ONDA Cloud Resources Security Guidelines

Table of Contents

1. Introduction

The main objective of this document is to provide a non-exhaustive description of some security measures to be taken into account when it comes to IT security within the ONDA DIAS Cloud resources.

ONDA DIAS is a cloud computing based service where the provider maintains the responsibility of the security aspects of the underlying infrastructure components such as hardware, networks, access management tools, etc.

Customers and belonging users are accountable for every security aspect from the operating system level up to the application level, and also for the private networks that are chosen to be deployed within the customer environment.

As such, ONDA DIAS customers shall define their security policies / measures that are relevant to their accountability, and make sure that their compliance is enforced within their environment.

2. Security Measures objectives

2.1. Policy

Security standards knowledge shall be acquired by the users in order to be able to maintain a secure environment.

Users shall identify custom preferred approaches to apply while accessing ONDA cloud resources proportionally to the nature of the activities and associated risks.

Security controls for provisioned systems shall be evaluated in line with these standards, and responsibilities are to be well understood by users in order to properly apply protection measures.

Users shall ensure that settings are enforced to guarantee:

- CONFIDENTIALITY: any data and information that is available to users shall be protected in a way that only authorized users have access.
- INTEGRITY: any data and information that is available to users shall be protected from alteration and accuracy and completeness must be guaranteed.
- AVAILABILITY: users are to ensure that authorized users can access data and information when required.
- Compliance:
    - Regulatory requirements: users shall ensure that any regulatory and legislative requirements will be met.
    - Contractual compliance: users shall ensure that the use of provisioned resources are in compliance with the ONDA DIAS terms and conditions, and that any information sharing is handled in compliance with specific policies.

In order to support the users in these commitments, ONDA DIAS has developed, implemented and maintained a management system and a set of processes enabling the protection of users provisioned environment for the virtual infrastructure.
Users shall therefore adhere to security best practices in order to maintain an efficient level of security within the cloud resources they have provisioned.

3. Security Measures guidelines

3.1. Data protection

Personal data, and any other data that is subject to licenses/policies, need to be protected from threats in accordance with applicable legislation.

ONDA users shall make sure that critical data are fairly and lawfully processed, obtained for specific purposes only, and processed in a manner that is compatible with those purposes.

3.2. ONDA provided protection tools

ONDA users are provided with some tools that allow them to easily provision public cloud resources while being able to apply security measures appropriately:

- The default access mechanism provided to users cloud instances is exclusively via the provisioning of an SSH key handshaking, and only the user owns the private key. This enforces the protection against unwanted access to users systems even from the cloud provider personnel.
- Provisioned instances are protected by default by a security group functionality that provided traffic filtering. Security groups can be further customized by users for their resources in order to additionally create filtering rules based on their needs.
- Users are also provided with the possibility to provision private networks, allowing to self-provision applications within a private network infrastructure where segmentation of any type can be configured at the user choice (i.e. north-south vs east-west network security zones for multi-tier applications and controlled traffic).
- Access to ONDA datasets through the Advanced API usage (ENS) is only granted via the provisioned cloud resources, allowing to avoid credentials management from the user side, while enforcing for restricted access to the data to allow for and availability. Data is accessed via the use of a read-only exposed NFS protocol.

3.3. ONDA business support

ONDA users also have access to a series of pre-packaged or customizable support services for the operations of their provisioned resources. Support services can also include security related services such as engineering support for the design of a secure infrastructure that leverages on the available tools of the public cloud environment, and with the use of best practices for provisioning security protection functionalities within the customer environment.

3.4. Technical security

Specific controls are to be implemented to manage and control remote access to user provisioned cloud resources.

In order to ensure protection of systems and private networks, users shall identify all the measures that need to be applied to make sure that systems and private networks are well protected.

Here are some suggested guidelines to be followed in order to achieve this:

- Vendor default accounts and passwords shall not be left unchanged before a system can be made accessible over Internet.
- Access to provisioned resources shall be made through secure communication protocols.
- Host based malware detection and protection software shall be enabled in order to detect, prevent and recover from malicious code or from unauthorized access attempts.
- Software patching shall be applied at least for security patches of used software in accordance with the risk to which the software vulnerability is exposing.

- Critical data and information should be backed up and ensure that restore procedures function correctly.
- Private networks should be configured with proper separation in case of sensitive data handling, and made not accessible from untrusted networks.
- Custom applications shall be developed in compliance with secure development principles.
- Firewall filtering rules shall be enabled to keep control over the allowed communication flows.
- Provisioned systems and resources shall be used in accordance with the purposes for which they are provisioned.
- An efficient approach in handling access credentials is to be used by enforcing passwords robustness and making credentials hard-to-guess.
    - Particular attention should be paid with the use of the credentials for API accesses, as the same credential pairs are used for the handling of the cloud resources purchases. Measures should be applied to protect these credentials as they are the same ones with which a user can make purchases and cloud resources provisioning on the ONDA web portal.
- Access to provisioned resources shall be allowed to authorised personnel only.

Users are free and required to customize the set of rules and guidelines to apply in order to protect provisioned resources.

End of the document