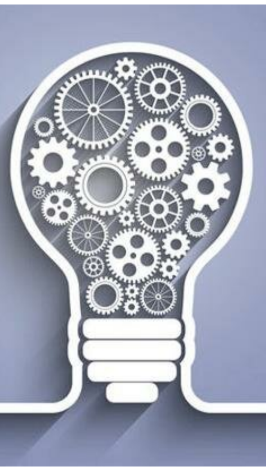
B2B Solutions
Let's build IT together



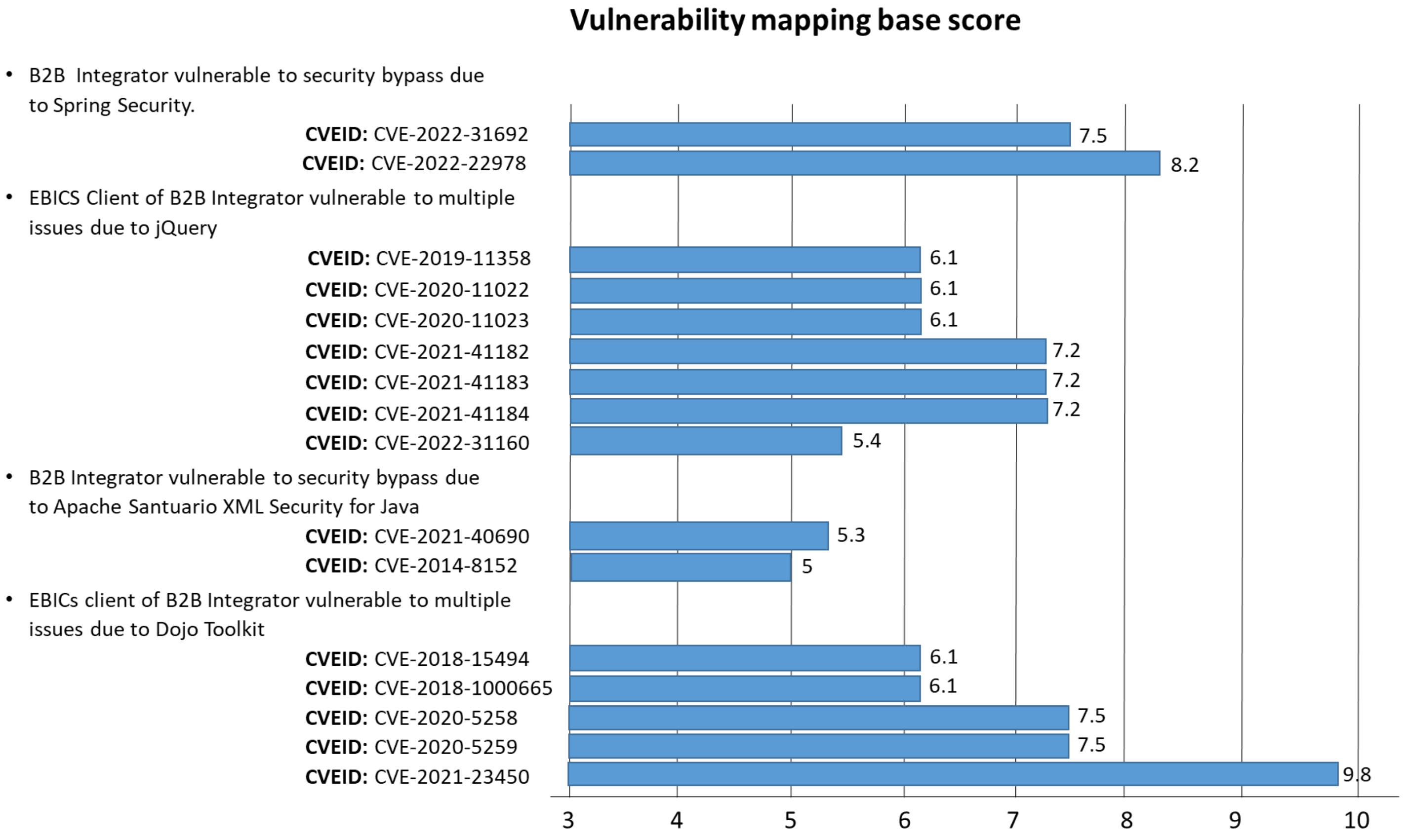
Integration News

T1 2023

IBM Sterling B2B Integrator: SECURITY NEWS.

In this issue:

- B2B Integrator vulnerable to security bypass due to Spring Security
- EBICS Client of B2B Integrator vulnerable to multiple issues due to jQuery
- B2B Integrator vulnerable to security bypass due to Apache Santuario XML Security for Java
- EBICs client of B2B Integrator vulnerable to multiple issues due to Dojo Toolkit



IBM Sterling B2B Integrator vulnerable to security bypass due to Spring Security

Vulnerability Details

CVEID: CVE-2022-31692
Description: VMware Tanzu Spring Security could allow a remote attacker to bypass security restrictions, caused by a flaw when using forward or include dispatcher types. By sending a specially-crafted request, an attacker could exploit this vulnerability to bypass authorization rules.
CVSS Base score: 7.5
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2022-22978
Description: Spring Security could allow a remote attacker to bypass security restrictions, caused by a flaw in the RegexRequestMatcher component. By misconfiguring RegexRequestMatcher with `.` in the regular expression, an attacker could exploit this vulnerability to bypass authorization and obtain access.
CVSS Base score: 8.2
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.0.3.7
	6.1.0.0 - 6.1.2.1

Remediation/Fixes

Product	IBM Sterling B2B Integrator	
Version	6.0.0.0 - 6.0.3.7	6.1.0.0 - 6.1.2.1
APAR	IT42896	IT42896
Remediation & Fix	Apply 6.0.3.8	Apply 6.1.2.2

Workarounds and Mitigations

None.

EBICS Client of IBM Sterling B2B Integrator vulnerable to multiple issues due to jQuery

IBM Sterling B2B Integrator has addressed the security vulnerabilities in jQuery.

CVEID: CVE-2019-11358
Description: jQuery, as used in Drupal core, is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote authenticated attacker could exploit this vulnerability to execute script in a victim's Web browser within the security context of the hosting Web site. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.
CVSS Base score: 6.1
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2020-11022
Description: jQuery is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the jQuery.htmlPrefilter method. A remote attacker could exploit this vulnerability to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.
CVSS Base score: 6.1
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2020-11023
Description: jQuery is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the option elements. A remote attacker could exploit this vulnerability to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.
CVSS Base score: 6.1
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2021-41182
Description: jQuery jQuery-UI is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the Datepicker widget. A remote attacker could exploit this vulnerability using the altField parameter to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.
CVSS Base score: 7.2
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2021-41183
Description: jQuery jQuery-UI is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the Datepicker widget. A remote attacker could exploit this vulnerability using the Text parameter to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.
CVSS Base score: 7.2
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2021-41184
Description: jQuery jQuery-UI is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the .position() function. A remote attacker could exploit this vulnerability using the of parameter to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.
CVSS Base score: 7.2
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2022-31160
Description: jQuery UI is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the check-box-radio widget. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's

Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.
CVSS Base score: 5.4
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.0.3.7
	6.1.0.0 - 6.1.2.1

Remediation/Fixes

Product	IBM Sterling B2B Integrator	
Version	6.0.0.0 - 6.0.3.7	6.1.0.0 - 6.1.2.1
APAR	IT42890	
Remediation & Fix	Apply 6.0.3.8	Apply 6.1.2.2

Workarounds and Mitigations

None.

IBM Sterling B2B Integrator vulnerable to security bypass due to Apache Santuario XML Security for Java

IBM Sterling B2B Integrator has addressed the secuirty vulnerabilities in Apache Santurio XML Security.

Vulnerability Details

CVEID: CVE-2021-40690
Description: Apache Santuario XML Security for Java could allow a remote attacker to bypass security restrictions, caused by the improper passing of the "secureValidation" property when creating a KeyInfo from a KeyInfoReference element. An attacker could exploit this vulnerability to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.
CVSS Base score: 5.3
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2014-8152
Description: Apache Santuario XML Security for Java could allow a remote attacker to bypass security restrictions, caused by the failure to report an error when trying to validate the signature by the streaming XML Signature verification code. An attacker could exploit this vulnerability to modify a specific XML document.
CVSS Base score: 5
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.0.3.7
	6.1.0.0 - 6.1.2.1

Remediation/Fixes

Product	IBM Sterling B2B Integrator	
Version	6.0.0.0 - 6.0.3.7	6.1.0.0 - 6.1.2.1
APAR	IT41105 IT41109 IT39312	IT41105 IT41109 IT39312
Remediation & Fix	Apply 6.0.3.8	Apply 6.1.2.2

Workarounds and Mitigations

None.

EBICs client of IBM Sterling B2B Integrator vulnerable to multiple issues due to Dojo Toolkit

IBM Sterling B2B Integrator has addressed the security vulnerabilities in Dojo Toolkit.

Vulnerability Details

CVEID: CVE-2018-15494
Description: Dojo Toolkit is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the DataGrid component. A remote attacker could exploit this vulnerability to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.
CVSS Base score: 6.1
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2018-1000665
Description: Dojo Objective Harness (DOH) is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by unit.html, testsDOH/_base/loader/i18n-exhaustive/i18n-test/unit.html and testsDOH/_base/i18nExhaustive.js. A remote attacker could exploit this vulnerability to execute script in a victim's Web browser within the security context of the hosting Web site. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.
CVSS Base score: 6.1
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2020-5258
Description: Dojo dojo could allow a remote attacker to inject arbitrary code on the system, caused by a prototype pollution flaw. By injecting other values, an attacker could exploit this vulnerability to overwrite, or pollute, a JavaScript application object prototype of the base object.
CVSS Base score: 7.5

CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2020-5259
Description: Dojo dojox could allow a remote attacker to inject arbitrary code on the system, caused by a prototype pollution flaw. By injecting other values, an attacker could exploit this vulnerability to overwrite, or pollute, a JavaScript application object prototype of the base object.
CVSS Base score: 7.5
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2021-23450
Description: Dojo dojox could allow a remote attacker to inject arbitrary code on the system, caused by a prototype pollution flaw. By injecting other values, an attacker could exploit this vulnerability to overwrite, or pollute, a JavaScript application object prototype of the base object.
CVSS Base score: 9.8
CVSS Temporal Score: Click here.
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.1.2.1

Remediation/Fixes

Product	IBM Sterling B2B Integrator
Version	6.0.0.0 - 6.1.2.1
APAR	IT43099
Remediation & Fix	Apply 6.1.2.2

Workarounds and Mitigations
None.

Note for all entries
SECURITY

The IIM versions of 6.0.3.8 and 6.1.2.2 are available on: Fix Central.

The container version of 6.1.2.2 is available in IBM Entitled Registry with following tags:

- cp.icr.io/cp/ibm-b2bi/b2bi:6.1.2.2 for IBM Sterling B2B Integrator
- cp.icr.io/cp/ibm-sfg/sfg:6.1.2.2 for IBM Sterling File Gateway

NEW

IBM Sterling B2B Integrator
What's new in 6.1.2.0

New features
Following new features are specific to IIM release:

- Apache log4j 1.x is removed and now we are using Apache log4j 2.17.2. However, you may still find Apache log4j 1.x references in various places which should be ignored. For details, refer to Known Issues.
- OOB admin users will be prompted to change their password with new install.

i **Note:** It is not applicable for upgraded setup.

- B2B Mail Client Adapter is now enhanced to access Microsoft Exchange Online with OAuth 2.0.

Following new features are specific to Certified Container release:

- Support for Linux® on PowerLE (ppc64le) architecture.
- Separate container image for the database setup job.
- Support for configuring init container for external resources such as db driver jar, jce policy, standards jar, SEAS integration jars and so on.
- Support for Performance Tuning Wizard updates by using the tuning jar utility.
- API auto scaling enhancements and performance improvements.
- Support for restricted security context in Red Hat OpenShift.
- Support for form view deployment with explicit license acceptance from the Red Hat OpenShift Developer Catalog.
- Certified Container support for Oracle CDB.
- Auto-configuration of GC Policy.
- Certified container support for integrations with MQ Operators and CD certified container.
- Support for overriding Liberty server.xml and jvm options parameters.
- Support for pre-defined Persistent Volume Claim (PVC) for resources, logs, and documents.
- Support for restart cluster via configuration.
- Enhanced security with out of the box deny all external ingress and egress network policies with option to define additional custom policies.
- Support for Integrating with EFK Logging Stack on OpenShift.

Stack updates
New security fixes and following stack upgrades are introduced in this release:

- Support for WebSphereMQ v9.2.0.5 is introduced in this release.
- log4j - 2.17.2
- Red Hat OpenShift Container Platform:
  - Version 4.8.0 or later fixes
  - Version 4.10.0 or later fixes
- Kubernates >= 1.22 and <= 1.25
- Helm >= 3.9

B2Bi 6.1.1.2 release updates

SSL+RMI. Security update and enhancing the RMI communication with SSL

What is RMI?

RMI (Remote Method Invocation) is an API that provides a mechanism to create distributed application in java. It allows an object to invoke methods on an object running in another JVM.

Threats posed

- Customer reported vulnerabilities due to plain sockets.
- Remote code Execution.

How RMI is used inside SI?

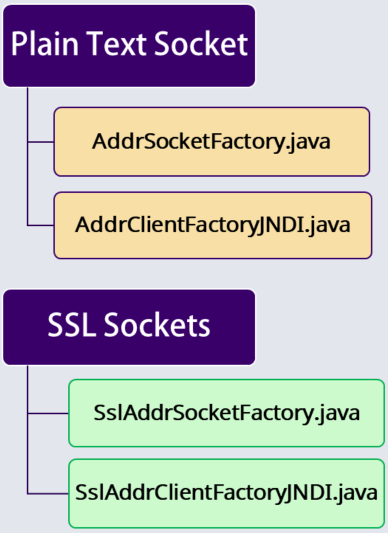
- RMI registry is accessed by JNDI (Java Naming and Directory Interface).
- JNDI API takes care of STUB creation for Client side.
- The Server Hosts object using RMI socketFactories and Registers the object inside JNDI tree.
- Ops server performs jndi.lookupRmi() method to look for RMI object inside JNDI Tree.
- If the Object is present in JNDI tree then the subsequent node shows available in OPS_NODE_INFO table.

SSL implementation on RMI

- Controlled by a new Property in security.properties
- useSSLforRMI=true/false (Default is false)

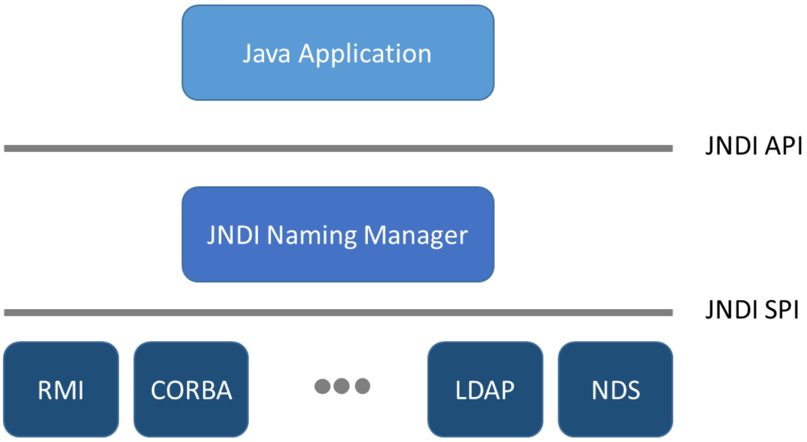
- For object Declaration Client and Server Sockets are used.
- By Default SI had Plain text socket.
- Based on the value of flag SSL sockets are used.
- SSL sockets use protocol TLSv1.2.

OCP is not covered yet, will be covered in future release.


Plain Text Socket
AddrSocketFactory.java
AddrClientFactoryJNDI.java
SSL Sockets
SslAddrSocketFactory.java
SslAddrClientFactoryJNDI.java

Flag Based Control

- If "**useSSLforRMI**=false" the ops server can communicate to RMI object servers on plain text socket.
- If "**useSSLforRMI**=true" the ops server will use SSL client socket and will be able to communicate to RMI object servers having SSL server sockets.



- Secure communication between Ops server and other JVM (ASI, Liberty, Adapter Container).

Sample ops command:

- ./opscmd.sh –nnode1 –cISUP
- ./opscmd.sh –nnode1 -cCHECKJNDI
- ./opscmd.sh –nnode1 –cLISTNODESTATUS

SSL Certificate Configuration

- Certificate (rmissl) gets created at install time as part of post install service routine.
- Once default cert is created, next upgrade will skip recreating it.
- Algorithm and key length used: RSA with 2048.
- Certificate stored in Database.
- Certificate adheres to NIST specifications.

Support for Custom Certificates

- The exiting certificate UI in dashboard can be used to create/update new certs with required specifications.

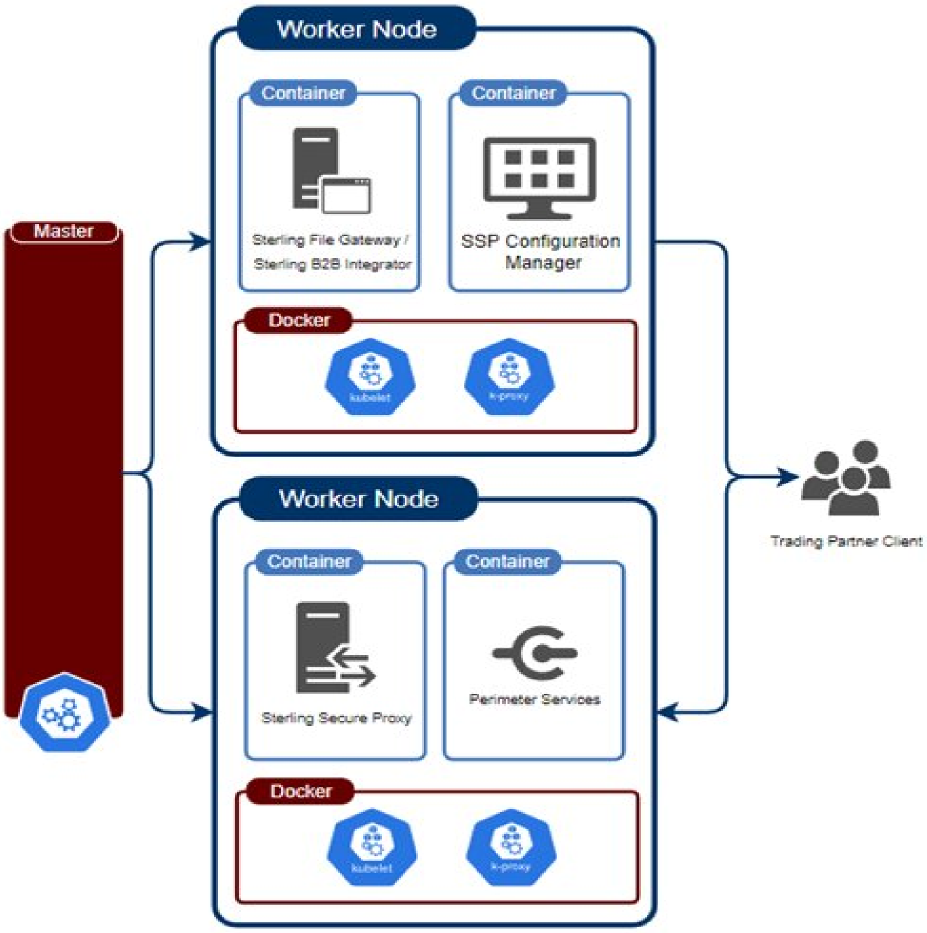
Methods to verify if SSL is enabled for RMI

- We can use open_SSLClient against the RMI port to validate the config.
  Configured certificate and TLS protocol value will be displayed with the below command.

  echo "" | openssl s_client -connect <HOST NAME>:<RMI PORT>.
- LOGs – system.log, ops.log, noapp.log. Additional loggings added for triaging SSLRMI related flows in DEBUG mode.
- Network trace can be captured against the specified Ports for RMI communication.

IBM Secure Proxy (SSP) and IBM Sterling External Authentication Server (SEAS) Implementations

SFTP, HTTP or FTP configuration on SSP in passthrough.



Implementation 1.

Migrate SSP and their configurations

These tasks focus on the migration of SSP configurations to a new environment and their validation.

Tasks:

- Migration artifacts from/to IBM Secure Proxy
- Certificates & Keys migration to IBM Secure Proxy
- Unit tests
- Evidences documentation
- Support

Implementation 2.

SFTP, HTTP or FTP configuration on SSP in passthrough.

This task focuses on implementing SSP in a MFT environment with the configuration of secure communications for the DMZ (Secure MFT environment).

Tasks:

- Study and generation of artifacts in IBM Secure Proxy for SFTP, HTTP, FTPS or C:D
- Study and generation of artifacts in IBM B2B Integrator for SFTP, HTTP, FTPS or C:D
- Certificates or Keys migration to IBM Secure Proxy
- Secure connections between SSP and SBI
- Unit tests
- Evidences documentation
- Support

This architecture contains all the advantages of installing a reverse proxy at the DMZ level.

Authentication is delegated to a Backend service, in this case, IBM Sterling File Gateway / IBM Sterling B2B Integrator.

A single open connection from the Trusted Zone to the DMZ for all incoming protocols.

Implementation 3.

SFTP configuration in SSP with SEAS in SSO delegating password to LDAP

This task focuses on the implementation of SSP and SEAS in a MFT environment with the configuration of secure communications for the DMZ and delegation of user and password authentication for inbound communications delegated to an LDAP or AD.

Tasks:

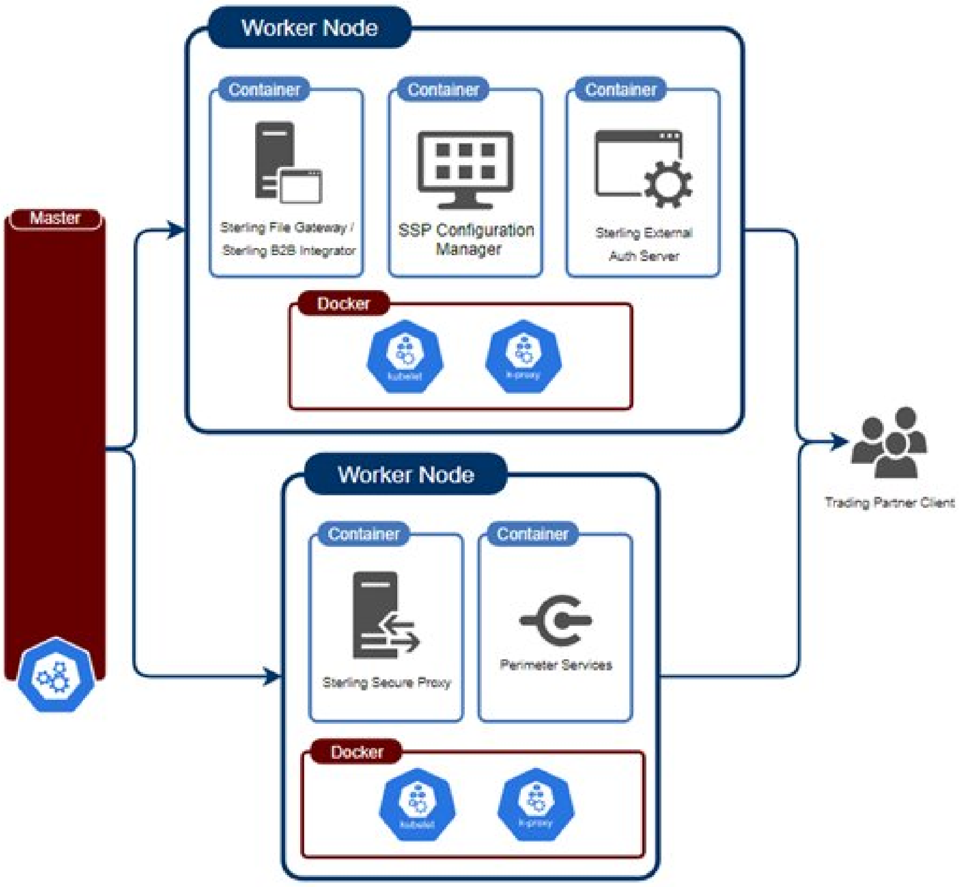
- Study and generation of artifacts in IBM Secure Proxy and IBM B2B Integrator for SFTP.
- Study and generation of artifacts in SEAS for password auth in LDAP.Keys configuration to IBM Secure Proxy.
- Secure connections between SSP and SBI.
- Unit tests.
- Evidences documentation.
- Support.

This architecture contains all the advantages of installing a reverse proxy at the DMZ level.

Authentication using user/password relation with a single validation thanks to the Single Sign On (SSO) functionality.

Authentication is done at DMZ level using SEAS communication which in turn delegates authentication to LDAP.

A single open connection from the Trusted Zone to the DMZ for all incoming protocols.



Implementation 4.

SFTP configuration in SSP with SEAS in SSO delegating password to LDAP and KEY to SBI

This task focuses on the implementation of SSP and SEAS in a MFT environment with the configuration of secure communications for the DMZ and delegation of user and password authentication for inbound communications delegated to an LDAP or AD and user and SSH key authentication delegated to SBI.

Tasks:

- Study and generation of artifacts in IBM Secure Proxy and IBM B2B Integrator for SFTP
- Study and generation of artifacts in SEAS for password auth in LDAP and key auth in SBI
- Keys configuration to IBM Secure Proxy
- Secure connections between SSP and SBI
- Unit tests
- Evidences documentation
- Support

This architecture contains all the advantages of installing a reverse proxy at the DMZ level.

Authentication using user-password and/or user-key relation with a single validation thanks to the Single Sign On (SSO) functionality.

Authentication is done at DMZ level using SEAS communication which in turn delegates authentication to LDAP for Password and SBI for Key.

A single open connection from the Trusted Zone to the DMZ for all incoming protocols.

Rating for security

- **Implementation 1:** Migrate SSP and their configurations
  Level 1 Low secure
- **Implementation 2:** SFTP, HTTP or FTP configuration on SSP in passthrough
  Level 2 Medium secure
- **Implementation 3:** SFTP configuration in SSP with SEAS in SSO delegating password to LDAP
  Level 3 High secure
- **Implementation 4:** SFTP configuration in SSP with SEAS in SSO delegating password to LDAP and KEY to SBI
  Level 3 High secure

Level 3 High secure

High Secure: The solution consists of up-to-date security elements.

Level 2 Medium secure

Medium Secure: The solution consists of up-to-date security elements but there is potential for improvement.

Level 1 Low secure

Low Secure: The solution lacks up-to-date security features and optimization is strongly recommended.

Communication

If you need more information about any of the contents of our newsletter, please do not hesitate to contact us. We will be happy to answer your questions.

info@b2b.solutions