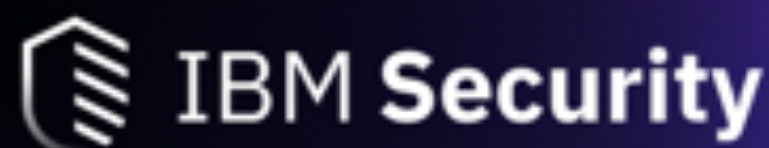


Hardening the IBM® Security Access Manager Appliance

—
IBM® Security Access Manager
31 March 2020



Join IBM VIP Rewards

Engage. Earn points. Get Rewards.



IBM VIP Rewards is a way to engage with and recognize the ways that you, the client, add value to IBM. Complete fun challenges and get rewarded for interacting with IBM, learning new technologies and sharing your knowledge.

Learn more...
ibm.biz/vip-rewards

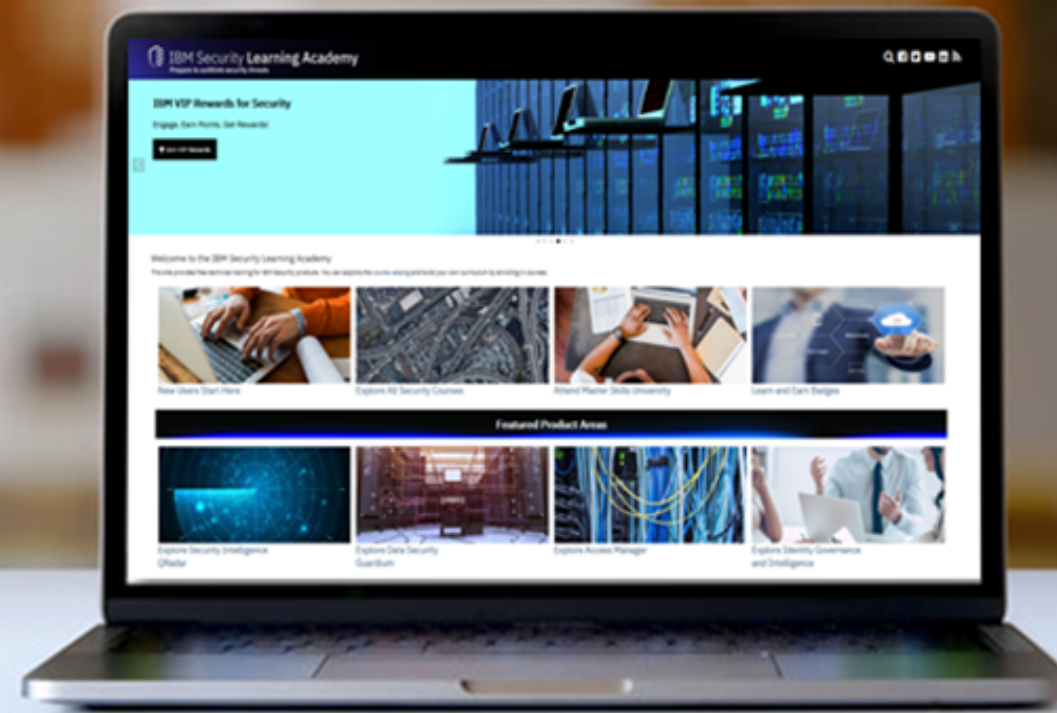
Join IBM VIP Rewards for Security...
ibm.biz/JoinIBMVIPRewards-Security



IBM VIP Rewards for **Security**

IBM Security Learning Academy

SecurityLearningAcademy.com



- Courses
- Videos
- Hands-on Labs
- Live Events
- Badges

Learning at no cost.

New content published daily.

Panel

Moderator

Kathy Hansen

Presenter

Jack Yarborough

Panelists

Annelise Quap

Daniel Comeau

Nicholas Lloyd

Table of Contents

- Objectives
- Agenda
- Hardening Overview
- TLS Channels
- HTTP Channels
- FIPS/NIST considerations
- OWASP Overview
- Github Assets to assist in Hardening
- Appendix A: Detailed Hardening Reference

Objectives

After this presentation an ISAM Administrator will be able to:

- Locate hardening related settings in their appliance components
- Tune TLS channels to add/remove ciphers and protocol versions
- Understand best practices for hardening appliances
- Understand impacts of hardening appliances
- Use command line utilities to systematically update appliances
 - cURL based REST API examples on Support Github

Agenda

Hardening Overview

- Appliance
- ISAM for Web
- ISAM AAC
- ISAM Federation

TLS Channels

HTTP Channels

FIPS/NIST

OWASP Overview

REST API framework

Hardening Overview

What is hardening?

NIST SP 800-123 defines hardening as :

“Configuring a host’s operating system and applications to reduce the host’s security weaknesses.”

What does this mean for the ISAM Appliance?

- Upgrading to the latest firmware and interim fixpack level available (9.0.7.1 IF3 at the time of this publication)
- Managing Configuration to minimize the exposed surfaces in your communication channels
- Adequately sizing and performance tuning your environments
- Reviewing Best Practice documents
 - OWASP Top Ten : <https://owasp.org/www-project-top-ten/>
- Publications that can be used to Harden your systems :
 - NIST SP 800-52 Rev. 2 : <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf>
 - NIST SP 800-123 : <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf>

ISAM Appliance Hardening Overview

Hardening Tactics

- Separate Management traffic and Application traffic using different subnets
- Send logs to remote syslog when possible
- Use TLS communications when utilizing remote syslog
- Use LDAP Management Authentication and Management Authorization Roles
- Require Client Certificate Authentication if possible for LMI authentication
- Change the built-in 'admin' password
- Change the embedded LDAP super admin password
- Define Multiple DNS servers for fault tolerance

ISAM for Web Hardening Overview

Hardening Tactics

- Explicitly disable legacy protocols via the configuration files
- Use TLS for communications where possible (LDAP, RTSS, TFIMSSO, AAC, OCSP)
- Enable certificate validation with OCSP servers
- Use strong cipher suites and order with strongest in preference
- Send Reverse Proxy logs to a Remote Syslog Server
 - Use TLS communications to the Remote Syslog Server
- Enable Mutual TLS authentication where possible

ISAM AAC Hardening Overview

Hardening Tactics

- Use external database for HVDB
 - Use an external database for configuration if possible
 - Use a 'secure' connection (TLS)
- Utilize Remote Syslog Forwarding for 'messages.log'
 - Use TLS communications when utilizing remote syslog
- Use a Client Secret for OAUTH clients
- Use Server Connections instead of hard coding credentials in mapping rules
- Change the 'easuser' password
- Use a certificate for 'easuser' authentication
- Create a new user to use as opposed to 'easuser'
 - Use a strong password
 - Use a certificate for authentication
- Enable CRL checking for partner signature validation and encryption certificates
- Limit Access to attribute collector endpoint

ISAM Federation Hardening Overview

Hardening Tactics

- Use an external database for the High Volume Database
 - Use a Secure connection (TLS)
- Use different certificates for signing and encryption
- Use different certificates for each federation
- Utilize remote syslog forwarder to export messages.log
- Change the 'easuser' password
- Use a certificate for 'easuser' authentication
- Create a new user to use as opposed to 'easuser'
 - Use a strong password
 - Use a certificate for authentication
- Enable CRL checking for partner signing/encryption certificates
- Remove unnecessary attributes from outgoing tokens (SAML Assertions, JWT)

TLS Channels

Hardening Tactics

- Disable outdated protocols
 - SSLv2
 - SSLv3
 - TLS 1.0
 - TLS 1.1
- Disable weak ciphers
 - Utilize Perfect Forward Secrecy
- Use CA Signed certificates
 - Minimum key sizes
 - RSA : 2048
 - ECDSA : 256
 - Minimum secure signature algorithms
 - RSA : SHA256withRSA
 - ECDSA : SHA256withECDSA
- Utilize Mutual TLS Certificate Authentication when possible

Different TLS Channels by Diagram

LDAP TLS connections

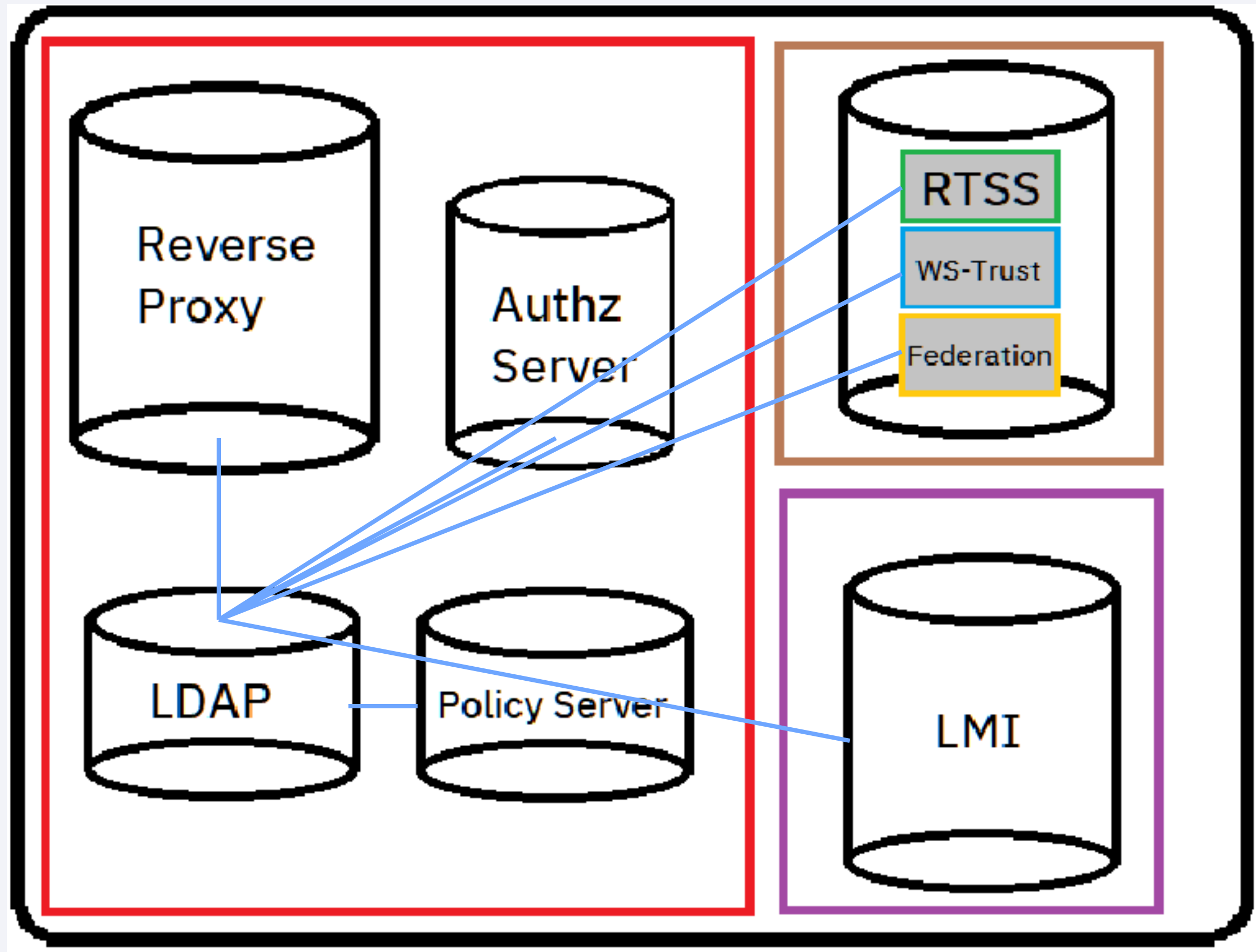
Policy Server :
[ldap] stanza

Authorization Server:
[ldap] stanza

Reverse Proxy :
[ldap] stanza

- AAC/Federation :
- Global Settings -> Server Connections
 - Mapping Rules -> UserLookupHelper
 - Attribute Sources
 - Policy Information Points
 - SCIM

- LMI :
- Remote Management Authentication

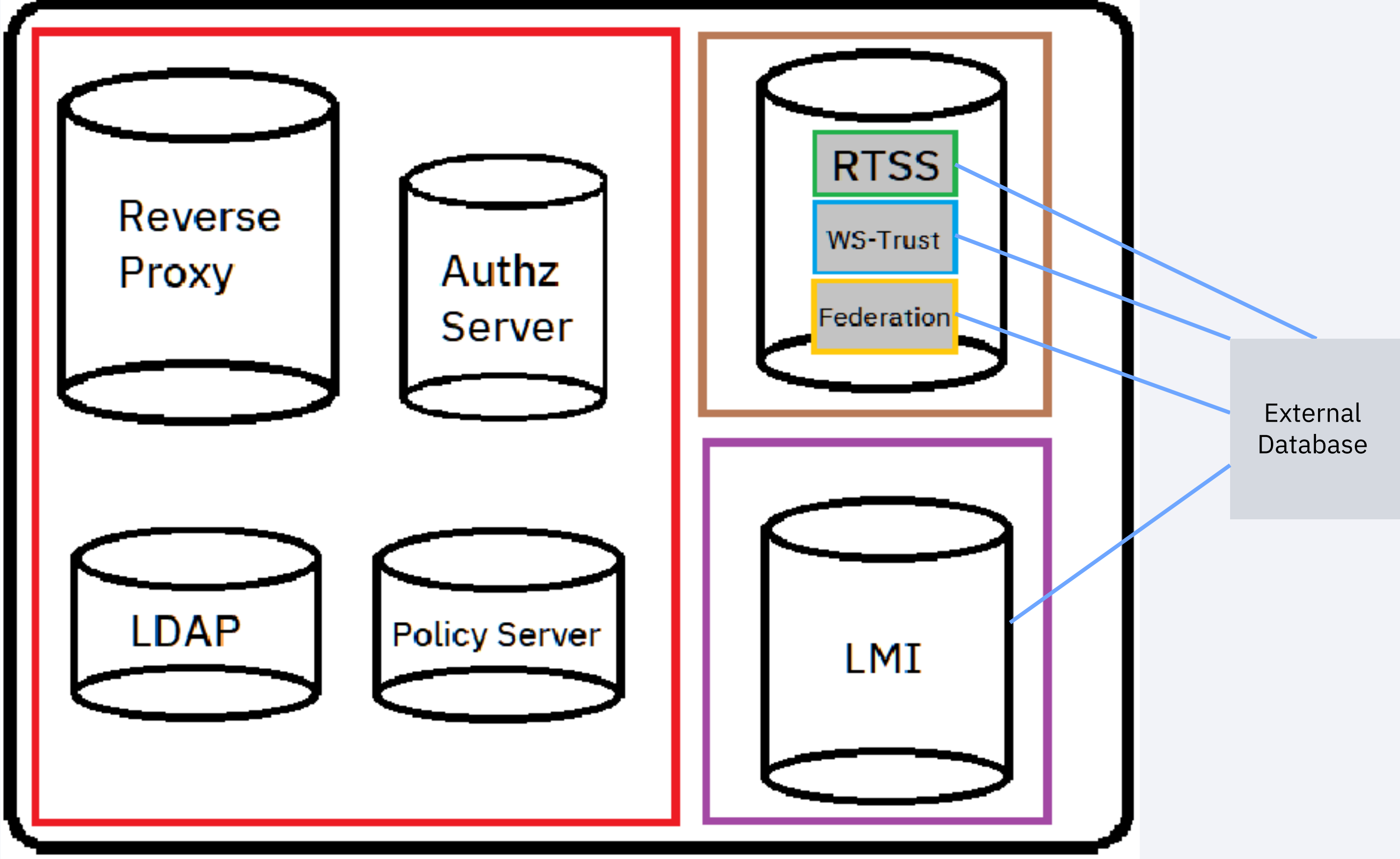


Different TLS Channels by Diagram

Database Connections

- AAC/Federation :
- Global Settings -> Server Connections
 - Policy Information Points

- Clustering :
- External Configuration Database
 - External High Volume Database



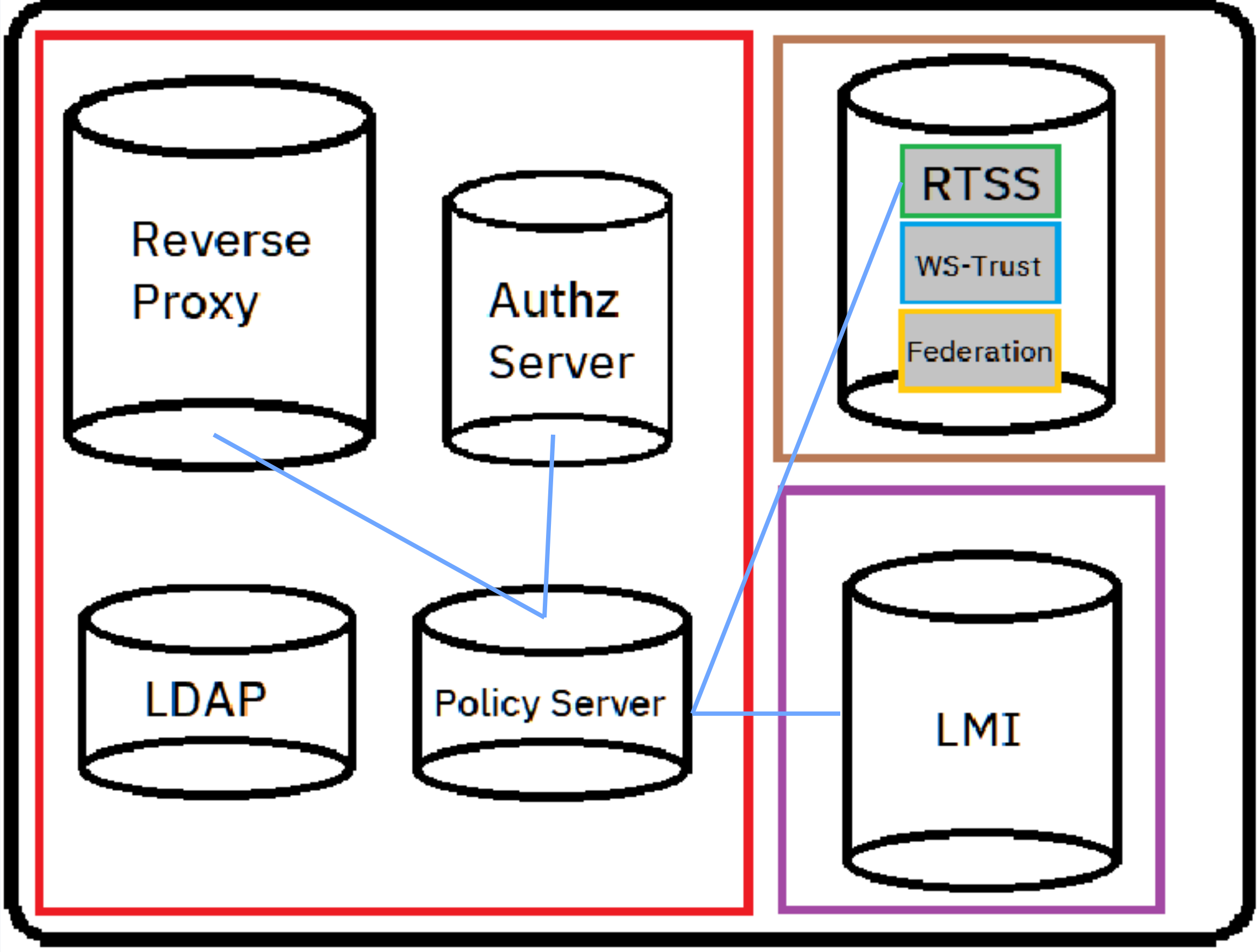
Different TLS Channels by Diagram

ISAM for Web Management

ISAM for Web components:
pd.conf : [ssl] stanza

- LMI:
- Policy Administration
 - Reverse Proxy Tracing
 - AAC Access Control Policy Attachment

- AAC/Federation:
- UserLookupHelper
 - Username Password authentication mechanism

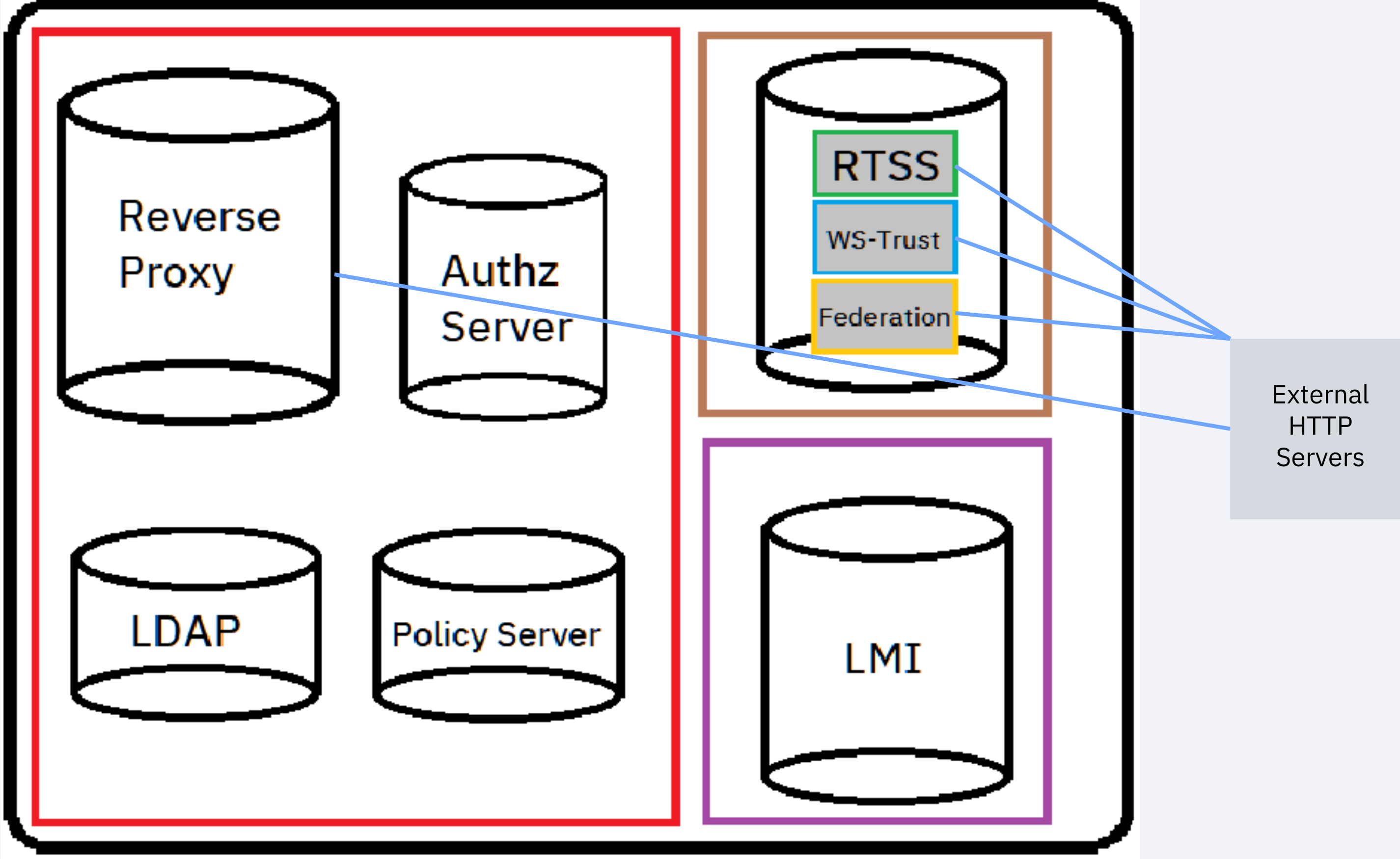


Different TLS Channels by Diagram

External HTTP Servers

- Reverse Proxy:
- [junction] stanza
 - GSO Credential Learning
 - ISIM Reverse Password Sync
 - OCSP

- AAC/Federation:
- Server Connections
 - Policy Information Points
 - External Mapping Callout

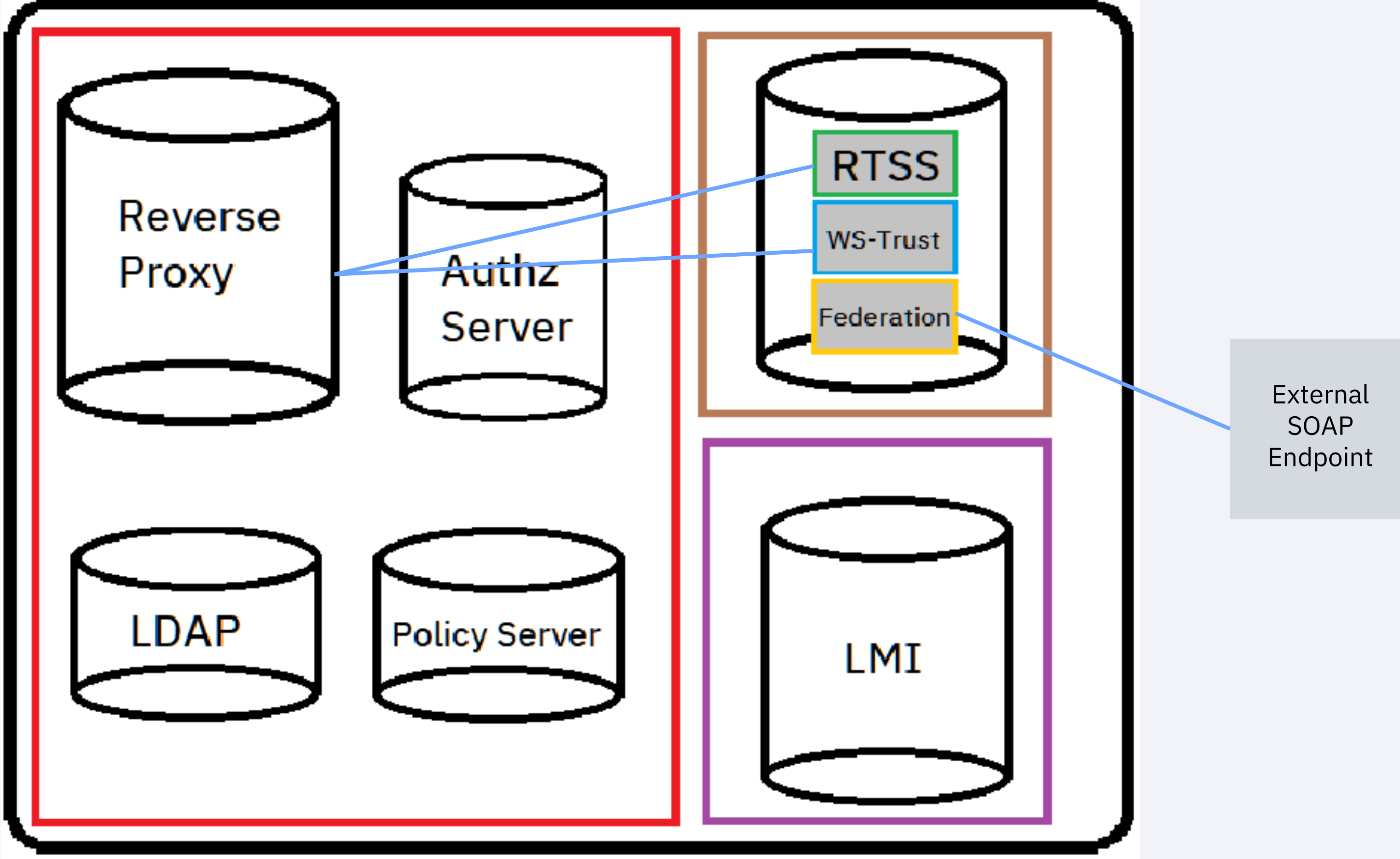


Different TLS Channels by Diagram

SOAP Channels

- Reverse Proxy:
- [rtss-cluster] stanza
 - [tfim-cluster] stanza
 - [dsess-cluster] stanza

- AAC/Federation:
- Trust Server
 - Artifact Resolution Binding



HTTP Channels

Hardening Tactics

- Utilize encryption for HTTP Connections
- Utilize persistent connections for client and server connections
- Set worker thread limits to prevent resource exhaustion
- Cache resources that don't change often
- Utilize the Web Application Firewall
- Utilize the 'LocalSTSCClient' as opposed to the 'HTTPClient' when making Trust Server calls in mapping rules
- Set your timeouts to reasonable values

HTTP Channels by Diagram

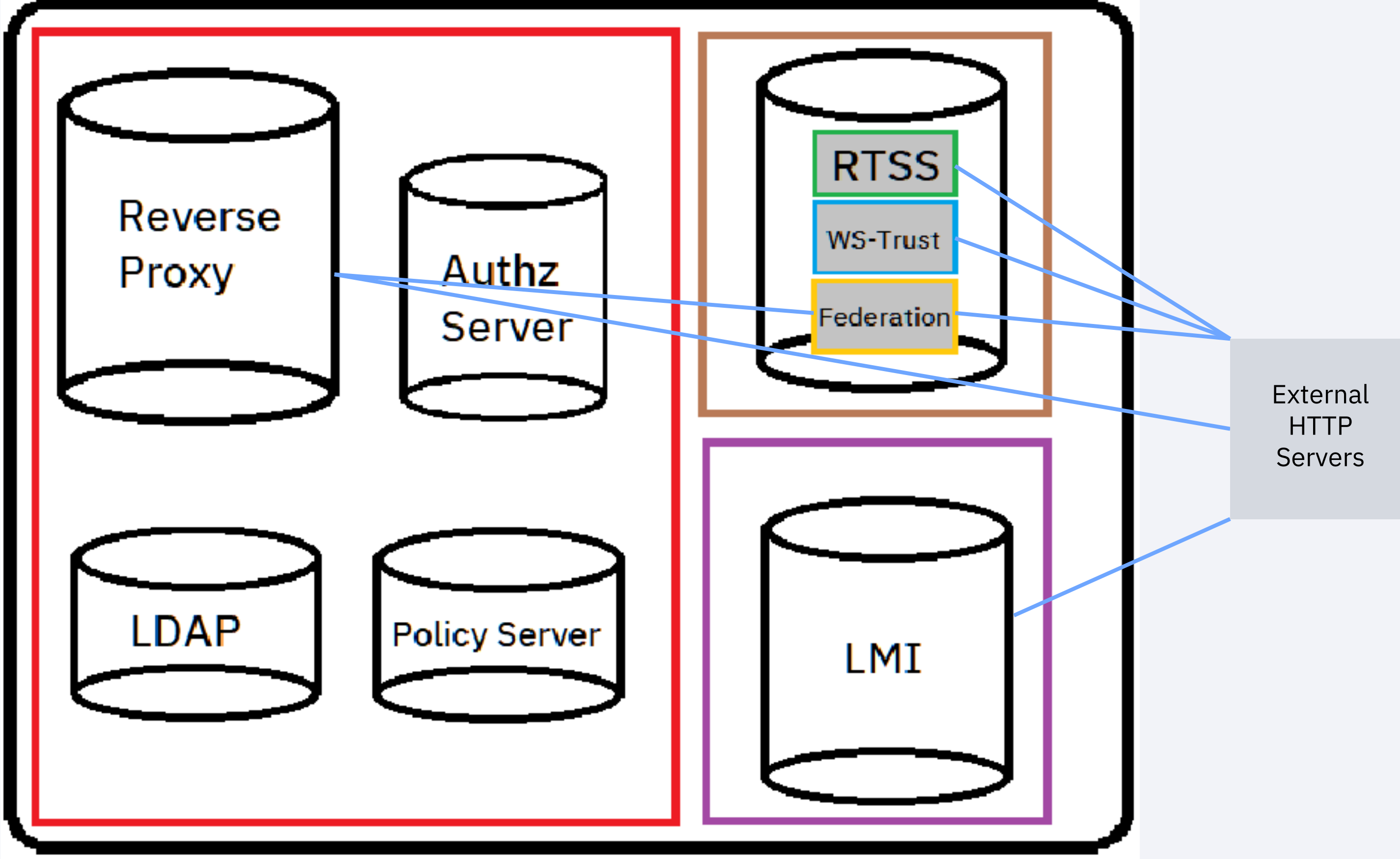
External HTTP Servers

Reverse Proxy:

- [junction] stanza
- GSO Credential Learning
- ISIM Reverse Password Sync
- OCSP

AAC/Federation:

- Server Connections
- Policy Information Points
- External Mapping Callout
- SCIM external schema
- CRL Endpoints



FIPS/NIST Considerations

Hardening Tactics

- Appliance FIPS mode
 - Can only be enabled during initial appliance setup
 - Cannot be disabled
- Utilize FIPS/NIST only when your organization requires
- ISAM for Web offers the following compliance levels
 - ssl-compliance
 - FIPS 140-2
 - NIST SP800-131a Transition
 - NIST SP800-131a Strict
 - NSA Suite B 128 bit
 - NSA Suite B 192 bit
 - Affects the PDCA signature algorithm and ISAM for Web Management Certificates issued to server components
- JVM/Internal component compliance is controlled by the following Advanced Tuning Parameter
 - nist.sp800-131a.strict

OWASP Top 10

Hardening Tactics

- Reference

<https://owasp.org/www-project-top-ten/>

Top Ten

- Injection
 - Upgrade to the latest firmware level and interim fixpack level
 - Validate all incoming and outgoing parameters
 - Utilize Web Application Firewall
 - Perform negative testing on forms and query parameters
- Broken Authentication
 - Do not share passwords
 - Only enable authentication mechanisms being used
 - Validate all authentication credentials
 - Explicitly deny access for super user credentials via Web/EAI/AAC/Federation channels
- Sensitive Data Exposure
 - Use only necessary macros in Reverse Proxy LRR or Management pages
 - Perform negative tests in Federation/AAC modules that take query/form parameters as input
- XML External Entity
 - Upgrade to the latest firmware level and interim fixpack level

OWASP Top 10

Hardening Tactics Continued

- Reference
<https://wasp.org/www-project-top-ten/>
- Broken Access Control
 - Explicitly attach unauthenticated ACLs only to resources that require them
 - Require Authentication by default
 - Use LDAP Groups to perform fine-grained access control for users
- Security Misconfiguration
 - Disable HTTP
 - Disable weak ciphers
 - Disable weak authentication
 - Require authentication for resources unless they explicitly need to be anonymously accessed
 - Require multi-factor authentication for sensitive assets
 - Upgrade to the latest firmware level and interim fixpack level
- Cross Site Scripting (XSS)
 - Utilize CORS
 - Utilize Content-Security-Policy headers
 - Utilize the Web Application Firewall on form validation endpoints

OWASP Top 10

Hardening Tactics Continued

- Reference
<https://owasp.org/www-project-top-ten/>
- Insecure Deserialization
 - Use provided JavaScript/Java classes for mapping rules
 - Upgrade to the latest firmware level and interim fixpack level
- Using Components with Known Vulnerabilities
 - Upgrade to the latest firmware level and interim fixpack level
- Insufficient Logging and Monitoring
 - Enable Auditing for Policy Server
 - Enable Auditing for Reverse Proxy
 - Enable Auditing for AAC/Federation
 - Offload all logging to a Remote Syslog Server via TLS connection
 - Utilize SNMP for system monitoring
 - Utilize AAC/Federation JVM Monitoring
 - <https://www.ibm.com/blogs/security-identity-access/monitoring-federation-advanced-access/>

Appendix A: Detailed Hardening Reference

ISAM for Web – Runtime Component – Policy Server

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Runtime Component ->> Manage -> Configuration Files -> ivmgrd.conf

- Explicitly disable legacy protocols via the configuration file :

```
[ssl]
```

```
...
```

```
ssl-v2-enable = no
```

```
ssl-v3-enable = no
```

```
tls-v10-enable = no
```

```
tls-v11-enable = no
```

```
tls-v12-enable = yes
```

- Explicitly disable weak Encryption Ciphers even for disabled protocols :

```
[ssl]
```

```
...
```

```
ssl-v3-cipher-specs = TLS_RSA_WITH_AES_256_CBC_SHA
```

```
tls-v10-cipher-specs = TLS_RSA_WITH_AES_256_CBC_SHA
```

```
tls-v11-cipher-specs = TLS_RSA_WITH_AES_256_CBC_SHA
```

```
tls-v12-cipher-specs = ...
```

ISAM for Web – Runtime Component – Policy Server

Hardening Tactics Continued

Configuration File location :

Secure Web Settings -> Manage -> Runtime Component ->> Manage -> Configuration Files -> ivmgrd.conf

- Enable TLS connections to your LDAP server

[ldap]

...

ssl-enabled = yes

ssl-keyfile = keyfile.kdb

- Consider Mutual TLS authentication to your LDAP server

[ldap]

...

ssl-keyfile-dn = cn=policyserverldapcert

- Set LDAP related timeouts

[ldap]

...

timeout = 20

authn-timeout = 20

search-timeout = 20

- Tune the TLS session cache size

[ssl]

...

ssl-session-cache-size = 40960

ISAM for Web – Runtime Component – LDAP Communications

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Runtime Component ->> Manage -> Configuration Files -> ldap.conf

- Extend the Password length of Service Accounts
 - Default is 8 characters
 - Industry standard has moved to 15 characters
 - Max length is 20 characters

```
[ldap]
```

```
...
```

```
min-pwd-length-for-serviceid = 15
```

- Specify a TLS keyfile that will house the Public keys for your LDAP server

```
[ldap]
```

```
ssl-keyfile = <keyfile>
```

- Explicitly disable out of date TLS protocols

```
[ldap]
```

```
...
```

```
ssl-v3-enable = no
```

```
tls-v10-enable = no
```

```
tls-v11-enable = no
```

```
tls-v12-enable = yes
```

ISAM for Web – Runtime Component – LDAP Communications

Hardening Tactics Continued

Configuration File location :

Secure Web Settings -> Manage -> Runtime Component ->> Manage -> Configuration Files -> ldap.conf

- Manually Specify and Order ciphers used for TLS communications

[ldap]

...

ssl-tls-cipher-specs = 352F

tls-v12-cipher-specs = <ciphers>

- Tune LDAP connection inactivity timeout

[ldap]

...

connection-inactivity = 30

- Setup Replica servers for your Primary or Federated Directories

[ldap]

...

replica = replica1.ldap.tivoli.com,636,readonly,5

replica = replica2.ldap.tivoli.com,636,readonly,5

[server:federated]

...

replica = fedreplica1.ldap.tivoli.com,636,readonly,5

replica = fedreplica2.ldap.tivoli.com,636,readonly,5

ISAM for Web – Runtime Component – LDAP Communications

Hardening Tactics Continued

Configuration File location :

Secure Web Settings -> Manage -> Runtime Component ->> Manage -> Configuration Files -> ldap.conf

- Enable TLS to your Federated Directories

```
[server:federated]
```

```
...
```

```
ssl-enabled = yes
```

ISAM for Web – Runtime Component – Management Communications

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Runtime Component ->> Manage -> Configuration Files -> pd.conf

- Explicitly disable out of date TLS protocols for Management Clients

[ssl]

...

ssl-v2-enable = no

ssl-v3-enable = no

tls-v10-enable = no

tls-v11-enable = no

tls-v12-enable = yes

- Explicitly configure Cipher sets favoring Strong ciphers

[ssl]

...

ssl-v3-cipher-specs = TLS_RSA_WITH_AES_256_CBC_SHA

tls-v10-cipher-specs = TLS_RSA_WITH_AES_256_CBC_SHA

tls-v11-cipher-specs = TLS_RSA_WITH_AES_256_CBC_SHA

tls-v12-cipher-specs = <ciphers>

ISAM for Web – Authorization Server

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Authorization Server ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Disable Remote access to Policy Database (disabled by default)

[ivaclld]

...

permit-unauth-remote-caller = FALSE

- Enable TLS connections to your LDAP Server

[ldap]

...

ssl-enabled = yes

- Set timeouts for LDAP operations

[ldap]

...

timeout = 30

authn-timeout = 30

search-timeout = 30

ISAM for Web – Authorization Server

Hardening Tactics Continued

Configuration File location :

Secure Web Settings -> Manage -> Authorization Server ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Configure LDAP replicas for robustness

[ldap]

...

replica = freddy,636,readonly,1

replica = barney,636,readwrite,2

replica = benny,636,readwrite,3

- Increase TLS session cache size

[ssl]

...

ssl-session-cache-size = 40960

- Explicitly disable out of date TLS protocols for Authorization server listening address

[ssl]

...

ssl-v2-enable = no

ssl-v3-enable = no

tls-v10-enable = no

tls-v11-enable = no

tls-v12-enable = yes

ISAM for Web – Authorization Server

Hardening Tactics Continued

Configuration File location :

Secure Web Settings -> Manage -> Authorization Server ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Explicitly configure cipher sets to use Strong ciphers

[ssl]

...

ssl-v3-cipher-specs = TLS_RSA_WITH_AES_256_CBC_SHA

tls-v10-cipher-specs = TLS_RSA_WITH_AES_256_CBC_SHA

tls-v11-cipher-specs = TLS_RSA_WITH_AES_256_CBC_SHA

tls-v12-cipher-specs = <ciphers>

ISAM for Web – Reverse Proxy – Server Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Disable HTTP

[server]

...

http = no

- Tune worker threads

[server]

...

worker-threads = <value>

- Suppress ISAM and Backend Server identities

[server]

...

suppress-server-identity = yes

suppress-backend-server-identity = yes

- Use strong encryption for Failover/ECSSO/CDSSO tokens:

[server]

...

pre-800-compatible-tokens = no

ISAM for Web – Reverse Proxy – Server Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Reject invalid host headers

```
[server]
```

```
...
```

```
reject-invalid-host-header = yes
```

- Use 'HTTP Only' flag for ISAM generated cookies (Session/Failover)

```
[server]
```

```
...
```

```
use-http-only-cookies = yes
```

- Consider adding per-user limits on worker threads

```
[server]
```

```
...
```

```
concurrent-session-threads-soft-limit = (integer number of threads per user)
```

```
concurrent-session-threads-hard-limit = (integer number of threads per user)
```

ISAM for Web – Reverse Proxy – Server Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Disable unsolicited logins
[server]

...

allow-unsolicited-logins = no

- Explicitly define what values are allowed in a request
 - All values that should be expected must be explicitly defined

[validate-headers]

...

host = www.ibm.com

host = vhj.ibm.com

host = identity.hyperv.lab

- Confirm the following headers are added to every request:
 - Syntax : <header> = <header value>

[rsp-header-names]

...

strict-transport-security = max-age=31536000; includeSubDomains

Content-Security-Policy = default-src 'self'; img-src 'self'; media-src 'self'; script-src 'self'

ISAM for Web – Reverse Proxy – Junction Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Set junction worker thread limits
[junction]

...

worker-thread-hard-limit = (integer % of total worker threads)

worker-thread-soft-limit = (integer % of total worker threads)

The worker thread hard limit is the percentage of total worker threads each junction can use across all servers

The worker thread soft limit is the percentage of total worker threads used that will generate a warning in the Reverse Proxy message log

This can also be set on a per-junction level if some junctions require higher/lower thread usage parameters:

- Prevent backend servers from setting domain cookies
 - Could lead to infrastructure exposure
 - May prevent the cookie from appearing in future requests

[junction]

...

allow-backend-domain-cookies = no

ISAM for Web – Reverse Proxy – Junction Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Validate domain cookies from backend servers if they are necessary
[junction]

...

validate-backend-domain-cookies = yes

- Validate that the domain in backend domain cookies only matches hosts we are configured to listen for
[junction]

...

support-virtual-host-domain-cookies = yes

- Allow junctions to set the 'HTTP Only' attribute on cookies
[junction]

...

pass-http-only-cookie-attr = yes

- Enable HTTP Persistent Connections for your junction servers
[junction]

...

max-cached-persistent-connections = (integer, number of connections per junction server)

persistent-con-timeout = (integer, seconds)

ISAM for Web – Reverse Proxy – LDAP Channel

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Connect using TLS

[ldap]

...

ssl-enabled = yes

ssl-keyfile = <keyfile>

- Enable LDAP operation timeouts

[ldap]

...

timeout = 20

authn-timeout = 20

search-timeout = 20

ISAM for Web – Reverse Proxy – Authentication Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Disable Basic Authentication

[ba]

ba-auth = none

- Prevent empty form fields in the ISAM login form

[forms]

...

allow-empty-form-fields = false

- Consider shutting down the socket if an invalid or no certificate is presented for Client Certificate Authentication

[certificate]

...

accept-client-certs = critical #Always request a client certificate. If a valid certificate is not presented the SSL handshake will fail.

- Map all your authentication mechanisms to an authentication level

[authentication-levels]

level = unauthenticated

level = password

level = ext-auth-interface

...

ISAM for Web – Reverse Proxy – Authentication Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Verify that the user id did not change during step-up
[step-up]

...

verify-step-up-user = yes

ISAM for Web – Reverse Proxy – Single Sign-On Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Disable failover cookie when possible
[failover]

...

failover-auth = none

- Use different keys for each CDSSO domain
[cdsso-peers]
websealB.domainB.com = A-B.key
websealC.domainC.com = A-C.key

ISAM for Web – Reverse Proxy – Cipher Configuration

Hardening Tactics 9.0.4.0+

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Enable SSL Quality of Protection Management

[ssl-qop]

ssl-qop-mgmt = yes

- Explicitly enable strong ciphers and order their preference

[ssl-qop-mgmt-default]

default = TLS_CHACHA20_POLY1305_SHA256

default = TLS_AES_128_CCM_8_SHA256

default = TLS_AES_256_GCM_SHA384

default = TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

default = TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

...

ISAM for Web – Reverse Proxy – Cipher Configuration

Hardening Tactics 9.0.3.1-

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Disable SSL QOP Management

```
[ssl-qop]
```

```
ssl-qop-mgmt = no
```

- Explicitly specify strong ciphers and order them by strength

```
[ssl]
```

```
#client channel
```

```
gsk-attr-name = string:240:{comma-separated cipher list on one line, in preferred order} # SSLv3 from client
```

```
gsk-attr-name = string:241:{comma-separated cipher list on one line, in preferred order} # TLSv1.0 from client
```

```
gsk-attr-name = string:242:{comma-separated cipher list on one line, in preferred order} # TLSv1.1 from client
```

```
gsk-attr-name = string:243:{comma-separated cipher list on one line, in preferred order} # TLSv1.2 from client
```

```
# junction channel
```

```
jct-gsk-attr-name = string:240:{comma-separated cipher list on one line, in preferred order} # SSLv3 to junctioned servers
```

```
jct-gsk-attr-name = string:241:{comma-separated cipher list on one line, in preferred order} # TLSv1.0 to junctioned servers
```

```
jct-gsk-attr-name = string:242:{comma-separated cipher list on one line, in preferred order} # TLSv1.1 to junctioned servers
```

```
jct-gsk-attr-name = string:243:{comma-separated cipher list on one line, in preferred order} # TLSv1.2 to junctioned servers
```

Reference Document:

<https://www.ibm.com/support/pages/how-may-specific-tls-ciphers-be-selected-and-ordered-https-communications-reverse-proxy-webseal>

ISAM for Web – Reverse Proxy – Cipher Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Reference list of TLSv1.2 Ciphers : RSA Perfect Forward Secrecy Prioritized

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_128_CBC_SHA

ISAM for Web – Reverse Proxy – Cipher Configuration

Hardening Tactics 9.0.3.1-

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Reference list of TLSv1.2 Ciphers : ECDSA Perfect Forward Secrecy Prioritized

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA

ISAM for Web – Reverse Proxy – Cipher Configuration

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Reference list of TLSv1.2 Ciphers : RSA Performance Prioritized

TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

ISAM for Web – Reverse Proxy – Client TLS Channel

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Use a CA Signed Certificate for the Reverse Proxy server certificate
 - The following value should not say 'WebSEAL-Test-Only' for production environments

[ssl]

...

webseal-cert-keyfile-label = hypervlabs

- Explicitly disable outdated versions of TLS

[ssl]

...

disable-ssl-v2 = yes

disable-ssl-v3 = yes

disable-tls-v1 = yes

disable-tls-v11 = yes

disable-tls-v12 = no

disable-tls-v13 = yes # default

- Increase the TLS Session cache size

[ssl]

...

ssl-max-entries = 40960

ISAM for Web – Reverse Proxy – Client TLS Channel

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Enable Online Certificate Status Protocol (OCSP) to validate client certificates [ssl]

...

The follow two options are used enable OCSP. Either or both can be used.

ocsp-enable = yes

#ocsp-url = <Absolute URL for OCSP responder>

The following are OCSP options for interacting with the OCSP Responder.

#ocsp-nonce-generation-enable = no

#ocsp-nonce-check-enable = no

#ocsp-retrieve-via-get = no

#ocsp-max-response-size = 20480

#ocsp-proxy-server-name = <proxy host name>

#ocsp-proxy-server-port = <proxy port number>

Refer to documentation for further configuration details

ISAM for Web – Reverse Proxy – Junction TLS Channel

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

- Enable OCSP for junction certificates
[junction]

...

jct-ocsp-enable = yes

- Explicitly disable older protocols for Junction Connections
[junction]

...

disable-ssl-v2 = yes

disable-ssl-v3 = yes

disable-tls-v1 = yes

disable-tls-v11 = yes

disable-tls-v12 = no

disable-tls-v13 = yes

ISAM for Web – Reverse Proxy – SOAP TLS Channel

Hardening Tactics

Configuration File location :

Secure Web Settings -> Manage -> Reverse Proxy ->> _select-instance_ -> Manage -> Configuration -> Edit Configuration File

Stanzas:

[tfim-cluster]

[oauth-cluster]

[dsess-cluster]

[rtss-cluster]

- Explicitly disable out of date TLS protocols

...

gsk-attr-name = enum:403:0

gsk-attr-name = enum:404:0

gsk-attr-name = enum:436:0

gsk-attr-name = enum:437:0

gsk-attr-name = enum:438:1

ISAM Appliance - LMI

Hardening Tactics

Configuration File location :

Manage System Settings -> System Settings -> Administrator Settings

- Explicitly disable outdated TLS protocols
key: Enabled Server Secure Protocols
value: TLSv1.2
- Explicitly disable outdated TLS protocols for outbound (client) connections
key: Enable TLS Protocols
value: TLSv1.2
- Explicitly disable SSLv3
key: Enable SSLv3
value: false

ISAM for AAC/Federation – Server TLS Channel

Hardening Tactics

Configuration location :

Secure Access Control -> Global Settings -> Runtime Parameters

Secure Federation -> Global Settings -> Runtime Parameters

- Tune JVM Heap sizes

key: Max Heap Size

value: (integer)

key: Min Heap Size

value: (integer)

- Enable CRL Distribution Point validation

key: Enable CRL DP Checking

value: true

- Allow Client Certificate Authentication (required for Mutual TLS authentication)

key: Accept Client Certificates

value: true

- Disable SSLv3

key: Enable SSLv3

value: false

- Explicitly Disable out of date TLS protocols

key: Enabled Server Secure Protocols

value: TLSv1.2 (dropdown)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics - Distributed Map

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Tune the Distributed Map cleanup interval
key: distributedMap.cleanupWait
value: (integer seconds)
- Tune the Distributed Map Entry lifetime (TTL)
key: distributedMap.defaultTTL
value: (integer seconds)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics - Attribute Collector

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Hash sensitive attributes stored in the Attribute Collector
key: attributeCollection.attributesHashEnabled
value: urn:ibm:security:sensitive:attributeA,urn:ibm:security:sensitive:attribute
- Use a SHA256 or higher algorithm for the attribute hash
key: attributeCollection.hashAlgorithm
value: (dropdown)
- Disable GET requests to the '/mga/sps/ac' endpoint
key: attributeCollection.enableGetAttributes
value: false
- If you must enable GET requests to the '/mga/sps/ac' endpoint, use a client whitelist
key: attributeCollection.getAttributesAllowedClients
value: hostname1,hostname2
- Tune the Attribute Collector timeout
key: attributeCollection.sessionTimeout
value: (integer seconds)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – Device Registration

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Require complete fingerprint for device registration
key: deviceRegistration.allowIncompleteFingerprints
value: false
- Cleanup Expired devices
key: deviceRegistration.checkForExpiredDevices
value: true
- Use batching to clean expired devices
key: deviceRegistration.cleanupThread.batchSize
value: (integer) – number of entries
- Review the Device Inactivity timeout
key: deviceRegistration.inactiveExpirationTime
value: (days)
- Review the allowed number of registered devices per user
key: deviceRegistration.maxRegisteredDevices
value: (integer) – number of devices
- Require successful device registration to proceed
key: deviceRegistration.permitOnIncompleteFingerprint
value: false

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – Runtime Properties

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Use a SHA-256 or stronger hash algorithm for generic runtime server activities

key: runtime.hashAlgorithm

value: SHA-256

- Define the hash algorithms to use for verification of hashed values

key: runtime.verificationHashAlgorithms

value: (comma separated list of algorithms)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – Single sign-on protocol service

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Use 'Secure' cookies
key: sps.setCookiesAsSecure
value: true
- Enable the 'x-frame-options' header with 'SAMEORIGIN' value
key: sps.doNotSendXFrameOptionsHeader
value: false
- Specify strings that stop processing when encountered as a query parameter
key: sps.illegalUrlSubstrings
value: "<script" - This is the documented example value
- Set a 'whitelist' for the 'Target' Query Parameter
key: sps.targetURLWhitelist
value: .*

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – Risk Engine

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Enable Risk Reports

key: riskEngine.reportsEnabled

value: true

- Tune the number of total reports to store

key: riskEngine.reportsMaxStored

value: (integer)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – Single sign-on protocol service

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Use 'Secure' cookies
key: sps.setCookiesAsSecure
value: true
- Enable the 'x-frame-options' header with 'SAMEORIGIN' value
key: sps.doNotSendXFrameOptionsHeader
value: false
- Specify strings that stop processing when encountered as a query parameter
key: sps.illegalUrlSubstrings
value: "<script" - This is the documented example value
- Set a 'whitelist' for the 'Target' Query Parameter
key: sps.targetURLWhitelist
value: .*

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – Session

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Tune or disable the HVDB session information cleanup interval

key: session.dbCleanupInterval

value: (integer seconds or 0 to disable)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – OAUTH 2.0

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Enable the 'x-frame-options' header with 'SAMEORIGIN' value
key: oauth20.doNotSendXFrameOptionsHeader
value: false
- Limit token cleanup to cluster primary master
key: oauth20.tokenCache.cleanupOnlyOnPrimaryMaster
value: true
- Tune the OAUTH 2.0 token cleanup interval
key: oauth20.tokenCache.cleanupWait
value: (integer seconds)
- Tune the cleanup thread batch size
key: oauth20.cleanupThread.batchSize
value: (integer)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – HTTPClient

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Use strong TLS protocols
key: util.httpClient.defaultSSLProtocol
value: TLSv1.2 (dropdown)
- Tune max number of Active Connections per remote host
key: util.httpClient.maxActiveConnections
value: hostname=(integer)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – One Time Password

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Review whether users should be able to retry submitting an OTP

key: otp.retry.enabled

value: (Boolean)

- Tune the number of retries

key: otp.retry.maxNumberOfAttempts

value: (integer)

- Tune the retry interval timeout

key: otp.retry.otpRetryTimeout

value: (integer seconds)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – Key Encryption and Signature Service

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Enable Certificate Revocation Validation

key: kess.crlEnabled

value: true

- Tune the interval between CRL checks

key: kess.crlInterval

value: (integer)

- Consider validating the remote hostname against the Certificate Common Name

key: kess.hostnameValidationDisabled

value: (Boolean)

ISAM for AAC/Federation – Advanced Configuration

Hardening Tactics – Mobile Multifactor Authenticators

Configuration location : Secure Access Control -> Global Settings -> Advanced Configuration

- Tune expired authenticator cleanup interval
key: mmfa.authenticator.cleanupWait
value: (integer)
- Consider cleaning up expired MMFA transactions only on the cluster Primary Master
key: mmfa.transaction.cleanupOnlyOnPrimaryMaster
value: (boolean)
- Tune the expired transaction cleanup interval
key: mmfa.transactionPending.cleanupInterval
value: (integer seconds)
- Tune the max number of archived transactions per user
key: mmfa.transactionArchival.maxCompletedPerUser
value: (integer)
- Tune the max number of pending transactions per user
key: mmfa.transactionArchival.maxPendingPerUser
value: (integer)
- Determine the amount of time before a pending transaction is considered expired
key: mmfa.transactionPending.minAgeBeforeAbort
value: (integer seconds)

ISAM Appliance – Embedded LDAP

Hardening Tactics

Configuration location : Manage System Settings -> System Settings -> Advanced Tuning Parameters

- Disable SSLv3 for the embedded ldap
key: wga_rte.embedded.ldap.enable.sslv3
value: false
- Disable TLS 1.0 and TLS 1.1, enable TLS 1.2 and set ciphers
key: wga_rte.embedded.ldap.ciphersuite
value: ECDHE-RSA-AES256-GCM-SHA384

Questions for the panel

Ask the panelists a question now

Enter your question in the Q&A area

Ask a question after this presentation

You are encouraged to ask follow-up questions in the Support forums:

<https://www.ibm.com/mysupport/s/forumshome>

IBM Security Verify Access Support forum:

<http://ibm.biz/VerifyAccessSupportForum>

For more information

Security Learning Academy: <https://www.securitylearningacademy.com/local/navigator/index.php?level=amg001>

IBM Knowledge Center for Security Verify Access: <https://www.ibm.com/support/knowledgecenter/en/SSPREK/welcome.html>

IBM Security Verify Access Support: <http://ibm.biz/supportSecVerifyAccess>

Useful links:

[Get started with IBM Security Support](#) [IBM Support](#)
[Sign up for My Notifications](#) [IBM Security Community](#)

Follow us:



www.youtube.com/user/IBMSecuritySupport



twitter.com/askibmsecurity



<http://ibm.biz/ISCS-LinkedIn>

Thank you

Follow us:

securitylearningacademy.com

ibm.biz/JoinIBMVIPRewards-Security

youtube/user/IBMSecuritySupport

[@AskIBMSecurity](https://twitter.com/AskIBMSecurity)

ibm.biz/IBMSecurityClientSuccess-LinkedIn

securityintelligence.com

xforce.ibmcloud.com

ibm.com/security/community

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

All names and references for organizations and other business institutions used in this deliverable's scenarios are fictional. Any match with real organizations or institutions is coincidental.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.