IBM GTS SPGI
Containers as a Service

Some Questions & Answers

Table of Contents

INTRODUCTION 1
QUESTIONS & ANSWERS 1
MANAGEMENT 1
WHAT ARE THE COMPONENTS USED FOR MONITORING? 1
IS THIS KIND OF MONITORING INTEGRATED WITH EXISTING IBM GSMA-BASED SOLUTIONS? 2
WHAT KIND OF ACCESS TO MONITORING DOES THE CLIENT HAVE? 2
WHAT ABOUT BACKUPS? WHAT IS THE BACKUP APPROACH FOR THE CONTAINERS? 2
ARE THE CONTAINERS SUBJECT TO ANY KIND OF COMPLIANCE ANALYSIS AND REPORTING? 3
BUT ARE THE CONTAINERS MANAGED? 3
WHAT KIND OF ACCESS TO LOGS IS PROVIDED? 4
SERVICE 4
ARE THERE NON-IBM PARTNERS INVOLVED IN DIFFERENT ASPECTS OF THE OFFERING? 4
IN WHAT ACCOUNTS IS THE OFFERING CURRENTLY BEING USED? 4
WHAT ABOUT INCIDENTS? WHAT IS THE STANDARD POLICY? 5
HOW IS INFORMATION ON THE OVERALL STATUS OF THE PLATFORM PRESENTED? 5
ARE SLAS MEASURED? HOW? 5
WHAT IS THE INCIDENTS AND CHANGE REQUEST PROCESS? 5
ADDITIONAL SERVICES 5
IS MIGRATION ANALYSIS A PART OF THE OFFERING? 5
IS THIS ANALYSIS ARTICULATED WITH OTHER UNITS (E.G. CLOUD, GBS)? . 6
CAAS AND CLOUD OFFERINGS 6
WHAT IS THE RELATION WITH ICP, AND CAN IT BE USED WHEN CONSIDERING CAAS? 6
IS THE KUBERNETES OFFERING IN IBM CLOUD ALSO SUPPORTED? 6
WAS ANY CAAS SOLUTION INCLUDED IN A DEAL WHICH UNDERWENT SIH REVISION? 6
DEVOPS 6
IS INTEGRATION WITH A CLIENT-OWNED DEVELOPMENT PIPELINE 7

SUPPORTED?
WHAT ARE THE LIMITS OF THE CAAS TEAM INTERVENTION IN TERMS OF THE APPLICATION DEVELOPMENT AND DEPLOYMENT PROCESS? 7
COSTING AND PRICING 7
IS THERE INFORMATION FOR THE TSMS IN TERMS OF COSTING? 7
IS THERE A RESPONSABILITY MATRIX OR SERVICE DESCRIPTION THAT QUICKLY IDENTIFIES THE SCOPE? 7
WHAT ARE THE KEY PRICE DRIVERS IN THE OFFERING? 7
ARE THERE DIFFERENT SERVICE TIERS? 8
ARE THERE MINIMUM REQUIREMENTS FOR AN INITIAL SETUP? 8
IS THERE A BOARDING PROCESS ALREADY TYPIFIED? 8
NON-FUNCTIONAL REQUIREMENTS 9
WHAT IS THE OVERALL DR APPROACH? 9
IS BUSINESS CONTINUITIY POSSIBLE AND/OR INTEGRATED INTO THE DESIGN? 9
ARE THERE HIGH-AVAILABILITY BLUEPRINTS/REQUIREMENTS/TOPOLOGIES THAT SHOULD BE USED FOR DIFFERENT SLAS? 9
ADDITIONAL DOUBTS 9
REMARKS ON THE SITUATION IN PORTUGAL 10

Introduction

This document was made in preparation of the on-site visit regarding the Containers as a Service (CaaS) offering developed by the Spanish colleagues and contained high-level highlights of the kind of doubts and questions that the Portuguese team had at the moment; not having an intimate knowledge of the solution it is likely that not all of them were apropriate but they were a reference to help the information sharing process.

The local team has read some of the more public information made available and explored the environment itself, so some of the questions and doubts below are not completely new, but they were kept here as a reference and to avoid incorrect assumptions.

After the visit the content was reviewed and the clarifications included, which resulted in a more "Q&A" style throughout.

Questions & Answers

Management

What are the components used for monitoring?

The Management Infrastructure is monitored using a set of tools which were chosen specifically for this solution and which are not the same as the usual IBM stack used in Strategic Outsourcing (SO); it currently uses Sensu and integrates with the overall workflow of the CaaS team.

As for the client containers themselves, monitoring them is increasingly the realm of the development teams given that monitoring is becoming strongly coupled with the applications themselves, which are instrumented with specific collections points and use specific libraries that are determined by the technological context of the application being developed. As such the monitoring of what runs inside the container is determined by what is defined in the container definition itself.

Is this kind of monitoring integrated with existing IBM GSMA-based solutions?

The solution is perfectly able to be integrated: it can send events to a REST endpoint. Including and normalising this events is something that should be done by the SMI team of the appropriate account should it be necessary.

What kind of access to monitoring does the client have?

The client is given access to all the dashboards that exist in the clusters: Kubernetes, Logstash, Fluentd, Elastic, Kibana, to name a few. Additionally most of the solutions have usable APIs that can be used.

What about backups? What is the backup approach for the containers?

Backups in a container environment are necessarily different since the containers themselves are largely read-only (and data generated is transient): they do not need to be backed up since they have no intrinsic state.

There are however situations where this isn't applicable, for example:

- Database servers which need to store data
- File-based sharing of persistent information

In this situations the backup solution is essentially to use whatever product is considered the standard**|—|**which for IBM SO customers is generally TSM and in some cases NAS storage like Netapp**|—|**when the deployment is on client premisses: in this situation NFS is used and backups can target the NFS mount.

When the deployment in in the cloud Duplicati can be used, targeting object storage.

For databases it is necessary to consider some scripting to stop/dump/start (or similar mechanism), and the results backed up to whatever solution is used.

Are the containers subject to any kind of compliance analysis and reporting?

In general, security compliance is currently focused on:

Primary Controls

- Base layer should be reviewed and approved;
- Additionals in the Dockerfile supervised by security team;

Secondary Controls

- Vulnerability scanning

In terms of the CaaS offering it should be noted that the responsability of the container is primarily of the client development team, and thus the role of reviewing the git commits for compliance is a role that is also retained by the client. Secondary controls are in this case something which, if necessary, should be done with specific tools (e.g. Aqua, IBM Vulnerability Advisor) that are acquired seperately.

Containers that are used by IBM should follow the same existing ISEC policies that are applied to VMs, within reason: there are many settings which do not make sense in a container context and trying to apply them is simply not sensible or possible.

But are the containers managed?

Talking about management of containers is a complex topic because managing containers is not the same as managing VMs: containers are recreated and modified and transient modifications are lost, and do not (as a rule) provide interactive access. As such the containers are built from "recipes" which are the main focus of changes.

As such the standard offering doesn’t include management of containers; the Advanced Services offering does include management of custumer application components in containers, something that could be used in situations were IBM is already managing the servers (as is the case in SO).

What kind of access to logs is provided?

The customer has access to all the output (stderr/stdout) of the containers via his access to Elastic (where fluentd sends the output); additionally application logs are covered by filebeat and logstash for integration into the client SIEM solution (or to Elastic).

Depending on the specific tools and processes used other approaches are possible and this analysis is part of the value proposition of the CaaS offering: An example of split logging shows one particular solution that allows for the distribution of logging information to two different aggregating platforms.

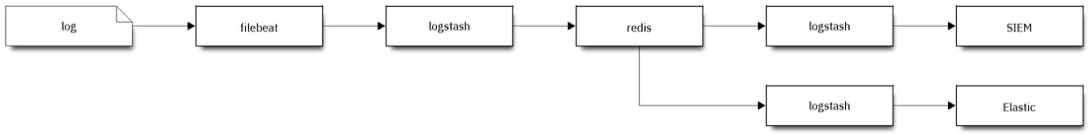

Figure 1. An example of split logging

Service

Are there non-IBM partners involved in different aspects of the offering?

Not at the present, but there are certainly opportunities for it. Work with GBS in terms of application modernisation is important since it is generally what drives the push to containers and thus make CaaS relevant. Additionally other companies have been partnering with IBM at an IBM Cloud level|—|New Relic, for example|—|and could be useful in this offering as well.

In what accounts is the offering currently being used?

The following are public references:

- Correos Express: more than 1400 daily users.
- Banco Sabadel: ~400 containers.

Additionaly the offering is also present in:

- Bankinter
- CaixaBank

What about incidents? What is the standard policy?

Emergency incidents have a 24x7 scope.

How is information on the overall status of the platform presented?

The client has acess to all the dashboards, which include Grafana for displaying the aggregated data that is collected; work is under way to also provide a simpler status page, based on Cachet, that conveys the main status indicators directly.

Are SLAs measured? How?

Yes, they are. Executions blocks and central management availability is measured and reports available via Sensu. Incident reply time is measured via the client IPC tools.

What is the incidents and change request process?

The CaaS team uses dedicated tools to manage requests, and in general terms should be considered as a third-party in terms of integration with existing accounts: a swivel-chair approach is adopted and the incidents that are opened in the customer IPC tool are duplicated in the CaaS tools. This allows the CaaS team to use Agile methods in terms of tracking and resolution and avoids focusing on integrating with a multitude of IPC tools and processes which would require a lot of work and fall outside the scope of the CaaS team value proposition.

Additional services

Is migration analysis a part of the offering?

There is an assessment ability that can focus on that and which is currently made on a per-project basis**|—|**but plans are under way to package it as a service with a more standard billing.

Is this analysis articulated with other units (e.g. Cloud, GBS)?

The CaaS team has the know-how to tackle it by itself and as done so in several projects, but there is no obstacle in working with other units. As mentioned GBS has an important role in application modernisation.

CaaS and Cloud offerings

What is the relation with ICP, and can it be used when considering CaaS?

IBM Cloud Private is one of the solutions that CaaS can use when considering a private deployment; whenever there is value in presenting ICP as the container platform in a customer (due to some of the differentiators it has) CaaS can be presented as the managed services part of the global value proposition, adding management and workflow integration to what would be otherwise be left to be done by the client or the IBM delivery teams.

Is the Kubernetes offering in IBM Cloud also supported?

Yes: in fact the IBM Cloud Container Service (ICCS) is the preferred container service for public deployments.

Was any CaaS solution included in a deal which underwent SIH revision?

Yes, it’s an ongoing process. We are aware that the current guidelines around the usage of ICP with IMI services can appear as a limitation to the adoption of CaaS but we’re working with the European organisation at several levels and the CaaS offering is positioning itself to be offered as a standard offering. That said it is perfectly possible to use CaaS today since the scope of requirements make it something that is not identical to what the ICP+IMI solution offers.

DevOps

Is integration with a client-owned development pipeline supported?

Not only supported, that integration is an absolutely critical aspect of the CaaS offering and a key differentiator. The CaaS team has experience in integrating existing DevOps workflows and also in proposing them when the maturity level is lower.

The CaaS offering also includes standartised deployment pipelines and a streamlined approach to common doubts and problems that arise when trying to integrate existing workflows, providing clear guidance based on its experience.

What are the limits of the CaaS team intervention in terms of the application development and deployment process?

While the CaaS team does not do applicational development we naturally participate in the DevOps workflow and works with the client to build, deploy and manage the applications that run on the CaaS platform.

Costing and pricing

Is there information for the TSMs in terms of costing?

Yes: there is an SDM model which is fully documented.

Is there a responsability matrix or service description that quickly identifies the scope?

Yes: we have prepared documentation that includes Statement of Work and other information that can be used as annexes in existing contracts.

What are the key price drivers in the offering?

The main platform baselines are:

- CaaS customer tenant
- Execution blocks

The execution blocks can additionally be extended in terms of RAM blocks.

The management services depend on the service tiers.

Are there different service tiers?

Yes:

- **Basic**: the base offering, includes the Execution Blocks and the Management Services.
- **Advanced**: adds additional management for application components deployed by costumers in the containers.
- **Integrated basic**: As above, but the scope is wider in that it CaaS responds to requests and incidents that affect application components running as containers.
- **Integrated advanced**: As above, but with the additional scope.

The difference between Basic and Advanced is in terms of the additional management of the applications running inside the containers, whereas the difference between Integrated and non-Integrated is the integration with customer IPC tools and procedures.

Are there minimum requirements for an initial setup?

The solution has very modest minimum requirements: two network ranges plus:

- *If Public*: an independent account (for security reasons).
- *If Private*: the minimum components necessary for the Execution Block (hardware, firewall, etc).

Is there a boarding process already typified?

More than a boarding process, the CaaS offering includes an end-to-end solution that starts with a workshop, includes a (paid) PoC and a process to get the client up and running (and *using* the platform).

Non-functional requirements

What is the overall DR approach?

The solution doesn't impose a DR approach and in general such approaches are determined by the application itself; that said CaaS is based on a modular architecture designed with a *share nothing* principle and this makes it possible to add a different clusters in different sites.

Is Business Continuitiy possible and/or integrated into the design?

Yes, depending on application design and the ability to leverage different datacentres. This is essentially defined by the application development team but the CaaS team has the necessary knowledge to advice in general terms.

Are there high-availability blueprints/requirements/topologies that should be used for different SLAs?

Aligned with applications and their best practices. We can offer to help in designing the application, case by case - we participate in that process as a consequence of our DevOps alignment and Agile methodology.

Additional doubts

The following are doubts which arised when preparing this document and after some additional reflection:

1. Is there some additional information around the vaulting/tokens solution that was mentioned?
2. The overall "release management" workflow was debated but we have forgotten some of the information; is there a document which shows the different steps, validation points, responsibles, etc, that a deployment takes from being developed to being finally deployed in Production?
3. It was mentioned that a new Resource Unit was being thought about to cover DB/MW: is this what is referred as Advanced Services or is it something different?

4. In general are those Advanced Services similar to what would be using the Basic ones and adding SO services to the containers (to the extent it is applicable)? The description of containers being "unmanaged" (which we used for debating security, for example) seems to run counter to the scope of services in thre Advanced Services which would seem to include "management" of what is inside the containers, thus triggering the compliance responsibility.
5. The issues around security are the ones in which we have more doubts/opinions.
    - Some are around the need to somehow go a bit deeper in terms of mapping currently provided compliance checking by IBM to containers.
    - Others are related to the mutability vs. imutability and what this means in terms of impacts and security risks.
6. Have you considered using all the framework that was developed to provide a non-container based option (as an add-on, not a replacement) that would essentially build VMs for those cases where containers are not feasible? I'm thinking of the advantages of leveraging all the existing experience in integrating with CD/CI, the Execution Blocks, etc, but instead of containers trigger the deployment of a VM. This is obviously more complex than this but the idea came to mind.

Remarks on the situation in Portugal

We have been exploring in different clients ways to improve the agility of delivery, reduce the time to deploy new infrastructure in reply to RFSs and align with new approaches (and skill sets) based on DevOps and Agile. We have experimented with different solutions and

- We use Github and Travis for workflow management and solution design, including the production of architectural documentation;
- We use Zenhub for project management in terms of Solution Design and project;
- We have made some PoCs around using a Continuous Deployment pipeline to automatically deploy virtualised resources or public cloud resources.

In terms of customers, the following are some of the largest in Portugal:

- **Millenium BCP**: strong Microsoft culture, reflected in the application and system choice. Currently exploring Azure and IBM is involved in a project to manage workloads in that platform. A ICP PoC is being proposed and deployed.
- **Caixa Geral de Depósitos**: currently being renegotiated, current scope is Unix but proposal includes adding distributed (including Linux and Windows).
- **Banco BPI**: strong Agile culture, we had a PoC (*Project Janus*) around Infrastructure-as-Code and deployment of VMs using Packer, Terraform and others. Recently acquired by Caixabank and the architectural governance is thus with ITnow. Large Linux based, but it's Oracle Linux.
- **Novo Banco**: a PoC of IPC is underway since there was a real opportunity, via an RFS, to deploy an application that was containerised. Large Linux base.

.