Annex A

Problem Statement, Challenges, Minimal Requirements, and Personas

Note to Bidders: Under Procurement Process 3.0, SCC is piloting an improved model of engagement with the private sector. The goal is to collect supplier feedback throughout the procurement process to quickly refine it when necessary.

Some suppliers have expressed concerns about the photos that represent the personas in Appendix A.

These concerns are legitimate. SSC is fully committed to promoting an environment free from racism, with equality and respect for differences.

Therefore, the photos have been replaced with avatars.

See the modified version below.

APM PROBLEM STATEMENT

SSC wishes to improve their visibility into the availability and performance of the application services currently delivered by SSC, partners and third parties. SSC wants to detect application issues, measure performance, and determine root cause of failures (performance issues/outages/failures) in a consolidated manner.

CHALLENGES:

1. Inconsistent Monitoring: Applications are being monitored in different ways, in different places, or sometimes not at all. There are gaps in coverage: isolated pockets, no common standards, and challenges with application availability. There is no reporting available on an enterprise level without robust capabilities for rolling up data from multiple sources or real-time reporting.

2. Insufficient Monitoring: SSC Partners and service lines are experiencing difficulty in acquiring a solution that can support application availability management, real user experience monitoring, application troubleshooting, and root cause analysis (full-service delivery stack).

3. Baselining: SSC has difficulty determining the baseline behaviour of applications in order to determine deviations from normal to provide reporting and analysis.

4. Proactive Challenges (Short term Impacts): Most IT failures impacting end-users are only discovered and reported by end-users. Traditional monitoring tools

either do not detect issues that impact the application or do not convey the impact on the application.

5. Long term Impacts: Application performance (i.e. response time), user experience, and user behaviour is often difficult to discern. Lacking this information, it is challenging to make informed decisions based on empirical data for the future of the application.

APM MINIMUM VIABLE REQUIREMENTS

DEFINITIONS

Application Components - application code, middleware, and databases, containers, operating systems, servers (virtual and physical), and storage which are required by the application. Application components may be located on-premises or in cloud deployments.

Datacentre components - operating systems, servers (virtual and physical), storage, and networking which are required by the application. Datacentre components may be located on-premises or in cloud deployments.

Trace - a record of a single request to the application as it moves end-to-end through the application components.

Transaction - a well-defined interaction with the application that uses specific application functionality.

Session - data about how the application appeared to the user and how the user interacted with the application over a period of time, such as from logging in until logging out.

Metric – a value, time stamp, and associated metadata. In most cases, a metric is captured at regular intervals.

Log – data in unstructured text format that is created at irregular intervals. Multiple logs may exist for each application and datacentre component.

Event – an asynchronous and time specific structured datum that indicates that something has occurred.

Able to – expression that refers to a functionality or a component of the solution that must be available to be actioned by users.

REQUIREMENTS

The sections below describe the expected minimal performance of the Solution. It describes what the solution must be able to do (functional requirements), how the solution must interact with environment and other devices, (non-functional requirements).

1. The solution must include Application Discovery Tracing and Diagnoses (ADTD):
   ADTD1: ADTD must be able to discover application components and their relationships.

   ADTD2: ADTD must be able to capture traces. A trace must enable deep inspection of the application code and interactions with other application components.

2. The solution must include Synthetic Transaction Monitoring (STM):

STM1: STM must be able to simulate user transactions with the application, including multistep transactions, and capture the result.

STM2: STM must simulate the user device, including execution of an application's web browser based JavaScript code.

STM3: STM must be performed from multiple locations in the network including from within the government of Canada datacentres, internal WAN location, and public WAN (internet) locations. Locations must include on-premises, private cloud, and public cloud.

STM4: STM must be able to simulate transactions against an application's API.

3. The solution must include Real User Monitoring (RUM):
   RUM1: RUM must be able to capture sessions as real users interact with the application.

   RUM2: RUM sessions must capture details of how the application is running in the user's web browser and the web browser's interactions with the datacentre for example: request response times and page render times.

   RUM3: RUM must include session playback, the ability to replay each user action (e.g. click or scroll) as if watching the user's screen.

   RUM4: RUM must NOT require anything on the user's device beyond a JavaScript enabled web browser.

   RUM5: RUM must be compatible with multiple web browsers, minimally Chrome and Safari, multiple user device types, minimally devices running IOS, Android, Windows, Mac, and Linux.

   RUM6: It must be able to select only a subset of sessions to be captured with RUM.

   RUM7: It must be possible to select a subset of RUM sessions to be included in session playback.

4. The solution must include IT Infrastructure Monitoring (ITIM):
   ITIM1: ITIM must be able to discover datacentre components and their relationships.

   ITIM2: ITIM must be able to detect and capture events from datacentre components. For example, service failures, failure of ICMP response, etc.

   ITIM3: ITIM must be able to capture metrics from the datacentre components. For example, CPU load, storage IO rate, etc.

   ITIM4: ITIM must be able to create events when metrics fall outside established thresholds and based on patterns found in logs.

5. The solution must operate with a variety of environments while being easy to deploy, configure, and maintain.
   ENV1: The solution must operate with applications:

- deployed in Government of Canada datacentres, private cloud, and public cloud;
- developed by the Government of Canada (including 3rd-parties), Commercial off the shelf (COTS) products, and Software as a Service (SaaS);
- created with various languages, including Java, C, Python, PHP, MS .Net;
- using various containers, middleware, and databases, at a minimum Docker, Kubernetes, Apache, WebLogic, and Oracle, MS SQL Server.

ENV2: The solution must provide integration with monitoring APIs for Software as a Service (SaaS) based solutions, at a minimum Microsoft Office 365, and cloud vendor monitoring APIs, Amazon Web Services Cloudwatch and Microsoft Azure Monitor.

ENV3: The solution must be able to be deployed to existing applications without changes being required to the application code.

ENV4: The solution must provide 99.9% up-time on a 24/7/365 basis.

ENV5: The solution must be able to deploy upgrades without interfering with operations, including rolling back to prior working state if required.

ENV6: The solution must be capable of scaling to 1,000 applications running on 15,000 servers for applications supporting millions of end users.

ENV 7: The solution must be able to store all data for at least 1 year after it is captured.

6. The solution must be able to analyze and store data, perform anomaly detection, and identify root cause:
AS1: The solution must be able to capture data from ADTD, STM, and ITIM on an ad-hoc and a scheduled basis.

AS2: Anomalies must be detected based on data captured by ADTD, STM, RUM, and ITIM that do not conform to expected behavior patterns.

AS3: Anomalies must include complete failures, partial failures, performance degradation, and trends that may lead to any of the aforementioned.

AS4: Anomalies must include deviations from contracted service level availability and performance thresholds for the application.

AS5: Anomalies must be classified based on severity and impact on the user.

AS6: Related anomalies must be correlated and displayed as a single anomaly.

AS7: The solution must indicate the root cause of an anomaly.

AS8: The root cause must indicate which application component has lead to the anomaly.

AS9: The root cause must indicate if a non-application component has lead to the anomaly, such as a WAN issue, or web browser issue.

AS10: The solution must be able to link data from sessions and transactions with the specific trace(s) that handled the associated requests.

7. The solution must include advanced dashboards, notification, reporting, and APIs to disseminate information:
   DIS1: The solution must provide a dashboard (web based interface). The dashboard must:

   - provide role-based security for application owners, application operators, application developers, IT operators, and service desk staff;
   - be available to at least 1000 concurrent dashboard users;
   - include single-sign-on for all components of the dashboard;
   - be able to display data captured from all components of the solution together;
   - be able to display all data collected by the solution in various forms, minimally tabular, graph, and map;
   - provide a list (tabular information) and map (diagrammatic information) of the relationships between application components;
   - allow data to be sorted and filtered;
   - provide views for application tuning, debugging and diagnostics;
   - provide views of events and anomalies to assist is resolving failures;
   - present baselines from data capture in the past and allow comparison with current performance data.

   DIS2: The solution must be able to send notification of new events and anomalies via, email, SMS, and API.

   DIS3: The solution must be able to direct events and anomalies to only interested users and APIs based on application impacted, root cause, and time of day.

   DIS4: The solution must provide standard out the box reporting and custom reports against all captured data.

   DIS5: The solution must provide comprehensive APIs for configuration, data import, and data export.

   DIS6: Aspects of the solution may require support of both official languages (English and French).

8. Security:
   SEC1: The solution must include remote management and administration through a management interface which provides secure (encrypted) connectivity.

   SEC2: The solution must meet Government of Canada standards for Protected B Data / High Integrity / High Availability

SEC3: the monitoring solution must comply with the defined IT infrastructure security standards.

SEC4: The solution must integrate with enterprise authentication methods, at a minimum Lightweight Directory Access Protocol (LDAP), for user authentication and authorization.

SEC5: The solution must be able to transmit confidential information with adequate protection from malicious attacks and accidental exposure (e.g., cross-contamination) by using the security infrastructure within SSC.

SSC Persona: Enterprise – Service Desk - Phil (Phillip)
Service Desk Representatives collect low level info from clients and applications to initiate actions to resolve IT Issues. They receive an alert from a dashboard, and look at it to determine severity and who it needs to be forwarded to.

Levels: CS1 and CS2

Goals	challenges
• Quickly collecting information and direct failures to the right service lines for resolution. Follow the event management process and support incident management. • Understanding overall view of application availability. • Knowing when something is wrong or working (and say it with confidence) • Wanting to have process well documented – want to follow the process	• Lack of information on what is really going on. Process is slow. • Overwhelmed with data that doesn't provide information. Receiving data from different sources and don't know how the data relates to one another. • Understaffed because of lack of proper tools.
values	fears
• Correct and timely information. • Resolution of immediate, current problems. • Processes they can follow.	• Don't know what is going on
expectations	Measures of success
• That they can see and say they know what is going on with confidence • Number of CIs per staff member to monitor the application – the higher the better.	• If a user calls and something is down, they can say they already know (proactive detection of issues) - the human has nothing new to tell them. • Tool gives them the right service line to contact (because root cause analysis could say the correct tool, dB, … that had the real issue)

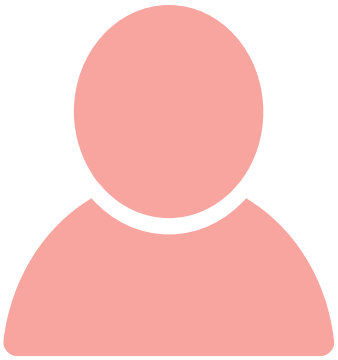
SSC Persona: Service Lines (support) - Zarah

Group that manages servers, dbs. Manages CIs or components on the CIs.

Levels: CS2 to CS4

Goals	challenges
• Keep the lights on (infrastructure running). 99% up time. • Receive accurate information from tool – metrics such as CPU use, how long a db query took. • Help in troubleshooting. • Work on new projects they are supposed to be working on, rather than fixing breaks/issues.	• Told something is wrong by 1st level support, need to analyze and validate that information • Networking personnel frequently get blamed for any issues that arise, despite other root causes
values	fears
• Correct information • No false alarms	• Don't know where to find their issues – even if they know it is their team's issue • Spend too much time fixing breaks
expectations	Measures of success
• Tickets contain correct info and direct attention to what is actually broken • Don't want to be bothered with false alarms	• The data (availability, performance, root cause analysis data) is correct • Information to quickly fix problems • No false alarms

SSC Persona: Account Executives – Ginette



This includes account executives, service delivery managers and account operational managers. We will focus on account executives. Account executives manage interface SSC and partner departments. Voice of customer within SSC. Every account executive does this differently.

Levels : EX1

Goals	challenges
• Customer satisfaction, customer is getting what they need from SSC. What customer satisfaction is varies from department to department. Their roles are as different as the partner departments. • 1)Show that SSC is meeting SLAs. SSC is delivering what is promised. Application up time, response time. • 2)SSC is evolving and improving to be able to do more. Offering better level of sophistication, showcasing roadmap and how SSC is improving.	• Lack of formal service for APM. Do have APM but don't offer as a formal service. • Not understanding what APM is. • Not being able to report on SSC's SLA compliance. Some specific applications have SLAs, in pockets. • Lack of time – responsible for all services. • Lack of being able to get in depth on any one topic.
values	**fears**
• Client satisfaction – happy customer. • Technical people that can back them up. Need SSC to provide timely information, responsive, accurate information, and be timely. Need data explained and	• They say something or commit to something that isn't true or can't be delivered by SSC • The APM will be too expensive to sell to the partners • The APM will make things worse for applications.

packaged for them. More information rather than data. • Consistency – they don't want things to change every week. Consistent clear messaging over time of an APM service. Also, consistency between partners. Consistency across SSC service catalog across all partner departments.	
expectations • APM is bridge between SSC and the client partner in terms of visibility for performance • APM provides impartial hard data on application performance. • Shorter meantime to fix (but this may be too detailed for them) because this underlines the need for APM. • Transform data from APM to provide information (tell me a story – story of how things are getting better). • All applications report for their partner(s) in one view.	Measures of success • We detect application issues extremely early before it impacts users. • Being able to demonstrate they met the SLAs • Improved SSC rating (by partners) – because of more visibility

SSC Persona: Service owners - Raynald

Service Owners manage entire service lines and are responsible for delivery of services.

Levels: CS5 (director level)

Goals	challenges
• To receive concise new data that is actionable • To understand how their service line is negatively impacting or positively supporting applications.	• Applications are a small part of what they do. They don't have as much time for application issues.
values	**fears**
• Care more about their own services	• They are missing something. Too much on their plate • Phone call at 3 am – will get pulled out of bed if they have to delegate.
expectations	**Measures of success**
• Low noise (don't show irrelevant information) • All information needs to be actioned by them • Provides data to support long term planning – ie capacity planning for life cycling	• No one is telling them something is wrong – not blaming them for an outage • Proactive – service line spends less time "firefighting" (reacting to breaks and issues) • Report showcasing SLAs have been met

Attachment 1

BID QUALIFICATION FORM

Provided as a separate document