INFN Cloud Security Recommendations

Document log

Issue	**Date**	**Comment**	**Authors**
1.0	2021 Jun 09	First version	WP4

Table of Contents

Introduction

The following rules are intended to cover 99% of use cases, and must be applied as they are written. It is recognized, however, that some use-cases exist that conflict with them. In any such case, it is possible to discuss the need for an exception by asking for a discussion with WP4, who will decide whether to grant the exception (limited only to the specific use-case being considered) or to suggest alternative implementation that would be in full compliance with the rules. It is never permitted to ignore any rules without having first obtained such specific exception.

Operating system

Security Recommendation	**Comments**

Use a supported OS version	Always use the latest version of the OS of choice, or at least a version that is actively supported and for which security updates are released regularly.
Use an updated version of the OS	Update the OS version as soon as a new one is available and stable. Hosts running OS versions that are going out of support must be updated.
Do a package update the at least once a month	Make sure the kernel and the software packages distributed by the vendor are up to date. Run an upgrade at least once a month.

Containerized environments

Security Recommendation	Comments
Periodically update the running docker images	Always use the latest version of the OS and application of choice, or at least a version that is actively supported and for which security updates are released regularly.
Run security scans on docker images before using them	Make sure that docker images used for your services are safe. Run a scan on specified resources or ask INFN-Cloud to do it for you

Application Software

Security Recommendation	Comments
Files which contain passwords must be readable only by the user that runs the program, and writable only by root.	Files containing passwords are common targets by hackers.
In house developed software must not have obsolete dependencies	Regular updates must not be avoided due to in house developed software dependencies. In house developed software must depend only on maintained software.
Third party software must be updated	Third party software (i.e. not coming from the OS release and not developed in house) must be up to date or at least supported and free from known vulnerabilities.

Use software securely	If guidelines for the safe use of a piece of software exist, follow them.
Enforce authentication and authorization on multiuser applications	Multiuser applications must follow the rules in the section below for credentials management.
Assess the security level of in house developed software	Run a security scan before releasing a product or ask INFN-Cloud to do it for you.

Authn/Authz

Security Recommendation	**Comments**
Do not use default credentials	Always change the default credentials
Do no hard code credentials in your code	
Enforce password policies	Make sure chosen passwords respect present password policies. The INFN accepted password policy is: Length: 10 characters Character classes: 3 Password history: 5 Minimum password life: 1 day Password validity: 1 year Also, do not use passwords based on or derived from your username
Limit anonymous access	Anonymous access must be enabled only if needed and must only allow for read operations.

Network Access Controls

General Rules

Security Recommendation	Comments
Encrypt all password protected connections.	Use SSL/TLS or SSH tunnels to encrypt all password-protected TCP connections.
Encrypt all connections, unless there is a strong reason not to do so.	Use SSL/TLS or SSH tunnels to encrypt TCP connections. Make sure the enabled cryptographic algorithms are considered secure.
When applicable, restrict instance access to authorized IP addresses.	Use the cloud middleware “security groups” as a mechanism to allow instance access from authorized IP addresses. Also host-based firewalls (such as iptables and firewalld) can be used to restrict network access to instances, in terms of ports, protocols, and packet types. These firewalls can be used to prevent potential network security attack reconnaissance (for example, port scanning) and intrusion attempts. Custom firewall rules can be configured, saved, and initialized on every instance boot.

SSH

Security Recommendation	Comments

Use a safe version of SSH	Make sure the SSH server version has no known vulnerabilities
Use public-key logins only	Periodically review SSH public keys in ~/.ssh/authorized_keys file.
Disable password logins	Mitigates password brute-force attacks
Disable root logins	Prevents root privileges for remote logins
Install and enable Fail2ban	Mitigates password brute-force attacks

HTTP/HTTPS

Security Recommendation	**Comments**
Encrypt all password protected connections. Use valid x509 certificates.	Use SSL/TLS to encrypt all password-protected HTTP connections. Make sure the enabled cipher suites and SSL/TLS protocol versions are considered secure.
Encrypt all connections, unless there is a strong reason not to do so. Use valid x509 certificates.	Use SSL/TLS to encrypt HTTP connections. Make sure the enabled cipher suites and SSL/TLS protocol versions are considered secure.