General Security Guidelines for ADA cloud

This list of security guidelines is not meant to cover all the possible cases and scenarios, but to serve as a starting point for keeping everyone secure.; please read it carefully.

Introduction

Security responsibility

> **Users** are responsible for the security of the virtualized resources under their control. This includes, but it is not limited to: **virtual machines, network configuration, user accounts, disk volumes**.

Security reports

> If you discover a critical security flaw or believe that your machine has been compromised, please contact us immediately at superc@cineca.it

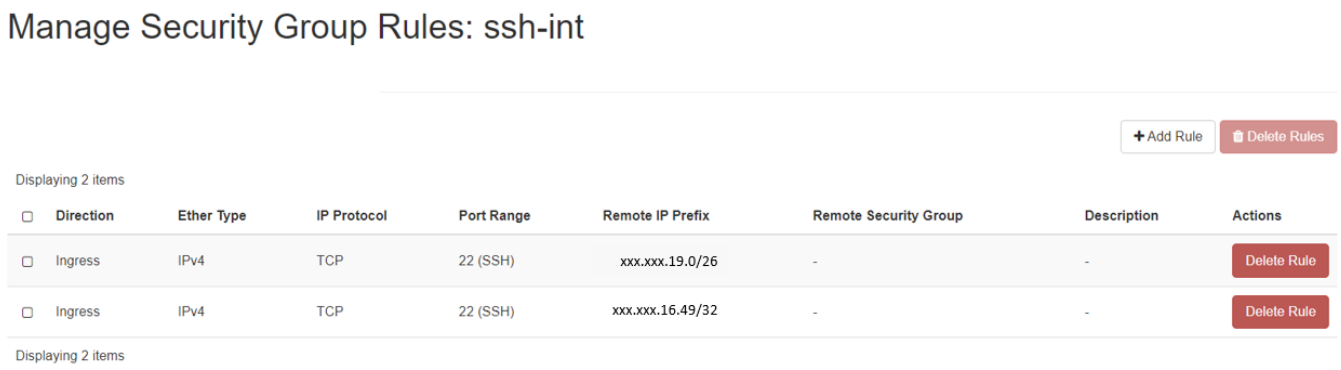
Network

It is very important to keep your network configuration as secure as possible, as it is the gate any intruder will use to enter in your system. It is relatively simple to apply some good practices that will give a good extra security layer. Here below few strategies are advised.

Restrictive firewall (white listing)

Your Virtual Machine (VM) instances should be configured so that they allow the minimum required access to run your application. By default, virtual machines have no external access (default security group rules in ADA Cloud), this means no single port is opened by default to the public Internet. In order to connect to them, or to provide any kind of service, access has to be explicitly granted. It is important to open only the ports that are needed and open them only for the least amount of IPs possible.

Every virtual machine running in ADA Cloud comes with ADA Cloud Security groups. ADA Cloud Security groups are the easiest way to apply a set of complex firewall rules to a set of virtual machines. This is an example of a security group that gives access to port 22/SSH to only 2 subnets (which could be the 2 public ranges that your organization uses in its office network):



Security groups are easy to configure and easy to visualize in the ADA Cloud dashboard under the Network tab or in each virtual machine's instance page.

Disable unneeded services

Do not run unnecessary services on your VM, even if they are not accessible from the outside. The more services you run, the more potential attack surfaces you have that top intruders might exploit.

Use secure protocols

Wherever possible, use encrypted and secure communication protocols to avoid man in the middle attacks; this is when someone get access to your communications and can read the data going through like in a public WIFI. For example: do not use HTTP, use instead HTTPS. Do not use FTP to transfer files, use instead FTPS, SFTP or S3.

If you need a web certificate for your VM, we suggest to use the service provided by Let's Encrypt.

Use intrusion detection software

Tools such as denyhosts or Fail2ban can be used to analyse log files and ban IP addresses that are attempting to make brute-force attacks to your application. They are very powerful tools, but they have to be used used with care as they can lead to false positives, i.e. Banning IPs that should not be banned. These tools are a best practice to provide 24/7 services, while may not be necessary for single user VMs.

DNS name

It is possible to ask CINECA for a DNS name association to the virtual machine by sending an email to superc@cineca.it.

- The reverse of the Floating IP (FIP) must be set to the *hostname* of the VM, with the following naming convention:
  - for external users: <VM-name>.ext.cineca.it
  - for CINECA staff: <VM-name>.cineca.it
- The record A in the DNS is set accordingly to the previous point. If the service should be exposed with a different name, you can ask to set the CNAME with the chosen different name. If no other information is provided, only the record A will be set.

Software

Running secure software is also very important. It is not a trivial task to develop fully secure software, but there are some simple strategies that will help with the task.

Automatic software updates

All operating systems have the ability to apply updates automatically. If you run regular updates, you are less exposed to known security problems. It is common that the fix is available before the security problem is published.

In Centos 8 and newer, you have `dnf-automatic`:

```
sudo yum install dnf-automatic -y
systemctl enable --now dnf-automatic-install.timer
```

For Centos 7, you have *yum-cron:*

```
sudo yum install yum-cron -y
sudo systemctl enable yum-cron.service
sudo systemctl start yum-cron.service
```

For Ubuntu, `unattended-upgrades` :

```
sudo apt install unattended-upgrades
```

Each OS version will have its own way to activate this.

Kernel updates: Some updates, such as kernel upgrades, require rebooting the virtual machines. Please schedule this into your regular maintenance.

If your use case does not support automatic updates, which is common for highly available setups, please make sure to schedule regular maintenance windows where the software upgrade is scheduled.

Subscribe to security announcements for your OS, if there is a security problem in your operating system, you need to find it out as soon as possible. You can subscribe to an appropriate mailing list, RSS feed, ... to keep an eye out for anything that requires urgent action.

Only install from reputable sources

Be mindful of the sources for the software you install. Only install software from reputable sources. If possible, use the distribution's package manager (`yum`, `dnf`, `apt`, ...). Packages managers make it easy to install software, keep it updated, and uninstall it. If the desired software is not available in the distribution package manager repository, an official source must be used. Follow the instructions on the official website of the software you need. If more than one source is offered, think about using the one that provides an easier life-cycle (install/update/uninstall/...), like snap or flatpak.

Security for databases

If you have databases in your VM please make sure that these:

- are not open to the whole internet (0.0.0.0/0)
- are password protected
- information is transferred via a secure connection.

Be mindful about the user accounts in the VM

Keep an eye on the user accounts enabled in your system. Some applications create default accounts which are unnecessary or even directly insecure. An ideal scenario might be three accounts:

- `root` with ssh disabled and no password. This is the default in the images provided on ADA Cloud for the different OS (i.e. Ubuntu, Centos,..).
- A user account for a sysadmin that can only be accessed via ssh keys and has sudo access. ADA Cloud VM images provide this user pre-configured as well, the name of the user depends on the distribution (`cloud-user`, `centos` or `ubuntu`), see the documentation for more information.
- and add user-level accounts that run a single service and have no login possible, neither remote nor local access.

Do not enable password login, **use SSH keys** instead (see how to set Key Pairs in the ADA Cloud User Guide). Passwords can be, with enough time and compute power, guessed with brute force. The average SSH server deals with thousands of such attacks every week. When using SSH keys, challenge-response authentication is used instead. This means that for each login a different challenge is asked and a different response is the correct one. No secret (password or key) ever travels across the network

Password protect your SSH keys and make sure your key never leaves the hardware where it was created.

- Do not store public keys (much less private) on the image used to create the VM.

Keep logs of your applications

Use the best practices for logging:

- Make sure that the services are logging to a secure location, that is as tamper-proof as possible.
- Keep the logs for a reasonably long amount of time.
- Consider logging to a remote server as well.

More information

If you are interested to learn more about security in cloud application, we advise to read the material provided by NeCTAR.

Acknowledgements

CINECA Team would like to acknowledge the following source of information for this page: https://docs.csc.fi/cloud/pouta/security/ .