DOCUMENT

NEVERFAIL
CONTINUOUS CONTROLS

CTAC AWS CONTENT GUIDE

Control Test Detailed Reference

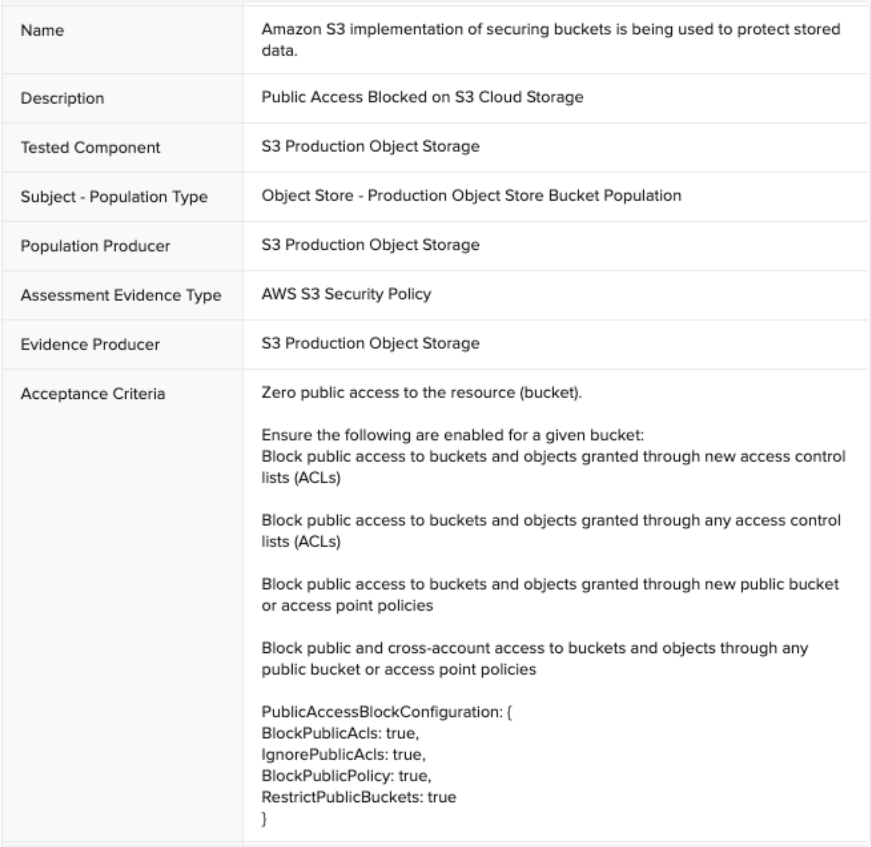
In this reference document, framework principles, population and evidence collection, evidence types, and assessment criteria will be provided. If a remediation bot exists for a particular test, this will also be annotated here.

AWS Control Tests Included

The following AWS Control Tests are included in your AWS Compliance Test Suite. More details are available in the Control Test Detailed Reference section below.

- Public Access Blocked on S3 Cloud Storage
- Production EC2 Instances Have RPO Less Than 48 Hours
- EC2 Instance Volumes Have Backup Policy Assigned
- Production RDS Databases Have RPO Less than 48 Hours
- Production RDS Databases Have Secure Configuration

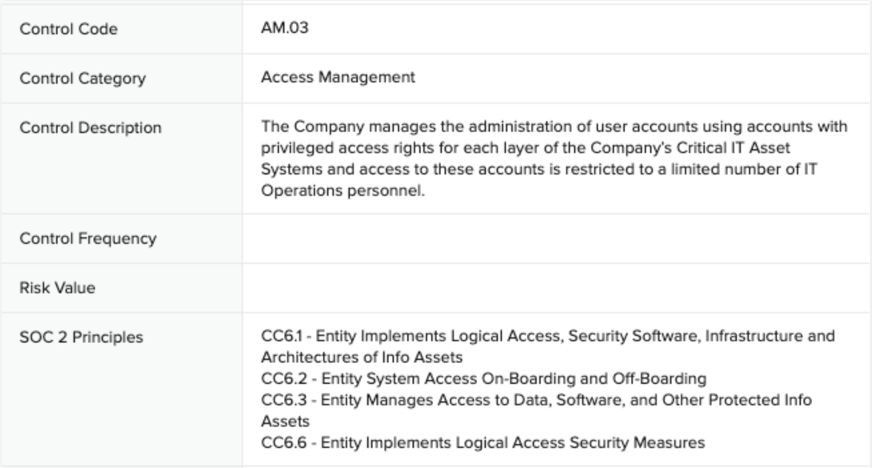
Control Test: Public Access Blocked on S3 Cloud Storage



Name	Amazon S3 implementation of securing buckets is being used to protect stored data.
Description	Public Access Blocked on S3 Cloud Storage
Tested Component	S3 Production Object Storage
Subject - Population Type	Object Store - Production Object Store Bucket Population
Population Producer	S3 Production Object Storage
Assessment Evidence Type	AWS S3 Security Policy
Evidence Producer	S3 Production Object Storage

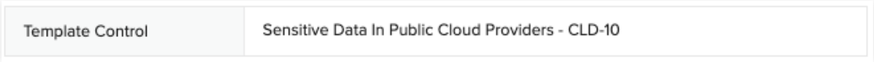
Acceptance Criteria	Zero public access to the resource (bucket).
	Ensure the following are enabled for a given bucket:
	Block public access to buckets and objects granted through new access control lists (ACLs)
	Block public access to buckets and objects granted through any access control lists (ACLs)
	Block public access to buckets and objects granted through new public bucket or access point policies
	Block public and cross-account access to buckets and objects through any public bucket or access point policies
	PublicAccessBlockConfiguration: {
	BlockPublicAcls: true,
	IgnorePublicAcls: true,
	BlockPublicPolicy: true,
	RestrictPublicBuckets: true
	}

Sample Auditee SOC 2 Control and Principles



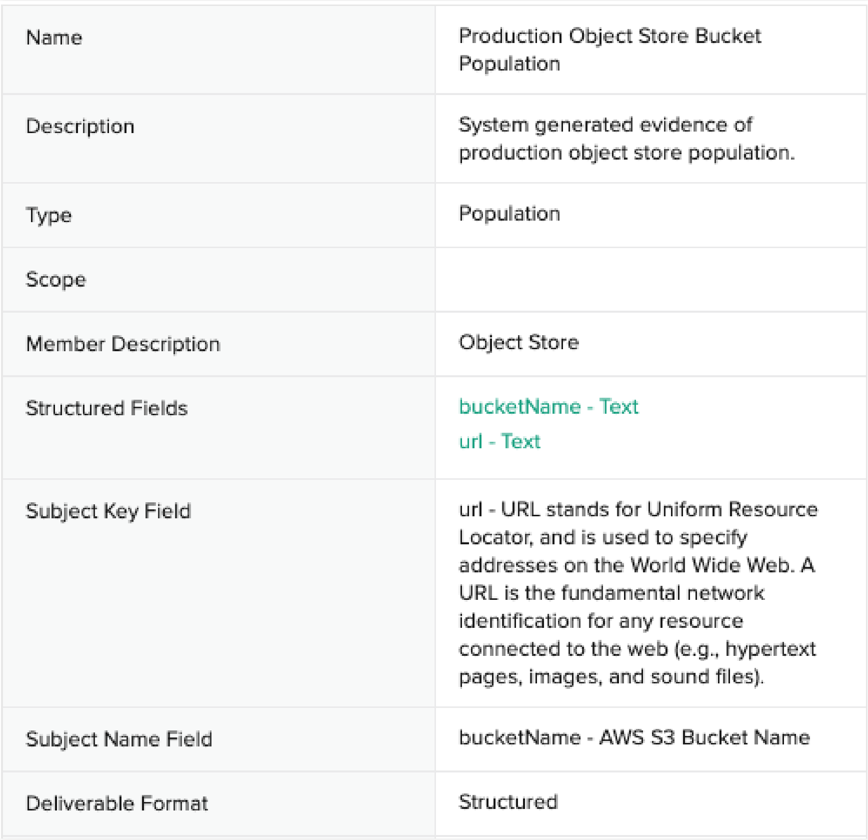
Control Code	AM.03
Control Category	Access Management
Control Description	The Company manages the administration of user accounts using accounts with privileged access rights for each layer of the Company's Critical IT Asset Systems and access to these accounts is restricted to a limited number of IT Operations personnel.
Control Frequency	
Risk Value	
SOC 2 Principles	CC6.1 - Entity Implements Logical Access, Security Software, Infrastructure and Architectures of Info Assets CC6.2 - Entity System Access On-Boarding and Off-Boarding CC6.3 - Entity Manages Access to Data, Software, and Other Protected Info Assets CC6.6 - Entity Implements Logical Access Security Measures

SOC 2 Template Controls and Principles



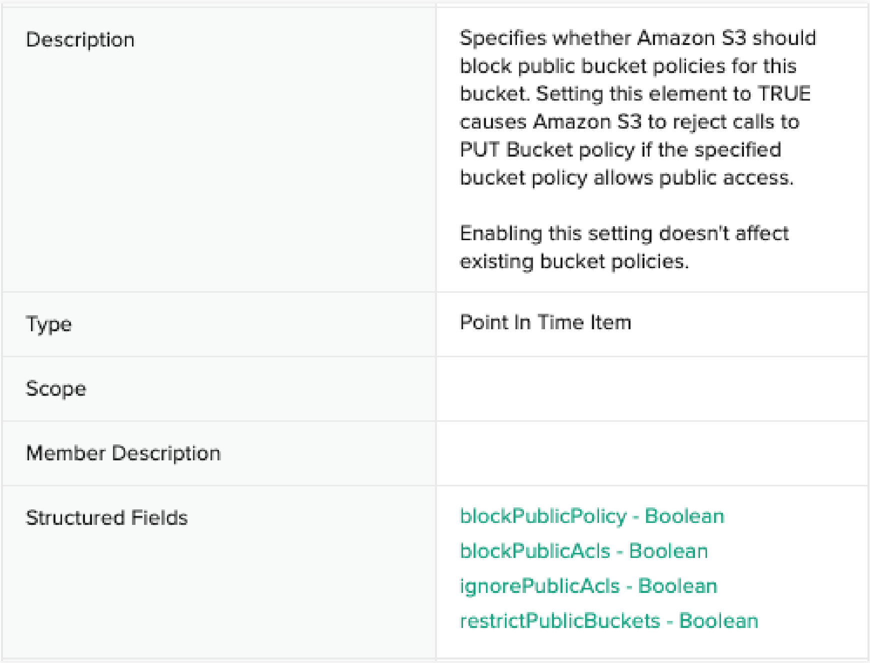
Template Control	Sensitive Data In Public Cloud Providers - CLD-10

Population: Production Object Store Buckets



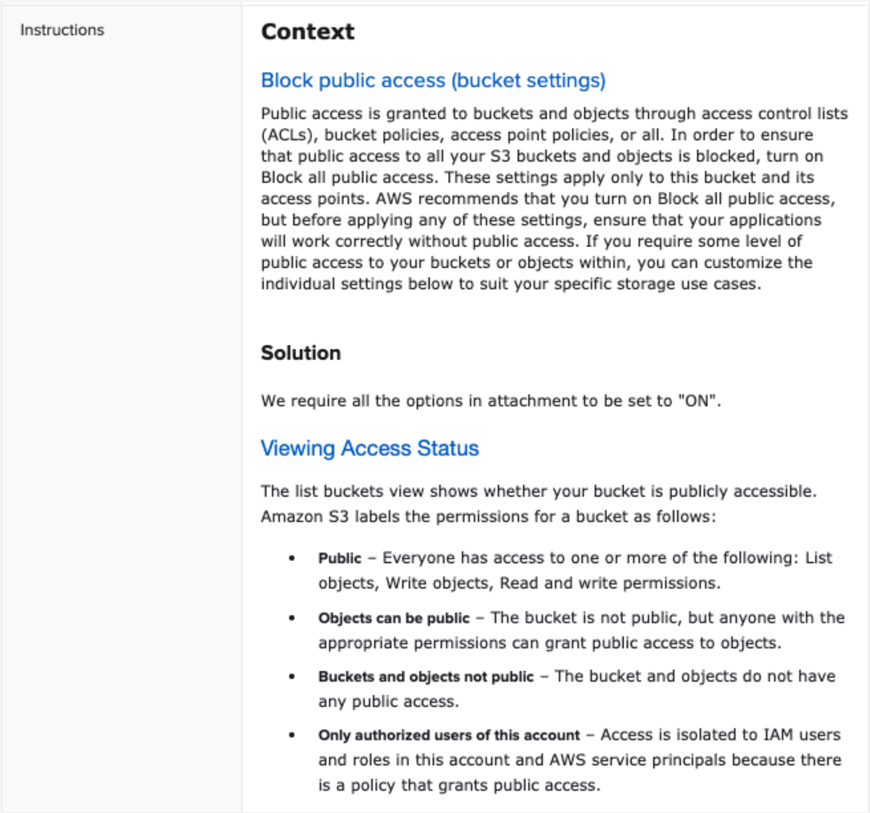
Name	Production Object Store Bucket Population
Description	System generated evidence of production object store population.
Type	Population
Scope	
Member Description	Object Store
Structured Fields	bucketName - Text url - Text
Subject Key Field	url - URL stands for Uniform Resource Locator, and is used to specify addresses on the World Wide Web. A URL is the fundamental network identification for any resource connected to the web (e.g., hypertext pages, images, and sound files).
Subject Name Field	bucketName - AWS S3 Bucket Name
Deliverable Format	Structured

Evidence: AWS S3 Bucket Security Policy



Description	Specifies whether Amazon S3 should block public bucket policies for this bucket. Setting this element to TRUE causes Amazon S3 to reject calls to PUT Bucket policy if the specified bucket policy allows public access. Enabling this setting doesn't affect existing bucket policies.
Type	Point In Time Item
Scope	
Member Description	
Structured Fields	blockPublicPolicy - Boolean blockPublicAcls - Boolean ignorePublicAcls - Boolean restrictPublicBuckets - Boolean

Evidence Collection KB: How to get AWS S3 Bucket Security Policy



Instructions

Context

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases.

Solution

We require all the options in attachment to be set to "ON".

Viewing Access Status

The list buckets view shows whether your bucket is publicly accessible. Amazon S3 labels the permissions for a bucket as follows:

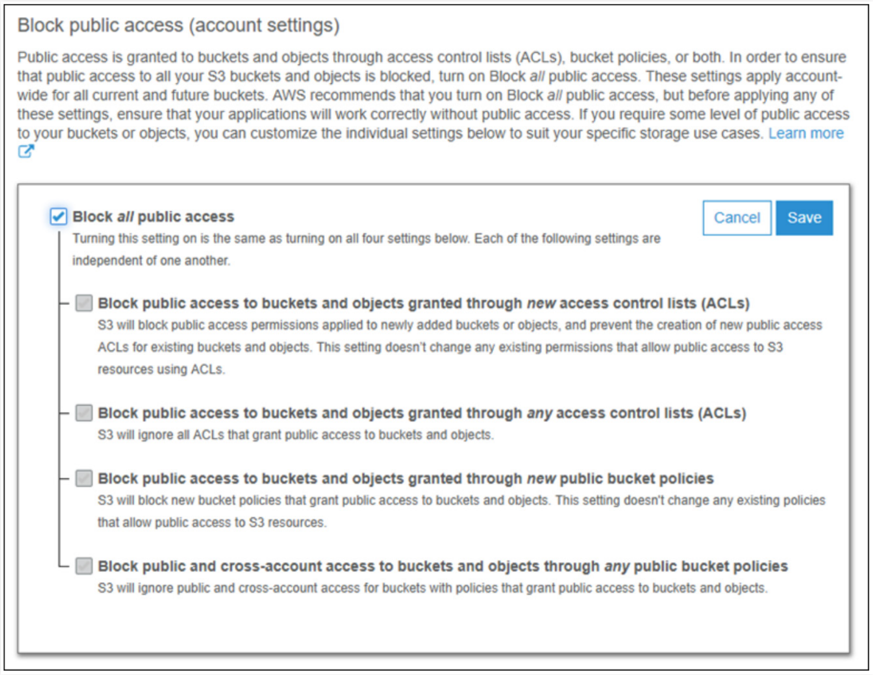
- **Public** – Everyone has access to one or more of the following: List objects, Write objects, Read and write permissions.
- **Objects can be public** – The bucket is not public, but anyone with the appropriate permissions can grant public access to objects.
- **Buckets and objects not public** – The bucket and objects do not have any public access.
- **Only authorized users of this account** – Access is isolated to IAM users and roles in this account and AWS service principals because there is a policy that grants public access.

Automated Assessment Gherkin

Gherkin	Scenario: Check if amazon buckets are publicly exposed Given an amazon bucket as subject from a list of buckets And a public policy for selected bucket as evidence When I get the values of blockPublicPolicy, blockPuclicAcls, ignorePublicAcls, restrictPublicBuckets Then values should be set to true

Remediation Bot: Block S3 bucket public access

The CTAC remediation bot uses S3 APIs to block all public access. For more information: [Using Amazon S3 block public access](#).



Block public access (account settings)

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

☑ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

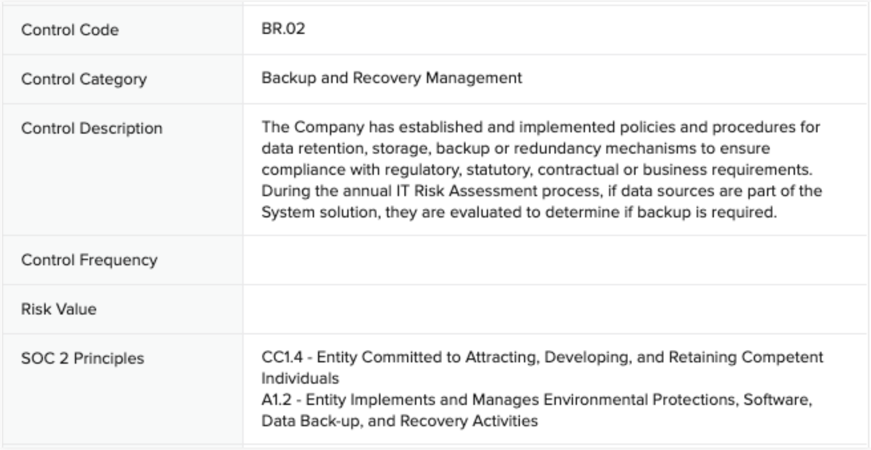
☐ **Block public access to buckets and objects granted through *new* public bucket policies**
S3 will block new bucket policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through *any* public bucket policies**
S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.

Control Test: Production EC2 instances have RPO less than 48 hours

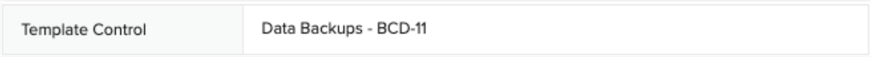
Description	Production EC2 instances have RPO less than 48 hours
Tested Component	AWS EC2 - US Regions
Subject - Population Type	EBS Volume - Volumes attached to EC2 Instances per US Region
Population Producer	AWS EC2 - US Regions
Assessment Evidence Type	Volume Snapshots
Evidence Producer	AWS EC2 - US Regions
Acceptance Criteria	Given a list of EC2 instances, check if each volume attached to that instance has at least one snapshot in last 48 hours.

Sample Auditee SOC 2 Control and Principles



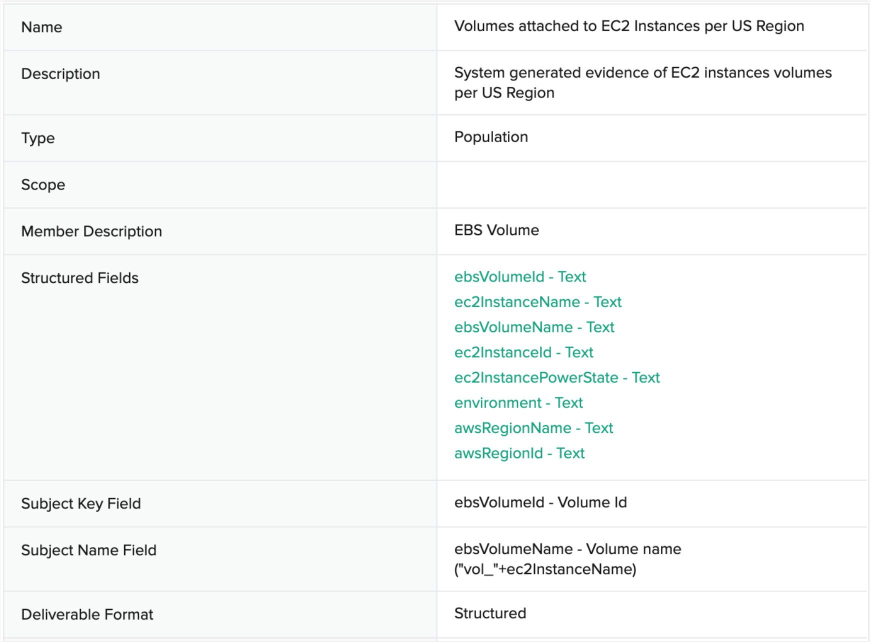
Control Code	BR.02
Control Category	Backup and Recovery Management
Control Description	The Company has established and implemented policies and procedures for data retention, storage, backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements. During the annual IT Risk Assessment process, if data sources are part of the System solution, they are evaluated to determine if backup is required.
Control Frequency	
Risk Value	
SOC 2 Principles	CC1.4 - Entity Committed to Attracting, Developing, and Retaining Competent Individuals A1.2 - Entity Implements and Manages Environmental Protections, Software, Data Back-up, and Recovery Activities

SOC 2 Template Controls and Principles



Template Control	Data Backups - BCD-11

Population: EBS Volumes attached to Production EC2 Instances - US Regions

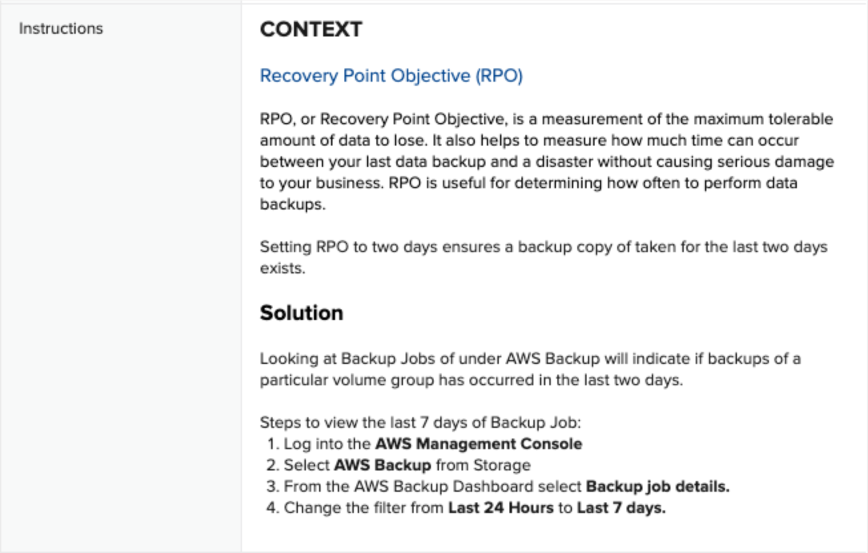


Name	Volumes attached to EC2 Instances per US Region
Description	System generated evidence of EC2 instances volumes per US Region
Type	Population
Scope	
Member Description	EBS Volume
Structured Fields	ebsVolumeId - Text ec2InstanceName - Text ebsVolumeName - Text ec2InstanceId - Text ec2InstancePowerState - Text environment - Text awsRegionName - Text awsRegionId - Text
Subject Key Field	ebsVolumeId - Volume Id
Subject Name Field	ebsVolumeName - Volume name ("vol_"+ec2InstanceName)
Deliverable Format	Structured

Evidence: Volume Snapshots

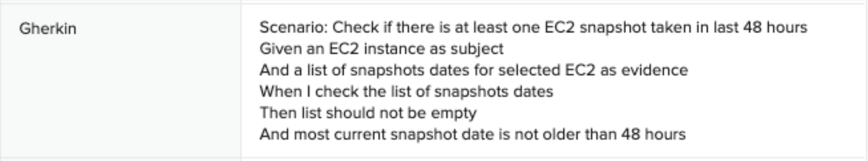
Description	System generated evidence of snapshot dates
Type	Population
Scope	
Member Description	
Structured Fields	snapshotDateTimestampList - Text ebsVolumeId - Text ec2InstanceName - Text ec2InstanceId - Text
Subject Key Field	ebsVolumeId - Volume Id
Subject Name Field	ebsVolumeId - Volume Id
Deliverable Format	Structured

Evidence Collection KB: How to get Volume Snapshots from Amazon Elastic Container Service (Amazon ECS)



Instructions	**CONTEXT** Recovery Point Objective (RPO) RPO, or Recovery Point Objective, is a measurement of the maximum tolerable amount of data to lose. It also helps to measure how much time can occur between your last data backup and a disaster without causing serious damage to your business. RPO is useful for determining how often to perform data backups. Setting RPO to two days ensures a backup copy of taken for the last two days exists. **Solution** Looking at Backup Jobs of under AWS Backup will indicate if backups of a particular volume group has occurred in the last two days. Steps to view the last 7 days of Backup Job: 1. Log into the **AWS Management Console** 2. Select **AWS Backup** from Storage 3. From the AWS Backup Dashboard select **Backup job details.** 4. Change the filter from **Last 24 Hours** to **Last 7 days.**

Automated Assessment

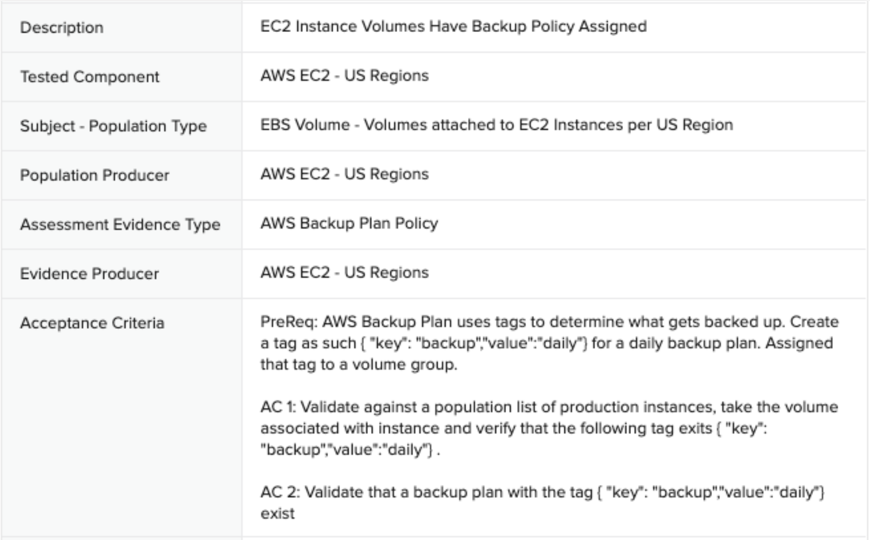


Gherkin	Scenario: Check if there is at least one EC2 snapshot taken in last 48 hours Given an EC2 instance as subject And a list of snapshots dates for selected EC2 as evidence When I check the list of snapshots dates Then list should not be empty And most current snapshot date is not older than 48 hours

Remediation Bot

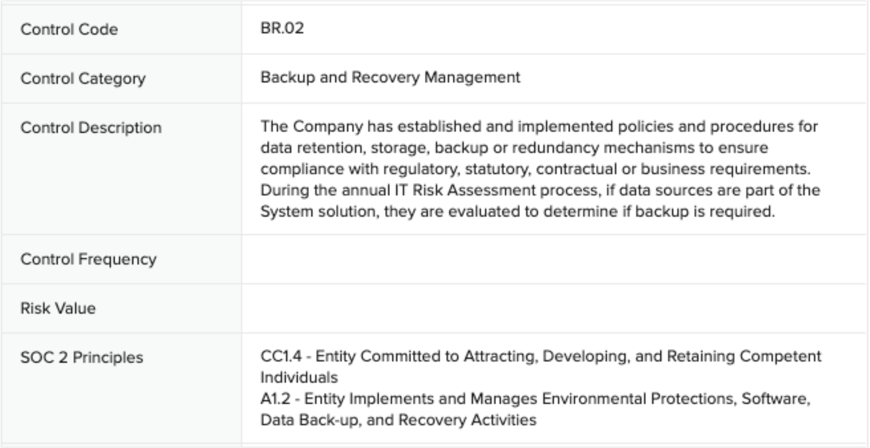
Remediation automation bot for this condition is still pending.

Control Test: Production EC2 Instance Volumes Have Backup Policy Assigned via Rule



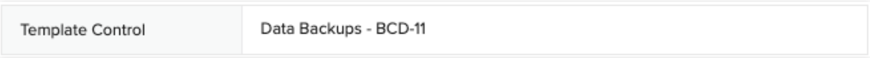
Description	EC2 Instance Volumes Have Backup Policy Assigned
Tested Component	AWS EC2 - US Regions
Subject - Population Type	EBS Volume - Volumes attached to EC2 Instances per US Region
Population Producer	AWS EC2 - US Regions
Assessment Evidence Type	AWS Backup Plan Policy
Evidence Producer	AWS EC2 - US Regions
Acceptance Criteria	PreReq: AWS Backup Plan uses tags to determine what gets backed up. Create a tag as such { "key": "backup","value":"daily"} for a daily backup plan. Assigned that tag to a volume group. AC 1: Validate against a population list of production instances, take the volume associated with instance and verify that the following tag exits { "key": "backup","value":"daily"} . AC 2: Validate that a backup plan with the tag { "key": "backup","value":"daily"} exist

Sample Auditee SOC 2 Control and Principles



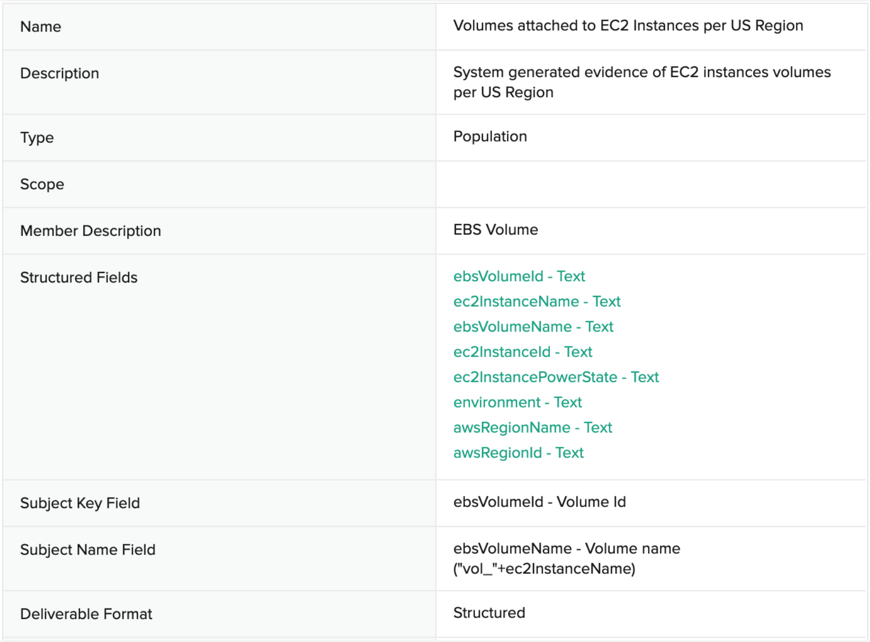
Control Code	BR.02
Control Category	Backup and Recovery Management
Control Description	The Company has established and implemented policies and procedures for data retention, storage, backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements. During the annual IT Risk Assessment process, if data sources are part of the System solution, they are evaluated to determine if backup is required.
Control Frequency	
Risk Value	
SOC 2 Principles	CC1.4 - Entity Committed to Attracting, Developing, and Retaining Competent Individuals A1.2 - Entity Implements and Manages Environmental Protections, Software, Data Back-up, and Recovery Activities

SOC 2 Template Controls and Principles



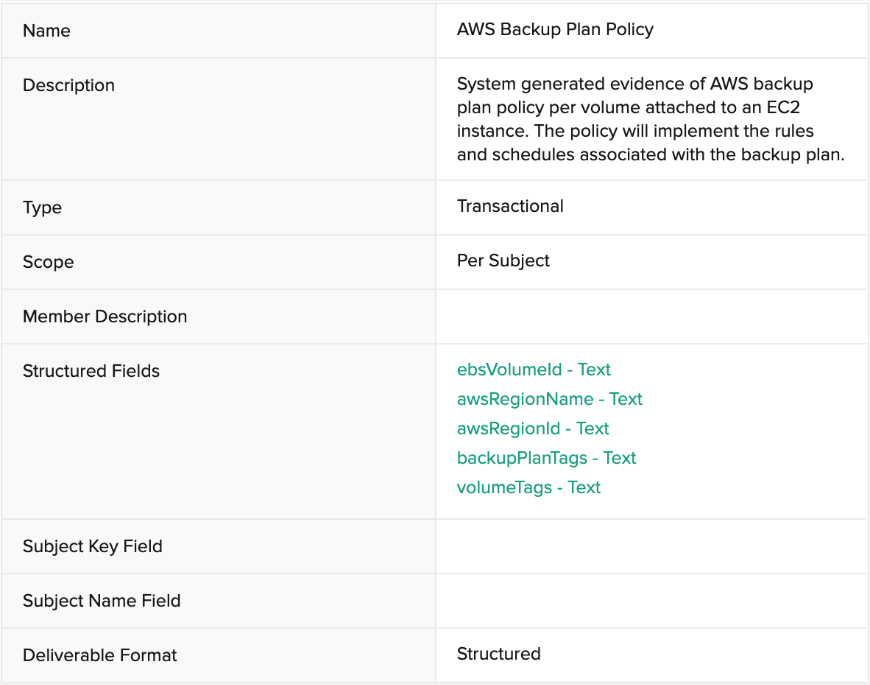
Template Control	Data Backups - BCD-11

Population: EBS Volumes attached to Production EC2 Instances - US Regions



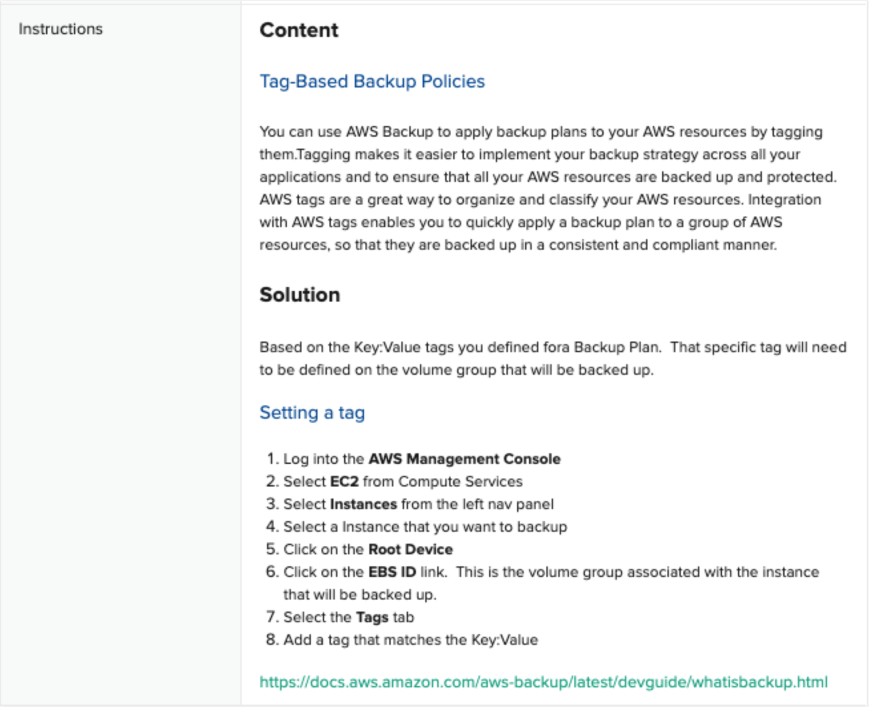
Name	Volumes attached to EC2 Instances per US Region
Description	System generated evidence of EC2 instances volumes per US Region
Type	Population
Scope	
Member Description	EBS Volume
Structured Fields	ebsVolumeId - Text ec2InstanceName - Text ebsVolumeName - Text ec2InstanceId - Text ec2InstancePowerState - Text environment - Text awsRegionName - Text awsRegionId - Text
Subject Key Field	ebsVolumeId - Volume Id
Subject Name Field	ebsVolumeName - Volume name ("vol_"+ec2InstanceName)
Deliverable Format	Structured

Evidence: AWS Backup Plan Policy



Name	AWS Backup Plan Policy
Description	System generated evidence of AWS backup plan policy per volume attached to an EC2 instance. The policy will implement the rules and schedules associated with the backup plan.
Type	Transactional
Scope	Per Subject
Member Description	
Structured Fields	ebsVolumeId - Text awsRegionName - Text awsRegionId - Text backupPlanTags - Text volumeTags - Text
Subject Key Field	
Subject Name Field	
Deliverable Format	Structured

Evidence Collection KB: How to get AWS Backup Plan Policy



Instructions

Content

Tag-Based Backup Policies

You can use AWS Backup to apply backup plans to your AWS resources by tagging them.Tagging makes it easier to implement your backup strategy across all your applications and to ensure that all your AWS resources are backed up and protected. AWS tags are a great way to organize and classify your AWS resources. Integration with AWS tags enables you to quickly apply a backup plan to a group of AWS resources, so that they are backed up in a consistent and compliant manner.

Solution

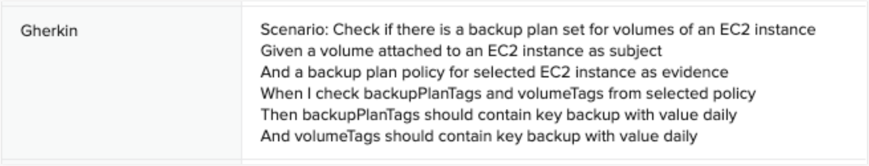
Based on the Key:Value tags you defined fora Backup Plan. That specific tag will need to be defined on the volume group that will be backed up.

Setting a tag

1. Log into the **AWS Management Console**
2. Select **EC2** from Compute Services
3. Select **Instances** from the left nav panel
4. Select a Instance that you want to backup
5. Click on the **Root Device**
6. Click on the **EBS ID** link. This is the volume group associated with the instance that will be backed up.
7. Select the **Tags** tab
8. Add a tag that matches the Key:Value

https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html

Automated Assessment



Gherkin

```
Scenario: Check if there is a backup plan set for volumes of an EC2 instance
Given a volume attached to an EC2 instance as subject
And a backup plan policy for selected EC2 instance as evidence
When I check backupPlanTags and volumeTags from selected policy
Then backupPlanTags should contain key backup with value daily
And volumeTags should contain key backup with value daily
```

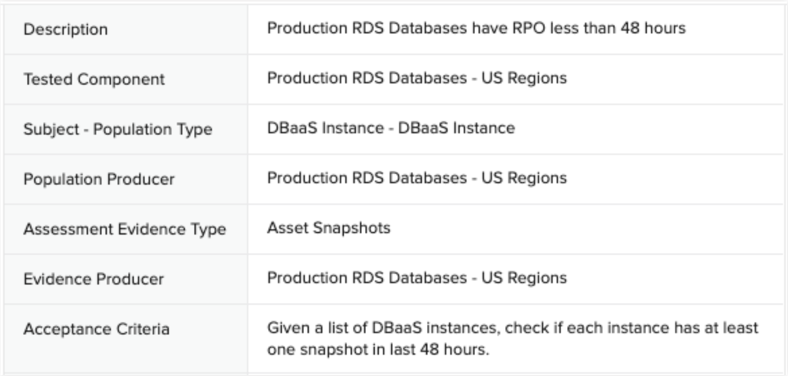
Remediation Bot: Set AWS Backup Plan Policy by Tag

In this case, the remediation bot re-applies a tag to the volume which will add it to a Backup Plan Policy based on the value of this tag. For the purposes of the POC, the uses the following example tag, but in your real AWS environment, any tag can be configured on a customer-specific basis:

“Key”: “backup”,

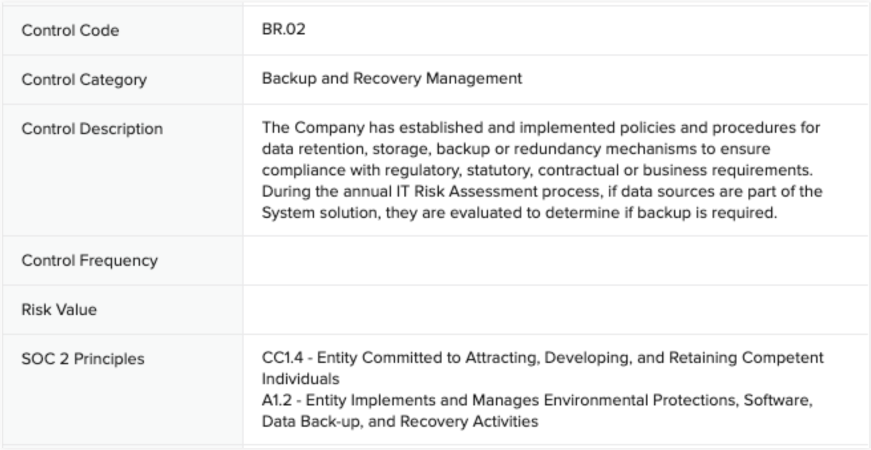
“Value”: “daily”

Control Test: Production RDS Databases Have RPO Less than 48 Hours



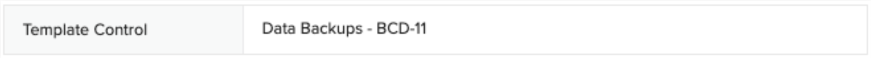
Description	Production RDS Databases have RPO less than 48 hours
Tested Component	Production RDS Databases - US Regions
Subject - Population Type	DBaaS Instance - DBaaS Instance
Population Producer	Production RDS Databases - US Regions
Assessment Evidence Type	Asset Snapshots
Evidence Producer	Production RDS Databases - US Regions
Acceptance Criteria	Given a list of DBaaS instances, check if each instance has at least one snapshot in last 48 hours.

Sample Auditee SOC 2 Control and Principles



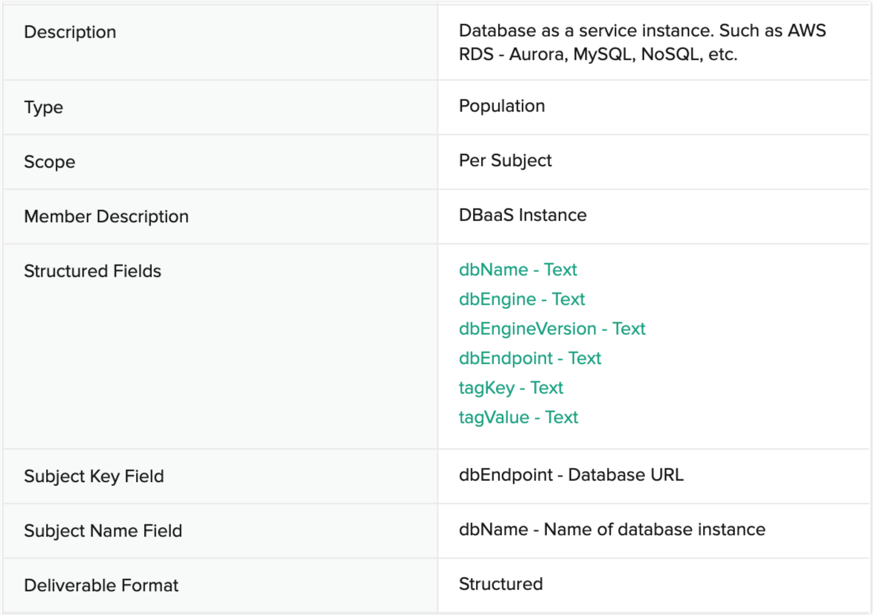
Control Code	BR.02
Control Category	Backup and Recovery Management
Control Description	The Company has established and implemented policies and procedures for data retention, storage, backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements. During the annual IT Risk Assessment process, if data sources are part of the System solution, they are evaluated to determine if backup is required.
Control Frequency	
Risk Value	
SOC 2 Principles	CC1.4 - Entity Committed to Attracting, Developing, and Retaining Competent Individuals A1.2 - Entity Implements and Manages Environmental Protections, Software, Data Back-up, and Recovery Activities

SOC 2 Template Controls and Principles



Template Control	Data Backups - BCD-11

Population: DBaaS Instances - US Regions

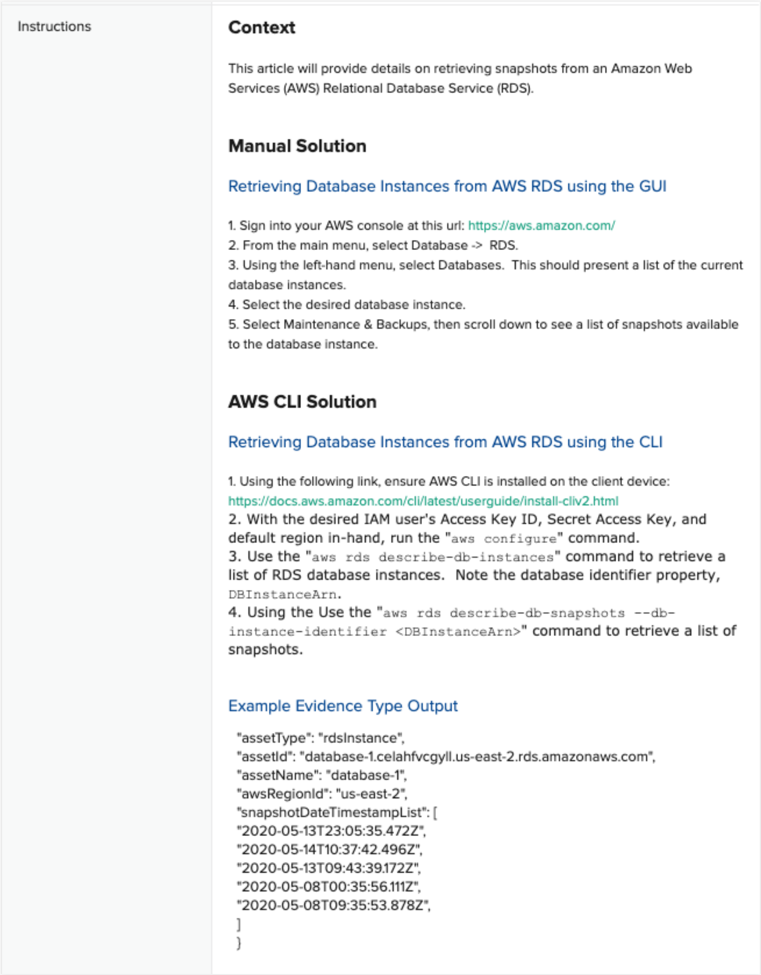


Description	Database as a service instance. Such as AWS RDS - Aurora, MySQL, NoSQL, etc.
Type	Population
Scope	Per Subject
Member Description	DBaaS Instance
Structured Fields	dbName - Text dbEngine - Text dbEngineVersion - Text dbEndpoint - Text tagKey - Text tagValue - Text
Subject Key Field	dbEndpoint - Database URL
Subject Name Field	dbName - Name of database instance
Deliverable Format	Structured

Evidence: Asset Snapshots

Name	Asset Snapshots
Description	List of available snapshots for a given entity.
Type	Point In Time Item
Scope	
Member Description	
Structured Fields	assetType - Text assetName - Text snapshotDateTimestampList - Text assetID - Text backupPolicySchedule - Text
Subject Key Field	
Subject Name Field	
Deliverable Format	Structured
Example	
KB Articles	How to get Asset Snapshots from AWS Relational Database Service (RDS)

Evidence Collection KB: How to get Asset Snapshots from AWS Relational Database Service (RDS)



Instructions

Context

This article will provide details on retrieving snapshots from an Amazon Web Services (AWS) Relational Database Service (RDS).

Manual Solution

Retrieving Database Instances from AWS RDS using the GUI

1. Sign into your AWS console at this url: https://aws.amazon.com/
2. From the main menu, select Database -> RDS.
3. Using the left-hand menu, select Databases. This should present a list of the current database instances.
4. Select the desired database instance.
5. Select Maintenance & Backups, then scroll down to see a list of snapshots available to the database instance.

AWS CLI Solution

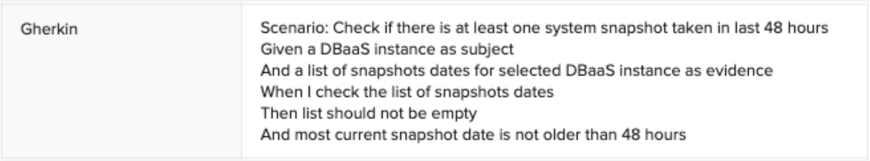
Retrieving Database Instances from AWS RDS using the CLI

1. Using the following link, ensure AWS CLI is installed on the client device: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html
2. With the desired IAM user's Access Key ID, Secret Access Key, and default region in-hand, run the "`aws configure`" command.
3. Use the "`aws rds describe-db-instances`" command to retrieve a list of RDS database instances. Note the database identifier property, `DBInstanceArn`.
4. Using the Use the "`aws rds describe-db-snapshots --db-instance-identifier <DBInstanceArn>`" command to retrieve a list of snapshots.

Example Evidence Type Output

```
"assetType": "rdsInstance",
"assetId": "database-1.celahfvcgyll.us-east-2.rds.amazonaws.com",
"assetName": "database-1",
"awsRegionId": "us-east-2",
"snapshotDateTimestampList": [
"2020-05-13T23:05:35.472Z",
"2020-05-14T10:37:42.496Z",
"2020-05-13T09:43:39.172Z",
"2020-05-08T00:35:56.111Z",
"2020-05-08T09:35:53.878Z",
]
}
```

Automated Assessment

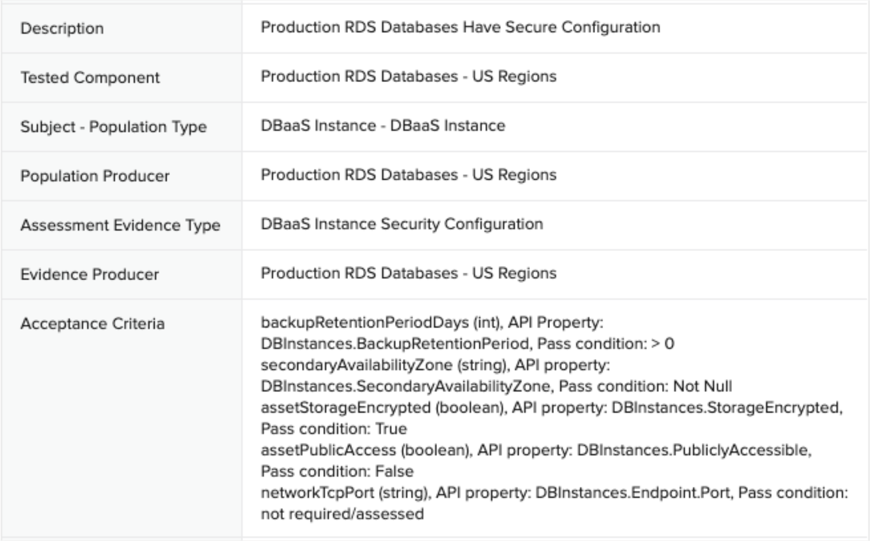


Gherkin	Scenario: Check if there is at least one system snapshot taken in last 48 hours Given a DBaaS instance as subject And a list of snapshots dates for selected DBaaS instance as evidence When I check the list of snapshots dates Then list should not be empty And most current snapshot date is not older than 48 hours

Remediation Bot: Create RDS DBaaS Instance Snapshot

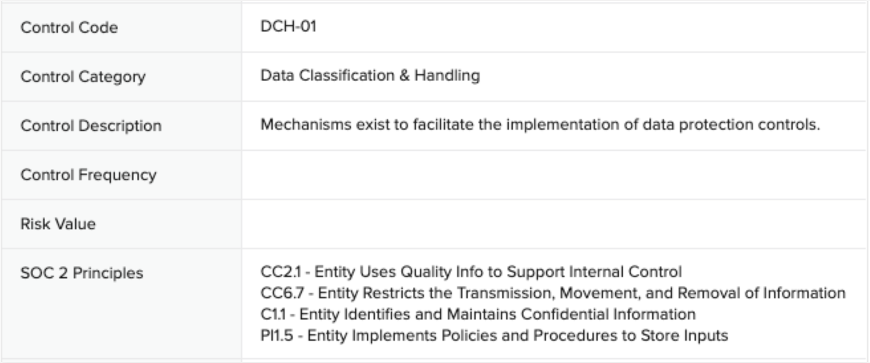
Remediation automation bot for this condition is still pending.

Control Test: Production RDS Databases Have Secure Configuration



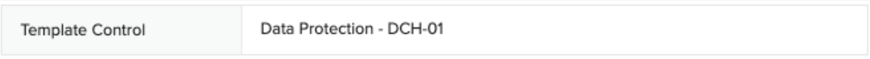
Description	Production RDS Databases Have Secure Configuration
Tested Component	Production RDS Databases - US Regions
Subject - Population Type	DBaaS Instance - DBaaS Instance
Population Producer	Production RDS Databases - US Regions
Assessment Evidence Type	DBaaS Instance Security Configuration
Evidence Producer	Production RDS Databases - US Regions
Acceptance Criteria	backupRetentionPeriodDays (int), API Property: DBInstances.BackupRetentionPeriod, Pass condition: > 0 secondaryAvailabilityZone (string), API property: DBInstances.SecondaryAvailabilityZone, Pass condition: Not Null assetStorageEncrypted (boolean), API property: DBInstances.StorageEncrypted, Pass condition: True assetPublicAccess (boolean), API property: DBInstances.PubliclyAccessible, Pass condition: False networkTcpPort (string), API property: DBInstances.Endpoint.Port, Pass condition: not required/assessed

Sample Auditee SOC 2 Control and Principles



Control Code	DCH-01
Control Category	Data Classification & Handling
Control Description	Mechanisms exist to facilitate the implementation of data protection controls.
Control Frequency	
Risk Value	
SOC 2 Principles	CC2.1 - Entity Uses Quality Info to Support Internal Control CC6.7 - Entity Restricts the Transmission, Movement, and Removal of Information C1.1 - Entity Identifies and Maintains Confidential Information PI1.5 - Entity Implements Policies and Procedures to Store Inputs

SOC 2 Template Controls and Principles



Template Control	Data Protection - DCH-01

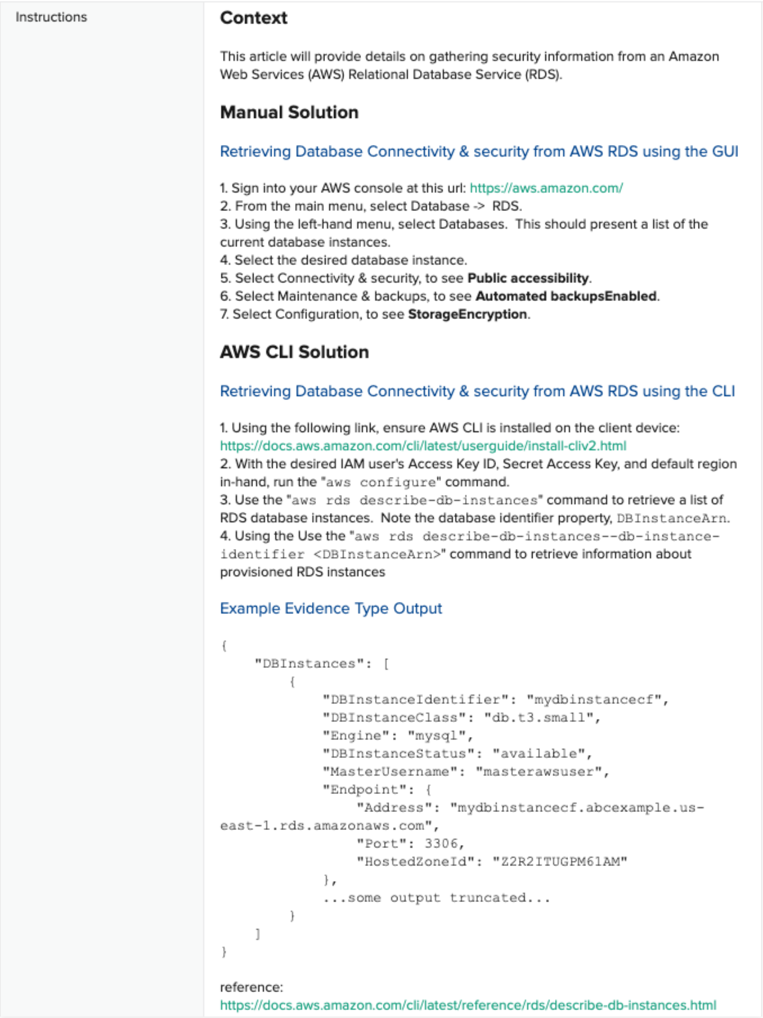
Population: DBaaS Instances - US Regions

Description	Database as a service instance. Such as AWS RDS - Aurora, MySQL, NoSQL, etc.
Type	Population
Scope	Per Subject
Member Description	DBaaS Instance
Structured Fields	dbName - Text dbEngine - Text dbEngineVersion - Text dbEndpoint - Text tagKey - Text tagValue - Text
Subject Key Field	dbEndpoint - Database URL
Subject Name Field	dbName - Name of database instance
Deliverable Format	Structured

Evidence: DBaaS Instance Security Configuration

Name	DBaaS Instance Security Configuration
Description	Describes several important security and integrity configurations for a DB software instance on a typical cloud provider, such as AWS.
Type	Transactional
Scope	Per Subject
Member Description	Configuration
Structured Fields	assetType - Text assetName - Text assetID - Text tagKey - Text tagValue - Text backupRetentionPeriodDays - Number secondaryAvailabilityZone - Text assetStorageEncrypted - Boolean assetPublicAccess - Boolean tcpPort - Text
Subject Key Field	assetID - Unique label for given asset
Subject Name Field	assetName - Asset Name
Deliverable Format	Structured

Evidence Collection KB: How to get DBaaS Instance Security Configuration



Instructions

Context

This article will provide details on gathering security information from an Amazon Web Services (AWS) Relational Database Service (RDS).

Manual Solution

Retrieving Database Connectivity & security from AWS RDS using the GUI

1. Sign into your AWS console at this url: https://aws.amazon.com/
2. From the main menu, select Database -> RDS.
3. Using the left-hand menu, select Databases. This should present a list of the current database instances.
4. Select the desired database instance.
5. Select Connectivity & security, to see **Public accessibility**.
6. Select Maintenance & backups, to see **Automated backupsEnabled**.
7. Select Configuration, to see **StorageEncryption**.

AWS CLI Solution

Retrieving Database Connectivity & security from AWS RDS using the CLI

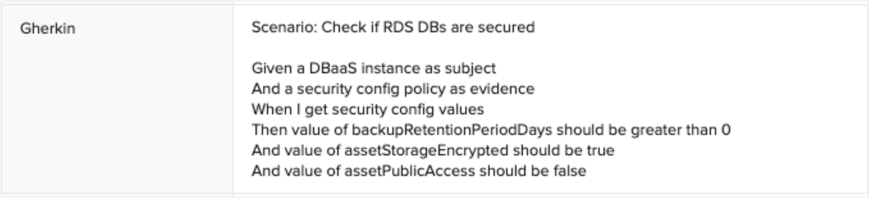
1. Using the following link, ensure AWS CLI is installed on the client device: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html
2. With the desired IAM user's Access Key ID, Secret Access Key, and default region in-hand, run the "`aws configure`" command.
3. Use the "`aws rds describe-db-instances`" command to retrieve a list of RDS database instances. Note the database identifier property, `DBInstanceArn`.
4. Using the Use the "`aws rds describe-db-instances--db-instance-identifier <DBInstanceArn>`" command to retrieve information about provisioned RDS instances

Example Evidence Type Output

```
{
    "DBInstances": [
        {
            "DBInstanceIdentifier": "mydbinstancecf",
            "DBInstanceClass": "db.t3.small",
            "Engine": "mysql",
            "DBInstanceStatus": "available",
            "MasterUsername": "masterawsuser",
            "Endpoint": {
                "Address": "mydbinstancecf.abcexample.us-
east-1.rds.amazonaws.com",
                "Port": 3306,
                "HostedZoneId": "Z2R2ITUGPM61AM"
            },
            ...some output truncated...
        }
    ]
}
```

reference:
https://docs.aws.amazon.com/cli/latest/reference/rds/describe-db-instances.html

Automated Assessment



Gherkin

```
Scenario: Check if RDS DBs are secured

Given a DBaaS instance as subject
And a security config policy as evidence
When I get security config values
Then value of backupRetentionPeriodDays should be greater than 0
And value of assetStorageEncrypted should be true
And value of assetPublicAccess should be false
```

Remediation Bot: Secure AWS RDS DBaaS Instance

Remediation automation bot for this condition is still pending.

Appendix A

AWS Functions and Evidence Types

AWS Collection Functions / Bots	AWS Remediation Functions / Bots	Related Evidence Types
• aws-getEc2Instances • aws-getVolumeSnapshots • aws-getVolumeBackupPlanPolicy • aws-getAllBuckets • aws-getS3BucketBlockPublicPolicy • aws-get-RdsDbs • aws-getRdsDbInstanceSecurityConfiguration • aws-getDBSnapshots	• aws-setVolumeBackupPlanPolicy • aws-enableS3BucketBlockPublicPolicy	• Asset Snapshots • AWS Backup Plan Policy • Volume Snapshots • AWS S3 Security Policy • Active AD User Report • DBaaS Instance Security Configuration