AMAZON WEB SERVICES

RISKRECON ASSESSMENT PLAYBOOK

A field guide and toolkit for assessing the security quality of Amazon Web Services deployments and operations

JUNE 2020

A playbook by RiskRecon, Inc. | WWW.RISKRECON.COM

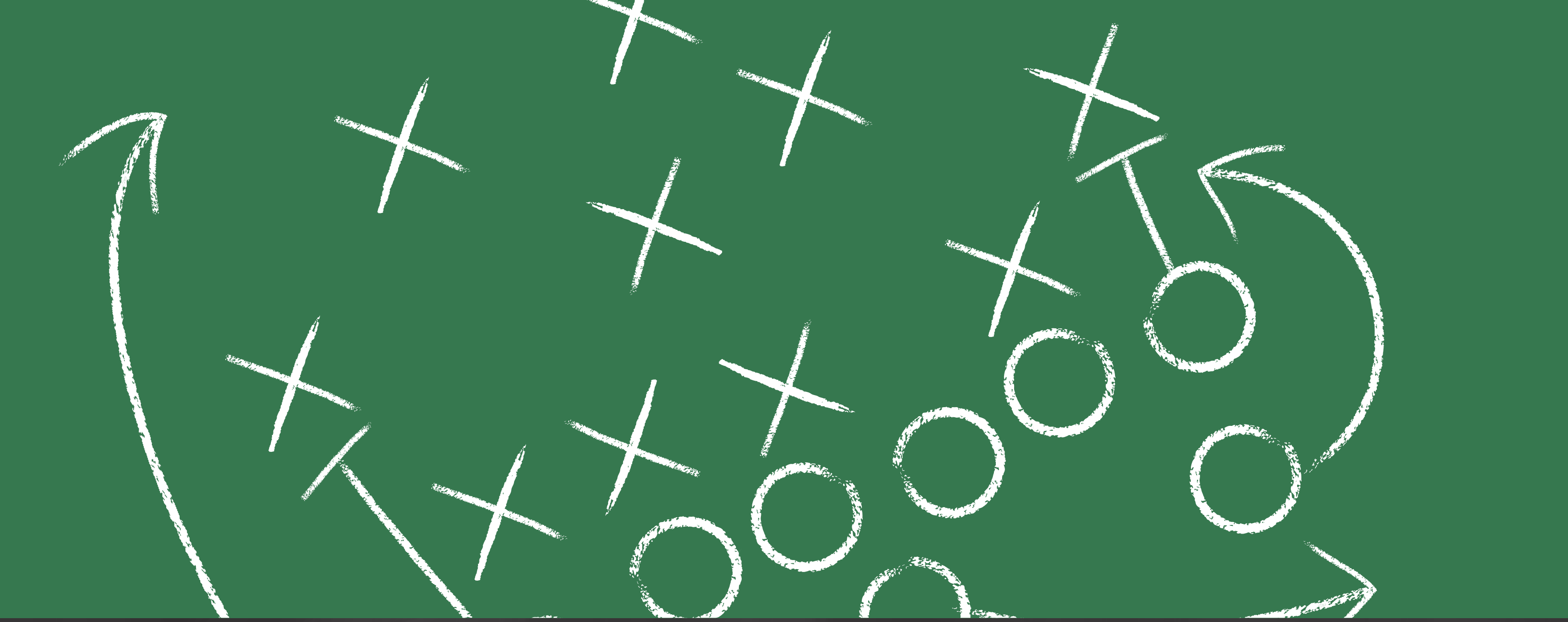
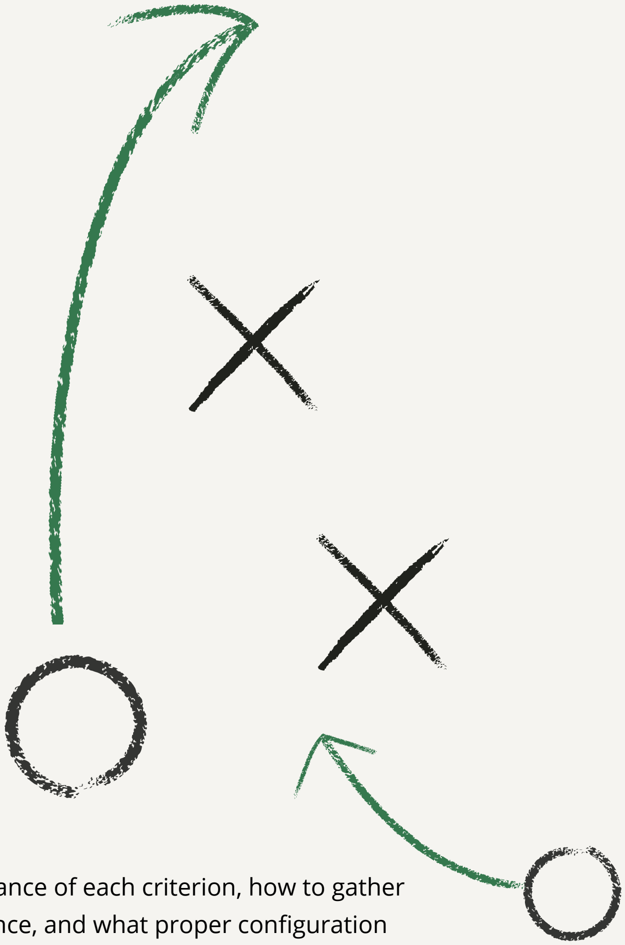


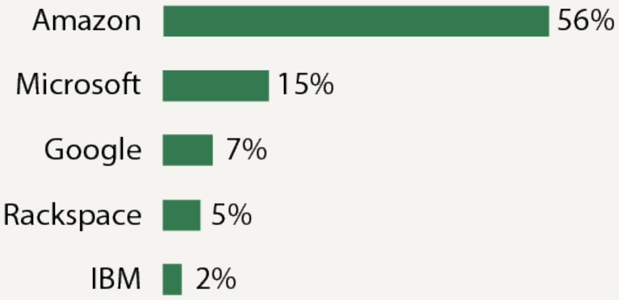
TABLE OF CONTENTS

INTRODUCTION



Achieving good third-party risk outcomes requires that your vendors operate secure cloud environments. According to RISKRECON'S 2019 CLOUD RISK SURFACE REPORT, 75% of organizations host at least one system with one of the top 5 cloud hosting providers. Amazon Web Services dominates all commercial clouds, hosting 56% of all Internet-facing cloud-hosted systems.

2019 Cloud Computing Marketshare



Where you have a lot of value at risk riding on your vendor's ability to maintain the security of their AWS environment, generic questions like, "Do you detect and monitor for security intrusion attempts?" are not enough. Achieving good outcomes requires getting into the right details and making sure the details are done right.

To that end, RiskRecon has developed the Amazon Web Services Core Assessment Playbook. This Playbook provides a step-by-step methodology for assessing the quality of the essential security configurations of any AWS deployment. Here you will find essential AWS environment assessment security criteria, explanations of the importance of each criterion, how to gather related evidence, and what proper configuration looks like. RiskRecon's AWS Core Security Assessment Questionnaire accompanies this Playbook.

RiskRecon believes that third-party assessments founded on objective evidence are the most effective way to achieve good risk outcomes. This AWS Assessment Playbook and the accompanying Questionnaire do just that - they help you achieve better risk outcomes by providing you the knowledge and tools for objectively assessing the security quality of any Amazon Web Services deployment.

ACKNOWLEDGEMENTS

The AWS Core Security Assessment Playbook was developed by experts in the fields of AWS security and third-party cybersecurity assessment from RiskRecon and Stratum Security. The project was led by Jonathan Ehret, a widely known third-party risk expert and RiskRecon's Vice President of Strategy and Risk. Jonathan was assisted by RiskRecon's head of AWS engineering, Jeff Pedersen, who is responsible for the operations and security of RiskRecon's massive AWS cloud computing environment.

Stratum Security provided additional subject matter expertise, developing the draft security assessment criteria. STRATUM SECURITY is a Washington D.C.-based security consulting firm that specializes in web application and cloud security assessments.

THE AWS CORE SECURITY CRITERIA

AWS provides a mind-boggling expanse of systems, services, and applications. An all-encompassing AWS security assessment guide would fill hundreds of pages. Rather than chew it all at once, we decided to start with the essential foundations on which an AWS environment is built. Each of the 33 criteria of the AWS Core Security Criteria was carefully selected based on its necessity to ensuring a secure AWS environment. RiskRecon will address the security of other AWS services in separate publications.

THE ASSESSMENT CRITERIA

The AWS Core Security Criteria covers six security domains. Each domain contains one or more security criterion. Each criterion is presented as follows:

- ID - The unique criterion identifier. This maps to the associated questionnaire.
- Criterion - The assessment criterion, phrased as a question.
- Why this is important - An explanation of why the criterion is important for securing the AWS environment.
- Validation steps - A description of how to collect the evidence necessary to assess compliance with the criterion.
- Acceptable responses - A listing of the configuration states that meet the criterion requirements.
- Failure responses - A listing of the configuration states that do not meet the criterion requirements.
- More info - A hyperlink to additional information related to the criterion.

THE QUESTIONNAIRE

We've instantiated these Criteria in a security questionnaire. Please feel free to use the questionnaire to assess the security of your vendor's AWS environments. Send it over to your vendors to fill out, or ask the questions over the phone. As you do this, we can guarantee two things. First, your vendor is going to have to get their AWS expert on the phone to answer your questions. Generic answers like "Yes, we do Identity and Access Management stuff" isn't going to fly. Second, you are are going to learn that many of your vendors have significant gaps in their environments that previously were not discovered. That is a good thing.

AWS ACCOUNT MANAGEMENT

WHAT

The AWS accounts and associated configurations structurally separate the various AWS environments (prod, staging, dev) to achieve effective separation of systems and user responsibilities. Access to the Root is protected using two-factor authentication and it is used only when no other options are available.

WHY

All aspects of AWS are controlled through administrative console-based configuration. Using accounts and related permissions to structurally segment the various environments and responsibilities helps ensure proper control and configuration.

ID: aws-core-1 Is the AWS Organizations service used for managing all AWS accounts?

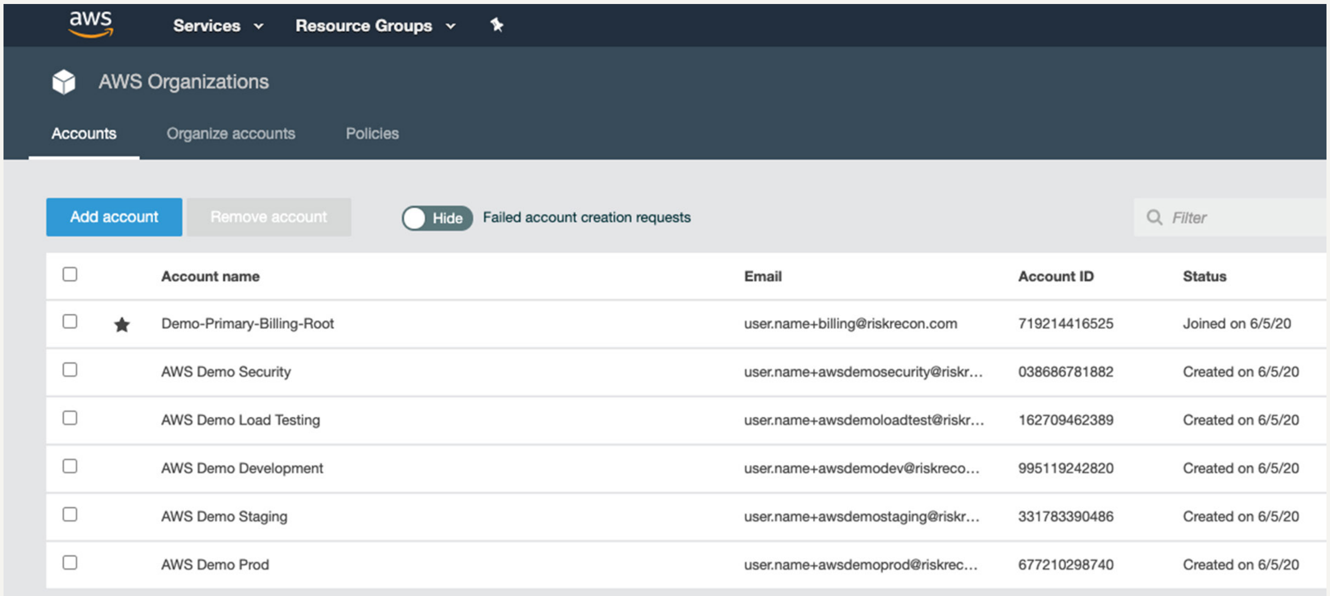
WHY IS THIS IMPORTANT?

The AWS Organizations service provides management of AWS account settings in a consistent manner, provides organization-wide security features and allows the use of AWS accounts as a boundary between environments.

VALIDATION STEPS

Access the Management Console for the AWS account and select the AWS Organizations service. Confirm whether an organization exists or not and all AWS accounts are part of that organization. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/organizations/home?region=us-east-1#/accounts



☐		Account name	Email	Account ID	Status
☐	★	Demo-Primary-Billing-Root	user.name+billing@riskrecon.com	719214416525	Joined on 6/5/20
☐		AWS Demo Security	user.name+awsdemosecurity@riskr...	038686781882	Created on 6/5/20
☐		AWS Demo Load Testing	user.name+awsdemoloadtest@riskr...	162709462389	Created on 6/5/20
☐		AWS Demo Development	user.name+awsdemodev@riskreco...	995119242820	Created on 6/5/20
☐		AWS Demo Staging	user.name+awsdemostaging@riskr...	331783390486	Created on 6/5/20
☐		AWS Demo Prod	user.name+awsdemoprod@riskrec...	677210298740	Created on 6/5/20

Figure 1: *Screenshot showing that AWS Organizations service is in use and managing multiple AWS accounts*

ACCEPTABLE RESPONSE(S)

- The AWS Organizations Service is being used to manage all accounts.

FAILURE RESPONSE(S)

- A single AWS account is being used that contains all resources.
- Multiple AWS accounts are being used; however, they are not part of an organization.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/ORGANIZATIONS/LATEST/USERGUIDE/ORGS_INTRODUCTION.HTML

ID: aws-core-2 Are separate AWS accounts being used for different development stages? (Dev, Staging, Production)

WHY IS THIS IMPORTANT?

Separation of development stages into separate AWS accounts creates a permissions boundary that ensures default separation of networks, IAM access, and other resource overlaps.

VALIDATION STEPS

In the Management Console select the CloudTrail service and select Trails view. The list of Trails should include at least one that has logs being sent to an S3 bucket in a dedicated AWS account for logging. The following screenshot can help validate the response:

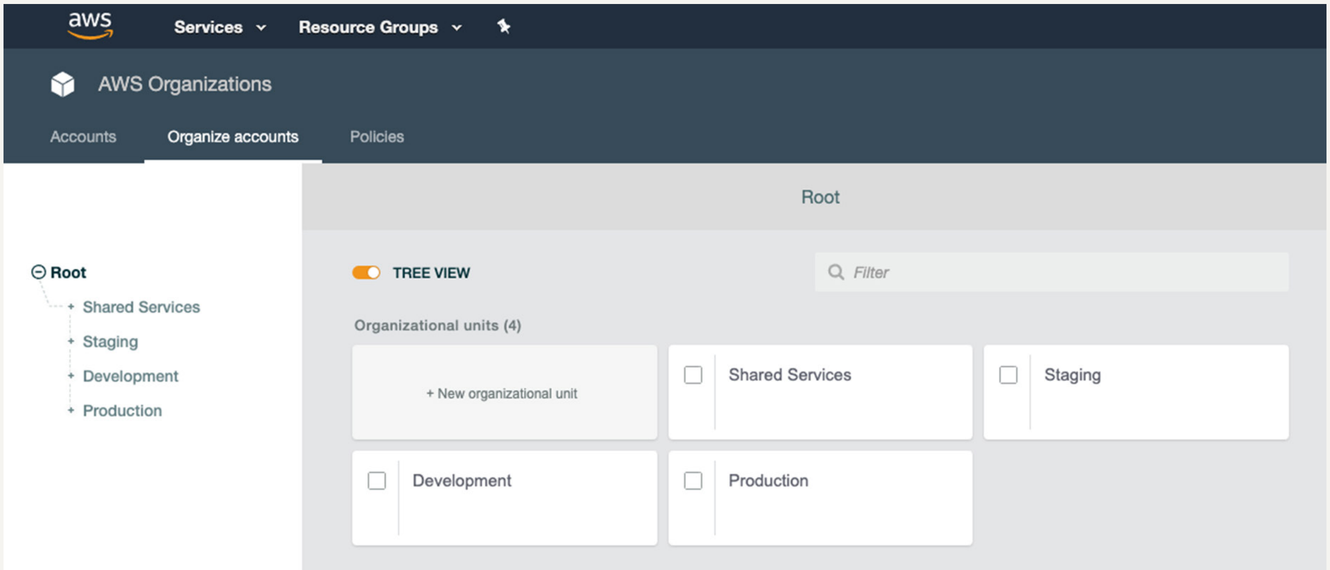


Figure 2: *Screenshot showing that AWS Organizations service is in use and managing multiple AWS accounts*

ACCEPTABLE RESPONSE(S)

- Dedicated AWS accounts exist to separate development, staging and production resources.

FAILURE RESPONSE(S)

- Development, staging and production resources share the same AWS account.

MORE INFO: HTTPS://D0.AWSSTATIC.COM/AWS-ANSWERS/AWS_MULTI_ACCOUNT_SECURITY_STRATEGY.PDF

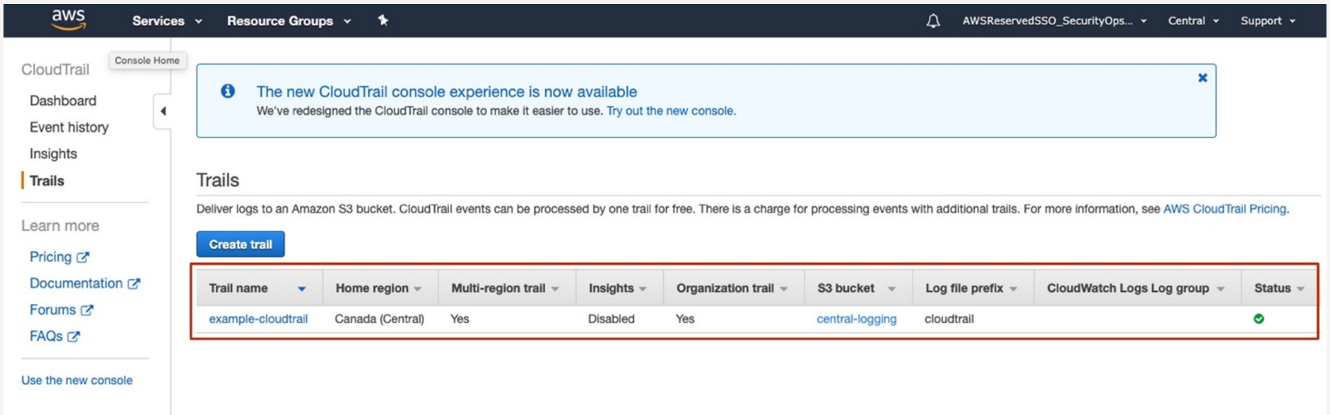
ID: aws-core-3 Is a dedicated AWS account being used for security audit and logging functions?

WHY IS THIS IMPORTANT?

Separation of security audit and logging functions into dedicated AWS accounts ensures a compromise in an AWS account does not allow an attacker to compromise or destroy logging functions.

VALIDATION STEPS

In the Management Console, select the CloudTrail service and select Trails view. The list of Trails should include at least one that has logs being sent to an S3 bucket in a dedicated AWS account for logging. The following screenshot can help validate the response:



The new CloudTrail console experience is now available

We've redesigned the CloudTrail console to make it easier to use. Try out the new console.

Trails

Deliver logs to an Amazon S3 bucket. CloudTrail events can be processed by one trail for free. There is a charge for processing events with additional trails. For more information, see AWS CloudTrail Pricing.

Trail name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs Log group	Status
example-cloudtrail	Canada (Central)	Yes	Disabled	Yes	central-logging	cloudtrail		✓

Figure 3: *Example of an organization trail configured to send trails from each member account to a S3 bucket.*

ACCEPTABLE RESPONSE(S)

- All AWS accounts have a trail enabled to send logs to a dedicated AWS account for logging.
- The AWS Organization has an organization trail configured to send logs to a dedicated AWS account for logging.

FAILURE RESPONSE(S)

- One or more AWS accounts do not send CloudTrail logs to a dedicated AWS account for logging.
- CloudTrail is not configured beyond the default settings.

MORE INFO: HTTPS://D0.AWSSTATIC.COM/AWS-ANSWERS/AWS_MULTI_ACCOUNT_SECURITY_STRATEGY.PDF

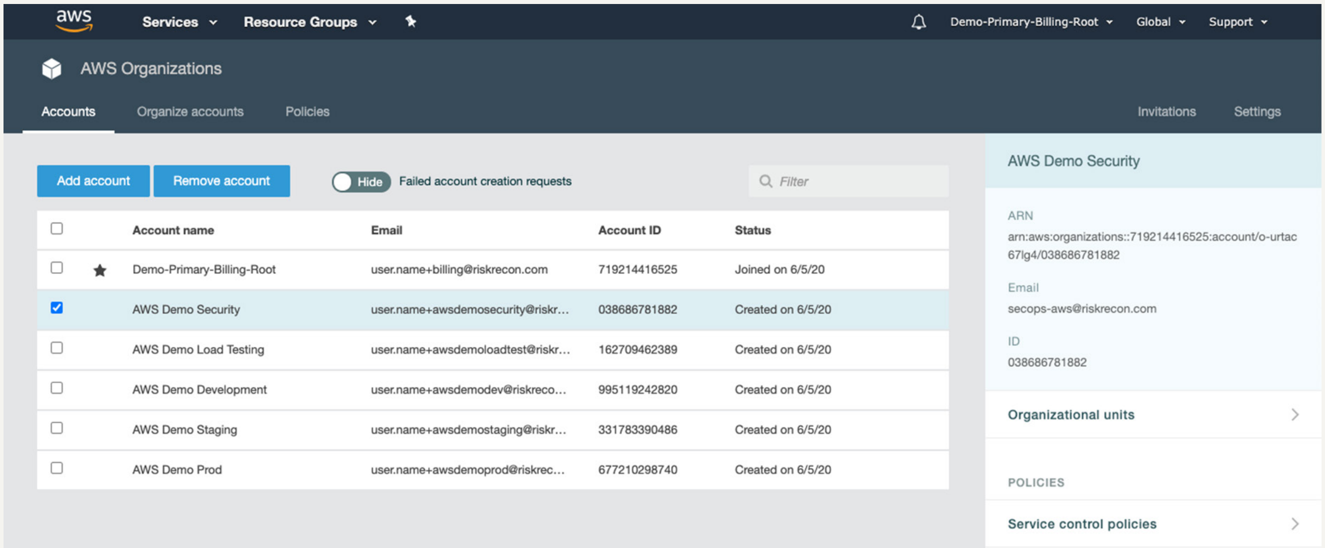
ID: aws-core-4 Is a shared email alias/group being used for the Root account of each AWS account?

WHY IS THIS IMPORTANT?

In the event an employee leaves the company, the associated AWS account may not be accessible or emails for the Root account may not be monitored. Instead create an email alias/group that is limited to select administrators or security team members.

VALIDATION STEPS

Access the Management Console for the Master AWS account, select the AWS Organizations service and select Accounts view. The Email column will show all the email addresses associated with each AWS account in the organization. The following screenshot can help validate the response:



☐		Account name	Email	Account ID	Status
☐	★	Demo-Primary-Billing-Root	user.name+billing@riskrecon.com	719214416525	Joined on 6/5/20
☑		AWS Demo Security	user.name+awsdemosecurity@riskr…	038686781882	Created on 6/5/20
☐		AWS Demo Load Testing	user.name+awsdemoloadtest@riskr…	162709462389	Created on 6/5/20
☐		AWS Demo Development	user.name+awsdemodev@riskreco…	995119242820	Created on 6/5/20
☐		AWS Demo Staging	user.name+awsdemostaging@riskr…	331783390486	Created on 6/5/20
☐		AWS Demo Prod	user.name+awsdemoprod@riskrec…	677210298740	Created on 6/5/20

AWS Demo Security

ARN
arn:aws:organizations::719214416525:account/o-urtac67lg4/038686781882

Email
secops-aws@riskrecon.com

ID
038686781882

Organizational units

POLICIES

Service control policies

Figure 4: *Example organization where each Root account has a unique email address that sends mail to a shared mailbox.*

ACCEPTABLE RESPONSE(S)

- All Root accounts use a shared email alias/group for the configured email.

FAILURE RESPONSE(S)

- A Root account has an individual's email address configured for the account email.

MORE INFO: [HTTPS://D0.AWSSTATIC.COM/AWS-ANSWERS/AWS_MULTI_ACCOUNT_SECURITY_STRATEGY.PDF](https://d0.awsstatic.com/aws-answers/AWS_Multi_Account_Security_Strategy.pdf)

ID: aws-core-5 Does each Root account have multi-factor authentication (MFA) enabled and no active access keys?

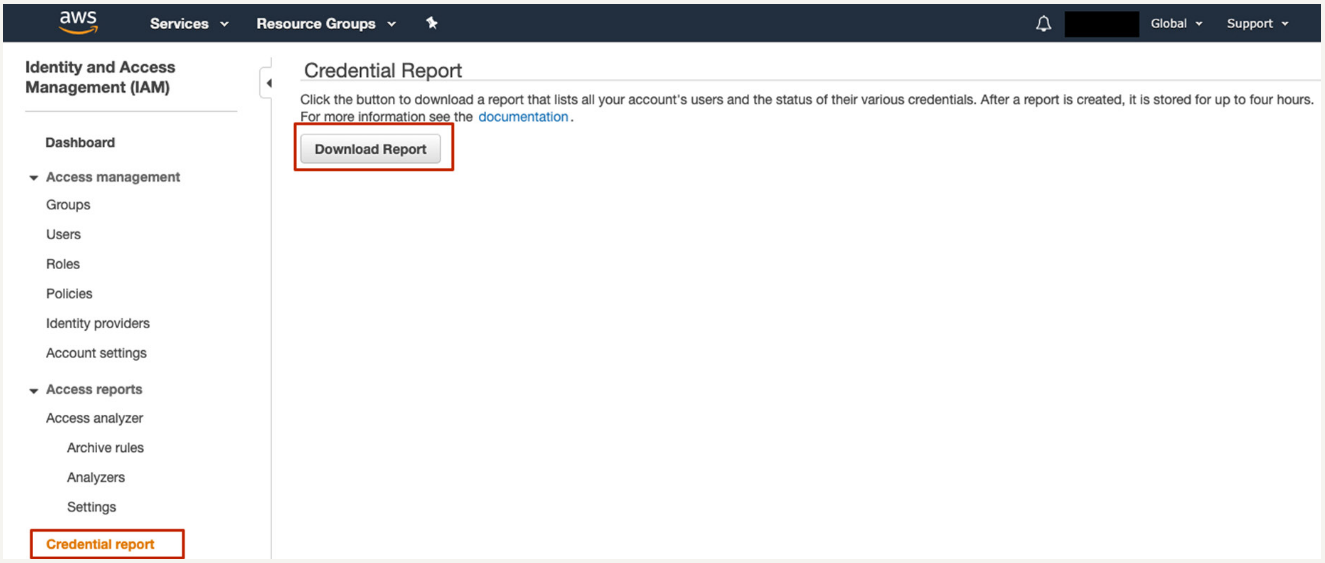
WHY IS THIS IMPORTANT?

The Root account has full access to everything in the AWS account and should be secured using multi-factor authentication in addition to a password. The Root account can also have access keys which have full access and are difficult to audit access to an individual. For that reason, IAM users or roles should be utilized as an alternative.

VALIDATION STEPS

In the **Management Console** select the **IAM service** and select **Credential report** view. Download the Report and confirm the **mfa_active** column is true and **access_key_1_active/ access_key_2_active** are both **false**. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/iam/home?region=us-east-1#/credential_report



Click the button to download a report that lists all your account's users and the status of their various credentials. After a report is created, it is stored for up to four hours. For more information see the documentation.

Figure 5: *Example showing where to download the credential report.*

ACCEPTABLE RESPONSE(S)

- All Root accounts have MFA enabled and have no active access keys.

FAILURE RESPONSE(S)

- A Root account has MFA disabled and/or has an active access key.

MORE INFO: [HTTPS://DOCS.AWS.AMAZON.COM/IAM/LATEST/USERGUIDE/ID_ROOT-USER.HTML](https://docs.aws.amazon.com/iam/latest/userguide/id_root-user.html)

ID: aws-core-6 Has the Root account been used in the last 7 days?

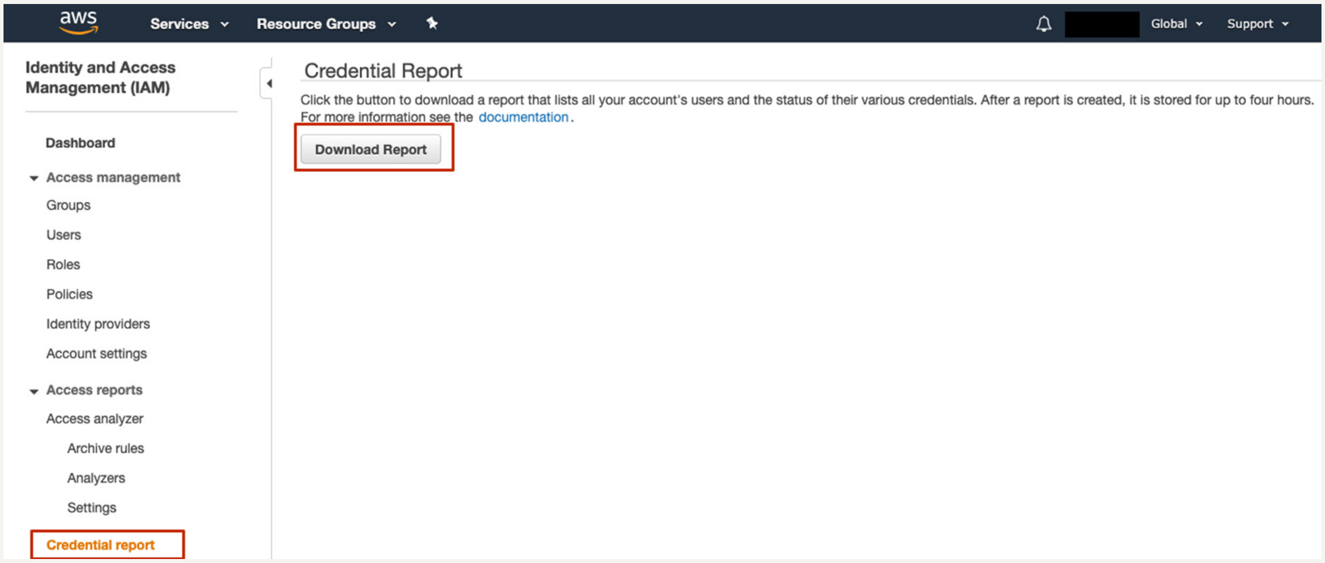
WHY IS THIS IMPORTANT?

The Root account has full access to everything in the AWS account and should not be used unless there is no other option available. For that reason, IAM users or roles should be utilized as an alternative

VALIDATION STEPS

In the Management Console select the IAM service and select Credential report view. Download the Report and confirm the password_last_used was not within the last 7 days. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/iam/home?region=us-east-1#/credential_report



Credential Report

Click the button to download a report that lists all your account's users and the status of their various credentials. After a report is created, it is stored for up to four hours. For more information see the documentation.

Figure 6: *Example showing where to download the credential report.*

ACCEPTABLE RESPONSE(S)

- No console login or API usage from the Root account in the last 7 days.

FAILURE RESPONSE(S)

- The Root account is regularly used and shows activity in the last 7 days.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/IAM/LATEST/USERGUIDE/ID_ROOT-USER.HTML

ID: aws-core-7 Does the AWS organization implement Service Control Policies (SCP)?

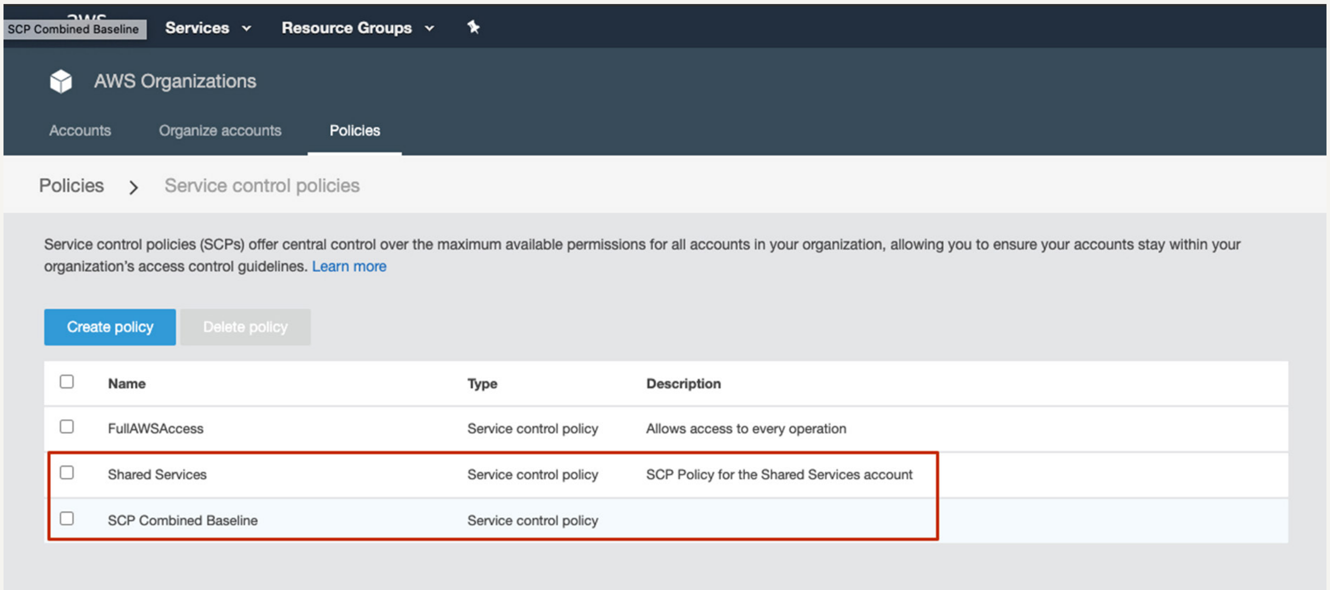
WHY IS THIS IMPORTANT?

Service control policies create guardrails for the implementation of resources in member AWS accounts. SCPs can be used to control whether users can create resources in a given region, prevent disabling security controls, and limit the usage of Root accounts.

VALIDATION STEPS

Access the Management Console for the Master AWS account, select the AWS Organizations service and select Policies view. Service Control Policies (SCP) should be enabled and custom policies should be assigned to accounts/OUs to restrict services or actions as appropriate. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/organizations/home?region=us-east-1#/policies/service-control



Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. Learn more

□	Name	Type	Description
□	FullAWSAccess	Service control policy	Allows access to every operation
□	Shared Services	Service control policy	SCP Policy for the Shared Services account
□	SCP Combined Baseline	Service control policy	

Figure 7: *Example organization with custom SCP policies, these should be applied to member accounts or OUs.*

ACCEPTABLE RESPONSE(S)

- SCPs are enabled and are being utilized to restrict regions, services and actions within member accounts.

FAILURE RESPONSE(S)

- SCPs are not enabled.
- SCPs are enabled but not being utilized to restrict or limit member accounts.
- The AWS Organization service is not being used.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/ORGANIZATIONS/LATEST/USERGUIDE/ORGS_MANAGE_POLICIES_SCP.HTML

ENCRYPTION

WHAT

AWS data store encryption features are implemented to encrypt data at rest.

WHY

Use of the AWS data store encryption feature helps prevent breach of data in the event of physical storage media theft or improper hardware redeployment or retirement.

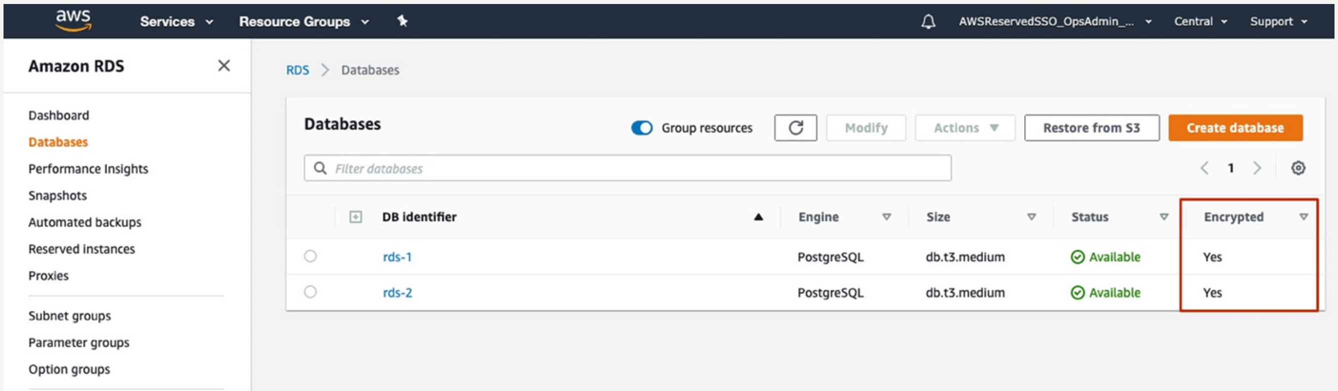
ID: aws-core-8 Are encryption at rest features implemented for RDS and other data stores?

WHY IS THIS IMPORTANT?

Encryption at rest provides encryption protection against a physical compromise or a failure in AWS processes for reuse of hardware.

VALIDATION STEPS

Encryption at rest is available for multiple data stores including RDS, ElasticSearch, Redshift, ElastiCache, S3 and other services. For RDS, in the Management Console select the RDS service and select Databases view. Select the preferences cog on the table and enable the Encrypted column. The Encrypted column will show the encryption status for each RDS instance. Other data stores can be checked in a similar manner or by directly viewing the resource configuration. The following screenshot can help validate the response:



DB identifier	Engine	Size	Status	Encrypted
rds-1	PostgreSQL	db.t3.medium	Available	Yes
rds-2	PostgreSQL	db.t3.medium	Available	Yes

Figure 8: *Example of RDS instances with encryption at rest enabled.*

ACCEPTABLE RESPONSE(S)

- All data stores in use, such as RDS databases, use encryption at rest.
- No data store services are being used in any AWS account.

FAILURE RESPONSE(S)

- RDS instances or other data stores do not implement encryption at rest settings available within AWS.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/AMAZONRDS/LATEST/USERGUIDE/OVERVIEW.ENCRYPTION.HTML

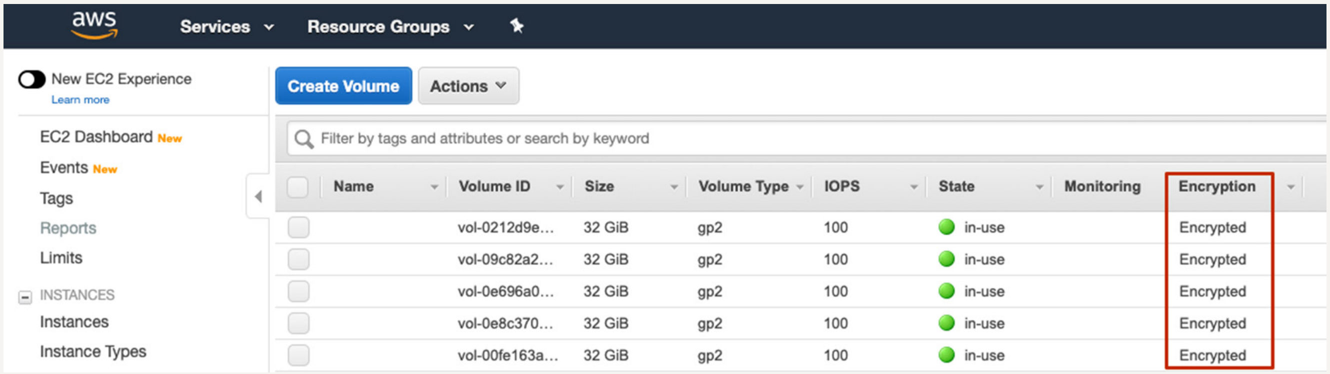
ID: aws-core-9 Is volume encryption implemented for all EC2 volumes and snapshots?

WHY IS THIS IMPORTANT?

Encryption at rest provides encryption protection against a physical compromise or a failure in AWS processes for reuse of hardware.

VALIDATION STEPS

In the Management Console select the EC2 service and select volumes or the snapshots view. The encryption status of each volume will be shown under the encryption column. The following screenshot can help validate the response:



Name	Volume ID	Size	Volume Type	IOPS	State	Monitoring	Encryption
	vol-0212d9e...	32 GiB	gp2	100	● in-use		Encrypted
	vol-09c82a2...	32 GiB	gp2	100	● in-use		Encrypted
	vol-0e696a0...	32 GiB	gp2	100	● in-use		Encrypted
	vol-0e8c370...	32 GiB	gp2	100	● in-use		Encrypted
	vol-00fe163a...	32 GiB	gp2	100	● in-use		Encrypted

Figure 9: *Example showing all volumes with encryption at rest enabled*

ACCEPTABLE RESPONSE(S)

- All EC2 volumes and snapshots implement volume encryption using the KMS service.
- Volumes or snapshots that contain sensitive data implement encryption using the KMS service.

FAILURE RESPONSE(S)

- Not all volumes and snapshots are configured to use volume encryption.
- Volumes and snapshots that contain sensitive data are not configured to use volume encryption.

MORE INFO: [HTTPS://DOCS.AWS.AMAZON.COM/AWSEC2/LATEST/USERGUIDE/EBSENCRYPTION.HTML](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html)

IDENTITY AND ACCESS MANAGEMENT

WHAT

The AWS environment is supported by a robust identity and access management infrastructure. Sensitive permissions are properly managed to ensure appropriate use. Programmatic access is strictly controlled.

WHY

A well-configured AWS identity and access management infrastructure helps ensure that all user access is appropriate and authorized, minimizing the likelihood of privilege abuse or error.

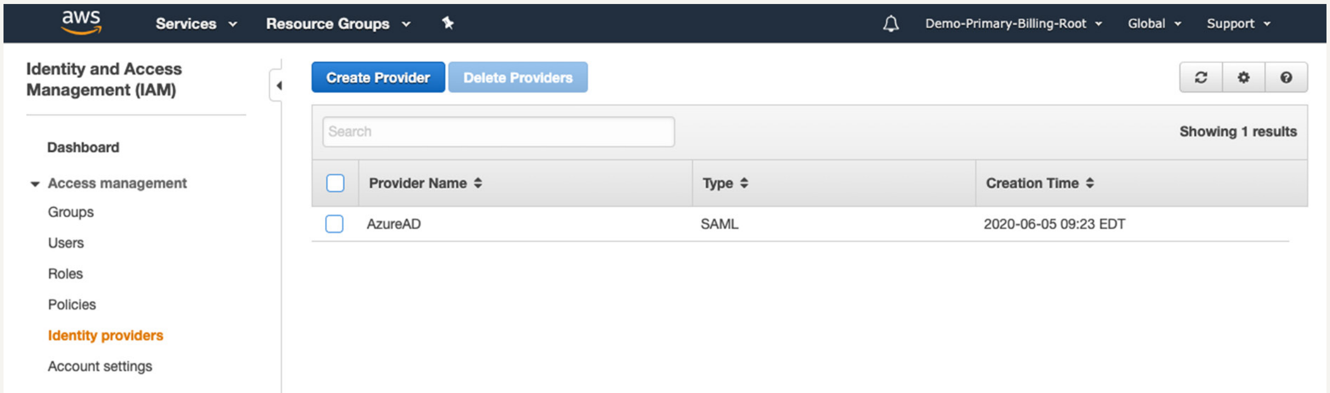
ID: aws-core-10 Is SAML based single sign-on being used for IAM access?

WHY IS THIS IMPORTANT?

Using single sign-on to access AWS accounts ensures company account standards are consistently enforced and access lifecycles are applied. Management of individual IAM accounts in a consistent manner is not scalable with multiple AWS accounts.

VALIDATION STEPS

In the Management Console select the IAM service and select the Identity providers view. At least one identity provider should be configured within the organization. The following screenshot can help validate the response:



	Provider Name	Type	Creation Time
□	AzureAD	SAML	2020-06-05 09:23 EDT

Figure 10: *Example of an AWS account with a SAML identity provider configured for IAM access.*

ACCEPTABLE RESPONSE(S)

- A SAML IDP such as G-Suite, Azure AD, Okta, AWS SSO or other provider is in use for single sign-on.
- A SAML IDP is configured in at least one AWS account and used to assume roles into other AWS accounts within an organization.

FAILURE RESPONSE(S)

- Individual IAM accounts are being used to access AWS accounts within the organization.

MORE INFO: [HTTPS://AWS.AMAZON.COM/IDENTITY/SAML/](https://aws.amazon.com/identity/saml/)

ID: aws-core-11 Does any AWS account have IAM users configured with console access?

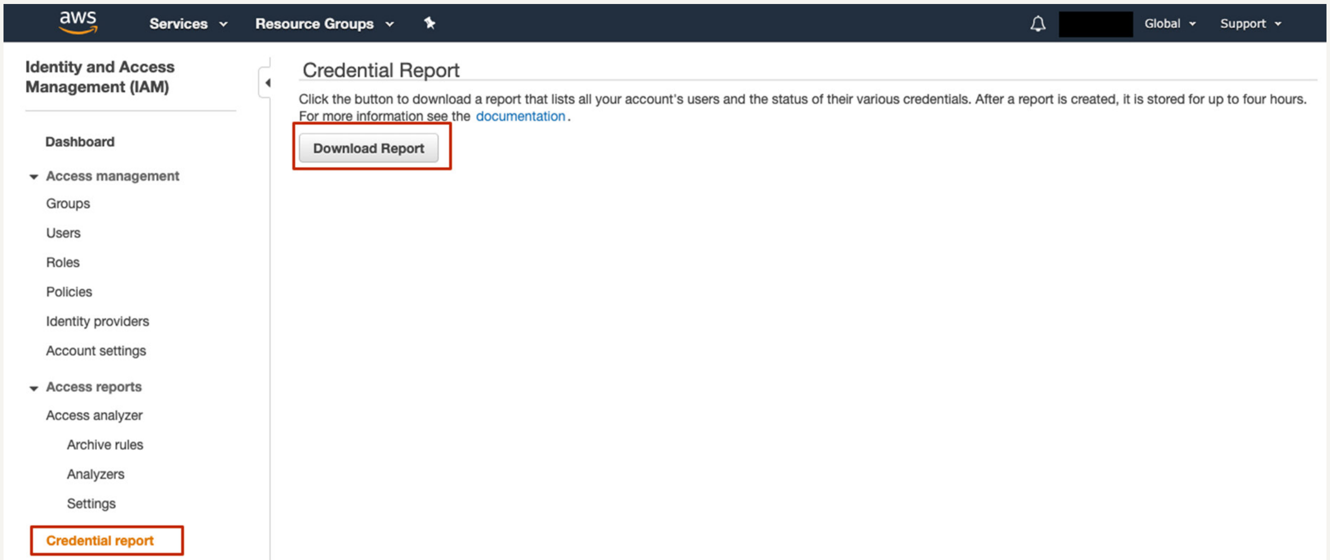
WHY IS THIS IMPORTANT?

IAM user accounts should be avoided as they cannot be consistently maintained across multiple AWS accounts. IAM user accounts used for programmatic access should not require console access.

VALIDATION STEPS

In the Management Console, select the IAM service and select Credential report view. Download the Report and confirm the password_enabled column is set to FALSE for all IAM user accounts. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/iam/home?region=us-east-1#/credential_report



Credential Report

Click the button to download a report that lists all your account's users and the status of their various credentials. After a report is created, it is stored for up to four hours. For more information see the documentation.

Figure 11: *Example showing where to download the credential report.*

ACCEPTABLE RESPONSE(S)

- AWS account access is managed using single sign-on or assuming roles from another account.

FAILURE RESPONSE(S)

- IAM user accounts are being used to access the AWS management console.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/IAM/LATEST/USERGUIDE/CONSOLE_CONTROLLING-ACCESS.HTML

ID: aws-core-12 Does any AWS account have access keys configured for programmatic access?

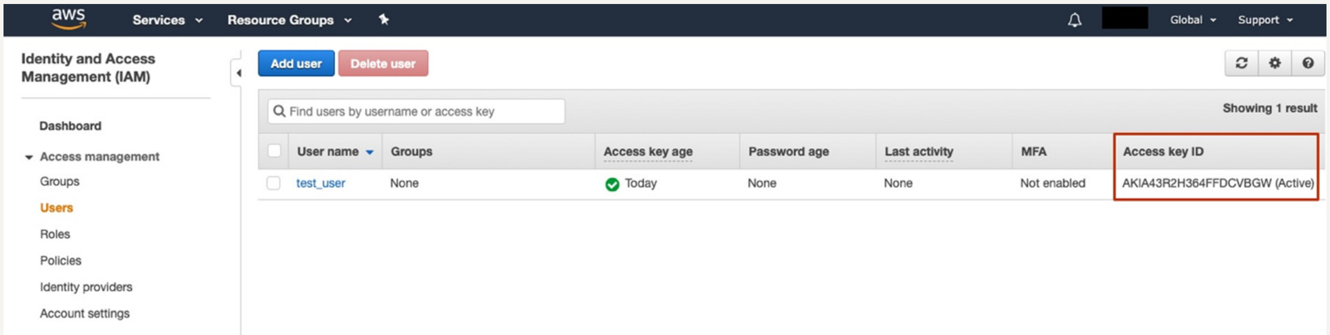
WHY IS THIS IMPORTANT?

Access keys are often used for application access to the AWS API and are shared between multiple individuals or systems. This situation increases the exposure to compromise and removes the ability to audit individual access to the AWS API. Alternative methods to access the AWS API should be used, such as IAM roles applied to an EC2 instance or assumed using single sign-on user access.

VALIDATION STEPS

In the Management Console select the IAM service and select the Users view. Select the settings cog for the table column configuration and enable the Access key ID column. This column will show active access keys within the AWS account. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/iam/home?region=us-east-1#/users



Showing 1 result

	User name	Groups	Access key age	Password age	Last activity	MFA	Access key ID
□	test_user	None	✓ Today	None	None	Not enabled	AKIA43R2H364FFDCVBGW (Active)

Figure 12: *Example of a test IAM user with an active access key which would be a failure response.*

ACCEPTABLE RESPONSE(S)

- Access keys are not being utilized for programmatic access and IAM roles are being used instead.
- A limited number of access keys are configured to allow a 3rd party solution to access the account. IAM policy access is restrictive for this account and the access keys are regularly rotated.

FAILURE RESPONSE(S)

- Access keys are being used as a primary method for users to interact with the AWS API.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/GENERAL/LATEST/GR/AWS-ACCESS-KEYS-BEST-PRACTICES.HTML

ID: aws-core-13 Does any AWS account have access keys that have not been used in > 90 days? (Or never used)

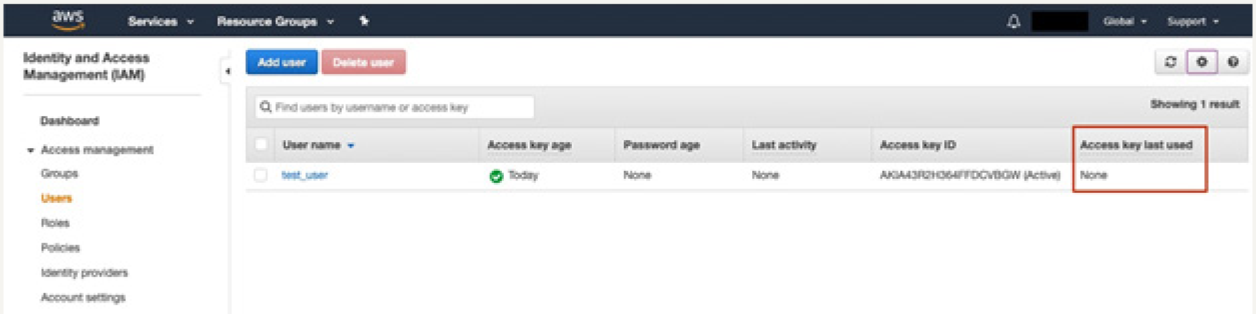
WHY IS THIS IMPORTANT?

Access keys are often used for application access to the AWS API and are shared between multiple individuals or systems. This situation increases the exposure to compromise and removes the ability to audit individual access to the AWS API. If access keys are not being regularly used they should be made inactive or deleted.

VALIDATION STEPS

In the Management Console, select the IAM service and select the Users view. Select the settings cog for the table column configuration and enable the Access key last used column. This column will show access keys that have not been used in > 90 days or have never been used. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/iam/home?region=us-east-1#/users



□	User name	Access key age	Password age	Last activity	Access key ID	Access key last used
□	test_user	✓ Today	None	None	AKIA43R2H364FFDCVBGW (Active)	None

Figure 13: *Example of an unused access key which would be a failure response*

ACCEPTABLE RESPONSE(S)

- All access keys have been used in the last 90 days.
- No IAM access keys exist in the AWS account.

FAILURE RESPONSE(S)

- IAM access keys exist that have not been used in > 90 days or never been used.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/GENERAL/LATEST/GR/AWS-ACCESS-KEYS-BEST-PRACTICES.HTML

ID: aws-core-14 Does any AWS account have access keys that have not been rotated in > 90 days?

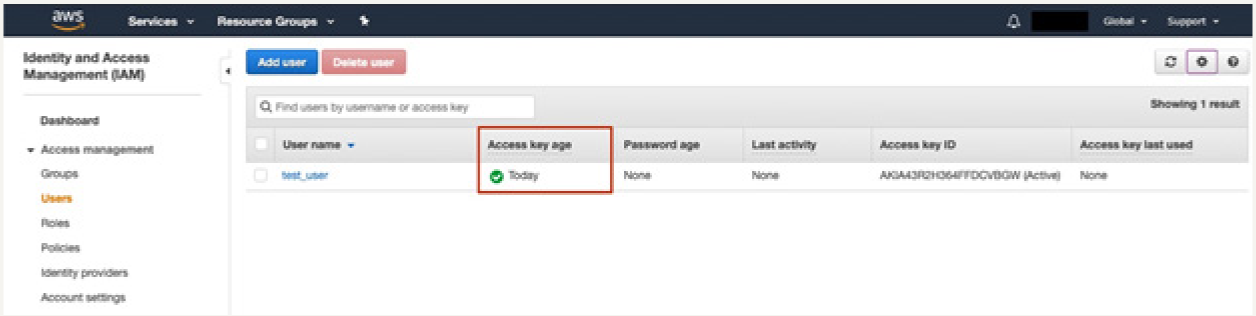
WHY IS THIS IMPORTANT?

Access keys are often used for application access to the AWS API and are shared between multiple individuals or systems. This situation increases the exposure to compromise and removes the ability to audit individual access to the AWS API. To help reduce exposure, access keys should be regularly rotated to reduce the window that an access key would be active.

VALIDATION STEPS

In the Management Console, select the IAM service and select the Users view. The Access key age column will show the number of days since the access key was created. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/iam/home?region=us-east-1#/users



	User name	Access key age	Password age	Last activity	Access key ID	Access key last used
□	test_user	✓ Today	None	None	AKIA43R2H364FFDCVBGW (Active)	None

Figure 14: *Example of an IAM user with an access key that is < 90 days old*

ACCEPTABLE RESPONSE(S)

- All access keys have an age < 90 days.
- No IAM access keys exist in the AWS account.

FAILURE RESPONSE(S)

- IAM access keys exist that have an age > 90 days and are not being regularly rotated.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/GENERAL/LATEST/GR/AWS-ACCESS-KEYS-BEST-PRACTICES.HTML

ID: aws-core-15 Does any AWS account have an IAM role that has not been used in > 90 days? (Or never used)

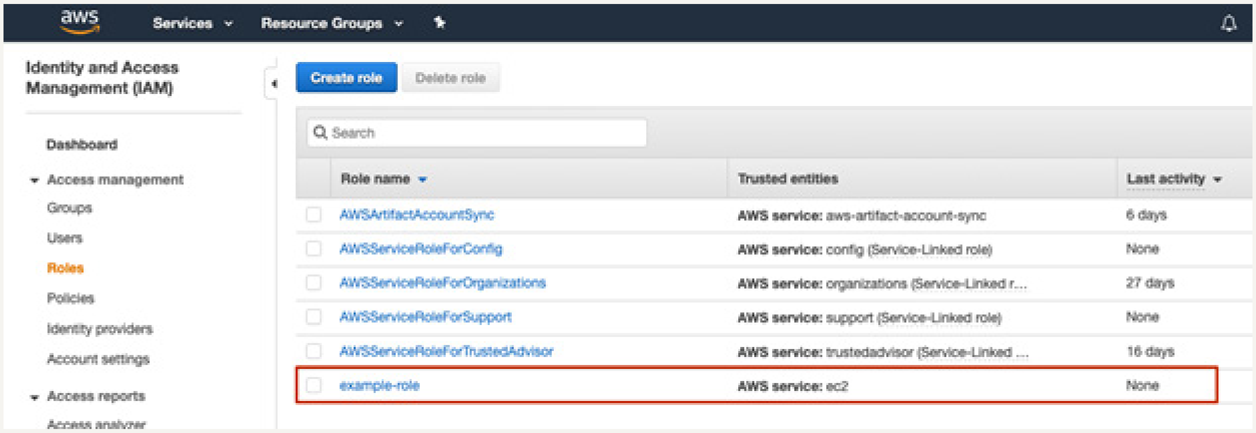
WHY IS THIS IMPORTANT?

IAM roles provide access to different AWS services using temporary security credentials. Similar to other user accounts, IAM roles should be periodically reviewed to determine if they are still being used and if not removed to prevent unauthorized access.

VALIDATION STEPS

In the Management Console select the IAM service and select the Roles view. The Last activity column will show the number of days since the IAM role was used. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/iam/home?region=us-east-1#/roles



	Role name	Trusted entities	Last activity
□	AWSArtifactAccountSync	**AWS service:** aws-artifact-account-sync	6 days
□	AWSServiceRoleForConfig	**AWS service:** config (Service-Linked role)	None
□	AWSServiceRoleForOrganizations	**AWS service:** organizations (Service-Linked r...	27 days
□	AWSServiceRoleForSupport	**AWS service:** support (Service-Linked role)	None
□	AWSServiceRoleForTrustedAdvisor	**AWS service:** trustedadvisor (Service-Linked ...	16 days
□	example-role	**AWS service:** ec2	None

Figure 15: *Example of a role that has never been used*

ACCEPTABLE RESPONSE(S)

- No, all IAM roles show activity within the last 90 days.
- Yes, some IAM roles related to AWS Service-Linked roles have not been used in the last 90 days however all custom roles are regularly used.

FAILURE RESPONSE(S)

- Yes, multiple custom IAM roles have not been used in the last 90 days.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/IAM/LATEST/USERGUIDE/BEST-PRACTICES.HTML#REMOVE-CREDENTIALS

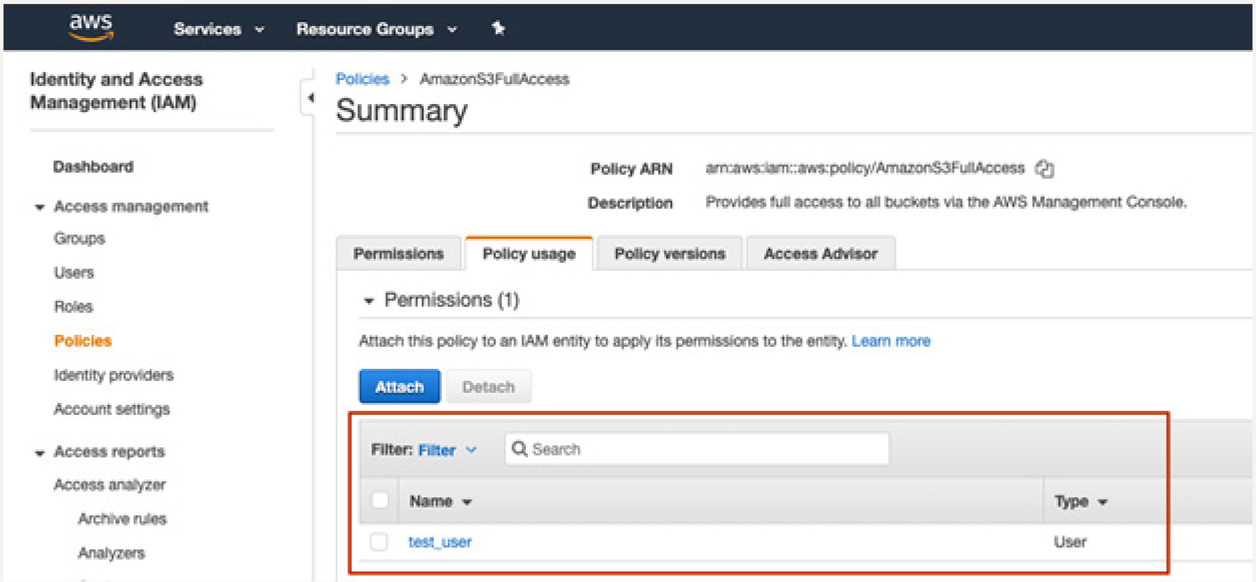
ID: aws-core-16 Does any AWS account have IAM users, groups or roles with AWS managed policies attached that permit full administrator access or full access to the S3 or IAM services?

WHY IS THIS IMPORTANT?

Use of the AWS managed policies provides broad access to services that do not follow a principle of least privilege. In addition to this resulting in user accounts having excessive privileges, a compromised account would provide the miscreant full access to specific services.

VALIDATION STEPS

In the Management Console select the IAM service and select the Policies view. Search for the AdministratorAccess policy and select the Policy Usage tab, this table will show IAM principals that have this policy attached. The same process can be completed for the AmazonS3FullAccess and IAMFullAccess policies. The following screenshot can help validate the response:



Policy ARN arn:aws:iam::aws:policy/AmazonS3FullAccess

Description Provides full access to all buckets via the AWS Management Console.

Attach this policy to an IAM entity to apply its permissions to the entity. Learn more

	Name	Type
□	test_user	User

Figure 16: *Example of IAM users with the AmazonS3FullAccess policy attached which would be a failure response*

ACCEPTABLE RESPONSE(S)

- IAM principals are not configured to use AWS managed policies.
- A limited number of IAM roles have the AdministratorAccess policy attached for administrator access but are not regularly used

FAILURE RESPONSE(S)

- AWS managed policies are primarily used to assign access within AWS accounts including the vAdministratorAccess, AmazonS3FullAccess and IAMFullAccess policies.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/IAM/LATEST/USERGUIDE/BEST-PRACTICES.HTML#GRANT-LEAST-PRIVILEGE

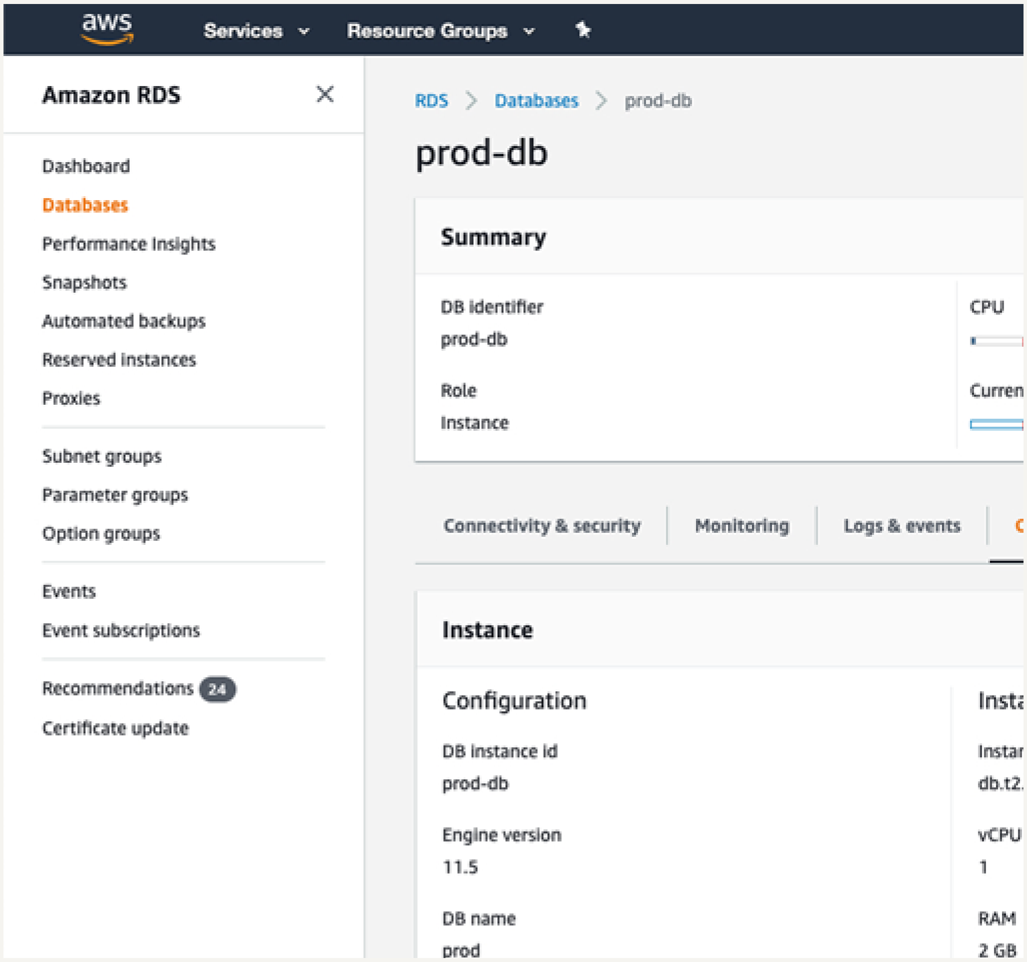
ID: aws-core-17 Do all RDS instances use IAM based authentication for database access?

WHY IS THIS IMPORTANT?

Without IAM authentication, access to the database is dependent on username and passwords that are manually provisioned and managed. This solution is not easily manageable and leads to shared database credentials within an organization.

VALIDATION STEPS

In the Management Console select the RDS service and select the Databases view. Spot check several databases by selecting a database and the Configuration tab. Under the instance configuration, it should show IAM db authentication as enabled. The following screenshot can help validate the response:



prod-db

Summary

DB identifier
prod-db

Role
Instance

CPU

Curren

Instance

Configuration

DB instance id
prod-db

Engine version
11.5

DB name
prod

Insta

Instar
db.t2.

vCPU
1

RAM
2 GB

Figure 17: *Example of an RDS instance configuration showing IAM authentication enabled*

ACCEPTABLE RESPONSE(S)

- All users and applications utilize IAM authentication to access the database.
- All users and applications utilize an authentication proxy that manages individual user access and offers auditing of database access.

FAILURE RESPONSE(S)

- IAM authentication is not being used to access the database.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/AMAZONRDS/LATEST/USERGUIDE/USINGWITHRDS.IAMDBAUTH.HTML

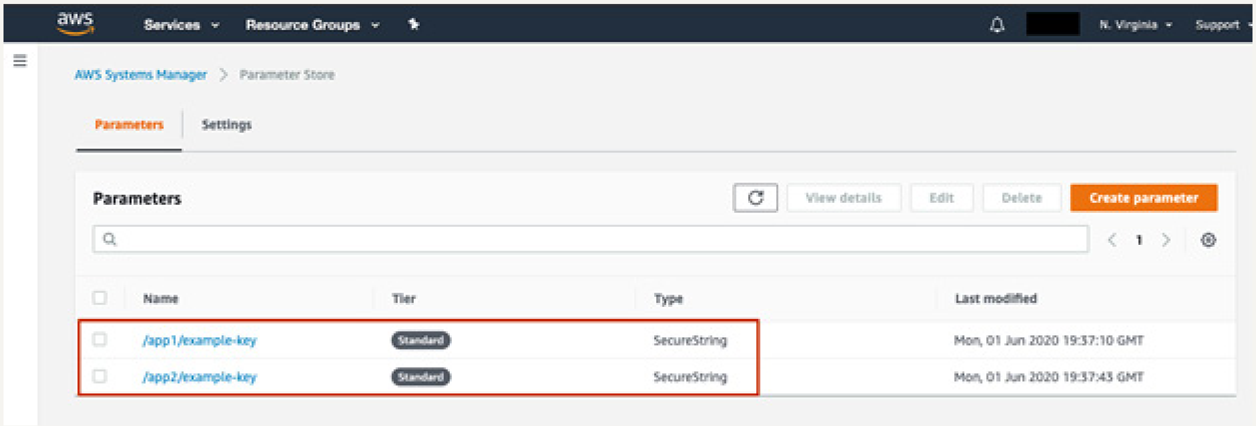
ID: aws-core-18 Is the AWS Secrets Manager or SSM Parameter Store being used for secrets management?

WHY IS THIS IMPORTANT?

Storing passwords in plaintext increases the risk of exposure to unauthorized users in the configurations of AWS services or other applications. This includes disclosure in Cloudformation templates, Lambda functions, EC2 user data or other data stores.

VALIDATION STEPS

In the Management Console, select the AWS Systems Manager service and select the Parameter Store view. Confirm that the parameter store or AWS Secrets Manager is being used for managing application secrets. The following screenshot can help validate the response:



Parameters

☐	Name	Tier	Type	Last modified
☐	/app1/example-key	Standard	SecureString	Mon, 01 Jun 2020 19:37:10 GMT
☐	/app2/example-key	Standard	SecureString	Mon, 01 Jun 2020 19:37:43 GMT

Figure 18: *Example of multiple parameters being stored as secrets in SSM parameter store*

ACCEPTABLE RESPONSE(S)

- AWS secrets manager, SSM parameter store or another secrets store is being used to manage secrets and secrets are not stored in plaintext.

FAILURE RESPONSE(S)

- No secrets management service is currently being used and secrets are stored in plaintext.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/SYSTEMS-MANAGER/LATEST/USERGUIDE/INTEGRATION-PS-SECRETSMANAGER.HTML

NETWORK SECURITY

WHAT

The AWS network is segmented into subnets according to required system network access requirements. Network services are limited to those that are secure and necessary. Internet-facing services are restricted to least privilege, exposing only those necessary for the given user population.

WHY

Segmenting systems into different subnets, such as public and internal, helps ensure that internal-only systems aren't accidentally exposed. Limiting network services to only those users who absolutely must access them reduces the likelihood of compromise.

ID: aws-core-19 Do any security groups permit non-HTTP service access from the Internet?

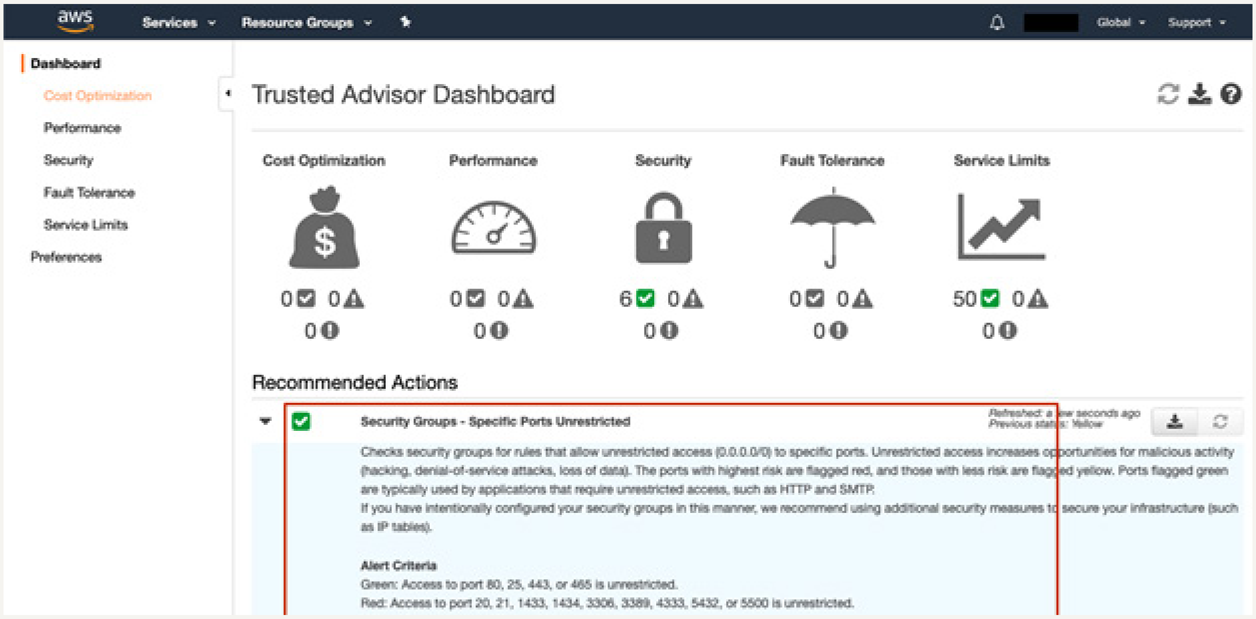
WHY IS THIS IMPORTANT?

Permitting access to management ports such as SSH, RDP or database services increases the attack services of the AWS environment and increases the risk of compromise from an Internet based attacker.

VALIDATION STEPS

In the Management Console select the Trusted Advisor service and select the Refresh button. Once the page is updated it will show the Security Groups – Specific Ports Unrestricted action which will detail unrestricted access to non-HTTP ports. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/trustedadvisor/home?region=us-east-1#/dashboard



Security Groups - Specific Ports Unrestricted

Refreshed: a few seconds ago
Previous status: Yellow

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data). The ports with highest risk are flagged red, and those with less risk are flagged yellow. Ports flagged green are typically used by applications that require unrestricted access, such as HTTP and SMTP.

If you have intentionally configured your security groups in this manner, we recommend using additional security measures to secure your infrastructure (such as IP tables).

Alert Criteria

Green: Access to port 80, 25, 443, or 465 is unrestricted.

Red: Access to port 20, 21, 1433, 1434, 3306, 3389, 4333, 5432, or 5500 is unrestricted.

Figure 19: *Example of a Trusted Advisor action showing no non-HTTP services are accessible from the Internet*

ACCEPTABLE RESPONSE(S)

- Only approved HTTP related services are accessible from the Internet.

FAILURE RESPONSE(S)

- Multiple security groups are configured to permit non-HTTP service access for management or database ports.

MORE INFO: HTTPS://D1.AWSSTATIC.COM/WHITEPAPERS/SECURITY/AWS_SECURITY_BEST_PRACTICES.PDF

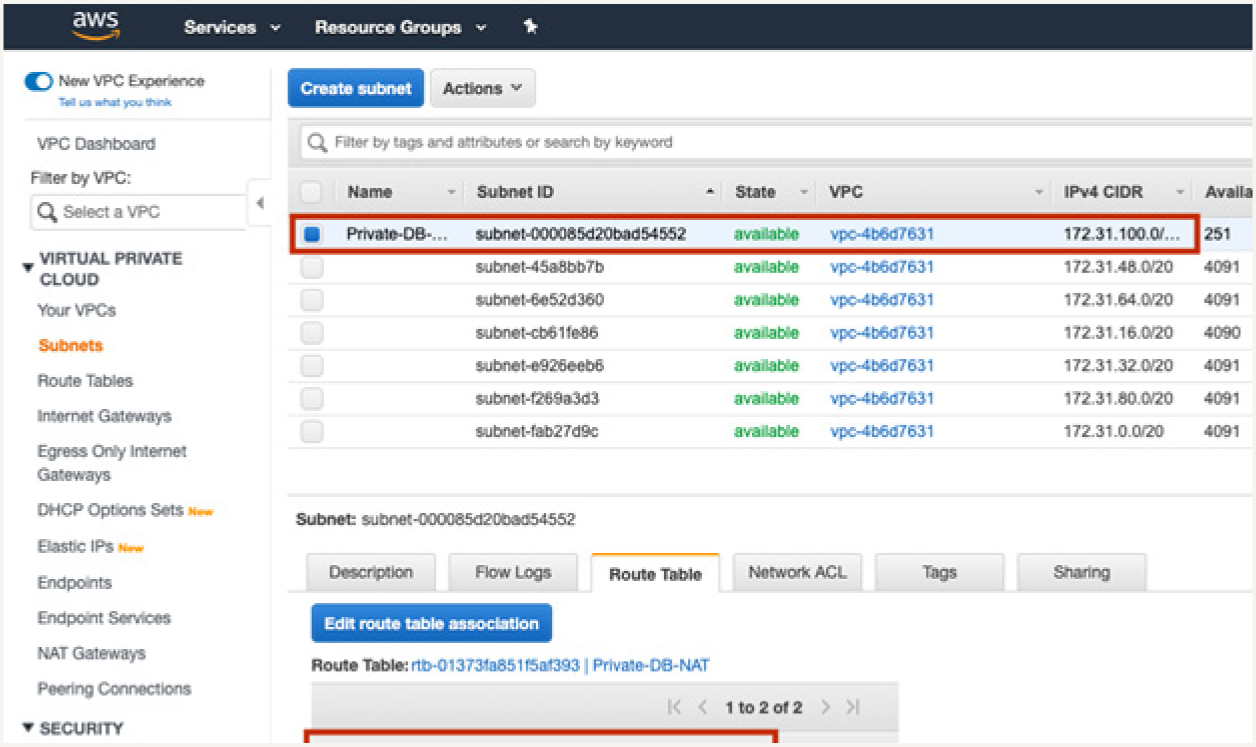
ID: aws-core-20 Are private subnets being used for internal servers, databases and other resources?

WHY IS THIS IMPORTANT?

Placing internal servers, databases, and other resources into a subnet that allows access via an Internet Gateway and assignment of public IPs increases the risk of misconfiguration exposing the resource to the Internet.

VALIDATION STEPS

In the Management Console select the VPC service and select the Subnets view. Spot check subnets containing internal servers, databases, and other resources to confirm that the Route Table configuration does not use an Internet Gateway. Private subnets will either have local routing, peer routing, or routing via a NAT gateway configured. The following screenshot can help validate the response:



	Name	Subnet ID	State	VPC	IPv4 CIDR	Availa
■	Private-DB-...	subnet-000085d20bad54552	available	vpc-4b6d7631	172.31.100.0/...	251
□		subnet-45a8bb7b	available	vpc-4b6d7631	172.31.48.0/20	4091
□		subnet-6e52d360	available	vpc-4b6d7631	172.31.64.0/20	4091
□		subnet-cb61fe86	available	vpc-4b6d7631	172.31.16.0/20	4090
□		subnet-e926eeb6	available	vpc-4b6d7631	172.31.32.0/20	4091
□		subnet-f269a3d3	available	vpc-4b6d7631	172.31.80.0/20	4091
□		subnet-fab27d9c	available	vpc-4b6d7631	172.31.0.0/20	4091

Subnet: subnet-000085d20bad54552

Route Table: rtb-01373fa851f5af393 | Private-DB-NAT

1 to 2 of 2

Figure 20: *Example of a subnet route table showing use of a NAT gateway in a private subnet configuration*

ACCEPTABLE RESPONSE(S)

- All internal servers, databases and other resources are within private subnets.

FAILURE RESPONSE(S)

- Internal servers, databases or other resources have traffic routed via the Internet Gateway and can be assigned a public IP.
- All internal servers, databases or other resources utilize the default VPC and are assigned public IP addresses.

MORE INFO: HTTPS://D1.AWSSTATIC.COM/WHITEPAPERS/SECURITY/AWS_SECURITY_BEST_PRACTICES.PDF

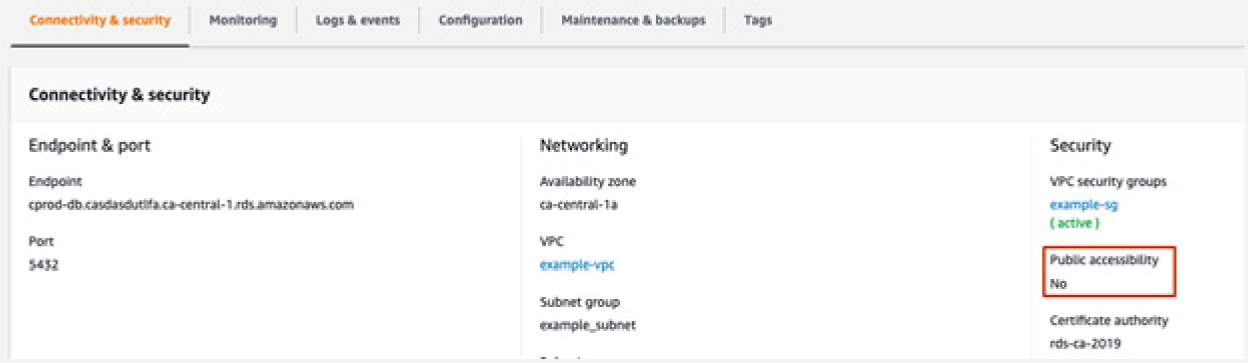
ID: aws-core-21 Are all RDS instances in private subnets and not publicly accessible?

WHY IS THIS IMPORTANT?

Having RDS instances configured to be publicly accessible increases the risk of unauthorized access from the Internet. Non-public RDS instances that exist in public subnets are more likely to be accidentally exposed to the Internet due to a configuration error.

VALIDATION STEPS

In the Management Console, select the RDS service and select the Databases view. Spot check several databases by selecting a database and the Connectivity & Security tab. Under the Security section, Public accessibility should be No. The following screenshot can help validate the response:



Connectivity & security

Endpoint & port

Endpoint
cprod-db.casdasdutlfa.ca-central-1.rds.amazonaws.com

Port
5432

Networking

Availability zone
ca-central-1a

VPC
example-vpc

Subnet group
example_subnet

Security

VPC security groups
example-sg
(active)

Public accessibility
No

Certificate authority
rds-ca-2019

***Figure 21:** Example showing RDS configuration with Public accessibility disabled*

ACCEPTABLE RESPONSE(S)

- All RDS instances are in private subnets and not publicly accessible.
- RDS instances are not being used in the AWS environment.

FAILURE RESPONSE(S)

- RDS instances are configured to be publicly accessible.

MORE INFO: HTTPS://AWS.AMAZON.COM/BLOGS/DATABASE/APPLYING-BEST-PRACTICES-FOR-SECURING-SENSITIVE-DATA-IN-AMAZON-RDS/

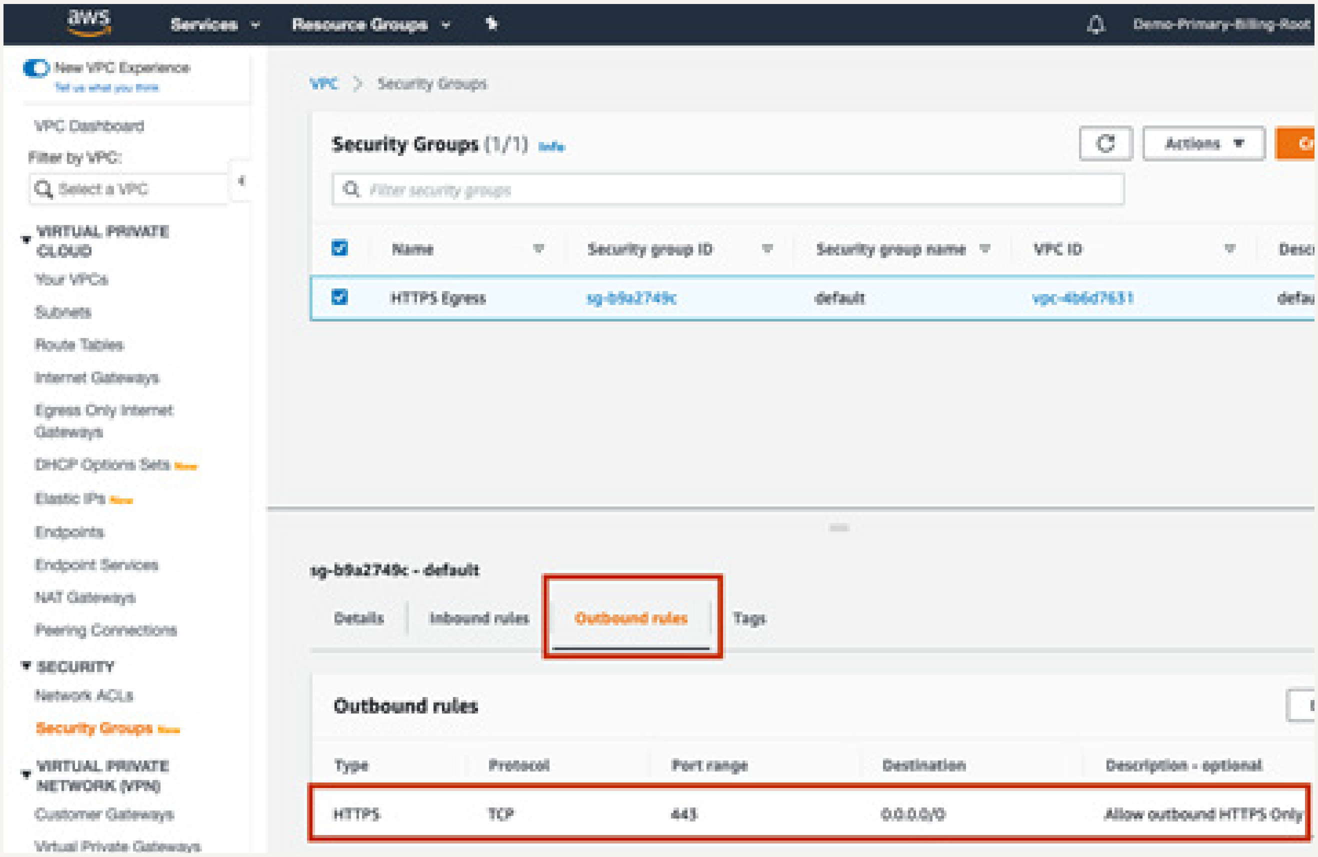
ID: aws-core-22 Are security groups for outbound network access implemented for each VPC?

WHY IS THIS IMPORTANT?

By default security groups permit unrestricted outbound network access. This configuration would allow an attacker inside the VPC to maintain a connection into the environment and to exfiltrate data depending on the level of compromise. Implementing outbound rules can help restrict or slow an attacker within the VPC environment.

VALIDATION STEPS

In the Management Console select the VPC service and select the Security Groups view. View the Outbound rules count column and spot check security groups with only 1 rule. If the rule permits All traffic to 0.0.0.0/0 there is no restrictions on outbound network access. The following screenshot can help validate the response:



Security Groups (1/1) Info

☑	Name	Security group ID	Security group name	VPC ID	Desc
☑	HTTPS Egress	sg-b9a2749c	default	vpc-4b6d7631	defau

sg-b9a2749c - default

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
HTTPS	TCP	443	0.0.0.0/0	Allow outbound HTTPS Only

Figure 22: *Example of a security group with only HTTPS permitted outbound*

ACCEPTABLE RESPONSE(S)

- Outbound rules have been implemented to restrict outbound network access for internal resources.

FAILURE RESPONSE(S)

- Outbound rules are configured to permit All traffic to the Internet.

MORE INFO: HTTPS://D1.AWSSTATIC.COM/WHITEPAPERS/SECURITY/AWS_SECURITY_BEST_PRACTICES.PDF

ID: aws-core-23 Do any S3 buckets permit open access permissions or allow access to any authenticated AWS user?

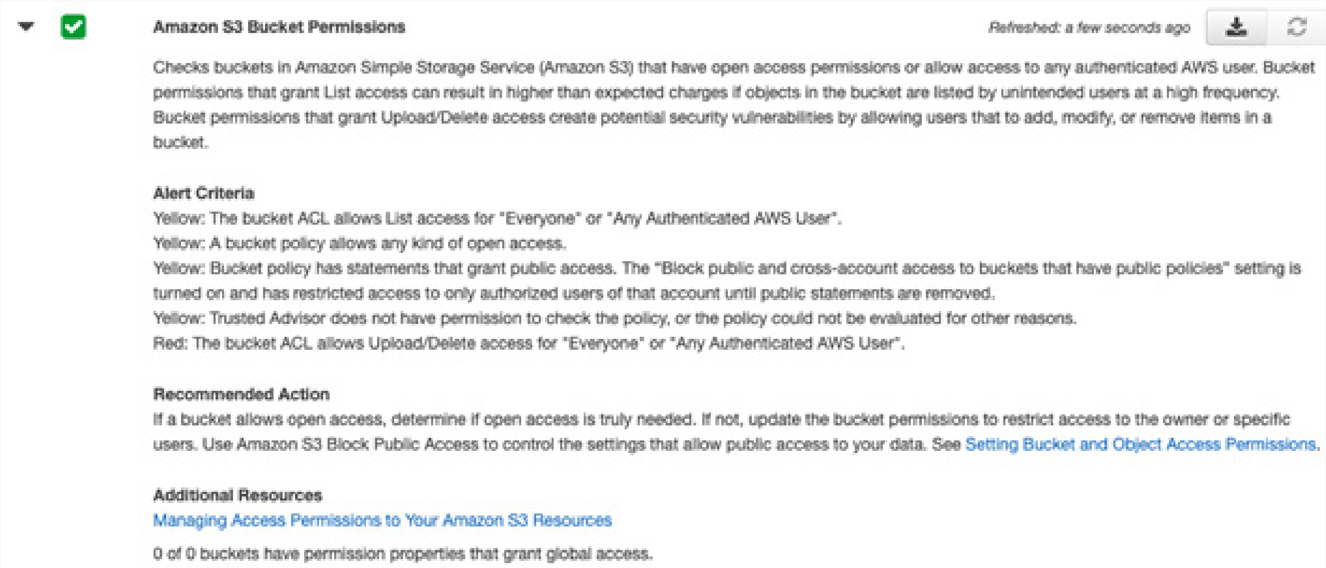
WHY IS THIS IMPORTANT?

Misconfigured S3 buckets are a common source of data breaches for companies moving to AWS. S3 bucket configurations should be regularly monitored and if possible block all public access using the account-level settings.

VALIDATION STEPS

In the Management Console select the Trusted Advisor service and select the Refresh button. Once the page is updated it will show the Amazon S3 Bucket Permissions action which will detail S3 buckets that permit open access. The following URL and screenshot can help validate the response:

- https://console.aws.amazon.com/trustedadvisor/home?region=us-east-1#/dashboard



☑ **Amazon S3 Bucket Permissions**

Refreshed: a few seconds ago

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions or allow access to any authenticated AWS user. Bucket permissions that grant List access can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant Upload/Delete access create potential security vulnerabilities by allowing users that to add, modify, or remove items in a bucket.

Alert Criteria
Yellow: The bucket ACL allows List access for "Everyone" or "Any Authenticated AWS User".
Yellow: A bucket policy allows any kind of open access.
Yellow: Bucket policy has statements that grant public access. The "Block public and cross-account access to buckets that have public policies" setting is turned on and has restricted access to only authorized users of that account until public statements are removed.
Yellow: Trusted Advisor does not have permission to check the policy, or the policy could not be evaluated for other reasons.
Red: The bucket ACL allows Upload/Delete access for "Everyone" or "Any Authenticated AWS User".

Recommended Action
If a bucket allows open access, determine if open access is truly needed. If not, update the bucket permissions to restrict access to the owner or specific users. Use Amazon S3 Block Public Access to control the settings that allow public access to your data. See Setting Bucket and Object Access Permissions.

Additional Resources
Managing Access Permissions to Your Amazon S3 Resources

0 of 0 buckets have permission properties that grant global access.

Figure 23: *Example of the Trusted Advisor action showing no buckets with open access*

ACCEPTABLE RESPONSE(S)

- No S3 buckets are configured to permit open access permissions or allow access to any authenticated AWS user.
- Some S3 buckets with objects intended for public access permit open access.

FAILURE RESPONSE(S)

- S3 buckets are configured to permit open access that may expose sensitive data.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/AMAZONS3/LATEST/DEV/SECURITY-BEST-PRACTICES.HTML

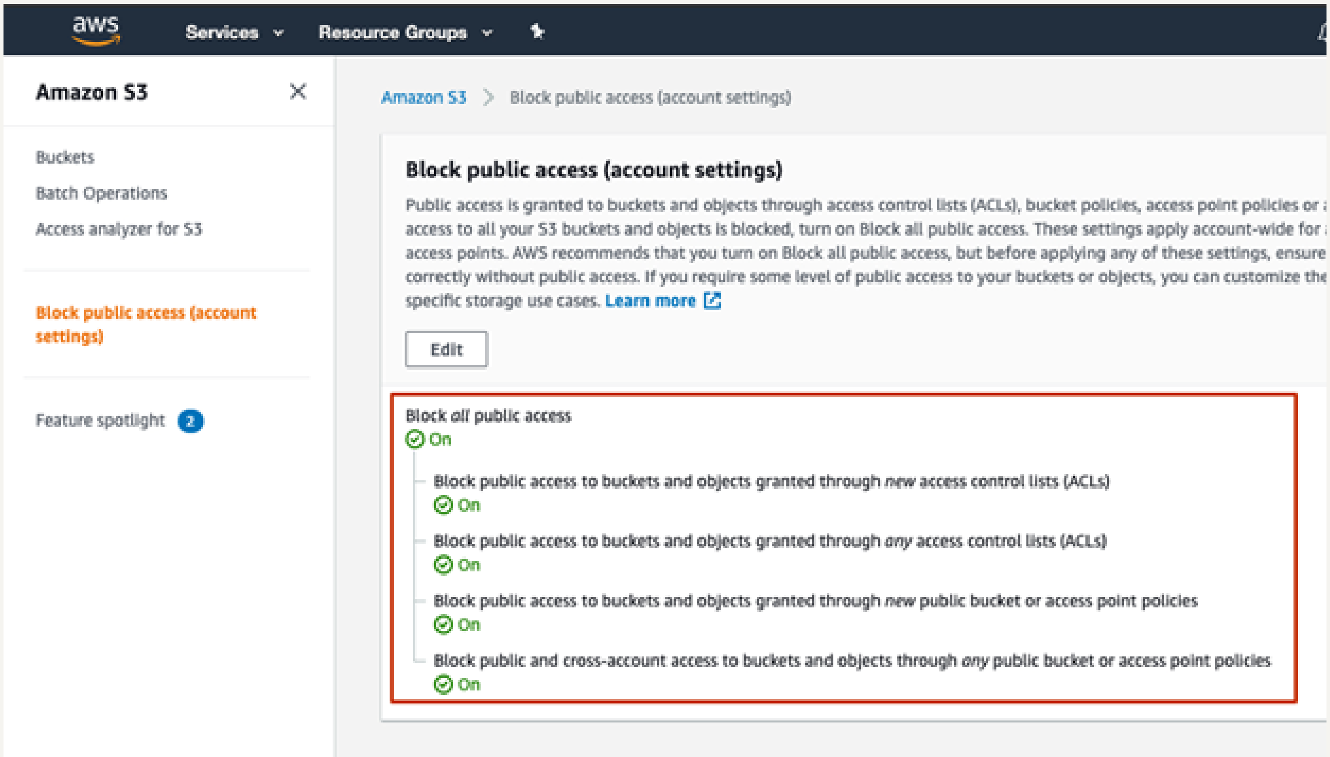
ID: aws-core-24 Are block public access settings enabled for all S3 buckets?

WHY IS THIS IMPORTANT?

Misconfigured S3 buckets are a common source of data breaches for companies moving to AWS. S3 bucket configurations should be regularly monitored and if possible block all public access using the account level settings.

VALIDATION STEPS

In the Management Console select the Amazon S3 service and select the Block Public access (account settings) view. Confirm Block all public access is configured as on. The following screenshot can help validate the response:



Block public access (account settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies or
access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply account-wide for
access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure
correctly without public access. If you require some level of public access to your buckets or objects, you can customize the
specific storage use cases. Learn more

Block *all* public access
On

- Block public access to buckets and objects granted through *new* access control lists (ACLs)
  On
- Block public access to buckets and objects granted through *any* access control lists (ACLs)
  On
- Block public access to buckets and objects granted through *new* public bucket or access point policies
  On
- Block public and cross-account access to buckets and objects through *any* public bucket or access point policies
  On

Figure 24: *Example of all Block public access settings enabled*

ACCEPTABLE RESPONSE(S)

- The 'Block all public access' option is turned on under the account settings.
- Some S3 buckets with objects intended for public access have Block public access options disabled however all other buckets have these settings enabled.

FAILURE RESPONSE(S)

- The Block public access options are disabled under account settings and within each bucket configuration.

MORE INFO: [HTTPS://DOCS.AWS.AMAZON.COM/AMAZONS3/LATEST/DEV/SECURITY-BEST-PRACTICES.HTML](https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.html)

DETECTION AND MONITORING

WHAT

The AWS Config service is enabled across the implementation and configured to inventory and report the configuration of all AWS assets. All systems are authorized and configured to security standards. Security event monitoring services are implemented and monitored.

WHY

Maintaining current knowledge of all assets and their configuration is essential to achieving good risk outcomes; you can't protect what you don't know exists or what you don't understand. Monitoring the environment for security events enables you to limit the impact of errors and incidents.

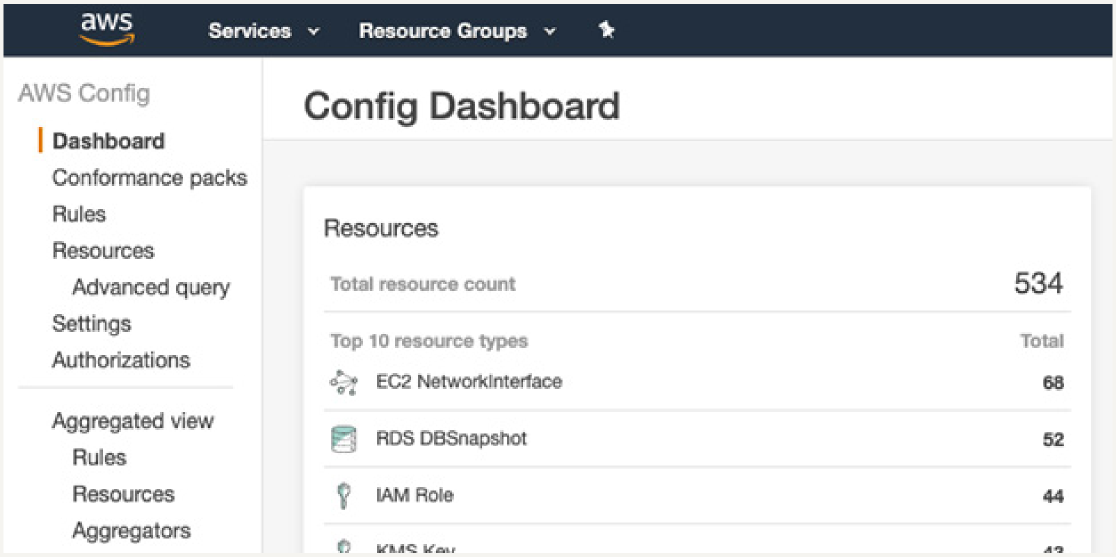
ID: aws-core-25 Is the AWS Config service enabled in all active regions?

WHY IS THIS IMPORTANT?

AWS Config provides the foundation for inventory gathering and configuration monitoring in AWS. In addition to providing an inventory of resources in each region, AWS Config integrates with other AWS services such as SecurityHub to identify misconfigurations. AWS Config can also automatically enforce or remediate misconfigurations using conformance packs and other rules.

VALIDATION STEPS

For each region with AWS resources, in the Management Console select the AWS Config service. Confirm the AWS config service is enabled including at least one region having global resources configured. The following screenshot can help validate the response:



Config Dashboard

Resources

Total resource count	534
Top 10 resource types	Total
EC2 NetworkInterface	68
RDS DBSnapshot	52
IAM Role	44
KMS Key	43

Figure 25: *Example of AWS Config enabled and recording resources in the AWS account*

ACCEPTABLE RESPONSE(S)

- AWS Config is enabled in all regions.
- AWS Config is enabled in all regions with AWS resources.

FAILURE RESPONSE(S)

- Multiple security groups are configured to permit non-HTTP service access for management or database ports.

MORE INFO: [HTTPS://DOCS.AWS.AMAZON.COM/CONFIG/LATEST/DEVELOPERGUIDE/WHATISCONFIG.HTML](https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html)

ID: aws-core-26 Is CloudTrail data events or access logs enabled for S3 buckets?

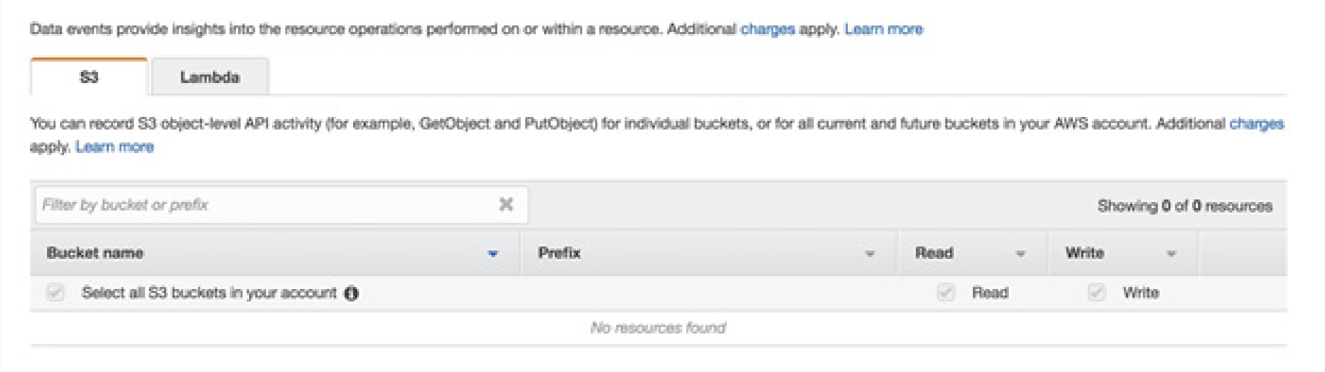
WHY IS THIS IMPORTANT?

By default there is limited audit logging enabled for actions against S3 buckets. In many cases, these buckets contain sensitive data and without additional audit logging there is no record of actions to access, modify or delete objects.

VALIDATION STEPS

In the Management Console select the CloudTrail service. Select a trail with S3 logging and confirm Data event logging is enabled for all current and future buckets. Alternatively, check S3 buckets to determine if access logging is enabled. The following screenshot can help validate the response:

- missing URL



Data events provide insights into the resource operations performed on or within a resource. Additional charges apply. Learn more

You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in your AWS account. Additional charges apply. Learn more

Filter by bucket or prefix ✕ Showing 0 of 0 resources

Bucket name	Prefix	Read	Write
☑ Select all S3 buckets in your account ⓘ		☑ Read	☑ Write

No resources found

Figure 26: *Example of a Trail with S3 data events enabled for all S3 buckets*

ACCEPTABLE RESPONSE(S)

- All S3 buckets are included in CloudTrail logging using the data events configuration.
- All S3 buckets containing important data have either CloudTrail logging using data events or access logging within the bucket configuration.

FAILURE RESPONSE(S)

- Neither S3 bucket access logging nor CloudTrail data events are configured to record audit events for S3 object actions.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/AWSCLOUDTRAIL/LATEST/USERGUIDE/LOGGING-DATA-EVENTS-WITH-CLOUDTRAIL.HTML

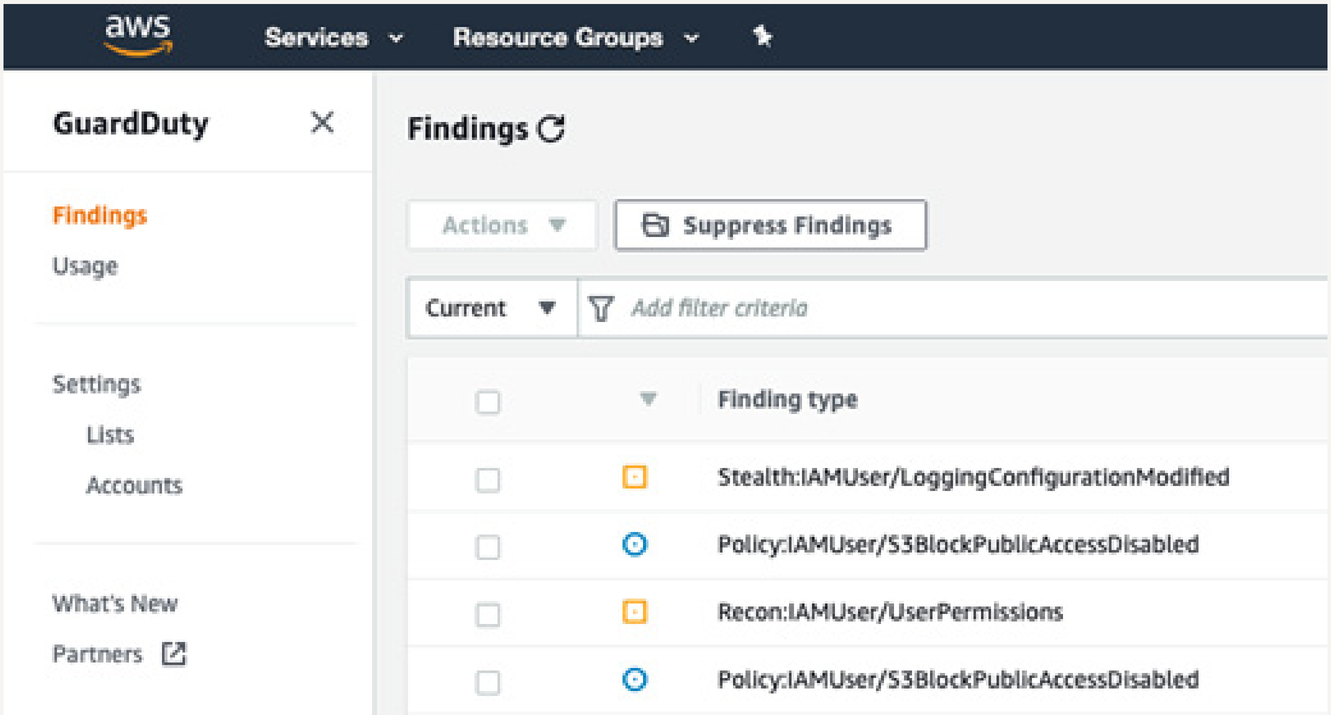
ID: aws-core-27 Is the GuardDuty service or other intrusion monitoring enabled in all active regions?

WHY IS THIS IMPORTANT?

GuardDuty offers a fully integrated intrusion monitoring solution that monitors both IAM and VPC flow activity. While the provided number of rules is limited, this AWS service provides an inexpensive and easily deployed solution to detect obvious intrusions into the AWS environment.

VALIDATION STEPS

For each region with AWS resources, in the Management Console select the GuardDuty service. Confirm the GuardDuty service is enabled in each active region. The following screenshot can help validate the response.



Finding type
Stealth:IAMUser/LoggingConfigurationModified
Policy:IAMUser/S3BlockPublicAccessDisabled
Recon:IAMUser/UserPermissions
Policy:IAMUser/S3BlockPublicAccessDisabled

Figure 27: *Example of GuardDuty being enabled and reporting findings*

ACCEPTABLE RESPONSE(S)

- GuardDuty or other intrusion monitoring solution is enabled within all active regions.

FAILURE RESPONSE(S)

- GuardDuty or other intrusion monitoring solution is not enabled.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/GUARDDUTY/LATEST/UG/WHAT-IS-GUARDDUTY.HTML

PROCESSES

WHAT

Methodologies and tools are used to reliably maintain the security of the environment.

WHY

Maintaining the security of the AWS environment using well established methodologies and tools helps ensure that desired outcomes are consistently achieved.

ID: aws-core-28 Are resources deployed within AWS using infrastructure as code (IaC) such as Terraform or CloudFormation?

WHY IS THIS IMPORTANT?

As the number of resources within an AWS environment grows it becomes increasingly difficult to manually deploy resources in a consistent manner. Without some form of automation there is an increased risk of misconfiguration. IaC solutions such as Terraform and CloudFormation provide methods to codify infrastructure and consistently deploy resources using this code against the AWS API.

VALIDATION STEPS

Obtain confirmation that resources are being deployed in an automated and consistent manner using a solution such as Terraform or CloudFormation.

ACCEPTABLE RESPONSE(S)

- Most AWS resources are deployed using IaC such as Terraform or CloudFormation.

FAILURE RESPONSE(S)

- AWS resources are deployed manually via the management console or API.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/AWSCLOUDFORMATION/LATEST/USERGUIDE/WELCOME.HTML

ID: aws-core-29 Are custom AMIs being regularly updated using a pipeline such as EC2 Image Builder or Packer?

WHY IS THIS IMPORTANT?

Use of older AMIs that have not been updated within a reasonable timeframe may result in deployment of new EC2 instances that start with unpatched vulnerabilities until fully updated. For interfacing services, this could lead to an exploitable vulnerability becoming accessible to the Internet as soon as the EC2 is deployed.

VALIDATION STEPS

Obtain confirmation that resources are being deployed in an automated and consistent manner using a solution such as Terraform or CloudFormation.

ACCEPTABLE RESPONSE(S)

- AMIs are regularly updated using an AMI pipeline.
- Custom AMIs are not being used within the AWS environment.

FAILURE RESPONSE(S)

- Custom AMIs have not been updated in > 6 months and are being used to deploy new EC2 instances.

MORE INFO: HTTPS://AWS.AMAZON.COM/IMAGE-BUILDER/

ID: aws-core-30 Has an AWS specific incident response plan been created and tested?

WHY IS THIS IMPORTANT?

Having an AWS specific incident response plan or playbook will help detail steps for handling an incident in the AWS environment. Incident response processes and steps often have to be customized for specific AWS services as they differ from on-premise resources. This includes documenting steps for investigation, forensics, containment, remediation and eradication.

VALIDATION STEPS

Obtain confirmation that an AWS specific incident response plan exists and has been tested.

ACCEPTABLE RESPONSE(S)

- An incident response plan exists that is specific to the AWS environment.

FAILURE RESPONSE(S)

- A general incident response plan exists but no specific steps or playbook for AWS environments.
- No incident response plan has been created.

MORE INFO: HTTPS://D1.AWSSTATIC.COM/WHITEPAPERS/AWS_SECURITY_INCIDENT_RESPONSE.PDF

ID: aws-core-31 Are S3 object and RDS snapshot backups stored in a dedicated AWS account for

WHY IS THIS IMPORTANT?

In the event the Production AWS account is compromised an attack may have the ability to delete backups stored within that account. To limit access to important backups they should be replicated or copied to a dedicated AWS account with limited access that does not overlap with the Production AWS account.

VALIDATION STEPS

Obtain confirmation that a backup solution has been implemented for important S3 objects and database backups.

ACCEPTABLE RESPONSE(S)

- Important S3 objects are replicated and RDS snapshots copied to a dedicated AWS account for backups.
- An alternative backup solution has been implemented to store files and database backups independent of the Production AWS account.

FAILURE RESPONSE(S)

- Backups are stored in the Production AWS account and no alternative backup solution has been implemented.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/AMAZONS3/LATEST/DEV/REPLICATION.HTML

ID: aws-core-32 Are EC2 instances regularly patched using system manager or other solution?

WHY IS THIS IMPORTANT?

Using an automated, monitored and scheduled patch management solution ensures timely and consistent updating of EC2 instances. Using manual methods may result in delayed security updates, lack of reporting and inconsistent application of patches.

VALIDATION STEPS

Obtain confirmation that a backup solution has been implemented for important S3 objects and database backups.

ACCEPTABLE RESPONSE(S)

- All EC2 instances are regularly patched using EC2 system manager.
- All EC2 instances are regularly patched using another patch management solution.

FAILURE RESPONSE(S)

- EC2 instances are manually patched on a schedule.
- EC2 instances are not regularly patched.

MORE INFO: HTTPS://AWS.AMAZON.COM/SYSTEMS-MANAGER/

ID: aws-core-33 How do you remotely access servers and databases hosted within AWS?

WHY IS THIS IMPORTANT?

Having management ports such as SSH, RDP and database services Internet accessible increases the risk of unauthorized access via brute forcing or exploitation of an unpatched vulnerability. Many management services are regularly targeted by automated scanners for exploitation and are not secure to access over the Internet. For example, many database services do not enforce an encrypted connection by default.

VALIDATION STEPS

Obtain confirmation that internal servers and databases are accessed using a bastion host or other remote access solution.

ACCEPTABLE RESPONSE(S)

- A bastion host is accessed using SSH and used to access internal servers and databases.
- A remote access solution such as AWS Systems Manager Session Manager or SSH proxy service is used to access internal servers and databases.

FAILURE RESPONSE(S)

- Internal servers and databases are directly accessed over the Internet.
- No steps are taken to limit Internet access to servers and databases.

MORE INFO: HTTPS://DOCS.AWS.AMAZON.COM/SYSTEMS-MANAGER/LATEST/USERGUIDE/SESSION-MANAGER.HTML

COPYRIGHT

The RiskRecon AWS Assessment Playbook by RiskRecon is licensed under a

CREATIVE COMMONS ATTRIBUTION-SHAREALIKE 4.0 INTERNATIONAL LICENSE.

LEGAL DISCLAIMER

RiskRecon, a Mastercard Company, makes no representations or warranties of any kind, express or implied, with respect to the contents of this document and the associated security questionnaire. Without limitation, RiskRecon specifically disclaims all representations and warranties, including but not limited to any and all implied warranties of merchantability, fitness or suitability for any purpose. Any action taken using the information in this document or the associated security questionnaire is strictly at the user's own risk.