Shared Services Canada

Cloud Product Management and Services

Cloud Discovery & Migration Readiness Process

Version Draft

GCDOCS <# 68861147>

2021-08-17

Revision History

| Version Number | Description | Date Modified | Author |
| --- | --- | --- | --- |
| 1.0 | Original Version | 2021-08-17 | TBS OCIO/SSC CPMS |
|  |  |  |  |

Table of Contents

[1 Purpose 1](#_Toc80103402)

[1.1 What Are Discovery and Migration Services? 1](#_Toc80103403)

[1.2 High-Level Architecture 2](#_Toc80103404)

[2 Application Discovery Readiness Process Overview 3](#_Toc80103405)

[2.1 Obtain Cloud Account 4](#_Toc80103406)

[2.2 Apply Guardrails 4](#_Toc80103407)

[2.3 Obtain Cloud Discovery Service ATO 5](#_Toc80103408)

[2.4 Discovery Readiness 5](#_Toc80103409)

[2.4.1 Request COM Application Discovery Service 5](#_Toc80103410)

[2.5 Deploy Cloud Discovery Service 5](#_Toc80103411)

[2.5.1 Provision Discovery Service 5](#_Toc80103412)

[2.5.2 Configure API Endpoints 6](#_Toc80103413)

[2.6 Run Discovery and Analysis 6](#_Toc80103414)

[3 Application Migration Readiness Process Overview 6](#_Toc80103415)

[3.1 Obtain Cloud Platform ATO 7](#_Toc80103416)

[3.2 Migration Readiness 8](#_Toc80103417)

[3.2.1 Formal WLM Engagement 8](#_Toc80103418)

[3.2.2 Request COM Cloud Migration Service Request 8](#_Toc80103419)

[3.3 Deploy Cloud Migration Service 8](#_Toc80103420)

[3.4 Execute Migrations 8](#_Toc80103421)

[Appendix A – Acronyms and Glossary 9](#_Toc80103422)

[List of Acronyms 10](#_Toc80103423)

# Purpose

Departments want better information on their current application portfolio, their architecture, and hosting costs before deciding what applications to migrate to public cloud services. Similarly, when departments have decided to proceed with migration, they seek automation to make the process as frictionless as possible.

Hyperscale I/PaaS providers typically provide include application discovery & migration services as part of their service offerings. How each provider implements these services may differ, but the outcome is the same; provide data to inform migration decisions and automate migration activities. These services are hybrid IT services as they span both the public cloud and data centre services.

This guide is meant to describe the readiness activities departments must undertake before deploying cloud-based discovery and migration services. It is not meant to be a comprehensive application migration guide. Discovery and migration services are described in a generic way and is not provider specific. This guide represents one piece of a larger migration puzzle.

## What Are Discovery and Migration Services?

All major P/IaaS hyperscale cloud providers offer services for discovering your current application deployment. Data collected includes, but not limited to:

* Technology stacks; software, versions, libraries
* Resource usage; storage and compute
* Dependencies; which applications communicate with other applications

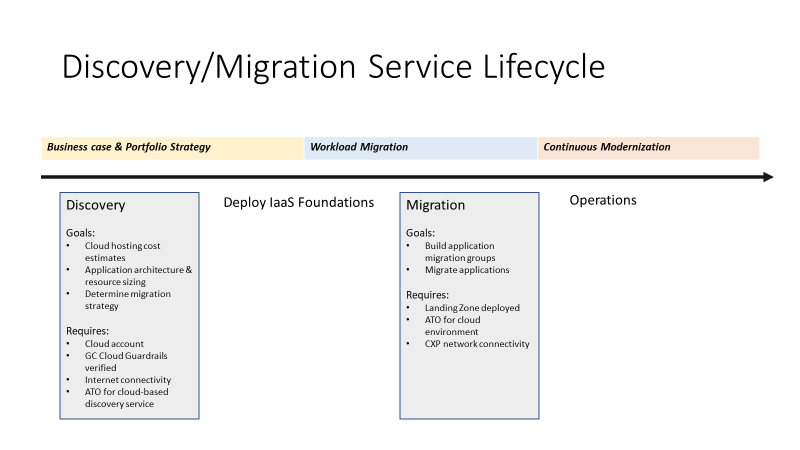
The collected data can be used to provide:

* Cloud hosting cost estimate
* Resource optimization recommendations
* Application groupings
* Security recommendations

The discovery services collect and analyze data about your current application portfolio. Migration services are used when an organization is ready to migrate applications to the cloud. The decisions made during the discovery phase help inform migration decisions such as:

* What portion of the application portfolio will migrate to cloud, which will not?
* Level of resource optimization required
* Technology stacks that may be difficult to migrate or require refactoring
* Migration groups comprised of applications grouped with a dimension of affinity
* Security attributes and mapping network architecture to a cloud landing zone

Migration services, again, rely of the deployment of the same/similar soft appliance with access to VMWare APIs. The migration service, typically, allows migration groups to be created and will execute on those migration groups.



1. Discover and Migration Service Lifecycle

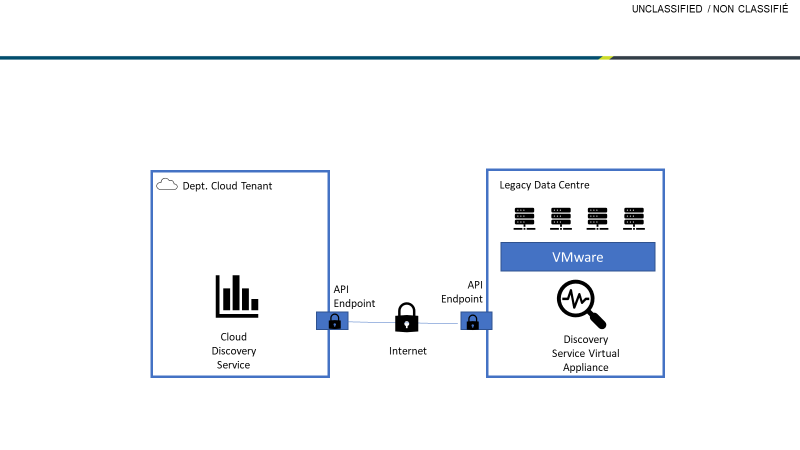
From a high-level view, discovery services can be used to inform the business case & application portfolio strategy. IF the decision is made to proceed with a migration of applications ot the cloud and the organization does not already have foundational elements such as a landing zone deployed or connectivity to the cloud exchange point (CXP), the department will proceed with those foundational pieces.

Once the department has formally started a workload migration project with SSC, they can proceed with application migration services.

Finally, once workloads are migrated to the cloud, the department begins cloud operations and the process of continuous modernization of the application portfolio. The migration to cloud rarely provides adequate time to modernize the application portfolio. The migration to cloud should be viewed as the beginning of a continuously modernization, but the cloud provides more modernization options to departments.

## High-Level Architecture

While the exact implementation of cloud-based discovery service differs from one provider to the next, generally, these are considered hybrid IT because as virtual appliance is deployed in the data centre and given access to VMWare APIs that collects data and sends that data to the cloud for processing and analysis. Because these services interact with VMWare, the scope of visibility is limited to virtualized workloads. Other, non-virtualized workloads, will require a different strategy.



1. Generic Cloud-based Discovery Service Architecture

Typically, the discovery service itself and the data collected is stored within a department’s cloud tenant. Communication between the service and the virtual appliance is through secure API endpoints. Encrypted communication can be over the internet or using dedicated connectivity. For discovery, it is recommended the internet be used. For migration, dedicated connectivity is recommended as to not saturate internet gateways.

# Application Discovery Readiness Process Overview

The deployment of a cloud discovery service requires the co-operation between SSC Cloud Operating Model and the department requesting the service. The deployment is further supported by the Canadian Centre for Cyber Security (CCCS) and Treasury Board of Canada Secretariat (TBS). Figure 3 below provides a high-level overview of the activities leading to readiness to deploy the service.



1. Application Discovery Service Readiness - Summary of Responsibilities

## Obtain Cloud Account

The department submits a request to obtain a cloud account for IaaS/PaaS cloud services with a GC-approved Cloud Service Provider (CSP) via the [GC Cloud Broker](https://cloud-broker.canada.ca/). Each client has been assigned two “designated users”, appointed by the departmental CIO, who has access to the request portal and can make requests on behalf of that client.

Departments can request a range of IP addresses to be assigned to them, as per SSC [Cloud IPAM Strategy](https://gccollab.ca/file/view/3690502/encloud-internet-protocol-address-management-cloud-ipamfrgestion-des-adresses-de-protocole-internet-dans-le-cloud-cloud-ipam). It is critical that departments integrate the IP Addresses provided into their future designs as this will facilitate network routing between their cloud environment and GC networks.

## Apply Guardrails

As per the Cloud PB Operationalization Framework, departments and agencies who are in-scope of the [Policy on Service and Digital](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603), must implement the enterprise-wide mandatory, minimum, initial 30-day [GC Cloud Guardrails](https://github.com/canada-ca/cloud-guardrails).

The guardrails are a subset of the recommended baseline controls for cloud, in accordance with the [Direction on the Secure Use of Commercial Cloud Services: SPIN 2017-02](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html) and the [GC Security Control Profile for Cloud-based GC Solutions for Protected B, Medium Integrity, Medium Availability (PBMM)](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html).

The guardrails should be applied based on [cloud usage profiles](https://www.gcpedia.gc.ca/gcwiki/images/8/84/GC_Cloud_Guardrails.pdf). Where possible, GC approved templates (i.e. GC Accelerators) should be leveraged. Using the GC Accelerators will aid in deploying Infrastructure as Code (IaC) which incorporates required technical guardrails.

Verification that the guardrails have been implemented is conducted by SSC Cloud Operations. Tools to support automated compliance checks are available in the github repositories referenced above.

Specifically for Guardrail 8, [*Segment and Separate*](https://github.com/canada-ca/cloud-guardrails/blob/master/EN/08_Segmentation.md), a firewall must be selected that has Virtual Private Network (VPN) capabilities including encryption algorithms compliant with the [*GC Encryption Standards*](https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111). Having a firewall or Unified Threat Management (UTM) device with this capability is a prerequisite for connectivity to the SSC Secure Cloud-to-Ground Service (GC TIP and GC CAP). Several offerings which satisfy this requirement can be found in the GC Cloud Marketplace.

To satisfy this requirement, clients must first procure licences through existing GC contracting vehicles. Next, a “Bring your own licence (BYOL)” request must be sent to the GC Cloud Brokering Service for licence activation in the public cloud tenancy. Clients will be asked to provide information on the contracting vehicle they used to procure the licences. For more information on BYOL, please contact ssc.cloud-infonuagique.spc@canada.ca.

## Obtain Cloud Discovery Service ATO

Departments are expected to continue to apply graduated safeguards that are commensurate with the risks to their information and IT assets, with more rigorous safeguards as asset values, service delivery requirements, and threats to confidentiality, availability or integrity increase.

This assessment must be signed-off by the appropriate authorities within the organization

Template assessment material can be found here based upon the Statistics Canada security assessment of Azure Migrate.

The department is expected to assess the cloud discovery service and the controls/configuration the department puts in place to safeguard the data collected and analyzed by the discovery service.

The cloud-based discovery service should be assessed by CCCS. If not, the department will be required to accept that risk and deepen its security assessment activities.

## Discovery Readiness

This activity requires that the appropriate agreements are signed and API endpoint flow details are provided.

### Request COM Application Discovery Service

Go to the cloud brokering portal and enter a application discovery service request???

## Deploy Cloud Discovery Service

At this point hybrid deployment of the service will start, or if there is insufficient capacity to perform capacity, you will be prioritized and scheduled discovery onboarding.

### Provision Discovery Service

Form your cloud management console or API calls, provision the discovery service if you have not already done so. Details on provisioning the service can be found from your respective provider.

### Configure API Endpoints

Working with SSC, configure the API endpoints to communicate with the virtual appliance deployed in the data centre.

## Run Discovery and Analysis

At this point, you should start receiving data about your current application portfolio, resource usage, and application affinities.

This data will allow for a full discovery of the technology stack currently deployed and make decisions regarding your migration strategy.

Similarly, the collected data will support cloud hosting costs and optimization decisions.

# Application Migration Readiness Process Overview

Like the deployment of the discovery service, the deployment of a cloud migration service requires readiness activities. Depending upon the provider, the service may be the same as the discovery service or may be a different service, but similar architecture.

At this point, it is assumed that the department has made migration decisions regarding its portfolio, cost analysis, engaged with the Workload Migration (WLM) project, and deployed foundational cloud pieces such as a landing zone and dedicated connectivity.



1. Application Migration Service Readiness - Summary of Responsibilities

## Obtain Cloud Platform ATO

Departments are expected to continue to apply graduated safeguards that are commensurate with the risks to their information and IT assets, with more rigorous safeguards as asset values, service delivery requirements, and threats to confidentiality, availability or integrity increase.

An initial starting point for the security controls for the cloud platform layer (your cloud environment), as a subset of the GC Cloud PBMM profile, will be made available to departments:

* For Azure, the starting point is made available via the [Canada PBMM Blueprint](https://azure.microsoft.com/en-ca/updates/new-canada-federal-pbmm-azure-blueprint-is-now-available/).
* For AWS, the ***Landing Zone*** is pre-configured by the vendor for all GC clients.

An iterative approach to designing, building, and assessing your cloud environment is expected. As part of this systems engineering activities, evidence will be generated to provide assurance for the implementation of the controls.

Performing a Security Assessment and Authorization (SA&A) of the cloud platform will facilitate a security inheritance model that can be leveraged by future information system deployments. This assessment must be signed-off by the appropriate authorities within the organization.

Treasury Board Secretariat has made some of their Azure [security assessment documentation](https://gccode.ssc-spc.gc.ca/GCCloudEnablement/Microsoft/tree/master/TBS%20Cloud%20Environment) available for other departments to leverage.

## Migration Readiness

This activity requires that the pre-requisite activities have been completed.

### Formal WLM Engagement

It is assumed that your department or data centre is in scope of the workload migration project. This engagement will ensure the governance is in place to escalate issues and gain SSC support for migrations.

### Request COM Cloud Migration Service Request

Go to the cloud brokering portal and enter a application migration service request???

## Deploy Cloud Migration Service

At this the deployment of the migration service will start, or if the migration service is the same as the discovery service, no additional activities may be required. It is highly recommended that for migration API-endpoints are routed through dedicated connectivity between GC WAN and the cloud provider instead of the internet.

## Execute Migrations

Using the migration groups created, test migrations can begin.

# Appendix A – Acronyms and Glossary

**Glossary**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| CXP | Cloud eXchange Providers are 3rd-party WAN-hosting companies that provide cost-effective, dedicated, low latency, high-bandwidth connectivity to multiple/simultaneous Cloud Service Providers (CSPs). |
| IaaS | Infrastructure as a Service: cloud-based services such as storage, networking, and virtualization. |
| PaaS | Platform as a Service: hardware and software tools available over the internet allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. |
| Private Cloud | The private cloud is defined as computing services offered either over the Internet or a private internal network and only to select users instead of the general public. Private cloud can be deployed “on premise” in a data centre behind a firewall. |
| Public Cloud | The public cloud is defined as computing services offered by third-party providers over the public Internet, making them available to anyone who wants to use or purchase them. |
| SaaS | Software as a Service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. SaaS applications are also known as “Web-based” software, “on-demand” software and “hosted” software. |

## List of Acronyms

| Acronym | Full Name |
| --- | --- |
| CCNE | Cloud and Computing Network of Expertise |
| CSP | Cloud Service Provider |
| CXP | Cloud eXchange Provider |
| GC EARB | Government of Canada Enterprise Architecture Review Board |
| IaC | Infrastructure as Code |
| PaaS | Platform as a Service |
| IaaS | Infrastructure as a Service |
| SaaS | Software as a Service |
| SA&A | Security Assessment and Authorization |