Managing and Auditing Organizational Migration to the Cloud
About Me

Brian Greidanus
bgreidan@telasasecurity.com

• 18+ years of security and compliance experience delivering consulting and managed services to enterprises, governments and universities.

• Currently:
  • Strategic and technical consulting
  • Program measurement and metrics development
  • Awareness training
Executive Summary

• Introduction to cloud computing

• Shared responsibility models

• Review of security controls and auditing capabilities for IaaS cloud providers:
  • Amazon Web Services
  • Microsoft Azure
Audience Input

• How many are familiar with cloud concepts, like IaaS, PaaS, SaaS?
• How many are using cloud providers today?
• How many are actively auditing cloud environments?
Introduction to Cloud Computing
Categories of Cloud Providers

Infrastructure as a Service

• Provide base hardware, networking, virtualization, where customers can build their own operating system and application stack.

• Major vendors include:
  • Amazon Web Services
  • Microsoft Azure
  • Google Cloud

Platform as a Service

• Provide operating system, middleware, development environment, where the customer is responsible for data and development of the application layer.

• PaaS vendors/offerings include:
  • AWS Elastic Beanstalk
  • Heroku
  • Google App Engine
Categories of Cloud Providers

Software as a Service

• Provide a complete computing stack, where the customer is only responsible for the configuration of an application layer.

• SaaS vendors/applications include:
  • Salesforce.com
  • Box.net
  • Office365
  • Google Apps
Similarities in Auditing Cloud and Legacy Environments

• Primary resources in public cloud environments are virtualized instances of existing technologies – servers, operating systems, databases, web applications

• Concepts of security architecture, identity management, network access control are all the same
Differences in Auditing between Cloud and Legacy Environments

- Cloud environments are dynamic, vs. more static legacy environments.
- Cloud-based environments include a dedicated management layer (akin to a hypervisor in virtual environments).
- There are numerous new services in cloud environments.
- Native API-based cloud services can be used to collect, filter, and analyze logs.
- Native cloud services can be used to perform auditing functions.
- Reliable asset management data.
Auditing Goals are the Same in Cloud as in Legacy

- Are our standards and practices in cloud environments aligned with organizational policy and relevant regulatory requirements?

- Can we successfully demonstrate the alignment of our standards and practices to internal and external auditors?
Standard Practices in Cloud Environments are Evolving

- There are multiple ways to accomplish many tasks

- Current pace of release/change is dizzying

- Auditors must prepare for rapid rate of change over next several years
Cloud Provider Shared Responsibility Model
AWS IaaS Shared Responsibility Model
Shared Responsibility by Type of Service

Source:
Shared Responsibility – Validate Vendor Adherence

Auditors need validation that cloud providers are honoring commitments that they make in the Shared Responsibility model.

- **Amazon AWS** – Resources provided in AWS Artifact
- **Microsoft Azure** – Resources provided in the Microsoft Trust Center
AWS Artifact

SOC 1 and SOC 2 reports
PCI attestation of compliance
Microsoft Trust Center

Audit Reports
Resources to help information security and compliance professionals understand cloud features, and to verify technical compliance and control requirements.

New and Archived Audit Reports
Use these reports to stay current on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

<table>
<thead>
<tr>
<th>Archived Compliance Reports</th>
<th>FedRAMP Reports</th>
<th>GRC Assessment Reports</th>
<th>ISO Reports</th>
<th>PCI DSS</th>
<th>SOC Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure - ISO 27001 Certificate - 11.2.2017</td>
<td>This documents details scope of ISO 27001 audit assessments for Microsoft’s Azure.</td>
<td>2018-02-21</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ISO reports
Key Reports Available

• SOC 1
• SOC 2
• PCI-DSS
• ISO 27001
• ISO 27018
Our Responsibility

How do we audit what we are responsible for?

This presentation will focus on tools and capabilities available to auditors in Azure and AWS
Amazon Web Services
AWS Overview

• Introduction / key terms

• AWS Security Domains
Introduction / Key Terms
Amazon Web Services (AWS) is a cloud Infrastructure-as-a-Service (IaaS) platform offering computing, data storage, and other IT solutions and utilities for modern organizations.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2</td>
<td>Elastic Compute Cloud is a web-based service that allows users to initiate virtual machines to provide compute capacity.</td>
</tr>
<tr>
<td>Instance</td>
<td>An EC2 Instance is a virtual server in EC2. So, “I am running 10 Windows Server 2008 EC2 instances” means “I have 10 virtual Windows 2008 Servers in Amazon EC2”.</td>
</tr>
<tr>
<td>Lambda</td>
<td>Serverless computing platform that runs code (Javascript, python, Java, C++, Go) in response to events and manages all underlying computing</td>
</tr>
<tr>
<td>S3</td>
<td>Simple Storage Service – data storage and retrieval.</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Private Cloud is a virtual network dedicated to an AWS account.</td>
</tr>
</tbody>
</table>
AWS Security Domains
AWS Security Domains – Well Architected Framework

- Identity and Access Management
- Detective Controls
- Infrastructure Security
- Data Protection
- Incident Response
• Identity and Access Management
• Detective Controls
• Infrastructure Protection
• Data Protection
• Incident Response
Identity and Access Management

- Protecting AWS Credentials
- Fine-grained Authorization

Key AWS Services
- IAM
- AWS Organizations
IAM
IAM Security Status

Key components of IAM security are highlighted in main menu.
Secure Root Account and Create Individual Users

AWS Root account is the account (e-mail address) used to set up AWS.

AWS Root account should not be used regularly.

Instead root account should be used to create users and groups within AWS IAM, and those users should be used for regular AWS authentication.
Delete Root Access Keys

Access keys are utilized for programmatic access to AWS (SDK, CLI) – root access keys should never be used.
Enable Multifactor Authentication

Numerous multi-factor authentication options available to secure AWS accounts.
Group Permissions in AWS

Hundreds of default permission policies available.
Group Permissions in AWS

Group policies are JSON files that specify the allowed actions for the group.
IAM Password Policy

Later we will use AWS Config to ensure enforcement.
AWS Organizations
AWS Organizations

AWS Organizations enables:

• Centralized management of accounts (into Organizational Units - OU)

• Centralized policy enforcement (via Service Control Policies – SCP).
AWS Organizations enables:

- Develop custom organization structures and rules
- Apply policies using custom organization structure
- Only permit use of authorized services (Mandatory access control)
AWS Organizations – Policy Creation

Policy creation (similar to Policy creation in IAM) to grant/deny permissions to OU groups.
• Identity and Access Management

• Detective Controls

• Infrastructure Protection

• Data Protection

• Incident Response
Detective Controls

• Capture and Analyze Logs

• Integrate auditing tools with notification and workflow

Key AWS Services

• S3
• Config
• CloudTrail
• CloudWatch
AWS S3
What is S3?

Simple Storage Service - simple Amazon Web Services interface that to store and retrieve data.

S3 Buckets are directories for S3 storage objects.
S3 Bucket Creation

Numerous options when creating buckets:

- Versioning
- Access logging
- Encryption
- Setting permissions for AWS and external users
Proper S3 Bucket Security

Improper S3 bucket permissions have been in the news recently.

Can use AWS Config (discussed later) to help ensure appropriate S3 bucket security.
CloudTrail
CloudTrail logs calls from AWS functions and sends logs to S3 storage buckets.

CloudTrail can capture logs from all major AWS services.
<table>
<thead>
<tr>
<th>Category</th>
<th>Business Description</th>
<th>eventSource</th>
<th>eventName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root access</td>
<td>Any activity from the root account</td>
<td>*</td>
<td>user=root</td>
</tr>
<tr>
<td>Route 53</td>
<td>Any change to external DNS</td>
<td>route53.amazonaws.com</td>
<td>*</td>
</tr>
<tr>
<td>S3</td>
<td>Delete an S3 storage bucket</td>
<td>s3.amazonaws.com</td>
<td>DeleteBucket</td>
</tr>
<tr>
<td>S3</td>
<td>Create a new S3 storage bucket</td>
<td>s3.amazonaws.com</td>
<td>CreateBucket</td>
</tr>
<tr>
<td>S3</td>
<td>Set (modify) the ACLs on the S3 storage bucket</td>
<td>s3.amazonaws.com</td>
<td>SetBucketAccessControlPolicy</td>
</tr>
<tr>
<td>IAM</td>
<td>Add a new user to AWS console</td>
<td>iam.amazonaws.com</td>
<td>CreateUser</td>
</tr>
<tr>
<td>IAM</td>
<td>Remove a user from AWS console</td>
<td>iam.amazonaws.com</td>
<td>DeleteUser</td>
</tr>
<tr>
<td>IAM</td>
<td>Add a user to a group</td>
<td>iam.amazonaws.com</td>
<td>AddUserToGroup</td>
</tr>
<tr>
<td>IAM</td>
<td>Attach a policy to a user</td>
<td>iam.amazonaws.com</td>
<td>AttachUserPolicy</td>
</tr>
<tr>
<td>IAM</td>
<td>Create an access key for a user</td>
<td>iam.amazonaws.com</td>
<td>CreateAccessKey</td>
</tr>
<tr>
<td>IAM</td>
<td>Create a new managed policy for an AWS account</td>
<td>iam.amazonaws.com</td>
<td>CreatePolicy</td>
</tr>
<tr>
<td>IAM</td>
<td>Create a new policy version (update a policy)</td>
<td>iam.amazonaws.com</td>
<td>CreatePolicyVersion</td>
</tr>
<tr>
<td>EC2</td>
<td>Create a route table</td>
<td>ec2.amazonaws.com</td>
<td>CreateRouteTable</td>
</tr>
<tr>
<td>EC2</td>
<td>Creates a route in a route table</td>
<td>ec2.amazonaws.com</td>
<td>CreateRoute</td>
</tr>
<tr>
<td>EC2</td>
<td>Create a VPC</td>
<td>ec2.amazonaws.com</td>
<td>CreateVpc</td>
</tr>
<tr>
<td>EC2</td>
<td>Creates an Amazon EBS-backed AMI</td>
<td>ec2.amazonaws.com</td>
<td>CreateImage</td>
</tr>
<tr>
<td>EC2</td>
<td>Create PVC Peering connection between two VPCs - can belong to another AWS account</td>
<td>ec2.amazonaws.com</td>
<td>CreateVpcPeeringConnection</td>
</tr>
<tr>
<td>EC2</td>
<td>Create a new network ACL</td>
<td>ec2.amazonaws.com</td>
<td>CreateNetworkAcl</td>
</tr>
<tr>
<td>EC2</td>
<td>Create an entry in a network ACL</td>
<td>ec2.amazonaws.com</td>
<td>CreateNetworkAclEntry</td>
</tr>
<tr>
<td>EC2</td>
<td>Create a network interface in the specified subnet</td>
<td>ec2.amazonaws.com</td>
<td>CreateNetworkInterface</td>
</tr>
<tr>
<td>EC2</td>
<td>Create a new security group in a specified VPC</td>
<td>ec2.amazonaws.com</td>
<td>CreateSecurityGroup</td>
</tr>
<tr>
<td>EC2</td>
<td>Create a subnet in an existing VPC</td>
<td>ec2.amazonaws.com</td>
<td>CreateSubnet</td>
</tr>
<tr>
<td>EC2</td>
<td>Create a VPN Gateway</td>
<td>ec2.amazonaws.com</td>
<td>CreateVpnGateway</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete a network ACL</td>
<td>ec2.amazonaws.com</td>
<td>DeleteNetworkAcl</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete a network ACL entry from an ACL</td>
<td>ec2.amazonaws.com</td>
<td>DeleteNetworkAclEntry</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete a network Interface</td>
<td>ec2.amazonaws.com</td>
<td>DeleteNetworkInterface</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete Route from routing table</td>
<td>ec2.amazonaws.com</td>
<td>DeleteRoute</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete route table</td>
<td>ec2.amazonaws.com</td>
<td>DeleteRouteTable</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete Internet Gateway</td>
<td>ec2.amazonaws.com</td>
<td>DeleteInternetGateway</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete Security Group</td>
<td>ec2.amazonaws.com</td>
<td>DeleteSecurityGroup</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete Snapshot from a volume</td>
<td>ec2.amazonaws.com</td>
<td>DeleteSnapshot</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete a specified subnet</td>
<td>ec2.amazonaws.com</td>
<td>DeleteSubnet</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete a volume</td>
<td>ec2.amazonaws.com</td>
<td>DeleteVolume</td>
</tr>
<tr>
<td>EC2</td>
<td>Delete a VPC</td>
<td>ec2.amazonaws.com</td>
<td>DeleteVpc</td>
</tr>
</tbody>
</table>
CloudTrail Event History

CloudTrail event history

<table>
<thead>
<tr>
<th>Event time</th>
<th>User name</th>
<th>Event name</th>
<th>Resource type</th>
<th>Resource ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-04-21, 12:24:30 AM</td>
<td>root</td>
<td>AttachRolePolicy</td>
<td>IAM Role and 1 more</td>
<td>AWSManagement</td>
</tr>
<tr>
<td>2018-04-21, 12:24:39 AM</td>
<td>root</td>
<td>AttachRolePolicy</td>
<td>IAM Role and 1 more</td>
<td>AWSManagement</td>
</tr>
<tr>
<td>2018-04-21, 12:24:35 AM</td>
<td>root</td>
<td>CreateRole</td>
<td>IAM Role</td>
<td>AROAOP</td>
</tr>
<tr>
<td>2018-04-21, 12:24:35 AM</td>
<td>root</td>
<td>CreateRole</td>
<td>IAM Role</td>
<td>AROAOP</td>
</tr>
<tr>
<td>2018-04-21, 12:24:35 AM</td>
<td>root</td>
<td>CreateRole</td>
<td>IAM Role</td>
<td>AROAOP</td>
</tr>
<tr>
<td>2018-04-21, 12:24:35 AM</td>
<td>root</td>
<td>CloudFormationStack</td>
<td>CloudFormation Stack</td>
<td>am.aws.com</td>
</tr>
<tr>
<td>2018-04-21, 12:03:43 AM</td>
<td>root</td>
<td>PutEvaluations</td>
<td>EC2 SecurityGroup</td>
<td>sg-6c53f5k</td>
</tr>
<tr>
<td>2018-04-21, 12:03:43 AM</td>
<td>root</td>
<td>PutEvaluations</td>
<td>EC2 SecurityGroup</td>
<td>sg-6c53f5k</td>
</tr>
<tr>
<td>2018-04-20, 11:35:59 AM</td>
<td>root</td>
<td>CreateCluster</td>
<td>EC2 VPC and 1 more</td>
<td>vpc-1281f</td>
</tr>
<tr>
<td>2018-04-20, 11:35:45 AM</td>
<td>root</td>
<td>CreateSecurityGroup</td>
<td>EC2 SecurityGroup</td>
<td>sg-6c53f5k</td>
</tr>
<tr>
<td>2018-04-20, 11:10:01 AM</td>
<td>root</td>
<td>PutEvaluations</td>
<td>EC2 VPC and 1 more</td>
<td>vpc-1281f</td>
</tr>
</tbody>
</table>
AWS Config
What is AWS Config?

AWS Config is a service that enables assessment, auditing, and evaluation of AWS resource configuration.

AWS Config continuously monitors and records AWS resource configurations and automatically evaluates recorded configurations against desired configurations.
Sample Config Policies (1 of 2)

**ec2-instances-in-vpc**
Checks whether your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.

**EC2**

**ec2-volume-inuse-check**
Checks whether EBS volumes are attached to EC2 instances. Optionally checks if EBS volumes are marked for deletion when an instance is terminated.

**EC2**

**eip-attached**
Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.

**EC2**

**elb-acm-certificate-required**
This rule checks whether the Elastic Load Balancer(s) uses SSL certificates provided by AWS Certificate Manager. You must use an SSL or HTTPS listener with your Elastic Load Balancer.

**ElasticLoadBalancing**

**encrypted-volumes**
Checks whether EBS volumes that are in an attached state are encrypted.

**EC2**

**iam-password-policy**
Checks whether the account password policy for IAM users meets the specified requirements.

**IAM**, **Periodic**

**iam-user-group-membership-check**
Checks whether IAM users are members of at least one IAM group.

**IAM**

**iam-user-no-policies-check**
Checks that none of your IAM users have policies attached. IAM users must inherit permissions from IAM groups or roles.

**IAM**

**rds-multi-az-support**
Checks whether high availability is enabled for your RDS DB instances.

**RDS**
Sample Config Policies (2 of 2)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rds-storage-encrypted</td>
<td>Checks whether storage encryption is enabled for your RDS DB instances.</td>
</tr>
<tr>
<td>s3-bucket-logging-enabled</td>
<td>Checks whether logging is enabled for your S3 buckets.</td>
</tr>
<tr>
<td>s3-bucket-server-side-encryption-enabled</td>
<td>Checks whether the S3 bucket policy denies the put-object requests that are not encrypted using AES-256 or AWS KMS.</td>
</tr>
<tr>
<td>restricted-ssh</td>
<td>Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.</td>
</tr>
<tr>
<td>s3-bucket-public-read-prohibited</td>
<td>Checks that your S3 buckets do not allow public read access.</td>
</tr>
<tr>
<td>s3-bucket-public-write-prohibited</td>
<td>Checks that your S3 buckets do not allow public write access.</td>
</tr>
<tr>
<td>s3-bucket-ssl-requests-only</td>
<td>Checks whether S3 buckets have policies that require requests to use Secure Socket Layer (SSL).</td>
</tr>
<tr>
<td>root-account-mfa-enabled</td>
<td>Checks whether the root user of your AWS account requires multi-factor authentication for console sign-in.</td>
</tr>
<tr>
<td>s3-bucket-versioning-enabled</td>
<td>Checks whether versioning is enabled for your S3 buckets. Optionally, the rule checks if MFA delete is enabled for your S3 buckets.</td>
</tr>
</tbody>
</table>
Create Custom Config Rules
Public repositories of Config rules provide Lambda functions
Config Dashboard

Once rules are in place, the Config Dashboard provides continuous compliance reporting.
CloudWatch
CloudWatch Logs – Metrics and Rules

• **Monitor Logs from Amazon EC2 Instances in Real-time**—CloudWatch Logs uses log data for monitoring (such as "404" status codes in an Apache access log).

• **Monitor AWS CloudTrail Logged Events**—Create alarms in CloudWatch and receive notifications of API activity captured by CloudTrail.

• **Log Route 53 DNS Queries** - Use CloudWatch Logs to log information about the DNS queries that Route 53 receives.
Routing Events of Interest using a rules engine
• Identity and Access Management

• Detective Controls

• Infrastructure Protection

• Data Protection

• Incident Response
Infrastructure Protection

- Protecting network and host-level boundaries
- System security configuration and maintenance
- Enforcing service-level protection

Key AWS Services

- Amazon VPC
- AWS Systems Manager
- Amazon Inspector
Amazon VPC
A virtual private cloud (VPC) is a virtual network dedicated to an AWS account, logically isolated from other virtual networks in the AWS Cloud. AWS resources, such as Amazon EC2 instances, are launched in VPCs.
AWS Systems Manager
AWS Systems Manager

**EC2 Systems Manager State Manager** – define and maintain consistent operating system configurations.

**EC2 Systems Manager Inventory** – collect and query information about instances and installed software.

**EC2 Systems Manager Patch Manager** – Deploy operating system and software patches automatically across large groups of instances.
Amazon Inspector
Amazon Inspector Setup

Configure rules packages and scope
Amazon Inspector Outputs

Section 3: Findings Summary

This section lists the rules that generated findings, the severity of the finding, and the number of instances affected. More details about the findings can be found in the "Findings Details" section. Rules that passed on all target instances available during the assessment run are listed in the "Passed Rules" section.

3.1: Findings table - Common Vulnerabilities and Exposures-1.1

No findings were generated for this rules package.

3.2: Findings table - Runtime Behavior Analysis-1.0

<table>
<thead>
<tr>
<th>Rule</th>
<th>Severity</th>
<th>Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insecure client protocols (general)</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>Insecure server protocols</td>
<td>Informational</td>
<td>1</td>
</tr>
<tr>
<td>Unused listening TCP ports</td>
<td>Informational</td>
<td>1</td>
</tr>
</tbody>
</table>

3.3: Findings table - Security Best Practices-1.0

No findings were generated for this rules package.
• Identity and Access Management
• Detective Controls
• Infrastructure Protection
• Data Protection
• Incident Response
Data Protection

- Data classification
- Encryption/tokenization
- Protecting data at rest
- Protecting data in transit
- Data backup/replication

Key AWS Services

- Resource Tagging
- Amazon KMS
- Amazon CloudHSM
- AWS Certificate Manager
- Amazon Macie
Resource Tagging
Resource Tagging allows organizations to create custom identification scheme for resources.
Amazon KMS
AWS KMS provides encryption key management.
Created keys utilized in AWS services.
Amazon CloudHSM

Uses dedicated hardware security module (HSM) appliances within the AWS Cloud to help organizations meet regulatory and contractual compliance requirements.
AWS Certificate Manager
AWS Certificate Manager

Manage and deploy certificates for AWS resources
Amazon Macie
Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.
• Identity and Access Management
• Detective Controls
• Infrastructure Protection
• Data Protection
• Incident Response
Incident Response in AWS

Important concepts for Incident Response in AWS:

• Data classification

• Take image snapshots and store in S3/Glacier

• Ability to provision new, trusted environments where investigation can take place.
AWS Auditing and Compliance Resources
Center for Internet Security Benchmark

• Commonly cited benchmark

https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf
CIS Benchmark Automation

https://github.com/awslabs/aws-security-benchmark
AWS Well-Architected Framework

• Identity and Access Management
• Detective Controls
• Infrastructure Security
• Data Protection
• Incident Response
Microsoft Azure
What is Azure?

Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers.
# Mapping AWS and Azure Security Auditing Services

<table>
<thead>
<tr>
<th></th>
<th>AWS Service</th>
<th>Azure Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity and Access Management</td>
<td>IAM</td>
<td>Azure Active Directory Management Groups</td>
</tr>
<tr>
<td></td>
<td>AWS Organizations</td>
<td></td>
</tr>
<tr>
<td>Detective Controls</td>
<td>S3</td>
<td>Azure Security Center</td>
</tr>
<tr>
<td></td>
<td>Config</td>
<td>Alerts</td>
</tr>
<tr>
<td></td>
<td>CloudTrail</td>
<td>Logging and Monitoring</td>
</tr>
<tr>
<td></td>
<td>CloudWatch Logs</td>
<td>Storage Accounts</td>
</tr>
<tr>
<td></td>
<td>CloudWatch Events</td>
<td>SQL Server and SQL Databases</td>
</tr>
<tr>
<td>Infrastructure Protection</td>
<td>Amazon VPC</td>
<td>Networking</td>
</tr>
<tr>
<td></td>
<td>AWS Systems Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amazon Inspector</td>
<td></td>
</tr>
<tr>
<td>Data Protection</td>
<td>Resource Tagging</td>
<td>Key Vault</td>
</tr>
<tr>
<td></td>
<td>Amazon KMS</td>
<td>Storage Service Encryption</td>
</tr>
<tr>
<td></td>
<td>Amazon CloudHSM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AWS Certificate Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amazon Macie</td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>
Azure Active Directory
Azure Active Directory - Users and Group Permissions
Azure Active Directory - Multi-factor Authentication
Azure Active Directory - Guest User Permissions
Azure Activity Logs
Following types of logs are captured in Azure Activity Logs:

- **Administrative** - Contains the record of all create, update, delete, and action operations performed through Resource Manager, including creation of virtual machines, deletion of network security groups, changes to role-based access control.

- **Security** - Alerts generated by Azure Security Center. Examples of events from this category include "Suspicious double extension file executed", "Brute force SQL credentials".

- **Service Health** - Contains the record of service health incidents in Azure. (e.g. SQL Azure in East US is experiencing downtime.)

- **Alert** - This category contains the record of all activations of Azure alerts. An example of the type of event in this category is "CPU % on myVM has been over 80 for the past 5 minutes." A variety of Azure systems have an alerting concept -- you can define a rule and receive a notification when conditions match that rule.

- **Autoscale** - This category contains the record of any events related to the operation of the autoscale engine based on any autoscale settings defined in the subscription.

- **Recommendation** - These events offer recommendations for how to better utilize resources.
Azure Activity Logs

<table>
<thead>
<tr>
<th>OPERATION NAME</th>
<th>STATUS</th>
<th>TIME</th>
<th>TIME STAMP</th>
<th>SUBSCRIPTION</th>
<th>EVENT INITIATED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write LinkedServices</td>
<td>Succeeded</td>
<td>8 h ago</td>
<td>Wed May 02 2022</td>
<td>Test Sub</td>
<td>Windows Azure Security Resource Provider</td>
</tr>
<tr>
<td>Write LinkedServices</td>
<td>Succeeded</td>
<td>20 h ago</td>
<td>Tue May 01 2022</td>
<td>Test Sub</td>
<td>Windows Azure Security Resource Provider</td>
</tr>
<tr>
<td>Write LinkedServices</td>
<td>Succeeded</td>
<td>1 d ago</td>
<td>Tue May 01 2022</td>
<td>Test Sub</td>
<td>Windows Azure Security Resource Provider</td>
</tr>
<tr>
<td>Write LinkedServices</td>
<td>Succeeded</td>
<td>2 d ago</td>
<td>Mon Apr 30 2022</td>
<td>Test Sub</td>
<td>Windows Azure Security Resource Provider</td>
</tr>
<tr>
<td>Write LinkedServices</td>
<td>Succeeded</td>
<td>3 d ago</td>
<td>Sun Apr 29 2022</td>
<td>Test Sub</td>
<td>Windows Azure Security Resource Provider</td>
</tr>
<tr>
<td>Overallocate</td>
<td>Succeeded</td>
<td>3 d ago</td>
<td>Sun Apr 29 2022</td>
<td>Test Sub</td>
<td><a href="mailto:bgreidan@gmail.com">bgreidan@gmail.com</a></td>
</tr>
<tr>
<td>Start</td>
<td>Succeeded</td>
<td>3 d ago</td>
<td>Sun Apr 29 2022</td>
<td>Test Sub</td>
<td><a href="mailto:bgreidan@gmail.com">bgreidan@gmail.com</a></td>
</tr>
<tr>
<td>ListKeys</td>
<td>Succeeded</td>
<td>3 d ago</td>
<td>Sun Apr 29 2022</td>
<td>Test Sub</td>
<td><a href="mailto:bgreidan@gmail.com">bgreidan@gmail.com</a></td>
</tr>
</tbody>
</table>
Azure Security Center
Enabling Microsoft Monitoring Agent
Security Center – Data Collection

Four categories of Security Events.
Preconfigured tiers of event log granularity:

- **4624** – successful login (minimal and common)
- **4704** – A user right was assigned (common only)
Security configuration for entirety of Azure subscription.

Azure Security Center – Security policy
Security Center Policy Alerting Configuration

• **System updates** – retrieves a daily list of available security and critical updates from Windows Update or Windows Server Update Services.

• **Security configuration** – analyzes operating system configurations daily to determine issues that could make the virtual machine vulnerable to attack.

• **Endpoint Protection** - recommends endpoint protection be provisioned for all Windows virtual machines to help identify and remove viruses, spyware, and other malicious software.
• **Disk encryption** – recommends enabling disk encryption in all virtual machines to enhance data protection at rest.

• **Network security groups** – recommends network security groups be configured to control inbound and outbound traffic to VMs that have public endpoints. This policy also assesses inbound security rules to identify rules that allow incoming traffic.

• **Web application firewall** – Recommends that web application firewall be enabled for external facing web servers.
Security Center Policy Alerting Configuration

• **Next generation firewall** – Security Center discovers deployments for which a next generation firewall is recommended, and then you can set up a virtual appliance.

• **Vulnerability assessment** – enables Vulnerability assessment recommendations for virtual machines.

• **Storage encryption** – When this setting is enabled, any new data in Azure Blobs and Files will be encrypted.
Security Center Policy Alerting Configuration

• **JIT network access** – When enabled, Security Center locks down inbound traffic to Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic should be locked down.

• **Adaptive application controls** – Adaptive application controls help control which applications can run on your VMs located in Azure.

• **SQL auditing and threat detection** – When enabled, recommends auditing of access to Azure Database be enabled for compliance and also advanced threat detection, for investigation purposes.
SQL encryption – When this setting is enabled, it recommends that encryption at rest be enabled for your Azure SQL Database, associated backups, and transaction log files. Even if your data is breached, it will not be readable.
Alerts
Enabling Azure Alerting
SQL Servers and SQL Databases
Enabling SQL auditing and threat detection sends detection messages through Azure Security Center discussed earlier.
The following SQL Security Message Types are available in Azure Security Center:

- **Vulnerability to SQL Injection**: Triggered when an application generates a faulty SQL statement in the database - may indicate a possible vulnerability to SQL injection attacks.

- **Potential SQL injection**: Triggered when by an active exploit against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.

- **Access from unusual location**: Triggered by a change in the access pattern to SQL server, where someone has logged on to the SQL server from an unusual geographical location or unusual Azure data center.

- **Access from unfamiliar principal**: Triggered when there is a change in the access pattern to SQL server, where someone has logged on to the SQL server using an unusual SQL user.

- **Access from a potentially harmful application**: Triggered when potentially harmful application is used to access the database. In some cases, alert detects penetration testing in action. In other cases, the alert detects an attack using common attack tools.

- **Brute force SQL credentials**: Triggered by an abnormal high number of failed logins with different credentials. In some cases, the alert detects penetration testing. In other cases, the alert detects brute force attack.
Similar setting to physical SQL servers – use Active Directory authentication instead of local.
Networking
Networking Configuration

Inbound and outbound firewall rules and network segmentation
Azure Auditing and Compliance Resources
Azure Security Domains

CIS benchmarks for Azure and AWS are new, reflect a rapidly changing environment, and will evolve.