IBM Cloud Pak for AIOps Proof-of-Concept for

MBBANK

Table of Contents

[Executive Summary 2](#_Toc193902467)

[Business Goals 2](#_Toc193902468)

[Contacts 3](#_Toc193902469)

[IBM/SVTECH Account Team 3](#_Toc193902470)

[MBB Team 3](#_Toc193902471)

[Proof of Concept Scope 5](#_Toc193902472)

[Use Cases Definitions: 6](#_Toc193902473)

[Use Case #1: Centralized platform for monitoring data 6](#_Toc193902474)

[Use Case #3: Incident confirmation using both pre-defined rules and AI 9](#_Toc193902475)

[Use Case #4: Probable root cause localization and remediation actions suggestion 12](#_Toc193902476)

[IBM/SVTECH Responsibilities 14](#_Toc193902477)

[MBB Responsibilities 14](#_Toc193902478)

[Sequence of Events 15](#_Toc193902479)

[POC Integration Architect 16](#_Toc193902480)

[POC Deployment Architect 16](#_Toc193902481)

[MBB POC Environment 17](#_Toc193902482)

[Hardware Requirements to be provided by the MBB 17](#_Toc193902483)

[Data Sources in the Scope of POC 18](#_Toc193902484)

## Executive Summary

### Business Goals

The primary objective of this Proof of Concept (POC) on AIOps is to address the existing challenges stemming from siloed teams within the organization. By leveraging Artificial Intelligence for IT Operations (AIOps), we aim to enhance collaboration, streamline communication, and establish common goals across departments. The focus lies on breaking down silos, fostering synergy, and driving efficiency through a unified approach to IT operations.

Through this POC, we aim to address the identified challenges by harnessing the power of Artificial Intelligence and advanced analytics. By breaking down silos, fostering collaboration, and aligning goals, we seek to transform the IT operations landscape, driving efficiency, and agility across the organization.

This POC will address improvements on:

* Centralized monitoring data from many monitoring tools
* Grouping/correlation/consolation data
* AI-assisted rule-base incident confirmation
* Probable root cause localization and remediation

## Contacts

### IBM/SVTECH Account Team

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Telephone** | **Email** |
| Linh Vũ | Sale | **+84946265381** | linh.vu@ibm.com |
| Trần Văn Đồng | Tech | **+84396738954** | Dong.Tran1@ibm.com |
| Trần Nhân | IBM Client Engineering | **+84 784888899** | Nhan.Tran@ibm.com |
| Yongjie Guo | IBM AP AIOps SWAT |  | Yongjie.Guo@ibm.com |
| Yang Kwang Gok | Asean Senior AIOps Technical Specialist |  | gohykw@sg.ibm.com |
| Phan Thanh Hoàng | Sale | **+84968919583** | hoang.phan@svtech.com.vn |
| Hoàng Trọng Tôn | Project Manager | **+84905608882** | ton.hoang@svtech.com.vn |
| Trần Sơn Tùng | AIOps Specialist | **+84868998836** | tung.tran@svtech.com.vn |
| Lương Thế Lâm | AIOps Specialist | **+84916057669** | lam.luong@svtech.com.vn |
| Bùi Thu Hà | AIOps Specialist | **+84 367997052** | ha.bt@svtech.com.vn |

### MBB Team

|  |  |  |  |
| --- | --- | --- | --- |
| **Name and POC Role** | **Title** | **Telephone** | **Email** |
| Phạm Văn Cường | Giám đốc |  | Cuongpv.ho@mbbank.com.vn |
| Nguyễn Tiến Tùng | Trưởng phòng |  | Tungnt16@mbbank.com.vn |
| Vũ Duy Phương | Trưởng Phòng |  | Phuongvd.ho@mbbank.com.vn |
| Vũ Ngọc Thưởng |  | **0865912410** | thuongvn@MBBANK.com.vn |
|  | TBD |  |  |
|  | TBD |  |  |
|  | TBD |  |  |
|  | **TBD** |  |  |

## Proof of Concept Scope

To prove the ability to achieve MBB’s Business Goals, IBM/SVTECH and MBB have identified the following Required Capabilities and associated Metrics.

List of use cases in scope with success criteria:

* Centralized monitoring data from many monitoring tools
* Grouping/correlation/consolation data
* ~~AI-assisted~~ rule-base incident confirmation
* Probable root cause localization and remediation

Business service: Mobile App (Mobile Banking). Define related components at technical perspective. **TBD.** For example: fund transfer for internal account. The business services should be monitored by the belowed tools:

* Application Monitoring: Don’t have.
* Infrastructure Monitoring: Splunk (RAM, CPU,… Server Monitoring) -> gather alert information.
  + Greylog: Syslog.
* Network Monitoring: Solarwinds, PRTG. Runing on-premises, Splunk. -> gather alert information.
* Topology Management: document files (visio).
* ITSM: SDP (sevice desk – incident and request management)
  + Output – ticketing:
  + Input - reference knowledge based:
  + Gather alert information.
* Others:
  + Grafana, Kibana of ELK.
  + Collect: java exporter, prometheus (process monitoring, transaction monitoring), cloud control of oracle database (OEM), ELK (log centralize for transaction)
  + Gather alert information.
  + Prometheus: Metric, Alert

System in PoC: K8s, VMware, Queue, T24

Env: UAT/DEV (K8s, VMware, Queue, T24)

High level flow

TBD. <Need MBB provide>

POC Start Date: 01 May 2025

POC Completion Date: 01 Oct 2025

## Use Cases Definitions:

|  |  |
| --- | --- |
| Use Case #1: Centralized platform for monitoring data | |
| **Situational Use Case** | Currently we have deferent monitoring tools for each layer (app, infra, logs, network) in each monitored target system (K8s, VMware, Queue, T24) need to do integration to Monitoring tools to have centralized platform for monitoring data. **Import topology data, log, metric, event** and create service views, where possible, to enable visualization of key services and prepare data for AIOps Processing. |
| **Existing Solution** | * ~~APM???: Monitored App, infra for (K8s, VMware, Queue, T24)~~ * ELK/Splunk: Monitored logs for (K8s, VMware, Queue, T24) * Grafana: Monitored App, infra for (K8s, VMware, Queue, T24) * SolarWinds: Monitored networks for (K8s, VMware, Queue, T24) |
| **Success Criteria (SC)** | 1. Integration of all tools in scope    1. ~~APM (Metric, Topology, Events)~~ Topology from file.    2. ELK/Splunk (logs treat as events)    3. Grafana (logs treat as events)    4. SolarWinds (simulated event of SolarWinds based on MBB topology) 2. Near real-time data collection: After Integration event shown in CP4AIOps’s Alert Viewer in near real-time 3. Near real-time data correlation: After Integration we can see 1 example event correlation from many data sources in near real-time in CP4AIOps’s Alert Viewer 4. Build and visualize topology graph: After Integration we can see 1 example topology graph of all components in the scope of business services |
| **Implementation and Test Scenarios** | **Steps 1**) APM  - MBB: Review and ensure system in scope (UAT) are on APM (events, metrics, topology)  - IBM/SVT: Configure CP4AIOps APM integrations    **Steps 2**) ELK/Splunk:  IBM propose integrating with ELK/Splunk and treating logs as AIOps events.  - IBM/SVT: [Configure CP4AIOps Webhook listener receiver](https://www.ibm.com/docs/en/cloud-paks/cloud-pak-aiops/4.8.1?topic=integrations-generic-webhook)  - IBM/SVT/MBB: Set Up ELK/Splunk Alert for Error/Exception/Warning Logs    **Steps 3**) [Grafana](https://grafana.com/docs/grafana/latest/alerting/configure-notifications/manage-contact-points/integrations/webhook-notifier/) Cloud: Webhook (treat Grafana alert as AIOps events)  - IBM/SVT: Configure CP4AIOps Webhook listener  - IBM/SVT: Configure Grafana to send notification using Webhook connector    **Steps 4) SolarWinds**: (Alerts, topology)  **Alerts**:  - IBM/SVT: Provide Normalized Alerts Schema  - IBM/SVT: Configure CP4AIOps Webhook listener  - IBM/SVT: Create script to simulate alerts to send to CP4AIOps Webhook  **Topology**:  - MBB: Export from SolarWinds because AIOps don’t have OOTB connection and SolarWinds is Prod env.   * IBM/SVT: Convert the file provided into the format for AIOPs File Observer. * IBM/SVT: Load the converted file and display the application topology.   **Step 5**) **Verify**  - MBB: Verify event from APM shown in CP4AIOps’s Alert Viewer in accordance with Success Criteria 1, 2  + Execute Performance test by push heavy load to increase 80% CPU in DB 🡪 Abnormalities from APM are shown on AIOps  + Execute Performance test by push heavy load to increase 80% CPU in App servers 🡪 Abnormalities from APM are shown on AIOps  - MBB: Verify event from ELK/Splunk shown in CP4AIOps’s Alert Viewer in accordance with Success Criteria 1, 2  + Make logs have “Warning” string in logs (index of App in scope) 🡪 Logs are shown on AIOPS  - MBB: Verify event from Grafana shown in CP4AIOps’s Alert Viewer in accordance with Success Criteria 1, 2  + Execute Performance test by push heavy load to increase 80% CPU in DB 🡪 Abnormalities from Grafana are shown on AIOps  + Execute Performance test by push heavy load to increase 80% CPU in App servers 🡪 Abnormalities from Grafana are shown on AIOps  - MBB: Verify events from SolarWinds shown in CP4AIOps’s Alert Viewer in accordance with Success Criteria 1, 2 🡪 Simulated events from Solar winds are shown on AIOps  - MBB: Verify event correlation shown in CP4AIOps’s Alert Viewer in accordance with Success Criteria 3  + Execute Stress Performance test to reach threshold on Application & Infra layer 🡪 Corelated abnormalities are generated from APM , Grafana are shown on AIOPS  - MBB: Verify topology graph shown in CP4AIOps’s Resource management Viewer in accordance with Success Criteria 3 |
| **Dependencies** | - MBB: To be able to generate Incident |

|  |  |
| --- | --- |
| Use Case #2: Incident confirmation using both pre-defined rules ~~and AI~~ | |
| **Situational Use Case:** | **Step 1.**  **Abnormality Detection**: ~~AI~~ system correlates data from monitoring tools (or self-collected) to detect abnormalities in metrics/events/logs **at least** in the monitoring data defined for each target systems  **Step 2.**  The AI grouping/correlation/consolidation the incoming events/alerts  **Step 3.**  **Pattern Matching And Confirmation**: The system matches the detected abnormality via pre-defined rules and AI to confirms incidents.  **Pre-defined:**  Logic is to use combination of business metrics abnormalities and other metrics to correlate (combine)  **Current pre-defined rules are based on combination of different alerts/metrics abnormalities manually correlated.** |
| **Existing Solution** | The main tools that are in scope and the staff will do manual correlation of the alert and anomaly from the monitoring tools to confirm all type of incidences. |
| **Success Criteria (SC)** | 1. Confirmed incidents must be easily recognizable on the UI, including information but not limited to:    1. **What** - Title and relevant description    2. **When** - Timestamp of an incident start and end (if closed).    3. **How** - Contributing abnormalities to this incident 2. Demonstrate AI capabilities in improving incident confirmation rules.    1. Must show how over time incident confirmation can be done with **minimal manual effort**for recurring incidents by creating/updating correlation(grouping) between abnormality which contribute to the incident confirmation. 3. Incident types confirmed based on pre-defined and AI include incident caused by:    1. Third party    2. Application    3. Infrastructure    4. Network    5. Database 4. At least 70% accuracy for known incident confirmation 5. Incident Confirmation time including time of data integrated plus 30 seconds (Acceptable Timebox). |
| **Implementation and Test Scenarios** | **Steps**:   1. Ingest data in the scope (already done in UC1) 2. IBM/SVT: Trained system on metric data 3. IBM/SVT/MBB: Generated metric anomaly alerts 4. IBM/SVT: Create correlated set of alerts. 5. MBB: Provide pre-defined rules    1. Rules for confirm incident based on Mobile App success rates 6. IBM/SVT: Simulate success rate to AIOps system 7. IBM/SVT: Create AIOps incident policy that trigger from this set of alerts. 8. MBB: Simulate incident    1. Third party: smoke test on Queue to Napas by MBB team, IBM/SVT simulate success rate to AIOps system, Mule trigger events 🡺 Incident created    2. Application: JDBC full, IBM/SVT simulate success rate to AIOps system 🡺 Incident created    3. Infrastructure: Stop 2 VMs run ESB, IBM/SVT simulate success rate to AIOps system 🡺 Incident created    4. Networks block/deny on the Security team and see APM can’t connect to DB, IBM/SVT simulate success rate to AIOps system 🡺 Incident created    5. Database: snapshot, stop DB, IBM/SVT simulate success rate to AIOps system 🡺 Incident created 9. IBM/SVT: group the abnormalities which contribute to the incident confirmation |
| **Dependencies** | MBB:   * Make sure history Metrics data (2 weeks of normal baseline data with 5 min interval) on APM . * Event data from multiple sources. (Refer to UC1) * Topology data corresponding to the event/alerts. (Refer to UC1) |

|  |  |
| --- | --- |
| Use Case #3: Probable root cause localization and remediation actions suggestion | |
| **Situational Use Case:** | The system leverages AI to analyze data and propose the probable root cause locations. It identifies the layer and component most likely responsible for the issue and displays this information on a user-friendly web interface.  By analyzing historical incident data and correlating it with current issues, the tool can recommend the highest probability predefined runbook or set of text-based recommendations of possible steps to recover/reduce severity of the incident via Web UI. |
| **Existing Solution** | Manual procedure recommended on root cause for remediation. |
| **Success Criteria:** | 1. Show probable root cause location(s) via text and visual topology of contributing layer/component for incident types:    1. Third party    2. Application    3. Infrastructure    4. Network    5. Database 2. Remediation actions are suggested via text/runbook for incident confirmed in **UC3** 3. Incident Confirmation time including time of data integrated plus 30 seconds (Acceptable Timebox). |
| **Implementation and Test Scenarios** | **Steps**:   1. AIOps System: probable cause analysis is functioning as expected. 2. IBM/SVT: Create sample runbooks and policy from ~10 runbooks that MBB provide 3. MBB: Provide the associate runbook linked to the incident 4. MBB: Simulate incident    1. Third party: smoke test on Queue by MBB team, IBM/SVT simulate success rate to AIOps system, Mule trigger events 🡺 AIOps provide top 3 probable root cause Incident created    2. Application: JDBC full, IBM/SVT simulate success rate to AIOps system 🡺 AIOps provide top 3 probable root cause Incident created    3. Infrastructure: Stop 2 VMs run ESB, IBM/SVT simulate success rate to AIOps system …🡺 AIOps provide top 3 probable root cause Incident created    4. Networks block/deny on the Security team and see APM can’t connect to DB, IBM/SVT simulate success rate to AIOps system 🡺 AIOps provide top 3 probable root cause Incident created    5. Database: snapshot, stop DB, IBM/SVT simulate success rate to AIOps system… 🡺 AIOps provide top 3 probable root cause Incident created 5. IBM/SVT: AIOPS show runbook linked to incident in GUI |
| **Dependencies** | MBB: Provide sample alert data link to the runbook. |

## IBM/SVTECH Responsibilities

* SVTECH will provide an engineer to assist with the deployment and configuration of the solution in your environment.
* The IBM/SVTECH team will ensure that the agreed required capabilities will be completed during the evaluation.
* IBM/SVTECH will perform weekly follow-up meetings to address any questions and continue with knowledge transfer to the MBB team.
* The IBM/SVTECH team will conduct an executive wrap up meeting at the end of the POC.

## MBB Responsibilities

* MBB will schedule resources and identified SMEs to be available during the POC.
* MBB will have all stakeholders and the executive team in the wrap-up meeting at the end of the POC.

## Sequence of Events

|  |  |
| --- | --- |
| **Start Date** | **Event** |
| 27 Feb 2025 | POC Document Prepared and Sent to MBB Team for Review |
| 7 Mar 2025 | POC Document Reviewed and Approved by MBB and Cloud Pak for AIOps Evaluation team |
| 10 Mar 2025 | POC preparation   * Hardware/Infra Preparation * Initial setup/configuration * Internet (proxy) setup * Remote access |
| 14 Mar 2025 | Integration according to scope and use cases |
| 19 Mar 2025 | Use case #1: configuration & testing |
| 26 Mar 2025 | Use case #2: configuration & testing |
| 31 Mar 2025 | Use case #3: configuration & testing |
| 02 Apr 2025 | Prepare POC Wrap-Up Documentation |
| 04 Apr 2025 | POC Wrap-up Meeting |

## POC Integration Architect

<To be discuss>

## POC Deployment Architect

<To be discuss>

## MBB POC Environment

### Hardware Requirements to be provided by the MBB

**Minimum requirement for Cloud Pak for AIOps deployment on Linux base VMs**

<https://www.ibm.com/docs/en/cloud-paks/cloud-pak-aiops/4.8.1?topic=linux-planning>

**8 worker + 3 master + 1 HA + 1 bastion + 1 Client windows + 1 VMs for Netcool**

* **Red Hat® Enterprise Linux® 9.4**
* **1 x load-balancer host: 4 CPU, 16 GB RAM, 300 GB disk**
* **3 x control plane nodes: 16 CPU, 32 GB RAM, 300 GB disk + (2 x 300 GB disks)**
* **8 x worker nodes: 16 CPU, 64 GB RAM, 300 GB disk + (1 x 300 GB disk)**
* **1 x Netcool host: 16 CPU, 32 GB RAM, 300 GB disk**
* **1 x bastion host: 4 CPU, 16 GB RAM, 300 GB disk**
* **1 x Client windows host: 4 CPU, 16 GB RAM, 300 GB disk**

A screenshot of a computer

AI-generated content may be incorrect.

**Recommended storage providers**

The following table shows the tested and supported storage providers that are recommended for a deployment of IBM Cloud Pak for AIOps.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Platform** | **IBM Cloud Storage (Block and File)** | **Red Hat® OpenShift® Data Foundation** | **IBM Storage Fusion** | **IBM Spectrum Scale Container Native** | **Portworx** |
| Azure Red Hat OpenShift (ARO) |  | Yes |  |  | Yes |
| Google Cloud Platform (GCP) |  | Yes |  |  | Yes |
| Red Hat OpenShift Container Platform |  | Yes | Yes | Yes | Yes |
| Red Hat OpenShift on IBM Cloud (ROKS) | Yes | Yes |  |  |  |
| Red Hat OpenShift Service on AWS (ROSA) |  |  |  |  | Yes |

### Data Sources in the Scope of POC

|  |  |
| --- | --- |
| Tool / Provider | How to get data |
| APM (Metrics, Topology, Events) | OOTB |
| SolarWinds | Simulate data |
| Grafana | Use as alert webhook |
| ELK/Splunk (Error/Exception/Warning Logs) | Use as alert webhook |