



IBM Cloud for Financial Services – Tech Zone Demo Environment
Ecosystem Engineering

Scanning for Compliance

This document will walk you through the demonstration of the Security and Compliance Center (SCC) showing you the controls that are being validated to the FS Cloud Reference architecture. The intent of this demo is to highlight the Security and Compliance Center, show relevant features, and help attendees understand how they can effectively use the SCC.

Goals for the Demo

- Familiarize the audience with the Security & Compliance Center
- View scan results by pass/fail
- View scan results per resource instance
- View failing compliance controls and reason for failure

Prerequisites

- If you have not already done so, request access to the FS Cloud demo environment at: <https://techzone.ibm.com/collection/ibm-cloud-for-financial-services>



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

Steps

Dashboard

1. Log in to the IBM Cloud account – <https://cloud.ibm.com>
2. This is an account where the IBM Cloud for Financial Services Reference Architecture has been deployed and the Security and Compliance Center has been set up to monitor and manage the security posture of the deployment.
3. Click on the “Hamburger” menu in the top left and select “Security and Compliance Center” from the menu.
- 4.

The screenshot shows the IBM Cloud dashboard interface. On the left, there's a sidebar with various service categories like Classic Infrastructure, Cloud Foundry, Functions, Kubernetes, OpenShift, Satellite, Security and Compliance, VMware, VPC Infrastructure, API Management, App Development, Container Registry, DevOps, Interconnectivity, Observability, and Schematics. The 'Security and Compliance' section is currently selected and expanded, showing sub-options: Getting started, Overview, Dashboard, Manage posture, Assess, Configure, Govern resources, Results, Configure, Gain insight, Insights, Findings, Configure, and Integrations. To the right of the sidebar, there are several cards: 'Architecture center' (Learn best practices and leverage reference architectures for the cloud), 'IBM Push Notifications' (Send real-time and personalized notifications to mobile and web applications via a unified push service), 'Incorporate DevOps into your process' (Shorten releases, improve reliability, and stay ahead of the competition with IBM DevOps), and a 'Learn' card (Learn and hc your u). Below these cards, there are sections for 'View all' (Results, Insights, Findings, Integrations) and 'Planned maintenance' (with a count of 12 items, 27 pending, 2 critical, 17 major, 1 minor, and 1 info). At the bottom left of the main content area, the URL <https://cloud.ibm.com/security-compliance/overview> is visible.

5. The Security and Compliance Center is an account-level service that can be used to continuously scan the environment to determine the current security posture of the deployed services, set up rules to govern how new services are provisioned, and monitor for threats and vulnerabilities in the



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

environment.

6. Navigate to the [SCC Dashboard](#) by clicking on the “Dashboard” link in the left-side menu.

7. The dashboard gives an overview of all the current security posture and results of the threat detection. Let's start by looking at how to manage the Security Posture.

Manage posture - Configure

1. Click on “Configure” → “Collectors” under the “Manage Posture” section on the left menu.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

The screenshot shows the IBM Cloud interface with the left sidebar open. Under the "Manage posture" section, the "Configure" menu is expanded, and "Collectors" is selected. The main content area is titled "Collectors". It displays a table with one row of data:

Name	Description	Last contact	Managed by	Endpoint type	Status
managed	-	2021-10-12 11:13:06 PM	IBM	Private	Inactive

Below the table, it says "Items per page: 25" and "1–1 of 1 item".

2. Before a scan can be run, a collector must be deployed. In this case, we have a provisioned an IBM-managed collector into the account and provided it with an API key that has the required permission to scan the resources within the account.
3. Click on “Configure” → “Scopes” under the “Manage Posture” section on the left menu.

The screenshot shows the IBM Cloud interface with the left sidebar open. Under the "Manage posture" section, the "Configure" menu is expanded, and "Scopes" is selected. The main content area is titled "Scopes". It displays a table with one row of data:

Name	Description	Last scan	Scan status
frontoffice		2021-10-12 12:58:28 PM	Validation completed

Below the table, there is a detailed view for the "frontoffice" scope:

Details	Last scan
Collectors	Type Validation
Time	2021-10-12 12:58:28 PM
Status	Validation completed

At the bottom, it says "Items per page: 25" and "1–1 of 1 item".

4. The next step is to define a scope. When the scope is created it is given a name and assigned a collector. The scope will then use the collector to discover the services available within the account.
5. Click on the name of the “frontoffice” scope to see the details.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

The screenshot shows the IBM Cloud Security and Compliance interface. At the top, there's a navigation bar with 'IBM Cloud', a search bar, and links for Catalog, Docs, Support, Manage, and a user profile. Below the navigation, the URL 'Security and Compliance / Scopes / frontoffice' is visible. On the left, a sidebar has 'Settings' selected and shows 'Event history'. The main content area displays a table for the 'frontoffice-scc' scope, which is 'Scope access' and 'managed' by 'IBM'. A status indicator shows '1-1 of 1 item' and 'Inactive'. To the right of the table is an 'Actions...' dropdown and a 'Details' button. Below this, a 'Resource type' section lists various resources under 'Inventory':

Resource type	Detail
Account	IBMid-550008K4QH
Identity and Access Management	IBMid-110000SNV8
Resource Groups	
Resource Group	frontoffice-edge
Resource Group	Default
Resource Group	frontoffice-management
Resource Group	techzone
Resource Group	frontoffice-workload
Resource Group	security-ops
Resource Group	frontoffice-common
Containers	

6. After the discovery scan runs, the inventory of resources are listed. At this point, if desired the list of resources can be pruned for this particular scope to include only a subset of the resources are included in the scan.
7. Click on “Configure” → “Profiles” under the “Manage Posture” section on the left menu.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

Name	Description	Type	Goals
CIS IBM Foundations Benchmark 1.0.0	CIS IBM Foundations Benchmark 1.0.0	Predefined	78
IBM Cloud Best Practices Controls 1.0	IBM Cloud Best Practices Controls 1.0	Predefined	345
IBM Cloud for Financial Services v0.1	IBM Cloud for Financial Services Best Practices v0.1	Predefined	134
IBM Cloud for Financial Services v0.1.1	IBM Cloud for Financial Services Best Practices v0.1.1	Predefined	124
IBM Cloud for Financial Services v0.1.2	IBM Cloud for Financial Services Best Practices v0.1.2	Predefined	135
Best Practices - AWS S3 Controls	Best Practices - AWS S3 Controls	Predefined	20
Best Practices - Firewalls	Best Practices - Firewalls	Predefined	1
Best Practices - Linux Hardening	Best Practices - Linux Hardening	Predefined	79
Best Practices - MySQL	Best Practices - MySQL	Predefined	7
Best Practices - SQL Server	Best Practices - SQL Server	Predefined	2
CIS - Kubernetes	CIS Kubernetes Benchmark v1.3.0	Predefined	96
CIS AWS 3-tier Web Architecture Benchmark 1.0	CIS AWS 3-tier Web Architecture Benchmark 1.0	Predefined	91

8. The next step is to determine the controls that will be evaluated against the scope to determine the current posture. The controls are grouped into Profiles. A number of profiles have been provided out of the box and custom profiles can be created to define a particular collection of controls.
9. Click on the “IBM Cloud for Financial Services v0.1.2” profile.
10. We will use the FS Cloud profile for this scan. The controls are organized into the NIST control families. (NIST stands for National Institute of Standards and Technology and it defined a standard control language and base set of controls.)
11. Expand the “AC” control family.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

The screenshot shows the IBM Cloud for Financial Services v0.1.2 interface. The left sidebar has a 'Controls' tab selected. The main area displays a table with two columns: 'Name' and 'Description'. The 'Name' column contains expandable sections for 'AC' (Access Control), 'AU' (Audit and Accountability), and 'CA' (Security Assessment and Authorization). The 'Description' column provides a brief overview of each category.

Name	Description
^ AC	Access Control
▼ AC-2: Account Management	
▼ AC-3: Access Enforcement	
▼ AC-4: Information Flow Enforcement	
▼ AC-5: Separation of Duties	
▼ AC-6: Least Privilege	
▼ AC-17: Remote Access	
▼ AU	Audit and Accountability
▼ CA	Security Assessment and Authorization

12. Within the control family a number of controls have been defined. The ‘AC’ control family defines the controls related to Access Control in the environment.
13. Expand the “AC-2” control.

The screenshot shows the same interface as above, but the 'AC-2: Account Management' section is now expanded. This reveals a detailed list of sub-controls under the AC-2 family, including AC-2(1) through AC-2(i).

Name	Description
^ AC	Access Control
^ AC-2: Account Management	
▼ AC-2(1): Account Management Automated System Account Management	
▼ AC-2(3): Account Management Automated System Account Management	
▼ AC-2(7): Account Management Privileged User Accounts	
▼ AC-2(a): Identifies and selects the following types of information system accounts to support organizational missions/business functions	
▼ AC-2(c): Establishes conditions for group and role membership	
▼ AC-2(f): Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined proced	
▼ AC-2(i): Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Assignment: organizat	
▼ AC-3: Access Enforcement	
▼ AC-4: Information Flow Enforcement	



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

14. In this case, the ‘AC-2’ control is broken down into sub-parts.
15. Expand the “AC-2(1)” control.

The screenshot shows the IBM Cloud for Financial Services v0.1.2 interface. The top navigation bar includes links for Catalog, Docs, Support, Manage, and a user profile icon. Below the navigation is a search bar and a breadcrumb trail: Security and Compliance / Profiles / IBM Cloud for Financial Services v0.1.2. On the left, a sidebar titled 'Controls' lists various compliance controls. The main content area displays the details for 'AC-2(1): Account Management | Automated System Account Management'. This section contains a list of 24 numbered goals, each with a brief description:

- 3000015: Check whether IAM users are attached to at least one access group
- 3000016: Check whether IAM policies for users are attached only to groups or roles
- 3000023: Check whether the account owner does not have an IBM Cloud API key created in IAM
- 3000024: Check whether IBM Cloud API keys that are managed in IAM are rotated at least every # days
- 3000025: Check whether an account owner has logged in to IBM Cloud in the past # days
- 3000026: Check whether user list visibility restrictions are configured in IAM settings for the account owner
- 3000030: Check whether IAM policies for service IDs are attached only to groups or roles
- 3000035: Check whether account access is managed only by IAM access groups
- 3000039: Check whether IBM Cloud API keys that are unused for 180 days are detected and optionally disabled
- 3000235: Check whether Hyper Protect Crypto Services encryption keys that are generated by the service are rotated automatically at least every # days
- 3000425: Check whether VPN for VPC authentication is configured with a strong pre-shared key with at least 24 alphanumeric characters
- 3000639: Check whether Container Registry access is managed only by IAM access groups
- 3000707: Check whether App ID user profile updates from client apps is disabled
- 3000708: Check whether App ID Cloud Directory users aren't able to update their own accounts
- 3000709: Check whether App ID Cloud Directory users aren't able to self-sign up to applications
- 3000711: Check whether App ID social identity providers are disabled
- 3000712: Check whether App ID anonymous authentication is disabled
- 3000713: Check whether App ID password strength regex is configured
- 3000714: Check whether App ID advanced password policies are enabled

16. The control contains one or more Goals that map the requirements of the control into specific rules that can be applied to the account and the provisioned services to verify compliance.
17. Click on one of the goals.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

The screenshot shows a detailed view of a security goal in the IBM Cloud Security and Compliance Center. The top navigation bar includes links for Catalog, Docs, Support, Manage, and a user profile. The main content area displays the following sections:

- Details:** A description stating "Check whether IAM users are attached to at least one access group". Below it, under "Environment", is "IBM" and under "Tags" are "IAM" and "IBM".
- Goal attributes:** A table showing a fact master attribute "IAM User Access Groups" with an attribute display name "exclude_owner_ac..." and an attribute key "Details".
- Goal logic:** A code snippet in JavaScript-like syntax used to determine compliance based on IAM user attachments.
- Validation report messages:** A table showing validation results for "Pass" (Fail) and "Not applicable" (Unable to perform). It also lists error codes: CTL.NOT_APPLICABLE.STATUS... and CTL.IBM_IAM_ACCOUNT_N...

18. From this view we can see the details for the goal including the logic used to determine compliance.
19. Return to the main page of the Security and Compliance Center - <https://cloud.ibm.com/security-compliance/overview>. Click on “Configure” → “Scans” under the “Manage Posture” section on the left menu.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

The screenshot shows the IBM Cloud for Financial Services Security and Compliance Center. The left sidebar is titled 'IBM Cloud' and includes sections for 'Security and Compliance' (Dashboard, Manage posture, Assess, Configure, Collectors, Credentials, Scopes, Profiles, Goals, Scans), 'Govern resources' (Results, Configure), and 'Gain insight' (Insights, Findings, Configure). The main content area is titled 'Scans' and shows a table of three scheduled scans. The table columns are Name, Scope, Profile, Type, and Scan frequency. The scans listed are: 'frontoffice - FS Cloud 0-1-2' (Scope: frontoffice, Profile: IBM Cloud for Financial Services v0.1.2, Type: Validation, Frequency: 1 day), 'frontoffice - Discovery' (Scope: frontoffice, Profile: -, Type: Discovery, Frequency: On-demand), and 'frontoffice - IBMCloudforFinancial' (Scope: frontoffice, Profile: IBM Cloud for Financial Services v0.1.2, Type: Validation, Frequency: On-demand). The table footer shows 'Items per page: 25' and '1-3 of 3 items'.

Name	Scope	Profile	Type	Scan frequency
frontoffice - FS Cloud 0-1-2	frontoffice	IBM Cloud for Financial Services v0.1.2	Validation	1 day
frontoffice - Discovery	frontoffice	-	Discovery	On-demand
frontoffice - IBMCloudforFinancial	frontoffice	IBM Cloud for Financial Services v0.1.2	Validation	On-demand

20. The last part of the configuration is to set up a scheduled scan. Here we've set up a scan that will run every day using the 'IBM Cloud for Financial Services v0.1.4' profile. It is also possible to run a scan on-demand against a particular profile.
21. Return to the Security and Compliance Center overview page - <https://cloud.ibm.com/security-compliance/overview>

Manage posture – Assess

1. Click on "Assess" → "Scan results" under the "Manage Posture" section on the left menu.



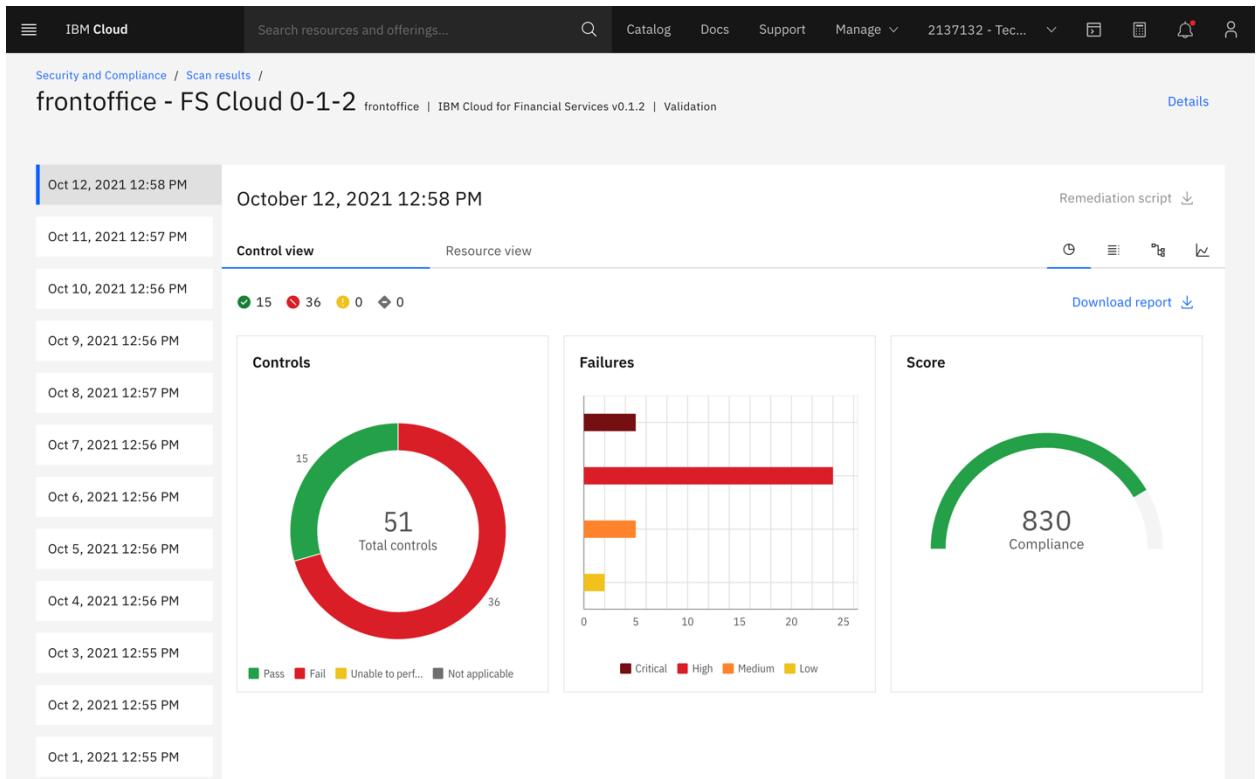
IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

Name	Scope	Profile	Last scan time	Last scan results
frontoffice - FS Cloud 0-1-2	frontoffice	IBM Cloud for Financial Services v0.1.2	2021-10-12 12:58:20 PM	✓15 ⚡36
frontoffice - IBMCloudforFinancial	frontoffice	IBM Cloud for Financial Services v0.1.2	2021-10-12 12:30:30 AM	✓15 ⚡36
Check transit gateway	fss-london-scan	IBM Cloud for Financial Services v0.1	2021-09-23 9:45:49 PM	✓7 ⚡31 ⚠10
IBM Best Practices	fss-london-scan	IBM Cloud Best Practices Controls 1.0	2021-09-23 5:54:31 PM	✓94 ⚡102 ⚠22 ⚫119
London-NIST	fss-london-scan	NIST	2021-09-23 4:21:56 PM	✓9 ⚡35 ⚠28 ⚫22
GDPR-scan	scope-falcon-cloud-native-prod	GDPR	2021-09-23 10:40:47 AM	⚠15 ⚫5
FS-Scan	fss-london-scan	IBM Cloud for Financial Services v0.1	2021-09-23 9:06:07 AM	✓6 ⚡31 ⚠8 ⚫3
FS-NIST-Production	fss-cloud	NIST	2021-09-23 1:04:31 AM	✓6 ⚡23 ⚠35 ⚫30
NIST-Production	scope-falcon-cloud-native-prod	NIST	2021-09-23 12:20:07 AM	✓8 ⚡30 ⚠26 ⚫30

2. The results of the on-demand and scheduled scans against the defined scopes are all listed here. We can look at the results of the scan for our ‘frontoffice’ scope.
3. Click on the “frontoffice - FS Cloud 0-1-2” result.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering



4. The initial view for the scan results shows the graphs for the Control view. Before getting into the specific results, it is important to understand what the values do and do not mean. The controls are measured by goals and if any one of the goals fail then the control fails. Often the same goal will be referenced by multiple controls, meaning that one error can fail multiple controls. Also, a failed control does not necessarily mean the environment has a vulnerability, just a configuration that doesn't match the base rule set.



In this account, to accommodate the demo environment there are a couple of known exceptions to the FS controls. For example: some of the network ACLs are opened to allow VPN traffic and public gateways are attached to the OpenShift cluster subnets to allow access to external repositories.

5. From left to right, this Controls graph shows the number of passing and failing controls. In this case, 15 of the controls passed and 36 have failed. The Failures graph shows the severity of the goals that failed. Finally, the Score graph gives an overall compliance score. Anything over 800 is a good score.
6. Click on the list view button to see the results by control.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

IBM Cloud Search resources and offerings... Catalog Docs Support Manage 2137132 - Tec... Details

Security and Compliance / Scan results / frontoffice - FS Cloud 0-1-2 frontoffice | IBM Cloud for Financial Services v0.1.2 | Validation

Oct 12, 2021 12:58 PM October 12, 2021 12:58 PM

Control view Resource view

15 36 0 0

Remediation script ↴ Download report ↴

October 12, 2021 12:58 PM

Oct 11, 2021 12:57 PM

Oct 10, 2021 12:56 PM

Oct 9, 2021 12:56 PM

Oct 8, 2021 12:57 PM

Oct 7, 2021 12:56 PM

Oct 6, 2021 12:56 PM

Oct 5, 2021 12:56 PM

Oct 4, 2021 12:56 PM

Oct 3, 2021 12:55 PM

Oct 2, 2021 12:55 PM

Oct 1, 2021 12:55 PM

Controls

51 Total controls

Pass Fail Unable to perf... Not applicable

Failures

Critical High Medium Low

Score

830 Compliance

IBM Cloud Search resources and offerings... Catalog Docs Support Manage 2137132 - Tec... Details

Download report ↴

15 36 0 0

Status Filter... Severity Filter... Search

Status	ID	Control	Severity	Resource details
🔴	AC-2(1)	Account Management Automated System Account Management	High	165 Pass, 122 Fail, 12 Unable to perform, 0 Not applicable
🔴	AC-2(3)	Account Management Automated System Account Management	Medium	0 Pass, 11 Fail, 0 Unable to perform, 0 Not applicable
🟢	AC-2(7)	Account Management Privileged User Accounts	-	1 Pass, 0 Fail, 0 Unable to perform, 0 Not applicable
🔴	AC-2(a)	Identifies and selects the following types of information system accounts to support organizational missions/business functions	Medium	0 Pass, 1 Fail, 0 Unable to perform, 0 Not applicable
🔴	AC-2(c)	Establishes conditions for group and role membership	High	147 Pass, 112 Fail, 0 Unable to perform, 0 Not applicable
🔴	AC-2(f)	Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions	High	18 Pass, 2 Fail, 1 Unable to perform, 0 Not applicable
🔴	AC-2(i)	Authorizes access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Assignment: organization-defined attributes (as required);	High	185 Pass, 139 Fail, 12 Unable to perform, 0 Not applicable
🔴	AC-3	Access Enforcement	High	163 Pass, 118 Fail, 0 Unable to perform, 0 Not applicable
🔴	AC-4	Information Flow Enforcement	Critical	191 Pass, 79 Fail, 2 Unable to perform, 0 Not applicable
🔴	AC-5(b)	Documents separation of duties of individuals	High	158 Pass, 117 Fail, 0 Unable to perform, 0 Not applicable
🔴	AC-6-0	Least Privilege	High	165 Pass, 119 Fail, 0 Unable to perform, 0 Not applicable
🟢	AC-6(10)	Least Privilege Prohibit Non-privileged Users from Executing Privileged Functions	-	4 Pass, 0 Fail, 0 Unable to perform, 0 Not applicable
🔴	AC-17(2)	Remote Access Protection of Confidentiality and Integrity Using Encryption	High	5 Pass, 12 Fail, 2 Unable to perform, 0 Not applicable

Determines that the information system is capable of auditing organization.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

7. Here we see the list of failed controls. We can drill down on a particular control to see the failing goals.
8. Click on the “AC-2(1)” control to see the list of goals.

The screenshot shows the IBM Cloud Security and Compliance interface. On the left, there's a sidebar with a timeline from Oct 1 to Oct 12, 2021. A specific control, "AC-2(1)", is selected. The main panel displays "Account Management | Automated System Account Management". It shows a table of goals, each with a unique ID, a description, and performance metrics (Pass, Fail, Unable to perform, Not applicable) across four categories: Green (Pass), Red (Fail), Yellow (Unable to perform), and Grey (Not applicable). The first goal, ID: 3000015, is highlighted in red, indicating a failure.

Control ID	Severity	Status	Number of goals
AC-2(1)	High	FAIL	25

Goals	Pass	Fail	Unable to perform	Not applicable
ID: 3000015 Check whether IAM users are attached to at least one access group	8	3	0	0
ID: 3000016 Check whether IAM policies for users are attached only to groups or roles	63	18	0	0
ID: 3000023 Check whether the account owner does not have an IBM Cloud API key created in IAM	1	0	0	0
ID: 3000024 Check whether IBM Cloud API keys that are managed in IAM are rotated at least every # days	4	7	0	0
ID: 3000025 Check whether an account owner has logged in to IBM Cloud in the past # days	0	1	0	0
ID: 3000026 Check whether user list visibility restrictions are configured in IAM settings for the account owner	1	0	0	0
ID: 3000030 Check whether IAM policies for service IDs are attached only to groups or roles	63	90	0	0
ID: 3000035 Check whether account access is managed only by IAM access groups	0	1	0	0
ID: 3000039 Check whether IBM Cloud API keys that are unused for 180 days are detected and optionally disabled	0	0	11	0
ID: 3000235 Check whether Hyper Protect Crypto Services encryption keys that are generated by the service are rotated automatically at least every # months	0	0	0	0
ID: 3000425 Check whether VPN for VPC authentication is configured with a strong pre-shared key with at least 128 bits of strength	0	0	1	0

9. This view shows the goals associated with this control and the current state. We can look at the details of a goal to see the values that are causing the failure.
10. Click on goal “3000015”.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

ID: 3000015 Check whether IAM users are attached to at least one access group

Status	Resource	Resource type	Actual value	Detail
Green	amtrice@us.ibm.com	Identity and Access Management:Users	[{"AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf"}]	User is attached to at least one access group
Green	Erik.Lind@ibm.com	Identity and Access Management:Users	[{"AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf"}]	User is attached to at least one access group
Red	matthewperrins@gmail.com	Identity and Access Management:Users	[]	User is not attached to any access group
Green	mjperrin@us.ibm.com	Identity and Access Management:Users	[{"AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf"}]	User is attached to at least one access group
Green	Noe.Samaille@ibm.com	Identity and Access Management:Users	[{"AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf"}]	User is attached to at least one access group
Green	ramragh1@in.ibm.com	Identity and Access Management:Users	[{"AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf"}, {"AccessGroupId-3ddc343-9acf-4f7b-89d3-8775f9822b9d"}, {"AccessGroupId-e7f4671e-387d-4b7e-8fbf-c23a35f92247"}]	User is attached to at least one access group
Red	seansund@gmail.com	Identity and Access Management:Users	[]	User is not attached to any access group

11. Goal 3000015 requires that every user is attached to an access group. The results show all of the users in the account and which ones are missing access groups.

12. Click on the “Resource view” to list the resource categories.

Control view Resource view Remediation script

Resources	Status
Access Control List	Red
Account	Red
Block Storage	Red
Cloud Certificate	Green
Cloud Key	Red
Cloud Key Protect	Red
Cloud Load Balancer	Red
Cloud Object Storage Bucket	Red
Cloud Security Group	Red
Hyper Protect Crypto	Green



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

13. Expand the “OpenShift Cluster” item

Virtual Private Network Cluster

frontoffice-cluster

frontoffice-workload-cluster

nlb-frontoffice-cluster-48d3a96f95acca62076e928d79df50cf-i000.eu-de.containers.appdomain.cloud

nlb-frontoffice-workload-clus-48d3a96f95acca62076e928d79df50cf-i000.eu-de.containers.appdomain.cloud

14. Click on the “frontoffice-workload-cluster” item, to see the controls that are scanned for this specific cluster and see the pass/fail status for each of the controls. Click on any of the controls to see details about that specific scan item.

The screenshot shows the IBM Best Practices interface under the "Security and Compliance / Scan results" section. On the left, there's a sidebar with a timeline of scans from Sep 13 to Sep 23. The main area is titled "frontoffice-workload-cluster". It displays a table of controls with columns for Resource type, Severity, Status, and Number of controls. One control is highlighted with a blue border: "ID: 10.2.3 Ensure OpenShift clusters version is up-to-date". Below this, there's a detailed view of the control with its ID, description, status, and severity. The status is "FAIL". The severity is "Medium". The description is "Check whether OpenShift version is up-to-date". The status is "FAIL". The severity is "Medium". The description is "OpenShift versions are not up-to-date". There are also buttons for "Pass", "Fail", "Unable to perform", and "Not applicable". At the bottom, there are pagination controls and a search bar.

15. Click on the “Control view” tab again then click on “Download report”.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

IBM Cloud Search resources and offerings... Catalog Docs Support Manage 2137132 - Tec... Details

Security and Compliance / Scan results / frontoffice - FS Cloud 0-1-2 frontoffice | IBM Cloud for Financial Services v0.1.2 | Validation

Oct 12, 2021 12:58 PM October 12, 2021 12:58 PM Remediation script

Oct 11, 2021 12:57 PM Control view Resource view Download report

Oct 10, 2021 12:56 PM

Oct 9, 2021 12:56 PM

Oct 8, 2021 12:57 PM

Oct 7, 2021 12:56 PM

Oct 6, 2021 12:56 PM

Oct 5, 2021 12:56 PM

Oct 4, 2021 12:56 PM

Oct 3, 2021 12:55 PM

Oct 2, 2021 12:55 PM

Oct 1, 2021 12:55 PM

Status Filter... Severity Filter... Search

Status	ID	Control	Severity	Resource details
●	AC-2(1)	Account Management Automated System Account Management	High	● 165 ● 121 ○ 12 □ 0
●	AC-2(3)	Account Management Automated System Account Management	Medium	● 0 ● 11 ○ 0 □ 0
●	AC-2(7)	Account Management Privileged User Accounts	-	● 1 ● 0 ○ 0 □ 0
●	AC-2(a)	Identifies and selects the following types of information system accounts to support organizational missions/business functions	Medium	● 0 ● 1 ○ 0 □ 0
●	AC-2(c)	Establishes conditions for group and role membership	High	● 147 ● 111 ○ 1 □ 0
●	AC-2(f)	Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions	High	● 18 ● 2 ○ 1 □ 0
●	AC-2(i)	Authorizes access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Assignment: organization-defined attributes (as required);	High	● 186 ● 137 ○ 12 □ 0
●	AC-3	Access Enforcement	High	● 164 ● 116 ○ 0 □ 0

IBM Cloud Search resources and offerings... Catalog Docs Support Manage 2137132 - Tec... Details

Security and Compliance / Scan results / frontoffice - FS Cloud 0-1-2 frontoffice | IBM Cloud for Financial Services v0.1.2 | Validation

Oct 12, 2021 12:58 PM October 12, 2021 12:58 PM

Oct 11, 2021 12:57 PM Control view Resource view

Oct 10, 2021 12:56 PM

Oct 9, 2021 12:56 PM

Oct 8, 2021 12:57 PM

Oct 7, 2021 12:56 PM

Oct 6, 2021 12:56 PM

Oct 5, 2021 12:56 PM

Oct 4, 2021 12:56 PM

Oct 3, 2021 12:55 PM

Oct 2, 2021 12:55 PM

Oct 1, 2021 12:55 PM

Status Filter... Severity Filter... Search

Status	ID	Control
●	AC-2(1)	Account Management Automated System Account Management
●	AC-2(3)	Account Management Automated System Account Management
●	AC-2(7)	Account Management Privileged User Accounts
●	AC-2(a)	Identifies and selects the following types of information system accounts to support organizational missions/business functions
●	AC-2(c)	Establishes conditions for group and role membership
●	AC-2(f)	Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions
●	AC-2(i)	Authorizes access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Assignment: organization-defined attributes (as required);
●	AC-3	Access Enforcement

Download report

Options Details

What type of report would you like to download?

Report types

Detailed You can choose specific details that you want included in your report.

Report format

PDF

Delta With the delta report, you can compare two scans to see how changes occur over time. The report is available as a PDF only.

Cancel Next



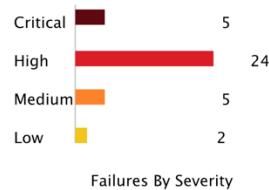
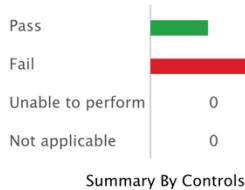
IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

16. A report of the scan results can also be downloaded as either a PDF or Excel spreadsheet to share with others.

Executive Summary

Report Generated	2021-10-13 04:25:21 PM UTC
FACTs Collected	2021-10-12 05:58:19 PM UTC
Validation Performed	2021-10-12 05:58:24 PM UTC
Report Profile	IBM Cloud for Financial Services v0.1.2
Scope	frontoffice
Report run by	IBMid-110000SNV8

Result	Critical	High	Medium	Low	Total
Passed:	2	6	6	1	15
Failed:	5	24	5	2	36
Unable to Perform:					
Not Applicable:					
TOTAL:	7	30	11	3	51



17. Return to the Security and Compliance Center overview page - <https://cloud.ibm.com/security-compliance/overview>

Govern resources

1. The Security and Compliance Center allows rules to define the constraints that should be placed on resources that are provisioned in the account.
2. Click on “Configure” → “Rules” under the “Govern resources” section on the left menu.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

Name	Service	Attachments	Labels	Enforcement actions
Stop cross-account connections	Transit Gateway	1	-	Disallow

3. This page lists the rules that have been configured for this account.
4. Click on the “Stop cross-account connections” rule to see the details.

```
        "rule_type": "user_defined",
        "target": {
            "service_name": "transit",
            "resource_kind": "service",
            "additional_target_attributes": []
        },
        "required_config": {
            "and": [
                {
                    "property": "cross_account_connection_approved",
                    "operator": "is_false",
                    "value": "false"
                }
            ],
            "enforcement_actions": [
                {
                    "action": "disallow"
                }
            ],
            "labels": []
        }
```

5. The rules are defined as allowed values for the various attributes of the service and an enforcement action. This rule is requiring that the ‘cross_account_connection_approved’ attribute for a Transit Gateway is false, meaning that a Transit Gateway cannot be created to connect VPCs across accounts.
6. Click on “Rules” in the breadcrumbs at the top then click on “Results” under the “Govern resources” section on the left menu.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

The screenshot shows the IBM Cloud Security and Compliance interface. The left sidebar is titled 'IBM Cloud' and includes sections for 'Security and Compliance', 'Dashboard', 'Manage posture', 'Assess', 'Configure', 'Govern resources', 'Results' (which is selected), 'Configure', 'Gain insight', 'Insights', 'Findings', 'Configure', 'Integrations', and 'Global settings'. The main content area is titled 'Evaluation results' and shows a timestamp of '2021-10-13 8:57:34 AM'. It displays a message: 'You are 100% compliant. Congratulations! Your latest scan came back completely compliant.' Below this is a table with the following data:

Name	Service	Noncompliant	Status
Stop cross-account connections	Transit Gateway	0	✓

At the bottom of the table, it says 'Items per page: 25' and '1-1 of 1 item'. There are also navigation icons for search, refresh, and download report.

7. The rules are enforced for any new services that are provisioned. The ‘Evaluation results’ view shows the compliance status of the existing services against the defined rules.
8. Click on “Insights” under the “Gain insights” section on the left menu.



IBM Cloud for Financial Services – Tech Zone Demo Environment Ecosystem Engineering

The screenshot shows the IBM Cloud Security and Compliance Center Insights dashboard. The left sidebar is titled 'IBM Cloud' and includes sections for 'Security and Compliance', 'Dashboard', 'Manage posture', 'Assess', 'Configure', 'Govern resources', 'Results', 'Configure', 'Gain insight', 'Insights' (which is selected), 'Findings', 'Configure', 'Integrations', and 'Global settings'. The main area is titled 'Insights' and shows the last updated date as 'Oct 13, 2021, 9:13:24 AM'. It features a summary section with counts for Critical (0/1), High (1/1), Medium (0/1), and Low (0/1) vulnerabilities. Below this is a 'Built-in Insights' section with three cards: 'Vulnerability in Images' (Vulnerability Advisor), 'Certificates' (Certificate Manager), and 'Suspicious Inbound Traffic' (Network Insights). The 'Certificates' card includes a bar chart showing certificate expiration status over time.

9. The Insights function of Security and Compliance Center monitors a number of services to watch for vulnerabilities and suspicious activity. The results of Vulnerability Advisor are monitored for issues with the images. Certificates in Certificate Manager are checked to notify of upcoming expirations. Finally, the Flow Logs are scanned for suspicious inbound and outbound network traffic within the VPC network. Additional tools and custom findings can be integrated into the Security and Compliance Center to give one dashboard to view security and compliance related information.

THIS CONCLUDES THE LAB STEPS