instance Name	LoadBalancer-4
	Port Number	90 and 9443
	Pool Name	AuthenticationUI-Pool
	Virtual Server and Port Number	LoadBalancer-4.example.com:90
	Monitor	http-monitor
Load Balancer 5	Virtual Service Address for Web Policy Agents.	
Web Policy Agents	Configured for cookie and IP— based stickiness and TCP (HTTP and LDAP) load balancing.	
	Instance Name	LoadBalancer-5
	Port Number	90
	Pool Name	WebAgent-Pool

TABLE F–1 Load Balancer Configurations *(Continued)*

Component	Description	
	Virtual Server and Port Number	LoadBalancer-5.example.com:90
	Monitor	WebAgent-http
Load Balancer 6	Virtual Service Address for J2EE Policy Agents	
J2EE Policy Agents	Configured for cookie and IP-based stickiness and TCP (HTTP and LDAP) load balancing.	
	Instance Name	LoadBalancer-6
	Port Number	91
	Pool Name	J2EEAgent-Pool
	Virtual Server and Port Number	LoadBalancer-6.example.com:91
	Monitor	tcp

◆ ◆ ◆ APPENDIX G

Message Queue Servers

TABLE G–1 Message Queue 1 Configuration

Component	Description	
Host	Computer system that hosts the Message Queue server.	
	Host Name	MessageQueue-1.example.com
Message Queue 1	Serves as a communications broker that enables Access Manager to communicate data with the session store.	
	Instance Name	msgqbroker
	Port Number	7777
	Administrative User	msgquser
	Administrative User Password	m5gqu5er
	Instance Directory	/opt/SUNWam

TABLE G–2 Message Queue 2 Configuration

Component	Description	
Host	Computer system that hosts the Message Queue server.	
	Host Name	MessageQueue-2.example.com
Message Queue 2	Serves as a communications broker that enables Access Manager to communicate data with the session store.	
	Instance Name	msgqbroker
	Port Number	7777
	Administrative User	msgquser

TABLE G–2 Message Queue 2 Configuration *(Continued)*

Component	Description	
	Administrative User Password	m5gqu5er
	Instance Directory	/opt/SUNWam

◆ ◆ ◆ APPENDIX H

Known Issues and Limitations

The information in this appendix will be updated as more information becomes available.

TABLE H–1 Known Issues and Limitations

Reference Number	Description
6490164	**Installing Access Manager with upper case results in "No Such Orrganization" error.** If you install Access Manager with the server host name and domain name in mixed-case letters, you may not be able to access the Access Manager console. A "No Such Organization" or "No Such Domain" message is displayed. **Workaround:** Log in to the Access Manager console using the fully-qualified DN of the amadmin such as`uid=amAdmin,ou=People,o=example.com`, then add you fully-qualified server name in all-lowercase letters to the Realm/DNS Alias list of the top-level realm. Click the top-level realm to see the realm properties, and you will see the list of Realm/DNS Aliases.

6477741	**Exception is thrown when you run the agentadmin utility.**
	The following exception is thrown when you run the agentadmin utility from the J2EE Policy Agent2.2 server (Hotpatch 3 for BEA Appserver 9.1).
	`# ./agentadmin --getUuid amadmin user example.com`
	`Failed to create debug directory`
	`Failed to create debug directory`
	`Failed to create debug directory`
	`Failed to create debug directory`
	`Failed to create debug directory`

TABLE H–1 Known Issues and Limitations *(Continued)*

Reference Number	Description
6476271	**BEA servers do not start up when startup script is not configured properly.** The BEA administration server and managed server will not start up if the start up script is not configured properly. When using J2EE Policy Agent 2.2 (Hotpatch-3) on BEA Application Server 9.1, you must append the following to the end of the file `setDomainEnv.sh` file: `. /usr/local/bea/user_projects/domains/mydomain/setAgentEnv_server1.sh` The `setDomainEnv.sh` file contains the call to `commEnv.sh`.
6472662	**When SSL terminates at the Access Manager load balancer, the console application changes protocol from HTTPS to HTTP.** When you try to access the Access Manager load balancer with a URL such as `https://`*loadbalancerURL:port*`/amserver/console`, you cannot access log in page because the console application changes the protocol from HTTPS to HTTP. **Workaround:**When you access the Access Manager load balancer, manually modify the URL to the following: `https://`*loadbalancerURL:port*`/amserver/UI/Login`.
6482952	**J2EE policy agent redirects to the context root in the goto URL .** The problem occurs when testing the sample application for the J2EE Policy Agent 2.2 for BEA Weblogic 9.1 Application Server. If you access a URL such as `http://`*agentLoadBalancerURL*`:`*port*`/agentsample/protectedservlet`, you are redirected to the Access Manager login page, but the `goto` part of the URL contains only this: `=http%3A%2F%2FagentLoadBalancerURL%3Aport%2Fagentsample`. The result is that after successful authentication, you are redirected to the index page of the application, and not the page that you had requested. **Workaround:** There is no workaround at this time.
6363157	**Performance is impacted due to unnecessary persistent searches.** The problem can occur, for example, when Access Manager uses LDAP roles. Persistent search is not necessary in this case, and one should be able to disable persistent searches without introducing additional risks to the system. **Workaround:** There is no workaround at this time.

TABLE H–1 Known Issues and Limitations *(Continued)*

Reference Number	Description
6489403	**Login to a sub-realm fails when using the Distributed Authentication UI.** The problem occurs when you attempt to access a sub-realm using a URL such as the following: `http://`*AuthenticationUIserver*`:1080/distAuth/UI/Login?realm=users&goto=http://`*hostName.domainName.com*`:1080` Instead of a login page, the following message is displayed: "No such Organization found." **Workaround:** There is no workaround at this time.

6467562	**Filtered role name missing ou=service in the container JAAS Subject.**
	
	When trying to use declarative security with J2EE agents, for any user in a sub-realm the role membership is not populated properly within the container JAAS Subject. It is missing `ou=services` in the `jaas_subject` role names. There is a mismatch between the role name returned from the Access Manager server and what is seen in the JAAS Subject.
	
	Workaround: In the `AMAgent.properties` file, remove the `ou=services` part in the mapping key `com.sun.identity.agents.config.privileged.attribute.mapping` . For example, change this:
	
	`com.sun.identity.agents.config.privileged.attribute.mapping [id\=manager,ou\=role,o\=users,ou\=services,o\=example.com] = am_manager_role`
	
	to
	
	`com.sun.identity.agents.config.privileged.attribute.mapping [id\=manager,ou\=role,o\=users,o\=example.com] = am_manager_role`