BEA AquaLogic® User Interaction

Deployment Planning

Document Revised: October 19, 2008

Contents

1. Welcome

2. Planning Portal Structure and Content

3. Securing AquaLogic User Interaction

4. Defining Administrative Roles

5. Migration and Staging

6. Provisioning Computers

CHAPTER 1

Welcome

The book provides an overview of planning an AquaLogic User Interaction deployment, and describes how to define administrative roles, stage deployments, and provision hardware.

For products and versions covered by this book, see the section Products Covered by the Deployment Guide in the *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, "Planning Portal Structure and Content" describes portal structure and content at a high level.

- Chapter 3, "Securing AquaLogic User Interaction" describes how to determine your security needs and measures to take to make your deployment more secure.
- Chapter 4, "Defining Administrative Roles" provides a high level overview of administrative roles.
- Chapter 5, "Migration and Staging" summarizes migration capabilities of AquaLogic User Interaction deployments.
- Chapter 6, "Provisioning Computers" summarizes host configuration and sizing requirements for an 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 ALUI 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.
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

CHAPTER 2

Planning Portal Structure and Content

This chapter describes portal structure and content at a high level.

The purpose of this chapter is to assist in planning portal structure and assigning administrative responsibility for managing portal content.

This chapter contains the following sections:

Single Portals and Federated Portals

It is possible to deploy a single portal or multiple, federated portals. Figure 2-1 illustrates a single portal deployment where different experience definitions provide a portal experience specific to each group of users. Figure 2-2 illustrates federated portals, where instead of experience definitions on a single portal, each federated portal provides a different portal experience.

Figure 2-1 Single Portal with Multiple Experience Definitions

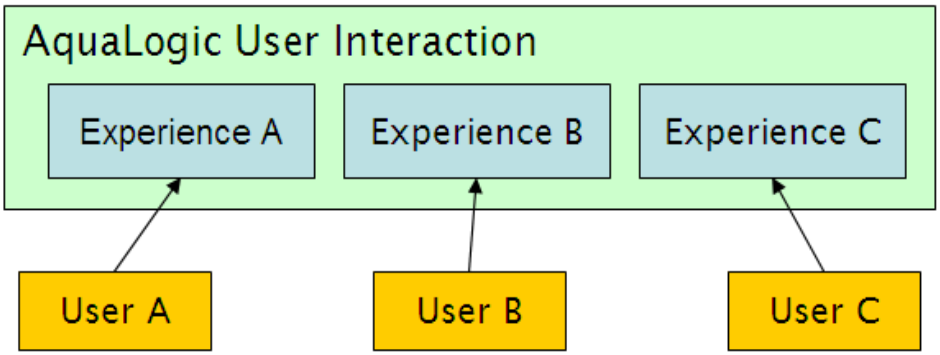
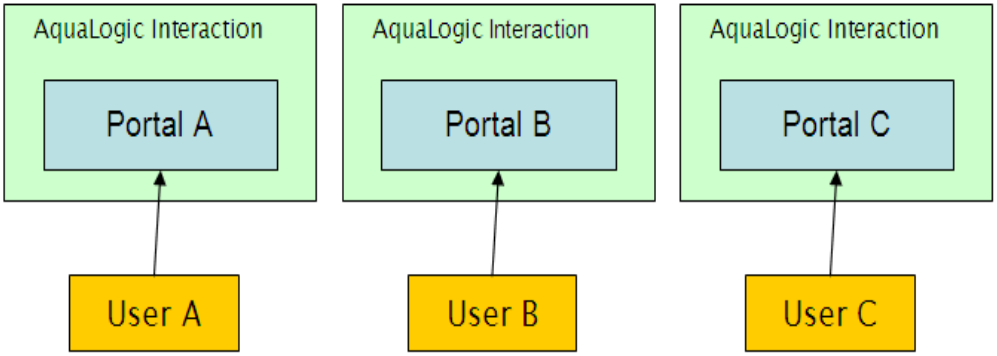


Figure 2-2 Federated Portals



Having a single portal with one or more experience definitions has benefits over deploying multiple federated portals. In a single portal deployment:

- Users have different experiences but are managed in a single place.
- The AquaLogic User Interaction deployment is easy to scale. IT needs only to look at total use for a single set of hardware versus fragmented use for multiple sets of hardware.
- It is easy to distribute enterprise-wide communications.
- It is easy to integrate enterprise-wide business processes.

- There is a common content management system

Experience Definitions

Experience definitions allow you to present different audiences with different branding and features in the portal.

For example, you could create an experience definition for a particular customer. The experience definition would include the customer's logo and company colors and include access to communities and knowledge directory folders specific to the needs of the customer.

Experience definitions are applied according to rules configured with the Experience Rules Manager.

For information on configuring experience definitions and rules, see the section Configuring Experience Definitions in the *Administrator Guide for AquaLogic Interaction.*

Communities

Communities are pages shared between members of a group to facilitate collaboration and communication on a particular project or on departmental goals.

Communities provide the following benefits:

- A consistent user experience for members of a department or project group.
- Discussion forums in which community-pertinent information is discussed and archived.
- A version-controlled repository for project or departmental documentation.

For details on implementing communties, see the documentation for *AquaLogic Interaction Collaboration*.

The following are potential use cases for communities:

- Business Unit Resource Center (Line of Business Communties)
- Interactive Workspace (Collaborative Communities)
- Customer or Partner Management Site (Sales and Service-Oriented Communities)
- Dashboards (Analytic Communities)
- Business Process Applications (Process Communities)

Business Unit Resource Center (Line of Business Communties)

Audience	• Business unit or department • Customers of that business unit or department
Content	• Community documents, links, calendar • Metrics • Expert finder • Q&A
Success indicators	• Strong departmental or group identity • Existing intranet as content source • Motivated community owner
Pitfalls to avoid	• Static page that people visit and forget
Suggested AquaLogic Interaction tools	• Portlet Framework - Microsoft Excel • Publisher

Interactive Workspace (Collaborative Communities)

Audience	• Ad hoc or established project workgroups
Content	• Project task list • Document management and archive • Project calendar • Threaded discussions • Project metrics
Success indicators	• Members spread out • Project has specific objectives and milestones • Project has outgrown e-mail and file-shares

Pitfalls to avoid	• Dustbin of history: old projects, communities that do not go away • Ghost town: two or three people are probably not enough
Suggested AquaLogic Interaction tools	• Collaboration • Studio • Portlet Framework - Microsoft Excel

Customer or Partner Management Site (Sales and Service-Oriented Communities)

Audience	• Customers or partners
Content	• Key customer or partner resources: documents, calendar • Self-service access to CRM or PRM system • Feedback mechanism • Customer-to-customer or partner-to-partner: facilitate community
Success indicators	• Portal-only access for critical information • Responsiveness to customer/partner feedback
Pitfalls to avoid	• No human input
Suggested AquaLogic Interaction tools	• Collaboration • Studio • Portlet Framework - Microsoft Excel

Dashboards (Analytic Communities)

Audience	• Management
Content	• Performance metrics • Financial documents
Success indicators	• Support to enforce consistent data formatting • Portal-only access for critical information • Culture of accountability based on metrics
Pitfalls to avoid	• Make sure the dashboards have fresh data • Make sure security works appropriately
Suggested AquaLogic Interaction tools	• Portlet Framework - Microsoft Excel • Integration Services for SAP and PeopleSoft

Business Process Applications (Process Communities)

Audience	• Users involved in process
Content	• Published content • Data from multiple systems • Workflow • Metrics
Success indicators	• Simple navigation, consistent branding a priority • Unified search criteria • Looking to utilize reusable components, common foundation
Pitfalls to avoid	• If you do not have a process, the software will not do it for you
Suggested AquaLogic Interaction tools	• Publisher • Collaboration • Process • Search • Studio • Portlet Framework - Microsoft Excel

Portlets

Portlets are applications embedded in a portal and can be interactive or solely informational. They are able to communicate preferences with the portal and to communicate with other portlets.

A portlet must be based on a web service. The web service controls the bulk of the portlet settings, such as the URL and cache settings. The portlet definition in the portal contains the name, width, type, and administrative preferences, if any.

Portlet templates allow multiple instances of the same portlet to be created, with each instance potentially different in appearance or information.

AquaLogic User Interaction includes pre-made portlets and the ability to easily create portlets using products such as Studio and Publisher.

Portlets can also be developed from scratch using the AquaLogic Interaction Development Kit (IDK). For details on portlet development, see Developing Portlets in the *Developer Documentation*.

AquaLogic Interaction Search

AquaLogic Interaction Search allows users to quickly and efficiently find a wide variety of information from sources across the enterprise, both inside and outside the AquaLogic User Interaction products. Search can be distributed across a multiple server cluster.

Searchable Content

There are a number of possible sources of searchable content, and it is important to understand the options for providing that content to end-users:

- **Knowledge Directory**: The core of the AquaLogic User Interaction knowledge management infrastructure is the Knowledge Directory—a hierarchy of folders that contain links to files of various formats, stored in different types of repositories. Files can be crawled into the Knowledge Directory or manually submitted and can be filtered into the folder hierarchy (also known as a taxonomy) in order to provide an entry point to high-quality, organized content. In addition to the out-of-the-box functionality, virtually any repository can be made searchable through the creation of Content Services. All items in the Knowledge Directory can be searchable.
- **Collaboration**: The project workspaces provided by Collaboration contain documents, threaded discussions, announcements, and task lists contributed and managed by distributed teams. All items in Collaboration can be searchable.
- **Publisher**: The form-based data entry and file management provided by Publisher allows specialized content submitted by users to be published and surfaced in the portal through portlets. All published content items associated with portlets can be searchable.
- **Portal Administrative Objects**: Users, web services, portlets, Content Services—all the objects that make up the administrative infrastructure of a portal are searchable. End-users can search for users (to view profile and expertise information), communities (to visit or join), and portlets (to add to a My Page). Administrators (who need to create and manipulate all types of objects) can search for a wider variety of items and have more advanced options in their search results.
- **Non-portal Searchable Content**: Legacy search engines and repositories with pre-existing search or query functionality can often contain valuable sources of content that for various reasons cannot be crawled into the portal or managed through Collaboration or Publisher. With search web services, any repository that can respond to queries can be extended with a web services adapter so that it can be searched from the portal. Results from a number of disparate search providers (both inside the enterprise and on the internet) can be aggregated in this way.

The Search administrator is responsible for creating and scheduling the initial search index jobs as well as update jobs. The Search administrator is also responsible for customizing search “Best Bets” and the search thesaurus.

Grid Search

Grid Search refers to distributing AquaLogic Interaction Search nodes over multiple servers. Search servers can be configured to be stand-alone or a node in a *search cluster*. In a search cluster, the search index is divided, or partitioned, across multiple search nodes.

You can manage the search cluster using the *Search Cluster Manager* or the command line utility *cadmin*.

For more information on administering Grid Search, see *Managing Grid Search* in the *Administrator Guide for AquaLogic Interaction.*

Grid Search Best Practices

1. Do not deploy multiple nodes on a single host in a production environment.
2. Schedule checkpoints when there is little or no planned indexing activity. This will help ensure that the checkpoint reflects the most up to date information and minimize recovery time.
3. Set the Search Cluster Manager Service to manual or disabled on all but one server. Only one instance of this service can be utilized by the portal.
4. A single search sever can be installed as a search cluster with one node, rather than a stand-alone search deployment. This helps streamline the process of adding future search nodes.
5. In a multiple node deployment, configure the cluster home directory on a server other than the search servers themselves. If the cluster home is located on one of the search servers, that server is a single point of failure for the entire cluster.
6. Cluster home should be located on a high-availablity file system with fast connectivity to the search node host machines. Ideally, the cluster home should be on a RAID file system to ensure availablity and falut tolerance.
7. Search nodes should be located within the same subnet on the network, and ideally on the same switch.

CHAPTER 3

Securing AquaLogic User Interaction

This chapter summarizes security concerns for AquaLogic User Interaction deployments. While this chapter provides a summary of security needs, it is not intended to replace the services of a qualified security professional.

This chapter is divided into the following sections:

For further details on securing your deployment, see the *Network Security* chapter of the *AqualLogic User Interaction Networking and Authentication Guide*.

Determining Your Security Needs

This section describes best practices for determining the security needs of your AquaLogic User Interaction deployment. It is divided into the following sections:

Understand Your Environment

To better understand your security needs, ask yourself the following questions:

- **Which resources am I protecting?**

  Many resources in the production environment can be protected, including information in databases accessed by AquaLogic Interaction and the availability, performance, applications, and the integrity of the website. Consider the resources you want to protect when deciding the level of security you must provide.

- **From whom am I protecting the resources?**

  For most websites, resources must be protected from everyone on the Internet. But should the website be protected from the employees on the intranet in your enterprise? Should your employees have access to all resources within the AquaLogic User Interaction environment? Should the system administrators have access to all AquaLogic User Interaction resources? Should the system administrators be able to access all data? You might consider giving access to highly confidential data or strategic resources to only a few well trusted system administrators. Perhaps it would be best to allow no system administrators access to the data or resources.

- **What will happen if the protections on strategic resources fail?**

  In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use the website. Understanding the security ramifications of each resource will help you protect it properly.

Hire Security Consultants or Use Diagnostic Software

Whether you deploy AquaLogic User Interaction on the Internet or on an intranet, it is a good idea to hire an independent security expert to go over your security plan and procedures, audit your installed systems, and recommend improvements. BEA partners offer services and products that can help you to secure a AquaLogic User Interaction production environment. For details, see the BEA Partner's Page at http://www.bea.com/partners.

Read Security Publications

For the latest information about securing web servers, BEA recommends the "Security Practices & Evaluations" information available from the CERT™ Coordination Center operated by Carnegie Mellon University.

For ALUI security advisories, refer to the BEA Support Center for ALUI products at http://support.plumtree.com/. Here, you can download security-related patches and subscribe to Support Alerts via email.

Report possible security issues in BEA's ALUI products in the following ways by contacting AquaLogic User Interaction technical support. For technical support contact information, see "BEA Documentation and Resources" on page 1-3.

Ensuring the Security of Your Production Environment

This section provides high-level descriptions of the security measures that can be employed to secure your AquaLogic User Interaction environment. It is divided into the following sections:

Securing the AquaLogic User Interaction Hosts

An AquaLogic User Interaction production environment is only as secure as the security of the the machines on which it is running. It is important that you secure the physical machine, the operating system, and all other software that is installed on the host machine. The following are suggestions for securing your AquaLogic Interaction host in a production environment. Also check with the manufacturer of the machine and operating system for recommended security measures.

Table 3-1 Securing AquaLogic User Interaction Hosts

Security Action	Description
Physically secure the hardware.	Keep your hardware in a secured area to prevent unauthorized operating system users from tampering with the deployment machine ore its network connections.
Secure networking services that the operating system provides	Have an expert review network services such as e-mail programs or directory services to ensure that a malicious attacker cannot access the operating system or system-level commands. The way you do this depends on the operating system you use. Sharing a file system with other machines in the enterprise network imposes risks of a remote attack on the file system. Be certain that the remote machines and the network are secure before sharing the file systmes from the machine that hosts AquaLogic User Interaction componets
Use a file system that can prevent unauthorized access.	Make sure the file system on each AquaLogic User Interaction component host can prevent unauthorized access to protected resources. For example, on a Windows computer, use only NTFS.

Table 3-1 Securing AquaLogic User Interaction Hosts

Security Action	Description
Set file access permissions for data stored on disk.	Set operating system file access permissions to restrict access to data stored on disk. This data includes, but is not limited to, the folowing: • Third-party authentication directories. • Portal configuration files. For example, operating systems such as Unix and Linux provide utilities such as umask and chmod to set the file access permissions. At a minimum, consider using “umask 066”, which denies read and write permissions to Group and Others..
Set file access permissions for data stored in the portal database.	Set operating system file access permissions to restrict access to data stored in the portal database.
Safeguard passwords.	The passwords for user accounts on production machines should be difficult to guess and should be guarded carefully. Set a policy to expire passwords periodically. Never code passwords in client applications.
Do not develop on a production machine.	Develop first on a development machine and then move code to the production machine when it is completed and tested. This process prevents bugs in the development environment from affecting the security of the production environment.
Do not install development and sample software on a production machine.	Do not install development tools on production machines. Keeping development tools off the production machine reduces the leverage intruders have should they get partial access to an AquaLogic User Interaction production machine. Do not install the AquaLogic User Interaction sample applications on production machines.
Enable security auditing.	Configure security auditing to enable monitoring of sensitive portal functions using the Audit Manager function.
Consider using additional software to secure your operating system.	Most operating system can run additional software to secure a production environment. For example, and Intrusion Detection System (IDS) can detect attempts to modify the production environment. Refer to the vendor of your operating system for information about available software.

Table 3-1 Securing AquaLogic User Interaction Hosts

Security Action	Description
Apply operation-system service packs and security patches.	Refer to the vendor of your operating system for a list of recommended service packs and security-related patches.
Apply the latest ALUI maintenance packs and impelment the latest security advisories.	If you are responsible for security related issues on your site, register on the ALUI Support Center page, http://support.plumtree.com, and subscribe to Support Alerts via email. In addition, you are advised to apply each maintenance pack as it is released. Maintenance packs are a roll-up of all bug fixes for each version of the product. You can download maintenance packs from http://commerce.bea.com/products/aqualogic/alui/alui.jsp

Securing Your Database

Most web applications use a database to store their data. Common databases used with AquaLogic User Interaction are Oracle 10G and Microsoft SQL Server. The databases frequently hold sensitive data. When creating your web application you must consider what data is going to be in the database and how secure you need to make that data. You also need to understand the security mechanisms provided by the manufacturer of the database and decide whether they are sufficient for your needs. If the mechanisms are not sufficient, you can use other security techniques to improve the security of the database, such as encrypting sensitive data before writing it to the database. For example, leave all customer data in the database in plain text except for the encrypted credit card information.

CHAPTER 4

Defining Administrative Roles

This chapter provides a high level overview of administrative roles.

The purpose of this chapter is to assist in developing a plan to assign administrative responsibility for managing portal objects.

Access Control Lists and Activity Rights

What users read, select, and modify in the portal is controlled by *access control lists* and *activity rights*.

Access Control Lists

An access control list (ACL) is a list of privileges associated with each folder or object in the portal. You can add users and groups to the ACL of an object in order to grant permission to perform certain tasks, such as viewing or modifying the object.

For details on using ACLs in the portal, see Setting User Access Privileges in the *Administrator Guide for AquaLogic Interaction.*

Activity Rights

You can associate activty rights with users and groups to allow users to perform specific tasks within the portal. For example, the *Access Administration* activity right allows a user to see the Administration tab in the portal and to access the administrative object hierarchy. There are a number of activity rights built into the portal. You can also create custom activity rights.

For more information on activity rights, including a full list of activity rights built into the portal, see Delegating Activity Rights in the *Administrator Guide for AquaLogic Interaction.*

Creating a Group Hierarchy

When creating a group hierarchy, begin with the users with the least rights and work towards the most powerful users. A group inherits the rights of its parent group, so the broadest groups with the least rights should be parent to more specific groups with greater rights.

For example, the engineering department creates an Engineer group (for all members of the department). The QA subset of the engineering department requires special access to certain bug tracking software, so a QA group should be created with the Engineer group as a parent. Administrative tasks on the bug tracking software is restricted to QA managers, so a group inheriting from the QA group is created for QA managers.

The Everyone group is the parent of all groups. All members of the Everyone group have the right to read and access their own profile.

The Administrator group is a child of all groups and has access to everything.

Assigning Activity Rights

The following table provides suggested activity rights for common roles found in an AquaLogic User Interaction deployment:

Role	Suggested Activity Rights
Content/Document Administrator	• Access Administration – to access the administration hierarchy • Edit Knowledge Directory – to create new document folders • Create Content Services – to create new Content Services • Create Data Sources – to access secured documents • Create Document Types – to force metadata onto documents • Create Filters – to automatically manage folders • Create Jobs – to run jobs • Access Utilities – to approve documents • Access Smart Sort – to re-sort entire folders of already categorized documents
Community Creator	• Access Administration • Create Communities – to create communities • Create Community Infrastructure – to create community and page templates
Portlet Creator	• Access Administration • Create Portlets – to create portlets • Create Web Service Infrastructure – to create the remote server and web service to create truly custom portlets
Group/User Creator	• Access Administration • Create Admin Folders – to make new admin folders to store users • Create Experience Definitions – to modify the user experience of users • Access Utilities – to create default profiles to apply initial layouts to users • Create Authentication Sources – to create authentication sources • Create Jobs • Create Profile Sources – to apply user information to synchronized users • Create Groups – to create groups • Create Users – to create users • Delegate Rights – to delegate rights to users (create activity groups)

Defining an Administrative Object Hierarchy

The Administrative Object Directory is a hierarchical folder structure that stores administrative objects.

Administrative objects include such objects as content services, portlets, and users. Each folder groups objects by object type. Each object's permissions default to the ACL of the folder.

For details on the Administrative Object Directory, see the Administrator Guide for AquaLogic Interaction.

The following guidelines can assist you in planning an administrative object hierarchy:

- Start with the end-user hierarchy rather than an organizational or management structure. End-users can see the administrative hierarchy in a few places in the portal. For example, by default, the Add Portlets and Join Communities pages search the administrative hierarchy for available portlets and communities and display a list of objects without showing their parent folders.

  Start by creating the hierarchy for communities and portlets (including portlet bundles) only and hide the administrative objects created during installation. For example, move all objects meant for administrators to a particular folder and restrict access to the folder so that end-users will not see it if they browse the hierarchy.

  The organization of the objects meant for administrators should be based on administrative structure or topic.

- Organize objects by topic rather than by object type. Objects are automatically grouped by type within each folder.

- Set ACLs for folders as early as possible. Objects created in a folder inherit the ACL of the folder. By planning access control early, you simplify managing object security.

- Manage user access by managing groups. Assigning a user to a group with permissions to a set of objects is easier than assigning each user to each object in the set.

Managing Quality through Object Migration

Creating a staging system for development and testing allows the AquaLogic User Interaction administrator to test object security. For information on object migration, see Chapter 5, "Migration and Staging."

CHAPTER 5

Migration and Staging

This chapter summarizes migration capabilities for AquaLogic User Interaction deployments.

The purpose of this chapter is to assist in planning development, QA, and production environments. By utilizing its migration capabilities you can stage the AquaLogic User Interaction deployment in a testing environment where you can test quality and gain acceptance prior to pushing it to production.

The following table summarizes migration capabilities.

Component	Migration Guidelines
Portal and Image Service	Follow the guidelines in the *Migrating, Backing Up, and Restoring Portal Objects* chapter of the *Administrator Guide for AquaLogic Interaction.*
Search	Search should not be migrated. The Search Update Agent job indexes new portal objects and documents.
• Identity Services • Content Services • Portlet Suite	Do not migrate these services. Import the original product **.pte** package and complete configuration as described in the installation guide for the specific product.
Publisher	Follow the guidelines in the *Migrating Publisher Objects* chapter of the *Administrator Guide for AquaLogic Publisher.*
Collaboration	Follow the guidelines in the *Migrating, Backing Up, and Restoring Portal Objects* chapter of the *Administrator Guide for AquaLogic Interaction.*

Component	Migration Guidelines
Studio	Follow the guidelines in the *Migrating, Backing Up, and Restoring Portal Objects* chapter of the *Administrator Guide for AquaLogic Interaction.* **Note:** – Migration is only relevant when the source and destination portals have distinct Studio installations. – Portlets must be created with a compatible version of Studio. – Do not include dependencies when creating the migration package. – Data in the source Studio portlet database is not migrated. Use the Studio data export/import functionality to move data. – If multiple Studio portlets share and underlying database, migrate these portlets in batch. This maintains the relationship between the portlets and their shared database.
Analytics	Do not migrate Analytics. Install and configure Analytics in the production environment.

CHAPTER 6

Provisioning Computers

This chapter summarizes host configuration and sizing requirements for an AquaLogic User Interaction deployment.

The purpose of this chapter is to assist in planning hardware provisioning for AquaLogic User Interaction deployment. For further assistance in provisioning hardware, contact your BEA representative.

Component Host Requirements

The following table provides guidelines for provisioning host computers for AquaLogic Interaction components.

Component	Host Requirements
Portal Service	Estimate hardware needs specific to anticipated load. For details, see "Evaluating Hardware Requirements for the Portal" on page 6-13. **Scaling Guide** For large deployments, install multiple Portal components and configure load balancing and failover. For details on load balancing and failover, see the Load Balancing section of the Networking and Authentication guide. **Security Guide** For details on security, see the Network Security section of the Networking and Authentication guide.
Administrative Portal	**Minimum** • Can additionally function as a Portal component in a Web farm. • Can be installed on the same host as Portal component and/or Image Service. • If not functioning as a Portal component, can be on the same host as Automation Service. **Recommended** A dedicated CPU. Some administrative actions are CPU-intensive. **Scaling Guide** No more than one Administrative Portal should be installed. **Security Guide** The Administrative Portal can be installed in a network environment that is only accessible by the AquaLogic User Interaction administrator.

Component	Host Requirements
Image Service	**Minimum** 256 MB RAM Can be installed on the same host computer as the Portal component. **Recommended** 512 MB RAM More processing power is required if you use SSL or compression. **Scaling Guide** For details on load balancing and failover, see the Load Balancing section of the Networking and Authentication guide. **Security Guide** For details on security, see the Network Security section of the Networking and Authentication guide.
Document Repository Service	**Minimum** 256 MB RAM **Recommended** • 512 MB RAM • Fault tolerant disk for document storage. **Scaling Guide** For details on load balancing and failover, see the Load Balancing section of the Networking and Authentication guide. **Security Guide** For details on security, see the Network Security section of the Networking and Authentication guide.

Component	Host Requirements
Automation Service	**Minimum** Should be on a separate host from the Portal component. If installed on the same host as the Portal, schedule all jobs to run in off-peak hours. **Recommended** • Dual processor, 1 Ghz or greater • 1 GB RAM **Scaling Guide** If you anticipate intensive use of identity service and content service jobs, install multiple automation services and configure load balancing. Because search performs document indexing and cannot be horizontally scaled, adding multiple automation services for the sole purpose of crawling content does not greatly improve system performance. For details on load balancing and failover, see the Load Balancing section of the Networking and Authentication guide. **Security Guide** For details on security, see the Network Security section of the Networking and Authentication guide.

Component	Host Requirements
Search	**Minimum** Small (up to 250,000 documents) Dual CPU, 2 GB RAM Medium (up to 500,000 documents) Dual CPU, 4GB RAM Two Search Partitions Larger (more than 500,000 documents, or very high search query load) 4 or more Search Partitions with dedicated Dual CPU, 4GB RAM Servers. Or 64-bit Solaris or AIX host (s), Dual CPU 1.3 Ghz or greater; 4-8 GB RAM, high performance I/O. **Recommended** Two or more x86 Dual CPU Servers with 3GB RAM each configured as a cluster. 64-bit Solaris or AIX host, Dual CPU 1.2 Ghz or greater; 4-8 GB RAM, high performance I/O. **Scaling Guide** CPU requirements are directly proportional to the search request throughput the component can support. Indexing speed is proportional to the speed of an individual CPU, per Search Partition. RAM supports internal caching done by Search. RAM requirements are proportional to the size and number of documents indexed.
Analytics	**Minimum** • Dual processor, 1 Ghz • 1 GB RAM **Recommended** Install on a separate host from the Portal component. **Scaling Guide** No more than one Analytics service should be installed. **Security Guide** Enable Unicast UDP on port 31314 for communication between Analytics and the Portal component. End-user access to Analytics is gatewayed by the Portal component, so the Analytics host computer can reside behind a DMZ firewall.

Component	Host Requirements
Collaboration	**Minimum** • Dual processor, 1 Ghz • 1 GB RAM Can reside on same host computer as other components that generate portlets, such as the Publisher, Studio, and Analytics. **Recommended** Install Collaboration on a separate host computer from other components to preclude contention for the JVM. **Scaling Guide** For details on load balancing and failover, see the *Load Balancing* section of the *Networking and Authentication* guide. **Security Guide** For details on security, see the *Network Security* section of the *Networking and Authentication* guide.
Publisher	**Minimum** • Dual processor, 1.2Ghz • 1 GB RAM Can reside on same host computer as other components that generate portlets, such as the Collaboration, Studio, and Analytics. **Recommended** Install Publisher on a separate host computer from other components to preclude contention for the JVM. **Scaling Guide** No more than one Publisher service should be installed. If capacity is an issue, install Publisher on a separate host with premium hardware. **Security Guide** ***Important!*** Configure your network to block port 8083 so that end users cannot access the port directly but Publisher components still have access from within the firewall. For more details on security, see the Network Security section of the Networking and Authentication guide.

Component	Host Requirements
Studio	**Minimum** • Dual processor, 1Ghz • 1 GB RAM Can reside on same host computer as other components that generate portlets, such as the Collaboration, Publisher, and Analytics. **Recommended** Install Studio on a separate host computer from other components to preclude contention for the JVM. **Scaling Guide** No more than one Studio service should be installed. If capacity is an issue, install Studio on a separate host with premium hardware. **Security Guide** For details on security, see the Network Security section of the *Networking and Authentication* guide.
AquaLogic Interaction API Service	**Minimum** Can be on the same host as a Portal component. **Recommended** Install on its own host. **Scaling Guide** No more than one AquaLogic Interaction API service should be installed. **Security Guide** You should not expose the SOAP API through the extranet. To protect it, install the AquaLogic Interaction API Service on a separate host from Portal components and locate the AquaLogic Interaction API Service host behind a firewall. For details on security, see the Network Security section of the Networking and Authentication guide.

Component	Host Requirements
Database Server	**Minimum** • 1 CPU, 1Ghz • 1 GB RAM **Recommended** • 2-8 CPU • 4 GB RAM Install on separate host computer. **Scaling Guide** Database Server Load Balancing The database server can be scaled using any database-compatible clustering technology. Currently, this means that scaling can only be provided by a larger machine. If necessary, each portal database can be placed on a separate computer and scaled separately. If running on Windows, failover of databases can be provided with Microsoft Cluster Services, and geographic load balancing and failover can be provided using SQL Server replication. However, this method is technically and administratively challenging and is not recommended unless availability requirements cannot be met otherwise. Oracle databases can be deployed for high availability. AquaLogic Interaction supports both client-side connection and server-side connection failover with Oracle RAC. **Security Guide** Install the database server behind a firewall and restrict access so that only computers that host AquaLogic Interaction components can access the database server host. End users do not need access to the database server host.

Component	Host Requirements
Remote Server - Identity Services (IDS)	**Minimum** • Dual processor, 1Ghz • 1 GB memory • 2 GB disk space **Recommended** Install on a separate host from the Portal component. To maximize performance, install in a network location that is in close proximity to back-end components. **Scaling Guide** Install additional Automation Services, as necessary, to accommodate a large number of IDS jobs. **Security Guide** End-user access to IDS portlets is gatewayed by the Portal component, so the IDS host computer can reside behind a DMZ firewall.

Component	Host Requirements
Remote Server - Content Services	**Minimum** Install on a separate host from the Portal component. **Recommended** To maximize performance, install in a network location that is in close proximity to backend data sources. **Scaling Guide** Install additional automation services, as necessary, to accommodate a large number of Content Service jobs. **Security Guide** End-user access to Content Service portlets is gatewayed by the Portal component, so the Content Service host computer can reside behind a DMZ firewall.
Remote Server - Portlets	**Minimum** Can share a host with other portlets and Web services. **Recommended** Install on a separate host from the portal component. To maximize performance, install in a network location that is in close proximity to backend components. **Scaling Guide** In general, caching enables static portlets with minimal personalization to scale very well to any number of users. Dynamic portlets with more personalization cannot be as effectively cached and so require more processing power. If necessary, improve performance by installing dynamic portlets on hosts with premium hardware. **Remote Server Load Balancing** Remote servers can be load balanced using Parallel Portal Engine load balancing. For details on load balancing and failover, see the Load Balancing section of the Networking and Authentication guide. **Security Guide** End-user access to portlets is gatewayed by the Portal component, so the remote server host computer for portlets can reside behind a DMZ firewall.

Optimization Strategies

The following table characterizes optimization strategies you might consider when you provision computer resources for your site.

Goal	Approach
Low initial hardware cost	Organizations optimizing for low initial hardware cost seek to buy the least expensive machines necessary to make the software work reliably. Given a choice between repurposing two existing single processor servers and spending $7,000 on a new multi-processor, multi-core server, they would choose the former.
Low hardware maintenance cost	Organizations optimizing for low hardware maintenance costs seek to reduce the number of machines needed to host the software. Because each additional computer incurs a minimum fixed cost in terms of administrative overhead, power consumption, space, and operating system license, these organizations would rather combine multiple ALUI components on a single, more powerful computer than distribute those components over multiple, less expensive machines.
High availability	Organizations optimizing for high availability are willing to spend extra money and effort to ensure that the portal and other ALUI components are available reliably to their users at all times. Such organizations typically purchase more computers and load balance them where possible, creating redundant configurations.
Low software maintenance cost	Organizations optimizing for low software maintenance cost assume that at some point in the life of the system, some part of the software will malfunction, and they seek both to lessen the chance that malfunctions will occur and lessen their impact when they do occur. Such organizations would typically purchase more individual computers to ensure that system components do not interfere with one another, and to reduce the risk that taking a computer out of the system to install new software will impact multiple system functions.
Scalability	Organizations optimizing for scalability assume that their deployments will be required to handle a large number of users. Such organizations would typically purchase extra hardware, and more expensive hardware, in order to create excess capacity in the system.

Goal	Approach
Performance	Organizations optimizing for performance seek to make their systems operate as fast as possible, especially in their ability to render pages quickly for end-users. Like organizations seeking to lower software maintenance costs, these organizations would distribute system components across a larger number of computers to ensure that each component has unrestricted access to the computing power it needs to perform its tasks the moment those tasks are called for.
Network Security	Organizations optimizing for network security seek to ensure that end-users touch only machines hosting the smallest amount of code and data. Such organizations also typically install firewalls between layers of their deployment, to ensure that if an intruder compromises one layer, the potential damage is limited. Such organizations tend to purchase more computers in order to isolate the Portal component, which end-users touch directly, from other components.

Evaluating Hardware Requirements for the Portal

Complete the steps in the following worksheet to evaluate hardware options.

Step	Calculation
Step 1	Estimate peak load using the following calculation: `Pages/sec = ((Power user pages/hr * #power users + Normal user pages/hr * #normal users + Infrequent user pages/hr * #infrequent users pages/hr) / (3600 sec/hr) * fraction of users who could log on who are actually connected` **Note:** Base your calculations on historical data for existing Web sites that serve a similar function. Use the following conventions to identify users: • Power users. A power user is one who routinely adds or deletes portal content. • Normal users. A normal user is one who routinely reads content. • Infrequent users. An infrequent user is one who does not routinely use the portal. Record your estimated peak load here: _____ pages/sec
Step 2	• Review the benchmark charts on "Portal Performance on Various Hardware Hosts" on page 6-14. • Choose a configuration that supports the peak load calculation from Step 1. In general, you want to provision a number of portal components that support a total of 2 to 3 times the estimated peak load from Step 1. For example, if you estimate peak load to be 15 pages/sec, you want to provision either: – One (1) portal component that can support 30-45 pages/sec – Two (2) or three (3) portal components that each support 15 pages/sec. • Record the benchmark capacity here: _____ pages/sec • Follow the steps described in Steps 3-10 to adjust this benchmark capacity to a real-life estimate of expected use.
Step 3	If users use My Pages more than communities, revise the number upward by approximately 5%.
Step 4	If users use the Knowledge Directory more than 20% of the time, revise the number downward by approximately 10%.
Step 5	If the deployment runs under SSL (security mode 2) on the portal component, without an SSL accelerator, subtract 10%.
Step 6	IF the deployment will use SSL to communicate to the majority of Portlets and Web Services, subtract 10%.

Step	Calculation
Step 7	If this portal also serves the administrative portal, revise the number downward by 5%.
Step 8	If you use a virus scanner on the portal , subtract 0-10%, depending on the virus scanner settings.
Step 9	If you use Tomcat as the Application Server and do not use the non-blocking Java connector (org.apache.coyote.http11.Http11NioProtocol), subtract 20%.
Step 10	If the system is deployed as a VMWare Virtual Machine, subtract 15%.
Step 11	After you have made the adjustments in Steps 3-10, does the configuration you selected in Step 2 still meet your capacity requirements?

Portal Performance on Various Hardware Hosts

Portal performance demonstrates the following general trends:

- Performance varies significantly on different types of server hardware.
- Performance is not dependent on the operating system, where platforms are otherwise similar.
- Performance is dependent on the JVM or CLR used and how these are tuned.
- In general, .NET and Java show similar performance, being nearly equal on most two-processor servers. However these vary somewhat in the sensitivity to processor frequency and system memory performance:
  - Java tends to be more sensitive to system memory performance.
  - .NET is more sensitive to processor cache size and processor frequency.

    These differences run approximately within a plus or minus 20% performance range at the very extreme.
- Overall performance is highly dependent on memory subsystem performance, which tends to be the most important performance-related property of a server. Memory subsystem performance can be characterized by the total aggregate system bandwidth to memory as well as the latency of memory access. For Intel Xeon-based systems, this is correlated with the processor bus speed. Systems with a 800Mhz bus significantly outperform those with a

400Mhz bus. Pentium III Xeon-based systems are also limited by their memory subsystem and scale poorly with extra CPUs.

The performance data in the table that follows is indicative of these general trends. This table provides benchmark data for the current version of the AquaLogic Interaction portal component. For each representative system, the load shown is the maximum sustainable load on the server with an average mix of page views on an uncustomized system. Various factors will influence the maximum sustainable load of individual deployments such as UI customizations, effective use of portlet caching, and different mixes of page types.

Pages per Second on AquaLogic Interaction 6.5

It is important that the performance measurements in the following table not be compared directly with the performance data for releases earlier than AquaLogic Interaction 6.5. A new benchmark was created for AquaLogic Interaction 6.5 that does more work per request and serves more sophisticated content than the previous benchmarks. In addition to richer content and more data in the system, HTTP compression is enabled and approximately 25% of the portlet request occur via HTTPS. Adaptive Layout mode is enabled for the benchmark.

The page distribution in the benchmark is approximately:

- 10% My Pages
- 30% Communities
- 10% Knowledge Directory
- 10% Searches
- 5% User Profiles
- 30% Gateway
- 5% other

The following table provides performance data for ALI 6.5.

System	System Details	Pages/Second
Xeon 2.4Ghz to 3.06Ghz, 533Mhz system bus, HyperThreading enabled (Dell PowerEdge 1750)	2 x 2.8Ghz Processors 512K L2	41
Xeon 3.2Ghz, 800Mhz system bus, HyperThreading enabled (Dell PowerEdge 1850)	2 x 3.2Ghz Processors 1M L2	67
Xeon MP 2.7Ghz, 400Mhz system bus, HyperThreading enabled (Dell PowerEdge 6650)	4 x 2.7Ghz Processor 512K L2 2M L3	67
Xeon 2.66Ghz, 1333Mhz system bus (Dell PowerEdge 1950)	4x2.66 Ghz Core 2 Xeon Dual Core	125
Opteron 2.2Ghz, 1000 MHz	2x2.2 Ghz Opteron Dual Core	105
UltraSparc IV 1.5Ghz Sun Fire V490	2 x 1.5 Ghz CPU	71
UltraSPARC-T1 1 GHz Sun Fire T1000	8 cores 32 threads 1GHz	74

Pages per Second on AquaLogic Interaction 6.1

The following table provides performance data for ALI 6.1. The benchmark used is different than that used in the previous section. Data from this table should not be compared to the ALI 6.5 performance data.

System	System Details	Pages/Second
Pentium III Xeon 1.4Ghz, 133 Mhz SDRAM (Dell PowerEdge 1650)	1 x 1.4Ghz Processor 512K L2	33
	2 x 1.4Ghz Processors 512K	44

System	System Details	Pages/Second
Xeon 2.4Ghz to 3.06Ghz, 533Mhz system bus, HyperThreading enabled (Dell PowerEdge 1750) **Note:** Mhz is less important than total processor cache for performance. Disabling HyperThreading decreases performance 12% with two CPUs and 25% with one.	1 x 2.4Ghz Processor 512K L2	56
	2 x 2.4Ghz Processors 512K L2	71
	1 x 2.8Ghz Processor 512K L2	58
	2 x 2.8Ghz Processors 512K L2	73
	1 x 3.06Ghz Processor 512K L21M L3	67
	2 x 3.06Ghz Processor 512K L2 1M L3	82
Xeon 3.2Ghz, 800Mhz system bus, HyperThreading enabled (Dell PowerEdge 1850) **Note:** The 800Mhz bus improves the performance of Xeon-based systems greatly. Disabling HyperThreading decreases performance by approximately 15% for dual-CPU systems and 25% for single CPU systems.	1 x 3.2Ghz Processor 1M L2	75
	2 x 3.2Ghz Processors 1M L2	100
Xeon MP 2.7Ghz, 512K L2 2M L3 caches, 400Mhz system bus, HyperThreading enabled (Dell PowerEdge 6650) **Note:** The 400Mhz bus of this system severely limits performance. This system is the only one with large differences in performance between .NET and Java platforms: .NET performs 25% better than the performance indicated here for the 4 processor node and performs equally well as Java for one processor.	1 x 2.7Ghz Processor 512K L2 2M L3	34
	2 x 2.7Ghz Processors 512K L2 2M L3	53
	4 x 2.7Ghz Processors 512K L2 2M L3	66

System	System Details	Pages/Second
UltraSparc III 1.0Ghz (Sun Fire 280R) **Note:** Most Sun systems scale the memory bandwidth with each CPU, and will scale well with increased CPU count.	1 x 1Ghz CPU	27
	2 x 1Ghz CPU	50
	4 x 1Ghz CPU	90
Power 5 1.5Ghz (IBM iSeries 520) **Note:** Power 5 based IBM systems scale memory with each pair of CPUs, and performance will scale with CPU count as a result.	2 x 1.5Ghz CPU	70