**WSA Use Case mock POC - Attendees**

**Details about the WebSphere 8.5.5.15 environment**

**-**  WAS 8.5.5.15 Installation location: /opt/IBM/WebSphere/AppServer85515/

- WAS 8..5.5.15 Profile and location: Profile AppSrv01 in /opt/IBM/WebSphere/AppServer85515/profiles/AppSrv01

- WAS 8.5.5.15 Server name: tWAS\_85515\_server

- WAS 8.5.5.15 Admin credentials: wsadmin/wsadmin

**Details about the WebSphere 9.0.5.7 environment**

- WAS 9.0.5.7 Installation location: /opt/IBM/WebSphere/AppServer9057/

- WAS 9.0.5.7 Profile and location: Profile AppSrv01 in /opt/IBM/WebSphere/AppServer9057/profiles/AppSrv01

- WAS 9.0.5.7 Server name: tWAS\_9057\_server

- WAS 9.0.5.7 Admin credentials: wsadmin/wsadmin

**Convenience scripts:**

* imcl\_ifix\_install.sh - Script to install iFIX IFPH4276 for CVE-2021-44228
* imcl\_ifix\_uninstall.sh - Script to uninstall iFIX IFPH4276 for CVE-2021-44228

**Accessing the environment:**

**Step 1: Login to OpenShift Console**

**Hint:** You can launch the **OpenShift console** from the ROKS Cluster in IBM Cloud.

**Hint:** You will be logged in with your IBM ID (which is your IBM intranet ID) that is mapped to the ROKS environment.

**Step 2: Login to the OpenShift CLI**

**Hint:** You can get the instructions for logging into OCP via CLI from the ROKS Cluster in IBM Cloud

**Hint:** Use the Desktop VM that is provided to login to OCP via CLI. We have installed the oc CLI there for you.

**Step 3: Go to the webSphere-automation project in OCP in the CLI and UI**

**Hint:** In the training environment, we installed websphere automation into the OC project named “**websphere-automation**”. You must work from that project when running CLI commands and accessing the WSA operator from the OCP console.

**Step 4: Obtain the WebSphere Automation Dashboard URL**

**Hint:** The product documentation section for accessing the WSA UI is here: <https://www.ibm.com/docs/en/ws-automation?topic=accessing-websphere-automation-ui>

**Hint:** Product documentation for finding the WSA URL: <https://www.ibm.com/docs/en/ws-automation?topic=ui-finding-websphere-automation#in-t-findroute>

**Hint:** The Was endpoint can be found in the instance of the “**wsa**” operator, from the OCP console. Look for Installed Operators

**Step 5: Obtain the password for the "admin" user in WebSphere Automation**

**Hint:** The product documentation section for accessing the WSA UI is here: <https://www.ibm.com/docs/en/ws-automation?topic=ui-default-administrator-profile#cf-c-defaultadmin>

**Step 6: Login to WebSphere Automation UI**

**Hint:** Login using the user: “admin” and the password you discovered from the previous step.

**Hint:** Use the login method: “IBM provided credentials (admin only)

**Use Case #3: Setup the email notifications for newly detected CVEs from WebSphere Automation**

**Hint:** The product documentation for setting up notifications is here: <https://www.ibm.com/docs/en/ws-automation?topic=automation-configuring-notifications>

**What you will do in this use case:**

* Configure WSA to use a Tech-Academy-provided SMTP server
* Configure WSA alert notifications to Tech-Academy designated email address(es)

**Step 1: Setup the SMTP server using the provided SMTP server that is configured for this training**

Use the following information to configure the SMTP server that is provided for the technical academy.

* SMTP server: **smtp.gmail.com**
* port: **465**
* Sender email address: **waswwdemo@gmail.com**
* Username: **waswwdemo@gmail.com (this is the email address that will SEND the email notifications)**
* Password: **vmbmpnheecccoxwc (This is an app password I setup in the Google account for the WAS Automation app)**

**Step 2: Setup the email addresses to receive notifications of newly detected CVEs from WebSphere Automation**

Add your personal or work email to receive notifications of new security vulnerabilities.

* 1. Click the **Add** button
  2. Enter *your* ***email address***
  3. click **Save**

**Use case #3 Evaluation Criteria:**

* Demonstrate to instructor that email notifications delivered to the designated email address(es) when new CVEs are detected as the two WAS servers are registered with WSA.
* Completion of Use case #4 is required to fulfil this use case evaluation criteria.

**Use Case 4: Integration with WAS ND servers**

**Hint:** The product documentation for registering Traditional WS servers is here: <https://www.ibm.com/docs/en/ws-automation?topic=monitoring-registering-websphere-application-server-traditional-servers>

**What you will do in this use case:**

* Obtain the information required to register WAS servers with the usage metering service in WSA
* Create the python script using the example code in the product documentation, which is used to register WAS servers to the usage metering service
* Register the WAS servers to the usage metering service in WSA
* Verify the WAS servers are now reporting security posture information in WSa
* Verify that you are receiving email notifications for CVE vulnerabilities in the newly registered WAS server

**Step 1**: get the **usage metering URL** in WebSphere Automation and save it to a file “/home/student/metering-url.txt” on the Desktop VM

**Hint:** must be logged into OCP via CLI

**Step 2**: Ensure the “metering-url.txt” file contains the metering URL

**Hint:** cat and gedit commands are available on the Desktop VM

**Step 3**: get the **api-key** that will be used to authenticate the WebSphere Application Servers during the registration process and save it to a file named “/home/student/api-key.txt” on the Desktop VM

**Step 4**: Ensure the “api-key.txt” file contains the token needed for authentication

**Step 5:** Start the WAS 8.5.5.15 server. It must be running to register to the metering service (WSA)

**Hint**: To start the WAS 8.5.5.15 server: /opt/IBM/WebSphere/AppServer85515/bin/startServer.sh tWAS\_85515\_server

**Step 6:** Create the create the file “**configuretWasUsageMetering.py”** on the Desktop VM. Then copy/paste the contents from the example in the product documentation into the python file.

## Hint: I recommend registering the WAS servers using the method described in the product documentation: “Running the example configuretWasUsageMetering wsadmin script to register your application server with WebSphere Automation” located here: <https://www.ibm.com/docs/en/ws-automation?topic=monitoring-registering-websphere-application-server-traditional-servers#cf-t-add-was__wsascript>

**Step 7:** Register the **WAS 8.5.5.15 server** with WebSphere Automation

**Hint:** Use wsadmin to run the **configuretWasUsageMetering.py script**

**Hint:** To use the files containing the metering service url and api-key, you can pass in the arguments to the script using:

url=$(cat /home/student/metering-url.txt) apiKey=$(cat /home/studentapi-key.txt)

**Hint:** The **trustStorePassword** parameter can be any password you choose**:** The TrustStore will be created during registration, with the password you pass in.

**Step 8:** Verify the WAS 8.5.5.15 is registered and is now listed in the **Application runtimes**  **> Security > Servers** view in the WSA dashboard.

**Step 9:** Check your email that you registered for notifications. Verify you received CVE notifications for the registered server. It may take a few minutes for the email to arrive to your inbox.

**Step 10:** Keep the email until the use case evaluation criteria is completed and signed-off for the mock POC.

**Step 11:** Start the WAS 9.0.5.7 server. It must be running to register to the metering service (WSA)

**Hint**: To start the WAS 9.0.5.7 server: /opt/IBM/WebSphere/AppServer9057/bin/startServer.sh tWAS\_9057\_server

**Step 12:** Register the **WAS 9.0.5.7 server** with WebSphere Automation

**Hint:** Use wsadmin to run the **configuretWasUsageMetering.py script**

**Hint:** To use the files containing the metering service url and api-key, you can pass in the arguments to the script using:

url=$(cat /home/student/metering-url.txt) apiKey=$(cat /home/studentapi-key.txt)

**Hint:** The **trustStorePassword** parameter can be any password you choose**:** The TrustStore will be created during registration, with the password you pass in.

**Step 13:** Verify the WAS 9.0.5.7 is registered and is now listed in the **Application runtimes**  **> Security > Servers** view in the WSA dashboard.

**Step 14:** Check your email that you registered for notifications. Verify you received CVE notifications for the registered server. It may take a few minutes for the email to arrive to your inbox.

**Step 15:** Keep the email until the use case evaluation criteria is completed and signed-off for the mock POC.

**Use case #4 Evaluation Criteria:**

* Confirm that configured WAS servers are successfully communicating with the WSA system and accurately reporting their application version/release/patch history/ fixpack status and operational posture
* Demonstrate the ease of monitoring multiple WAS server deployments using the WSA User Interface (web client)
* Review detailed CVE and patch history of WAS servers to understand when an issue was detected, when it was fixed, and days exposed
* Illustrate that CVE vulnerabilities are detected and reported to the WSA system as servers are registered
* Illustrate email notifications received as servers are registered

**Use Case 5: Install WebSphere iFix or Fixpack to resolve CVE**

**What you will do in this use case:**

* Review unresolved CVEs of WAS servers as reported in WSA dashboard
* Identify a high severity CVE to resolve, and patch one of the two WAS servers (8.5.5.15 or 9.0.5.7)
  + Download the recommended iFIX from IBM Fix Central
  + Using traditional WAS installation manager tool, install the recommended iFIX to resolve a high severity CVE that is detected.
* Illustrate resolved CVEs and patch updates/changes to a particular WAS server are reported to the WSA system in real time (or near real time)

**Step 1:** Review the CVEs for the 8.5.5.15 or 9.0.5.7 server in WSA.

**Step 2**: Determine a high severity unresolved CVE to resolve via WebSphere intermediate Fix (iFix) installation

**Step 3**: View the IBM Security bulletin for the CVE you intend to resolve. Identify the recommended iFix that needs to be installed to resolve the CVE

**Step 4:** Download the recommended iFIx for the selected CVE

**Hint**: Be sure to download the iFix for the version of WebSphere that you are patching. Even for the same CVE, the patch is different from 8.5.5 and 9.0.5 WAS servers

**Hint:** If you cannot access IBM FIX central using your IBM ID, let the instructor know, so an alternative solution can be provided. We have downloaded a specific iFIX for a high severity CVE, for this situation.

**Step 5:** Install the iFIx into the WAS server

**Hint**: Server must be stopped to install the iFIX, and restarted after the fix is applied

**Hint:** iFixes are installed using IBM Installation Manager (IM). You can use the IM UI which can be launched from **/opt/IBM/InstallationManager/eclipse/launcher.** Or you can update a script that we provide, which installs and iFIX using the Installation Manager command rather than the UI. This script is **imcl\_ifix\_install.sh** and is provided in the git hub repository for the technical academy. (You will need to make simple modifications to the script to install your specific iFIX).

**Step 6**: in WSA, view the updated security details for the patched server.

* Show iFix installed via the patch history
* Show the CVE is now resolved
* Show the list of Applied iFixes for the servers
* Show the specific CVE, and identify the servers which are patched, and which still show vulnerability to the specific CVE
* Show the number of days the servers have been vulnerable. (Hint: num days is relative to the day the server was registered with WSA)

**Use case #5 Evaluation Criteria:**

* Illustrate resolved CVEs and patch updates/changes to a particular WAS server are reported to the WSA system in real time (or near real time).
* Be prepared to showcase, to the instructor, the items in step 6 of this use case

**Use Case 6: Audit Reporting – Security roles and permissions**

**What you will do in this use case:**

* Configure a new user and user role for permissions to generate/view audit report detailing the current WAS estate inventory and its version/release/fixpack/APAR status

**Step 1:** As WSA **admin** user (your default user you are logged in with now), go **to Administration > Access Control** in WSA

**Step 2:** Add a new user (which will NOT have administrative role)

**Hint:** IN the add user dialog, enter the IBM ID of the user which is assigned the IBM Cloud / ROKS account. For example, for me its “kevinlp@us.ibm.com”

**Step 3:** Assign the “WebSphere Automation Security” role to the new user

**Hint:** You can assign roles directly, or create a new group and assign to the group… But do not use the admin group that exists.

**Step 4:** Logout of WSA as the admin user

**Step 5:** Login to WSA as the new non admin user

**Hint:** Use the “OpenShift Authentication” method, not the “IBM provided credentials” method

**Hint:** For IBMers, this user is mapped to your W3 ID, you will be prompted to login through SSO, providing your W3 credentials

**Step 6:** In WSA, view the left navigation menu. Verify that you do not have Administration links

**Step 7:** Go to the **Operate > Application runtimes > Security** view

**Step 8:** Export the generated report to CVS-formatted file, which is a snapshot of the current security posture of all registered servers

**Use case #6 Evaluation Criteria:**

* Added your [IBMID@us.ibm.com](mailto:IBMID@us.ibm.com) user to WSA
* Added **WebSphere Automation Security** role to your new user
* Login using **OpenShift Authentication** Login for this new user
* Confirm the new non-admin user can view the current state of the WAS servers
* Export generated report to CSV-formatted file

## Presentation the Proof of Concept Results

The POC team will prepare and deliver an informal walk-though demonstration showcasing the Proof of Concept results to the instructors. During the walk-through, it may not be feasible to demonstrate the Evaluation Criteria for all the Use Cases due to time constraints and/or other restrictions. For those use cases that cannot be actively demonstrated, the POC tea will describe to the instructor how each use case was validated.

**POC Completion Criteria:**

* The PoC project will be considered complete when all Use Cases have been achieved and signed off by the instructor
* To complete this POC, All use cases that are in scope must be demonstrated to Tech Academy instructor, showing completion criteria of the mock POC