Abstract

This paper put insight on how the security mechanisms enforced by cloud computing providers of their IaaS platforms and enabling their users to utilize the platforms securely. This paper provides the assessment of two popular IaaS platforms with respect to the following criteria: network security, authentication and API security, security attack protection and high availability, logging and monitoring, access right control, and security. The assessment is based on the information provided by cloud computing providers and usage of the IaaS platforms.

References


https://cloud.google.com/logging/docs/view/logs_index, 2015, [Online; accessed 06.11.2015].
https://cloud.google.com/logging/pricing, 2015, [Online; accessed 06.11.2015].
23. M. Seaborn and T. Dullien, “Exploiting the DRAM rowhammer bug to gain kernel
privileges,”
http://googleprojectzero.blogspot.de/2015/03/exploiting-dramrowhammer-bug-to-gain.html,
2015, [Online; accessed 06.11.2015].
http://docs.openstack.org/openstack-ops/content/projects_users.html, 2015, [Online; accessed
06.11.2015].
25. “AWS - Manage Permissions and Policies,”
06.11.2015].
26. “Configuring permissions on Google Cloud Platform,”
https://cloud.google.com/docs/permissions-overview, 2015, [Online; accessed 06.11.2015].
https://cloud.google.com/compute/docs/autoscaler/, 2015, [Online; accessed 06.11.2015].
28. “AWS Shared Responsibility Model,”
06.11.2015].
https://cloud.google.com/security/, 2015, [Online; accessed 06.11.2015].
06.11.2015].

Index Terms

Computer Science
Distributed Systems

Keywords

Cloud computing, Infrastructure as a Service, security, Amazon Web Services, Google Cloud
Platform.