

A decorative graphic on the left side of the page, featuring a complex network of thin, light blue lines connecting various points, resembling a mesh or a web structure. It is partially overlaid by a light blue diagonal band.

EPAM Cloud Infrastructure Orchestrator ver.2.1.63

What's New

February 2015

[CI2WN-S60-63](#)

Version 1.0

Legal Notice: This document contains privileged and/or confidential information and may not be disclosed, distributed or reproduced without the prior written permission of EPAM®.

CONTENT

Content	2
1 Overview	3
2 Improved Access for Delivery Managers	4
3 Default Owners for VMs	5
4 Cloud Expansion: New Regions	6
4.1 Mac Region Introduction	6
4.2 New AWS Region	7
5 Maestro CLI Improvements	8
5.1 Command: or2-report.....	8
5.2 Command: or2-prohibit-terminate-instances	9
5.3 Command: or2-describe-regions	9
5.4 Command: or2-help	10
5.5 Command: or2-convert-maestro-stack	11
6 Platform Services Updates	12
6.1 Ambari Service Update	12
6.2 Docker Service on Azure	13
7 Security Updates	14
7.1 AWS Security Groups Changes	14
7.2 Scheduled and Initiated Nessus Scanning	15
7.3 Nessus Scan Report	15
7.4 EPAM Weekly Vulnerability Report	16
8 Knowledge Base Updates	17
Table of Figures.....	18
Version history.....	19

1 OVERVIEW

EPAM Orchestration Framework version 2.1.63 was released on February 13, 2016. During the latest weeks, we concentrated on EPAM orchestration stabilization, usability improvements, and, to greater extent, on Cloud security improvements, as this point becomes increasingly crucial as Cloud usage grows.

Thus, we are glad to introduce the following new features and improvements:

- Advanced Cloud access was granted to projects' Delivery Managers
- The solution to set up default Owners for VMs is introduced
- EPAM-MAC region is introduced to allow EPAM Cloud users to order virtual and hardware MacOS servers in terms of self-service.
- A new AWS region is added (South Korea, AWS-AP-NORTHEAST-2).
- Several useful updates are introduced to Maestro CLI.
- Cluster management functionality is improved for the Ambari Service.
- AWS Security Groups rules were changed.
- Nessus Vulnerability scanning procedures were improved.

These changes are described in details further in this document.



Our users often address us with the questions for EPAM Private Cloud SLA details and clarifications. For you to be more acquainted with the subject and to prevent misunderstandings and unexpected situations, we strongly recommend to review [EPAM Cloud Service Offering](#) document.

2 IMPROVED ACCESS FOR DELIVERY MANAGERS

For the success of each project, it is essential not only to provide project teams with a sufficient set of effective development tools, but also to give an effective resource and expenses control tool to the project's persons in charge.

Such tool is the **Manage Cloud** wizard which gives access to strategic project settings:

- Personal Cloud permissions of each project member
- Cloud permissions of groups of project members with the same project roles
- Monthly project's financial quotas
- Daily project's resource creation quotas
- Cloud Notification plans

The wizard has already proved to be of help for **Project Managers** and **Project Coordinators**, and starting with Orchestration v.2.1.63, **Delivery Managers** can also use it for the sake of project needs:

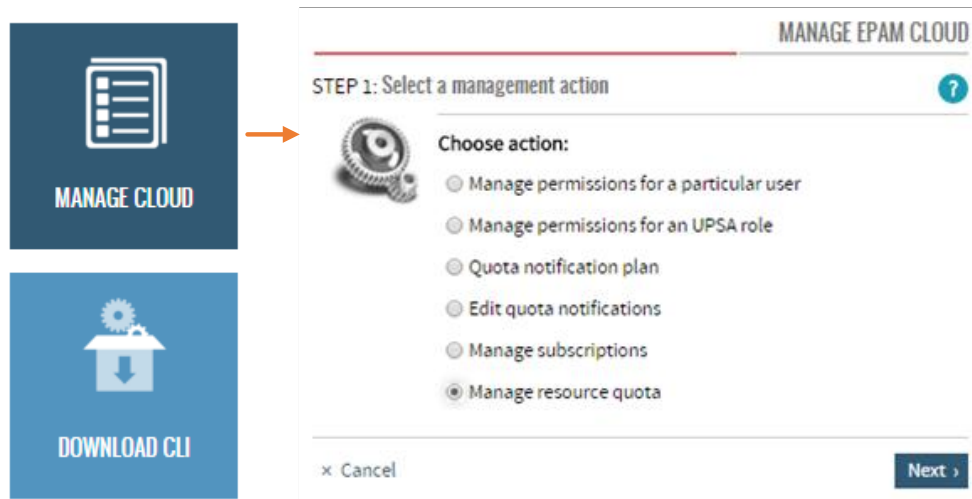


Figure 1 - Manage Cloud Wizard

3 DEFAULT OWNERS FOR VMS

Typically, EPAM Orchestrator automatically detects the user who initiated creation of a new VM, and sets this user as the VM's Owner.

The Owner is a person who retrieves the notifications regarding the VMs state changes and all the respective messages.

Besides this, the VM Owner typically becomes a contact point for other project members and support teams in case any information on the server is needed, or it is necessary to perform some actions on it.

However, there are situations, in which a VM's owner is not specified.

With the current update, we introduced the solution that allows to establish automatic Owner setup for such cases.

In case automatic detection failed, the **Project Manager** of the project to which the VM is assigned, is specified as its Owner.

Please remember, that you can always manually change the instance Owner by calling the **or2chow** command and specifying the new Owner's email address:

```
or2chow -r DEMOREG -p DEMOPRO -i instance_ID -e user_user@epam.com
```



4 CLOUD EXPANSION: NEW REGIONS

4.1 MAC REGION INTRODUCTION

MacOS becomes more and more desired among EPAM Cloud users. Before these days, to get a MacOS instance, one had to address the Support team and wait for the request to be processed.

With the EPAM Orchestration v.2.1.63 we are glad to announce the introduction of **EPAM-MAC** region, designed to enable Mac resources provisioning in terms of self-service.

The region is hosted in Minsk (BY), and hosts two types of instances – virtual and hardware, each having its own specifics.



- **Virtual.** Virtual MacOS instances are based on **MacOS 10.10 Yosemite** operating system. The instances details are:
 - **Image name:** MacOS_10.10_Yosemite
 - **Shape:** Any standard EPAM Cloud shape (recommended – MEDIUM)
 - **System Disk:** 60GB
 - **Billing:** Same as in EPAM-BY1 region
 - **Login:** Use **or2console** command and **user/user** credentials
 - **Limitations:** checkpoints are not available.

To run such an instance, use the standard `or2run` command, and provide the new instance details, e.g.:

```
or2run -p <project> -r EPAM-MAC -i macos_10.10_Yosemite -s <shape>
```



With the introduction of the EPAM-MAC region, all the MacOS VMs that were previously created in Cloud, were automatically moved from EPAM-BY1 to EPAM-MAC. Thus, to address these VMs, please use the new region name.

- **Hardware.** The other type of resources that can be provided in EPAM-MAC region, are reusable hardware Macmini (OS X 10.11.2) servers that can be provided for projects' needs. The specifics of this kind of resources are:
 - **Image name:** macmini_os_X
 - **Shape:** Large (2CPU, 8GB RAM) only
 - **System Disk:** 300GB, not extendable
 - **Billing:** \$30/Month, calculated hourly
 - **Login:** via VNC console
 - **Limitations:**
 - Instance operations strictly limited: only **or2run**, **or2kill**, **or2report**, **or2settag**, **or2din** commands are available. You can also see all the instance-related info on UI.

- Limited number of available servers. To check whether there are Macmini instances available, please use the **or2vps** command:

```
or2vps -r EPAM-MAC
```

In case there are no free Macmini servers, you will get a respective “low capacity” message when trying to request one.

In this case, please, wait till one of the servers in use, is released.

To order a hardware Mac, use the standard **or2run** command, and provide the new instance details, e.g.:

```
or2run -p <project> -r EPAM-MAC -i macmini_os_X -s LARGE
```



Macmini hardware servers are also physically located in Minsk. As these servers are very sensitive to network latency, it is highly recommended to use them only if you are also located in Minsk.

4.2 NEW AWS REGION

Amazon Web Services continues expanding its coverage all over the world, and one of the latest updates is the establishment of a new Asia Pacific region, based in Seoul (South Korea) – **ap-northeast-2**.



To provide our users with the widest possible scope of AWS facilities, we immediately reacted on the update, and supported the region within the scope of EPAM Cloud integration with Amazon.

Starting from February 13, the users whose projects are activated in Amazon, can start using the new region with EPAM Cloud tools, referencing it as **AWS-AP-NORTHEAST-2**, e.g:

```
or2run -p DEMOPRO -r AWS-AP-NORTHEAST-2 -i W2012Std
```

There are no special conditions for using this region via EPAM Cloud.

For more details on the native AWS services, supported in the region, please see the [Regional Product Services](#) page on AWS web-site.

5 MAESTRO CLI IMPROVEMENTS

Maestro Command line continues to be an important tool, widely used by project teams. Thus, although EPAM Cloud team pays much attention to improve its usability and informative value.

With the current production update, we introduce four significant updates to Maestro CLI:

- **or2-prohibit-terminate-instances** command is added to allow instance lock from termination
- **or2-describe-regions** command output was expanded
- **or2-help** command output formatting was changed, help by regions enabled
- **or2-report** command allows to get billing reports by manager's account to users, who are subscribed for this account
- **or2-convert-maestro-stack-template** command was introduced to allow converting Maestro Stacks to AWS CloudFormation ones.

The details on these updates can be found further in this section.

Beside this, we also introduced a number of usability improvements to Maestro CLI:

- Commands execution date is displayed in console at command call
- **or2-change-owner** command is supported for AWS-hosted instances
- **or2-describe-instances** command allows to specify multiple region parameter
- **or2-price** command output now includes checkpoints and volumes pricing for inactive instances
- **or2-describe-maestro-stacks** and **or2-describe-maestro-stack-resources** commands: project and region parameters are not obligatory any more
- **or2-run-maestro-stack** command now supports attributes separated by comma

5.1 COMMAND: OR2-REPORT

For account managers, it is often important to get a unified report for a set of projects. For such cases, EPAM Orchestrator includes a solution, known as **EPC Account**.

An **EPC Account** is a **logical group** of PMC Projects that can be associated to a cost-center. When an Account Manager submits a request for creating an account, they specify the account name and the list of the projects to be included to the EPC Account.

After that, the people specified as EPC Account contacts, get access to the aggregated billing information on all the account-related projects by calling the **or2report** command:

```
or2report -m 07 -y 2014 --account-name --type total
```

The requested report will be mailed as a .csv file and contain the list of the user's projects, the cost centers in which they are priced (each cost center is bound to a virtualization region), the reporting period and the cost:

A	B	C	D
PROJECT	C_CENTER	PERIOD	VALUE
EPM-AAA	SS/IT/IS/DC	2014-07	211.00621906
EPM-AAA	SS/IT/EUC/CIS/BY	2014-07	994.242380
EPM-BBB	SS/IT/EUC/CIS/RU	2014-07	584.921714
EPM-BBB	SS/IT/EUC/EU/HU	2014-07	2541.289888

Figure 2 - Account Report

However, sometimes it is needed to provide the access to an EPC account's billing information to people outside this account's contact list.

With the previous Orchestration update, we introduced the possibility to subscribe specific users to Monthly Summary Reports, by Account Manager's name. To do this, one needs to [submit a request to Cloud Support](#) and provide the name of the Account Manager, to whose report new people should be subscribed.

With the current release, the users subscribed for Summary reports this way, also get the possibility to use the **or2report** command to retrieve the respective EO Account's billing information.

5.2 COMMAND: OR2-PROHIBIT-TERMINATE-INSTANCES

With the current Orchestration version, we introduce a new command which allows to protect your instances from undesirable termination.

This is the **or2-prohibit-terminate-instances (or2prkill)** command that can be called by any user who has permissions to terminate instances in Cloud (for more details on the subject, see [User Permissions](#) page).

To lock a VM from termination, call the command, specifying instance ID, project and region:

```
or2prkill -p DEMOPRO -r DEMOREG -i instance_ID
```

If the same command is run on a locked VM, the termination prohibit will be removed.

5.3 COMMAND: OR2-DESCRIBE-REGIONS

The **or-describe-regions (or2dreg)** command was updated so that now it provides not only the list of the regions, available for the specified project, but also the respective regions technical details:

```
D:\maestro-cli-qa\bin>or2dreg -p DEMOPRO -t EPAM
Response:
=====
name      | access | virtType | orchType | status | monthSla | coefficient | quotaLimit | quotaPolicy |
=====
EPAM-BY1  | Advanced | ESX      | HP CSA   | RUNNING | 98.5%    | 1           | 2500       | enabled     |
EPAM-HU1  | Advanced | ESX      | HP CSA   | RUNNING | 98.5%    | 1.00       | N/A        | N/A        |
EPAM-KZ1  | Advanced | HyperU   | HP CSA   | RUNNING | 98.5%    | 1           | N/A        | N/A        |
EPAM-MSQ3 | Advanced | KVM      | HP CSA   | RUNNING | 98.5%    | 1.00       | N/A        | N/A        |
EPAM-HWU  | Advanced | Hardware | HP CSA   | RUNNING | 98.5%    | 1           | N/A        | N/A        |
=====
```

Figure 3 - or2dreg command output

Where:

- o **name:** the name of the region, in which the project is activated

- **access:** EPAM Cloud access level of the user who called the command. There are four levels, each including a group of permitted actions:
 - **guest:** READ, META, VM, STORAGE
 - **low:** READ, META, VM, STORAGE, NEW_RESOURCES
 - **medium:** READ, META, VM, STORAGE, NEW_RESOURCES, KILL_RESOURCES
 - **advanced:** READ, META, VM, STORAGE, NEW_RESOURCES, KILL_RESOURCES, ADVANCED_MANAGEMENT

You can find the details on the actions, included to each group, on the [User Permissions](#) page.

- **virtType:** the regions' virtualization type
- **orchType:** the type of the orchestrator used
- **status:** the current status of the region
- **monthSla:** the region's availability statistics, based on the information gathered during the latest four weeks
- **coefficient:** the regions' billing coefficient
- **quotaLimit:** the project's quota limit in the region, if any
- **quotaPolicy:** specifies whether quotas are applied to the project or not

5.4 COMMAND: OR2-HELP

The **or2help** command was complemented with the **--region/-r** parameter which allows to see only the commands available in the specified region.

The command output is also improved: by default, the commands go alphabetically with brief descriptions. In case you need the commands with detailed parameters info, you can use the **-full** flag.

On the example below, you can see the difference in the outputs for the **or2help** command launched for the AWS-USEAST region:

```
D:\maestro-cli\bin>or2help -r AWS-USEAST
Response:
=====
command | alias | description
=====
or2-add-ao-account | or2addacc | Creates an EPAM Cloud account to combine costs for different projects
or2-allocate-static-ip | or2alsip | Allocates a static IP to the project.
or2-ambari-cluster | or2ac | Manage Ambari cluster.
or2-ansible-dynamic-inventory | or2adi | Returns Ansible dynamic inventory in a JSON format for a specified pro
or2-ansible-group-properties | or2agp | Manages ansible group properties (e.g. set, delete, describe)
or2-ansible-groups | or2ag | Manages ansible groups (e.g. create, delete, describe).
or2-ansible-hosts | or2ah | Manages ansible hosts (e.g. include, exclude, describe).
or2-ansible-init | or2aa | Initializes Ansible environment for a specified project in zone.
or2-associate-static-ip | or2assip | Associates the specified static IP to the given VM.
or2-attach-volume | or2attvol | Attaches specified storage volume to the specified instance

D:\maestro-cli\bin>or2help -r AWS-USEAST --full
Usage: or2-add-ao-account(or2addacc) [options]
Options:
 * -c, --contact Account contact email. For several contacts repeat the
 parameter: -c email1 -c email2 -c emailN.
 * -d, --description Project account description.
 --full Show full command output
 Default: false
 --help Display command help
 Default: false
 -P, --plain-output Use plain output view
 Default: false
 * -p, --pmc-code Project PMC code. For several project codes repeat the
 parameter: -p pmcCode1 -p pmcCode2 -p pmcCodeN.
```

Figure 4 - or2dreg command outputs in different modes

5.5 COMMAND: OR2-CONVERT-MAESTRO-STACK

These days, more and more teams set up their environments on different platforms – EPAM Cloud, AWS, Azure, and switch between them depending on their needs.

In such cases, it is important to have a unified solution that would allow to initiate automated setup with a single set of tools, with minimum customization for each specific platform.

EPAM Orchestrator supports its native Maestro, and AWS CloudFormation stacks – tools that allow to pre-define resource settings in specific files, called **stack templates**, and automatically apply these settings by referencing these files.

Maestro Stacks can be written manually and uploaded to Orchestrator, or created with the Stack Builder wizard available on the Dashboard. They can be applied to resources on all the platforms with which Orchestrator works – EPAM, AWS, and Azure.

Meanwhile, AWS usage grows, and sometimes it is necessary to use a stack outside Orchestrator, or complement is with some AWS-specific functionality.

Thus, to provide higher compatibility with AWS and give Cloud users the ability to apply created templated outside EPAM Orchestration, we introduced the **or2-convert-maestro-stack-template (or2cmst)** command to convert Maestro Stacks to CloudFormation ones.

An example of the command call is given below:

```
or2cmst -p demoproject -r aws_region -f template_path [-d output_path]
```

Where:

- **region** parameter value is the name of the AWS region where you plan to run the stack. Due to platforms specifics, image names used in Maestro and CloudFormation stacks are different, and for each AWS region, there is a special instance type corresponding to one EPAM Cloud image.

To omit unexpected failures in templates processing, please repeat the conversion procedure for each of region where you plan to run the template.

- **template_path** is the path on you workstation where the source template (.json) is stored.
- **output_path** is the path on your workstation where the resulting template (.json) will be saved. If you do not specify this parameter, the template text will be outputted to the console.

If you need to convert a Maestro Stack template that was uploaded to Orchestration, but you don't have it on your workstation, follow the instruction below:

1. Run the **Stack Builder** tool.
2. On **Step 1**, click the **Catalog** button.
3. Select the **project** to which the template was uploaded
4. Select the template **owner** (or the "All" option)
5. Select the "**Maestro**" template type
6. Select the template.
7. Select the template text and copy it to the clipboard.
8. Open any text editor, paste the template text and save the file in .json format.



6 PLATFORM SERVICES UPDATES

6.1 AMBARI SERVICE UPDATE

Traditionally, the new Orchestration version comes up with a number of updates, related to platform services provisioning.

This time, we introduced the following improvements to the Ambari service, designed to assist with Hadoop clusters monitoring and management.



For more details on the service usage, please see [this page](#).

Thus, in the current version of Orchestration, we expanded the **or2-ambari-cluster** commands facilities by adding the new items to the **--action/-a** parameter

- **--action describe** – this action allows to get the information on the existing Ambari server and all the related cluster instances:

```
or2ac -c testcl -p DEMOPRO -r EPAM-BY1 -a describe
Date: 2016-02-10T09:20:33+00:00
Response:
=====
serviceName | groupName | instanceSearchId | dnsName | instanceState | stackId
-----
ambari-server | | i-548c629c | ECS000031396.epam.com | running | EPM-CIT2AmbariServer-ee
ambari-agent | hgroup1 | i-8a913070 | ECS000031398.epam.com | running | EPM-CIT2AmbariCluster-t
ambari-agent | hgroup2 | i-3ef3d699 | ECS000031397.epam.com | running | EPM-CIT2AmbariCluster-t
ambari-agent | hgroup3 | i-765a8a40 | ECS000031399.epam.com | running | EPM-CIT2AmbariCluster-t
```

Figure 5 - or2ac -a describe command response

- **--action stop** – this action allows to stop all Ambari cluster instances at once

```
or2ac -c testcl -p DEMOPRO -r EPAM-BY1 -a stop
Are you sure you want to stop Ambari cluster? Type "yes" for confirmation: yes
Date: 2016-02-10T09:20:47+00:00
Response:
=====
instanceId | dnsName | privateIp | state | created
-----
i-3ef3d699 | ECS000031397.epam.com | 10.6.133.148 | stopping | 2016-02-09T15:16:54+00:00 |
i-765a8a40 | ECS000031399.epam.com | 10.6.133.151 | stopping | 2016-02-09T15:16:56+00:00 |
i-8a913070 | ECS000031398.epam.com | 10.6.129.241 | stopping | 2016-02-09T15:16:55+00:00 |
```

Figure 6 - or2ac -a stop command response

- **--action start** – this action allows to start all the stopped Ambari cluster instances and all the services in Ambari:

```

or2ac -c testcl -p DEMOPRO -r EPAM-BY1 -a start
Date: 2016-02-10T09:23:00+00:00
Response:
=====
instanceId | state |
=====
i-3ef3d699 | starting |
-----
i-765a8a40 | starting |
-----
i-8a913070 | starting |
-----
    
```

Figure 7 - or2ac -a start command response

6.2 DOCKER SERVICE ON AZURE

Please be informed that currently Docker service malfunctioning on Azure can be evidenced. This is a temporary issue that will be solved as soon as we switch to the latest Docker version (which will be done by the next Orchestration update).

Meanwhile, by following [this link](#), you can find the instructions on Docker Swarm.

7 SECURITY UPDATES

EPAM Cloud is constantly growing and becomes more distributed, engaging increasing number of projects and users, available regions and managed resources, etc.

This takes a number of enterprise-level questions to the new level. New challenges come in the fields of management, auditing, and, as one of the most essential ones – security.

With the beginning of the year, we started cooperating with the Security Department in order to improve the existing Cloud Security system according to the coming changes.

EPAM Cloud team carefully gathered all the feedbacks and suggestions from our users and colleagues, and as a result, came up with the Security Update roadmap, that is described in details on our [Feature Requests](#) page, where you can find the details on the coming and implemented changes, together with estimated deadlines.

Although the process of Cloud Security improvement has been started quite recently, we are glad to inform that some of the planned changes have already been implemented and are coming with Orchestration v.2.1.63.

7.1 AWS SECURITY GROUPS CHANGES

AWS Security group is a solution that allows to control traffic on virtual servers. Each security group includes up to 50 rules that are used to control the traffic rules for the instances, associated with the group.

For AWS instances managed by Orchestrator, these rules specify the list of EPAM IP addresses by which the traffic exchange can be performed.

Starting from February 13, 2015, security group rules change for instances in AWS regions. This allows to provide access to AWS instances from all EPAM offices at once.

All new instances, created with either EPAM or AWS tools, will get four security groups assigned to them by default. Three of the security groups include allowed IPs from EPAM offices in the respective regions. The fourth one is empty and can be customized by request to provide external access:

Security Group Name	Covered Regions
epam-world	US, Canada, Kazakhstan, China, India, Armenia
epam-europe	Offices in Europe
epam-by-ru	Offices in Russia and Belarus
Customer	Customers and custom IPs

In most cases, the change does not require any additional actions from user sides.

However, some adjustments can be needed in case you requested custom rules for your project.

7.2 SCHEDULED AND INITIATED NESSUS SCANNING

EPAM Orchestrator has its internal tools to monitor infrastructure events in Cloud, to check permissions and to detect situations when users leave projects, active in Cloud.



Orchestrator gathers and analyzes information covering these areas, and detects vulnerable points, which are aggregated in Weekly Vulnerability Reports ([Section 7.4](#)).

Besides this, recently, we started integration with [Nessus Vulnerability Scanner](#), one of the leading solutions in security scanning field.

EPAM Orchestrator sends scanning requests to one of Nessus scanners automatically in the following cases:

- Scheduled scanning starts each Saturday, at 00:00 AM. Nessus scanner checks all the instances hosted in AWS and in EPAM's DMZ.
- Orchestrator detects one of the following events when processing logs from EPAM Cloud and AWS logs provided by CloudTrail service:
 - An AWS security group includes an IP which does not belong to the list of EPAM addresses.
 - A security group includes 0.0.0.0/0 IP
 - A security group change is detected before a schedule execution



Additional scanning will not be initiated if security group changes are detected on a VM that has already been exposed to Internet.

Moreover, a VM's Owner and the manager of the project to which the VM is assigned, can request additional scanning of a specific VM by submitting a request to the [Support](#) team. Before submitting the request, please make sure that the target VM has the Owner specified. You can also specify the type of scenario that should be used during the scanning

7.3 NESSUS SCAN REPORT

As soon as Nessus finishes scanning, it sends the report to projects' primary contacts and Cloud Support teams.

The report provides information on the top 5 vulnerabilities detected on the scanned resources, as well as the details on these vulnerabilities and the overall statistics on each of the scanned servers.

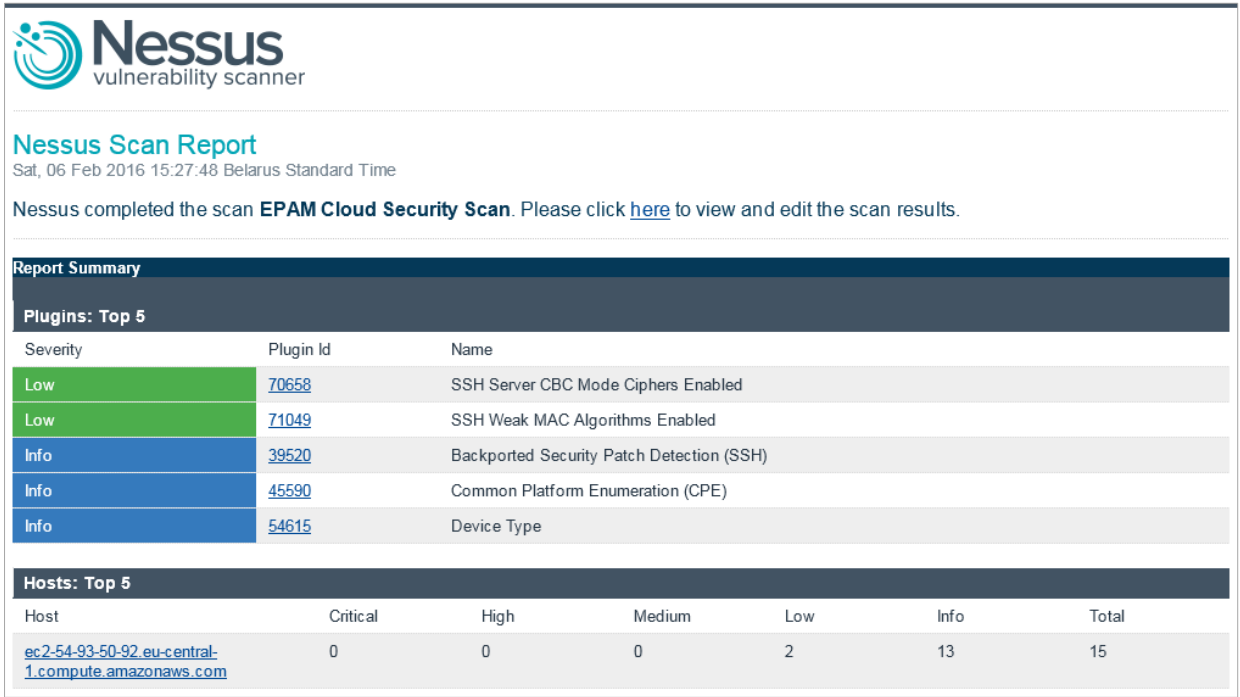


Figure 8 - Nessus Scan Report



Please note that vulnerabilities marked as Critical should be resolved by project teams within 30 days. Those with High severity should be resolved within 60 days.

In case you have any questions regarding the detected vulnerabilities or their resolution, please contact the [Security](#) group.

7.4 EPAM WEEKLY VULNERABILITY REPORT


As it has been mentioned above, Orchestration performs a number of checks with its own tools. The process includes analyzing logs gathered within EPAM internal regions and coming from AWS CloudTrail service.

Some logged events are considered those that increase infrastructure vulnerability. They are:

- Security group was changed on an AWS instance
- An instance Owner was fired, but their resources are still active in Cloud
- An instance had to be stopped automatically, but it wasn't.

The information on such events is gathered, and, at the end of each week, Orchestrator delivers the Weekly Vulnerability report listing the detected issues.

The report includes the list of the instances on which vulnerabilities were detected, including the vulnerabilities descriptions.


Project: **DEMOPRO**
February 8, 2016

Zone	Security Group	Instance Id	Owner	Comment
AWS-EUCENTRAL	sg-4995	i-26e74		Security group was changed for instance i-26e74. A scan for vulnerabilities was started.

This resources were found during daily scan. Please check resources and Nessus scan report result.

Zone	Security Group	Instance Id	Owner	Comment
AWS-EUCENTRAL	sg-4995	i-26e74		Security group was changed for instance i-26e74. A scan for vulnerabilities was started.

This resources were found during monthly full scan for AWS resources. Please check resources and Nessus scan report result.

Please check email box later for detailed scan result!

Useful commands

```

-- or2din --project DEMOPRO --region <region> --instance <instanceId>
-- or2chow --project DEMOPRO --region <region> --instance <instanceId> --email <owner email>
-- or2dkey --project DEMOPRO --region <region>
                    
```

[Terms & Conditions](#). Copyright © 2016 EPAM Inc. All rights reserved.

Figure 9 - Weekly Vulnerability Report

Please pay attention to the weekly vulnerability report and take all the necessary actions to resolve the detected issues.

If you have any questions regarding vulnerabilities management, please contact the [Support L1.5 team](#).

8 KNOWLEDGE BASE UPDATES

After the main part of EPAM Cloud Documentation restructuring and optimization plan was finished, we concentrated on stabilizing the knowledge base and updating the FAQ sections according to our users requests.

Thus, we come up with the following updates:

- [Terms and Conditions](#) document was updated, formatting was changed.
- [Quick Start Guide](#) was updated with SSH connection and personal quotas details.
- [Cloud Services Guide](#) was updated with the information on RDB and Ambari services.
- [Maestro CLI User Guide](#) was updated according to the latest changes in Maestro CLI facilities

In addition, a number of [FAQ](#) questions were added and clarified.

Please note that the documentation is being under constant development and changes together with EPAM Cloud Orchestration. Feel free to address the [Cloud Consulting](#) team if you have any comments or suggestions on the knowledge base improvements.

TABLE OF FIGURES

Figure 1 - Manage Cloud Wizard	4
Figure 2 - Account Report	9
Figure 3 - or2dreg command output.....	9
Figure 4 - or2dreg command outputs in different modes	10
Figure 5 - or2ac -a describe command response	12
Figure 6 - or2ac -a stop command response	12
Figure 7 - or2ac -a start command response	13
Figure 8 - Nessus Scan Report	16
Figure 9 - Weekly Vulnerability Report.....	17

VERSION HISTORY

Version	Date	Summary
1.0	February 13, 2016	First published