



**Ganpat
University**

॥ विद्यया समाजोत्कर्षः ॥

**Institute of
Computer
Technology**

Name: Tushar Panchal

En.No: 21162101014

Sub: CS (Cloud Security)

Branch: CBA

Batch:71

PRACTICAL 01

❖ Scenario :

Your organization, XYZ Corp, is migrating its e-commerce platform to the IBM Cloud. As a part of this migration, the company needs to ensure that the new cloud environment complies with industry regulations such as PCI-DSS for handling payment information and GDPR for protecting customer data. The goal is to implement IBM Cloud Security and Compliance Center to continuously monitor and maintain the security and compliance posture of the e-commerce platform.

Go through the requirement and perform the following tasks:

1: Provision the Security and Compliance Center:

Log in to XYZ Corp's IBM Cloud account. Navigate to the Security and Compliance Center and provision the service.

2: Configure the Service:

Connect the e-commerce platform's cloud resources to the Security and Compliance Center. Enable data collection for security and compliance metrics.

3: Define and Apply Policies:

Identify PCI-DSS and GDPR compliance requirements. Create and apply security and compliance policies within the Security and Compliance Center.

4: Run Initial Security Scans:

Initiate security scans on the e-commerce platform. Analyze results to identify and prioritize issues.

5: Remediate Identified Issues:


Develop and implement remediation plans. Validate changes to ensure issues are resolved effectively.

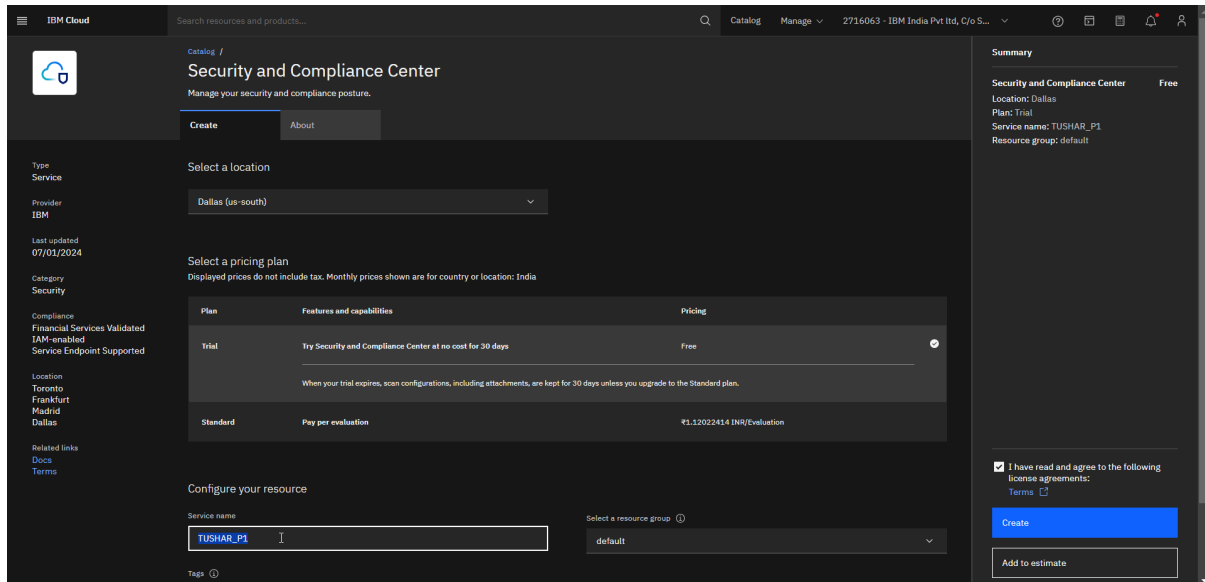
6: Enable Continuous Monitoring, Review and Improve:

Set up continuous monitoring and configure alerts. Generate and review compliance reports regularly. Conduct regular reviews and update policies and procedures.

TASK: Identify AI Security Guardrails 2.0 (1.0.0) compliance requirements. Create an Attachment using the predefined AI Security Guardrails profile and initiate security scans. Analyze results to identify issues and Validate any 3 changes to ensure issues are resolved effectively.

Example: Toolchain issues, key protect issues, IBM cloud object storage issues, and Watson Machine learning issues can be rectified.

 **Step 1:** Create Security and Compliance Centre service and enter region and name.



IBM Cloud

Search resources and products...

Catalog / Manage 2716063 - IBM India Pvt Ltd, C/o S...

Security and Compliance Center

Manage your security and compliance posture.

Create About

Type: Service

Provider: IBM

Last updated: 07/01/2024

Category: Security

Compliance: Financial Services Validated, IAM-enabled, Service Endpoint Supported

Location: Toronto, Frankfurt, Madrid, Dallas

Related links: Docs, Terms

Select a location

Dallas (us-south)

Select a pricing plan

Displayed prices do not include tax. Monthly prices shown are for country or location: India

Plan	Features and capabilities	Pricing
Trial	Try Security and Compliance Center at no cost for 30 days	Free
When your trial expires, scan configurations, including attachments, are kept for 30 days unless you upgrade to the Standard plan.		
Standard	Pay per evaluation	¥1.12022414 INR/Evaluation

Configure your resource

Service name: TUSHAR_P1

Select a resource group: default

Tags

Summary

Security and Compliance Center Free

Location: Dallas

Plan: Trial

Service name: TUSHAR_P1

Resource group: default

☒ I have read and agree to the following license agreements. [Terms](#)

Create

Add to estimate

» **Step 2:** In Control Libraries, go to CIS IBM benchmark library.

Control libraries

View the controls that are available by default in IBM Cloud or create a library to add the controls that your organization has already identified as required.

Plan
Your Trial plan expires in 29 days. To ensure that your scans are not interrupted, upgrade to the Standard plan. [Upgrade](#)

Type: All [Create](#) [+](#)

Name	Type	Controls	Last modified
CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)	Predefined	67	06/25/2024, 7:52 AM

» **Step 3:** Here, all controls and benchmarks are visible as per categories, components, specs and controls.

CIS IBM Cloud Foundations Benchmark v1.1.0

Details

Choose a version to review: **1.1.0**

Description: CIS IBM Cloud Foundations Benchmark version 1.1.0

ID: 51ca566e-c559-412b-8d64-f05b57044c32

Updated on: 06/25/2024, 7:52 AM

Created by: IBM Cloud

Type: Predefined

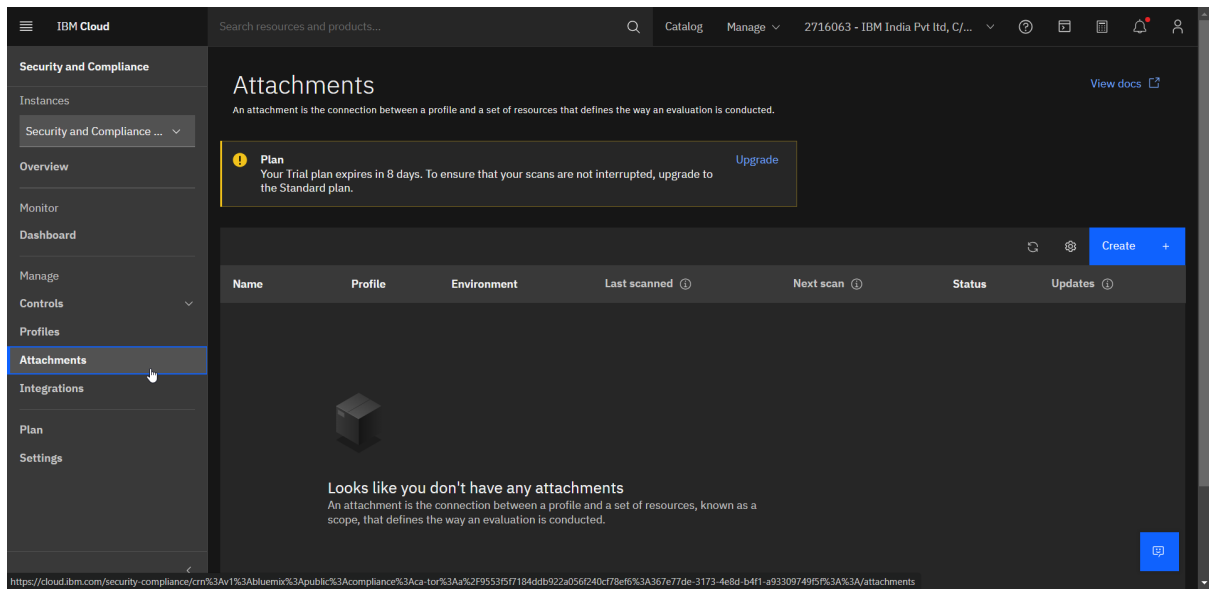
Controls: 67

Grouped by control | Grouped by specification | Grouped by component | Grouped by category

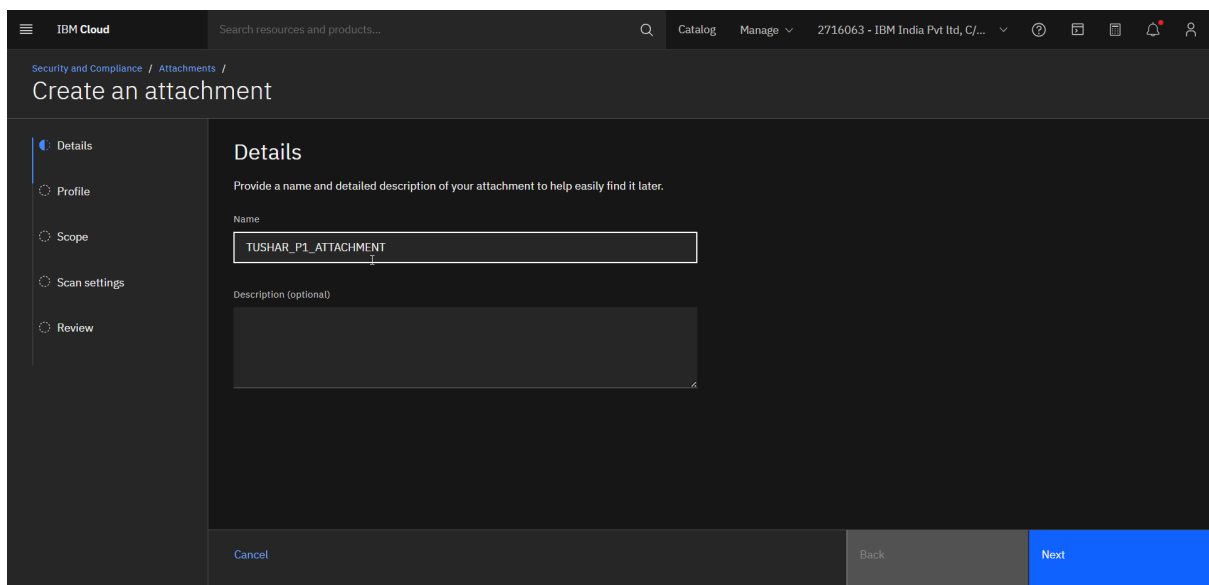
Category: All | Assessments: Has Assess... | Search

Name	Description	Category	Specifications
1.4	Restrict user API key creation and service ID creation in the account via IAM roles	Identity and Access Management	2
1.5	Ensure no owner account API key exists	Identity and Access Management	1

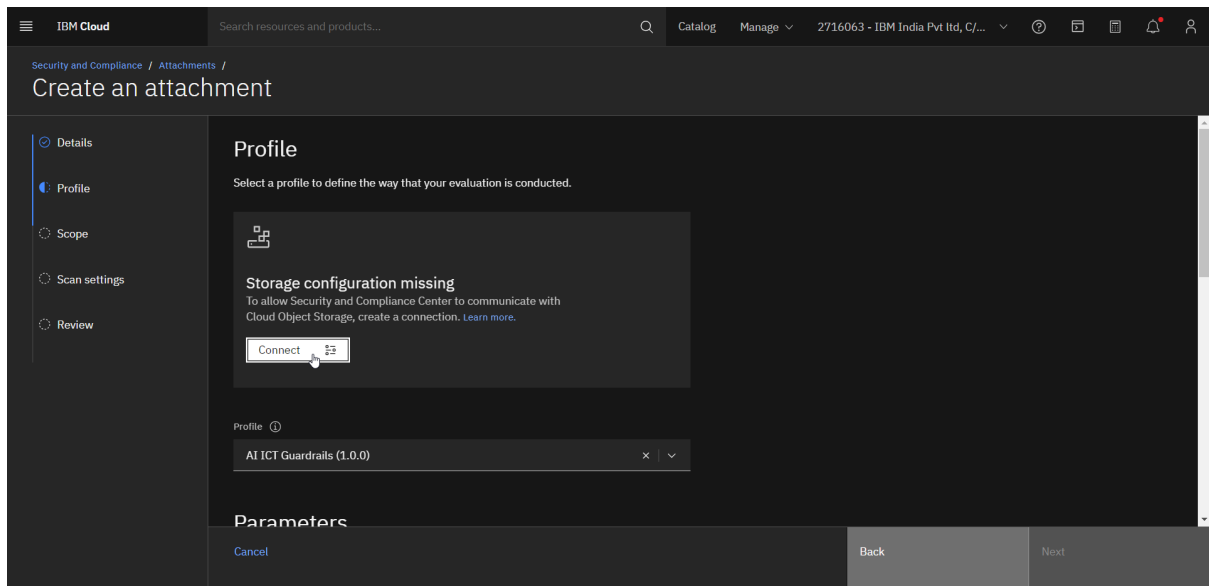
» **Step 4 :** Now in service home, visit attachments and add one.



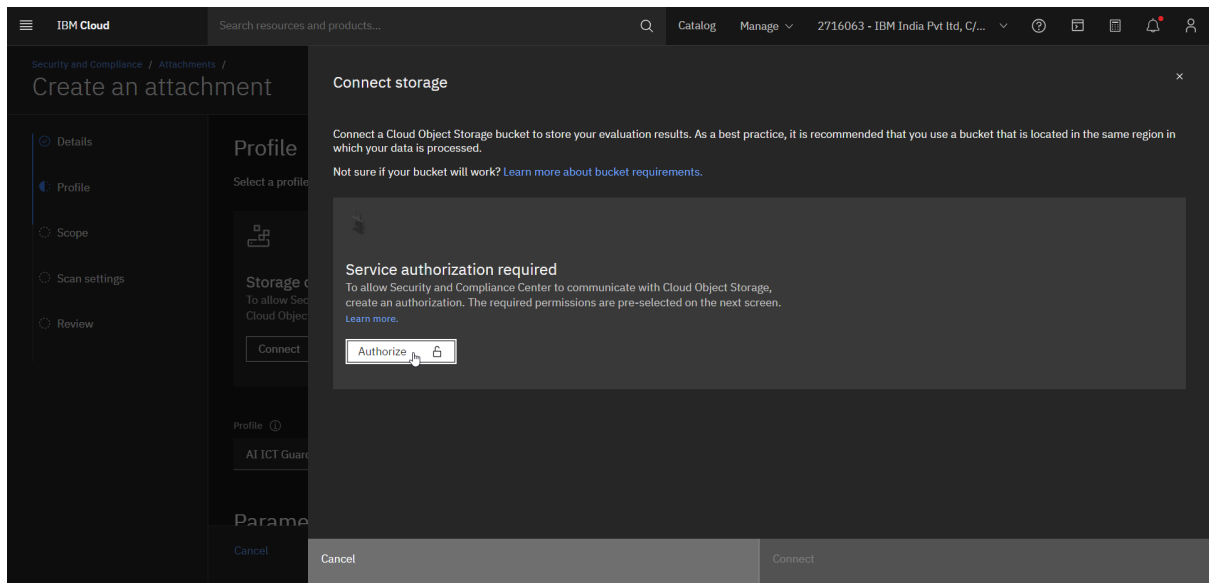
» **Step 5 :** Enter name and proceed further.



» **Step 6 :** Now, the storage is needed to proceed, Cloud Object Bucket can be used also here.



» **Step 7 :** Authorize the service instance.



Step 8: Select the object storage instance.

IBM Cloud

Search resources and products...

Catalog Manage 2716063 - IBM India Pvt Ltd, C/...

Security and Compliance / Attachments / Create an attachment

Details Profile Scope Scan settings Review

Profile

Select a profile

Storage

To allow Security and Compliance to access Cloud Object Storage

Connect

Authorize service to service access for Security and Compliance

Select a target service

Select a target service for Security and Compliance to access as the source service. Only one service can be added at a time.

Target service

Cloud Object Storage

region

Region

All regions

serviceInstance

string equals

serviceInstance

Cloud Object Storage-2v (f56f5908-9e6e...)

All instances

Cloud Object Storage-2v (f56f5908-9e6e...)

Cloud Object Storage-987 (83711d37-42...)

Cloud Object Storage-Aryan_security (b7...)

resource

string equals

resourceType

string equals

Cancel Review

Step 9: Allow write access to the security service instance.

IBM Cloud

Search resources and products...

Catalog Manage 2716063 - IBM India Pvt Ltd, C/...

Security and Compliance / Attachments / Create an attachment

Details Profile Scope Scan settings Review

Profile

Select a profile

Storage

To allow Security and Compliance to access Cloud Object Storage

Connect

Authorize service to service access for Security and Compliance

Select a target service

Cloud Object Storage

region

Region

All regions

serviceInstance

string equals

serviceInstance

Cloud Object Storage-2v (f56f5908-9e6e...)

All instances

Cloud Object Storage-2v (f56f5908-9e6e...)

Cloud Object Storage-987 (83711d37-42...)

Cloud Object Storage-Aryan_security (b7...)

resource

string equals

resourceType

string equals

Prefix

string equals

Delimiter

string equals

Path

string equals

Access

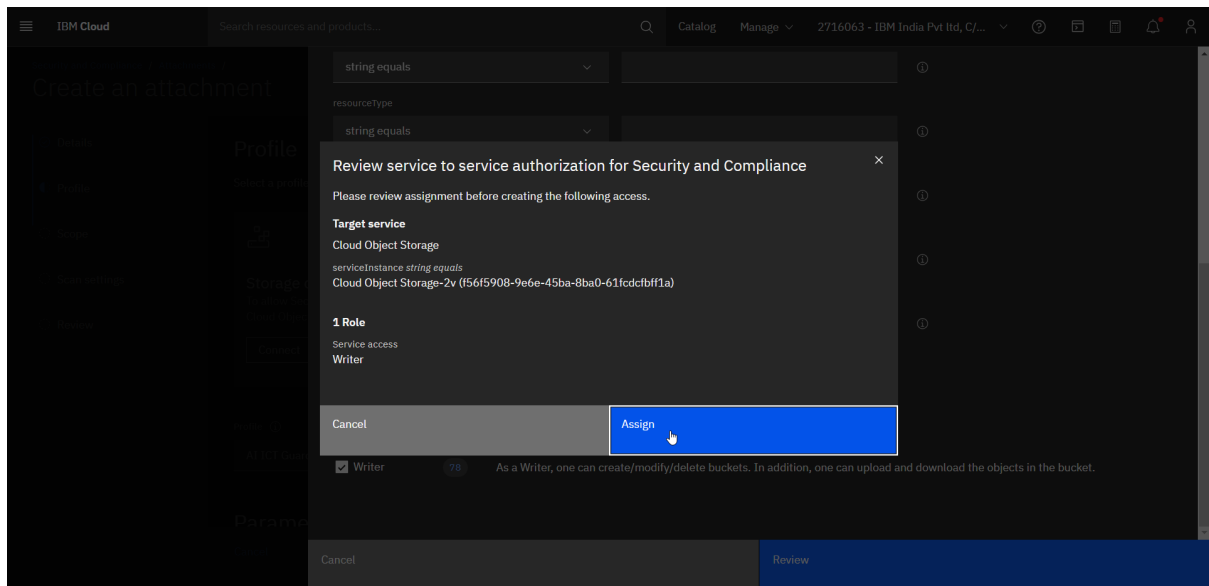
Select a role to determine the level of access for the source service.

Service access

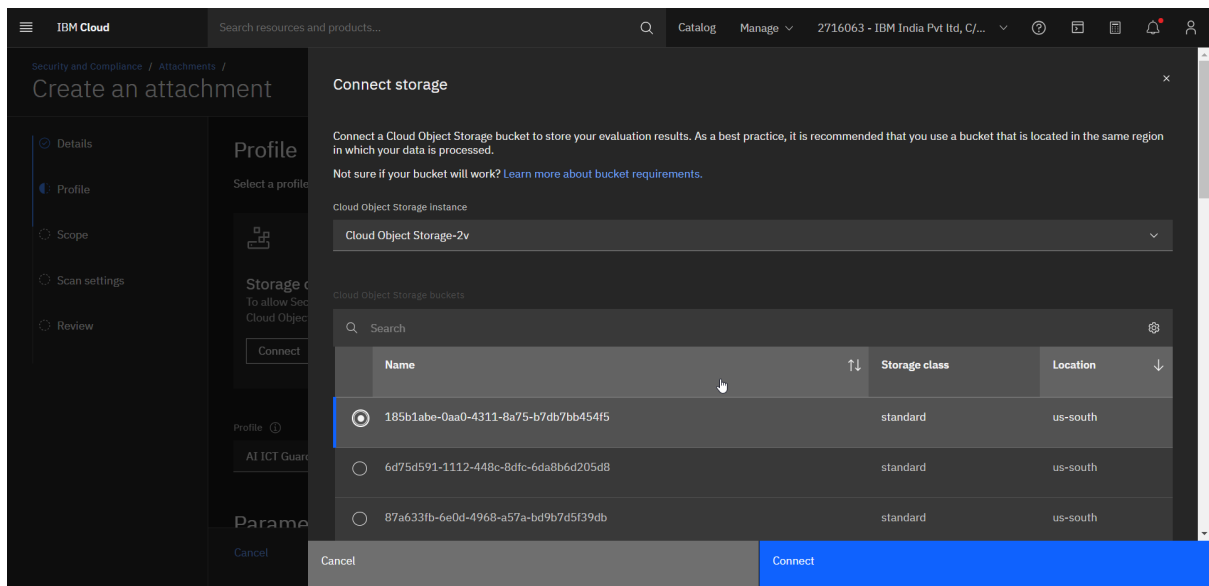
Writer

As a Writer, one can create/modify/delete buckets. In addition, one can upload and download the objects in the bucket.

Cancel Review



➤ **Step 10 :** After assigning the role, now select the bucket to be used here.



Step 11: Select the scope of this service instance.

IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C/...

Security and Compliance / Attachments / Create an attachment

Details Profile Scope Scan settings Review

Scope

Target a scope to define the way that your evaluation is conducted.

Scope ①
Ganpat-2021-Sem6-rg x | v

Exclude resource groups (optional)
Select exclusions

Target account scope (optional)
Select a target account scope(s)

Cancel Back Next

Step 12: Scan settings should be everyday as recommended here to avoid intrusion and threats or any failure due to weak security.

IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C/...

Security and Compliance / Attachments / Create an attachment

Details Profile Scope Scan settings Review

Scan settings

Define the details of the evaluation for this scope and profile selection.

Schedule
Select the frequency at which you want to evaluate your selected resources.

Frequency

☒ Every day (recommended)
☐ Every 7 days
☐ Every 30 days
☐ None

Failure notifications
Optionally, you can choose to be notified if evaluations fail during a scan. The alerts can be sent by threshold or individual control.

☒ Notify me

Cancel Back Next

Step 13 : Review settings and create attachment.

Security and Compliance / Attachments / Create an attachment

Review

Before you begin evaluating your resources, review your settings and ensure that all of your configurations are correct for your targeted scope.

Details

Name	Description (optional)
TUSHAR_P1_ATTACHMENT_NEW	-

Profile

Profile	Version
AI ICT Guardrails	1.0.0

Parameters

Component: All

Cancel Back Create

Step 14 : After scan is completed the next scan will be after 24 hours.

Security and Compliance

Attachments

An attachment is the connection between a profile and a set of resources that defines the way an evaluation is conducted.

Plan
Your Trial plan expires in 8 days. To ensure that your scans are not interrupted, upgrade to the Standard plan.

Upgrade

Name	Profile	Environment	Last scanned	Next scan	Status	Updates
TK_P1_ATTCH	CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)	IBM Cloud	08/19/2024, 12:09 PM	08/20/2024	Latest version	-

Create

➤ **Step 15:** Click on the attachment and click the profile details.

Attachment details

Name: TK_P1_ATTCH
Description (optional): -

ID: 1960e6ee-7a8f-434b-801d-e34677031d17

Profile name: [CIS IBM Cloud Foundations Benchmark v1.1.0 \(1.1.0\)](#)

Environment: IBM Cloud

Scope: Ganpat-2021-Sem6-rg
Type: Resource group

Exclusions: None

Buttons: Scope, Scan settings, Parameters

Background Table:

Name	Profile	Environment	Last updated
TK_P1_ATTCH	CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0)	IBM Cloud	08/04/2024

URL: <https://cloud.ibm.com/security-compliance/cm%3Av1%3Abluema%3Apublic%3Acompliance%3Aca-tor%3Aa%2F95535f7184ddb922a056f240cf78e6%3A367e77de-3173-4e8d-b4f1-a93309749f5f%3A%3A/profiles/48279384-3d29-4089-8259-8ed354774b4a>

➤ **Step 16:** All controls are visible here.

CIS IBM Cloud Foundations Benchmark v1.1.0

View docs | Actions

Plan
Your Trial plan expires in 8 days. To ensure that your scans are not interrupted, upgrade to the Standard plan. [Upgrade](#)

Overview | Attachments (1)

Version details

Choose a version to review: 1.1.0

Controls: 67
Published: 06/24/2024, 8:31 AM
Status: Latest version

Environment: IBM Cloud
Type: Predefined
ID: 48279384-3d29-4089-8259-8ed354774b4a

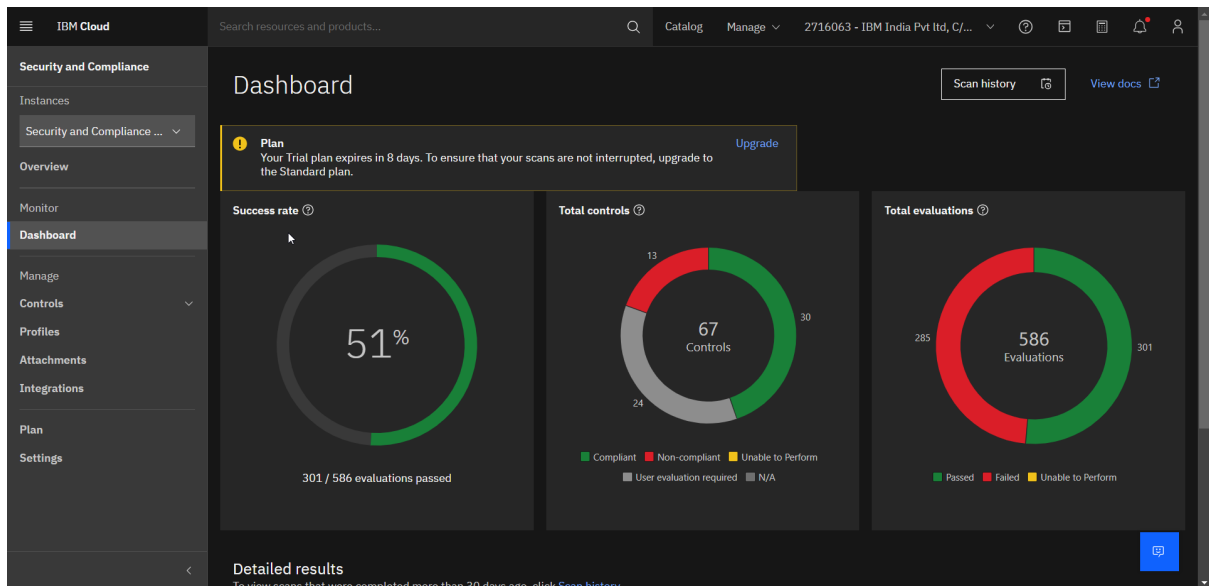
Description
CIS IBM Cloud Foundations Benchmark version 1.1.0

Grouped by control | Grouped by specification | Grouped by component | Grouped by category

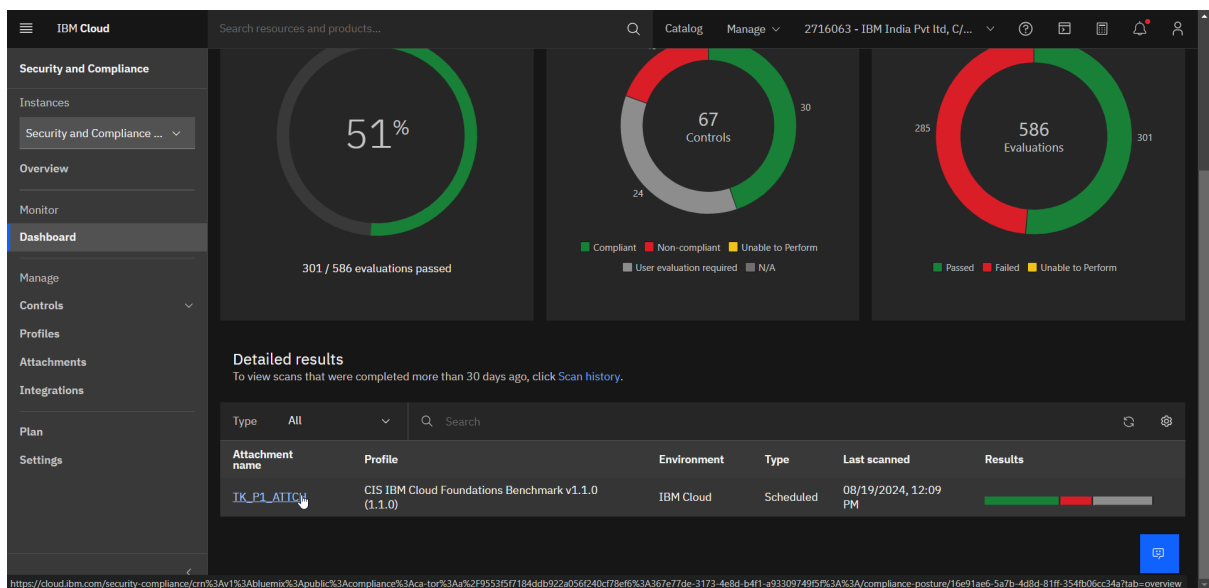
Category: All | Assessments: Has Assess... | Search

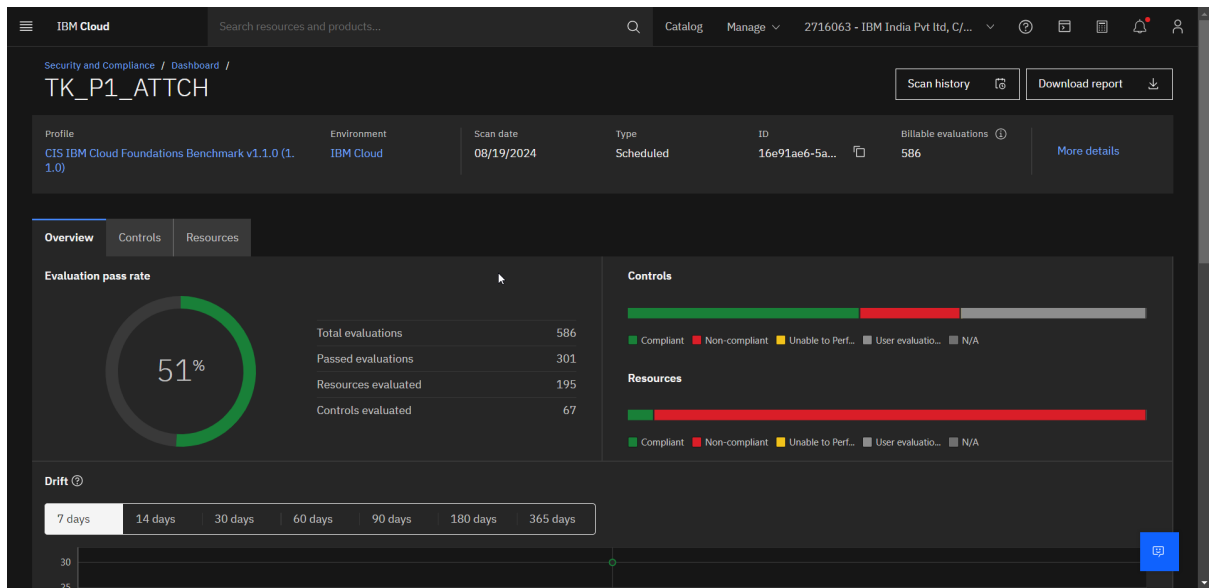
Name	Description	Category	Specifications
------	-------------	----------	----------------

» **Step 17 :** In dashboard on service home, the results are mentioned.



» **Step 18 :** Click on the attachment to check its detailed results.





➤ **Step 19:** In controls, it shows the security problems like here in case of object storage public access and managed keys.

TK_P1_ATTCH

Profile: CIS IBM Cloud Foundations Benchmark v1.1.0 (1.1.0) | Environment: IBM Cloud | Scan date: 08/19/2024 | Type: Scheduled | ID: 16e91ae6-5a... | Billable evaluations: 586

Overview | **Controls** | Resources

Name	Description	Category	Specifications	Evaluation
1.1	Monitor account owner for frequent, unexpected, or unauthorized logins	Identity and Access Management	0	Non-compliant
1.10	Ensure contact email is valid	Identity and Access Management	1	Compliant
1.11	Ensure contact phone number is valid	Identity and Access Management	1	Non-compliant
1.12	Ensure IAM users are members of access groups and IAM policies are assigned only to access groups	Identity and Access Management	1	Compliant
1.13	Ensure a support access group has been created to manage incidents with IBM Support	Identity and Access Management	1	Compliant
1.14	Minimize the number of users with admin privileges in the account	Identity and Access Management	0	Non-compliant

» **Step 20 :** In dashboard of security service, click on the details of control and check the recommended remediation to solve the issue.

The screenshot shows the IBM Cloud Security Service dashboard. On the left, a sidebar lists resources under 'Highest priority resources'. The main panel displays the details of a control named 'testsecurity'. The control is of Type 'Automated', Method 'IBM Cloud rule', and Component 'Cloud Object Storage'. Its status is 'Failed'. The description states: 'Check whether Cloud Object Storage is accessible only by using private endpoints'. Below this, a table shows noncompliant properties:

Property	Description	Operator	Expected value	Actual value
firewall.allowed_network_type	List of network endpoint types (public, private, or direct) that are allowed.	is_not_empty	[""]	

Below the table, the 'Recommended Remediation' section provides instructions:

The rule might fail if the Cloud Object Storage bucket is not configured to be accessible only by using a private endpoint.

1. Use the API to set the Cloud Object Storage network type to Private.
2. It's not possible to use the console to update the Cloud Object Storage bucket to be accessible only by using a private endpoint.
3. For more information see, [Make changes to a bucket's configuration](#).

» **Step 21 :** Also the scan can be run at custom time by option visible in attachments tab on service home.

The screenshot shows the IBM Cloud Security Service dashboard for the 'CIS IBM Cloud Foundations Benchmark v1.1.0'. The 'Attachments (1)' tab is selected. A table lists the attachment:

Name	Environment	Version	Last scanned	Next scan	Status	Updates
TK_P1_ATTACH	IBM Cloud	1.1.0	08/19/2024, 12:09 PM	08/20/2024	Latest version	-

A context menu is open for the attachment, showing options: Edit, Run scan, View scan results, Pause scan, and Delete. The 'Run scan' option is highlighted.

TASK: Identify AI Security Guardrails 2.0 (1.0.0) compliance requirements. Create an Attachment using the predefined AI Security Guardrails profile and initiate security scans. Analyze results to identify issues and Validate any 3 changes to ensure issues are resolved effectively.

Example: Toolchain issues, key protect issues, IBM cloud object storage issues, and Watson Machine learning issues can be rectified.

➤ **Step 22 :** Visit AI Security Guardrails profile.

The screenshot shows the IBM Cloud Security and Compliance console. The left sidebar contains navigation options: Overview, Monitor, Dashboard, Manage, Controls, Profiles (selected), Attachments, Integrations, Plan, and Settings. The main content area is titled 'Profiles' and includes a warning banner about the trial plan expiring in 8 days. Below the banner is a table of profiles:

Name	Type	Last updated	Attachments
AI ICT Guardrails (1.0.0)	Predefined	07/29/2024, 8:55 AM	0
AI Security Guardrails 2.0 (1.0.0)	Predefined	07/08/2024, 8:58 AM	0

A 'Create' button is visible in the top right corner of the table.

➤ **Step 23 :** Create new attachment.

The screenshot shows the IBM Cloud Security and Compliance console with the 'Attachments (0)' tab selected. The main content area is titled 'AI Security Guardrails 2.0' and includes a warning banner about the trial plan expiring in 8 days. Below the banner, there is a section titled 'Create an attachment to start scanning' with instructions to attach the profile to a scope to begin scanning. A 'Create' button is visible in the top right corner of the section.

Below the instructions, there is a table with columns: Name, Environment, Version, Last scanned, Next scan, Status, and Updates. The table is currently empty.

IBM Cloud Search resources and products...

Security and Compliance / Profiles / AI Security Guardrails 2.0 /

Create an attachment

Details

Provide a name and detailed description of your attachment to help easily find it later.

Name

TK_PRACTICAL1_TASK

Description (optional)

Cancel Back Next

» **Step 24 :** Select all parameters and set scan scope and frequency.

IBM Cloud Search resources and products...

Security and Compliance / Profiles / AI Security Guardrails 2.0 /

Create an attachment

Profile

Profile ⓘ
AI Security Guardrails 2.0 (1.0.0)

Parameters

Component: All Search

Description	Parameters	Component
✓ Check whether Container Registry Vulnerability Advisor scans for critical or high vulnerabilities in the system at least every # day(s)	1	Container Registry
✓ Check whether Virtual Servers for VPC instance has the minimum # interfaces	1	Virtual Server for VPC
✓ Check whether Virtual Servers for VPC instance has all interfaces with IP-spoofing disabled	1	Virtual Server for VPC
✓ Check whether Security Groups for VPC contains no outbound rules in security groups that specify destination IP 8.8.8.8/32 to DNS port	1	Security Group for VPC

Cancel Back Next

IBM Cloud

Search resources and products...

Catalog

Manage

2716063 - IBM India Pvt Ltd, C/...

Security and Compliance / Profiles / AI Security Guardrails 2.0 /

Create an attachment

Details

Profile

Scope

Scan settings

Review

Scope

Target a scope to define the way that your evaluation is conducted.

Scope ^①

Ganpat-2021-Sem6-rg x | v

Exclude resource groups (optional)

Select exclusions v

Target account scope (optional)

Select a target account scope(s) v

Cancel

Back

Next

IBM Cloud

Search resources and products...

Catalog

Manage

2716063 - IBM India Pvt Ltd, C/...

Security and Compliance / Profiles / AI Security Guardrails 2.0 /

Create an attachment

Details

Profile

Scope

Scan settings

Review

Scan settings

Define the details of the evaluation for this scope and profile selection.

Schedule

Select the frequency at which you want to evaluate your selected resources.

Frequency

☒ Every day (recommended)

☐ Every 7 days

☐ Every 30 days

☐ None

Failure notifications

Optionally, you can choose to be notified if evaluations fail during a scan. The alerts can be sent by threshold or individual control.

☐ Notify me

Cancel

Back

Next

IBM Cloud

Search resources and products...

Catalog

Manage

2716063 - IBM India Pvt Ltd, C/...

Security and Compliance / Profiles / AI Security Guardrails 2.0 /

Create an attachment

Details

Profile

Scope

Scan settings

Review

Review

Before you begin evaluating your resources, review your settings and ensure that all of your configurations are correct for your targeted scope.

Details

Name

TK_PRACTICAL1_TASK

Description (optional)

-

Profile

Profile

AI Security Guardrails 2.0

Version

1.0.0

Parameters

Component:

All v

Q Search

Cancel

Back

Create

» **Step 25 :** It will take time and let the scan finish.

The screenshot shows the IBM Cloud AI Security Guardrails 2.0 interface. The top navigation bar includes 'IBM Cloud', a search bar, and user information. The main header displays 'Security and Compliance / Profiles / AI Security Guardrails 2.0'. A notification banner indicates a trial plan expiration. The 'Attachments (1)' tab is active, showing a table of scan results.

Name	Environment	Version	Last scanned	Next scan	Status	Updates
TK_PRACTICAL1_TASK	IBM Cloud	1.0.0	08/19/2024, 12:25 PM	Scan in progress	Latest version	-

» **Step 26 :** After scan completion, check services and security compliances, like here cloud storage bucket should contain firewall for additional security as mentioned in results.

The screenshot shows the IBM Cloud Details page for a Cloud Object Storage bucket. The 'Details' section includes a description, type, component, method, resource, and status. The 'Noncompliant properties' tab is active, displaying a table of noncompliant properties.

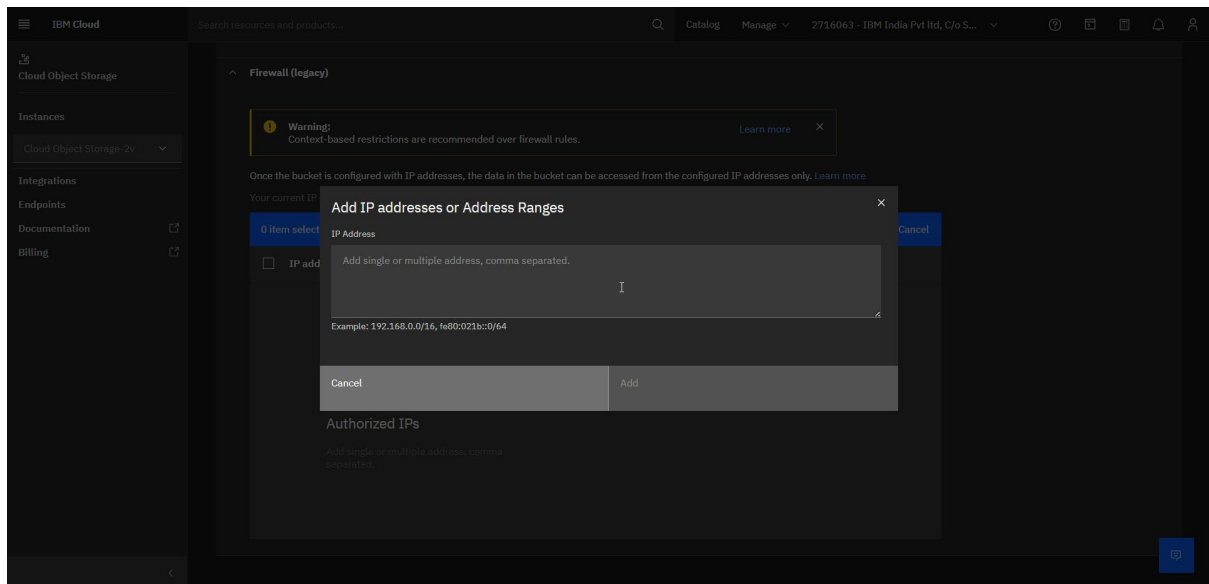
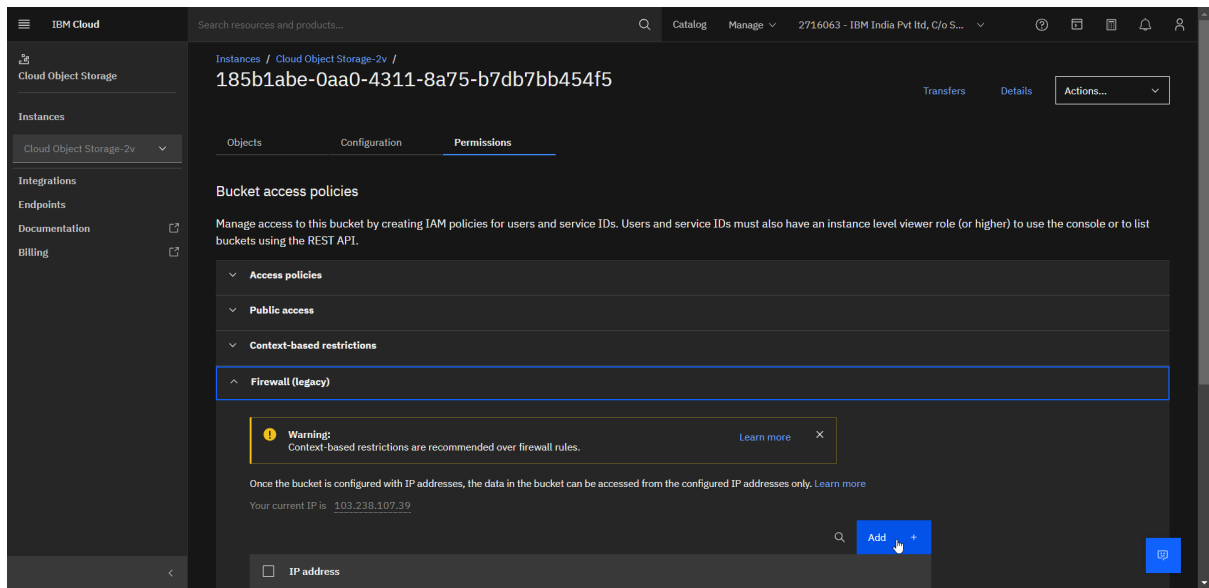
Property	Description	Operator	Expected value	Actual value
firewall.allowed_ip	List of allowed originating (source) IP addresses/ranges. The list can contain up to 1000 IPv4 or IPv6 addresses/ranges in CIDR notation.	is_not_empty		[""]

Recommended Remediation:

This rule might fail if the Cloud Object Storage bucket network access is not configured with a specific firewall IP range.

1. Select Storage to view your resource list.
2. Next, select the service instance with your bucket. The Cloud Object Storage console opens.
3. Select the bucket that you want to limit access to authorized IP addresses.
4. Click the Permissions tab.
5. Select Firewall (Network) from the list of options.

» **Step 27 :** Now, it can be solved as mentioned, adding legacy firewall to bucket allowing specific IP addresses or the ranges respectively.



➡ Further solutions can be made as per provided steps and sufficient access to resource groups and respective resources