Redbooks
ibm.com/redbooks

IBM Security Access Manager Appliance Deployment Patterns

Shahnawaz Backer

James Darwin

Vasfi Gucer

Chris Hockings

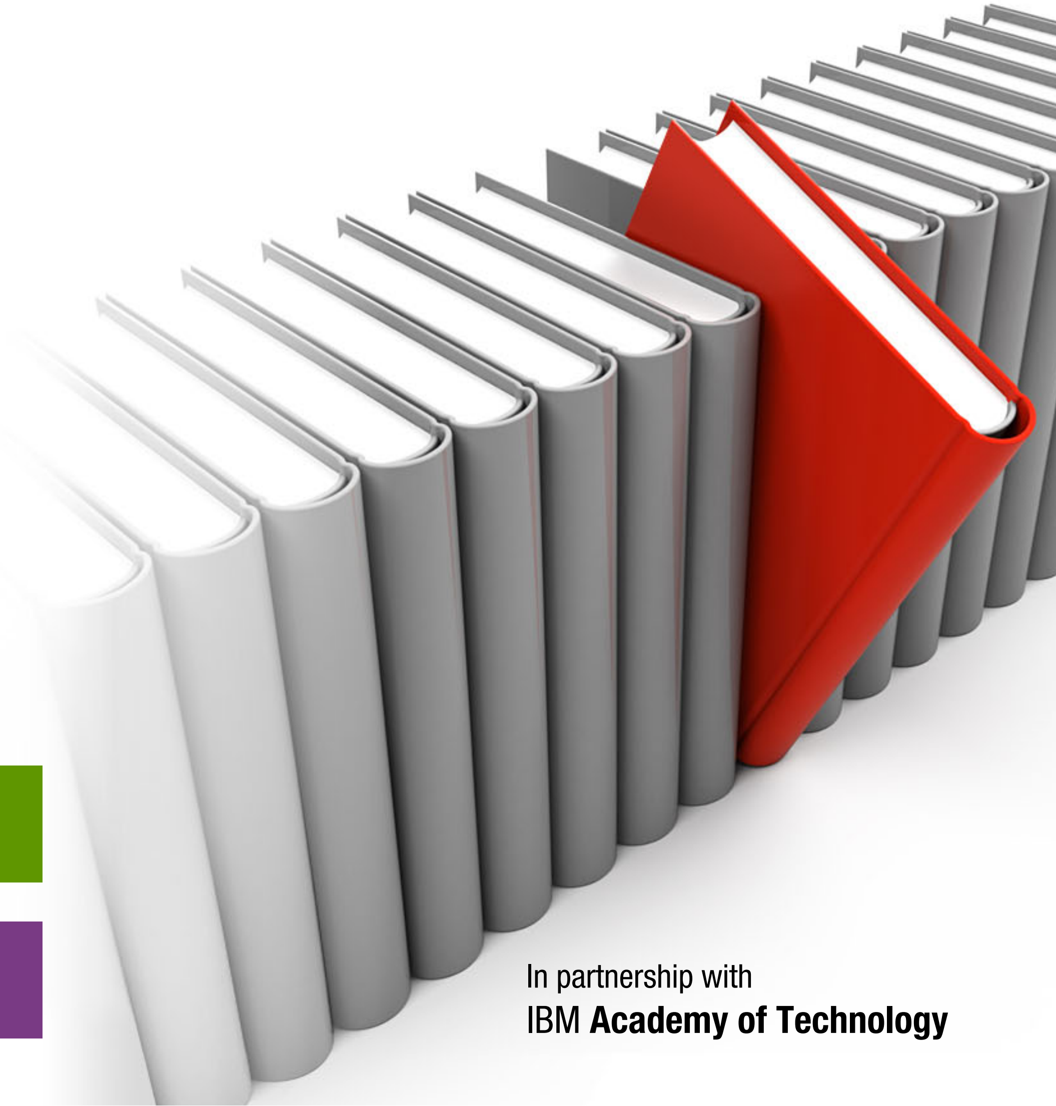
Trevor Norvill

Nilesh Patel

Martin Schmidt

Asha Shivalingaiah

Serge Vereecke



Mobile

Security

In partnership with
IBM **Academy of Technology**

IBM

Redpaper

International Technical Support Organization

IBM Security Access Manager Appliance Deployment Patterns

October 2015

REDP-5256-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (October 2015)

This edition applies to IBM Security Access Manager Version 9.0.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

DataPower®
IBM®
IBM MobileFirst™
QRadar®
Redbooks®
Redpaper™
Redbooks (logo) ®
Tivoli®
Trusteer®
WebSphere®
WPM®
z/OS®

The following terms are trademarks of other companies:

Fiberlink, MaaS360, and We do IT in the Cloud. device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM Company.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Microsoft, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

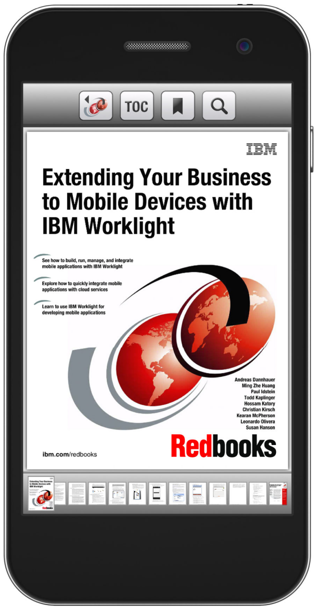
Other company, product, or service names may be trademarks or service marks of others.

Find and read thousands of IBM Redbooks publications

- ► Search, bookmark, save and organize favorites
- ► Get up-to-the-minute Redbooks news and announcements
- ► Link to the latest Redbooks blogs and videos

Get the latest version of the Redbooks Mobile App

iOS ◄ **Download Now** ► Android



IBM

Extending Your Business to Mobile Devices with IBM Worklight

See how to build, run, manage, and integrate mobile applications with IBM Worklight

Explore how to quickly integrate mobile applications with cloud services

Learn to use IBM Worklight for developing mobile applications

Andreas Dannhauer
Ming Zhe Huang
Paul Idstein
Todd Kaplinger
Hossam Katory
Christian Kirsch
Kearan McPherson
Leonardo Olivera
Susan Hanson

ibm.com/redbooks

Redbooks

Promote your business in an IBM Redbooks publication

Place a Sponsorship Promotion in an IBM® Redbooks® publication, featuring your business or solution with a link to your web site.

Qualified IBM Business Partners may place a full page promotion in the most popular Redbooks publications. Imagine the power of being seen by users who download millions of Redbooks publications each year!

ibm.com/Redbooks
About Redbooks → Business Partner Programs

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

IBM® Security Access Manager is a modular, integrated access management appliance that helps secure access to web, mobile, and cloud workloads. It is offered both as a physical appliance and as a virtual appliance image that runs on several popular hypervisors. The integrated appliance form factor enables easier and more flexible deployment and maintenance.

This IBM Redpaper™ publication describes the different Security Access Manager Appliance V9.0 deployment patterns and uses hands-on examples to demonstrate how to initially configure systems in those deployments. It also describes various deployment considerations, such as networking, high-availability, performance, disaster recovery, and scalability. All of these deployment patterns are covered within the context of realistic business scenarios.

This paper is especially helpful to Security Access Manager architects and deployment specialists.

Authors

This paper was produced by a team of specialists from around the world working at the IBM International Technical Support Organization.

Shahnawaz Backer is a Certified Security Specialist with the IBM Security division. He works with clients across the ASEAN region to identify vulnerabilities in business assets and recommends solutions to improve security and identify how IBM Security solutions can help protect their IT and business assets.

James Darwin is a member of the IBM Security Architecture Consulting team. As a member of this worldwide team, James is primarily responsible for the Asia Pacific region, guiding strategic client success, enablement, and technical vitality. He works closely with the IBM product development organization to ensure that products are updated to meet the demands of the evolving security market.

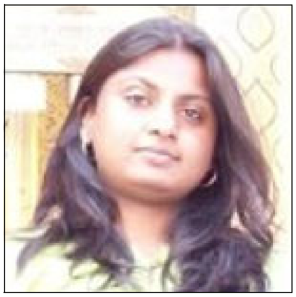
Vasfi Gucer is an IBM Redbooks® Project Leader with the IBM International Technical Support Organization. He has more than 20 years of experience in the areas of systems management, networking hardware, and software. He writes extensively and teaches IBM classes about IBM products worldwide. His focus has been on cloud computing for the last three years. Vasfi is also an IBM Certified Senior IT Specialist, Project Management Professional (PMP), IT Infrastructure Library (ITIL) V2 Manager, and ITIL V3 Expert.

Chris Hockings is an IBM Master Inventor and Executive IT Specialist. He is also a member of the IBM Worldwide Security Centre of Excellence team and the IBM Academy of Technology. He leads a team of security technology experts in the Australia Development Lab and across the worldwide IBM Security Systems SWAT team.

Trevor Norvill is a senior accredited IT Specialist working for IBM Software Group. He is based on the Gold Coast in Australia. He has worked in IBM Security technical pre-sales, post-sales lab services, and product development roles. During his nine years at IBM, he has gained extensive experience helping IBM clients design, deploy, and customize IBM Security solutions. His certifications include Advanced Deployment Professional in IBM Security Management solutions and IT Infrastructure Library (ITIL) V3. He holds a degree in computer systems engineering, with honors, from the University of Queensland.

Nilesh Patel, Security Solution Architect at Prolifics, is an identity and access management and security intelligence expert with 10 years of experience in information technology. He has extensive experience in enterprise security architecture and in design and implementation of security solutions. Nilesh has customized integration modules for identity and access management and security intelligence products. He is an IBM accredited Master Author and has written or co-authored many technical papers and delivered many technical webcasts to educate others about new features and the integration of IBM Security products. Before Prolifics, Nilesh worked with IBM as a senior identity and access management and security intelligence professional.

Martin Schmidt is a Senior Managing Consultant in IBM Security Division. He is responsible for the successful deployment of IBM Security Systems identity and access management solutions (former IBM Tivoli®) in various customer environments. He is responsible for the full project lifecycle from vision, design and architecture to deployment, go live and ongoing support. He has successfully deployed several identity and access management solutions in the financial, retail, and healthcare industry, ranging from quick start point projects to highly integrated and customized solutions providing internal as well as customer facing identity management experiences.



Asha Shivalingaiah is an IT Specialist who works with the IBM Security advanced solutions engineering team. She has had various responsibilities across development, testing, pre-sales, post-sales, and services during her tenure with IBM.

Serge Vereecke is a Certified Security Architect in the IBM Security Services group. His role involves security architecture and solution design for projects that are based on the IBM Security product portfolio. His areas of expertise include system integration and information security that focuses on identity and access management, single sign-on, and cloud computing security. Serge has more 12 years of experience in the IT industry and holds a PhD in chemistry from K.U. Leuven, Belgium.

Thanks to the following people for their contributions to this project:

LindaMay Patterson
IBM International Technical Support Organization

Axel Buecker, Brian T Mulligan, Jason Keenaghan, Sten Drescher, Judith Broadhurst
IBM USA

Lesley Nuttall
IBM UK

Now you can become a published author, too

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time. Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us.

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form:

  ibm.com/redbooks

- Send your comments by email:

  redbooks@us.ibm.com

- Mail your comments:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

IBM Security Access Manager design and architecture

This chapter describes the key features, benefits, design and architecture of IBM Security Manager.

This chapter includes the following sections:

1.1 Introduction

Over the past decade, web technologies have revolutionized the delivery of information and services. The technologies provide the basis for business functions, such as customer service, sales, and purchasing based on the traditional web, mobile, and cloud. These capabilities are a prerequisite to competitiveness. Customers, partners, and business constituents need real-time access to corporate information. They need to develop new capabilities to respond to whatever the market throws at them, such as becoming more efficient, cost-effective, and gaining advantages over their competitors. At the same time, compliance and sophisticated attacks have become real concerns that c-level executives and board members are facing.

To automate core business processes, a company gives its users (who are likely to be customers, suppliers, and employees) access to corporate information and applications through a comprehensive extranet. When it comes to security, people are the weakest link. With the advancement in mobile and cloud technology, traditional security barriers are not enough. Cyber-criminals are organized, sophisticated, and more opportunistic than ever. They use social media to mine personal data and exploit immature IT environments and business channels to find new ways to gain access to the enterprise. To combat these attacks, you need an intelligent, adaptive, and context aware security perimeter. As a threat aware identity and access management (IAM) solution, IBM Security Access Manager (Security Access Manager) is an all-in-one appliance that provides Base, Advanced Access, and Federation capabilities for secure access to web, mobile, and the cloud.

In order to understand what the Security Access Manager appliance does, you need to first understand some common problems that need to be addressed in any organization. The authentication process is complicated when the user accesses information from multiple devices, such as computers, mobile and tablets, or multiple locations over the Internet. Users should be able to securely authenticate from a web browser or a wireless device with no client software requirements. In addition, there are often hundreds of web servers in a large enterprise, some of them deployed locally, some of them in the cloud, with users needing access privileges, and in some cases different privileges for each server or application they access. This approach can lead to many architectural discussions that need to be considered when designing the security infrastructure. The more login IDs and passwords required, the more help desk time devoted to answer password-related calls is needed. In addition, if the authentication is decentralized, administrators are needed to manage the access controls for each individual server or possible application. This situation also requires additional development work and support from the application team. If the access control is decentralized, consider how many entries must be added or removed when a user's access privileges change or when an employee joins or leaves the company.

Security Access Manager addresses these potential problems and others by providing a security solution that provides the following advantages:

- Manages secure access controls for all of the servers and applications centrally
- Protects applications from advanced security threats, including the top 10 web application risks identified by the Open Web Application Security Project (OWASP)
- Combines the capabilities of a reverse proxy server, single sign-on server, web application firewall, centralized Policy server, load balancer, distributed session caching, federation, and context-aware policy enforcement-packaged in one solution
- Safeguards mobile interactions across the enterprise

- Highly scalable and configurable, so it helps organizations reduce the costs and complexities of multichannel access management
- Demonstrates continuous compliance by integrating with IBM QRadar® Security Intelligence platform

1.1.1 Concerns addressed by Security Access Manager

Security Access Manager addresses the following concerns:

- Pressure to deliver secure access to multiple web and mobile applications to expanding internal and external user populations
- Complexity and cost resulting from the implementation and maintenance of multiple access management systems targeted at different groups of users (for example, employees, contractors, customers) and access scenarios (for example, web, mobile, API)
- Inability to ensure easy access to valid users while restricting access to suspicious users
- Need to comply with security and privacy regulations by demonstrating consistent, policy-based user access security across channels (web, mobile, cloud)
- High help desk costs related to user access, including costs attributable to cross-domain scenarios
- Frustrated users whose productivity descreases due to numerous passwords, lockouts, and other password-related issues

1.1.2 Security Access Manager key benefits

IBM Security Access Manager V9.0 delivers a modular security appliance that helps secure user access and protect content against common web attacks. It offers the following key benefits:

- Enhances user productivity while ensuring secure user access to web and mobile applications through SSO, session management, strong authentication, and context-based access policy enforcement
- Provides better protection from advanced threats, including OWASP top 10 web application risks
- Integrates with IBM MobileFirst™ platform, IBM MobileFirst Protect (formerly, MaaS360® by Fiberlink®, an IBM company), and BM Security Trusteer® Fraud Protection for easier mobile access development and rich mobile context for access decisions
- Scales to support hundreds of millions of users
- Federated SSO for increased user productivity and trust through SSO across separately managed infrastructure domains, including easily configurable connections to popular software as a service (SaaS) applications

1.2 Security Access Manager licenses

Security Access Manager is offered both as a physical appliance and as a virtual appliance image that runs on several popular hypervisors.

It is structured as a base appliance (called the *platform*) with optional add-on modules. All required code is included with the platform, and organizations enable add-on module functions by entering the appropriate activation keys. This allows users the flexibility to more easily support many use scenarios while minimizing the additional software required.

Security Access Manager V9.0 is available in the following form factors:

- Physical appliance

  Security Access Manager physical appliances are priced by appliance. There is no license restriction on the number of users.

- Virtual appliance

  Security Access Manager virtual appliances are priced by user value unit (UVU) and processor value unit (PVU). A PVU license has no restriction to the number of users.

With regard to licensing, the Security Access Manager family of products has been repackaged in Security Access Manager V9.0 release to include a full portfolio lineup.

Repackaging in Security Access Manager V9.0: Security Access Manager V9.0 combines functions that are available in the IBM Security Access Manager for Web and IBM Security Access Manager for Mobile appliances with functions from IBM Tivoli Federated Identity Manager into an integrated access management appliance. The modular appliance form factor enables easier and more flexible deployment and maintenance.

Security Access Manager V9.0 is offered as a platform with the following easily usable, separately licensed add-on modules:

- IBM Security Access Manager

  This is the platform offering of Security Access Manager, which provides the following capabilities:

  - Critical user access management for web, mobile, and cloud
  - Scalable enforcement point
  - Single sign-on
  - Session management
  - Coarse-grained authorization
  - Comprehensive protection against evolving web application threats

  This platform offering replaces IBM Security Access Manager for Web deployment and serves as a platform for add-on modules.

- Advanced Access Control module

  The Advanced Access Control add-on module provides the following benefits:

  - Dynamic and context-aware policy decision engine
  - Tight integration with strong and multifactor authentication
  - Easy integration in apps and other enforcement points

- Federation module

  The Federation add-on module provides an extensible federation engine that includes the following functions:

  – Identity mediation
  – Federated single sign-on for SaaS and enterprise applications
  – Leveraging standard protocols, such as SAML 2.0 and OpenID connect

Figure 1-1 shows the production and non-production physical appliances licensed for each installation.

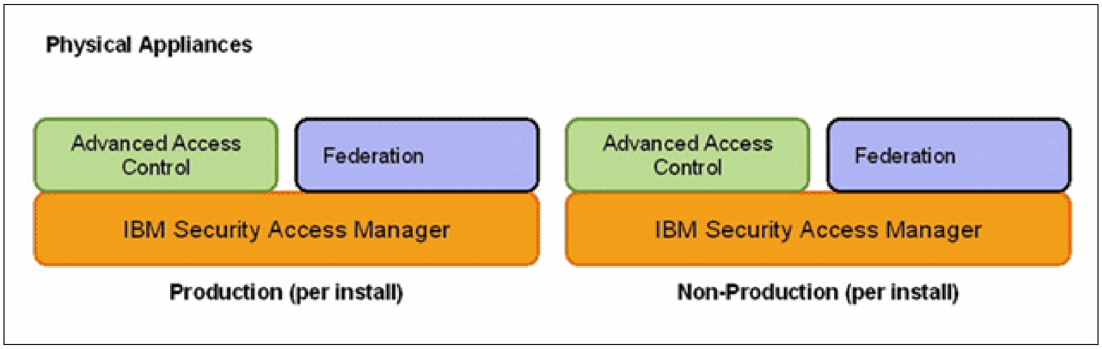


Figure 1-1 Production and non-production physical appliances

Figure 1-2 shows the production virtual appliances that are licensed based on processor value unit (PVU) and user value unit (UVU) and the non-production virtual appliances that are licensed based on PVUs.

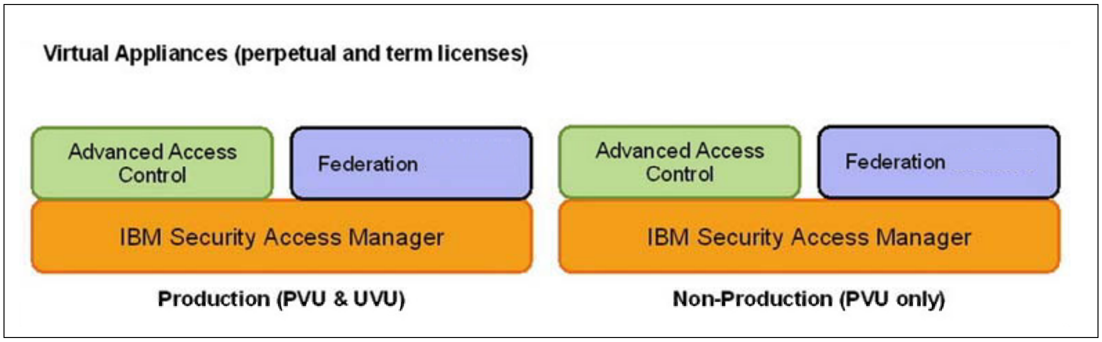

Virtual Appliances (perpetual and term licenses)
Advanced Access Control
Federation
IBM Security Access Manager
Advanced Access Control
Federation
IBM Security Access Manager
Production (PVU & UVU)
Non-Production (PVU only)

Figure 1-2 Production and non-production physical appliancesVirtual appliances

The term *non-production* refers to an internal development and test environment for internal activities done in other than a production environment. It includes testing, performance tuning, fault diagnosis, internal benchmarking, staging, quality assurance activity, and developing internally used additions or extensions by using published application programming interfaces.

Note: The high availability and disaster recovery deployments are not considered non-production.

1.3 Logical architecture of Security Access Manager the all-in-one appliance

Security Access Manager is an integrated physical and virtual appliance. The activation keys are used to enable the modules that you want on a particular appliance. Lading the Indexed Security Access Manager platform activation key onto a Security Access Manager appliance enables all of the Security Access Manager platform components on that appliance.

Figure 1-3 depicts logical building blocks of Security Access Manager an all-in-one appliance.

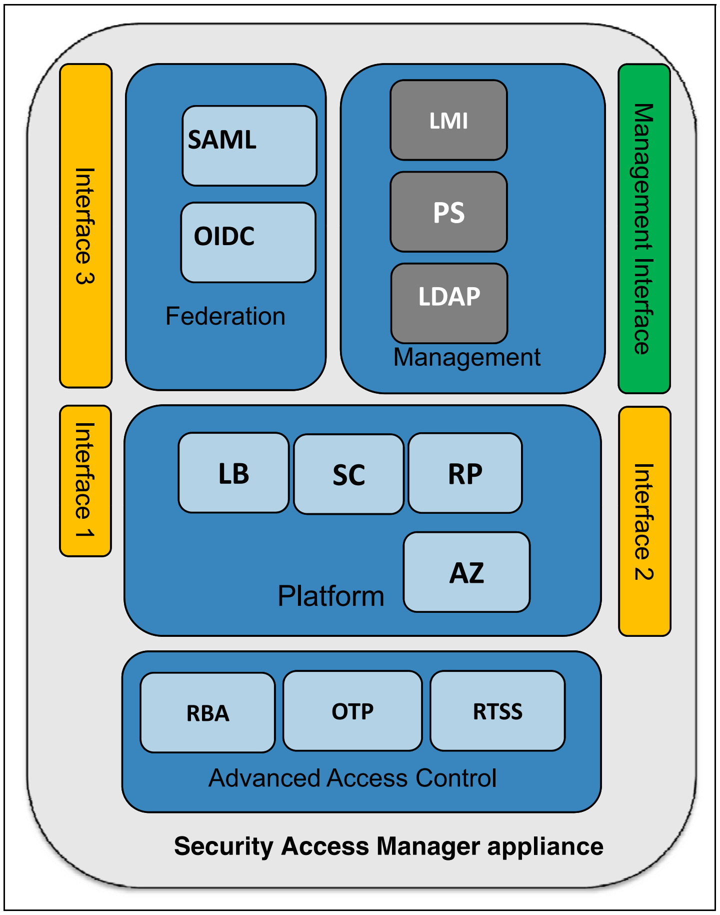


Figure 1-3 Logical building blocks of Security Access Manager

> **Note:** *Management* in Figure 1-3 is included in the license. It is not a separately licensed component.

See Table 1-1 on page 7 for an explanation of each service shown in Figure 1-3 for the Security Access Manager platform (previously known as *Security Access Manager Base*) and two separately licensed add-on modules:

- Security Access Manager *Advanced Access Control module*
- Security Access Manager *Federation module*

Some of these services are explained further in the sections that follow.

Table 1-1 Explanation of components in the figure

Component ID	Component name
Security Access Manager platform	
PS	Policy server
LDAP	Embedded Lightweight Directory Access Protocol server
LMI	Local Management Interface
AZ	Authorization service
RP	Reverse proxy
LB	Load balancer
DSC	Distributed session cache
Security Access Manager Federation module	
SAML	Security Assertion Markup Language
OIDC	OpenID Connect
Security Access Manager Advanced Access Control module	
RBA	Risk-based access
OTP	One-time password service
RTSS	Runtime security service

1.3.1 Security Access Manager platform

This section describes the components in the Security Access Manager platform.

Policy server

The Policy server manages the master copy of the authorization policy that is enforced by the Web Reverse Proxy and Authorization components. The Policy server is also responsible for distributing the policy to the various Security Access Manager components. This policy distribution is done over a mutually authenticated, certificate-based, secure connection. The certificates for this scheme are issued and managed by the Security Access Manager Policy server.

Only a single Policy server can be active in a Security Access Manager domain at any time. However, high availability can be achieved using a warm standby failover pattern. It does not need to load balance traffic between the Policy server and the other Security Access Manager components, because failover notification is handled at the application protocol level and does not rely on shared virtual IP addresses. The **pdadmin** (administrative command line) tool also connects to the Policy server so that administrative commands can be executed.

Databases

Security Access Manager uses following databases:

- Policy database

  The Policy server maintains a master copy of the policies that are enforced by the Web Reverse Proxy and Authorization Servers. This master copy policy is persisted in the Policy database. The Policy database is automatically copied to every member in a cluster where the Policy server is configured on the primary master of the cluster. This is not a relational database and does not need to be managed as such.

- Configuration database

  The appliance configuration is stored in a PostgreSQL database on the appliance. This database is replicated across a cluster. Interfaces are not available to manage this database by using traditional database utilities.

- Geolocation database

  The geolocation database stores data for mapping an IP address to the country, region, and city where the browser client is likely located. The geolocation database is replicated across a cluster. The Security Access Manager appliance ships with a sample geolocation database. Maxmind[1] offers geolocation data that is suitable for import into this database. Maxmind offers both no charge and (more accurate) chargeable forms of the data, with monthly updates.

- Runtime database

  The runtime database is not used by the Security Access Manager platform, but it is used by the add-on modules, such as the Advanced Access Control module, to store high-volume data (including device fingerprints). The runtime database can be configured as an embedded database on the appliance or as an external database. The embedded runtime database is replicated across a cluster. However, the cluster does not provide high availability nor failover for an external database. The external database server is responsible for ensuring high availability.

Authorization Server

The Authorization Server provides a remote Policy Decision Point (PDP) for authentication and authorization requests made through the Security Access Manager Authorization API (also known as the *aznAPI*). Multiple Authorization Servers can be configured in a Security Access Manager domain. The authorization policy that is enforced by an Authorization Server is maintained in the Policy server, with a copy stored in the Authorization Server, so decisions can be made locally without contacting the Policy server.

Note: The Authorization Server is not a mandatory component within a Security Access Manager deployment, but is used whenever a remote authorization service needs to call Security Access Manager for an authorization decision. It is not used by the Advanced Access Control module.

[1] https://www.maxmind.com/en/home

LDAP server

The Security Access Manager appliance includes an embedded LDAP server. By default, the appliance administrator users are defined in this local registry. The embedded LDAP server is a supported registry for smaller deployments. Administrator users can also be moved to an external user registry, if you prefer. Also, every environment is different and this presents unique challenges to integrate user registries with Security Access Manager. However, Security Access Manager supports all industry leading user registries, such as these examples:

- Active Directory Lightweight Directory Service (AD LDS)
- IBM z/OS® Security Server LDAP Server
- IBM Security Directory Server
- Novell eDirectory Server
- Sun Java System Directory Server

Along with the listed user repositories, Security Access Manager provides the Security Access Manager registry adapter for IBM WebSphere® Application Server federated repositories to use the Security Access Manager Registry Direct Java API to perform registry-related operations.

Management interface

Each of the Security Access Manager appliances provides a RESTful web service API for remote management and a browser-based management GUI interface, called the *Local Management Interface* (LMI).

The RESTful API uses JavaScript Object Notation (JSON) and is accessible only via the management network interfaces of an appliance. Most of the management operations for an appliance can be performed through this management API.

Similar to the RESTful API, the LMI is accessible only via the management network interfaces of an appliance. Itcan be used to perform a full set of management operations for the appliance.

A subset of the appliance configuration and management commands is available in a command-line interface (CLI) that is included in each appliance. This CLI can be accessed directly from the appliance console or via a Secure Shell (SSH) session with the management interface of the appliance.

The method to access the console differs between the hardware appliance and the virtual appliance:

- For the hardware appliance, a serial console device must be connected to a serial port on the appliance.
- For the virtual appliance, the console can be accessed by using the appropriate VMWare tools (for example, VMWare vSphere Client).

No direct access to the underlying operating system is available for an appliance. All configuration and management can be done only via the appliance CLI, management REST API, or LMI.

Protocol Analysis module

The Protocol Analysis module (PAM) is a component developed and supported by the IBM threat protection technologies product team. This component offers the following multiple layers of protection for web-based interaction:

Application-layer heuristics	Proprietary algorithms to block malicious use of applications
Web injection logic	For protection against web-based attacks
Shellcode heuristics	To block exploitative payloads
Content analysis	To expose hidden attacks
Protocol anomaly detection	To prevent attacks at the deepest network layers

Optionally, this component can be configured to provide protocol-level protection for web requests that pass through the IBM Security Access Manager Web Reverse Proxy, including both blocking and non-blocking (that is, reporting only) modes for identified threats are available.

Load balancer

A load balancer is included in the appliance for distributing requests across clustered Web Reverse Proxy servers. This load balancing can be done at Layer 4 or Layer 7, and subsequent requests from the same client are forwarded to the same instance of the Web Reverse Proxy.

Note: The load balancer is supported for frontend load balancing only.

Load balancers can be replicated with a designated primary server. A heartbeat between the servers is used to detect whether the primary server is active. If the secondary load balancer detects that the primary server has become unavailable, it assumes the virtual IP address and starts accepting requests from clients.

Web Reverse Proxy

The Security Access Manager Web Reverse Proxy, known as WebSEAL in earlier versions of Security Access Manager, is a reverse proxy web server that handles authentication, session management, and coarse-grained authorization (URL level) for a specified set of protected web applications. The connections to the protected web applications are known as *junctions*.

The Web Reverse Proxy can be configured to add information for single sign-on and entitlement propagation in the HTTP headers of requests sent via these junctions. The Web Reverse Proxy balances loads and handles failover across multiple instances of web server junctions.

The authorization policy enforced by Web Reverse Proxy is maintained through the Security Access Manager Policy server, with a local copy stored in the Web Reverse Proxy so authorization decisions can be made locally without contacting the Policy server. This policy can include the requirements to perform finer-grained authorization decisions by using the Advanced Access Control services (such as context-based access and OAuth).

Distributed session cache

The Web Reverse Proxy stores its session table in the distributed session cache (DSC) on a Security Access Manager appliance. The DSC is implemented as a SolidDB in-memory database and is replicated across a cluster. This allows all instances of a replicated Web Reverse Proxy in a cluster to share the same session table data.

The introduction of the DSC removes the need for the Session Management Server (SMS) and the failover cookie from earlier versions of Security Access Manager. DSC is the replacement for the SMS, and you can consider using it as an alternative to the failover cookie.

1.3.2 Advanced Access Control module

The Advanced Access Control module is one of the add-on modules available for Security Access Manager platform. It requires an explicit license to activate it on the appliance.

This module provides a dynamic and context-aware policy decision engine that is tightly integrated with strong and multifactor authentication. It integrates easily in applications and other enforcement points. In Security Access Manager V9.0, the Advanced Access Control module replaces the Security Access Manager for Mobile.

1.3.3 Federation module

The Federation module is also an add-on module. An explicit license is required to activate it on the appliance.

The Federation module provides an extensible federation engine for identity mediation and federated single sign-on for both SaaS and enterprise applications. It uses standard protocols, such as SAML 2.0 and OpenID connect.

1.4 Summary

Security Access Manager V9.0 is a modular, integrated access management appliance that helps increase security of access to web, mobile, and cloud workloads. The integrated appliance form factor enables easier and more flexible deployment and maintenance.

Security Access Manager is offered both as a physical appliance and as a virtual appliance image that runs on several popular hypervisors. In this chapter, we reviewed the key features and benefits of Security Access Manager and described the logical architecture of the all-in-one appliance.

2

IBM Security Access Manager clustering

This chapter describes key concepts of IBM Security Access Manager clustering technology. The chapter includes the clustering roles a Security Access Manager appliance can perform, an overview of Security Access Manager cluster services, port considerations when planning a deployment, how the cluster replicates data, and how Security Access Manager appliance clustering works with traditional Security Access Manager availability features.

This chapter includes the following sections:

2.1 Introduction

Security Access Manager is a key piece of security infrastructure, so it is important to ensure the availability of the service that it provides. To support a range of availability requirements, the product provides redundancy capabilities in all of its components, by design. The Security Access Manager appliance introduces several new system components and to support availability scenarios new clustering technology compared to pre-appliance versions has been added.

Setting up a Security Access Manager cluster offers the following business benefits:

- Reduced cost of ownership

  Appliance clustering enables simpler configuration and maintenance when multiple replicated components are deployed across a distributed appliance topology. This results in quicker time to value for the solution, easier maintainance, and decreased costs.

  Using the clustered onboard appliance directory, configuration databases, and runtime database enables deployment of a highly available solution without the need for additional specialized hardware, software, and services skills as an external database and directory server are not required.

- Automated disaster recovery

  The Security Access Manager appliance allows the cluster to recover from Security Access Manager component failures quickly and easily. Enhanced clustering capabilities allow the system to recognize failures and move workloads to alternative components automatically. This potentially reduces downtime, which can help meet committed service levels and improve customer experiences.

This chapter describes Security Access Manager clustering technology in detail, including how it can be used to deliver more economical and more robust solutions. We also include a use case example.

2.2 Clustering concepts and technology

The Security Access Manager platform has always provided features to support complex availability requirements. The Security Access Manager appliance platform introduces additional, complementary clustering services to allow for better management of system components in appliance deployment scenarios. The cluster services also provide additional automated failover capabilities during appliance failure scenarios at run time.

The following chapter describes key concepts of Security Access Manager clustering technology, including the clustering roles that a Security Access Manager appliance can perform, an overview of Security Access Manager cluster services, port considerations when planning a deployment, how the cluster replicates data, and how Security Access Manager appliance clustering works with traditional Security Access Manager availability features.

2.2.1 Cluster roles

Appliance clustering technology uses a master/node system to simplify the operation of the cluster and optimize consistency and availability of cluster services. When designing a Security Access Manager solution with clustering, a key decision is selecting the number of appliance instances to include in a Security Access Manager cluster. Each appliance can be assigned a functional role in the operation of the cluster. The appliance has several available roles:

- Primary master

  The primary master maintains the authoritative source of data and coordinates cluster operations. All configuration updates must be made to this appliance, and any updates made to non-primary masters will be ignored.

  When a Security Access Manager appliance is first configured, it is designated as the primary master of a stand-alone cluster. When a Security Access Manager cluster is configured, a single appliance instance is nominated to function as the primary master. The primary master can be moved to another appliance during failover scenarios by nominating it in the Local Management Interface of a non-master server.

  Note: Some primary master functions that provide runtime services, such as a distributed session cache (DSC), offer automatic runtime failover. Other primary master functions that are not critical to runtime services, such as Policy server failover, require an administrator to nominate a new primary master.

- Replica masters

  All other Security Access Manager appliances in the cluster can be assigned backup appliance master roles. These servers are referred to as the *secondary*, *tertiary*, and *quaternary* master for each additional Security Access Manager appliance that is added to the cluster as a master. The purpose of these servers is to provide a backup of the master data and be available to be promoted if a primary is required. The tertiary and quaternary are used only for the DSC component. The tertiary and quaternary are not required unless the DSC is deployed.

- Nodes

  All non-master appliances join the cluster as nodes. When an appliance is configured as a node, it can access and share the configuration and runtime information of the primary master, but it cannot be promoted to perform the primary master function. A node can be changed to serve a master role by nominating it in the Local Management Interface.

- Restricted nodes

  Nodes can be configured to be restricted nodes. This prevents a node from being nominated as a master role and restricts the node from using the policy administration tool for modifying security policy. This is used to restrict nodes in the DMZ from hosting writable copies of cluster data stores and for keeping access to administrative functions confined to appropriate network security zones.

Table 2-1outlines the roles that each additional appliance adds to the capability of the runtime cluster.

Table 2-1 Roles each appliance adds to runtime cluster

Number of masters	Roles	Considerations
1	Primary master	The configuration provides no failover for the configuration cluster service, the runtime cluster service, or the distributed session cache (DSC)
2	Primary master Secondary master	The addition of a secondary master provides failover for cluster services, which includes the replicated file system, DSC, configuration database cluster service, and runtime database cluster service.
3	Primary master Secondary master Tertiary master	The tertiary master is only used by the DSC. The configuration and runtime databases treat the tertiary node as a non-master node for replication purposes.
4	Primary master Secondary master Tertiary master Quaternary master	The quaternary master is only used by the DSC. The configuration and runtime databases treat the tertiary node as a non-master node for the purpose of replication.

- External reference entity

  The external reference entity is a network device that is external to the Security Access Manager system. Its purpose is to deal with failover scenarios when primary and secondary masters are configured. If a master loses its connection to the other master, it needs to determine if the other master is offline or if there is a network fault. Each master uses an external reference entity connectivity test to determine the appropriate action to take. as shown in Figure 2-1.

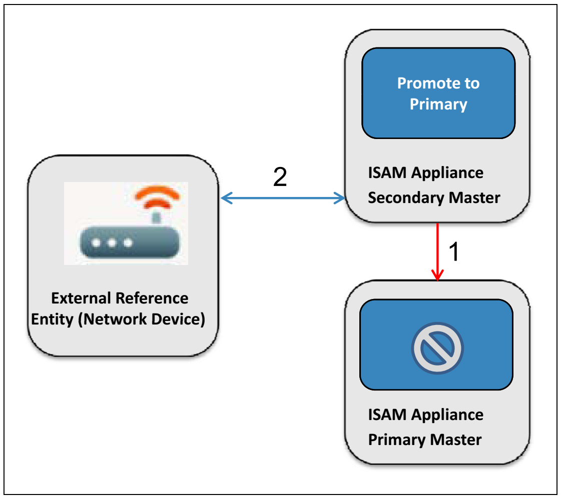

Promote to Primary
ISAM Appliance Secondary Master
2
1
External Reference Entity (Network Device)
ISAM Appliance Primary Master

Figure 2-1 Failover scenario

This failover scenario shown shows the following scenario details:

- The primary master has failed. The secondary master is able to detect that it cannot contact the primary master via the failed connection (item 1 in Figure 2-1 on page 16).
- The secondary master detects that it is still able to communicate with the external reference entity via the connection (item 2 in Figure 2-1 on page 16). The clustering services determine that the primary has failed and promote the secondary master to the primary master role.

2.2.2 Clustering services

Security Access Manager cluster services allow the appliance to securely replicate different types of data throughout the cluster appropriately depending on its function. The appliance provides the following services to allow for easy configuration of clustered appliances and runtime high availability of services:

- Replicated file system cluster service

  This cluster service allows appliance configuration files to be shared across the cluster. It stores data such as basic configuration data for the Security Access Manager runtime or Policy server or SSL certificate key files. The appliance files system is not directly exposed to Security Access Manager administrators or users, but configuration files can be viewed through the Local Management Interface.

  The Local Management Interface provides two options that control how data is replicated between the nodes of a Security Access Manager cluster:

  - The Security Access Manager runtime *Replicate with Cluster* option allows the Security Access Manager runtime configuration, Policy server configuration, and user registry configuration to be replicated across to all nodes.
  - The Security Access Manager Secure Sockets Layer (SSL) certificate *Replicate with Cluster* option allows all SSL certificates to be replicated across all nodes.

  All updates to configuration files hosted on the replicated file system must be made only to the primary master Local Management Interface when a cluster is enabled. When an update is detected on the primary master, the appliance cluster manager process synchronizes the update to all other nodes and masters in the cluster. The replicated file system also will re-synchronize when the appliance file system starts. The system also does periodic checks to ensure that all copies of the file system are synchronized. An administrator cannot make configuration changes on non-master nodes, because the configuration options are disabled on these nodes.

  If the primary master is changed through the Local Management Interface, all cluster configuration files are updated to reflect the new master configuration. For example, the master/host configuration item in the `pd.conf` file is updated to point to the new master server.

- Configuration database cluster service

  This service persists information specifically related to the configuration of the Advanced Access Control and Federation components. These components do not use the replicated file system and, instead, store configuration data in a database. Information persisted in this cluster service, such as policies and federation definitions, changes infrequently after the system is set up.

All updates to the configuration database cluster service must be made only on the primary master. When an update is detected on the primary master, the appliance clustering daemon synchronizes the update to all other nodes. Because this service deals with replicating configuration data, as opposed to runtime data, the appliance can batch these for distribution to other nodes.

The primary maintains the only writable copy of the configuration database. The configuration database is distributed to all nodes that require the information, including the secondary master and nodes running the Advanced Access Control and Federation components. Nodes use the local replica configuration database for read operations. Nodes that do not run the components that require this service do not host a copy of the configuration database.

The Security Access Manager appliance provides an onboard implementation of the data store that hosts this service, by default. Optionally, this service can be externalized to a database system for large enterprise deployments.

- Runtime database cluster service

  The runtime database cluster service maintains information related to runtime operations in the system for the Security Access Manager Advanced Access Control and Federation components. Data maintained by this service is needed in real time by the system, so it is critical that it be both consistent and available across the cluster at all times. Examples of data managed by this cluster service include federation data, such as OAuth grants, and context-based access data, such as device finger prints and session attributes.

  This database is replicated to only the primary master and secondary masters. Federation and Advanced Access Control runtime components use the primary master for all read and write operations. There are no local copies of the databases replicated to appliance nodes.

  The Security Access Manager appliance provides a highly available database implementation for small and medium-sized deployments. Optionally, data storage for this service can be externalized to a database system for large enterprise deployments.

- Distributed session cache cluster service

  This service maintains and replicates session information used by the distributed session cache (DSC). Its purpose is to provide a centralized session store so that a consistent session experience can be provided for clients that use Web Reverse Proxy across a Security Access Manager cluster. The DSC replaces the Security Access Manager Session Management Server that was in previous Security Access Manager releases. It also enables concurrent session policy and cluster-wide termination of sessions to be implemented.

  If enabled, the DSC is critical to the runtime operation of reverse proxy services, so the DSC service must be configured for high availability. Unlike other Security Access Manager appliance cluster services, data maintained by the DSC cluster service cannot be externalized to another system.

  The DSC has its own clustering technology, separate from the runtime database, because it has unique requirements for consistency and availability of the service. For a highly available solution, the DSC data store must be maintained on at least the primary and secondary masters. It is the only service to also use the tertiary and quaternary masters if configured. These options add resilience to appliance failures that might be required, depending on the service levels required for the solution.

  If the DSC is enabled, Security Access Manager reverse proxy automatically sets appropriate configuration items to use the available DSC servers.

- Directory service cluster service

  The Security Access Manager appliance provides an embedded directory service to store user identity information for small deployments. When using the embedded directory server the appliance can provide a solution to support high availability directory requirements using appliance clustering technology. The embedded directory service hosts registry data on the primary and secondary masters. Data is replicated between the primary and secondary server.

  It can also be externalized to a supported directory server technology of choice. If the solution uses an external directory server, high availability must be implemented by using native directory server tools.

2.2.3 Port consideration

A typical Security Access Manager deployment consists of appliance instances configured as reverse proxies in the corporate DMZ. Separate appliance instances that are configured with the Policy server, Federation, and Advanced Access Control components are deployed in protected network segments. Networking best practice requires network segregation to minimize exposure of components that manage policy and user data.

Cluster communication takes place between nodes by using port forwarding over Secure Shell (SSH) on port 22, as shown in Figure 2-2.

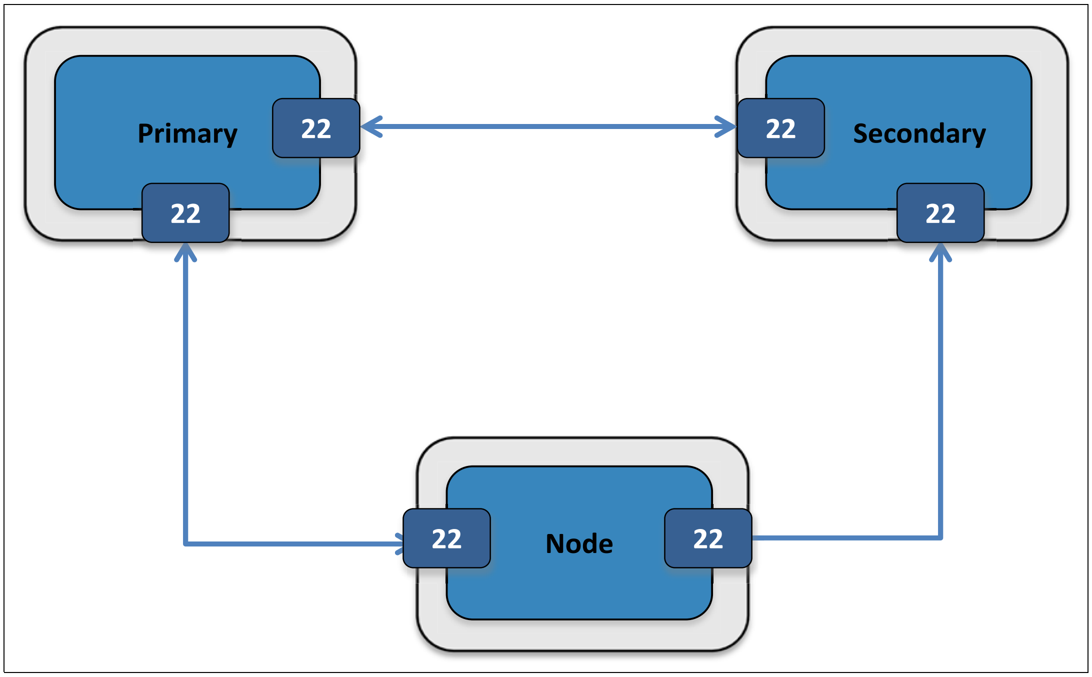


Figure 2-2 Cluster communication over SSH (port 22)

The following constraints apply to the direction of communication between cluster services (Figure 2-2 on page 19):

- The replicated file system requires that port 22 be open in both direction.
- Reverse proxies poll the master for updates but as reverse proxies require that the replicated file system port 22 be opened bidirectionally.
- The distributed session cache requires port 22 to be open in both directions between primary master, secondary master, tertiary master, and quaternary masters, respectively.

2.2.4 Appliance cluster replication mechanism

Internally, appliance processes that use cluster services communicate with the 127.0.0.1 interface to simplify the channels of communication. The clustering technology directs updates between appliances instances as required by its cluster configuration using port forwarding over SSH. Port forwarders are set up and removed dynamically to facilitate communication between processes that are running on master appliances and using processes running on nodes. This activity is coordinated by the cluster services.

When implementing a Security Access Manager project, internal communication is hidden by SSH tunnels. However, it is useful to understand how the port forwarding occurs for debugging purposes. When the appliance cluster is configured, a starting port is specified. By default this port is 2020. Security Access Manager configures tunnels using this as the first port and incrementing the port number for each additional process that requires communication with the cluster.

As an example, Table 2-2 shows the internal tunneling ports and the port that is using processes when the default starting port of 2020 is used.

Table 2-2 Internal tunneling ports and the consuming port for processing

Component	Internal port	Consumer port
Primary DSC	2026	2036
Secondary DSC	2027	2037
Primary LDAP	389	389
Replica LDAP	NA	390
Policy server	NA - uses IP of master	NA - uses IP of master

Figure 2-3 shows how the Security Access Manager cluster communicates internally. For firewall configuration, all traffic goes over the SSH port 22, with the exception of communication to the Policy server, which is over the traditional default port of 7135.

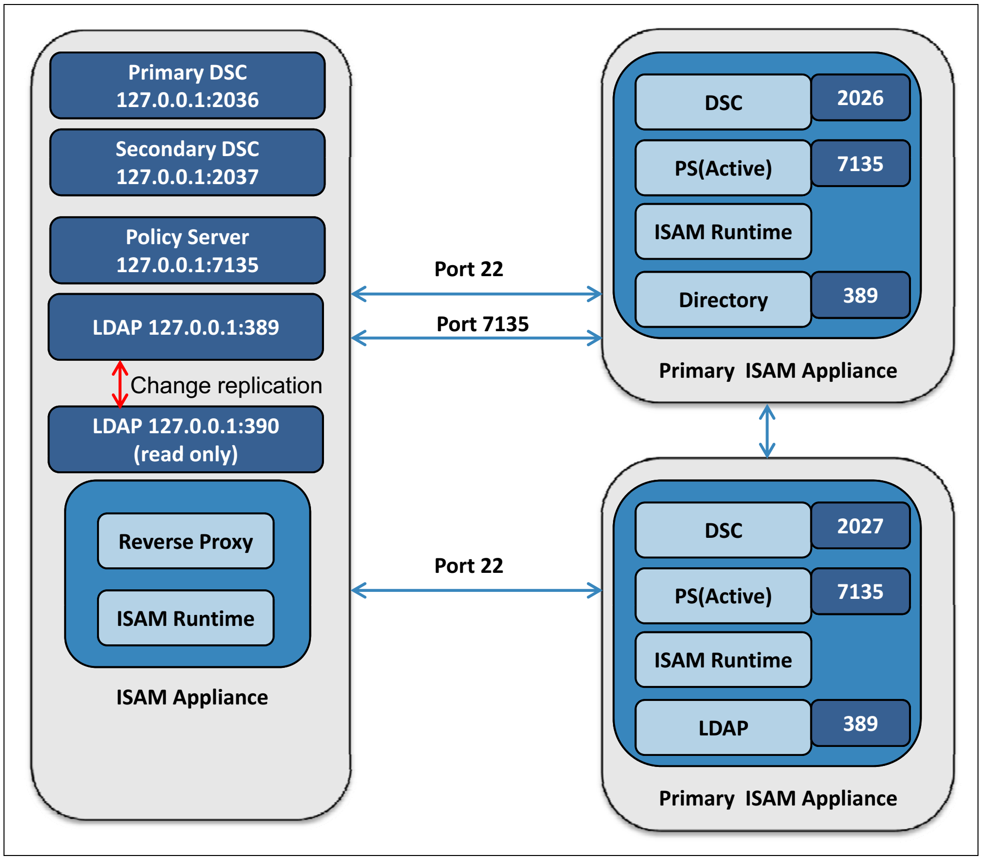


Figure 2-3 Port forwarding over SSH for DSC

The Policy server and directory server clustering shown in Figure 2-3 follows these procedures:

- When a reverse proxy is configured with the distributed session cache, the configuration shows the reverse proxy DSess configuration references:
  - Server = 9,http://127.0.0.1:2036/DSess/services/DSess
  - Server = 8,http://127.0.0.1:2037/DSess/services/DSess

  This is illustrated at the left side of Figure 2-3. Appliance clustering configuration is set up to tunnel this traffic to the configured primary and secondary masters, respectively, via SSH and is mapped to port 2026 and 2027 on the primary and secondary masters, respectively.
- As illustrated at the left side of Figure 2-3 on page 18, the Security Access Manager runtime references 127.0.0.1 on port 389/636 for the user registry configuration. This is port-forwarded to the primary master over SSH. There is a local LDAP *read-only* replica that listens on port 390 for failover scenarios.
- The Policy server is configured to talk to the IP address of the primary master server on port 7135. When the primary master is changed to another appliance, the cluster services reconfigure the Security Access Manager runtime to point to the new primary master.

2.2.5 Traditional availability features

Some high availability capabilities of the Security Access Manager V9 appliance build on capabilities in traditional Security Access Manager software components, such as the following features:

- Reverse proxy configuration replication

  Security Access Manager software offerings provide the ability to replicate reverse proxy configuration by using the **`pdadmin`** server task command. This mechanism has been enhanced in the appliance to allow easy synchronization of reverse proxy configuration through the appliance Local Management Interface. Reverse proxy instances pull configuration from a configured master reverse proxy instance.

  The reverse proxy clustering capability is separate from the clustering services that are described in the rest of this section.

  When replicating reverse proxy configuration, consider these factors:

  – The reverse proxy master must be specified to be the authoritative source of configuration information. This is done via the `is-master` configuration item in the reverse proxy configuration.

  – All other reverse proxy cluster instances must reference a master reverse proxy instance. This is done by using the `azn-server-name` of the master instance.

  – All servers must be able to resolve the host name of each appliance in the reverse proxy cluster. The `azn-server-name` contains the host name of the master reverse proxy instance, and all non-master instances must be able to resolve this to pull configuration from the master. You will receive error messages in the non-master reverse proxy message logs if the system is unable to resolve the host name.

  When a reverse proxy instance master is updated, all non-master instances must be restarted to retrieve the new configuration.

  Note: The **`pdadmin`** server task command can still be used to update Web Reverse Proxy configuration for existing script purposes.

- Directory server failover

  Security Access Manager components have built-in capabilities to load balance between multiple directory servers for high availability. This feature is used by the appliance for both onboard directory and external directory implementations.

- Failover mechanisms for reverse proxy

  The Security Access Manager Web Reverse Proxy can provide client-side failover, using a symmetrically encrypted failover cookie.

2.3 High availability clustering failure scenarios

This section examines how a Security Access Manager cluster responds when a clustered Security Access Manager component fails.

2.3.1 Policy server failure

Security Access Manager Version 9 enables Policy server high availability via an active/inactive model. The active Policy server resides on the primary master appliance. The secondary hosts a backup Policy server. The Policy server is used to administer policies, such as users, groups, access control lists, protected object policies, authorization rules, and other policies associated with the Security Access Manager protected object space. Because Security Access Manager deals with policy updates, it is not considered a critical runtime component.

Failover involves switching the primary master to the secondary master. This is a manual process through the Local Management Interface. Actions follow this sequence:

1. The Security Access Manager policy database maintains an up-to-date copy on both the primary and secondary masters by actively synchronizing the database.
2. An administrator nominates the secondary master as the new primary master by selecting **Make Primary** in the appliance cluster configuration. This action deactivates the Policy server that is running on the primary master and starts the Policy server on the secondary master.
3. The Security Access Manager run time is then reconfigured to use the new primary master server.
4. Reverse proxy instances need to be restarted for changes to take effect.

2.3.2 Advanced Access Control or Federation failure

There are two Security Access Manager appliance scenarios that can affect the Advanced Access Control or Federation components:

- Failure of the Federation or Advanced Access Control run time

  When a reverse proxy instance is configured to use the Federation or Advanced Access Control service, several servers can be specified for failover scenarios. When an appliance that is hosting the Federation and Advanced Access Control run time fails, the reverse proxy detects the failure and can select an alternative runtime server to use. The appliance cluster is not involved in this process, because the reverse proxy component provides native capabilities to perform this function.

- Failure of the primary master

  When an appliance hosting a primary master fails, the configuration database and runtime database become unavailable. The Advanced Access Control and Federation components require these services to function. However, they are treated differently by the appliance clustering technology.

Figure 2-4 shows configuration database replication.

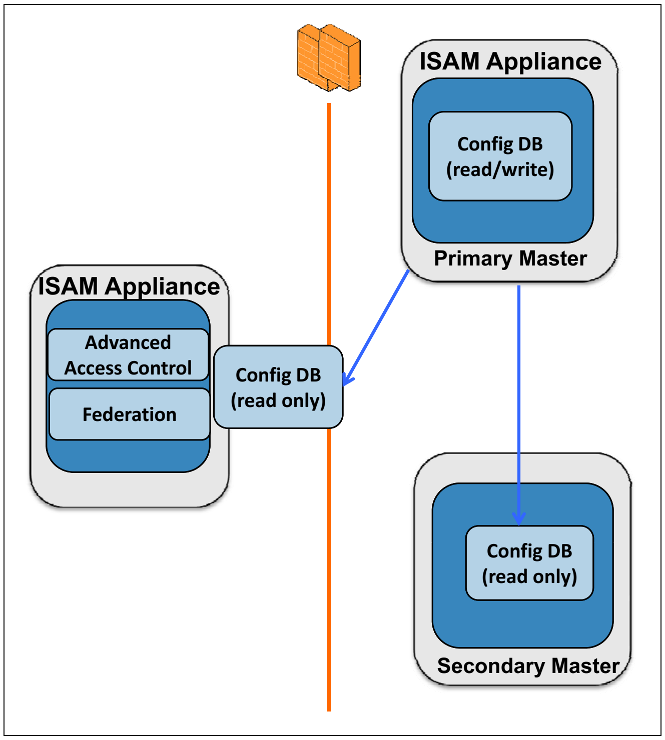


Figure 2-4 Configuration database replication

As shown in Figure 2-4, the configuration database performs the following tasks:

- Configuration database is replicated to all nodes that require the configuration to function. This includes appliances hosting the Federation and Advanced Access Control runtime components.
- The Advanced Access Control and Federation components can use a local copy of the configuration database for read-only operations. All write operations must be made at the primary master.
- These components can provide service with a read-only copy of the configuration database, but configuration changes cannot be made. To restore the ability to configure the components, the secondary master must be promoted to a primary server, at which point it becomes a read/write copy and all other nodes become read-only.

Figure 2-5 shows runtime database failover.

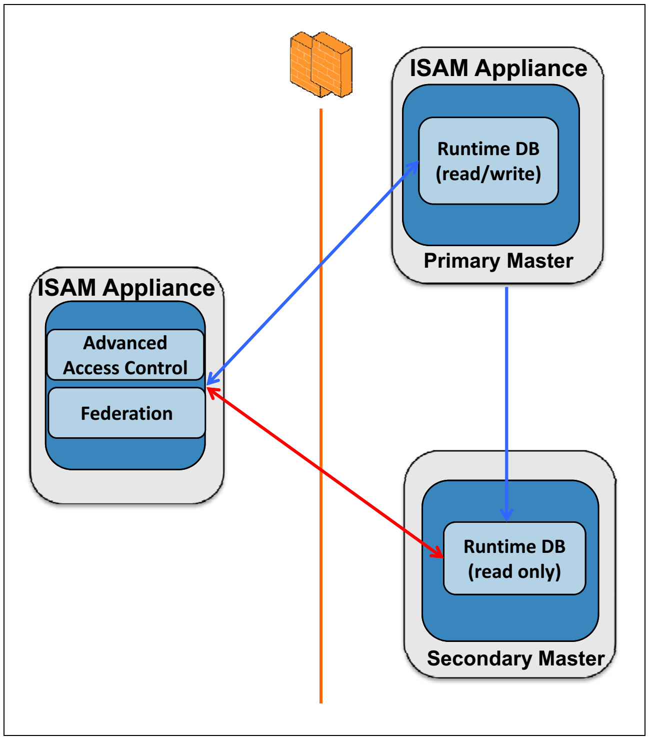


Figure 2-5 Runtime database failover

The runtime database has the following characteristics:

- It is hosted only on the primary and secondary masters.
- The Advanced Access Control and Federation runtime components read and write data to the primary master via appliance cluster communication implemented with SSH tunnels.
- The primary master and secondary servers are synchronized with each other by using SSH tunnels that are controlled by the appliance cluster manager.
- If the primary master fails, the Advanced Access Control component, Federation component, and secondary master detect the failure. The cluster is dynamically reconfigured to promote the secondary master to a primary master for the runtime database cluster service.
- All components that use the runtime database cluster service are also dynamically reconfigured to use the new primary runtime database.

2.3.3 Embedded directory failure

The embedded directory server uses an LDAP server deployed on the primary master for read and write operations. When the primary master fails, directory clients such as reverse proxy instances can use a local read-only replica that is configured on internal port 390 to continue servicing requests. Port 390 is not visible outside the appliance.

The local replica server is a read-only server, so no write operations can be performed. To restore LDAP write capabilities, a new primary master must be selected by an administrator through the Local Management Interface.

Note: If features are used that require LDAP writable operations, such as the reverse proxy *last login time* attribute, the local read-only replica cannot store this information.

2.3.4 Distributed session cache failure

The DSC has fully automatic failover capabilities. When a primary master fails, the reverse proxy configuration is pre-configured to automatically select the next available master appliance and perform session operations against the new server. An administrator can configure up to four masters for DSC failover scenarios.

2.4 Networking

The Security Access Manager provides a significant amount of flexibility in the way the networks can be configured to address scenarios for both the physical and the virtual appliance deployment patterns. The physical appliance has to deal with real items, such as physical network cards and network cabling. The virtual appliance potentially requires more flexibility when being deployed in a private, public, or hybrid cloud.

Appliance interfaces with names in the format of `1.x` are real interfaces that correspond to the network adapters on your physical appliance or to the adapters that are attached to your virtual appliance.

The appliance also supports the use of a virtual local area network (VLAN), which allows the LAN to be segmented without requiring physical rearrangement. Appliance Interfaces with names in the format of `1.x:<vlanid>` are virtual interfaces.

Creating network interfaces and VLANs can be done through the CLI, the LMI, and the REST APIs. When the appliance is initialized, at least the first Local Management Interface is usually defined so that the LMI can be accessed after the initialization sequence is finished.

You can add or delete virtual interfaces, but you cannot delete real interfaces. When you add an interface, you are effectively adding a VLAN to a specific interface. Each interface on the appliance is configured with a static address and a netmask (`<address>/<mask>`), or if you want to use Dynamic Host Configuration Protocol (DHCP) to assign addresses, you can select **Auto**. Multiple additional addresses can then be configured on that same network, assuming they are within that same subnet.

The appliance has the concept of management and application *addresses*. The management services (Policy server, the internal LDAP server, and LMI services) all listen on the management interfaces. Other services, such as the reverse proxy, the distributed session cache, and the Authorization server listen on application addresses.

One or more addresses on the Security Access Manager appliance can be flagged as the management interfaces. At least one management interface must be defined before the run time can be configured. If more that one are configured, the management services listen on all defined management interfaces. It is best to create the management interface as a static IP to reduce the dependency on DHCP servers. Each new network interface must be configured with non-overlapping, unique subnets.

Example 2-1, Example 2-2, and Example 2-3show more detail.

Example 2-1 Network interface configuration -- interface 1.1

```
Interface 1.1 = 10.251.140.52/255.255.255.0 (or 10.251.140.52/24)
```

The consideration for Example 2-1 is that addresses in the range < 10.251.140.0 - 10.251.140.254> can be configured on this interface.

Example 2-2 shows a network interface configuration with multiple interfaces.

Example 2-2 Network interface configuration -- multiple interfaces

```
Interface 1.1 = 10.251.140.52/255.255.255.0 (or 10.251.140.52/24)
Interface 1.2 = 10.251.141.52/255.255.255.0 (or 10.251.140.52/24)
Interface 1.3 = 10.251.142.52/255.255.255.0 (or 10.251.140.52/24)
```

These are the considerations for Example 2-2:

- Addresses in <10.251.140.0 - 10.251.140.254> range can be configured on interface 1.1.
- Addresses in <10.251.141.0 - 10.251.141.254> range can be configured on interface 1.2.
- Addresses in <10.251.142.0 - 10.251.142.254> range can be configured on interface 1.3.

Example 2-3 shows another network interface configuration with multiple interfaces. In this more complex example the 10.51.140.x/24 address space is split into four different subnets. This might be desirable for performance reasons or to allow specific routing rules to be applied.

Example 2-3 Network interface configuration, multiple interfaces

```
Interface 1.1 = 10.51.140.52/255.255.255.192 or 10.51.140.52/26
Interface 1.2 = 10.51.140.80/255.255.255.192 or 10.51.140.80/26
Interface 1.3 = 10.51.140.176/255.255.255.192 or 10.51.140.176/26
Interface 1.4 = 10.51.140.200/255.255.255.192 or 10.51.140.200/26
```

The following considerations are for Example 2-3:

- Addresses in <10.51.140.0 - 10.51.140.63> range can be configured on interface 1.1
- Addresses in <10.51.140.65 - 10.51.140.127> range can be configured on interface 1.2
- Addresses in <10.51.140.129 - 10.51.140.191> range can be configured on interface 1.3
- Addresses in <10.51.140.193 - 10.51.140.254> range can be configured on interface 1.4

Table 2-3 shows the number of usable hosts for various prefix size and network masks.

Table 2-3 Number of usable hosts for various prefix size and network masks

Prefix size	Network mask	Available subnets	Usable hosts per subnet	Total usable hosts
/24	255.255.255.0	1	254	254
/25	255.255.255.128	2	126	252
/26	255.255.255.192	4	62	248
/27	255.255.255.224	8	30	240
/28	255.255.255.240	16	14	224
/29	255.255.255.248	32	6	192
/30	255.255.255.252	64	2	128
/31	255.255.255.254	128	2	256

2.4.1 Ports and protocols

This section describes all the listening ports that can be configured on the Security Access Manager appliance. This is important to understand so that only the necessary firewall rules are put in place to allow this traffic and block all other traffic.

Listening ports become active depending on several factors:

- The number of configured network interfaces and virtual IP addresses
- The enabled activation keys (such as federated servers and advances access)
- The configured services on a particular appliance (such as the reverse proxy and the authorization services)

Figure 2-6 on page 29 1 shows a stand-alone (non-clustered) appliance with a single management interface and four application interfaces configured. It has all available services configured.

Note: This is certainly not a typical setup for a single appliance. However, it has been set up this way to help with the understanding the potential network and port configurations. This does not include information about data replication and clustering, which is covered in Chapter 2, “IBM Security Access Manager clustering” on page 13.

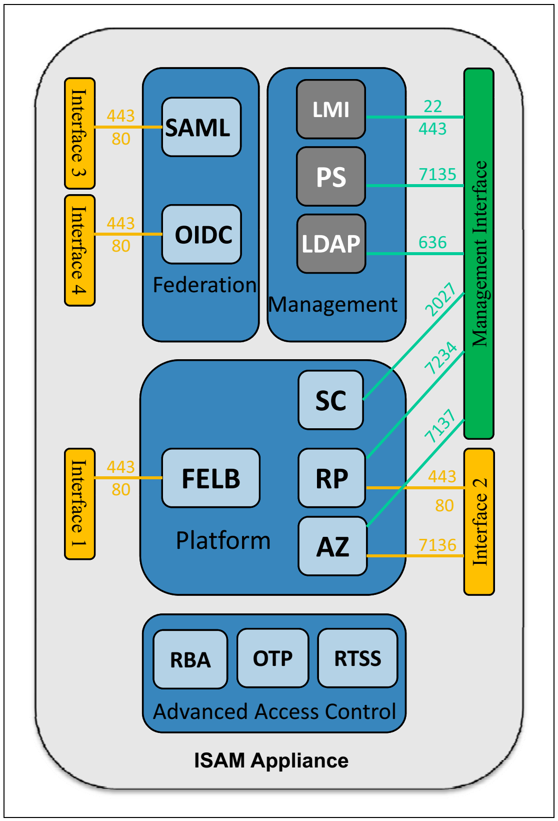


Figure 2-6   Security Access Manager appliance listening ports

In general, when the appliance is communicating with another appliance, for example appliance-to-appliance communication, the Local Management Interface is used for that communication channel. When the appliance is communicating with any other, third-party IT entity, one (or all) of the application interfaces are used. See Table 2-4.

Table 2-4   Listening ports and services

Label	Services	Protocols	Listening ports
FELB	Front-end load balancer	HTTP, HTTPS	433, 80
SAML	SAML Federation	HTTP, HTTPS	443, 80
OIDC	Open ID Connect	HTTP, HTTPS	443, 80
SC	Distributed session cache		2027
RP	Reverse proxy	HTTP, HTTPS, Internal	443, 80, 7234+
AZ	Authorization service	Internal, Internal	7136+, 7137+
LMI	Local Management Interface	HTTPS, Internal	443, 22
PS	Policy server	Internal	7135
LDAP	Embedded LDAP directory	LDAPv3 (TLS)	636

All network addresses (0.0.0.0)

On the appliance, you will notice that when configuring services, you are sometimes given the option of a network address of `0.0.0.0`. When this network is chosen, the services listen on all configured *application networks*.

Available tools

The appliance console provides a useful command-line tool that functions simillarly to **`netstat -a`**. It is under **Tools** (simply type *tools* on the CLI), and it's called *connections*. First, it displays a list of listening services (network:port), and then it lists all active inbound and outgoing network connections on the appliance.

The internal network (172.0.0.1)

When you run the **`connections`** command on the CLI, you'll see that the appliance also uses the loopback device (127.0.0.1) for much of its local service-to-service communication. These connections are not really important in this context, because they are internal to the appliance and never leave the local network.

2.5 Deployment use case example

The following use case example requires a sophisticated clustered solution that uses Security Access Manager technology because of the company's size, complex environment, and nonfunctional requirements.

Company A is a large business with more than 1,000,000 customers. It is rolling out an on-premises access management solution to protect web-based applications by providing authentication, authorization, and federated single sign-on services. The access management solution also needs to provide a consistent session experience and the ability for an administrator to terminate web sessions within the system.

To mitigate increasing online threats, Company A is also rolling out Advanced Access Control capabilities to assess the risk of access using the context of the request. The context includes the geolocation of IP addresses, contents of the request, and the user's existing authentication level. Company A wants to use a one-time password (OPT) that is delivered in a Short Message Service (SMS) text message to provide additional identity assurance to customers who are perceived to be high-risk by corporate policy.

The solution must provide very high service levels, with no more than 24 hours of downtime per year. To accommodate this, there is a primary site configured with redundant components and a deployment at a separate site for disaster scenarios.

Figure 2-5 on page 25 shows a Security Access Manager clustering solution for Company A.

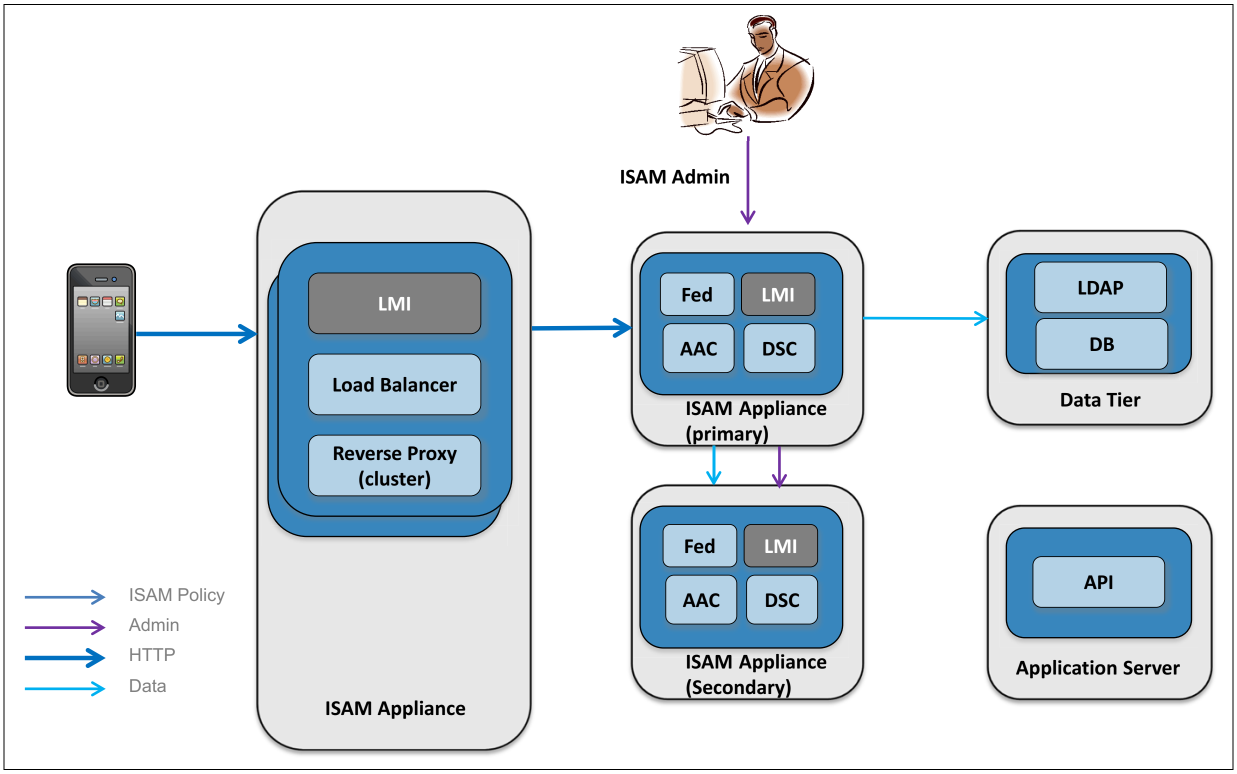


Figure 2-7 Security Access Manager clustering solution

Company A has chosen a solution with the following clustering features:

- To handle the demand for their services, they have decided to deploy several reverse proxy instances to handle the load and provide a highly available solution.
- They will use a reverse proxy cluster to replicate configuration changes between reverse proxy instances to allow for easier, more consistent, and cost-effective deployment and maintenance.
- Federation modules have been activated for an OpenID Connect solution.
- The Security Access Manager Advanced Access Control feature has been activated to deliver the context-based access requirements.
- The DSC has been deployed to deliver their session consistency and session termination requirements. They determined that a primary and secondary Security Access Manager appliance were enough for their availability needs.
- A primary and secondary Security Access Manager appliance is deemed to be an acceptable availability solution for the runtime Advanced Access Control and federation requirements.
- Due to the scale of the solution, they have selected an external LDAP directory and database. A highly available solution will be implemented with native tools.

2.6 Summary

To meet a range of availability requirements, Security Access Manager provides redundancy capabilities in all of its components, by design. The Security Access Manager appliance platform introduces additional, complementary clustering services to allow for better management of system components in appliance deployment scenarios. The cluster services also provide additional automated failover capabilities during appliance failure scenarios at run time.

In this chapter, we reviewed Security Access Manager clustering services and high availability clustering failure scenarios by using a deployment use case example.

3

Single appliance cluster pattern

This chapter details the deployment pattern that enables an organization to easily and securely extend on-premises authentication to include single sign-on to cloud-based services and the hosting of a small number of non-critical, low-risk applications. The pattern uses the IBM Security Access Manager platform, and its embedded components, with the Federation module add-on in a minimal deployment configuration.

The chapter outlines the clustering consideration for a set of appliances deployed in a DMZ with the Security Access Manager deployment scenario. It includes the following sections:

- 3.1, “Introduction” on page 34
- 3.2, “Deployment use case” on page 35
- 3.3, “Summary” on page 41

3.1 Introduction

A single clustered appliance model can be adopted in several scenarios, such as the following examples:

- *Non-production test environments* to enable developers and integration teams to quickly test end-to-end scenarios. This deployment requires the configuration of a minimal set of the Security Access Manager services on a single appliance. Automation through scripted deployment is expected to play a major role in setting up these appliances.
- *Production environments* where the availability requirements can cater for outages associated with scheduled maintenance and unplanned outages and also the emphasis is on minimal deployment footprint. There are two primary use cases:
  - To enable employee access to cloud services
  - For simple deployments with a small number of applications that are not critical to the business

  This use case assumes that a small number of replicated appliances are deployed in a DMZ.

Important: Under these conditions, you must be aware of and assess the risks that are associated with these patterns and choose whether to accept the risks of deploying multiple Security Access Manager security components as a single cluster. These risks exist from both availability and threat perspectives.

This chapter details the production deployment pattern where an organization wishes to securely extend their on-premises authentication to include single sign-on to cloud based services or hosting or a small number of non-critical, low risk applications. The pattern will use the Security Access Manager platform (and its assumed embedded components) with the Federation add-on in a minimal deployment configuration. It will outline the clustering consideration for a set of appliances deployed in a DMZ-only Security Access Manager deployment scenario.

Note: It is unlikely that this pattern would be recommended for environments where a security policy is developed and maintained for applications that are hosted on-premises. This is simply because there is no separation between the administrative and the runtime components. In environments where this is required, it is expected that standard n-tier architectures be maintained and deployed. This deployment pattern enables a distinct separation of the sensitive policy and user data into a zone designed for it.

3.2 Deployment use case

Company A is a midsize business with 2000 employees. They have subscribed to a cloud service for customer relationship management (CRM) from Company B. Both organizations have agreed on the use of Security Assertion Markup Language (SAML) 2.0 as the single sign-on standard. They have selected the SAML Browser Post profile for its simplicity and common market use.

Company A uses Microsoft Active Directory (AD) for user authentication. They want to extend the use of AD-based Kerberos authentication to the access of cloud services. They want to implement a cloud single sign-on integration without introducing any new user credentials by using on an existing enterprise directory deployment. The organization is also concerned about exposing their enterprise directory service to the cloud, either directly or by replication.

Company A is also aware that, in the future, users will expect to access cloud service while using their personal computers at home. Therefore, they need a service that provides internet strength resiliency to potential attack and one that can be deployed both with on the intranet and internet facing. They have chosen Security Access Manager as the product deployment technology.

Figure 3-1 displays the use case to be developed. Company A extending its onsite protected credentials to allow access to cloud based CRM service by Company B. In the first instance, the on-premises deployment will be extended to include Company B resources.

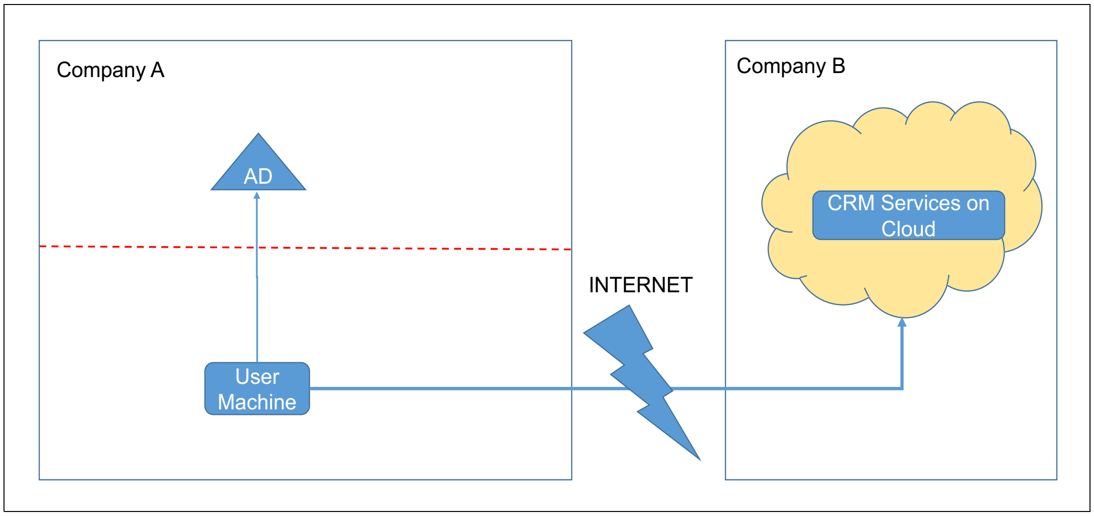


Figure 3-1 Deployment use case

3.2.1 Implementing the solution

The single appliance deployment pattern as displayed in Figure 3-2 on page 36 can be used to satisfy the aforementioned requirements. The deployment will allow the users to access CRM service, without the need to introduce any new credentials. To achieve this capability following steps will be performed:

- Security Access Manager platform appliances with Federation add-on will be deployed.
- Security Access Manager will be configured to use Active Directory credentials.
- SAML 2.0 agreement will be configured between Company A and the CRM provider on the cloud, Company B.

Figure 3-2 shows the conceptual diagram that shows the components and the functional responsibilities of each.

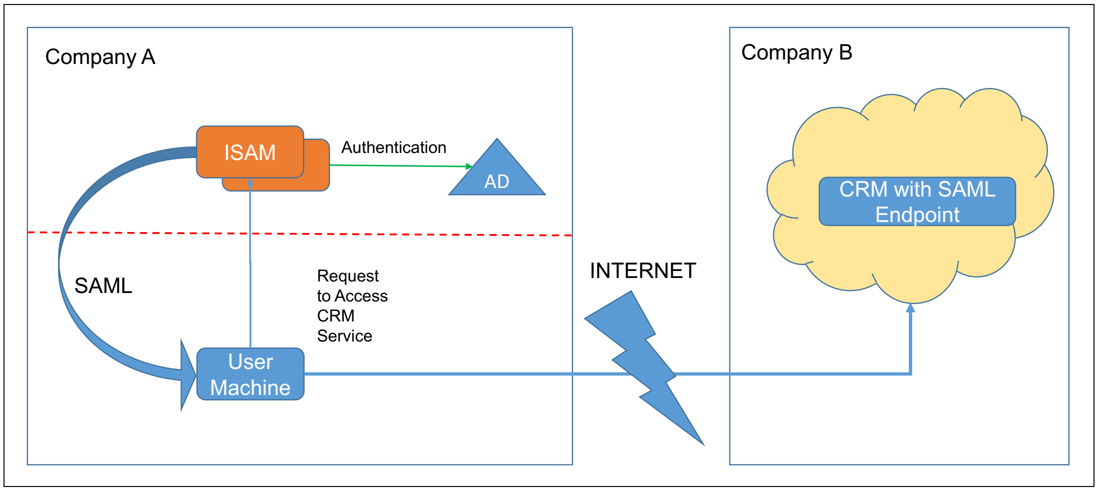


Figure 3-2 Single Appliance Cluster pattern

Company A's users will be provided with a URL to access the CRM site. The URL can be either hosted on intranet or can be provisioned onto the user's desktop (or browser). When a user accesses the URL, the request will be intercepted by Security Access Manager, forcing the user to authenticate with the AD credentials. These credentials may be of the form of a user name and password or a Kerberos ticket. The Security Access Manager instance will then generate a SAML token using the keys supplied by Company B. The user will then be redirected to the CRM service. Company B will validate the SAML token and enable the user to access the CRM service.

3.2.2 Solution components

The Security Access Manager appliance provides for multiple components and add-ons. To achieve this particular use case, Company A will need a License Entitlement of Security Access Manager platform, along with the Federation add-on. Company A can select from either of Physical or Virtual deployment. The software is the same regardless of the form of appliance deployment.

Environmental components

The functional components that required for the single appliance deployment pattern are displayed in Figure 3-3 on page 37. The solution requires a minimum of two Security Access Manager virtual images for high availability (HA) purposes with the following components enabled:

- Reverse proxy (RP)

  The reverse proxy component fronts the federation solution and provides for the authentication to AD.

- Federation module (FM)

  This is an add-on module that provides the SAML capabilities.

- Load balancer (LB)

  The built-in load balancer provides high availability and load balancing for the Security Access Manager appliances.

- Policy server (PS)

  This server manages coarse-grained authorization policies for the appliance.

- Local Management Interface (LMI)

  The web interface manages the appliance.

- Embedded directory server (DS)

  For deployment of this scale, the Security Access Manager embedded LDAP repository is used for authentication. The users' credentials do not need to be synchronized between Security Access Manager and the corporate Active Directory installation.

Figure 3-3 depicts all the components that will be enabled on the Security Access Manager appliance. For high availability purposes, there will be two appliances, and the RP component and Federation add-on will be in active/active configuration. The PS will be in primary/secondary relationship. The configuration data will be clustered across the appliances, with the primary interface used for configuration.

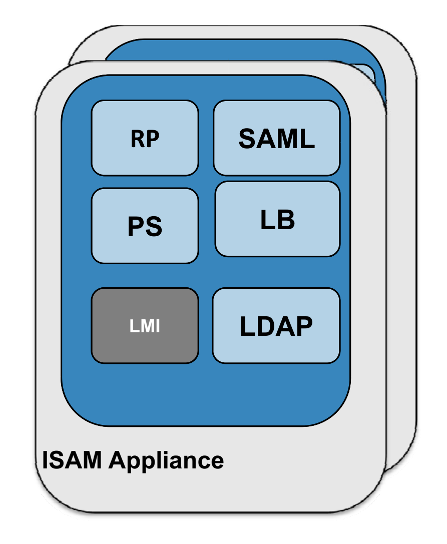


Figure 3-3 Functional components required for the Single Appliance Cluster pattern

Important: This pattern does not provide for context-based access (CBA) or fine-grained access control. For a situation where fine-grained access control or CBA is needed, this deployment pattern needs to be extended to include a separate Security Access Manager Advanced Access Control module, as listed in Chapter 1, "IBM Security Access Manager design and architecture" on page 1.

3.2.3 Architectural considerations

The Security Access Manager-based solution must be robust and highly available. There can be no single point of failure that jeopardizes the operational aspects. The sections that follow outline the setup to provide for these considerations.

Security Access Manager component requirements

Figure 3-4 on page 39 illustrates the high availability of all the following solution components:

- Web reverse proxy (WRP)

  Components are deployed in an active/active approach. The client-side single sign-on (SSO) high availability is achieved by using the Security Access Manager Failover cookie feature, not the distributed session cache (DSC). This simplifies the clustering replication that is required for sessions across the cluster.

- Federation module

  SAML and OIDC, both shown in Figure 3-4 on page 39, are the two components that make up the Federation module. This module uses an active/active approach. The load is balanced by Security Access Manager reverse proxy junction capabilities, so the junctions with the federation services are replicated across the cluster pair and serve the same function as an identity provider.

- LDAP server

  The embedded LDAP server is made highly available by using appliance clustering. This service is used for building the users' credentials after they have authenticated with AD.

- Policy server (PS)

  This server takes an active-standby (primary-secondary approach) by using the appliance-clustering feature that is described in Chapter 2, "IBM Security Access Manager clustering" on page 13.

The AD is used to authenticate the users. In this deployment scenario, it is typical to use Kerberos as an authentication mechanism to provide desktop-based single sign-on. The configuration of that is beyond the scope of this paper, but the resulting federation flows and deployment pattern is not dependent on authentication.

Networking considerations

Security Access Manager appliance provides 2 management interfaces and 4 application interfaces that need to be configured and allocated to appropriate services. Figure 3-4 displays the interface allocation. A virtual IP address will be required by the load balancer to spread the load between the two reverse proxies.

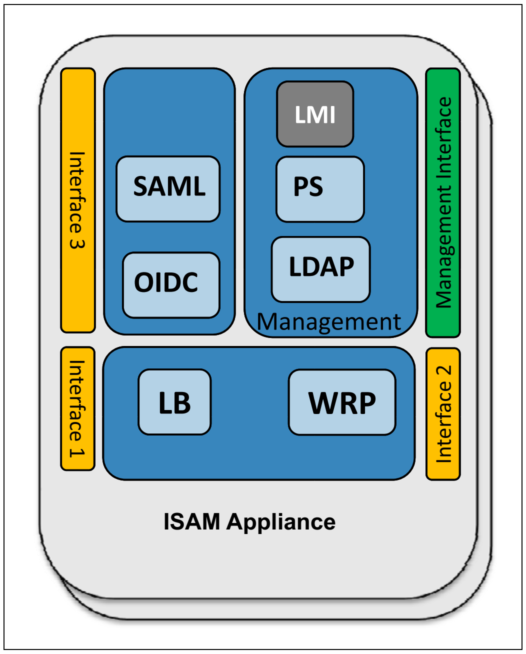


Figure 3-4 Networking considerations for the Single Appliance Cluster pattern

Details about appliance networking are covered in 2.4, “Networking” on page 26 and appliance clustering is covered in 2.2, “Clustering concepts and technology” on page 14.

3.2.4 Sequence diagram for cloud access

This pattern provides Company A’s internal users access to cloud CRM services. The solution follows a particular flow where an internal user is authenticated and granted access. Figure 3-5 illustrates this flow.

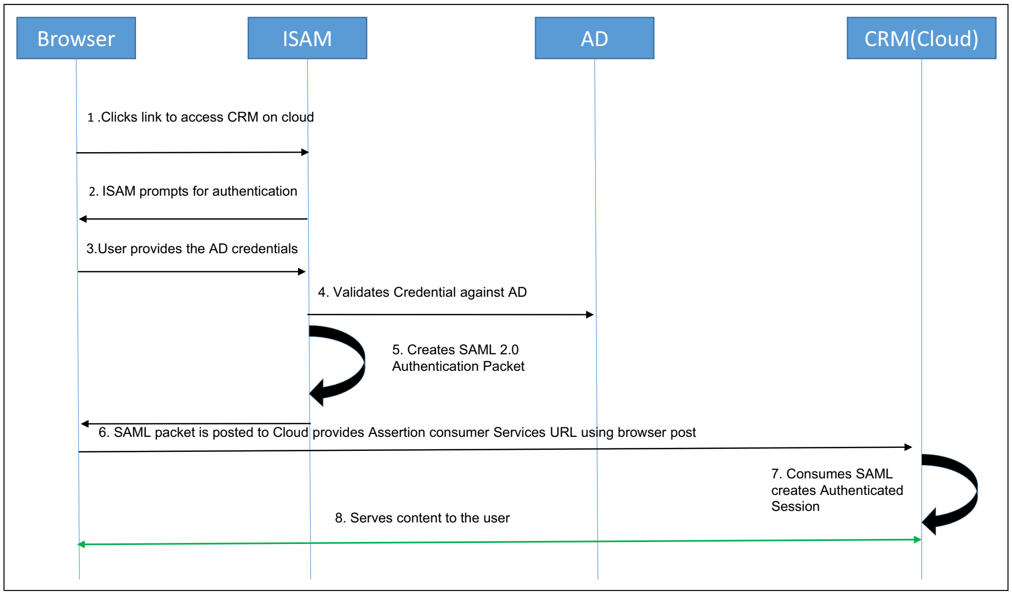

Browser
ISAM
AD
CRM(Cloud)
1 .Clicks link to access CRM on cloud
2. ISAM prompts for authentication
3.User provides the AD credentials
4. Validates Credential against AD
5. Creates SAML 2.0
Authentication Packet
6. SAML packet is posted to Cloud provides Assertion consumer Services URL using browser post
7. Consumes SAML
creates Authenticated
Session
8. Serves content to the user

Figure 3-5 Sequence diagram for the Single Appliance Cluster pattern

Figure 3-5 shows the sequence of activities before a user is granted access:

1. The user clicks the link to access CRM from an intranet portal or from a shortcut link on a desktop or in a browser. The URL is that of the identity provider-initiated single sign-on of the Federation module, hosted as part of Security Access Manager.
2. Security Access Manager intercepts the request and inspects for an authentication session. Because session information is not available, the user sees the login page.
3. User provides his Active Directory credentials (Kerberos authentication might also be used).
4. Security Access Manager validates the credential against the Active Directory.
5. After successful authentication, Security Access Manager triggers the Federation add-on module. Federation engine creates the SAML 2.0 packet.
6. The SAML 2.0 packet is posted to the registered Assertion Consumer Service URL of the cloud provider using a browser redirect.
7. The cloud provider uses the SAML and creates an authenticated session.
8. The cloud provider serves content to the user’s browser.

3.3 Summary

The single appliance cluster pattern provides organization capability to extend the use of the on-premises credential to cloud services in a standards-compliant, secure manner. The solution is easy to deploy and maintain in a production environment. The single appliance cluster pattern can also be used in development and other non-production test environments to support production deployments, as outlined in the chapters that follow.

The complexity of clustering Security Access Manager components is not described this chapter. Instead, it serves as an introduction to a simple environment that can be automatically scripted for a limited number of use cases.

4

Multiple appliances in a single location

This chapter describes applying multiple appliances in a single location. It includes three common use cases, their deployment patterns, and architectural considerations.

This chapter includes the following sections:

4.1 Introduction

To support critical business systems, the data center is an essential part of the IT infrastructure containing server, storage, and operational management. When deploying a critical system, such as Security Access Manager, the number and location of the data centers are important considerations in the deployment plan.

In a traditional (non-cloud) on-premises deployment, one of the common data center topologies still in use today is the two-site topology, with two sites within a certain distance of each other and operated in either active/standby or active/active mode.

In an active/standby configuration, production workload is placed in the primary (active) site and non-production workload, such as disaster recovery or development, is placed in the secondary (standby) site.

When considering the deployment of Security Access Manager appliances in a single location, several additional considerations and constraints must be taken into account:

- Availability
- Virtualization (software and hardware)
- Network security zones
- Monitoring
- Performance
- Scaling

Infrastructure virtualization is also creating new infrastructure and security challenges to provide consistent levels of isolation, monitoring, and policy enforcement. Organizations want to consolidate servers that belong to different network security zones. A *network security zone* is a construct to implement a defined level of security across a network and a logical area within a networking environment. Data flowing in and out of the security zone is subject to restrictions, but data flows are relatively free within the zone.

These are examples of network zones:

- DMZs, a firewall configurations for securing local area networks
- Application defined zones
- Extranet or intranet zones

Before discussing the overall solution topology and the deployment patterns, we need to clarify some key terms, such as high availability, fault tolerance, because these terms are often misrepresented or misunderstood. For example, there is a difference between high availability and fault tolerance, and choosing either of these can result in different deployment patterns.

Availability is a measure of the accessibility of a system or application, not including scheduled downtime.

High availability refers to the ability of a system or component to be operational and accessible when required for use for a specified period of time. The system or component is equipped to handle faults in an unplanned outage gracefully and to continue providing the intended functions. Some high availability systems have components that automatically switch over, but some require a combination of manual intervention and scripting.

Fault tolerance refers to the ability of a system to continue operation in case of failure of one or more of its components. This term is usually referenced with high availability, particularly at the hardware level. Hardware redundancy (the addition of extra hardware for fault detection and toleration) is commonly employed in fault-tolerant systems.

Clustering is a technique to create multiple copies of components that are running actively and collaborating seamlessly to present a single, unified system.

In this section, we consider virtual and physical deployment architectures of Security Access Manager with a focus on nonfunctional requirements, such as scaling, performance, and high availability factors. The architectures described in this paper are based on preferred practice principles.

4.2 Web and federated single sign-on use case

A midsize company wants to implement web SSO with on-premises web applications and federated SSO that is based on the SAML2 standard, with some SaaS applications. The number of users allows the deployment of an embedded LDAP. The clients of the solution are browser-based devices, PCs, notebooks.

4.2.1 Solution components

For this deployment use case, the company needs a license entitlement for the Security Access Manager platform with the Federation add-on module. Both the virtual and physical appliance can be selected.

If there is an existing IBM DataPower® Gateway deployment, the Security Access Manager module for DataPower can be deployed for the Web Reverse Proxy component. The solution requires a minimum of two Security Access Manager nodes for high availability purposes and four Security Access Manager nodes when considering network security.

Figure 4-1 shows a schematic overview of the components required for this deployment pattern and their deployment within a single location. Each component is redundant within this pattern.

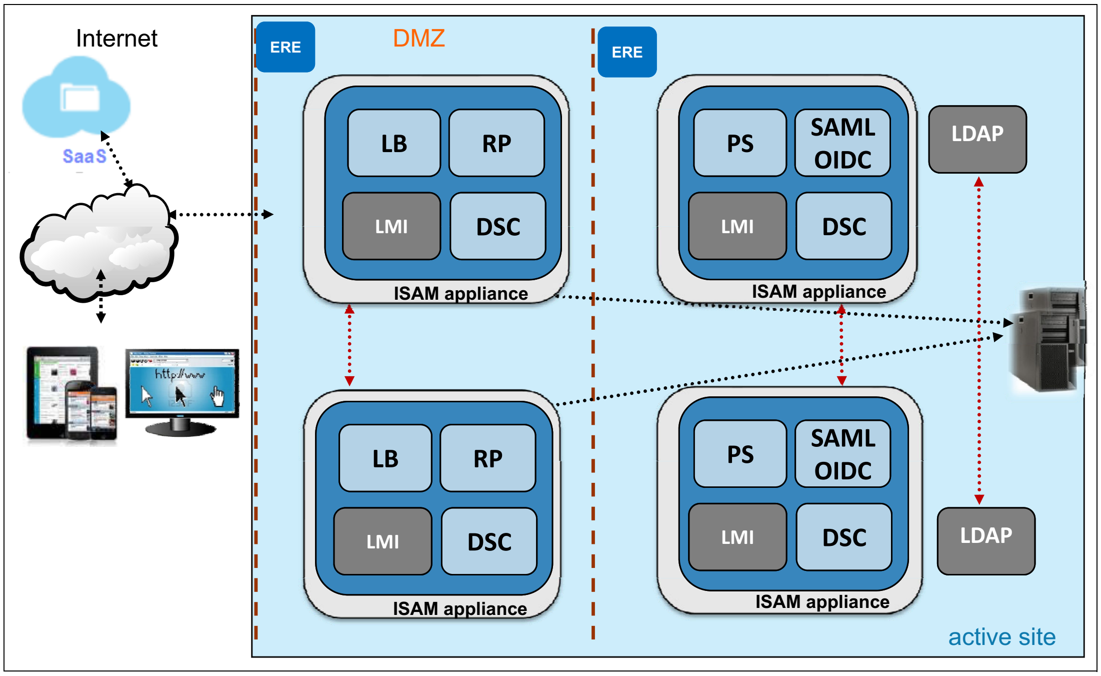


Figure 4-1 Deployment components for the federated and web SSO use case

4.2.2 Architectural considerations

The allocation of Security Access Manager components is based on high availability, performance, and security requirements. The Web Reverse Proxy component is deployed on a gateway appliance in the DMZ network zone. To guarantee the availability of the Web Reverse Proxy servers, a front-end load balancer is activated.

The front-end load balancer (FELB) load balances the requests across a cluster of appropriately configured web reverse proxies. With the FELB, a Security Access Manager cluster is self-load-balancing with one appliance designated as the distributor of traffic across the front of the Web Reverse Proxy servers. The Security Access Manager FELB simplifies the architecture by eliminating the need for separate load balancers.

The load balancer not distributes the requests to only the Web Reverse Proxy servers, but it also checks the health of the Web Reverse Proxy servers. If one of the Web Reverse Proxy servers is down, all requests are automatically redirected to the remaining servers. The two load balancer nodes monitor each other by using a heartbeat mechanism. If the master node fails, the secondary becomes the master, so users will not notice any disruption of service.

The embedded directory server will replicate the data with the standby embedded directory server on the other appliance. Nodes in the DMZ can be configured as restricted nodes, which means that those nodes cannot be promoted to any of the master roles.

The external reference entity (ERE), which can be any network device, has to be configured in the nodes to be able to handle split-brain scenarios. In this scenario, the node can contact the ERE to determine whether there is a network fault or the other node is down.

The Federation module will be deployed on the two appliances in the trusted zone, in an active-active mode being load balanced by the appliances in the DMZ. In the context of Federated single sign-on, the Web Reverse Proxy servers are acting as a point of contact providing authentication service and the session management service functions.

4.2.3 Clustering

The Security Access Manager appliances are grouped to work together in a cluster environment. The distributed session cache (DSC) cluster service is activated. The distributed session cache (DSC) can be used for session storage by all of the Security Access Manager appliances in a cluster.

When a failover event occurs, the Security Access Manager appliance retrieves the session data information of the user from the DSC. It therefore maintains the existing session state. The primary master of the DSC cluster acts as the distributed session cache server, and the DMZ nodes act as the DSC client.

The master DSC cluster is on the Security Access Manager appliance that contains the Policy server, which must also be on the primary master if you want high availability. The Security Access Manager Policy server component can be hosted on the same machine as the embedded directory server (LDAP) component and can also be configured for high availability.

4.3 Web and federated single sign-on with an external user registry

A large company wants to achieve web SSO with on-premises web applications and federated SSO that is based on the SAML2 standard with several SaaS applications. The number of users does not allow the deployment of the embedded LDAP. The clients of the solution are browser-based devices, PCs, and notebooks.

4.3.1 Solution components

For the use case previously described, the company needs a license entitlement for Security Access Manager platform with the Federation add-on. The solution is an extension of the web and federated SSO use case, but it requires a separate deployment of the user registry nodes.

Figure 4-2 shows a schematic overview of the components that are required for this deployment pattern.

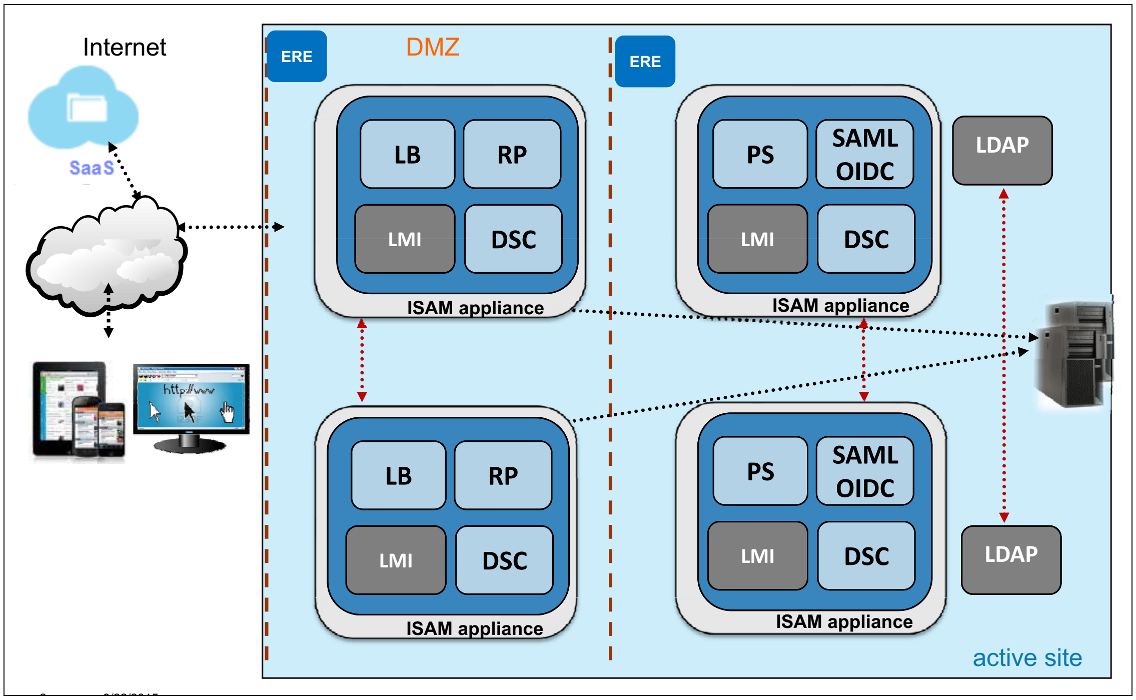


Figure 4-2 Deployment components for the federated and web SSO use case with an external user registry

4.3.2 Architectural considerations

The architectural considerations described in the Section 4.2, “Web and federated single sign-on use case” on page 45 are also applicable to this scenario. The user registry is externalized from the Security Access Manager appliance and requires a cluster and data replication mechanism. This replication process keeps the data in multiple directories synchronized providing redundancy of information.

The most common data replication patterns used are the *master-replica topology*, the *peer-peer topology* (also called the master-secondary), and the *master-forwarder-replica topology*. The user registry cluster mechanism is use of either an LDAP proxy or a virtual IP and corresponding heartbeat mechanism.

4.4 Context-based access use case

A large company wants to implement context-based authorizations (CBA) on web accesses. One-time password (OTP) tokens will be used as the second factor authentication to protect critical applications. The number of users does not allow the deployment of the embedded LDAP and runtime database. The clients of the solution are mobile devices, browser-based devices, PCs, and notebooks.

4.4.1 Solution components

The deployment of this scenario will require a license entitlement of Security Access Manager platform with the Advanced Access Control module add-on.

Figure 4-3 represents the deployment of the components required for this pattern.

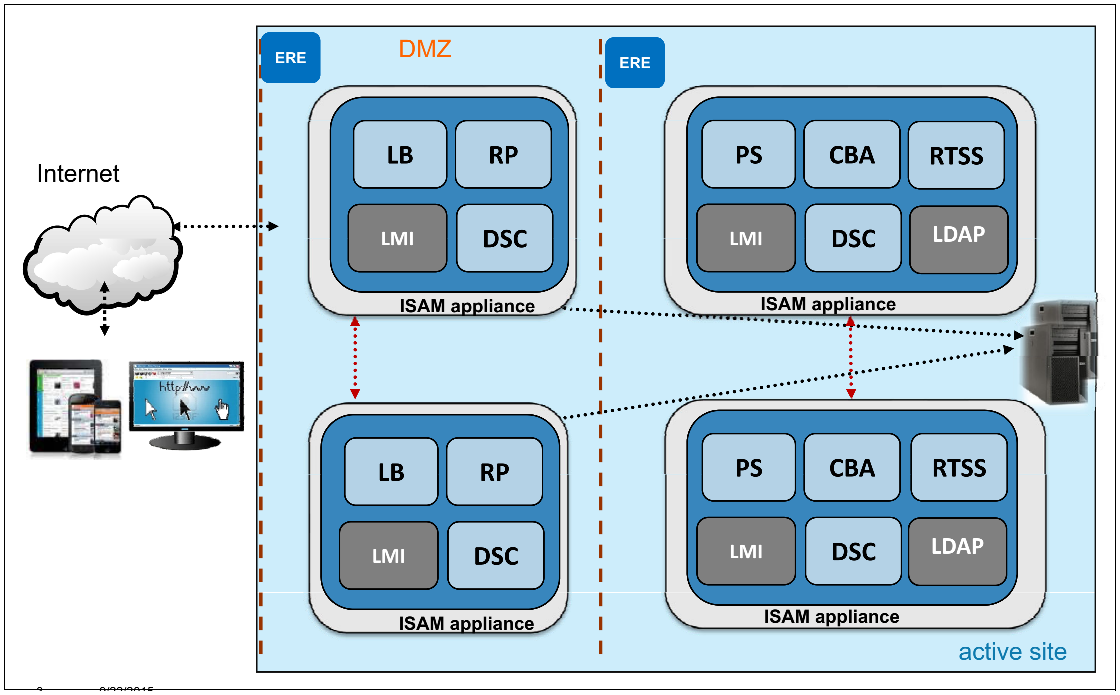


Figure 4-3 Activated components on the Security Access Manager appliances

4.4.2 Architectural considerations

The Advanced Access Control module will be deployed on the two appliances in the trusted zone. This allows the deployment of the runtime security service, which will enforce access policies attached to resources and the runtime database used for device fingerprinting.

The runtime security services external authorization service (EAS) on the Web Reverse Proxy component provides the policy enforcement point function for context-based access. The runtime security service (RTSS) evaluates and decides on the access policy.

The Advanced Access Control module RTSS component can also interact with third-party enforcement points such as IBM DataPower. The RTSS component interacting with the Web Reverse Proxy servers is load-balanced by the junction load balancing mechanism.

4.4.3 Clustering

Both the distributed session cache (DSC) and the runtime database cluster service are activated. The amount of data (such as, the number of registered devices registered, size of the fingerprinting and so forth), to be stored in the runtime database will determine if an external runtime database is required or not. Both the primary master for the DSC and the runtime database can be deployed on the same Security Access Manager appliance.

4.5 Summary

The pattern of multiple appliances in a single location enables you to deploy complex scenarios, ranging from web SSO, federate SSO, and mobile scenarios. The modules required (Security Access Manager platform, the Advanced Access Control module, and the Federation module) and the components required are determined by the use cases that clients need to support.

The distributed deployment of the Security Access Manager components and the clusters that can be configured allow deployment of the solution for high availability and disaster recovery throughout the single location. In cases where other disaster recovery requirements are applicable, deployment patterns in multiple data centers are to be considered.

5

Twin Data Center pattern

This chapter describes Twin Data Center deployments, which can be used to facilitate development of an identity and access management (IAM) and disaster recovery strategy and plans.

This chapter includes the following sections:

5.1 Introduction

Most global organizations run too many data centers in too many countries. This is normally the result of business expansion, either organically or through acquisition, over many years. Although the logic of business growth makes sense, having too many data centers results in excessive capital and operational costs, an overly complex architecture, and, in many cases, a lack of business and IT agility.

The Twin Data Center topology provides many benefits, in particular allowing for an adequate level of disaster recovery. The Twin Data Center topology can be through an active/active configuration where each data center splits the production and development work and can failover the load to the other site if there is a disaster.

For a Twin Data Center (TDC), the following approaches can be taken regarding the applications being serviced by the data centers. Figure 5-1 shows strict separation of applications between the TDCs.

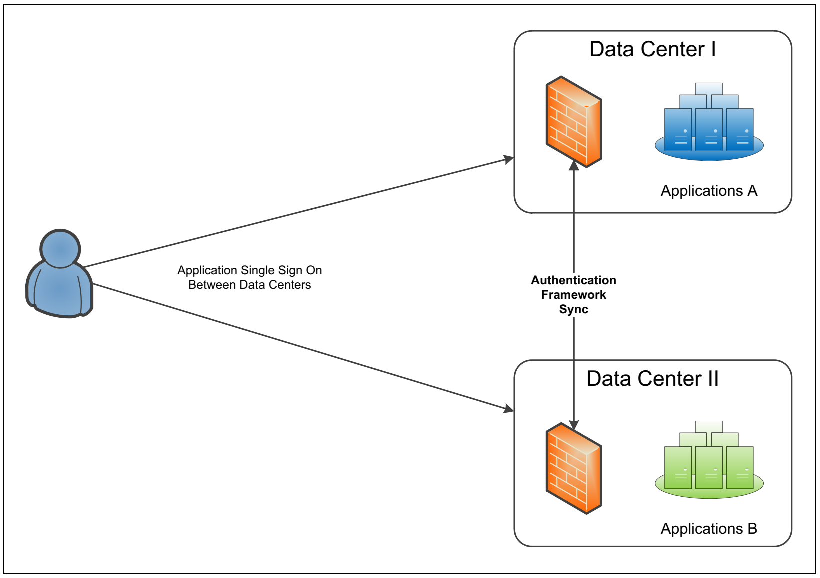


Figure 5-1 TDC with strict separation between data centers

This approach still requires that the IAM framework is synchronized between the data centers to allow for application single sign-on for the user.

Figure 5-2 shows application failover between TDCs.

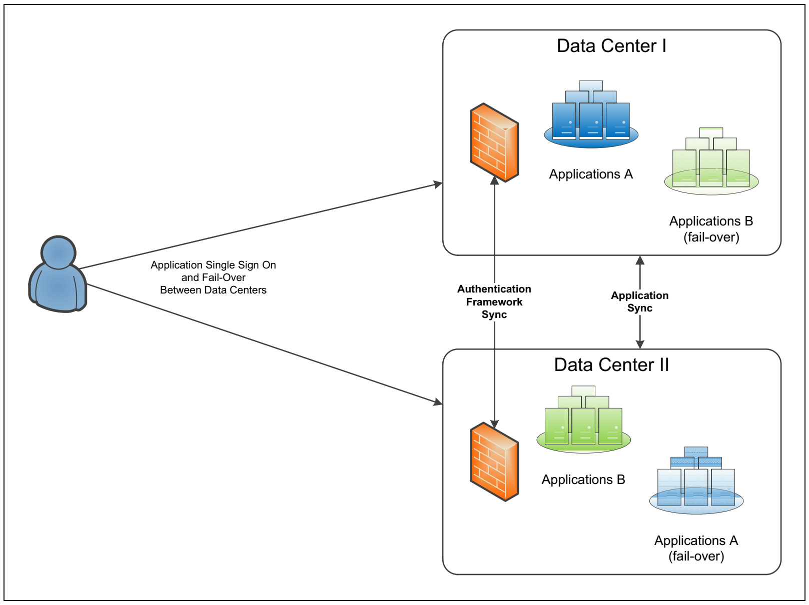

Data Center I
Applications A
Applications B (fail-over)
Application Single Sign On and Fail-Over Between Data Centers
Authentication Framework Sync
Application Sync
Data Center II
Applications B
Applications A (fail-over)

Figure 5-2 Application failover between TDCs

In this approach, the applications are split logically into two groups, with each group considered the primary application in one data center and the *standby* in the other data center. This architecture emulates a traditional Production Disaster Recovery site setup from the application point of view. Just as before, this approach requires the identity and access management framework to be synchronized between the data centers to allow for application single sign-on from a user point of view. Figure 5-3 shows a Full Twin Data Center.

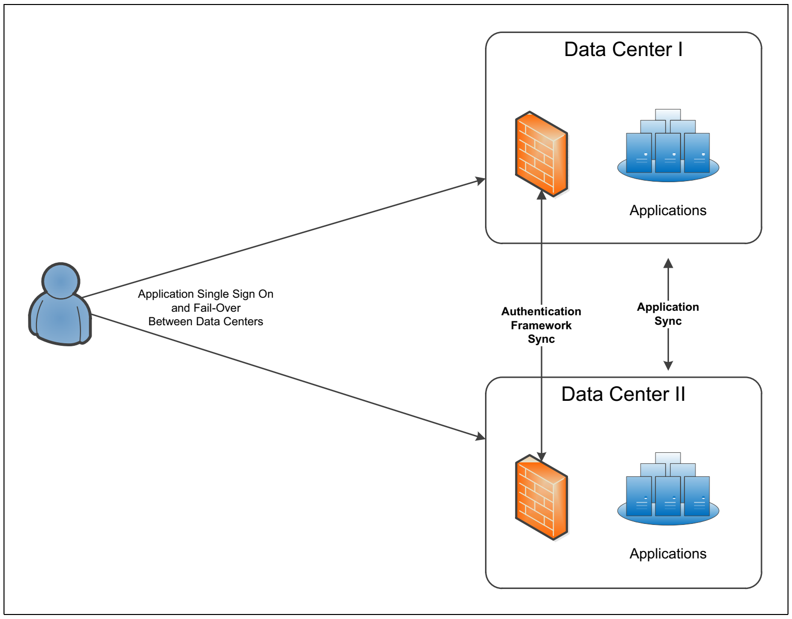

Data Center I
Applications
Application Single Sign On and Fail-Over Between Data Centers
Authentication Framework Sync
Application Sync
Data Center II
Applications

Figure 5-3 Full Twin Data Center

This approach balances all applications between both data centers. It is usually supported with a global load balancer, using this setup to provide *better service* to the user, by ensuring the user is accessing the "closest" data center. It also requires that the IAM framework is synchronized between the data centers to allow for application single sign-on from an user point of view.

5.2 Deployment use case

Company A is a large business with 2000 employees, servicing a customer base of millions of users. Company A provides web-based customer portals for its users and federated partners, which adds value for their customers. In addition, the company provides external facing employee portals to allow field personnel (agents) to access enterprise applications.

Company A wants to achieve a highly available and robust internet presence for the users and agents. They ensure this capability by using a Twin (east-west) Data Center deployment of its infrastructure. The customer-facing applications are serviced from both data centers. Agent applications are serviced from the East Coast data center, with the West Coast providing a standby capability.

This use case shows the Twin Data Center implementation of a Security Access Manager deployment. This deployment pattern can support any of the scenarios, and most large enterprise can use any combination or even all of the application deployment patterns. The key observation is that, from an access management point of view, the application pattern has only a small impact on the actual security component deployment.

5.2.1 Clustering

When considering clustering within the Security Access Manager Appliance, you have to look at the various levels of clusters within a given Security Access Manager deployment.

The main cluster (or appliance cluster), controls the Security Access Manager Policy server and the distributed session cache, which can be described by the following types of cluster members:

- Primary appliance

  This is the current controlling appliance for the cluster, all other cluster members register to that appliance and the appliance acts as the Policy server for the access manager deployment.

- Secondary, tertiary, and quaternary appliances

  These are appliances that are being replicated from the Primary and can take over functions of the Primary even if the Primary is down.

- Standard appliances

  These are configured to the cluster but are not dedicated as a potential primary. These appliances can be elevated to standby primaries, but the primary appliances must be available.

- Restricted appliances

  These are part of a cluster but have been restricted in their functions and cannot be elevated to a standby primary or a primary appliance. This action is to ensure that appliances in lower network zones can be deployed without a potential for advanced access to the cluster within the DMZ.

Figure 5-4 shows a typical appliance deployment and replication pattern for a Twin Data Center deployment.

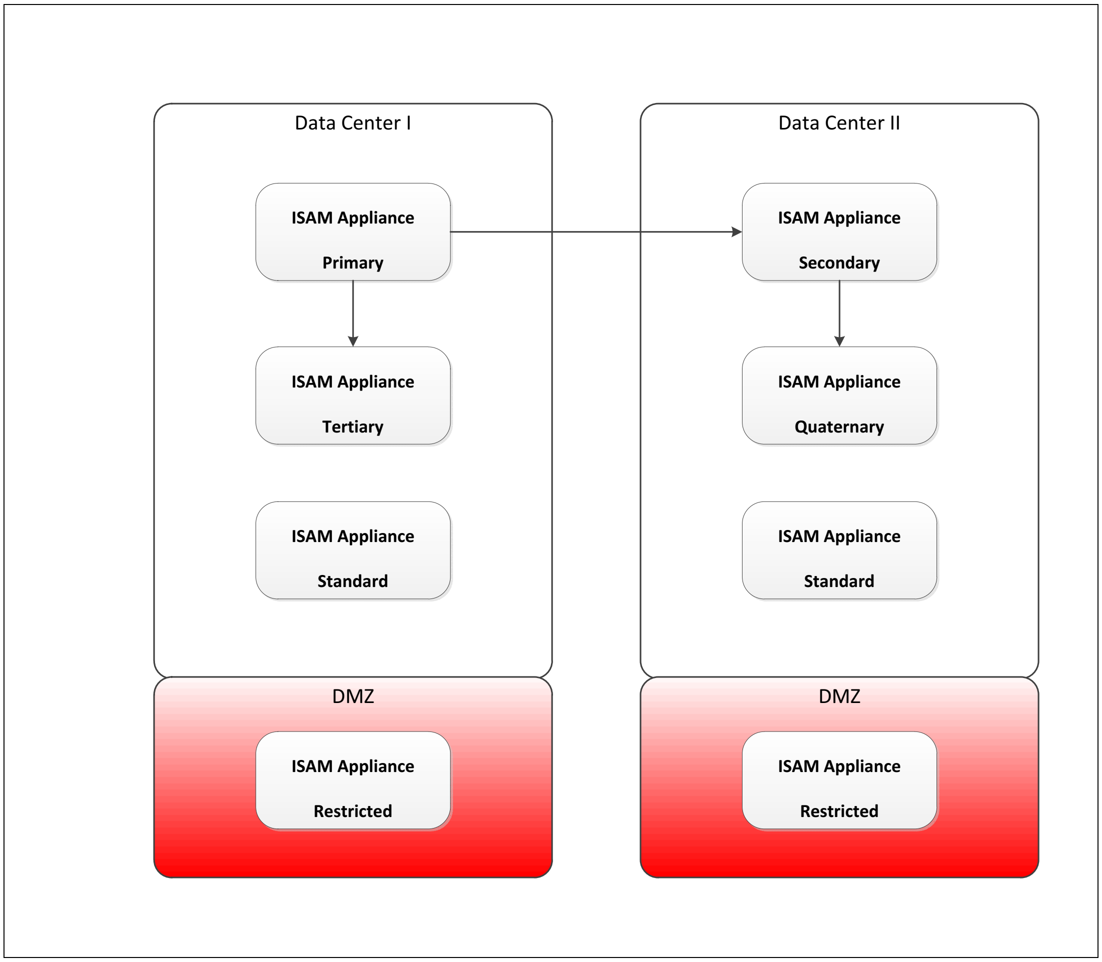


Figure 5-4 Typical appliance deployment and replication pattern for a TDC deployment

Note: There are two steps in the replication to the quaternary appliance. There is no appliance cluster replication to members of the cluster that are not marked as *master* and appliances that are not part of the cluster.

5.2.2 Name resolution or domain name services

Name resolution or domain name services (DNS) play a larger role within a Twin Data Center configuration than in a regular deployment. Various services require that they can be accessed on a single point (such as a Policy server) or accessed through the closest available service (such as a user registry).

Access to the closest resource can be achieved using load balancers or DNS resolution. This is a common practice in the Active Directory world, where a DNS name always resolves to the closest domain controller.

Services should be accessed by the components in the following ways:

- Primary cluster appliance

  There is only one, and all cluster members access this component.

- Policy server (on primary cluster appliance)

  There is only one Policy server and all configured clients access this component. (If the components are part of the cluster, a primary take over is automatic, if the component is not part of the cluster, the configuration needs to be changed manually.)

- Distributed session cache

  The distributed session cache can be access via any of the four master appliances. The components should access the master appliance in the respective (same) data center.

- Authorization server

  The Authorization server can be configured as a cluster across both data centers. The components should access the Authorization server in the respective (same) data center.

- Advanced Access Control (AAC)

  The Advanced Access Control module can be configured as a cluster across both data centers. The components should access the AAC service in the respective (same) data center.

- Federation

  The Federation module can be configured as a cluster across both data centers. The components should access the Federation module in the respective (same) data center.

5.2.3 Implementation details

This section describes and illustrates implementation details.

Conceptual diagram

Figure 5-5 shows the components and their deployment within the two data centers. Each component has redundancy within each data center. Most components are the primary point of contact for components within the same data center. Singular components, such as the Policy server, are the point of contact for all components.

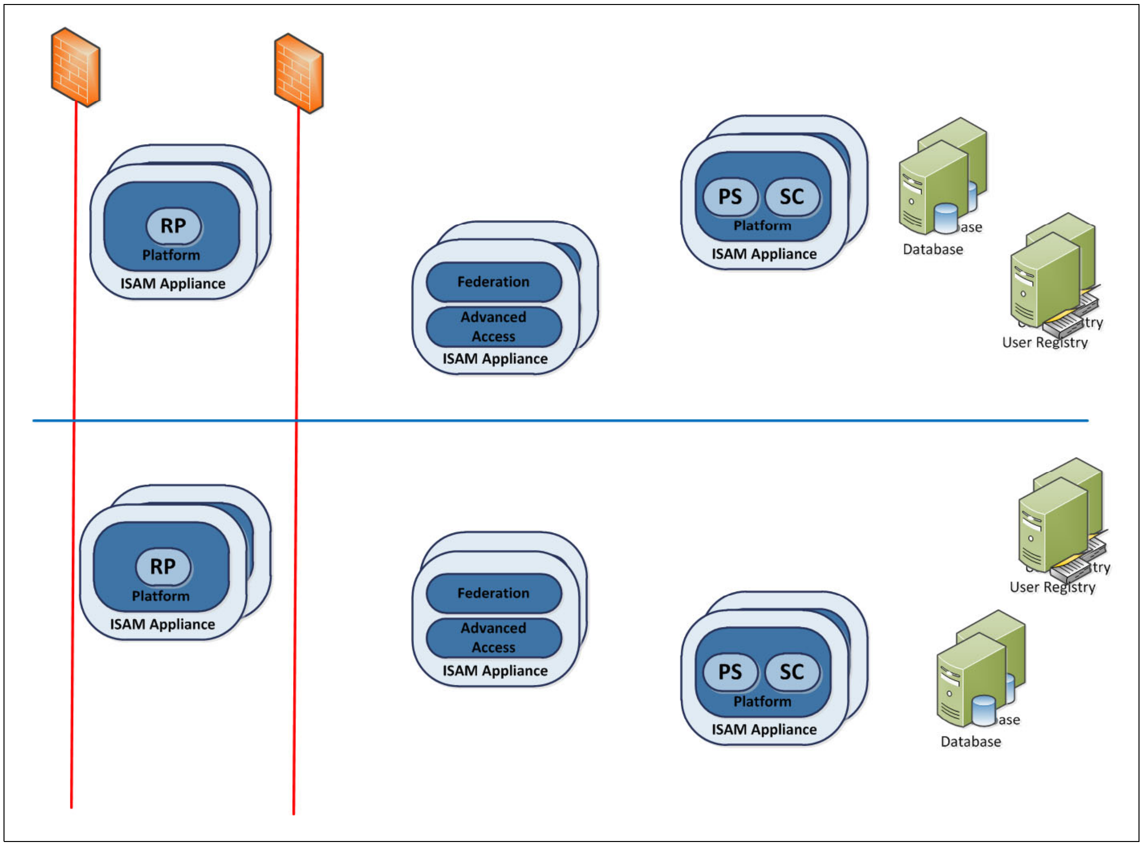


Figure 5-5 Components and their deployment within the two data centers

Data replication

Data replication for the user registry, database (AA), and the platform (PS, SC, also referred to as *DSC*) are performed between the components within the same data center and across data centers. Some of these replications might be bidirectional. See Figure 5-6.

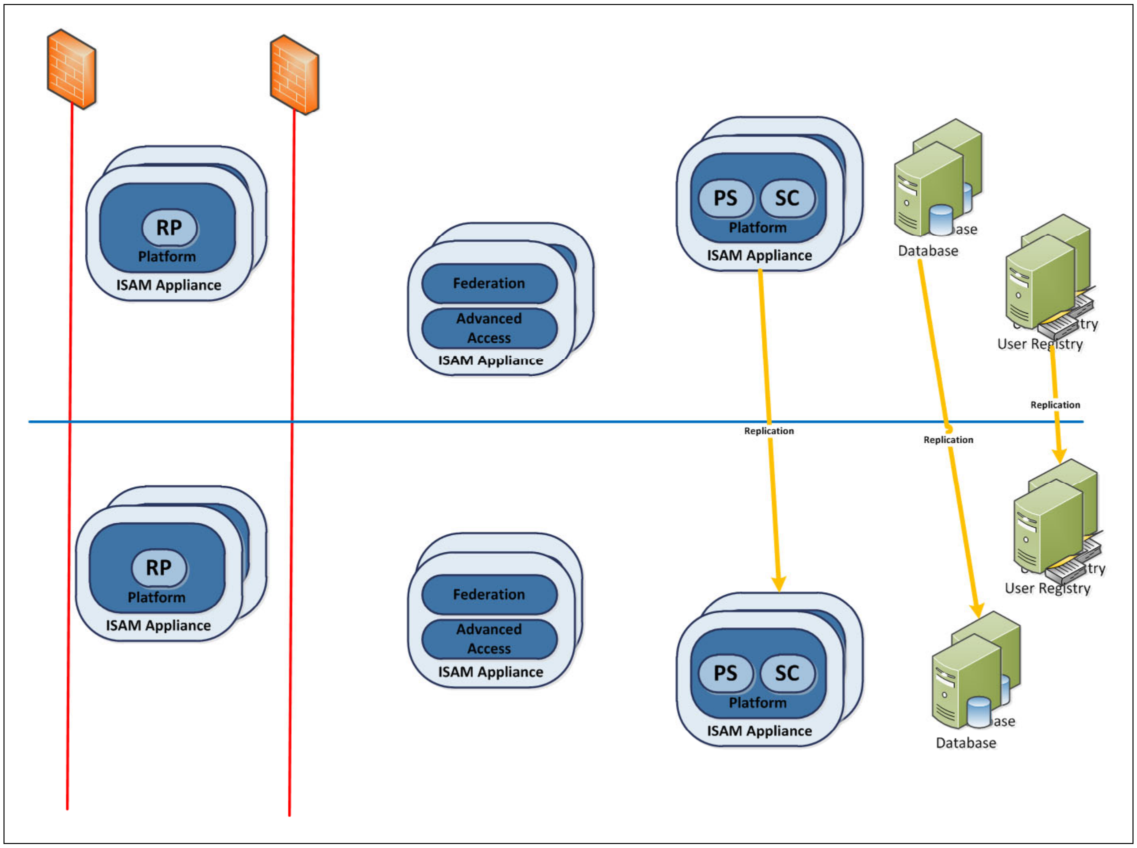


Figure 5-6 Data replication

Base policy administration and distribution

Policy administration interfaces, such as IBM Web Portal Manager (IBM WPM®) and **`pdadmin`**, exist on multiple components but communicate with the primary cluster master, which is the Policy server (PS). The Policy server manages the policy and distributes it to the clients. The policy distribution is from a single point to all members that are registered as Security Access Manager servers. See Figure 5-7.

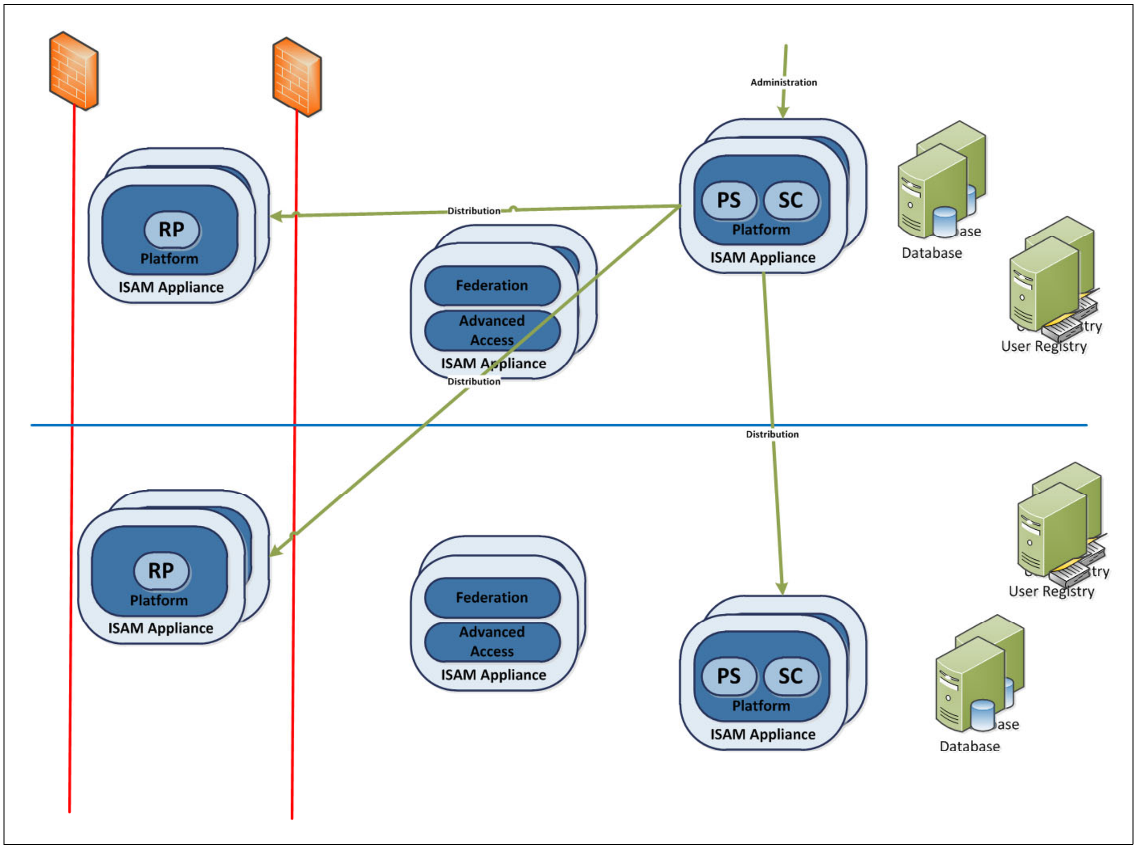


Figure 5-7 Using the Policy server

Federation and advanced access administration and distribution

Policy administration for the Federation and Advanced Access (F/AA) controls are performed on the master appliance for the F/AA cluster. The policies are stored in an external database that is replicated across the data center. Each F/AA partner uses the closest database to make access decisions. See Figure 5-8.

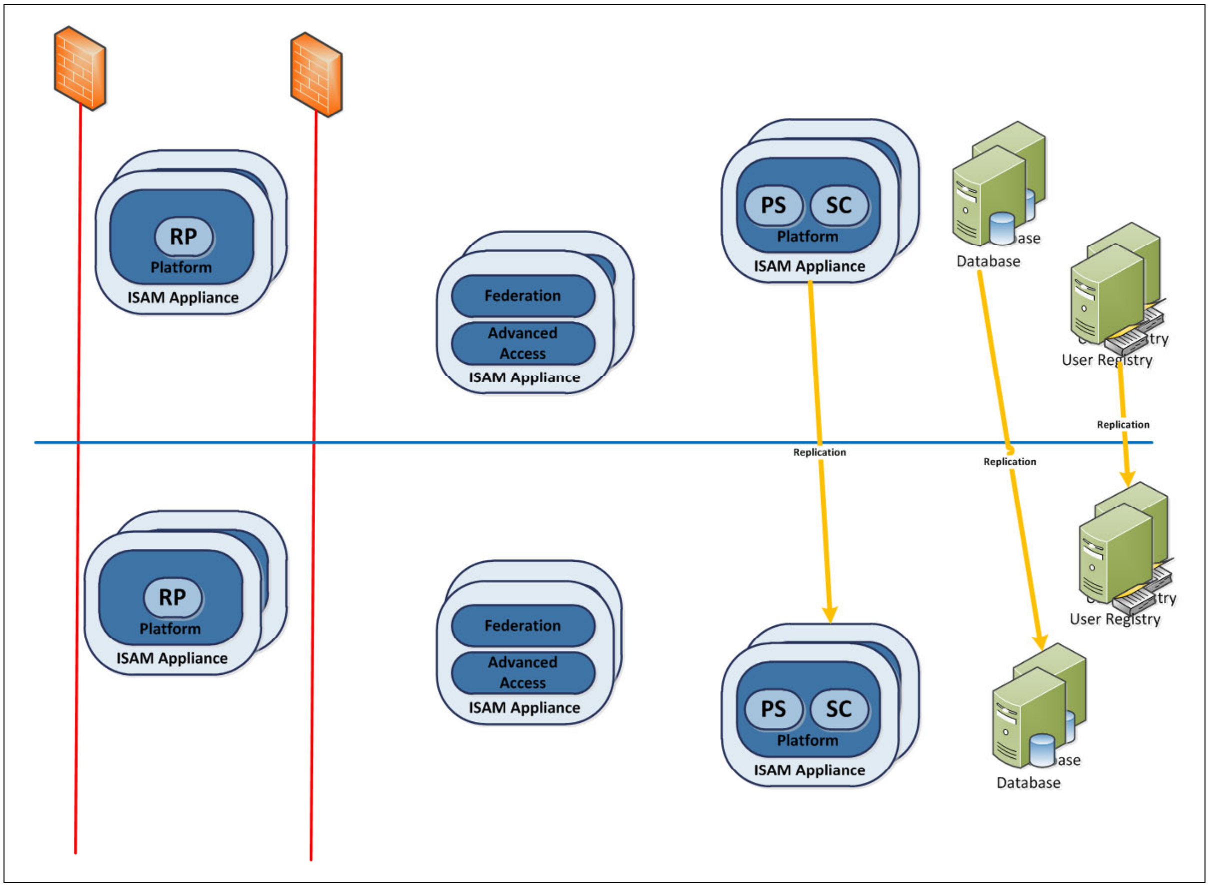


Figure 5-8 Policy administration for Federation and Advanced Access

Authentication

The point of contact for the authentication is the Web Reverse Proxy (RP). The RP contacts the user registries to perform the initial authentication, session creation and authorization. It might contact the Advanced Access module (CBA or OAuth) or Federation (junction) if the security policy demands that. These Federation or Advanced Access (F/AA) components, in turn, might access their databases or additional policy information points, as needed. See Figure 5-9.

Each of the RPs is configured into the SC, so users have a seamless experience regardless of which RP they access.

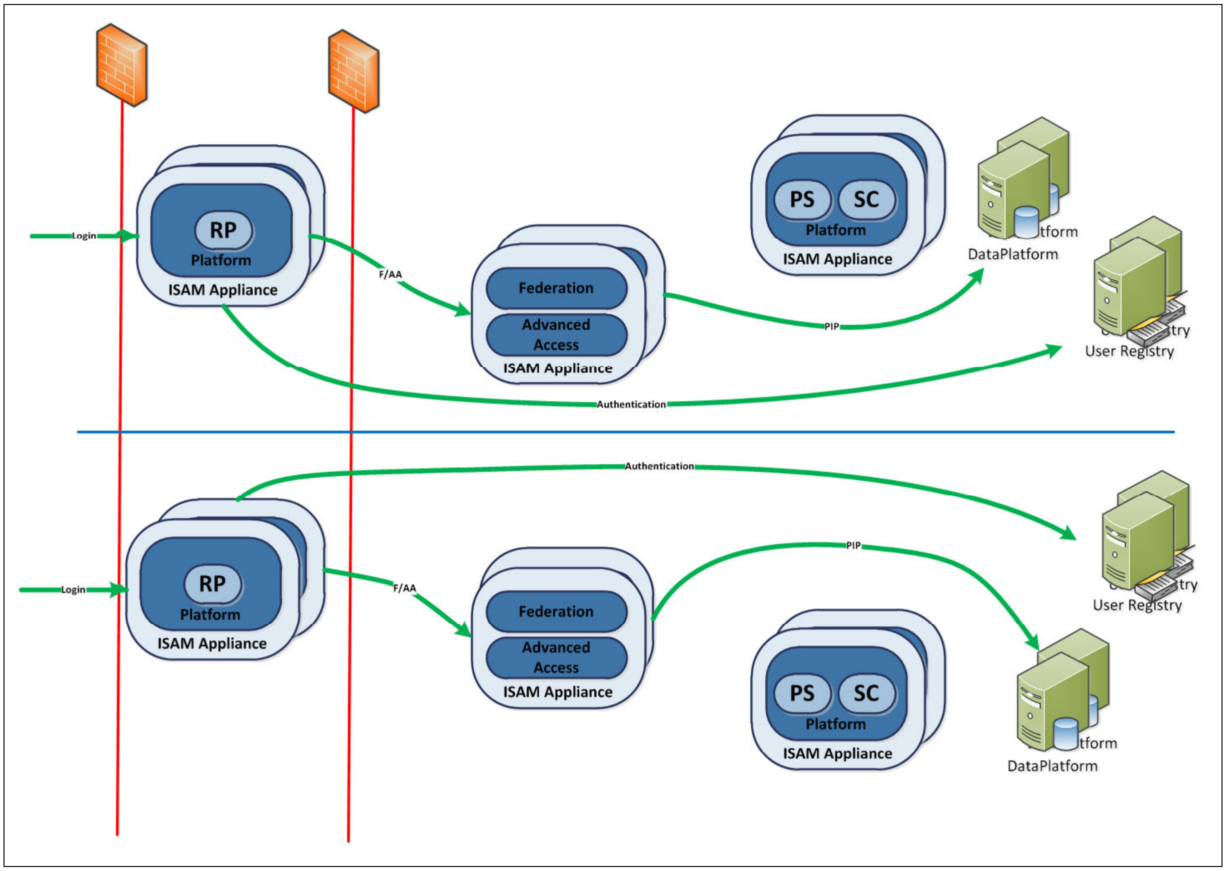


Figure 5-9 Access via the reverse proxy

Session management

To achieve single sign-on between all RP servers, the SC is enabled. The SC service is enabled on the cluster master appliances inside of the trusted network. Sessions are created during authentication and used during access validation. The RP server uses the SC servers in the same data center and the SC servers replicate the session state between each master appliance in the cluster. See Figure 5-10.

Sessions can be managed from any cluster member by using the **`pdadmin`** command-line tool or the REST management interface.

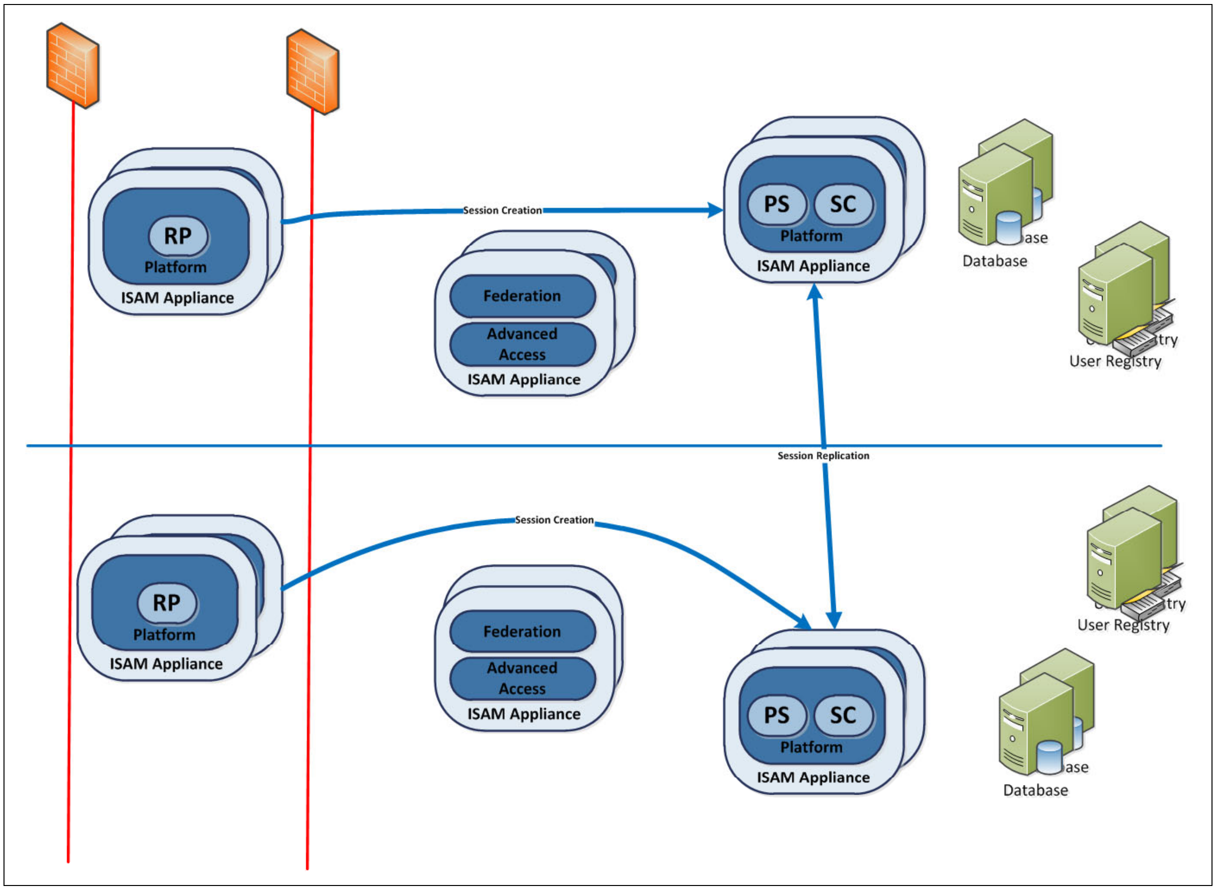


Figure 5-10 Enable single sign-on between all RP servers using the distributed session cache

5.2.4 Disaster recovery

With the proliferation of multiple data center implementations, business continuity and disaster recovery needs to focus not just on the security infrastructure, but also start looking at how that security infrastructure supports the applications that are mapping to the business. Both IT and the business decision makers need to establish processes and procedures that provide a broader approach to ensure business continuity and be sure that disaster recovery procedures are implemented.

The description in this chapter about Twin Data Center deployments can be used to facilitate the development of an identity, access management, and disaster recovery strategy and plan.

5.3 Summary

The Twin Data Center topology can be through an active/active configuration, where each data center splits the production and development work and can fail over the load to the other site in the event of a disaster. This topology provides many benefits. In particular, it allows for an adequate level of disaster recovery.

In this chapter we reviewed the implementing considerations for this topology within the context of a use case example.

6

Security Access Manager and DataPower integration patterns

This chapter describes the integration patterns that are addressed through integration of IBM Security Access Manager, IBM DataPower Gateway, and IBM API Management solutions.

This chapter includes the following sections:

6.1 Introduction

Historically, industry trends have dictated several different gateway technologies deployed as network protection devices within an organization’s firewall configuration for securing local area networks (known as a DMZ) or internal trusted network zone. This situation has resulted in production environments with several different technologies (often not integrated) acting as security gateways. This approach has increased the complexity and, therefore, the cost of maintaining Internet-facing services.

As a result of this complexity and the recognition that reduced complexity improves defense for Internet-based attacks, IBM embarked on a technology convergence strategy for service hosting. The initial concern was mobile device access, so the focus was on the convergence of IBM DataPower Gateway and IBM Security Access Manager’s reverse proxy solution.

6.2 Integration strategy

Mobile device proliferation has resulted in the IT industry and organizations considering more effective means of exposing services to consumers. The traditional service-oriented architecture (SOA) domain focused on business-to-business use cases, but the complexity associated makes SOA and its security model unsuitable for large-scale adoption.

The mobile requirements demand that organizations expose data and services through application programming interfaces (APIs) to potentially millions of devices. Invoking these APIs by using lightweight protocols, such as REST, has resultd in new requirements for securing these protocols, with the entry point to an organization being deployable components in the appropriate network zone.

This demand has led to a new range of technology solutions related to IBM API Management. From a security perspective, overlapping capabilities within DataPower Gateway appliances and Security Access Manager are required. A convergence strategy has resulted in the release of Security Access Manager capabilities for DataPower Gateway. The converged capability is managed by a DataPower Gateway add-on called IBM Security Access Manager for DataPower. It is available to existing DataPower customers as a separately licensed add-on capability. This capability enables both web and mobile traffic to be hosted through the same point of contact.

6.3 Architectural components and personas

Figure 6-1 shows the components and personas (roles) that are involved in the different use cases that are supported by this converged offering. The sections that follow highlight the scenarios that are supported and explain how the components and personas interact to address business requirements.

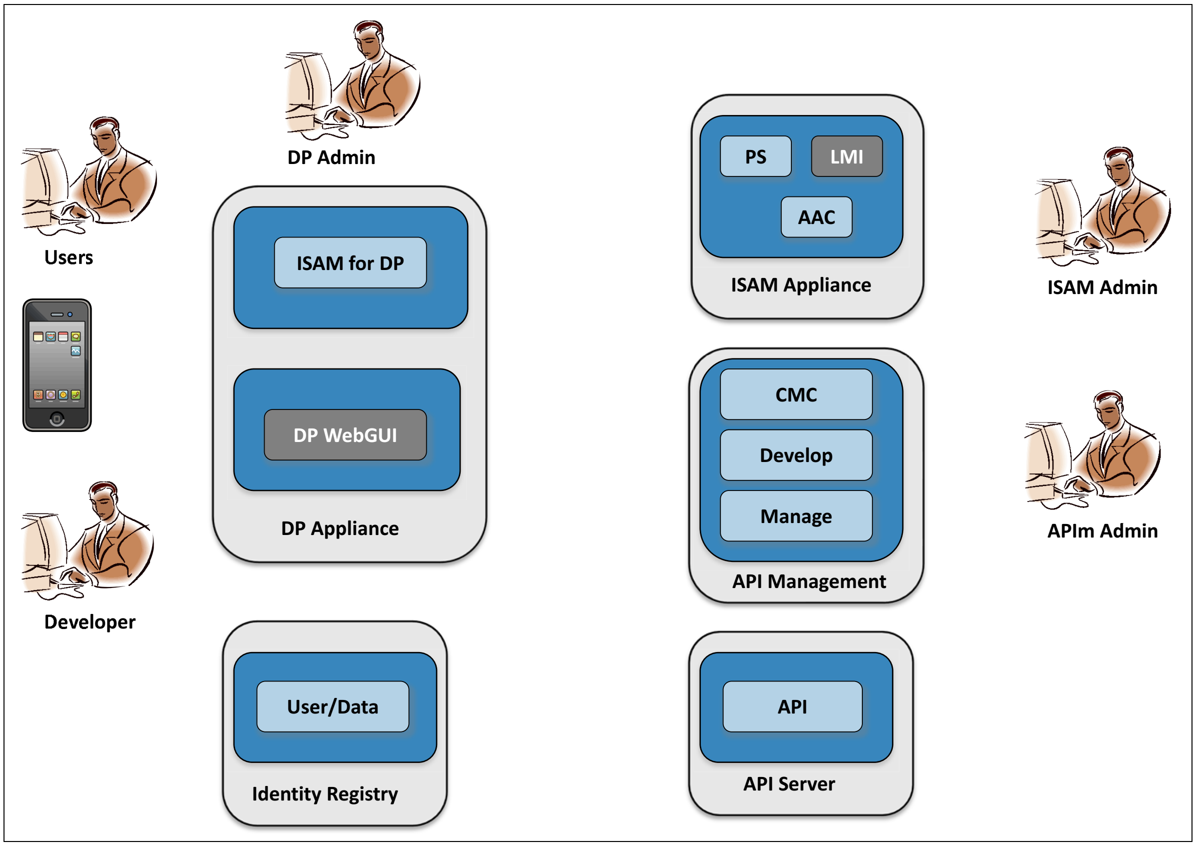


Figure 6-1 Deployment components

The following list describes the components and personas shown in Figure 6-1.

- IBM Security Access Manager (platform) (shown as ISAM Appliance in Figure 6-1)

  Security Access Manager is an appliance-based solution that enables secure user and device access to Internet-hosted services. It is a platform that organizations rely on to protect their web-based services. Security Access Manager provides critical user access management for web, mobile, and cloud services.

  In comparison to DataPower Gateway, Security Access Manager focuses on the security of the user and the policies associated with that user accessing resources. It provides a scalable enforcement point, single sign-on, session management, coarse-grained authorization, and comprehensive protection against evolving web application threats.

- IBM Security Access Manager Advanced Access Control (shown as AAC in Figure 6-1)

  Advanced Access Control is the licensed module of the Security Access Manager platform appliance. The relevant components for this pattern are OAuth support, device registration, fingerprinting, context-based access, and multifactor strong authentication support.

- IBM DataPower (shown as DP Appliance in Figure 6-1 on page 67)

  IBM DataPower multichannel appliances are a family of network devices that can help accelerate XML and web service deployments while extending SOA infrastructure. These appliances are used in a variety of user scenarios to enable security, control, integration, and optimized access for a range of workloads, including mobile, web, API, business-to-business (B2B), web services, and SOA.

  DataPower appliances have capabilities to control, and optimize the network availability and security in a secure and integrated fashion. Secure, Integrated, Control, and Optimize the network availability and security. DataPower ensures that security standards and policies are appropriately implemented. Therefore, it provides a policy-based solution for ensuring secure interoperability of these services.

- IBM API Management (shown as API Management in Figure 6-1 on page 67)

  IBM API Management provides a developer portal, API analytics, and development acceleration for the DataPower Gateway platform. This product is introduced in this section to highlight the integration between IBM Security Access Manager and IBM API Management.

- IBM Security Access Manager for DataPower (shown as ISAM for DP in Figure 6-1 on page 67)

  The IBM Security Access Manager for DataPower module provides the reverse proxy component that enables centralized user authentication and coarse-grained authorization, advance session management, web single sign-on (SSO), enforcement of context-based access and mobile SSO policies, and strong authentication, including one-time password and multifactor authentication.

6.3.1 Personas

The following personas were introduced in Figure 6-1 on page 67:

- Users

  The organization’s customers or staff who are operating browsers or mobile apps that are running on devices

- DP Admin

  Administers the DataPower Gateway SOA appliance

- Security Access Manager (SAM) Admin

  Administers appliance instances, configuration of components and access policy of the components hosted on the appliance

- IBM API Management (APIm) Admin

  Creates, manages, and secures use of business services from select developer communities.

- Developers

  Develops using the self-service API published by IBM API Management for use in applications

6.4 Integration use cases

There are three distinct use cases for the integration of Security Access Manager and DataPower Gateway:

- Web and IBM API Management Convergence

  This use case is the collocation of web and SOA-based services on a single set of gateway appliances. The primary use case is service consolidation.

- Enhanced IBM API Management

  This use case addresses the requirement for integrating the DataPower Gateway platform with IBM Security Access Manager for Mobile as a policy decision point (PDP), guided through the creation, publication, and management of an API.

- Advanced API and Access Management

  This use case addresses the requirement for adding advanced access management capabilities to a mobile use case.

The following sections outline these use cases and deployment patterns.

6.4.1 Converged multi-channel platform for mobile, web and SOA workloads

Company A is an enterprise organization with over 100,000 customers. Company A has DataPower Gateway hosted demilitarized zone (DMZ) as a policy enforcement point (PEP) for traditional B2B web services. The DataPower Gateway instances have capacity to host additional services, and the team is considering hosting the Internet Banking web and mobile applications. With Security Access Manager for DataPower capabilities added to these appliances, the DataPower Gateway can add enterprise grade Web Reverse Proxy capabilities to host this additional Internet traffic. This is an opportunity to use existing investment in DataPower Gateway and internal team skill set to Security Access Manager capabilities.

IBM Security Access Manager for DataPower is an integrated software module for DataPower Gateway that provides access management security for web, mobile and cloud workloads. It enables a single, converged gateway solution for securing an organization's current and future business channel needs.

Relevant personas

The following personas are introduced:

- Users

  The organization’s customers or staff who are operating browsers or mobile apps that are running on devices

- DP Admin

  Administers the DataPower SOA appliance

- Security Access Manager (SAM) Admin

  Administers appliance instances, configuration of components and access policy of the components hosted on the appliance

Conceptual diagram

Figure 6-2 shows the components and interaction points between the components in a deployment.

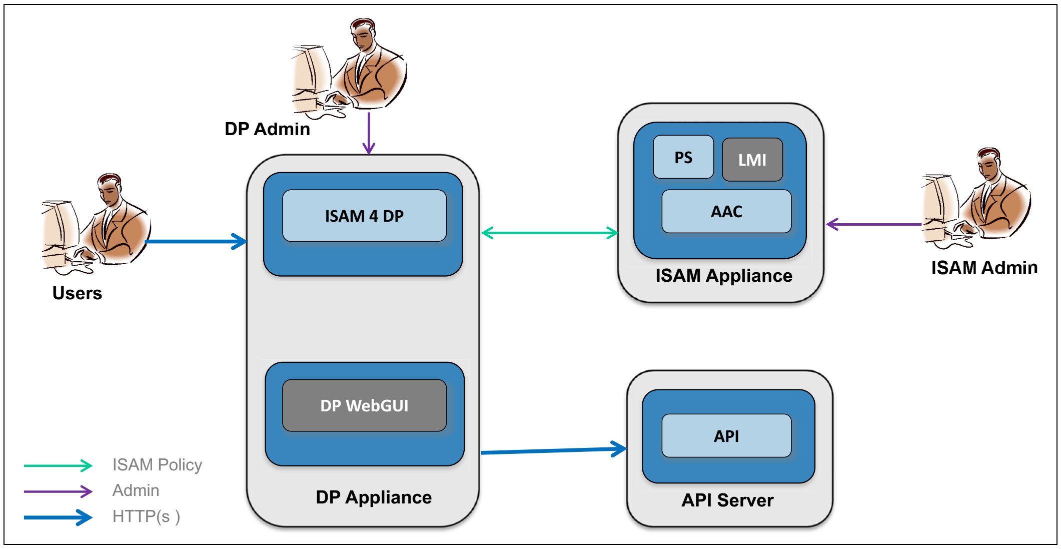


Figure 6-2 Convergence use case

The components shown previously in Figure 6-2 use the following functional configurations:

- IBM Security Access Manager for DataPower is configured with Security Access Manager for reverse proxy.
- APIs are published on API Management server (API server), as shown in Figure 6-2, and are accessible through Security Access Manager for DataPower.
- Security Access Manager platform appliance is configured with a Policy server for reverse proxy to communicate and advance access control, optionally, for extended policy decisions.

Sequence diagrams

Figure 6-3 shows the sequence diagram for the convergence use case.

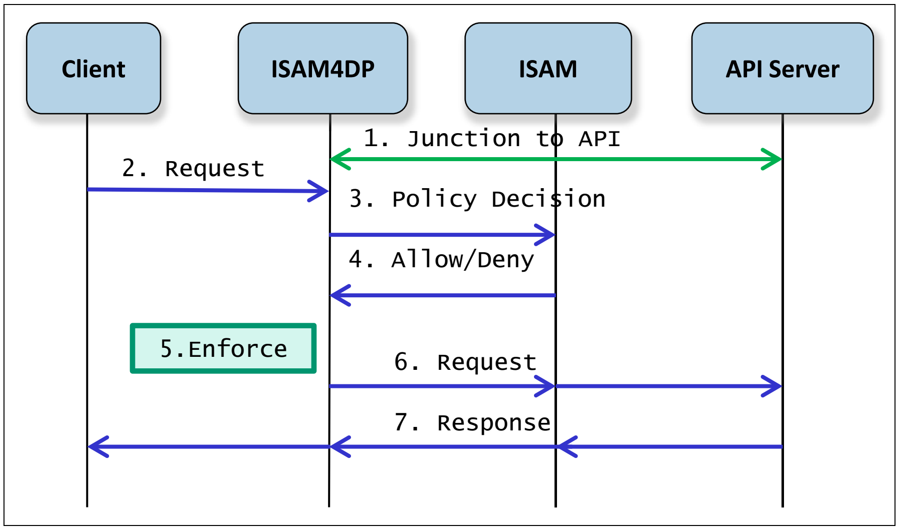


Figure 6-3 Sequence diagram for the convergence use case

For this workflow, Company A is using existing DataPower Gateway resources to host Security Access Manager Reverse Proxy instances. The workflow description of Figure 6-3 on page 70 involves the following details:

1. Security Access Manager reverse proxy creates connections to backend APIs (as Security Access Manager junctions). This action allows the Security Access Manager for DataPower component to ensure that the user access control policies are satisfied before being passed to the API (or web) server. These connections to backend APIs guide the runtime flow.
2. A client (browser or device) sends an HTTP request to this junction on the reverse proxy.
3. The request is authenticated by Security Access Manager for DataPower (to a configured directory) and makes an authorization decision that is based on the configured policy. Optionally, it can use the IBM Security Access Manager Advanced Access Control module. In this optional case, Security Access Manager Advanced Access Control sends an allow or deny decision.
4. Security Access Manager for DataPower acts as an enforcement point, based on the decision and the scope provided by the Security Access Manager Advanced Access Control.
5. The request is forwarded to be serviced from the API (or web) server.
6. The response page is relayed through Security Access Manager for DataPower to the client.

Key business benefits of integration

By combining the access management features of IBM Security Access Manager for DataPower with the message-level security, IT platform security and application integration of DataPower Gateway, Company A can implement a single security gateway for the following instances:

- Centralized user authentication and coarse-grained authorization
- Session management and web single sign-on (SSO)
- Context-based access and mobile SSO
- Strong authentication, including one-time password and multifactor authentication

The company can maximize their investment in the DataPower Gateway platform by using available resources for hosting and securing their web traffic.

6.4.2 Enforce and manage access to API services

Company A has DataPower Gateway deployed as an API gateway. This gateway allows the organization to expose their data and web content through APIs while ensuring that appropriate security controls are applied at this gateway. An enterprise deployment mandates that management controls around these APIs be centralized to cater for the nonfunctional aspects of a production deployment. This includes the ability to set policies across a cluster of enforcement points, manage versions of APIs, and control the entitlements to access them.

High-level solution proposal

When deploying APIs in a cluster, access mechanisms mandate the use of a persistent data store to provide a consistent way to manage entitlements that are distributed to registered client devices. Security Access Manager Advanced Access Control includes an authorization server that can provide this persistence.

Security Access Manager has junctions that connect with the backend. Therefore, DataPower Gateway is able to provide the policy enforcement point (PEP) capabilities by using the Security Access Manager Advanced Access Control authorization service to validate clients' requests to an API. The Security Access Manager Advanced Access Control service is then able to provide token management capabilities to the user.

Relevant personas

The following personas are referenced in this scenario:

- Users

  The organization's customers or staff who are operating browsers or mobile apps that are running on devices

- Security Access Manager Admin

  Administers appliance instances, configuration of components and access policy of the components hosted on the appliance

- Developers

  Develops web applications by using the self-service API published by IBM API Management for use in applications.

Conceptual diagram

Figure 6-4 shows the components and interaction points among the components in a deployment.

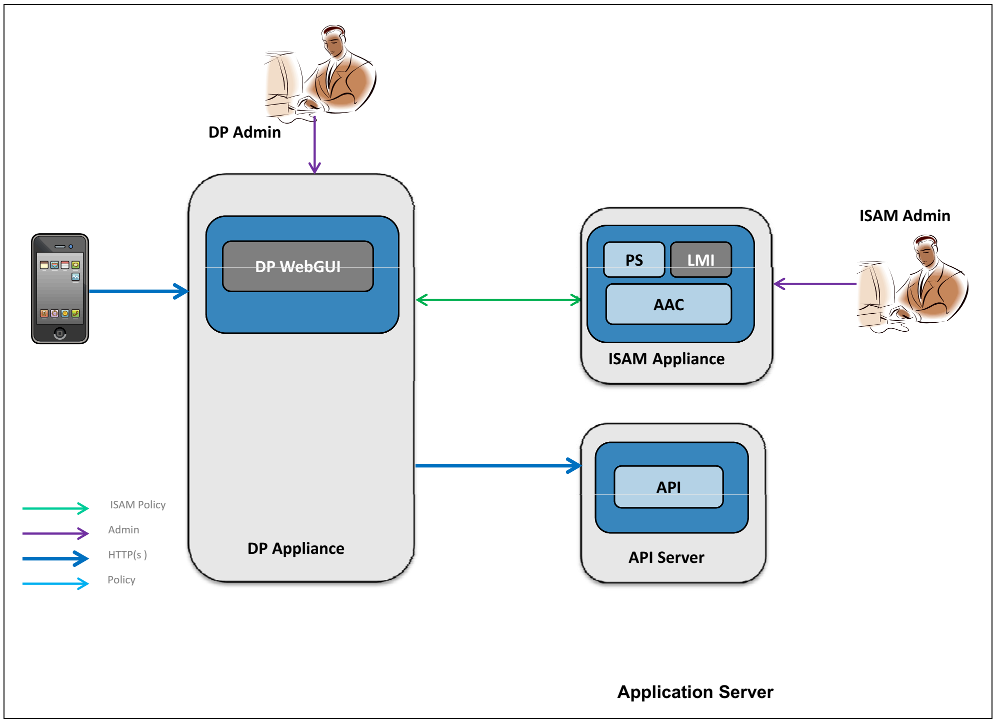


Figure 6-4 Enforce and manage use case

The functional configuration of each component in this use case is as follows:

- Security Access Manager for DataPower is configured with Security Access Manager reverse proxy.
- Security Access Manager platform appliance is configured with Policy server for reverse proxy to communicate.
- APIs are published on API Manager and are accessible through DataPower and protected by OAuth.
- Security Access Manager for DataPower reverse proxy has junction configured to route requests through DataPower API Gateway configuration.
- Security Access Manager appliance is configured with advance access control optionally for extended policy decisions.
- Security Access Manager Advanced Access Control feature provides an OAuth data store to persist OAuth tokens and to revoke and manage permissions when necessary. Security Access Manager Advanced Access Control is configured as the Authorization server for access to APIs through DataPower.

Sequence diagram

The sequence diagram for this use case is shown in Figure 6-5.

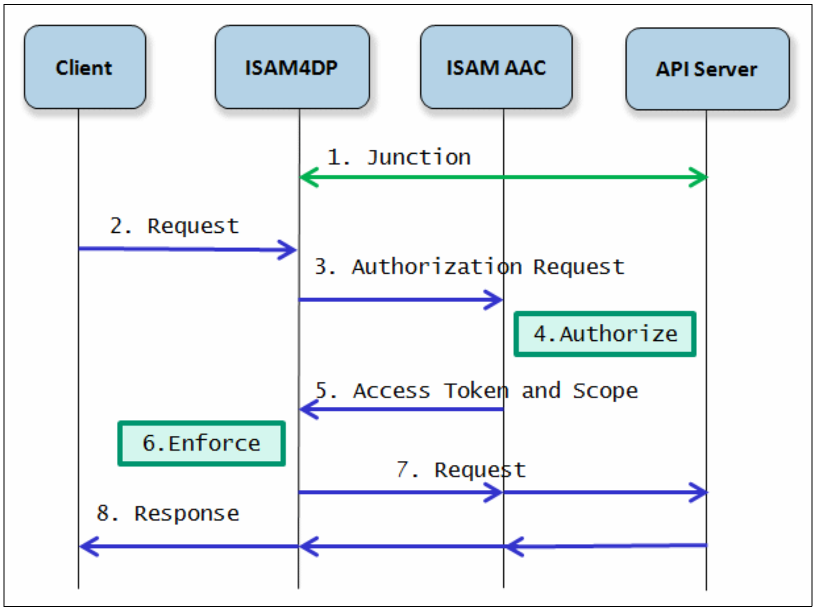


Figure 6-5 Sequence diagrams enforce and manage use case

For this workflow Company A has DataPower Gateway acting as an enforcement gateway, Security Access Manager module offers fine grained authorization to these APIs managed the IBM API Management. Figure 6-5 involves the following workflows:

1. Security Access Manager on DataPower Gateway have junctions to the backend API.
2. Clients request the API through the Security Access Manager reverse proxy junction, which is hosted on DataPower Gateway.
3. Authorization requests for the APIs are forwarded to Security Access Manager Advanced Access Control for access with client ID and the client secret.
4. Security Access Manager Advanced Access Control performs relevant checks and authorizes.

5. Security Access Manager Advanced Access Control grants the access token and scope.
6. DataPower Gateway enforces access, based on the authorization decision and the scope provided.
7. The request is then serviced through IBM API Management and the backend.
8. The response is serviced through reverse proxy to the client.

Key business benefits of integration

With this integration in place, DataPower Gateway provides the ability to manage runtime access entitlements for deployments that use the OAuth protocols. Because Security Access Manager Advanced Access Control persists OAuth tokens into a manageable data store, the user or an administrator can revoke these tokens at any time. This capability is particularly important in a mobile use case to mitigate the risks associated with *lost*, *sold*, or *stolen* devices.

6.4.3 Enforce multifactor or context-based access to API services

This scenario enhances previous use case to include Advanced Access Control capabilities using API Management.

Company A provides insurance and banking services through an API-based solution hosted by DataPower Gateway. Authorization capabilities vary across the deployed services. In some instances course-grained API entitlements suffice. For example, finding the closest ATM does not require user access management or access to APIs for balance checks from financial consolidation applications.

However, more advanced use cases exist where the user authorization must consider device characteristics (such as malware presence) and user-based entitlements. When Company A exposes all of these capabilities on a single banking service, each API has different levels of risk, varying from single factor authentication to the ability to monitor and handle fraud.

High-level solution proposal

To maintain risk-based access, Company A has Security Access Manager for DataPower as a reverse proxy instance co-hosted on DataPower Gateway. This means that they have both web and API access through the same Internet-based channel. Access to the hosted applications and APIs can then be varied based on the security requirements, allowing a broad range of client device capabilities to access the web and API services.

For mobile access, APIs can be managed by the IBM API Management capabilities, and user and device context can be used to enforce appropriate access controls. The result is a deployed solution that can handle for both API entitlements and user-based access control at the gateway. The solution also offers the ability to implement two-factor authentication mechanisms and fraud and threat protection for the highest-risk exposed services.

Relevant personas

The following personas are referenced in this scenario:

- Users

  The organization’s customers or staff who are operating browsers or mobile apps that are running on devices

- Security Access Manager (SAM) administrators

  Administers appliance instances, configuration of components, and access policy of the components hosted on the appliance

- Developers

  Develops web applications by using the self-service API published by IBM API Management for use in applications

- IBM API Management Administrators

  Manage and enforce use of business services from select developer communities

Conceptual diagram

The following diagram shows the components and interaction points between the components in a deployment.

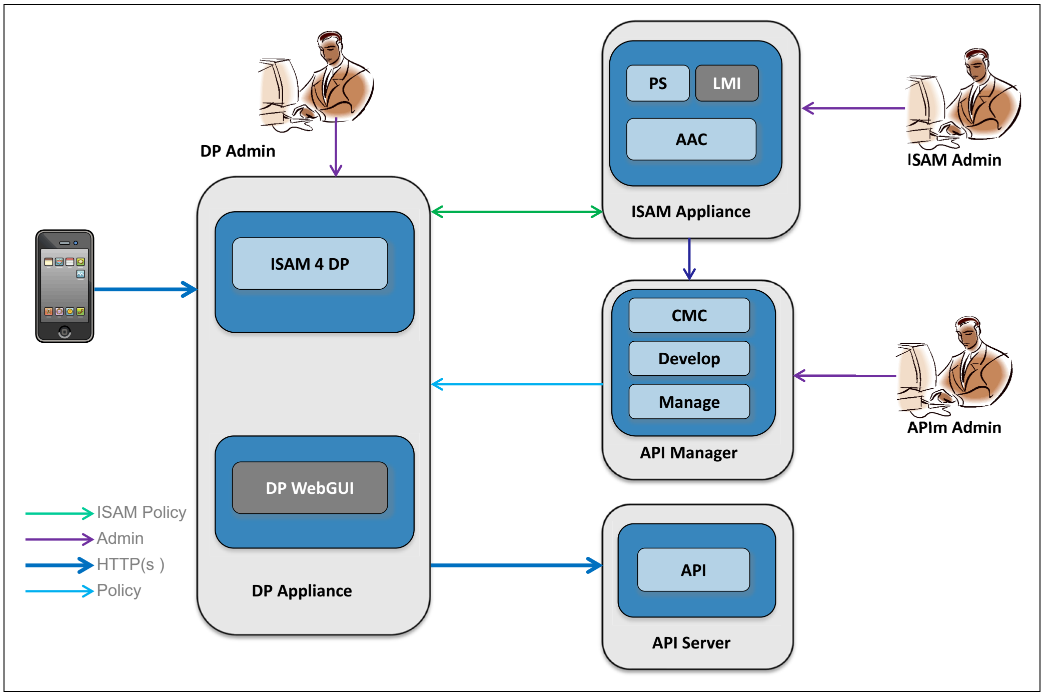


Figure 6-6 Context-based access use case

The components shown in Figure 6-6 have the following functional configurations:

- Security Access Manager for DataPower is configured with Security Access Manager reverse proxy.
- Security Access Manager platform appliance is configured with Policy server for reverse proxy to communicate.
- APIs are published on API Manager and are accessible through DataPower and protected by OAuth.
- Security Access Manager for DataPower reverse proxy has a junction configured to route requests through DataPower API Gateway configuration.
- Security Access Manager appliance is configured with advance access control (optional) for extended policy decisions.
- Security Access Manager Advanced Access Control provides an OAuth data store to persist OAuth tokens, revoke and manage grants when necessary. Security Access Manager Advanced Access Control is configured as the Authorization server for access to APIs through DataPower.

- Security Access Manager Advanced Access Control is also configured to perform context-based access decisions related to APIs through the Security Access Manager junctions and policies that are attached to the various endpoints on that junction.

Sequence diagram

This section outlines both the management and the runtime sequences.

Figure 6-7 shows the management sequence diagram.

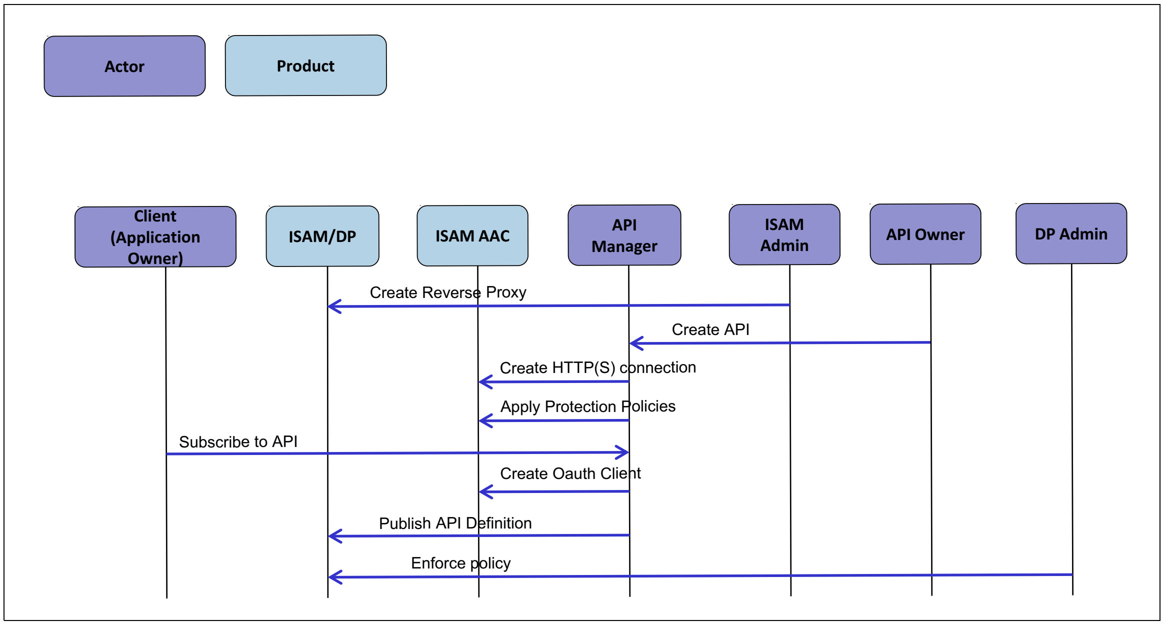


Figure 6-7 Context-based access management workflow use case

Figure 6-8 shows the runtime sequence diagram.

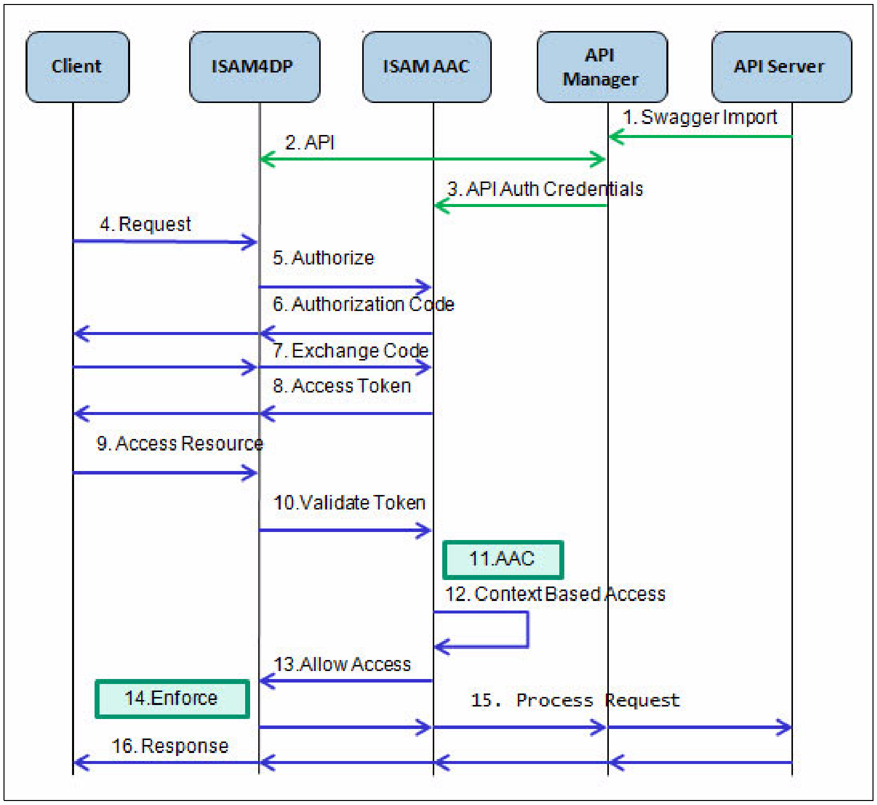


Figure 6-8 Context-based access runtime workflow use case

For this workflow, consider an application that uses Company A's exposed API for accessing the financial data of a user. What follows is a description of the workflows that are shown in Figure 6-8:

1. Swagger Import is one of the standard methods of deploying API resources from an application to IBM API Management.
2. When an API is created as a resource and included in a plan, an access point is created on DataPower Gateway as a junction to access the backend API.
3. In addition to the API in this pattern, API authorization credentials, such as OAuth client ID and client secret, are created on Security Access Manager Advanced Access Control for OAuth implementation later in the workflow.
4. A client requests the API through the Security Access Manager reverse proxy junction that is hosted on DataPower Gateway.
5. The authorization request for the API is forwarded to Security Access Manager Advanced Access Control for access with the client ID and client secret.
6. Authorization code for the scope is provided by the Security Access Manager Advanced Access Control.
7. The client application exchanges the authorization code for an access token.
8. The Access Token is sent to the client application.
9. The client sends the access token and the access request to the resource.
10. The token is sent for validation to Security Access Manager Advanced Access Control.

11. After the token is validated, Security Access Manager Advanced Access Control checks the risk-based access assessment for any context-based access policy and decisions.
12. Based on the context-based policy, decisions can be made to allow or deny or to notify and allow the device to continue.
13. The access decision and scope are sent to DataPower Gateway because it is the policy enforcement point.
14. DataPower Gateway enforces access based on the authorization decision and the scope provided.
15. The request is then serviced through IBM API Management and the backend.
16. The response is serviced through reverse proxy to the client.

Key business benefits of integration

This integration offers several benefits:

- Enhances API security controls to consider the user and device (for example, fraud)
- Introduces the ability to guide policy-based decisions, resulting in strong authentication challenges to mobile platforms
- Adds session management capabilities, so a user can log out from hosted services
- Converges the best of API security (for example, schema verification and API entitlements) with preferred access management capabilities in a single appliance

6.5 Summary

In this chapter, we described the patterns that are addressed through the integration of IBM Security Access Manager, IBM DataPower Gateway, and IBM API Management solutions. This integration enables both web and mobile traffic to be hosted through the same point of contact.

This capability is managed by an add-on to the DataPower Gateway called IBM Security Access Manager for DataPower. It is available to existing DataPower customers as a separately licensed capability. In this chapter, we reviewed deployment considerations for this add-on within the context of a use case.

Related publications

The publications listed in this section are particularly suitable for more detailed information about the topics covered in this paper.

Online resources

IBM Security Integration Factory

http://ibm.co/1nM74Jy

IBM Knowledge Center

http://www.ibm.com/support/knowledgecenter/

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

(0.1”spine)
0.1”<->0.169”
53<->89 pages

REDP-5256-00

ISBN 0738454559

Printed in U.S.A.