Loss of Availability (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Adversaries may attempt to disrupt essential components or systems to prevent the delivering of IT services. Adversaries may leverage native Cloud API functionality to delete resources such as VMs, storage accounts or data bases. They can also use native portal capabilities to remove access accounts’ ability to control Cloud resources. As Amazon and Azure offer more edge integrated services, this disruption could also affect physical device operation and sensor collections.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Co-Residence Identification and Resource Exhaustion | As pointed out in a research papers written by the University of California San Diego, WPI and the Massachusetts Institute of Technology, co-residence is the process of identifying cloud instances that share the same underlying physical infrastructure, despite being separated virtually. Once virtual machine co-residence has been identified it may be possible to attempt to exhaust resources of the physical host to degrade the performance of other clients VM on the host |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Utilize Templates | | Whenever possible use templates to define and create your cloud infrastructure and store a copy of those templates outside the cloud - preferably in a version controlled repo. Templates enable the quick creation of virtual infrastructure and settings to their desired state. |
| Utilize Backups | | Cloud backup services can be used to restore cloud data from a certain point of time before data was altered or destroyed. |
|  | AWS | To have a data backup in an AWS environment, AWS Backup can be used. This is a way to centralize and automate backup services, as well as enforce backup policies that might include aspects such as encryption requirements and audit the activity on the backup. The backup service is PCI and ISO compliant and is HIPAA eligible. There are different backups available: cloud-native (across all AWS services) and hybrid (across AWS and on premise data). To accomplish this a backup plan needs to be created that defines criteria on how to manage the backups (ie. how frequently to backup, how long to keep the backups, etc.), then the resources to backup are assigned. Once the resources are backed up they can be minored, modified, or restored. To get started with this information can be found here: [**https://aws.amazon.com/backup/getting-started/**](https://aws.amazon.com/backup/getting-started/)**.** For more information on the service refer here: [**https://aws.amazon.com/backup/**](https://aws.amazon.com/backup/)**.** Access to and introduction video can be found here: [**https://www.aws.training/Details/Video?id=29646**](https://www.aws.training/Details/Video?id=29646)**.** |
|  | Azure | To have a data backup in an Azure environment, Azure Backup service can be used. This allows for on-premises, Azure VMs, Azure file shares, SQL server in Azure VMs, and SAP HANA databases in Azure VMs to be backed up. There are multiple ways this can be accomplished; through the portal, PowerShell, CLI, and ARM template. From the portal a VM to be backed up can be selected, then enable to backup resource, start the backup job, monitor the backup job, and when you no longer need the deployment it can then be cleared up. Using PowerShell and CLI has the same steps (just accomplished through different commands) first a recovery service vault will be created, then the backup will need to be enabled for the service being backed up, then the backup job will need to be started, then monitored, and lastly clean up the deployment. Lastly, to deploy with the ARM template first the template has to be reviewed and edited as needed, then deploy the template, then the deployment must be validated by starting a backup job, monitoring it, and cleaning up the resources.  On this page multiple tutorials can be found for backing up specific resources: [**https://docs.microsoft.com/en-us/azure/backup/tutorial-backup-vm-at-scale**](https://docs.microsoft.com/en-us/azure/backup/tutorial-backup-vm-at-scale). Full details on how to deploy backup services utilizing different resources can be found below:  Portal: [**https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal**](https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal)  PowerShell: [**https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-powershell**](https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-powershell)  CLI: [**https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-cli**](https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-cli)  ARM Template: [**https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-template**](https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-template) |
| Provide redundant servers/services | | Azure and AWS make it easy to assign redundant servers/services to the same workload that can be located in different locales and be automatically spun up based on performance criteria |

Detections

|  |  |
| --- | --- |
| **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. Wait a minute! A fast, Cross-VM attack on AES Gorka Irazoqui, Mehmet Sinan Inci, Thomas Eisenbarth, and Berk Sunar Worcester Polytechnic Institute, Worcester, MA, USA – Accessed August 6,2020
2. https://cseweb.ucsd.edu/~savage/papers/CCS09.pdf. Accessed July 2, 2020.