CIS Benchmarks

CIS Alibaba Cloud Foundation Benchmark

v1.0.0 - 12-11-2020

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

Overview

This security configuration benchmark covers foundational elements of Alibaba Cloud. The recommendations detailed here provides prescriptive guidance for configuring security options for a subset of Alibaba Cloud services with an emphasis on foundational, testable, and architecture agnostic settings. Specific Alibaba Cloud Services in scope for this document include:

- Elastic Compute Service (ECS)
- Virtual Private Cloud (VPC)
- Object Storage Service (OSS)
- Relational Database Service (RDS)
- Container Service for Kubernetes (ACS)
- Key Management Service (KMS)
- Resource Access Management (RAM)
- ActionTrail
- Security Center

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 Alibaba Cloud services.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. 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
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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 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 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 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
Matthew Woods
Ning Zhang
Lina Tian
YUE GUAN
Wangfeng Hu
Raymond Huang
Laiqiang Ding
Guangrui Wu
Ruj Wang
Pengfei Chen
Wudong Chen
Jun Ma
Hongbin Xu
Zhengzhong Zhou
Lin Kuan-Yeh
Dahu Kuang
Zixuan Zhang
Tim Coakley

Recommendations

1 Identity and Access Management

This section contains recommendations for configuring identity and access management related options.

1.1 Avoid the use of the "root" account (Manual)

Profile Applicability:

- Level 1

Description:

An Alibaba Cloud account can be viewed as a “root” account. The "root" account has full control permissions to all cloud products and resources under such account. It is highly recommended that the use of this account should be avoided.

Rationale:

The "root" account is the owner of the resources under an Alibaba Cloud account. This account pays for and has full control permissions to resources. Minimizing the use of such account and adopting the principle of least privilege for access management can reduce the risk of accidental or unauthorized changes and disclosure of highly privileged credentials.

Audit:

You can enable ActionTrail for your account, and create a trail to deliver all action logs to Alibaba Cloud Log Service. Then, you can enable an alarm to discover the usage of "root" account and receive notifications on those conditions.
Implement the **Ensure a log metric filter and alarm exist for usage of "root" account** recommendation in the Logging and Monitoring section to receive notifications of root account usage.
Note: There are a few conditions under which the use of the root account is required, such as requesting account security report or configuring multi-factor authentication (MFA) for the root account.

Remediation:

All users should operate resources at the RAM user level and follow the principle of least privilege. Follow the remediation instructions of the **Ensure RAM policies are attached only to groups or roles** recommendation. For more information about RAM user, see terms of RAM user.

References:

1. https://www.alibabacloud.com/help/doc-detail/102600.htm

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

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.

1.2 Ensure no root account access key exists (Manual)

Profile Applicability:

- Level 1

Description:

Access keys provide programmatic access to a given Alibaba Cloud account. It is recommended that all access keys associated with the root account be removed.

Rationale:

An Alibaba Cloud account can be viewed as a "root" account. The root account has the highest privilege of an Alibaba Cloud account. Removing access keys associated with the root account limits the opportunity that the account can be compromised.

Impact:

Programs that already use root account access keys may stop working if you disable or delete the access keys without replacing them with other RAM user access keys in your program.

Audit:

Perform the following to determine if the root account has access keys:
Through the management console:

1. Logon to RAM console by using your Alibaba Cloud account (root account).
2. In the **left-side navigation** pane, click **Overview**.
3. In the **Security Check** section, make sure that **No AK for Root Account** is marked as **Finished**.

Remediation:

Perform the following to delete or disable active root access keys:
Through the management console

1. Logon to RAM console by using your Alibaba Cloud account (root account).
2. Move the pointer over the account icon in the upper-right corner and click **AccessKey**.
3. Click **Continue** to manage **AccessKey**.
4. On the **Security Management** page, find the target access keys and perform the following operations:
    - Click **Disable** to disable the target access keys temporarily.

- Click **Delete** to delete the target access keys permanently.

Default Value:

By default, no access key is created for the root account.

References:

1. https://www.alibabacloud.com/help/doc-detail/102600.htm

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

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.

1.3 Ensure MFA is enabled for the "root" account (Manual)

Profile Applicability:

- Level 1

Description:

With MFA enabled, anytime the “root” account logs on to Alibaba Cloud, it will be prompted for username and password followed by an authentication code from the virtual MFA device. It is recommended that MFA be enabled for the “root” user.

Rationale:

It is important to prevent “root” account from being compromised. Enabling MFA requires the “root” account holder to provide additional information on top of username and password.

When MFA is enabled, an attacker faces at least two different authentication mechanisms. The additional security makes it harder for an attacker to gain access to protected resources or data.

Audit:

Perform the following to determine if an MFA device is enabled for the “root” account:
Through the management console:

1. Logon to RAM console by using your Alibaba Cloud account (root account).
2. In the **left-side navigation** pane, click **Overview**.
3. In the **Security Check** section, make sure that **Enable MFA for Root Account** is marked as **Finished**.

Remediation:

Perform the following to enable MFA for “root” account
Through the management console:

1. Logon to RAM console by using your Alibaba Cloud account (root account).
2. Move the pointer over the account icon in the upper-right corner and click **Security Settings**.
3. In the **Account Protection** section, Click Edit.
4. On the displayed page, select a scenario and select **TOTP**.
5. Click **Submit**.
6. On the displayed page, click **Verify now**.

7. Enter the **verification code** and click **Submit**.
8. Download and install a mobile application that supports **TOTP MFA**, such as Google Authenticator, on your mobile phone.
   Note: If you already installed Google Authenticator, click **Next**.
   - For iOS: Install Google Authenticator from the App Store.
   - For Android: Install Google Authenticator from the Google Play Store.
     Note: You need to install a QR code scanner from the Google Play Store for Google Authenticator to identify QR codes.
9. After you install Google Authenticator, go back to the **Identity Verification** page and click **Next**.
10. Open Google Authenticator and tap **BEGIN SETUP**.
    - Tap Scan barcode and scan the QR code on the **Identity Verification** page.
    - Tap **Manual** entry, enter the username and key, and then tap the **check mark** (√) icon.
      Note: You can obtain the username and key by moving the pointer over **Scan failed** on the **Identity Verification** page.
11. On the **Identity Verification** page, enter the 6-digit verification code obtained from Google Authenticator and click **Next**.
    Note: The verification code is refreshed at an interval of 30 seconds.

References:

1. http://tools.ietf.org/html/rfc6238
2. https://www.alibabacloud.com/help/doc-detail/28635.htm

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

1.4 Ensure that multi-factor authentication is enabled for all RAM users that have a console password (Automated)

Profile Applicability:

- Level 1

Description:

Multi-Factor Authentication (MFA) adds an extra layer of protection on top of a username and password. With MFA enabled, when a user logs on to Alibaba Cloud, they will be prompted for their user name and password followed by an authentication code from their virtual MFA device. It is recommended that MFA be enabled for all users that have a console password.

Rationale:

MFA requires users to verify their identities by entering two authentication factors. When MFA is enabled, an attacker faces at least two different authentication mechanisms. The additional security makes it harder for an attacker to gain access to protected resources or data.

Audit:

Perform the following to determine if an MFA device is enabled for all RAM users having a console password:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of each RAM user.
4. In the **Console Logon Management** section, if **Console Access** is set to **Enabled**, make sure that **Required to Enable MFA** is set to **Yes**.

Through the CLI
Run the following command to determine if an MFA device is enabled for a RAM user:

```
aliyun ram GetUserMFAInfo --UserName <ram_user>
```

Note: If an error is reported, no MFA device is enabled for the RAM user.

Remediation:

Perform the following to determine if an MFA device is enabled for all RAM users having a console password:

Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of each RAM user.
4. In the **Console Logon Management** section, click **Modify Logon Settings**.
5. Select **Enabled for Console Password Logon**, and **Required for Enable MFA**.
   Note: After you select **Enabled for Console Password Logon**, and **Required for Enable MFA** when modifying the logon settings of a
   RAM user, the user can go to step 7 when logging on to the RAM console for the first time.
6. In the MFA Device section, click **Enable the device**.
7. Download and install Google Authenticator on your mobile phone.
   - For iOS: Install Google Authenticator from the App Store.
   - For Android: Install Google Authenticator from the Google Play Store.
     Note: You need to install a QR code scanner from the Google Play Store for Google Authenticator to identify QR codes.
8. Open Google Authenticator and tap **BEGIN SETUP**.
   - Tap Scan barcode and scan the QR code displayed on the **Scan the code** tab in the console.
   - Tap **Manual entry**, enter the username and key, and then tap the **check mark** (√) icon.
     Note: You can obtain the username and key from the **Retrieval manually enter information** tab in the console.
9. On the **Scan the code** tab, enter the two consecutive security codes obtained from Google Authenticator and click **Enable**.
   Note: The security code is refreshed at an interval of 30 seconds.
   For more information, see Enable an MFA device for a RAM user.

References:

1. http://tools.ietf.org/html/rfc6238
2. https://www.alibabacloud.com/help/doc-detail/93720.htm
3. https://www.alibabacloud.com/help/doc-detail/119555.htm

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication

Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

1.5 Ensure users not logged on for 90 days or longer are disabled for console logon (Automated)

Profile Applicability:

- Level 1

Description:

Alibaba Cloud RAM users can logon to Alibaba Cloud console by using their user name and password. If a user has not logged on for 90 days or longer, it is recommended to disable the console access of the user.

Rationale:

Disabling users from having unnecessary logon privileges will reduce the opportunity that an abandoned user or a user with compromised password to be used.

Impact:

RAM users who still need to log on to the management console or other Alibaba Cloud sites may encounter logon failure.

Audit:

Perform the following to determine if a user has not logged on for 90 days or longer:
Through the management console:

1. Logon RAM console.
2. Choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of each RAM user.
4. In the **Console Logon Management** section, check the latest logon time of each user in the **Last Console Logon** field.
5. Make sure that each user does not have a last console logon time dated earlier than 90 days ago.

Remediation:

Perform the following to disable console logon for a user:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Users**.

3. In the **User Logon Name/Display Name** column, click the username of the target RAM user.
4. In the **Console Logon Management** section, click **Modify Logon Settings**.
5. In the **Console Password Logon** section, select **Disabled**.
6. Click **OK**.

Through the CLI

```
aliyun ram DeleteLoginProfile --UserName <ram_user>
```

CIS Controls:

Version 7

16.9 Disable Dormant Accounts
Automatically disable dormant accounts after a set period of inactivity.

1.6 Ensure access keys are rotated every 90 days or less (Automated)

Profile Applicability:

- Level 1

Description:

An access key consists of an access key ID and a secret, which are used to sign programmatic requests that you make to Alibaba Cloud. RAM users need their own access keys to make programmatic calls to Alibaba Cloud from the Alibaba Cloud SDKs, CLIs, or direct HTTP/HTTPS calls using the APIs for individual Alibaba Cloud services. It is recommended that all access keys be regularly rotated.

Rationale:

Access keys might be compromised by leaving them in codes, configuration files, on premise and cloud storages, and then stolen by attackers. Rotating access keys will reduce the window of opportunity that a compromised access key to be used.

Audit:

Perform the following to determine if access keys are rotated within 90 days:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Groups**.
3. In the **User Logon Name/Display Name** column, click the username of each RAM user.
4. In the **User AccessKeys** section, check the **date** and **time** that an access key was created.
5. Make sure that no user has an access key created earlier than 90 days ago.

Through the CLI:
Run the following command to obtain a list of access keys of a RAM user, and then determine if the access keys are rotated within 90 days according to the CreateDate parameter:

```
aliyun ram ListAccessKeys --UserName <ram_user>
```

Note: In the output, if the **AccessKey** parameter is empty, no access key exists.

Remediation:

Perform the following to disable and delete access keys:

Through the management console:

1. Logon to RAM console.
2. In the left-side navigation pane, click **Users** under **Identities**.
3. In the **User Logon Name/Display Name** column, click the username of the target RAM user.
4. In the **User AccessKeys** section, click **Create AccessKey**.
5. Click **OK** to create a new AccessKy pair for rotation.
6. Update all applications and systems to use the new AccessKey pair.
7. Disable the original AccessKey pair by following below steps:
   a) Log on to RAM console.
   b) In the left-side navigation pane, click **Users** under **Identities**.
   c) On the **Users** page, click username of the target RAM user in the **User Logon Name/Display Name** column.
   d) In the **User AccessKeys** section, find the target AccessKey pair and click **Disable**.
8. Confirm that your applications and systems are working.
9. Delete the original AccessKey pair by following below steps:
   a) Log on to RAM console.
   b) In the left-side navigation pane, click Users under Identities.
   c) In the **User Logon Name/Display Name** column, click the username of the target RAM user.
   d) In the **User AccessKeys** section, find the target access keys and Click **Delete**.
   e) In the dialog box that appears, select I am aware of the risk and confirm the deletion.
10. Click **OK**.

Through the CLI:

- Run the following command to delete an access key:

```
aliyun ram DeleteAccessKey --UserAccessKeyId <access_key_ID> --UserName
<ram_user >
```

- Run the following command to disable an active access key:

```
aliyun ram UpdateAccessKey --UserAccessKeyId <access_key_ID> --Status
Inactive --UserName <ram_user>
```

- Run the following command to delete an access key:

```
aliyun ram DeleteAccessKey --UserAccessKeyId <access_key_ID> --UserName
<ram_user >
```

Your programs that use access keys may stop working if you rotate the access keys without replacing them in your program prior to the rotation.

References:

1. https://www.alibabacloud.com/help/doc-detail/116806.htm
2. https://www.alibabacloud.com/help/doc-detail/116808.htm
3. https://www.alibabacloud.com/help/doc-detail/152682.htm
4. https://www.alibabacloud.com/help/doc-detail/116401.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.7 Ensure RAM password policy requires at least one uppercase letter (Automated)

Profile Applicability:

- Level 1

Description:

RAM password policies can be used to ensure password complexity. It is recommended that the password policy require at least one uppercase letter.

Rationale:

Enhancing complexity of a password policy increases account resiliency against brute force logon attempts.

Audit:

Perform the following to ensure the password policy is configured as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, make sure that the value of **Required Elements in Password** contains **Upper-Case Letter**.

Through the CLI:

```
aliyun ram GetPasswordPolicy
```

In the output, make sure that the **RequireUppercaseCharacters** parameter is set to **true**.

Remediation:

Perform the following to set the password policy as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, click **Edit Password Rule**.
4. In the **Required Elements in Password** section, select **UpperCase Letter**.
5. Click **OK**.

Through the CLI:

```
aliyun ram SetPasswordPolicy --RequireUppercaseCharacters true
```

Default Value:

The default password policy does not enforce any element in a password.

References:

1. https://www.alibabacloud.com/help/doc-detail/116413.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.8 Ensure RAM password policy requires at least one lowercase letter (Automated)

Profile Applicability:

- Level 1

Description:

RAM password policies can be used to ensure password complexity. It is recommended that the password policy require at least one lowercase letter.

Rationale:

Enhancing complexity of a password policy increases account resiliency against brute force logon attempts.

Audit:

Perform the following to ensure the password policy is configured as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, make sure that the value of **Required Elements** in Password contains **Lowercase Letters**.

Through the CLI:

```
aliyun ram GetPasswordPolicy
```

In the output, make sure that the **RequireLowercaseCharacters** parameter is set to **true**.

Remediation:

Perform the following to set the password policy:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, click **Edit Password Rule**.
4. In the **Required Elements in Password** section, select **Lowercase Letter**.
5. Click **OK**.

Through the CLI:

```
aliyun ram SetPasswordPolicy --RequireLowercaseCharacters true
```

Default Value:

The default password policy does not enforce any element in a password.

References:

1. https://www.alibabacloud.com/help/doc-detail/116413.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.9 Ensure RAM password policy require at least one symbol (Automated)

Profile Applicability:

- Level 1

Description:

RAM password policies can be used to ensure password complexity. It is recommended that the password policy require at least one symbol.

Rationale:

Enhancing complexity of a password policy increases account resiliency against brute force logon attempts.

Audit:

Perform the following to ensure the password policy is configured as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, make sure that the value of **Required Elements in Password** contains **Symbols**.

Through the CLI:

```
aliyun ram GetPasswordPolicy
```

In the output, make sure that the **RequireSymbols** parameter is set to **true**.

Remediation:

Perform the following to set the password policy as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, click **Edit Password Rule**.
4. In the **Required Elements in Password** section, select **Symbols**.
5. Click **OK**.

Through the CLI:

```
aliyun ram SetPasswordPolicy --RequireSymbols true
```

Default Value:

The default password policy does not enforce any element in a password.

References:

1. https://www.alibabacloud.com/help/doc-detail/116413.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.10 Ensure RAM password policy require at least one number (Automated)

Profile Applicability:

- Level 1

Description:

RAM password policies can be used to ensure password complexity. It is recommended that the password policy require at least one number.

Rationale:

Enhancing complexity of a password policy increases account resiliency against brute force logon attempts.

Audit:

Perform the following to ensure the password policy is configured as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, make sure that the value of **Required Elements in Password** contains **Numbers**.

Through the CLI:

```
aliyun ram GetPasswordPolicy
```

In the output, make sure that the **RequireNumbers** parameter is set to **true**.

Remediation:

Perform the following to set the password policy as expected:
Through the management console

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, click **Edit Password Rule**.
4. In the **Required Elements in Password** section, select **Numbers**.
5. Click **OK**.

Through the CLI

```
aliyun ram SetPasswordPolicy --RequireNumbers true
```

Default Value:

The default password policy does not enforce any element in a password.

References:

1. https://www.alibabacloud.com/help/doc-detail/116413.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.11 Ensure RAM password policy requires minimum length of 14 or greater (Automated)

Profile Applicability:

- Level 1

Description:

RAM password policies can be used to ensure password complexity. It is recommended that the password policy require a minimum of 14 or greater characters for any password.

Rationale:

Enhancing complexity of a password policy increases account resiliency against brute force logon attempts.

Audit:

Perform the following to ensure the password policy is configured as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, make sure that the value of **Password Length** is **<14>** to **<32>** characters.

Through the CLI:

```
aliyun ram GetPasswordPolicy
```

In the output, make sure that the **MinimumPasswordLength** parameter is set to **<14>** or a greater number.

Remediation:

Perform the following to set the password policy:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, click **Edit Password Rule**.
4. In the **Password Length** field, enter **<14>** or a greater number.
5. Click **OK**.

Through the CLI

```
aliyun ram SetPasswordPolicy --MinimumPasswordLength 14
```

Default Value:

The default password policy requires a minimum of 8 characters for a password.

References:

1. https://www.alibabacloud.com/help/doc-detail/116413.htm

Additional Information:

The value range of Password Retry Constraint Policy is from 0 to 32.

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.12 Ensure RAM password policy prevents password reuse (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended that the password policy prevent the reuse of passwords.

Rationale:

Preventing password reuse increases account resiliency against brute force logon attempt.

Audit:

Perform the following to ensure the password policy is configured as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, make sure that the value of **Password History Check Policy** is **Disable Using Latest 5 Passwords**.

Through the CLI:

```
aliyun ram GetPasswordPolicy
```

In the output, make sure that the **PasswordReusePrevention** parameter is set to **5**.

Remediation:

Perform the following to set the password policy as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, click **Edit Password Rule**.
4. In the **Password History Check Policy** field, enter **5**.
5. Click **OK**.

Through the CLI:

```
aliyun ram SetPasswordPolicy --PasswordReusePrevention 5
```

Default Value:

The default password policy does not prevent password reuse.

References:

1. https://www.alibabacloud.com/help/doc-detail/116413.htm

Additional Information:

The value range of Password History Check Policy is from 0 to 24.

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.13 Ensure RAM password policy expires passwords within 90 days or less (Automated)

Profile Applicability:

- Level 1

Description:

RAM password policies can require passwords to be expired after a given number of days. It is recommended that the password policy expire passwords after 90 days or less.

Rationale:

Reducing the password lifetime increases account resiliency against brute force logon attempts. Additionally, requiring regular password changes help in the following scenarios:

- list text here Passwords can be stolen or compromised sometimes without your knowledge. This can happen through a system compromise, software vulnerability, or internal threat.
- Many people use the same password for many systems such as work, email, and personal.
- Compromised end user workstations might have a keystroke logger.

Audit:

Perform the following to ensure the password policy is configured as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, make sure that the value of **Password Validity Period** does not exceed **90 Days**.

Through the CLI:

```
aliyun ram GetPasswordPolicy
```

In the output, make sure that the **MaxPasswordAge** parameter is set to **<90>** or a smaller number.

Remediation:

Perform the following to set the password policy as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, click **Edit Password Rule**.
4. In the **Password Validity Period** field, enter **<90>** or a smaller number.
5. Click **OK**.

Through the CLI:

```
aliyun ram SetPasswordPolicy --MaxPasswordAge 90
```

Default Value:

The default password policy does not prevent password reuse.

References:

1. https://www.alibabacloud.com/help/doc-detail/116413.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.14 Ensure RAM password policy temporarily blocks logon after 5 incorrect logon attempts within an hour (Automated)

Profile Applicability:

- Level 1

Description:

RAM password policies can temporarily block logon after several incorrect logon attempts within an hour. It is recommended that the password policy is set to temporarily block logon after 5 incorrect logon attempts within an hour.

Rationale:

Temporarily blocking logon for incorrect password input increases account resiliency against brute force logon attempts.

Audit:

Perform the following to ensure the password policy is configured as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, make sure that the value of **Password Retry Constraint Policy** is **A Maximum of 5 Logon Attempts with Incorrect Password within One Hour**.

Through the CLI:

```
aliyun ram GetPasswordPolicy
```

In the output, make sure that the **MaxLoginAttemps** parameter is set to **<5>** or a smaller number.

Remediation:

Perform the following to set the password policy as expected:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Settings**.
3. In the **Password Strength Settings** section, click **Edit Password Rule**.

4. In the **Password Retry Constraint Policy** field, enter **<5>** or a smaller number.
5. Click **OK**.

Through the CLI:

```
aliyun ram SetPasswordPolicy --MaxLoginAttemps 5
```

Default Value:

The default password policy does not prevent password reuse.

References:

1. https://www.alibabacloud.com/help/doc-detail/116413.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.15 Ensure RAM policies that allow full ":*" administrative privileges are not created (Automated)*

Profile Applicability:

- Level 1

Description:

RAM policies represent permissions that can be granted to users, groups, or roles. It is recommended and considered a standard security advice to grant least privilege—that is, granting only the permissions required to perform tasks. Determine what users need to do and then create policies with permissions only fits those tasks, instead of allowing full administrative privileges.

Rationale:

It is more secure to start with a minimum set of permissions and grant additional permissions as necessary, rather than starting with permissions that exceed the necessity and then trying to tighten them later.

Providing full administrative privileges exposes your resources on Alibaba Cloud to potentially unwanted actions.

RAM policies that have a statement with "Effect": "Allow", "Action": "*", and "Resource": ""* should be prohibited.

Impact:

If you edit the policy document, or remove all references from the policy, the identities using this policy may encounter access denied errors for the actions and resources that are not covered by their current permissions.

Audit:

Perform the following to check what permissions are allowed inside a policy:
Through the management console:

1. Logon to RAM console.
2. Choose **Permissions > Policies**.
3. From the **Policy Type** drop-down list, select **Custom Policy**.
4. In the **Policy Name** column, click the name of each policy.
5. In the **Policy Document** section, make sure that no policy has a statement that includes "**Effect**": "**Allow**", "**Action**": "*", and*

*"**Resource**": ""*, or any policy with such statement is not attached to any RAM identities (including RAM user, group, or role).

Through the CLI:

1. Run the following command to obtain a list of policies

```
aliyun ram ListPolicies --PolicyType Custom
```

2. For each policy returned, run the following command to determine if any policies allow full administrative privileges:

```
aliyun ram GetPolicy --PolicyName <policy_name> --PolicyType Custom
```

Note: In the preceding command, **policy_name** is the value of the **PolicyName** parameter in each policy the ListPolicies command returned.
In the output, check the value of PolicyDocument under DefaultPolicyVersion to make sure that no policy has a statement that includes "**Effect**": "**Allow**", "**Action**": "*", and "**Resource**": ""*, or make sure that the value of **AttachmentCount** under **Policy** is set to **0** for such policies.

Remediation:

Perform the following to detach the policy that has full administrative privileges and remove them:
Through the management console:

1. Logon to RAM console.
2. Choose **Permissions > Policies**.
3. From the **Policy Type** drop-down list, select **Custom Policy**.
4. In the **Policy Name** column, click the name of the target policy.
5. In the **Policy Document** section, check whether the policy has a statement that includes "**Effect**": "**Allow**", "**Action**": "*", and "**Resource**": ""*.
   - If it does not, skip this section.
   - If it does, edit the policy to remove such statement or remove the policy from any RAM users, user groups, or roles that have this policy attached.
     - To edit the policy:
     a. On the **Policy Document** tab, click **Modify Policy Document**.
     b. Remove the entire "**Statement**" element which contains the full *:* administrative privilege, or modify it to a smaller permission.
     - To remove all references from the policy:

a. Go to the **References** tab, review if there is any reference of the custom policy.
b. For each reference, click **Revoke Permission**.

6. Click **OK**.

Through the CLI:

1. Run the following command to list all RAM users, groups, and roles to which the specified policy (i.e. policy with .) is attached:

```
aliyun ram ListEntitiesForPolicy --PolicyName <policy_name> --PolicyType
Custom
```

2. Run the following command to detach the policy from all RAM users:

```
aliyun ram DetachPolicyFromUser --PolicyName <policy_name> --PolicyType
Custom --UserName <ram_user >
```

3. Run the following command to detach the policy from all RAM user groups:

```
aliyun ram DetachPolicyFromGroup --PolicyName <policy_name> --PolicyType
Custom --GroupName <ram_group>
```

4. Run the following command to detach the policy from all RAM roles:

```
aliyun ram DetachPolicyFromRole --PolicyName <policy_name> --PolicyType
Custom --RoleName <ram_role>
```

Default Value:

By default, no custom policy is created.

References:

1. https://www.alibabacloud.com/help/doc-detail/93733.htm
2. https://www.alibabacloud.com/help/doc-detail/116803.htm
3. https://www.alibabacloud.com/help/doc-detail/116818.htm

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.16 Ensure RAM policies are attached only to groups or roles (Automated)

Profile Applicability:

- Level 1

Description:

By default, RAM users, groups, and roles have no access to Alibaba Cloud resources. RAM policies are the means by which privileges are granted to users, groups, or roles. It is recommended that RAM policies be applied directly to groups and roles but not users.

Rationale:

Assigning privileges at the group or role level reduces the complexity of access management as the number of users grows. Reducing access management complexity may in-turn reduce opportunity for a principal to inadvertently receive or retain excessive privileges.

Impact:

There may be cases that a user needs to have permissions that cannot be covered by the groups it joins or roles it can assume. It may still be needed to attach specific policies to RAM users for certain operation that cannot be grouped with other permission under role or group.

Audit:

Perform the following to determine if policies are attached directly to users:
Through the management console:

1. Logon to RAM console.
2. Choose **Identities > Users**.
3. In the **User Logon Name/Display Name** column, click the username of each RAM user.
4. Click the **Permissions** tab.
5. On the **Individual** tab, make sure that no policy exists.

Through the CLI:

1. Run the following command to obtain a list of RAM users:

```
aliyun ram ListUsers
```

2. For each user returned, run the following command to determine if any policies are attached to the user:

```
aliyun ram ListPoliciesForUser --UserName <ram_user>
```

If any polices are returned, the user has a direct policy attached.

Remediation:

Perform the following to create a RAM user group and assign a policy to it:
Through the management console:

1. Log on to RAM console.
2. Choose **Identities > Users**.
3. Click **Create Group**, and enter the group name, display name, and description.
4. Click **OK**.
5. In the **Group Name/Display Name** column, find the target RAM user group and click **Add Permissions**.
6. In the **Select Policy** section, select the target policy or policies and click **OK**.

Through the CLI:

1. Run the following command to create a RAM user group:

```
aliyun ram CreateGroup –GroupName <ram_user_group>
```

2. Run the following command to attach a policy to the group:

```
aliyun ram AttachPolicyToGroup --GroupName <ram_user_group> --PolicyName
<policy_name> --PolicyType <System|Custom>
```

Perform the following to add a user to a given group:
Through the management console:

1. Log on to RAM console.
2. Choose **Identities > Groups**.
3. In the **Group Name/Display Name** column, find the target RAM user group and click **Add Group Members**.
4. In the **User** section, select the target RAM user and click **OK**.

Through the CLI:
Run the following command to add a RAM user to a user group:

```
aliyun ram AddUserToGroup --GroupName <ram_user_group> --UserName <ram_user >
```

Perform the following to remove a direct association between a user and policy:

Through the management console:

1. Logon to RAM console.
2. Choose **Permissions > Grants**.
3. In the **Principal** column, find the target RAM user and click **Revoke Permission**.
4. Click **OK**.

Through the CLI:

Run the following command to remove a policy from a RAM user:

```
aliyun ram DetachPolicyFromUser --PolicyName <policy_name> --PolicyType
<System|Custom> --UserName <ram_user >
```

References:

1. https://www.alibabacloud.com/help/doc-detail/116809.htm
2. https://www.alibabacloud.com/help/doc-detail/116815.htm
3. https://www.alibabacloud.com/help/doc-detail/116147.htm
4. https://www.alibabacloud.com/help/doc-detail/116820.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

2 Logging and Monitoring

This section covers recommendations addressing Logging and Monitoring on Alibaba Cloud.

2.1 Ensure that ActionTrail are configured to export copies of all Log entries (Automated)

Profile Applicability:

- Level 1

Description:

ActionTrail is a web service that records API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the Alibaba Cloud service. ActionTrail provides a history of API calls for an account, including API calls made via the Management Console, SDKs, command line tools.

Rationale:

The API call history produced by ActionTrail enables security analysis, resource change tracking, and compliance auditing. Moreover, ensuring that a multi-regions trail exists will ensure that any unexpected activities occurring in otherwise unused regions are detected. Global Service Logging should be enabled by default to capture recording of events generated on Alibaba Cloud global services for a multi-regions trail, therefore, ensuring the recording of management operations that are performed on all resources in an Alibaba Cloud account.

Impact:

OSS lifecycle features can be used to manage the accumulation and management of logs over time. See the following resource for more information on these features:
http://help.aliyun.com/document_detail/31863.html

Audit:

Perform the following to determine if ActionTrail is enabled for all regions:
Through the management Console:

1. Logon to ActionTrail Console.
2. Click on **Trails** on the left navigation pane, you will be presented with a list of trails across all regions.
3. Ensure at least one **Trail** has All specified in the Region column.
4. Click on a trail via the link in the Name column.
5. Ensure Logging is set to **Enable** to export log copies to OSS for storage.

6. Ensure **Yes** is selected for **Apply Trail to All Regions**.

Through CLI:
Ensure Trail is set to enable and Trail Region is set to All

```
aliyuncli actiontrail DescribeTrails
```

Remediation:

Perform the following to enable global (Multi-region) ActionTrail logging:
Through the management Console:

1. Logon to ActionTrail Console.
2. Click on **Trails** on the left navigation pane.
3. Click **Add new trail**.
   a. Enter a trail name in the **Trail name box**.
   b. Set **Yes** for **Apply Trail to All Regions**.
   c. Specify an OSS bucket name in the OSS bucket box.
   d. Specify an SLS project name in the SLS project box.
   e. Click **Create**.

Through CLI:

```
aliyuncli actiontrail CreateTrail --Name <trail_name> --OssBucketName
<oss_bucket_for_actiontrail> --RoleName aliyunactiontraildefaultrole
--SlsProjectArn <sls_project_arn_for_actiontrail> --SlsWriteRoleArn
<sls_role_arn_for_actiontrail> --EventRW <api_type_for_actiontrail>

aliyuncli actiontrail UpdateTrail --Name <trail_name> --OssBucketName
<oss_bucket_for_actiontrail> --RoleName aliyunactiontraildefaultrole
--SlsProjectArn <sls_project_arn_for_actiontrail> --SlsWriteRoleArn
<sls_role_arn_for_actiontrail> --EventRW <api_type_for_actiontrail>
```

Default Value:

By default, there are no trails configured. Once the trail is enabled, it applies to all regions by default.

References:

1. https://www.alibabacloud.com/help/doc-detail/28829.htm

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

2.2 Ensure the OSS used to store ActionTrail logs is not publicly accessible (Automated)

Profile Applicability:

- Level 1

Description:

ActionTrail logs a record of every API call made in your Alibaba Cloud account. These logs file are stored in an OSS bucket. It is recommended that the access control list (ACL) of the OSS bucket, which ActionTrail logs to, shall prevent public access to the ActionTrail logs.

Rationale:

Allowing public access to ActionTrail log content may aid an adversary in identifying weaknesses in the affected account's use or configuration.

Audit:

Perform the following to determine if any public access is granted to an OSS bucket via an ACL:

Through the Management Console:

1. Logon to ActionTrail Console.
2. In the API activity history pane on the left, click **Trails**.
3. In the **Trails** pane, note the bucket names in the OSS bucket column.
4. Log on to OSS Console.
5. For each bucket noted in step 3, click on the bucket and click **Basic Settings**.
6. In the **Access Control List** pane, click the **Configure**.
7. The **Bucket ACL** tab shows three kind of grants, **Private Public Read**, **Public Read/Write**.
8. Ensure **Private** be set to the bucket.

Through CLI:

1. Get the name of the OSS bucket that ActionTrail is logging to:

```
aliyuncli actiontrail DescribeTrails
```

2. Ensure the Bucket ACL is to be set private:

```
ossutil set-acl oss://<bucketName> private -b
```

Remediation:

Perform the following to remove any public access that has been granted to the bucket via an ACL:

Through the Management Console:

1. Logon to OSS Console.
2. Right on the bucket and click **Basic Settings**.
3. In the **Access Control List** pane, click the **Configure**.
4. The **Bucket ACL** tab shows three kind of grants. Like **Private**, **Public Read**, **Public Read/Write**.
5. Ensure **Private** be set to the bucket.
6. Click **Save** to save the ACL.

Default Value:

By default, OSS buckets are not publicly accessible.

References:

1. https://help.aliyun.com/document_detail/31954.html

CIS Controls:

Version 7

6 Maintenance, Monitoring and Analysis of Audit Logs
Maintenance, Monitoring and Analysis of Audit Logs

2.3 Ensure audit logs for multiple cloud resources are integrated with Log Service (Manual)

Profile Applicability:

- Level 1

Description:

Log Service provides functions of log collection and analysis in real time across multiple cloud resources under the authorized resource owners. This enable the large-scale corporate for security governance over all resources owned by multiple accounts by integrating the log from different sources and monitoring. For example, Log Service supports the integration to collect logs from the following sources:

- ActionTrail is a cloud service that records API calls made in a given Alibaba Cloud account.
- ApsaraDB RDS and DRDS audit records all data manipulation language (DML) and data definition language (DDL) operations through network protocol analysis and only consumes a small amount of CPU resources. The Trial Edition of SQL Explorer retains SQL log data generated within up to one day free of charge.
- Object Storage Service (OSS) support recording every changes to its resources including bucket, ACL, replications, and files, as well as file access logs.
- The access log feature of SLB can be applied to HTTP- and HTTPS-based Layer 7 load balancing. Access logs can contain about 30 fields such as the time when a request is received, the IP address of the client, processing latency, request URI, backend server (ECS instance) address, and returned status code. As an Internet access point, SLB needs to distribute a large number of access requests.
- Alibaba Cloud API Gateway provides API hosting service to facilitate micro-service aggregation, frontend and backend isolation, and system integration. Each API request corresponds to an access record, which contains information such as the IP address of the API caller, requested URL, response latency, returned status code, and number of bytes for each request and response. With the preceding information, you can understand the operating status of your web services.
- NAS audit and access log support to record each request to Network File System (NFS) file system including file changes and access, details of the access request, such as the operation type, target object, and response status of the current user. Log Service also provides rich functions such as real-time query and analysis, and dashboard presentation for this part of logs.

Rationale:

Sending the audit logs to Log Service will facilitate real-time and historic activity logging based on user, API, resource, and IP address, and provides benefits to collect logs under

multiple accounts, store logs centrally, establish alarms and notifications for anomalous or sensitivity account activity, and extend the default log retention period to 180 days.

Impact:

RDS Audit Log integration requires to enable SQL Explorer feature on RDS side, which may introduce extra charge.

Audit:

Perform the following to ensure the logs are integrated with Log Services:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail**, **RDS SQL Audit Logs**, **OSS Access Logs**, **SLB Access Log**, **NAS Access Log**, **API Gateway Access log** are **Enabled** under the **Access to Cloud Products > Global Configuration** page.
4. Ensure all resource owners account are tracked under the **Multi-Account Configurations > Global Configuration** page.
5. Ensure the **Status** is **Green** under the **Access to Cloud Products > Status Dashboard** page.

Remediation:

Perform the following to ensure the logs are integrated with Log Services:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to Access to **Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.
   b. Check the appropriate product logging selection, such as **Action Trail**, **RDS SQL Audit Logs**, **OSS Access Logs**, **SLB Access Log**, **NAS Access Log**, **API Gateway Access log** and configure a proper storage period (in days).
   c. Click **Save** to save the changes.
4. Go to **Multi-Account Configurations > Global Configuration** page.
   a. Modify it to input the other resource owner account ID.
   b. Click **Save** to save the changes.
5. Go to **Access to Cloud Products > Status Dashboard** page to ensure the **Status** is **Green**.

Default Value:

Not enabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/84920.htm

Additional Information:

1. Multi-Account configurations enable to collect audit logs into one log store under one central account.
2. If you configure log collection for the first time, please authorize Log Service upon the prompts on the user console page. The authorization enables Log Service to distribute product audit related logs to your Logstore.
3. If you configure log collection for a specific resource owner in Multi-Account page for the first time, please authorize between the current resource owner and the other resource owner by referring to the guide from the reference page below.
4. After changes to the configuration, The Status will become either Green, Red or Orange in several minutes. Refresh the page to check the latest status. If it's not Green, please refer to the guide from the reference page below.
5. RDS Audit Logs collection only support specific regions for certain types of RDS, please refer to the guide from the reference page below.
6. Audit log collection by Log Service is from the time when you enable the Audit Log function on Log Service. It does not support historical audit log collection to trace back the audit log records before Audit Log function on Log Service is enabled.
7. The audit log collection for newly created instance are automatically enabled once the instance is created by default for NAS and API Gateway. However it may delay several minutes for RDS and SLB audit logs collection.

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

2.4 Ensure Log Service is enabled for Container Service for Kubernetes (Manual)

Profile Applicability:

- Level 1

Description:

Log Service shall be connected with Kubernetes clusters of Alibaba Cloud Container Service to collect the audit log for central monitoring and analysis. You can simply enable Log Service when creating a cluster for log collection.

Rationale:

By enabling Log Service Audit Log function to integrate audit log of Kubernetes, it is possible to capture all events on container to improve the security of serverless cluster. Central log collection and monitoring allows access to all log information on one dashboard which can be useful in security and incident response workflows.

Audit:

Perform the following to ensure the Kubernetes logs are integrated with Log Services:

1. Logon to ACK Console.
2. Click **Cluster > Cluster** in the left-side navigation pane and select a cluster to click **Action > Manage**.
3. Ensure the **Cluster Auditing** page is available.

Remediation:

Perform the following ensure the Log Service for Kubernetes clusters is enabled:

1. Logon to ACK Console.
2. Click **Clusters** in the left-side navigation pane and click **Create Kubernetes Cluster** in the upper-right corner.
3. Scroll to the bottom of the page and select the **Using Log Service** check box. The log plug-in will be installed in the newly created Kubernetes cluster.
4. When you select the **Using Log Service** check box, project options are displayed. A project is the unit in Log Service to manage logs.
5. After you complete the configuration, click **Create** in the upper-right corner.
6. In the displayed dialog box, click **OK**.

Default Value:

Logging is disabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/87540.htm

Additional Information:

It's highly recommended to enable the log service when creating a cluster. If it's not enabled, a relative complex set of steps needs to be followed in order to enable the log service. Please refer to https://www.alibabacloud.com/help/doc-detail/87540.htm for more detail.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

2.5 Ensure virtual network flow log service is enabled (Manual)

Profile Applicability:

- Level 1

Description:

The flow log can be used to capture the traffic of an Elastic Network Interface (ENI), Virtual Private Cloud (VPC) or Virtual Switch (VSwitch). The flow log of a VPC or VSwitch shall be integrated with Log Service to capture the traffic of all ENIs in the VPC or VSwtich including the ENIs created after the flow log function is enabled. The traffic data captured by flow logs is stored in Log Service for real-time monitoring and analysis. A capture window is about 10 minutes, during which the traffic data is aggregated and then released to flow log record.

Rationale:

By integrating virtual network flow log to Log Service, the inbound and outbound traffic over the ENI in your VPC is captured for monitoring and analysis which can be useful in monitoring network traffic and access control rules as well as network trouble shooting.

Audit:

Perform the following ensure the virtual network flow log is enabled:

1. Logon to VPC console.
2. In the left-side navigation pane, click **FlowLog**.
3. Select the region to which the target flow log belongs.
4. On the **FlowLog** page, ensure the target flow log and logstore is configured.

Remediation:

Perform the following ensure the virtual network flow log is enabled:

1. Logon to VPC console.
2. In the left-side navigation pane, click **FlowLog**.
3. Select the region to which the flow log is to be created.
4. On the **FlowLog** page, click **Create FlowLog**.
5. On the **Create FlowLog** page, set the required parameters by following the instruction, and then click **OK**.

Default Value:

Logging is disabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/90628.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.6 Ensure Anti-DDoS access and security log service is enabled (Manual)

Profile Applicability:

- Level 2

Description:

Alibaba Cloud Anti-DDoS Pro supports integration with Log Service for website access log (including HTTP flood attack logs) to enable the real-time analysis and reporting center features. The log collected can be monitored on a central dashboard on Log Service.

Rationale:

By integrating Anti-DDoS access and security log to Log Service, the website access log and flood attack logs can be collected and monitored to enable real-time query and improve the network security.

Impact:

Extra charge will incur.

Audit:

Perform the following ensure the Anti-DDoS access and security log is enabled:

1. Logon to Anti-DDoS Pro Console, and go to the **Log > Full Log** page.
2. Select the specific website.
3. Ensure the **Log Collection** is turned on.
4. Ensure the **log volume usage indicator** is sufficient for log storage.

Remediation:

Perform the following ensure the Anti-DDoS access and security log is enabled:

1. Logon to Anti-DDoS Pro Console, and go to the **Log > Full Log** page.
2. Select the specific website for which you want to enable the **Full Log** service and click to turn on the **Status** switch.

Default Value:

Logging is disabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/85007.htm

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.7 Ensure Web Application Firewall access and security log service is enabled (Manual)

Profile Applicability:

- Level 2

Description:

Log Service collects log entries that record visits to and attacks on websites that are protected by Alibaba Cloud Web Application Firewall (WAF), and supports real-time log query and analysis. The query results are centrally displayed in dashboards.

Rationale:

The WAF access and security log shall be enabled to enable timely analytical investigation on visits to and attacks on your websites and help security engineers to develop protection strategies.

Impact:

Extra charge will incur by enabling the log.

Audit:

Perform the following ensure the WAF access and security log is enabled:

1. Logon to WAF Console.
2. Choose **App Market > App Management**.
3. Click **Configure** in **Real-time Log Query and Analysis Service**.
4. On **Log Service** page, select the specific domain name of your website.
5. Ensure the **Status** switch on the right is turned on.
6. Ensure the **log volume usage indicator** is sufficient for log storage.

Remediation:

Perform the following ensure the Anti-DDoS access and security log is enabled:

1. Logon to WAF Console.
2. Choose **App Market > App Management**.
3. Select the region where your WAF instance is located.
4. Click **Upgrade** in **Real-time Log Query and Analysis Service**.
5. Enable **Log Service**.
6. Select the log storage period and the log storage size, and click **Buy Now**.

7. Return to the WAF Console and choose **App Market > App Management**, and then click **Authorize** in **Real-time Log Query and Analysis Service**.
8. Click **Agree** to authorize WAF to write log entries to your exclusive logstore.
9. Return to the WAF Console and choose **App Market > App Management** and then, click **Configure** in **Real-time Log Query and Analysis Service**.
10. On the **Log Service** page, select the domain name of your website that is protected by WAF, and turn on the **Status** switch on the right to enable WAF Log Service. These log entries can be queried and analyzed in real time.

Default Value:

Logging is disabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/95267

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.8 Ensure Cloud Firewall access and security log analysis is enabled (Manual)

Profile Applicability:

- Level 2

Description:

Log Service collects log entries of internet traffic that are protected by Cloud Firewall, and supports real-time log query and analysis. The query results are centrally displayed in dashboards.

Rationale:

The Cloud Firewall log shall be enabled with the Log Service to collect and store real-time log of both inbound and outbound traffic for timely analysis, reports, alarms and downstream computing interconnection and provides the detailed results displaying centrally on dashboard to monitor and improve network security.

Impact:

Extra charge will incur by enabling the log.

Audit:

Perform the following ensure the Cloud Firewall access and security log is enabled:

1. Logon to Cloud Firewall Console.
2. In the left-side navigation pane, select **Advanced Features > Log Analysis**.
3. Ensure the **Status** switch on the right side is enabled.
4. Ensure the **log volume usage indicator** is not exhausted.

Remediation:

Perform the following ensure the Cloud Firewall access and security log is enabled:

1. Logon to Cloud Firewall Console.
2. In the left-side navigation pane, select **Advanced Features > Log Analysis**.
3. Click **Active Now** on the **Log Analysis** page.
4. Select your **log storage capacity**, and then click **Pay** to complete the payment.
5. Go back to **Log Analysis** page on Cloud Firewall console.
6. Click the **Status** on the right side to enable the Log Analysis service.

Default Value:

Logging is disabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/113184.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.9 Ensure Security Center Network, Host and Security log analysis is enabled (Manual)

Profile Applicability:

- Level 2

Description:

Log Service collects log entries of Security Center for security logs, network logs, and host logs, with 14 subtypes, including

1. Security logs

    a. Vulnerability logs

    b. Baseline logs

    c. Security alerting logs

2. Security logs

    a. Vulnerability logs

    b. Baseline logs

    c. Security alerting logs

3. Network logs

    a. DNS logs

    b. Local DNS logs

    c. Network session logs

    d. Web logs

4. Server logs

    a. Process initiation logs

    b. Network connection logs

    c. System logon logs

d. Brute-force cracking logs

e. Process snapshots

f. Account snapshots

g. Port listening snapshots

The Log Service supports real-time log query and analysis over the logs mentioned above. The query results are centrally displayed in dashboards.

Rationale:

The Security Center log shall be enabled to collect and store real-time security log, network log and server log to better protect your assets in real time.

Impact:

Extra charge will incur by enabling the log.

Audit:

Perform the following ensure the Cloud Firewall access and security log is enabled:

1. Logon to Security Center Console.
2. In the left-side navigation pane, select **Investigation > Log Analysis** to enter the **Activate Log Analysis** page.
3. In the **Activate Log Analysis** page, ensure the switch for the specific log type are turned on.
4. Ensure the **log volume usage indicator** is not exhausted.

Remediation:

Perform the following ensure the Cloud Firewall access and security log is enabled:

1. Logon to Security Center Console.
2. In the left-side navigation pane, select **Investigation > Log Analysis** to enter the **Activate Log Analysis** page.
3. Click **Active Now** on the **Activate log Analysis** page.
4. On the **Purchase** page, check **Full Log** and configure some other settings as needed.
5. Click **Purchase Now**.
6. In the **Activate log Analysis** click **Activate log Analysis** to complete the authorization.
7. In the **log type** menu, check the log types to enable the log collection.

Default Value:

Logging is disabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/93065.htm
2. https://www.alibabacloud.com/help/doc-detail/93117.htm

Additional Information:

Only Security Center Enterprise Edition supports full log service and provides features for accurate real-time log querying and log analysis.

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.10 Ensure log monitoring and alerts are set up for RAM Role changes (Manual)

Profile Applicability:

- Level 1

Description:

It is recommended that a query and alarm should be established for RAM Role creation, deletion and updating activities.

Rationale:

Alibaba Cloud Resource Access Management (RAM) provides predefined roles that give granular access to specific resources and prevent unwanted access to other resources. Log Service provides ability to create custom monitoring query: monitoring role creation, deletion and updating activities will help in identifying any potential malicious actions at early stage.

Audit:

Perform the following to ensure the log monitoring and alerts are set up for RAM Role Changes:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
("event.serviceName": ResourceManager or "event.serviceName": Ram) and
("event.eventName": CreatePolicy or "event.eventName": DeletePolicy or
"event.eventName": CreatePolicyVersion or "event.eventName":
UpdatePolicyVersion or "event.eventName": SetDefaultPolicyVersion  or
"event.eventName": DeletePolicyVersion) | select count(1) as c
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for RAM Role Changes:

1. Logon to SLS Console.

2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.
   b. Check the **Action Trail** and configure a proper days.
   c. Click **Save** to save the changes.
4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query

```
("event.serviceName": ResourceManager or "event.serviceName": Ram) and
("event.eventName": CreatePolicy or "event.eventName": DeletePolicy or
"event.eventName": CreatePolicyVersion or "event.eventName":
UpdatePolicyVersion or "event.eventName": SetDefaultPolicyVersion  or
"event.eventName": DeletePolicyVersion) | select count(1) as c
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default

References:

1. https://www.alibabacloud.com/help/doc-detail/91784.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.11 Ensure log monitoring and alerts are set up for Cloud Firewall changes (Manual)

Profile Applicability:

- Level 2

Description:

It is recommended that a metric filter and alarm be established for Cloud Firewall rule changes.

Rationale:

Monitoring for Create or Update firewall rule events gives insight network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Perform the following to ensure the log monitoring and alerts are set up for Cloud Firewall Changes:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
"event.serviceName": "Cloudfw" and ("event.eventName":
CreateVpcFirewallControlPolicy or "event.eventName":
DeleteVpcFirewallControlPolicy or "event.eventName":
ModifyVpcFirewallControlPolicy) | select count(1) as c
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up Cloud Firewall Changes:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.

b. Check the **Action Trail** and configure a proper days.
c. Click **Save** to save the changes.

4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query

```
"event.serviceName": "Cloudfw" and ("event.eventName":
CreateVpcFirewallControlPolicy or "event.eventName":
DeleteVpcFirewallControlPolicy or "event.eventName":
ModifyVpcFirewallControlPolicy) | select count(1) as c
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.12 Ensure log monitoring and alerts are set up for VPC network route changes (Manual)

Profile Applicability:

- Level 1

Description:

It is recommended that a metric filter and alarm be established for VPC network route changes.

Rationale:

Routes define the paths network traffic takes from a VM instance to another destinations. The other destination can be inside your VPC network (such as another VM) or outside of it. Every route consists of a destination and a next hop. Traffic whose destination IP is within the destination range is sent to the next hop for delivery. Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for VPC network route changes.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are Enabled under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
("event.serviceName": Ecs or "event.serviceName": Vpc) and
("event.eventName": CreateRouteEntry or "event.eventName":
DeleteRouteEntry or "event.eventName": ModifyRouteEntry or
"event.eventName": AssociateRouteTable or "event.eventName":
UnassociateRouteTable) | select count(1) as c
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for VPC network route changes:

1. Logon to SLS Console.

2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.
   b. Check the **Action Trail** and configure a proper days.
   c. Click Save to save the changes.
4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query

```
("event.serviceName": Ecs or "event.serviceName": Vpc) and
("event.eventName": CreateRouteEntry or "event.eventName":
DeleteRouteEntry or "event.eventName": ModifyRouteEntry or
"event.eventName": AssociateRouteTable or "event.eventName":
UnassociateRouteTable) | select count(1) as c
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.13 Ensure log monitoring and alerts are set up for VPC changes (Manual)

Profile Applicability:

- Level 1

Description:

It is recommended that a log search/analysis query and alarm be established for VPC changes.

Rationale:

Monitoring changes to VPC will help ensure VPC traffic flow is not getting impacted.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for VPC changes.

1. Logon to the SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
("event.serviceName": Ecs or "event.serviceName": Vpc) and
("event.eventName": CreateVpc or "event.eventName": DeleteVpc or
"event.eventName": DisableVpcClassicLink or "event.eventName":
EnableVpcClassicLink or "event.eventName": DeletionProtection or
"event.eventName": AssociateVpcCidrBlock or "event.eventName":
UnassociateVpcCidrBlock or "event.eventName": RevokeInstanceFromCen or
"event.eventName": CreateVSwitch or "event.eventName": DeleteVSwitch or
"event.eventName": CreateVSwitch) | select count(1) as c
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for VPC changes:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.

b. Check the **Action Trail** and configure a proper days.
c. Click Save to save the changes.

4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query

```
("event.serviceName": Ecs or "event.serviceName": Vpc) and
("event.eventName": CreateVpc or "event.eventName": DeleteVpc or
"event.eventName": DisableVpcClassicLink or "event.eventName":
EnableVpcClassicLink or "event.eventName": DeletionProtection or
"event.eventName": AssociateVpcCidrBlock or "event.eventName":
UnassociateVpcCidrBlock or "event.eventName": RevokeInstanceFromCen or
"event.eventName": CreateVSwitch or "event.eventName": DeleteVSwitch or
"event.eventName": CreateVSwitch) | select count(1) as c
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.14 Ensure log monitoring and alerts are set up for OSS permission changes (Manual)

Profile Applicability:

- Level 1

Description:

It is recommended that a metric filter and alarm be established for OSS Bucket RAM changes.

Rationale:

Monitoring changes to OSS permissions may reduce time to detect and correct permissions on sensitive OSS bucket and objects inside the bucket.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for OSS permission changes.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **OSS** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target oss_log

```
(operation:  PutBucket and request_uri: acl) or operation: PutObjectAcl|
select bucket, count (1) as c group by bucket
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for OSS permission changes:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.
   b. Check the **OSS** and configure a proper days.
   c. Click **Save** to save the changes.
4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.

5. Select **Log Management > OSS Log**.
6. In the search/analytics console, input below query

```
(operation:  PutBucket and request_uri: acl) or operation: PutObjectAcl|
select bucket, count (1) as c group by bucket
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.15 Ensure log monitoring and alerts are set up for RDS instance configuration changes (Manual)

Profile Applicability:

- Level 1

Description:

It is recommended that a metric filter and alarm be established for RDS Instance configuration changes.

Rationale:

Monitoring changes to RDS Instance configuration changes may reduce time to detect and correct misconfigurations done on database server.

Below are the few of configurable Options which may impact security posture of a RDS Instance:

1. Enable auto backups and high availability: Misconfiguration may adversely impact Business continuity, Disaster Recovery and High Availability.
2. Authorize networks : Misconfiguration may increase exposure to the untrusted networks.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for SQL instance configuration changes.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
"event.serviceName": rds and ("event.eventName": ModifyHASwitchConfig or
"event.eventName": ModifyDBInstanceHAConfig or "event.eventName":
SwitchDBInstanceHA or "event.eventName": ModifyDBInstanceSpec or
"event.eventName": MigrateSecurityIPMode or "event.eventName":
ModifySecurityIps or "event.eventName": ModifyDBInstanceSSL or
"event.eventName": MigrateToOtherZone or "event.eventName":
UpgradeDBInstanceKernelVersion or "event.eventName":
UpgradeDBInstanceEngineVersion or "event.eventName":
```

```
ModifyDBInstanceMaintainTime or "event.eventName":
ModifyDBInstanceAutoUpgradeMinorVersion or "event.eventName":
AllocateInstancePublicConnection or "event.eventName":
ModifyDBInstanceConnectionString or "event.eventName":
ModifyDBInstanceNetworkExpireTime or "event.eventName":
ReleaseInstancePublicConnection or "event.eventName": SwitchDBInstanceNetType
or "event.eventName": ModifyDBInstanceNetworkType or "event.eventName":
ModifyDBInstanceSSL or "event.eventName":
ModifyDTCSecurityIpHostsForSQLServer or "event.eventName":
ModifySecurityGroupConfiguration or "event.eventName": CreateBackup or
"event.eventName": ModifyBackupPolicy or "event.eventName": DeleteBackup or
"event.eventName": CreateDdrInstance or "event.eventName":
ModifyInstanceCrossBackupPolicy) | select count(1) as cnt
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for RDS instance configuration changes:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.
   b. Check the **Action Trail** and configure a proper days.
   c. Click **Save** to save the changes.
4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query

```
"event.serviceName": rds and ("event.eventName": ModifyHASwitchConfig or
"event.eventName": ModifyDBInstanceHAConfig or "event.eventName":
SwitchDBInstanceHA or "event.eventName": ModifyDBInstanceSpec or
"event.eventName": MigrateSecurityIPMode or "event.eventName":
ModifySecurityIps or "event.eventName": ModifyDBInstanceSSL or
"event.eventName": MigrateToOtherZone or "event.eventName":
UpgradeDBInstanceKernelVersion or "event.eventName":
UpgradeDBInstanceEngineVersion or "event.eventName":
ModifyDBInstanceMaintainTime or "event.eventName":
ModifyDBInstanceAutoUpgradeMinorVersion or "event.eventName":
AllocateInstancePublicConnection or "event.eventName":
ModifyDBInstanceConnectionString or "event.eventName":
ModifyDBInstanceNetworkExpireTime or "event.eventName":
ReleaseInstancePublicConnection or "event.eventName": SwitchDBInstanceNetType
or "event.eventName": ModifyDBInstanceNetworkType or "event.eventName":
ModifyDBInstanceSSL or "event.eventName":
ModifyDTCSecurityIpHostsForSQLServer or "event.eventName":
ModifySecurityGroupConfiguration or "event.eventName": CreateBackup or
"event.eventName": ModifyBackupPolicy or "event.eventName": DeleteBackup or
"event.eventName": CreateDdrInstance or "event.eventName":
ModifyInstanceCrossBackupPolicy) | select count(1) as cnt
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.16 Ensure a log monitoring and alerts are set up for unauthorized API calls (Manual)

Profile Applicability:

- Level 1

Description:

Real-time monitoring of API calls can be achieved by directing ActionTrail Logs to LogService and establishing corresponding query and alarms. It is recommended that a query and alarm be established for unauthorized API calls.

Rationale:

Monitoring unauthorized API calls will help reveal application errors and may reduce time to detect malicious activity.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for unauthorized API calls.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
"event.eventType": ApiCall and ("event.errorCode": "NoPermission" or
"event.errorCode": "NoPermission.*" or "event.errorCode": "Forbidden" or
"event.errorCode": "Forbbiden" or "event.errorCode": "Forbidden.*" or
"event.errorCode": "InvalidAccessKeyId" or "event.errorCode":
"InvalidAccessKeyId.*" or "event.errorCode": "InvalidSecurityToken" or
"event.errorCode": "InvalidSecurityToken.*" or "event.errorCode":
"SignatureDoesNotMatch" or "event.errorCode": "InvalidAuthorization" or
"event.errorCode": "AccessForbidden" or "event.errorCode": "NotAuthorized")
| select count(1) as cnt
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for unauthorized API calls:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.
   b. Check the **Action Trail** and configure a proper days.
   c. Click **Save** to save the changes.
4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query

```
"event.eventType": ApiCall and ("event.errorCode": "NoPermission" or
"event.errorCode": "NoPermission.*" or "event.errorCode": "Forbidden" or
"event.errorCode": "Forbbiden" or "event.errorCode": "Forbidden.*" or
"event.errorCode": "InvalidAccessKeyId" or "event.errorCode":
"InvalidAccessKeyId.*" or "event.errorCode": "InvalidSecurityToken" or
"event.errorCode": "InvalidSecurityToken.*" or "event.errorCode":
"SignatureDoesNotMatch" or "event.errorCode": "InvalidAuthorization" or
"event.errorCode": "AccessForbidden" or "event.errorCode": "NotAuthorized")
| select count(1) as cnt
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

2.17 Ensure a log monitoring and alerts are set up for Management Console sign-in without MFA (Manual)

Profile Applicability:

- Level 1

Description:

Real-time monitoring of API calls can be achieved by directing ActionTrail Logs to Log Service and establishing corresponding query and alarms. It is recommended that a query and alarm be established for console logins that are not protected by multi-factor authentication (MFA).

Rationale:

Monitoring for single-factor console logins will increase visibility into accounts that are not protected by MFA.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for Management Console sign-in without MFA.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
"event.eventName": ConsoleSignin and "addionalEventData.loginAccount": false
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for Management Console sign-in without MFA:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.

b. Check the **Action Trail** and configure a proper days.
c. Click **Save** to save the changes.

4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query

```
"event.eventName": ConsoleSignin and "addionalEventData.loginAccount": false
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

2.18 Ensure a log monitoring and alerts are set up for usage of "root" account (Manual)

Profile Applicability:

- Level 1

Description:

Real-time monitoring of API calls can be achieved by directing ActionTrail Logs to Log Service and establishing corresponding query and alarms. It is recommended that a query and alarm be established for console logins that are not protected by root login attempts.

Rationale:

Monitoring for root account logins will provide visibility into the use of a fully privileged account and an opportunity to reduce the use of it.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for usage of “root” account.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
"event.eventName": ConsoleSignin and "event.userIdentity.type" : root-account
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for usage of “root” account:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.
   b. Check the **Action Trail** and configure a proper days.
   c. Click **Save** to save the changes.

4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query

```
"event.eventName": ConsoleSignin and "event.userIdentity.type" : root-account
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

4.9 Log and Alert on Unsuccessful Administrative Account Login

Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

2.19 Ensure a log monitoring and alerts are set up for Management Console authentication failures (Manual)

Profile Applicability:

- Level 2

Description:

Real-time monitoring of API calls can be achieved by directing ActionTrail Logs to Log Service and establishing corresponding query and alarms. It is recommended that a query and alarm be established for failed console authentication attempts.

Rationale:

Monitoring failed console logins may decrease lead time to detect an attempt to brute force a credential, which may provide an indicator, such as source IP, that can be used in other event correlation.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for Management Console authentication failures.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
"event.eventName": ConsoleSignin and "event.errorCode" : *  and not
"event.errorCode" : "" | select count(1) as cnt
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for Management Console authentication failures:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.

b. Check the **Action Trail** and configure a proper days.
c. Click **Save** to save the changes.

4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query

```
"event.eventName": ConsoleSignin and "event.errorCode" : *  and not
"event.errorCode" : "" | select count(1) as cnt
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/28810.htm
2. https://www.alibabacloud.com/help/en/doc-detail/91784.htm
3. https://www.alibabacloud.com/help/en/doc-detail/93517.html

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

2.20 Ensure a log monitoring and alerts are set up for disabling or deletion of customer created CMKs (Manual)

Profile Applicability:

- Level 2

Description:

Real-time monitoring of API calls can be achieved by directing ActionTrail Logs to Log Service and establishing corresponding query and alarms. It is recommended that a query and alarm be established for customer created KMSs which have changed state to disabled or deletion.

Rationale:

Data encrypted with disabled or deleted keys will no longer be accessible.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for disabling or deletion of customer created CMKs.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
"event.serviceName": Kms and ("event.eventName": DisableKey or
"event.eventName": ScheduleKeyDeletion or "event.eventName":
DeleteKeyMaterial
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for disabling or scheduled deletion of customer created CMKs:

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.

b. Check the **Action Trail** and configure a proper days.
c. Click **Save** to save the changes.

4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query.

```
"event.serviceName": Kms and ("event.eventName": DisableKey or
"event.eventName": ScheduleKeyDeletion or "event.eventName":
DeleteKeyMaterial
```

7. Create a dashboard and set alert for the query result

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

2.21 Ensure a log monitoring and alerts are set up for OSS bucket policy changes (Manual)

Profile Applicability:

- Level 1

Description:

Real-time monitoring of API calls can be achieved by directing ActionTrail Logs to Log Service and establishing corresponding query and alarms. It is recommended that a query and alarm be established for changes to OSS bucket policies.

Rationale:

Monitoring changes to OSS bucket policies may reduce time to detect and correct permissive policies on sensitive OSS buckets.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for OSS bucket policy changes.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
"event.eventName": PutBucketLifecycle or "event.eventName": PutBucketPolicy
or "event.eventName": PutBucketCors or "event.eventName": PutBucketEncryption
or "event.eventName": PutBucketReplication or "event.eventName":
DeleteBucketPolicy or "event.eventName": DeleteBucketCors or
"event.eventName": DeleteBucketLifecycle or "event.eventName":
DeleteBucketEncryption or "event.eventName": DeleteBucketReplication) |
select bucket, count(1) as cnt
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for OSS bucket policy changes.

1. Logon to SLS Console.

2. Click **Log Service Audit Service** in the navigation pane.
3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.
   b. Check the **Action Trail** and configure a proper days.
   c. Click **Save** to save the changes.
4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query.

```
"event.eventName": PutBucketLifecycle or "event.eventName": PutBucketPolicy
or "event.eventName": PutBucketCors or "event.eventName": PutBucketEncryption
or "event.eventName": PutBucketReplication or "event.eventName":
DeleteBucketPolicy or "event.eventName": DeleteBucketCors or
"event.eventName": DeleteBucketLifecycle or "event.eventName":
DeleteBucketEncryption or "event.eventName": DeleteBucketReplication) |
select bucket, count(1) as cnt
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

2.22 Ensure a log monitoring and alerts are set up for security group changes (Manual)

Profile Applicability:

- Level 2

Description:

Real-time monitoring of API calls can be achieved by directing ActionTrail Logs to Log Service and establishing corresponding query and alarms. Security Groups are a stateful packet filter that controls ingress and egress traffic within a VPC. It is recommended that a query and alarm be established changes to Security Groups.

Rationale:

Monitoring changes to security group will help ensure that resources and services are not unintentionally exposed.

Audit:

Perform the following steps to ensure log monitoring and alerts are set for security group changes.

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane to go to the **Log Service Audit Service** page.
3. Ensure the **Action Trail** are **Enabled** under the **Access to Cloud Products > Global Configuration** page, and click **Central Project**.
4. Select **Alerts**.
5. Ensure below alert rule has been enabled and saved in the target actiontrail_log

```
(event name: CreateSecurityGroup or event name: AuthorizeSecurityGroup or
event_name: AuthorizeSecurityGroupEgress or event_name: RevokeSecurityGroup
or event_name: RevokeSecurityGroupEgress or event_name: JoinSecurityGroup or
event_name: LeaveSecurityGroup or event_name: DeleteSecurityGroup or
event_name: ModifySecurityGroupPolicy) | select count(1) as cnt
```

Remediation:

Perform the following to ensure the log monitoring and alerts are set up for security group changes。

1. Logon to SLS Console.
2. Click **Log Service Audit Service** in the navigation pane.

3. Go to **Access to Cloud Products > Global Configuration** page.
   a. Select a location of project for logs.
   b. Check the **Action Trail** and configure a proper days.
   c. Click **Save** to save the changes.
4. Go to **Access to Cloud Products > Global Configurations** click **Central Project**.
5. Select **Log Management > Actiontrail Log**.
6. In the search/analytics console, input below query.

```
(event_name: CreateSecurityGroup or event_name: AuthorizeSecurityGroup or
event_name: AuthorizeSecurityGroupEgress or event_name: RevokeSecurityGroup
or event_name: RevokeSecurityGroupEgress or event_name: JoinSecurityGroup or
event_name: LeaveSecurityGroup or event_name: DeleteSecurityGroup or
event_name: ModifySecurityGroupPolicy) | select count(1) as cnt
```

7. Create a dashboard and set alert for the query result.

Default Value:

The monitoring dashboard and alert is not set by default.

References:

1. https://www.alibabacloud.com/help/en/doc-detail/91784.htm

CIS Controls:

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership

Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

2.23 Ensure that Logstore data retention period is set 365 days or greater (Manual)

Profile Applicability:

- Level 2

Description:

Ensure Activity Log Retention is set for 365 days or greater

Rationale:

Logstore life cycle controls how your activity log is exported and retained. It is recommended to retain your activity log for 365 days or more in order to have time to respond to any incidents.

Audit:

Perform below steps to ensure the log retention is set to 365 days or greater.

1. Logon to SLS Console.
2. In the **Projects** section, click the target project name. On the page that appears, click the plus sign (**+**) next to the search box.
3. In the dialog box that appears, check whether the **Permanent Storage** is turned on, which means the log data will be stored permanently, or else
4. Ensure the **Data Retention Period** is set to 365 or greater.

Remediation:

Perform below steps to ensure the log retention is set to 365 days or greater.

1. Logon to SLS Console.
2. Find the project in the **Projects** section, and then click the target project name.
3. On the page that appears, click **Modify a Logstore** icon next to the Logstore, and then choose **Modif**y.
4. On the page that appears, click **Modify**, modify the **Data Retention Period**, to 365 or greater and then click **Save**.

Default Value:

The Permanent Storage is turned off by default.

References:

1. https://www.alibabacloud.com/help/doc-detail/48990.htm

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

3 Networking

This section covers recommendations addressing networking on Alibaba Cloud.

3.1 Ensure legacy networks does not exist (Manual)

Profile Applicability:

- Level 1

Description:

In order to prevent use of legacy networks, ECS instances should not have a legacy network configured.

Rationale:

Legacy networks have a single network IPv4 prefix range and a single gateway IP address for the whole network. With legacy networks, you cannot create subnetworks or switch from legacy to auto or custom subnet networks. Legacy networks can thus have an impact for high network traffic ECS instance and subject to the single point of failure.

Audit:

1. Logon to ECS Console
2. In the left-side navigation pane, choose **Instance & Image** > **Instances**.
3. Check all ECS instances to ensure the **Network Type** is not **classic**

Remediation:

1. Logon to ECS Console
2. In the left-side navigation pane, choose **Instance & Image** > **Instances**.
3. Click **Create Instance**.
4. Specify the basic instance information required by following the instruction and click **Next: Networking**.
5. Select the **Network Type** of **VPC**.

Default Value:

By default the ECS are create with VPC Network Type.

References:

1. https://www.alibabacloud.com/help/doc-detail/87190.htm

CIS Controls:

Version 7

11.1 Maintain Standard Security Configurations for Network Devices

Maintain standard, documented security configuration standards for all authorized network devices.

3.2 Ensure that SSH access is restricted from the internet (Manual)

Profile Applicability:

- Level 2

Description:

Security groups provide stateful filtering of ingress/egress network traffic to Alibaba Cloud resources. It is recommended that no security group allows unrestricted ingress access to port 22 or port 3389.

Rationale:

Removing unfettered connectivity to remote console services, such as SSH or RDP, reduces a server's exposure to risk.

Impact:

All SSH or RDP connections from outside of the network to the concerned VPC(s) will be blocked. There could be a business need where ssh access is required from outside of the network to access resources associated with the VPC. In that case, specific source IP(s) should be mentioned in firewall rules to white-list access to SSH or RDP port for the concerned VPC(s).

Audit:

1. Logon to ECS Console
2. In the left-side navigation pane, choose **Network & Security > Security Groups**.
3. Ensure **Port** is not equal to **22** or **3389** and Action is not Allow.
4. Ensure **IP Ranges** is not equal to **0.0.0.0** under Source filters.

Remediation:

1. Logon to ECS Console
2. Go to **Security Group**
3. Find the **Security Group** you want to modify
4. Modify **Source IP** range to **specific IP**
5. **Save**

Default Value:

SSH connection is allowed by default.

References:

1. https://www.alibabacloud.com/help/doc-detail/25475.htm
2. https://www.alibabacloud.com/help/doc-detail/100380.htm

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

12.4 Deny Communication over Unauthorized Ports

Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

3.3 Ensure VPC flow logging is enabled in all VPCs (Manual)

Profile Applicability:

- Level 2

Description:

You can use the flow log function to monitor the IP traffic information for an ENI, a VSwitch or a VPC. If you create a flow log for a VSwitch or a VPC, all the Elastic Network Interfaces, including the newly created Elastic Network Interfaces, are monitored. Such flow log data is stored in Log Service, where you can view and analyze IP traffic information. It is recommended that VPC Flow Logs be enabled for packet "Rejects" for VPCs.

Rationale:

VPC Flow Logs provide visibility into network traffic that traverses the VPC and can be used to detect anomalous traffic or insight during security workflows.

Impact:

Currently, the flow log function is available for free. However, corresponding storage and indexing fees associated with the use of Log Service are billed. Before you activate the flow log function, note the following: • The object where a flow log is created can only be ENI. • Only the following resource types support the creation of flow logs: VPC, VSwitch, and ENI. • The maximum number of flow log instances that can be created in each region is 10. If you need to create more flow log instances, open a ticket.

Audit:

1. Logon to VPC console.
2. In the left-side navigation pane, click **FlowLog**.
3. Check for every existing VPC to ensure that there is an associated **VPC ID** on the **FlowLog** tab.

Remediation:

1. Logon to VPC console.
2. In the left-side navigation pane, click **FlowLog**.
3. Follow the instruction to create **FlowLog** for each of your VPCs

Default Value:

By default, Flow Logs is not enabled when you create a new VPC

References:

1. https://www.alibabacloud.com/help/doc-detail/90628.html

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

12.5 Configure Monitoring Systems to Record Network Packets

Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.

3.4 Ensure routing tables for VPC peering are "least access" (Manual)

Profile Applicability:

- Level 2

Description:

Once a VPC peering connection is established, routing tables must be updated to establish any connections between the peered VPCs. These routes can be as specific as desired, even peering a VPC to only a single host on the other side of the connection.

Rationale:

Although the routing table is empty by default upon creation for any newly created routing table, hence it denies any default access, it is recommended that the table entry is only added based on the least access principle. Being highly selective in peering routing tables is a very effective way of minimizing the impact of breach as resources outside of these routes are inaccessible to the peered VPC.

Audit:

1. Logon to VPC console.
2. Open the **routing table**
3. Review **routing tables of peered VPCs** for whether they route all subnets of each VPC and whether that is necessary to accomplish the intended purposes for peering the VPCs.

Remediation:

1. Logon to VPC console.
2. Open the **routing table**
3. Remove and add **route table** entries to ensure that **the least number of subnets or hosts** as is required to accomplish the purpose for peering are routable.

References:

1. https://www.alibabacloud.com/help/doc-detail/97766.htm

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
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.

3.5 Ensure the security group are configured with fine grained rules (Manual)

Profile Applicability:

- Level 2

Description:

Security groups provide stateful filtering of ingress/egress network traffic to Alibaba Cloud resources. It is recommended that all security group configured with fine grained rules.

Rationale:

Configure fine grained security group rules is a very effective way of minimizing the impact of breach as resources outside of these rules are inaccessible to the ECS instance.

Audit:

1. Logon to ECS Console.
2. In the left-side navigation pane, choose **Network & Security > Security Groups**.
3. Ensure the rules in each of your security groups are all necessary for your operation.

Remediation:

1. Logon to ECS Console.
2. In the left-side navigation pane, choose **Network & Security > Security Groups**.
3. Remove any unnecessary rules in all security groups.

References:

1. https://www.alibabacloud.com/help/doc-detail/25475.htm

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

12.4 Deny Communication over Unauthorized Ports
Deny communication over unauthorized TCP or UDP ports or application traffic to

ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

4 Virtual Machines

This section covers recommendations addressing virtual machines on Alibaba Cloud.

4.1 Ensure that 'Unattached disks' are encrypted (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that unattached disks in a subscription are encrypted.

Rationale:

Cloud disk encryption protects your data at rest. The cloud disk data encryption feature automatically encrypts data when data is transferred from ECS instances to disks, and decrypts data when the data is read from disks.

Audit:

1. Logon to ECS Console
2. In the left pane, click to **expand Storage and Snapshots**, click **Disks**
3. Select each **Disk**
4. Ensure that each disk has **Disks Encryption** has **Encryption** checked with the value of **key tag** is **true**

Remediation:

1. Logon to ECS Console
2. In the left-side navigation pane, choose **Storage & Snapshots > Disk**.
3. In the upper-right corner of the **Disks** page, click **Create Disk**.
4. In the **Disk** section, check the **Disk Encryption** box and then select a key from the drop-down list.

Default Value:

By default, data disks are not encrypted.

References:

1. https://www.alibabacloud.com/help/doc-detail/59643.htm

Additional Information:

After a data disk is created, you can only encrypt the data disk by manually copying data on the unencrypted disk to a new encrypted disk. The disk encryption status cannot be directly converted from unencrypted to encrypted.

CIS Controls:

Version 7

14.8 Encrypt Sensitive Information at Rest

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.

4.2 Ensure that 'Virtual Machine's disk' are encrypted (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that disk are encrypted when it is created with the creation of VM instance.

Rationale:

ECS cloud disk encryption protects your data at rest. The cloud disk data encryption feature automatically encrypts data when data is transferred from ECS instances to disks, and decrypts data when the data is read from disks.

Audit:

1. Logon to ECS Console
2. In the left pane, click to expand **Storage and Snapshots**, click **Disks**
3. Select each **Data disk**
4. Ensure that each **disk** under **Data disks** has encryption

Remediation:

Encrypt a system disk when copying an image in the ECS console by following the below steps:

1. Logon to ECS Console
2. In the left-side navigation pane, choose **Instances & Images > Instances**
3. In the top navigation bar, select a region.
4. On the **Images** page, click the **Custom Image** tab.
5. Select the target image and click copy **Image** in the **Actions** column.
6. In the **Copy Image** dialog box, check the **Encrypt** box and then select a key from the drop-down list.
7. Click **OK**.

You can encrypt a data disk when creating an instance by following the below steps:

1. Logon to ECS Console
2. In the left-side navigation pane, choose **Instances & Images > Instances**
3. On the **Instances** page, click **Create Instance**
4. On the **Basic Configurations** page, find the **Storage** section and perform the following steps
   a) Click **Add Disk**

b) Specify the disk category and capacity of data disk
c) Select **Disk Encryption** and then select a key from the drop-down list.

Default Value:

Not checked

References:

1. https://www.alibabacloud.com/help/doc-detail/59643.htm

Additional Information:

You cannot directly convert unencrypted disks to encrypted disks. You can encrypt system disks only when you are copying the custom images. You can encrypt the data disk by manually creating an encrypted data disk and then copy the data on unencrypted disk to the new encrypted disk.

CIS Controls:

Version 7

14.8 Encrypt Sensitive Information at Rest
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.

4.3 Ensure no security groups allow ingress from 0.0.0.0/0 to port 22 (Manual)

Profile Applicability:

- Level 1

Description:

Security groups provide stateful filtering of ingress/egress network traffic to Alibaba Cloud resources. It is recommended that no security group allows unrestricted ingress access to port 22.

Rationale:

Rationale: Removing unfettered connectivity to remote console services, such as SSH, reduces a server's exposure to risk.

Impact:

For valid operation needs, such as updating an existing environment, care should be taken to ensure that administrators currently relying on an existing ingress from 0.0.0.0/0 have access to ports 22 through another security group.

Audit:

1. Logon to ECS Console .
2. In the left pane, click to **expand Network and Security**, click **Security Groups**
3. For each **security group**, perform the following:
4. Select the **security group**
5. Click **Add Rules**
6. Click the **Inbound tab**
7. Ensure **no rule** exists that has **a port range** that includes **port 22** and has an **Authorization Object of 0.0.0.0/0**

Note: A Port value of ALL or a port range such as 0-1024 also includes port 22.

Remediation:

1. Logon to ECS Console .
2. In the left pane, click to expand **Network** and **Security**, click **Security Groups**
3. For each **security group**, perform the following:
   a)Select the **security group**
   b)Click **Add Rules**

c)Click the **Inbound tab**
d)Identify **the rules** to be removed
f)Click **Delete** in the **Remove column**
g)Click **OK**

Default Value:

By default, Authorization Object and port range are not set.

References:

1. https://www.alibabacloud.com/help/doc-detail/51170.htm

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.4 Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389 (Manual)

Profile Applicability:

- Level 1

Description:

Security groups provide filtering of ingress/egress network traffic to Aliyun resources. It is recommended that no security group allows unrestricted ingress access to port 3389.

Rationale:

Removing unfettered connectivity to remote console services, such as RDP, reduces a server's exposure to risk.

Impact:

For valid operation needs, such as updating an existing environment, care should be taken to ensure that administrators currently relying on an existing ingress from 0.0.0.0/0 have access to ports 3389 through another security group.

Audit:

1. Logon to ECS Console .
2. In the left pane, click to expand **Network** and **Security**, click **Security Groups**
3. For each **security group**, perform the following:
4. Select the **security group**
5. Click **Add Rules**
6. Click the **Inbound tab**
7. Ensure no rule exists that has a port range that includes **port 3389** and has an **Authorization Object of 0.0.0.0/0**

Note: A Port value of ALL or a port range such as 0-1024 also includes port 3389.

Remediation:

1. Logon to ECS Console .
2. In the left pane, click to expand **Network** and **Security**, click **Security Groups**

For each **security group**, perform the following:

1. Select the **security group**

2. Click **Add Rules**
3. Click the **Inbound tab**
4. Identify the rules **to be removed**
5. Click **Delete** in the Remove column
6. Click **OK**

Default Value:

By default, Authorization Object and port range are not set.

References:

1. https://www.alibabacloud.com/help/doc-detail/51170.htm

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.5 Ensure that the latest OS Patches for all Virtual Machines are applied (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that the latest OS patches for all virtual machines are applied.

Rationale:

Windows and Linux virtual machines should be kept updated to: • Address a specific bug or flaw • Improve an OS or application's general stability • Fix a security vulnerability The Alibaba Cloud Security Center checks for the latest updates in Linux and Windows systems. If an ECS instance is missing a system update, the Security Center will recommend system updates be applied.

Audit:

Through the Alibaba Cloud Management Console:

1. Logon to Security Center Console
2. Select **Vulnerabilities**
3. Ensure all vulnerabilities are fixed

Remediation:

Through the Alibaba Cloud Management Console:

1. Logon to Security Center Console
2. Select **Vulnerabilities**
3. Apply all patches for vulnerabilities

Default Value:

By default, patches are not automatically deployed.

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools

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.

4.6 Ensure that the endpoint protection for all Virtual Machines is installed (Manual)

Profile Applicability:

- Level 1

Description:

Install endpoint protection for all virtual machines.

Rationale:

Installing endpoint protection systems (like Security Center for Alibaba Cloud) provides for real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious software attempts to install itself or run on ECS.

Audit:

Through the Alibaba Cloud Management Console:

1. Logon to Security Center Console
2. Select **Overview**
3. Ensure all ECS are installed with Security Center agent

Remediation:

Through the Alibaba Cloud Management Console:

1. Logon to Security Center Console
2. Select **Settings**
3. Click **Agent**
4. On the **Agent** tab, select the virtual machines without Security Center agent installed
5. Click **Install**

Default Value:

Not installed

CIS Controls:

Version 7

8.2 Ensure Anti-Malware Software and Signatures are Updated

Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

5 Storage

This section covers recommendations addressing storage on Alibaba Cloud.

5.1 Ensure that OSS bucket is not anonymously or publicly accessible (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended that the access policy on OSS bucket does not allows anonymous and/or public access.

Rationale:

Allowing anonymous and/or public access grants permissions to anyone to access bucket content. Such access might not be desired if you are storing any sensitive data. Hence, ensure that anonymous and/or public access to a bucket is not allowed.

Impact:

Customers may set ACL to public due to the business needs.

Audit:

The anonymous or public access to OSS bucket can be restricted through both Bucket Access Control List (ACL) and Bucket Policy.
Using the Bucket ACL:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Basic Setting` in top middle of the console
4. Under ACL section, ensure the Bucket ACL is set to `Private.

Using Bucket Policy:

1. Logon to OSS console.
2. Click `Bucket`, and then click the name of target bucket.
3. Click the `Files` tab. On the page that appears, click `Authorize`.
4. In the Authorize dialog box that appears, click `Authorize`.
5. In the Authorize dialog box that appears, ensure the `Anonymous Accounts (*)` is selected under `Accounts` and `None` is selected under `Authorized Operation`.

Remediation:

The anonymous or public access to OSS bucket can be restricted through both Bucket ACL and Bucket Policy.

Using the Bucket ACL:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Basic Setting` in top middle of the console
4. Under ACL section, click on `configure`
5. Click `Private`
6. Click `Save`

Using Bucket Policy:

1. Logon to OSS console.
2. Click `Bucket`, and then click the name of target bucket.
3. Click the `Files` tab. On the page that appears, click `Authorize`.
4. In the Authorize dialog box that appears, click `Authorize`.
5. In the Authorize dialog box that appears, choose the `Anonymous Accounts (*)` for Accounts and choose `None for` Authorized Operation`.
6. Click `OK`.

Default Value:

Private

References:

1. https://www.alibabacloud.com/help/doc-detail/31896.htm

Additional Information:

To implement access restrictions on buckets, configuring Bucket Policy is a preferred way than configuring Bucket ACL considering the general access control rules on Alibaba Cloud as below:

1. If the access control is configured through both Bucket Policy and Bucket ACL, the ultimate access control effect is the combination of the “allowed” policy configured through Bucket Policy and Bucket ACL. For example, if the public read is selected under Bucket ACL and certain RAM account is configured as allowed to read and write under Bucket Policy, the ultimate access allowed is to allow public read and write by certain RAM account.
2. If there is any conflict between the configuration of Bucket Policy and Bucket ACL, “Deny” rules prevails. For example, if the public read is selected under Bucket ACL

and certain RAM account is configured as configured as None for Authorized Operation under Bucket Policy, the ultimate access allow the public ready except those RAM accounts configured as “Deny” through Authorized Operation.

CIS Controls:

Version 7

12.4 Deny Communication over Unauthorized Ports

Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

16 Account Monitoring and Control

Account Monitoring and Control

5.2 Ensure that there are no publicly accessible objects in storage buckets (Manual)

Profile Applicability:

- Level 1

Description:

It is recommended that storage object ACL should not grant public access.

Rationale:

Allowing public access to objects allows anyone with an internet connection to access sensitive data that is important to your business. Also note that even if a bucket ACL applied on storage does not allow public access, there could be object specific ACLs that allows public access to the specific access to the specific objects inside the buckets. Hence it is important to check object ACLs at individual object level.

Impact:

Customers may set ACL to public due to the business needs.

Audit:

Through the Management Console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Files` in top middle of the console
4. Click on `View details` in the right column on a target object
5. Ensure File ACL is set to `private`

Remediation:

Through the Management Console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Files` in top middle of the console
4. Hover on `More` in the right column on a target object
5. Click `Set ACL`
6. Click `Private`
7. Click `Save`

Default Value:

By Default, object ACLs is inherited from corresponding bucket ACL.

References:

1. https://www.alibabacloud.com/help/doc-detail/31909.htm

CIS Controls:

Version 7

12.4 Deny Communication over Unauthorized Ports

Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

13 Data Protection

Data Protection

5.3 Ensure that logging is enabled for OSS buckets (Automated)

Profile Applicability:

- Level 1

Description:

OSS Bucket Access Logging generates a log that contains access records for each request made to your OSS bucket. An access log record contains details about the request, such as the request type, the resources specified in the request worked, and the time and date the request was processed. It is recommended that bucket access logging be enabled on the OSS bucket.

Rationale:

By enabling OSS bucket logging on target OSS buckets, it is possible to capture all events which may affect objects within an target buckets. Configuring logs to be placed in a separate bucket allows access to log information which can be useful in security and incident response workflows.

Impact:

Extra cost for log storage may incur.

Audit:

Perform the following ensure the OSS bucket has access logging is enabled:
Through the management console:

1. Logon to the OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Under `Log`, ensure `Enabled` is checked.

Remediation:

Perform the following to enable OSS bucket logging:
Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Under `Log`, click `configure`
4. Configure bucket logging
5. Click the `Enabled` checkbox

6. Select Target Bucket from list
7. Enter a Target Prefix
8. Click `Save`

Default Value:

Logging is disabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/31900.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

5.4 Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1

Description:

Enable the data encryption in transit.

Rationale:

The secure transfer enhances the security of OSS bucket by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access storage accounts, the connection must use HTTPS. Any requests using HTTP will be rejected.

Audit:

Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Files` in top middle of the console
4. Click on `Authorize`
5. Ensure a policy is set to `None (Authorized Operation)` and `http (Conditions:Access Method)`

Remediation:

Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Files` in top middle of the console
4. Click on `Authorize`
5. Click on Whole Bucket,*, None (Authorized Operation) and http (Conditions:Access Method)
6. Click on `Save`

Default Value:

None.

References:

1. https://www.alibabacloud.com/help/doc-detail/85111.htm

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

5.5 Ensure that the shared URL signature expires within an hour (Manual)

Profile Applicability:

- Level 1

Description:

Expire the shared URL signature within an hour.

Rationale:

URL signature is a URL that grants access rights to OSS. You can add signature information to a URL so that you can forward the URL to the third party for authorized access.

A URL signature can be provided to the third party for authorized access. Providing a URL signature to these clients allows them access to a resource for a specified period of time. This time should be set as low as possible, and preferably no longer than an hour.

Audit:

Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click `Files` in top middle of the console
4. Click `View Details` in the right column on a target object
5. Ensure `Validity Period` is set to less than 3600

Remediation:

Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Files` in top middle of the console
4. Click on `View Details` in the right column on a target object
5. Set `Validity Period` to a value less than 3600

Default Value:

300 seconds.

References:

1. https://www.alibabacloud.com/help/doc-detail/31912.htm

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

5.6 Ensure that URL signature is allowed only over https (Manual)

Profile Applicability:

- Level 1

Description:

URL signature should be allowed only over HTTPS protocol.

Rationale:

URL signature is a URL that grants access rights to OSS. You can add signature information to a URL so that you can forward the URL to the third party for authorized access.A URL signature can be provided to the third party for authorized access. It is recommended to allow such access requests over HTTPS protocol only.

Audit:

Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Files` in top middle of the console
4. Click on `View Details` in the right column on a target object
5. Ensure `HTTPS` is set to `Enabled`

Remediation:

Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Files` in top middle of the console
4. Click on `View Details` in the right column on a target object
5. Set `HTTPS` to `Enabled`

Default Value:

Enabled

CIS Controls:

Version 7

16.10 Ensure All Accounts Have An Expiration Date

Ensure that all accounts have an expiration date that is monitored and enforced.

5.7 Ensure network access rule for storage bucket is not set to publicly accessible (Automated)

Profile Applicability:

- Level 2

Description:

Restricting default network access helps to provide a new layer of security, since OSS accept connections from clients on any network. To limit access to selected networks, the default action must be changed.

Rationale:

Audit:

Access can be granted to public internet IP address ranges, to enable connections from specific internet or on-premises clients. When network rules are configured, only applications from allowed networks can access OSS bucket.

Audit:

Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Files` in top middle of the console
4. Click on `Authorize`
5. Ensure a policy is set to be granted to public internet IP address ranges

Remediation:

Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on a target OSS bucket
3. Click on `Files` in top middle of the console
4. Click on `Authorize`
5. Click on Whole Bucket,*,None, Condition IP = specified IP address or IP address segment
6. Click on `Save`

Default Value:

Not set.

References:

1. https://www.alibabacloud.com/help/doc-detail/85111.htm

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

5.8 Ensure server-side encryption is set to 'Encrypt with Service Key' (Manual)

Profile Applicability:

- Level 2

Description:

Enable server-side encryption (Encrypt with Service Key) for objects.

Rationale:

Server-side encryption protects your data at rest.

Impact:

Service key incurs an additional cost from accessing the KMS service.

Audit:

Perform the following to determine if the OSS bucket is configured to use SSE-KMS:
Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on the target OSS bucket
3. Click on `Basic Setting` in top middle of the console
4. Under the Server-side Encryption section, ensure the target OSS Bucket Encryption is set to `KMS` and the Encryption Method of KMS and the service key (alias/acs/oss) is selected.

Remediation:

Through the management console:
Perform the following to configure the OSS bucket to use SSE-KMS:

1. Logon to OSS console.
2. In the bucket-list pane, click on the target OSS bucket
3. Click `Basic Setting` in top middle of the console
4. Under the Server-side Encryption section, click on `configure`
5. Click `KMS` and select KMS service key(alias/acs/oss)

Default Value:

Not encrypted.

References:

1. https://www.alibabacloud.com/help/doc-detail/108880.htm

CIS Controls:

Version 7

13 Data Protection
Data Protection

5.9 Ensure server-side encryption is set to 'Encrypt with BYOK' (Manual)

Profile Applicability:

- Level 2

Description:

Enable server-side encryption (Encrypt with BYOK) for objects.

Rationale:

Server-side encryption protects your data at rest.

Impact:

Service key incurs an additional cost from accessing the KMS service.

Audit:

Perform the following to determine if the OSS bucket is configured to use SSE-KMS:
Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on the target OSS bucket
3. Click on `Basic Setting` in top middle of the console
4. Under the Server-side Encryption section, ensure the target OSS Bucket Encryption is set to KMS and a customer created KMS key ID is specified in the KMS Key Id field.

Remediation:

Perform the following to configure the OSS bucket to use SSE-KMS:
Through the management console:

1. Logon to OSS console.
2. In the bucket-list pane, click on the target OSS bucket
3. Click on `Basic Setting` in top middle of the console
4. Under the Server-side Encryption section, click on `configure`
5. Click on `KMS` and select an existing CMK from the KMS key Id drop-down menu
6. Click `save`

Default Value:

By default, Buckets are not set to be encrypted.

References:

1. https://www.alibabacloud.com/help/doc-detail/108880.htm

CIS Controls:

Version 7

13 Data Protection
Data Protection

6 Relational Database Services

This section covers security recommendations that you should follow to secure relational database services (RDS).

6.1 Ensure that RDS instance requires all incoming connections to use SSL (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to enforce all incoming connections to SQL database instance to use SSL.

Rationale:

SQL database connections if successfully trapped (MITM); can reveal sensitive data like credentials, database queries, query outputs etc. For security, it is recommended to always use SSL encryption when connecting to your instance. This recommendation is applicable for PostgreSQL and MySQL Instances.

Audit:

Through the management console:

1. Logon to RDS Console.
2. Select the region where the target instance is located.
3. Click the ID of the target instance to enter the Basic Information page.
4. In the left-side navigation pane, click `Data Security` to go to the Security page.
5. Click the `SSL Encryption` tab.
6. Check the button `SSL Encryption is Enabled`.

Remediation:

Through the management console:

1. Logon to RDS Console.
2. Select the region where the target instance is located.
3. Click the ID of the target instance to enter the Basic Information page.
4. In the left-side navigation pane, click `Data Security`.
5. Click the `SSL Encryption` tab.
6. Click the switch next to `Disabled` in the `SSL Encryption` parameter.
7. In the Configure SSL dialog box, select the endpoint for which you want to enable SSL encryption and then click `OK`.
8. Click `Download CA Certificate` to download an SSL certificate.
9. The downloaded SSL certificate is a package including the following files:
   p7b file: is used to import the CA certificate on Windows OS.

PEM file: is used to import the CA certificate on other systems or for other applications.
JKS file: is a Java truststore certificate file used for importing CA certificate chains in Java programs. The password is apsaradb.

Default Value:

Encryption is off by default.

References:

1. https://www.alibabacloud.com/help/doc-detail/32474.htm

Additional Information:

You can choose to encrypt the private or public endpoint, but note that you can encrypt only one endpoint.

CIS Controls:

Version 7

13 Data Protection
Data Protection

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

6.2 Ensure that RDS Instances are not open to the world (Automated)

Profile Applicability:

- Level 1

Description:

Database Server should accept connections only from trusted Network(s)/IP(s) and restrict access from the world.

Rationale:

To minimize attack surface on a Database server Instance, only trusted/known and required IP(s) should be white-listed to connect to it. Authorized network should not have IPs/networks configured to 0.0.0.0 or /0 which will allow access to the instance from anywhere in the world.

Audit:

Through the management console:

1. Logon to RDS Console.
2. In the upper left corner, select the region where the target instance is located.
3. Locate the target instance and click its ID.
4. In the left-side navigation pane, click `Data Security` to visit the Security page.
5. On the `Whitelist Settings` tab, check if the authorized servers' IPs have been configured, and it is not configured as 0.0.0.0 or /0.

Note: You can also click Add a Whitelist Group to create a new group.

Remediation:

Through the management console:

1. Logon to RDS Console.
2. In the upper left corner, select the region where the target instance is located.
3. Locate the target instance and click its ID.
4. In the left-side navigation pane, click `Data Security` to visit the Security page.
5. On the `Whitelist Settings` tab page, follow below instructions based on your scenario:

- To access the RDS instance from an ECS instance located within a VPC, click `Edit` for the default VPC whitelist.

- To access the RDS instance from an ECS instance located within a classic network, click `Edit` for the default Classic Network whitelist.
- To access the RDS instance from a server or computer located in a public network, click `Edit` for the default Classic Network whitelist.

6. In the displayed Edit Whitelist dialog box, remove any 0.0.0.0 or /0 entries, and only add the IP addresses that need to access the instance, and then click `OK`.

- If you add an IP address range, such as 10.10.10.0/24, any IP address in 10.10.10.X format can access the RDS instance.
- If you add multiple IP addresses or IP address ranges, separate them with a comma (without spaces), for example, 192.168.0.1,172.16.213.9.
- You can click Add Internal IP Addresses of ECS Instance to display the IP addresses of all the ECS instances under your Alibaba Cloud account and add to the whitelist.

Default Value:

By default, the whitelist setting is '127.0.0.1' that is not allowing any connection from any server.

References:

1. https://www.alibabacloud.com/help/doc-detail/26198.htm

Additional Information:

For RDS instances that is upgraded to IPv6, please use the appropriate IPv6 configuration to ensure the whitelist is not open for all.

CIS Controls:

Version 7

13 Data Protection
Data Protection

14.6 Protect Information through Access Control Lists
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.

6.3 Ensure that 'Auditing' is set to 'On' for applicable database instances (Automated)

Profile Applicability:

- Level 1

Description:

Enable SQL auditing on all RDS except SQL Server 2012/2016/2017 and MariaDB TX.

Rationale:

The Alibaba Cloud allows MySQL instance to be created as a service. Enabling auditing at the server level ensures that all existing and newly created databases on the MySQL instance are audited. Auditing policy applied on the MySQL database does not override auditing policy and settings applied on the particular MySQL server where the database is hosted. Auditing tracks database events and writes them to an audit log in the Alibaba Cloud MySQL account. It also helps to maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.

Impact:

By activating Auditing, the system then automatically starts charging an hourly fee of US$ 0.0018 per GB.

Audit:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID.
4. In the left-side navigation pane, select `SQL Explorer`.
5. Check if there is a “Welcome to Use SQL Explore” page, as such a page indicates that the auditing is not yet enabled. If the auditing is enabled, then the SQL Explorer should show the SQL Explore dashboard directly.

Remediation:

Through the management console:

1. Logon to RDS Console.

2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID.
4. In the left-side navigation pane, select `SQL Explorer`.
5. Click `Activate Now`.
6. Specify the SQL log storage duration (for how long you want to keep the SQL log), and click `Activate`.

Default Value:

Disable

References:

1. https://www.alibabacloud.com/help/doc-detail/96123

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

6.4 Ensure that 'Auditing' Retention is 'greater than 6 months' (Automated)

Profile Applicability:

- Level 1

Description:

Database SQL Audit Retention should be configured to be greater than 90 days.

Rationale:

Audit Logs can be used to check for anomalies and give insight into suspected breaches or misuse of information and access.

Audit:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID.
4. In the left-side navigation pane, select `SQL Explore`.
5. Click `Service Setting` button on the top right corner.
6. In the service setting page, assure the storage duration is set as '6 months' or longer.

Remediation:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID.
4. In the left-side navigation pane, select `SQL Explore`.
5. Click `Service Setting` button on the top right corner.
6. In the service setting page, enable 'Activate SQL Explore', set the storage duration as '6 months' or longer.

Default Value:

Active SQL Explorer is disabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/96123.htm

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data

Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

6.5 Ensure that 'TDE' is set to 'Enabled' on for applicable database instance (Automated)

Profile Applicability:

- Level 1

Description:

Enable Transparent Data Encryption on every RDS instance.

Rationale:

RDS Database transparent data encryption helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and log files at rest without requiring changes to the application.

Audit:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID.
4. In the left-side navigation pane, click `Data Security` to go to the Security page.
5. Click the `TDE` tab.
6. Check the button TDE Status is `Enabled`.

Remediation:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID to enter the Basic Information page.
4. In the left-side navigation pane, click `Data Security` to go to the Security page.
5. Click the `TDE` tab.
6. On the `TDE` tab, find `TDE Status` and click the switch next to `Disabled`.
7. In the displayed dialog box, choose automatically generated key or custom key, click `Confirm`.

- Encrypt a table

a. For RDS for MySQL, connect to the instance and run the following command to encrypt tables.

```
alter table <tablename> engine=innodb, block_format=encrypted
```

b. For RDS for SQL Server, click Configure TDE, select the databases to encrypt, add them to the right, and click OK.

- Decrypt data

a. To decrypt a MySQL table encrypted by TDE, run the following command:

```
alter table <tablename> engine=innodb, block_format=default
```

b. To decrypt a SQL Server table encrypted by TDE, click Configure TDE and move the database to the left.

Default Value:

Disabled

References:

1. https://www.alibabacloud.com/help/doc-detail/33510.html

Additional Information:

SQL Server 2008 R2, SQL Server 2008R2, SQL Server 2012 Enterprise Edition, SQL Server 2016 Enterprise Edition, SQL Server 2017 Enterprise Edition and MySQL 5.6/5.7/8.0 all support TED enablement. You have logged in with an Alibaba Cloud account rather than a RAM user account. KMS shall be activated. If KMS is not yet activated, you will be prompted to activate it when attempting to enable TDE.

CIS Controls:

Version 7

14.8 Encrypt Sensitive Information at Rest

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.

6.6 Ensure RDS instance TDE protector is encrypted with BYOK (Use your own key) (Automated)

Profile Applicability:

- Level 2

Description:

TDE with BYOK support provides increased transparency and control, increased security with an HSM-backed KMS service, and promotion of separation of duties. With TDE, data is encrypted at rest with a symmetric key (called the database encryption key). With BYOK support for TDE, the DEK can be protected with an asymmetric key that is stored in the KMS. Based on business needs or criticality of data, it is recommended that the TDE protector is encrypted by a key that is managed by the data owner (BYOK).

Rationale:

Bring Your Own Key (BYOK) support for Transparent Data Encryption (TDE) allows user control of TDE encryption keys and restricts who can access them and when. Alibaba Cloud KMS, a cloud-based key management system is the service where TDE has integrated support for BYOK. With BYOK, the database encryption key is protected by an asymmetric key stored in the KMS.

Audit:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID.
4. In the left-side navigation pane, click `Data Security` to go to the Security page.
5. Click the `TDE` tab.
6. Check the button `TDE Status` is `Enabled` and a custom key ID is shown for the Key field and the status is Valid.

Remediation:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.

3. Locate the target instance, and click the instance ID to enter the Basic Information page.
4. In the left-side navigation pane, click `Data Security` to go to the Security page.
5. Click the `TDE` tab.
6. On the `TDE` tab, find `TDE Status` and click the switch next to `Disabled`.
7. In the displayed dialog box, choose `custom key`, click `Confirm`.

Default Value:

Disabled

References:

1. https://www.alibabacloud.com/help/doc-detail/96121.htm

CIS Controls:

Version 7

14.8 Encrypt Sensitive Information at Rest

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.

6.7 Ensure parameter 'log_connections' is set to 'ON' for PostgreSQL Database (Automated)

Profile Applicability:

- Level 1

Description:

Enable log_connections on PostgreSQL Servers.

Rationale:

Enabling log_connections helps PostgreSQL Database to log attempted connection to the server, as well as successful completion of client authentication. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

Audit:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID to enter the Basic Information page.
4. In the left-side navigation pane, select `Parameters` and ensure the `log_connection` is set as `On` in the Actual Value column.

Remediation:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID to enter the Basic Information page.
4. In the left-side navigation pane, select `Parameters`.
5. Click the `Edit` icon of `log_connection` parameter next the `Actual Value` column.
6. Enter `On` as the `Actual Value` and click `Confirm`.
7. Click `Apply Change`s.
8. In the message that appears, click `Confirm`.

Default Value:

Off

References:

1. https://www.alibabacloud.com/help/doc-detail/96751.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

6.8 Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable log_disconnections on PostgreSQL Servers.

Rationale:

Enabling log_disconnections helps PostgreSQL Database to log session terminations of the server, as well as duration of the session. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

Audit:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID to enter the Basic Information page.
4. In the left-side navigation pane, select `Parameters` and ensure the `log_disconnections` is set as `On` in the Actual Value column.

Remediation:

Through the management console:

1. Login to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID to enter the Basic Information page.
4. In the left-side navigation pane, select `Parameters`.
5. Click the `Edit` icon of `log_disconnections` parameter next the `Actual Value` column.
6. Enter `On` as the `Actual Value` and click `Confirm`.
7. Click `Apply Changes`.
8. In the message that appears, click `Confirm`.

Default Value:

Off

References:

1. https://www.alibabacloud.com/help/doc-detail/96751.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

6.9 Ensure server parameter 'log_duration is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable log_duration on PostgreSQL Servers.

Rationale:

Enabling log_duration helps PostgreSQL Database to Logs the duration of each completed SQL statement which in turn generates query and error logs. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Audit:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID to enter the Basic Information page.
4. In the left-side navigation pane, select `Parameters` and ensure the `log_durantion` is set as `On` in the Actual Value column.

Remediation:

Through the management console:

1. Logon to RDS Console.
2. In the upper-left corner, select the region of the target instance.
3. Locate the target instance, and click the instance ID to enter the Basic Information page.
4. In the left-side navigation pane, select `Parameters`.
5. Click the `Edit` icon of `log_durantion` parameter next the `Actual Value` column.
6. Enter `On` as the `Actual Value` and click `Confirm`.
7. Click `Apply Changes`.
8. In the message that appears, click `Confirm`.

Default Value:

Off

References:

1. https://www.alibabacloud.com/help/doc-detail/96751.htm

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

7 Kubernetes Engine

This section covers recommendations addressing Kubernetes Engine on Alibaba Cloud.

7.1 Ensure Log Service is set to 'Enabled' on Kubernetes Engine Clusters (Automated)

Profile Applicability:

- Level 1

Description:

Log Service is a complete real-time data logging service on Alibaba Cloud to support collection, shipping, search, storage and analysis for logs. It includes a user interface to call the Log Viewer and an API to management logs pragmatically. Log Service could automatically collect, process, and store your container and audit logs in a dedicated, persistent datastore. Container logs are collected from your containers. Audit logs are collected from the kube-apiserver or the deployed ingress. Events are logs about activity in the cluster, such as the deleting of Pods or Secrets.

Rationale:

By enabling you will have container and system logs, Kubernetes Engine deploys a per-node logging agent that reads container logs, adds helpful metadata, and then stores them. The logging agent would help to collecting the following sources:

• kube-apiserver audit logs

• ingress visiting logs

• Standard output and standard error logs from containerized processes

For events, Kubernetes Engine uses a Deployment in the kube-system namespace which automatically collects events and sends them to Log Service. Log Service is compatible with JSON formats.

Audit:

Through the management console:

1. Logon to ACK console
2. Select the target cluster and click its name into cluster detail page
3. Select `Cluster Auditing` on the left column and check if audit page shown

Remediation:

Through the management console:

1. Logon to ACK console
2. Click `Create Kubernetes Cluster` and set `Enable Log Service` to `Enabled` when creating cluster

Default Value:

By default, logging service is disabled when you create a new cluster using console.

References:

1. https://help.aliyun.com/document_detail/91406.html
2. https://help.aliyun.com/document_detail/86532.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

7.2 Ensure CloudMonitor is set to Enabled on Kubernetes Engine Clusters (Automated)

Profile Applicability:

- Level 1

Description:

The monitoring service in Kubernetes Engine clusters depends on the Alibaba Cloud CloudMonitor agent to access additional system resources and application services in virtual machine instances. The monitor can access metrics about CPU utilization, some disk traffic metrics, network traffic, and disk IO information, which help to monitor signals and build operations in your Kubernetes Engine clusters.

Rationale:

By Enabling CloudMonitor installation you will have system metrics and custom metrics. System metrics are measurements of the cluster's infrastructure, such as CPU or memory usage. For system metrics, a monitor controller would be created and periodically connects to each node and collects metrics about its Pods and containers, then sends the metrics to CloudMonitor server. Metrics for usage of system resources are collected from the CPU, Memory, Evictable memory, Non-evictable memory, and Disk sources.

Audit:

Through the management console:

1. Logon to ACK console
2. Select the target cluster and click its name into cluster detail page
3. Select the Nodes on the left column and click the `Monitor` link on the `Actions` column of the selected node
4. Check if OS Metrics data existing in the CloudMonitor page of the selected ECS node

Remediation:

Through the management console:

1. Logon to ACK console
2. Click the `Create Kubernetes Cluster` button and set `CloudMonitor Agent` to `Enabled` under creation options.

Default Value:

By default, CloudMonitor Agent installation is disenabled when you create a new cluster using console.

References:

1. https://help.aliyun.com/document_detail/125508.html
2. https://help.aliyun.com/document_detail/102337.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

7.3 Ensure role-based access control (RBAC) authorization is Enabled on Kubernetes Engine Clusters (Automated)

Profile Applicability:

- Level 1

Description:

In Kubernetes, authorizers interact by granting a permission if any authorizer grants the permission. The legacy authorizer in Kubernetes Engine grants broad, statically defined permissions. To ensure that RBAC limits permissions correctly, you must disable the legacy authorizer. RBAC has significant security advantages, can help you ensure that users only have access to specific cluster resources within their own namespace and is now stable in Kubernetes.

Rationale:

In Kubernetes, RBAC is used to grant permissions to resources at the cluster and namespace level. RBAC allows you to define roles with rules containing a set of permissions, and the subaccounts who bind the roles could only have the permissions to access the specific resources in the cluster or namespaces defined in RBAC policies.

Audit:

Through the management console:

1. Logon to ACK console
2. Select the target RAM sub-account in the `Clusters` -> `Authorizations` page
3. After RAM user/role is selected, configure the RBAC roles on specific clusters or namespaces

Remediation:

Through the management console:

1. Logon to ACK console
2. Select the target RAM sub-account and configure the RBAC roles on specific clusters or namespaces.

Default Value:

By default, RBAC authorization is enabled on ACK clusters, and the legacy authorizations as ABAC is disenable. Besides, the RAM sub-users have no permissions to access any resources in ACK clusters by default.

References:

1. https://help.aliyun.com/document_detail/87656.html
2. https://help.aliyun.com/document_detail/119596.html

CIS Controls:

Version 7

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

7.4 Ensure Cluster Check triggered at least once per week for Kubernetes Clusters (Automated)

Profile Applicability:

- Level 1

Description:

Kubernetes Engine's cluster check feature helps you verify the system nodes and components healthy status. When you trigger the checking, the process would check on the health state of each node in your cluster and also the cluster configuration as kubelet\docker daemon\kernel and network iptables configuration, if there are fails consecutive health checks, the diagnose would report to admin for further repair.

Rationale:

Kubernetes Engine uses the node's health status to determine if a node needs to be repaired. A node reporting a Ready status is considered healthy. The cluster administrator could choose to trigger the cluster check periodically. An cluster healthy checking including:

• The cloud resource healthy status, including the VPC/VSwitch SLB and every ECS node status in cluster.

• The kubelet, docker daemon, kernel, iptables configurations on every node in cluster.

Kubernetes Engine generates the diagnose report when checking finish. You can check the diagnose suggestion on ACK console.

Audit:

Through the management console:

1. Logon to ACK console
2. Select the target cluster and open the `More` pop-menu for advance options on cluster.
3. Select `Overview` page on left column and check if the `Last check status` is `Normal`.
4. Verify the checking time and details in Global Check.

Remediation:

Through the management console:

1. Logon to ACK console

2. Select the target cluster and open the `More` pop-menu for advance options on cluster
3. Select `Global Check` and click the `Start` button to trigger the checking

Default Value:

By default, the cluster checking process is not auto triggered, the cluster administrator could start it in ACK console.

References:

1. https://help.aliyun.com/document_detail/114882.html

CIS Controls:

Version 7

19 Incident Response and Management
Incident Response and Management

7.5 Ensure Kubernetes web UI / Dashboard is not enabled (Automated)

Profile Applicability:

- Level 1

Description:

Dashboard is a web-based Kubernetes user interface. It can be used to deploy containerized applications to a Kubernetes cluster, troubleshoot your containerized application, and manage the cluster itself along with its attendant resources. You can use Dashboard to get an overview of applications running on your cluster, as well as for creating or modifying individual Kubernetes resources (such as Deployments, Jobs, DaemonSets, etc). For example, you can scale a Deployment, initiate a rolling update, restart a pod or deploy new applications using a deploy wizard.

Rationale:

You should disable the Kubernetes Web UI (Dashboard) when running on Kubernetes Engine. The Kubernetes Web UI (Dashboard) is backed by a highly privileged Kubernetes Service Account. It is recommended to use ACK User Console instead of Dashboard to avoid any privileged escalation via compromise the dashboard.

Audit:

Through the management console:

1. Logon to ACK console
2. Select the target cluster and select the kube-system namespace in the `Namespace` pop-menu
3. Input `dashboard` in the deploy filter bar, and make sure there is no result exist after the filter.

Remediation:

Through the management console:

1. Logon to ACK console
2. Select the target cluster and select the kube-system namespace in the `Namespace` pop-menu
3. Input `dashboard` in the deploy filter bar, make sure there is no result exist after the filter, delete the dashboard deployment by selecting the `Delete` in `More` pop-menu.

Default Value:

By default, the kube-dashboard would not install in cluster, and the overview console use the managed dashboard which controlled by ACK service.

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

7.6 Ensure Basic Authentication is not enabled on Kubernetes Engine Clusters (Automated)

Profile Applicability:

- Level 1

Description:

Basic authentication allows a user to authenticate to the cluster with a username and password and it is stored in plain text without any encryption. Disabling Basic authentication will prevent attacks like brute force. Its recommended to use either client certificate or RAM for authentication.

Rationale:

When disabled, you will still be able to authenticate to the cluster with client certificate or RAM. A client certificate is a base 64-encoded public certificate used by clients to authenticate to the cluster endpoint, and ACK cluster would auto generate the client certificate for each logging RAM user.

Audit:

1. ssh into any master node in cluster
2. Make sure the basic-auth-file not exist in apiserver manifest with below command:

```
cat /etc/kubernetes/manifests/kube-apiserver.yaml | grep basic-auth-file
```

Remediation:

1. ssh into any master node in cluster
2. Make sure the basic-auth-file not exist in apiserver manifest with below command:

```
cat /etc/kubernetes/manifests/kube-apiserver.yaml | grep basic-auth-file
```

3. If you found basic-auth-file existing in apiserver manitfest, please override the manifest file with new manifest content to not include the basic-auth-file and then restart the apiserver, you need repeat the action on all of the master nodes

Default Value:

By default, Basic authentication is not enabled when you create a new cluster.

References:

1. https://help.aliyun.com/document_detail/86494.html
2. https://help.aliyun.com/document_detail/123848.html
3. https://github.com/AliyunContainerService/ack-ram-authenticator

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

7.7 Ensure Network policy is enabled on Kubernetes Engine Clusters (Automated)

Profile Applicability:

- Level 1

Description:

A network policy is a specification of how groups of pods are allowed to communicate with each other and other network endpoints. NetworkPolicy resources use labels to select pods and define rules which specify what traffic is allowed to the selected pods. The Kubernetes Network Policy API allows the cluster administrator to specify what pods are allowed to communicate with each other.

Rationale:

By default, pods are non-isolated; they accept traffic from any source. Pods become isolated by having a NetworkPolicy that selects them. Once there is any NetworkPolicy in a namespace selecting a particular pod, that pod will reject any connections that are not allowed by any NetworkPolicy. (Other pods in the namespace that are not selected by any NetworkPolicy will continue to accept all traffic.)

Audit:

Through the management console:

1. Logon to ACK console
2. Click the `Create Kubernetes Cluster` button and make sure `Terway` is selected in `Network Plugin` option.

Remediation:

Only the Terway network plugin support the Network Policy feature, so please make sure not choose Flannel as network plugin when creating cluster.
Through the management console:

1. Logon to ACK console
2. Click the `Create Kubernetes Cluster` button and select `Terway` in `Network Plugin` option.

Default Value:

By default, Network Policy is disabled when you create a new cluster, and you should choose the Terway as the cluster network plugin when creating the cluster.

References:

1. https://help.aliyun.com/document_detail/97621.html
2. https://help.aliyun.com/document_detail/86949.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

14.1 Segment the Network Based on Sensitivity
Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

7.8 Ensure ENI multiple IP mode support for Kubernetes Cluster (Automated)

Profile Applicability:

- Level 1

Description:

Alibaba Cloud ENI (Elastic Network Interface) has supported assign ranges of internal IP addresses as aliases to a single virtual machine's ENI network interfaces. This is useful if you have lots of services running on a VM and you want to assign each service a different IP address without quota limitation.

Rationale:

With the feature of ENI multiple IP mode, Kubernetes Engine clusters can allocate IP addresses from a CIDR block known to Terway network plugin. This makes your cluster more scalable and allows your cluster to better interact with other Alibaba Cloud products and entities. Using ENI multiple IPs has several benefits:

• Pod IPs are reserved within the network ahead of time, which prevents conflict with other compute resources.

• Firewall controls for Pods can be applied separately from their nodes.

• Alias IPs allow Pods to directly access hosted services without using a NAT gateway.

Audit:

Through the management console:

1. Logon to ACK console
2. Select the target cluster name and go into the cluster detail page
3. Check if the meta of `Network Plugin` in `Cluster` Information is `Terway`

Remediation:

Only the Terway network plugin support the Network Policy feature, so please make sure not choose Flannel as network plugin when creating cluster.
Through the management console:

1. Logon to ACK console

2. Click the `Create Kubernetes Cluster` button and select `Terway` in `Network Plugin` option.

Default Value:

By default, ENI multiple IP mode is not support in Flannel network plugin which is the default plugin when creating the cluster, and you should choose the Terway as the cluster network plugin when creating the cluster.

References:

1. https://github.com/AliyunContainerService/terway/blob/master/README.md#eni-secondary-ip-pod
2. https://help.aliyun.com/document_detail/97467.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

14.1 Segment the Network Based on Sensitivity
Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).

7.9 Ensure Kubernetes Cluster is created with Private cluster enabled (Automated)

Profile Applicability:

- Level 1

Description:

A private cluster is a cluster that makes your master inaccessible from the public internet. In a private cluster, nodes do not have public IP addresses, so your workloads run in an environment that is isolated from the internet. Nodes have addresses only in the private address space. Nodes and masters communicate with each other privately using VPC peering.

Rationale:

With a Private cluster enabled, VPC network peering gives you several advantages over using external IP addresses or VPNs to connect networks, including:

• Network Latency: Public IP networking suffers higher latency than private networking.

• Network Security: Service owners do not need to have their services exposed to the public Internet to reduce any associated risks.

• Network Cost: Alibaba Cloud charges egress bandwidth pricing for networks using external IPs to communicate even if the traffic is within the same zone. If, however, the networks are peered they can use internal IPs to communicate and save on those egress costs. Regular network pricing still applies to all traffic.

Audit:

Through the management console:

1. Logon to ACK console
2. Select the target cluster name and go into the cluster detail page
3. Check if there is no meta of API Server Public Network Endpoint under Cluster Information

Remediation:

Through the management console:

1. Logon to ACK console

2. Click the `Create Kubernetes Cluster` button and make sure `Public Access` is not `enabled`.

Default Value:

By default, public access is not enabled when creating new cluster.

References:

1. https://help.aliyun.com/document_detail/100380.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

8 Security Center

This section covers security recommendations to follow when setting various security policies on an Alibaba Cloud subscription. A security policy defines the set of controls, which are recommended for resources within the specified Alibaba Cloud subscription. Please note that the majority of the recommendations mentioned in this section only produce an alert if a security violation is found. They do not actually enforce security settings by themselves. Alerts should be acted upon and remedied wherever possible.

8.1 Ensure that Security Center is Advanced or Enterprise Edition (Automated)

Profile Applicability:

- Level 2

Description:

The Advanced or Enterprise Edition enables threat detection for network and endpoints, providing malware detection, webshell detection and anomaly detection in Security Center.

Rationale:

The Advanced or Enterprise Edition allows for full protection to defend cloud threats.

Audit:

Through the management console:

1. Logon to Security Center Console
2. Select `Overview`
3. Ensure `Current Edition` is `Advanced` or `Enterprise Edition`

Remediation:

Through the management console:

1. Logon to Security Center Console.
2. Select `Overview`.
3. Click `Upgrade`.
4. Select `Advanced` or `Enterprise Edition`.
5. Finish order placement.

Default Value:

Not installed.

References:

1. https://www.alibabacloud.com/help/product/28498.htm

CIS Controls:

Version 7

3.1 Run Automated Vulnerability Scanning Tools

Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

8.1 Utilize Centrally Managed Anti-malware Software

Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.2 Ensure that all assets are installed with security agent (Automated)

Profile Applicability:

- Level 2

Description:

Enable protection on all endpoints.

Rationale:

The endpoint protection of Security requires an agent to be installed on the endpoint to work. Such an agent-based approach allows the security center to provide a set of more comprehensive endpoint intrusion detection and protection capabilities, such as includes remote logon detection, webshell detection and removal, anomaly detection (detection of abnormal process behaviors and abnormal network connections), and detection of changes in key files and suspicious accounts in systems and applications.

Audit:

Through the management console:

1. Logon to Security Center Console.
2. Select `Overview`.
3. Ensure `Unprotected Assets` is 0.

Remediation:

Through the management console:

1. Logon to Security Center Console.
2. Select `Settings`.
3. Click `Agent`.
4. On Client to be installed tab, select all items on the list.
5. Click `On-click installation` to install the agent all asset.

Default Value:

Not installed.

References:

1. https://www.alibabacloud.com/help/doc-detail/111650.htm

CIS Controls:

Version 7

3.1 Run Automated Vulnerability Scanning Tools

Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

8.1 Utilize Centrally Managed Anti-malware Software

Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.3 Ensure that Automatic Quarantine is enabled (Manual)

Profile Applicability:

- Level 2

Description:

Enable automatic quarantine of virus protection in Security Center.

Rationale:

Once a virus is detected, the automatic quarantine feature prevents the virus from being executed.

Audit:

Through the management console:

1. Logon to Security Center Console.
2. Select `Settings`.
3. Click `General`.
4. Ensure `Virus Blocking` is enabled.

Remediation:

Through the management console:

1. Logon to Security Center Console.
2. Select `Settings`.
3. Click `General`.
4. Enable `Virus Blocking`.

Default Value:

Not enabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/111847.htm

CIS Controls:

Version 7

3.1 Run Automated Vulnerability Scanning Tools

Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

8.1 Utilize Centrally Managed Anti-malware Software

Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

8.4 Ensure that Webshell detection is enabled on all web servers (Manual)

Profile Applicability:

- Level 2

Description:

Enable webshell detection on all web servers to scans periodically the Web directories for detecting webshells on servers.

Rationale:

Web servers are exposed to the Internet and they are commonly attacked through injected webshell by attackers.

Audit:

Through the management console:

1. Logon to Security Center Console.
2. Select `Settings`.
3. Click `General`.
4. Click `Manage` in `Webshell Detection`.
5. Ensure all web servers are included.

Remediation:

Through the management console:

1. Logon to Security Center Console.
2. Select `Settings`.
3. Click `General`.
4. Click `Manage` in `Webshell Detection`.
5. Add all web servers.

Default Value:

Not enabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/111847.htm

CIS Controls:

Version 7

3.1 Run Automated Vulnerability Scanning Tools

Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

8.5 Ensure that notification is enabled on all high risk items (Automated)

Profile Applicability:

- Level 1

Description:

Enable all risk item notification in Vulnerability, Baseline Risks, Alerts and Accesskey Leak event detection categories.

Rationale:

To make sure that relevant security operators would receive notifications as soon as security events happens.

Audit:

Through the management console:

1. Logon to Security Center Console.
2. Select `Settings`.
3. Click `Notification`.
4. Review notification settings and ensure all high-risk items are enabled.

Remediation:

Through the management console:

1. Logon to Security Center Console.
2. Select `Settings`.
3. Click `Notification`.
4. Enable all high-risk items on Notification setting.

Default Value:

Not enabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/111648.htm

CIS Controls:

3.7 Utilize a Risk-rating Process

Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

8.6 Ensure that Config Assessment is granted with privilege (Manual)

Profile Applicability:

- Level 2

Description:

Grant Security Center's Cloud Platform Configuration Assessment the privilege to access other cloud product.

Rationale:

Prior to using Cloud Platform Configuration Assessment, it requires privilege to assess other cloud product's settings.

Audit:

Through the management console:

1. Logon to Security Center Console.
2. Select `Config Assessment`.
3. Ensure that the prompt of asking privilege is not shown.

Remediation:

Through the management console:

1. Logon to Security Center Console.
2. Select `Config Assessment`.
3. Click `Authorize`.

Default Value:

No privilege is authorized by default.

References:

1. https://www.alibabacloud.com/help/doc-detail/42302.htm

CIS Controls:

Version 7

3.3 Protect Dedicated Assessment Accounts

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.

8.7 Ensure that scheduled vulnerability scan is enabled on all servers (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that scheduled vulnerability scan is enabled on all servers.

Rationale:

Be sure that vulnerability scan is performed periodically to discover system vulnerabilities in time.

Audit:

1. Logon to Security Center Console.
2. Select Vulnerabilities.
3. Click Settings.
4. Ensure that all type of vulnerabilities is enabled.
5. Ensure that High and Medium vulnerabilities scan level are enabled.

Remediation:

1. Login to Security Center Console.
2. Select Vulnerabilities.
3. Click Settings.
4. Apply all type of vulnerabilities.
5. Enable High and Medium vulnerabilities scan level.

Default Value:

Not enabled.

References:

1. https://www.alibabacloud.com/help/doc-detail/109076.htm

CIS Controls:

Version 7

3.6 Compare Back-to-back Vulnerability Scans

Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

8.8 Ensure that Asset Fingerprint automatically collects asset fingerprint data (Manual)

Profile Applicability:

- Level 2

Description:

The Enterprise Edition enables asset fingerprint collection for endpoints providing a collection of port, software, processes, scheduled tasks and middleware in Security Center.

Rationale:

The Enterprise Edition allows for enhanced investigation collection of artifacts to identify root cause in a more timely manner of single or multiple server instances hosted within the cloud.

Audit:

Through the management console:

1. Logon to Security Center Console
2. Select `Investigation` > `Asset Fingerprints`
3. Click `Settings`
4. Ensure the Refresh Frequencies are all set to Collected once a day

Remediation:

Through the management console:

1. Logon to Security Center Console
2. Select `Investigation`> `Asset Fingerprints`
3. Click `Setting` and set the Refresh Frequencies
4. Set refresh frequency Automatic collection to Collected once a day

Default Value:

Not Enabled

References:

1. https://www.alibabacloud.com/help/doc-detail/146565.htm

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Identity and Access Management**		
1.1	Avoid the use of the "root" account (Manual)	☐	☐
1.2	Ensure no root account access key exists (Manual)	☐	☐
1.3	Ensure MFA is enabled for the "root" account (Manual)	☐	☐
1.4	Ensure that multi-factor authentication is enabled for all RAM users that have a console password (Automated)	☐	☐
1.5	Ensure users not logged on for 90 days or longer are disabled for console logon (Automated)	☐	☐
1.6	Ensure access keys are rotated every 90 days or less (Automated)	☐	☐
1.7	Ensure RAM password policy requires at least one uppercase letter (Automated)	☐	☐
1.8	Ensure RAM password policy requires at least one lowercase letter (Automated)	☐	☐
1.9	Ensure RAM password policy require at least one symbol (Automated)	☐	☐
1.10	Ensure RAM password policy require at least one number (Automated)	☐	☐
1.11	Ensure RAM password policy requires minimum length of 14 or greater (Automated)	☐	☐
1.12	Ensure RAM password policy prevents password reuse (Automated)	☐	☐
1.13	Ensure RAM password policy expires passwords within 90 days or less (Automated)	☐	☐
1.14	Ensure RAM password policy temporarily blocks logon after 5 incorrect logon attempts within an hour (Automated)	☐	☐
1.15	Ensure RAM policies that allow full "*:*" administrative privileges are not created (Automated)	☐	☐
1.16	Ensure RAM policies are attached only to groups or roles (Automated)	☐	☐
2	**Logging and Monitoring**		
2.1	Ensure that ActionTrail are configured to export copies of all Log entries (Automated)	☐	☐
2.2	Ensure the OSS used to store ActionTrail logs is not publicly accessible (Automated)	☐	☐
2.3	Ensure audit logs for multiple cloud resources are integrated with Log Service (Manual)	☐	☐

2.4	Ensure Log Service is enabled for Container Service for Kubernetes (Manual)	☐	☐
2.5	Ensure virtual network flow log service is enabled (Manual)	☐	☐
2.6	Ensure Anti-DDoS access and security log service is enabled (Manual)	☐	☐
2.7	Ensure Web Application Firewall access and security log service is enabled (Manual)	☐	☐
2.8	Ensure Cloud Firewall access and security log analysis is enabled (Manual)	☐	☐
2.9	Ensure Security Center Network, Host and Security log analysis is enabled (Manual)	☐	☐
2.10	Ensure log monitoring and alerts are set up for RAM Role changes (Manual)	☐	☐
2.11	Ensure log monitoring and alerts are set up for Cloud Firewall changes (Manual)	☐	☐
2.12	Ensure log monitoring and alerts are set up for VPC network route changes (Manual)	☐	☐
2.13	Ensure log monitoring and alerts are set up for VPC changes (Manual)	☐	☐
2.14	Ensure log monitoring and alerts are set up for OSS permission changes (Manual)	☐	☐
2.15	Ensure log monitoring and alerts are set up for RDS instance configuration changes (Manual)	☐	☐
2.16	Ensure a log monitoring and alerts are set up for unauthorized API calls (Manual)	☐	☐
2.17	Ensure a log monitoring and alerts are set up for Management Console sign-in without MFA (Manual)	☐	☐
2.18	Ensure a log monitoring and alerts are set up for usage of "root" account (Manual)	☐	☐
2.19	Ensure a log monitoring and alerts are set up for Management Console authentication failures (Manual)	☐	☐
2.20	Ensure a log monitoring and alerts are set up for disabling or deletion of customer created CMKs (Manual)	☐	☐
2.21	Ensure a log monitoring and alerts are set up for OSS bucket policy changes (Manual)	☐	☐
2.22	Ensure a log monitoring and alerts are set up for security group changes (Manual)	☐	☐
2.23	Ensure that Logstore data retention period is set 365 days or greater (Manual)	☐	☐
3	**Networking**		
3.1	Ensure legacy networks does not exist (Manual)	☐	☐
3.2	Ensure that SSH access is restricted from the internet (Manual)	☐	☐
3.3	Ensure VPC flow logging is enabled in all VPCs (Manual)	☐	☐

3.4	Ensure routing tables for VPC peering are "least access" (Manual)	☐	☐
3.5	Ensure the security group are configured with fine grained rules (Manual)	☐	☐
4	**Virtual Machines**		
4.1	Ensure that 'Unattached disks' are encrypted (Manual)	☐	☐
4.2	Ensure that 'Virtual Machine's disk' are encrypted (Manual)	☐	☐
4.3	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22 (Manual)	☐	☐
4.4	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389 (Manual)	☐	☐
4.5	Ensure that the latest OS Patches for all Virtual Machines are applied (Manual)	☐	☐
4.6	Ensure that the endpoint protection for all Virtual Machines is installed (Manual)	☐	☐
5	**Storage**		
5.1	Ensure that OSS bucket is not anonymously or publicly accessible (Automated)	☐	☐
5.2	Ensure that there are no publicly accessible objects in storage buckets (Manual)	☐	☐
5.3	Ensure that logging is enabled for OSS buckets (Automated)	☐	☐
5.4	Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)	☐	☐
5.5	Ensure that the shared URL signature expires within an hour (Manual)	☐	☐
5.6	Ensure that URL signature is allowed only over https (Manual)	☐	☐
5.7	Ensure network access rule for storage bucket is not set to publicly accessible (Automated)	☐	☐
5.8	Ensure server-side encryption is set to 'Encrypt with Service Key' (Manual)	☐	☐
5.9	Ensure server-side encryption is set to 'Encrypt with BYOK' (Manual)	☐	☐
6	**Relational Database Services**		
6.1	Ensure that RDS instance requires all incoming connections to use SSL (Automated)	☐	☐
6.2	Ensure that RDS Instances are not open to the world (Automated)	☐	☐
6.3	Ensure that 'Auditing' is set to 'On' for applicable database instances (Automated)	☐	☐
6.4	Ensure that 'Auditing' Retention is 'greater than 6 months' (Automated)	☐	☐
6.5	Ensure that 'TDE' is set to 'Enabled' on for applicable database instance (Automated)	☐	☐

6.6	Ensure RDS instance TDE protector is encrypted with BYOK (Use your own key) (Automated)	☐	☐
6.7	Ensure parameter 'log_connections' is set to 'ON' for PostgreSQL Database (Automated)	☐	☐
6.8	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated)	☐	☐
6.9	Ensure server parameter 'log_duration is set to 'ON' for PostgreSQL Database Server (Automated)	☐	☐
7	**Kubernetes Engine**		
7.1	Ensure Log Service is set to 'Enabled' on Kubernetes Engine Clusters (Automated)	☐	☐
7.2	Ensure CloudMonitor is set to Enabled on Kubernetes Engine Clusters (Automated)	☐	☐
7.3	Ensure role-based access control (RBAC) authorization is Enabled on Kubernetes Engine Clusters (Automated)	☐	☐
7.4	Ensure Cluster Check triggered at least once per week for Kubernetes Clusters (Automated)	☐	☐
7.5	Ensure Kubernetes web UI / Dashboard is not enabled (Automated)	☐	☐
7.6	Ensure Basic Authentication is not enabled on Kubernetes Engine Clusters (Automated)	☐	☐
7.7	Ensure Network policy is enabled on Kubernetes Engine Clusters (Automated)	☐	☐
7.8	Ensure ENI multiple IP mode support for Kubernetes Cluster (Automated)	☐	☐
7.9	Ensure Kubernetes Cluster is created with Private cluster enabled (Automated)	☐	☐
8	**Security Center**		
8.1	Ensure that Security Center is Advanced or Enterprise Edition (Automated)	☐	☐
8.2	Ensure that all assets are installed with security agent (Automated)	☐	☐
8.3	Ensure that Automatic Quarantine is enabled (Manual)	☐	☐
8.4	Ensure that Webshell detection is enabled on all web servers (Manual)	☐	☐
8.5	Ensure that notification is enabled on all high risk items (Automated)	☐	☐
8.6	Ensure that Config Assessment is granted with privilege (Manual)	☐	☐
8.7	Ensure that scheduled vulnerability scan is enabled on all servers (Automated)	☐	☐
8.8	Ensure that Asset Fingerprint automatically collects asset fingerprint data (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Dec 11, 2020	1.0.0	Document Created