Deployment Planning Guide

ForgeRock Access Management 5

ForgeRock AS
201 Mission St, Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Abstract

Guide to planning ForgeRock# Access Management deployments. ForgeRock Access Management provides authentication, authorization, entitlement and federation software.

Table of Contents

Preface

The Deployment Planning Guide helps you to plan the deployment of ForgeRock Access Management, including implementing training teams and partners, customization and hardening, and development of a proof-of-concept implementation.

Other tasks include performing integration with client applications, integration with auditing tools, automation and continuous integration when necessary, running functional and non-functional testing, documenting procedures and tracking changes, acceptance in production, maintaining and supporting the solution in production, and planning for expansion and upgrade.

This guide is written for access management designers, developers, and administrators who build, deploy, and maintain ForgeRock Access Management services and features for their organizations.

About ForgeRock Identity Platform™ Software

ForgeRock Identity Platform™ is the only offering for access management, identity management, user-managed access, directory services, and an identity gateway, designed and built as a single, unified platform.

The platform includes the following components that extend what is available in open source projects to provide fully featured, enterprise-ready software:

- ForgeRock Access Management (AM)
- ForgeRock Identity Management (IDM)
- ForgeRock Directory Services (DS)
- ForgeRock Identity Gateway (IG)

Chapter 1

Introduction to Deployment Planning

The Deployment Planning Guide presents the key features and possible solutions to protect your Identity and Access Management (IAM) deployments. The guide discusses the benefits and advantages of implementations. It also provides examples of deployment to help you determine which features you might want to include in your deployments.

1.1. Understanding Identity Access Management

The proliferation of cloud-based technologies, mobile devices, social networks, Big Data, enterprise applications, and business-to-business (B2B) services has spurred the exponential growth of identity information, which is often stored in varied and widely-distributed identity environments.

The challenges of securing such identity data and the environments that depend on the identity data are daunting. Organizations that expand their services in-house or globally through internal development or through acquisitions must manage identities across wide spectrum of identity infrastructures. This expansion requires a careful integration of acquisitions must manage identities across a wide spectrum of identity infrastructures. This expansion requires a careful integration of disparate access management systems, platform-dependent architectures with limited scalability, and ad-hoc security components.

ForgeRock, a leader in the IAM market, provides proven solutions to securing your identity data.

Identity Management is the automated provisioning, updating, and de-provisioning of identities over their lifecycles. Access Management is the authentication and authorization of identities who desire privileged access to an organization's resources. Access management encompasses the central auditing of operations performed on the system by customers, employees, and partners. Access management also provides the means to share identity data across different access management systems, legacy implementations, and networks.

1.2. More than Just Single Sign-On

OpenAM is an all-in-one, centralized access management solution, securing protected resources across the network and providing authentication, authorization, Web security, and Federation Services in a single, integrated solution. OpenAM is deployed as a simple `.war` file and provides production-proven platform independence, flexible and extensible components, as well as a high availability and a highly scalable infrastructure. Using open standards, OpenAM is fully extensible, and can expand its capabilities through its SDKs and numerous REST endpoints.

OpenAM is part of the ForgeRock Identity Platform, and provides identity and access management of mobile-ready, cloud, enterprise, social, and partner services. The ForgeRock Identity Platform provides global consumer services across any platform for any connected device or any Internet-connected entity.

The ForgeRock Identity Platform features the following products:

- **OpenAM**. Context-Based Access Management System. OpenAM is an all-in-one industry-leading access management solution, providing authentication, authorization, federation, Web services security, adaptive risk, and entitlements services among many other features. OpenAM is deployed as a simple `.war` file, featuring an architecture that is platform independent, flexible, and extensible, and highly available and scalable.

- **OpenIDM**. Cloud-Focused Identity Administration. OpenIDM is a lightweight provisioning system, built on resource-oriented principles. OpenIDM is a self-contained system, providing workflow, compliance, synchronization, password management, and connectors. OpenIDM features a next-generation modular architecture that is self-contained and highly extensible.

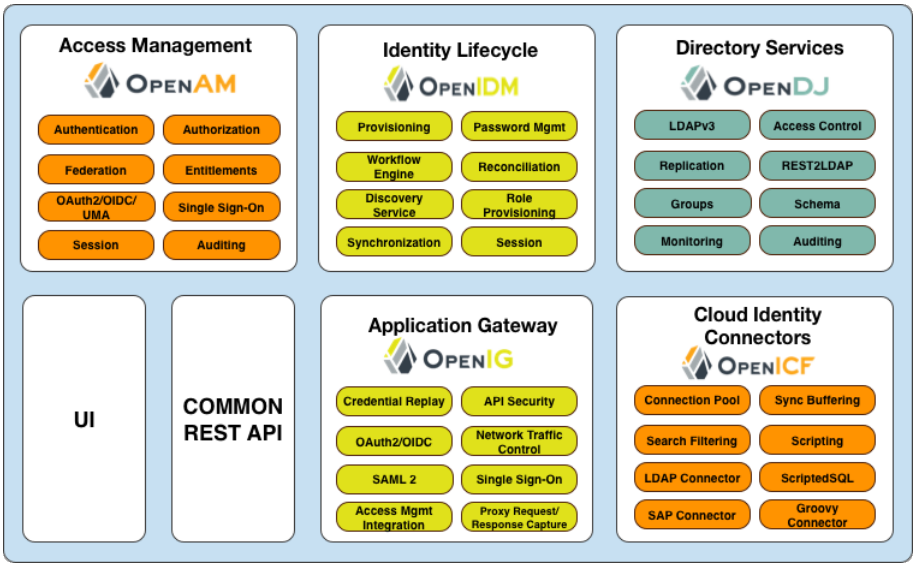
- **OpenDJ**. Internet Scale Directory Server. OpenDJ provides full LDAP protocol support, multi-protocol access, cross-domain replication, common REST framework, SCIM support, and many other features.

- **OpenIG**. No Touch Single Sign-On (SSO) to enterprise, legacy, and custom applications. OpenIG is a reverse proxy server with specialized session management and credential replay functionality. OpenIG works together with OpenAM to integrate Web applications without needing to modify the target application or the container that it runs in.

- **OpenICF**. Enterprise and Cloud Identity Infrastructure Connectors. OpenICF provides identity provisioning connections offering a consistent layer between target resources and applications and exposing a set of programming functions for the full lifecycle of an identity. OpenICF connectors are compatible with OpenIDM, Sun Identity Manager, Oracle® Waveset, Brinqa® GRC Platform, and so forth.

Figure 1.1, "ForgeRock Identity Platform" illustrates these components:

Figure 1.1. ForgeRock Identity Platform

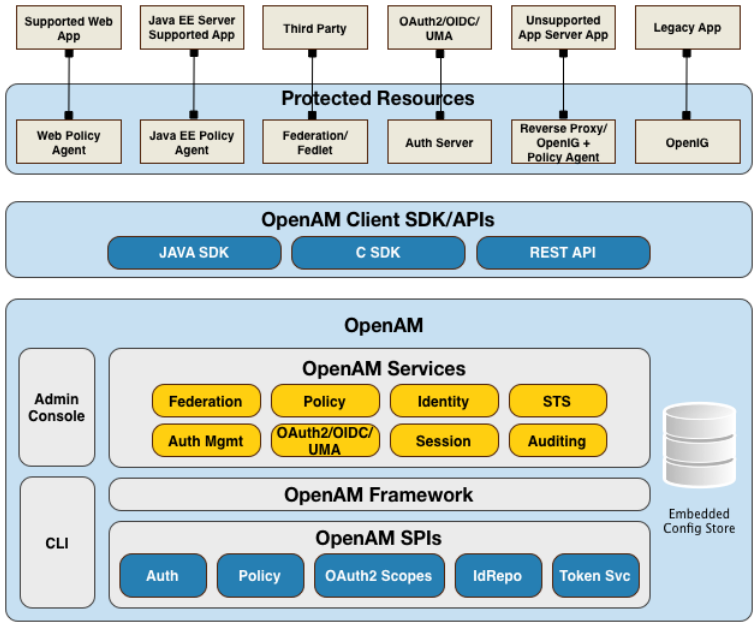


1.3. Server Overview

OpenAM is a centralized access management server, securing protected resources across the network and providing authentication, authorization, Web security, and federation services in a single, integrated solution. OpenAM manages access to the protected resources by controlling who has access, when, how long, and under what conditions by centralizing disparate hardware and software services for cloud, enterprise, mobile, and business-to-business (B2B) systems.

Figure 1.2, "Architecture" illustrates the OpenAM architecture.

Figure 1.2. Architecture



OpenAM features a highly modular and flexible architecture with multiple plugin points to meet any customer deployment. It leverages industry standard protocols, such as HTTP, XML, SOAP, REST, SAML 2.0, OAuth 2.0, OpenID Connect 1.0, and so forth to deliver a high performance, highly scalable, and highly available access management solution over the network. OpenAM services are 100% Java-based, proven across multiple platforms and containers in many production deployments.

OpenAM core server can be deployed and integrated within existing network infrastructures. OpenAM provides the following distribution files:

Table 1.1. Distribution Files

File	Description
`OpenAM-${softwareVersion}.war`	The distribution `.war` file includes the core server code with an embedded OpenDJ directory server, which stores configuration data and simplifies deployments. The distribution includes an administrative graphical user interface (GUI) Web console. During installation, the `.war` file accesses properties to obtain the fully qualified domain name, port, context path, and the location of the configuration folder. These properties can be obtained from the `boot.json` file in the OpenAM installation directory, from environment variables, or from a combination of the two. This is identical to the `AM-${platform.long.version}.war` file provided for download.

File	Description
`ClientSDK-13.5.0-1.jar`	OpenAM provides a client SDK for developers to code extensions for their web applications to access OpenAM's services. The client SDK contains the Java packages, classes, property files, and sample code to help you develop your code.
`ExampleClientSDK-CLI-13.5.0-1.zip`	OpenAM provides client SDK examples to help you run them on OpenAM. The `zip` distribution file contains setup scripts and samples that you can run to learn how to use the client SDK.
`ExampleClientSDK-WAR-13.5.0-1.war`	The example client SDK also comes in a `.war` file, which installs on your container.
`Fedlet-${softwareVersion}.zip`	OpenAM provides an OpenAM Fedlet, a light-weight SAML v2.0 service provider. The Fedlet lets you set up a federated deployment without the need of a fully-featured service provider.
`IDPDiscovery-${softwareVersion}.war`	OpenAM provides an IdP Discovery Profile (SAMLv2 binding profile) for its IdP Discovery service. The profile keeps track of the identity providers for each user.
`OpenAM-Soap-STS-Server-${softwareVersion}.war`	OpenAM provides a SOAP-based security token service (STS) server that issues tokens based on the WS-Security protocol[a].
`SSOAdminTools-${softwareVersion}.zip`	OpenAM provides an `ssoadm` command-line tool that allows administrators to configure and maintain OpenAM as well as create their own configuration scripts. The `zip` distribution file contains binaries, properties file, script templates, and setup scripts for UNIX and windows servers.
`SSOConfiguratorTools-${softwareVersion}.zip`	OpenAM provides configuration and upgrade tools for installing and maintaining your server. The `zip` distribution file contains libraries, legal notices, and supported binaries for these configuration tools. Also, you can view example configuration and upgrade properties files that can be used as a template for your deployments.

[a]AM also provides REST-based STS service endpoints, which you can directly utilize on the AM server.

The *ForgeRock BackStage* website hosts downloadable versions of OpenAM, including a `.zip` file with all of the OpenAM components, the `.war` file, OpenAM tools, the configurator, policy agents, and documentation. Verify that you review the Software License and Subscription Agreement presented before you download OpenAM files.

ForgeRock offers the services you need to deploy OpenAM commercial builds into production, including training, consulting, and support.

1.4. Key Benefits

The goal of OpenAM is to provide secure, low friction access to valued resources while presenting the user with a consistent experience. OpenAM provides excellent security, which is totally transparent to the user.

OpenAM provides the following key benefits to your organization:

- **Enables Solutions for Additional Revenue Streams**. OpenAM provides the tools and components to quickly deploy services to meet customer demand. For example, OpenAM's Federation Services supports quick and easy deployment with existing SAMLv2, OAuth2, and OpenID Connect systems. For systems that do not support a full SAMLv2 deployment, OpenAM provides a *Fedlet*, a small SAML 2.0 application, which lets service providers quickly add SAML 2.0 support to their Java applications. These solutions open up new possibilities for additional revenue streams.
- **Reduces Operational Cost and Complexity**. OpenAM can function as a hub, leveraging existing identity infrastructures and providing multiple integration paths using its authentication, SSO, and policies to your applications without the complexity of sharing Web access tools and passwords for data exchange. OpenAM decreases the total cost of ownership (TCO) through its operational efficiencies, rapid time-to-market, and high scalability to meet the demands of our market.
- **Improves User Experience**. OpenAM enables users to experience more services using SSO without the need of multiple passwords.
- **Easier Configuration and Management**. OpenAM centralizes the configuration and management of your access management system, allowing easier administration through its console and command-line tools. OpenAM also features a flexible deployment architecture that unifies services through its modular and embeddable components. OpenAM provides a common REST framework and common user interface (UI) model, providing scalable solutions as your customer base increases to the hundreds of millions. OpenAM also allows enterprises to outsource IAM services to system integrators and partners.
- **Increased Compliance**. OpenAM provides an extensive entitlements service, featuring attribute-based access control (ABAC) policies as its main policy framework with features like import/export support to XACML, a policy editor, and REST endpoints for policy management. OpenAM also includes an extensive auditing service to monitor access according to regulatory compliance standards.

1.5. History

OpenAM's timeline is summarized as follows:

- In 2001, Sun Microsystems releases iPlanet Directory Server, Access Management Edition.
- In 2003, Sun renames iPlanet Directory Server, Access Management Edition to Sun ONE Identity Server.
- Later in 2003, Sun acquires Waveset.
- In 2004, Sun releases Sun Java Enterprise System. Waveset Lighthouse is renamed to Sun Java System Identity Manager and Sun ONE Identity Server is renamed to Sun Java System Access Manager. Both products are included as components of Sun Java Enterprise System.
- In 2005, Sun announces an open-source project, OpenSSO, based on Sun Java System Access Manager.

- In 2008, Sun releases OpenSSO build 6, a community open-source version, and OpenSSO Enterprise 8.0, a commercial enterprise version.
- In 2009, Sun releases OpenSSO build 7 and 8.
- In January 2010, Sun was acquired by Oracle and development for the OpenSSO products were suspended as Oracle no longer planned to support the product.

In February 2010, a small group of former Sun employees founded ForgeRock to continue OpenSSO support, which was renamed to OpenAM. ForgeRock continued OpenAM's development with the following releases:

- 2010: OpenAM 9.0
- 2011: OpenAM 9.5
- 2012: OpenAM 10 and 10.1
- 2013: OpenAM 11.0
- 2014: OpenAM 11.1, 12.0, and 12.0.1
- 2015: OpenAM 11.0.3 and 12.0.2
- 2016: OpenAM 12.0.3, 12.0.4, 13.0.0, and 13.5.0
- 2017: Access Management 5

ForgeRock continues to develop, enhance, and support the industry-leading OpenAM product to meet the changing and growing demands of the market.

ForgeRock also took over responsibility for support and development of the OpenDS directory server, which was renamed as OpenDJ. ForgeRock plans to continue to maintain, enhance, and support OpenDJ.

Chapter 2

Planning the Deployment Architecture

This chapter presents the elements involved in planning deployment architecture.

2.1. Importance of Deployment Planning

Deployment planning is critical to ensuring your OpenAM system is properly implemented within the time frame determined by your requirements. The more thoroughly you plan your deployment, the more solid your configuration will be, and you will meet timelines and milestones while staying within budget.

A deployment plan defines the goals, scope, roles, and responsibilities of key stakeholders, architecture, implementation, and testing of your OpenAM deployment. A good plan ensures that a smooth transition to a new product or service is configured and all possible contingencies are addressed to quickly troubleshoot and solve any issue that may occur during the deployment process. The deployment plan also defines a training schedule for your employees, procedural maintenance plans, and a service plan to support your OpenAM system.

2.2. Deployment Planning Considerations

When planning a deployment, you must consider some important questions regarding your system.

- **What are you protecting?** You must determine which applications, resources, and levels of access to protect? Are there plans for additional services, either developed in-house or through future acquisitions that also require protected access?
- **How many users are supported?** It is important to determine the number of users supported in your deployment based on system usage. Once you have determined the number of users, it is important to project future growth.
- **What are your product service-level agreements?** In addition to planning for the growth of your user base, it is important to determine the production service-level agreements (SLAs) that help determine the current load requirements on your system and for future loads. The SLAs help define your scaling and high-availability requirements.

  For example, suppose you have 100,000 active users today, and each user has an average of two devices (laptop, phone) that get a session each day. Suppose that you also have 20 protected applications, with each device hitting an average of seven protected resources an average of 1.4 times daily. Let's say that works out to about 200,000 sessions per day with 7 x 1.4 = ~10 updates to each session object. This can result in 200K session creations, 200K session deletions, and 2M session updates.

  Now, imagine next year you still have the same number of active users, 100K, but each has an average of three devices (laptop, phone, tablet), and you have added another 20 protected applications. Assume the same average usage per application per device, or even a little less per device. You can see that although the number of users is unchanged, the whole system needs to scale up considerably.

  You can scale your deployment using vertical or horizontal scaling. Vertical scaling involves increasing components to a single host server, such as increasing the number of CPUs or increasing heap memory to accommodate a larger session cache or more policies. Horizontal scaling involves adding additional host servers, possibly behind a load balancer, so that the servers can function as a single unit.
- **What are your high availability requirements?** High availability refers to your system's ability to operate continuously for a specified length of time. It is important to design your system to prevent single points of failure and for continuous availability. Based on the size of your deployment, you can create an architecture using a single-site configuration. For larger deployments, consider implementing a multi-site configuration with replication over WAN in combination with one of the following two alternatives:

  - Stateless sessions
  - Sticky load-balancing with highly available stateful sessions

  Which type of clients will be supported? The type of client determines the components required for the deployment. For example, applications supported in a Web server require the use of a Web

policy agent. Applications deployed in Java EE containers require the use of a Java EE policy agent. An AJAX application can use the OpenAM's RESTful API. Legacy or custom applications can use the OpenIG Identity Gateway. Applications in an unsupported application server can use a reverse proxy with a policy agent. Third party applications can use federation or a fedlet, or an OpenID Connect or an OAuth 2.0 component.

- **What are your SSL/TLS requirements?** There are two common approaches to handling SSL. First, using SSL through to the application servers themselves, for example, using SSL on the containers. Or second, using SSL offloading via a network device and running HTTP clear internally. You must determine the appropriate approach as each method requires different configurations. Determining SSL use early in the planning process is vitally *important*, as adding SSL later in the process is more complicated and could result in delays in your deployment.
- **What are your other security requirements?** The use of firewalls provides an additional layer of security for your deployment. If you are planning to deploy the OpenAM server behind a firewall, you can deploy a reverse proxy, such as OpenIG. For another level of security, consider using multiple DNS infrastructures using zones; one zone for internal clients, another zone for external clients. To provide additional performance, you can deploy the DNS zones behind a load balancer.
- **Ensure all stakeholders are engaged during the planning phase**. This effort includes but is not limited to delivery resources, such as project managers, architects, designers, implementers, testers, and service resources, such as service managers, production transition managers, security, support, and sustaining personnel. Input from all stakeholders ensures all viewpoints are considered at project inception, rather than downstream, when it may be too late.

2.3. Deployment Planning Steps

The general deployment planning steps can be summarized as follows:

- **Project Initiation**. The Project Initiation phase begins by defining the overall scope and requirements of the deployment. The following items can be planned:
  - Determine the scope, roles and responsibilities of key stakeholders and resources required for the deployment.
  - Determine critical path planning including any dependencies and their assigned expectations.
  - Run a pilot to test the functionality and features of OpenAM and uncover any possible issues early in the process.
  - Determine training for administrators of the environment and training for developers, if needed.
- **Architecting**. The Architecting phase involves designing the deployment. The following items can be planned:
  - Determine the use of products, map requirements to features, and ensure the architecture meets the functional requirements.

- Ensure that the architecture is designed for ease of management and scale. TCO is directly proportional to the complexity of the deployment.
- Determine how the Identity, Configuration, and Core Token Service (CTS) data stores are to be configured.
- Determine the sites configuration.
- Determine where SSL is used in the configuration and how to maintain and update the certificate keystore and truststore for OpenAM's components, such as the agent installer, **ssoadm** tool, agent server, and other OpenAM servers. Planning for SSL at this point can avoid more difficulty later in the process.
- Determine if OpenAM will be deployed behind a load balancer with SSL offloading. If this is the case, you must ensure that the load balancer rewrites the protocol during redirection. If you have a policy agent behind a load balancer with SSL offloading, ensure that you set the policy agent's override request URL properties.
- For multiple OpenAM deployments, there is a requirement to deploy a layer 7 cookie-based load balancer and intelligent keep-alives (for example, `/openam/isAlive.jsp`). The network teams should design the appropriate solution in the architecting phase.
- Determine requirements for vertical scaling, which involves increasing the Java heap based on anticipated session cache, policy cache, federation session, and restricted token usage. Note that vertical scaling could come with performance cost, so this must be planned accordingly.
- Determine requirements for horizontal scaling, which involves adding additional OpenAM servers and load balancers for scalability and availability purposes.
- Determine whether to configure OpenAM to issue stateful or stateless sessions. Stateless sessions allow for easier horizontal scaling but do not provide equivalent functionality to stateful sessions.
- Determine if any coding is required including extensions and plugins. Unless it is absolutely necessary, leverage the product features instead of implementing custom code. OpenAM provides numerous plugin points and REST endpoints.

- **Implementation**. The Implementation phase involves deploying your OpenAM system. The following items should be considered:
  - Install and configure the OpenAM server, datastores, and components. For information on installing OpenAM, see the Installation Guide.
  - Maintain a record and history of the deployment to maintain consistency across the project.
  - Tune OpenAM's JVM, caches, LDAP connection pools, container thread pools, and other items. For information on tuning OpenAM, see Section 8.4, "Tuning an Instance" in the *Setup and Maintenance Guide*.

  - Tune the OpenDJ directory server. Consider tuning the database back end, replication purge delays, garbage collection, JVM memory, and disk space considerations. For more information, see the OpenDJ directory server documentation.
  - Consider implementing separate file systems for both OpenAM and OpenDJ, so that you can keep log files on a different disk, separate from data or operational files, to prevent device contention should the log files fill up the file system.
- **Automation and Continuous Integration**. The Automation and Continuous Integration phase involves using tools for testing:
  - Set up a continuous integration server, such as Jenkins, to ensure that builds are consistent by running unit tests and publishing Maven artifacts. Perform continuous integration unless your deployment includes no customization.
  - Ensure your custom code has unit tests to ensure nothing is broken.
- **Functional Testing**. The Functional Testing phase should test all functionality to deliver the solution without any failures. You must ensure that your customizations and configurations are covered in the test plan.
- **Non-Functional Testing**. The Non-Functional Testing phase tests failover and disaster recovery procedures. Run load testing to determine the demand of the system and measure its responses. You can anticipate peak load conditions during the phase.
- **Supportability**. The Supportability Phase involves creating the runbook for system administrators including procedures for backup and restores, debugging, change control, and other processes. If you have a ForgeRock Support contract, it ensures everything is in place prior to your deployment.

2.4. Preparing Deployment Plans

When you create a good concrete deployment plan, it ensures that a change request process is in place and utilized, which is essential for a successful deployment. This section looks at planning the full deployment process. When you have addressed everything in this section, then you should have a concrete plan for deployment.

2.4.1. Planning Training

Training provides common understanding, vocabulary, and basic skills for those working together on the project. Depending on previous experience with access management and with OpenAM, both internal teams and project partners might need training.

The type of training team members need depends on their involvement in the project:

- All team members should take at least some training that provides an overview of OpenAM. This helps to ensure a common understanding and vocabulary for those working on the project.

- Team members planning the deployment should take an OpenAM deployment training before finalizing your plans, and ideally before starting to plan your deployment.

  OpenAM not only offers a broad set of features with many choices, but the access management it provides tends to be business critical. OpenAM deployment training pays for itself as it helps you to make the right initial choices to deploy more quickly and successfully.

- Team members involved in designing and developing OpenAM client applications or custom extensions should take training in OpenAM development in order to help them make the right choices. This includes developers customizing the OpenAM UI for your organization.

- Team members who have already had been trained in the past might need to refresh their knowledge if your project deploys newer or significantly changed features, or if they have not worked with OpenAM for some time.

ForgeRock University regularly offers training courses for OpenAM topics, including OpenAM development and deployment. For a current list of available courses, see http://forgerock.com/services/university/.

When you have determined who needs training and the timing of the training during the project, prepare a training schedule based on team member and course availability. Include the scheduled training plans in your deployment project plan.

ForgeRock also offers an accreditation program for partners, offering an in-depth assessment of business and technical skills for each ForgeRock product. This program is open to the partner community and ensures that best practices are followed during the design and deployment phases.

2.4.2. Planning Customization

When you customize OpenAM, you can improve how the software fits your organization. OpenAM customizations can also add complexity to your system as you increase your test load and potentially change components that could affect future upgrades. Therefore, a best practice is to deploy OpenAM with a minimum of customizations.

Most deployments require at least some customization, like skinning end user interfaces for your organization, rather than using the OpenAM defaults. If your deployment is expected to include additional client applications, or custom extensions (authentication modules, policy conditions, and so forth), then have a team member involved in the development help you plan the work. The Development Guide can be useful when scoping a development project.

Although some customizations involve little development work, it can require additional scheduling and coordination with others in your organization. An example is adding support for profile attributes in the identity repository.

The more you customize, the more important it is to test your deployment thoroughly before going into production. Consider each customization as sub-project with its own acceptance criteria, and consider plans for unit testing, automation, and continuous integration. See Section 2.4.8, "Planning Tests" for details.

When you have prepared plans for each customization sub-project, you must account for those plans in your overall deployment project plan. Functional customizations, such as custom authentication modules or policy conditions might need to reach the pilot stage before you can finish an overall pilot implementation.

2.4.3. Planning a Pilot Implementation

Unless you are planning a maintenance upgrade, consider starting with a pilot implementation, which is a long term project that is aligned with customer-specific requirements.

A pilot shows that you can achieve your goals with OpenAM plus whatever customizations and companion software you expect to use. The idea is to demonstrate feasibility by focusing on solving key use cases with minimal expense, but without ignoring real-world constraints. The aim is to fail fast before you have too much invested so that you can resolve any issues that threaten the deployment.

Do not expect the pilot to become the first version of your deployment. Instead, build the pilot as something you can afford to change easily, and to throw away and start over if necessary.

The cost of a pilot should remain low compared to overall project cost. Unless your concern is primarily the scalability of your deployment, you run the pilot on a much smaller scale than the full deployment. Scale back on anything not necessary to validating a key use case.

Smaller scale does not necessarily mean a single-server deployment, though. If you expect your deployment to be highly available, for example, one of your key use cases should be continued smooth operation when part of your deployment becomes unavailable.

The pilot is a chance to try and test features and services before finalizing your plans for deployment. The pilot should come early in your deployment plan, leaving appropriate time to adapt your plans based on the pilot results. Before you can schedule the pilot, team members might need training and you might require prototype versions of functional customizations.

Plan the pilot around the key use cases that you must validate. Make sure to plan the pilot review with stakeholders. You might need to iteratively review pilot results as some stakeholders refine their key use cases based on observations.

2.4.4. Planning Security Hardening

When you first configure OpenAM, there are many options to evaluate, plus a number of ways to further increase levels of security. You can change the following default configuration properties:

- The main OpenAM administrative account has a default user name, `amadmin`.
- You can set up OpenAM using HTTPS rather than HTTP.
- An OpenAM policy agent administrative account exists and has a default user name, `UrlAccessAgent`.
- The primary session cookie has a default name, `iPlanetDirectoryPro`.

- Initially, only the top-level realm exists. Other realms and fully qualified domain name realm/DNS aliases must be configured separately.
- The top-level realm includes a demo user, `demo`, with the default password `changeit`.
- Default keystores exist in the *`config-dir`*`/openam/` path, with several self-signed keys and identical passwords. For more information about the default keystores in OpenAM and their demo key aliases, see Chapter 5, "*Setting Up Keys and Keystores*" in the *Setup and Maintenance Guide*.
- By default, OpenAM connects to directory servers as the directory root user, `cn=Directory Manager`.
- By default, the list of `goto` and `gotoOnFail` URLs is not restricted.
- On a server that includes the AM console, all the endpoints defined in the Web application descriptor, `WEB-INF/web.xml`, are available for use.
- To prevent cross-site scripting attacks, you can configure session cookies as HTTP Only by setting the property `com.sun.identity.cookie.httponly=true`. This property prevents third-party scripts from accessing the session cookie.
- You can deploy a reverse proxy within delimitarized zone (DMZ) firewalls to limit exposure of service URLs to the end user as well as block access to back end configuration and user data stores to unauthorized users.

You must therefore plan to secure the deployment as described in Chapter 4, "*Securing Installations*" in the *Installation Guide*.

At minimum, make sure you include the following tasks in the overall plan:

- Change default settings and administrative user credentials.
- Protect service ports (using firewalls, install a reverse proxy).
- Disable unused endpoints.
- Separate administrative access from client access.
- Secure communications so that OpenAM clients access services over HTTPS.
- Use secure cookies with cookie hijacking protection for CDSSO, so messages for federated configurations perform signing and encryption as necessary, and OpenAM accesses providers securely (for example using LDAP + StartTLS, or LDAPS to access directory services).
- Secure processes and files (for example with SELinux, using a dedicated non-privileged user and port forwarding, and so forth).

2.4.5. Planning With Providers

OpenAM delegates authentication and profile storage to other services. OpenAM can store configuration, policies, session, and other tokens in an external directory service. OpenAM can also participate in a circle of trust with other SAML entities. In each of these cases, a successful deployment depends on coordination with service providers, potentially outside of your organization.

The infrastructure you need to run OpenAM services might be managed outside your own organization. Hardware, operating systems, network, and software installation might be the responsibility of providers with which you must coordinate.

When working with providers, take the following points into consideration.

- Shared authentication and profile services might have been sized prior to or independently from your access management deployment.

  An overall outcome of your access management deployment might be to decrease the load on shared authentication services (and replace some authentication load with single-sign on that is managed by OpenAM), or it might be to increase the load (if, for example, your deployment enables many new applications or devices, or enables controlled access to resources that were previously unavailable).

  Identity repositories are typically backed by shared directory services. Directory services might need to provision additional attributes for OpenAM. This could affect not only directory schema and access for OpenAM, but also sizing for the directory services that your deployment uses.

- If your deployment uses an external directory service for OpenAM configuration data and OpenAM policies, then the directory administrator must include attributes in the schema and provide access rights to OpenAM. The number of policies depends on the deployment. For deployments with thousands or millions of policies to store, OpenAM's use of the directory could affect sizing.

- If your deployment uses an external directory service as a backing store for the OpenAM Core Token Service (CTS), then the directory administrator must include attributes in the schema and provide access rights to OpenAM.

  CTS load tends to involve more write operations than configuration and policy load, as CTS data tend to be more volatile, especially if most tokens concern short-lived sessions. This can affect directory service sizing.

  CTS enables cross-site session high availability by allowing a remote OpenAM server to retrieve a user session from the directory service backing the CTS. For this feature to work quickly in the event of a failure or network partition, CTS data must be replicated rapidly including across WAN links. This can affect network sizing for the directory service.

  When configured to issue stateless sessions, OpenAM does *not* write the stateless sessions to CTS. Instead, OpenAM uses CTS for session blacklists. Session blacklisting is an optional OpenAM feature that provides logout integrity.

- SAML federation circles of trust require organizational and legal coordination before you can determine what the configuration looks like. Organizations must agree on which security data they share and how, and you must be involved to ensure that their expectations map to the security data that is actually available.

  There also needs to be coordination between all SAML parties, (that is, agreed-upon SLAs, patch windows, points of contact and escalation paths). Often, the technical implementation is considered, but not the *business requirements*. For example, a common scenario occurs when a

service provider takes down their service for patching without informing the identity provider or vice-versa.

- When working with infrastructure providers, realize that you are likely to have better sizing estimates after you have tried a test deployment under load. Even though you can expect to revise your estimates, take into account the lead time necessary to provide infrastructure services.

  Estimate your infrastructure needs not only for the final deployment, but also for the development, pilot, and testing stages.

For each provider you work with, add the necessary coordinated activities to your overall plan, as well as periodic checks to make sure that parallel work is proceeding according to plan.

2.4.6. Planning Integration With Client Applications

When planning integration with OpenAM client applications, the applications that are most relevant are those that register with OpenAM; therefore, you should make note of the following types of client applications registering with OpenAM:

- OpenAM policy agents reside with the applications they protect.

  By default, OpenAM policy agents store their configuration profiles in OpenAM. OpenAM then sends policy agents notifications when their configurations change.

  Policy agents authenticate to OpenAM with a user name and password.

  To delegate administration of multiple policy agents, OpenAM lets you create a group profile for each realm to register the policy agent profiles.

  While the OpenAM administration manages policy agent configuration, application administrators are often the ones who install policy agents. You must coordinate installation and upgrades with them.

- OAuth 2.0 clients and OpenID Connect 1.0 relying parties also register profiles with OpenAM.

  OpenAM optionally allows registration of such applications without prior authentication. By default, however, registration requires an access token granted to an OAuth 2.0 client with access to register profiles.

  If you expect to allow dynamic registration, or if you have many clients registering with your deployment, then consider clearly documenting how to register the clients, and building a client to register clients.

- You must configure Circles of Trust for SAML 2.0 federations, so registration happens at configuration time, rather than at runtime.

  Address the necessary configuration as described in Section 2.4.5, "Planning With Providers".

If your deployment functions as a SAML 2.0 Identity Provider (IDP) and shares Fedlets with Service Providers (SP), the SP administrators must install the Fedlets, and must update their Fedlets for changes in your IDP configuration. Consider at least clearly documenting how to do so, and if necessary, build installation and upgrade capabilities.

- If you have custom client applications, consider how they are configured and how they must register with OpenAM.
- REST API client applications authenticate based on a user profile.

  REST client applications can therefore authenticate using whatever authentication mechanisms you configure in OpenAM, and therefore do not require additional registration.

For each client application whose integration with OpenAM requires coordination, add the relevant tasks to your overall plan.

2.4.7. Planning Integration With Audit Tools

OpenAM and policy agents can log audit information to flat files or alternatively, to a relational database. Log volumes depend on usage and on logging levels. By default, OpenAM generates both access and error messages for each service, providing the raw material for auditing the deployment. The Reference covers what you can expect to find in log messages.

In order to analyze the raw material, however, you must use other software, such as Splunk, which indexes machine-generated data for analysis.

If you require integration with an audit tool, plan the tasks of setting up logging to work with the tool, and analyzing and monitoring the data once it has been indexed. Consider how you must retain and rotate log data once it has been consumed, as a high volume service can produce large volumes of log data.

Include these plans in the overall plan.

2.4.8. Planning Tests

In addition to planning tests for each customized component, test the functionality of each service you deploy, such as authentication, policy decisions, and federation. You should also perform non-functional testing to validate that the services hold up under load in realistic conditions. Perform penetration testing to check for security issues. Include acceptance tests for the actual deployment. The data from the acceptance tests help you to make an informed decision about whether to go ahead with the deployment or to roll back.

2.4.8.1. Planning Functional Testing

Functional testing validates that specified test cases work with the software considered as a black box.

As ForgeRock already tests OpenAM and policy agents functionally, focus your functional testing on customizations and service-level functions. For each key service, devise automated functional tests. Automated tests make it easier to integrate new deliveries to take advantage of recent bug fixes and to check that fixes and new features do not cause regressions.

Tools for running functional testing include Apache JMeter and Selenium. Apache JMeter is a load testing tool for Web applications. Selenium is a test framework for Web applications, particularly for UIs.

As part of the overall plan, include not only tasks to develop and maintain your functional tests, but also to provision and to maintain a test environment in which you run the functional tests before you significantly change anything in your deployment. For example, run functional tests whenever you upgrade OpenAM, OpenAM policy agents, or any custom components, and analyze the output to understand the effect on your deployment.

2.4.8.2. Planning Service Performance Testing

For written service-level agreements and objectives, even if your first version consists of guesses, you turn performance plans from an open-ended project to a clear set of measurable goals for a manageable project with a definite outcome. Therefore, start your testing with clear definitions of success.

Also, start your testing with a system for load generation that can reproduce the traffic you expect in production, and provider services that behave as you expect in production. To run your tests, you must therefore generate representative load data and test clients based on what you expect in production. You can then use the load generation system to perform iterative performance testing.

Iterative performance testing consists in identifying underperformance and the bottlenecks that cause it, and discovering ways to eliminate or work around those bottlenecks. Underperformance means that the system under load does not meet service level objectives. Sometimes re-sizing and/or tuning the system or provider services can help remove bottlenecks that cause underperformance.

Based on service level objectives and availability requirements, define acceptance criteria for performance testing, and iterate until you have eliminated underperformance.

Tools for running performance testing include Apache JMeter, for which your loads should mimic what you expect in production, and Gatling, which records load using a domain specific language for load testing. To mimic the production load, examine both the access patterns and also the data that OpenAM stores. The representative load should reflect the expected random distribution of client access, so that sessions are affected as in production. Consider authentication, authorization, logout, and session timeout events, and the lifecycle you expect to see in production.

Although you cannot use actual production data for testing, you can generate similar test data using tools, such as the OpenDJ **makeldif** command, which generates user profile data for directory services. OpenAM REST APIs can help with test provisioning for policies, users, and groups.

As part of the overall plan, include not only tasks to develop and maintain performance tests, but also to provision and to maintain a pre-production test environment that mimics your production environment. Security measures in your test environment must also mimic your production

environment, as changes to secure OpenAM as described in Section 2.4.4, "Planning Security Hardening", such as using HTTPS rather than HTTP, can impact performance.

Once you are satisfied that the baseline performance is acceptable, run performance tests again when something in your deployment changes significantly with respect to performance. For example, if the load or number of clients changes significantly, it could cause the system to underperform. Also, consider the thresholds that you can monitor in the production system to estimate when your system might start to underperform.

2.4.8.3. Planning Penetration Testing

Penetration testing involves attacking a system to expose security issues before they show up in production.

When planning penetration testing, consider both white box and black box scenarios. Attackers can know something about how OpenAM works internally, and not only how it works from the outside. Also, consider both internal attacks from within your organization, and external attacks from outside your organization.

As for other testing, take time to define acceptance criteria. Know that ForgeRock has performed penetration testing on the software for each enterprise release. Any customization, however, could be the source of security weaknesses, as could configuration to secure OpenAM.

You can also plan to perform penetration tests against the same hardened, pre-production test environment also used for performance testing.

2.4.8.4. Planning Deployment Testing

Deployment testing is used as a description, and not a term in the context of this guide. It refers to the testing implemented within the deployment window after the system is deployed to the production environment, but before client applications and users access the system.

Plan for minimal changes between the pre-production test environment and the actual production environment. Then test that those changes have not cause any issues, and that the system generally behaves as expected.

Take the time to agree upfront with stakeholders regarding the acceptance criteria for deployment tests. When the production deployment window is small, and you have only a short time to deploy and test the deployment, you must trade off thorough testing for adequate testing. Make sure to plan enough time in the deployment window for performing the necessary tests and checks.

Include preparation for this exercise in your overall plan, as well as time to check the plans close to the deployment date.

2.4.9. Planning Documentation and Tracking Changes

The OpenAM product documentation is written for readers like you, who are architects and solution developers, as well as for OpenAM developers and for administrators who have had OpenAM training.

The people operating your production environment need concrete documentation specific to your deployed solution, with an emphasis on operational policies and procedures.

Procedural documentation can take the form of a runbook with procedures that emphasize maintenance operations, such as backup, restore, monitoring and log maintenance, collecting data pertaining to an issue in production, replacing a broken server or policy agent, responding to a monitoring alert, and so forth. Make sure in particular that you document procedures for taking remedial action in the event of a production issue.

Furthermore, to ensure that everyone understands your deployment and to speed problem resolution in the event of an issue, changes in production must be documented and tracked as a matter of course. When you make changes, always prepare to roll back to the previous state if the change does not perform as expected.

Include documentation tasks in your overall plan. Also, include the tasks necessary to put in place and to maintain change control for updates to the configuration.

2.4.10. Planning Maintenance and Support in Production

If you own the architecture and planning, but others own the service in production, or even in the labs, then you must plan coordination with those who own the service.

Start by considering the service owners' acceptance criteria. If they have defined support readiness acceptance criteria, you can start with their acceptance criteria. You can also ask yourself the following questions:

- What do they require in terms of training in OpenAM?
- What additional training do they require to support your solution?
- Do your plans for documentation and change control, as described in Section 2.4.9, "Planning Documentation and Tracking Changes", match their requirements?
- Do they have any additional acceptance criteria for deployment tests, as described in Section 2.4.8.4, "Planning Deployment Testing"?

Also, plan back line support with ForgeRock or a qualified partner. The aim is to define clearly who handles production issues, and how production issues are escalated to a product specialist if necessary.

Include a task in the overall plan to define the hand off to production, making sure there is clarity on who handles monitoring and issues.

2.4.11. Planning Rollout Into Production

In addition to planning for the hand off of the production system, also prepare plans to roll-out the system into production. Rollout into production calls for a well-choreographed operation, so these are likely the most detailed plans.

Take at least the following items into account when planning the rollout:

- Availability of all infrastructure that OpenAM depends upon the following elements:
  - Server hosts and operating systems
  - Web application containers
  - Network links and configurations
  - Load balancers
  - Reverse proxy services to protect OpenAM
  - Data stores, such as directory services
  - Authentication providers
- Installation for all OpenAM services.
- Installation of OpenAM client applications:
  - Policy agents
  - Fedlets
  - SDK applications
  - OAuth 2.0 applications
  - OpenID Connect 1.0 applications
- Final tests and checks.
- Availability of the personnel involved in the rollout.

In your overall plan, leave time and resources to finalize rollout plans toward the end of the project.

2.4.12. Planning for Growth

Before rolling out into production, plan how to monitor the system to know when you must grow, and plan the actions to take when you must add capacity.

Unless your system is embedded or otherwise very constrained, after your successful rollout of access management services, you can expect to add capacity at some point in the future. Therefore, you should plan to monitor system growth.

You can grow many parts of the system by adding servers or adding clients. The parts of the system that you cannot expand so simply are those parts that depend on writing to the directory service.

The directory service eventually replicates each write to all other servers. Therefore, adding servers simply adds the number of writes to perform. One simple way of getting around this limitation is to split a monolithic directory service into several directory services. That said, directory services often are not a bottleneck for growth.

When should you expand the deployed system? The time to expand the deployed system is when growth in usage causes the system to approach performance threshold levels that cause the service to underperform. For that reason, devise thresholds that can be monitored in production, and plan to monitor the deployment with respect to the thresholds. In addition to programming appropriate alerts to react to thresholds, also plan periodic reviews of system performance to uncover anything missing from regular monitoring results.

2.4.13. Planning for Upgrades

In this section, "upgrade" means moving to a more recent release, whether it is a patch, maintenance release, minor release, or major release. For definitions of the types of release, see Appendix A, "*Release Levels and Interface Stability*" in the *Release Notes*.

Upgrades generally bring fixes, or new features, or both. For each upgrade, you must build a new plan. Depending on the scope of the upgrade, that plan might include almost all of the original overall plan, or it might be abbreviated, for example, for a patch that fixes a single issue. In any case, adapt deployment plans, as each upgrade is a new deployment.

When planning an upgrade, pay particular attention to testing and to any changes necessary in your customizations. For testing, consider compatibility issues when not all agents and services are upgraded simultaneously. Choreography is particularly important, as upgrades are likely to happen in constrained low usage windows, and as users already have expectations about how the service should behave.

When preparing your overall plan, include a regular review task to determine whether to upgrade, not only for patches or regular maintenance releases, but also to consider whether to upgrade to new minor and major releases.

2.4.14. Planning for Disaster Recovery

Disaster recovery planning and a robust backup strategy is essential when server hardware fails, network connections go down, a site fails, and so on. Your team must determine the disaster recovery procedures to recover from such events.

Chapter 3

Example Deployment Topology

You can configure OpenAM in a wide variety of deployments depending on your security requirements and network infrastructure. This chapter presents an example enterprise deployment, featuring a highly available and scalable architecture across multiple data centers.

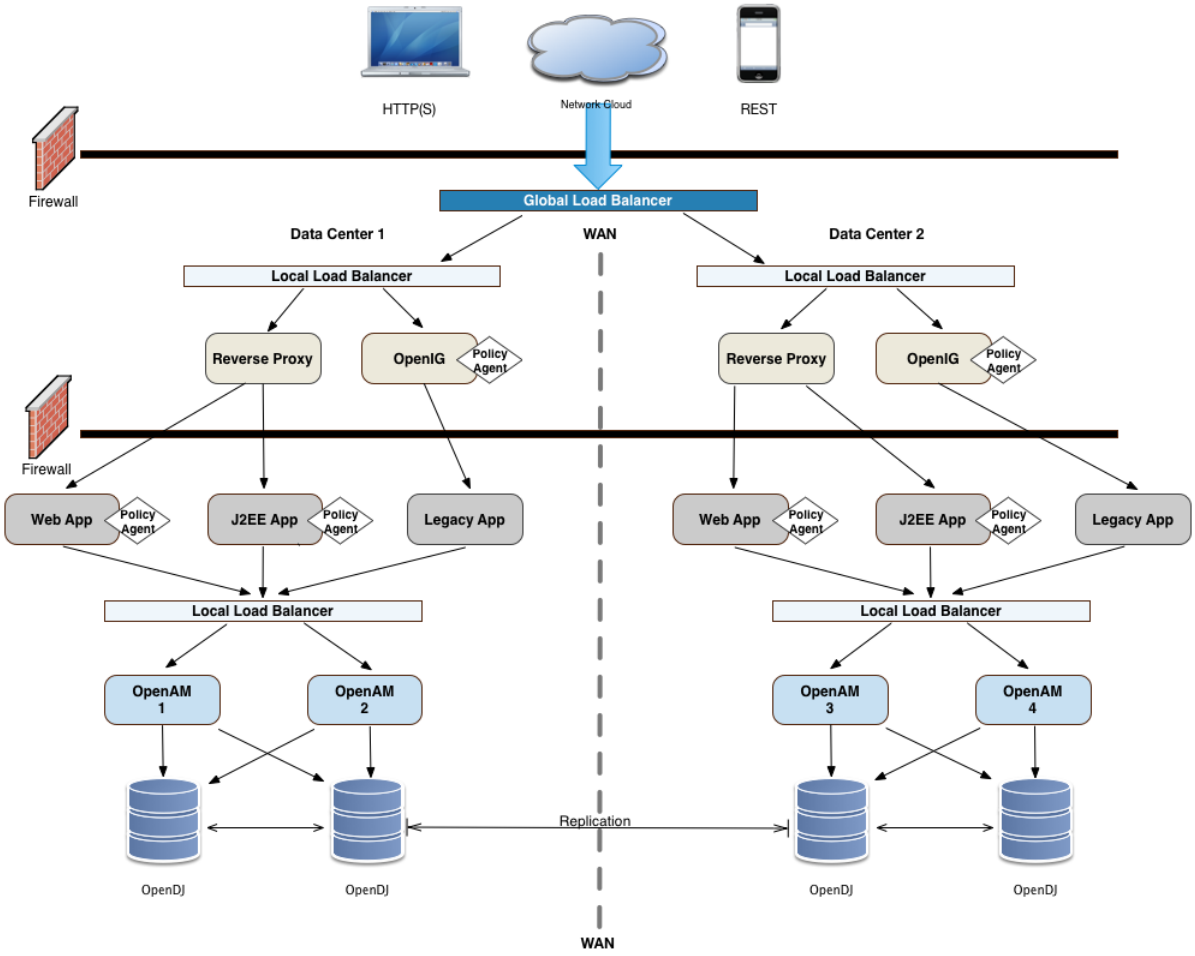
3.1. About the Example Topology

Figure 3.1, "Deployment Example" presents an example topology of a multi-city multi-data-center deployment across a wide area network (WAN). The example deployment is partitioned into a two-tier architecture. The top tier is a DMZ with the initial firewall securing public traffic into the network. The second firewall limits traffic from the DMZ into the application tier where the protected resources are housed.

Note

The example components in this chapter are presented for illustrative purposes. ForgeRock does not recommend specific products, such as reverse proxies, load balancers, switches, firewalls, and so forth, as OpenAM can be deployed within your existing networking infrastructure.

Figure 3.1. Deployment Example



3.2. The Public Tier

The public tier provides an extra layer of security with a DMZ consisting of load balancers and reverse proxies. This section presents the DMZ elements.

3.2.1. The Global Load Balancer

The example deployment uses a global load balancer (GLB) to route DNS requests efficiently to multiple data centers. The GLB reduces application latency by spreading the traffic workload among data centers and maintains high availability during planned or unplanned down time, during which it quickly re-routes requests to another data center to ensure online business activity continues successfully.

You can install a cloud-based or a hardware-based version of the GLB. The leading GLB vendors offer solutions with extensive health-checking, site affinity capabilities, and other features for most systems. Detailed deployment discussions about global load balancers are beyond the scope of this guide.

3.2.2. Front End Local Load Balancers

Each data center has local front end load balancers to route incoming traffic to multiple reverse proxy servers, thereby distributing the load based on a scheduling algorithm. Many load balancer solutions provide server affinity or stickiness to efficiently route a client's inbound requests to the same server. Other features include health checking to determine the state of its connected servers, and SSL offloading to secure communication with the client.

You can cluster the load balancers themselves or configure load balancing in a clustered server environment, which provides data and session high availability across multiple nodes. Clustering also allows horizontal scaling for future growth. Many vendors offer hardware and software solutions for this requirement. In most cases, you must determine how you want to configure your load balancers, for example, in an active-passive configuration that supports high availability, or in an active-active configuration that supports session high availability.

There are many load balancer solutions available in the market. You can set up an external network hardware load balancer, or a software solution like HAProxy (L4 or L7 load balancing) or Linux Virtual Server (LVS) (L4 load balancing), and many others.

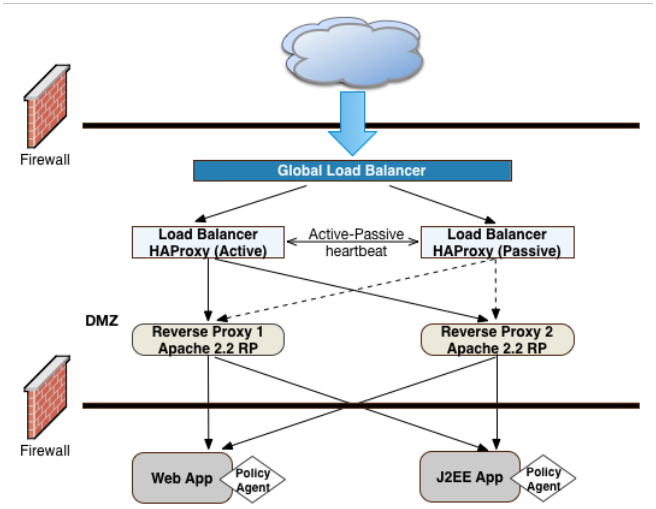
3.2.3. Reverse Proxies

The reverse proxies work in concert with the load balancers to route the client requests to the back end Web or application servers, providing an extra level of security for your network. The reverse proxies also provide additional features, like caching to reduce the load on the Web servers, HTTP compression for faster transmission, URL filtering to deny access to certain sites, SSL acceleration to offload public key encryption in SSL handshakes to a hardware accelerator, or SSL termination to reduce the SSL encryption overhead on the load-balanced servers.

The use of reverse proxies has several key advantages. First, the reverse proxies serve as an highly scalable SSL layer that can be deployed inexpensively using freely available products, like Apache HTTP server or nginx. This layer provides SSL termination and offloads SSL processing to the reverse proxies instead of the load balancer, which could otherwise become a bottleneck if the load balancer is required to handle increasing SSL traffic.

Figure 3.2, "Frontend Load Balancer Reverse Proxy Layer" illustrates one possible deployment using HAProxy in an active-passive configuration for high availability. The HAProxy load balancers forward the requests to Apache 2.2 reverse proxy servers. For this example, we assume SSL is configured everywhere within the network.

Figure 3.2. Frontend Load Balancer Reverse Proxy Layer

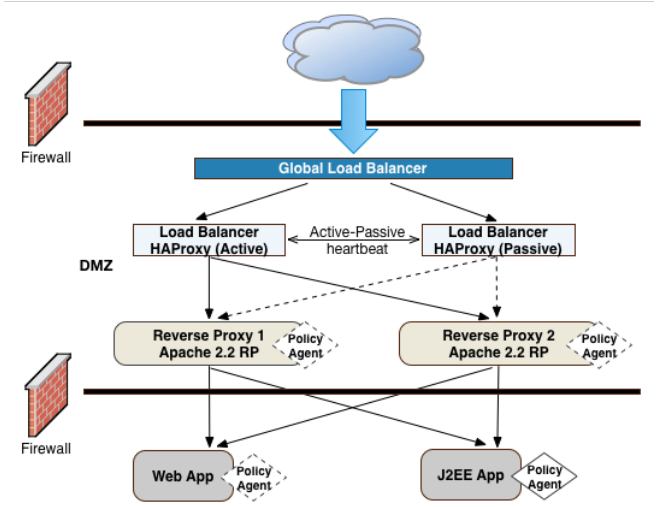


Another advantage to reverse proxies is that they allow access to only those endpoints required for your applications. If you need the authentication user interface and OAuth2/OpenID Connect endpoints, then you can expose only those endpoints and no others. A good rule of thumb is to check which functionality is required for your public interface and then use the reverse proxy to expose only those endpoints.

A third advantage to reverse proxies is when you have applications that sit on non-standard containers for which ForgeRock does not provide a native agent. In this case, you can implement a reverse proxy in your Web tier, and deploy a policy agent on the reverse proxy to filter any requests.

Figure 3.3, "Frontend Load Balancers and Reverse Proxies with Agent" shows a simple topology diagram of your Web tier with agents deployed on your reverse proxies. The dotted policy agents indicate that they can be optionally deployed in your network depending on your configuration, container type, and application.

Figure 3.3. Frontend Load Balancers and Reverse Proxies with Agent



3.2.4. OpenIG

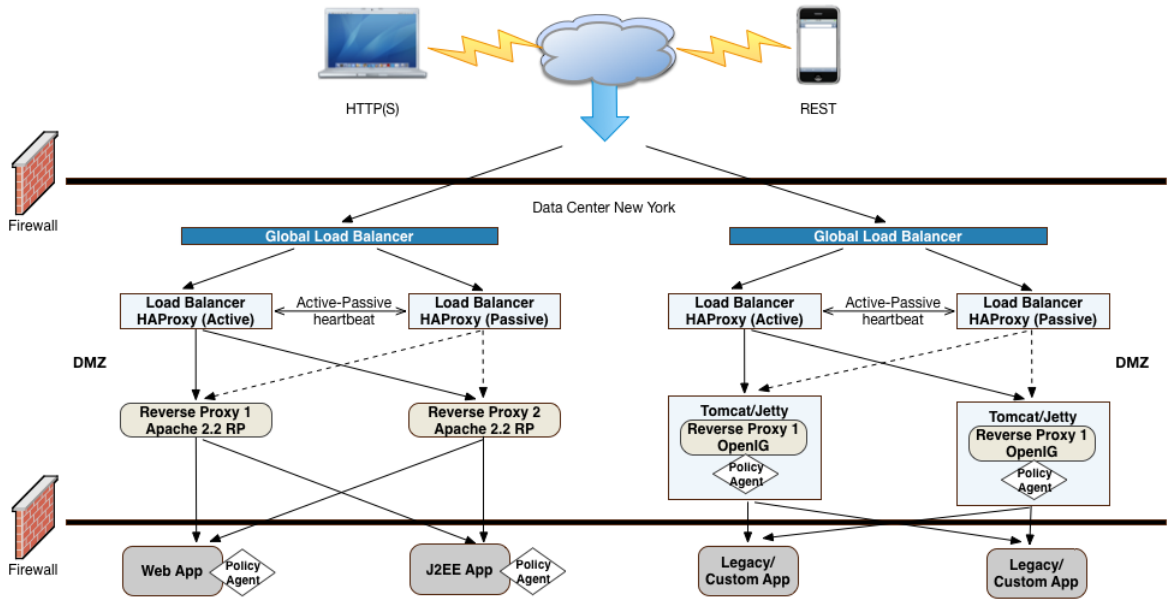
ForgeRock's application gateway product, OpenIG, is a versatile, Java EE servlet-based reverse proxy server. OpenIG allows you to integrate your applications into existing networks using current standards, such as SAML 2.0 federation, OAuth 2.0 and OpenID Connect 1.0, custom or legacy applications, or other vendor solutions without altering native applications. With OpenIG, you can extend OpenAM's authentication and authorization (policy) services to provide SSO across your mobile, social, partner, and Web applications.

OpenIG provides a set of servlet filters that you can use as-is or chained together with other filters to provide complex operations processing on HTTP requests and responses. You can also write your own custom filters for legacy or custom applications. For more information, see the OpenIG documentation.

You can deploy OpenIG on Tomcat or Jetty servers, allowing it to intercept the HTTP requests and carry out filtering operations on each request, and then log the user directly into the application. In such cases, you can deploy a policy agent for authorization purposes on the request.

However, in the example deployment, you may not need to deploy a policy agent as OpenIG functions strictly as a reverse proxy in the DMZ. The inclusion of the policy agent in the illustration only indicates that you can deploy a policy agent with OpenIG when deployed on a Web container or app server.

Figure 3.4. Front End Load Balancers



Note

Some authentication modules may require additional user information to authenticate, such as the IP address where the request originated. When OpenAM is accessed through a load balancer or proxy layer, you can configure OpenAM to consume and forward this information with the request headers.

3.2.5. SSL Termination

One important security decision ia whether to terminate SSL or offload your SSL connections at the load balancer. Offloading SSL effectively decrypts your SSL traffic before passing it on as HTTP or at the reverse proxy. Another option is to run SSL pass-through where the load balancer does not decrypt the traffic but passes it on to the reverse proxy servers, which are responsible for the decryption. The other option is to deploy a more secure environment using SSL everywhere within your deployment.

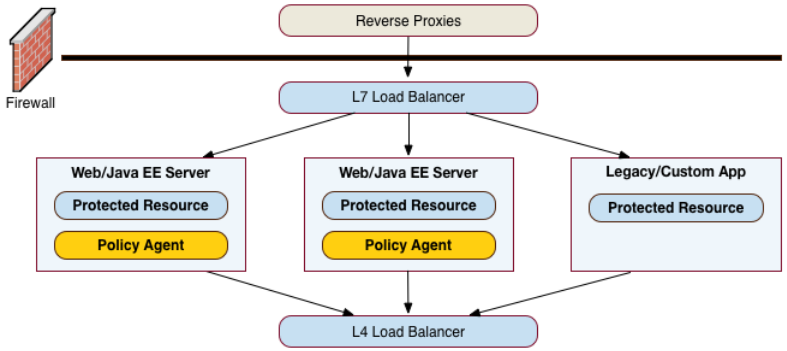
3.3. About the Application Tier

The application tier is where the protected resources reside on Web containers, application servers, or legacy servers. The policy agents intercept all access requests to the protected resources on the

Web or app server and grants access to the user based on policy decisions made on the OpenAM servers. For a list of supported Web application containers, see Section 2.4, "Web Application Container Requirements" in the *Release Notes*.

Because OpenAM is Java-based, you can install the server on a variety of platforms, such as Linux, Solaris, and Windows. For a list of platforms that OpenAM has been tested on, see Section 2.2, "Operating System Requirements" in the *Release Notes*.

Figure 3.5. App Server Deployment



OpenAM provides a cookie (default: `amlbcoookie`) for *sticky load balancing* to ensure that the load balancer optimally routes requests to the OpenAM servers. When the client sends an access request to a resource, the policy agent redirects the client to an authentication login page. Upon successful authentication, the policy agent forwards the request via the load balancer to one of the OpenAM servers.

In OpenAM deployments with stateful sessions, the OpenAM server that authenticated the user maintains the session in its in-memory cache. Best performance is achieved when the load balancer sends requests to the server that authenticated the user. If the request is sent to another OpenAM server, that server must retrieve the session from the Core Token Service token store.

Directing OpenAM requests to the server that authenticated the user is preferable only for OpenAM deployments that use stateful sessions. Because stateless sessions reside in the session token cookie (default: `iPlanetDirectoryPro`) rather than in the Core Token Service token store, any OpenAM server in a cluster can handle a request with a stateless session without retrieving the session from the CTS token store.

To direct requests to the OpenAM server that authenticated the user, the load balancer should use the value specified in the OpenAM load balancer cookie, `amlbcookie`, which you can configure to uniquely identify a server within a site.

The load balancer inspects the sticky cookie to determine which OpenAM server should receive the request. This ensures that all subsequent requests involving the session are routed to the correct server.

3.4. Policy Agents

Policy agents are components that are installed on Web containers or application servers to protect the resources deployed there. Policy agents function as a type of gatekeeper to ensure clients are authenticated and authorized to access the resource as well as enforce SSO with registered devices.

OpenAM provides two main policy agents: Web Policy Agent (WPA) and J2EE Policy Agent. The Web Policy Agent is a native plugin to a Web server and is distributed as a zip file. Web policy agents filter requests for Web server resources without any changes to the resources. The J2EE Policy Agent is set up as a servlet filter within the application server. Protected Java EE application configurations must be changed to filter requests through the Java EE policy agent.

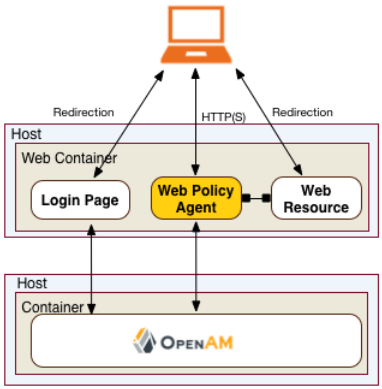
Both policy agents have the following features:

- **Cookie Reset**. Policy agents can be configured to reset any number of cookies in the session before the client is redirected for authentication. This feature is typically used when the policy agent is deployed with a parallel authentication mechanism and cookies need to be reset. Make sure that the `name`, `domain`, and `path` properties are defined.
- **Disable Policy Evaluation**. Policy agents act as a policy enforcement point (PEP) during the authorization phase for a client application. This feature is typically used when the policy agent is only used for SSO and does not require a policy evaluation request to OpenAM.
- **Not-Enforced URLs/URIs List**. Policy agents protect all resources on the Web server or in a Web application that it serves and grants access only if the client has been authenticated and authorized to access the resources. However, there may be some resources, such as public HTML pages, graphics, or stylesheet files that do not require policy evaluation. To account for such files, the policy agent maintains a Not-Enforced URL list, specifying the URLs or resources that are available to any user. J2EE agents use a Not-Enforced URI list.
- **URL Correction**. OpenAM is aware of the access management network and its registered clients, implementing a fully qualified domain name (FQDN) mapper that can be configured to correct invalid URLs. It also holds a list of invalid URLs and compares them to the URL the policy agent is attempting to access.
- **Attribute Injection Into Requests**. Policy agents can be configured to inject user profile attributes into cookies, requests, and HTTP headers.
- **Notifications**. Both agents have the ability to receive configuration notifications from OpenAM. In deployments with stateful sessions, both agents can receive session notifications from OpenAM.
- **Cross-Domain Single Sign-On**. In deployments with stateful sessions, both agents can be configured for cross-domain single sign-on (CDSSO).

3.4.1. Web Policy Agents

A Web policy agent is an installable component on a Web server that is configured to be called by the Web server when a client requests access to a protected resource on a Web site. The Web policy agent runs authentication and authorization services to allow the user access to a protected resource.

Figure 3.6. Web Policy Agent

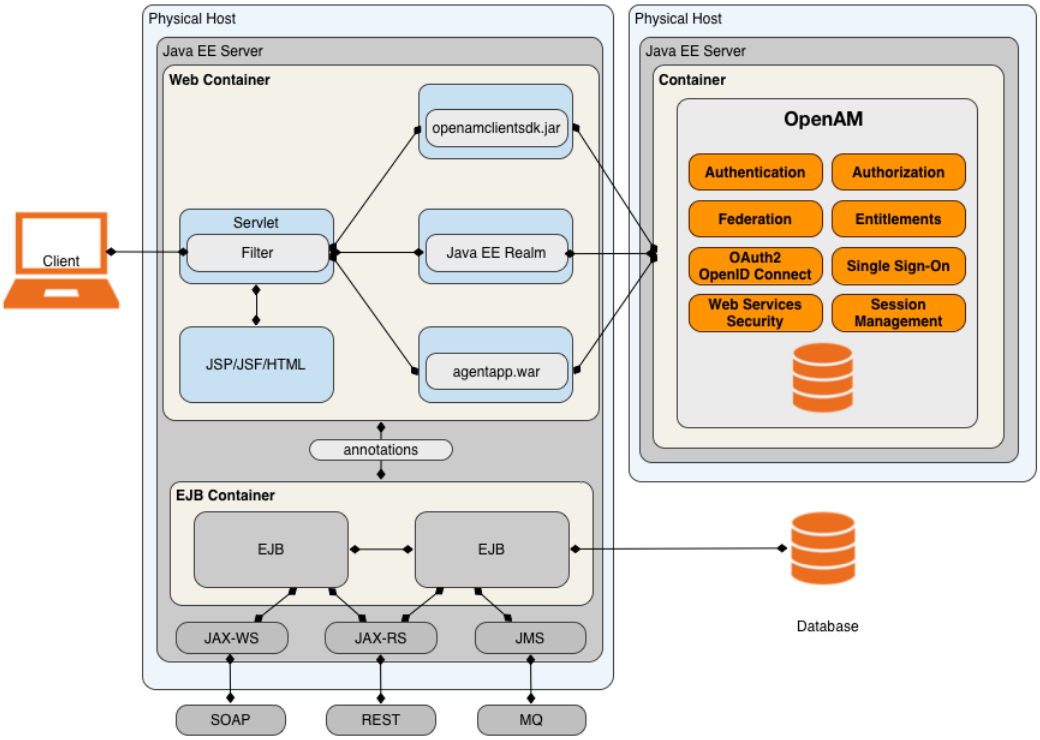


Web Policy Agents are supported on different architectures, although not all Web server types and architecture combinations are supported. You can view the list of supported Web policy agents in the OpenAM Web Policy Agent documentation.

3.4.2. Java EE Policy Agents

The J2EE policy agent is made up of a servlet filter and a J2EE realm. The servlet filter manages authentication and URL-based authorization to the protected application and implements SSO. The filter must be integrated into the application using the application's Web deployment descriptor. The J2EE realm is configured into the security settings of the application server and maps J2EE roles to OpenAM users and groups.

Figure 3.7. Java EE Policy Agent



OpenAM provides a variety of J2EE policy agents for application servers. You can view the list of supported Java EE policy agents in the OpenAM Java EE Policy Agent documentation.

3.5. Sites

OpenAM provides the capability to logically group two or more redundant OpenAM servers into a *site*, allowing the servers to function as a single unit identified by a site ID across a LAN or WAN. When you set up a single site, you place the OpenAM servers behind a load balancer to spread the

load and provide system failover should one of the servers go down for any reason. You can use round-robin or load average for your load balancing algorithms.

Note

Round-robin load balancing should only be used for a first time access of OpenAM or if the `amlbcookie` is not set; otherwise, cookie-based load balancing should be used.

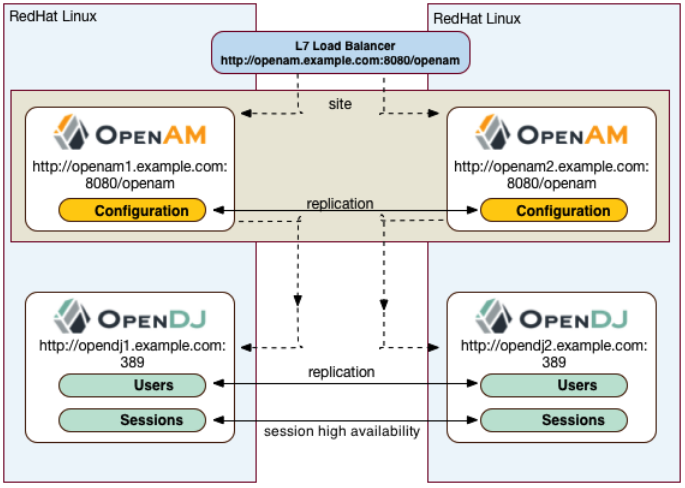
In OpenAM deployments with stateful sessions, the set of servers comprising a site provides uninterrupted service. Stateful sessions, which are stored in OpenAM's CTS, are shared among all servers in a site. If one of the OpenAM servers goes down, other servers in the site read the user session data from the CTS store, allowing the user to run new transactions or requests without re-authenticating to the system.

OpenAM provides uninterrupted session availability if all servers in a site use the same Core Token Service, which is replicated across all servers. For more information, see Chapter 3, "*Implementing the Core Token Service*" in the *Installation Guide*.

OpenAM deployments with stateless sessions do not use the CTS for session storage and retrieval to make sessions highly available. Instead, sessions are stored in HTTP cookies on clients.

Figure 3.8, "Application Tier Deployment" shows a possible implementation using RedHat Linux servers with OpenAM installed on each server. You can implement routing software, like Keepalived in such a deployment. If you require L7 load balancing, you can consider many other software and hardware solutions. OpenAM relies on OpenDJ's SDK for load balancing, failover, and heartbeat capabilities to spread the load across the directory servers or to throttle performance.

Figure 3.8. Application Tier Deployment



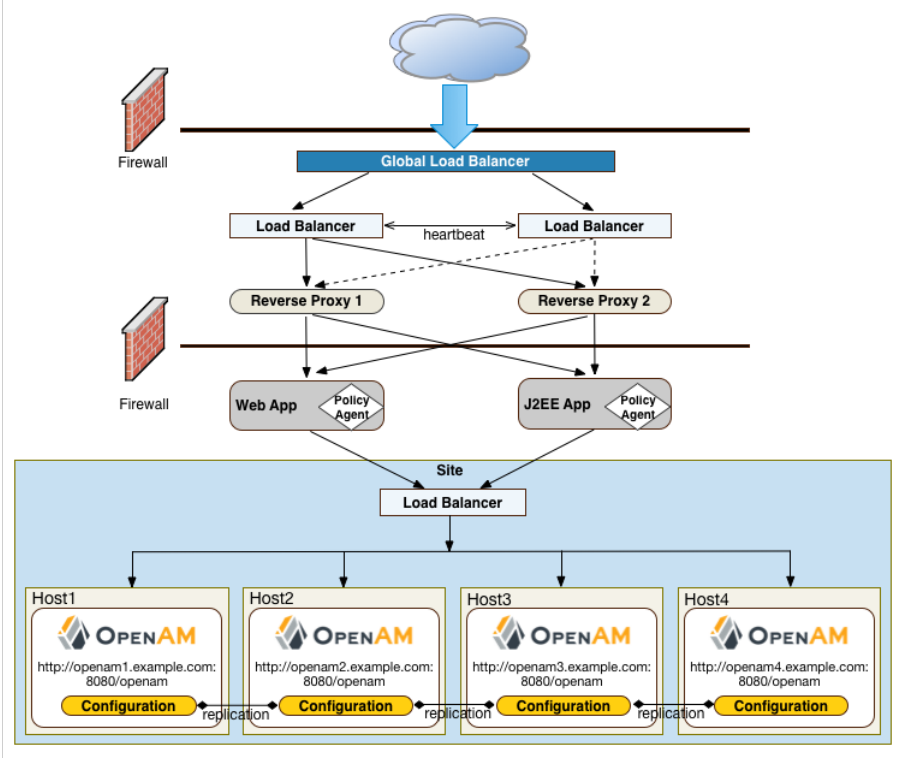
Note

When protecting OpenAM with a load balancer or proxy service, configure your container so that OpenAM can trust the load balancer or proxy service.

One possible configuration (seen in Figure 3.9, "Site Deployment With a Single Load Balancer") is to set up a load balancer with multiple OpenAM servers. You configure the load balancer to be sticky using the value of the OpenAM cookie, `amlbcookie`, which routes client requests to that primary server. If the primary OpenAM server goes down for any reason, it fails over to another OpenAM server. Session data also continues uninterrupted if a server goes down as it is shared between OpenAM servers. You must also ensure that the container trusts the load balancer.

You must determine if SSL should be terminated on the load balancer or communication be encrypted from the load balancer to the OpenAM servers.

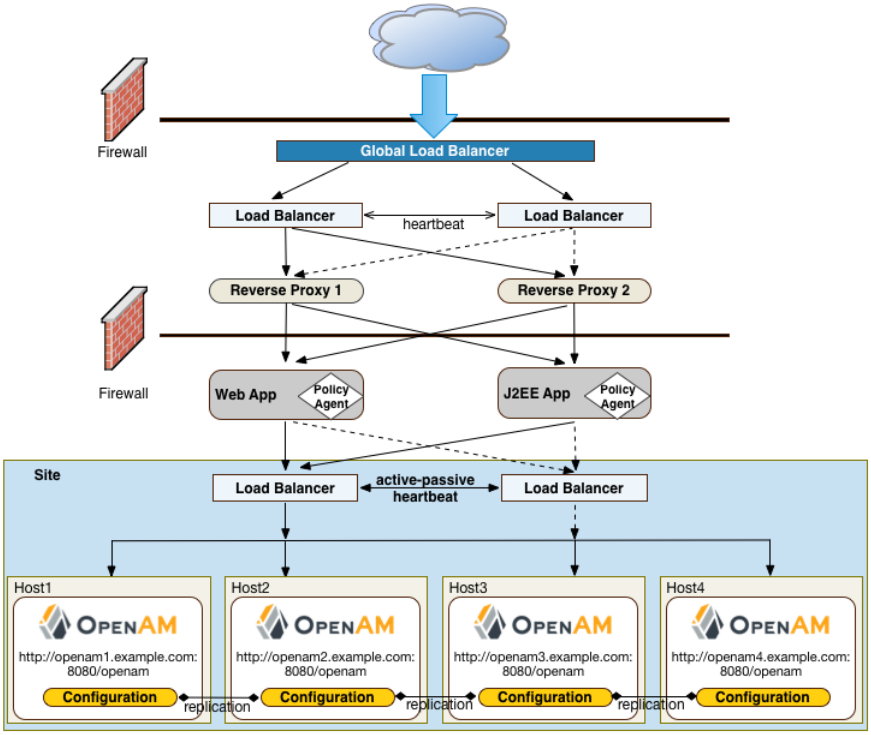
Figure 3.9. Site Deployment With a Single Load Balancer



One problem with Figure 3.9, "Site Deployment With a Single Load Balancer" is that the load balancer is a single point of failure. If the load balancer goes down, then the system becomes inoperable.

To make the deployment highly available, you can set up another variation of the deployment by fronting more than one load balancer to the set of OpenAM servers in an active/passive configuration that provides high availability should one load balancer go down for an outage.

Figure 3.10. Site Deployment With Multiple Load Balancers



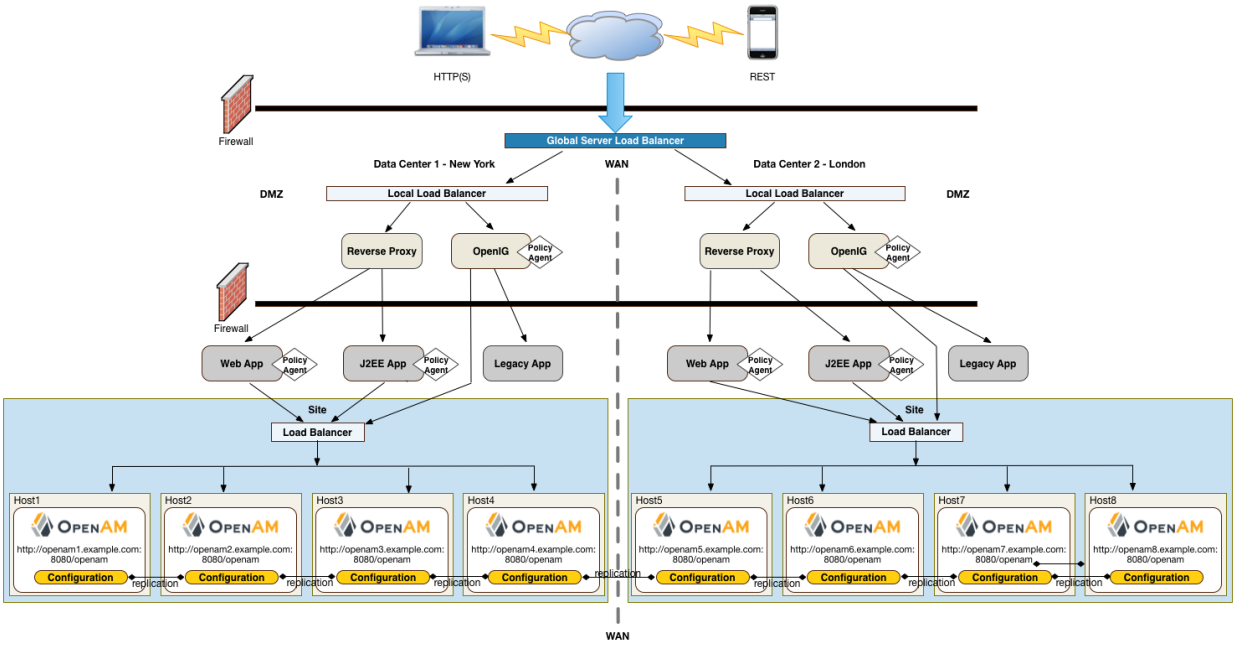
3.5.1. Multiple Sites

Another deployment variation is to set up multiple redundant sites, typically across a WAN network, which provides high availability for stateful sessions. This setup can be seen in Figure 3.11, "Site Deployment With Multiple Sites" If the load balancer in one site goes down, the other site can resume processing requests with the authenticated user session running without interruption. If an OpenAM server goes down, it fails over to another OpenAM server while also keeping the authenticated user session active with uninterrupted service.

Policy agent configuration and other configuration data can be shared among multiple, redundant sites, so that if one site fails, the other site can continue without requiring re-logging.

For optimum performance, you want to keep sites local to your geographical location with session high availability taking place only within a data center. The possible loss of a data center means clients must reestablish sessions, which may be an acceptable trade-off given the performance cost of highly-replicated systems across multiple sites over WAN. You must determine the optimum topology based on your performance and availability objectives.

Figure 3.11. Site Deployment With Multiple Sites



For more information, see Section 2.2, "Installing Multiple Servers" in the *Installation Guide*.

3.6. Back End Directory Servers

Each OpenAM server comes out-of-the-box with an embedded OpenDJ directory server that you can configure to store policies, configuration data, identity data, and CTS tokens. The embedded directory server is best suited for small systems or for evaluation purposes. It is not generally recommended for large-scale production systems.

- **Identity Data Stores**. For identity repositories, OpenAM provides built-in support for LDAP and JDBC storage systems. You can implement a number of different directory server vendors for storing your identity data, allowing you to configure your directory servers in a number of deployment typologies. For a list of supported data stores, see Section 2.5, "Data Store Requirements" in the *Release Notes*.

When configuring external LDAP Identity data stores, you must manually carry out additional installation tasks that could require a bit more time for the configuration process. For example, you must manually add schema definitions, access control instructions (ACIs), privileges for reading and updating the schema, and resetting user passwords. For more information, see Section 1.4.1, "Preparing an External Identity Repository" in the *Installation Guide*.

If OpenAM does not support your particular identity data store type, you can develop your own customized plugin to allow OpenAM to run method calls to fetch, read, create, delete, edit, or authenticate to your identity store data. For more information, see Section 3.3, "Customizing Identity Data Stores" in the *Setup and Maintenance Guide*.

You can configure the Data Store authentication module to require the user to authenticate against a particular identity data store for a specific realm. OpenAM associates a realm with at least one identity repository and authentication process. When you initially configure OpenAM, you define the identity repository for authenticating at the top level realm (/), which is used to administer OpenAM. From there, you can define additional realms with different authentication and authorization services as well as different identity repositories if you have enough identity data. For more information, see Chapter 2, "*Setting Up Realms*" in the *Setup and Maintenance Guide*.

- **Configuration Data Stores**. OpenAM stores configuration data in the embedded OpenDJ directory server. Configuration data includes authentication information that defines how users and groups authenticate, identity data store information, service information, policy information for evaluation, and partner server information that can send trusted SAML assertions. For a list of supported data stores, see Section 2.5, "Data Store Requirements" in the *Release Notes*.

  The embedded OpenDJ directory server may be sufficient for your system, but you may want to deploy an external configuration store if required for large-scale systems with many policies or many realms. Like external identity stores, you must manually add schema definitions, ACIs, privileges for reading and updating the schema, and indexes for attributes used to access the configuration data.

  SAML keys are stored in the configuration store and are thus replicated. Also, OpenAM's signing keys are shipped with a test certificate. If you upgrade the keystore, you need to redistribute the certificates to all nodes so that they can continue to communicate with each other. For more information, see Chapter 5, "*Setting Up Keys and Keystores*" in the *Setup and Maintenance Guide*.

- **CTS Data Stores**. The CTS provides persistent and highly available token storage for OpenAM stateful sessions, OAuth 2.0, UMA, stateless session blacklist (if enabled), SAML 2.0 tokens for Security Token Service token validation and cancellation (if enabled), push notification for authentication, and cluster-wide notification.

  CTS traffic is volatile compared to configuration data, so deploying CTS as a dedicated external data store is advantageous for systems with many users and many sessions. For more information, see Chapter 3, "*Implementing the Core Token Service*" in the *Installation Guide*.

When configuring multiple external directory servers, make sure to deploy them with an active/passive load balancing algorithm. This setup eliminates the possibility of directory read-write errors if replication is not quick enough. For example, if an attribute is updated on OpenDJ-1 but read

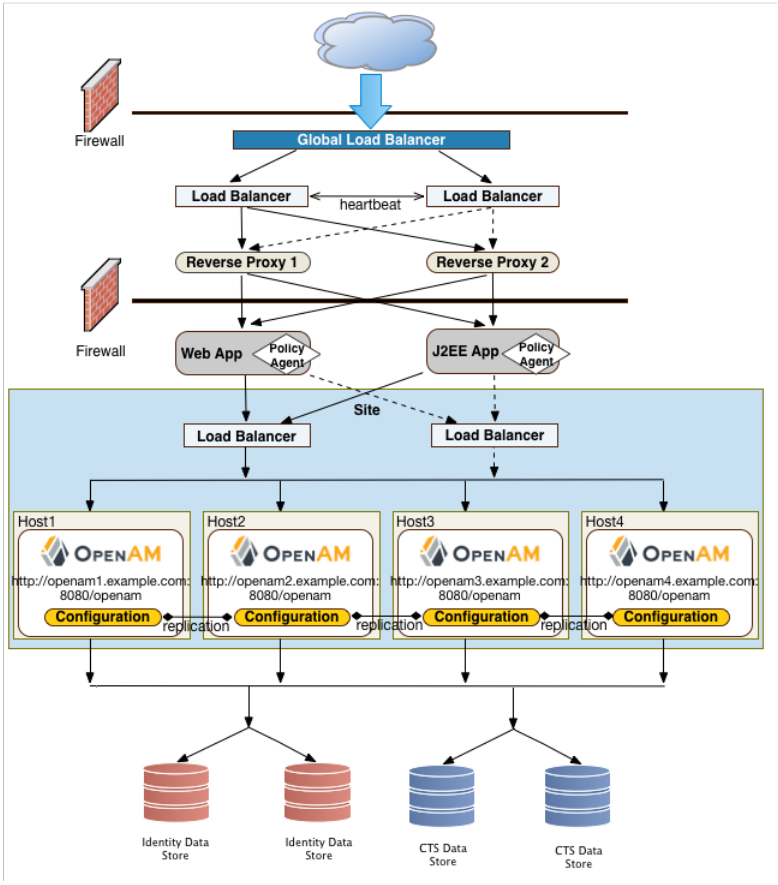
from OpenDJ-2, and if replication is not quick enough and the attribute is not written or updated in OpenDJ-2, an error could result. For the CTS token store, you can also use an affinity deployment, which allows you to scale across multiple writable directory server instances. See Section 3.1, "General Recommendations for CTS Configuration" in the *Installation Guide* for more information about CTS affinity deployments.

Figure 3.12, "Site Deployment With External Datastores" shows a basic back end deployment with separate external identity, configuration, and CTS data stores. You can use load balancers to spread the load or throttle performance for the external data stores. Although not shown in the diagram, you can also set up a directory tier, separating the application tier from the repositories with another firewall. This tier provides added security for your identity repository or policy data.

Note

ForgeRock recommends that you use the OpenAM's embedded OpenDJ directory server as the configuration data store and only set up an external configuration store if necessary.

Figure 3.12. Site Deployment With External Datastores



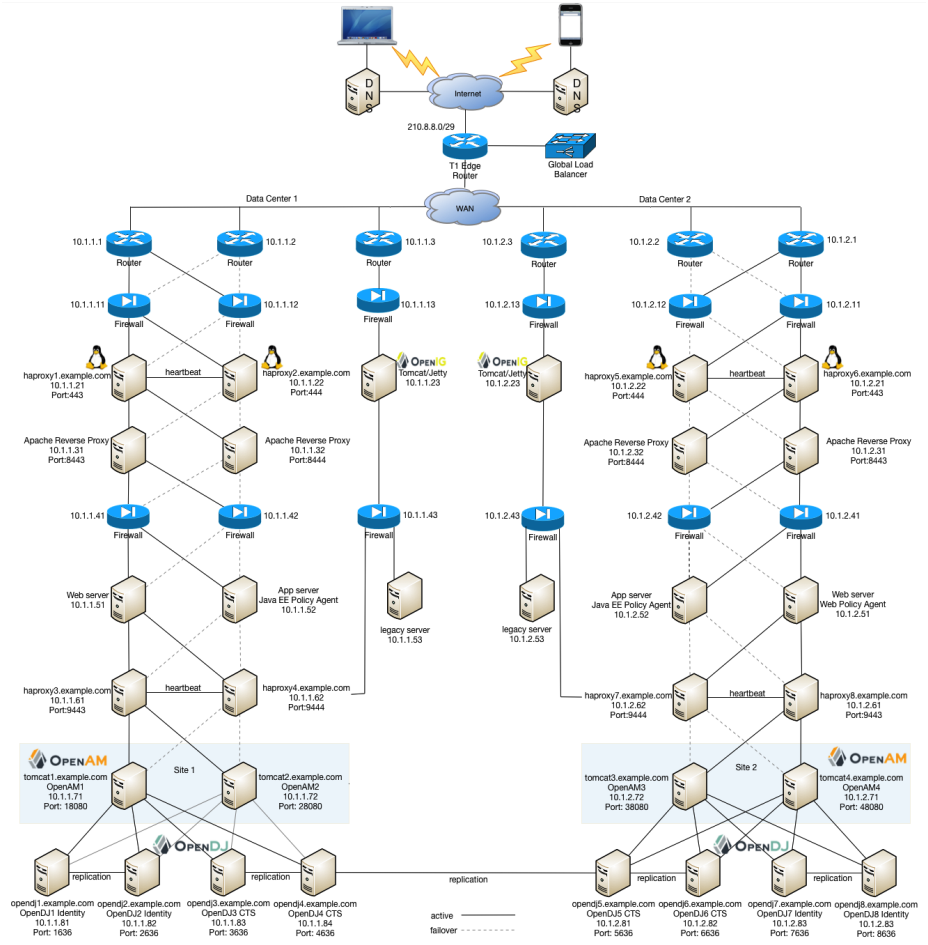
3.7. Example Topology Configuration Diagram

Figure 3.13, "Example Deployment Configuration Diagram" shows a simplified configuration diagram of the example deployment presented in this chapter (shown in Figure 3.1, "Deployment Example"). The example deploys the various servers on Linux hosts.

The firewalls can be a hardware or software solution or a combination firewall-router can be implemented in the deployment. The local load balancers are implemented using HAProxy servers in an active-passive configuration. You can also use Linux Keepalived for software load balancing or one of the many other solutions available. The Web and application servers have the Web policy agent and Java EE policy agent installed on each server respectively. OpenAM is deployed on Tomcat hosted on a Linux server. Within each datacenter, the OpenAM servers are configured as sites for failover and stateful session high availability.

The directory servers are OpenDJ servers that store identity and CTS data. For presentation purposes only, the configuration data is assumed to be stored within the embedded directory store on each OpenAM server. The OpenIG example does not show redundancy for high availability also due to presentation purposes.

Figure 3.13. Example Deployment Configuration Diagram



3.8. Realms

The previous sections in this chapter present the logical and physical topologies of an example highly available OpenAM deployment, including the clustering of servers using *sites*. One important configuration feature of OpenAM is its ability to run multiple client entities to secure and manage applications through a single OpenAM instance.

OpenAM supports its multiple clients through its use of *realms*. You configure realms within OpenAM to handle different sets of users to whom you can set up different configuration options, storage requirements, delegated administrators, and customization options per realm.

Typically, you can configure realms for customers, partners, or employees within your OpenAM instance, for different departments, or for subsidiaries. In such cases, you create a global administrator who can delegate privileges to realm administrators, each specifically responsible for managing their respective realms.

Chapter 4

Sizing Hardware and Services For Deployment

This chapter covers sizing servers, network, storage, and service levels required by your OpenAM deployment.

4.1. Sizing For Availability

Any part of a system that can fail eventually will fail. Keeping your service available means tolerating failure in any part of the system without interrupting the service. You make OpenAM services highly available through good maintenance practices and by removing single points of failure from your architectures.

Removing single points of failure involves replicating each system component, so that when one component fails, another can take its place. Replicating components comes with costs not only for the deployment and maintenance of more individual components, but also for the synchronization of anything those components share. Due to necessary synchronization between components, what you spend on availability is never fully recovered as gains in capacity. (Two servers cannot do quite twice the work of one server.) Instead you must determine the right trade offs for the deployment.

To start thinking about the trade offs, answer the following questions.

- What is the impact of the OpenAM service becoming unavailable?

  In an online system this could be a severe problem, interrupting all access to protected resources. Most deployments fall into this category.

  In an embedded system protecting local resources, it might be acceptable to restart the service.

  Deployments that require always-on service availability require some sort of load balancing solution at minimum between OpenAM and OpenAM client applications. The load balancer itself must be redundant, too, so that it does not become a single point of failure. Illustrations in Chapter 3, "*Example Deployment Topology*", show multiple levels of load balancing for availability and firewalls for security.

- Is the service critical enough to warrant deployment across multiple sites?

  OpenAM allows you to deploy replicated configurations in different physical locations, so that if the service experiences complete failure at one site, you can redirect client traffic to another site and continue operation. The question is whether the benefit in reducing the likelihood of failure outweighs the costs of maintaining multiple sites.

When you need failover across sites, one of the costs is (redundant) WAN links scaled for inter-site traffic. OpenAM synchronizes configuration and policy data across sites, and by default also synchronizes session data as well. OpenAM also expects profiles in identity data stores to remain in sync. As shown in Chapter 3, "*Example Deployment Topology*", the deployment involves directory service replication between sites.

- What happens if individual session information is lost?

  In OpenAM, stateful sessions are stored in the CTS, so even if a server fails, sessions remain available as long as the CTS is available.

  In deployments where an interruption in access to a protected resource could cause users to lose valuable information, configuring the CTS correctly can prevent the loss. The underlying directory service should replicate sessions stored in CTS. Because session information can be quite volatile—more volatile than configuration and policy data—replication of the CTS across sites can therefore call for more WAN bandwidth, as more information is shared across sites.

Once you have the answers to these questions for the deployment, you can draw a diagram of the deployment, checking for single points of failure to avoid. In the end, you should have a count of the number of load balancers, network links, and servers that you need, with the types of clients and an estimated numbers of clients that access the OpenAM service.

Also, you must consider the requirements for non-functional testing, covered in Section 2.4.8, "Planning Tests". While you might be able to perform functional testing by using a single OpenAM server with the embedded OpenDJ server for user data store, other tests require a more complete environment with multiple servers, secure connections, and so forth. Performance testing should reveal any scalability issues. Performance testing should also run through scenarios where components fail, and check that critical functionality remains available and continues to provide acceptable levels of service.

4.2. Sizing For Service Levels

Beyond service availability, your aim is to provide some level of service. You can express service levels in terms of throughput and response times. For example, the service level goal could be to handle an average of 10,000 authentications per hour with peaks of 25,000 authentications per hour, and no more than 1 second wait for 95% of users authenticating, with an average of 100,000 live SSO sessions at any given time. Another service level goal could be to handle an average of 500 policy requests per minute per policy agent with an average response time of 0.5 seconds.

When you have established your service level goals, you can create load tests for each key service as described in Section 2.4.8.2, "Planning Service Performance Testing". Use the load tests to check your sizing assumptions.

To estimate sizing based on service levels, take some initial measurements and extrapolate from those measurements.

- For a service that handles policy decision (authorization) requests, what is the average policy size? What is the total size of all expected policies?

  To answer these questions, you can measure the current disk space and memory occupied by the configuration directory data. Next, create a representative sample of the policies that you expect to see in the deployment, and measure the difference. Then, derive the average policy size, and use it to estimate total size.

  To measure rates of policy evaluations, you can monitor policy evaluation counts over SNMP. For details, see Section 8.3.2.2, "SNMP Monitoring for Policy Evaluation" in the *Setup and Maintenance Guide*.

- For a service that stores stateful sessions, access, and refresh tokens, or other authentication-related data in the CTS backing store, what is the average session or access/refresh token size? What is the average total size of CTS data?

  As with policy data, you can estimate the size of CTS data by measuring the CTS directory data.

  The average total size depends on the number of live CTS entries, which in turn depends on session and token lifetimes. The lifetimes are configurable and depend also on user actions like logout, that are specific to the deployment.

  For example, suppose that the deployment only handles stateful SSO sessions, session entries occupy on average 20 KB of memory, and that you anticipate on average 100,000 active sessions. In that case, you would estimate the need for 2 GB (100,000 x 20,000) RAM on average if you wanted to cache all the session data in memory. If you expect that sometimes the number of active sessions could rise to 200,000, then you would plan for 4 GB RAM for the session cache. Keep in mind that this is extra memory needed in addition to memory needed for everything else that the system does including running OpenAM server.

  Session data is relatively volatile, as the CTS creates session entries when sessions are created. CTS deletes session entries when sessions are destroyed due to logout or timeout. Sessions are also modified regularly to update the idle timeout. Suppose the rate of session creation is about 5 per second, and the rate of session destruction is also about 5 per second. Then you know that the underlying directory service must handle on average 5 adds and 5 deletes per second. The added entries generate on the order of 100 KB replication traffic per second (5/s x 20 KB plus some overhead). The deleted entries generate less replication traffic, as the directory service only needs to know the distinguished name (DN) of the entry to delete, not its content.

  You can also gather statistics about CTS operations over SNMP. For details, see Section 8.3.2, "Monitoring CTS Tokens" in the *Setup and Maintenance Guide*.

- What level of network traffic do you expect for session change notifications?

  When sizing the network, you must account for change notifications from the Core Token Server token store to the OpenAM server. OpenAM uses the change notifications to ensure consistency between sessions stored authoritatively in the Core Token Service and cached in OpenAM server memory.

In OpenAM deployments, there is no direct network traffic between OpenAM servers.

- What increase in user and group profile size should you expect?

  OpenAM stores data in user profile attributes. OpenAM can use or provision many profile attributes, as described in Procedure 3.1, "To Configure an Identity Data Store" in the *Setup and Maintenance Guide*.

  When you know which attributes are used, you can estimate the average increase in size by measuring the identity data store as you did for configuration and CTS-related data. If you do not manage the identity data store as part of the deployment, you can communicate this information with the maintainers. For a large deployment, the increase in profile size can affect sizing for the underlying directory service.

- How does the number of realms affect the configuration data size?

  In a centrally managed deployment with only a few realms, the size of realm configuration data might not be consequential. Also, you might have already estimated the size of policy data. For example, each new realm might add about 1 MB of configuration data to the configuration directory, not counting the policies added to the realm.

  In a multi-tenant deployment or any deployment where you expect to set up many new realms, the realm configuration data and the additional policies for the realm can add significantly to the size of the configuration data overall. You can measure the configuration directory data as you did previously, but specifically for realm creation and policy configuration, so that you can estimate an average for a new realm with policies and the overall size of realm configuration data for the deployment.

4.3. Sizing Systems

Given availability requirements and estimates on sizing for services, estimate the required capacity for individual systems, networks, and storage. This section considers the OpenAM server systems, not the load balancers, firewalls, independent directory services, and client applications.

Although you can start with a rule of thumb, you see from the previous sections that the memory and storage footprints for the deployment depend in large part on the services you plan to provide. With that in mind, to performance test a basic deployment providing SSO, you can start with OpenAM systems having at least 4 GB free RAM, 4 CPU cores (not throughput computing cores, but normal modern cores), plenty of local storage for configuration, policy, and CTS data, and LAN connections to other OpenAM servers. This rule of thumb assumes the identity data stores are sized separately, and that the service is housed on a single local site. Notice that this rule of thumb does not take into account anything particular to the service levels you expect to provide. Consider it a starting point when you lack more specific information.

4.3.1. Sizing System CPU and Memory

OpenAM services use CPU resources to process requests and responses, and essentially to make policy decisions. Encryption, decryption, signing, and checking signatures can absorb CPU resources when processing requests and responses. Policy decision evaluation depends both on the number of policies configured and on their complexity.

Memory depends on space for OpenAM code, on the number of live connections OpenAM maintains, on caching of configuration data, user profile data, and stateful session data, and importantly, on holding embedded directory server data in memory. The OpenAM code in memory probably never changes while the server is running, as JSPs deployed are unlikely ever to change in production.

The number of connections and data caching depending on server tuning, as described in Section 8.4, "Tuning an Instance" in the *Setup and Maintenance Guide*.

If OpenAM uses the embedded OpenDJ directory server, then the memory needed depends on what you store in the embedded directory and what you calculated as described in Section 4.2, "Sizing For Service Levels". The embedded OpenDJ directory server shares memory with the OpenAM server process. By default, the directory server takes half of the available heap as database cache for directory data. That setting is configurable as described in the OpenDJ directory server documentation.

4.3.2. Sizing Network Connections

When sizing network connections, you must account for the requests and notifications from other servers and clients, as well as the responses. This depends on the service levels that the deployment provides, as described in Section 4.2, "Sizing For Service Levels". Responses for browser-based authentication can be quite large if each time a new user visits the authentication UI pages, OpenAM must respond with the UI page, plus all images and JavaScript logic and libraries included to complete the authentication process. Inter-server synchronization and replication can also require significant bandwidth.

For deployments with sites in multiple locations, be sure to account for configuration, CTS, and identity directory data over WAN links, as this is much more likely to be an issue than replication traffic over LAN links.

Make sure to size enough bandwidth for peak throughput, and do not forget redundancy for availability.

4.3.3. Sizing Disk I/O and Storage

As described in Section 5.1.1, "Disk Storage Requirements", the largest disk I/O loads for OpenAM servers arise from logging and from the embedded OpenDJ directory server writing to disk. You can estimate your storage requirements as described in that section.

I/O rates depend on the service levels that the deployment provides, as described in Section 4.2, "Sizing For Service Levels". When you size disk I/O and disk space, you must account for peak rates

and leave a safety margin when you must briefly enable debug logging to troubleshoot any issues that arise.

Also, keep in mind the possible sudden I/O increases that can arise in a highly available service when one server fails and other servers must take over for the failed server temporarily.

Another option is to consider placing log, configuration, and database files on a different file system to maximize throughput and minimize service disruption due to a file system full or failure scenarios.

Chapter 5

Hardware and Software Requirements

You can configure OpenAM in a wide variety of deployments depending on your security requirements and network infrastructure.

5.1. Hardware Requirements

This section covers hardware requirements for OpenAM.

5.1.1. Disk Storage Requirements

This section considers disk storage requirements for OpenAM server, OpenAM policy agents, and OpenIG gateway.

5.1.1.1. Server Disk Storage Requirements

Disk storage requirements for OpenAM servers depend partly on OpenAM itself and partly on your deployment. Disk storage requirements also depend on the space needed for binaries and configuration data, space for log files and rate of writes for logs, space for directory data and file system requirements when using an embedded OpenDJ directory server.

For initial installation, a few hundred MB is sufficient, not including the downloaded files.

- The OpenAM `.war` file size varies from release to release, but if your container holds one `.war` file and one directory with the contents of the `.war` file, the disk space required is on the order of 300 MB.

  This space requirement remains stable as you use OpenAM.

- The OpenAM configuration directory initially fits in approximately 50 MB of disk space including the embedded OpenDJ directory server.

  This space requirement grows as you use OpenAM.

By default, OpenAM servers write audit logs to flat files under *`config-dir`*`/openam/logs/` . Alternatively, OpenAM servers can write audit logs to `syslog`, or to a relational database.

When using flat-file audit logging, OpenAM lets you configure rotation and purging for logs under`openam/logs/`, so you can effectively cap the maximum disk space used for logs. Make sure, however, that you retain the information you need before logs are purged. Also make sure that your

disk can keep pace with the volume of logging, which can be significant in high volume deployments, as OpenAM logs not only errors, but also access messages.

For details about audit logging configuration, see Chapter 6, "*Setting Up Audit Logging*" in the *Setup and Maintenance Guide*.

By default, OpenAM servers write debug logs to flat files under `config-dir/openam/debug/`. OpenAM lets you configure rotation for debug logs. As you can change debug log levels at runtime when investigating issues, debug log volume is not as predictable as for regular logs. Leave a margin in production environments, so that you can turn up debug log levels to diagnose problems.

For details about debug logging configuration, see Section 9.2, "Debug Logging" in the *Setup and Maintenance Guide*.

When using the embedded OpenDJ directory server, take the following into account:

- OpenDJ is designed to work with local storage for the database, but not for network file system (NFS) nor network-attached storage (NAS) due to some file system locking functions that OpenDJ needs. High performance storage, like solid state drives (SSD), is essential if you need to handle high write throughput.

  By default, OpenAM's configuration directory resides under the `$HOME` directory of the user running the container. `$HOME` directories can be mounted over the network.

  This is not an issue if you are using OpenDJ mainly for configuration data. It can however be a serious problem when you use OpenDJ to back the CTS in a high-volume deployment.

- Embedded OpenDJ directory server log files are stored under `config-dir/opends/logs/`. As for OpenAM, you can configure OpenDJ directory server log rotation and purging. The default cap for access logs is 2 GB.

- OpenAM stores policy information in the configuration directory. The space this takes up depends on the policies you have.

- By default, OpenAM stores CTS information in the configuration directory. The space this takes up depends on the volume of traffic to the server and whether OpenAM is configured for stateless sessions.

- With the default database implementation, OpenDJ database files handling sustained writes can grow to about double their initial size on disk.

- For OpenDJ on Linux systems, enable file system write barriers and ensure the file system journaling mode is ordered to avoid directory database file corruption after crashes or power failures. For details on enabling write barriers and setting the journaling mode for data, see the options for your file system in the **mount** command manual page.

- OpenDJ directory server uses file descriptors when handling connections.

  Defaults can be limited to 1024 file descriptors per user on Linux systems. Consider increasing this limit to at least 64K. For details, see Section 1.1.3, "Setting Maximum File Descriptors" in the *Installation Guide*.

5.1.1.2. Policy Agent Disk Storage Requirements

Policy agents are implemented as libraries or Web applications, and so tend to be small on disk, not more than a few MB.

You can configure policy agents to perform local logging to files, or to send log messages to OpenAM for remote logging. For details, see the *Configuration Reference* for your policy agent.

Debug messages are logged to local files, however, not remotely. Debug logging volume depends on log level. As for OpenAM, leave a margin in production environments so that you can turn up debug log levels to diagnose problems.

5.1.1.3. OpenIG Disk Storage Requirements

The OpenIG Web application can vary in size from release to release. On disk, the `.war` file is under 50 MB. For containers that keep both the `.war` file and an unpacked version, the total size is under 100 MB.

By default, OpenIG configuration resides under the `$HOME` directory of the user who runs the container.

If you use the default log sink, messages are sent to the container logs. Manage those as you would any container logs.

Capture logging and any logging you perform from scriptable filters and handlers can potentially generate significant write traffic. Furthermore, OpenIG does not run rotation or purging for such logs. You must manage any logs OpenIG generates using a `CaptureFilter` or log messages from scriptable filters and handlers.

Both normal log messages and debug messages go to the log sink. As for other components, debug logging volume depends on log level. Leave a margin in production environments so that you can turn up debug log levels to diagnose problems.

5.1.1.4. Disk Storage Recommendations

The following are based on the preceding information in this section. When deciding on disk storage, keep the following recommendations in mind:

- Plan enough space and enough disk I/O to comfortably absorb the load for logs.

  Check your assumptions in testing. For example, make sure that logs are cleaned up so that they do not exceed your space threshold even in long-duration testing.

- For deployments where an embedded OpenDJ directory service handles high throughput, make sure you use a local file system and that the user running the container has enough file descriptors.

- When using local policy agent logs, make sure you have a mechanism in place to clean them up.

- For OpenIG, make sure you turn off `CaptureFilter` logging, scriptable filter, and handler debug logging before moving to production.

5.1.2. Random Access Memory Requirements

OpenAM core services require a minimum JVM heap size of 1 GB and, when running on JDK 7, a minimum permanent generation size of 256 MB. If you are including the embedded OpenDJ directory, OpenAM requires at least a 2 GB heap, as 50% of that space is allocated to OpenDJ.

Note

Ensure that the `Xms` and `Xmx` JVM parameters are set to the same value to prevent a large garbage collection as the memory profile increases from the default up to the `Xms` value. Also, setting `Xms` and `Xmx` to the same value ensures that small controlled garbage collection events minimize application unresponsiveness.

5.2. Software Requirements

The following sections list software requirements for deploying OpenAM server and policy agent software.

5.2.1. Operating System Requirements

ForgeRock supports customers using ForgeRock Access Management server software on the following operating system versions:

Table 5.1. Supported Operating Systems

Operating System	Version
Red Hat Enterprise Linux, Centos, Amazon Linux	6, 7
Amazon Linux	Amazon Linux 2016.09
SuSE	11
Ubuntu	14.04 LTS, 16.04 LTS
Solaris x64	10, 11
Solaris Sparc	10, 11
Windows Server	2012, 2012 R2, 2016

5.2.2. Java Requirements

Table 5.2. JDK Requirements

Vendor	Version
Oracle JDK	7, 8
IBM SDK, Java Technology Edition (Websphere only)	7

Vendor	Version
OpenJDK	8

Important

Support for Oracle JDK 7 and IBM SDK 7 will be removed in a future version.

5.2.3. Web Application Container Requirements

Table 5.3. Web Containers

Web Container	Version
Apache Tomcat	7, 8, 8.5
Oracle WebLogic Server	12c
JBoss Enterprise Application Platform	7.0
WildFly AS	9, 10, 10.1
IBM WebSphere	8.5.5.8+

The web application container must be able to write to its own home directory, where OpenAM stores configuration files.

5.2.4. Data Store Requirements

Table 5.4. Supported Data Stores

Data Store	Version	CTS Datastore	Config Datastore	User Datastore	UMA Datastore
Embedded OpenDJ	4.0	✓	✓	✓	✓
External OpenDJ	2.6, 2.6.4			✓	
	3.0, 3.5, 4.0	✓	✓	✓	✓
Oracle Unified Directory	11g			✓	
Oracle Directory Server Enterprise Edition	11g			✓	
Microsoft Active Directory	2012, 2012 R2, 2016			✓	
IBM Tivoli Directory Server	6.3			✓	

5.2.5. Supported Clients

The following table summarizes supported clients and their minimum required versions:

Table 5.5. Supported Clients

Client Platform	Native Apps[a]	Chrome 33+	Internet Explorer 9+ [b]	Edge 0.1+	Firefox 28+	Safari 6.2+	Mobile Safari
Windows 7 or later	✓	✓	✓	✓	✓		
Mac OS X 10.8 or later	✓	✓			✓	✓	
Ubuntu 12.04 LTS or later	✓	✓			✓		
iOS 7 or later	✓	✓					✓
Android 4.3 or later	✓	✓					

[a] *Native Apps* is a placeholder to indicate OpenAM is not just a browser-based technology product. An example of a native app would be something written to use our REST APIs, such as the sample OAuth 2.0 Token Demo app.
[b]Internet Explorer 9 is the minimum required for end users. For the administration console, Internet Explorer 11 is required.

5.2.6. Java EE Agents Platform Requirements

The following table summarizes platform support.

Table 5.6. Supported Operating Systems & Web Application Containers

Operating Systems (OS)	OS Versions	Web Application Containers & Versions
CentOS Red Hat Enterprise Linux Oracle Linux	5, 6, 7	Apache Tomcat 6, 7, 8 IBM Web Sphere Application Server 8, 8.5 JBoss Enterprise Application Platform 6 JBoss Application Server 7 Jetty 8 (at least 8.1.13) Oracle WebLogic Server 11g, 12c
Microsoft Windows Server	2008, 2008 R2, 2012, 2012 R2	Apache Tomcat 6, 7, 8
Oracle Solaris x64 Oracle Solaris SPARC	10, 11	Apache Tomcat 6, 7, 8 Oracle WebLogic Server 11g, 12c
Ubuntu Linux	12.04 LTS, 14.04 LTS	Apache Tomcat 6, 7, 8 IBM Web Sphere Application Server 8, 8.5 JBoss Enterprise Application Platform 6 JBoss Application Server 7 Jetty 8 (at least 8.1.13)

Operating Systems (OS)	OS Versions	Web Application Containers & Versions
		Oracle WebLogic Server 11g, 12c

5.2.7. Web Policy Agents Platform Requirements

The following table summarizes platform support.

Table 5.7. Supported Operating Systems & Web Servers

Operating Systems (OS)	OS Versions	Web Servers & Versions
CentOS Red Hat Enterprise Linux Oracle Linux	5, 6, 7	Apache HTTP Server 2.2 Apache HTTP Server 2.4
Microsoft Windows Server	2008 R2	Microsoft IIS 7
	2008 R2	Microsoft IIS 7.5
	2012, 2012 R2	Microsoft IIS 8
Oracle Solaris x64 Oracle Solaris SPARC	10, 11	Apache HTTP Server 2.2 Apache HTTP Server 2.4
Ubuntu Linux	12.04 LTS, 14.04 LTS	Apache HTTP Server 2.2 Apache HTTP Server 2.4

Before installing web policy agents on your platform, also make sure that the system provides the required components.

All Systems

If agents use secure connections (SSL, TLS), then also make sure that OpenSSL is installed.

Linux Systems

Before installing web policy agents on Linux, make sure the system can run **gcc** 4.4.7. `libc.so.6` must be available and it must support the GLIBC_2.3 ABI. You can check this by running the following command: **strings libc.so.6 | grep GLIBC_2**.

Microsoft Windows Systems

Before installing the IIS 7 web policy agent on Microsoft IIS 7 or IIS 8, make sure that the optional Application Development component of Web Server (IIS) is installed. In the Windows Server 2012 Server Manager for example, Application Development is a component of Web Server (IIS) | Web Server.

Oracle Solaris Systems

Before installing web policy agents on Solaris 10, make sure you have applied the latest shared library patch for C++, at least 119963-16 on SPARC or 119964-12 on x64. The library is bundled on Solaris 10 update 5 and later.

Chapter 6

Getting Started for Architects and Deployers

The following section provides general instructions to get started with an OpenAM deployment.

6.1. Plan the Deployment

The initial process is the planning phase of your project.

- **Learn about OpenAM**. You can access online information, meet with your ForgeRock Sales representative, go to a seminar, or call ForgeRock about OpenAM's capabilities.

  The following are some general questions that you may want to have answered:

Table 6.1. Initial Questions

Initial Tasks	Done ?	
Understand the access management problems that OpenAM helps to solve	Y	N
Learn how to protect a Web site with OpenAM	Y	N
Get to know the OpenAM software deliverables	Y	N
Get to know the tools for administering OpenAM	Y	N
Get to know the APIs for OpenAM client applications	Y	N
Find out how to get help and support from ForgeRock and partners	Y	N
Find out how to get training from ForgeRock and partners	Y	N
Find out how to keep up to date on new development and new releases	Y	N
Find out how to report problems	Y	N

- **Set up a Demo or Pilot**. View an OpenAM demo or set up a pilot to determine how you want to use OpenAM to protect your site(s). ForgeRock Sales representatives can assist you with a demo or pilot.

- **Attend a Training Class**. ForgeRock presents effective training classes to deploy OpenAM in your environment. See ForgeRock University for more information.

- **Complete the Accreditation Program**. Complete the product-specific ForgeRock Accreditation Program to gain in-depth design and deployment expertise or seek partners who are ForgeRock Accredited Partners.

- **Determine Your Service Level Agreements**. ForgeRock provides a set of standard service level agreements that you can sign up for. ForgeRock also provides custom service level agreements if the standard set does not meet your needs.

Table 6.2. Standard SLAs

Priority	Gold	Silver	Bronze
Urgent (P1)	2 Hour	4 Hour	Next Business Day
High (P2)	4 Hour	8 Hour	2 Business Days
Normal (P3)	6 Hour	Next Business Day	3 Business Days
Low (P4)	Next Business Day	2 Business Days	4 Business Days

- **Determine Your Services**. ForgeRock provides a full, proven-production Identity Management stack to meet your requirements.

Table 6.3. Services

Services Task	Done ?	
Understand the services OpenAM software provides	Y	N
Determine which services to deploy	Y	N
Determine which services the deployment consumes (load balancing, application container, authentication services, configuration storage, profile storage, token/session storage, policy storage, log storage)	Y	N
Determine which services the deployment provides (SSO, CDSSO, SAML Federation IDP/SP, XACML PDP, REST STS, OAuth 2.0/OpenID Connect 1.0, and so forth)	Y	N
Determine which resources OpenAM protects (who consumes OpenAM services)	Y	N

- **Determine Your Deployment Objectives**. OpenAM provides proven performance and security in many production deployments. You should determine your overall deployment objectives.

Table 6.4. Deployment Objectives

Deployment Objectives	Done ?	
Define deployment objectives in terms of service levels (expectations for authentication rates, active sessions maintained, session life cycles, policies managed, authorization decision rates, response times, throughput, and so forth)	Y	N
Define deployment objectives in terms of service availability (OpenAM service availability, authentication availability, authorization decision availability, session availability, elasticity)	Y	N
Understand how OpenAM services scale for high availability	Y	N
Understand the restrictions in an OpenAM deployment that uses stateless sessions	Y	N
Plan for availability (number of sites and servers, load balancing and OpenAM software configuration)	Y	N

Deployment Objectives	Done ?	
Define the domains managed and domains involved in the deployment	Y	N
Define deployment objectives for delegated administration	Y	N
Agree with partners for federated deployments on circles of trust and terms	Y	N

- **Plan Sizing**. At this stage, you should determine the sizing estimates for your deployment. ForgeRock Sales Engineers can assist you in this task.

Table 6.5. Sizing

Sizing	Done ?	
Derive sizing estimates from service levels and availability	Y	N
Understand how to test sizing estimates (load generation tools?)	Y	N
Size servers for OpenAM deployment: CPU	Y	N
Size servers for OpenAM deployment: Memory	Y	N
Size servers for OpenAM deployment: Network	Y	N
Size servers for OpenAM deployment: I/O	Y	N
Size servers for OpenAM deployment: Storage	Y	N
Quantify impact on external services consumed (LDAP, other auth services, load balancing, and so forth)	Y	N
Plan testing and acceptance criteria for sizing	Y	N

- **Plan the Topology**. Plan your logical and physical deployment.

Table 6.6. Topology Planning

Topology	Done ?	
Specify the logical and physical deployment topology (show examples of each)	Y	N
Determine whether to use the embedded or external directory service for configuration, CTS, and user data	Y	N
Plan installation of OpenAM services (including external dependencies)	Y	N
Plan installation of OpenAM policy agents, Fedlets, and OpenIG (might be done by partner service providers)	Y	N
Plan integration with client applications	Y	N
Plan customization of OpenAM (XUI, user profile attributes, authentication modules, identity repositories, OAuth 2.0 scope handling, OAuth 2.0 response types, post-authentication actions, policy evaluation, session quota exhaustion actions, policy evaluation, identity data storage, OpenAM service, custom logger, custom Web policy agents).	Y	N

- **Plan Security**. At this stage, you must plan how to secure your deployment.

Table 6.7. Security

Security	Done ?	
Understand security guidelines, including legal requirements	Y	N
Change default settings and administrative user credentials	Y	N
Protect service ports (Firewall, Dist Auth UI, reverse proxy)	Y	N
Turn off unused service endpoints	Y	N
Separate administrative access from client access	Y	N
Secure communications (HTTPS, LDAPS, secure cookies, cookie hijacking protection, key management for signing and encryption)	Y	N
Determine if components handle SSL acceleration or termination	Y	N
Securing processes and files (e.g. with SELinux, dedicated non-privileged user and port forwarding, and so forth)	Y	N

- **Post-Deployment Tasks**. At this stage, you should plan your post-deployment tasks to sustain and monitor your system.

Table 6.8. Post-Deployment Tasks

Post Deployment Tasks	Done ?	
Plan administration following OpenAM deployment (services, agents/OpenIG, delegated administration)	Y	N
Plan monitoring following deployment	Y	N
Plan how to expand the deployment	Y	N
Plan how to upgrade the deployment	Y	N

6.2. Install the Components

The installation process requires that you implement your deployment plan.

- **Plan the Overall Deployment**. The initial planning step involves establishing the overall deployment. You should determine who is responsible for each task and any external dependencies.
- **Determine What To Install**. Based on your deployment plan, determine what you need to install.
- **Determine Your System Requirements**. Based on your deployment plan, determine your system requirements.
- **Prepare the Operating System**. Prepare your operating system, depending on the OS: Linux, Solaris, Windows, Cloud (Amazon EC2, OpenStack, and so forth), Virtual Machines (VMWare, Xen, Hyper-V, and so forth)

- **Prepare the Java Environment**. Prepare your Java environment, depending on your vendor type: Oracle, IBM, OpenJDK.
- **Prepare the App Server**. Prepare your application server, depending on type: Apache Tomcat, JBoss 4/5, WildFly, Jetty, Oracle WebLogic, IBM WebSphere. Also, prepare each app server for HTTPS.
- **Prepare the Directory Servers**. Prepare the configuration directory server, OpenDJ for the core token service (CTS), and the LDAP identity repository. For information on installing data repositories, see Chapter 1, "*Preparing for Installation*" in the *Installation Guide*.
- **Obtain the OpenAM Software**. The *ForgeRock BackStage* website hosts downloadable versions of OpenAM, including a `.zip` file with all of the OpenAM components, the `.war` file, OpenAM tools, the configurator, policy agents, OpenIG, and documentation. Verify that you review the Software License and Subscription Agreement presented before you download OpenAM files.
- **Configure OpenAM**. Install and configure OpenAM with or without the AM console, the setup tools (configurator), configuration tools (`ssoadm`, `ampassword`, `amverifyarchive`), or set up your scripted install and configuration of OpenAM. For information on installing OpenAM, see the Installation Guide.
- **Set up your Realms**. Within OpenAM, set up your realms and realm administrators if any. For more information on realms, see Chapter 2, "*Setting Up Realms*" in the *Setup and Maintenance Guide*.
- **Configure Session State**. Configure sessions as stateful or stateless. For more information on session state, see Section 1.8.1, "Session State" in the *Authentication and Single Sign-On Guide*.
- **Install Another OpenAM Instance**. Set up an identical instance of your first OpenAM instance. For information on installing multiple OpenAM servers, see Section 2.2, "Installing Multiple Servers" in the *Installation Guide*.
- **Secure OpenAM**. Configure OpenAM to access external resources over HTTPS and LDAPS. Set up secure cookies and certificates. For more information, see Chapter 4, "*Securing Installations*" in the *Installation Guide*.
- **Configure High Availability**. Configure the load balancers, site(s), and reverse proxies. Configure OpenAM for session high availability and server failover. For information about deploying OpenAM behind a load balancer and configuring sites, see Section 2.2, "Installing Multiple Servers" in the *Installation Guide*. For an example of a reverse proxy with OpenAM, see *Simple Apache Reverse Proxy for OpenAM with Certificate-Based Authentication*.
- **Prepare the Policy Agent Profiles**. Prepare the policy agent profile, agent authenticator, policy agent configuration, bootstrap configuration for a Java EE or Web policy agent. For more information, see Creating Agent Profiles in the *OpenAM Java EE Policy Agent Guide* or Creating Agent Profiles in the *OpenAM Web Policy Agent Guide*.
- **Install the Policy Agents**. Install the policy agents depending on the app server or Web server type. For app servers, Apache Tomcat, JBoss, Jetty, Oracle WebLogic, IBM WebSphere. For Web servers, Apache , Microsoft IIS. Set up any script installations of the policy agents. For more information, see the OpenAM Web Policy Agent documentation.

- **Customizing the OpenAM User Interface**. Customize OpenAM for your organization. For information on customizing the OpenAM user interface, see the UI Customization Guide.
- **Install OpenIG**. Determine which OpenIG deliverable to install (whether federation is involved). Prepare the Apache Tomcat, JBoss, Jetty, Oracle WebLogic app servers for installation. Install OpenIG. See the OpenIG documentation for details.
- **Plan Application and Host Backup**. Determine your backup strategy including LDIF exports, file system backups, tar files, and so forth. Also, consider log rotation and retention policies. For more information on backups, see Section 8.1, "Backing Up and Restoring Configurations" in the *Setup and Maintenance Guide*.
- **Plan an OpenAM Upgrade**. You should know what is new or fixed in an upgrade version as well as the differences and compatibility between the current version and an upgrade. Know the limitations of an upgrade version. Plan a live upgrade without service interruption. Plan an offline upgrade with service interruption. Plan the test of the upgrade and revert a failed upgrade. For more information on upgrades, see the Upgrade Guide.
- **Upgrade OpenAM**. Upgrade OpenAM and other instances with or without the AM console. Upgrade the setup tools (configurator), configuration tools (`ssoadm`, `ampassword`, `amverifyarchive`), and the Java EE and/or Web policy agents. Upgrade OpenIG. For more information on upgrades, see the Upgrade Guide.
- **Remove OpenAM**. If required, remove OpenAM with or without the AM console. Remove setup and configuration tools. Remove the Java EE and/or Web policy agents. Remove OpenIG. For more information on removing OpenAM, see Chapter 5, "*Removing Installations*" in the *Installation Guide*.

Appendix A. Getting Support

For more information or resources about OpenAM and ForgeRock Support, see the following sections:

A.1. Accessing Documentation Online

ForgeRock publishes comprehensive documentation online:

- The ForgeRock Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.
- ForgeRock core documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

Core documentation therefore follows a three-phase review process designed to eliminate errors:

- Product managers and software architects review project documentation design with respect to the readers' software lifecycle needs.
- Subject matter experts review proposed documentation changes for technical accuracy and completeness with respect to the corresponding software.
- Quality experts validate implemented documentation changes for technical accuracy, completeness in scope, and usability for the readership.

The review process helps to ensure that documentation published for a ForgeRock release is technically accurate and complete.

Fully reviewed, published core documentation is available at http://backstage.forgerock.com/. Use this documentation when working with a ForgeRock Identity Platform release.

A.2. Joining the ForgeRock Community

Visit the Community resource center where you can find information about each project, download trial builds, browse the resource catalog, ask and answer questions on the forums, find community events near you, and find the source code for open source software.

A.3. Getting Support and Contacting ForgeRock

ForgeRock provides support services, professional services, classes through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see https://www.forgerock.com.

ForgeRock has staff members around the globe who support our international customers and partners. For details, visit https://www.forgerock.com, or send an email to ForgeRock at info@forgerock.com.

Glossary

Access control	Control to grant or to deny access to a resource.
Account lockout	The act of making an account temporarily or permanently inactive after successive authentication failures.
Actions	Defined as part of policies, these verbs indicate what authorized subjects can do to resources.
Advice	In the context of a policy decision denying access, a hint to the policy enforcement point about remedial action to take that could result in a decision allowing access.
Agent administrator	User having privileges only to read and write policy agent profile configuration information, typically created to delegate policy agent profile creation to the user installing a policy agent.
Agent authenticator	Entity with read-only access to multiple agent profiles defined in the same realm; allows an agent to read web service profiles.
Application	In general terms, a service exposing protected resources. In the context of OpenAM policies, the application is a template that constrains the policies that govern access to protected resources. An application can have zero or more policies.
Application type	Application types act as templates for creating policy applications. Application types define a preset list of actions and functional logic, such as policy lookup and resource comparator logic.

	Application types also define the internal normalization, indexing logic, and comparator logic for applications.
Attribute-based access control (ABAC)	Access control that is based on attributes of a user, such as how old a user is or whether the user is a paying customer.
Authentication	The act of confirming the identity of a principal.
Authentication chaining	A series of authentication modules configured together which a principal must negotiate as configured in order to authenticate successfully.
Authentication level	Positive integer associated with an authentication module, usually used to require success with more stringent authentication measures when requesting resources requiring special protection.
Authentication module	OpenAM authentication unit that handles one way of obtaining and verifying credentials.
Authorization	The act of determining whether to grant or to deny a principal access to a resource.
Authorization Server	In OAuth 2.0, issues access tokens to the client after authenticating a resource owner and confirming that the owner authorizes the client to access the protected resource. OpenAM can play this role in the OAuth 2.0 authorization framework.
Auto-federation	Arrangement to federate a principal's identity automatically based on a common attribute value shared across the principal's profiles at different providers.
Bulk federation	Batch job permanently federating user profiles between a service provider and an identity provider based on a list of matched user identifiers that exist on both providers.
Circle of trust	Group of providers, including at least one identity provider, who have agreed to trust each other to participate in a SAML v2.0 provider federation.
Client	In OAuth 2.0, requests protected web resources on behalf of the resource owner given the owner's authorization. OpenAM can play this role in the OAuth 2.0 authorization framework.
Conditions	Defined as part of policies, these determine the circumstances under which which a policy applies. Environmental conditions reflect circumstances like the client IP address, time of day, how the subject authenticated, or the authentication level achieved.

	Subject conditions reflect characteristics of the subject like whether the subject authenticated, the identity of the subject, or claims in the subject's JWT.
Configuration datastore	LDAP directory service holding OpenAM configuration data.
Cross-domain single sign-on (CDSSO)	OpenAM capability allowing single sign-on across different DNS domains.
Delegation	Granting users administrative privileges with OpenAM.
Entitlement	Decision that defines which resource names can and cannot be accessed for a given subject in the context of a particular application, which actions are allowed and which are denied, and any related advice and attributes.
Extended metadata	Federation configuration information specific to OpenAM.
Extensible Access Control Markup Language (XACML)	Standard, XML-based access control policy language, including a processing model for making authorization decisions based on policies.
Federation	Standardized means for aggregating identities, sharing authentication and authorization data information between trusted providers, and allowing principals to access services across different providers without authenticating repeatedly.
Fedlet	Service provider application capable of participating in a circle of trust and allowing federation without installing all of OpenAM on the service provider side; OpenAM lets you create Java Fedlets.
Hot swappable	Refers to configuration properties for which changes can take effect without restarting the container where OpenAM runs.
Identity	Set of data that uniquely describes a person or a thing such as a device or an application.
Identity federation	Linking of a principal's identity across multiple providers.
Identity provider (IdP)	Entity that produces assertions about a principal (such as how and when a principal authenticated, or that the principal's profile has a specified attribute value).
Identity repository	Data store holding user profiles and group information; different identity repositories can be defined for different realms.
Java EE policy agent	Java web application installed in a web container that acts as a policy agent, filtering requests to other applications in the container with policies based on application resource URLs.

Metadata	Federation configuration information for a provider.
Policy	Set of rules that define who is granted access to a protected resource when, how, and under what conditions.
Policy Agent	Agent that intercepts requests for resources, directs principals to OpenAM for authentication, and enforces policy decisions from OpenAM.
Policy Administration Point (PAP)	Entity that manages and stores policy definitions.
Policy Decision Point (PDP)	Entity that evaluates access rights and then issues authorization decisions.
Policy Enforcement Point (PEP)	Entity that intercepts a request for a resource and then enforces policy decisions from a PDP.
Policy Information Point (PIP)	Entity that provides extra information, such as user profile attributes that a PDP needs in order to make a decision.
Principal	Represents an entity that has been authenticated (such as a user, a device, or an application), and thus is distinguished from other entities. When a Subject successfully authenticates, OpenAM associates the Subject with the Principal.
Privilege	In the context of delegated administration, a set of administrative tasks that can be performed by specified subjects in a given realm.
Provider federation	Agreement among providers to participate in a circle of trust.
Realm	OpenAM unit for organizing configuration and identity information. Realms can be used for example when different parts of an organization have different applications and user data stores, and when different organizations use the same OpenAM deployment. Administrators can delegate realm administration. The administrator assigns administrative privileges to users, allowing them to perform administrative tasks within the realm.
Resource	Something a user can access over the network such as a web page. Defined as part of policies, these can include wildcards in order to match multiple actual resources.
Resource owner	In OAuth 2.0, entity who can authorize access to protected web resources, such as an end user.

Resource server	In OAuth 2.0, server hosting protected web resources, capable of handling access tokens to respond to requests for such resources.
Response attributes	Defined as part of policies, these allow OpenAM to return additional information in the form of "attributes" with the response to a policy decision.
Role based access control (RBAC)	Access control that is based on whether a user has been granted a set of permissions (a role).
Security Assertion Markup Language (SAML)	Standard, XML-based language for exchanging authentication and authorization data between identity providers and service providers.
Service provider (SP)	Entity that consumes assertions about a principal (and provides a service that the principal is trying to access).
Session	The interval that starts with the user authenticating through OpenAM and ends when the user logs out, or when their session is terminated. For browser-based clients, OpenAM manages user sessions across one or more applications by setting a session cookie. See also Stateful session and Stateless session.
Session high availability	Capability that lets any OpenAM server in a clustered deployment access shared, persistent information about users' sessions from the CTS token store. The user does not need to log in again unless the entire deployment goes down.
Session token	Unique identifier issued by OpenAM after successful authentication. For a Stateful session, the session token is used to track a principal's session.
Single log out (SLO)	Capability allowing a principal to end a session once, thereby ending her session across multiple applications.
Single sign-on (SSO)	Capability allowing a principal to authenticate once and gain access to multiple applications without authenticating again.
Site	Group of OpenAM servers configured the same way, accessed through a load balancer layer. The load balancer handles failover to provide service-level availability. Use sticky load balancing based on `amlbcookie` values to improve site performance. The load balancer can also be used to protect OpenAM services.
Standard metadata	Standard federation configuration information that you can share with other access management software.
Stateful session	An OpenAM session that resides in the Core Token Service's token store. Stateful sessions might also be cached in memory on one or

	more OpenAM servers. OpenAM tracks stateful sessions in order to handle events like logout and timeout, to permit session constraints, and to notify applications involved in SSO when a session ends.
Stateless session	An OpenAM session for which state information is encoded in OpenAM and stored on the client. The information from the session is not retained in the CTS token store. For browser-based clients, OpenAM sets a cookie in the browser that contains the session information.
Subject	Entity that requests access to a resource When a subject successfully authenticates, OpenAM associates the subject with the Principal that distinguishes it from other subjects. A subject can be associated with multiple principals.
User data store	Data storage service holding principals' profiles; underlying storage can be an LDAP directory service, a relational database, or a custom `IdRepo` implementation.
Web policy agent	Native library installed in a web server that acts as a policy agent with policies based on web page URLs.