

# CIS AWS Storage Services Benchmark

v1.0.0 - 07-03-2024

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

# Table of Contents

<b>Terms of Use .....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b>Overview .....</b>	<b>5</b>
Intended Audience.....	5
Consensus Guidance .....	6
Typographical Conventions.....	7
<b>Recommendation Definitions.....</b>	<b>8</b>
Title.....	8
Assessment Status.....	8
Automated .....	8
Manual.....	8
Profile .....	8
Description.....	8
Rationale Statement .....	8
Impact Statement.....	9
Audit Procedure.....	9
Remediation Procedure.....	9
Default Value.....	9
References .....	9
CIS Critical Security Controls® (CIS Controls®).....	9
Additional Information.....	9
Profile Definitions .....	10
Acknowledgements .....	11
<b>Recommendations .....</b>	<b>12</b>
<b>1 Introduction.....</b>	<b>12</b>
1.1 AWS Storage Backups (Manual) .....	13
1.2 Ensure securing AWS Backups (Manual) .....	14
1.3 Ensure to create backup template and name (Manual).....	16
1.4 Ensure to create AWS IAM Policies (Manual) .....	18
1.5 Ensure to create IAM roles for Backup (Manual).....	19
1.6 Ensure AWS Backup with Service Linked Roles (Manual) .....	20
<b>2 Elastic Block Store (EBS).....</b>	<b>21</b>
2.1 Ensure creating EC2 instance with EBS (Manual) .....	22
2.2 Ensure configuring Security Groups (Manual).....	24
2.3 Ensure the proper configuration of EBS storage (Manual).....	25
2.4 Ensure the creation of a new volume (Manual) .....	27
2.5 Ensure creating snapshots of EBS volumes (Manual) .....	30

2.6 Ensure Proper IAM Configuration for EC2 Instances (Manual).....	33
2.7 Ensure creating IAM User (Manual) .....	37
2.8 Ensure the Creation of IAM Groups (Manual) .....	41
2.9 Ensure Granular Policy Creation (Manual) .....	44
2.10 Ensure Resource Access via Tag-based Policies (Manual) .....	47
2.11 Ensure Secure Password Policy Implementation (Manual) .....	50
2.12 Ensure Monitoring EC2 and EBS with CloudWatch (Manual) .....	53
2.13 Ensure creating an SNS subscription (Manual).....	56
<b>3 Elastic File System (EFS) .....</b>	<b>57</b>
3.1 EFS (Manual).....	58
3.2 Ensure Implementation of EFS (Manual) .....	60
3.3 Ensure EFS and VPC Integration (Manual).....	63
Audit Procedures for AWS Redundancy and Scalability.....	63
3.4 Ensure controlling Network access to EFS Services (Manual) .....	65
3.5 Ensure using Security Groups for VPC (Manual) .....	67
3.6 Ensure Secure Ports (Manual) .....	68
3.7 Ensure File-Level Access Control with Mount Targets (Manual) .....	71
3.8 Ensure managing mount target security groups (Manual) .....	73
3.9 Ensure using VPC endpoints - EFS (Manual) .....	75
3.10 Ensure managing AWS EFS access points (Manual) .....	77
3.11 Ensure accessing Points and IAM Policies (Manual) .....	80
3.12 Ensure configuring IAM for AWS Elastic Disaster Recovery (Manual) .....	83
<b>4 FSx.....</b>	<b>85</b>
4.1 FSX (AWS Elastic File Cache) (Manual) .....	86
4.2 Amazon Elastic File Cache (Manual).....	88
4.3 Ensure the creation of an FSX Bucket (Manual) .....	91
4.4 Ensure the creation of Elastic File Cache (Manual) .....	93
4.5 Ensure installation and configuration of Lustre Client (Manual) .....	95
4.6 Ensure EC2 Kernel compatibility with Lustre (Manual) .....	97
4.7 Ensure mounting FSx cache (Manual) .....	99
4.8 Ensure exporting cache to S3 (Manual) .....	101
4.9 Ensure cleaning up FSx Resources (Manual) .....	102
<b>5 Simple Storage Service (S3) .....</b>	<b>104</b>
5.1 Amazon Simple Storage Service (Manual).....	105
5.2 Ensure direct data addition to S3 (Manual) .....	107
5.3 Ensure Storage Classes are Configured (Manual).....	109
<b>6 Elastic Disaster Recovery (EDR) .....</b>	<b>111</b>
6.1 Ensure Elastic Disaster Recovery is Configured (Manual).....	112
6.2 Ensure AWS Disaster Recovery Configuration (Manual) .....	116
6.3 Ensure functionality of Endpoint Detection and Response (EDR) (Manual) .....	118
6.4 Ensure configuration of replication settings (Manual).....	120
6.5 Ensure proper IAM configuration for AWS Elastic Disaster Recovery (Manual) .....	122
6.6 Ensure installation of the AWS Replication Agent (Manual) .....	124
6.7 Ensure proper configuration of the Launch Settings (Manual) .....	126
6.8 Ensure execution of a recovery drill (Manual) .....	128
6.9 Ensure Continuous Disaster Recovery Operations (Manual).....	130
6.10 Ensure execution of a Disaster Recovery Failover (Manual) .....	133
6.11 Ensure execution of a failback (Manual) .....	135
6.12 Ensure CloudWatch Metrics for AWS EDR (Manual).....	138
6.13 Ensure working of EDR (Manual) .....	140
<b>Appendix: Summary Table .....</b>	<b>142</b>
<b>Appendix: CIS Controls v7 IG 1 Mapped Recommendations .....</b>	<b>146</b>

<b><i>Appendix: CIS Controls v7 IG 2 Mapped Recommendations .....</i></b>	<b><i>148</i></b>
<b><i>Appendix: CIS Controls v7 IG 3 Mapped Recommendations .....</i></b>	<b><i>150</i></b>
<b><i>Appendix: CIS Controls v7 Unmapped Recommendations.....</i></b>	<b><i>152</i></b>
<b><i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations .....</i></b>	<b><i>153</i></b>
<b><i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations .....</i></b>	<b><i>155</i></b>
<b><i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations .....</i></b>	<b><i>157</i></b>
<b><i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i></b>	<b><i>159</i></b>
<b><i>Appendix: Change History .....</i></b>	<b><i>160</i></b>

# Overview

All CIS Benchmarks™ focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches.
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches.

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for configuring security options for the services within the Compute category in AWS. This Benchmark is intended to be used in conjunction with the CIS Amazon Web Services Foundations Benchmark. For more information about this approach see the Introduction section of this document.

The specific AWS Services in scope for this document include:

- Amazon Elastic Block Store (EBS)
- Amazon Elastic File System (EFS)
- Amazon FSx
- Amazon Simple Storage Service (S3)
- AWS Elastic Disaster Recovery (EDS)

To obtain the latest version of this guide, please visit <http://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at [benchmarkinfo@cisecurity.org](mailto:benchmarkinfo@cisecurity.org).

## Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, platform deployment, and/or DevOps personnel who plan to develop, deploy, assess, or secure solutions in Amazon Web Services.

## Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

## Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<code>&lt;Monospace font in brackets&gt;</code>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
<b>Bold font</b>	Additional information or caveats things like <b>Notes</b> , <b>Warnings</b> , or <b>Cautions</b> (usually just the word itself and the rest of the text normal).



# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

## Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

## **Impact Statement**

Any security, functionality, or operational consequences that can result from following the recommendation.

## **Audit Procedure**

Systematic instructions for determining if the target system complies with the recommendation.

## **Remediation Procedure**

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## **Default Value**

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

## **References**

Additional documentation relative to the recommendation.

## **CIS Critical Security Controls® (CIS Controls®)**

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

## **Additional Information**

Supplementary information that does not correspond to any other field but may be useful to the user.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide security-focused best practice hardening of a technology; and
- limit the impact to the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability
- acts as a defense in depth measure
- may impact the utility or performance of the technology
- may include additional licensing, cost, or addition of third-party software

## Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

### **Contributor**

Mike Wicks

Chantel Duckworth

# Recommendations

## 1 Introduction

### **Benchmark Approach:**

The suggested approach for securing your cloud environment is to start with the CIS Amazon Web Services Foundations Benchmark found here: [https://www.cisecurity.org/benchmark/amazon\\_web\\_services/](https://www.cisecurity.org/benchmark/amazon_web_services/). The CIS Foundations benchmark provides prescriptive guidance for configuring a subset of Amazon Web Services with an emphasis on foundational, testable, and architecture agnostic settings including:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- AWS CloudWatch
- AWS Simple Notification Service (SNS)
- AWS Simple Storage Service (S3)
- AWS VPC (Default)

The Amazon Web Services Foundation Benchmark is what you should start with when setting up your AWS environment. It is also the foundation for which all other AWS service category benchmarks are built on so that as you grow your cloud presence and usage of the services offered you have the necessary guidance to securely configure your environment as it fits with your company's policy.

After configuring your environment to the CIS Amazon Web Services Foundations Benchmark, we suggest implementing the necessary configurations for the services utilized as defined in the associated product and service category benchmarks. The CIS storage services Benchmark provides prescriptive guidance for configuring security options for the services within storage in AWS. The specific AWS Services in scope for this document include:

- Amazon Elastic Block Store (EBS)
- Amazon Elastic File System (EFS)
- Amazon FSx
- Amazon Simple Storage Service (S3)
- AWS Elastic Disaster Recovery (DRS)

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS Amazon Web Services Benchmarks, please register on CIS WorkBench at <https://workbench.cisecurity.org> and join the CIS Amazon Web Services Benchmarks community.

## *1.1 AWS Storage Backups (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

AWS Storage Backups is a managed AWS Service that establishes high resiliency to your cloud resources. AWS Storage Backups are like making extra copies of your important stuff on Amazon's computers. It is an excellent strategy to ensure that the data and resources you use remain available in the event of unrecoverable damage or loss to your resources.

### **Rationale:**

AWS Backups enable you to back up and restore all data lost during the attack, While AWS Storage Backups provide a level of security, there are numerous methods to fortify your backups, ensuring the protection of your data and services.

### **Audit:**

### **Remediation:**

## 1.2 Ensure securing AWS Backups (Manual)

### Profile Applicability:

- Level 2

### Description:

As an AWS administrator, it's important to know what you're responsible for. You're responsible for keeping things safe in the cloud, which means taking care of the resources and data on AWS. Here's what you need to secure, according to AWS documentation:

1. Responsible for alert communication with AWS.
2. Managing access credentials for AWS resources.
3. Configuring backup plans according to organization policies.
4. Ensuring backup recovery capability.
5. Including AWS Backups in the organization's disaster recovery procedures.
6. Ensuring user awareness and familiarity with AWS Backups platform usage

### Rationale:

AWS will send periodic emails regarding the status of your backups and any service issues. The administrator must address any communicated issues from AWS, such as billing problems or backup inactivity, and take necessary steps to resolve them.

### Audit:

#### CREATING AN AWS BACKUP:

Creating an AWS Backup involves selecting the desired data, specifying backup frequency, and choosing storage options. Below we'll walk through how to create and configure an AWS Backup instance.

1. Sign into AWS Console:  
To sign into the AWS Console 'https://console.aws.amazon.com/billing/home#/', users navigate to the AWS Management Console website and enter their credentials, including their username and password.
2. Access the AWS Backup Service Dashboard in the AWS Management Console:  
AWS Management Console and type "Backup" or navigate through the services menu to find the "Storage" category, where AWS Backup is listed.
3. Create Backup Plan:  
Choose "Create backup plan" from the options provided. You can either create a custom plan tailored to your requirements or option for a per-defined template offered by AWS

**Remediation:****References:**

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



## 1.3 Ensure to create backup template and name (Manual)

### Profile Applicability:

- Level 2

### Description:

To create a backup plan, select a template and specify a name for the plan. Additionally, define backup rules according to your requirements and then click on create backup option.

### Rationale:

### Audit:

Backup Resources:

Once you've made your backup plan, it's time to put it into action and start backing up your stuff.

Let's start by backing up an S3 storage bucket.

To back up Elastic Beanstalk instance stored on AWS S3, we'll need to tag its Amazon Resource Name (ARN) with a backup plan. In S3, go to "properties" to attach the backup plan to the resource:

1. Copy the ARN from the console:  
From the AWS Management Console, copy the ARN (Amazon Resource Name) associated with the Elastic Beanstalk instance. This unique identifier will be used to tag the resource for backup.
2. Assign the resource:
  - After copying the ARN, return to the AWS Management Console and access Amazon Backup.
  - Choose the backup plan recently created, then proceed to assign the resource you wish to backup, such as the S3 bucket containing the Elastic Beanstalk resource.
  - Finally, navigate to "Resource Assignments" to complete the process. Choose "Assign Resources" and provide a name for the assignment. For now, maintain the role as Default. In subsequent sections, we'll explore implementing custom IAM roles and policies for your backup operations.  
Select the resource(s) that you want to backup. You have the option to backup all your resources, but we're just going to back up the specific Elastic Beanstalk resource for now.

The resources are now being backed up according to the schedule established by your organization.

**Remediation:**

The AWS backup vault serves as the storage location for your backups. It's crucial to manage access to these backups to prevent unauthorized access and ensure data security.

**References:**

1. <https://docs.aws.amazon.com/aws-backup/latest/devguide/how-it-works.html>

## *1.4 Ensure to create AWS IAM Policies (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

AWS IAM policies, specify the desired permissions for accessing AWS resources and define the conditions under which those permissions are granted. Configure the appropriate policies to keep your resources secure.

### **Rationale:**

Managing AWS IAM policies is crucial to safeguard your backups from unauthorized access, ensuring that only approved users can manipulate or view sensitive data.

### **Audit:**

To create a role for AWS Backup, follow these steps:

1. Navigate to the "IAM Dashboard" in the AWS Console.
2. Select "Roles" from the left-hand menu.
3. Click on the "Create Role" button.
4. Choose "AWS Service" as the trusted entity.
5. Select "AWS Backup" as the service that will use this role.
6. Choose a policy to apply to the role or create a custom policy.
7. Review the role details and provide a meaningful name for the role.
8. Click on "Create Role" to finalize the creation of the role for AWS Backup.

### **Remediation:**

AWS IAM policies, restricting access to backup resources, and implementing additional security measures to prevent future incidents.

### **References:**

1. [https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

## *1.5 Ensure to create IAM roles for Backup (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

An AWS Identity and Access Management (IAM) role is similar to a user, in that it is an AWS identity with permissions policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it.

### **Rationale:**

While Service Linked Roles offer quick deployment, using default configurations isn't recommended for security best practices.

### **Audit:**

To create a role for AWS Backup, follow these steps:

1. Navigate to the "IAM Dashboard" in the AWS Console.
2. Select "Roles" from the left-hand menu.
3. Click on the "Create Role" button.
4. Choose "AWS Service" as the trusted entity.
5. Select "AWS Backup" as the service that will use this role.
6. Choose a policy to apply to the role or create a custom policy.
7. Review the role details and provide a meaningful name for the role.
8. Click on "Create Role" to finalize the creation of the role for AWS Backup.

### **Remediation:**

Assess your organization's needs to determine whether to utilize Service Linked Roles for AWS backups.

### **Default Value:**

When using the AWS Backup console for the first time, you can choose to have AWS Backup create a default service role for you. This role has the permissions that AWS Backup needs to create and restore backups on your behalf.

### **References:**

1. <https://docs.aws.amazon.com/IAM/latest/UserGuide/using-service-linked-roles.html>

## *1.6 Ensure AWS Backup with Service Linked Roles (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

AWS Service Linked Roles are IAM roles designed specifically for AWS Backup. These roles come with default configurations allowing access to all AWS resources by default.

### **Rationale:**

While Service Linked Roles offer quick deployment, using default configurations isn't recommended for security best practices.

### **Audit:**

Create service-linked role for AWS Backup:

You don't need to create a service-linked role manually. AWS Backup automatically creates it when you list resources to back up, set up cross-account backup, or perform backups using the AWS Management Console, AWS CLI, or AWS API.

If you delete this role, you can recreate it by following the same steps. AWS Backup will create it for you again when needed.

### **Remediation:**

Assess your organization's needs to determine whether to utilize Service Linked Roles for AWS backups.

### **References:**

1. <https://docs.aws.amazon.com/aws-backup/latest/devguide/using-service-linked-roles.html>

## 2 Elastic Block Store (EBS)

Amazon EBS is a block level file storage system that runs on EC2. EBS can be used as a hard drive that's mounted on an EC2 instance (virtual machine). EBS can store data as a standalone apart from EC2. This means that data can persist to the block storage service while an EC2 instance is offline. Out of the box EBS functions as an unformatted file system that needs to be configured and mounted on top of an EC2 instance. EBS can be used as both a storage and boot drive; for the purposes of this document, we will focus on EBS as a storage device. EBS comes with many different options to fit the specific needs of an application. EBS is most likely the right choice if you need quick access to read and write files to the cloud and you need these files to be stored long term. You can also rapidly unmount the file system from one EC2 instance and deploy it to another instance by using snapshots.

## 2.1 Ensure creating EC2 instance with EBS (Manual)

### Profile Applicability:

- Level 2

### Description:

EBS are storage volumes that you attach to Amazon EC2 instances. After you attach a volume to an instance, you can use it in the same way you would use a local hard drive attached to a computer, for example to store files or to install applications.

### Rationale:

### Audit:

Creating EC2 instance with Volume:-

To create an EC2 instance with a volume in AWS, you can follow these general steps:

1. Initializing a Secure EC2 Instance:  
Navigate to the EC2 dashboard within your AWS console. Make sure you're in the region that's right for you.  
Select "Launch Instance".
2. Naming the EC2 instance:  
Name your EC2 instance according to the proper naming convention set by your organization.
3. Configure the operating system:  
You can choose any operating system according to your needs. In this tutorial, Ubuntu is the OS of choice.
4. Create a key pair  
Next, create a key pair. You will need this to login your EC2 instance. We're going to log in via SSH.  
Select "Create new key pair". Give your key a name, select RSA encryption, and select Open SSH.  
As you can see by the prompt, you will need to keep the private key that's generated secure on your local computer. This is how you will access your EC2 instance. Select "Create key pair" your secret key will start downloading as a ".pem" file.




### Add Storage:

1. Click "Add New Volume" to add a new volume.
2. Specify the volume type (e.g., General Purpose SSD, Provisioned IOPS SSD, Magnetic).
3. Set the size of the volume in GB minimum of 8GB.
4. You can add multiple volumes if needed.

**Remediation:****References:**

1. <https://aws.amazon.com/ebs/>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			



## 2.2 Ensure configuring Security Groups (Manual)

### Profile Applicability:

- Level 2

### Description:

Security groups are your first line of defense for the EC2 instance. A security group is a firewall that controls inbound and outbound traffic.

### Rationale:





Security groups play a critical role in maintaining the security of your AWS resources. It is advisable to restrict traffic to only what is necessary for accessing your instance, thereby minimizing potential security risks.

### Audit:

Open traffic for SSH, HTTP, and HTTPS. Make sure to allow traffic from anywhere, unless you will be accessing the instance from a secure workstation or server with a static IP address.

### Remediation:

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>12.3 <u>Securely Manage Network Infrastructure</u></b> Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## 2.3 Ensure the proper configuration of EBS storage (Manual)

### Profile Applicability:

- Level 2

### Description:

All computer instances need to have a device on which to store files. EBS is built on top of EC2 instances as a block storage device.

### Rationale:

Remember that we are working with cloud computing. Rather than purchasing and manually installing disk drives on a server, AWS allows you to virtually add storage using Elastic Block Store (EBS).

### Impact:

Failure to properly configure EBS storage can lead to data loss, performance issues, increased costs, security vulnerabilities, and operational downtime. Ensuring correct configuration is crucial to maintain data integrity, efficiency, cost-effectiveness, security, and reliability.

### Audit:






### Remediation:

1. **Open the Amazon EC2 Console:** Navigate to the EC2 Dashboard in the AWS Management Console.
2. **Select Volumes:** Under the "Elastic Block Store" section, select "Volumes".
3. **Create Volume:**
  - Click on "Create Volume".
  - Choose the volume type (e.g., General Purpose SSD (gp2), Provisioned IOPS SSD (io1), etc.).
  - Specify the size and availability zone.
  - Optionally, configure additional settings such as IOPS, encryption, and tags.
4. **Attach Volume to Instance:**
  - Select the volume you created.
  - Click on "Actions" and choose "Attach Volume".
  - Select the instance to which you want to attach the volume and specify the device name.
5. **Format and Mount the Volume** (on the instance):
  - Connect to your instance using SSH.
  - List available disks using the command: `lsblk`.
  - Format the new volume (e.g., `sudo mkfs -t ext4 /dev/xvdf` for ext4 filesystem).

- Create a mount point (e.g., `sudo mkdir /mnt/data`).
  - Mount the volume (e.g., `sudo mount /dev/xvdf /mnt/data`).
6. **Configure Automatic Mounting (optional):**
- Edit the `/etc/fstab` file to add an entry for the new volume to ensure it mounts automatically on reboot.
  - Example entry: `/dev/xvdf /mnt/data ext4 defaults,nofail 0 2`.

By following these steps, you can effectively configure and manage EBS storage for your AWS instances.

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u></b> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>11.1 <u>Maintain Standard Security Configurations for Network Devices</u></b> Maintain standard, documented security configuration standards for all authorized network devices.			

## 2.4 Ensure the creation of a new volume (Manual)

### Profile Applicability:

- Level 2

### Description:

Leave the root volume unchanged and create a new volume. To ensure the security of the instance and prevent data loss, select "no" under the "delete on termination" option and encrypt your volume using AWS KMS. A default key is available for encrypting the volume.

### Rationale:

By leaving the root volume unchanged and creating a new volume, you separate critical data from the operating system. Selecting "no" for the "delete on termination" option ensures that data on the new volume is not automatically deleted when the instance is terminated, protecting against accidental data loss. Encrypting the volume using AWS KMS adds an additional layer of security, safeguarding the data against unauthorized access. The use of a default key for encryption simplifies the process while maintaining strong security measures.

### Impact:

Not following these steps can lead to data loss, security risks, operational disruptions, and prolonged recovery times. Setting "delete on termination" to "no" prevents data deletion upon instance termination, while encrypting the volume with AWS KMS protects against unauthorized access. Storing critical data separately from the root volume ensures operational continuity and easier recovery.

### Audit:

To audit this configuration in AWS, follow these steps:

1. **Access the AWS Management Console:** Log in to your AWS account and navigate to the AWS Management Console.
2. **Review EBS Volumes:**
  - Go to the EC2 Dashboard and select "Volumes" under the "Elastic Block Store" section.
  - Check the properties of each volume to ensure that the root volume is unchanged and new volumes are created as needed.
3. **Check "Delete on Termination" Setting:**
  - In the "Volumes" section, select each volume and click on the "Actions" button.
  - Select "Modify Volume" and ensure that "Delete on Termination" is set to "no" for the critical volumes.






- Alternatively, go to the "Instances" section, select an instance, click on the "Actions" button, choose "Instance Settings," and then "Change Termination Protection."
- 4. **Verify Encryption:**
  - In the "Volumes" section, check the "Encrypted" column to confirm that the volumes are encrypted.
  - For detailed information, select a volume and view its details to ensure it is encrypted using AWS KMS.
- 5. **Review IAM Policies:**
  - Navigate to the IAM Dashboard and review the policies attached to users, groups, and roles to ensure they have appropriate permissions to create, modify, and encrypt EBS volumes.
- 6. **Use AWS Config:**
  - Enable AWS Config to continuously monitor and record AWS resource configurations.
  - Create AWS Config rules to check for compliance with best practices, such as ensuring volumes are encrypted and "Delete on Termination" is set to "no."
- 7. **Generate Reports:**
  - Use AWS CloudTrail to review logs of API calls made to EBS volumes, ensuring compliance with the required configurations.
  - Generate compliance reports using AWS Config and AWS CloudTrail to provide evidence of adherence to best practices.

By following these steps, you can effectively audit your EBS configurations to ensure data security, integrity, and operational reliability.

## **Remediation:**

1. **Volume Configurations:**
  - After configuring your volume, ensure the settings meet your requirements. To secure your file system and prevent data loss, verify that the "Delete on Termination" option is set to "no," the volume is encrypted, and the KMS key is correctly specified. For this EBS instance, we are using the default KMS key.
2. **Availability Zone Consistency:**
  - Ensure your EBS volume is in the same Availability Zone as your EC2 instance. An EBS volume can only be attached to an EC2 instance within the same Availability Zone. You can mount and unmount EBS volumes to any EC2 instance within the same zone as needed.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<u>11.1 Maintain Standard Security Configurations for Network Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.			

## 2.5 Ensure creating snapshots of EBS volumes (Manual)

### Profile Applicability:

- Level 2

### Description:

A snapshot is a backup of your EBS volume that captures its state at a specific point in time, storing only the data changes since the last snapshot to optimize storage costs and speed. Snapshots are crucial for data recovery, creating new EBS volumes, and replicating data across AWS regions for disaster recovery and high availability.

Restoring from a snapshot allows you to create a new EBS volume and attach it to an EC2 instance in the same availability zone, ensuring data integrity and accessibility.

### Rationale:

The rationale behind using EBS snapshots is to ensure efficient and cost-effective data backup and recovery. By capturing only the data changes since the last snapshot, storage costs are minimized and the backup process is expedited. Snapshots are essential for maintaining data integrity, facilitating quick recovery, and enabling seamless data replication across regions, thereby enhancing disaster recovery capabilities and operational resilience.

### Impact:

Not utilizing EBS snapshots can lead to significant risks and drawbacks. Without snapshots, data recovery becomes more complex and time-consuming, increasing the risk of prolonged downtime in the event of data loss or system failure. Additionally, the absence of incremental backups can lead to higher storage costs and inefficient use of resources. The lack of data replication across regions can severely compromise disaster recovery efforts, making it challenging to maintain high availability and operational continuity. Overall, failing to use snapshots undermines data integrity, security, and the ability to quickly restore critical information.

### Audit:

To audit the use of EBS snapshots in AWS, follow these steps:

1. **Access the AWS Management Console:**
  - Log in to your AWS account and navigate to the AWS Management Console.
2. **Review EBS Snapshots:**
  - Go to the EC2 Dashboard and select "Snapshots" under the "Elastic Block Store" section.
  - Check the list of snapshots to ensure regular backups are being created for all critical volumes.
3. **Verify Snapshot Policies:**

- Ensure that snapshot lifecycle policies are in place and configured correctly.
- Go to the "Lifecycle Manager" under the EC2 Dashboard and review policies for automated snapshot creation and retention.
- 4. Check Snapshot Status and Details:**
  - Review the status of each snapshot to ensure they are completed successfully.
  - Verify the details of snapshots, such as description, creation time, and the volume ID associated with each snapshot.
- 5. Inspect IAM Policies and Permissions:**
  - Navigate to the IAM Dashboard and review the policies attached to users, groups, and roles.
  - Ensure that only authorized personnel have permissions to create, delete, and manage snapshots.
- 6. Use AWS Config Rules:**
  - Enable AWS Config to continuously monitor and record AWS resource configurations.
  - Create AWS Config rules to check for compliance with best practices, such as ensuring snapshots are created regularly and are not older than a specific period.
- 7. Review AWS CloudTrail Logs:**
  - Use AWS CloudTrail to review logs of API calls related to EBS snapshots.
  - Ensure that all snapshot activities are logged and can be traced back to authorized users and roles.
- 8. Generate Reports:**
  - Utilize AWS Config and AWS CloudTrail to generate compliance and activity reports.
  - Review these reports to ensure adherence to snapshot policies and identify any anomalies or unauthorized activities.

By following these steps, you can effectively audit the use of EBS snapshots to ensure data integrity, security, and compliance with best practices.

## **Remediation:**

To create an EBS snapshot on AWS, follow these steps:

- 1. Access the AWS Management Console:**
  - Log in to your AWS account and navigate to the AWS Management Console.
- 2. Navigate to the EC2 Dashboard:**
  - In the AWS Management Console, select "EC2" from the services menu to open the EC2 Dashboard.
- 3. Select the Volume:**
  - In the left-hand navigation pane, under "Elastic Block Store," click on "Volumes."









- Find the volume you want to snapshot from the list and select it by clicking the checkbox next to it.
- 4. **Create a Snapshot:**
  - With the volume selected, click on the "Actions" button at the top of the page.
  - From the dropdown menu, select "Create Snapshot."
- 5. **Configure the Snapshot:**
  - In the "Create Snapshot" dialog box, provide a description for the snapshot. This helps identify the snapshot later.
  - Review the volume ID to ensure it is the correct volume.
- 6. **Initiate the Snapshot Creation:**
  - Click the "Create Snapshot" button to start the snapshot creation process.
- 7. **Monitor the Snapshot:**
  - Navigate to the "Snapshots" section under "Elastic Block Store" in the left-hand navigation pane.
  - Find your snapshot in the list and monitor its status. The snapshot creation process might take some time, depending on the size of the volume and the amount of data.
- 8. **Verify Completion:**
  - Once the snapshot status changes to "completed," it indicates that the snapshot has been successfully created and is available for use.

By following these steps, you can create an EBS snapshot to ensure you have a backup of your volume at a specific point in time.

#### References:

1. <https://docs.aws.amazon.com/ebs/latest/userguide/ebs-creating-snapshot.html>

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>11.1 Establish and Maintain a Data Recovery Process</b> Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>10.1 Ensure Regular Automated Back Ups</b> Ensure that all system data is automatically backed up on regular basis.			

## 2.6 Ensure Proper IAM Configuration for EC2 Instances (Manual)

### Profile Applicability:

- Level 2

### Description:

IAM, or Identity and Access Management, is a vital security service used to control and manage access to AWS resources, ensuring only authorized users and services can interact with them. It allows you to create users and groups, set permissions, enforce multi-factor authentication, and implement least privilege principles to enhance security and compliance.

### Rationale:

The rationale behind using IAM is to enhance security by controlling and managing access to AWS resources, ensuring that only authorized users and services can interact with them. This minimizes the risk of unauthorized access and potential security breaches, while also allowing for the implementation of best practices such as multi-factor authentication and least privilege principles, which further strengthen the security and compliance of your AWS environment.

### Impact:

Not implementing IAM properly can lead to significant security vulnerabilities, including unauthorized access to AWS resources, data breaches, and potential loss of sensitive information. Without IAM, it is challenging to enforce access controls, monitor user activity, and implement security best practices such as multi-factor authentication and least privilege principles. This can result in increased risk of malicious attacks, operational disruptions, non-compliance with regulatory requirements, and substantial financial damage.

### Audit:

1. **Access the AWS Management Console:**
  - Log in to your AWS account and navigate to the AWS Management Console.
2. **Review IAM Users and Roles:**
  - Go to the IAM Dashboard and select "Users" to review all user accounts.
  - Check each user for appropriate permissions, MFA enablement, and adherence to the principle of least privilege.
  - Similarly, review the "Roles" section to ensure roles have the correct permissions and are assigned appropriately.
3. **Check IAM Policies:**
  - In the IAM Dashboard, navigate to "Policies" and review both AWS managed and customer-managed policies.

- Ensure that policies follow the principle of least privilege and do not grant excessive permissions.
- 4. **Analyze IAM Groups:**
  - Review the groups in the IAM Dashboard under "Groups."
  - Ensure that users are grouped appropriately and that groups have suitable permissions.
- 5. **Examine MFA Settings:**
  - Verify that Multi-Factor Authentication (MFA) is enabled for all users with console access.
  - In the IAM Dashboard, click on "Users" and check the "Security credentials" tab for each user to confirm MFA setup.
- 6. **Audit IAM Activity:**
  - Use AWS CloudTrail to review logs of IAM activities, including user logins, policy changes, and other management activities.
  - Ensure that all IAM activities are logged and can be traced back to authorized users.
- 7. **Implement AWS Config Rules:**
  - Enable AWS Config to continuously monitor IAM configurations.
  - Create and apply AWS Config rules that check for compliance with best practices, such as ensuring all users have MFA enabled and policies are not overly permissive.
- 8. **Generate IAM Reports:**
  - Use AWS IAM Access Analyzer to identify permissions granted to resources that can be accessed from outside your AWS account.
  - Generate IAM credential reports from the IAM Dashboard to review the status of all IAM users, including when their passwords were last used and when their access keys were last rotated.
- 9. **Conduct Regular Reviews:**
  - Schedule regular audits to review IAM configurations and policies.
  - Periodically update and refine IAM policies and permissions to ensure ongoing compliance and security.

## **Remediation:**

1. **Restrict Overly Permissive Policies:**
  - Identify and modify any IAM policies that are overly permissive. Update policies to grant the least privilege necessary for users to perform their tasks.
  - Use IAM policy simulator to test and validate the changes to ensure they do not disrupt operations.
2. **Enable Multi-Factor Authentication (MFA):**
  - For all users with console access, enable MFA. This adds an additional layer of security.
  - Navigate to the IAM Dashboard, select "Users," and enable MFA under the "Security credentials" tab for each user.
3. **Rotate Access Keys:**

- Regularly rotate access keys for IAM users to reduce the risk of compromised credentials.
  - In the IAM Dashboard, select "Users," go to the "Security credentials" tab, and create new access keys. Then, disable and delete old access keys after confirming the new keys are functioning correctly.
4. **Remove Unnecessary Users and Roles:**
    - Delete any IAM users or roles that are no longer needed to minimize potential security risks.
    - Review each user and role, and remove those that are inactive or no longer required.
  5. **Implement Role-Based Access Control (RBAC):**
    - Group users by their roles and assign permissions based on job functions.
    - Use IAM groups to manage permissions collectively rather than individually for each user.
  6. **Regularly Review and Update IAM Policies:**
    - Set up a regular schedule to review and update IAM policies to ensure they remain aligned with security best practices and organizational changes.
    - Use AWS Config and AWS Config Rules to continuously monitor policy changes and ensure compliance.
  7. **Enable AWS CloudTrail and AWS Config:**
    - Ensure that AWS CloudTrail is enabled to log all IAM activities. Configure it to capture and analyze logs for unauthorized access and policy changes.
    - Enable AWS Config to continuously monitor IAM resource configurations and compliance with best practices.
  8. **Conduct Security Awareness Training:**
    - Provide regular security training for all users to educate them on best practices for using IAM and the importance of security measures like MFA and least privilege access.
  9. **Implement IAM Access Analyzer:**
    - Use IAM Access Analyzer to identify and remediate permissions that allow external access to your resources.
    - Regularly review the findings and adjust permissions to ensure that only the necessary external access is granted.

## References:

1. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>6.8 Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	<b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

## 2.7 Ensure creating IAM User (Manual)

### Profile Applicability:

- Level 2

### Description:

IAM users are individuals whose accounts have been created by the AWS administrator, providing them access to specific AWS resources. These users have undergone identity verification with your organization, ensuring that only authorized personnel can manage and interact with your AWS environment.

### Rationale:

The purpose of creating IAM users and verifying their identities with your organization is to ensure that only authorized individuals have access to AWS resources, enhancing security and preventing unauthorized access. This practice helps maintain control over your AWS environment, ensuring that sensitive data and critical operations are managed by trusted and validated personnel.

### Impact:

Not creating IAM users and verifying their identities can lead to unauthorized access to your AWS resources, increasing the risk of security breaches and data leaks. This lack of control can result in compromised sensitive data, unauthorized changes to critical systems, and overall reduced security posture, potentially causing significant operational and financial damage to your organization.

### Audit:

1. **Access the AWS Management Console:**
  - Log in to your AWS account and navigate to the AWS Management Console.
2. **Review IAM Users:**
  - Go to the IAM Dashboard and select "Users."
  - Check the list of IAM users to ensure that only authorized users are present.
3. **Check User Details:**
  - For each user, click on their name to view their details.
  - Verify the "User ARN" and ensure that the user was created by an authorized administrator.
  - Check the "Security credentials" tab to see if Multi-Factor Authentication (MFA) is enabled for added security.
4. **Verify Identity Policies:**
  - Review the policies attached to each user to ensure they are appropriate for the user's role.

- Check that permissions follow the principle of least privilege, granting only the necessary access.
- 5. **Monitor Login Activity:**
  - Use AWS CloudTrail to review login activities for each IAM user.
  - Check for any unusual login patterns or unauthorized access attempts.
- 6. **Use AWS IAM Access Analyzer:**
  - Enable IAM Access Analyzer to identify any IAM resources shared outside your AWS account.
  - Review findings to ensure that only verified and authorized users have access to your resources.
- 7. **Generate IAM Credential Reports:**
  - In the IAM Dashboard, go to "Credential reports" and generate a report.
  - Review the report for details on all IAM users, including their access key age, password age, and MFA status.
- 8. **Implement AWS Config Rules:**
  - Enable AWS Config to continuously monitor IAM configurations.
  - Create and apply AWS Config rules to check for compliance with identity verification and user management best practices.
- 9. **Review IAM Roles and Groups:**
  - Ensure that roles and groups are properly configured and assigned only to authorized users.
  - Verify that roles have the correct trust relationships and that group memberships are appropriate for the user's responsibilities.
- 10. **Schedule Regular Audits:**
  - Set up regular intervals to audit IAM users and their access rights.
  - Keep records of audit findings and remediation actions to maintain a secure and compliant AWS environment.

## **Remediation:**




1. **Remove Unauthorized Users:**
  - Go to the IAM Dashboard, select "Users," and review the list of users.
  - Identify any unauthorized or unverified users and delete their accounts to prevent unauthorized access.
2. **Enable Multi-Factor Authentication (MFA):**
  - For each IAM user, go to the "Security credentials" tab and enable MFA.
  - Ensure all users have MFA configured to enhance security and reduce the risk of unauthorized access.
3. **Update User Policies:**
  - Review the policies attached to each IAM user.
  - Modify policies to follow the principle of least privilege, ensuring users have only the permissions necessary for their role.
  - Remove any overly permissive policies that could lead to security risks.
4. **Rotate Access Keys:**
  - For IAM users with long-lived access keys, create new keys and update the applications or services using them.

- Delete the old access keys to reduce the risk of compromised credentials.
- Encourage regular rotation of access keys as a security best practice.
- 5. Review and Correct IAM Roles and Groups:**
  - Ensure IAM roles are assigned only to authorized users and that trust relationships are properly configured.
  - Check group memberships and remove users who should not be part of specific groups.
  - Update role policies to adhere to the principle of least privilege.
- 6. Configure AWS IAM Access Analyzer:**
  - Enable IAM Access Analyzer to continuously monitor and analyze access to your IAM resources.
  - Address any findings related to unauthorized or overly broad access permissions.
- 7. Implement and Enforce IAM Policies:**
  - Create and enforce organizational IAM policies that require identity verification for all users.
  - Use AWS Organizations and Service Control Policies (SCPs) to enforce these policies across all accounts within your organization.
- 8. Enable AWS Config and Create Compliance Rules:**
  - Enable AWS Config to monitor IAM configurations and compliance.
  - Create AWS Config rules to ensure all users have MFA enabled, policies adhere to least privilege, and access keys are rotated regularly.
- 9. Conduct Regular Training:**
  - Provide regular security awareness training for all users to emphasize the importance of secure IAM practices.
  - Educate users on how to properly use IAM features and the significance of identity verification.
- 10. Schedule Regular Reviews and Audits:**
  - Establish a schedule for regular audits of IAM configurations and access controls.
  - Document findings and remediation actions taken during each audit.
  - Continuously improve your IAM practices based on audit results and evolving security threats.






## References:

1. [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_users\\_create.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.1 <u>Establish an Access Granting Process</u></b> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			



Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.2 <u>Establish an Access Revoking Process</u></b> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	<b>16.2 <u>Configure Centralized Point of Authentication</u></b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

## 2.8 Ensure the Creation of IAM Groups (Manual)

### Profile Applicability:

- Level 2

### Description:

IAM Groups are collections of users that share the same permissions for accessing AWS resources. For instance, you can create a group named "Administrators," which includes users who require full access to your AWS environment. This simplifies permission management by assigning common access policies to all members of the group.

### Rationale:

IAM groups in AWS simplify permission management by grouping users with similar access needs and applying common access policies, reducing administrative overhead and enhancing security through the principle of least privilege. This approach ensures consistency, scalability, and ease of auditing, strengthening the overall security posture of the AWS environment.

### Audit:

#### 1. Enable AWS CloudTrail:

- Navigate to the AWS Management Console and open the CloudTrail service.
- Create a new trail or ensure that an existing trail is configured to capture API activity in your AWS account.
- Verify that CloudTrail is recording events related to IAM actions, including changes to IAM groups.

#### 2. Review CloudTrail Logs:

- Access the CloudTrail console and navigate to the Event History or Insights section.
- Filter the logs to focus on IAM-related events, such as CreateGroup, AddUserToGroup, RemoveUserFromGroup, and PutGroupPolicy.
- Analyze the logs to track changes made to IAM groups, including user additions/removals and modifications to group policies.

#### 3. Utilize AWS Config:

- Open the AWS Config console and ensure that AWS Config is enabled for your AWS account.
- Set up AWS Config rules to monitor IAM configurations, including IAM groups.
- Configure rules to check for compliance with security standards or organizational policies regarding IAM group settings and permissions.

#### 4. Check IAM Console:

- Access the IAM console in the AWS Management Console.

- Navigate to the "Groups" section to view a list of IAM groups in your account.
- Review the details of each group, including its members and attached policies, to ensure they align with your security requirements.

## **Remediation:**

### **1. CloudTrail and AWS Config Configuration:**

- If CloudTrail or AWS Config is not enabled, configure them to capture and monitor IAM activities and configurations respectively. Enable logging and set up appropriate rules to track IAM group changes and ensure compliance.

### **2. Review CloudTrail Logs for Anomalies:**

- Regularly review CloudTrail logs to identify any unauthorized or unexpected changes to IAM groups.
- Investigate any anomalies detected in the logs, such as unauthorized user additions or policy modifications, and take appropriate action to rectify them.

### **3. AWS Config Remediation Rules:**

- Define AWS Config rules to automatically detect non-compliant IAM group configurations.
- Configure remediation actions within AWS Config to automatically revert any deviations from the desired IAM group settings back to the compliant state.

### **4. IAM Group Cleanup:**

- Periodically review IAM groups to ensure they are still necessary and relevant.
- Remove any unused or obsolete IAM groups to reduce the attack surface and simplify permission management.

### **5. Permissions Review:**

- Regularly review the permissions assigned to IAM groups to ensure they follow the principle of least privilege.
- Remove any excessive permissions or policies that are not required for the group's intended purpose.

### **6. Security Best Practices:**

- Implement security best practices for IAM, such as enforcing multi-factor authentication (MFA) for privileged IAM users and regularly rotating access keys.
- Train IAM administrators and users on security best practices to prevent inadvertent misconfigurations and unauthorized access.

### **7. Documentation and Monitoring:**

- Document IAM group configurations, policies, and access controls to maintain an audit trail and facilitate future audits.
- Set up monitoring alerts to notify administrators of any suspicious activities related to IAM groups.

## References:

1. [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_groups\\_create.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_create.html)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 Define and Maintain Role-Based Access Control</b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	<b>16.1 Maintain an Inventory of Authentication Systems</b> Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.		●	●
v7	<b>16.2 Configure Centralized Point of Authentication</b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

## 2.9 Ensure Granular Policy Creation (Manual)

### Profile Applicability:

- Level 2

### Description:

Granular policies are meticulously tailored to AWS resources, ensuring precision in access control measures.

### Rationale:

Emphasizing granular policies in AWS ensures that access control measures are precisely aligned with the requirements of each resource, bolstering security and minimizing unauthorized access. By tailoring policies to specific resources, organizations can adhere more closely to the principle of least privilege, mitigating risks and maintaining compliance with regulatory standards.

### Audit:

#### 1. Review IAM Policies:

- Access the IAM console in the AWS Management Console.
- Navigate to the "Policies" section to view all IAM policies.
- Examine each policy to ensure they are finely tuned and specific to the resources they are intended to control access to.

#### 2. Utilize AWS Config:

- Open the AWS Config console and ensure that AWS Config is enabled for your AWS account.
- Set up Config rules to monitor IAM policies for granularity.
- Configure rules to detect policies that are overly broad or provide unnecessary permissions.

#### 3. CloudTrail Analysis:

- Access the CloudTrail console and review the logs.
- Look for API calls related to IAM policy modifications.
- Analyze the logs to ensure that policy changes align with the principles of granular access control.

#### 4. Manual Review:

- Conduct manual reviews of IAM policies and their associated resources.
- Verify that policies are scoped to specific resources and actions, rather than providing blanket permissions.

#### 5. Automated Scanning:

- Utilize third-party AWS security tools that offer automated scanning and analysis of IAM policies for granularity.
- Configure these tools to regularly scan and identify any policies that may not adhere to granular access control principles.

#### 6. Continuous Monitoring:

- Implement continuous monitoring solutions to track changes to IAM policies in real-time.
- Set up alerts to notify administrators of any policy modifications that may deviate from granular access control best practices.

## **Remediation:**

### **1. Policy Refinement:**

- Review existing IAM policies to identify those that are overly broad or lack granularity.
- Refine these policies to restrict permissions to only the resources and actions necessary for each user or group.

### **2. IAM Policy Simulator:**

- Utilize the IAM Policy Simulator in the AWS Management Console to test the effectiveness of policy changes.
- Simulate various access scenarios to ensure that policies are granting the intended level of access without unintended consequences.

### **3. Access Reviews:**

- Conduct regular access reviews to ensure that IAM policies remain aligned with the principle of least privilege.
- Identify and remove any unnecessary permissions or policies that grant excessive access to resources.

### **4. AWS Config Remediation:**

- Configure AWS Config rules to automatically remediate non-compliant IAM policies.
- Set up remediation actions to adjust policies to adhere to granular access control principles automatically.

### **5. Employee Training:**

- Provide training and guidance to IAM administrators on best practices for crafting granular policies.
- Ensure that administrators understand the importance of restricting permissions to only what is necessary for each user or group.

### **6. Monitoring and Alerting:**

- Implement continuous monitoring solutions to detect and alert on any deviations from granular access control policies.
- Set up alerts to notify administrators of any unauthorized changes to IAM policies in real-time.

### **7. Documentation and Documentation:**

- Document changes made to IAM policies and keep records of policy adjustments.
- Maintain up-to-date documentation on IAM policies and access controls for reference during audits and compliance assessments.

## References:

1. <https://docs.aws.amazon.com/tag-editor/latest/userguide/tags-in-iam-policies.html>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	<b>16.2 <u>Configure Centralized Point of Authentication</u></b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

## 2.10 Ensure Resource Access via Tag-based Policies (Manual)

### Profile Applicability:

- Level 2

### Description:

For optimal granularity in EC2 access, configuring IAM policies via tags proves highly effective. This involves editing the JSON text editor to specify access permissions based on specific tags. In the provided example, I'm granting the "developers" group access exclusively to the newly created EC2 image, as illustrated in the attached screenshot depicting the policy creation process.

### Rationale:

Implementing IAM policies based on tags in EC2 enables administrators to finely tailor access control, granting permissions dynamically according to resource attributes. This approach enhances security and scalability by aligning access rights with specific resource requirements while minimizing manual intervention.

### Audit:

#### 1. Review IAM Policies:

- Access the IAM console in the AWS Management Console.
- Navigate to the "Policies" section and review policies associated with EC2 resources.
- Ensure that policies utilize condition keys related to EC2 tags for granting access.

#### 2. IAM Policy Simulator:

- Utilize the IAM Policy Simulator to simulate access scenarios based on EC2 tags.
- Test various tag-based policy configurations to verify that access is granted or denied appropriately.

#### 3. CloudTrail Analysis:

- Access the CloudTrail console and review logs related to IAM policy changes.
- Look for API calls related to modifications of policies using tag-based conditions.

#### 4. AWS Config Rules:

- Configure AWS Config rules to monitor IAM policies for tag-based conditions.
- Set up rules to detect policies that do not include tag-based conditions or are overly permissive.

#### 5. Manual Review:

- Manually inspect IAM policies to ensure they include tag-based conditions where applicable.



- Verify that policies accurately reflect the intended access control based on EC2 resource tags.
- 6. **Automated Scanning:**
  - Utilize third-party AWS security tools that offer automated scanning and analysis of IAM policies for tag-based conditions.
  - Configure these tools to regularly scan IAM policies and identify any deviations from best practices.
- 7. **Continuous Monitoring:**
  - Implement continuous monitoring solutions to track changes to IAM policies in real-time.
  - Set up alerts to notify administrators of any unauthorized modifications or policy changes that do not adhere to tag-based access control principles.

## **Remediation:**

1. **Policy Adjustment:**
  - Review existing IAM policies associated with EC2 resources to ensure they include tag-based conditions where applicable.
  - Modify policies to incorporate tag-based conditions for granular access control, ensuring that access is granted or denied based on resource attributes.
2. **IAM Policy Simulator Validation:**
  - Utilize the IAM Policy Simulator to validate the effectiveness of policy adjustments.
  - Test various access scenarios to verify that policies accurately reflect the intended access control based on EC2 resource tags.
3. **AWS Config Remediation:**
  - Configure AWS Config rules to automatically remediate IAM policies that do not include tag-based conditions.
  - Set up remediation actions to adjust policies to adhere to tag-based access control principles automatically.
4. **Employee Training:**
  - Provide training to IAM administrators on best practices for crafting IAM policies based on tags.
  - Ensure that administrators understand the importance of utilizing tag-based conditions for granular access control in EC2.
5. **Monitoring and Alerting:**
  - Implement continuous monitoring solutions to detect and alert on any deviations from tag-based access control policies.
  - Set up alerts to notify administrators of any unauthorized modifications or policy changes that do not adhere to tag-based access control principles.
6. **Documentation and Documentation:**
  - Document changes made to IAM policies to include tag-based conditions.
  - Maintain up-to-date documentation on IAM policies and access controls for reference during audits and compliance assessments.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.7 <u>Centralize Access Control</u></b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	<b>14.7 <u>Enforce Access Control to Data through Automated Tools</u></b> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			●

## 2.11 Ensure Secure Password Policy Implementation (Manual)

### Profile Applicability:

- Level 2

### Description:

Password policies outline the appropriate parameters for password configuration within an organization.

### Rationale:

Clear password policies provide essential guidelines for maintaining strong authentication practices, reducing the risk of unauthorized access and data breaches within an organization. By enforcing requirements for complex passwords and regular updates, these policies help bolster cybersecurity defenses and ensure compliance with industry standards and regulations.

### Audit:

#### 1. Review IAM Policies:

- Access the IAM console in the AWS Management Console.
- Navigate to the "Password Policy" section to review the current password policy settings.
- Ensure that the password policy aligns with industry best practices and organizational security requirements, including parameters such as minimum length, complexity requirements, and password expiration.

#### 2. AWS Config Rules:

- Configure AWS Config rules to monitor IAM password policies.
- Set up rules to check for compliance with password policy requirements, such as minimum length, complexity, and expiration settings.
- Use AWS Config to continuously assess the configuration of IAM password policies and identify any non-compliant settings.

#### 3. CloudTrail Analysis:

- Access the CloudTrail console and review logs related to IAM password policy changes.
- Look for API calls related to modifications of password policy settings.
- Analyze the logs to ensure that password policy changes are authorized and adhere to organizational security standards.

#### 4. Manual Review:

- Manually inspect the IAM password policy settings to verify compliance with security requirements.
- Check for parameters such as minimum password length, complexity requirements (e.g., uppercase, lowercase, special characters), and password expiration settings.

## Remediation:

### 1. Revise and Update Password Policies:

- Navigate to the IAM dashboard in the AWS Management Console.
- Go to the "Account settings" section to review and adjust the password policy.
- Strengthen the policy by setting requirements for password length, complexity (including uppercase, lowercase, numbers, and special characters), and rotation policies.

### 2. Enforce Password Changes:

- If the audit reveals passwords that do not comply with the updated policy, require users to change their passwords immediately.
- Implement mandatory password updates at regular intervals to ensure ongoing compliance with the policy.

### 3. Enable AWS Config for Continuous Compliance:

- Use AWS Config to continuously monitor and record IAM password policies.
- Set up AWS Config rules that automatically check compliance with your organization's password policy standards.

### 4. Utilize Multi-Factor Authentication (MFA):






- Enable MFA for an additional layer of security on all user accounts, especially for accounts with elevated permissions.
- Regularly audit the use of MFA across your AWS environment to ensure it is enabled and functioning correctly.

### 5. Automate Alerts and Responses:

- Set up real-time alerts for any non-compliant changes to password policies or unexpected password resets.
- Automate responses where possible to enforce compliance immediately when a deviation from the password policy is detected.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.7 Centralize Access Control</b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v8	<b>6.8 Define and Maintain Role-Based Access Control</b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>4.2 Change Default Passwords</b> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.			
v7	<b>4.5 Use Multifactor Authentication For All Administrative Access</b> Use multi-factor authentication and encrypted channels for all administrative account access.			

## 2.12 Ensure Monitoring EC2 and EBS with CloudWatch (Manual)

### Profile Applicability:

- Level 2

### Description:

CloudWatch is an AWS monitoring service that allows you to keep an eye on your AWS resources. You can track metrics via log files or worldclass data visuals. AWS CloudWatch allows the administrator to keep an eye on his/her AWS resources. You can set up alarms, monitor activity, and analyze log data. CloudWatch is a must to keep your AWS EBS and EC2 resources secure.

### Rationale:

Using CloudWatch to monitor EC2 instances and EBS volumes is essential for enhancing operational oversight and ensuring optimal performance within the AWS environment. This approach provides real-time insights into resource usage and system health, enabling proactive adjustments and timely responses to potential issues, thereby maintaining high availability and efficiency.

### Impact:

Failing to monitor EC2 instances and EBS volumes with CloudWatch can lead to delayed detection of performance issues and resource bottlenecks, potentially causing system outages and degraded user experiences. Without this monitoring, organizations also miss opportunities for proactive optimizations, increasing the risk of unexpected downtime and higher operational costs.

### Audit:

Creating an AWS CloudWatch Dashboard:

1. Navigate to the AWS CloudWatch Console - <https://us-east-2.console.aws.amazon.com/cloudwatch/home?region=us-east-2#home>.
2. Select the dashboard type that's right for you. Give the dashboard a name. Name the dashboard as something memorable. You can select which resources you want to monitor. Select "EBS."
3. Create an alarm - Alarms are important to send you an alert as soon as something suspicious happens on your volume. You can create an alarm to alert you when a certain threshold of IOPS are reached. To create alarm, follow steps -
  - Go to "Alarms" on the left hand side of the CloudWatch dashboard.
  - Select "Create a new alarm".
  - Select "EBS".
  - Select what you want to monitor. We're going to choose to monitor the write operations of an EBS volume.

- Go back to the volume that was created in EC2 dashboard and copy the volume ID under the “volume ID” field.
- Configure the settings that you want to trigger an alarm.
- Move onto the next step before continuing.

## Remediation:

### 1. Enable CloudWatch Monitoring:

- Access the AWS Management Console, navigate to the EC2 dashboard, and select the instances and EBS volumes.
- Enable detailed monitoring on each EC2 instance and EBS volume to collect data at a higher granularity.

### 2. Configure CloudWatch Alarms:

- In the CloudWatch console, set up alarms based on key performance metrics such as CPU utilization, disk read/write operations, and network traffic.
- Configure these alarms to notify administrators via email or SMS when thresholds are breached, allowing for immediate action.

### 3. Establish Baselines:

- Analyze historical performance data from CloudWatch to establish baseline performance metrics for each instance and volume.
- Use these baselines to identify abnormal behavior or performance degradation over time.







### 4. Automate Responses:

- Utilize AWS CloudWatch Events and AWS Lambda to automate responses to specific alarms, such as scaling operations or initiating recovery processes.
- Ensure these automated scripts are tested and reflect the operational policies of your organization.

## References:

1. [https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch\\_Embedded\\_Metric\\_Format\\_View.html](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Embedded_Metric_Format_View.html)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise’s audit log management process, has been enabled across enterprise assets.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>6.5 <u>Central Log Management</u></b> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●



## 2.13 Ensure creating an SNS subscription (Manual)

### Profile Applicability:

- Level 2

### Description:

Create an SNS notification to send to the system administrator's email address.

### Rationale:

### Audit:

Creating an SNS subscription:

1. Navigate to SNS service in the AWS console - <https://us-east-2.console.aws.amazon.com/sns/v3/home?region=us-east-2#/homepage> (make sure you are in the correct region).
2. Navigate to "topics".
3. Create a new topic.
4. Select the ARN of the topic.
5. Select the "Email" protocol if you wish to have the alarms delivered to your email.
6. Enter the correct email address of an administrator.
7. Select "Create Subscription".

To attach the SNS notification service to the alarm - select the SNS subscription that you just created and create the alarm.

### Remediation:

### References:

1. <https://docs.aws.amazon.com/sns/latest/dg/sns-getting-started.html>

### 3 Elastic File System (EFS)

Amazon Elastic File System (EFS) automatically grows and shrinks as you add and remove files with no need for management or provisioning. AWS EFS is a serverless file storage service that allows users to easily configure filesystems. AWS takes care of provisioning, patching, and deploying the file system when you use EFS. This file system is built to scale without any user configuration changes. This means that the file system automatically gets bigger as the storage needs increase. The file system will also shrink with decreasing requirements, ensuring you only pay for what you need.

### 3.1 EFS (Manual)

#### Profile Applicability:

- Level 2

#### Description:

AWS EFS is a scalable and fully-managed storage service that enables you to quickly deploy file systems without the hassle of configuring, patching, or maintaining them.

#### Rationale:

Utilize AWS EFS to streamline your file system deployment, allowing the service to handle the heavy lifting for you.

#### Impact:

Not using AWS EFS for your file system deployment can lead to increased management overhead, as you'll need to manually configure, patch, and maintain the systems. This manual effort is time-consuming and complex, raising the potential for errors that could result in downtime and data loss. By not leveraging AWS EFS, you miss out on the streamlined, automated management and scalability that the service provides, potentially impacting your operational efficiency and reliability.

#### Audit:

To create an Amazon EFS (Elastic File System), you can follow these steps:

1. Sign in to the AWS Management Console and navigate to the Amazon EFS console - <https://us-east-2.console.aws.amazon.com/efs?region=us-east-2#/get-started>.
2. Click on the "Create file system" button.
3. Enter a name for your file system.
4. Choose a VPC for your file system
5. Then you have to go to File system settings to edit configurations , then you have to select Lifecycle management , performance settings and File system protection , and then click save changes.

#### Remediation:

To create an Amazon EFS (Elastic File System), follow these steps:












1. **Open the Amazon EFS Console:** Sign in to your AWS Management Console and navigate to the Amazon EFS service.

2. **Create File System:** Click on the "Create file system" button to start the creation process.
3. **Configure File System:** Select your desired VPC (Virtual Private Cloud) and availability zones for the file system. Optionally, you can configure settings like throughput mode and lifecycle management.
4. **Configure Access Points:** Set up access points if needed, to control access permissions and streamline access management.
5. **Review and Create:** Review your settings and click on the "Create" button to create the file system.
6. **Mount the File System:** Once created, use the provided mount targets and instructions to mount the file system to your EC2 instances or other resources.

#### References:

1. <https://us-east-2.console.aws.amazon.com/efs?region=us-east-2#/get-started>

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>7.3 <u>Perform Automated Operating System Patch Management</u></b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b>3.4 <u>Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	<b>5.4 <u>Deploy System Configuration Management Tools</u></b> Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.			

## 3.2 Ensure Implementation of EFS (Manual)

### Profile Applicability:

- Level 2

### Description:

AWS EFS is a fully managed storage service that enables rapid file system deployment without the need for configuration, patching, or maintenance.

### Rationale:

The rationale behind using AWS EFS is to simplify and expedite the deployment of file systems, eliminating the need for manual configuration, patching, and maintenance. This allows you to focus on other critical aspects of your operations while benefiting from a reliable, scalable, and fully managed storage solution.

### Impact:

Not using AWS EFS can lead to increased complexity and time-consuming manual management for configuration, patching, and maintenance. This raises the risk of human error, system downtime, and data loss, while also making it more challenging to scale your file systems efficiently.

### Audit:

1. Navigate to console - <https://us-east-1.console.aws.amazon.com/efs/home?region=us-east-1#/get-started>.
2. Select "Create File System". Give the file system a name and select the default VPC. Select "Create".
3. Encrypting data at rest - The EFS is encrypted automatically upon creation..
4. Attach the EFS to an EC2 instance.
5. Navigate to file system details - Select the radio box next to the file system that was just created and select "view details".
6. Creating an NFS directory on your EC2 instance - Launch your EC2 instance. Once connected, Type following command:  
`“sudo mkdir efs”`  
to create a new efs directory.
7. Mounting an NFS directory on your EC2 instance - Navigate to find your EC2 DNS information  
Paste this command into the console after making the efs directory

```
sudo mount -t nfs -o  
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport  
mount-target-DNS:/ ~/efs-mount-point ``
```

NOTE: The encryption takes place as soon as you mount the directory. This encrypts the data in transit.

8. Terminating the EC2 instance - The EFS file system that was just mounted doesn't persist on reboot. You can consult the AWS documentation to see how you can write a script to automatically mount the file system upon every reboot.

## Remediation:










To remediate the issues of manual file system management, follow these steps to create and use Amazon EFS:

1. **Open the Amazon EFS Console:** Sign in to the AWS Management Console and navigate to the Amazon EFS service.
2. **Create a New File System:** Click on "Create file system" to start the setup process.
3. **Configure Settings:** Select your desired VPC, availability zones, throughput mode, and any additional settings like lifecycle management.
4. **Set Up Access Points:** Configure access points to control permissions and simplify access management.
5. **Review and Create:** Verify your settings and click "Create" to finalize the file system setup.
6. **Mount the File System:** Use the provided mount targets and instructions to attach the file system to your EC2 instances or other resources.

## References:

1. <https://aws.amazon.com/efs/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v8	<b>8.3 <u>Ensure Adequate Audit Log Storage</u></b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	<b>5.2 <u>Maintain Secure Images</u></b> Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.			
v7	<b>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></b> Only allow access to authorized cloud storage or email providers.			

### 3.3 Ensure EFS and VPC Integration (Manual)

#### Profile Applicability:

- Level 2

#### Description:

You can use EFS as a network file system across availability zones on a virtual private cloud. This capability allows the organization to create a highly available file sharing solution. Leveraging AWS VPC and EC2 in tandem with AWS EFS makes for a highly available and scalable cloud file storage solution.

#### Rationale:

Redundancy and scalability are crucial for maintaining uninterrupted services. By integrating these AWS services, users can harness the full power of AWS, ensuring a resilient and scalable infrastructure.

#### Impact:

Not integrating AWS services for redundancy and scalability can lead to service disruptions and increased downtime. This approach also limits your ability to efficiently handle growing workloads, negatively impacting performance and user experience.

#### Audit:

#### Audit Procedures for AWS Redundancy and Scalability

1. **Create Mount Targets in Each Availability Zone:** Ensure EFS is attached in each availability zone by creating mount targets in each subnet. Although multiple subnets can exist per availability zone, verify that EFS is configured to work with one subnet per zone to maintain redundancy.
2. **Monitor EFS with CloudWatch:** Use AWS CloudWatch to automatically monitor your EFS service. Check that alarms are configured and logs and events are tracked effectively, providing real-time insights into the performance and health of your file systems.

#### Remediation:










Create an EC2 instance in each availability zone within your VPC.

#### References:

1. <https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-conceptual>



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v8	<b>16.7 <u>Use Standard Hardening Configuration Templates for Application Infrastructure</u></b> Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.			
v7	<b>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></b> Only allow access to authorized cloud storage or email providers.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

### 3.4 Ensure controlling Network access to EFS Services (Manual)

#### Profile Applicability:

- Level 2

#### Description:

It's important that you secure access to your resources on your AWS VPC network. There are several ways to ensure that you control what traffic is accessing your resources. Some of which include tightening down network layer security using a Security Group and a NACL within the VPC console. You can also tighten down Security Groups within your EC2 console and by using AWS IAM. Maintaining network security is a high priority to ensure that no unauthorized users can access the data stored on your EFS service.

#### Rationale:

Maintaining network security is a best practice essential for keeping your data safe and secure.

#### Impact:

Failing to maintain network security can lead to significant vulnerabilities, exposing your data to unauthorized access, breaches, and potential data loss. This can result in severe financial, operational, and reputational damage to your organization.

#### Audit:




#### Remediation:







Implement network security access controls.

#### References:

1. <https://docs.aws.amazon.com/efs/latest/ug/NFS-access-control-efs.html>

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>13.5 <u>Manage Access Control for Remote Assets</u></b> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	<b>1.7 <u>Deploy Port Level Access Control</u></b> Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.			
v7	<b>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></b> Only allow access to authorized cloud storage or email providers.			

### 3.5 Ensure using Security Groups for VPC (Manual)

#### Profile Applicability:

- Level 2

#### Description:

A security group controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

#### Rationale:

#### Audit:

1. Go to <https://console.aws.amazon.com/vpc/>
2. Navigate to Security Groups and select on the VPC that houses your mount target.
3. Ensure that incoming traffic is restricted to SSH access on port 22 using TCP protocol and outbound traffic is accepting all traffic.

#### Remediation:

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.7 Centralize Access Control</b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v8	<b>13.9 Deploy Port-Level Access Control</b> Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			●
v7	<b>1.7 Deploy Port Level Access Control</b> Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●

## 3.6 Ensure Secure Ports (Manual)

### Profile Applicability:

- Level 2

### Description:

Securing network ports is essential for protecting AWS storage services like Amazon S3, EFS, and EBS. By configuring security groups and network access control lists (NACLs) to allow only necessary traffic, you minimize the risk of unauthorized access. Regular audits and monitoring of port usage ensure that only approved ports and protocols are operational, enhancing the overall security of your AWS storage environment.

### Rationale:

By limiting traffic to only necessary and approved ports and protocols, you reduce the attack surface and enhance the overall security of your storage environment. Regular audits and monitoring further ensure that security measures remain effective and up-to-date, safeguarding your data from emerging threats.

### Impact:

Not securing network ports in AWS storage services can lead to significant vulnerabilities, exposing your data to unauthorized access and potential breaches. This lack of control increases the risk of attacks, such as port scanning and exploitation of open ports, which can result in data loss, corruption, and theft. Consequently, your organization may face severe financial losses, operational disruptions, and damage to its reputation.

### Audit:

#### 1. Review Security Group Configurations:

1. Navigate to "Security Groups" under "Network & Security".
2. Verify that security groups are configured to allow only necessary inbound and outbound traffic.
3. Ensure rules are in place to restrict access to critical storage services, such as Amazon S3, EFS, and EBS.

#### 2. Check Network Access Control Lists (NACLs):

○

##### Steps:









1. Navigate to "Network ACLs" under "Security".
2. Ensure NACLs are configured to control traffic to and from subnets, allowing only necessary ports and protocols.
3. Verify that rules are implemented to deny unauthorized access.

#### 3. Monitor VPC Flow Logs:

- - Steps:**
    1. Enable VPC Flow Logs for each VPC.
    2. Regularly review flow logs to monitor traffic and identify any unauthorized access attempts or anomalies.
    3. Investigate and remediate any unusual traffic patterns.
- 4. **Inspect IAM Policies and Roles:**
  - - Steps:**
      1. Review IAM policies to ensure they enforce least privilege principles for access to storage services.
      2. Verify that roles are appropriately assigned and used to control access to security groups and NACLs.
- 5. **Enable and Review AWS CloudTrail Logs:**
  - - Steps:**
      1. Ensure CloudTrail is enabled in all regions.
      2. Regularly review CloudTrail logs for any changes to security groups, NACLs, and IAM policies.
      3. Set up alerts for critical security events related to port configurations.
- 6. **Conduct Regular Penetration Testing:**
  - - Steps:**
      1. Conduct tests to identify vulnerabilities in port configurations.
      2. Review findings and implement necessary security measures to address identified issues.
      3. Ensure compliance with AWS penetration testing policies.
- 7. **Verify Encryption in Transit:**
  - - Steps:**
      1. Ensure that data encryption is enabled for data in transit.
      2. Verify that encryption keys are managed securely using AWS Key Management Service (KMS).
      3. Check that all communication with storage services is encrypted.
- 8. **Implement and Review Security Best Practices:**
  - - Steps:**
      1. Implement recommended best practices for securing network ports and storage services.
      2. Regularly review and update security configurations to align with evolving best practices.
      3. Conduct periodic training for staff on security best practices and AWS configurations.

## Remediation:

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	<b>13.9 <u>Deploy Port-Level Access Control</u></b> Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			
v7	<b>1.7 <u>Deploy Port Level Access Control</u></b> Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## 3.7 Ensure File-Level Access Control with Mount Targets (Manual)

### Profile Applicability:

- Level 2

### Description:

Mount targets act as gateways, enabling resources to be accessed across different availability zones within a VPC. When you create an EFS file system, mount targets are automatically provisioned in each availability zone associated with the VPC. This ensures high availability and redundancy, allowing seamless and efficient access to the EFS file system from any availability zone.

### Rationale:

Using mount targets ensures seamless access to the EFS file system across different availability zones within a VPC. This automatic provisioning of mount targets in each availability zone provides high availability and redundancy, essential for maintaining uninterrupted data access. It simplifies configuration and enhances the resilience and scalability of the file system architecture.

### Impact:

Not using mount targets can lead to inefficient and unreliable access to the EFS file system across availability zones. This lack of automatic provisioning reduces high availability and redundancy, increasing the risk of service interruptions and data access issues. Consequently, your infrastructure may suffer from decreased performance, higher latency, and potential data loss or downtime.

### Audit:

### Remediation:









Control access by modifying mount targets in each availability zone.

### References:

1. <https://docs.aws.amazon.com/efs/latest/ug/accessing-fs.html>



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	<b>14.7 <u>Enforce Access Control to Data through Automated Tools</u></b> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

## 3.8 Ensure managing mount target security groups (Manual)

### Profile Applicability:

- Level 2

### Description:

Managing security groups for mount targets is essential for controlling access to your Amazon EFS file systems. By configuring these security groups, you ensure that only authorized network traffic can access your file systems, enhancing security. Regular reviews and updates of security group rules maintain strict access control, protecting your data from unauthorized access and potential breaches.

### Rationale:

The rationale for managing security groups for mount targets is to ensure robust access control and security for your Amazon EFS file systems. By configuring these security groups, you restrict access to only authorized network traffic, thereby minimizing the risk of unauthorized access and potential data breaches. Regularly reviewing and updating these rules helps maintain strong security measures and compliance with organizational policies and industry standards.

### Impact:

Not managing security groups for mount targets can lead to significant vulnerabilities, exposing your Amazon EFS file systems to unauthorized access and potential breaches. This lack of control increases the risk of malicious attacks, data theft, and data corruption. Consequently, your organization may face severe financial losses, operational disruptions, and damage to its reputation.

### Audit:










1. Navigate to EFS.
2. Select file systems.
3. Click the radio box and select "view details".
4. Select the "manage" button.
5. Select "Networking" tab.
6. This will bring up a screen for each of your mount points.
7. To edit Security Groups, select "Manage". From here, you can edit security groups for each mount point. This gives you control of how traffic can flow between each subnet.

### Remediation:

### References:

1. <https://docs.aws.amazon.com/efs/latest/ug/accessing-fs.html>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	<b>13.9 <u>Deploy Port-Level Access Control</u></b> Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			
v7	<b>1.7 <u>Deploy Port Level Access Control</u></b> Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

### 3.9 Ensure using VPC endpoints - EFS (Manual)

#### Profile Applicability:

- Level 2

#### Description:

With AWS PrivateLink, VPC Endpoints allow services to communicate within AWS using private IP addresses within approved CIDR ranges. This communication can be achieved without the need for a VPN, ensuring secure and efficient data transfer.

#### Rationale:

The rationale behind using AWS PrivateLink with VPC Endpoints is to enable secure and efficient communication between services within AWS. By using private IP addresses within approved CIDR ranges, it eliminates the need for a VPN, reducing complexity and potential points of failure. This approach enhances security, reduces latency, and ensures data remains within the AWS network, aligning with best practices for secure and reliable cloud architecture.

#### Impact:

Not using AWS PrivateLink with VPC Endpoints can lead to several issues, including increased security risks and potential data exposure since services would need to communicate over the public internet or through more complex VPN setups. This can result in higher latency, reduced performance, and greater vulnerability to attacks. Additionally, managing VPN connections adds complexity and potential points of failure, compromising the overall efficiency and reliability of your network architecture.

#### Audit:

Creating a FIPS compliant interface endpoint for EFS:

1. Navigate to VPC Console: <https://console.aws.amazon.com/vpc/>.
2. Select "Endpoints" on the sidebar.
3. Select "Create endpoint."
4. Name the endpoint.
5. Copy and paste this services into the services bar:  
com.amazonaws.region.elasticfilesystem-fips – replace "region:" with us-east-1 or whatever region you're using.
6. Select your VPC.
7. For subnets, select the availability zone and then select private subnet.
8. Select the Security Group for the VPC endpoint.
9. For policy: select "full access".
10. Create a tag for future reference / granular IAM permissions.
11. Create endpoint.











## Remediation:

Use VPC Endpoints in tandem with AWS Private Link to secure your EFS connections.

## References:

1. [https://docs.aws.amazon.com/efs/latest/ug/efs-vpc-endpoints.html#:~:text=To%20establish%20a%20private%20connection,private%20network%20\(VPN\)%20connection.](https://docs.aws.amazon.com/efs/latest/ug/efs-vpc-endpoints.html#:~:text=To%20establish%20a%20private%20connection,private%20network%20(VPN)%20connection.)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>13.5 <u>Manage Access Control for Remote Assets</u></b> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v8	<b>14.5 <u>Train Workforce Members on Causes of Unintentional Data Exposure</u></b> Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	<b>13.1 <u>Maintain an Inventory Sensitive Information</u></b> Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.			

### 3.10 Ensure managing AWS EFS access points (Manual)

#### Profile Applicability:

- Level 2

#### Description:

EFS access points serve as gateways to your EFS file system, allowing applications to interact with the file system across various resources. Proper configuration of these access points within your applications is crucial to ensure seamless and secure access. By configuring EFS access points, you can control and manage which users have access to specific resources in your EFS environment, enhancing security and operational efficiency.

#### Rationale:

The rationale behind properly configuring EFS access points is to ensure secure and efficient interaction between your applications and the EFS file system. By setting up these access points correctly, you can control and manage user permissions, ensuring that only authorized users can access specific resources. This not only enhances the security of your data but also improves operational efficiency by preventing unauthorized access and potential data breaches.

#### Audit:

1. Creating an EFS access point:  
You can create an EFS access point through the amazon CLI, AWS console, and with the EFS API. An EFS can only have up to 1,000 access points.
2. Mounting an EFS access point:  
Consult the section where we mounted an EFS file system on an EC2 instance. While inside the resource you want to configure an access point for, type in this command:

```
mount -t efs -o tls,iam,accesspoint=fsap-abcdef0123456789a fs-  
abc0123def456789a: /localmountpoint
```

3. Enforcing a User Identity with an EFS access point:  
You can enforce user identity to ensure that users and groups with proper permissions are able to access the EFS file system. In order to do this, you must specify the user and group ID you wish to have ownership of the files. When **enforcement** is enabled, that file that is was created by the user will automatically show ownership to belong to the user. When enforcement is enabled, the access point considers the User ID, group ID, and secondary group ID. It ignored the NFS client's ID.

Note: enforcing the user ID is subject to the "ClientRootAccess" IAM permission. If either the User ID or Group ID = 0, then you must explicitly allow "ClientRootAccess" permission.

4. Enforcing a root directory with an access point:

If you wish to override the root directory of the EFS, you can make the root directory that of the access point. To enforce the root directory with an access point, you must specify three things upon provisioning the EFS mount point:

- Owner UID
- Group GID
- Permissions

To access an EFS from an access point, a root directory must be created and enforced. Reminder: You must specify permissions for the access point root directory. If these permissions are not defined, a root directory will not be created on the mount point, and you will not be able to access EFS from an access point.

5. Security Model for access point root directories:

When a root directory override is in effect, the EFS behaves like a Linux server with a no\_subtree\_check option enabled.





**Remediation:**





Implement AWS EFS access points

**References:**

1. <https://docs.aws.amazon.com/efs/latest/ug/efs-access-points.html>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	<b>14.7 <u>Enforce Access Control to Data through Automated Tools</u></b> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			



### 3.11 Ensure accessing Points and IAM Policies (Manual)

#### Profile Applicability:

- Level 2

#### Description:

You can use IAM policies to control access to your EFS access points. To achieve this, utilize the `elasticfilesystem:AccessPointArn` IAM condition key. The `AccessPointArn` represents the Amazon Resource Name (ARN) of the access point that the file system is mounted with.

#### Rationale:

The rationale for using IAM policies with the `elasticfilesystem:AccessPointArn` condition key is to ensure precise and secure access control to EFS access points. By specifying the access point's ARN, you can restrict interactions to authorized users and resources only, thereby enhancing data security and preventing unauthorized access. This approach maintains the integrity and confidentiality of your data within the AWS environment.

#### Audit:

Below is a same IAM policy copied from the AWS documentation:




```
{
  "Version": "2012-10-17",
  "Id": "MyFileSystemPolicy",
  "Statement": [
    {
      "Sid": "App1Access",
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::111122223333:role/app1" },
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Condition": {
        "StringEquals": {
          "elasticfilesystem:AccessPointArn": "arn:aws:elasticfilesystem:us-east-1:222233334444:access-point/fsap-01234567"
        }
      }
    },
    {
      "Sid": "App2Access",
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::111122223333:role/app2" },
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Condition": {
        "StringEquals": {
          "elasticfilesystem:AccessPointArn": "arn:aws:elasticfilesystem:us-east-1:222233334444:access-point/fsap-89abcdef"
        }
      }
    }
  ]
}
```

## Remediation:

## References:

1. <https://docs.aws.amazon.com/efs/latest/ug/efs-access-points.html>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	<b>1.7 <u>Deploy Port Level Access Control</u></b> Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

### 3.12 Ensure configuring IAM for AWS Elastic Disaster Recovery (Manual)

#### Profile Applicability:

- Level 2

#### Description:

Before installing the AWS Elastic Disaster Recovery client, you need to configure AWS IAM permissions and users for both the AWS Replication and AWS Failback Client.

#### Rationale:

Configuring AWS IAM permissions and users before installing the AWS Elastic Disaster Recovery client ensures that the AWS Replication and AWS Failback Client have the necessary access rights. This setup is essential for maintaining security and preventing unauthorized access. Proper IAM configuration guarantees the smooth operation of disaster recovery processes, safeguarding your data and ensuring system reliability.

#### Audit:

To create DRS Agent User, follow following steps:

1. Navigate to the AWS IAM Console - <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home>.
2. Create new user. This user will only be able to access the Elastic disaster recovery agent installation resource. Accordingly, name the user "DSRuser".
3. Allow Programmatic access: This allows the user to access resources programmatically with a secure key rather than having to enter a password.
4. elect "attach policies directly" and search for "AWSElasticDisasterRecoveryAgentInstallationPolicy".
5. Create user.

To create Failback Agent User, Follow the steps above with these two modifications:

1. Name the user "FailbackAgentuser".
2. Apply the "AWSElasticDisasterRecoveryFailbackInstallationPolicy".










#### Remediation:

Configure IAM Credentials for AWS Elastic Disaster Recovery.

#### References:

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

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			
v7	<b>1.7 <u>Deploy Port Level Access Control</u></b> Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 4 FSx

Amazon FSx provides fully managed, high-performance file storage solutions tailored for various workloads. It includes Amazon FSx for Windows File Server for Windows-based applications, Amazon FSx for Lustre for high-performance computing and data processing, and Amazon FSx for NetApp ONTAP for advanced data management capabilities. These services ensure seamless integration, scalability, and reliability for diverse storage needs.

## 4.1 FSX (AWS Elastic File Cache) (Manual)

### Profile Applicability:

- Level 2

### Description:

Amazon File Cache is a fully managed, high speed cache on AWS that is used to process file data, regardless of where the data is stored. AWS File Cache is a serverless service on AWS that spares the administrators from the burden of managing file servers and storage volumes, updating hardware, configuring software, running out of capacity, or tuning performance. AWS Elastic cache is capable of handling hundreds of GB/s of throughput and up to millions of operations per second. AWS FSx is an excellent service for cost optimization and high scalability. Amazon File Cache automatically loads data into the cache when it's accessed for the first time and automatically releases data when it's not used.

### Rationale:

Amazon File Cache is used as a temporary, high performance storage location for data that's stored in on-premises file systems, AWS file systems, and Amazon S3 buckets. This service is used for data processing and is best suited for applications that need high data processing speeds. This is not a long term storage option.

### Audit:

### Remediation:












You can link your cache to S3 data repositories or to any file system that supports the NFSv3 protocol. The NFS data repository can either be on premises or in the cloud and you can link a maximum of eight repositories. All the linked repositories must be using the same file system; either S3 or NFS. When linked to a data repository, Amazon File Cache transparently presents S3 or NFS objects as files and directories.

Amazon File Cache is compatible to be used interchangeably with Amazon Elastic Compute Service, Amazon Elastic Container Service, and Amazon Elastic Kubernetes Service.

### References:

1. <https://aws.amazon.com/fsx/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	<b>8.3 <u>Ensure Adequate Audit Log Storage</u></b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	<b>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></b> Only allow access to authorized cloud storage or email providers.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			



## 4.2 Amazon Elastic File Cache (Manual)

### Profile Applicability:

- Level 2

### Description:

Amazon File Cache is available in the following AWS Regions:

1. US East (N. Virginia)
2. US East (Ohio)
3. US West (Oregon)
4. Canada (Central)
5. Europe (Frankfurt)
6. Europe (Ireland)
7. Europe (London)
8. Europe (Stockholm)
9. Asia Pacific (Hong Kong)
10. Asia Pacific (Mumbai)
11. Asia Pacific (Seoul)
12. Asia Pacific (Tokyo)
13. Asia Pacific (Singapore)
14. Asia Pacific (Sydney)

Amazon Elastic File Cache Compatibility: In order to use AWS FSx, you must ensure that the operating system you're using on the compute instance is compatible with AWS FSx. Below are the compatible operating systems:

1. Amazon Linux 2 and Amazon Linux
2. Red Hat Enterprise Linux (RHEL)
3. CentOS
4. Rocky Linux
5. Ubuntu. The Lustre client must be installed on these systems in order for the FSx service to work.

### Rationale:

The rationale behind creating Amazon Elastic File Cache is to enhance the performance and scalability of cloud-based applications by providing a high-speed, scalable file caching solution. This service reduces latency and improves access times for frequently accessed data, thereby optimizing application performance and user experience. Additionally, it helps manage and reduce storage costs by efficiently utilizing cached data, ensuring that resources are used effectively while maintaining high performance standards.

## Impact:

Not implementing Amazon Elastic File Cache can lead to increased latency and slower access times for frequently accessed data, resulting in suboptimal performance for cloud-based applications. This can negatively affect user experience and productivity. Additionally, without an efficient caching solution, there may be higher storage costs due to inefficient use of resources, and the system may struggle to handle high demand, leading to potential performance bottlenecks and scalability issues.

## Audit:

Creating Amazon Elastic File Cache:

Before you can start using Amazon Elastic File Cache, you must set up an Amazon Elastic Compute Instance and an S3 bucket.

We're going to create a new EC2 instance and S3 bucket for the sake of this tutorial.

Creating an EC2 instance for FSx:

Make sure that whatever AMI you select is compatible with Lustre 2.12 client.









- Navigate to the Amazon EC2 console.
- Select "Launch Instance".
- Give your server a name.
- Select "Ubuntu" or an operating system that's compatible with FSx.
- Select default VPC and security group.
- Select or create private SSH keys.
- Leave the rest of the settings default.
- Create Instance.




## Remediation:

## References:

1. <https://aws.amazon.com/fsx/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	<b>8.3 <u>Ensure Adequate Audit Log Storage</u></b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	<b>6.4 <u>Ensure adequate storage for logs</u></b> Ensure that all systems that store logs have adequate storage space for the logs generated.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><b>14.6 <u>Protect Information through Access Control Lists</u></b></p> <p>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.</p>			

## 4.3 Ensure the creation of an FSX Bucket (Manual)

### Profile Applicability:

- Level 2

### Description:

An S3 bucket will store the data that Amazon Elastic File Cache accesses

### Rationale:

Storing data in S3 ensures scalability, durability, and cost-efficiency, while Amazon Elastic File Cache enhances access speed by caching frequently accessed data. This combination leverages the strengths of both services, providing a seamless and efficient data storage and retrieval solution.

### Audit:




1. Navigate to the Amazon S3 bucket console.  
<https://s3.console.aws.amazon.com/s3/>.
2. Select "Create Bucket".
3. Give your bucket a name and select the region. Note: your bucket must be a unique name that's not used anywhere else on AWS.
4. Block public access: This is an internal service that will not be accessed outside of our internal AWS network. Keep the "block public access" setting checked.
5. Enable bucket versioning.
6. Leave the rest of the settings as default.
7. Select "create bucket."
8. Create a path in your bucket, give it a name and leave the encryption as default for now.









### Remediation:

### References:

1. <https://docs.aws.amazon.com/fsx/latest/LustreGuide/create-dra-linked-data-repo.html>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.3 <u>Ensure Adequate Audit Log Storage</u></b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	<b>6.4 <u>Ensure adequate storage for logs</u></b> Ensure that all systems that store logs have adequate storage space for the logs generated.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 4.4 Ensure the creation of Elastic File Cache (Manual)

### Profile Applicability:

- Level 2

### Description:

With the prerequisites completed, we can now proceed to create our Elastic File Cache.

### Rationale:

By implementing an Elastic File Cache, frequently accessed data is stored closer to the application, reducing latency and speeding up access times. This approach optimizes resource utilization, improves user experience, and ensures that the system can handle high-demand workloads effectively.

### Audit:

1. Navigate to the AWS Elastic File Cache console:  
<https://console.aws.amazon.com/fsx/>.
2. Click the hamburger menu on the left side of the screen and select “caches”.
3. Select “Create Cache”
4. Give your Cache a name. Choose a name that you will remember.
5. Select the amount of storage capacity you need for your cache. We’ll select 1.2 TiB for this tutorial. You can select storage capacity in increments of 1.2 TiB.
6. Select the amount of throughput capacity. The amount of Throughput capacity is calculated by multiplying the cache storage capacity by the throughput tier. For example, for a 1.2 TiB cache, it's 1200 MB/s; for a 9.6 TiB cache, it's 9600 MB/s. Throughput capacity is the sustained speed at which the file server that hosts your cache can serve data.
7. In the Network & Security section, provide networking and security group information:
  - For Virtual Private Cloud (VPC) choose the correct amazon VPC that you want to associate with your cache. We’re going to use the default VPC.
  - For VPC Security Groups, the ID for the default security group for your VPC should already be added.
  - For Subnet, you can choose any of the available subnets.
8. In the Encryption section, choose the Default aws/fsx KMS encryption keys to protect your data by encrypting your data at-rest.
9. You have the option to create tags; this is an optional step.
10. Select “next”.
11. In the Data repository associations (DRAs) section, there are no DRAs linking your cache to S3 or NFS repositories. We need to link the cache that we’re creating to the Amazon S3 bucket that we created earlier.
  - For Data repository type, choose S3
  - For Data repository path, type the path of the S3 bucket that you want to associate with this cache. For example:

```
s3://{example-bucket}/{example-prefix}
```
- To access this URL, go back to the S3 bucket that was just created and navigate to the directory of the folder that you created. Select "copy AWS URI".
- For cache path, enter the name of a high-level directory such as /ns1 or subdirectory such as ns1/subdir within Amazon File Cache to associate with the S3 data repository. The first forward slash in the path is required.
12. Select "next" this will take you to the summary page.
13. Choose "Create Cache." You will see your cache in the FSx dashboard.
```

## Remediation:

## References:

1. <https://aws.amazon.com/filecache/>

## 4.5 Ensure installation and configuration of Lustre Client (Manual)

### Profile Applicability:

- Level 2

### Description:

To utilize the newly created File Cache, you must install the Lustre Client on your EC2 instance.

### Rationale:

The Lustre Client facilitates efficient communication between the EC2 instance and the File Cache, ensuring high-performance data access and improved overall system efficiency. This setup is crucial for optimizing data processing and leveraging the benefits of the File Cache.

### Audit:

Follow along to install the Lustre Client on Ubuntu 22.04:

1. Launch your EC2 instance. Navigate to the folder of your secure key and ssh into the instance using this command:
  - `ssh -i "{KEY.pem}" ubuntu@{your ec2 instance}`
  - When prompted to log in with the SSH key, enter in "yes"
  - You should now be connected to your EC2 instance.
2. Run the following command to download and install the public Lustre key:

```
wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
```

3. Add the AWS Lustre package repository to your local package manager using the following command:

```
sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu jammy main" >/etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
```

4. Determine which kernel is currently running on your client instance and update as needed. The AWS Lustre client on Ubuntu 22.02 requires kernel 5.15.0.1020-aws or later for both x86 based EC2 instances and Arm-based EC2 instances powered by AWS Graviton processors:
  - a. Run the following command to find out which kernel your machine is running:  
`uname -r`













- If your kernel is not up to date, run the following command: This will install the kernel update, Lustre client update, as well as reboot your system.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
- If your kernel is up to date and you just want to install the latest Lustre
version, run this command:
sudo apt install -y lustre-client-modules-$(uname -r)
```

## Remediation:

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                 |  |    |    |
| v8               | <b>14.2 <u>Train Workforce Members to Recognize Social Engineering Attacks</u></b><br>Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.                                                                                                          |  |    |    |
| v7               | <b>5.2 <u>Maintain Secure Images</u></b><br>Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates. |                                                                                     |  |  |
| v7               | <b>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></b><br>Only allow access to authorized cloud storage or email providers.                                                                                                                                                       |                                                                                     |  |  |

## 4.6 Ensure EC2 Kernel compatibility with Lustre (Manual)

### Profile Applicability:

- Level 2

### Description:

The latest kernel included with the Ubuntu Amazon EC2 AMI is not compatible with the Lustre service, which is crucial for mounting the cache on your EC2 instance. To downgrade your kernel, specific prerequisites must be met if you are using the default Ubuntu machine image as of November 8, 2023.

### Rationale:

The latest kernel version is not supported by Lustre, and meeting the prerequisites for downgrading will allow you to leverage Lustre's high-performance file system capabilities effectively. This ensures optimal data access and processing efficiency on your EC2 instance.

### Audit:

Follow the steps to downgrade your kernel:

1. List all of the available Lustre packages by typing in this command: `sudo apt-cache search lustre-client-modules`. This will show a list of supported modules with corresponding kernel versions in ascending order from top to bottom. The most recent version in this case is "lustre-client-modules-5.15.0-1049-aws". Save this information for the next commands.
2. Install the most recent linux image that supports the Lustre client with this command:

```
sudo apt-get install -y linux-image-5.15.0-1049-aws
sudo sed -i 's/GRUB_DEFAULT=.\/+\/GRUB\ _DEFAULT="Advanced options for
Ubuntu>Ubuntu, with Linux 5.15.0-1049-aws"/' /etc/default/grub
```

3. Reboot your system by typing "sudo reboot".
4. Install the correct Lustre module: .









```
sudo apt-get install -y lustre-client-modules-$(uname -r)
```

### Remediation:

### References:

1. <https://docs.aws.amazon.com/fsx/latest/LustreGuide/install-lustre-client.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                     | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v8               | <b><u>13.11 Tune Security Event Alerting Thresholds</u></b><br>Tune security event alerting thresholds monthly, or more frequently.                                                                                                                                                                                                         |                                                                                     |                                                                                     |  |
| v7               | <b><u>5.2 Maintain Secure Images</u></b><br>Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.                              |                                                                                     |  |  |
| v7               | <b><u>13.4 Only Allow Access to Authorized Cloud Storage or Email Providers</u></b><br>Only allow access to authorized cloud storage or email providers.                                                                                                                                                                                    |                                                                                     |  |  |

## 4.7 Ensure mounting FSx cache (Manual)

### Profile Applicability:

- Level 2

### Description:

Mounting the FSx cache is a crucial step to optimize data retrieval and system performance. This process involves connecting the FSx file system to your compute instances, allowing them to access cached data efficiently. Properly mounting the FSx cache ensures low-latency access to frequently used data, enhances overall application performance, and leverages the full capabilities of the AWS FSx service. This setup is essential for achieving high performance and efficient data processing in your AWS environment.

### Rationale:

By connecting the FSx file system to your compute instances, you enable low-latency access to frequently used data, significantly improving application performance. This setup leverages the full capabilities of the AWS FSx service, ensuring efficient data processing and resource utilization in your AWS environment. Properly mounting the FSx cache is essential for achieving high performance and operational efficiency.

### Audit:

To mount your cache, follow the next steps:

1. Make a directory for the mount point with the following command:

```
sudo mkdir -p /mnt
```

2. Mount the Amazon file cache to the directory that you just created. Use the following command and replace these names:
  - Replace `cache_dns_name` with the actual file cache's Domain Name System (DNS) name
  - Replace `mountname` with the cache's mount name, which you can get by running the `describe-file-caches` AWS CLI command or `DescribeFileCaches` API operation

```
sudo mount -t lustre -o relatime,flock cache_dns_name@tcp:/mountname /mnt
```









Note: Make sure your EC2 instance is in the same VPC as your cache.

If done correctly, the path of your folder will show up in the `/mnt` folder.

You can also use the `df` command to see the DNS and mount point is attached to your file system:

## Remediation:

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v7               | <b>3.3 <u>Protect Dedicated Assessment Accounts</u></b><br>Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.                                                                                                                                           |      |  |  |
| v7               | <b>5.2 <u>Maintain Secure Images</u></b><br>Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.                                                                                         |      |  |  |
| v7               | <b>6.4 <u>Ensure adequate storage for logs</u></b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                                                                                                                                                                                                                                                      |      |  |  |
| v7               | <b>8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u></b><br>Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. |      |  |  |

## 4.8 Ensure exporting cache to S3 (Manual)

### Profile Applicability:

- Level 2

### Description:

The S3 bucket we created earlier will store the files generated at this mount point.

### Rationale:

The rationale behind using the S3 bucket to store files generated at the mount point is to ensure scalable, durable, and cost-effective storage for your data. By exporting files to S3, you benefit from its high availability and robust data management features, which enhances data security and accessibility. This approach also optimizes storage resource utilization and simplifies data backup and retrieval processes.

### Audit:

We can export the files that were created to the S3 bucket using the following steps:

1. Create a file on the FSx mount point:
2. Run the command:

```
sudo touch efx.txt
```

3. Now run the command:

```
sudo lsm hsm_archive efx.txt
```

4. Now check your S3 bucket that was created earlier.

### Remediation:

### References:

1. <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/backups-exporting.html>

## 4.9 Ensure cleaning up FSx Resources (Manual)

### Profile Applicability:

- Level 2

### Description:

Cleaning up FSx resources involves removing unused or unnecessary FSx file systems and associated components to optimize costs and maintain a secure cloud environment. This includes deleting redundant file systems, snapshots, and mount targets, while ensuring all data is backed up or migrated. Regular cleanup prevents resource sprawl, reduces expenses, and maintains the overall health and performance of your AWS infrastructure.

### Rationale:

The rationale for cleaning up FSx resources is to optimize costs and ensure a secure and efficient cloud environment. By removing unused or unnecessary file systems, snapshots, and mount targets, you prevent resource sprawl and reduce unnecessary expenses. Regular cleanup also helps maintain the overall health and performance of your AWS infrastructure, ensuring it remains organized and secure.

### Audit:

To clean the FSx resources -










1. Terminate the EC2 instance.
2. Delete Fsx cache - On the actions drop down, select delete cache.
3. Verify that you want to delete the service.
4. Select **Delete**. It will take some time to delete the cache.
5. Delete the S3 Bucket  
Before you can delete the bucket you must first empty the bucket. Check the radio box and select **Empty**  
Select the bucket that you want to delete and select **Delete** in the S3 console.

### Remediation:

### References:

1. <https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/getting-started-step3.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                   | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.8 <u>Document Data Flows</u></b><br>Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.                                                      |                                                                                     |  |  |
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.                                                                                                                                                                                           |  |  |  |
| v7               | <b>7.8 <u>Implement DMARC and Enable Receiver-Side Verification</u></b><br>To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards. |                                                                                     |  |  |
| v7               | <b>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></b><br>Only allow access to authorized cloud storage or email providers.                                                                                                                                                                                                                  |                                                                                     |  |  |



## **5 Simple Storage Service (S3)**

Object storage built to retrieve any amount of data from anywhere.

## 5.1 Amazon Simple Storage Service (Manual)

### Profile Applicability:

- Level 2

### Description:

Amazon Simple Storage Service (Amazon S3) is an object storage service that provides industry-leading scalability, data availability, security, and performance. It allows customers of all sizes and industries to store and protect any amount of data for virtually any use case, including data lakes, cloud-native applications, and mobile apps. With cost-effective storage classes and intuitive management features, you can optimize costs, organize data, and configure precise access controls to meet your specific business, organizational, and compliance requirements.

### Rationale:

By utilizing S3, businesses of all sizes can efficiently store and protect large amounts of data, ensuring it is accessible when needed. The service's cost-effective storage classes and user-friendly management features help optimize costs and streamline data organization. Additionally, S3's fine-tuned access controls allow organizations to meet specific business, organizational, and compliance requirements, enhancing overall data management and security.

### Audit:

How Amazon S3 works:

1. To store your data in Amazon S3, you first create a bucket and specify a bucket name and AWS Region. Then, you upload your data to that bucket as objects in Amazon S3. Each object has a key (or key name), which is the unique identifier for the object within the bucket.
2. S3 provides features that you can configure to support your specific use case. For example, you can use S3 Versioning to keep multiple versions of an object in the same bucket, which allows you to restore objects that are accidentally deleted or overwritten. Buckets and the objects in them are private and can be accessed only if you explicitly grant access permissions. You can use bucket policies, AWS Identity and Access Management (IAM) policies, access control lists (ACLs), and S3 Access Points to












manage  
access.

**Remediation:**

**References:**

1. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html>

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.                                                                                                                                                                                                                                       |    |    |    |
| v7               | <b>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></b><br>Only allow access to authorized cloud storage or email providers.                                                                                                                                                                                                                                                              |                                                                                       |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 5.2 Ensure direct data addition to S3 (Manual)

### Profile Applicability:

- Level 2

### Description:

Your bucket name must be unique and not already in use on AWS. Click on your bucket name, and in the right corner, you will find an option to upload data directly to your S3 bucket. You can choose the file option to upload individual files, images, or even entire folders.

### Rationale:

Accessing the upload option within your bucket simplifies the process of adding data, making it easy to manage and organize your files. This streamlined approach allows for efficient data storage, retrieval, and management within the AWS S3 environment, enhancing overall operational efficiency.

### Audit:

Access Point in S3 Bucket:

Access points are named network endpoints that are attached to buckets which simplify managing data access at scale in S3. To see if any of the access points attached to this bucket grant public or cross-account access, go to IAM Access Analyzer for S3.












1. Enter a name for the access point. The name must be unique within the AWS account and Region.
2. Choose the VPC (Virtual Private Cloud) and subnet where you want the access point to be accessible. This determines the network traffic routing for the access point.
3. Optionally, you can configure additional settings such as permissions, bucket policy, and endpoint policy for the access point.
4. Review the settings, and click on "Create access point" to create the access point

### Remediation:

### References:

1. <https://docs.aws.amazon.com/redshift/latest/dg/tutorial-loading-data-upload-files.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.                                                                                                                                                                                                                                       |  |  |  |
| v7               | <b>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></b><br>Only allow access to authorized cloud storage or email providers.                                                                                                                                                                                                                                                              |                                                                                     |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 5.3 Ensure Storage Classes are Configured (Manual)

### Profile Applicability:

- Level 2

### Description:

Amazon S3 offers various storage classes to optimize cost and performance based on data access patterns and retention needs. Standard Storage is for frequently accessed data, while Standard-IA and One Zone-IA are for infrequent access, with the latter offering cost savings by storing in a single Availability Zone. Intelligent-Tiering automatically moves data between access tiers based on usage, and Glacier and Glacier Deep Archive provide low-cost options for long-term archival storage with varying retrieval times. Each class balances availability, durability, performance, and cost, enabling a tailored storage strategy to meet specific requirements.

### Rationale:

This approach ensures frequently accessed data is readily available, while infrequently accessed data is stored cost-effectively, balancing availability, durability, and cost.









### Audit:

### Remediation:

### References:

1. <https://aws.amazon.com/s3/storage-classes/>

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                   | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                            |  |  |  |
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.                                                                                                                                                                                           |  |  |  |
| v7               | <b>7.8 <u>Implement DMARC and Enable Receiver-Side Verification</u></b><br>To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards. |                                                                                       |  |  |

| Controls Version | Control                                                                                                                                                      | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v7               | <p>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></p> <p>Only allow access to authorized cloud storage or email providers.</p> |      | ●    | ●    |

## 6 Elastic Disaster Recovery (EDR)

AWS Elastic Disaster Recovery is an AWS service that allows you to create and maintain backups of your workloads on AWS, specifically your servers. AWS Elastic Disaster Recovery is essential to providing high resilience to your AWS workloads. It works by establishing and maintaining backups in AWS regions of your choosing, to ensure that your backups are safe, durable, and highly available if something goes wrong in the availability zone or region that your AWS server resides.



## 6.1 Ensure Elastic Disaster Recovery is Configured (Manual)

### Profile Applicability:

- Level 2

### Description:

AWS Elastic Disaster Recovery is a service that enables you to create and maintain backups of your workloads on AWS, particularly your servers. This service is crucial for ensuring high resilience for your AWS workloads. It operates by establishing and maintaining backups in selected AWS regions, guaranteeing that your data is safe, durable, and highly available in the event of issues in the primary availability zone or region where your AWS server is located.

### Rationale:

AWS Elastic Disaster Recovery is crucial for establishing high resiliency in the cloud, synonymous with effective disaster recovery. High resiliency measures your organization's ability to respond to and recover from disasters impacting IT infrastructure. Achieving high resiliency minimizes downtime and long-term costs associated with outages, while low resiliency can result in prolonged downtime, potential data loss, and even permanent infrastructure damage.

### Audit:

#### 1. Review Disaster Recovery Plans:

- Log in to the AWS Management Console.
- Navigate to the AWS Elastic Disaster Recovery service.
- Locate and open the disaster recovery plans.
- Verify that the plans are current and comprehensive, covering all critical workloads.
- Ensure that the plans specify clear recovery time objectives (RTO) and recovery point objectives (RPO).

#### 2. Check Backup Configurations:

- In the AWS Elastic Disaster Recovery dashboard, review the list of protected servers and workloads.
- Confirm that backups are enabled for all critical servers and workloads.
- Verify the backup schedule and frequency to ensure they meet organizational requirements.
- Check that backups are being stored in the correct AWS regions as specified in the disaster recovery plan.

#### 3. Test Recovery Procedures:

- Identify a non-production environment to conduct recovery drills.
- Initiate a simulated disaster scenario to test the recovery procedures.
- Execute the recovery process for each critical workload.
- Measure and document the time taken to recover each workload.
- Compare the measured recovery times against the RTO and RPO.

- Identify and document any issues or delays encountered during the recovery process.
- 4. **Monitor Backup Integrity:**
  - Open the AWS CloudWatch console.
  - Set up CloudWatch Alarms to monitor the status of backups.
  - Configure alerts for any failed or incomplete backups.
  - Regularly review the CloudWatch logs to verify that backups are successfully completed and stored.
- 5. **Evaluate Backup Storage and Security:**
  - Access the AWS S3 or Glacier console, depending on where backups are stored.
  - Verify that all backup data is encrypted in transit and at rest.
  - Check the storage settings to confirm that data is being stored in secure, durable storage solutions.
  - Review the access control policies to ensure that only authorized personnel have access to backup data.
- 6. **Ensure Compliance with Policies and Regulations:**
  - Review organizational and regulatory compliance requirements relevant to disaster recovery.
  - Ensure that the disaster recovery practices and configurations comply with these requirements.
  - Document the compliance efforts, including any specific steps taken to meet industry standards and regulations.
  - Prepare reports or evidence of compliance for any upcoming audits or assessments.

## **Remediation:**

1. **Update Disaster Recovery Plans:**
  - **Action:** Log in to the AWS Management Console.
  - **Procedure:**
    - Navigate to the AWS Elastic Disaster Recovery service.
    - Locate and review the current disaster recovery plans.
    - Update the plans to ensure they are comprehensive and cover all critical workloads.
    - Ensure that the plans specify clear recovery time objectives (RTO) and recovery point objectives (RPO).
    - Save and document the updated plans.
2. **Correct Backup Configurations:**
  - **Action:** Verify and adjust backup settings.
  - **Procedure:**

- In the AWS Elastic Disaster Recovery dashboard, review the list of protected servers and workloads.
- Enable backups for any critical servers and workloads that are not currently being backed up.
- Adjust the backup schedule and frequency to meet organizational requirements.
- Ensure backups are stored in the correct AWS regions as specified in the disaster recovery plan.

### 3. Conduct Recovery Procedure Drills:

○

**Action:** Test and refine recovery procedures.

○

#### **Procedure:**

- Identify a non-production environment to conduct recovery drills.
- Simulate a disaster scenario to test the recovery procedures.
- Execute the recovery process for each critical workload.
- Measure and document the time taken to recover each workload.
- Compare the measured recovery times against the RTO and RPO.
- Identify and address any issues or delays encountered during the recovery process.
- Update the recovery procedures based on the findings from the drill.

### 4. Ensure Backup Integrity:

○

**Action:** Monitor and verify the integrity of backups.

○

#### **Procedure:**

- Open the AWS CloudWatch console.
- Set up CloudWatch Alarms to monitor the status of backups.
- Configure alerts for any failed or incomplete backups.
- Regularly review CloudWatch logs to verify that backups are successfully completed and stored.
- Resolve any issues identified in the logs, such as incomplete or failed backups.

### 5. Enhance Backup Storage and Security:

○

**Action:** Improve the storage and security of backup data.

○

#### **Procedure:**

- Access the AWS S3 or Glacier console, depending on where backups are stored.
- Ensure all backup data is encrypted in transit and at rest.
- Adjust storage settings to confirm that data is being stored in secure, durable storage solutions.
- Review and update access control policies to ensure only authorized personnel can access backup data.

- Implement any additional security measures necessary to protect the backup data.







#### 6. Ensure Compliance with Policies and Regulations:

- **Action:** Align disaster recovery practices with compliance requirements.

#### ○ **Procedure:**

- Review organizational and regulatory compliance requirements relevant to disaster recovery.
- Adjust disaster recovery practices and configurations to ensure compliance with these requirements.
- Document the compliance efforts, including specific steps taken to meet industry standards and regulations.
- Prepare and maintain reports or evidence of compliance for any upcoming audits or assessments.

#### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                           | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>11.2 <u>Perform Automated Backups</u></b><br>Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.                                            |  |  |  |
| v7               | <b>10.2 <u>Perform Complete System Backups</u></b><br>Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system. |  |  |  |

## 6.2 Ensure AWS Disaster Recovery Configuration (Manual)

### Profile Applicability:

- Level 2

### Description:

It's important to understand how the network on EDR works. This isn't a simple service to configure, but it works with multiple work loads over the network. You can connect your on-premises or third-party cloud service to AWS EDR over the network. Below are the descriptions of the AWS network architecture:

1. Your local network inside the data center or cloud a. Connect an AWS Replication Agent to each of your resources.
2. AWS Cloud Architecture a. Choose the AWS Region that you want to house your disaster recovery instances. b. Create AWS API Endpoints for EC2, Disaster Recovery, and S3. c. Upon creation of Disaster Recovery endpoints, two subnets will be created in your VPC i. Staging Area Subnets: Replication servers with EBS volumes attached to each disk on the replication servers. ii. Recovery Subnets: Recovery EC2 instances attached to EBS volumes/ d. Connect local network over TCP port 443 to EDR and S3 e. Connect local replication agent to AWS replication servers over TCP port 1500 f. Connectivity out of staging area: Connect staging area on AWS to EDR over TCP port 443 g. Allow connection to S3 over TCP 443 h. Allow connectivity to EC2 over TCP 443 to connect to API Endpoint

### Rationale:




### Audit:








### Remediation:

### References:

1. <https://aws.amazon.com/disaster-recovery/>

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                     | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>11.4 Establish and Maintain an Isolated Instance of Recovery Data</b><br>Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services. |  |  |  |

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>13.3 <u>Deploy a Network Intrusion Detection Solution</u></b><br>Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service. |                                                                                     |  |  |
| v7               | <b>10.4 <u>Ensure Protection of Backups</u></b><br>Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.                                           |  |  |  |
| v7               | <b>13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u></b><br>Only allow access to authorized cloud storage or email providers.                                                                                                                                              |                                                                                     |  |  |

## 6.3 Ensure functionality of Endpoint Detection and Response (EDR) (Manual)

### Profile Applicability:

- Level 2

### Description:

Establish and maintain an effective Endpoint Detection and Response (EDR) system to proactively monitor, detect, and respond to security threats on endpoints such as computers, mobile devices, and servers. This involves deploying EDR software that continuously collects data from endpoints, analyzes this data for signs of malicious activity, and provides real-time alerts and detailed incident reports. Regularly test and update the EDR system to ensure it can accurately identify and mitigate advanced threats, including zero-day exploits and sophisticated malware, ensuring comprehensive protection and swift response to potential security incidents.

### Rationale:

Ensuring the functionality of Endpoint Detection and Response (EDR) systems is essential for early detection and swift response to security threats on endpoints. These systems continuously monitor and analyze endpoint data, providing real-time alerts and detailed incident reports to identify and mitigate potential threats. Regular testing and updates of the EDR system ensure it remains effective against advanced threats, maintaining comprehensive protection for the organization's assets.









### Audit:

1. Preparing the Environment for EDR - Before getting started with EDR, you must prepare the environment that you want to back up.
2. Preparing the Source Server - Allow direct access to Elastic Disaster Recovery and Amazon S3 AWS service API endpoints through HTTPS protocol (TCP port 443). Direct outbound TCP port 1500 from the source server to the staging area subnet, which contains the replication servers.
3. Preparing the Staging Area Subnet - Allow Direct access to EDR, S3, and EC2 through HTTPS protocol (TCP port 443)  
Direct inbound TCP port 1500 for replication traffic
4. Accessing the AWS Elastic Disaster Recovery Console -
  - Search for "AWS Elastic Disaster Recovery" in the AWS Console.
  - Select "Elastic Disaster Recovery"
5. Configuring the Replication Settings Template - Select **Configure and Initialize** in the AWS Elastic Disaster Recovery screen. You will be navigated to setup your replication settings template. This will create a staging area in a subnet of your choice and a replication server instance types. The default replication server instance type will be a t3 micro EC2 instance. This is good for normal workloads with small I/O operations.

6. Next, configure EBS encryption and volume types. This will depend on your workload requirements.
7. To encrypt EBS volumes, leave the setting as “default.” If you wish to make a custom encryption setting, you will need to create an AWS KMS key.
8. Configure the security group to your specific needs. Remember what ports need to be opened on inbound / outbound traffic that was specified in previous steps: You can choose how you want your data routed and if you want to throttle network traffic to reserve bandwidth. To keep your data as secure as possible, it’s recommended to get set up with a VPN or AWS direct connect, so your backups are not traveling over the public internet.  
Point in time policy defines the snapshot retention time. Because Elastic Disaster Recovery service uses incremental backups, it’s not necessary to keep old copies of backups.  
Now, you’re ready to launch this template.

## Remediation:

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>13.2 <u>Deploy a Host-Based Intrusion Detection Solution</u></b><br>Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.                                                                                                                     |      |  |  |
| v8               | <b>13.3 <u>Deploy a Network Intrusion Detection Solution</u></b><br>Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service. |      |  |  |
| v7               | <b>8.6 <u>Centralize Anti-malware Logging</u></b><br>Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.                                                                                                               |      |  |  |
| v7               | <b>12.6 <u>Deploy Network-based IDS Sensor</u></b><br>Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.                                                   |      |  |  |



## 6.4 Ensure configuration of replication settings (Manual)

### Profile Applicability:

- Level 2

### Description:

Set up and maintain the replication settings to ensure accurate and efficient data duplication across systems. Proper configuration includes specifying source and target locations, defining replication schedules, and setting bandwidth limits to optimize performance. Regularly review and update these settings to accommodate changes in data volume and network conditions, ensuring data integrity and availability during replication processes.

### Rationale:













Proper configuration of replication settings is essential to ensure data consistency and availability across systems. Accurate replication schedules and bandwidth management optimize performance and prevent network congestion. Regular reviews and updates of these settings help adapt to changes in data volume and network conditions, maintaining efficient and reliable data replication processes.

### Audit:

1. Select “Configure and Initialize” in the AWS Elastic Disaster Recovery screen. You will be navigated to setup your replication settings template. This will create a staging area in a subnet of your choice and a replication server instance types. The default replication server instance type will be a t3 micro EC2 instance. This is good for normal workloads with small I/O operations.
2. Next, configure EBS encryption and volume types. This will depend on your workload requirements. To encrypt EBS volumes, leave the setting as “default.” If you wish to make a custom encryption setting, you will need to create an AWS KMS key.
3. Configure the security group to your specific needs. Remember what ports need to be opened on inbound / outbound traffic that was specified in previous steps:
  - Configure Additional Replication settings.
  - You can choose how you want your data routed and if you want to throttle network traffic to reserve bandwidth.  
To keep your data as secure as possible, it’s recommended to get set up with a VPN or AWS direct connect, so your backups are not traveling over the public internet.
  - Point in time policy defines the snapshot retention time. Because Elastic Disaster Recovery service uses incremental backups, it’s not necessary to keep old copies of backups.  
Now, you’re ready to launch this template.

## Remediation:

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                            | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>11.2 Perform Automated Backups</u></b><br>Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.                                                                                             |  |  |  |
| v8               | <b><u>11.4 Establish and Maintain an Isolated Instance of Recovery Data</u></b><br>Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services. |  |  |  |
| v7               | <b><u>10.4 Ensure Protection of Backups</u></b><br>Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.                        |  |  |  |
| v7               | <b><u>10.5 Ensure Backups Have At least One Non-Continuously Addressable Destination</u></b><br>Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.                                                  |  |  |  |

## 6.5 Ensure proper IAM configuration for AWS Elastic Disaster Recovery (Manual)

### Profile Applicability:

- Level 2

### Description:

Set up and maintain Identity and Access Management (IAM) roles and policies specifically for AWS Elastic Disaster Recovery. This includes defining least-privilege access for users and services, creating roles for automated processes, and enforcing multi-factor authentication (MFA) for added security. Regularly review and update IAM policies to adapt to changes in the organization and to maintain compliance with security best practices, ensuring that only authorized personnel and services can access and manage disaster recovery resources.

### Rationale:

Proper IAM configuration for AWS Elastic Disaster Recovery ensures that only authorized users and services have access to critical recovery functions, reducing the risk of unauthorized access and potential security breaches. Implementing least-privilege access and MFA enhances security by limiting permissions and adding an extra layer of authentication. Regular reviews and updates of IAM policies help maintain security compliance and adapt to organizational changes, ensuring continuous protection of disaster recovery resources.

### Audit:

To create DRS Agent User, follow following steps:

1. Navigate to the AWS IAM Console - <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home>.
2. Create new user. This user will only be able to access the Elastic disaster recovery agent installation resource. Accordingly, name the user "DSRuser".
3. Allow Programmatic access: This allows the user to access resources programmatically with a secure key rather than having to enter a password.
4. elect "attach policies directly" and search for "AWSElasticDisasterRecoveryAgentInstallationPolicy".
5. Create user.

To create Failback Agent User, Follow the steps above with these two modifications:

1. Name the user "FailbackAgentuser".
2. Apply the "AWSElasticDisasterRecoveryFailbackInstallationPolicy".

**Remediation:****Default Value:**

Configure IAM Credentials for AWS Elastic Disaster Recovery.

**References:**

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

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                              | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>6.7 Centralize Access Control</b><br>Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.                                                                                                                                                                                                                                                                            |      | ●    | ●    |
| v8               | <b>6.8 Define and Maintain Role-Based Access Control</b><br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. |      |      | ●    |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.                       | ●    | ●    | ●    |
| v7               | <b>14.7 Enforce Access Control to Data through Automated Tools</b><br>Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.                                                                                                                                                                                                                      |      |      | ●    |

## 6.6 Ensure installation of the AWS Replication Agent (Manual)

### Profile Applicability:

- Level 2

### Description:

Set up and verify the installation of the AWS Replication Agent on all relevant systems to facilitate efficient and reliable data replication. This process includes downloading the agent, configuring it according to best practices, and ensuring it is correctly integrated with your AWS environment. Regularly check the agent's performance and update it as needed to maintain optimal functionality and data integrity during replication processes.

### Rationale:

Installing the AWS Replication Agent is crucial for enabling efficient and reliable data replication, ensuring that critical data is accurately duplicated across systems. Proper configuration and integration with your AWS environment optimize the agent's performance, enhancing data availability and disaster recovery capabilities. Regular checks and updates of the replication agent help maintain its effectiveness, ensuring data integrity and minimizing the risk of replication failures.

### Audit:

1. On the source servers page, from Actions, choose add servers to obtain the agent installer link.
2. On your source server (in our case, the EC2 instance that was already created) download the appropriate agent installer for your operating system.
  - For Linux instance on US-East-1. Substitute your region in the {Region} brackets of this command:

```
wget -O ./aws-replication-installer-init https://aws-elastic-disaster-recovery-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/aws-replication-installer-init
```

3. Run following command:

```
chmod +x aws-replication-installer-init; sudo ./aws-replication-installer-init
```

4. Type in your region. Region is case sensitive: if you're in us-east-1, make sure you type "us-east-1".
5. If you're using SSH, you will be prompted with your activation ID and secret activation key. Make sure you have those accessible for the IAM user you're

using. You can generate a new key from the IAM dashboard if you forgot to save your key.

6. Select “Enter” to replicate all servers.
7. All servers should replicate.
8. Make sure your OS is up to date. If you run into an error replicating your devices, view the documentation on troubleshooting the AWS replication installation here: <https://docs.aws.amazon.com/mgn/latest/ug/installation-requirements.html>.
9. If install runs successfully, the source server will appear in your Elastic Disaster Recovery Console dashboard on the “source servers” page. This will signify the beginning of the replication process.

## Remediation:

## References:

1. <https://docs.aws.amazon.com/mgn/latest/ug/agent-installation.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                              | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>6.7 Centralize Access Control</b><br>Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.                                                                                                                                                                                                                                                                            |      | ●    | ●    |
| v8               | <b>6.8 Define and Maintain Role-Based Access Control</b><br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. |      |      | ●    |
| v7               | <b>3.4 Deploy Automated Operating System Patch Management Tools</b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.                                                                                                                                                                                            | ●    | ●    | ●    |
| v7               | <b>5.4 Deploy System Configuration Management Tools</b><br>Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.                                                                                                                                                                                                             |      | ●    | ●    |

## 6.7 *Ensure proper configuration of the Launch Settings (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Set up and verify the launch settings to ensure systems and applications start correctly and securely. This includes defining startup parameters, specifying required resources, and configuring security settings to prevent unauthorized changes. Regularly review and update these settings to align with best practices and organizational requirements, ensuring optimal performance and security at launch.

### **Rationale:**

Proper configuration of launch settings is crucial for ensuring that systems and applications start securely and perform optimally. Defining startup parameters and resource requirements prevents potential issues and enhances efficiency. Regular reviews and updates to these settings help maintain alignment with best practices and evolving organizational needs, thereby strengthening security and operational reliability from the moment of launch.










### **Audit:**

The settings can be changed after instances have been launched, but a new instance must be launched for new launch settings to take effect.

1. Select launch settings on the source server page
2. Configure launch settings
  - On the launch settings page, next to general launch, select “edit”
3. Configure EC2 launch template
  - Enable auto assign public IP and change the instance type to a t2.medium
4. Set version to default in the console
5. Set the default version that was just created to default version
6. Return to the dashboard and confirm your configurations are correct.

## Remediation:

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b><u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u></b><br>Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.                                                                                                                                                    |  |    |    |
| v8               | <b><u>16.7 Use Standard Hardening Configuration Templates for Application Infrastructure</u></b><br>Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening. |                                                                                     |    |    |
| v7               | <b><u>5.2 Maintain Secure Images</u></b><br>Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.                                                                                                                                               |                                                                                     |    |    |
| v7               | <b><u>5.4 Deploy System Configuration Management Tools</u></b><br>Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.                                                                                                                                                                                                                              |                                                                                     |  |  |



## 6.8 Ensure execution of a recovery drill (Manual)

### Profile Applicability:

- Level 2

### Description:

To ensure your organization is prepared for a disaster, it's crucial to verify that your disaster recovery services function as expected. Your IT team should conduct regular recovery drills on your AWS Elastic Recovery Instance to confirm everything operates smoothly and according to plan.

### Rationale:

Regular recovery drills are essential to verify the functionality of your disaster recovery services and ensure your organization is well-prepared for any disruptions. By conducting these drills on your AWS Elastic Recovery Instance, you can identify and address potential issues before they impact operations. This proactive approach enhances the reliability and effectiveness of your disaster recovery plan, providing confidence that your systems can recover swiftly and efficiently in the event of a disaster.

### Audit:

Steps to perform a recovery drill:

1. Navigate to source servers tab in AWS Elastic Disaster Recovery Dashboard.
2. Make sure that all servers you launch show as "Ready" under "status," report as "healthy" in the data replication status column, and that pending actions show as "initiate drill".
3. Select "initiate drill" under the orange dropdown menu. Make sure that you don't initiate a real recovery job.
4. Choose a recovery point. Normally, it makes sense to choose the most recent recovery point, but you can also choose a recovery point from earlier.
5. Select the orange "initiate drill" to initiate the recovery drill.
6. To complete the recovery drill, clean up your resources by deleting the recovery instance by selecting actions and "terminate recovery instances".

### Remediation:

### References:

1. <https://docs.aws.amazon.com/drs/latest/userguide/failback-preparing.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                             | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>11.5 <u>Test Data Recovery</u></b><br>Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.                                                                                                                                                                                                                                                                                          |      | ●    | ●    |
| v8               | <b>17.7 <u>Conduct Routine Incident Response Exercises</u></b><br>Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.                                                |      | ●    | ●    |
| v7               | <b>10.3 <u>Test Data on Backup Media</u></b><br>Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.                                                                                                                                                                                                                                      |      | ●    | ●    |
| v7               | <b>19.7 <u>Conduct Periodic Incident Scenario Sessions for Personnel</u></b><br>Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them. |      | ●    | ●    |

## 6.9 Ensure Continuous Disaster Recovery Operations (Manual)

### Profile Applicability:

- Level 2

### Description:

Maintain ongoing disaster recovery operations to ensure that systems and data can be swiftly restored in the event of a disruption. This involves regularly updating and testing recovery plans, monitoring replication processes, and verifying the integrity and accessibility of backups. Continuously evaluate and improve disaster recovery strategies to adapt to evolving threats and organizational changes, ensuring resilience and minimal downtime during incidents.

### Rationale:

Maintaining continuous disaster recovery operations is essential for ensuring that systems and data can be quickly and effectively restored following a disruption. Regular updates and tests of recovery plans, along with constant monitoring of replication processes, help verify the integrity and availability of backups. This proactive approach allows organizations to adapt to evolving threats and changes, ensuring resilience and minimizing downtime during incidents, which ultimately protects business continuity and reduces potential losses.

### Audit:

#### 1. Review Disaster Recovery Plan:

- Verify that a comprehensive disaster recovery (DR) plan exists and is regularly updated.
- Ensure the DR plan includes detailed procedures for data backup, system recovery, and failover processes.
- Check for documentation of roles and responsibilities during a disaster event.

#### 2. Check Backup and Replication Settings:

- Confirm that AWS Backup is configured correctly for all critical systems and data.
- Review the settings for Amazon RDS, EBS snapshots, S3 versioning, and other AWS services to ensure backups are automated and scheduled appropriately.
- Ensure that replication settings are configured to replicate data across multiple AWS regions for added redundancy.

#### 3. Test Recovery Procedures:

- Verify that regular recovery drills are conducted to test the DR plan's effectiveness.
- Check the logs and reports from these drills to ensure that any issues identified are addressed promptly.











- Ensure that the most recent recovery drill results are documented and reviewed by relevant stakeholders.
- 4. **Monitor and Log Review:**
  - Ensure CloudWatch logs and alarms are set up to monitor backup and replication processes.
  - Review CloudTrail logs to verify that DR-related actions are being logged and monitored.
  - Check for alerts and notifications related to backup failures, replication issues, or any anomalies in the DR processes.
- 5. **Evaluate Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO):**
  - Verify that the DR plan specifies RTO and RPO for all critical systems and data.
  - Ensure that actual recovery times and points from recent drills meet or exceed the defined objectives.
- 6. **Review Access Controls:**
  - Check IAM policies to ensure that only authorized personnel have access to manage and initiate disaster recovery operations.
  - Verify that multi-factor authentication (MFA) is enabled for accounts with access to DR resources.
- 7. **Assess Security and Compliance:**
  - Ensure that data encryption is enabled for all backups and replicated data.
  - Verify compliance with industry standards and regulations (e.g., GDPR, HIPAA) concerning data protection and disaster recovery.
- 8. **Continuous Improvement:**
  - Review post-mortem reports from actual incidents and recovery drills to identify areas for improvement.
  - Ensure that feedback loops are in place for continuous enhancement of the DR plan and procedures.
  - Confirm that lessons learned from incidents and drills are incorporated into the DR plan.
- 9. **Regular Updates and Communication:**
  - Ensure the DR plan is reviewed and updated at least annually or whenever significant changes occur in the IT environment.
  - Verify that all relevant personnel are trained on the DR procedures and aware of their roles.
  - Check that regular communication channels are established for DR updates and training sessions.

## **Remediation:**

## **References:**

1. <https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                             | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>11.1 <u>Establish and Maintain a Data Recovery Process</u></b><br>Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.                                                              |  |  |  |
| v8               | <b>11.5 <u>Test Data Recovery</u></b><br>Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.                                                                                                                                                                                                                                                                                          |                                                                                     |  |  |
| v7               | <b>10.2 <u>Perform Complete System Backups</u></b><br>Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.                                                                                                                                                                                                   |  |  |  |
| v7               | <b>19.7 <u>Conduct Periodic Incident Scenario Sessions for Personnel</u></b><br>Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them. |                                                                                     |  |  |

## 6.10 Ensure execution of a Disaster Recovery Failover (Manual)

### Profile Applicability:

- Level 2

### Description:

Execute a comprehensive disaster recovery failover to transition operations from the primary system to a backup system during disruptions. This process includes ensuring all critical data and applications are accurately replicated to the backup site for seamless operational continuity. Regularly test and document the failover process to identify and resolve any issues, maintaining readiness to minimize downtime and data loss during real disasters.

### Rationale:

Executing a comprehensive disaster recovery failover is essential to ensure operational continuity during disruptions. Accurate replication of critical data and applications to the backup site guarantees that business operations can continue seamlessly. Regular testing and documentation of the failover process help identify and resolve potential issues, maintaining a state of readiness and minimizing downtime and data loss in actual disaster scenarios.

### Audit:

Follow the steps where we learned how to conduct a recovery drill with the below modifications:

1. Choose the server that you want to recover and failover. On the initiate recovery job menu, choose “initiate recovery.”
2. Choose a point in time to recover from backup.
3. Choose initiate recovery to create a recovery job.

Note: You can use the job details to monitor the progress and status of the recovery job.

After the recovery job has completed, the last recovery result of your source server will report “successful.”

The EC2 instance ID of the launched recovery instance will also be listed in the source server overview.

You can test if the recovery instance is functioning by testing the EC2 instance that is in the source server overview.

### Remediation:












### Default Value:

Implement a disaster recovery failover.

## References:

1. <https://docs.aws.amazon.com/drs/latest/userguide/failback-preparing-failover.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                            | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>11.4 <u>Establish and Maintain an Isolated Instance of Recovery Data</u></b><br>Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services. |    |    |    |
| v8               | <b>11.5 <u>Test Data Recovery</u></b><br>Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.                                                                                                                                         |                                                                                       |    |    |
| v7               | <b>10.4 <u>Ensure Protection of Backups</u></b><br>Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.                        |    |    |    |
| v7               | <b>10.5 <u>Ensure Backups Have At least One Non-Continuously Addressable Destination</u></b><br>Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.                                                  |  |  |  |

## 6.11 Ensure execution of a failback (Manual)

### Profile Applicability:

- Level 2

### Description:

This method involves transitioning operations back from the backup or recovery system to the primary system after the resolution of a disruption or disaster. You can execute a failback either to the original server, ensuring continuity and restoring the previous state, or to a new server, which might be necessary if the original server is compromised or no longer functional. The failback process ensures that all updated data and configurations are transferred back, maintaining the integrity and functionality of the primary system.

### Rationale:

A failback is crucial for restoring normal operations after a disaster recovery scenario. Transitioning operations back to the primary system ensures continuity and leverages the original environment's configurations and settings. This process can be directed either to the original server, maintaining the existing infrastructure, or to a new server if the original is compromised. Ensuring all data and configurations are accurately transferred back preserves system integrity and functionality, reducing downtime and allowing the organization to resume normal operations efficiently.

### Impact:

Failback Prerequisites:

- The volumes on the server you are failing back to are the same size or larger than the recovery instance if failing back to a new server.
- The failback client has the proper permissions to access both Elastic Disaster Recovery and S3 services on TCP port 1500 inbound and TCP port 443 outbound to communicate with the failback client.
- A public IP is added to the recovery instance.

### Audit:

Performing the failback:

1. Download the failback client ISO
2. Attach the ISO to your original server and boot up the server.
  - The failback client will prompt for the IAM access key and secret key generated when making the user with the permission to access the failback. It will also ask for the region of the recovery instance. Remember: regions are case sensitive. If you're in US east 1, type "us-east-1."
  - If you are failing back to the original server, the failback client will automatically detect the recovery instance and map the data volumes for replication.
  - If you are failing back to a new server, you may need to manually specify from a list of available recovery instances and map the data volumes.











- The failback client will verify that the chosen recovery instance has connectivity to the Elastic Disaster Recovery service.
- The replication software will be downloaded to the failback client and then configured. Connectivity will be made between the failback client and the replication agent on the recovery instance to begin data replication.
- 3. Return to the elastic disaster recovery console and recovery instances to see the current state of replication. Failing back to the original server will show “rescan” in the console, while failing back to a new instance will perform an “initial sync.”
- 4. After the data replication is completed, you will be able to perform the failback.
  - Check the state of the recovery instance to ensure that it’s ready to complete a failback.
  - Select your recovery instance, then choose failback for the chosen recovery instance(s).
  - Choose failback again to complete a failback for the chosen recovery instance(s). During the failback process, the failback client will prepare your source server for normal operation. After it has completed successfully, the failback client will return “failback completed successfully” in the console.
- 5. Reboot the server and return to normal operations.
- 6. Clean up failback job; terminate recovery job by following the steps outlined above when we ran a drill.

#### Remediation:

#### References:

1. <https://docs.aws.amazon.com/drs/latest/userguide/failback-performing-main.html>

#### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>11.1 <u>Establish and Maintain a Data Recovery Process</u></b><br>Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |
| v8               | <b>11.5 <u>Test Data Recovery</u></b><br>Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.                                                                                                                                                                                                                             |                                                                                       |  |  |
| v7               | <b>10.2 <u>Perform Complete System Backups</u></b><br>Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.                                                                                                                                      |  |  |  |

| Controls Version | Control                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v7               | <b>10.3 <u>Test Data on Backup Media</u></b><br>Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working. |      | ●    | ●    |

## 6.12 Ensure CloudWatch Metrics for AWS EDR (Manual)

### Profile Applicability:

- Level 2

### Description:

Set up and monitor AWS CloudWatch metrics for Endpoint Detection and Response (EDR) to track and analyze the performance and security of your AWS environment. This involves configuring CloudWatch to collect detailed logs and metrics on EDR activities, such as threat detections, response actions, and system health. Regularly review these metrics to identify trends, anomalies, and potential security issues, enabling proactive management and timely responses to ensure the effectiveness of your EDR solution.

### Rationale:

Implementing AWS CloudWatch metrics for Endpoint Detection and Response (EDR) is essential for maintaining a secure and efficient AWS environment. By collecting detailed logs and metrics on EDR activities, you gain valuable insights into the performance and health of your security measures. Regular review of these metrics allows for the early detection of trends, anomalies, and potential security threats, enabling proactive management and swift responses to maintain the integrity and effectiveness of your EDR solution. This continuous monitoring ensures that your security posture remains robust and adaptive to evolving threats.

### Audit:

1. **Sign in to the AWS Management Console:**
  - Open the [AWS Management Console](#) and sign in with your credentials.
2. **Navigate to CloudWatch:**
  - In the AWS Management Console, navigate to the **CloudWatch** service.
3. **Create a CloudWatch Log Group:**
  - Select **Logs** from the navigation pane.
  - Click on **Create log group**.
  - Enter a name for the log group and click **Create**.
4. **Configure AWS EDR to Send Logs to CloudWatch:**
  - Go to the AWS EDR (Elastic Disaster Recovery) console.
  - In the AWS EDR console, configure your settings to send logs and metrics to the CloudWatch log group you created.
5. **Set Up CloudWatch Alarms:**
  - In the CloudWatch console, select **Alarms** from the navigation pane.
  - Click on **Create Alarm**.
  - Select the metric you want to monitor from the list of AWS EDR metrics.
  - Configure the conditions for the alarm (e.g., threshold, period, etc.).
  - Set the actions to take when the alarm state is triggered (e.g., send a notification).

- Review and create the alarm.
- 6. **Create CloudWatch Dashboards:**
  - In the CloudWatch console, select **Dashboards** from the navigation pane.
  - Click on **Create dashboard**.
  - Enter a name for your dashboard and click **Create**.
  - Add widgets to the dashboard by selecting the relevant AWS EDR metrics.
  - Customize the widgets to display the data in a meaningful way (e.g., graphs, numbers).
- 7. **Enable CloudWatch Logs Insights:**
  - In the CloudWatch console, select **Logs Insights** from the navigation pane.
  - Choose the log group you created for AWS EDR.
  - Use CloudWatch Logs Insights queries to analyze the log data and extract meaningful insights.
- 8. **Set Up CloudWatch Events:**
  - In the CloudWatch console, select **Events** from the navigation pane.
  - Click on **Create rule**.
  - Define the event source and the specific events you want to capture (e.g., changes in EDR status).
  - Set the target for the event (e.g., send a notification, invoke a Lambda function).
  - Configure the rule and click **Create rule**.

## Remediation:

## References:

1. <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html>

## 6.13 Ensure working of EDR (Manual)

### Profile Applicability:

- Level 2

### Description:

### Rationale:

### Audit:

1. Preparing the Environment for EDR - Before getting started with EDR, you must prepare the environment that you want to back up.
2. Preparing the Source Server - Allow direct access to Elastic Disaster Recovery and Amazon S3 AWS service API endpoints through HTTPS protocol (TCP port 443). Direct outbound TCP port 1500 from the source server to the staging area subnet, which contains the replication servers.
3. Preparing the Staging Area Subnet - Allow Direct access to EDR, S3, and EC2 through HTTPS protocol (TCP port 443)  
Direct inbound TCP port 1500 for replication traffic
4. Accessing the AWS Elastic Disaster Recovery Console -
  - Search for “AWS Elastic Disaster Recovery” in the AWS Console.
  - Select “Elastic Disaster Recovery”
5. Configuring the Replication Settings Template - Select **Configure and Initialize** in the AWS Elastic Disaster Recovery screen. You will be navigated to setup your replication settings template. This will create a staging area in a subnet of your choice and a replication server instance types. The default replication server instance type will be a t3 micro EC2 instance. This is good for normal workloads with small I/O operations.
6. Next, configure EBS encryption and volume types. This will depend on your workload requirements.
7. To encrypt EBS volumes, leave the setting as “default.” If you wish to make a custom encryption setting, you will need to create an AWS KMS key.
8. Configure the security group to your specific needs. Remember what ports need to be opened on inbound / outbound traffic that was specified in previous steps: You can choose how you want your data routed and if you want to throttle network traffic to reserve bandwidth. To keep your data as secure as possible, it's recommended to get set up with a VPN or AWS direct connect, so your backups are not traveling over the public internet. Point in time policy defines the snapshot retention time. Because Elastic Disaster Recovery service uses incremental backups, it's not necessary to keep old copies of backups.  
Now, you're ready to launch this template.

## Remediation:

# Appendix: Summary Table

| CIS Benchmark Recommendation |                                                            | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                            | Yes                      | No                       |
| <b>1</b>                     | <b>Introduction</b>                                        |                          |                          |
| 1.1                          | AWS Storage Backups (Manual)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2                          | Ensure securing AWS Backups (Manual)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3                          | Ensure to create backup template and name (Manual)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4                          | Ensure to create AWS IAM Policies (Manual)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5                          | Ensure to create IAM roles for Backup (Manual)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6                          | Ensure AWS Backup with Service Linked Roles (Manual)       | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2</b>                     | <b>Elastic Block Store (EBS)</b>                           |                          |                          |
| 2.1                          | Ensure creating EC2 instance with EBS (Manual)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2                          | Ensure configuring Security Groups (Manual)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3                          | Ensure the proper configuration of EBS storage (Manual)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4                          | Ensure the creation of a new volume (Manual)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5                          | Ensure creating snapshots of EBS volumes (Manual)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6                          | Ensure Proper IAM Configuration for EC2 Instances (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.7                          | Ensure creating IAM User (Manual)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.8                          | Ensure the Creation of IAM Groups (Manual)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.9                          | Ensure Granular Policy Creation (Manual)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.10                         | Ensure Resource Access via Tag-based Policies (Manual)     | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                   | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                   | Yes                      | No                       |
| 2.11                         | Ensure Secure Password Policy Implementation (Manual)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.12                         | Ensure Monitoring EC2 and EBS with CloudWatch (Manual)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.13                         | Ensure creating an SNS subscription (Manual)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>3</b>                     | <b>Elastic File System (EFS)</b>                                  |                          |                          |
| 3.1                          | EFS (Manual)                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2                          | Ensure Implementation of EFS (Manual)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3                          | Ensure EFS and VPC Integration (Manual)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4                          | Ensure controlling Network access to EFS Services (Manual)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5                          | Ensure using Security Groups for VPC (Manual)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6                          | Ensure Secure Ports (Manual)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7                          | Ensure File-Level Access Control with Mount Targets (Manual)      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.8                          | Ensure managing mount target security groups (Manual)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.9                          | Ensure using VPC endpoints - EFS (Manual)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10                         | Ensure managing AWS EFS access points (Manual)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11                         | Ensure accessing Points and IAM Policies (Manual)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.12                         | Ensure configuring IAM for AWS Elastic Disaster Recovery (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4</b>                     | <b>FSx</b>                                                        |                          |                          |
| 4.1                          | FSX (AWS Elastic File Cache) (Manual)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2                          | Amazon Elastic File Cache (Manual)                                | <input type="checkbox"/> | <input type="checkbox"/> |



| CIS Benchmark Recommendation |                                                                            | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                            | Yes                      | No                       |
| 4.3                          | Ensure the creation of an FSX Bucket (Manual)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4                          | Ensure the creation of Elastic File Cache (Manual)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5                          | Ensure installation and configuration of Lustre Client (Manual)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6                          | Ensure EC2 Kernel compatibility with Lustre (Manual)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.7                          | Ensure mounting FSx cache (Manual)                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.8                          | Ensure exporting cache to S3 (Manual)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.9                          | Ensure cleaning up FSx Resources (Manual)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5</b>                     | <b>Simple Storage Service (S3)</b>                                         |                          |                          |
| 5.1                          | Amazon Simple Storage Service (Manual)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2                          | Ensure direct data addition to S3 (Manual)                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3                          | Ensure Storage Classes are Configured (Manual)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6</b>                     | <b>Elastic Disaster Recovery (EDR)</b>                                     |                          |                          |
| 6.1                          | Ensure Elastic Disaster Recovery is Configured (Manual)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2                          | Ensure AWS Disaster Recovery Configuration (Manual)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3                          | Ensure functionality of Endpoint Detection and Response (EDR) (Manual)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4                          | Ensure configuration of replication settings (Manual)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5                          | Ensure proper IAM configuration for AWS Elastic Disaster Recovery (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6                          | Ensure installation of the AWS Replication Agent (Manual)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.7                          | Ensure proper configuration of the Launch Settings (Manual)                | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                           | Set Correctly            |                          |
|------------------------------|-----------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                           | Yes                      | No                       |
| 6.8                          | Ensure execution of a recovery drill (Manual)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.9                          | Ensure Continuous Disaster Recovery Operations (Manual)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.10                         | Ensure execution of a Disaster Recovery Failover (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.11                         | Ensure execution of a failback (Manual)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.12                         | Ensure CloudWatch Metrics for AWS EDR (Manual)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.13                         | Ensure working of EDR (Manual)                            | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v7 IG 1 Mapped Recommendations

| Recommendation |                                                                   | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                   | Yes                      | No                       |
| 2.5            | Ensure creating snapshots of EBS volumes                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6            | Ensure Proper IAM Configuration for EC2 Instances                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.11           | Ensure Secure Password Policy Implementation                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.12           | Ensure Monitoring EC2 and EBS with CloudWatch                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1            | EFS                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure EFS and VPC Integration                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure File-Level Access Control with Mount Targets               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.8            | Ensure managing mount target security groups                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.9            | Ensure using VPC endpoints - EFS                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10           | Ensure managing AWS EFS access points                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11           | Ensure accessing Points and IAM Policies                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.12           | Ensure configuring IAM for AWS Elastic Disaster Recovery          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | FSX (AWS Elastic File Cache)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Amazon Elastic File Cache                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure the creation of an FSX Bucket                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Amazon Simple Storage Service                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2            | Ensure direct data addition to S3                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1            | Ensure Elastic Disaster Recovery is Configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2            | Ensure AWS Disaster Recovery Configuration                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4            | Ensure configuration of replication settings                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5            | Ensure proper IAM configuration for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6            | Ensure installation of the AWS Replication Agent                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.9            | Ensure Continuous Disaster Recovery Operations                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.10           | Ensure execution of a Disaster Recovery Failover                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.11           | Ensure execution of a failback                                    | <input type="checkbox"/> | <input type="checkbox"/> |



# Appendix: CIS Controls v7 IG 2 Mapped Recommendations

| Recommendation |                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------|--------------------------|--------------------------|
|                |                                                          | Yes                      | No                       |
| 2.2            | Ensure configuring Security Groups                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3            | Ensure the proper configuration of EBS storage           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4            | Ensure the creation of a new volume                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5            | Ensure creating snapshots of EBS volumes                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6            | Ensure Proper IAM Configuration for EC2 Instances        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.7            | Ensure creating IAM User                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.8            | Ensure the Creation of IAM Groups                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.9            | Ensure Granular Policy Creation                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.11           | Ensure Secure Password Policy Implementation             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.12           | Ensure Monitoring EC2 and EBS with CloudWatch            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1            | EFS                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure Implementation of EFS                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure EFS and VPC Integration                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure controlling Network access to EFS Services        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure using Security Groups for VPC                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6            | Ensure Secure Ports                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure File-Level Access Control with Mount Targets      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.8            | Ensure managing mount target security groups             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.9            | Ensure using VPC endpoints - EFS                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10           | Ensure managing AWS EFS access points                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11           | Ensure accessing Points and IAM Policies                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.12           | Ensure configuring IAM for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | FSX (AWS Elastic File Cache)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Amazon Elastic File Cache                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure the creation of an FSX Bucket                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure installation and configuration of Lustre Client   | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                   | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                   | Yes                      | No                       |
| 4.6            | Ensure EC2 Kernel compatibility with Lustre                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.7            | Ensure mounting FSx cache                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.9            | Ensure cleaning up FSx Resources                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Amazon Simple Storage Service                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2            | Ensure direct data addition to S3                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3            | Ensure Storage Classes are Configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1            | Ensure Elastic Disaster Recovery is Configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2            | Ensure AWS Disaster Recovery Configuration                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3            | Ensure functionality of Endpoint Detection and Response (EDR)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4            | Ensure configuration of replication settings                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5            | Ensure proper IAM configuration for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6            | Ensure installation of the AWS Replication Agent                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.7            | Ensure proper configuration of the Launch Settings                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.8            | Ensure execution of a recovery drill                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.9            | Ensure Continuous Disaster Recovery Operations                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.10           | Ensure execution of a Disaster Recovery Failover                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.11           | Ensure execution of a failback                                    | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v7 IG 3 Mapped Recommendations

| Recommendation |                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------|--------------------------|--------------------------|
|                |                                                          | Yes                      | No                       |
| 2.1            | Ensure creating EC2 instance with EBS                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2            | Ensure configuring Security Groups                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3            | Ensure the proper configuration of EBS storage           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4            | Ensure the creation of a new volume                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5            | Ensure creating snapshots of EBS volumes                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6            | Ensure Proper IAM Configuration for EC2 Instances        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.7            | Ensure creating IAM User                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.8            | Ensure the Creation of IAM Groups                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.9            | Ensure Granular Policy Creation                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.10           | Ensure Resource Access via Tag-based Policies            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.11           | Ensure Secure Password Policy Implementation             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.12           | Ensure Monitoring EC2 and EBS with CloudWatch            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1            | EFS                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure Implementation of EFS                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure EFS and VPC Integration                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure controlling Network access to EFS Services        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure using Security Groups for VPC                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6            | Ensure Secure Ports                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure File-Level Access Control with Mount Targets      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.8            | Ensure managing mount target security groups             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.9            | Ensure using VPC endpoints - EFS                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10           | Ensure managing AWS EFS access points                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11           | Ensure accessing Points and IAM Policies                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.12           | Ensure configuring IAM for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | FSX (AWS Elastic File Cache)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Amazon Elastic File Cache                                | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                   | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                   | Yes                      | No                       |
| 4.3            | Ensure the creation of an FSX Bucket                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure installation and configuration of Lustre Client            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure EC2 Kernel compatibility with Lustre                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.7            | Ensure mounting FSx cache                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.9            | Ensure cleaning up FSx Resources                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Amazon Simple Storage Service                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2            | Ensure direct data addition to S3                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3            | Ensure Storage Classes are Configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1            | Ensure Elastic Disaster Recovery is Configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2            | Ensure AWS Disaster Recovery Configuration                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3            | Ensure functionality of Endpoint Detection and Response (EDR)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4            | Ensure configuration of replication settings                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5            | Ensure proper IAM configuration for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6            | Ensure installation of the AWS Replication Agent                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.7            | Ensure proper configuration of the Launch Settings                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.8            | Ensure execution of a recovery drill                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.9            | Ensure Continuous Disaster Recovery Operations                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.10           | Ensure execution of a Disaster Recovery Failover                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.11           | Ensure execution of a failback                                    | <input type="checkbox"/> | <input type="checkbox"/> |



# Appendix: CIS Controls v7 Unmapped Recommendations

| Recommendation |                                             | Set Correctly            |                          |
|----------------|---------------------------------------------|--------------------------|--------------------------|
|                |                                             | Yes                      | No                       |
| 1.1            | AWS Storage Backups                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2            | Ensure securing AWS Backups                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3            | Ensure to create backup template and name   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4            | Ensure to create AWS IAM Policies           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5            | Ensure to create IAM roles for Backup       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6            | Ensure AWS Backup with Service Linked Roles | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.13           | Ensure creating an SNS subscription         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4            | Ensure the creation of Elastic File Cache   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.8            | Ensure exporting cache to S3                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.12           | Ensure CloudWatch Metrics for AWS EDR       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.13           | Ensure working of EDR                       | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 IG 1 Mapped Recommendations

| Recommendation |                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------|--------------------------|--------------------------|
|                |                                                          | Yes                      | No                       |
| 2.3            | Ensure the proper configuration of EBS storage           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4            | Ensure the creation of a new volume                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5            | Ensure creating snapshots of EBS volumes                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.7            | Ensure creating IAM User                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.12           | Ensure Monitoring EC2 and EBS with CloudWatch            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1            | EFS                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure Implementation of EFS                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure controlling Network access to EFS Services        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6            | Ensure Secure Ports                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure File-Level Access Control with Mount Targets      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.8            | Ensure managing mount target security groups             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.9            | Ensure using VPC endpoints - EFS                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10           | Ensure managing AWS EFS access points                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11           | Ensure accessing Points and IAM Policies                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.12           | Ensure configuring IAM for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | FSX (AWS Elastic File Cache)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Amazon Elastic File Cache                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure the creation of an FSX Bucket                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure installation and configuration of Lustre Client   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure EC2 Kernel compatibility with Lustre              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.9            | Ensure cleaning up FSx Resources                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Amazon Simple Storage Service                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2            | Ensure direct data addition to S3                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3            | Ensure Storage Classes are Configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1            | Ensure Elastic Disaster Recovery is Configured           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2            | Ensure AWS Disaster Recovery Configuration               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------|--------------------------|--------------------------|
|                |                                                    | Yes                      | No                       |
| 6.4            | Ensure configuration of replication settings       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.7            | Ensure proper configuration of the Launch Settings | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.9            | Ensure Continuous Disaster Recovery Operations     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.10           | Ensure execution of a Disaster Recovery Failover   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.11           | Ensure execution of a failback                     | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 IG 2 Mapped Recommendations

| Recommendation |                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------|--------------------------|--------------------------|
|                |                                                          | Yes                      | No                       |
| 2.1            | Ensure creating EC2 instance with EBS                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2            | Ensure configuring Security Groups                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3            | Ensure the proper configuration of EBS storage           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4            | Ensure the creation of a new volume                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5            | Ensure creating snapshots of EBS volumes                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.7            | Ensure creating IAM User                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.10           | Ensure Resource Access via Tag-based Policies            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.11           | Ensure Secure Password Policy Implementation             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.12           | Ensure Monitoring EC2 and EBS with CloudWatch            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1            | EFS                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure Implementation of EFS                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure EFS and VPC Integration                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure controlling Network access to EFS Services        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure using Security Groups for VPC                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6            | Ensure Secure Ports                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure File-Level Access Control with Mount Targets      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.8            | Ensure managing mount target security groups             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.9            | Ensure using VPC endpoints - EFS                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10           | Ensure managing AWS EFS access points                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11           | Ensure accessing Points and IAM Policies                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.12           | Ensure configuring IAM for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | FSX (AWS Elastic File Cache)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Amazon Elastic File Cache                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure the creation of an FSX Bucket                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure installation and configuration of Lustre Client   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure EC2 Kernel compatibility with Lustre              | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                   | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                   | Yes                      | No                       |
| 4.9            | Ensure cleaning up FSx Resources                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Amazon Simple Storage Service                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2            | Ensure direct data addition to S3                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3            | Ensure Storage Classes are Configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1            | Ensure Elastic Disaster Recovery is Configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2            | Ensure AWS Disaster Recovery Configuration                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3            | Ensure functionality of Endpoint Detection and Response (EDR)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4            | Ensure configuration of replication settings                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5            | Ensure proper IAM configuration for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6            | Ensure installation of the AWS Replication Agent                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.7            | Ensure proper configuration of the Launch Settings                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.8            | Ensure execution of a recovery drill                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.9            | Ensure Continuous Disaster Recovery Operations                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.10           | Ensure execution of a Disaster Recovery Failover                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.11           | Ensure execution of a failback                                    | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 IG 3 Mapped Recommendations

| Recommendation |                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------|--------------------------|--------------------------|
|                |                                                          | Yes                      | No                       |
| 2.1            | Ensure creating EC2 instance with EBS                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2            | Ensure configuring Security Groups                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3            | Ensure the proper configuration of EBS storage           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4            | Ensure the creation of a new volume                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5            | Ensure creating snapshots of EBS volumes                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6            | Ensure Proper IAM Configuration for EC2 Instances        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.7            | Ensure creating IAM User                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.8            | Ensure the Creation of IAM Groups                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.9            | Ensure Granular Policy Creation                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.10           | Ensure Resource Access via Tag-based Policies            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.11           | Ensure Secure Password Policy Implementation             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.12           | Ensure Monitoring EC2 and EBS with CloudWatch            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1            | EFS                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure Implementation of EFS                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure EFS and VPC Integration                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure controlling Network access to EFS Services        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure using Security Groups for VPC                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6            | Ensure Secure Ports                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure File-Level Access Control with Mount Targets      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.8            | Ensure managing mount target security groups             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.9            | Ensure using VPC endpoints - EFS                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10           | Ensure managing AWS EFS access points                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11           | Ensure accessing Points and IAM Policies                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.12           | Ensure configuring IAM for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | FSX (AWS Elastic File Cache)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Amazon Elastic File Cache                                | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                   | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                   | Yes                      | No                       |
| 4.3            | Ensure the creation of an FSX Bucket                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure installation and configuration of Lustre Client            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure EC2 Kernel compatibility with Lustre                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.9            | Ensure cleaning up FSx Resources                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Amazon Simple Storage Service                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2            | Ensure direct data addition to S3                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3            | Ensure Storage Classes are Configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1            | Ensure Elastic Disaster Recovery is Configured                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2            | Ensure AWS Disaster Recovery Configuration                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3            | Ensure functionality of Endpoint Detection and Response (EDR)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4            | Ensure configuration of replication settings                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5            | Ensure proper IAM configuration for AWS Elastic Disaster Recovery | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6            | Ensure installation of the AWS Replication Agent                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.7            | Ensure proper configuration of the Launch Settings                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.8            | Ensure execution of a recovery drill                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.9            | Ensure Continuous Disaster Recovery Operations                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.10           | Ensure execution of a Disaster Recovery Failover                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.11           | Ensure execution of a failback                                    | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 Unmapped Recommendations

| Recommendation |                                             | Set Correctly            |                          |
|----------------|---------------------------------------------|--------------------------|--------------------------|
|                |                                             | Yes                      | No                       |
| 1.1            | AWS Storage Backups                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2            | Ensure securing AWS Backups                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3            | Ensure to create backup template and name   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4            | Ensure to create AWS IAM Policies           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5            | Ensure to create IAM roles for Backup       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6            | Ensure AWS Backup with Service Linked Roles | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.13           | Ensure creating an SNS subscription         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4            | Ensure the creation of Elastic File Cache   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.7            | Ensure mounting FSx cache                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.8            | Ensure exporting cache to S3                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.12           | Ensure CloudWatch Metrics for AWS EDR       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.13           | Ensure working of EDR                       | <input type="checkbox"/> | <input type="checkbox"/> |



# Appendix: Change History

| Date       | Version | Changes for this version |
|------------|---------|--------------------------|
| 07/03/2024 | V1.0.0  | Document Created         |