Amazon Connect and Data Residency

Background:

In May 2020, a department requested Treasury Board of Canada Secretariat Chief Information Officer Branch provide details on how the GC's data residency policy would be applied to the Amazon Connect service.

This document is an overview of those details. This document is not a replacement for the CIO's responsibility set out in the Directive on Service and Digital to exercise his or her discretion when evaluating data residency.

Architecture of Amazon Connect:

Amazon Connect is a cloud-based call centre service. AWS has shared with the department, under a non-disclosure agreement, the roadmap for making Amazon Connect available in the Canadian region. This section will discuss the architecture of Amazon Connect with a focus on where data is stored and processed and when. AWS has provided architectural details regarding Amazon Connect's architecture through a non-disclosure agreement and are not provided in this document. Voice calls can be recorded using Amazon Connect. All recordings and data are stored in AWS' object storage services known as S3[1]. The S3 storage services is regionalized. This means all storage of customer content can be stored in the Canadian region. It is important to note that the customer must provide this configuration. It is the customer's responsibility to choose the region for storage.

While customer data can be stored in a Canadian region, it is important to note that the Amazon Connect service, located outside of Canada, must keep meta-data locally where the service itself is located (outside of Canada). This meta-data includes call start and end time stamps, and configuration settings (workflows, routings, user access, etc..). At the time of writing this analysis, there is no ability to store meta-data in Canada.

Policy Reference:

Requirement 4.4.1.10 of the Directive on Service and Digital states the following requirement for departmental Chief Information Officers:

"Ensuring computing facilities located within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad, such as a diplomatic or consular mission, be identified and evaluated as a principal delivery option for all sensitive electronic information and data under government control that has been categorized as Protected B, Protected C or is Classified."

[1] Data Security with Amazon Connect, 2017 (obtained under a Non-Disclosure Agreement)

- It is important to note that the evaluation of residency is a CIO's decision, however Canada is the principal delivery option.
- The policy statement only applies to Protected B data and up.

Requirement 4.4.1.9.1 of the Directive on Service and Digital also states that departmental CIOs must evaluate cloud as the principle delivery option.

"Supporting the use of cloud services first by ensuring they are:

Identified and evaluated as a principal delivery option when initiating new departmental, enterprise, and community of interest cluster IT investments, initiatives, strategies and projects;"

Guidance Reference:

At the time of writing this analysis, the Guideline for the Policy on Service and Digital was in draft, however it still provides additional information, including how the departmental CIO should evaluate if it is appropriate for data to be hosted outside of Canada.

The policy statement is focused on where data is stored. Information in transit outside of Canada is not restricted by policy. Whether the data is at rest or in transit, that data should have the appropriate safeguards in place.

The evaluation criteria a CIO should use when evaluating the residency of data at rest includes:

- Reputation: Will the decision locate data outside of Canada likely cause injury to the Government of Canada's reputation?
- Legal or contractual: Are there legal or contractual restrictions on where the data in question is located?
- Market availability: Is the service only available outside of Canada?
- Business value: Does the business value gained outweigh the perceived risks of hosting the data outside of Canada?
- Technical capability: Do technical capabilities exist that reduce the perceived risks of hosting the data outside of Canada?

Overview of Details Provided to the Department

The architecture of Amazon Connect allows customer data, the data that is most likely to be considered Protected B, to be stored in Canada even though the data does flow through and is processed in the US. Meta-data, which is less likely to be information categorized as Protected B, is stored in the US.

Amazon connect is a cloud-based service. Choosing a cloud-based service is aligned to the cloud first policy requirement.

The preferred solution would be to host Amazon Connect in a Canadian Region. AWS has committed to make Amazon Connect available in Canada in the future. That commitment provides a roadmap to a preferred solution.

The current, US-only, solution can be viewed as technically meeting the policy requirement, however, it is recommended that departmental CIOs confirm:

1. Customer data, such as call recordings, are configured to be stored in a Canadian region and do not remain stored in a US region. The categorization of that data should also be confirmed.
2. Categorize the meta-data that is stored outside of Canada. Even if the meta-data is found to be Protected B, this does not prohibit the data to remain outside of Canada, but the departmental CIO should be informed as to its categorization before making that decision.
3. While Amazon Connect meets the residency requirements, the departmental CIO should still weigh the evaluation criteria such as the possibility of reputational damage. While the service may not store Protected B data outside of Canada, the service is located outside of Canada. Does the departmental CIO view this as a low risk scenario? Given the protections in place, ability to store data outside of Canada, and the business value provided, it is likely to be viewed as low risk, but the departmental CIO must make that final decision.

Scott Levac
Director of Cloud Oversight and Core Technologies
Office of the Chief Information Officer
Treasury Board of Canada Secretariat