



EPAM Cloud

SECURITY POLICY

EPM-CSUP – EPAM Cloud Service

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®.

EPAM Public | Effective Date: 12-Mar-2018

Related Artifacts	
Ref.	Name
https://epa.ms/cloud-doc-terms	EPAM Cloud Terms and Conditions

Terms and Definitions	
EPAM Cloud Service (EPAM Cloud, Cloud)	A part of the existing EPAM ecosystem providing the possibility for project teams to manage virtual infrastructures in EPAM private regions and on external Cloud platforms via a self-service solution, as well as to monitor infrastructure performance and events, collect logs, process Cloud-related billing, etc.
EPAM Orchestration	A complex application enabling EPAM Cloud Service performance.
Cloud Asset (Asset)	Any value, hosted in Cloud. This includes, but is not limited to, information, virtual servers, hardware servers.
Cloud Security (Security)	A set of techniques, rules and regulations, aimed to protect assets within EPAM Cloud.
Security issue	Conditions under which vulnerabilities can arise.
Security check	Measures and steps taken to detect security issues and vulnerabilities.
Project	A Project in terms of EPAM Systems organizational chart.
Cloud UI	A Web application designed to provide access to EPAM Cloud facilities.
Maestro Command Line (Maestro CLI)	Command line interface designed to provide access to EPAM Cloud facilities.
External user	EPAM Cloud service user who is not employed by EPAM Systems.
Cloud user (user)	An EPAM employee using EPAM Cloud service.
Cloud action (action)	An action aimed to modify a virtual infrastructure in Cloud.
Primary contacts	Project Manager, Delivery Manager
Secondary contact	Project Coordinator
VM Owner	The user acting as a contact point for an instance and responsible for the instance security.

CONTENTS

1	INTRODUCTION	4
1.1	THE SCOPE OF THE DOCUMENT	4
1.2	PURPOSE OF THE DOCUMENT	4
2	PARTIES DEFINITION	4
3	EPAM CLOUD SECURITY RULES AND REGULATIONS	5
3.1	MAIN POINTS	5
3.2	ACCESS TO EPAM CLOUD.....	5
3.2.1	General Points	5
3.2.2	Permissions.....	6
3.2.3	Access to VMs.....	6
3.2.4	Service Accounts	6
3.2.5	Simple User Account.....	6
3.2.6	Providing Access to External Users.....	7
3.2.7	Project Deactivation.....	7
3.3	VMS MANIPULATIONS, APPLICATIONS, AND DATA	7
3.4	NETWORK SECURITY.....	8
3.5	EVENTS AUDIT	8
3.6	USING EXTERNAL CLOUD PROVIDERS	9
3.6.1	Security in AWS.....	9
3.6.2	Security in Azure	10
3.6.3	Security in GCP	11
3.7	VULNERABILITIES DETECTION AND MANAGEMENT	12
3.7.1	Security checks	12
3.7.2	Vulnerabilities management	12
3.8	CLOUD E-MAILS AND NOTIFICATIONS	13

1 INTRODUCTION

1.1 THE SCOPE OF THE DOCUMENT

The document describes the main concepts of security in EPAM Cloud Service, specifies the main approaches, rules and regulations applied to ensure the security of Cloud assets. It applies to all Employees of EPAM Systems and related contractors or third party users (if any).

The owner and approver of this document is the Head of Global IT Operations. EPAM Cloud Consulting team is responsible for its maintenance.

1.2 PURPOSE OF THE DOCUMENT

The purpose of the document is to define the main security-related approaches in Cloud and the scopes of responsibility of all parties.

2 PARTIES DEFINITION

- 2.1. Cloud Users (Users): EPAM employees using EPAM Cloud facilities for project or personal needs. A person becomes a Cloud User as soon as at least one project they are assigned to is activated in Cloud.
- 2.2. Security Group: the team of EPAM employees, responsible for EPAM assets security.
- 2.3. Support Teams: all teams responsible for EPAM Cloud provisioning and maintenance.
- 2.4. Level 1.5 Support Team: EPAM Cloud team, responsible for Cloud infrastructure monitoring, escalation of complex issues to L2 Support Team, 24/7/365 availability, monitoring Cloud configuration and templates development, and other.
- 2.5. Level 2 Support Team: EPAM Cloud team, responsible for the development hardware servers, HP OO stack, HP CSA, OpenStack and their maintenance and development.
- 2.6. Level 3 Support Team: EPAM Cloud team, responsible for fixing issues in the following areas: UI usability, UPSA integration, ESP Integration, reporting and billing, product issues, template libraries.
- 2.7. Cloud Consulting Team: EPAM Cloud team, responsible for initial project onboarding, existing project migration, migration process help, providing answers for general and specific Cloud Computing questions, client communication on architecture, delivery of training materials, EPAM Cloud knowledge base development, acknowledging user feedback, reacting on and monitoring initial user requests.

The team, responsible for EPAM Cloud policies review.
- 2.8. License Group: the team of EPAM employees, responsible for licensing and licenses verification in EPAM.
- 2.9. Network Team: the team of EPAM employees, responsible for networking settings and related operations.

3 EPAM CLOUD SECURITY RULES AND REGULATIONS

3.1 MAIN POINTS

- 3.3.1. EPAM Cloud is subject to the security policies applied in EPAM Systems, as well as to service-specific security rules and tools.
- 3.3.2. EPAM Orchestration update is performed according to the Production Update Plan, created by EPAM Cloud Support L3 team.
- 3.3.3. EPAM Cloud Support teams notify users on upcoming service unavailability by delivering respective SINs (Service Interruption Notifications) beforehand.
- 3.3.4. If necessary, the user should take all the measures that would ensure the security of their Cloud assets after the SIN period.
- 3.3.5. The user can utilize EPAM Orchestration's auto-configuration facilities to configure their infrastructures. Both out-of-the-box and custom scripts can be used for this purpose.

3.2 ACCESS TO EPAM CLOUD

3.2.1 General Points

- 3.2.1.1. The access to EPAM Cloud is provided on the domain level (with ADFS).
- 3.2.1.2. A user can access and manage the infrastructure only on the projects they are assigned to.
- 3.2.1.3. User's access to EPAM Cloud facilities is possible only after the activation of the respective project in Cloud. The activation is performed by request and after the approval of the project's manager or coordinator. The projects are charged for Service usage.
- 3.2.1.4. User access to EPAM Cloud is provided via Cloud UI (<https://cloud.epam.com>) and Maestro CLI (https://cloud.epam.com/site/develop/maestro_c=l=i/maestro-cli.zip).
- 3.2.1.5. The access via Cloud UI is provided via EPAM SSO tool and is possible from both EPAM network and Internet.
- 3.2.1.6. The access via Maestro CLI is available only from within EPAM network.
- 3.2.1.7. The access via Maestro CLI is provided by a unique UID, created by EPAM Orchestrator based on the user's EPAM domain or PMC credentials, and stored into a special (default.cr) file and in Orchestration's database.
- 3.2.1.8. Each user is responsible for the safekeeping of their default.cr file. The file directory must not be shared for external access.
- 3.2.1.9. The UID generated by EPAM Orchestrator should be changed by user each 3 months. Otherwise, the UID gets expired and the user cannot access Orchestrator with this UID, until it is updated.
- 3.2.1.10. Maestro Command Line allows up to 5 login attempts. If the user makes 5 consecutive failed login attempts, they get blocked in Orchestration for 30 minutes. The lock is removed automatically 30 minutes after the first incorrect credentials input. Unlocking by request is impossible.
- 3.2.1.11. The user can perform operations, allowed by EPAM Cloud hybridization with external cloud providers, via Cloud UI, Maestro CLI, and native tools of the respective provider.
- 3.2.1.12. EPAM Cloud functions can be accessed by external users (the users who are not employees of EPAM) only in exceptional cases, by request and after specific approval from EPAM Global Information Security Head and the responsible Account manager.

3.2.1.13. Each EPAM Cloud user should keep to standard EPAM AD credentials rotation policy.

3.2.2 Permissions

3.2.2.1. The scope of actions available for each user in Cloud is defined by their permission settings.

3.2.2.2. The default set of permissions for each user depends on their project role, according to the map described on [User Permissions page/Account Management guide](#).

3.2.2.3. Project Manager, Project Coordinator, and Delivery Manager can customize permissions for specific users or role-based user groups by means of Cloud UI.

3.2.3 Access to VMs

3.2.3.1. Access to VMs in EPAM Regions is performed via RDP with Domain credentials (for Windows), via SSH (for Linux), or VNC Client (for Mac).

3.2.3.2. If a VM is created within the scope of a platform service provisioning, the access credentials can be generated by Orchestrator.

3.2.3.3. In case a user requests a Linux instance in EPAM-KZ1 region or a hardware Mac server, they must change the default login credentials before they start working on these servers.

3.2.3.4. Access to VMs in AWS is provided via SSH (for Linux) or by decrypted AWS password (for Windows).

3.2.3.5. Access to VMs in Azure is provided by credentials generated automatically at VMs creation. The credentials are not stored on Orchestrator's side.

3.2.3.6. Access to Linux VMs on GCP is performed with the SSH key, specified during the instance creation, and the user name which depends on the system family (user: ubuntu, user: centos, user: debian).

3.2.3.7. Access to Windows VMs on GCP is performed under the Administrator user name, and the password, retrieved with the or2console command call (which should include an SSH key of 2048 size).

3.2.4 Service Accounts

3.2.4.1. A service account can be created by request to the Cloud Support L1.5 team in order to facilitate CI/CD processes on the project.

3.2.4.2. A service account name should comply with the following syntax:
auto_<project_name>_<comment>@epam.com

3.2.4.3. A service account can access Maestro CLI and API.

3.2.4.4. The access is provided to a service account by a unique UID, created by EPAM Orchestrator based on the account's credentials, and stored into a special (default.cr) file and in Orchestration's database.

3.2.4.5. The UID generated by EPAM Orchestrator should be changed by the account owner each 12 months. Otherwise, the UID gets expired and the user cannot access Orchestrator with this UID, until it is updated.

3.2.5 Simple User Account

3.2.5.1. A simple user account is an account created manually by request to the Cloud Support team.

- 3.2.5.2. A simple user account is linked to a specific project.
- 3.2.5.3. A simple user account is created based on the existing EPAM service account, or for an external user, who needs to have access to EPAM Cloud.
- 3.2.5.4. A simple user account creation should be approved by the Project Manager.
- 3.2.5.5. A simple user account has limited access to EPAM Cloud, and the set of the provided permissions is based on the details of the user creation request.
- 3.2.5.6. A simple user account expires in 12 months after creation.

3.2.6 Providing Access to External Users

- 3.2.6.1. An external user can get access to viewing and managing virtual infrastructures of a project only by request from the project authorities (Project manager, Account Manager, Project Coordinator, Delivery Manager).
- 3.2.6.2. The external user permissions are defined by the user requestor, who should specify the list of permission groups to which the user should be assigned.
- 3.2.6.3. Each external user should be added to EPAM AD and assigned to the target project by project authorities before access to EPAM Cloud is granted to such user.
- 3.2.6.4. The external user account expires in 12 months after creation.

3.2.7 Project Deactivation

- 3.2.7.1. A project can be deactivated in Cloud by special request to the Cloud Support team.
- 3.2.7.2. All the project virtual resources should be terminated or migrated before the project is deactivated in Cloud.
- 3.2.7.3. When a project status is set to CLOSED in UPSA, the project is automatically deactivated in Cloud.
- 3.2.7.4. In case a project has virtual resources at the moment when the project closure request is submitted, the Cloud Support team contacts the project responsible persons to clarify whether the resources should be terminated or migrated, and acts according to the provided decision.

3.3 VMS MANIPULATIONS, APPLICATIONS, AND DATA

- 3.3.1. The applications, data, and settings included to default Cloud images, are verified by Enterprise admins and IT Security team according to corporate security policy.
- 3.3.2. VM owner, Project Manager, Project Coordinator, and Delivery Manager are responsible for the securing and safekeeping of the data stored in project virtual infrastructure.
- 3.3.3. The user is responsible for all changes and customizations on the VMs under EPAM Orchestrator's control, unless this changes are applied by Cloud Support Team or Security Group.
- 3.3.4. The applications and data added to VMs by the user, as well as used via VMs, must comply with corporate licensing and security standards.
- 3.3.5. License-related rights and permissions are controlled by the License Management Support team.

- 3.3.6. A custom image can be imported to EPAM Orchestration for a specific project, by request to EPAM Support Portal. Before the image is imported, it is subjected to security check by the Security Group and License group. The import procedure is held by the Cloud Support L1.5 team.
- 3.3.7. VMs and other virtual resources are terminated by the user on the self-service basis.
- 3.3.8. The user can request assistance from Cloud Support L1.5 team in case they encounter any issues with VMs termination.
- 3.3.9. In exceptional/emergency cases, Cloud Support L1.5 team can restore a terminated VM from the recycle bin within 7 days after the VM termination.

3.4 NETWORK SECURITY

- 3.4.1. By default, all the VMs run in EPAM regions, are created in a default VLAN (Virtual Local Area Network).
- 3.4.2. EPAM Cloud Support L1.5 team can move a VM to a custom VLAN by request. After a VM is moved to a custom VLAN, it cannot be returned to the default one.
- 3.4.3. By default, Cloud VMs in EPAM regions are available only from EPAM network.
- 3.4.4. VMs can be exposed to Internet by request to EPAM Service Desk, according to one of the scenarios, described by the Security Group, and available in EPAM knowledge base by [this link](#).
- 3.4.5. The user should review the exposure scenarios and perform all the necessary preparations before submitting the exposure request.
- 3.4.6. The exposure of a VM to Internet is performed according to the following procedure:
 - a. The Security Group verifies that the VM meets all the Cloud and Corporate security requirements.
 - b. In special cases, Security Group verifies additional security-related solutions and approaches.
 - c. Cloud Support L1.5 team places the VM to the DMZ.
 - d. Cloud Support L1.5 team assigns an external IP, provided by EPAM Network team, to the VM. The connection details are sent to the VM Owner via email.

3.5 EVENTS AUDIT

- 3.5.1. EPAM Orchestrator logs all the events related to users' actions in EPAM Cloud, performed via CLI, API, or Cloud UI.
- 3.5.2. The information about the events is stored during 100 days.
- 3.5.3. The user can access the information on the events in their projects with both Maestro CLI and Cloud UI.
- 3.5.4. EPAM Orchestrator does not store logs on events that were performed bypassing Orchestrator.
- 3.5.5. Cloud Support L1.5 team can address AWS, Azure, or GCP Support to request help in investigating events that were performed bypassing Orchestrator.

3.6 USING EXTERNAL CLOUD PROVIDERS

- 3.6.1. User's access to an external platform's facilities is possible only after the activation of the respective project on this platform. The activation is performed by request and after the approval of the project's manager or coordinator.
- 3.6.2. The access to external Cloud providers' facilities via EPAM Orchestrator is enabled with Cloud UI and Maestro CLI by the same credentials as those used for private EPAM regions.
- 3.6.3. The access to native tools of external Cloud providers is provided by request to the users who have respective permissions, and if it is justified by project needs.
- 3.6.4. People who got access to native tools of external Cloud providers are personally responsible for the access credentials (login/password) to these tools.

3.6.1 Security in AWS

- 3.6.1.1. All VMs created in AWS are not available from outside EPAM network by default.
- 3.6.1.2. All VMs created in AWS, by default, have a set of security groups which allow to access these VMs from EPAM Offices. One security group is dedicated to custom rules, set up according to project needs.
- 3.6.1.3. In emergency cases, the Cloud Support team can edit or remove a custom security group without preliminary notice, if this group carries a security threat to the Cloud-based infrastructure.
- 3.6.1.4. VMs can be exposed to Internet by request to EPAM Service Desk. The exposure is performed in following steps:
 - a. The Security Group verifies that the VM meets all the Cloud and Corporate security requirements.
 - b. In special cases, Security Group verifies additional security-related solutions and approaches.
 - c. To establish access from Internet, Cloud Support L1.5 team sets up the VM's security groups.
- 3.6.1.5. AWS instances of t1.micro type cannot be exposed to Internet.
- 3.6.1.6. Security group changes can be performed either by request to Cloud Support l1.5 team or by users who have an IAM user with the respective permissions.
- 3.6.1.7. A user can get access to AWS management console via EPAM SSO, or by requesting an IAM user access.
- 3.6.1.8. The AWS access via EPAM SSO provides the user with the permissions, determined by their project roles.
- 3.6.1.9. IAM user access to AWS can be granted temporarily (automatically by a respective call to Orchestrator, if the user has the respective permission) or permanently (by request to Cloud Support L1.5 team, after approval from the respective Project Manager).
- 3.6.1.10. Temporary IAM access to AWS is cancelled after 60 minutes idle.
- 3.6.1.11. Permanent IAM User credentials should be rotated each 90 days.
- 3.6.1.12. Permanent IAM User accounts must have multi-factor authentication mechanism activated. Virtual MFA device usage is recommended.

- 3.6.1.13. In case a permanent IAM User account does not have multi-factor authentication activated, EPAM Cloud Support teams can block (delete) it without preliminary notice.
- 3.6.1.14. By default, IAM users have no permissions to create IAM users and manage security groups. The creation of new IAM users (including IAM roles creation) and security groups management are under the responsibility of the Cloud Support groups with close cooperation with the IT security team.
- 3.6.1.15. Additional permissions can be granted to IAM users only by grounded request.
- 3.6.1.16. All IAM User names should comply with the syntax: <domain_name>@epam.com.
- 3.6.1.17. Any IAM User should be assigned to a unit (project member or auto user) belonging to a specific project, which is marked in UPSA as active.
- 3.6.1.18. An IAM user access owner is responsible for all actions performed under their IAM user account, and their consequences.
- 3.6.1.19. In case a permanent IAM user account is inactive for over 30 days, it can be removed, with prior notification to the IAM account owner.
- 3.6.1.20. All AWS instances, except t1.micro type, are subject to Nessus security scanning, triggered by Orchestrator regularly or in case specific threatening events are detected.
- 3.6.1.21. AWS instances of t1.micro type are not scanned by Nessus, either automatically or manually.
- 3.6.1.22. VM's owner can request additional scanning of a specific VM.
- 3.6.1.23. Authorization to Linux instances can be performed only via SSH keys.
- 3.6.1.24. EPAM Cloud Team and Security Group can establish additional monitoring over events in AWS in order to detect threatening activities.
- 3.6.1.25. If Orchestrator detects unexpected or unusual events in AWS, a respective warning is sent to the project teams and Security Group and/or respective Cloud Support groups.
- 3.6.1.26. All abuse notifications from AWS should be answered immediately and resolved within one day. VM Owners, projects primary and secondary contacts are responsible for this.
- 3.6.1.27. Cloud Support team can block the project AWS account in case if an AWS abuse issue is not resolved within one day.

3.6.2 Security in Azure

- 3.6.2.1. A user can access virtual infrastructures in Azure via EPAM Orchestrator, if their project is activated in Azure via EPAM Cloud.
- 3.6.2.2. When a project is activated in Azure, a network security group is created for the new Azure subscription in order to allow access only for specified EPAM IP-addresses.
- 3.6.2.3. In emergency cases, the Cloud Support team can edit or remove a custom security group without preliminary notice, if this group carries a security threat to the Cloud-based infrastructure.
- 3.6.2.4. The user can get access to the Azure portal, in terms of self-service, in case they have the respective permissions level.
- 3.6.2.5. The user's access to the project subscription in Azure is revoked within 24 hours after the user's project membership is cancelled.
- 3.6.2.6. Project VMs in one region are connected into one network so that they can reach each other by internal IPs.
- 3.6.2.7. EPAM Cloud Team and Security Group can establish additional monitoring over events in Azure in order to detect threatening activities.
- 3.6.2.8. All abuse notifications from Azure should be answered immediately and resolved within one day. VM Owners, projects primary and secondary contacts are responsible for this.

- 3.6.2.9. Cloud Support team can block the project Azure account in case if an Azure abuse issue is not resolved within one day.
- 3.6.2.10. Project VMs can be exposed to Internet by request to EPAM Service Desk. The exposure is performed in following steps:
 - a. The Security Group verifies that the VM meets all the Cloud and Corporate security requirements.
 - b. To establish access from Internet, Cloud Support L1.5 team sets up the VM's security groups.
 - c. The access to Azure Portal is provided automatically for users by a respective call to Orchestrator, in case the user has the permissions to perform such call.

3.6.3 Security in GCP

- 3.6.3.1. All VMs created in GCP are not available from outside EPAM network by default.
- 3.6.3.2. All VMs created in GCP are affected by the project firewall that allows accessing the VMs only from EPAM Offices (check by IP addresses).
- 3.6.3.3. In emergency cases, the Cloud Support team can edit or remove custom firewall rules without preliminary notice, if these rules carry a security threat to the Cloud-based infrastructure.
- 3.6.3.4. VMs hosted in GCP can connect to each other only by internal IP address or host name.
- 3.6.3.5. VMs can be exposed to Internet by request to EPAM Service Desk. The exposure is performed in following steps:
 - a. The Security Group verifies that the VM meets all the Cloud and Corporate security requirements.
 - b. In special cases, Security Group verifies additional security-related solutions and approaches.
 - c. The Cloud Support L1.5 team sets up the firewall rules to establish access from Internet to the VM.
- 3.6.3.6. Firewall changes can be performed either by request to Cloud Support l1.5 team or by users who have access to the GCP console.
- 3.6.3.7. The temporary access to the GCP can be retrieved by a user who has proper permissions, by a respective call to Orchestrator.
- 3.6.3.8. The temporary access expires at 2 AM UTC after the access granting.
- 3.6.3.9. Permanent access to GCP via an IAM can be provided by request to Cloud Support L1.5 team, after approval from the respective Project Manager.
- 3.6.3.10. A GCP IAM can be granted only to employees with job function level 2 and higher.
- 3.6.3.11. The IAM access to a project is provided by linking the project and the IAM account. One IAM account can have access to several projects.
- 3.6.3.12. All IAM User names should comply with the syntax: <domain_name>@epam.com.
- 3.6.3.13. Permanent IAM User accounts must have multi-factor authentication mechanism activated.
- 3.6.3.14. In case a permanent IAM User account does not have multi-factor authentication activated, EPAM Cloud Support teams can block (delete) it without preliminary notice.
- 3.6.3.15. IAM user access owner is responsible for all actions performed under their IAM user account, and their consequences.
- 3.6.3.16. The IAM access to a project is cancelled automatically within 24 hours after the account owner leaves this project, or by the Project Manager's request to the Cloud Support L1.5 team.
- 3.6.3.17. A GCP IAM account cannot be removed or suspended, unless the employee is dismissed.

- 3.6.3.18. GCP instances are not subject to automatic or manually triggered Nessus scans. VM owner is responsible for the resource security.
- 3.6.3.19. Authorization to Linux instances can be performed only via SSH keys. The user name depends on the system family (user: ubuntu, user: centos, user: debian, etc).
- 3.6.3.20. Windows instances are run without a key, but to get the password, the user needs to run the or2console command and provide a key (required size: 2048).
- 3.6.3.21. EPAM Cloud Team and Security Group can establish additional monitoring over events in GCP in order to detect threatening activities.
- 3.6.3.22. All abuse notifications from GCP should be answered immediately and resolved within one day. VM Owners, projects primary and secondary contacts are responsible for this.
- 3.6.3.23. Cloud Support team can block the project GCP account in case if an GCP abuse issue is not resolved within one day.

3.7 VULNERABILITIES DETECTION AND MANAGEMENT

3.7.1 Security checks

- 3.7.1.1. EPAM Cloud Support and Security teams can perform security check operations on users' assets in Cloud without advance notice.
- 3.7.1.2. Security checks of Cloud VMs and assets can be performed both manually (by Cloud Support teams and/or Security group) or automatically (by tools and applications properly configured for this purpose).
- 3.7.1.3. Security checks include scanning by Nessus Vulnerability Scanner, which can be performed according to one of the predefined policies (see Appendix A).
- 3.7.1.4. Security checks performed within VM exposure procedures are performed by the Security Group only.
- 3.7.1.5. Security check tools are approved by EPAM Global Information Security Head and Global IT Security Manager, and set up by Cloud Support L3 team and Security Group.
- 3.7.1.6. Security check procedures are defined and approved by EPAM Global Information Security Head.
- 3.7.1.7. Security check results are delivered to Cloud Support teams, Security Group, and the responsible project persons (VM owners, primary and secondary contacts).
- 3.7.1.8. The security checks include checking the security groups and detecting those that can lead to security vulnerabilities (the rules are described in Appendix B).

3.7.2 Vulnerabilities management

- 3.7.2.1. VM owners, Project Managers, Delivery Managers, Project Coordinators are responsible for resolving issues and vulnerabilities detected on the VMs assigned to their projects.
- 3.7.2.2. If security scanning detects vulnerabilities or issues on Cloud VMs, the users related to problem resources get notified on this automatically, or manually.
- 3.7.2.3. Each user is responsible for fixing vulnerabilities and issues on their related resources in terms of self-service.
- 3.7.2.4. The urgency of issues and vulnerabilities resolving depends on the vulnerability/issue type:
 - a. Vulnerabilities:
 - Critical: 30 days

- High: 60 days
 - Medium: 60 days
 - b. Issues:
 - Critical: 7 days
 - High: 10 days
 - Medium: 10 days
- 3.7.2.5. In case a user does not resolve the issue or vulnerability they are responsible for, Security Team informs user's manager on the issue.
- 3.7.2.6. If necessary, Security Team provides assistance with vulnerabilities and issues resolving, by appropriate request to EPAM Support Portal and within the scope of their responsibilities.
- 3.7.2.7. In case the reported issues or vulnerabilities are not fixed within the specified time, Cloud Support L1.5 team and the Security Group can take security measures on the threat isolation. These measures can vary from instance isolation or suspension to full blocking, depending on the results of evaluation of the potential threat and the business needs.

3.8 CLOUD E-MAILS AND NOTIFICATIONS

- 3.8.1. EPAM Orchestration and Cloud support teams deliver Cloud-related notifications to the members of the projects, activated in Cloud, in order to assure sufficient informational support on the events, changes and issues (including security) related to EPAM Cloud in general, and project VMs, particularly.
- 3.8.2. Each notification is addressed to the users who can be influenced by the action, event, or issue described in the message, or to whom the provided information is considered to be important.
- 3.8.3. The user can unsubscribe from notifications or set up filtering rules in their email client. In this case, the user is responsible for any consequences that result from the delivered information loss.
- 3.8.4. The user should keep to corporate information security rules, when they share the information and the materials delivered in Cloud-related emails.

APPENDIX A. NESSUS SECURITY SCANNING POLICIES

Policy Name	Policy Description	Scan Type
EPM-Srv-noWebApp-noCreds (Default)	The policy is configured for servers that do not host web applications. Operating system and Databases are checked. Web applications and networking equipment scanning is not included. No authorization is needed.	Black Box
Wrk-noCreds	The policy is configured for workstations scanning. Databases, networking equipment, web applications scanning is not included. Accounts are not used for scanning.	Black Box
Wrk-Creds	The policy is configured for workstations scanning. Databases, networking equipment, web applications scanning is not included. Local administrator account is used for scanning. Authorization allows to detect more issues on the target VM.	White Box
EPM-Srv-WebApp-noCreds	The policy is configured for web application servers check. Operating system, database, and web applications check is included. Networking equipment is not scanned. The procedure takes more time than the one where web applications are not scanned.No accounts are used for scanning.	Black Box
EPM-Srv-WebApp-Clickjacking	The policy is configured for web application servers check and provides quick urgent scanning of web applications for Clickjacking vulnerability only, with maximum page number and depths crawl. No authorization is needed for this type of scan. The policy is configured for web application servers check and provides quick urgent scanning of web applications for Clickjacking vulnerability only, with maximum page number and depths crawl. No authorization is needed for this type of scan.	Black Box
EPM-FULL-Creds_ANY_	The scanning is performed without any limitations and optimization measures. All elements are scanned. All accounts that have ever been created since the VM run, are used during the procedure. The whole procedure can take significant time.	White Box
EPM-Discovery	The policy is configured to perform quick scanning of any network range, in order to detect new assets and unauthorized devices. The scanning allows to create the network map. Vulnerabilities check is not performed.	Black Box
EPM-Srv-noWebApp-Creds*	The policy is configured for servers that do not host web applications. Operating system and Databases are checked. Web applications and networking equipment scanning is not included. Different accounts are used for scanning.	White Box
EPM-Windows-Torrents*	The policy is configured for quick scanning Windows workstations and servers for torrents and P2P applications. No other vulnerabilities will be detected. Authorization is needed.	White Box

EPM-Srv-WebApp-Creds*	The policy is configured for web application servers check. Operating system, database, and web applications check is included. Networking equipment is not scanned. The procedure takes more time than the one where web applications are not scanned. Different accounts can be used for scanning.	White Box
EPM-Lan-Creds*	The policy is configured for networking equipment check. Operating system, databases, web applications are not scanned. Different accounts are used for scanning.	White Box
EPM_bitlocker*	The policy is configured to check whether Windows servers and workstations have encrypting enabled. Scanning can detect the encrypted disks and the TPM module. No other vulnerabilities checks are included. Scanning needs authorization.	White box
* These policies need authentication for scanning. If you want your VM be scanned with these policies, please submit a respective request to the Security Team,		

APPENDIX B. SECURITY GROUP CHECK RULES

During the security groups check, the following ports are reviewed:

Protocol	Port	Source	Recommendation	Checked source	Vulnerable
Inbound					
TCP/UDP	21	ANY (even if it will be exposed for particular IPs)	Don't use 21 port. EPAM has FTP servers that can be used for information exchange.	0.0.0.0/0	TRUE
				10.23.14.145/32	TRUE
				46.133.203.215/32	TRUE
	22	0.0.0.0/0	Expose to EPAM IPs only.	0.0.0.0/0	TRUE
				10.23.14.145/32	FALSE
				46.133.203.215/32	TRUE
	80	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	137	0.0.0.0/0	Expose to EPAM IPs only.	0.0.0.0/0	TRUE
				10.23.14.145/32	FALSE
				46.133.203.215/32	TRUE
	443	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	445	0.0.0.0/0	Expose to EPAM IPs only.	0.0.0.0/0	TRUE
				10.23.14.145/32	FALSE
				46.133.203.215/32	TRUE
	3389	0.0.0.0/0	Expose to EPAM IPs only.	0.0.0.0/0	TRUE
				10.23.14.145/32	FALSE
				46.133.203.215/32	TRUE
	6881	ANY (even if it will be exposed for particular IPs)	Don't use port 6881. EPAM prohibits exposing this port without exceptions	0.0.0.0/0	TRUE
				10.23.14.145/32	TRUE
				46.133.203.215/32	TRUE
8000	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE	
			46.133.203.215/32	FALSE	
			10.23.14.145/32	FALSE	
8001	0.0.0.0/0	Expose to particular external IPs	0.0.0.0/0	TRUE	
			46.133.203.215/32	FALSE	
			10.23.14.145/32	FALSE	
8080	0.0.0.0/0			0.0.0.0/0	TRUE

Protocol	Port	Source	Recommendation	Checked source	Vulnerable		
			Expose to particular external IPs.	46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		
				0.0.0.0/0	TRUE		
			8081	0.0.0.0/0	Expose to particular external IPs.	46.133.203.215/32	FALSE
						10.23.14.145/32	FALSE
						0.0.0.0/0	TRUE
	9000	0.0.0.0/0	Expose to particular external IPs.	46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		
				0.0.0.0/0	TRUE		
	9443	0.0.0.0/0	Expose to particular external IPs.	46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		
				0.0.0.0/0	TRUE		
ANY	rest of 0-65535	0.0.0.0/0	Define particular ports for exposing and external range of IPs.	0.0.0.0/0	TRUE		
Outbound							
TCP/UDP	25	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE		
				46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		
	465	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE		
				46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		
	587	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE		
				46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		
	993	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE		
				46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		
	995	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE		
				46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		
	2525	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE		
				46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		
	2526	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE		
				46.133.203.215/32	FALSE		
				10.23.14.145/32	FALSE		

REVISION HISTORY					
Ver.	Description of Change	Author	Date	Approved	
				Name	Effective Date
0.1	Initial draft	Svitlana Ostnek	March, 2016	Dzmitry Pliushch Andrii Gusiev Aliaksei Brusiantsov	28-Mar-2016
0.5	Prepared for publishing	Dzmitry Pliushch Aliaksei Brusiantsov	April, 2016	Eli Feldman Ivan Tabaravets Sasha Kazlouski Sergey Sinkevich Sergey Sakhonenko Sreenu Pasunuri Yuri Rybkin	11-Apr-2016
0.9	Updated with AWS-related changes	Dzmitry Pliushch Aliaksei Brusiantsov	April, 2016	Eli Feldman Ivan Tabaravets Sasha Kazlouski Sergey Sinkevich Sergey Sakhonenko Sreenu Pasunuri Yuri Rybkin	20-Apr-2016
1.0	First published	Dzmitry Pliushch Aliaksei Brusiantsov	May, 2016	Eli Feldman Ivan Tabaravets Sasha Kazlouski Sergey Sinkevich Sergey Sakhonenko Sreenu Pasunuri Yuri Rybkin	07-May-2016
1.1	Updated with IAM users management details. Updated project contacts.	Dzmitry Pliushch Aliaksei Brusiantsov	October, 2016	Sergey Sinkevich Sreenu Pasunuri Mikhail Kazouski Aliaksei Brusiantsov Dzmitry Pliushch	22-Oct-2016
1.2	Updated with the GCP info	Andrei Paulau	July, 2017	Sergey Sinkevich Sreenu Pasunuri Ivan Tabaravets Aliaksei Brusiantsov	15-Jul-2017
1.3	Added information on Service Accounts, providing access to external users, and updated details on credentials updates Updated information on Security Checks, added Appendix A and B	Andrei Paulau	August, 2017	Sergey Sinkevich Sreenu Pasunuri Ivan Tabaravets Aliaksei Brusiantsov	10-Aug-2017
1.4	Reviewed access regulations. Updated permissions info. Added Simple User Account section. Updated Network Security section with exposure recommendations. AWS IAM users provisioning and management updated. Azure portal access details added. Security Groups	Andrei Paulau	February, 2018	Sergey Sinkevich Sreenu Pasunuri Ivan Tabaravets Aliaksei Brusiantsov	23-Feb-2017

REVISION HISTORY					
Ver.	Description of Change	Author	Date	Approved	
				Name	Effective Date
1.5	QA review	Oleksandr Dmytriyeu	05-Mar-2018	Sergey Sinkevich Sreenu Pasunuri Ivan Tabaravets Aliaksei Brusiantsov	05-Mar-2018
1.6	Specified EPAM Cloud consulting as a team, responsible for the policy review and update.	Andrei Paulau	06-Mar-2018	Sergey Sinkevich Sreenu Pasunuri Ivan Tabaravets Aliaksei Brusiantsov	12-Mar-2018