SECURITY, PRIVACY AND RELIABILITY GUIDE

CLOUD-A

LAST UPDATED 10.15.2015

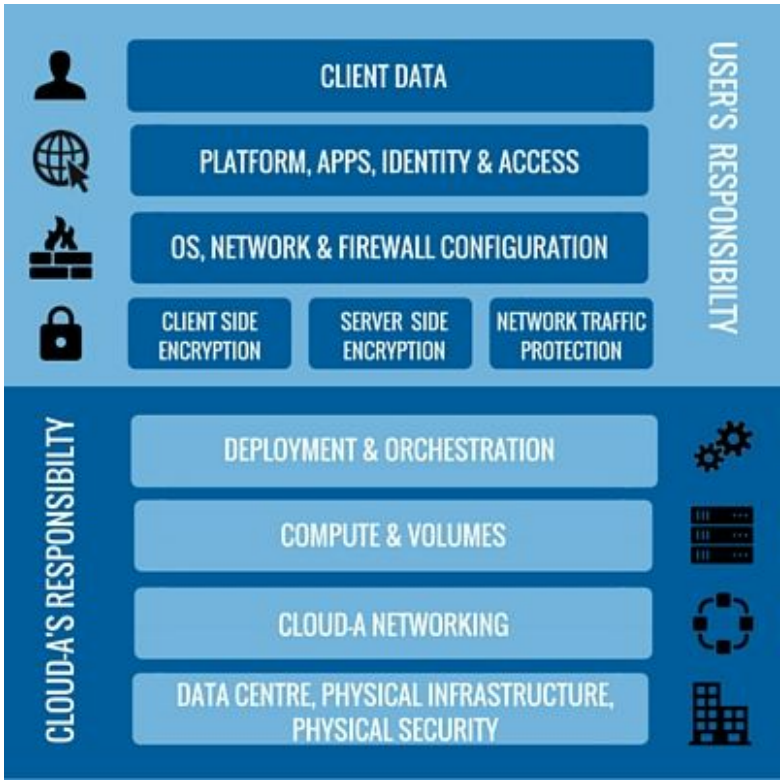
Introduction

An important thing to consider when using any cloud product with personal information is that the organization who transfers the personal information to the 3rd party (cloud provider) remains accountable for that data. It is the responsibility of the data transferring organization to perform due diligence to ensure that they are comfortable with the security and redundancy of the cloud provider's platform. This process in itself becomes a partnership between the data transferring organization and the cloud provider.

Partnering with Cloud-A for Private Data Security

Cloud-A prides ourself on enabling our users to offer high performing, highly secure, Canadian resident solutions. In addition to maintaining bulletproof infrastructure, we work closely with our users and provide them with the tools to ensure that their cloud infrastructure is secure.

It is imperative that Cloud-A user's take accountability and responsibility for securing their own data in the cloud. This starts with understanding the **Cloud-A Security Partnership Model** (Below.)



We understand that not every organization has the internal technical resources to implement policies, procedures and best practises for securing private data, so we have partnered with Lyrical Security, a Toronto based security services provider who offers a wide range of security products and services to secure your Cloud-A tenant environments.

Cloud-A has partnered with Lyrical security to offer Cloud-A Managed Security Services, a suite of services designed specifically for Cloud-A.

Canadian Data Residency

Cloud-A Commitment

All Cloud-A physical infrastructure, systems, offices, employees and ownership are in Canada. Always. No client data will ever be moved without notification. Cloud-A's office and primary data centre facility is located in Halifax, Nova Scotia, Canada. Cloud-A Computing Inc. (Cloud-A) is a privately owned, registered corporation in the province of Nova Scotia, Canada (N.S Limited Company.) Neither Cloud-A or it's shareholder have any business interests or otherwise that bind Cloud-A to the laws of any country other than Canada.

User Responsibility

To ensure that client data is always resident in Canada, it is the user's responsibility to ensure that their data is organized and accounted for within their Cloud-A infrastructure. It is important to be aware of multiple copies of data that you may have previously stored on another non-Canadian cloud provider's infrastructure.

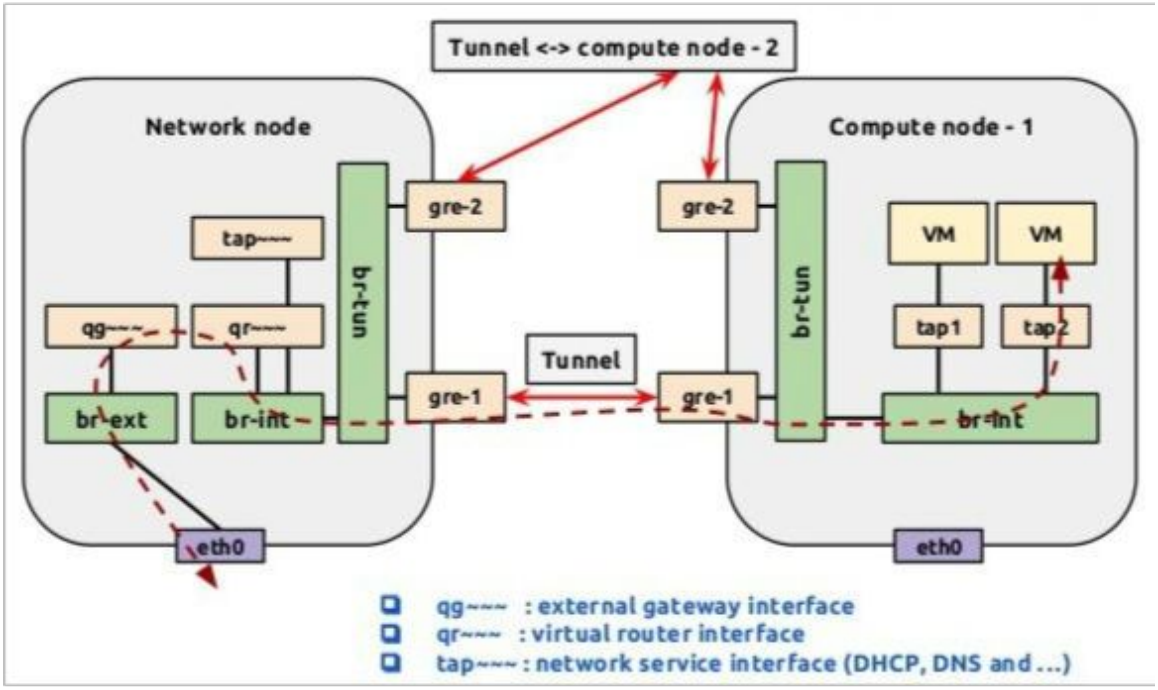
Security

Cloud-A Commitment

- Cloud-A operates in a SOC 2 (formerly SAS 70 Reports) TIA 942 Tier III data centre which is equipped with complete physical security: perimeter alarms, biometric authentication, CCTV monitoring and historical 30+ day records.
- Cloud-A manages our own Border Gateway Protocol (BGP) allowing us to make our own core routing decisions on how we interconnect with our several upstream internet service providers.
- Cloud-A has implemented and proactively monitors and manages a Distributed Denial of Service (DDoS) mitigation system.
- Cloud-A Security Operations Centre (SOC) proactively manages redundant, highly available firewalls and routers at the entry point of our network.
- Cloud-A's proactively manages a robust suite of network monitoring tools to identify network traffic anomalies and security threats.

- All client networks are fully segregated with Generic Routing Encapsulation (GRE) a tunneling protocol that encapsulates packets in order to route other protocols over IP networks.

Cloud-A Virtual Network Traffic Encapsulation via GRE



This diagram shows how traffic flows within Cloud-A's internal network from via GRE tunnelling

- All virtual servers are individually contained and segregated with both a hypervisor and AppArmor which limits the data access ability of a VM to only that VM's specific data. AppArmor proactively protects the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good behavior and preventing even unknown application flaws from being exploited. AppArmor security policies completely define what system resources individual applications can access, and with what privileges.
- Cloud-A is dedicated to consistent update and upgrade paths for all hypervisors, and physical host operating systems. Updates and upgrades are completed with with zero downtown to our users because of the ability to live migrate tenant environments across multiple physical hosts.
- Cloud-A provides our users with all of the tools to setup secure networks with our virtual private networking. Some of the built in security tools that Cloud-A provides to our users include:

Secure Access

User access points, also called API endpoints, allow secure HTTP access (HTTPS) so that users can establish secure communication sessions with your Cloud-A services using SSL/TLS.

Firewalls (Security Groups)

Users can control how accessible their instances are by configuring built-in firewall rules When your virtual instances reside within a Virtual Private Cloud (VPC) network like the tenant networks in Cloud-A, you can control egress as well as ingress.

For ingress traffic (to an instance)

- Only traffic matched with security group rules are allowed.
- When there is no rule defined, all traffic is dropped.

For egress traffic (from an instance)

- Only traffic matched with security group rules are allowed.
- When there is no rule defined, all egress traffic is dropped.
- When a new security group is created, rules to allow all egress traffic are automatically added.

Virtual Private Networking

The Cloud-A Virtual Private Cloud (VPC) service allows users to add another layer of network security to their instances by creating private subnets and even adding an IPsec VPN tunnel between your home network and your Cloud-A VPC.

Centralized Key Management

For users who use encryption extensively and require strict control of their keys, we offer a convenient management option for creating and administering the keys used to encrypt your data, or access your servers.

User Responsibility

Users are responsible for using unique, secure passwords on their instances, encrypting their drives, creating and managing secure virtual private networks, performing updates and patching as required, and monitoring and auditing their instances.

Redundancy

Cloud-A Commitment

- Cloud-A only operates redundant, enterprise class infrastructure (storage, servers and networking) and software capable of live migration and automatic failover within the data centre
- Cloud-A's Data centre has multiple upstream data and internet connections to Tier 1 carriers and providers, 2N In-line UPS system, high-capacity Uninterruptible Power Supplies, 3 phase 120-208 V K-13 PDUs, state-of-the-art fire suppression systems, and multiple backup diesel generators with extended on-site fuel storage (72 hours+)

User Responsibility

Cloud-A users are responsible for properly backing up the data that resides on their virtual infrastructure.

Reliability

SLA

Definitions

The following terms have the meanings set forth below when used in this SLA:

SLA: Service Level Agreement between Cloud A and the customer.

Cloud Server: Virtual elastic server with a mix RAM, CPU and Disk resources, running Linux or Windows, paid by the hour and controllable via the Web Control Panel or the compute API.

Cloud Storage: Virtual disk for persistent object storage, accessible and controllable via the Web Control Panel or the storage API.

Web Control Panel: The Cloud A dashboard provided at https://dash.clouda.ca/ where clients may log in to manage their services.

Scheduled Maintenance: Planned periods during which Cloud A's operations teams will execute maintenance tasks on the server, storage or network infrastructure, to update, correct or secure it. Scheduled maintenance periods are subject to prior notification to customers by email or through messages displayed in the Web Control Panel.

Emergency Maintenance: Maintenance windows that may be set for which Cloud A provides customer Notification at least four (4) hours before the beginning of an emergency maintenance window and identifies the service impacting reason for the maintenance.

Notification: A message displayed in the Web Control Panel or sent by email, with important information regarding a maintenance operation (scheduled or emergency).

Maintenance Window: A period, identified by a date, start and stop time, during which maintenance operations will be carried by Cloud A's operations teams. Maintenance operations will only be initiated at the start time and will be completed on or before the stop time.

Force Majeure: Extraordinary event or circumstance beyond the control of Cloud A, such as a war, strike, riot, crime, or an event described by the legal term act of God

(such as hurricane, flooding, earthquake, volcanic eruption, etc.), that prevents Cloud A from fulfilling its obligations under the general terms and conditions.

Acceptable Use Policy

Compliance required by both parties to the use of Cloud A Services, as described in https://www.clouda.ca/other/tos/.

Risk Mitigation Strategy and Communication Plan

In running a public cloud, it is essential that Cloud-A takes all necessary steps to mitigate any risks associated with security threats both at the infrastructure layer, as well as the client layer. In some rare situations, where a tenant poses a risk to other tenants' cloud infrastructure and/or the underlying cloud framework, Cloud-A reserves the right to intervene in the form of pausing, powering off, or terminating a tenant's infrastructure.

Grounds for Intervention

Given the diversity of existing security risk and the rapid emergence of new security threats on a daily basis, grounds for Cloud-A intervention and the type of intervention is situational and is often assessed on a case-by-case basis. With that said, Cloud-A has identified activities, trends and behaviors which we have classified as ground for intervention.

The following activities are grounds for Cloud-A intervention:

- Tenant's infrastructure being targeted by DoS / DDoS attack(s) causing significant network bandwidth consumption
- Tenant's infrastructure found to be participating in DoS / DDoS attack(s)
- Tenant's infrastructure found to be participating in a botnet of any shape or form
- Tenant's infrastructure found to be hosting illegal content as per Canadian law

Notification Policy

In the case of Cloud-A intervention due to security risk, it is our policy to notify the account contact and/or affiliated Cloud-A service partner within 2 hours of the intervention when deemed appropriate to do so, and according to Canadian law. It is the responsibility of the Cloud-A service partner and the end user to disclose the account affiliation(s) to Cloud-A.

Privacy Policy

Cloud A is strongly committed to protecting the privacy of all clients using its products and /or services. Our primary goal is to contribute to provide a safe and secure environment for consumers and site visitors.

Disclosure

We do not disclose information about your individual visits with any other company, group, or individual. All information gathered by Cloud A from an existing/new client is used for either (a) communicating with that client or (b) providing support for that client. Cloud A may share such information in response to any legal processes, such as a court order or subpoena, or in special cases such as a physical threat to you or others.

Information

The purpose of storing any personal information you may provide us when you visit our site or fill out any Cloud A forms, is to enable Cloud A to maintain communication with you. We will not sell, share, or give this information to any other company. Cloud A will only disclose user information to the proper authorities, when we believe in good faith that the law requires it.

We remind our users that whenever you give out personal information on the Internet, that information can be intercepted in transit. While we strive to protect any personal information in our possession, we cannot guarantee the security of any information you disclose online and you do so at your own risk except for on our secure pages. Cloud A will only receive credit card and other personal information over a SSL encrypted connection.

By using our site, you agree to the Cloud A Privacy Policy. If you do not agree to this policy, please do not use our site. Your continued use of the Cloud A site following the posting of changes to these terms will mean you accept those changes. This terms may be changed or modified at any time without notice, and by using our site, you agree to the privacy policy in place at that time.

General Terms

Service credit claims must be submitted in writing, within 30 days from the SLA violation to which they refer, via email to support@clouda.ca.

If the parties agree that Cloud A has failed to meet any service level guarantee during any given calendar month, Cloud A will credit the customer's account with the defined compensation.

Service credits shall apply only to the usage fee paid by the customer over the one-month period under analysis, for the affected services or resources.

The payment of the compensation shall be the customer's sole and entire remedy from Cloud A for any downtime arising under this agreement.

The customer agrees to correct problems and attempt to minimize the recurrence of problems for which customer is responsible and may prevent Cloud A from meeting the SLA.

A customer is not entitled to receive a service credit in the following cases:

If any downtime was caused by customer initiated actions whether implemented by customer or by Cloud A;

If any downtime was caused by an operating system or application malfunctioning or misuse by the customer and not a failure on the underlying network and physical host infrastructure directly and solely managed by Cloud A;

If any downtime was due to Scheduled Maintenance and within the defined Maintenance Window announced;

If any downtime was due to a Force Majeure event;

If the customer had his account suspended for any day of the month under analysis caused by non-payment of the usage fees;

Downtime due to the acts or omissions of the customer, its employees, agents, third party contractors or vendors;

Any event or condition not wholly within the control of Cloud A and violations of its Acceptable Use Policy.

Service Level Guarantees

Service Availability

Availability level	Max downtime	Compensation
>=99.99%	4m 19s	0%
>=99.95% and <99.99%	21m 36s	2%
>=99.50% and <99.95%	3h 36m	5%
>=99.00% and <99.50%	7h 12m	10%
>=90.00% and <99.00%	72h	50%
<90.00%	720h	100%

Web Control Panel Availability

Availability level	Max downtime	Compensation
>=99.50%	3h 36m	0%
>=99.00% and <99.50%	7h 12m	5%
>=90.00% and <99.00%	72h	10%
<90.00%	720h	15%

Cloud-A Status

www.status.clouda.ca

Cloud-A operates a system status page, which can be subscribed to, that provides up to the minute status information about all of Cloud-A's services.

Resources

Cloud-A Managed Security Services
Cloud-A SSH Key Management
Configuring Cloud-A Security Groups
Configuring a VPN server using Cloud-Init
Encrypted Volumes: Linux Edition
Linux Security Best Practises for the Cloud