BEA AquaLogic® User Interaction

Networking and Authentication Guide

Document Revised: December 19 2007

Contents

1. Welcome

2. Network Security

3. Authentication and SSO

4. Load Balancing

Welcome

This book describes networking concepts and configurations pertaining to an AquaLogic User Interaction deployment

For an overview of all deployment documentation, see the *AquaLogic User Interaction Deployment Overview*.

For products and versions covered by this book, see the section Products Covered by the Deployment Guide in the *AquaLogic User Interaction Deployment Overview* book.

How to Use This Book

Audience

This guide is written to provide guidance to people responsible for the design and deployment of the AquaLogic User Interaction system. Access to resources with strong knowledge of the platform operating system, database, web and application servers, and any other third-party software is recommended.

Organization

This guide includes the following chapters:

- This chapter provides information on how to use this guide and describes general resources available to assist in the AquaLogic User Interaction deployment.

- Chapter 2, "Network Security," provides an overview of network security options for the AquaLogic User Interaction deployment, including the AquaLogic User Interaction security architecture and using SSL.
- Chapter 3, "Authentication and SSO," describes authentication and SSO options for the AquaLogic User Interaction deployment, including third-party SSO providers, remote authentication, and credential brokering.
- Chapter 4, "Load Balancing," provides and overview of load balancing and redundancy with the AquaLogic User Interaction deployment.

Typographical Conventions

This book uses the following typographical conventions.

Table 1-1 Typographical Conventions

Convention	Typeface	Examples/Notes
• File names • Folder names • Screen elements	**bold**	• Upload **Procedures.doc** to the portal. • The log files are stored in the **logs** folder. • To save your changes, click **Apply Changes**.
• Text you enter	`computer`	Type `Marketing` as the name of your community.
• Variables you enter	`computer with angle brackets (<>)`	Enter the base URL for the Remote Server. For example, `http://<my_computer>/`.
• New terms • Emphasis • Object example names	*italic*	• *Portlets* are Web tools embedded in your portal. • The URI *must* be a unique number. • The example Knowledge Directory displayed in Figure 5 shows the *Human Resources* folder.

BEA Documentation and Resources

This section describes other documentation and resources provided by BEA.

Table 1-2 BEA Documentation and Resources

Resource	Description
Installation and Upgrade Guides	These guides describe the prerequisites (such as required software) and procedures for installing or upgrading the various AquaLogic User Interaction products. These guides are available under the appropriate product sections on edocs.bea.com.
Administrator Guides	These guides describe how to manage and maintain the various AquaLogic User Interaction products. These guides are available under the appropriate product sections on edocs.bea.com.
Release Notes	The release notes provide information about new features, issues addressed, and known issues in the release of various AquaLogic User Interaction products. They are available on edocs.bea.com.
Online Help	The online help is written for all levels of AquaLogic User Interaction users. It describes the user interface for AquaLogic User Interaction components and gives detailed instructions for completing tasks in AquaLogic User Interaction products. To access online help, click the help icon.
Developer Guides, Articles, API Documentation, Blogs, Newsgroups, and Sample Code	These resources are provided for developers on the BEA dev2dev site (dev2dev.bea.com). They describe how to build custom applications using AquaLogic User Interaction and how to customize AquaLogic User Interaction products and features.

Table 1-2 BEA Documentation and Resources

Resource	Description
AquaLogic User Interaction Support Center	The AquaLogic User Interaction Support Center is a comprehensive repository for technical information on AquaLogic User Interaction products. From the Support Center, you can access products and documentation, search knowledge base articles, read the latest news and information, participate in a support community, get training, and find tools to meet most of your AquaLogic User Interaction-related needs. The Support Center encompasses the following communities: **Technical Support Center** Submit and track support incidents and feature requests, search the knowledge base, access documentation, and download service packs and hotfixes. **User Group** Visit the User Group section to collaborate with peers and view upcoming meetings. **Product Center** Download products, read release notes, access recent product documentation, and view interoperability information. **Developer Center** Download developer tools and documentation, get help with your development project, and interact with other developers via BEA's dev2dev newsgroups. **Education Services** Find information about available training courses, purchase training credits, and register for upcoming classes. If you do not see the Support Center when you log in to http://support.plumtree.com, contact ALUIsupport@bea.com for the appropriate access privileges.

Table 1-2 BEA Documentation and Resources

Resource	Description
Technical Support	If you cannot resolve an issue using the above resources, BEA Technical Support is happy to assist. Our staff is available 24 hours a day, 7 days a week to handle all your technical support needs. E-mail: ALUIsupport@bea.com Phone Numbers: U.S.A. +1 866.262.PLUM (7586) or +1 415.263.1696 Europe +44 1494 559127 Australia/NZ +61 2.9923.4030 Korea +82 27676 888 Singapore +1 800.1811.202

Network Security

This chapter provides an overview of security options for an AquaLogic User Interaction deployment.

The purpose of this chapter is assist in developing a security plan and should not be considered a replacement for the services of qualified security professionals. BEA does not not advocate the use of any specific security configuration. BEA does provide professional consulting services to assist in securing an AquaLogic User Interaction deployment. To engage BEA professional services, contact your BEA representative.

This chapter discusses the following topics:

- "Security Architecture" on page 2-1 provides an overview of the AquaLogic User Interaction component security architecture, including intra-component communication, firewalls, and the DMZ.
- "SSL" on page 2-4 provides an overview of SSL in the AquaLogic User Interaction deployment, including how and where CA certificates should be imported into the various AquaLogic User Interaction services.

Security Architecture

This section describes AquaLogic User Interaction component architecture from a network security perspective. This includes how various components communicate with each other and which components need to be exposed to the end consumer.

Component Communication

With the exception of the database and Search, all requests from the AquaLogic Interaction portal component are made using HTTP 1.1. This provides the following security advantages:

- There are third party tools to help monitor and audit HTTP 1.1 traffic.
- Each component web service uses a single, configurable port number, which eases firewall configuration.
- The AquaLogic Interaction portal component implements the full range of HTTP security, including SSL/TLS certificates and basic authentication.
- Single Sign-On (SSO) third party products that are designed to protect HTTP traffic can be used to protect web services residing in the internal network. For details on SSO and AquaLogic Interaction, see Chapter 3, “Authentication and SSO.”

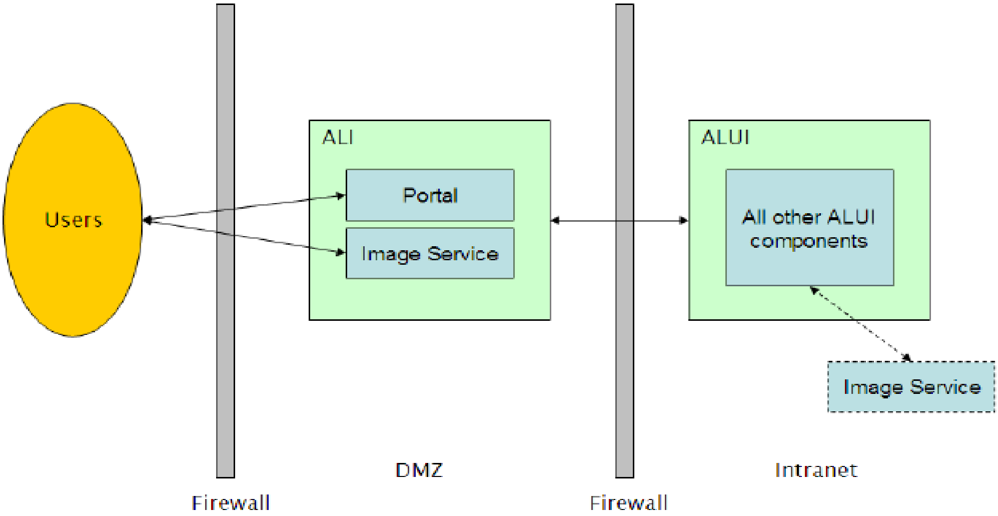
Communication between the ALUI components can be further secured by:

- Using a separate network or subnet for the ALUI components and the DB.
- Using technologies such as IPSec, VPN, or SSL.

AquaLogic User Interaction and the DMZ

A basic security architecture that limits external exposure to AquaLogic User Interaction products and other backend systems is illustrated in Figure 2-1.

Figure 2-1 Basic Security Architecture



In this configuration, only the AquaLogic Interaction Portal component and Image Service are placed within the DMZ. The AquaLogic Interaction Portal component and Image Service should be the only AquaLogic Interaction components installed in the DMZ. When the Portal is separate from other AquaLogic Interaction components, persistent data in the search and database components and backend tasks in the automation service are isolated from the external network.

The Portal gateways requests to all other AquaLogic User Interaction components and backend services, communicating with HTTP 1.1 across the firewall and into the internal network. The server housing the AquaLogic Interaction Portal should be hardened by a security professional, as it receives direct user requests. All communication should be SSL-encrypted.

To avoid traffic across the firewall between non-portal AquaLogic User Interaction components and the Image Service, another Image Service can be placed within the internal network.

Note: This is one potential network topology. For topologies involving software and hardware loadbalancing, see Chapter 4, “Load Balancing.”

SSL

Configuring AquaLogic User Interaction to use SSL is a relatively complex procedure that requires knowledge of SSL and CA certificates. This section provides an overview of the procedure. For more details, see the Administrator Guide for AquaLogic Interaction.

In the general case, the AquaLogic Interaction portal Image Service would be secured with SSL, while another, unsecured Image Service would reside in the internal network for other AquaLogic User Interaction components. In this case the AquaLogic User Interaction Activity Services would use the unsecured Image Service and would only need to be configured for SSL communication with the Portal.

The following sections explain how to configure the various AquaLogic User Interaction components for SSL:

1. "Security Modes" on page 2-5
2. "Configuring AquaLogic Interaction for SSL" on page 2-6
3. "Importing CA Certificates" on page 2-7
4. "Configuring Activity Services to Use a Secure Portal or Image Service" on page 2-8

Security Modes

After AquaLogic Interaction components are installed, the security mode for the portal can be set. The security mode specifies how SSL is incorporated into your AquaLogic User Interaction deployment. Security mode options are described in the following table:

Security Mode	Description
0	Portal pages remain in whatever security mode—http or https—that the user initially uses to access the portal. For example, if a user accesses the portal via http, all the portal pages will remain http; if a user accesses the portal via https, all the portal pages will remain https. This is the default setting. **Note:** This mode is not recommended for production deployments or deployments that are exposed to the external network.
1	Certain portal pages are always secured via SSL and other pages are not. For example, the login page might always be secured but a directory browsing page might not. The page types that are secured are configurable. **Note:** This mode is not generally recommended.
2	All portal pages are always secured via SSL. Use this mode if there is no SSL accelerator. In this mode, the Web server should provide an SSL endpoint. **Note:** Configuring the SSL endpoint directly on a Tomcat application server is not recommended. A Web server should be used in front of the application server, and the SSL certificate should be installed on the Web server.
3	The portal uses an SSL accelerator. This is the most common configuration for production deployments. As with Security Mode 2, users are not connecting to the application server directly, so the front-end application server and the channel between the accelerator and the application sever must be secured.

For detailed information on configuring these settings, see the Administrator Guide for AquaLogic Interaction.

Configuring AquaLogic Interaction for SSL

Use the following steps to configure AquaLogic Interaction for SSL:

1. Configure SSL on Web servers or SSL accelerators that front-end the AquaLogic Interaction Portal and Image Service components. Refer to your Web server or SSL accelerator documentation for instructions on configuring SSL and creating, signing, and installing an SSL certificate.

2. Configure the Portal component:

   a. **<PT_HOME>/settings/config/portalconfig.xml**.

   b. Ensure that **HTTPSecurePort** and **HTTPPort** are set to the ports you want to use.

   c. Change **ApplicationURL0** from * to

      http://host_name:port/portal/server.pt

      Note: The port number is not necessary for .NET deployments.

   d. Change **SecureApplicationURL0** from * to

      https://host_name:port/portal/server.pt

      Note: The port number is not necessary for .NET deployments.

   e. If multiple URL mappings are configured, ensure that these entries are updated as in **c** and **d**. Refer to the comments in the configuration file for more information on URL mapping.

   f. Change **SecurityMode** from 0 to 1, 2, or 3.

   g. Change **ImageServerSecureBaseURL** from http to https. Ensure that the Image Service port is correct.

3. If the Image Service is secured with SSL, set **ImageServerConnectionURL** to the secure URL. The CA certificate used by the Image Service must be imported into the Portal application server. For details, see "Importing CA Certificates" on page 2-7.

   If any portlets or remote servers use JSControls or Adaptive Portlets, the image service CA certificate must be imported into their runtimes as well. The JSControls libraries are embedded in server and IDK products, but are identified by XML stored on the Image Service.

4. If any remote server — including portlet servers, authentication sources, profile sources, or content services — is secured with SSL, import the remote server CA certificate into the Portal application server. For details, see "Importing CA Certificates" on page 2-7.

5. Configure Collaboration, Publisher, Studio, and Workflow to use the SSL-secured Portal and Image Service. For details, see "Configuring Activity Services to Use a Secure Portal or Image Service" on page 2-8.

Importing CA Certificates

For each application server that makes requests to an SSL-secured service, the CA certificate from the secured service must be imported. The following two sections detail the process for importing CA certificates into a Java Application Server or IIS and .NET.

Importing CA Certificates Into a Java Application Server or Standalone AquaLogic User Interaction Product

For Java application servers the CA certificate is imported into the cacerts keystore.

To import the CA certificate:

1. On the computer that makes requests to an SSL secured service, open a command prompt.
2. Copy the CA certificate to this computer.

   Note: The CA certificate is in the CA of the secured service. Save the .der encoded certificate as a .cer file.

3. Import the certificate using **keytool**. For example:

   keytool -v -import -trustcacerts -alias CA_alias -file CA_certificate_path -keystore CA_keystore_path

   where

   – *CA_alias* is the alias for the CA. For example, *verisign* or the server hostname.

   – *CA_certificate_path* is the path and filename of the .cer file to be imported.

   – *CA_keystore_path* is the path to the cacerts keystore. The cacerts keystore is typically located under the home of the JVM being run by the application server, **<JVM_home>/lib/security/cacerts**.

4. When prompted, enter the password for the cacerts keystore. The default password is *changeme*.

Importing CA Certificates into IIS and .NET

For IIS and .NET, the CA certificate is imported into the MMC.

1. On the computer that makes requests to an SSL secured service, open a command prompt.
2. Copy the CA certificate to this computer.

   Note: The CA certificate is in the CA of the secured service. Save the .der encoded certificate as a .cer file.
3. Run MMC from the command line,

   > *mmc*
4. Click **Console | Add/Remove Snap-in**.
5. Click **Add**.
6. Click **Certificates**.
7. Click **Computer Account** and then click **Next**.
8. Click **local computer** and then click **Finish**.
9. Close the Add Standalone Snap-in dialog box.
10. Close the Add/Remove Snap-in dialog box by clicking **OK**.
11. In the MMC tree, expand to **Console Root | Certificates | Trusted Root Certificate Authorities | Certificates**.
12. Right click **Certificates** and select **All Tasks | Import**. Click **Next**.
13. Select the CA certificate to import. Click **Next**.
14. Choose to place all certificates in the **Trusted Root Certification Authorties** store.
15. Click **Next** and then click **Finish**.
16. Restart IIS.

Configuring Activity Services to Use a Secure Portal or Image Service

This section describes how to configure Collaboration, Publisher, Studio, and Workflow to use a secure Portal or Image Service.

Configuring Collaboration to Use a Secure Portal or Image Service

Collaboration does not require any changes to function in security modes 1 or 2, as it uses the Portal's Image Service settings. A certificate is not required.

If you are using Security Mode 3, import the certificate of the CA that signed the Image Service and/or Portal certificate into Collaboration. For details, see "Importing CA Certificates" on page 2-7.

However, if the host/port of the normal Image Service URL used by browsing users is not accessible from Collaboration (for example, the Image Service is on a different machine than Collaboration), you must change the jscontrols component that Collaboration uses. This problem generates error messages that are displayed in the Calendar portlets. To avoid these errors:

1. Open the Collaboration **config.xml** configuration file, located in **<PT_HOME>/ptcollab/5.0/settings/config**.
2. In the following line, set the URL to the value of **ImageServerConnectionURL** set in the portal **portalconfig.xml** configuration file.

```
<jscontrols>
   <imageServerConnectionURL>[URL]</imageServerConnectionURL>
```

Configuring Publisher to Use a Secure Portal or Image Service

1. If the Image Service is secured with SSL:
   a. Open the Publisher **content.properties** configuration file, located in **<PT_HOME>/ptcs/6.3/settings/config**.
   b. Change the following Image Service entries:
   – For Security Modes 1 or 2, find and replace all occurrences of `http://machine_name/imageserver` with `https://machine_name/imageserver`, where `machine_name` is the name of the computer hosting Publisher.
   – For Security Mode 3, change the following entries:

```
CommunityImagePublishBrowserLocation=https://machine_name/imageserve
r/plumtree/portal/templates

CommunityImagePreviewBrowserLocation=https://machine_name/imageserve
r/plumtree/portal/templates/preview

CommunityStyleSheetListURL=http://machine_name/imageserver/plumtree/
common/public/css/community-themes.txt
```

```
JSComponents.AlternateImageServerUrl=http://machine_name/imageserver
```

Note: Some of the above entries are HTTP and some are HTTPS. Ensure that the port is correct for each.

2. Import the CA certificate from the Image Service and Portal into Publisher. For details, see "Importing CA Certificates" on page 2-7.

3. Restart Publisher.

Configuring Studio to Use a Secure Portal or Image Service

Import the CA certificate from the Image Service and Portal into Studio. For details, see "Importing CA Certificates" on page 2-7.

Configuring Workflow to Use a Secure Portal or Image Service

1. If you changed the AlternateImageServerURL in the content.properties file, perform the following steps so that Publisher can communicate the alternate Image Service URL to Workflow:

   a. Restart Publisher. This writes the URL to Workflow.

   b. After Publisher has restarted, restart Workflow. This forces the Workflow Web application to re-query Publisher for the alternate Image Service URL.

2. Import the CA certificate from the Image Service and Portal into Workflow. For details, see "Importing CA Certificates" on page 2-7.

CHAPTER 3

Authentication and SSO

This chapter describes the various authentication options for an AquaLogic User Interaction deployment.

By default, AquaLogic User Interaction performs authentication using credentials stored in the AquaLogic Interaction Portal database. Beyond basic portal authentication, AquaLogic User Interaction can delegate authentication to other backend systems, such as:

- A remote authentication tier, such as an LDAP service. For details, see "Delegating to a Remote Authentication Tier" on page 3-2.
- An SSO Provider such as Oblix. For details, see "Delegating to an SSO Provider" on page 3-3.
- Windows Integrated Authentication. For details, see "Delegating to Windows Integrated Authentication" on page 3-4.

Access control lists allow permissions to be granted to users and groups, and user and group properties can be pulled from backend services and mapped to portal users and groups. For details, see "Access Control Lists and Profile Sources" on page 3-4.

Authenticated users can have their credential information brokered to other backend services, allowing a single login to the portal to enable access to various systems. For details, see "Brokering Credentials" on page 3-5.

Delegating Authentication

The portal can be configured to delegate authentication to various other systems, including remote authentication tiers such as LDAP servers and Active Directory, SSO providers such as Oblix or Netegrity, and Windows Integrated Authentication (WIA). The following sections describe delegating authentication to these systems.

Delegating to a Remote Authentication Tier

Authentication can be delegated to a remote authentication tier by implementing an AquaLogic Interaction *authentication service*. The authentication service serves two roles: synchronization and authentication.

Synchronization against a backend authentication source imports users and groups into the AquaLogic Interaction portal database. This must be done before the portal user can authenticate against the backend authentication source. Passwords are not imported. This allows portal object permissions to be mapped to external users and groups, while maintaining authentication solely by the backend authentication source.

Authentication allows the portal to query a backend authentication source using a user's credentials. The sequence of events in the process is as follows:

1. The user browses to the main portal page and is presented the login screen. User enters credentials.
2. AquaLogic Interaction sends a request to the backend authentication source using the configured AquaLogic Interaction authentication service.
3. The backend authentication source returns validity of user credentials.
4. If the user is authenticated, access to their profile in the portal is granted. If the user is not authenticated, they are presented with the login screen.
5. AquaLogic Interaction stores credentials in memory, and the user is identified by a browser cookie, if configured to do so. This allows the the user to be logged in automatically next time he visits the portal.

AquaLogic Interaction includes pre-made authentication services supporting LDAP and Active Directory backend systems. In addition, you can develop custom authentication services to authenticate against any backend system.

Additional resources

- For details on configuring a pre-made authentication service, see Configuring an Authentication Source in the *Administrator Guide for AquaLogic Integration.*
- For details on creating a custom authentication service, start with Authentication Services Internals in the *AquaLogic User Interaction Development Documentation*.

Delegating to an SSO Provider

Delegating authentication to an SSO provider can circumvent the AquaLogic Interaction login screen and present the user with the login method of the SSO provider. This allows authentication by non-Web form mechanisms, such as keycards or biometric authentication.

The sequence of events of this process as follows:

1. The user browses to the main portal page address.
2. The portal forwards this request to the SSO provider.
3. The SSO provider determines whether the user is already authenticated or needs to be authenticated. This might be done by checking the user’s browser cookies or by another method.
4. If the user is not authenticated, the SSO provider does what is necessary to gather credentials and authenticate the user.
5. The SSO provider returns the user to the portal and instructs AquaLogic Interaction to grant the user access to his profile.

Additional resources

- For details on configuring an authentication source for an SSO provider, see Configuring an SSO Authentication Provider for Use with the Portal in the *Administrator Guide for AquaLogic Integration.*
- For details on configuring the portal to use an SSO provider, see Configuring the Portal for SSO in the *Administrator Guide for AquaLogic Interaction*.
- For details on configuring the portal and SSO, see Deploying Single Sign-On in the *Administrator Guide For AquaLogic Interaction.*

Delegating to Windows Integrated Authentication

Delegating to Windows Integrated Authentication (WIA) is similar to delegating to an SSO source. With WIA, the user's credentials are the same as their Windows network credentials. When the user browses to the portal page, the portal uses Windows to authenticate the user.

Prior to authenticating with WIA, user information must be crawled into the portal database using an Active Directory authentication source.

The sequence of events in the WIA authentication process is as follows:

1. The user logged into a Windows network browses to the main portal page.
2. The Portal returns a 401 Unauthorized message to the user browser.
3. The browser and portal perform the WIA handshake to validate the user.
4. The portal accepts the authentication and grants access to the user's profile.

For WIA to work, the user must be logged into a Windows network and be using a browser, such as Internet Explorer, that supports the WIA handshake. WIA will fail over an HTTP proxy.

Additional resources

- For details on configuring an authentication source for WIA, see Configuring the Windows Integrated Authentication Service in the *Administrator Guide for AquaLogic Interaction.*
- For details on configuring the portal to use WIA, see Configuring Integration with WIA in the *Administrator Guide for AquaLogic Interaction.*
- For details on configuring the portal and SSO, see *Deploying Single Sign-On* in the *Administrator Guide For AquaLogic Interaction.*

Access Control Lists and Profile Sources

Access Control Lists (ACLs) allow users and groups to be granted permission to use and modify objects in the portal. Portal users who authenticate with any of the methods described in the section "Delegating Authentication" on page 3-2 can be identified within the portal database and added to object ACLs.

A *profile service* uses an authentication service to pull user properties from backend systems such as LDAP services. Properties in the backend system are mapped to AquaLogic Interaction portal properties and synchronized with the authentication service.

Additional Resources

- For details on configuring ACLs, see Setting User Access Privileges in the *Administrator Guide For AquaLogic Interaction.*
- For details on configuring profile services, see Importing User Profiles from Profile Sources in the *Administrator Guide For AquaLogic Interaction.*
- For details on developing profile services, start with Profile Service Internals in the *AquaLogic User Interaction Development Documentation*.

Brokering Credentials

The credentials of a logged in user can be made available to other systems being accessed via the AquaLogic Interaction portal. This allows applications in the portal to display information from systems such as email or other enterprise applications without requiring for the user to log into each of these systems separately.

There are various ways AquaLogic Interaction can pass credentials to backend systems:

- **PassThrough:** The credentials the user supplied at login can be sent to the remote tier as a Basic Authentication header. This is useful if both the portal login and the backend system login are based on the same authentication source, such as an LDAP service.
- **Preferences:** Preferences can be created to hold the user's credential, to be set individually by the end user. Preferences are stored encrypted in the portal database and controlled by the end-user.
- **UserInfo:** User properties are mapped to credential information stored in an LDAP service or other backend source. Credentials are automatically populated for each user.
- **SSO:** An SSO token can be forwarded to the remote tier. This only works if the remote tier application can accept an SSO token. In cases where an SSO token is not accepted, some SSO Providers provide an API to convert the SSO token to name and password. This is dependent on the SSO vendor and the configuration of the SSO provider.
- **Lockbox**: User credentials can be stored in a lockbox in the AquaLogic Interaction credential vault. The credential vault provides a central repository that securely stores and manages credentials. Portlets that need credentials to access backend systems can securely retrieve appropriate user credentials.

Additional resources

- For details on brokering credentials to existing applications, see Managing User Credentials for Existing Applications and Using Portlets to Access Existing Web Applications, both in the *Administrator Guide for AquaLogic Interaction.*
- For details on developing portlets that use brokered credentials, start with Introduction: Portlet Security in the *AquaLogic User Interaction Development Documentation*.

Load Balancing

This chapter provides an overview of load balancing and failover options for an AquaLogic User Interaction deployment.

The purpose of this chapter is to assist in incorporating load balancing and redundancy into your network topology planning. Load balancing and redundancy options require third-party software or hardware and should be implemented with the aid of experts familiar with those third-party products. BEA provides professional consulting services to assist in planning an AquaLogic User Interaction deployment. To engage BEA professional services, contact your BEA representative.

This chapter is divided into two sections:

- "Load Balancing AquaLogic Interaction" on page 4-1 covers load balancing and failover strategies for the portal and other AquaLogic Interaction components.
- "Load Balancing Activity Services" on page 4-4 covers load balancing AquaLogic User Interaction Activity Services and clustering for Collaboration.

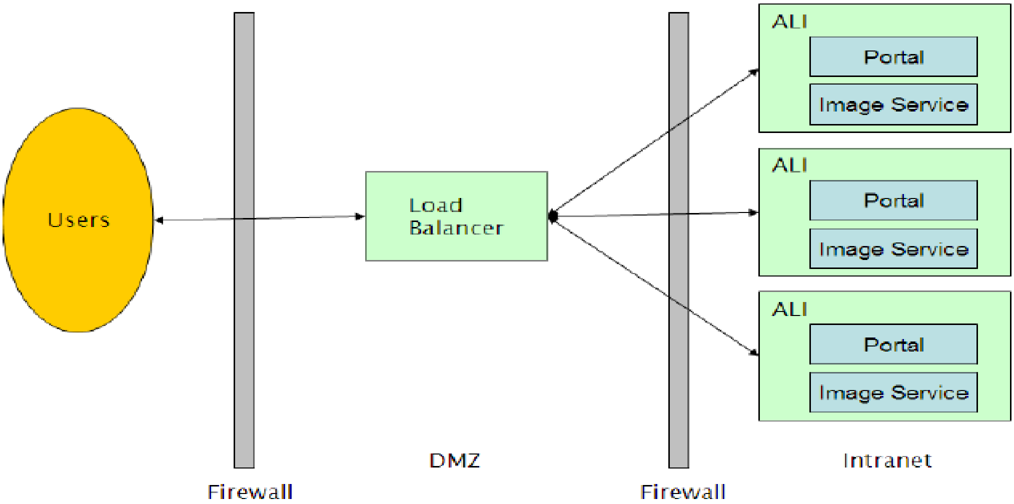
Load Balancing AquaLogic Interaction

The following sections provide examples of load balancing strategies for AquaLogic Interaction components.

Load Balancing the AquaLogic Interaction Portal Component

A typical configuration for hardware load balancing is to put the load balancer network appliance in the DMZ and have it route requests to an AquaLogic Interaction Portal server farm, as illustrated in Figure 4-1.

Figure 4-1 Hardware Load Balancing AquaLogic Interaction



The AquaLogic Interaction Portal can be used with any load balancing system that supports sticky IPs, including Cisco LocalDirector, F5 Big-IP, and Windows NLB, as well as the Apache Web server. BEA does not advocate any specific load balancer.

Session states are maintained by the portal Web servers themselves. If a portal server is taken out of the server farm, user sessions on that server are lost and users will need to log back into the portal.

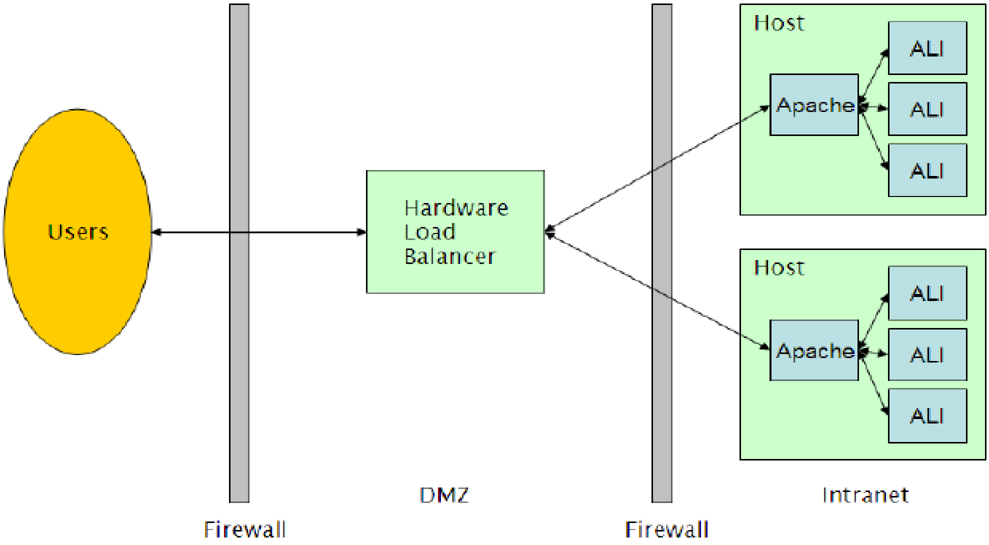
It is possible for the portal to become unresponsive while the portal Web server is still operational. In this case, the load balancer will assume that the portal is still alive. The load balancer should perform content verification to ensure that the portal is actually available.

The load balancer should send requests to the host with the most available resources instead of performing round-robin distribution of requests. Users use the portal component in different ways, and some users will tax the portal server more heavily than others.

For maximum fault tolerance, load balancers should be clustered.

Another potential load balancing topology is illustrated in Figure 4-2.

Figure 4-2 Multiple AquaLogic Interaction Instances on One Server



In this example, multiple instances of AquaLogic Interaction are running on a single host, with each portal server listening to a different port. On each host, an instance of Apache balances the load between the instances of AquaLogic Interaction. There are multiple hosts running this configuration, and these hosts are load-balanced by a hardware load balancer in the DMZ. Sticky IPs must be maintained throughout.

On hardware that supports a large number of users, this configuration minimizes the number of user sessions lost in the event of a portal failure.

Load Balancing the Image Service

The Image Service serves static content and does not require sticky IPs. Any number of Image Services can be load balanced.

Load Balancing the Document Repository Service

The document repository service can be load balanced using IP load balancing. This provides partial failover; however, all document repository hosts must share a single, writable file system backing store.

The backing store cannot be load balanced, but failover can be achieved by using a shared local disk with MSCS for failover or a network share implemented with NAS or MSCS.

Load Balancing the Automation Service

The Automation Service requires no additional technology for load balancing or failover. Install multiple Automation Services in the AquaLogic Interaction system and designate jobs to run on any set of available servers.

If a server fails mid-job, the job will not complete on another server; however, if the job is scheduled to run periodically, another Automation Service will pick up and run the job.

Load Balancing Search

Search performance can be improved by installing multiple Search instances. Dedicate one instance for indexing jobs and the remaining instances for queries. The indexing instance cannot be load balanced and does not support failover.

There are three levels of load capacity:

1. A single server performing both indexing and query services.
2. One server performing indexing and one server providing query services.
3. One server performing indexing and multiple servers providing query services. The query servers can be proxied through a third-party load balancer.

Load Balancing Activity Services

The following sections describe how to load balance AquaLogic User Interaction Activity Services.

The following AquaLogic User Interaction products should not be load balanced:

- AquaLogic Interaction Administrative Portal
- AquaLogic Interaction API Service

- Analytics
- Publisher
- Studio

PPE-LB Load Balancing Activity Services

The AquaLogic Interaction portal component provides the **Parallel Portal Engine Load Balancer** (PPE-LB) to facilitate load balancing and failover services to Activity Services and other portlet Web service providers utilizing HTTP messaging. This eliminates the need for third-party load balancers for middle-tier messaging.

To configure AquaLogic User Interaction Collaboration for clustering, see "Clustering AquaLogic Interaction Collaboration" on page 4-7.

Caution: Not all portlets can be load balanced. If the portlet caches data in memory with the assumption that the underlying database will not be modified, load balancing will cause issues. Consult the portlet documentation or portlet developer to determine if specific portlets can be load balanced.

Configuring the PPE-LB

The PPE-LB is configured by editing DNS so that one server name (the cluster name) resolves to each IP address in the cluster. Each remote server in the cluster must have a unique IP address and must have the same software installed.

Use **nslookup** from the portal server to verify that the cluster name resolves to all intended remote server addresses.

Caution: Editing the **hosts** file on a Windows host is not equivalent to configuring DNS. Windows caches and returns only the first IP address instead of returning all IP addresses associated with the cluster.

Note: If the DNS server cannot be configured, contact BEA Customer Support for Windows registry settings that can provide equivalent functionality.

PPE-LB and SSL

When using SSL between the AquaLogic Interaction Portal and the remote servers, create a single SSL certifiate by name and add it to each machine in the remote server cluster.

PPE Configuration Settings

The PPE is implemented with the OpenHTTP standard. OpenHTTP settings are configured in the ALI portal component by editing **<PT_HOME>/settings/common/serverconfig.xml**.

The following settings are configurable:

Setting	Description
ForceHttp10	Sends HTTP/1.0 requests instead of HTTP/1.1. The sockets are closed after sending a single request.
TraceBodyAndHeaders	For debugging only. Traces the values of headers and some parts of the body of the requests/responses to AquaLogic Interaction Logging. Turned off by default because headers might contain passwords in cleartext.
HttpCacheSizeMb	Defines maximum size of the cached data. Cache uses an LRU algorithm to decide which old entry should be kicked out in order to accommodate newer data.
ConnectionCacheTimeoutSec	Defines the time that the socket remains unused in the cache before being closed by OpenHTTP.
MinimumDNSThreads	Specifies the minimum number of threads that are used to perform DNS lookups.
MaximumDNSThreads	Specifies the maximum number of threads that are used to perform DNS lookups.
ProxyURL	Specifies the URL for a proxy host.
ProxyUser	Specifies an authentication user name for the proxy connection.
ProxyPassword	Specifies an authentication password for the proxy connection.
ProxyBypass	Contains a list of hosts accessed directly instead of through the proxy.
ProxyBypassLocal	Boolean flag specifies that hosts in the same domain should not be accessed through the proxy. If a hostname has no "." (dots) in its name it is considered local and in the same DNS domain.

Clustering AquaLogic Interaction Collaboration

Collaboration supports clustering to provide load balancing and fail over. In clustering mode, multiple instances of Collaboration communicate with each other to maintain a single, consistent logical image.

Configuring the Portal for Collaboration Clustering

The portal provides load balancing through mapping one domain name to multiple IP addresses. A single domain name that contains the IP addresses of each Collaboration server to be clustered must be provided. Use this name as the portlet remote server name.

Configuring Collaboration for Clustering

You configure Collaboration by editing two files, **config.xml** and **cluster.xml**. The files are located in **<PT_HOME>/ptcollab/<ver>/settings/config**

To enable clustering, perform the following steps on each Collaboration server to be clustered:

1. In **config.xml**, change the following:

   ```
   <cluster enabled=”no”>cluster.xml</cluster>
   ```

   to

   ```
   <cluster enabled=”yes”>cluster.xml</cluster>
   ```

2. Save **config.xml** and restart the Collaboration server.

By default, Collaboration uses UDP multicasting for communicating between servers. This is the most efficient option and is appropriate for most deployments. In environments where UDP multicasting is not allowed, configure Collaboration to use UDP unicasting.

To configure Collaboration to use UDP unicasting, perform the following steps on each Collaboration server to be clustered:

1. In **cluster.xml**, nominate one of the machines in the cluster to be the coordinator:

   ```
   <coordinator-host>machine.name</coordinator-host>
   <coordinator-port>9990</coordinator-port>
   ```

   Note: The port number can be any free port number.

2. Change the cluster profile to *lan-cluster*:

   ```
   <profiles profile=’lan-multicast-cluster’>
   ```

   to

```
<profiles profile='lan-cluster'>
```

3. Save **cluster.xml** and restart the Collaboration server.

Another optional configuration is to use the **wan-cluster** profile. The **wan-cluster** profile uses TCP to communicate directly with specific Collaboration instances.

To enable **wan-cluster**, perform the following steps on each Collaboration server to be clustered:

1. In **cluster.xml**, add one or more Collaboration instances to the `<hosts>` node. For example, if there are three Collaboration instances, collab01, collab02, and collab03, edit the collab01 **cluster.xml** to include the other two instances:

   ```
   <hosts>collab02[$port],collab03[$port]</hosts>
   ```

   Note: The **$port** string will be automatically replaced with the <port> setting already configured in **cluster.xml**.

2. In **cluster.xml**, change the cluster profile to *wan-cluster*:

   ```
   <profiles profile='lan-multicast-cluster'>
   ```

   to

   ```
   <profiles profile='wan-cluster'>
   ```

3. Save **cluster.xml** and restart the Collaboration server.