CIS Benchmarks

CIS IBM Cloud Foundations Benchmark

v1.0.0 - 11-12-2020

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

Terms of Use 1

Overview 7

Intended Audience 7

Consensus Guidance 7

Typographical Conventions 8

Assessment Status 8

Profile Definitions 9

Acknowledgements 10

Recommendations 11

1 IAM 11

1.1 Monitor account owner for frequent, unexpected, or unauthorized logins (Manual) 12

1.2 Ensure API keys unused for 180 days are detected and optionally disabled (Manual) 15

1.3 Ensure API keys are rotated every 90 days (Manual) 17

1.4 Restrict user API key creation and service ID creation in the account via IAM roles (Manual) 19

1.5 Ensure no owner account API key exists (Manual) 21

1.6 Ensure compliance with IBM Cloud password requirements (Manual) 23

1.7 Ensure multi-factor authentication (MFA) is enabled for all users in account (Manual) 25

1.8 Ensure multi-factor authentication (MFA) is enabled for the account owner (Manual) 27

1.9 Ensure multi-factor authentication (MFA) is enabled at the account level (Manual) 29

1.10 Ensure contact email is valid (Manual) 31

1.11 Ensure contact phone number is valid (Manual) 33

1.12 Ensure IAM users are members of access groups and IAM policies are assigned only to access groups (Manual) 35

1.13 Ensure a support access group has been created to manage incidents with IBM Support (Manual) 37

1.14 Minimize the number of users with admin privileges in the account (Manual) 39

1.15 Minimize the number of Service IDs with admin privileges in the account (Manual) 41

1.16 Ensure IAM does not allow public access to Cloud Object Storage (Manual) 43

1.17 Ensure Inactive User Accounts are Suspend (Manual) 46

1.18 Enable audit logging for IBM Cloud Identity and Access Management (Manual) 48

1.19 Ensure Identity Federation is set up with a Corporate IDP (Manual) 50

2 Storage 52

2.1 Cloud Object Storage 52

2.1.1 Cloud Object Storage Encryption 53

2.1.1.1 Ensure Cloud Object Storage encryption is done with customer managed keys (Manual) 54

2.1.1.2 Ensure Cloud Object Storage Encryption is set to On with BYOK (Manual) 56

2.1.1.3 Ensure Cloud Object Storage Encryption is set to On with KYOK (Manual) 59

2.1.2 Ensure network access for Cloud Object Storage is restricted to specific IP range (Manual) 62

2.1.3 Ensure network access for Cloud Object Storage is set to be exposed only on Private end-points (Manual) 64

2.1.4 Ensure Cloud Object Storage bucket access is restricted by using IAM and S3 access control (Manual) 66

2.1.5 Disable public (anonymous) access to IBM Cloud Object Storage buckets (Manual) 69

2.2 File Block Storage 71

2.2.1 Cloud Block Storage Encryption 72

2.2.1.1 Ensure Block Storage is encrypted with customer managed keys (Manual) 73

2.2.1.2 Ensure Block Storage is encrypted with BYOK (Manual) 75

2.2.1.3 Ensure Block Storage is encrypted with KYOK (Manual) 77

2.2.2 Ensure 'OS disk' are encrypted with Customer managed keys (Manual) 79

2.2.3 Ensure 'Data disks' are encrypted with customer managed keys (Manual). 81

2.2.4 Ensure 'Unattached disks' are encrypted with customer managed keys (Manual) 83

3 Maintenance, Monitoring and Analysis of Audit Logs 85

3.1 Ensure auditing is configured in the IBM Cloud account (Manual) 86

3.2 Ensure that archiving is enabled for audit events (Manual) 92

3.3 Ensure that events are collected and processed to identify anomalies or abnormal events (Manual) 98

3.4 Ensure alerts are defined on custom views to notify of unauthorized requests, critical account actions, and high-impact operations in your account (Manual).108

3.5 Ensure the account owner can login only from a list of authorized countries/IP ranges (Manual) 113

3.6 Ensure Activity Tracker data is encrypted at rest (Manual)........115

3.7 Ensure Activity Tracker trails are integrated with LogDNA Logs (Manual) ..117

4 IBM Cloud Databases Family........122

4.1 Ensure IBM Cloud Databases disk encryption is enabled with customer managed keys (Manual) 123

4.2 Ensure IBM Cloud Databases are only accessible via HTTPS or TLS Connections (Manual)........126

4.3 Ensure network access to IBM Cloud Databases service is set to be exposed on “Private end points only” (Manual) 128

4.4 Ensure IBM Cloud Databases disk encryption is set to On (Manual)........131

5 Cloudant........133

5.1 Ensure Cloudant encryption is set to On (Automated)........134

5.2 Ensure IBM Cloudant encryption is enabled with customer managed keys (Manual) 136

5.3 Ensure IBM Cloudant is only accessible via HTTPS or TLS Connections (Automated)........141

6 Networking 143

6.1 IBM Cloud Internet Services........143

6.1.1 Enable TLS 1.2 at minimum for all inbound traffic on IBM Cloud Internet Services Proxy (Manual) 144

6.1.2 Ensure Web application firewall is set to ON in IBM Cloud Internet Services (CIS) (Manual) 147

6.1.3 Ensure DDoS protection is Active on IBM Cloud Internet Services (Manual) 151

6.2 IBM Virtual Private Cloud (VPC) 155

6.2.1 Ensure no VPC access control lists allow ingress from 0.0.0.0/0 to port 22 (Manual) 156

6.2.2 Ensure the default security group of every VPC restricts all traffic (Manual) 158

6.2.3 Ensure no VPC security groups allow ingress from 0.0.0.0/0 to port 3389 (Manual) 160

6.2.4 Ensure no VPC security groups allow ingress from 0.0.0.0/0 to port 22 (Manual) 162

6.2.5 Ensure no VPC access control lists allow ingress from 0.0.0.0/0 to port 3389 (Manual) 164

7 Containers 166

7.1 IBM Kubernetes Service 166

7.1.1 Use a Key Management Service (KMS) provider to encrypt data in Kubernetes secrets 167

7.1.1.1 Ensure Kubernetes secrets data is encrypted with bring your own key (BYOK) (Manual) 168

7.1.1.2 Ensure Kubernetes secrets data is encrypted with keep your own key (KYOK) (Manual) 172

7.1.2 Ensure TLS 1.2 for all inbound traffic at IBM Cloud Kubernetes Service Ingress (Automated) 177

7.1.3 Ensure IBM Cloud Kubernetes Service worker nodes are updated to the latest image to ensure patching of vulnerabilities (Automated) 180

7.1.4 Ensure that clusters are accessible only by using private endpoints (Automated) 183

7.1.5 Ensure IBM Cloud Kubernetes Service cluster has image pull secrets enabled (Automated) 186

7.1.6 Ensure IBM Cloud Kubernetes Service clusters have the monitoring service enabled (Automated) 188

7.1.7 Ensure IBM Cloud Kubernetes Service clusters have the logging service enabled (Automated) 192

7.2 Container Registry 196

7.2.1 Block deployments of vulnerable images to Kubernetes clusters (Automated) 197

8 Key Management 200

8.1 IBM Key Protect for IBM Cloud 200

8.1.1 Ensure IBM Key Protect has automated rotation for customer managed keys enabled (Automated) 201

8.1.2 Ensure the IBM Key Protect service has high availability (Manual) 207

9 Security and Compliance 209

9.1 Ensure alerts are enabled for vulnerabilities discovered in container images in Container Registry (Automated) 210

10 IBM Cloud Certificate Manager 213

10.1 Ensure certificates generated through IBM Cloud Certificate Manager are automatically renewed before expiration (Automated) 214

Appendix: Summary Table 216

Appendix: Change History 220

Overview

This security configuration Benchmark covers foundational elements of IBM Cloud. The recommendations detailed here are important security considerations when designing your infrastructure on IBM Cloud Services.
To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at BenchmarkInfo@cisecurity.org.

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 on the IBM Cloud Platform.

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

Editor
Zeeshan Khan
Maria Luisa Lopez de Silanes Ruiz
Shaun Kelley
JOSHUA MINTZ
Michael Breslin
Neil Taylor
Nikhil Gupta
Alex Parker
Ben Lopez
Shawn Authement
Luis Casco-Arias
Patricia Casey
Kayla McDonald
Janet Van
Alex Greer
Venky Nerkunam

Recommendations

1 IAM

IAM enables you to securely authenticate users for platform services and control access to resources consistently across IBM Cloud. A set of IBM Cloud services is enabled to use IBM Cloud IAM for access control, and are organized into resource groups within your account so you can give users access quickly to more than one resource at a time. Each of these services is labeled as "IAM-enabled" in the catalog. You can use IAM access policies to assign users and service IDs access to resources within your account. And, you can group users and service IDs into an access group to easily give all members of the group the same level of access.

1.1 Monitor account owner for frequent, unexpected, or unauthorized logins (Manual)

Profile Applicability:

- Level 1

Description:

Monitor login activity of the account owner to prevent unauthorized usage of the privileged account.

Rationale:

The owner of an IBM Cloud account by default has administrative privileges across the account.

To prevent unauthorized or unintended usage, login credentials should never be shared and users in an organization should be granted least privilege to complete their required tasks.

To manage the account, administrators are granted permissions to manage services and Cloud resources. Therefore, access by the account owner to the account to run tasks should be minimum. By controlling the number of times that the account owner logs in to the account, you can:

- Monitor owner's access to the IBM Cloud account
- Identify abnormal behavior
- Enforce that administrators and operators of the services in your Cloud account are the ones managing the Cloud resources with their controlled and limited permissions.

When a user log in to the account, a security login event in generated. The event reports who has logged in successfully in the account. You can use these security events to monitor the number of times that the account owner has logged in to the account, and generate an alert if the number exceeds a threshold that you set in a period of time that you specify.

Monitoring login activity of the account owner can help prevent unauthorized or unintended actions taken in the account.

Audit:

Before you can monitor and manage IAM event data with IBM Cloud Activity Tracker with LogDNA, you must provision an instance of the service in IBM Cloud in the Frankfurt (eu-

de) region.
To provision an IBM Cloud Activity Tracker with LogDNA instance in a Public Cloud region, consider the following information:

- You must select the service plan that is associated with the instance, and the plan that determines the retention period for your events.
- You can choose from 7, 14, or 30-day retention periods.
  Alternatively, IBM Cloud Activity Tracker with LogDNA offers a Lite plan that you can use to view your events as they pass through the system. You can view events by using event tailing. You can also design filters to prepare for upgrading to a longer retention period plan. This plan has a 0-day retention period.

Complete the following steps to launch the Activity Tracker with LogDNA web UI:

1. Log in to your IBM Cloud account. After you log in with your user ID and password, the IBM Cloud dashboard opens.
2. Click the **Menu icon > Observability**.
3. Select **Activity Tracker**. The list of *IBM Cloud Activity Tracker with LogDNA* instances is displayed.
4. Select the instance in the region where you want to view events. Then, click **View LogDNA**.

The IBM Cloud Activity Tracker with LogDNA web UI opens and shows the Everything view. Through this view, you can see the events in your account for the region that you have selected.
To ensure the owner of the account has not logged in more than # times the past 24 hours, complete the following steps:
First, you need to identify the email of the account owner.

1. In the Cloud UI, go to **Manage > Access (IAM)**, then select **Users**.
2. Identify the user that has the tag *owner*.
3. Select the account owner. Then, click **Details**.
4. Copy the email address of the account owner.

Second, launch the Activity Tracker instance in Frankfurt. This is the instance where login security events are collected in the account.
In the *Views* section, look for a view that monitors the account owner login attempts. The search query should be set to: `(action login) AND initiator.name:<email address>`, where is the account owner's email address.
Then, check that the view has configured an alert and 1 or more notification channels.

Remediation:

Complete the following steps to monitor how many times an account owner logs in to the account:
First, you need to identify the email of the account owner.

1. In the Cloud UI, go to **Manage > Access (IAM)**, then select **Users**.
2. Identify the user that has the tag *owner*.
3. Select the account owner. Then, click **Details**.
4. Copy the email address of the account owner.

Launch the Activity Tracker instance in Frankfurt. This is the instance where login security events are collected in the account. In the *Views* section, select the **Everything** view. Then, enter the following query in the search bar: `(action login) AND initiator.name:<email address>`. Replace with the account owner's email address.
The view now reports all the login actions that are reported for the account owner.
Next, you can define an alert on the view to get a notification when N number of events are received within a 24 hour period. The value of N depends on how you operate your cloud. You can start with a default value of 25 and increase or decrease depending on the tasks that the account administrator cam perform in the account.

Default Value:

no default value.

References:

1. https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=Activity-Tracker-with-LogDNA-at_events_iam

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

16.13 Alert on Account Login Behavior Deviation
Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

1.2 Ensure API keys unused for 180 days are detected and optionally disabled (Manual)

Profile Applicability:

- Level 1

Description:

Monitor API key usage in your account and search for API keys that are unused or used infrequently.

Rationale:

If an API key is unused for long period in your account, it must be disabled (locked) as a security best practice. All API keys, even those that are used infrequently, must be rotated periodically.

Impact:

To reduce the likelihood of accidental exposure or leaking, monitoring for infrequently used API keys can indicate that an API key can be locked and even deleted, if there is no anticipated future usage.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Go to the Menu icon. Then, select **Observability** to access the *Observability* dashboard.
3. Select **Activity Tracker** from the page navigation menu
4. Check for instances of *IBM Cloud Activity Tracker with LogDNA*
5. Generate events and configure a view in Activity Tracker with LogDNA, see https://cloud.ibm.com/docs/services/Activity-Tracker-with-LogDNA?topic=logdnaat-tutorial_iam_apikeys#tutorial_iam_apikeys_step2

API:N/A

Remediation:

You must create an instance of the Activity Tracker with LogDNA service in the Frankfurt region to start tracking IAM events. Use a minimum of a 7-day event search.

Default Value:

By default, API key monitoring with Activity Tracker with LogDNA is not enabled.

References:

1. https://cloud.ibm.com/docs/services/Activity-Tracker-with-LogDNA?topic=logdnaat-tutorial_iam_apikeys
2. https://cloud.ibm.com/docs/services/Activity-Tracker-with-LogDNA?topic=logdnaat-at_events_iam#at_events_iam_apikeys

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.3 Ensure API keys are rotated every 90 days (Manual)

Profile Applicability:

- Level 1

Description:

Replace production API keys with new API keys regularly, every 90 days for example, as a best practice to secure your account.

Rationale:

API key rotation can help reduce the impact to your organization if an API key becomes exposed or compromised. If you suspect that a key might have been leaked or compromised, the key must be rotated out of production and deleted.

Impact:

Any resource that is using an API key that has been rotated out of production will encounter errors until the API key has been updated.

Audit:

Console:
To find out when an API key was created, complete the following steps:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access(IAM) > API keys**.
3. Identify an API key and from the **Actions** menu, select **Details**.
4. View the date the API key was created.

API:N/A

Remediation:

To create new API key, complete the following steps:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access (IAM) > API keys**.
3. Click **Create an IBM Cloud API key**.
   To rotate an API key, replace an old API key anywhere it is used with the newly created API key.

Delete an old API key:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access (IAM) > API keys**.
3. Identify the API key you want to delete, and from the Actions menu, select **Delete**.

Default Value:

By default, an API key rotation mechanism is not enabled. API key rotation is a manual process

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-userapikey

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.4 Restrict user API key creation and service ID creation in the account via IAM roles (Manual)

Profile Applicability:

- Level 1

Description:

Use IAM settings to restrict user API key creation and service ID (and related API key) creation in the account. Enable both settings to restrict all users in the account from creating user API keys and service IDs except those with an IAM policy that explicitly allows it.

Rationale:

API keys allow access to an IBM Cloud account. The API key inherits all assigned access for the user or service identity for which it is created, and the access is not limited to just the account where the API key is created because it inherits any policies assigned to the user. So, if the identity has access to resources from multiple accounts, then the API key inherits the access from all accounts. Therefore, it is possible that a user's API key can be used to generate a token and access resources that a user has access to outside of the account where the API key was created.

In order to prevent the creation of unauthorized API keys and service IDs, it is recommended that only users with a need for this action be given the privilege to do so.

Impact:

This process involves two IAM controls. Enabling the restriction of user API keys will prevent users in an account from creating user API keys, except those with an explicit IAM policy to do so. Enabling the restriction of service ID creation will prevent users in an account from creating service IDs, except those with an explicit IAM policy to do so.

Audit:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click Manage -> Access (IAM).
3. Click Settings.
4. In the Account section of the Settings page, ensure that Restrict API key creation and Restrict service ID creation are enabled.

Remediation:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click Manage -> Access (IAM).
3. Click Settings.
4. In the Account section of the Settings page, ensure that Restrict API key creation and Restrict service ID creation are enabled.
5. Once enabled, only users with the correct IAM policies will be able to create user API keys and service IDs.

Default Value:

By default, user API key creation and service ID creation are not restricted.

References:

1. https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=Activity-Tracker-with-LogDNA-at_events_iam#at_events_iam_apikeys
2. https://cloud.ibm.com/docs/account?topic=account-userapikey

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.5 Ensure no owner account API key exists (Manual)

Profile Applicability:

- Level 1

Description:

API keys by definition allow access to your account and resources in your account. The API key inherits all assigned access for the user identity for which it is created, therefore an API key created by an account owner has account-owner level access to resources in the account.

Rationale:

In accordance with the practice of granting least privilege, API keys should not be created by an account owner because of the level of privilege automatically granted to account-owner created API keys.

Impact:

The API key inherits all assigned access for the user identity for which it is created, therefore an API key created by an account owner has account-owner level access to resources in the account.

Audit:

To check for the existence of an API key created by the account owner, complete the following steps.

1. Login as the account owner at cloud.ibm.com
2. Click Manage -> Access (IAM)
3. Click API keys
4. Check for any API keys that appear under the "My IBM Cloud API keys" view

Remediation:

To delete an API key, complete the following steps:

1. Login as the account owner at cloud.ibm.com
2. In the console, go to Manage -> Access (IAM)
3. Click on API keys
4. Identify the row of the API key that you want to delete and select Delete from the Actions List of actions icon menu (found on the right hand side of the row).

5. Then, confirm the deletion by clicking Delete.

Default Value:

By default, there are no account-owner API keys created in an account.

References:

1. https://cloud.ibm.com/docs/account?topic=account-userapikey

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.6 Ensure compliance with IBM Cloud password requirements (Manual)

Profile Applicability:

- Level 1

Description:

A strong password is a very important step towards account security and safety. Passwords should never be shared with anyone, and must follow the strong password requirements as follow.

- Password must contain at least one uppercase letter
- Password must contain at least one lowercase letter
- Password must contain at least one number
- Password must contain at least 8 characters
- Passwords should not be reused
- Password must only contain ASCII characters
- Password cannot contain: spaces, or any of these characters- `;:{"?)<>
- Ensure the usage of a password meter which coaches user to create a stronger password than the minimum

Rationale:

A strong password can help prevent unauthorized access to an IBM Cloud account.

Impact:

IBM Cloud automatically prevents the usage of any passwords that do not meet password requirements, when the users are created in IBMid system. When enterprises integrate through enterprise federation (using SAML), then enterprise identity system is responsible for enforcing password strength.

Audit:

IBM Cloud automatically prevents the usage of passwords that do not meet password requirements, when the users are created in IBMid system. When enterprises integrate through enterprise federation (using SAML), then enterprise identity system is responsible for enforcing password strength.

Remediation:

IBM Cloud automatically prevents the usage of any passwords that do not meet password requirements, when the users are created in IBMid system. When enterprises integrate through enterprise federation (using SAML), then enterprise identity system is responsible for enforcing password strength.

Default Value:

By default, all passwords associated with users in IBMid system must meet these requirements. When enterprises integrate with IBM Cloud through enterprise federation (using SAML), then enterprise identity system is responsible for enforcing password strength.

References:

1. https://cloud.ibm.com/docs/account?topic=account-ts_logintoibm

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.7 Ensure multi-factor authentication (MFA) is enabled for all users in account (Manual)

Profile Applicability:

- Level 1

Description:

Requires users to provide multiple factors of login credentials to authenticate their identity and gain access to IBM Cloud resources.

Rationale:

Multifactor authentication (MFA) adds an additional layer of security to an account by requiring users to provide an additional login credential. This requirement helps protect accounts from stolen, phished, or weak password exploits.

Impact:

Depending on the administrator's selection, users might be required to provide an additional authentication factor prior to gaining access to IBM Cloud resources. API keys for users and service IDs continue to work after MFA is enabled.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access (IAM)**.
3. Click **Settings > Account login**.
4. Verify *Multifactor authentication* does not say *None*

API:N/A

Remediation:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access (IAM)**.
3. Click **Settings > Account login**.
4. Click **Edit** for the Account login setting.
5. Select *None*, *Non-federated users only*, or *All users* depending on which type of authentication you want to require.

6. Select the checkbox to confirm that you understand the impact of requiring MFA for users in your account, if you select the non-federated users only option.
7. Click **Update**.

Default Value:

By default, MFA is disabled.

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-enablemfa

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.8 Ensure multi-factor authentication (MFA) is enabled for the account owner (Manual)

Profile Applicability:

- Level 1

Description:

Requires account owner to provide multiple factors of login credentials to authenticate their identity and gain access to IBM Cloud resources.

Rationale:

Multifactor authentication (MFA) adds an additional layer of security to an account by requiring users to provide an additional login credential. This requirement helps protect accounts from stolen, phished, or weak password exploits.

Impact:

Depending on the administrator's selection, users might be required to provide an additional authentication factor prior to gaining access to IBM Cloud resources. API keys for users and service IDs continue to work after MFA is enabled.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access (IAM)**.
3. Click **Settings > Account login**.
4. Verify *Multifactor authentication* does not say *None*.

API:N/A

Remediation:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access (IAM)**.
3. Click **Settings > Account login**.
4. Click **Edit** for the Account login setting.
5. Select *None*, *Non-federated users only*, or *All users* depending on which type of authentication you want to require.

6. Select the checkbox to confirm that you understand the impact of requiring MFA for users in your account, if you select the non-federated users only option.
7. Click **Update**.

Default Value:

By default, MFA is disabled.

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-enablemfa

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.9 Ensure multi-factor authentication (MFA) is enabled at the account level (Manual)

Profile Applicability:

- Level 1

Description:

Requires users to provide multiple factors of login credentials to authenticate their identity and gain access to IBM Cloud resources.

Rationale:

Multifactor authentication (MFA) adds an additional layer of security to an account by requiring users to provide an additional login credential. This requirement helps protect accounts from stolen, phished, or weak password exploits.

Impact:

Depending on the administrator's selection, users might be required to provide an additional authentication factor prior to gaining access to IBM Cloud resources. API keys for users and service IDs continue to work after MFA is enabled.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access (IAM)**.
3. Click **Settings > Account login**.
4. Verify *Multifactor authentication* does not say *None*

API:N/A

Remediation:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access (IAM)**.
3. Click **Settings > Account login**.
4. Click **Edit** for the Account login setting.
5. Select *None*, *Non-federated users only*, or *All users* depending on which type of authentication you want to require.

6. Select the checkbox to confirm that you understand the impact of requiring MFA for users in your account, if you select the non-federated users only option.
7. Click **Update**.

Default Value:

By default, MFA is disabled.

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-enablemfa

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.10 Ensure contact email is valid (Manual)

Profile Applicability:

- Level 1

Description:

In order to receive emails and account alerts related to an IBM Cloud account, a valid email address should always be on record with IBM Cloud. If you lose access to an email address, you should update your email address on record to ensure continuity of correspondence.

Rationale:

Maintaining a valid email address on record is important to make sure you receive important account related information.

Impact:

Maintaining a valid email address on record allows you to receive correspondence from IBM Cloud about your account.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Avatar icon > Profile**.
3. Verify the *Email* field in the *Contact information* section contains your correct email address.

Remediation:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Avatar icon > Profile**.
3. Click the **Edit** link in the *Contact information* section
4. Update your email to the correct email address.

Default Value:

By default, the email address on record is provided during account creation.

References:

1. https://cloud.ibm.com/docs/account?topic=account-usersettings

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.11 Ensure contact phone number is valid (Manual)

Profile Applicability:

- Level 1

Description:

A valid phone number should be on record with IBM Cloud in the event that IBM needs to contact you regarding your IBM Cloud account.

Rationale:

Maintaining a valid phone number on record is important to make sure you receive important account related information.

Impact:

Maintaining a valid phone number on record allows you to receive phone calls from IBM Cloud about your account when necessary.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Avatar icon > Profile**.
3. Verify the *Primary phone number* and *Alternate phone number* fields in the *Contact information* section contain your correct phone numbers.

Remediation:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Avatar icon > Profile**.
3. Click the **Edit** link in the *Contact information* section
4. Update your Primary and Alternate phone numbers.

Default Value:

By default, there is no phone number on record.

References:

1. https://cloud.ibm.com/docs/account?topic=account-usersettings

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.12 Ensure IAM users are members of access groups and IAM policies are assigned only to access groups (Manual)

Profile Applicability:

- Level 1

Description:

Simplify and secure the access management process by using access groups when you assign access to groups of users with identical access needs.

Rationale:

You can create an access group so that you can organize a set of users and service IDs into a single entity that makes it easy for you to assign access. You can assign a single policy to the group instead of assigning the same access multiple times for each individual user or service ID.

Impact:

Using access groups reduces the number of policies that must be created and managed in the account and simplifies the process of adding new users or service IDs or modifying user and service IDs access.

Audit:

Console:
Audit user access policies:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access (IAM)**.
3. Click **Users** and select a user by clicking on the username.
4. Click **Access Policies**.
   ***If the user has individual access policies and you wish to remove them, complete the following steps.
5. Locate the row containing the access policy you wish to remove. Click the actions icon corresponding to that row and click Remove.

API:N/A

Remediation:

Assign an access policy to an Access Group:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access(IAM)**.
3. Click **Access Groups**.
4. Click an Access Group name, then click the **Access Policies** tab
5. Click **Assign access**.

Add members to an Access Group:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access(IAM)**.
3. Click **Access Groups**.
4. Click an Access Group name.
5. Click **Add Users**.

Delete an access policy for a user:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menubar, click **Manage > Access(IAM)**.
3. Click Users.
4. Click on a user name.
5. Click the Access Policies tab
6. Locate the row containing the access policy you wish to remove. Click the actions icon corresponding to that row and click Remove.

Default Value:

By default, only the Public Access Group is enabled in IBM Cloud accounts.

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-groups#groups

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.13 Ensure a support access group has been created to manage incidents with IBM Support (Manual)

Profile Applicability:

- Level 1

Description:

If you experience problems with IBM Cloud®, you can use support cases to get help with technical, access (IAM), billing & usage, and invoice or sales inquiry issues. You can create and manage a support case by using the Support Center. Access to Support Center is governed via IAM roles. In order to access Support Center, a user must have viewer or higher on the Support Center service. To create or edit service cases, a user must have editor or higher on the Support Center service. After you submit a support case, the support team investigates the issue based on your type of support plan.

The types of available support depends on the support level of the account. Your support plan also determines the severity level that you can assign to support cases. For more information, see Case severity and response time.

Rationale:

Support cases are used to raise issues to IBM Cloud. Access to IBM Cloud Support Center is managed via IAM roles. IAM roles can be used to efficiently control which users in an organization can view support cases, which can view, edit, and delete support cases, and which have no access at all. You can configure different levels of Support Center access using Access Groups.

Impact:

Users with access to IBM Cloud Support Center can create and/or manage support tickets based on their IAM role. Support Center access should be managed and assigned using Access Groups.

Audit:

1. In the IBM Cloud console, go to **Manage > Access (IAM)**, and then select **Access Groups**.
2. Look for an access group relating to Support Center. Access Group names are customizable and vary from customer to customer.
3. To verify the access policies for an Access Group, click on an Access Group name and then click **Access policies**.

4. Check for access policies on the Support Center service.

Remediation:

1. In the IBM Cloud console, go to **Manage > Access (IAM)**, and then select **Access Groups**.
2. Select **Create Access Group**.
3. Give the Access Group a descriptive name, for example, Support Center Viewers or Support Center Admins.
4. Optionally, provide a brief description.
5. Click **Create**.
6. Once the Access Group is created, click on the *Access Policies* tab.
7. Click **Assign Access**.
8. Click on **Account Management** and select *Support Center* from the drop down menu.
9. Select the Support Center role(s) that meet your use case. Descriptions are provided for each role in the IAM UI.
10. Click **add**.
11. Click **Assign**.
12. Click on the *Users* tab.
13. Click **Add users**
14. Select users from the list and click **Add to group**.

Default Value:

By default, users do not have access to IBM Cloud Support Center.

References:

1. https://cloud.ibm.com/docs/get-support?topic=get-support-access

CIS Controls:

Version 7

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

1.14 Minimize the number of users with admin privileges in the account (Manual)

Profile Applicability:

- Level 1

Description:

Comply with the principle of granting least privilege by using Access Groups to manage admin privileges and by avoiding the use of broadly scoped access policies.

Rationale:

The principle of granting least privilege mandates that a user must only be given access to the resources that are required to complete their task. This task can be hard to maintain when managing large numbers of users. Instead of assigning administrative privileges to individual users, create Access Groups with administrative privileges and add or remove users from these Access Groups as needed. Additionally, instead of using the Platform Administrator role for all IAM-enabled services, IBM Cloud users can grant access to specific resources and account management services to better comply with the principle of granting least privilege.

Impact:

Managing administrative access via Access Groups simplifies the process of adding/removing admin privileges from users in the account. Having too many users with Administrative privileges goes against the principle of granting least privileges and mean many possible holes for any security attack.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access(IAM)**.
3. Click **Users** and select an User by clicking on the User name.
4. Click on the **Access Policies** tab.
5. View the access policies assigned to the User to verify if that User has Administrator Role assigned.
6. Verify that not too many such users with Administrative privileges exist

API: N/A

Remediation:

To remove excessive number of Users with Administrative privileges, follow the following steps.

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access(IAM)**.
3. Click **Users** and select an User by clicking on the User name.
4. Click on the **Access Policies** tab.
5. View the access policies assigned to the User to verify if that User has Administrator Role assigned.
6. If there are many such users with Administrative privileges, select to remove the Administrative privilege or Remove that User from the list of users.

API: N/A

Default Value:

By default, there are no administrator Access Groups in the account.

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-userroles

CIS Controls:

Version 7

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

1.15 Minimize the number of Service IDs with admin privileges in the account (Manual)

Profile Applicability:

- Level 1

Description:

Comply with the principle of granting least privilege by using Access Groups to manage admin privileges and by avoiding the use of many Service IDs with Administrative Privileges.

Rationale:

The principle of granting least privilege mandates that a Service ID must only be given access to the resources that are required to complete their task. This task can be hard to maintain when managing large numbers of users. Instead of assigning administrative privileges to individual Service ID, create Access Groups with administrative privileges and add or remove Service IDs from these Access Groups as needed. Additionally, instead of using the Platform Administrator role for all IAM-enabled services, IBM Cloud users can grant access to specific resources and account management services to better comply with the principle of granting least privilege.

Impact:

Managing administrative access via Access Groups simplifies the process of adding/removing admin privileges from users in the account. Having too many Service IDs with Administrative privileges goes against the principle of granting least privileges and mean many possible holes for any security attack.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access(IAM)**.
3. Click **Service IDs** and select a Service ID by clicking on the Service ID name.
4. Click on the **Access Policies** tab.
5. View the access policies assigned to the Service ID to verify if that Service ID has Administrator Role assigned.
6. Verify that not too many such Service IDs with Administrative privileges exist

API: N/A

Remediation:

To remove excessive number of Users with Administrative privileges, follow the following steps.

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access(IAM)**.
3. Click **Service IDs** and select a Service ID by clicking on the Service ID name.
4. Click on the **Access Policies** tab.
5. View the access policies assigned to the User to verify if that Service ID has Administrator Role assigned.
6. If there are many such Service IDs with Administrative privileges, select to remove the Administrative privilege or Remove that Service ID from the list of Service IDs.

API: N/A

Default Value:

By default, there are no administrator Access Groups in the account.

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-userroles

CIS Controls:

Version 7

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

1.16 Ensure IAM does not allow public access to Cloud Object Storage (Manual)

Profile Applicability:

- Level 1

Description:

IBM Cloud features the capability for users with specific access roles to create access policies that allow all users (authenticated and non-authenticated) to access resources in the account. This “all users” access in turn ends up in public (including non-authenticated) access to resources. Determine if this capability is required by your organization and disable if not required.

Rationale:

Some customer use cases require that certain files or data are made available for all users to access, both authenticated and non-authenticated. Even if the public access setting is enabled, resources in your account are not publicly accessible unless an administrator level user has explicitly created a policy to create public access for a resource. As a best practice, if this capability is not required by your organization, it must be disabled to prevent unintentional misuse.

Impact:

If the public access setting is enabled in the account, an administrator level user can create access policies to make resources publicly accessible. Resources are not publicly accessible unless an administrator creates an access policy, regardless of setting.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click Manage > Access (IAM).
3. Click Settings.
4. In the public access section of IAM Settings, observe the Public access group setting.
5. If the Public access group setting is disabled, IAM is not providing public access to COS.
6. If the Public access group setting is enabled, proceed to the Access groups page by clicking Access Groups.

7. From the list of Access Groups, select Public Access by clicking on the Access Group name.
8. Ensure that there are no access policies present for COS in the list of access policies.

Remediation:

Console:
To disable the Public Access Group:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access (IAM)**.
3. Click **Settings > Public Access**.
4. Disable Public Access to disable the Public Access Group.

To keep the Public Access Group enabled and verify that no access policies for COS exist:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click Manage > Access (IAM).
3. Click Settings.
4. In the public access section of IAM Settings, observe the Public access group setting.
5. If the Public access group setting is disabled, IAM is not providing public access to COS.
6. If the Public access group setting is enabled, proceed to the Access groups page by clicking Access Groups.
7. From the list of Access Groups, select Public Access by clicking on the Access Group name.
8. Ensure that there are no access policies present for COS in the list of access policies.
9. To delete an access policy, click on the action menu icon for the access policy and click Remove.

API:
https://cloud.ibm.com/docs/iam?topic=iam-public#disable-public-api

Default Value:

By default, the public access group is enabled and there is no public access allowed to COS.

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-public

CIS Controls:

Version 7

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

1.17 Ensure Inactive User Accounts are Suspend (Manual)

Profile Applicability:

- Level 1

Description:

Revoke access privileges for users in an IBM Cloud account that are inactive, typically defined as user accounts with no logins in a given time frame.

Rationale:

Users can become inactive for a number of reasons, for example, vacation, parental leave, new roles within the company, or sick leave. If a user's access needs to be temporarily revoked, you can suspend an account to prevent a login.

Impact:

After a user's status is updated to **Suspended**, the user is unable to gain access to any IBM Cloud resources.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access (IAM)**.
3. To view a list of users in the account, click **Users**.
4. The user list will also show the status for each user in the account.
5. To change a users' status, click on a user name.
6. Under *User details*, select the desired status in the User status drop down.
7. Click **Apply**.

To check the last time a user logged in, follow the steps to enable Activity Tracker with LogDNA in recommendation *Enable audit logging for IBM Cloud Identity and Access Management*.
API:
https://cloud.ibm.com/apidocs/user-management#get-user-profile

Remediation:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage > Access (IAM)**.
3. To view a list of users in the account, click **Users**.
4. The user list will also show the status for each user in the account.
5. To suspend a user, click on a user name.
6. Under *User details*, select **Suspended** in the User status drop down.
7. Click **Apply**.

Default Value:

By default, if an IBMid is associated with the user, user accounts are *Active*; if no IBMid is associated with the user, user accounts are *Pending*. When a new user completes the IBM Cloud onboarding agreement, the *Pending* status changes to *Active*.

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-status

CIS Controls:

Version 7

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

1.18 Enable audit logging for IBM Cloud Identity and Access Management (Manual)

Profile Applicability:

- Level 1

Description:

Use the IBM Cloud Activity Tracker with LogDNA service to monitor certain IAM events.

Rationale:

As a security officer, auditor, or manager, you can use the IBM Cloud Activity Tracker with LogDNA service to track how users and applications interact with IBM Cloud Identity and Access Management (IAM). You can use this service to investigate abnormal activity and critical actions and comply with regulatory audit requirements.

Impact:

Activity Tracker with LogDNA allows you to track the following IAM events:

- Managing access groups by creating and deleting groups or adding and removing users
- Creating, updating, or deleting service IDs
- Creating, updating, or deleting API keys
- Creating, updating, or deleting access policies
- Logging in to IBM Cloud by using an API key, authorization code, passcode, password, or an API key that is associated with a service ID

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Go to the Menu icon. Then, select **Observability** to access the *Observability* dashboard.
3. Select **Activity Tracker** from the page navigation menu
4. Check that you can see an *IBM Cloud Activity Tracker with LogDNA* instance in Frankfurt and one instance for each location where you operate in the IBM Cloud.

API:
https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=Activity-Tracker-with-LogDNA-at_events_iam#at_events_iam_apikeys

Remediation:

You must create an instance of the IBM Cloud Activity Tracker with LogDNA service in the Frankfurt region to start tracking IAM events. Use a minimum of a 7-day event search. Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Go to the Menu icon. Then, select **Observability** to access the *Observability* dashboard.
3. Select **Activity Tracker** from the page navigation menu
4. Click **Create instance** to create an instance of *IBM Cloud Activity Tracker with LogDNA*.
5. In the *Select a region* drop down, choose *Frankfurt*
6. Select a pricing plan, service name, resource group, and provide optional tags. Choose a plan that offers a minimum of 7-day event search.
7. Click **Create**.

Default Value:

By default, audit logging with Activity Tracker with LogDNA is not enabled.

References:

1. https://cloud.ibm.com/docs/account

CIS Controls:

Version 7

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

1.19 Ensure Identity Federation is set up with a Corporate IDP (Manual)

Profile Applicability:

- Level 1

Description:

Allow users to log in to IBM Cloud by using their corporate Identity Provider (IdP) to authenticate.

Rationale:

Identity Federation allows enterprises to use their enterprise Identity Provider (IdP) to integrate with IBM Cloud, and alleviates the need for enterprise users to remember a separate username and password from IBMid system. The enterprise IdP also allows your enterprise to manage user access, set log in rules, apply corporate governance policies to the log in process, and set things like password expiration rules and character requirements.

Impact:

After the account is federated, users use their corporate login credentials to access IBM Cloud.

Audit:

Console:
During log in, a federated IBM Cloud account redirects you to an external IdP that is configured during the identity federation process.
API:
N/A

Remediation:

Contact https://www.ibm.com/cloud/support to begin the identity federation process.

Default Value:

By default, IBM Cloud accounts are not federated with an external IdP.

References:

1. https://cloud.ibm.com/docs/iam?topic=iam-federated_id

CIS Controls:

Version 7

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

2 Storage

2.1 Cloud Object Storage

IBM® Cloud Object Storage stores encrypted and dispersed data across multiple geographic locations. Information stored with IBM® Cloud Object Storage is encrypted and dispersed across multiple geographic locations, and accessed over popular protocols like HTTPS using a modern RESTful API.

2.1.1 Cloud Object Storage Encryption

Objects stored in IBM Cloud Object Storage need to be encrypted at all times for client data security. By default all objects stored in IBM Cloud Object Storage are encrypted at-rest using provider-managed keys and no user action is needed. Optionally, you can also leverage IBM Cloud Object Storage integration with IBM Cloud Key Management Services to further add another layer of encryption to the Data Encryption Keys (DEKs) associated with the data (objects) stored in Cloud Object Storage buckets.

2.1.1.1 Ensure Cloud Object Storage encryption is done with customer managed keys (Manual)

Profile Applicability:

- Level 2

Description:

Users can store objects in IBM Cloud Object Storage buckets by providing their own encryption keys which get applied at a per object level.

Rationale:

Users can have added security and granular control over the encryption keys at a per object level.

Impact:

Users can configure Cloud Object Storage and use their own root keys when uploading objects. For any key rotation (or new key usage) users will have to issue a GET operation with the old key and a PUT operation with the new key.

Audit:

Using Console: N/A
Using API/CLI:
Use of Server-Side Encryption with Customer-Provided Keys (SSE-C) can be validated by the following steps:
Note: *Ensure that you have completed the configuration setup to use the CLI by following the guidelines on the Using the AWS CLI page*

1. Review the metadata of the object that is encrypted using the customer-provided key. The operation can be performed using an API call or via a command-line interface. Here is an example call to get the object metadata:
```
aws --endpoint https://s3.private.au-syd.cloud-object-
storage.appdomain.cloud s3api head-object --bucket <bucket-name> --key
<object-name> --sse-customer-algorithm=AES256 --sse-customer-
key=<customer-key-used-to encrypt-the-object>
```
2. The presence of the object headers `SSECustomerKeyMD5` and `SSECustomerAlgorithm` from the API/CLI response should confirm that the object is encrypted using the key.

Remediation:

Using Console: N/A
Using API/CLI:
Objects can be uploaded with your own key by using a PUT object request with key specific headers. Please refer to Server-Side Encryption with Customer-Provided Keys for additional information.

Default Value:

By default, all objects stored in IBM Cloud Object Storage are encrypted by using randomly generated keys and an all-or-nothing-transform (AONT) also known as provider managed keys. Clients can provide their own encryption keys for a per-object level encryption by using the IBM Cloud Object Storage Server-Side Encryption with Customer-Provided Keys (SSE-C) option.

References:

1. • Data encryption with IBM Cloud Object Storage: https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-encryption
2. • Server-Side Encryption with Customer-Provided Keys: https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-sse-c

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.

2.1.1.2 Ensure Cloud Object Storage Encryption is set to On with BYOK (Manual)

Profile Applicability:

- Level 2

Description:

You can use IBM Cloud encryption key management service, for example Key Protect, to bring your own root key (BYOK) to IBM Cloud and use it to add envelope encryption for data that is stored in IBM Cloud Object Storage buckets.

Rationale:

When it comes to encryption of data at rest in IBM Cloud, the best practice is to allow customers to manage customer root keys (CRK) that are used to protect customer data stored in data and storage services in IBM Cloud. Bring your Own Key (BYOK) allows customers to ensure no one outside of their organization has access to the root key and and with the support of BYOK, customers can manage the lifecycle of their customer root keys where they can create, rotate, delete those keys. This provides a significant level of control where those CRKs are managed by the customer, which in turn increases both security control as well as meet relevant compliance requirements. These CRKs can be used in turn to protect the data encryption keys used to encrypt the data.

Impact:

For Bring your Own Key (BYOK) encryption with Cloud Object Storage integration and Key Protect key management service you will need to review and understand how you can leverage the integration to handle key lifecycle events (for example key rotation, deletion, restore). Refer to the Cloud Object Storage integration with Key Protect section to learn about key lifecycle management and Key Protect product page to find out more about the key lifecycle events.

Audit:

You can use the IBM Cloud Object Storage bucket configuration properties to verify whether a Cloud Object Storage bucket is enabled to use Key Protect.
From Console:
Navigate to your Cloud Object Storage instance:

1. Log in to IBM Cloud at https://cloud.ibm.com

2. Click the **Menu** icon and select **Resource List**
3. On the **Resource List** page under **Storage**, select the Cloud Object Storage instance that you have provisioned.
4. Click on the appropriate bucket that you would like to check
5. Click on ***Configuration*** and scroll down to ***Associated key management service*** to check/confirm if a Key Protect key management service is associated

Remediation:

You will not be able to add Key Protect as the key management service once data is already written to a Cloud Object Storage bucket. In order to ensure that objects are encrypted using Key Protect root keys you will need to create a new Cloud Object Storage bucket, set it to use Key Protect key management service and then upload/copy the existing objects to this new bucket.

Default Value:

By default, use of Key Protect encryption key management service with IBM Cloud Object Storage buckets is not enabled.

References:

1. • Data encryption with IBM Cloud Object Storage: https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-encryption
2. • Integrated service availability page: https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-service-availability
3. • https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-compatibility-api-bucket-operations#compatibility-api-key-protect

Additional Information:

Creating a Cloud Object Storage bucket with Key Protect (Bring Your Own Key):

1. From your Cloud Object Storage instance page, create a new Cloud Object Storage bucket by clicking **Create bucket**.
2. To create the bucket, in the ***Create bucket*** section, select **Custom bucket.**
3. In the bucket configuration section, you can select the option to use **Key Protect** under ***Key management services***

Note: In order to configure a Cloud Object Storage bucket to use Key Protect key management service you will need an instance of Key Protect along with appropriate access authorization to your Cloud Object Storage instance.

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.

2.1.1.3 Ensure Cloud Object Storage Encryption is set to On with KYOK (Manual)

Profile Applicability:

- Level 2

Description:

You can use IBM Cloud encryption key management services, for example, Hyper Protect Crypto Services to keep and manage exclusive control over the root keys used to add envelop encryption for data that is stored in IBM Cloud Object Storage buckets.

Rationale:

When it comes to encryption of data at rest in IBM Cloud, the best practice is to allow customers use encryption capabilities offered by Hardware Security Module crypto service. IBM Cloud Hyper Protect Crypto Services offers Keep your Own Key (KYOK) capabilities that allow customers to have exclusive key control over encryption keys. This provides a significant level of control over encryption keys where only authorized users have access (no privileged users included IBM Cloud Admins) to encryption keys, in turn increases both security control as well as meet relevant compliance requirements.

Impact:

For Keep your Own Key (KYOK) encryption using IBM Cloud Hyper Protect Crypto Services key management service you will need to review and understand how key lifecycle events (for example key rotation) need to be handled. Refer to the Hyper Protect Crypto Services product page for details around the key lifecycle events supported.

Audit:

You can use the IBM Cloud Object Storage bucket configuration properties to verify whether a Cloud Object Storage bucket is configured to use Hyper Protect Crypto Services key management service.
Navigate to your Cloud Object Storage instance:

1. Log in to IBM Cloud at https://cloud.ibm.com
2. Click the **Menu** icon and select **Resource List**
3. On the **Resource List** page under **Storage**, select the Cloud Object Storage instance that you have provisioned.
4. Click on the appropriate bucket that you would like to check

5. Click on ***Configuration*** and scroll down to ***Associated key management service*** to check/confirm if Hyper Protect Crypto Services key is configured with the bucket

Remediation:

You will not be able to add Hyper Protect Crypto Services as the key management service once data is already written to a Cloud Object Storage bucket. In order to ensure that objects are encrypted using Hyper Protect Crypto Services root keys you will need to create a new Cloud Object Storage bucket, set it to use Hyper Protect Crypto Services key management service and then upload/copy the existing objects to this new bucket.

Default Value:

By default, use of Hyper Protect Crypto Services key management service with IBM Cloud Object Storage buckets is not enabled.

References:

1. • Data encryption with IBM Cloud Object Storage: https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-encryption
2. • Integrated service availability page: https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-service-availability

Additional Information:

Create a Cloud Object Storage bucket with Hyper Protect Crypto Services (Keep Your Own Key):

1. From your Cloud Object Storage instance page, create a new Cloud Object Storage bucket by clicking **Create bucket**.
2. To create the bucket, in the ***Create bucket*** section, select **Custom bucket**.
3. In the bucket configuration section, you can select the option to use **Hyper Protect Crypto Services** under ***Key management services***

Note: In order to configure a Cloud Object Storage bucket to use Hyper Protect Crypto Services you will need an instance of Hyper Protect Crypto Services along with appropriate access authorization to your Cloud Object Storage instance.

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.

2.1.2 Ensure network access for Cloud Object Storage is restricted to specific IP range (Manual)

Profile Applicability:

- Level 2

Description:

IBM Cloud Object Storage bucket firewall restricts all access to data unless the request originates from a list of allowed IP addresses.

Rationale:

Restrict access to your data stored in Cloud Object Storage buckets and enhance security controls by creating a firewall rule that will only allow data access to the list of IP addresses you specify.

Impact:

For any application(s) that depend upon or access data stored in Cloud Object Storage buckets to conduct its operation(s) you must ensure that the network it is using to access Cloud Object Storage buckets is also included in the COS firewall. Not doing so could possibly result in disruption of the activities.

Audit:

To check or confirm that an IBM Cloud Object Storage bucket is accessible only from a list of authorized IP addresses, you can navigate to **Access Policies** section available under your bucket information and check **Authorized IPs** list.

1. Go to IBM Cloud Console: https://cloud.ibm.com/resources
2. Under **Storage** click on the Cloud Object Storage instance you want to check (*you will be directed to a default bucket listing page*)
3. Click on the Cloud Object Storage bucket for which you want to review the bucket firewall information
4. At the bucket information screen, click on the **Access policies** section on the left navigation
5. Within *Bucket access policies* you will see the tab **Authorized IPs**
6. Review the list of IPs to ensure it includes the IPs you want authorized

Remediation:

Follow the steps outlined to add an IP to the list of Authorized IPs in bucket firewall policies.

Using the console to set a firewall

From the IBM Cloud console dashboard, you can restrict access to your content by setting a firewall.

Set a list of authorized IP addresses

1. Start by selecting **Storage** to view your resource list.
2. Next, select the service instance with your bucket from within the **Storage** menu. This takes you to the Object Storage Console.
3. Select the bucket that you want to limit access to authorized IP addresses.
4. Select **Access policies** from the navigation menu.
5. Select the **Authorized IPs** tab.
6. Click on **Add** and specify a list of IP addresses in CIDR notation, for example 192.168.0.0/16, fe80:021b::0/64. *Addresses can follow either IPv4 or IPv6 standards.*
7. Click **Add**.
8. The firewall will not be enforced until the address is saved in the console. Click **Save all** to enforce the firewall.
   Note that all objects in this bucket are only accessible from those IP addresses.

Default Value:

By default Cloud Object Storage buckets can only be accessed by authenticated users.

References:

1. https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-setting-a-firewall
2. https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-setting-a-firewall#firewall-api

CIS Controls:

Version 7

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

2.1.3 Ensure network access for Cloud Object Storage is set to be exposed only on Private end-points (Manual)

Profile Applicability:

- Level 1

Description:

IBM Cloud Object Storage bucket firewall restricts all access to data unless the request originates from a list of allowed IP addresses that are part of the private subnets only.

Rationale:

Restrict access to your data stored in Cloud Object Storage buckets and enhance security controls by creating a firewall rule that will only allow data access to the list of IP addresses that are part of your private subnet.

Impact:

Ensuring network access is accessible via private subnets requires that you update the settings in Cloud Object Storage bucket configuration by following additional steps outlined in the remediation section.

Audit:

To check or confirm that an IBM Cloud Object Storage bucket is accessible only from a list of authorized IP addresses from private subnets, you can navigate to **Access policies** section available under your bucket information and check **Authorized IPs** list.

1. Go to IBM Cloud Console: https://cloud.ibm.com/resources
2. Under **Storage** click on the Cloud Object Storage instance you want to check. *(you will be directed to a default bucket listing page)*
3. Click on the Cloud Object Storage bucket for which you want to review the bucket firewall information
4. At the bucket information screen, click on the **Access policies** section on the left navigation.
5. Within Bucket access policies you will see the tab **Authorized IPs**
6. Review the list of private IPs/subnets to ensure it includes the IPs/subnets you want authorized, for example, `10.0.0.0/8` would authorize all the private IP addresses that are part of the IBM Cloud Infrastructure to access the bucket.

Remediation:

Follow the steps outlined to add an IP/subnet to the list of Authorized IPs in bucket firewall policies.

Using the console to set a firewall

From the IBM Cloud console dashboard, you can restrict access to your content by setting a firewall.

Set a list of authorized IP addresses

1. Start by selecting **Storage** to view your resource list.
2. Next, select the service instance with your bucket from within the **Storage** menu. This takes you to the Object Storage Console.
3. Select the bucket that you want to limit access to authorized IP addresses.
4. Select **Access policies** from the navigation menu.
5. Select the **Authorized IPs** tab.
6. Click on **Add** and specify a list of IP addresses in CIDR notation, for example `192.168.0.0/16`, `fe80:021b::0/64`. *Addresses can follow either IPv4 or IPv6 standards.*
7. Click **Add**.
8. The firewall will not be enforced until the address is saved in the console. Click **Save all** to enforce the firewall.
   Note that all objects in this bucket are only accessible from those IP addresses.

Default Value:

By default, Cloud Object Storage buckets can only be accessed by authenticated users.

References:

1. https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-setting-a-firewall
2. https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-setting-a-firewall#firewall-api

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.

2.1.4 Ensure Cloud Object Storage bucket access is restricted by using IAM and S3 access control (Manual)

Profile Applicability:

- Level 1

Description:

Access controls on the Cloud Object Storage buckets are governed via IBM Identity and Access Management (IAM). However, some permissions can also be granted (or restricted) via S3 access controls.

Rationale:

Assign IAM access roles for users and Service IDs against buckets, by using either the UI or the CLI to create policies. The S3 Access Control is performed using ACLs granted against buckets and objects.

Impact:

Organizations can use Cloud Object Storage to store sensitive data that may need to be restricted. Therefore, creation of a new Cloud Object Storage bucket requires careful review and planning around access controls provided by IBM Cloud environment to ensure data access can be restricted to only those having valid business need.

Audit:

Reviewing assigned access using IAM
Complete the following steps to review your assigned access in an account that you have been added to:

1. In the console, click **Manage** > **Access (IAM)**, and select **Users** or **Manage > Access (IAM)**, and select **Service IDs**, depending on which identity you want to review.
2. Select your name or the service ID.
3. Review the assigned access in the **Access policies** section.

Reviewing S3 ACLs to buckets
View the S3 ACLs via API or CLI. A typical API call is shown:

```
curl -X "GET" "https://{endpoint}/{bucket-name}?acl" \
     -H "Authorization: Bearer {token}" \
```

Remediation:

Granting Access to a COS Bucket using IAM
Using the UI
To create a new bucket-level policy:

1. Navigate to the **Access IAM** console from the **Manage** menu.
2. Select **Users** from the left navigation menu.
3. Select a user.
4. Select the **Access Policies** tab to view the user's existing policies, assign a new policy, or edit an existing policy.
5. Click **Assign access** to create a new policy.
6. Choose **Assign access to resources**.
7. First, select **Cloud Object Storage** from the services menu.
8. Then, select the appropriate service instance. Enter `bucket` in the **Resource type** field and the bucket name in the **Resource ID** field.
9. Select the wanted service access role. Selecting the lozenge with the number of actions show the actions available to the role.
10. Click **Assign**

Using the CLI
From a terminal run the following command:

```
ibmcloud iam user-policy-create <user-name> \
      --roles <role> \
      --service-name cloud-object-storage \
      --service-instance <resource-instance-id> \
      --resource-type bucket \
      --resource <bucket-name>
```

To list existing policies:

```
ibmcloud iam user-policies <user-name>
```

To edit an existing policy:

```
ibmcloud iam user-policy-update <user-name> <policy-id> \
      --roles <role> \
      --service-name cloud-object-storage \
      --service-instance <resource-instance-id> \
      --resource-type bucket \
      --resource <bucket-name>
```

The same set of accesses can be assigned to a service id as well. Please follow the procedure documented in https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-iam-bucket-permissions#iam-service-id

Granting S3 ACLs to buckets
Grant the S3 ACLs via API or CLI. A Typical API call is shown:

```
curl -X "PUT" "https://{endpoint}/{bucket-name}?acl" \
     -H "Authorization: Bearer {token}" \
     -H "x-amz-acl: <scope>"
```

Default Value:

By default, users or service ids which have Cloud Object Storage service role access to the Cloud Object Storage service instances will have access to the Cloud Object Storage buckets under them as well.

References:

1. • https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-iam-bucket-permissions
2. • https://cloud.ibm.com/docs/account?topic=account-assign-access-resources
3. • https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-iam-public-access#public-access-object

2.1.5 Disable public (anonymous) access to IBM Cloud Object Storage buckets (Manual)

Profile Applicability:

- Level 1

Description:

You can disable public (anonymous) access to IBM Cloud Object Storage buckets.

Rationale:

Buckets might have to hold open data sets for academic, research, or image repositories that are used by web applications and content delivery networks. You can make these buckets publicly accessible by using the **Public Access** group. But when buckets contain non-public data (e.g., restricted, internal, confidential or sensitive data), it is important to have public access disabled. To disable the public access, a previously defined access policy must be removed.

Impact:

By default, public access to Cloud Object Storage buckets is disabled. If an access policy is defined that allows public access, you can disable the policy by using the console.

Audit:

To check if an access policy exists for a Cloud Object Storage bucket, you can list the access policies for the **Public Access** group.

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage** > **Access (IAM)**.
3. Click **Access groups**.
4. Select **Public Access**
5. Check the list of access polices to see if one exists for the relevant Cloud Object Storage bucket.

Remediation:

To disable public access for buckets, complete the following steps:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. From the Menu bar, click **Manage** > **Access (IAM)**.
3. Click **Access groups**.

4. Click **Public Access** to see a list of all public access policies currently in use.
5. Find the policy that corresponds to the bucket that you want to return to enforced access control.
6. From the list of actions, select **Remove**.
7. Confirm that you want to remove the policy. The policy is removed from the bucket.

Default Value:

By default, public access to Cloud Object Storage buckets is disabled.

References:

1. Information around Enabling and Disabling Public access to the COS bucket is available from the product page: https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-iam-public-access#iam-public-access-console

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.

2.2 File Block Storage

IBM Cloud™ Block Storage is persistent, high-performance iSCSI storage that is provisioned and managed independently of compute instances. iSCSI-based Block Storage LUNs are connected to authorized devices through redundant multi-path I/O (MPIO) connections.

Block Storage brings best-in-class levels of durability and availability with an unmatched feature set. It is built by using industry standards and best practices. Block Storage is designed to protect the integrity of the data and maintain availability through maintenance events and unplanned failures, and provide a consistent performance baseline.

2.2.1 Cloud Block Storage Encryption

Objects stored in IBM Cloud Block Storage need to be encrypted at all times for client data security. By default all objects stored in IBM Cloud Block Storage are encrypted at-rest by ensuring user selects an encryption key from various available options. These options are:

1. Use provider-managed keys for Encryption
2. Use IBM Cloud KeyProtect Service for managing encryption keys or
3. Use IBM Cloud hardware HSM supported Hyper Protect Service for managing encryption keys

2.2.1.1 Ensure Block Storage is encrypted with customer managed keys (Manual)

Profile Applicability:

- Level 2

Description:

By default, IBM Cloud Block Storage provides provider-managed encryption for all data. For enhanced security, customers can bring their own encryption keys and manage them through IBM Key Management Services – Key Protect or Hyper Protect Crypto Services (HPCS). Provider-managed encryption is turned on by default and cannot be turned off.

Rationale:

With customer-managed keys, only customers can access and manage their master root keys, giving them full control over their data security.

Audit:

You can use the IBM Cloud Block Storage configuration properties to verify whether a Cloud Object Storage bucket is enabled to use Key Protect.
From Console, Navigate to your Cloud Object Storage instance:

1. In the IBM Cloud console, go to **Menu icon > VPC Infrastructure > Storage > Block storage volumes**. A list of all block storage volumes displays.
2. For each of the volumes listed, ensure the encryption field is **Not** pointing to "Provider Managed"

Remediation:

You will not be able to change encryption option once data is already written to a Cloud Block Storage Volume. In order to ensure that objects are encrypted using customer managed keys you will need to create a new Cloud Block Storage volume, set it to use either Key Protect or Hyper Protect key management service and then upload/copy the existing objects to this new volume.

Default Value:

Provider managed

References:

1. https://cloud.ibm.com/vpc-ext

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.

2.2.1.2 Ensure Block Storage is encrypted with BYOK (Manual)

Profile Applicability:

- Level 2

Description:

By default, IBM Cloud Block Storage provides provider-managed encryption for all data. For enhanced security, customers can bring their own encryption keys and manage them through IBM Key Management Service – Key Protect . The customer can chose to use BYOK instead of provider-managed keys for enhanced security

Rationale:

When it comes to encryption of data at rest in IBM Cloud, the best practice is to allow customers to manage customer root keys(CRK) that are used to protect customer data stored in data and storage services in IBM Cloud. Bring your Own Key(BYOK) allows customers to ensure no one outside of their organization has access to the root key and and with the support of BYOK, customers can manage the lifecycle of their customer root keys where they can create, rotate, delete those keys. This provides a significant level of control where those CRKs are managed by the customer, which in turn increases both security control as well as meet relevant compliance requirements. These CRKs can be used in turn to protect the data encryption keys used to encrypt the data.

Audit:

You can use the IBM Cloud Block Storage configuration properties to verify whether a Cloud Object Storage bucket is enabled to use Key Protect.
From Console, Navigate to your Cloud Object Storage instance:

1. In the IBM Cloud console, go to Menu icon > VPC Infrastructure > Storage > Block storage volumes. A list of all block storage volumes displays.
2. For each of the volumes listed, ensure the encryption field pointing to "Key Protect"

Remediation:

You will not be able to add Key Protect as the key management service once data is already written to a Cloud Block Storage Volume. In order to ensure that objects are encrypted using Key Protect keys you will need to create a new Cloud Block Storage volume, set it to use Key Protect key management service and then upload/copy the existing objects to this new volume.

Default Value:

Provider Managed

References:

1. https://cloud.ibm.com/vpc-ext

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.

2.2.1.3 Ensure Block Storage is encrypted with KYOK (Manual)

Profile Applicability:

- Level 2

Description:

By default, IBM Cloud Block Storage provides provider-managed encryption for all data. For enhanced security, customers can bring their own encryption keys and manage them through IBM Key Management Service – Hyper Protect Crypto Services (HPCS). The customer can chose to use BYOK instead of provider-managed keys for enhanced security

Rationale:

When it comes to encryption of data at rest in IBM Cloud, the best practice is to allow customers use encryption capabilities offered by Hardware Security Module crypto service. IBM Cloud Hyper protect Crypto Service offers Keep your Own Key (KYOK) capabilities that allow customers to have exclusive key control over encryption keys. This provides a significant level of control over encryption keys where only authorized users have access (no privileged users included IBM Cloud Admins) to encryption keys, in turn increases both security control as well as meet relevant compliance requirements.

Audit:

You can use the IBM Cloud Block Storage configuration properties to verify whether a Cloud Object Storage bucket is enabled to use Hyper Protect Crypto Service. From Console, Navigate to your Cloud Object Storage instance:

1. In the IBM Cloud console, go to Menu icon > VPC Infrastructure > Storage > Block storage volumes. A list of all block storage volumes displays.
2. For each of the volumes listed, ensure the encryption field pointing to "Hyper Protect".

Remediation:

You will not be able to add Hyper Protect Crypto Services as the key management service once data is already written to a Cloud Block Storage Volumes. In order to ensure that objects are encrypted using Hyper Protect Crypto Services you will need to create a new Cloud Block Storage volume, set it to use Hyper Protect Crypto Services key management service and then upload/copy the existing objects to this new volume.

Default Value:

Provider managed

References:

1. https://cloud.ibm.com/vpc-ext

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.

2.2.2 Ensure 'OS disk' are encrypted with Customer managed keys (Manual)

Profile Applicability:

- Level 2

Description:

By default, IBM Cloud Block Storage provides provider-managed encryption for all data. For enhanced security, customers can bring their own encryption keys and manage them through IBM Key Management Services – Key Protect or Hyper Protect Crypto Services (HPCS). Provider-managed encryption is turned on by default and cannot be turned off.

Rationale:

With customer-managed keys, only customers can access and manage their master root keys, giving them full control over their data security.

Audit:

You can use the IBM Cloud Block Storage configuration properties to verify whether a Cloud Object Storage bucket is enabled to use Key Protect or Hyper Protect key management services.
From Console, Navigate to your Cloud Object Storage instance:

1. In the IBM Cloud console, go to Menu icon > VPC Infrastructure > Storage > Block storage volumes. A list of all block storage volumes displays.
2. For each volumes listed with Attachment Type column value "Boot", ensure the encryption field is **Not** pointing to "Provider Managed".

Remediation:

You will not be able to change encryption option once data is already written to a Cloud Block Storage Volume. In order to ensure that objects are encrypted using customer managed keys you will need to create a new Cloud Block Storage volume, set it to use either Key Protect or Hyper Protect key management service and then upload/copy the existing objects to this new volume.

Default Value:

Provider Managed

References:

1. https://cloud.ibm.com/vpc-ext

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.

2.2.3 Ensure 'Data disks' are encrypted with customer managed keys (Manual)

Profile Applicability:

- Level 2

Description:

By default, IBM Cloud Block Storage provides provider-managed encryption for all data. For enhanced security, customers can bring their own encryption keys and manage them through IBM Key Management Services – Key Protect or Hyper Protect Crypto Services (HPCS). Provider-managed encryption is turned on by default and cannot be turned off.

Rationale:

With customer-managed keys, only customers can access and manage their master root keys, giving them full control over their data security.

Audit:

You can use the IBM Cloud Block Storage configuration properties to verify whether a Cloud Object Storage bucket is enabled to use Key Protect or Hyper Protect key management services.
From Console, Navigate to your Cloud Object Storage instance:

1. In the IBM Cloud console, go to Menu icon > VPC Infrastructure > Storage > Block storage volumes. A list of all block storage volumes displays.
2. For each volumes listed with Attachment Type column value "Data", ensure the encryption field is **Not** pointing to "Provider Managed".

Remediation:

You will not be able to change encryption option once data is already written to a Cloud Block Storage Volume. In order to ensure that objects are encrypted using customer managed keys you will need to create a new Cloud Block Storage volume, set it to use either Key Protect or Hyper Protect key management service and then upload/copy the existing objects to this new volume.

Default Value:

Provider managed

References:

1. https://cloud.ibm.com/vpc-ext

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.

2.2.4 Ensure 'Unattached disks' are encrypted with customer managed keys (Manual)

Profile Applicability:

- Level 2

Description:

By default, IBM Cloud Block Storage provides provider-managed encryption for all data. For enhanced security, customers can bring their own encryption keys and manage them through IBM Key Management Services – Key Protect or Hyper Protect Crypto Services (HPCS). Provider-managed encryption is turned on by default and cannot be turned off.

Rationale:

With customer-managed keys, only customers can access and manage their master root keys, giving them full control over their data security.

Audit:

You can use the IBM Cloud Block Storage configuration properties to verify whether a Cloud Object Storage bucket is enabled to use Key Protect or Hyper Protect key management services.
From Console, Navigate to your Cloud Object Storage instance:

1. In the IBM Cloud console, go to Menu icon > VPC Infrastructure > Storage > Block storage volumes. A list of all block storage volumes displays.
2. For each volumes listed without any value in the "Attachment Type" column, ensure the encryption field is **Not** pointing to "Provider Managed".

Remediation:

You will not be able to change encryption option once data is already written to a Cloud Block Storage Volume. In order to ensure that objects are encrypted using customer managed keys you will need to create a new Cloud Block Storage volume, set it to use either Key Protect or Hyper Protect key management service and then upload/copy the existing objects to this new volume.

Default Value:

Provider managed

References:

1. https://cloud.ibm.com/vpc-ext

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.

3 Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

3.1 Ensure auditing is configured in the IBM Cloud account (Manual)

Profile Applicability:

- Level 1

Description:

Collect audit events from IBM Cloud resources so that you can monitor activity in your IBM Cloud account.

Rationale:

IBM Cloud™ Activity Tracker with LogDNA is a Cloud service that you can use to monitor the activity of your IBM Cloud account. For example, you can use this service to investigate abnormal activity and critical actions, and comply with regulatory audit requirements. The audit events that are collected comply with the Cloud Auditing Data Federation (CADF) standard. Each audit event includes information about the initiator of the action, the action that is run, the target resource on which the action is requested, the observer, and the outcome of the action. For more information about the format, see Event fields.

Activity Tracker collects two types of events for audit-enabled services in the IBM Cloud:

- Management events
- Data events

Data events access or modify customer data. Management events report on operational actions on IBM Cloud resources. Both types of events generate events for create, read, update, and delete (CRUD) actions.

Every user that accesses the IBM Cloud Activity Tracker with LogDNA service in your account must be assigned an access policy with an IAM user role defined. The policy determines what actions the user can perform within the context of the service or instance that you select. The allowable actions are customized and defined as operations that are allowed to be performed on the service. The actions are then mapped to IAM user roles.

Tip: To organize a set of users and service IDs into a single entity that makes it easy for you to manage IAM permissions, use access groups. You can assign a single policy to the group instead of assigning the same access multiple times for each individual user or service ID.

The following types of roles are available in IBM Cloud:

- Platform management roles enable users to perform tasks on service resources at the platform level, for example, assign user access for the service, create or delete

service IDs, create instances, assign policies for your service to other users, and bind instances to applications.
- Service access roles enable users to be assigned varying levels of permission for calling the service's API, such as viewing data and configuring alerts.

Impact:

Failure to meet this control limits your ability to monitor activity in your IBM Cloud account. It also restricts your ability to identify the initiator of actions in your account, the resources affected, and details about the request. In addition, if IAM permissions are not set properly, you can expose your organization's audit information to non-authorized users.

Audit:

To check that you are collecting audit events from IBM Cloud resources so that you can monitor activity in your IBM Cloud account, you can use the following check list to ensure that auditing is configured in an IBM Cloud account:

1. Ensure that service instances of the IBM Cloud Activity Tracker with LogDNA service are provisioned in each region where you operate in the Cloud. Only one Activity Tracker instance is allowed in each IBM Cloud location where the service is available.
2. Ensure that an Activity Tracker instance is provisioned in Frankfurt. This instance acts as a global domain and collects audit events that report user actions in the IBM Cloud where the scope expands beyond a single region, such as managing users.
3. Ensure that access control groups (ACG) are configured in your account to manage user access.
   a. Check that you have multiple access groups to manage permissions to operate audit service instances in IBM Cloud, and to view and manage audit data.
   b. Check each access group documents the scope of the type of access users get when they are added to the group.
   c. Check the policies and roles that are configured in each access group. They must restrict access to users or service IDs taking into account the scope of the access group.
   d. Check that the users that are added to each access group are correct taking into account their role in the Cloud account.

To check if audit instances are provisioned and configured in the account, complete the following steps:
Note: To complete these steps, your IBM Cloud user ID (IBMid) must have the following roles:

- A platform role with viewer role for the IBM Cloud Activity Tracker with LogDNA service for the account

- A service role with reader role for the IBM Cloud Activity Tracker with LogDNA service for the account
- Identity and Access Management (IAM) permissions to view access groups in the account

UI instructions:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Go to the Menu icon. Then, select **Observability** to access the *Observability* dashboard.
3. Select **Activity Tracker** from the page navigation menu
4. Check that you can see an Activity Tracker instance in Frankfurt and one instance for each location where you operate in the IBM Cloud.
5. To launch the LogDNA web UI, for each instance, select View LogDNA.
6. In the LogDNA web UI, verify that you can see audit events, and that they comply with the IBM event format that is documented. For more information about the format, see Event fields.

CLI instructions:

1. Log in to IBM Cloud.
   Run the following command:
   ```
   ibmcloud login -a cloud.ibm.com
   ```
   For a federated account, run the following command:
   ```
   ibmcloud login -a cloud.ibm.com --sso
   ```
2. List all the audit instances that are provisioned in your account. Run the following command:
   ```
   ibmcloud resource service-instances --service-name logdnaat --all-resource-groups
   ```
3. Check that you have one instance in Frankfurt, and one instance for each location where you operate in the IBM Cloud.

Note: You can view events through the LogDNA web UI only. Therefore, you must launch the LogDNA web UI from the IBM Cloud console to verify that events are being collected.
To verify that access groups are available in the account to manage permissions working with audit service instances, complete the following steps:
UI instructions:

1. Log in to IBM Cloud at `https://cloud.ibm.com`.
2. From the Menu bar, select **Manage > Access (IAM)**.
3. Select **Access groups** from the page navigation menu.
4. Find the access groups that grant permissions to work with the IBM Cloud Activity Tracker with LogDNA service.
5. Check the description to identify the scope.

6. Check the list of users and service IDs. Verify that they should be members of the group.
7. Check that policies and roles are aligned with the scope of the access group.

CLI instructions:

1. Log in to IBM Cloud.
   Run the following command:
   `ibmcloud login -a cloud.ibm.com`
   For a federated account, run the following command:
   `ibmcloud login -a cloud.ibm.com --sso`
2. List the access groups in the account. Run the following command:
   `ibmcloud iam access-groups`

Repeat the following steps for each access group that you identify.

3. Get information about each access group.
   Run the following command to list the details of an access group:
   `ibmcloud iam access-group {Access Group Name} --output JSON`
   Check the description to identify the scope.
4. Check the list of users and service IDs. Verify that they should be members of the group.
   To get the list of users that belong to an access group, run the following command:
   `ibmcloud iam access-group-users {Access Group Name}--output JSON`
   To get the list of service IDs that belong to an access group, run the following command:
   `ibmcloud iam access-group-service-ids {Access Group Name} --output JSON`
5. Check that policies and roles are aligned with the scope of the access group.
   Run the following command to get details of the policies and roles configured for the access group:
   `ibmcloud iam access-group-policies {Access Group Name} --output JSON`

Remediation:

1. If an Activity Tracker instance is not provisioned in each of the locations where you operate in IBM Cloud, you must provision an instance of the service.
   To provision an audit instance, choose any of the following options:
   - Provision an instance through the IBM Cloud Catalog.
   - Provision an instance through the Observability dashboard.
   - Provision an instance through the CLI.
2. If an Activity Tracker instance is not provisioned in Frankfurt, you must provision one.
   To provision an audit instance, choose any of the following options:
   - Provision an instance through the IBM Cloud Catalog.
   - Provision an instance through the Observability dashboard.
   - Provision an instance through the CLI.

3. If you are missing access groups or policies, complete the following steps to remediate the problem:
    - If access groups are not configured, you must create one or more access groups. When you create, or when you edit an access group, you can add a description to the access group.
    - If the access group to manage administration permissions is missing policies, assign administrative policies to the access group.
    - If the access group to manage user permissions is missing policies, assign user policies to the access group.
    - If you want to add users to the access group, see Add users to the access group.
    - If you want to add service IDs to the access group, see Add service IDs to the access group.
    - If you need to remove users or service IDs, see Removing access.
    - If you need to modify a policy, see Editing existing access.

Default Value:

By default, management audit events are generated and collected automatically. However, you must configure the IBM Cloud Activity Tracker with LogDNA service in your account to view and manage events, and to be notified of specific scenarios.

For most of the services in IBM Cloud, data events are generated and collected automatically. However, there are some exceptions where you must opt-in to collect them, such as IBM Cloud Object Storage.

References:

1. IBM Cloud Activity Tracker with LogDNA: Adoption guidelines for regulated and highly available workloads: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=logdnaat-adoption
2. IBM Cloud Activity Tracker with LogDNA service plans: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=logdnaat-service_plan
3. Managing access for IBM Cloud Activity Tracker with LogDNA: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=logdnaat-iam

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.

6.5 Central Log Management

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

3.2 Ensure that archiving is enabled for audit events (Manual)

Profile Applicability:

- Level 2

Description:

Archive events for long-term storage so that you have access to data for a longer period of time, you can comply with highly regulated environments, you can recover quickly in the eventuality of a disaster scenario, and you can adhere to internal data storage policies.

Rationale:

When you provision an instance of IBM Cloud Activity Tracker with LogDNA, you associate a service plan that defines the number of days that data is available for search, troubleshooting, and analysis.

In specific scenarios, the maximum number of days that data is available for search (30 days) is not sufficient and requires a long-term data storage solution. For example, highly regulated environments impose strict storage policies where they define the minimum number of days that log data must be saved for. Internal corporate regulations can also impose data storage policies. You might be affected by a natural disaster and you must recover fast. In any of these sample scenarios, you must implement an archiving solution that allows you to keep data for long-term storage.

Data that is managed by the IBM Cloud Activity Tracker with LogDNA service is encrypted at rest. Data that is archived to a bucket that is hosted in IBM Cloud Object Storage is encrypted by default using randomly generated keys and an all-or-nothing-transform.

While this IBM Cloud Object Storage default encryption model provides at-rest security, some workloads need to be in possession of the encryption keys used. You can manage your keys manually by providing your own encryption keys - referred to as Server-Side Encryption with Customer-Provided Keys (SSE-C). With IBM Cloud Object Storage, you also have a choice to use IBM's integration capabilities with IBM Cloud Key Management Services like IBM Key Protect and Hyper Protect Crypto Services. Depending on the security requirements, you can decide whether to use IBM Key Protect or IBM Hyper Protect Crypto Services for your IBM Cloud Object Storage buckets.

- IBM Key Protect for IBM Cloud helps you provision encrypted keys for apps across IBM Cloud services. As you manage the lifecycle of your keys, you can benefit from knowing that your keys are secured by FIPS 140-2 Level 3 certified cloud-based hardware security modules (HSMs) that protect against the theft of information.

- Hyper Protect Crypto Services is a single-tenant, dedicated HSM that is controlled by you. The service is built on FIPS 140-2 Level 4-certified hardware, the highest offered by any cloud provider in the industry.

If you use IBM Cloud Activity Tracker with LogDNA, you can archive data that is available through an audit instance to an IBM Cloud Object Storage bucket, for example. You can configure the bucket to meet all your internal and external regulations.

There are two types of data that you must consider archiving: events, and service instance metadata, such as views, templates, screens, and alerts.

As guidance, events must be kept for as long as internal compliance requires. If no requirements exist, consider a minimum of 365 days.

Impact:

If you have regulatory or organizational requirements that determine the number of days that data must be available, failure to meet this control can result in breaching compliance.

In addition, if data is corrupted or not archived, and you do not claim it within the number of days that are available for search, you can lose data.

If you have requirements that define the bucket specification, policies, and encrypting requirements, you might be in breach of infrastructure compliance.

Audit:

Use the following check list to ensure that archiving is configured for each of your audit instances:

1. Ensure that IBM Cloud Activity Tracker with LogDNA instances are provisioned with a service plan that includes the ability to configure archiving to an external storage service.
2. Ensure that each audit instance has archiving enabled and configured.
3. Ensure that you have access to storage, for example, check that you have an instance of the IBM Cloud Object Storage service provisioned in your account.
   Consider using IBM Cloud Object Storage (COS) with IBM Log Analysis with LogDNA. Connectivity is done via private endpoints within the IBM Cloud private network, making the connection and transfer more secure. This integration reduces latency, benefits from IBM Cloud network security, and offers faster archive response times.
4. Ensure that you have multiple COS buckets available to archive your data. Check the bucket configuration to verify that it meets your corporate and external market regulations.
   Consider using a bucket for each audit instance so that you can customize the bucket to meet security requirements. These requirements might be related to the type of

data that is archived and to external regulations like EU-managed requirements, for example.

5. Ensure that the bucket has the following features enabled:
   - A key management service is configured. For example, check IBM Cloud Key Protect is configured so that you can use your own key to encrypt data.
   - Auditing to IBM Cloud Object Storage is enabled and that the options read and data events are included for write and read operations.
   - Monitoring with IBM Cloud Monitoring with Sysdig is enabled.
   - Expiration rules that define when archive files are automatically deleted are configured. As guidance, events must be kept for as long as internal compliance requires. If no requirements exist, consider a rule that keeps files for a minimum of 365 days.
   - [Optional] A retention policy is configured so that objects are protected from deletion or overwriting for a specified amount of time.
     Note: A retention policy is not supported when Key Protect is enabled.
   - [Optional] An archive policy is configured so that objects that are rarely accessed are moved from their default bucket storage class to the archive storage class after a certain period.
6. Ensure that you use different credentials to archive data from your audit instance to your bucket.
   - Consider using a service ID for each audit instance to configure the archiving of data so that you can manage authentication and authorization permissions for each audit instance in your account.
   - A service ID is used by IBM Log Analysis with LogDNA to authenticate and access the IBM Cloud Object Storage instance.
7. Ensure that each service ID has only write permission to the bucket where you plan to archive the events.
8. Ensure that archive files are not corrupted.

To verify that archiving is configured for an audit instance in your account, complete the following steps:
Repeat these steps for all the audit instances in the account.
Note: To complete these steps, your IBM Cloud user ID (IBMid) must have the following roles:

- A platform role with viewer role for the IBM Cloud Activity Tracker with LogDNA service for the account
- A platform role with operator role for the IBM Cloud Object Storage service for the account
- A service role with manager role for the IBM Cloud Activity Tracker with LogDNA service for the account so that you can verify that archiving is configured

UI instructions:

1. Log in to IBM Cloud at https://cloud.ibm.com.

2. Go to the Menu icon. Then, select **Observability** to access the *Observability* dashboard.
3. Select **Activity Tracker** from the page navigation menu
4. For each audit instance, complete the following steps:
    - Check the service plan is one that includes search days.
    - Check that archiving is configured for each audit instance.
        - To launch the LogDNA web UI, select **View LogDNA**.
        - In the LogDNA web UI, select **Settings**. Then, select **Archiving**.
        - Verify that archiving is configured for the audit instance.
            - Check the bucket name.
            - Check the endpoint value to make sure that the private endpoints are configured. To verify the correct value, you must check the bucket configuration in IBM Cloud Object Storage.
            - Check the permissions granted to the API key, limit write access to the audit instance only. To verify the permissions, you must identify the credential (service ID) on which you restricted permissions.
            - Check that the Cloud Object Storage instance ID is the one where data should be archived. You might have different COS instances to archive data.
5. Expand the Navigation Menu and select **Resource list**. Find the COS instance where the bucket that is configured for archiving is available.
    - Open the COS console, and select the bucket.
    - Check the bucket configuration. Check for compatibility of policies and how the ones that are configured for a bucket meet your requirements:
        - Check that a key management service is configured.
        - Check that Activity Tracker is configured.
        - Check that monitoring is configured.
        - Check each expiration.
        - Check the retention policy is configured.
        - Check the archive policy is configured.
    - Check that events are archived and the archive files are not corrupted:
        - Download a subset of files, preferably with different dates and sizes.
        - Open the files and verify that you can read the content.
6. From the Menu bar, click **Manage > Access (IAM)**.
7. Check the service ID policies:
    - Select **Service IDs**.
    - Find the service ID that is configured in the LogDNA instance.
    - To open the Service ID dashboard, select the service ID.
    - Verify the service ID has write permission on the COS bucket.
        - Select **Access Groups**. Verify that the permissions the service ID gets through each access group are valid.
        - Select **Access Policies**. Verify that the permissions are valid.

Remediation:

1. If the option to configure archiving is not allowed, upgrade the instance's service plan.
2. If archiving is not enabled for an instance, review and define the archiving strategy. Then, configure archiving for an audit instance.
3. If you cannot find an instance of IBM Cloud Object Storage (COS) in your account, provision one.
4. If you have a bucket that does not have full control over the data encryption keys, configure one of the supported options. IBM® Cloud Object Storage provides several options to encrypt your data.
5. If you have a bucket that does not have an expiration rule to automatically delete objects, configure one for the bucket based on your compliance and organizational requirements. The minimum expiration must be 365 days. For more information, see Delete stale data with expiration rules.
6. If you have a bucket that does not have an archive policy to store long-term data that is rarely accessed, configure one for the bucket based on your compliance and organizational requirements. For more information, see Archive cold data with transition rules.
7. If you have a bucket that does not have Activity Tracker events enabled so that you can monitor any interaction of users and services with the bucket, enable Activity Tracker events for the bucket.
8. If you have a bucket that does not enable monitoring with IBM Cloud Monitoring with Sysdig, configure the bucket.
9. If you want to create a bucket, see create and configure a bucket.
    - Configure one of the supported options to add additional encryption capabilities. For more information, see IBM® Cloud Object Storage provides several options to encrypt your data.
    - Configure an expiration rule to automatically delete objects. Configure a rule for the bucket based on your compliance and organizational requirements. The minimum expiration must be 365 days. For more information, see Delete stale data with expiration rules.
    - Configure an archive policy to store long-term data that is rarely accessed. Configure a policy for the bucket based on your compliance and organizational requirements. For more information, see Archive cold data with transition rules.
    - Enable Activity Tracker events on the bucket so that you can monitor any interaction of users and services with the bucket. For more information, see enable Activity Tracker events for the bucket.
    - Enable monitoring for the bucket.
    - If the service ID that is used to archive events from a LogDNA instance to a COS bucket does not have restricted permissions to be able to write only to the bucket that is specified in the configuration, modify the permissions. Ensure that the policies that are granted to the service ID only grant permissions to write to the bucket defined in the LogDNA archiving configuration.

- If the file is corrupted or an archive file is not available in your bucket, open a ticket with IBM. Make sure that you claim the data before reaching the maximum number of search days that is indicated in the service plan. Data is lost after it reaches the maximum number of search days.

Default Value:

By default, archiving of events and metadata is not enabled for any audit instance.

IBM Cloud Activity Tracker with LogDNA does not backup your data. You are responsible for archiving your events. When you enable archiving of your data, you are responsible for checking that your archived files are not corrupted, and the maintenance of your archived files.

References:

1. IBM Cloud Activity Tracker with LogDNA: Adoption guidelines for regulated and highly available workloads: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=logdnaat-adoption
2. IBM Cloud Activity Tracker with LogDNA service plans: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=logdnaat-service_plan
3. IBM Cloud Object Storage: https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-getting-started
4. IBM Cloud Object Storage managing encryption: https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-encryption

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.

3.3 Ensure that events are collected and processed to identify anomalies or abnormal events (Manual)

Profile Applicability:

- Level 1

Description:

Events that you collect and centralize in the IBM Cloud Activity Tracker with LogDNA service provide information about actions that take place on your account. You can analyze this data to resolve problems, identify anomalies, and be notified of abnormal situations.

Rationale:

IBM Cloud Activity Tracker with LogDNA adds audit capabilities to your IBM Cloud architecture.

Each event reports information about who requested an action on your account (initiator details), what action was requested, the resource on which the action was requested (target details), and outcome of the request. Each event is based on the Cloud Auditing Data Federation (CADF) standard. For more information about the IBM event definition, see Event types and Event fields.

In IBM Cloud Activity Tracker with LogDNA (AT), events from core IBM Cloud platform services are collected automatically and available for analysis through the audit instances in your account. Events are also collected automatically for enabled-AT services. However, some services might require an upgrade of the service plan, a configuration setting, or both, for you to be able to collect and analyze them.

Core platform Activity Tracker events are available for all IBM Cloud services. These events include provisioning and deletion of service instances, tagging, and IAM management.

Through an audit instance, you can troubleshoot events in real time to diagnose issues and identify problems.

By using the live streaming tail feature in the **Everything view**, you can diagnose issues, analyze stack traces and exceptions, identify the source of errors, and monitor different event sources through a single view.

By using custom views, you can show a subset of data by applying pre-defined filters and natural language queries to the **Everything View**.

Impact:

The recommended custom views allow you to monitor actions that take place in your account, the level of threat of those actions in your account, and abnormal situations. If you are missing any of these views and the ability to check that events are available through them, exposes a potential security risk by hiding a possible gap of events that are critical to control what happens in the account. In addition, views can have alerts attached to them so that you are notified quickly of abnormal situations. If you do not have the right views, you lose the ability to configure alerts and pre-empt situations that might require your attention.

Audit:

Use the following checklist to ensure that events are collected and processed to identify anomalies or abnormal events:
This checklist assumes that you have a different IBM Cloud account for development, staging, Q&A, and production. When you separate accounts by domain (for example, production versus development), you isolate events for each domain and location. You can only have one Activity Tracker instance in each region and each account. You use IAM to define permissions to view and manage events in an instance.
Note: When a user gets read permissions to see events in an Activity Tracker instance, the user gets visibility of all events in the region. Therefore, separate domains by account to avoid exposing production logs to non-authorized users.

Checklist

The checklist must be applied to each environment independently.

1. Ensure that events from core IBM Cloud core platform services, such as IAM are collected and available through the audit instance in Frankfurt. Check that each core service has one or more custom views to analyze the data.
   Note: These types of events are only available for the search period. You might have to pull archive data to verify these events, or run a test to see that they are being generated properly.
   - Check that you see provisioning events
   - Check that you see IAM identity login events
   - Check that you see IAM access group and policy events.
2. Ensure that events from enabled IBM Cloud services are collected in each region where you operate. Check that events are available in the audit instance that is available in the same region as your service instances.
   - Check for additional configuration steps that a service might require.
   - Check that you have a custom view for each service.

    - Check that events for a specific service are available for analysis through the custom view.
3. Views can be classified in categories. For example, a category might be aligned with a line of business.
    - Ensure that views are grouped in categories.
    - Check that each view belongs to the correct category.
4. Check that custom views are defined for each service to monitor events that have an outcome of failure.
5. Check that custom views are defined for each service to monitor events that report high level threat actions in your account. These events report deletion actions in the account.
6. Check that custom views are defined for each service to monitor events that report changes to resources in the account. For example, these events report actions that modify the state of a resource in your account.
7. Check that custom views are defined for each service to monitor events that report unauthorized or forbidden access to run actions in the account.
8. Check that custom views are defined for each service to monitor events that report user management actions in the account.
9. Check that custom views are defined for each service to monitor events that report actions on user management and related IAM actions.

UI Instructions

UI instructions that you can use to check that you have custom views to monitor activity in your account:

1. Log in to IBM Cloud at `https://cloud.ibm.com`.
2. Go to the Menu icon. Then, select **Observability** to access the *Observability* dashboard.
3. Click **Activity Tracker**.
4. Look for views that report events from core IBM Cloud core platform services, such as IAM. Check that the search criteria of the views match the query indicated in the search criteria provided.
    - Check that each view displays events with actions listed in the Events that are generated section.
    - Check the description of each view and ensure that it is clear and reflects the type of events that are available through the view.
    - Name your view according to your organization's naming convention.

    Service to check: *IAM Identity*

```
 Query: *_platform:iam-identity*

 Events that are generated: [Events that are generated when a user or
app logs in to the IBM Cloud](https://cloud.ibm.com/docs/Activity-
Tracker-with-LogDNA?topic=Activity-Tracker-with-LogDNA-
at_events_iam#at_events_iam_login)

 Activity Tracker instance location: *Frankfurt*
```

Service to check: *IAM Access Management (IAM AM)*

```
 Query: *_platform:iam-am*

 Events that are generated: [Events that are generated when you manage
IAM policies](https://cloud.ibm.com/docs/Activity-Tracker-with-
LogDNA?topic=Activity-Tracker-with-LogDNA-
at_events_iam#at_events_iam_policies)

 Activity Tracker instance location: *Frankfurt*
```

Service to check: *IAM Groups*

```
 Query: *_platform:iam-groups*

 Events that are generated: [Events that are generated when you manage
access groups](https://cloud.ibm.com/docs/Activity-Tracker-with-
LogDNA?topic=Activity-Tracker-with-LogDNA-
at_events_iam#at_events_iam_access)

 Activity Tracker instance location: *Frankfurt*
```

5. Look for views that report events from enabled IBM Cloud services.
    - Check that the search query to filter data in the custom view is in the following format:

      ```
      _platform:<Service Name>
      ```

    - Check the description for each view.
    - Check that the name of each view follows your organization's naming convention.

   To see the list of available services, see Cloud services.
   To see where events are available for analysis, see Cloud services locations.

6. Check that views are organized and grouped by category.
   a. In the LogDNA web UI, select Settings. Then, select Categories.
   b. Select Views.
   c. Check the views that are within each category.
7. Look for views that report events that fail from enabled IBM Cloud services.
    - Check that the search query to filter data in the custom view is in the following format:

```
_platform:<Service Name> AND outcome:failure
```

- Check the description for each view.
- Check that the name of each view follows your organization’s naming convention.

To see the list of available services, see Cloud services.

To see where events are available for analysis, see Cloud services locations.

8. Look for views that report high level of threat actions in your account.
    - Check that the search query to filter data in the custom view is in the following format:

    ```
    _platform:<Service Name> AND severity:critical
    ```

    - Check the description for each view.
    - Check that the name of each view follows your organization’s naming convention.

    To see the list of available services, see Cloud services.

    To see where events are available for analysis, see Cloud services locations.

9. Look for views that report actions that modify the state of resources in your account.
    - Check that the search query to filter data in the custom view is in the following format:

    ```
    _platform:<Service Name> AND severity:warning
    ```

    - Check the description for each view.
    - Check the name of each view follows your organizations naming convention.

    To see the list of available services, see Cloud services.

    To see where events are available for analysis, see Cloud services locations.

10. Look for views that report unauthorized or forbidden permissions on in your account.
    - Use the following search query to check that the custom view reports unauthorized access to run the action due to lack of permissions (RC 401):

    ```
    reason.reasonCode:401
    ```

    - Use the following search query to check that the custom view reports forbidden access to run the action due to missing credentials (RC 403):

```
reason.reasonCode:403
```

- Check the description for each view.
- Check that the name of each view follows your organization's naming convention.

11. Look for views that report user management actions in your account.
    - Use the following search query to check that the custom view reports user management actions in the account:

```
(_platform:BSS AND action:user-management)
```

    - Use the following search query to check user management and related IAM actions in your account:

```
-(_platform:iam-identity AND (action login)) AND  (_platform:iam
OR (_platform:BSS AND action:user-management))
```

    - Check the description for each view.
    - Check that the name of each view follows your organization's naming convention.
12. Look for views that report successful logins in your account.
    - Use the following search query to check the custom view:

```
_platform:iam-identity AND (action login)
```

    - Check the description for each view.
    - Check that the name of each view follows your organization's naming convention.
13. Look for views that report Security Advisor findings, that is, security incidents that are monitored by IBM Cloud Security Advisor in your account.
    - Check the description for each view.
    - Check that the name of each view follows your organization's naming convention.

Remediation:

UI instructions that you can use to create custom views when one or more are missing in the account:

1. Log in to IBM Cloud at `https://cloud.ibm.com`.
2. Click the Menu icon.
3. Click **Observability > Activity Tracker**.
4. If you are missing views to monitor events from core IBM Cloud core platform services, such as IAM, create custom views for each of the following services. Use the search criteria provided.

    - Check that each view displays events with actions listed in the Events that are generated section.
    - Add a description to each view.
    - Name your view according to your organization’s naming convention.

    Service to check: *IAM Identity*

```
 Query: *_platform:iam-identity*

 Events that are generated: [Events that are generated when a user or
app logs in to the IBM Cloud](https://cloud.ibm.com/docs/Activity-
Tracker-with-LogDNA?topic=Activity-Tracker-with-LogDNA-
at_events_iam#at_events_iam_login)

 Activity Tracker instance location: *Frankfurt*
```

    Service to check: *IAM Access Management (IAM AM)*

```
 Query: *_platform:iam-am*

 Events that are generated: [Events that are generated when you manage
IAM policies](https://cloud.ibm.com/docs/Activity-Tracker-with-
LogDNA?topic=Activity-Tracker-with-LogDNA-
at_events_iam#at_events_iam_policies)

 Activity Tracker instance location: *Frankfurt*
```

    Service to check: *IAM Groups*

```
 Query: *_platform:iam-groups*

 Events that are generated: [Events that are generated when you manage
access groups](https://cloud.ibm.com/docs/Activity-Tracker-with-
LogDNA?topic=Activity-Tracker-with-LogDNA-
at_events_iam#at_events_iam_access)

 Activity Tracker instance location: *Frankfurt*
```

5. If you are missing views to monitor events from enabled IBM Cloud services, create custom views for each one of them.
    - Use the following search query to filter data in the custom view:

```
_platform:<Service Name>
```

    - Add a description to each view.
    - Name your view according to your organization’s naming convention.

    To see the list of available services, see [Cloud services](#).
    To see where events are available for analysis, see [Cloud services locations](#).

6. If views are not organized and grouped by category, create as many categories as you want, and assign views.
    1. In the LogDNA web UI, select **Settings**. Then, select **Categories**.
    2. Select **Views**.
    3. Click **Add a Category**.
    4. Enter the name of the category.
    5. Drag views from the *All Views* section to the new category.
7. If you are missing views to monitor events from enabled IBM Cloud services that report failures, create custom views for each one of them.
   Use the following search query to filter data in the custom view:

   ```
   _platform:<Service Name> AND outcome:failure
   ```

   Add a description to each view.

   Name your view according to your organization's naming convention.

   To see the list of available services, see Cloud services.

   To see where events are available for analysis, see Cloud services locations.

8. If you are missing views to monitor events that report high level of threat actions in your account, create custom views for each one of them.
   Use the following search query to filter data in the custom view:

   ```
   _platform:<Service Name> AND severity:critical
   ```

   Add a description to each view.

   Name your view according to your organization's naming convention.

   To see the list of available services, see Cloud services.

   To see where events are available for analysis, see Cloud services locations.

9. If you are missing views to monitor events that report actions that modify the state of resources in your account, create custom views for each one of them.
   Use the following search query to filter data in the custom view:

   ```
   _platform:<Service Name> AND severity:warning
   ```

   Add a description to each view.

   Name your view according to your organization's naming convention.

   To see the list of available services, see Cloud services.

   To see where events are available for analysis, see Cloud services locations.

10. If you are missing views to monitor events that report unauthorized or forbidden permissions in your account, create custom views for each one of them.
    Use the following search query to filter data in the custom view that reports unauthorized access to run the action due to lack of permissions (RC 401):

```
reason.reasonCode:401
```

Use the following search query to filter data in the custom view that reports forbidden access to run the action due to missing credentials (RC 403):

```
reason.reasonCode:403
```

Add a description to each view.
Name your view according to your organization's naming convention.

11. If you are missing views to monitor events that report user management actions in your account, create custom views for each one of them.
    Use the following search query to filter data in the custom view that report user management actions in the account:

```
(_platform:BSS AND action:user-management)
```

Use the following search query to filter data in the custom view to report user management and related IAM actions in your account:

```
-(_platform:iam-identity AND (action login)) AND  (_platform:iam OR
(_platform:BSS AND action:user-management))
```

Add a description to each view.
Name your view according to your organization's naming convention.

12. If you are missing views to monitor events that report successful logins in your account, create a custom view.
    Use the following search query to filter data in the custom view:

```
_platform:iam-identity AND (action login)
```

Add a description to the view.
Name your view according to your organization's naming convention.

13. If you are missing views to monitor events that report Security Advisor findings, that is, security incidents that are monitored by IBM Cloud Security Advisor in your account, check that the Security Advisor service is provisioned in the account. Then, create a custom view for each integrated platform service.
    For example, for Certificate Manager findings, use the following search query to filter data in the custom view:

```
initiator.name:'IBM Certificate Manager' host:security-advisor
action:security-advisor.findings.write
```

Add a description to the view.
Name your view according to your organization's naming convention.

Default Value:

IBM Cloud Activity Tracker with LogDNA does not include default templates for views or alerts.

You can define your own views, alerts, and notification channels. Default notification channels are configured by using presets.

References:

1. IBM Cloud Activity Tracker with LogDNA: Adoption guidelines for regulated and highly available workloads: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=logdnaat-adoption
2. IBM Cloud Activity Tracker with LogDNA service plans: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=logdnaat-service_plan

CIS Controls:

Version 7

6.6 Deploy SIEM or Log Analytic tool
Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.

6.7 Regularly Review Logs
On a regular basis, review logs to identify anomalies or abnormal events.

3.4 Ensure alerts are defined on custom views to notify of unauthorized requests, critical account actions, and high-impact operations in your account (Manual)

Profile Applicability:

- Level 2

Description:

Events that you collect and centralize in the IBM Cloud Activity Tracker with LogDNA service provide information about actions that take place on your account. You can define alerts to notify promptly of problems, anomalies, and abnormal situations.

Rationale:

IBM Cloud Activity Tracker with LogDNA adds audit capabilities to your IBM Cloud architecture.

Each event reports information about who requested an action on your account (initiator details), what action was requested, the resource on which the action was requested (target details), and outcome of the request. Each event is based on the Cloud Auditing Data Federation (CADF) standard. For more information about the IBM event definition, see Event types and Event fields.

Events from enabled IBM Cloud services and core IBM Cloud platform services are collected automatically and available for analysis through the audit instances in your account. Check out the services that send events to the platform service events instance.

Core platform Activity Tracker events are available for all IBM Cloud services. These events include provisioning and deletion of service instances, tagging, and IAM management.

By using the live streaming tail feature through the **Everything view**, you can diagnose issues, analyze stack traces and exceptions, identify the source of errors, and monitor different event sources through a single view.

By using custom views, you can show a subset of data by applying pre-defined filters and natural language queries to the **Everything view**.

On custom views, you can issue alerts to be notified of important actions. To act promptly on events that you identify as critical or warning, DevOps teams can configure alert notification integrations to the following systems: email, Slack, web hook, and PagerDuty.

Impact:

The recommended alerts on custom views allow you to monitor actions that take place in your account, the level of threat of those actions in your account, and abnormal situations. If you are missing any of these views and the ability to check that events are available through them, exposes a potential security risk by hiding a possible gap of events that are critical to control what happens in the account. In addition, views can have alerts attached to them so that you are notified quickly about abnormal situations. If you do not have the right views, you lose the ability to configure alerts and pre-empt situations that might require your attention.

Audit:

Use the following checklist to ensure that events are collected and processed to identify anomalies or abnormal events.
This checklist assumes that you have a different IBM Cloud account for development, staging, Q&A, and production. The checklist must be applied to each environment independently.

1. Check that alerts are defined based on templates, known as presets in LogDNA. When you use a preset, you can manage access control to notifications from a centralize location.
   The alert condition should indicate the following information:
   - Type of alert: presence
   - Condition: Notify when 1 or more matches appear within 1 minute
   - Send the alert when 1 line shows in the view

   For example, when you configure an email alert, using a preset helps you manage access control to alert notifications. When a user configures an email alert directly on a view, you specify directly on the view's alert who the recipients are. If you decide to remove a user, you must manually delete that user from the alert. If you have multiple views, you must check view by view that the user is not a recipient of the email alert.

2. For each custom view, check the purpose of the view and what notification channels are configured.
   - Email alerts: Check that an email alert is used to verify that the alert on a view is working, and to inform users of situations about which they have requested information.
   - Slack alerts: Check that a Slack alert is used to inform users about routine scenarios that they might want to monitor.
   - PagerDuty alert: Check that a PagerDuty alert is used to notify users immediately so that they can take prompt action.

   - Webhook alerts: Check that a webhook alert is used when users want to use a third-party tool to get and manage notifications.
3. Check that alerts have been configured for each of the following custom views:
   - Custom views that are defined for each service to monitor events that have an outcome of failure.
   - Custom views that are defined for each service to monitor events that have a severity set to critical. These events report deletion actions in the account.
   - Custom views that are defined for service to monitor events that have a severity set to warning. These events report actions that modify the state of a resource in your account.
   - Custom views that are defined for each service to monitor events that have a reason code set to 403 or 409. These events report requests on a service that are not authorized.
   - Custom views that are defined for each service to monitor events that report actions on access groups, changes of policies, user management, service IDs. These events report IAM actions in the account.
   - Custom views that report Security Advisor findings, that is, security incidents that are monitored by IBM Cloud Security Advisor in your account.

UI instructions that you can use to check that alerts on custom views are defined and working.
This checklist assumes that you have a different IBM Cloud account for development, staging, Q&A, and production. The checklist must be applied to each environment independently.

1. Log in to IBM Cloud at `https://cloud.ibm.com`.
2. Go to the Menu icon. Then, select **Observability** to access the *Observability* dashboard.
3. Click **Activity Tracker**.
4. For each region where you run operations, launch the Activity Tracker in that region by clicking **View LogDNA**. Then, complete the following steps. You must always check Frankfurt because this region is where platform information is available.
5. Check that alert definitions and notification channels are defined:
   - Select **Settings**. Then, select **Alerts**.
   - Check that alerts are defined based on templates, known as presets in LogDNA.
   - In the **View-specific alerts** section, check for individual alerts. If you have individual alerts, identify the type (email, Slack, webhook, PagerDuty), the LogDNA view that is associated with the alert, and notification destination. Check that there is a business need for the alert.
   - In the **Presets** section, check that each notification channel is correct and has valid destinations. Then, check that the views that are included in each preset send alerts to the destinations that are configured in the preset.
6. Check that all views outlined in the previous control have at least one alert notification channel configured:

    - Select **Views**.
    - For each view, select the view name. Then, select **Edit alert**.
    - Select each notification channel, and verify the condition:
        - Type of alert: presence
        - Condition: Notify when 1 or more matches appear within 1 minute
        - Send the alert when 1 line shows in the view
    - For each notification channel, verify the purpose of the alert and the configuration details:
        - Email alerts: Check that an email alert is used to verify that the alert on a view is working, and to inform users about situations that they have requested information about. Check that the recipient is a functional ID. If individual users are included in the recipients, check that they have clearance to access the information.
        - Slack alerts: Check that a Slack alert is used to inform users about routine scenarios that they might want to monitor. Check that the webhook corresponds to a channel and the people in the channel have clearance to access the information.
        - PagerDuty alert: Check that a PagerDuty alert is used to notify users immediately so that they can take prompt action. Check that the PagerDuty (PD) credentials correspond to the PD instance where you are managing alerts.
        - Webhook alerts: Check that a webhook alert is used when you want to use a third-party tool to get and manage notifications. Check the webhook configuration is valid and goes to the third-party tool.

7. For each custom view and alert notification channel, verify that you see an alert notification so that you can validate that the alert is being generated.

Remediation:

UI instructions that you can use to create alerts on custom views:

1. Log in to IBM Cloud at`https://cloud.ibm.com`.
2. Click the Menu icon.
3. Click **Observabilty > Activity Tracker**.
4. For each region where you run operations, launch the Activity Tracker in that region by clicking View LogDNA . Then, complete the following steps. You must always check Frankfurt because this region is where platform information is available.
5. Configure alerts on views for each audit instance.

Default Value:

IBM Cloud Activity Tracker with LogDNA does not include default templates for views or alerts.

You can define your own views, alerts, and notification channels.

Default notification channels are configured by using presets.

References:

1. IBM Cloud Activity Tracker with LogDNA: Adoption guidelines for regulated and highly available workloads: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=logdnaat-adoption
2. IBM Cloud Activity Tracker with LogDNA service plans: https://cloud.ibm.com/docs/Activity-Tracker-with-LogDNA?topic=logdnaat-service_plan

CIS Controls:

Version 7

6.6 Deploy SIEM or Log Analytic tool
Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.

6.7 Regularly Review Logs
On a regular basis, review logs to identify anomalies or abnormal events.

6.8 Regularly Tune SIEM
On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

3.5 Ensure the account owner can login only from a list of authorized countries/IP ranges (Manual)

Profile Applicability:

- Level 1

Description:

Monitor the account owner's access to the IBM Cloud account is done from authorized locations that are restricted by IP addresses.

Rationale:

By default, a user can log in from any IP address.

In IBM Cloud, you can restrict a user to log in only from specific IP addresses. Therefore, you can define for the account owner the list of IP addresses that are allowed. Other IP addresses will be restricted.

This configuration feature per user allows you to restrict access from controlled locations and adds an additional level of security into your IBM Cloud account.

When a user such as the account owner logs in, information about its IP address is included in the Activity Tracker security event. You can monitor and be notified when this event is generated in the account. You can obtain in the security event information about unauthorized location.

Impact:

Failure to meet this control limits your ability to control that the account manager can only access and operate in the account from locations that are authorized and allowed by your organization.

Audit:

Complete the following steps to check if you monitor the locations from which the account owner logs in to the account:
First, you need to identify the email of the account owner.

1. In the Cloud UI, go to **Manage > Access (IAM)**, then select **Users**.
2. Identify the user that has the tag *owner*.
3. Select the account owner. Then, click **Details**.
4. Copy the email address of the account owner.

Second, launch the Activity Tracker instance in Frankfurt. This is the instance where login security events are collected in the account.
In the *Views* section, look for a view that monitors the account owner login attempts. The search query should be set to: `(action login) AND initiator.name:<email address> AND -initiator.host.address:(<list of IP addresses>)`, where is the account owner email address, and is the list of authorized IP addresses that are separated by `OR`, for example, (xxx.xxx.xxx.xxx OR xxx.xxx.xxx.xxx).
Then, check that the view has configured an alert and 1 or more notification channels.

Remediation:

Complete the following steps to monitor the locations from which the account owner logs in to the account:
First, you need to identify the email of the account owner.

1. In the Cloud UI, go to **Manage > Access (IAM)**, then select **Users**.
2. Identify the user that has the tag *owner*.
3. Select the account owner. Then, click **Details**.
4. Copy the email address of the account owner and the list of authorized IP addresses.

Launch the Activity Tracker instance in Frankfurt. This is the instance where login security events are collected in the account. In the *Views* section, select the **Everything** view. Then, enter the following query in the search bar: `(action login) AND initiator.name:<email address> AND -initiator.host.address:(<list of IP addresses>)`. Replace with the account owner's email address. Replace with the list of IP addresses that are separated by `OR`, for example, (xxx.xxx.xxx.xxx OR xxx.xxx.xxx.xxx) and configured for the account owner. The view now reports all the events that are reported when the account owner tries to login from an unauthorized location.
Next, you can define an alert on the view to get a notification immediately after 1 event is received.

Default Value:

There is no default value.

CIS Controls:

Version 7

16.13 Alert on Account Login Behavior Deviation
Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

3.6 Ensure Activity Tracker data is encrypted at rest (Manual)

Profile Applicability:

- Level 1

Description:

Ensure Activity Tracker data is encrypted at rest.

Rationale:

LogDNA uses encrypted storage for all its rest data.

Customers can elect to archive the Activity Tracker data to an IBM Cloud Object Storage (COS) bucket for long-term storage. By default, all objects that are stored in COS are encrypted by using randomly generated keys and an all-or-nothing-transform (AONT). Cloud Object Storage further supports additional key management scenarios to encrypt your data. This encryption model is called customer-managed encryption:

1. You can manage your keys manually by providing your own encryption keys - referred to as Server-Side Encryption with Customer-Provided Keys (SSE-C).
2. You can choose to use the integration capabilities with IBM Cloud® Key Management Services like IBM® Key Protect and Hyper Protect Crypto Services.

Impact:

Failure to adopt a customer-managed encryption model for audit data that is archived for long-term storage can breach infrastructure compliance where you are required to use your keys for encrypting data that you manage.

Audit:

1. Ensure that you need long-term storage of your audit data.
2. Ensure that archiving is enabled on each of the Activity Tracker instances in your account.
3. If archiving is enabled, ensure that you have access to storage, for example, check that you have an instance of the IBM Cloud Object Storage service provisioned in your account.
4. Ensure that you have multiple COS buckets available to archive your data. Check the bucket configuration to verify that it meets your corporate and external market regulations.
   Consider using a bucket for each audit instance so that you can customize the bucket to meet security requirements. These requirements might be related to the type of

data that is archived and to external regulations like EU-managed requirements, for example.
5. Ensure that the CIS control `Ensure that archiving is enabled for audit events` is met.

Remediation:

If you need long-term storage of your audit data and you do not have Cloud Object Storage configured to archive the data from your Activity Tracker instances, complete the following steps:

1. If the option to configure archiving is not allowed, upgrade the instance's service plan.
2. If archiving is not enabled for an instance, review and define the archiving strategy. Then, configure archiving for an audit instance.
3. If you cannot find an instance of IBM Cloud Object Storage (COS) in your account, provision one.
4. If you have a bucket that does not have full control over the data encryption keys, configure one of the supported options. IBM® Cloud Object Storage provides several options to encrypt your data.

Default Value:

LogDNA uses encrypted storage for all its rest data.

By default, all objects that are stored in COS are encrypted by using randomly generated keys and an all-or-nothing-transform (AONT).

References:

1. IBM Cloud Object Storage: https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-getting-started
2. IBM Cloud Object Storage managing encryption: https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-encryption

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.

3.7 Ensure Activity Tracker trails are integrated with LogDNA Logs (Manual)

Profile Applicability:

- Level 1

Description:

Check whether Activity Tracker trails are integrated with LogDNA Logs.

Rationale:

IBM Cloud™ Activity Tracker with LogDNA is a Cloud service that you can use to monitor the activity of your IBM Cloud account. IBM Log Analysis with LogDNA is a service that you can use to analyze and monitor operational logs. Both services offer the same features to manage audit events and logs. However, Activity Tracker trails are not integrated with LogDNA Logs.

- The data that is collected and processed by the IBM Cloud Activity Tracker with LogDNA service is associated with that location and not visible to the other regions by virtue of this association.
- The data that is collected and processed by the IBM Log Analysis with LogDNA service is associated with that location and not visible to the other regions by virtue of this association.
- Within a service instance, data is isolated per LogDNA instance within a region. The IBM Cloud Activity Tracker with LogDNA service offers soft isolation for data storage. Data is mixed together in the same data stores and segmented by tags that are associated with each of the records to enforce access control policies.

When audit data and logs are archived for long-term storage, archives of your operational logs and auditing events can be archived to the same IBM Cloud Object Storage (COS) location.

Impact:

Failure to meet this control will prevent you from managing long-term data, logs and audit events, from a common location.

Audit:

Use the following checklist to ensure Activity Tracker trails are integrated with LogDNA Logs:

1. Ensure that IBM Cloud Activity Tracker with LogDNA instances are provisioned with a service plan that includes the ability to configure archiving to an external storage service.
2. Ensure that IBM Log Analysis with LogDNA instances are provisioned with a service plan that includes the ability to configure archiving to an external storage service.
3. Ensure that you have access to storage, for example, check that you have an instance of the IBM Cloud Object Storage service provisioned in your account.
4. Ensure that you have 1 COS bucket available to archive your data. Check the bucket configuration to verify that it meets your corporate and external market regulations.
5. Ensure that each audit instance has archiving enabled and configured to the bucket identified in step 4.
6. Ensure that each logging instance has archiving enabled and configured to the bucket identified in step 4.

To check if audit and logging instances are provisioned and configured in the account, complete the following steps:
Note: To complete these steps, your IBM Cloud user ID (IBMid) must have the following roles:

- A platform role with viewer role for the IBM Cloud Activity Tracker with LogDNA service and the IBM Log Analysis with LogDNA service for the account
- A service role with reader role for the IBM Cloud Activity Tracker with LogDNA service and the IBM Log Analysis with LogDNA service for the account
- A platform role with viewer role for the IBM Cloud Object Storage service for the account
- Identity and Access Management (IAM) permissions to view access groups in the account

UI instructions:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Go to the Menu icon. Then, select **Observability** to access the *Observability* dashboard.
3. Select **Activity Tracker** from the page navigation menu to see the auditing instances. Select **Logging** from the page navigation menu to see the logging instances.
4. Check that you can see an Activity Tracker instance in Frankfurt and one instance for each location where you operate in the IBM Cloud.
5. To launch the LogDNA web UI, for each instance, select *View LogDNA*.
6. In the LogDNA web UI, verify that you can see audit events.
7. Identify the LogDNA instance ID in the LogDNA URL. This ID is used as part of the name of the archive file.

CLI instructions:

1. Log in to IBM Cloud.
   Run the following command:
   ```
   ibmcloud login -a cloud.ibm.com
   ```
   For a federated account, run the following command:
   ```
   ibmcloud login -a cloud.ibm.com --sso
   ```
2. List all the audit instances that are provisioned in your account.
   Run the following command:
   ```
   ibmcloud resource service-instances --service-name logdnaat --all-
   resource-groups
   ```
   List all the logging instances that are provisioned in your account. Run the following command:
   ```
   ibmcloud resource service-instances --service-name logdna --all-
   resource-groups
   ```
3. For Activity Tracker, check that you have one instance in Frankfurt, and one instance for each location where you operate in the IBM Cloud.
4. Get the LogDNA instance ID. This value is used as part of the archive file name. Run the following command:
   ```
   ibmcloud resource service-instance INSTANCE_NAME --output JSON | grep
   dashboard_url
   ```

To check the COS instance and bucket in the account where logs and events are archived, complete the following steps:

1. Identify the CRN of the COS instance where archived data must be located.
   Run the following command to get the list of instances that are available in the account and their CRNs:
   ```
   ibmcloud resource service-instances --type service_instance --service-
   name cloud-object-storage --all-resource-groups --output JSON
   ```
2. Identify the bucket.
   Run the following command to list all the buckets that are available in the COS instance:
   ```
   ic cos list-buckets --ibm-service-instance-id <INSTANCE-CRN>
   ```
3. For each LogDNA instance, identify the corresponding archive files for that instance.
   Run the following command:
   ```
   ic cos list-objects --bucket <BUCKET-NAME> --region <REGION-NAME>
   ```
   Note: You must see archive files that include the LogDNA instance ID. If you cannot see any files for that instance, then that instance is not being archived to the bucket.

To verify that archiving is enabled in a LogDNA instance, complete the following steps:
Note: To complete these steps, your IBM Cloud user ID (IBMid) needs the following roles in addition to the ones specified earlier:

- A platform role with operator role for the IBM Cloud Object Storage service for the account

- A service role with manager role for the IBM Cloud Activity Tracker with LogDNA service and the IBM Log Analysis with LogDNA service for the account, so that you can verify that archiving is configured

UI instructions:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Go to the Menu icon. Then, select **Observability** to access the *Observability* dashboard.
3. Select **Activity Tracker** or **Logging** from the page navigation menu
4. For each instance, check that archiving is configured for each audit instance.
    - To launch the LogDNA web UI, select **View LogDNA**.
    - In the LogDNA web UI, select **Settings**. Then, select **Archiving**.
    - Verify that archiving is configured for the audit instance.
    - Check the bucket name.
    - Check the endpoint value to make sure that the private endpoints are configured. To verify the correct value, you must check the bucket configuration in IBM Cloud Object Storage.
    - Check the permissions granted to the API key, limit write access to the audit instance only. To verify the permissions, you must identify the credential (service ID) on which you restricted permissions.
    - Check that the Cloud Object Storage instance ID is the one where data should be archived. You might have different COS instances to archive data.

Remediation:

1. If the option to configure archiving is not allowed, upgrade the instance's service plan.
2. If archiving is not enabled for an instance, review and define the archiving strategy. Then, configure archiving for an audit instance.
3. If you cannot find an instance of IBM Cloud Object Storage (COS) in your account, provision one.
4. If you want to create a bucket, see create and configure a bucket.

Default Value:

By default, archiving of events and logs is not enabled for any LogDNA instance.

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.

6.4 Ensure adequate storage for logs

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

4 IBM Cloud Databases Family

The IBM Cloud Databases family is a selection of ubiquitous industry databases that run as a cloud-native service with a common consumption, security, and architectural model. These databases have a common control plane API and CLI for non-database engine operations like scaling, whitelisting, reading available backups. This makes the implementation and audit of platform-level security control exactly the same across a variety of different database technology, aside from changing the name of the requested resource to match your desired product.

Databases that follow this paradigm are: Databases for PostgreSQL, Databases for MongoDB, Databases for Elasticsearch, Databases for RabbitMQ, Databases for Redis, Databases for etcd, Databases for EDB, Databases for DataStax

4.1 Ensure IBM Cloud Databases disk encryption is enabled with customer managed keys (Manual)

Profile Applicability:

- Level 1

Description:

IBM Cloud Databases provides automatic encryption at rest when provisioning the service. It is not an option to deploy a database service without encryption at rest. However, using the service's integration with IBM Key Protect, customers are able to bring their own encryption key at provision time for the database.

Before any UI or CLI commands. Follow authorization instructions between the HSM and Database service.

1. Open your IBM Cloud dashboard.
2. From the menu bar, click **Manage > Access (IAM)**.
3. In the side navigation, click **Authorizations**.
4. Click **Create**.
5. In the **Source service** menu, select the service of the deployment. For example, *Databases for PostgreSQL* or *Messages for RabbitMQ*
6. In the **Source service instance** menu, select *All instances*.
7. In the **Target service menu**, select *Key Protect*.
8. Select or retain the default value *Account* as the resource group for the Target Service 9 In the **Target service Instance ID** menu, select the service instances to authorize.
9. Under **Service access**, check the box to enable the *Reader* role.
10. Click **Authorize**.
11. Service Creation via UI or CLI with the appropriate encryption key from IBM Key Protect

Via UI:

1. Head to the respective catalog page of the service you want to provision with a customer-managed encryption key (e.g., https://cloud.ibm.com/catalog/services/databases-for-postgresql)
2. Fill out the form with the desired region, RAM, CPU, Disk, Database version, and Networking settings.
3. Click **Select a Key Protect instance**, your authorized Key Protect instances will appear in the dropdown. Select the one you want to use.

4. Directly to the right, click **Select a disk encryption key**. A list of available encryption keys from the previously selected Key Protect instance will be selectable for encrypting your database at rest.

Via CLI:

Run the following command after logging into IBM Cloud via the CLI

```
ibmcloud resource service-instance-create example-database <service-name>
standard us-south \

-p \ '{"disk_encryption_key_crn": "crn:v1:<...>:key:<id>"}'
```

Rationale:

When it comes to encryption of data at rest in IBM Cloud, we recommend for customers to manage customer root keys that are used to protect customer data stored in data and storage services in IBM Cloud. With the support of Bring Your Own Key (BYOK), customers can manage lifecycle of their customer root keys where they can create, rotate, delete those keys. This provides a significant level of control where those CRKs are managed by the customer, which in turn increases both security control as well as meet relevant compliance requirements. These CRKs are usd in turn to protect the data encryption keys used to encrypt the data.

Impact:

If a customer does not bring their own encryption key at provision time, they are not able to cryptoshred the database or revoke the database's access to the encryption key rendering it unable to boot storage.

Audit:

Through the Console:

1. Log on to your IBM Cloud account
2. Go to the **Menu icon > Resource List** to access your list of account resources
3. Click the Database service you are interested in to open the service dashboard.
4. Ensure you are on the **Manage** page in the left pane.
5. You should be on the **Overview** tab. Scroll down to the *security* section.
6. The *security* section will show an *Encryption Key* section under **Disks.** If the value shown is *Automatic Key* this means the deployment does not have a customer-managed encryption key through IBM Key Protect

Through the CLI:

1. At a minimum, have the Viewer role for the IBM Cloud Databases deployment.
2. Run `ibmcloud cdb deployment-about <CRN> [--all] [--json]` This will return the Encryption Key Status, if the deployment is created with a customer-managed encryption key, the key CRN will display here.

Remediation:

There is no zero-downtime remediation procedure . Customer must restore a backup with a new encryption key or create a net new database instance with Bring Your Own Key enabled.
To restore a backup with a new encryption key:

1. Ensure you have the Viewer Privileges on the IBM Cloud Databases deployment to read a backup file and X privileges on IBM Cloud platform to create a resource
2. Ensure you have service to service authorization set up between IBM Cloud Databases and IBM Key Protect, directions for granting this access can be found here
3. Be sure to replace SERVICE_INSTANCE_NAME and KEY PROTECT KEY CRN with a new service instance name and your desired Key Protect key CRN respectively before running this command. For more information, please view our documentation.

```
ibmcloud resource service-instance-create SERVICE_INSTANCE_NAME databases-
for-postgresql standard us-south -p '{"backup_id":"xyz-inital-
backup","disk_encryption_key_crn":"DISK_ENCRYPTION_KEY_CRN"}'
```

4. This will create a new database instance from backup with the requested customer managed encryption key.

Default Value:

The default value when creating a deployment is automatic disk and backup encryption key management by IBM Cloud Databases

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 IBM Cloud Databases are only accessible via HTTPS or TLS Connections (Manual)

Profile Applicability:

- Level 1

Description:

The IBM Cloud Databases services can only be connected to over TLS or HTTPS connections. This behavior is by default and is non-configurable. Customers are provided self-signed certificates and most appropriately configure driver or application to utilize these certificates and encryption in motion.

To connect to the database with a self-signed certificate for TLS, follow the following steps

Via UI

1. Driver you use to connect needs to be able to support encryption.
2. Copy the certificate information from the Connections panel or the Base64 field of the connection information on the IBM Cloud Databases UI.
3. If needed, decode the Base64 string into text.
4. Save the certificate to a file. (You can use the Name that is provided or your own file name).
5. Provide the path to the certificate to the driver or client.
6. Connect to database

Via CLI

1. `ibmcloud login`
2. `ibmcloud cdb`
3. `ibmcloud cdb deployment-ca-cert "CRN"`
4. Copy and save the command's output (it will be text decoded from Base64) to a file and provide the file's path to the driver.

Rationale:

IBM Cloud databases are typically used by our customers to store business-critical data. When these kinds of data are uploaded or accessed, it is highly recommended and required to keep the channel encrypted to ensure data cannot be accessed by a bad actor or incorrect entity

Impact:

Any lack in protecting this data in motion using strong encryption could result in a bad actor accessing the data and possibly causing damage to the relevant organizations.

Audit:

Remediation:

There is no remediation procedure available on database side. If client side is having issues connecting to the database, the client must ensure that they are using TLS 1.2> or HTTPS from application or client library.

Default Value:

Only encrypted communication to the database is accepted.

CIS Controls:

Version 7

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

4.3 Ensure network access to IBM Cloud Databases service is set to be exposed on “Private end points only” (Manual)

Profile Applicability:

- Level 1

Description:

All Cloud Databases deployments offer integration with IBM Cloud Service Endpoints. It gives you the ability to enable connections to your deployments from the public internet and over the IBM Cloud Private network.

Service Endpoints are available in all IBM Cloud Multi-Zone Regions and some Single-Zone Regions. If your deployments are in Osl01, you aren't able to use private endpoints. Deployments in all other regions are able to use Service Endpoints.

Public endpoints provide a connection to your deployment on the public network. At provision time, a public endpoint is the default option for all deployments. Your environment needs to have internet access to connect to a deployment.

A deployment with a service endpoint on the private network gets an endpoint that is not accessible from the public internet. All traffic is routed to hardware dedicated to Cloud Databases deployments and remains on the IBM Cloud Private network. All traffic to and from this endpoint is free and unmetered as long as the traffic remains in IBM Cloud. Once your environment has access to the IBM Cloud Private network, an internet connection is not required to connect to your deployment.

Rationale:

The use of public endpoints exposes data that is contained in the database to unnecessary risk from the outside internet.

Impact:

Some applications are not run in the IBM Cloud. Therefore, they cannot rely on the IBM Cloud network backbone to maintain communication from application to the database over the private network. In this case, the customer may choose to enable "Public" endpoints which allow access to the database from the internet. Customers that are required to do should IP Whitelist the database before enabling "Public" endpoints.

Audit:

From the Console:

1. Log on to your IBM Cloud account
2. Go to the **Menu icon > Resource List** to access your list of account resources
3. Click the Database service you are interested in to open the service dashboard.
4. Ensure you are on the **Manage** page in the left pane.
5. Click the **Settings** tab in the middle of the page and scroll down to *Service endpoints*
6. Review the toggle that displays the status of Private endpoint and Public endpoint enablement. Ensure, Public is toggled *off* and Private is toggled *on*.

From the API:

1. Access to the API uses token authentication, by using the header Authorization: Bearer . The token must be IAM-issued. You can send in an IAM API key directly as the token or use the API key to generate an IAM Bearer Token.
2. Insert the region your deployment is in and the CRN of your deployment as indicated by {}
   ```
   curl -X GET
   https://api.{region}.databases.cloud.ibm.com/v4/ibm/deployments/{id} -H
   'Authorization: Bearer <>' \
   ```

This will return something like:

```
{
  "deployment": {
    "id": "crn",
    "name": "crn",
    "type": "database",
    "platform_options": {
      "key_protect_key_id": ""
    },
    "version": "x.y",
    "admin_username": "admin",
    "enable_private_endpoints": true,
    "enable_public_endpoints": false
  }
}
```

Ensure that *enable_private_endpoints* is *true* and that *enable_public_endpoints* is *false*.

Remediation:

From the Console:

1. Log on to your IBM Cloud account
2. Go to the **Menu icon > Resource List** to access your list of account resources
3. Click the Database service you are interested in to open the service dashboard.

4. Ensure you are on the **Manage** page in the left pane.
5. Click the **Settings** tab in the middle of the page and scroll down to *Service endpoints*
6. Select *Private endpoint* toggle to be turned *on* and *Public endpoint* to be turned *off*.
7. Click **Update Endpoints**

From the CLI:
You can use the ibmcloud resource service-instance-update command in the CLI, specifying the endpoint with the --service-endpoints flag. This can be done online with no downtime

```
ibmcloud resource service-instance-update <service-name> --service-endpoints
<endpoint-type>
```

Changing the type of endpoints available on your deployment does not cause any downtime from a database perspective. However, if you disable an endpoint that is being used by you or your applications, those connections are dropped.
From the API:
You can use the Resource Controller API, with a `PATCH` request to the /resource_instances/{id} endpoint.
**Figure out more detail here, should be copy and paste for *every* service
**

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.

4.4 Ensure IBM Cloud Databases disk encryption is set to On (Manual)

Profile Applicability:

- Level 1

Description:

Data stored in IBM Cloud Databases need to be encrypted at rest at all times for client data security.

Rationale:

With IBM Cloud Databases client data is encrypted at-rest by default and no user action is needed. Encryption ensures client data is protected at all times and access is only provided to users that have the required credentials which can be authenticated.

Impact:

Shared impact

Audit:

Since the default and immutable value is that the database is encrypted at rest, the only auditable procedure identifies the type of encryption used IBM managed encryption key or customer-managed.
Via UI:

1. Log on to your IBM Cloud account
2. Go to the **Menu icon > Resource List** to access your list of account resources
3. Click the Database service you are interested in to open the service dashboard.
4. Ensure you are on the **Manage** page in the left pane.
5. You should be on the **Overview** tab. Scroll down to the *security* section.
6. Details of the ownership of encryption at rest for the database can be viewed here. There are two options: 1. IBM managed encryption at rest with us automatically owning and storing the encryption keys or 2. Customer managed encryption keys through IBM Key Protect. Your selected option will show in this section.

Via API:

1. Generate an API key or IAM bearer token following these instructions
2. Pick the IBM Cloud Databases API url for the region your database is in.
3.
   ```
   curl -X GET
   ```

```
https://api.{region}.databases.cloud.ibm.com/v5/ibm/deployments/{id} -H
'Authorization: Bearer <>' \
```

4. The response will show something like

```
{
  "deployment": {
    "id": "crn:v1:staging:public:databases-for-enterprisedb:us-
south:a/b9552134280015ebfde430a819fa4bb3:5589ecbf-de5f-4eac-9917-
df0dd7e706c8::",
    "name": "crn:v1:staging:public:databases-for-enterprisedb:us-
south:a/b9552134280015ebfde430a819fa4bb3:5589ecbf-de5f-4eac-9917-
df0dd7e706c8::",
    "type": "enterprisedb",
    "platform_options": {
      "disk_encryption_key_crn": "",
      "backup_encryption_key_crn": ""
    },
    "version": "12",
    "admin_usernames": {
      "database": "admin"
    },
    "enable_private_endpoints": false,
    "enable_public_endpoints": true,
    "disablements": []
  }
}
```

5. The lack of text in "disk_encryption_key_crn": and"backup_encryption_key_crn": means that your deployment is encrypted at rest with IBM managed encryption keys. If there is text after "crn" then that will be the unique identifier of the encryption key that is customer-managed for encryption at rest or for backups.

Remediation:

No remediation procedure. Impossible for end-user to impact this control in a negative way.

Default Value:

By default all objects stored on IBM Cloud Databases are encrypted at-rest.

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.

5 Cloudant

Cloudant is a database, run as a service in the IBM Cloud. Its job is to store your application's data securely and allow you to retrieve it quickly and efficiently. The foundation of the IBM Cloudant managed database service is the Apache CouchDB database. IBM is active in the Apache CouchDB committee, employs members of the PMC, and commits most of its feature, functions, and enhancements back to the open source project. Over the last few years, IBM made significant effort to align the core feature set of IBM Cloudant and CouchDB. We contributed key features like IBM Cloudant Query/Mango query language, full-text search, and partition queries to CouchDB.

Apache CouchDB and IBM Cloudant are nearly fully API compatible, which means they can serve as drop-in replacements for each other in your application. They speak the same replication protocol so that you can seamlessly synchronize data between IBM Cloudant and CouchDB instances. However, some differences between the fully managed cloud service IBM Cloudant and self-managed open source Apache CouchDB still exist.

5.1 Ensure Cloudant encryption is set to On (Automated)

Profile Applicability:

- Level 1

Description:

Data stored in IBM Cloudant needs to be encrypted at-rest at all times for client data security.

Rationale:

With IBM Cloudant, client data is encrypted at-rest by default and no user action is needed.

Impact:

With IBM Cloudant, all client data is encrypted at-rest with no action required by the user. There is no impact as it is automatic and data at-rest encryption cannot be disabled by the user.

Audit:

Since the default and immutable value is that data stored in Cloudant is encrypted at-rest, the only auditable procedure is to verify in the console that disk encryption is stated as "Yes".

1. Log on to your IBM Cloud account
2. Go to the **Menu icon > Resource List** to access your list of account resources
3. Click the Cloudant service you are interested in to open the service dashboard.
4. Select **Manage** from the left navigation menu
5. Select the **Overview** tab.
6. In the **Deployment details** section, ensure the *Disk encryption* field is set to *Yes* (this field is not user-configurable)

Remediation:

No remediation procedure. Impossible for end-user to impact this control in a negative way.

Default Value:

By default all data stored on IBM Cloudant is encrypted at-rest.

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.

5.2 Ensure IBM Cloudant encryption is enabled with customer managed keys (Manual)

Profile Applicability:

- Level 1

Description:

IBM Cloudant encrypts all client data at-rest by default. For customers using a Dedicated Hardware plan instance, it is optional to use the service's integration with IBM Key Protect for customers to bring their own encryption key at provision time for the instance.

To provision a Cloudant Dedicated Hardware plan instance using Bring-Your-Own-Key with Key Protect, first ensure you are logged into your IBM Cloud account at https://cloud.ibm.com/. Note a paid account is required to provision a Cloudant Dedicated Hardware plan instance.

Before provisioning the Dedicated Hardware plan instance with BYOK with Key Protect, follow the authorization instructions between Key Protect and Cloudant:

1. Open your IBM Cloud dashboard.
2. From the menu bar, click `Manage` > `Access (IAM)`.
3. In the side navigation, click `Authorizations`.
4. Click `Create`.
5. In the Source service menu, select the `Cloudant` in `Account`.
6. In the Source service instance menu, select `All instances`.
7. In the Target service menu, select `Key Protect` in `Account`, and leave Instance ID of `string equals` `All instances`.
8. Enable the `Reader` role by checking the checkbox.
9. Click `Authorize`.

Ensure the necessary encryption key(s) in Key Protect have been created. (See IBM Key Protect documentation for those steps.)

Next provision a Cloudant Dedicated Hardware plan instance and choose the BYOK with Key Protect option during the provisioning process:

Via UI:

1. From the IBM Cloud Dashboard, click on `Create resource`.
2. Type `Cloudant` in the search bar and click the Cloudant tile to open it.
3. Select `Cloudant` offering.
4. Click the `Dedicated` tab.

5. Click `Create Host`.
6. Select the IBM Cloud region.
7. Configure the Cloudant instance by specifying the `Instance name` and `Resource group`.
8. Under Configure Host, choose the `Location for deployment` to specify the physical location of the Dedicated Hardware plan instance.
9. Choose `Yes` or `No` for `Will the data stored require HIPPA compliance?`.
10. To use a customer-managed (BYOK) encryption key, choose the KMS instance under `Key Management Service instance`.
11. Under Disk encryption key, choose the name of the encryption key to use from the KMS instance in the previous step.
12. Click `Create` to provision the Dedicated Hardware plan instance. Note that during provisioning, a spinning wheel appears next to the instance in your IBM Cloud Dashboard. A request is sent to provision a Dedicated Hardware plan instance on bare metal servers. Provisioning time is asynchronous and can take up to 5 days.

Via CLI:

1. Login to the IBM Cloud via the CLI.
2. Run the following command to provision a Cloudant Dedicated Hardware plan instance using a customer-managed encryption key stored in IBM Key Protect:

```
ibmcloud resource service-instance-create <name> cloudantnosqldb dedicated-
hardware <region> -p '{"location":"<location>", "hipaa":"<hipaa>",
"kms_instance_crn": "<kms_instance_crn>", "kms_key_crn": "<kms_key_crn>"}'
```

Where the customer parameters to enter are as follows:

- `name`: An arbitrary name of the Cloudant Dedicated Hardware instance.
- `region`: The major region where you want to deploy, for example us-south, us-east, etc.
- `location`: The actual physical location of the Dedicated Hardware plan instance, which might differ from the `region`. The location can be in any IBM Cloud location, including major regions and locations outside the major regions.
- `hipaa`: Either `true` or `false`.
- `kms_instance_crn`: An optional parameter that must be set to the CRN of the Key Protect instance housing the encryption key for BYOK. All IBM Cloudant environments are encrypted. If you would like to BYOK with Key Protect, supply the CRN of the Key Protect instance that holds the encryption key. Otherwise, don't supply this parameter in the CLI, which means the environment is encrypted with an IBM Cloudant-managed key.
- `kms_key_crn`: This parameter is required if you use the `kms_instance_crn` parameter. Otherwise, it must not be supplied in the CLI command. The `kms_key_crn` parameter is set to the CRN of the encryption key stored in the Key Protect instance defined by the `kms_instance_crn` parameter.

Below is an example CLI command with the parameters populated with sample values:

```
ibmcloud resource service-instance-create cloudant-dedicated-with-byok
cloudantnosqldb dedicated-hardware us-south -p '{"location":"dallas",
"hipaa":"false", "kms_instance_crn": "crn:v1:bluemix:public:kms:us-
south:a/abcdefg7df5907a4ae72ad28d9f493d6:888a5a41-543c-4ca7-af83-
74da3bb8f711::", "kms_key_crn": "crn:v1:bluemix:public:kms:us-
south:a/abcdefg7df5907a4ae72ad28d9f493d6:888a5a41-543c-4ca7-af83-
74da3bb8f711:key:0123c653-f904-4fe7-9fdb-5097e1ed85db"}'
```

Rationale:

When it comes to encryption of data at rest in IBM Cloud, we recommend for customers to manage customer root keys that are used to protect customer data stored in data and storage services in IBM Cloud. With the support of Bring Your Own Key (BYOK), customers can manage lifecycle of their customer root keys where they can create, rotate, delete those keys. This provides a significant level of control where those CRKs are managed by the customer, which in turn increases both security control as well as meet relevant compliance requirements. These CRKs are used in turn to protect the data encryption keys used to encrypt the data.

Impact:

If a customer does not bring their own encryption key at provision time, they are not able to crypto-shred the data or revoke the database's access to the encryption key, which would render the database unable to read the data.

Audit:

Users can audit whether a Cloudant Dedicated Hardware environment is using a customer-managed key by viewing associations between root keys and associated cloud services in the IBM Key Protect UI or API. Use the steps below to see the associations and verify that the Cloudant Dedicated Hardware plan instance(s) have the appropriate associations listed to show the use of customer-managed encryption key in Key Protect.
Via UI:

1. Log in to the IBM Cloud console.
2. Go to `Menu` > `Resource List` to view a list of your resources.
3. From your IBM Cloud resource list, select your provisioned instance of Key Protect.
4. On the application details page, select the `Associated Resources` tab on the left side menu.
5. On the Associated resources page, use the `Associated Resources` table to browse the registrations in your service.
6. Click the `^` icon under the `Details` column to view a list of details for a specific registration.

7. Click `Filter` button to filter for resources by key ID, Cloud Resource Name (CRN), and retention policy.

Via API:
You can retrieve the registration details that are associated with a specific root key by making a GET call to the following endpoint:

```
https://<region>.kms.cloud.ibm.com/api/v2/keys/<key_ID>/registrations
```

View the registrations that are associated with a root key by running the following cURL command:

```
 $ curl -X GET \
     "https://<region>.kms.cloud.ibm.com/api/v2/keys/<key_ID>/registrations"
\
     -H "authorization: Bearer <IAM_token>" \
     -H "bluemix-instance: <instance_ID>"
```

where the variables are as follows:

- `region`: Required. The region abbreviation, such as `us-south` or `eu-gb`, that represents the geographic area where your Key Protect instance resides.
- `key_ID`: Required. The identifier for the root key that is associated with the cloud resources that you want to view.
- `IAM_token`: Required. Your IBM Cloud access token. Include the full contents of the IAM token, including the Bearer value, in the cURL request.
- `instance_ID`: Required. The unique identifier that is assigned to your Key Protect service instance.

Remediation:

The process to remediate a configuration where there is no use of a customer-managed encryption is as follows:

1. Provision a new Cloudant Dedicated Hardware plan instance using a customer-managed key as shown in details above.
2. Create new Cloudant instance(s) on the Dedicated Hardware plan instance that is using a customer-managed key as needed.
3. Replicate data over from the Cloudant instances not using a customer-managed key to the instances on the Dedicaed Hardware environment using the customer-managed key. This process requires use of the Cloudant replication feature as shown in the Cloudant documentation.

4. Delete any Cloudant instances on environments that do not use customer-managed keys once the replication is complete.

Default Value:

The default value is `Automatic disk encryption key (default)`, which means the disk encryption will be done with an IBM-managed key and not a customer managed key. Customers must choose to use IBM Key Protect with a customer-managed key.

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.

5.3 Ensure IBM Cloudant is only accessible via HTTPS or TLS Connections (Automated)

Profile Applicability:

- Level 1

Description:

IBM Cloudant instances can only be connected to over TLS or HTTPS connections. This behavior is by default and is non-configurable.

Rationale:

With IBM Cloudant, all access is over HTTPS by default an no user action is needed to ensure all data in transit is encrypted.

Impact:

With IBM Cloudant, all access is over HTTPS by default with no action required by the user. There is no impact as TLS and HTTPS connections are automatic and not user-configurable.

Audit:

Since the default and immutable value is that all access to Cloudant is over HTTPS, the only auditable procedure is to verify access to a Cloudant instance over HTTPS works while access over HTTP fails.

1. Log on to your IBM Cloud account
2. Go to the **Menu icon > Resource List** to access your list of account resources
3. Click the Cloudant service you are interested in to open the service dashboard.
4. Select **Manage** from the left navigation menu
5. Select the **Overview** tab.
6. In the **Deployment details** section, ensure the *External Endpoint* and *External Endpoint (preferred)* fields have prefixes of `https://`
7. Ensure you can connect to the instance over `https://` by clicking on **Launch Dashboard** or running a `curl` against the endpoint listed.
8. Ensure you cannot connect if you change the `https://` to `http://` in the URL and should result in a response of > port 80: Connection refused

Examples using command line tool `curl`:
With HTTPS:

```
$ curl https://3dde8a0f-19d8-4698-a70e-e4757714a180-bluemix.cloudant.com
{"couchdb":"Welcome","version":"2.1.1","vendor":{"name":"IBM
Cloudant","version":"8158","variant":"paas"},"features":["geo","access-
ready","iam","partitioned","pluggable-storage-
engines","scheduler"],"features_flags":["partitioned"]}
```

Without HTTPS:

```
$ curl http://3dde8a0f-19d8-4698-a70e-e4757714a180-bluemix.cloudant.com
curl: (7) Failed to connect to 3dde8a0f-19d8-4698-a70e-e4757714a180-
bluemix.cloudant.com port 80: Connection refused
```

Remediation:

No remediation procedure. Impossible for end-user to impact this control in a negative way.

Default Value:

With IBM Cloudant, all access is over HTTPS by default with no action required by the user.

CIS Controls:

Version 7

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

6 Networking

6.1 IBM Cloud Internet Services

IBM Cloud™ Internet Services (CIS), powered by Cloudflare, offers three main capabilities to enhance your workflow: security, reliability, and performance.

6.1.1 Enable TLS 1.2 at minimum for all inbound traffic on IBM Cloud Internet Services Proxy (Manual)

Profile Applicability:

- Level 1

Description:

The Transport Layer Security (TLS) options let you control whether visitors can browse your website over a secure connection, and when they do, how IBM Cloud™ Internet Services connects to your origin server. Ensure minimum TLS level for TLS termination is set to TLS 1.2. Use the latest version of the TLS protocol (TLS 1.3) for improved security and performance by switching from **Disabled** to **Enabled** or **Enabled+ORTT** in the list.

TLS encryption modes

Set the TLS mode by selecting one of the following options from the Mode list.

These options are listed in the order from the least secure (Off) to the most secure (End-to-End CA signed).

- Off (not recommended)
- Client-to-Edge (edge to origin not encrypted, self-signed certificates are not supported)
- End-to-End flexible (edge to origin certificates can be self-signed)
- End-to-End CA signed (default and recommended)
- HTTPS only origin pull (Enterprise only)

Traffic encryption - Minimum TLS version

Set the minimum TLS version for traffic trying to connect to your site by selecting one of the versions from the list.

By default, this is set to 1.2. Higher TLS versions provide additional security, but might not be supported by all browsers. This could result in some customers being unable to connect to your site.

The minimum TLS version applies to whichever **TLS encryption mode** is selected.

Rationale:

Use the latest version of the TLS protocol for improved security and performance. TLS1.1 is now considered obsolete and has some vulnerabilities.

Impact:

Higher TLS versions provide additional security, but might not be supported by all browsers. This could result in some customers being unable to connect to your site.

Audit:

The Minimum TLS setting can be audited using the following mechanisms
IBM Cloud Console

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon --> Resource list**
3. Select the Cloud Internet Service Instance
4. Select the domain that needs to be audited from the domains drop down
5. Choose the **Security** section from the left panel.
6. Click on the **TLS** tab in the Security panel.
7. Verify the **Traffic Encryption - Minimum TLS Version** is set to a value of *TLS 1.2(default)* or higher

IBM Cloud CLI

1. Verify `min_tls_version` must be set to `1.2` or higher

```
ibmcloud cis tls-settings e476aba943b5d7d29b96135c78aa55c9 --output json
{
    "min_tls_version": "1.2",
    "ssl": "strict",
    "tls_1_2_only": "off",
    "tls_1_3": "off",
    "universal": true
}
```

Remediation:

IBM Cloud Console

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon -- Resource list**
3. Select the Cloud Internet Service Instance that needs to be remediated from the domains drop down.
4. Choose the **Security** section from the left panel.
5. Click on the **TLS** tab in the Security panel.
6. Change the TLS version on **Traffic Encryption - Minimum TLS Version** to *TLS 1.2(default)*

IBM Cloud CLI

1. Set `min_tls_version` to `1.2`

```
    ibmcloud cis tls-settings-update  <DOMAIN_ID> -i <Instance-Name> --min-
tls-version 1.2
```

Default Value:

The default TLS mode is set to TLS1.2 for any TLS termination on Cloud Internet Services

References:

1. https://cloud.ibm.com/docs/cis?topic=cis-cis-tls-options
2. https://cloud.ibm.com/docs/cis?topic=cis-manage-your-ibm-cis-for-optimal-security
3. https://cloud.ibm.com/docs/cis?topic=cis-cli-plugin-cis-cli#waf
4. https://cloud.ibm.com/docs/cis?topic=cis-cli-plugin-cis-cli#overview
5. https://cloud.ibm.com/docs/cis?topic=cis-getting-started

CIS Controls:

Version 7

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

6.1.2 Ensure Web application firewall is set to ON in IBM Cloud Internet Services (CIS) (Manual)

Profile Applicability:

- Level 1

Description:

The Web Application Firewall (WAF) protects against ISO Layer-7 attacks, which can be some of the most tricky.

What is a Web Application Firewall?

A WAF helps protect web applications by filtering and monitoring HTTP traffic between a web application and the internet. A WAF is an OSI protocol Layer-7 defense in the OSI model, and it is not designed to defend against all types of attacks.

Deploying a WAF in front of a web application is like placing a shield between the web application and the internet. A proxy server protects a client machine's identity by using an intermediary (for outgoing traffic), but a WAF is a type of reverse-proxy that protects the server from exposure by having the client's traffic pass through the WAF before reaching the server (for incoming traffic).

Key benefits of a CIS WAF

The IBM Cloud™ Internet Services WAF is an easy way to set up, manage, and customize security rules to protect your web applications from common web threats. See the following list for key features:

- **Easy setup**: The CIS WAF is part of our overall service, which takes just a few minutes to set up. After you redirect your DNS to us, you can switch on the WAF and set up the rules you need.
- **Detailed reporting** See greater detail in the reporting, for example, threats blocked by rule/rule group.

Rationale:

A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

Types of attacks WAF can prevent

A WAF typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF usually is part of a suite of tools, which together can create a holistic defense against a range of attack vectors.

How a WAF works

WAF is a type of reverse-proxy that protects the server from exposure by having the client requests pass through the WAF before reaching the server. It acts as shield placed between the web application and the internet.

A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic.

The value of a WAF comes from the speed and ease with which its policy modifications can be implemented, thereby allowing a faster response to varying attack vectors. For example, during a DDoS attack, rate limiting can be implemented by modifying WAF policies.

Impact:

A WAF is an OSI protocol Layer-7 defense in the OSI model, and it is not designed to defend against all types of attacks. When a WAF is enabled on Cloud Internet Services the TLS traffic is terminated at the proxy, unencrypted, inspected for any attacks, and then re-encrypted and forwarded on to the application. Another thing to consider with WAF is that there may be false positives based on the application patterns and clients may get blocked or challenged. This can be mitigated by tuning WAF.

Audit:

The Web Application Firewall setting can be audited using the following mechanisms
IBM Cloud Console

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon --> Resource list**
3. Select the Cloud Internet Service Instance
4. Select the domain that needs to be audited from the domains drop down
5. Choose the **Overview** from the left panel (this should be the default landing page)
6. Under *Security* section **Web Application Firewall** should show up as *Enabled*

IBM Cloud CLI

```
ibmcloud cis waf-setting <DNS_DOMAIN_ID> -i Instance-Name

Displaying WAF setting of domain 'DNS_DOMAIN_ID' ...
OK
```

```
  ID      waf
  Mode    On
```

Remediation:

The Web Application Firewall can be enabled using the following mechanisms
IBM Cloud Console

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon --> Resource list**
3. Select the Cloud Internet Service Instance
4. Select the domain that needs to be audited from the domains drop down
5. Choose the **Security** section from the left panel.
6. Click on the **WAF** tab in the *Security* panel.
7. Switch the toggle to *On*

IBM Cloud CLI

```
     ibmcloud cis waf-setting-update <DNS_DOMAIN_ID> waf-enable -i Instance-
Name
     Updating WAF setting of domain 'e476aba943b5d7d29b96135c78aa55c9' ...
     OK
     WAF setting was updated successfully.

     ID      waf
     Mode    On
```

Default Value:

The Default value for the Web Application Firewall is *Off* in Cloud Internet Services.

References:

1. https://cloud.ibm.com/docs/cis?topic=cis-manage-your-ibm-cis-for-optimal-security#best-practice-activate-waf-safely
2. https://cloud.ibm.com/docs/cis?topic=cis-waf-q-and-a
3. https://cloud.ibm.com/docs/cis?topic=cis-cli-plugin-cis-cli#waf
4. https://cloud.ibm.com/docs/cis?topic=cis-cli-plugin-cis-cli#overview
5. https://cloud.ibm.com/docs/cis?topic=cis-getting-started

Additional Information:

The proxy mode for the service must be enabled for the traffic to pass through the Web Application Firewall.

CIS Controls:

Version 7

9.5 Implement Application Firewalls
Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

6.1.3 Ensure DDoS protection is Active on IBM Cloud Internet Services (Manual)

Profile Applicability:

- Level 1

Description:

IBM Cloud Internet services provides automatic DDoS protection for any proxied DNS records or a Range Application. For an application to be protected against DDoS attacks the DNS records or the Global Load Balancer should be proxied. It is recommended that the DNS records in Cloud Internet Services for any networks or applications that need to be protected must be proxied. In addition it is required to allowlist only IPs from the Cloud Internet Services on your application ingress points. The list of ips to be allow listed is found here.

Rationale:

A distributed denial of service (DDoS) attack is a malicious attempt to disrupt normal traffic of a server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. DDoS attacks achieve effectiveness by utilizing many compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up a highway, preventing regular traffic from arriving at its destination.

DDoS attack vectors target varying components of a network connection. While nearly all DDoS attacks involve overwhelming a target device or network with traffic, attacks can be divided into three categories. An attacker can use one or multiple attack vectors, and might even cycle through these attack vectors based on countermeasures taken by the target.

Common types are:

- Application layer attacks (Layer 7)
- Protocol attacks (Layer 3 and Layer 4)
- Volumetric attacks (amplification attacks)

Application layer attacks An application layer attack is sometimes referred to as a Layer-7 DDoS attack (in reference to the 7th layer of the OSI model). The goal of these attacks is to exhaust the resources of the victim, by targeting the layer where web pages are generated on the server and delivered to the visitors in response to HTTP requests (that is, the application layer). Layer-7 attacks are challenging, because the traffic can be difficult to identify as malicious.

Protocol attacks Protocol attacks utilize weaknesses in Layer 3 and Layer 4 of the ISO protocol stack to render the target inaccessible. These attacks, also known as a state-exhaustion attacks, cause a service disruption by consuming all the available state table capacity of web application servers, or of intermediate resources such as firewalls and load balancers.

Volumetric attacks This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the wider internet. Large amounts of data are sent to a target using a form of amplification, or by other means of creating massive traffic, such as requests from a botnet.

Impact:

Allowing proxy will route your data through the Cloud Internet Services proxy and will be decrypted and inspected for layer7 DDoS attacks.

Audit:

The different types of mechanisms to audit if DDoS is enabled are as follows:
IBM Cloud Console

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon --> Resource list**
3. Select the Cloud Internet Service Instance
4. Click on **Reliability** on the Left Navigation panel.
5. Click on the **Global Load Balancers** tab.
6. Verify each GLB indicates that proxy is enabled by the green toggle.
7. Click on the **DNS** tab.
8. Verify each DNS record indicates that proxy is enabled by the green toggle.

IBM Cloud CLI

1. Run the following ibmcloud cli command and review the value of the *proxied* property to verify it is set to *true*

```
 ibmcloud cis glbs <DOMAIN_ID> --output json
[
    {
        "id": "9f46452de6eaa7473ac0ba6b7e7b9502",
        "created_on": "2020-07-20T14:45:34.982552Z",
        "modified_on": "2020-09-16T23:48:50.391727Z",
        "name": "hrtrt.test.com",
        "fallback_pool": "56290bfc54621463c89e493189c055f6",
        "enabled": true,
        "default_pools": [
            "56290bfc54621463c89e493189c055f6"
        ],
        "proxied": true,
        "session_affinity": "none",
        "steering_policy": "off",
        "AvailablePools": "0/1"
    }
]

ibmcloud cis dns-records <DOMAIN_ID>
Getting DNS Records in domain 'e476aba943b5d7d29b96135c78aa55c9' for service
instance 'Test' ...
OK
ID                                  Name              Type    Content
Proxied   TTL
8f2e55e8d471d79e17e8abb6907a04fb   test.test.com     A       9.9.88.7
true      1
150f601ac48c22c2bc2b0521b72c96aa   www.test.com      A       169.5.9.12
false     1
```

Remediation:

The different types of mechanisms to audit if DDoS is enabled are as follows:
IBM Cloud Console

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon --> Resource list**
3. Select the Cloud Internet Service Instance
4. Click on **Reliability** on the Left Navigation panel.
5. Click on the **Global Load Balancers** tab.
6. Change the toggle for the *Proxied* column to green.
7. Click on the **DNS** tab.
8. Change the toggle for *Proxy* column for the relevant DNS records to green.

IBM Cloud CLI

1. Run the following ibmcloud cli commands to set the value of the *proxied* property to *true*

- Global Load Balancer

```
 ibmcloud cis glb-update e476aba943b5d7d29b96135c78aa55c9
9f46452de6eaa7473ac0ba6b7e7b9502 --json '{
        "name": "hrtrt.test.com",
        "fallback_pool": "56290bfc54621463c89e493189c055f6",
        "default_pools": ["56290bfc54621463c89e493189c055f6"],
        "proxied": true
}'  --output json
{
    "id": "9f46452de6eaa7473ac0ba6b7e7b9502",
    "created_on": "0001-01-01T00:00:00Z",
    "modified_on": "2020-09-17T02:03:28.804283Z",
    "name": "hrtrt.test.com",
    "ttl": 30,
    "fallback_pool": "56290bfc54621463c89e493189c055f6",
    "enabled": true,
    "default_pools": [
        "56290bfc54621463c89e493189c055f6"
    ],
    "proxied": true,
    "session_affinity": "none",
    "steering_policy": "off",
    "AvailablePools": "0/1"
}
```

- DNS Records

```
ibmcloud cis dns-record-update <DOMAIN_ID> <DNS_RECORD_ID> --proxied true
Updating DNS Record '8f2e55e8d471d79e17e8abb6907a04fb' in domain
'e476aba943b5d7d29b96135c78aa55c9' for service instance 'Test Instance' ...
OK

ID              8f2e55e8d471d79e17e8abb6907a04fb
Created On      2020-09-17 01:35:11.348361 +0000 UTC
Modified On     2020-09-17 01:35:11.348361 +0000 UTC
Name            test.test.com
Type            A
Content         9.9.88.7
Domain ID       e476aba943b5d7d29b96135c78aa55c9
Domain Name     test.com
Proxied         true
TTL             1
```

Default Value:

Default value for Proxy for all DNS records and GLBs are set to disabled.

References:

1. https://cloud.ibm.com/docs/cis?topic=cis-distributed-denial-of-service-ddos-attack-concepts
2. https://cloud.ibm.com/docs/cis?topic=cis-manage-your-ibm-cis-for-optimal-security#best-practice-activate-waf-safely
3. https://cloud.ibm.com/docs/cis?topic=cis-cis-allowlisted-ip-addresses

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

6.2 IBM Virtual Private Cloud (VPC)

With IBM Cloud™ Virtual Private Cloud (VPC), you can use the UI, CLI, and API to quickly provision generation 2 virtual server instances for VPC with high network performance. VPC infrastructure contains a number of Infrastructure-as-a-Service (IaaS) offerings, including Virtual Servers for VPC. Use the following information to understand a simple use case for planning, creating, and configuring resources for your VPC, and learn about additional VPC overviews and VPC tutorials.

6.2.1 Ensure no VPC access control lists allow ingress from 0.0.0.0/0 to port 22 (Manual)

Profile Applicability:

- Level 1

Description:

VPC access control lists filter all incoming and outgoing traffic in IBM Cloud VPC. An ACL is a built-in, virtual firewall where ACL rules control traffic to and from the subnets, rather than to and from the virtual servers. It is recommended that no ACL allows unrestricted ingress access to port 22.

Rationale:

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

Impact:

For updating an existing environment, care should be taken to ensure that administrators currently relying on an ingress from 0.0.0.0/0 have access to ports 22 through another, more restrictive, access control list.

Audit:

Perform the following tasks to determine if the account is configured as prescribed:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->Access Control Lists**.
3. For each access control list, perform the following:
   a. Select the access control list name.
   b. Ensure no Inbound Rule exists that has a port range that includes port `22` and has a Source of `0.0.0.0/0`. A *port range* value of *ALL* or a *port range* that includes port `22`, e.g. `0-1024`, are inclusive of port `22`.

Remediation:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->Access Control Lists**.
3. For each security group, perform the following:
   a. Select the access control list name.

b. Identify the Inbound rule to be removed.
c. Using the **Options** icon, select **Delete**.

Default Value:

Unless modified, the *allow-all-network-acl* access control list has *Access* set to *Allow*, *protocol* set to *Any*, a *port range* of *Any* and a *Source* of `0.0.0.0/0`.

References:

1. https://cloud.ibm.com/docs/vpc?topic=vpc-using-acls

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.

6.2.2 Ensure the default security group of every VPC restricts all traffic (Manual)

Profile Applicability:

- Level 1

Description:

VPC security groups provide stateful filtering of ingress/egress network traffic to Virtual Server. It is recommended that no security group allows unrestricted ingress access to a Virtual Server. Unless modified, the default security group allows inbound traffic from all members of the group that is, all other virtual servers that are attached to this security group.

Rationale:

Removing uncontrolled connectivity to a Virtual Server, reduces a server's exposure to risk.

Impact:

For updating an existing environment, care should be taken to ensure that Virtual Servers currently relying on ingress have the required access.

Audit:

Perform the following tasks to determine if the account is configured as prescribed:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->VPC Layout and Security Groups**.
3. For the default security group, perform the following:
   a. Ensure no Inbound Rule exists that allows unrequited traffic to the Virtual Servers.

Remediation:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->VPC Layout and Security Groups**.
3. For the default security group, perform the following:
   a. Identify the Inbound rule.
   b. Update the rule to only allow the required traffic flow.

Default Value:

Unless modified, the default security group allows inbound traffic from all members of the group that is, all other virtual servers that are attached to this security group.

References:

1. https://cloud.ibm.com/docs/vpc?topic=vpc-updating-the-default-security-group

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.

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

Profile Applicability:

- Level 1

Description:

VPC security groups provide stateful filtering of ingress/egress network traffic to Virtual Server Instances. It is recommended that no security group allows unrestricted ingress access to port 3389.

Rationale:

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

Impact:

For updating an existing environment, care should be taken to ensure that administrators currently relying on an ingress from `0.0.0.0/0` have access to port `3389` through another, more restrictive, access control list.

Audit:

Perform the following tasks to determine if the account is configured as prescribed:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->Security Groups**.
3. For each security group, perform the following:
   a. Select the security group name.
   b. Ensure no Inbound Rule exists that has a port range that includes port `3389` and has a *Source* of `0.0.0.0/0`. Note that a *port range* value of *ALL* or a *port range* that includes port `3389`, e.g. `3300-3400`, are inclusive of port `3389`.

Remediation:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->Security Groups**.
3. For each security group, perform the following:
   a. Select the access control list name.
   b. Identify the Inbound rule to be removed.
   c. Using the **Options** icon, select **Delete**.

Default Value:

There are no default rules in the default security group with a value of 3389.

References:

1. https://cloud.ibm.com/docs/vpc?topic=vpc-using-acls

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.

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

Profile Applicability:

- Level 1

Description:

VPC security groups provide stateful filtering of ingress/egress network traffic to Virtual Servers. It is recommended that no security group allows unrestricted ingress access to port 22.

Rationale:

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

Impact:

For updating an existing environment, care should be taken to ensure that administrators currently relying on an ingress from `0.0.0.0/0` have access to port `22` through another, more restrictive, security group.

Audit:

Perform the following tasks to determine if the account is configured as prescribed:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->Security Groups**.
3. For each security group, perform the following:
   a. Select the security group name.
   b. Ensure no Inbound Rule exists that has a value that includes port `22` and has a *Source* of `0.0.0.0/0`. Note that a *port range* value of *ALL* or a *port range* that includes port `22`, e.g. `0-1024`, are inclusive of port `22`.

Remediation:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->Security Groups**.
3. For each security group, perform the following:
   a. Select the security group name.
   b. Identify the Inbound rule to be removed.
   c. Using the **Options** icon, select **Delete**.

Default Value:

Unless modified, the default security group includes a rule with *protocol* set to *TCP*, a value of `22` and a *Source* of `0.0.0.0/0`.

References:

1. https://cloud.ibm.com/docs/vpc?topic=vpc-using-acls

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.

6.2.5 Ensure no VPC access control lists allow ingress from 0.0.0.0/0 to port 3389 (Manual)

Profile Applicability:

- Level 1

Description:

VPC access control lists filter all incoming and outgoing traffic in IBM Cloud VPC. An ACL is a built-in, virtual firewall where ACL rules control traffic to and from the subnets, rather than to and from the virtual servers. It is recommended that no ACL allows unrestricted ingress access to port 3389.

Rationale:

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

Impact:

For updating an existing environment, care should be taken to ensure that administrators currently relying on an ingress from `0.0.0.0/0` have access to port `3389` through another, more restrictive, access control list.

Audit:

Perform the following tasks to determine if the account is configured as prescribed:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->Access Control Lists**.
3. For each access control list, perform the following:
   a. Select the access control list name.
   b. Ensure no Inbound Rule exists that has a *port range* that includes port `3389` and has a Source of `0.0.0.0/0`. Note that a *port range* value of *ALL* or a *port range* that includes port `3389`, e.g. `3300-3400`, are inclusive of port `3389`.

Remediation:

1. Login to the IBM Cloud Portal at https://cloud.ibm.com.
2. At the Menu icon, select **VPC Infrastructure-->Access Control Lists**.
3. For each security group, perform the following:
   a. Select the access control list name.

b. Identify the Inbound rule to be removed.
c. Using the **Options** icon, select **Delete**.

Default Value:

Unless modified, the *allow-all-network-acl* access control list has *Access* set to *Allow*, *protocol* set to *Any*, a *port range* of *Any* and a *Source* of `0.0.0.0/0`.

References:

1. https://cloud.ibm.com/docs/vpc?topic=vpc-using-acls

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.

7 Containers

7.1 IBM Kubernetes Service

Deploy highly available containerized apps in Kubernetes clusters and use the powerful tools of IBM Cloud™ Kubernetes Service to automate, isolate, secure, manage, and monitor your workloads across zones or regions.

First, create a cluster with a few clicks in the IBM Cloud console. Then, deploy your first containerized app to your cluster through the Kubernetes dashboard.

7.1.1 Use a Key Management Service (KMS) provider to encrypt data in Kubernetes secrets

Protect sensitive information in your IBM Cloud™ Kubernetes Service cluster to ensure data integrity and to prevent your data from being exposed to unauthorized users.

Understanding Key Management Service (KMS) providers

You can protect the etcd component in your Kubernetes master and Kubernetes secrets by using a Kubernetes key management service (KMS) provider that encrypts secrets with encryption keys that you control.

When you enable a KMS provider in your cluster, your own KMS root key is used to encrypt data in etcd, including the LUKS secrets. Etcd is the component of the master that stores the configuration files of your Kubernetes resources, such as deployments and secrets. Data in etcd is stored on the local disk of the Kubernetes master and is backed up to IBM Cloud Object Storage. Data is encrypted during transit to IBM Cloud Object Storage and at rest. When you enable a KMS provider, a wrapped data encryption key (DEK) is stored in etcd. The DEK encrypts the secrets in your cluster that store service credentials and the LUKS key. Because the root key is in your KMS instance, you control access to your encrypted secrets. To unwrap the DEK, the cluster uses the root key from your KMS instance. For more information about how key encryption works, see Envelope encryption.

Supported KMS providers

IBM Cloud Kubernetes Service supports the following KMS providers:

- IBM® Key Protect for IBM Cloud™ for public cloud or on-prem environments.
- Hyper Protect Crypto Services for keep your own key (KYOK) crypto unit support.

Because adding a different KMS provider requires updating the managed master default configuration, you cannot add other KMS providers to the cluster.

When you enable a KMS provider in your cluster, your own KMS root key is used to encrypt data in etcd, including the LUKS secrets. Using your own encryption root key adds a layer of security to your etcd data and Kubernetes secrets and gives you more granular control of who can access sensitive cluster information.

7.1.1.1 Ensure Kubernetes secrets data is encrypted with bring your own key (BYOK) (Manual)

Profile Applicability:

- Level 1

Description:

IBM® Key Protect for IBM Cloud™ helps you provision encrypted keys for apps across IBM Cloud services. Use the IBM Key Protect for IBM Cloud key management service (KMS) to encrypt data in Kubernetes secrets and prevent unauthorized users from accessing sensitive app information (for example, credentials and keys). Keys are generated by FIPS 140-2 Level 3 certified hardware security modules (HSMs) that are located in secure IBM Cloud data centers.

Rationale:

You can encrypt data with customer managed keys in Kubernetes secrets to prevent unauthorized users from accessing sensitive app information. Using your own encryption root key adds a layer of security to your etcd data and Kubernetes secrets and gives you more granular control of who can access sensitive cluster information.

When it comes to encryption of data at rest in IBM Cloud, we recommend for customers to manage customer root keys (CRK) that are used to protect customer data stored in data and storage services in IBM Cloud. With the support of Bring Your Own Key (BYOK), customers can manage lifecycle of their customer root keys where they can create, rotate, delete those keys. This provides a significant level of control where those CRKs are managed by the customer, which in turn increases both security control as well as meet relevant compliance requirements. These CRKs are used in turn to protect the data encryption keys (DEK) used to encrypt the data.

Impact:

You cannot disable KMS provider encryption. Do not delete root keys in your KMS instance, even if you rotate to use a new key. If you delete a root key that a cluster uses, the cluster becomes unusable, loses all its data, and cannot be recovered.

Similarly, if you disable a root key, operations that rely on reading secrets fail. Unlike deleting a root key, however, you can reenable a disabled key to make your cluster usable again.

If you lose your key, you will not be able to recover the data. Standard pricing for Key Protect applies.

Audit:

1. Install the etcd CLI (`etcdctl`) version 3 or later. See https://github.com/etcd-io/etcd/releases.
2. Set your terminal session context to use the appropriate `etcdctl` API version.

```
export ETCDCTL_API=3
```

3. Run the `ibmcloud ks cluster config` command and include the `--admin` option, which downloads the etcd certificates and keys for your cluster, and the `--output zip > <cluster_name_or_ID>.zip` option, which saves your cluster configuration files to a compressed folder.

```
ibmcloud ks cluster config -c <cluster_name_or_ID> --admin --output zip >
<cluster_name_or_ID>.zip
```

4. Decompress the compressed folder.
5. Get the server field for your cluster. In the output, copy only the master URL, without `https://` and the node port.

```
cat ./<cluster_name_or_ID>/kube-config.yaml | grep server
```

6. Get the `etcdPort` for your cluster.

```
ibmcloud ks cluster get -c <cluster_name_or_ID> --output json | grep etcdPort
```

7. Get the name of a secret in your cluster.

```
kubectl get secrets [-n <namespace>]
```

8. Confirm that the Kubernetes secrets for the cluster are encrypted. Replace the `secret_name`, `master_url`, and `etcd_port` fields with the values that you previously retrieved, and replace `<cluster_name_or_ID>` with the name of the cluster in your compressed folder file path.

```
etcdctl get /registry/secrets/<secret_namespace>/<secret_name> --endpoints
https://<master_url>:<etcd_port> --key="./<cluster_name_or_ID>/admin-key.pem"
--cert="./<cluster_name_or_ID>/admin.pem" --
cacert="./<cluster_name_or_ID>/ca.pem"
```

9. Ensure the output is unreadable and scrambled, indicating that it is encrypted.

Remediation:

From Console:

1. Log in to your IBM Cloud account.
2. To view the list of services that are available on IBM Cloud, click **Catalog**.
3. From the **All Categories** navigation pane, click the **Security and Identity** category.
4. From the list of services, click the **Key Protect** tile.
5. Select a service plan, and click **Create** to provision an instance of Key Protect in the account, region, and resource group where you are logged in.
6. To view a list of your resources, go to **Menu** > **Resource List**.
7. From your IBM Cloud resource list, select your provisioned instance of Key Protect.
8. To create a new key, click **Add key** and select the **Create a key** window. Specify the key's name and key type.
9. When you are finished filling out the key's details, click **Create key** to confirm.
10. From the Clusters console, select the cluster that you want to enable encryption for.
11. From the **Overview** tab, in the **Summary** > **Key management service** section, click **Enable**.
12. Select the **Key management service instance** and **Root key** that you want to use for the encryption.
13. Click **Enable**.
14. Verify that the KMS enablement process is finished. From the **Summary** > **Master status** section, you can check the progress.
15. After the KMS provider is enabled in the cluster, data in etcd and new secrets that are created in the cluster are automatically encrypted by using your root key.
16. To encrypt existing secrets with the root key, rewrite the secrets. This cannot be done from the console. See the **From Command Line** section.

From Command Line:

1. Log in to IBM Cloud through the IBM Cloud CLI.

```
ibmcloud login [--sso]
```

2. Select the region and resource group where you want to create a Key Protect instance.

```
ibmcloud target -r <region_name> -g <resource_group_name>
```

3. Provision a public or private Key Protect instance.

```
ibmcloud resource service-instance-create <instance_name> kms tiered-pricing
<region> [-p '{"allowed_network": "private-only"}']
```

4. Create a customer root key (CRK) in your KMS instance. You can't use the CLI for this action; you must use the GUI or API. See the above **From Console** section.
5. Get the ID of the KMS instance that you previously created.

```
ibmcloud ks kms instance ls
```

6. Get the ID of the root key that you previously created.

```
ibmcloud ks kms crk ls --instance-id <KMS_instance_ID>
```

7. Enable the KMS provider to encrypt secrets in your cluster. Fill in the options with the information that you previously retrieved. The KMS provider's private service endpoint is used by default to download the encryption keys. To use the public service endpoint instead, include the `--public-endpoint` option. The enablement process can take some time to complete.

```
ibmcloud ks kms enable -c <cluster_name_or_ID> --instance-id
<kms_instance_ID> --crk <root_key_ID> [--public-endpoint]
```

8. Verify that the KMS enablement process is finished. The process is finished when the Master Status is Ready.
9. After the KMS provider is enabled in the cluster, data in etcd and new secrets that are created in the cluster are automatically encrypted by using your root key.
10. Set the context for your cluster.

```
ibmcloud ks cluster config -c <cluster_name_or_ID>
```

11. With cluster-admin access, rewrite the secrets to encrypt them.

```
kubectl get secrets --all-namespaces -o json | kubectl replace -f -
```

Default Value:

Kubernetes secrets are Base64 encoded but not encrypted.

References:

1. https://cloud.ibm.com/docs/containers?topic=containers-encryption#keyprotect
2. https://cloud.ibm.com/docs/containers?topic=containers-encryption#kms
3. https://cloud.ibm.com/docs/key-protect

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.

7.1.1.2 Ensure Kubernetes secrets data is encrypted with keep your own key (KYOK) (Manual)

Profile Applicability:

- Level 1

Description:

IBM Cloud® Hyper Protect Crypto Services (Hyper Protect Crypto Services for short) is a dedicated key management service and hardware security module (HSM) based on IBM Cloud. This service allows you to take the ownership of the cloud HSM to fully manage your encryption keys and to perform cryptographic operations. Use Hyper Protect Crypt Services, a dedicated key management service (KMS) and hardware security module (HSM), to encrypt data in Kubernetes secrets and prevent unauthorized users from accessing sensitive app information, for example, credentials and keys.

Rationale:

You can encrypt data with customer managed keys in Kubernetes secrets to prevent unauthorized users from accessing sensitive app information. Using your own encryption root key adds a layer of security to your etcd data and Kubernetes secrets and gives you more granular control of who can access sensitive cluster information.

When it comes to encryption of data at rest in IBM Cloud, we recommend for customers to manage customer root keys (CRK) that are used to protect customer data stored in data and storage services in IBM Cloud. With the support of Keep You Own Key (KYOK), customers can maintain exclusive control of their HSMs and their keys. Also, customers can manage lifecycle of their customer root keys where they can create, rotate, delete those keys. This provides a significant level of control where those CRKs are managed by the customer, and exclusive control of the HSM, which in turn increases both security control as well as meet relevant compliance requirements. These CRKs are used in turn to protect the data encryption keys (DEK) used to encrypt the data. KYOK is supported by Hyper Protect Crypto Services and is the only service in the cloud industry that is built on FIPS 140-2 Level 4-certified hardware

Impact:

You cannot disable KMS provider encryption. Do not delete root keys in your KMS instance, even if you rotate to use a new key. If you delete a root key that a cluster uses, the cluster becomes unusable, loses all its data, and cannot be recovered.

Similarly, if you disable a root key, operations that rely on reading secrets fail. Unlike deleting a root key, however, you can reenable a disabled key to make your cluster usable again.

If you lose your key, you will not be able to recover the data. Standard pricing for Hyper Protect Crypto Services applies.

Audit:

1. Install the etcd CLI (`etcdctl`) version 3 or later.
2. Set your terminal session context to use the appropriate `etcdctl` API version.

```
export ETCDCTL_API=3
```

3. Run the `ibmcloud ks cluster config` command and include the `--admin` option, which downloads the `etcd` certificates and keys for your cluster, and the `--output zip > <cluster_name_or_ID>.zip` option, which saves your cluster configuration files to a compressed folder.

```
ibmcloud ks cluster config -c <cluster_name_or_ID> --admin --output zip >
<cluster_name_or_ID>.zip
```

4. Decompress the compressed folder.
5. Get the server field for your cluster. In the output, copy only the master URL, without `https://` and the node port.

```
cat ./<cluster_name_or_ID>/kube-config.yaml | grep server
```

6. Get the etcdPort for your cluster.

```
ibmcloud ks cluster get -c <cluster_name_or_ID> --output json | grep etcdPort
```

7. Get the name of a secret in your cluster.

```
kubectl get secrets [-n <namespace>]
```

8. Confirm that the Kubernetes secrets for the cluster are encrypted. Replace the secret_name, master_url, and etcd_portfields with the values that you previously retrieved, and replace <cluster_name_or_ID> with the name of the cluster in your compressed folder file path.

```
etcdctl get /registry/secrets/<secret_namespace>/<secret_name> --endpoints
https://<master_url>:<etcd_port> --key="./<cluster_name_or_ID>/admin-key.pem"
--cert="./<cluster_name_or_ID>/admin.pem" --
cacert="./<cluster_name_or_ID>/ca.pem"
```

9. Ensure the output is unreadable and scrambled, indicating that it is encrypted.

Remediation:

From Console:

1. Log in to your IBM Cloud account.
2. To view the list of services that are available on IBM Cloud, click **Catalog**.
3. Search for **Hyper Protect Crypto Services**.
4. Select a service plan, and click **Create** to provision an instance of Hyper Protect Crypto Services in the account, region, and resource group where you are logged in.
5. To view a list of your resources, go to **Menu** > **Resource List**.
6. From your IBM Cloud resource list, select your provisioned instance of Hyper Protect Crypto Services.
7. To create a new key, click **Add key** and select the **Create a key** window. Specify the key's name and key type.
8. When you are finished filling out the key's details, click **Create** key to confirm.
9. From the Clusters console, select the cluster that you want to enable encryption for.
10. From the **Overview** tab, in the **Summary** > **Key management service** section, click **Enable**.
11. Select the **Key management service** instance and **Root key** that you want to use for the encryption.
12. Click **Enable.**
13. Verify that the KMS enablement process is finished. From the **Summary** > **Master status** section, you can check the progress.
14. After the KMS provider is enabled in the cluster, data in etcd and new secrets that are created in the cluster are automatically encrypted by using your root key.
15. To encrypt existing secrets with the root key, rewrite the secrets. This cannot be done from the console. See the From Command Line section.

From Command Line:

1. Log in to IBM Cloud through the IBM Cloud CLI.

```
ibmcloud login [--sso]
```

2. Select the region and resource group where you want to create a Hyper Protect Crypto Services instance.

```
ibmcloud target -r <region_name> -g <resource_group_name>
```

3. Provision a public or private Hyper Protect Crypto Services instance.

```
ibmcloud resource service-instance-create <instance_name> kms tiered-pricing
<region> [-p '{"allowed_network": "private-only"}']
```

4. Create a customer root key (CRK) in your KMS instance. You can't use the CLI for this action, you must use the GUI or API. See the above **From Console** section.
5. Get the ID of the KMS instance that you previously created.

```
ibmcloud ks kms instance ls
```

6. Get the ID of the root key that you previously created.

```
ibmcloud ks kms crk ls --instance-id <KMS_instance_ID>
```

7. Enable the KMS provider to encrypt secrets in your cluster. Fill in the options with the information that you previously retrieved. The KMS provider's private service endpoint is used by default to download the encryption keys. To use the public service endpoint instead, include the `--public-endpoint` option. The enablement process can take some time to complete.

```
ibmcloud ks kms enable -c <cluster_name_or_ID> --instance-id
<kms_instance_ID> --crk <root_key_ID> [--public-endpoint]
```

8. Verify that the KMS enablement process is finished. The process is finished when the Master Status is Ready.
9. After the KMS provider is enabled in the cluster, data in etcd and new secrets that are created in the cluster are automatically encrypted by using your root key.
10. Set the context for your cluster.

```
ibmcloud ks cluster config -c <cluster_name_or_ID>
```

12. With cluster-admin access, rewrite the secrets to encrypt them.

```
kubectl get secrets --all-namespaces -o json | kubectl replace -f -
```

Default Value:

Kubernetes secrets are Base64 encoded but not encrypted.

References:

1. https://cloud.ibm.com/docs/containers?topic=containers-encryption#keyprotect
2. https://cloud.ibm.com/docs/hs-crypto

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.

7.1.2 Ensure TLS 1.2 for all inbound traffic at IBM Cloud Kubernetes Service Ingress (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all insecure (HTTP) client requests to applications and services hosted on IBM Cloud Kubernetes Service are redirected to secure TLS connections (HTTPS), and ensure that only TLS versions 1.2+ are supported.

You set up your Ingress ALB to secure your domain with the IBM-provided TLS certificate or your custom TLS certificate. Some users might try to access your apps by using an insecure `http` request to your ALB domain, for example `http://www.myingress.com`, instead of using `https`. You can use the redirect annotation to always convert insecure HTTP requests to HTTPS.

Rationale:

HTTPS uses the TLS protocol to provide a secure, encrypted connection between the client and the server. This protocol secures incoming requests to protect users from attack, for example, man in the middle attacks. IBM Cloud Kubernetes Service allows HTTPS to be configured, and it is highly recommended to do so. If you do not use this annotation, insecure HTTP requests are not converted into HTTPS requests by default and might expose unencrypted confidential information to the public.

Impact:

Incoming requests will not be able to use HTTP because all incoming requests will be redirected to HTTPS. Legacy clients that require TLS 1.0 or 1.1 support will not be able to access your apps.

Audit:

1. Get the configuration for the `ibm-cloud-provider-ingress-cm` configmap resource.

```
kubectl get cm ibm-cloud-provider-ingress-cm -n kube-system -o yaml
```

2. In the `data` section, ensure that the `ssl-protocols` key is not present, or if it is present, ensure that it does not include TLSv1 or TLSv1.1.
3. Get the configuration for your Ingress resource. by running the following command:

```
kubectl get ingress <my_ingress> -n <my_namespace> -o yaml
```

4. In the `annotations` section, ensure that the `ingress.bluemix.net/redirect-to-https` key is set to `"True"`.

```
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
 name: myingress
 annotations:
   ingress.bluemix.net/redirect-to-https: "True"
spec:
 tls:
 - hosts:
   - mydomain
   secretName: mytlssecret
 rules:
 - host: mydomain
   http:
     paths:
     - path: /
       backend:
         serviceName: myservice
         servicePort: 8080
```

Remediation:

1. Edit the configuration file for the `ibm-cloud-provider-ingress-cm` configmap resource by running the following command:

```
kubectl edit cm ibm-cloud-provider-ingress-cm -n kube-system
```

2. In the `data` section, remove the `ssl-protocols` key, or remove TLSv1 and TLSv1.1 from the value.
3. Edit the configuration for your Ingress resource by running the following command:

```
kubectl edit ingress <my_ingress> -n <my_namespace>
```

4. In the `annotations` section, add `ingress.bluemix.net/redirect-to-https: "True"`.

```
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
 name: myingress
 annotations:
   ingress.bluemix.net/redirect-to-https: "True"
spec:
 tls:
 - hosts:
   - mydomain
```

```
    secretName: mytlssecret
  rules:
  - host: mydomain
    http:
      paths:
      - path: /
        backend:
          serviceName: myservice
          servicePort: 8080
```

Default Value:

The default setting supports only TLS 1.2 and 1.3. Redirecting HTTP requests to HTTPS is disabled by default.

References:

1. https://cloud.ibm.com/docs/containers?topic=containers-ingress_annotation#ssl_protocols_ciphers
2. https://cloud.ibm.com/docs/containers?topic=containers-ingress_annotation#redirect-to-https
3. https://cloud.ibm.com/docs/containers?topic=containers-cs_cli_install

CIS Controls:

Version 7

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

7.1.3 Ensure IBM Cloud Kubernetes Service worker nodes are updated to the latest image to ensure patching of vulnerabilities (Automated)

Profile Applicability:

- Level 1

Description:

Update the worker nodes in a cluster to the latest patch version so that security fixes are applied to those worker nodes.

Rationale:

As security updates and patches are put in place for the API server and other master components, you must be sure that the worker nodes remain in sync. You can make two types of updates: updating only the patch version, or updating the `major.minor` version with the patch version. This benchmark is only in relation to updating the patch version, not the major or minor versions. Updating the patch version in a timely manner ensures patching of known vulnerabilities and will keep your worker nodes more secure.

Impact:

The worker node update also updates the worker node to the same `major.minor` version as the master if a `major.minor` update is also available.

Audit:

From Console:

1. Log in to the IBM Cloud console.
2. To view a list of your resources, go to **Menu** > **Resource List**.
3. From your IBM Cloud resource list, select your cluster.
4. Select the **Worker Nodes** tab.
5. For each listed worker node, ensure that next to the **Version** no information icon is present indicating that an update is available. If there is an information icon indicating there is an update available, then the worker node is not running the latest available image.

From Command Line:

1. List the clusters in your IBM Cloud account

```
ibmcloud ks cluster ls
```

2. List the workers for a given cluster.

```
ibmcloud ks workers -c <cluster_name_or_ID>
```

3. Ensure that next to the version for a worker node no asterisk (*) is present indicating that an update is available.
   a. Here is an example output that shows that there is an available update for a worker node

```
ibmcloud ks workers -c mykubecluster-free
OK
ID                                                         Public IP
Private IP      Flavor   State    Status   Zone    Version
kube-btdsgk5d0t1lpluh7f40-mykubeclust-default-000000d1   173.193.100.98
10.76.216.200   free     normal   Ready    hou02   1.17.11_1538*

* To update to 1.17.12_1541 version, run 'ibmcloud ks worker update'. Review
and make any required version changes before you update:
'https://ibm.biz/upworker'

b. Here is an example output showing there are no available updates for a
worker node

ibmcloud ks workers -c mykubecluster-free
OK
ID                                                         Public IP
Private IP      Flavor   State    Status   Zone    Version
kube-btdsgk5d0t1lpluh7f40-mykubeclust-default-000000d1   173.193.100.98
10.76.216.200   free     normal   Ready    hou02   1.17.12_1541
```

Remediation:

From Console:

1. Log in to the IBM Cloud console.
2. Optional: Add capacity to your cluster by resizing the worker pool. The pods on the worker node can be rescheduled and continue running on the added worker nodes during the update.
3. To view a list of your resources, go to **Menu** > **Resource List**.
4. From your IBM Cloud resource list, select your cluster.
5. Select the **Worker Nodes** tab.
6. Select the checkbox for each worker node that you want to update. An action bar is displayed over the table header row.
7. From the action bar, click **Update**.

From Command Line:

1. Complete the prerequisite steps.

2. Optional: Add capacity to your cluster by resizing the worker pool. The pods on the worker node can be rescheduled and continue running on the added worker nodes during the update.
3. List the worker nodes in your cluster and note the ID and Primary IP of the worker node that you want to update.

```
ibmcloud ks worker ls --cluster <cluster_name_or_ID>
```

4. Replace the worker node to update the worker node to the latest patch version at the same `major.minor` version.

```
ibmcloud ks worker replace --cluster <cluster_name_or_ID> --worker
<worker_node_ID>
```

5. Repeat these steps for each worker node that you want to update.
6. Optional: After the replaced worker nodes are in a Ready status, resize the worker pool to meet the cluster capacity that you want.

Default Value:

Worker nodes are not updated unless the user initiates an update.

References:

1. https://cloud.ibm.com/docs/containers?topic=containers-update#vpc_worker_node
2. https://cloud.ibm.com/docs/containers?topic=containers-cs_versions#update_types
3. https://cloud.ibm.com/docs/containers?topic=containers-cs_versions#version_types

CIS Controls:

Version 7

18.4 Only Use Up-to-date And Trusted Third-Party Components
Only use up-to-date and trusted third-party components for the software developed by the organization.

7.1.4 Ensure that clusters are accessible only by using private endpoints (Automated)

Profile Applicability:

- Level 1

Description:

Disable the public service endpoint so that communication to the master from both the worker nodes and cluster users is established over the private network through the private service endpoint.

Rationale:

When using only the private service endpoint, services are no longer being served on an internet routable IP address. It is more secure and increasingly common for cloud consumers to want limited or no access to the public internet from any of their services.

Impact:

To access the master, cluster users must either be in your VPC network or connect through a VPC VPN connection. If your worker nodes must access a public endpoint outside of the cluster, you must enable a public gateway on the VPC subnets that worker nodes are deployed to.

Audit:

From Console:

1. Log in to the IBM Cloud console at https://cloud.ibm.com/.
2. To view a list of your resources, go to **Menu** > **Resource List**.
3. From your IBM Cloud resource list, select your cluster.
4. From the **Overview** tab, if the **Public service endpoint URL** field has a button that says **Enable**, then the public service endpoint is disabled.

From Command Line:

1. Get the info for your cluster.

```
ibmcloud ks cluster get --cluster <cluster_name_or_ID>
```

2. If the Public Service Endpoint URL field in the output is not populated, then the public service endpoint is disabled.

Remediation:

From Console:

1. Log in to the IBM Cloud console at https://cloud.ibm.com/.
2. To view a list of your resources, go to **Menu** > **Resource List**.
3. From your IBM Cloud resource list, select your cluster.
4. From the **Overview** tab, click the **Disable** button for the public service endpoint.
5. In the modal, click **Disable** to confirm.
6. In the next modal, click **Refresh** to initiate an API server refresh.
7. Optional: Add capacity to your cluster by resizing the worker pool. The pods on the worker node can be rescheduled and continue running on the added worker nodes during the update.
8. From the **Worker Nodes** tab, select your worker nodes and click **Replace**.
9. In the modal, click **Replace** to confirm.

From Command Line:

1. Disable the public service endpoint.

```
ibmcloud ks cluster feature disable public-service-endpoint --cluster
<cluster_name_or_ID>
```

2. Confirm the action by clicking **yes**.
3. Optional: Add capacity to your cluster by resizing the worker pool. The pods on the worker node can be rescheduled and continue running on the added worker nodes during the update.
4. Replace the worker nodes so that their configuration is updated to remove the public service endpoint.

```
ibmcloud ks worker replace --cluster <cluster_name_or_ID> --worker
<worker_node_ID>
```

Default Value:

The public service endpoint is enabled by default. The private service endpoint is enabled and cannot be disabled.

References:

1. https://cloud.ibm.com/docs/containers?topic=containers-plan_clusters#vpc-workeruser-master

CIS Controls:

Version 7

12.2 Scan for Unauthorized Connections across Trusted Network Boundaries
Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

7.1.5 Ensure IBM Cloud Kubernetes Service cluster has image pull secrets enabled (Automated)

Profile Applicability:

- Level 1

Description:

Image pull secrets are credentials that authorize your cluster to pull images from a private image registry. IBM Cloud Kubernetes Service integrates with IBM Cloud Container Registry and provides pull secrets for IBM Cloud Container Registry in the `default` Kubernetes namespace.

Rationale:

IBM Cloud Kubernetes Service clusters pull images from image registries to run containers. If the image registry is private, the cluster needs credentials to pull images from it. Because IBM Cloud Kubernetes Service and IBM Cloud Container Registry are often used in tandem, it is important to have image pull secrets for IBM Cloud Container Registry enabled in your cluster.

Impact:

Pull secrets are created in the `default` namespace of your cluster. If you want to pull images to other Kubernetes namespaces, then you must copy the pull secrets to those other namespaces.

Audit:

From Console:

1. Log in to the IBM Cloud console at https://cloud.ibm.com/.
2. To view a list of your resources, go to **Menu** > **Resource List**.
3. From your IBM Cloud resource list, select your cluster.
4. From the **Overview** tab, the **Image pull secrets** field should say **Enabled**.

From Command Line:

1. Get the information for your cluster.

```
ibmcloud ks cluster get --cluster <cluster_name_or_ID>
```

2. The Pull Secrets field in the output should say "enabled in the default namespace."

Remediation:

From Console:

1. Log in to the IBM Cloud console at https://cloud.ibm.com/.
2. To view a list of your resources, go to **Menu** > **Resource List**.
3. From your IBM Cloud resource list, select your cluster.
4. From the **Overview** tab, for **Image pull secrets**, click **Enable**.
5. In the modal, click **Enable** to confirm.

From Command Line:

1. Run the following command to create a service ID for the cluster and assign the service ID an IAM Reader service role for IBM Cloud Container Registry. The command also creates an API key to impersonate the service ID credentials and stores the API key in a Kubernetes image pull secret in the default namespace of the cluster.

```
ibmcloud ks cluster pull-secret apply --cluster <cluster_name_or_ID>
```

Default Value:

Image pull secrets are enabled by default unless the user that created the cluster did not have the required permissions for IBM Cloud Container Registry in IAM. Clusters created before 25 February 2019 have token-based image pull secrets rather than API key-based image pull secrets, and therefore must be updated.

References:

1. https://cloud.ibm.com/docs/containers?topic=containers-registry#imagePullSecret_migrate_api_key
2. https://cloud.ibm.com/docs/containers?topic=containers-registry#cluster_registry_auth_default

CIS Controls:

Version 7

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

7.1.6 Ensure IBM Cloud Kubernetes Service clusters have the monitoring service enabled (Automated)

Profile Applicability:

- Level 1

Description:

Metrics help you monitor the health and performance of your clusters. Create a monitoring configuration to forward cluster and app metrics to IBM Cloud Monitoring with Sysdig.

Use the IBM Cloud Kubernetes Service observability plug-in to create a monitoring configuration for IBM Cloud Monitoring with Sysdig in your cluster, and use this monitoring configuration to automatically collect and forward metrics to IBM Cloud Monitoring with Sysdig.

With IBM Cloud Monitoring with Sysdig, you can collect cluster and pod metrics, such as the CPU and memory usage of your worker nodes, incoming and outgoing HTTP traffic for your pods, and data about several infrastructure components. In addition, the agent can collect custom application metrics by using either a Prometheus-compatible scraper or a StatsD facade.

IBM Cloud Monitoring with Sysdig is a cloud-native, and container-intelligence management system that you can include as part of your IBM Cloud architecture. Use it to gain operational visibility into the performance and health of your applications, services, and platforms. It offers administrators, DevOps teams and developers full stack telemetry with advanced features to monitor and troubleshoot, define alerts, and design custom dashboards. IBM Cloud Monitoring with Sysdig is operated by Sysdig in partnership with IBM.

Rationale:

Gain operational visibility into the performance and health of your apps and your cluster by deploying a Sysdig agent to your worker nodes. The agent collects pod and cluster metrics, and sends these metrics to IBM Cloud Monitoring with Sysdig.

Get critical Kubernetes and container insights for dynamic microservice monitoring.

IBM Cloud Monitoring with Sysdig auto-discovers Kubernetes environments providing out-of-the-box dashboards and alerts for clusters, nodes, namespaces, services, deployments, pods and more. A single agent per node dynamically discovers all microservices and auto-collects metrics and events from various sources including Kubernetes, hosts, networks, containers, processes, applications and custom metrics like Prometheus, JMX, and StatsD.

Mitigate the impact of abnormal situations with proactive notifications.

IBM Cloud Monitoring with Sysdig includes alerts and multi-channel notifications that you can use to reduce the impact on your day to day operations and accelerate your reaction and response time to anomalies, downtime, and performance degradation. Notification channels that you can easily configure include email, slack, PagerDuty, Webhooks, OpsGenie, and VictorOps.

Impact:

Before you provision an instance, consider the following information:

- The account owner can create, view, and delete an instance of a service in the IBM Cloud. This user can also grant permissions to other users to work with the IBM Cloud Monitoring with Sysdig service.
- Other IBM Cloud users with administrator or editor permissions can manage the IBM Cloud Monitoring with Sysdig service in the IBM Cloud. These users must also have platform permissions to create resources within the context of the resource group where they plan to provision the instance.

After you provision an instance, you must configure metric sources, enable platform metrics, or both. After the IBM Cloud Monitoring with Sysdig agent is deployed in a metric source, collection and forwarding of metrics to the instance is automatic. The IBM Cloud Monitoring with Sysdig agent automatically collects and reports on pre-defined metrics. You can configure which metrics to monitor in an environment.

You can only configure 1 Sysdig instance in a region to automatically collect platform metrics.

Standard pricing for IBM Cloud Monitoring with Sysdig applies.

Audit:

From Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon --> Resource list**
3. Select your cluster under *Clusters* to go to the details page.
4. Select the **Overview** tab
5. Under **Monitoring** there should be a button to **Launch** the Sysdig dashboard. If instead the button is labeled **Connect**, then monitoring is not enabled.

From Command Line:

1. Check whether a logging configuration is added to your cluster. If one is added, the output of this command will include the monitoring instance name and ID along with some other information.

```
ibmcloud ob monitoring config list --cluster <cluster_name_or_ID>
```

Remediation:

From Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon --> Resource list**
3. Select your cluster under *Clusters* to go to the details page.
4. Select the **Overview** tab
5. Under **Monitoring** click *Connect*.
6. Select the region and the IBM Cloud Monitoring with Sysdig service instance that you want to use (or *create an instance*), and click **Connect**.

From Command Line:

1. Create the Sysdig monitoring configuration.

```
ibmcloud ob monitoring config create --cluster <cluster_name_or_ID> --
instance <Sysdig_instance_name_or_ID>
```

Default Value:

IBM Cloud Monitoring with Sysdig is not configured by default.

References:

1. https://cloud.ibm.com/docs/containers?topic=containers-health#sysdig
2. https://cloud.ibm.com/docs/Monitoring-with-Sysdig

CIS Controls:

Version 7

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

6.6 Deploy SIEM or Log Analytic tool
Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.

6.8 Regularly Tune SIEM

On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

7.1.7 Ensure IBM Cloud Kubernetes Service clusters have the logging service enabled (Automated)

Profile Applicability:

- Level 1

Description:

Create a logging configuration to forward cluster and app logs to IBM Log Analysis with LogDNA. IBM Log Analysis with LogDNA offers administrators, DevOps teams, and developers advanced features to filter, search, and tail log data, define alerts, and design custom views to monitor application and system logs.

Rationale:

Troubleshoot logs in real time to diagnose issues and identify problems.

By using the live streaming tail feature, developers and DevOps teams can diagnose issues, analyze stack traces and exceptions, identify the source of errors, and monitor different log sources through a single view.

Issue alerts to be notified of important actions.

To act promptly on application and services events that you identify as critical or warning, DevOps teams can configure alert notification integrations to the following systems: email, Slack, webHook, and PagerDuty.

Export logs to a local file for analysis or to an archive service to meet auditing requirements.

Export specific log lines to a local copy or archive logs from IBM Log Analysis with LogDNA to IBM Cloud Object Storage. Log lines are exported in JSON line format. Logs are archived in JSON format and preserve the metadata that is associated with each line.

Control logging infrastructure costs by customizing what logs to manage through IBM Log Analysis with LogDNA.

Control the cost of your logging infrastructure in the IBM Cloud by configuring the log sources for which you want to collect and manage logs.

Impact:

Before you provision an instance of IBM Log Analysis with LogDNA, consider the following information:

- Log data is hosted on the IBM Cloud.
- The IBM Log Analysis with LogDNA service is operated by LogDNA.
- Your users must have platform permissions to create, view, and delete an instance of a service in the IBM Cloud.
- Your users must have platform permissions to create resources within the context of the resource group where you plan to provision the LogDNA instance.

After you provision an instance of IBM Log Analysis with LogDNA, an account is created in LogDNA, and you receive the ingestion key for your account. Then, you must configure your log sources.

Different pricing plans are available that you can choose for an IBM Log Analysis with LogDNA instance. Each plan defines the number of days that data is retained for search, the number of users allowed to manage the data, and the LogDNA features that are enabled.

Audit:

From Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon --> Resource list**
3. Select your cluster under *Clusters* to go to the details page.
4. Select the **Overview** tab
5. Under **Logging** there should be a button to **Launch** the LogDNA dashboard. If instead the button is labeled **Connect**, then logging is not enabled.

From Command Line:

1. Install the IBM Cloud Kubernetes Service observability plug-in.

```
ibmcloud plugin install observe-service
```

2. Check whether a logging configuration is added to your cluster. If one is added, the output of this command will include the logging instance name and ID along with some other information.

```
ibmcloud ob logging config list --cluster <cluster_name_or_ID>
```

Here is example output showing a cluster which has logging enabled

```
ibmcloud ob logging config list --cluster example_cluster_logging_enabled
Listing configurations...

OK

Instance name:      IBM Log Analysis with LogDNA-r9
Instance ID:        eb70d90c-846a-475a-8e9d-577c2c122186
CRN:                crn:v1:bluemix:public:logdna:us-
south:a/9c1bf944d2043179dae70822c0168e15:eb70d90c-846a-475a-8e9d-
577c2c122186::
Agent Namespace:    ibm-observe
Private Endpoint:   false
Discovered Agent:   false
```

Remediation:

From Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon --> Resource list**
3. Select your cluster under *Clusters* to go to the details page.
4. Select the **Overview** tab
5. Under **Logging**, click **Connect**.
6. Select the region and the IBM Log Analysis with LogDNA service instance that you want to use, and click **Connect**.

From Command Line:

1. Install the IBM Cloud Kubernetes Service observability plug-in.

```
ibmcloud plugin install observe-service
```

2. Create the LogDNA logging configuration.

```
ibmcloud ob logging config create --cluster <cluster_name_or_ID> --instance
<LogDNA_instance_name_or_ID>
```

Default Value:

By default, logs are generated and written locally for all of the following IBM Cloud Kubernetes Service cluster components: worker nodes, containers, applications, persistent storage, Ingress application load balancer, Kubernetes API, and the `kube-system` namespace. However, the logging service for collecting, forwarding, and viewing these logs is not enabled for IBM Cloud Kubernetes Service clusters by default.

References:

1. https://cloud.ibm.com/docs/containers?topic=containers-health#logdna

2. https://cloud.ibm.com/docs/containers?topic=containers-observability_cli
3. https://cloud.ibm.com/docs/Log-Analysis-with-LogDNA

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.

7.2 Container Registry

Use IBM Cloud™ Container Registry to store and access private container images in a highly available and scalable architecture.

IBM Cloud Container Registry provides a multi-tenant, highly available, scalable, and encrypted private image registry that is hosted and managed by IBM®. You can use IBM Cloud Container Registry by setting up your own image namespace and pushing container images to your namespace.

7.2.1 Block deployments of vulnerable images to Kubernetes clusters (Automated)

Profile Applicability:

- Level 1

Description:

Vulnerability Advisor provides security management for IBM Cloud Container Registry, generating a security status report that includes suggested fixes and best practices. Images for which Vulnerability Advisor reports vulnerabilities should not be deployed to Kubernetes clusters. Container Image Security Enforcement (CISE) retrieves information from Vulnerability Advisor to block deployments of vulnerable images.

Rationale:

Container images contain various packages that can be vulnerable to common vulnerabilities and exposures (CVEs). If an image contains such vulnerable packages, it is at risk of being exploited by malicious actors. Vulnerability Advisor scans images for CVEs to identify any potential issues with your container images. If an issue is detected in one of your images, that image should not be deployed to a Kubernetes cluster, to prevent exposure.

Impact:

If the Container Image Security Enforcement admission controller is deployed in a cluster and is configured to enforce Vulnerability Advisor policies, deployments of images that have not passed the Vulnerability Advisor scan are blocked.

Audit:

1. Set the cluster as the context for this session.

```
ibmcloud ks cluster config --cluster <cluster_name_or_ID>
```

2. Set up Helm in your cluster.
3. Use Helm to list releases.

```
helm list
```

4. Check the output for a release for which the chart is `ibmcloud-image-enforcement`. A version is appended to that name, for example, `ibmcloud-image-enforcement-0.2.10`.
5. When CISE is installed, it creates a cluster-wide default policy. Get this default policy.

```
kubectl get clusterimagepolicies.securityenforcement.admission.cloud.ibm.com
ibmcloud-default-cluster-image-policy -o yaml
```

6. In the `repositories` array, check for the following output. This configuration will block the deployment of images that have not passed the Vulnerability Advisor scan. Specifically, in the *va* section, ensure *enabled* is **true**

```
- name: '*'
  policy:
    va:
      enabled: true
```

Remediation:

1. Set the cluster as the context for this session.

```
ibmcloud ks cluster config --cluster <cluster_name_or_ID>
```

2. Set up Helm in your cluster.
3. Add the IBM chart repository to your Helm client.

```
helm repo add iks-charts https://icr.io/helm/iks-charts
```

4. Install the Container Image Security Enforcement Helm chart into your cluster.

For Helm 2:

```
helm install --name cise iks-charts/ibmcloud-image-enforcement
```

For Helm 3:

```
helm install cise iks-charts/ibmcloud-image-enforcement
```

5. Container Image Security Enforcement is now installed, and applies the default security policy for all Kubernetes namespaces in your cluster. For information about customizing the security policy for Kubernetes namespaces in your cluster, or the cluster overall, see Customizing policies.

Default Value:

Vulnerable images can be deployed to Kubernetes clusters by default.

References:

1. https://cloud.ibm.com/docs/Registry?topic=Registry-security_enforce
2. https://cloud.ibm.com/docs/containers?topic=containers-helm#helm

CIS Controls:

Version 7

3.2 Perform Authenticated Vulnerability Scanning
Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.

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 Key Management

8.1 IBM Key Protect for IBM Cloud

IBM® Key Protect for IBM Cloud™ helps you provision encrypted keys for apps across IBM Cloud services.

From the Key Protect dashboard, you can create new keys for cryptography, or you can import your existing keys.

Choose from two key types:

Root keys

Root keys are symmetric key-wrapping keys that you fully manage in Key Protect. You can use a root key to protect other cryptographic keys with advanced encryption. To learn more, see Protecting data with envelope encryption.

Standard keys

Standard keys are symmetric keys that are used for cryptography. You can use a standard key to directly encrypt and decrypt data.

8.1.1 Ensure IBM Key Protect has automated rotation for customer managed keys enabled (Automated)

Profile Applicability:

- Level 2

Description:

In Key Protect, you can set a rotation policy for a key or manually rotate the key.

IBM Cloud Key Management Service (KMS): Key Protect (KP) allows customers to rotate the Data Encryption Key (DEK) which is key material stored within the KMS Hardware Security Module (HSM), which is tied to the key ID of the Customer Created customer master key (CMK). It is the DEK that is used to perform cryptographic operations such as encryption and decryption. When it's time to rotate the key based on the rotation interval that you specify, Key Protect automatically replaces the root key with new key material. Automated key rotation currently retains all prior DEK keys so that decryption of encrypted data can take place transparently.

How key rotation works

Key rotation works by securely transitioning key material from an Active to a Deactivated key state. To replace the deactivated or retired key version, the new key version moves into the Active state and becomes available for cryptographic operations.

Frequency of key rotation

After you generate a root key in Key Protect, you decide the frequency of its rotation. You might want to rotate your keys due to personnel turnover, process malfunction, or according to your organization's internal key expiration policy.

Rotate your keys regularly, for example every 30 days, to meet cryptographic best practices.

Rationale:

Rotating keys on a regular basis helps you meet industry standards and cryptographic best practices. The following describes the main benefits of key rotation:

- **Cryptoperiod management for keys** - Key rotation limits how long your information is protected by a single key. By rotating your root keys at regular intervals, you also shorten the cryptoperiod of the keys. The longer the lifetime of an encryption key, the higher the probability for a security breach.

- **Incident mitigation** - If your organization detects a security issue, you can immediately rotate the key to mitigate or reduce costs that are associated with key compromise.

Impact:

After a rotation completes, a new key version becomes available for protecting data encryption keys (DEKs) with *envelope encryption*. Retired root key versions moves to the *Deactivated* state, where they can only be used to unwrap and access older DEKs that aren't yet protected by the latest root key.

To secure your envelope encryption workflow, rewrap your DEKs after you rotate a root key so that your at-rest data is protected by the newest root key.

Alternatively if Key Protect detects that you're using retired key versions to unwrap a DEK, the service automatically reencrypts the DEK and returns a wrapped data encryption key (WDEK) that's based on the latest root key.

Audit:

Console:

1. Log in to the IBM Cloud console.
2. Go to **Menu > Resource List** to view a list of your resources.
3. From your IBM Cloud resource list, select your provisioned instance of Key Protect.
4. On the application details page, use the *Keys* table to browse the keys in your service.
5. Click the ▯ **icon** to open a list of options for a specific key.
6. From the options menu, click **Manage policy** to manage the rotation policy for the key.
7. From the list of rotation options, if your key has an existing rotation policy, the interface displays the key's existing rotation period.

API:
For a high-level view, you can browse the rotation policies that are associated with a root key by making a GET call to the following endpoint.

```
https://<region>.kms.cloud.ibm.com/api/v2/keys/<key_ID>/policies
```

1. Retrieve your service and authentication credentials.
2. Retrieve the rotation policy for a specified key by running the following cURL command.

```
$ curl -X GET \
    "https://<region>.kms.cloud.ibm.com/api/v2/keys/<key_ID>/policies" \
    -H "authorization: Bearer <IAM_token>" \
    -H "bluemix-instance: <instance_ID>" \
    -H "content-type: application/vnd.ibm.kms.policy+json" \
    -H "correlation-id: <correlation_ID>"
```

Replace the variables in the example request according to the following table.

```
Variable       Description
key_ID  Required. The unique identifier for the root key that has an existing
rotation policy.
region  Required. The region abbreviation, such as us-south or eu-gb, that
represents the geographic area where your Key Protect instance resides.
For more information, see Regional service endpoints.

IAM_token      Required. Your IBM Cloud access token. Include the full
contents of the IAM token, including the Bearer value, in the cURL request.
For more information, see Retrieving an access token.

instance_ID    Required. The unique identifier that is assigned to your Key
Protect service instance.
For more information, see Retrieving an instance ID.

correlation_ID The unique identifier that is used to track and correlate
transactions.
A successful GET api/v2/keys/{id}/policies response returns policy details
that are associated with your key.
```

CLI:
Run the following command to get a list of all the keys and their associated KeyIDs
For each key, note the keyID and run the following command to get the key rotation status:

```
ibmcloud kp key policies KEY_ID
     -i, --instance-id INSTANCE_ID
    [-d, --dual-auth]
    [-o, --output      OUTPUT]
    [-r, --rotation]

Required parameters
KEY_ID    The ID of the key that you want to query. To retrieve a list of
your available keys, run the kp keys command.
-i, --instance-id      The IBM Cloud instance ID that identifies your Key
Protect instance. You can export KP_INSTANCE_ID=INSTANCE_ID instead of
specifying -i.

Optional parameters
-d, --dual-auth    Show policies that have a dual-auth-delete policy.
-o, --output    Set the CLI output format. By default, all commands print in
table format. To change the output format to JSON, use --output json.
-r, --rotation    Show policies that have a rotation policy.
```

Remediation:

Console:

1. Log in to the IBM Cloud console.
2. Go to **Menu > Resource List** to view a list of your resources.
3. From your IBM Cloud resource list, select your provisioned instance of Key Protect.
4. On the application details page, use the *Keys* table to browse the keys in your service.
5. Click the ⍰ **icon** to open a list of options for a specific key.
6. From the options menu, click **Manage policy** to manage the rotation policy for the key.
7. From the list of rotation options, select a frequency of rotation in months. If your key has an existing rotation policy, the interface displays the key's existing rotation period.
8. Click **Create policy** to set the policy for the key.

API:

Create or update a rotation policy for your root key by making a PUT call to the following endpoint.

```
https://<region>.kms.cloud.ibm.com/api/v2/keys/<key_ID>/policies
```

1. Retrieve your service and authentication credentials.
2. Create or update a rotation policy for a specified key by running the following cURL command.

```
$ curl -X PUT \
    "https://<region>.kms.cloud.ibm.com/api/v2/keys/<key_ID>/policies" \
    -H "authorization: Bearer <IAM_token>" \
    -H "bluemix-instance: <instance_ID>" \
    -H "content-type: application/vnd.ibm.kms.policy+json" \
    -H "correlation-id: <correlation_ID>" \
    -d '{
            "metadata": {
                "collectionType": "application/vnd.ibm.kms.policy+json",
                "collectionTotal": 1
            },
            "resources": [
                {
                    "type": "application/vnd.ibm.kms.policy+json",
                    "rotation": {
                        "interval_month": <rotation_interval>
                    }
                }
            ]
        }'
```

Replace the variables in the example request according to the following table.

```
Variable       Description
key_ID  Required. The unique identifier for the root key that you want to
create a rotation policy for.
region  Required. The region abbreviation, such as us-south or eu-gb, that
represents the geographic area where your Key Protect instance resides.
For more information, see Regional service endpoints.

IAM_token      Required. Your IBM Cloud access token. Include the full
contents of the IAM token, including the Bearer value, in the cURL request.
For more information, see Retrieving an access token.

instance_ID    Required. The unique identifier that is assigned to your Key
Protect service instance.
For more information, see Retrieving an instance ID.

correlation_ID The unique identifier that is used to track and correlate
transactions.
rotation_interval      Required. An integer value that determines the key
rotation interval time in months. The minimum is 1 and the maximum is 12.
This can also overwrite an existing rotation interval for an update.
A successful PUT api/v2/keys/{id}/policies response returns policy details
that are associated with your key.
```

CLI:
Run the following command to enable key rotation by updating the key rotation policy:

```
ibmcloud kp key policy-update rotation KEY_ID
     -i, --instance-id      INSTANCE_ID
    [-m, --monthly-interval MONTHS]
    [-o, --output           OUTPUT]

Required parameters
KEY_ID    The ID of the key that you want to query. To retrieve a list of
your available keys, run the kp keys command.

Optional parameters
-m, --monthly-interval     Set the key rotation interval in months. The
deault is 1 (one) month. The rotation interval must be 1 to 12 months.
-o, --output     Set the CLI output format. By default, all commands print in
table format. To change the output format to JSON, use --output json.
```

Default Value:

By default, IBM Cloud accounts CKM and DEK depend on the account admin to set key rotation policy.

References:

1. https://cloud.ibm.com/docs/key-protect?topic=key-protect-key-rotation
2. https://cloud.ibm.com/docs/key-protect?topic=key-protect-set-rotation-policy
3. https://cloud.ibm.com/docs/key-protect?topic=key-protect-view-key-versions
4. https://cloud.ibm.com/docs/key-protect?topic=key-protect-rotate-keys

5. https://cloud.ibm.com/docs/key-protect?topic=key-protect-cli-reference#kp-key-policies
6. https://cloud.ibm.com/docs/key-protect?topic=key-protect-cli-reference#kp-key-policy-update-rotation

CIS Controls:

Version 7

13 Data Protection
Data Protection

8.1.2 Ensure the IBM Key Protect service has high availability (Manual)

Profile Applicability:

- Level 1

Description:

IBM® Key Protect for IBM Cloud™ is a regional key management service with automatic features that help keep your applications secure and operational.

Key Protect can be configured to provide high availability capabilities, such as IBM-owned infrastructure in multizone regions, to meet local access and low latency requirements for each supported region. Additionally, it can be configured to continuously back up keys in the region that the service operates in, and automatically recover and restart service components after any disaster event. You are responsible to plan for availability configuration on the different regions, and copying keys into a backup instance of Key Protect on a periodic basis.

Rationale:

Applications that communicate over networks are subject to transient faults. You should design your application to interact with Key Protect by using modern resiliency techniques, such as Exponential backoff. High availability of the key management service is necessary for both load balancing and fault tolerance.

Disaster recovery is about surviving a catastrophic failure or loss of availability in a single location. For the console and platform services, there are no actions that you need to take to prepare for an event of a catastrophic failure in a region.

Impact:

High availability and disaster recovery are available for the Key Management Service. Customers are responsible to use and configure the high availability approach according to their needs, and to backup the keys on a regular basis.

Audit:

Console:
To get a list of Key Protect instances from the IBM Cloud console, complete the following steps.

1. Log in to your IBM Cloud account.
2. Click **Catalog** to view the list of services that are available on IBM Cloud.

3. From the *All Categories* navigation pane, click the **Security and Identity** category.
4. From the list of services, click the **Key Protect** tile.
5. Review the instance of Key Protect in the account, region, and resource group where you are logged in.

API: N/A

Remediation:

Console:
To get a list of Key Protect instances from the IBM Cloud console, complete the following steps.

1. Log in to your IBM Cloud account.
2. Click **Catalog** to view the list of services that are available on IBM Cloud.
3. From the *All Categories* navigation pane, click the **Security and Identity** category.
4. From the list of services, click the **Key Protect** tile.
5. Select a service plan, and click **Create** to provision an instance of Key Protect in the account, region, and resource group where you are logged in.

Default Value:

By default, IBM Cloud Key Protect Service is ready but not configured for high availability. It is the customer discretion to configure HA according to their needs.

References:

1. https://cloud.ibm.com/docs/key-protect?topic=key-protect-provision
2. https://cloud.ibm.com/docs/key-protect?topic=key-protect-shared-responsibilities
3. https://cloud.ibm.com/docs/key-protect?topic=key-protect-ha-dr

CIS Controls:

Version 7

13 Data Protection
Data Protection

9 Security and Compliance

With IBM Cloud® Security and Compliance Center, you can embed security checks into your every day workflows to help monitor for security and compliance. By monitoring for risks, you can identify security vulnerabilities and quickly work to mitigate the impact and fix the issue.

9.1 Ensure alerts are enabled for vulnerabilities discovered in container images in Container Registry (Automated)

Profile Applicability:

- Level 1

Description:

With IBM Cloud™ Security Advisor, you can instantly view the security posture of your IBM Cloud services through a single, centralized dashboard.

The service receives security information from various sources and displays any security alerts or vulnerabilities that require your attention in the service dashboard. Out of the box, there are several pre-populated cards in your dashboard. These findings are from security services in IBM Cloud, but you can also add cards or custom partner solutions so that all of your security tools can be accessed from the same location.

Through pre-integrated findings, you can monitor:

- Certificates that you manage with IBM Cloud Certificate Manager
- Vulnerabilities in container images that are stored in IBM Cloud Container Registry

Monitoring vulnerabilities in container images

With Container Registry, you have access to Vulnerability Advisor, which continuously scans the images in your Container Registry instance for potential security issues. If issues are found, you are alerted and can view a comprehensive report in your Security Advisor dashboard.

Enable alerts for critical/high/medium vulnerabilities discovered in container images in Container Registry to ensure that workload vulnerabilities are addressed in a timely manner and not deployed to a production environment.

Rationale:

Security Insights in the IBM Cloud Security and Compliance Center offers notification alerts in Vulnerability Advisor to identify vulnerabilities in developer owned and base container images which are often overlooked. This feature alerts for vulnerabilities in images used explicitly and implicitly. It is recommended alerts for critical/high/medium vulnerable container images in Container Registry be enabled for every image.

Impact:

A significant percentage of data breaches are caused by users who have forgotten to update their dependency and runs a more vulnerable version in production. If the control of alerts is not utilized, vulnerable images will likely be written into production more often than desired and will quickly be vulnerable to a cyberattack. With Security Advisor alerts in place, you are notified and can start resolving issues immediately.

Before you begin Before you get started with alerts, you must have the following prerequisites:

- The Manager IAM role.
- A configured webhook. If you don't have one already, try using Cloud Functions.

Audit:

Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon > Security and Compliance**.
3. In the *Gain insight* section of the navigation, click **Configure-->Alerts**.
4. Verify that at least one channel is listed and is set to *Enabled*.

Remediation:

All remediation steps must be applied to the vulnerability in the container image by image owners.
Console:

1. Log in to IBM Cloud at https://cloud.ibm.com.
2. Click **Menu icon > Security and Compliance**.
3. In the *Gain insight* section of the navigation, click **Configure-->Alerts**.
4. Click **Create channel**.
5. Provide a *Name*, optional *Description*, and *Channel endpoint*.
6. Under *Severity for notifications*, Select *Critical*, *High*, and *Medium*
7. Click **Save**

Default Value:

By default, Vulnerability Advisor alerts are not configured for container images in Container Registry.

References:

1. https://nvd.nist.gov/800-53/Rev4/control/RA-5

2. https://cloud.ibm.com/docs/security-advisor?topic=security-advisor-getting-started
3. https://cloud.ibm.com/security-advisor#/notifications

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.

10 IBM Cloud Certificate Manager

IBM Cloud Certificate Manager is a managed service on IBM Cloud that allows to securely manage the lifecycle of digital certificates, ensure certificates are valid and renewed before expiration (when applicable). Certificate Manager provides integrated experience with various components of IBM Cloud such as Kubernetes Service, API Gateway, VPC Load Balancer, Cloud Internet Services, Activity Tracker and more. It is recommended that Certificate Manager be used for any workload running on IBM Cloud.

10.1 Ensure certificates generated through IBM Cloud Certificate Manager are automatically renewed before expiration (Automated)

Profile Applicability:

- Level 1

Description:

You can use the IBM Cloud™ Certificate Manager service dashboard to manage certificates that you obtain from third-party issuers, or order from Certificate Manager, to use with your IBM cloud-based apps or services.

You can manually or automatically renew certificates that you order through Certificate Manager. You can also disable the auto-renewal feature after you enable it. You can set a certificate to automatically renew while you're ordering. Or, you can enable auto-renewal after it's configured.

Rationale:

Cloud applications and services running on the platform might use certificate for different purposes - TLS or mTLS, client/server authentication and more. Ensuring your certificates are stored securely, and renewed before they expired is crucial to maintaining high security posture.

Impact:

Without proper Certificate Management practices in place organization risk to be vulnerable to impersonation attacks in case certificates used for authentication will be leaked and service outages in case certificates are not renewed on time.

Audit:

1. Log in to IBM Cloud at https://cloud.ibm.com
2. Click the **Menu** icon and select **Resource List**
3. On the **Resource List** page under **Services**, perform the following for each Certificate Manager instance that you have provisioned.
   a. Click on the Certificate Manager instance to view the configuration for the service.
   b. Click on **Your certificates**.
   c. Examine the **Expires In** column and verify that none of the certificates have expired
   d. Verify the **auto renew** toggle is set to **on**

Remediation:

1. Log in to IBM Cloud at https://cloud.ibm.com
2. Click the **Menu** icon and select **Resource List**
3. On the **Resource List** page under **Services**, perform the following for each Certificate Manager instance that you have provisioned.
   a. Click on the Certificate Manager instance to view the configuration for the service.
   b. In order to renew the certificate manually click on the options menu and select **Renew**.
   c. Note certificates manually imported into Certificate Manager cannot be automatically renewed. In order to renew those certificates click the options menu and select **Reimport**.

The process can be automated by configuring Slack or Webhook based expiration notifications in the Notifications section of Certificate Manager Dashboard. From the Certificate Manager instance configuration screen,

1. Click **Notifications**.
2. Click the **Create** button.
3. Select the *Channel type* and enter in the *Channel endpoint* URL.
4. Ensure the *Enable/Disable* toggle is set to **On**.
5. Click the **Save icon**

Default Value:

By default auto-renew is turned off and certificates must be manually renewed

References:

1. http://cloud.ibm.com/docs/certificate-manager

CIS Controls:

Version 7

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

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**IAM**		
1.1	Monitor account owner for frequent, unexpected, or unauthorized logins (Manual)	□	□
1.2	Ensure API keys unused for 180 days are detected and optionally disabled (Manual)	□	□
1.3	Ensure API keys are rotated every 90 days (Manual)	□	□
1.4	Restrict user API key creation and service ID creation in the account via IAM roles (Manual)	□	□
1.5	Ensure no owner account API key exists (Manual)	□	□
1.6	Ensure compliance with IBM Cloud password requirements (Manual)	□	□
1.7	Ensure multi-factor authentication (MFA) is enabled for all users in account (Manual)	□	□
1.8	Ensure multi-factor authentication (MFA) is enabled for the account owner (Manual)	□	□
1.9	Ensure multi-factor authentication (MFA) is enabled at the account level (Manual)	□	□
1.10	Ensure contact email is valid (Manual)	□	□
1.11	Ensure contact phone number is valid (Manual)	□	□
1.12	Ensure IAM users are members of access groups and IAM policies are assigned only to access groups (Manual)	□	□
1.13	Ensure a support access group has been created to manage incidents with IBM Support (Manual)	□	□
1.14	Minimize the number of users with admin privileges in the account (Manual)	□	□
1.15	Minimize the number of Service IDs with admin privileges in the account (Manual)	□	□
1.16	Ensure IAM does not allow public access to Cloud Object Storage (Manual)	□	□
1.17	Ensure Inactive User Accounts are Suspend (Manual)	□	□
1.18	Enable audit logging for IBM Cloud Identity and Access Management (Manual)	□	□
1.19	Ensure Identity Federation is set up with a Corporate IDP (Manual)	□	□
2	**Storage**		
2.1	**Cloud Object Storage**		
2.1.1	**Cloud Object Storage Encryption**		

2.1.1.1	Ensure Cloud Object Storage encryption is done with customer managed keys (Manual)	□	□
2.1.1.2	Ensure Cloud Object Storage Encryption is set to On with BYOK (Manual)	□	□
2.1.1.3	Ensure Cloud Object Storage Encryption is set to On with KYOK (Manual)	□	□
2.1.2	Ensure network access for Cloud Object Storage is restricted to specific IP range (Manual)	□	□
2.1.3	Ensure network access for Cloud Object Storage is set to be exposed only on Private end-points (Manual)	□	□
2.1.4	Ensure Cloud Object Storage bucket access is restricted by using IAM and S3 access control (Manual)	□	□
2.1.5	Disable public (anonymous) access to IBM Cloud Object Storage buckets (Manual)	□	□
2.2	**File Block Storage**		
2.2.1	**Cloud Block Storage Encryption**		
2.2.1.1	Ensure Block Storage is encrypted with customer managed keys (Manual)	□	□
2.2.1.2	Ensure Block Storage is encrypted with BYOK (Manual)	□	□
2.2.1.3	Ensure Block Storage is encrypted with KYOK (Manual)	□	□
2.2.2	Ensure 'OS disk' are encrypted with Customer managed keys (Manual)	□	□
2.2.3	Ensure 'Data disks' are encrypted with customer managed keys (Manual)	□	□
2.2.4	Ensure 'Unattached disks' are encrypted with customer managed keys (Manual)	□	□
3	**Maintenance, Monitoring and Analysis of Audit Logs**		
3.1	Ensure auditing is configured in the IBM Cloud account (Manual)	□	□
3.2	Ensure that archiving is enabled for audit events (Manual)	□	□
3.3	Ensure that events are collected and processed to identify anomalies or abnormal events (Manual)	□	□
3.4	Ensure alerts are defined on custom views to notify of unauthorized requests, critical account actions, and high-impact operations in your account (Manual)	□	□
3.5	Ensure the account owner can login only from a list of authorized countries/IP ranges (Manual)	□	□
3.6	Ensure Activity Tracker data is encrypted at rest (Manual)	□	□
3.7	Ensure Activity Tracker trails are integrated with LogDNA Logs (Manual)	□	□
4	**IBM Cloud Databases Family**		
4.1	Ensure IBM Cloud Databases disk encryption is enabled with customer managed keys (Manual)	□	□

4.2	Ensure IBM Cloud Databases are only accessible via HTTPS or TLS Connections (Manual)	□	□
4.3	Ensure network access to IBM Cloud Databases service is set to be exposed on “Private end points only” (Manual)	□	□
4.4	Ensure IBM Cloud Databases disk encryption is set to On (Manual)	□	□
5	**Cloudant**		
5.1	Ensure Cloudant encryption is set to On (Automated)	□	□
5.2	Ensure IBM Cloudant encryption is enabled with customer managed keys (Manual)	□	□
5.3	Ensure IBM Cloudant is only accessible via HTTPS or TLS Connections (Automated)	□	□
6	**Networking**		
6.1	**IBM Cloud Internet Services**		
6.1.1	Enable TLS 1.2 at minimum for all inbound traffic on IBM Cloud Internet Services Proxy (Manual)	□	□
6.1.2	Ensure Web application firewall is set to ON in IBM Cloud Internet Services (CIS) (Manual)	□	□
6.1.3	Ensure DDoS protection is Active on IBM Cloud Internet Services (Manual)	□	□
6.2	**IBM Virtual Private Cloud (VPC)**		
6.2.1	Ensure no VPC access control lists allow ingress from 0.0.0.0/0 to port 22 (Manual)	□	□
6.2.2	Ensure the default security group of every VPC restricts all traffic (Manual)	□	□
6.2.3	Ensure no VPC security groups allow ingress from 0.0.0.0/0 to port 3389 (Manual)	□	□
6.2.4	Ensure no VPC security groups allow ingress from 0.0.0.0/0 to port 22 (Manual)	□	□
6.2.5	Ensure no VPC access control lists allow ingress from 0.0.0.0/0 to port 3389 (Manual)	□	□
7	**Containers**		
7.1	**IBM Kubernetes Service**		
7.1.1	**Use a Key Management Service (KMS) provider to encrypt data in Kubernetes secrets**		
7.1.1.1	Ensure Kubernetes secrets data is encrypted with bring your own key (BYOK) (Manual)	□	□
7.1.1.2	Ensure Kubernetes secrets data is encrypted with keep your own key (KYOK) (Manual)	□	□
7.1.2	Ensure TLS 1.2 for all inbound traffic at IBM Cloud Kubernetes Service Ingress (Automated)	□	□
7.1.3	Ensure IBM Cloud Kubernetes Service worker nodes are updated to the latest image to ensure patching of vulnerabilities (Automated)	□	□

7.1.4	Ensure that clusters are accessible only by using private endpoints (Automated)	□	□
7.1.5	Ensure IBM Cloud Kubernetes Service cluster has image pull secrets enabled (Automated)	□	□
7.1.6	Ensure IBM Cloud Kubernetes Service clusters have the monitoring service enabled (Automated)	□	□
7.1.7	Ensure IBM Cloud Kubernetes Service clusters have the logging service enabled (Automated)	□	□
7.2	**Container Registry**		
7.2.1	Block deployments of vulnerable images to Kubernetes clusters (Automated)	□	□
8	**Key Management**		
8.1	**IBM Key Protect for IBM Cloud**		
8.1.1	Ensure IBM Key Protect has automated rotation for customer managed keys enabled (Automated)	□	□
8.1.2	Ensure the IBM Key Protect service has high availability (Manual)	□	□
9	**Security and Compliance**		
9.1	Ensure alerts are enabled for vulnerabilities discovered in container images in Container Registry (Automated)	□	□
10	**IBM Cloud Certificate Manager**		
10.1	Ensure certificates generated through IBM Cloud Certificate Manager are automatically renewed before expiration (Automated)	□	□

Appendix: Change History

Date	Version	Changes for this version
Nov 12, 2020	1.0.0	Document Created