Cloud Admin Portal/API (version 1.0)

**Cloud Service Label: IaaS, PaaS, SaaS**

Description

The cloud admin portal/API is accessible from any place in the world. By design, all Azure and AWS resources are theoretically accessible from this universal interface. Only identity credentials stand in the way of anyone accessing anyone else’s resources and information. The circumstance is not much improved for unclassified government only clouds, which also widely expose their portal and API and again rely on credentials to arbitrate access.

An adversary may use a portal with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, the GCP Command Center can be used to view all assets, findings of potential security risks, and to run additional queries, such as finding public IP addresses and open ports.

Passwords to gain access to the portal/API can be stolen from administrator or privileged user workstations that interact with the portal/API through traditional harvesting techniques like spear phishing. 2FA greatly reduces the chance that such attacks will work. However even with 2FA, it may be possible for adversaries to use the token obtained after 2FA authentication for some brief period of time to gain access to your resources, if they have access to the machine that was granted access by 2FA. Within AWS, other accounts without 2FA may still be granted access to some or all of your resources through IAM roles. The portal/APIs themselves are complex web applications that change constantly. As such they may have intermittent security flaws that enable adversaries to by-pass the credential process and gain access to your resources.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Azure Portal Vulnerability | Azure API was theorized to have a significant flaw checking credentials for certain API routines based on successful demonstrations on Azure Stack Hub version of the portal. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| [Multi-factor Authentication](https://attack.mitre.org/mitigations/M1032) | | Use multi-factor authentication for user and privileged accounts. Do not manage Cloud portals from machines that perform user email and web browsing tasks. All users should be required to utilize two factor authentication. |
|  | *AWS* | This can be enforced by first creating a policy that would prohibit actions except those that allow a user to change their password or manage 2FA, then attaching a policy to a group that includes all user accounts where they can be allowed all access if they sign in with 2FA. Once these actions are completed it should be tested to verify the access is given correctly. To see full details on how to complete this view AWS documentation at: **https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\_users-self-manage-mfa-and-creds.html.** |
|  | *Azure* | This can be done by creating a MFA registration policy. It can than be assigned to all users (with the ability to exclude some if need be, but is not recommended). Make sure once the policy is created and added to users that it is then being enforced, once enforced it should be tested for verification. To see full details on how to complete this view Azure documentation at: **https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy.** |
|  | *GCP* | This can be done by first enabling it on the current account being used by admin to assign the roles, then enable two factor on an instance by instance or project by project basis, then assigning the requirements based on IAM roles and applying it to all users. To see full details on how to complete this view Azure documentation at: **https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication.** |
| Least Privilege | | All access given to users in the cloud environment should be assigned by the necessary privileges needed for team members to complete their job responsibilities. Ensure that temporary access tokens are issued rather than permanent credentials, especially when access is being granted to entities outside of the internal security boundary. |
|  | *AWS* | To implement least privilege in an AWS environment IAM policies will be used. This gives the ability to allow users to perform list, read, write, permissions management, or tagging actions. AWS suggests utilizing *last accessed information* and A*WS CloudTrail event history* to get a better understanding of privileges that might be needed or reduced based on a specific role. Full details can be found at **https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege.** |
|  | *Azure* | To implement least privilege in an Azure environment Azure Active Directory roles will be used. Azure outlines different tasks and the least privileged role that are suggested to be associated with the task. Those details can be found at: **https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-delegate-by-task.** To learn how to assign specific roles it can be done via the Azure Active Directory Portal. Instructions on how to assign roles can be found here: **https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-manage-roles-portal.** |
|  | *GCP* | To implement least privilege in GCP it is recommended to use predefined roles (which allow for granular access permissions) instead of primitive roles (roles/owner, roles/editor, and roles/viewer). Full details on the difference between types of roles can be found here: **https://cloud.google.com/iam/docs/understanding-roles.** To assign these roles IAM service accounts are used and complete details can be found at: **https://cloud.google.com/iam/docs/using-iam-securely#least\_privilege.** |

Detection

Monitor account activity logs to see actions performed and activity associated with the cloud service management console. Some cloud providers, such as AWS and Azure, provide distinct log events for login attempts to the management console.

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Create Log Metric Filters and Alarms for AWS | To create a metric filter and alarm:   1. Create a metric filter that checks for IAM policy changes and the *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter and SNS topic created in steps 1 and 2 respectively |
| Monitor Activity in AWS Account | Various services in AWS offer logging features that allow for detection capabilities. These include CloudFront, CloudTrail, CloudWatch, Config, and S3. |
| Monitor for Suspicious Activity in Azure | Azure AD can generate anomaly reports than can be run on a daily basis. Azure AD Identity Protection show current risks in its dashboard and provides daily email summary notifications. Policies can also be configured to alert to specific issues. |
| Create Log Metric Filters and Alarms for CloudTrail | To create a metric filter and alarm:   1. Create a filter that checks for CloudTrail changes and the specific *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic that the alarm will notify 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter from step 1 and SNS topic in step 2 |
| Create Activity Log Alerts in Azure | To create log activity alerts for deletion in the Azure Console:   1. Navigate to *Monitor’ / ‘Alerts* 2. Select *Manage alert rules* 3. Click on the Alert *Name* where Condition contains *operationName equals Microsoft.Network/networkSecurityGroups/securityRules/delete* 4. Hover a mouse over *Condition* to ensure it is set to *Whenever the Administrative Activity Log “Delete Security Rule (networkSecurityGroups/securityRules)” has “any” level with “any” status and event is initiated by “any*” |
| Create, View, and Manage Activity Alerts in Azure Monitor | To create a log alert in the Azure portal:   1. Select **Monitor -> Alerts** 2. Select **New alert rule** of the **Alerts** window 3. Provide information in **Define alert condition** 4. Provide details in **Define alert details** 5. Specify action group for new alert rule under **Action group**, or create a new action group with + **New group** 6. Select **Yes** for the **Enable rule upon creation** option 7. Select **Create alert rule**   To view and manage alerts:   1. Select **Monitor -> Alerts -> Manage alert rules** 2. Select the rule you want to modify and double-click to edit the rule options 3. Click **Save** |
| Azure Resource Manager Templates | Azure Resource Manager templates in the format of JSON files that can be used to configure metric alerts in Azure Monitor. These templates can be used for simple static and dynamic threshold metric alerts, availability tests, and monitoring multiple resources. |
| Enable CloudTrail across all regions in AWS | To enable CloudTrail across all regions:   1. Sign into the AWS Management Console and open the CloudTrail console 2. Click on *Trails* 3. Set necessary Trails to All option in the I column 4. Click on a trail via the link *Name* column 5. Set *Logging* to *ON* 6. Set *Apply trail to all regions* to *Yes* |
| Configure log profile to capture activity logs for all regions in Azure | To set up activity logs for all regions:   1. Navigate to Azure console 2. Go to *Activity log* 3. Select *Export* 4. Select *Subscription* 5. Check *Select all* in *Regions* 6. Select *Save* |

References

1. <https://aws.amazon.com/blogs/security/how-do-i-protect-cross-account-access-using-mfa-2/>. Accessed February 15, 2020
2. <https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-i/>. Accessed February 15, 2020
3. <https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_users-self-manage-mfa-and-creds.html>. Accessed July 28, 2020
4. <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy>. Accessed July 28, 2020
5. https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication. Accessed July 28, 2020
6. <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege>. Accessed July 29, 2020
7. <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-delegate-by-task>. Accessed July 29, 2020
8. <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-manage-roles-portal>. Accessed July 29, 2020
9. <https://cloud.google.com/iam/docs/understanding-roles>. Accessed July 29, 2020
10. <https://cloud.google.com/iam/docs/using-iam-securely#least_privilege>. Accessed July 29, 2020