GUIDE TO CLOUD SECURITY

CLOUD-A

LAST UPDATED 06.15.2015

info@clouda.ca | 1-855-925-6831 | www.clouda.ca

Whether it is for compliance purposes, protecting trade secrets, or safeguarding sensitive client information, data security is a priority for every organization in any industry. With the rapid adoption of public cloud environments, it is imperative to understand how cloud affects how you secure your data. At the most basic level, it is understanding which parties are responsible for the different layers of security, so to clarify how this works with Cloud-A, we have created the Guide to Securing Your Data with Cloud-A.

It is Cloud-A's responsibility to ensure that our infrastructure is bulletproof and that we follow security best practises, but once a client launches an instance, they have free reign to manage their cloud infrastructure as they please.

Here are some best practises and client responsibilities for securing your data with Cloud-A

Passwords 101

Password strength is the most basic layer of security in any scenario, but it is of the utmost importance. Weak passwords are a simple point of failure that the most ametuer attacker can take advantage of. A strong password should be between 10 and 12 characters, it should have a mixture of uppercase and lowercase letters, as well as numbers and symbols. There are tools available to assist with creating and keeping track of your passwords.
Check out LastPass (https://lastpass.com/)

Encryption is Key

Although the infrastructure that your Cloud-A instances reside on and the OpenStack platform that orchestrates and manages that infrastructure is built and managed with security as the top priority, it is the users responsibility to ensure that the drives of their cloud servers are protected. We recommend encrypting the drives (volumes) that are attached to your Cloud-A instances. Encryption is a great way to keep your valuable data safe at rest, as it make your data unreadable to any unintended recipient. For more details on configuration and benefits, you can check out our blog post: Encrypted Volumes: Linux Edition

Lock Down Security Groups

Cloud-A's security group functionality allows you to create firewall rules that can be applied to your instances. Instances are launched with all of the ports locked down and you can create your own firewall rules that you can allocate to your instances. It is important to use inclusive firewall rules rather than exclusive. Exclusive firewall rules allow all traffic through except for the traffic matching the ruleset. Inclusive firewall rules do the reverse as they only allow traffic matching the rules through

and block everything else. When creating your firewall rules, It is best practise to only allow internet access to servers that require it. You can use your internal networks created with Cloud-A's virtual private networking to connect servers that do not require internet access.

Understand that Cloud Security is a Partnership

Once you launch an instance on Cloud-A, you have full control over that virtual machine. It is up to the end user, or the Cloud-A integration partner to manage that virtual machine, ensure that it is patched, updated and that it is used appropriately. There is a level of knowledge that is required to operate a server securely. If you do not have that level of knowledge in-house, we advise that you seek out an organization that can provide these services. Cloud-A can help recommend partners who can assist with these services. Many organizations with stringent requirements for data security require advanced security services such as intrusion protection and detection and live security monitoring. Cloud-A's go-to security partner for these advanced security services is GoSecure.

CLOUD-A CLOUD-A FOR MORE INFORMATION CONTACT: GEOFF SULLIVAN
GEOFF@CLOUDA.CA