



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>

Resources

- These slides can be used to set the context for the Security and Compliance Center before conducting the demo of the environment:
<https://ibm.box.com/s/s0ybat8p4eh48tw8mgs49zg1j4jexzhq>



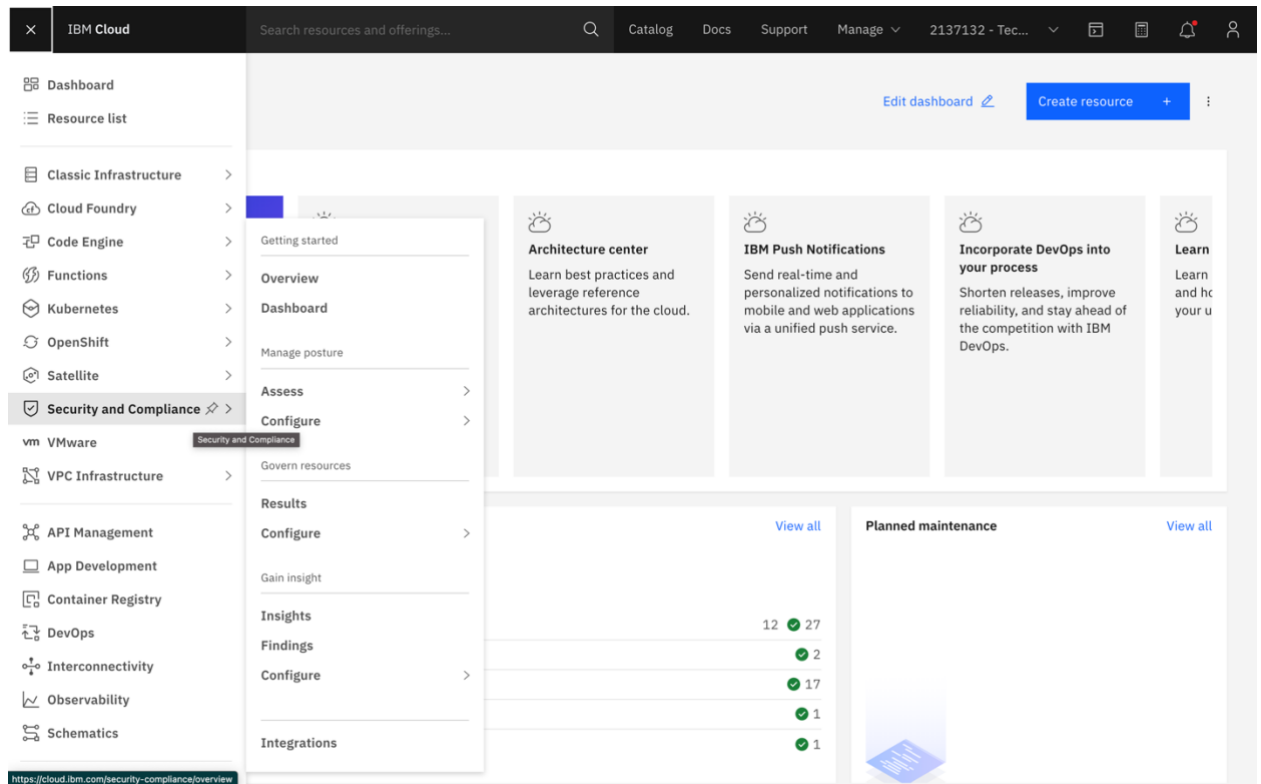
IBM Cloud for Financial Services – Tech Zone Demo Environment

Hybrid Cloud Ecosystem – Ecosystem Labs

Demo Steps

Dashboard

1. Log in to the IBM Cloud account – <https://cloud.ibm.com>
2. Say: “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.

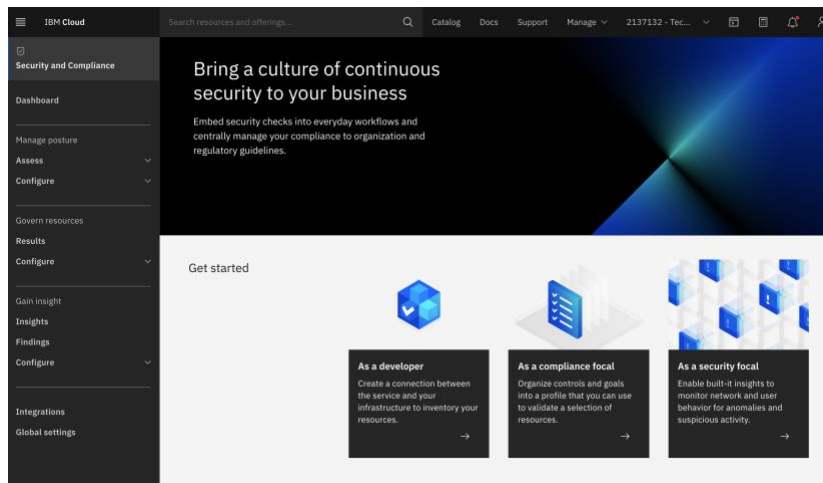


5. Say: “The Security and Compliance Center is an account-level service that can be used to continuously scan the environment to determine the current security posture of the deployed services, set up rules to govern how new services are provisioned, and monitor for threats and vulnerabilities in the

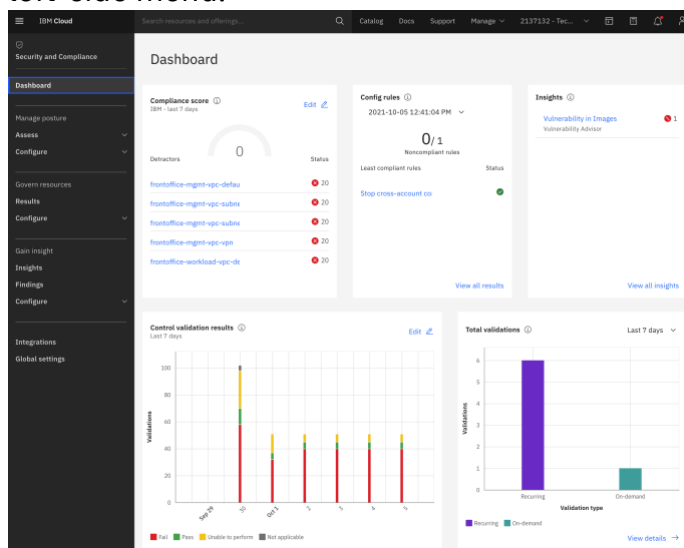


IBM Cloud for Financial Services – Tech Zone Demo Environment Hybrid Cloud Ecosystem – Ecosystem Labs

environment.”



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



7. Say: “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

Hybrid Cloud Ecosystem – Ecosystem Labs

IBM Cloud

Search resources and offerings...

Catalog Docs Support Manage 2137132 - Tec...

Security and Compliance

Dashboard

Manage posture

Assess

Configure

Collectors

Credentials

Scopes

Profiles

Collectors

View docs

Status: 10 x Filter... Endpoint type: All Search Create +

Name	Description	Last contact	Managed by	Endpoint type	Status
managed	-	2021-10-12 1:13:06 PM	IBM	Private	Inactive

Items per page: 25 1-1 of 1 item 1 1 of 1 page

- Say: “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.”
- Click on “Configure” → “Scopes” under the “Manage Posture” section on the left menu.

IBM Cloud

Search resources and offerings...

Catalog Docs Support Manage 2137132 - Tec...

Security and Compliance

Dashboard

Manage posture

Assess

Configure

Collectors

Credentials

Scopes

Profiles

Goals

Scans

Govern resources

Results

Scopes

View docs

Status: Active Search Create +

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

Details Last scan

Collectors Type

managed Validation

Time

2021-10-12 12:58:28 PM

Status

Validation completed

Items per page: 25 1-1 of 1 item 1 1 of 1 page

- Say: “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.”
- Click on the name of the “frontoffice” scope to see the details.



IBM Cloud for Financial Services – Tech Zone Demo Environment

Hybrid Cloud Ecosystem – Ecosystem Labs

The screenshot shows the IBM Cloud console interface. The top navigation bar includes the IBM Cloud logo, a search bar, and links to Catalog, Docs, Support, and Manage. The main content area is titled 'frontoffice' and shows a list of resources under the 'Inventory' section. The left sidebar contains 'Settings' and 'Event history'. The right sidebar has 'Actions...' and 'Details' buttons. The main table lists resources with columns for 'Resource type' and 'Detail'.

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. Say: “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

Hybrid Cloud Ecosystem – Ecosystem Labs

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. Say: “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. Say: “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

Hybrid Cloud Ecosystem – Ecosystem Labs

Security and Compliance / Profiles / IBM Cloud for Financial Services v0.1.2

Controls

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. Say: “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.

Security and Compliance / Profiles / IBM Cloud for Financial Services v0.1.2

Controls

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 procedures	
AC-2(i): Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Assignment: organization-defined	
AC-3: Access Enforcement	
AC-4: Information Flow Enforcement	



IBM Cloud for Financial Services – Tech Zone Demo Environment Hybrid Cloud Ecosystem – Ecosystem Labs

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

The screenshot displays the IBM Cloud for Financial Services v0.1.2 interface. The top navigation bar includes the IBM Cloud logo, a search bar, and links to Catalog, Docs, Support, and Manage. The main header shows the breadcrumb "Security and Compliance / Profiles /" and the title "IBM Cloud for Financial Services v0.1.2". A left sidebar contains a "Controls" section. The main content area shows the "AC-2(1): Account Management | Automated System Account Management" control expanded, revealing a list of 14 sub-goals (3000015 through 3000714) that map specific requirements to account and service configurations.

IBM Cloud for Financial Services v0.1.2

Controls

AC-2(1): Account Management | Automated System Account Management

- 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. Say: “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

Hybrid Cloud Ecosystem – Ecosystem Labs

The screenshot displays the IBM Cloud Security and Compliance Center interface. The top navigation bar includes the IBM Cloud logo, a search bar, and links to Catalog, Docs, Support, and Manage. The main content area is titled "Security and Compliance / Profiles / IBM Cloud for Financial ... / 30000015".

Details

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

Environment: IBM

Tags: IAM, IBM

Goal attributes

Fact master attribute	Attribute display name	Attribute key
Details	IAM User Access Groups	exclude_owner_ac...

Validation report messages

Pass	Fail
-	-
Not applicable	Unable to perform
CTL.NOT_APPLICABLE.STAT...	CTL.IBM_IAM_ACCOUNT_N...
Fact master value missing	
CTL.FACT_DETAILS_NOT_FOUND	

Goal logic

```
var objectName = 'Identity and Access Management';
var objectType = 'Identity and Access Management:Users';
var displayEv = 'CTL.IBM_IAM_USER_ATTACHED_TO_GROUPS.EV';
var info = '';
var actualValue = '';
var resultList = [];
try {
  var iamUsers = '';
  if (isDataAvailable(Details, "list_users")) {
    iamUsers = Details['list_users'];
  }
  if (iamUsers === undefined || iamUsers === "" || iamUsers.length === 0) {
    info = "CTL.IBM_IAM_USER_NOT_FOUND";
    var result_dict = getObjectResult(Status.UNABLE_TO_PERFORM, displayEv, "", actualValue,
      "", info,
      objectName, objectType, "");
  }
}
```

18. Say: "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

Hybrid Cloud Ecosystem – Ecosystem Labs

IBM Cloud

Search resources and offerings...

Catalog Docs Support Manage 2137132 - Tec...

Security and Compliance

Dashboard

Manage posture

Assess

Configure

Collectors

Credentials

Scopes

Profiles

Goals

Scans

Govern resources

Results

Configure

Gain insight

Insights

Findings

Configure

Scans

View docs

Status: Active

Schedule +

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

Items per page: 25 1-3 of 3 items

1 1 of 1 page

20. Say: “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 v0.1.2’ 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

Hybrid Cloud Ecosystem – Ecosystem Labs

The screenshot displays the IBM Cloud Security and Compliance console. The left sidebar contains navigation options: Security and Compliance, Dashboard, Manage posture, Assess, Scan results (selected), Remediation, Inventory, Configure, Govern resources, Results, Configure, Gain insight, Insights, Findings, Configure, and Integrations. The main content area is titled 'Scan results' and includes a search bar, 'View docs' link, and 'Generate a report' button. A table lists scan results with columns: Name, Scope, Profile, Last scan time, and Last scan results. The table contains 9 rows of scan data. At the bottom, there is a pagination bar showing 'Items per page: 25' and '1-9 of 9 items'.

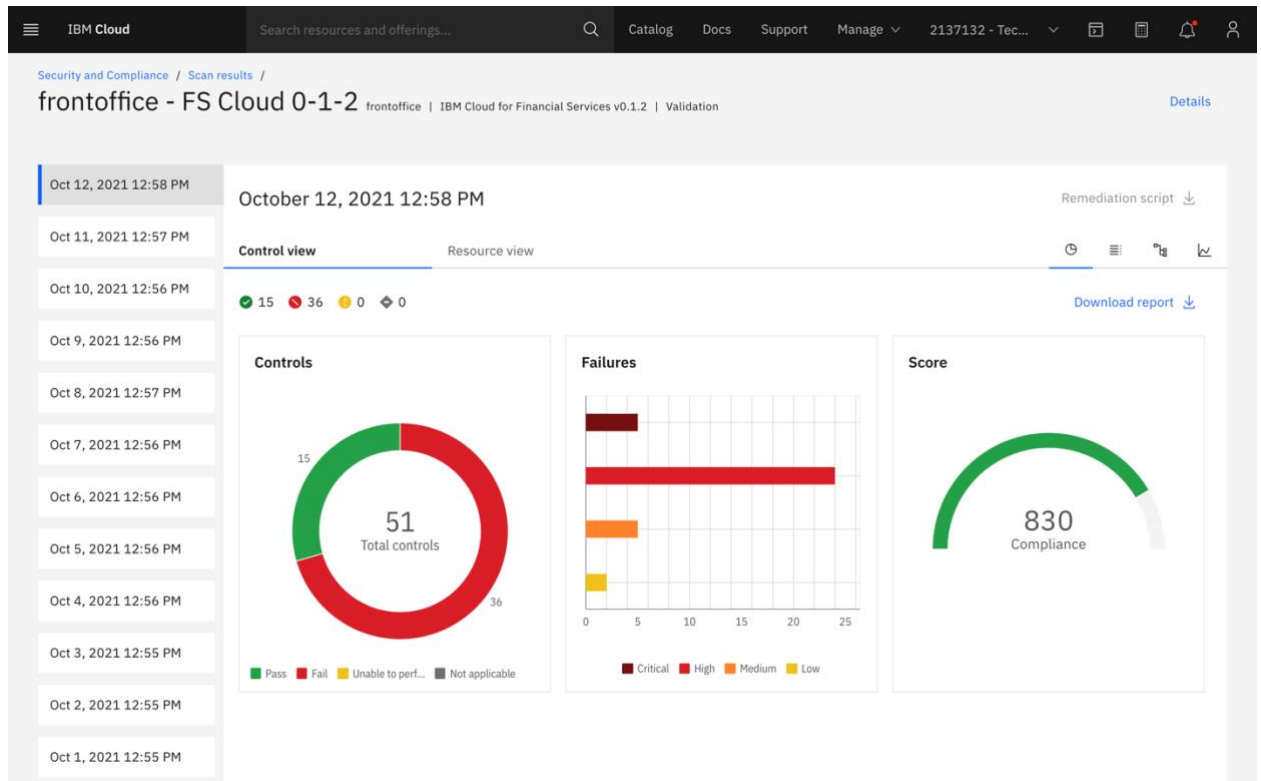
Name	Scope	Profile	Last scan time	Last scan results
frontoffice - FS Cloud 0-1-2	frontoffice	IBM Cloud for Financial Services v0.1.2	2021-10-12 12:58:20 PM	15 (pass) 36 (fail)
frontoffice - IBMCloudforFinancial	frontoffice	IBM Cloud for Financial Services v0.1.2	2021-10-12 12:30:30 AM	15 (pass) 36 (fail)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

Items per page: 25 1-9 of 9 items 1 1 of 1 page

2. Say: “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 Hybrid Cloud Ecosystem – Ecosystem Labs



4. Say: “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.”



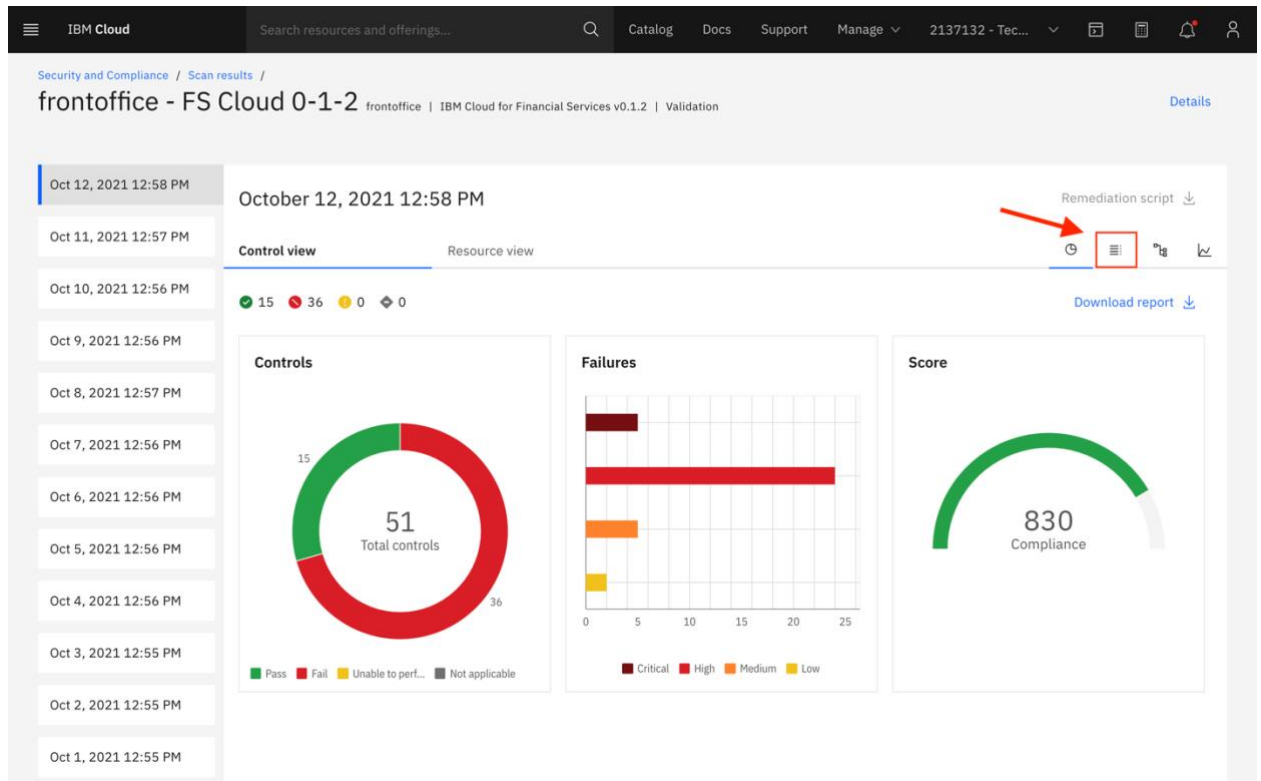
In this account, to accommodate the demo environment there are a couple of known exceptions to the FS controls. For example: some of the network ACLs are opened to allow VPN traffic and public gateways are attached to the OpenShift cluster subnets to allow access to external repositories.

5. Say: “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

Hybrid Cloud Ecosystem – Ecosystem Labs



IBM Cloud

Search resources and offerings...

Catalog Docs Support Manage 2137132 - Tec...

Download report

15 36 0 0

Status Filter... Severity Filter... Search

Status	ID	Control	Severity	Resource details
Fail	AC-2(1)	Account Management Automated System Account Management	High	165 122 12 0
Fail	AC-2(3)	Account Management Automated System Account Management	Medium	0 11 0 0
Pass	AC-2(7)	Account Management Privileged User Accounts	-	1 0 0 0
Fail	AC-2(a)	Identifies and selects the following types of information system accounts to support organizational missions/business functions	Medium	0 1 0 0
Fail	AC-2(c)	Establishes conditions for group and role membership	High	147 112 0 0
Fail	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
Fail	AC-2(i)	Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Assignment: organization-defined attributes (as required);	High	185 139 12 0
Fail	AC-3	Access Enforcement	High	163 118 0 0
Fail	AC-4	Information Flow Enforcement	Critical	191 79 2 0
Fail	AC-5(b)	Documents separation of duties of individuals	High	158 117 0 0
Fail	AC-6-0	Least Privilege	High	165 119 0 0
Pass	AC-6(10)	Least Privilege Prohibit Non-privileged Users from Executing Privileged Functions	-	4 0 0 0
Fail	AC-17(2)	Remote Access Protection of Confidentiality and Integrity Using Encryption	High	5 12 2 0
Fail		Determines that the information system is capable of auditing organization-		



IBM Cloud for Financial Services – Tech Zone Demo Environment Hybrid Cloud Ecosystem – Ecosystem Labs

7. Say: “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.

frontoffice - FS Cloud 0-

Account Management | Automated System Account Management

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

Goals

Goal ID	Goal Description	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: 3000435	Check whether VPN for VPC authentication is configured with a strong pre-shared key with at	0	0	1	0

9. Say: “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

Hybrid Cloud Ecosystem – Ecosystem Labs

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

Environment: IBM, Resource category: XaaS, Resource type: Identity and Access Management, Resource: Identity and Access Management

Expected value
IAM users should be attached to at least one access group

Status	Resource	Resource type	Actual value	Detail
✓	amtrice@us.ibm.-com	Identity and Access Management:Users	["AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf","AccessGroupId-74e75fe3-432a-4e50-af75-146483080434"]	User is attached to at least one access group
✓	Erik.Lind@ibm.com	Identity and Access Management:Users	["AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf"]	User is attached to at least one access group
✗	matthewperrins@gmail.com	Identity and Access Management:Users	[]	User is not attached to any access group
✓	mjperrin@us.ibm.-com	Identity and Access Management:Users	["AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf","AccessGroupId-74e75fe3-432a-4e50-af75-146483080434","AccessGroupId-8c38a89c-2ce6-4e46-ba19-876736d4e531"]	User is attached to at least one access group
✓	Noe.Samaille@ibm.com	Identity and Access Management:Users	["AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf"]	User is attached to at least one access group
✓	ramragh1@in.ibm.-com	Identity and Access Management:Users	["AccessGroupId-1aa081e9-05ab-4f2a-ba1f-deefcb7856cf","AccessGroupId-3ddc3343-9acf-4f7b-89d3-8775f9822b9d","AccessGroupId-e7f4671e-387d-4b7e-8bfec23a35f9224"]	User is attached to at least one access group
✗	seansund@gmail.-com	Identity and Access Management:Users	[]	User is not attached to any access group

11. Say: “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.

IBM Best Practices

Control view **Resource view**

Resources

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



IBM Cloud for Financial Services – Tech Zone Demo Environment Hybrid Cloud Ecosystem – Ecosystem Labs

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.

frontoffice-workload-cluster

Resource type	Severity	Status	Number of controls
container	Medium	FAIL	5

Controls

100% Pass 100% Fail 0% Unable to perform 0% Not applicable

ID: 10.2.3 Ensure OpenShift clusters version is up-to-date 100% Pass 0% Fail 0% Unable to perform 0% Not applicable

Goal Status	All	Search		
Status	Goal ID	Goal description	Severity	Detail
100% Pass 0% Fail 0% Unable to perform 0% Not applicable	3000907	Check whether OpenShift version is up-to-date	Medium	OpenShift versions are not up-to-date

Items per page: 25 1-1 of 1 item 1 1 of 1 page

ID: 10.2.4	Ensure OpenShift clusters is accessible only by using private endpoints	100% Pass 0% Fail 0% Unable to perform 0% Not applicable
ID: 10.2.5	Ensure OpenShift cluster has image pull secrets enabled	100% Pass 0% Fail 0% Unable to perform 0% Not applicable
ID: 10.2.6	Ensure OpenShift clusters are enabled with IBM Cloud Monitoring	100% Pass 0% Fail 0% Unable to perform 0% Not applicable
ID: 10.2.7	Ensure OpenShift clusters are enabled with IBM Log Analysis	100% Pass 0% Fail 0% Unable to perform 0% Not applicable

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



IBM Cloud for Financial Services – Tech Zone Demo Environment

Hybrid Cloud Ecosystem – Ecosystem Labs

IBM Cloud

Search resources and offerings...

Catalog Docs Support Manage 2137132 - Tec...

Security and Compliance / Scan results /

frontoffice - FS Cloud 0-1-2 frontoffice | IBM Cloud for Financial Services v0.1.2 | Validation

Details

Oct 12, 2021 12:58 PM

October 12, 2021 12:58 PM

Remediation script

Control view Resource view

15 36 0 0

Download report

Status Filter... Severity Filter... Search

Status	ID	Control	Severity	Resource details
1	AC-2(1)	Account Management Automated System Account Management	High	165 121 12 0
1	AC-2(3)	Account Management Automated System Account Management	Medium	0 11 0 0
2	AC-2(7)	Account Management Privileged User Accounts	-	1 0 0 0
1	AC-2(a)	Identifies and selects the following types of information system accounts to support organizational missions/business functions	Medium	0 1 0 0
1	AC-2(c)	Establishes conditions for group and role membership	High	147 111 0 0
1	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
1	AC-2(i)	Authorize 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
1	AC-3	Access Enforcement	High	164 116 0 0

IBM Cloud

Search resources and offerings...

Catalog Docs Support Manage 2137132 - Tec...

Security and Compliance / Scan results /

frontoffice - FS Cloud 0-1-2 frontoffice | IBM Cloud for Financial Services v0.1.2 | Validation

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 Hybrid Cloud Ecosystem – Ecosystem Labs

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

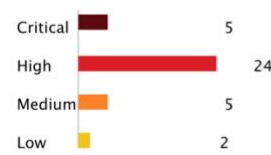
Executive Summary

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



Summary By Controls



Failures By Severity

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

Govern resources

1. Say: “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

Hybrid Cloud Ecosystem – Ecosystem Labs

Configuration rules

Labels: Filter... Create +

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

Rules per page: 25 1-1 of 1 items 1 1 of 1 pages

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

Stop cross-account connections Rule

Parameters

Attachments

Services

Transit Gateway

Description

Disallow cross-account connection requests for Transit Gateway. This is to fix Goal ID 3000417.

Enforcement actions

Disallow

Labels

No labels selected.

```
{
  "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": "-"
      }
    ]
  },
  "enforcement_actions": [
    {
      "action": "disallow"
    }
  ],
  "labels": []
}
```

- Say: “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.”
- 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 Hybrid Cloud Ecosystem – Ecosystem Labs

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

Security and Compliance

- Dashboard
- Manage posture
- Assess
- Configure
- Govern resources
- Results**
- Configure
- Gain insight
- Insights
- Findings
- Configure
- Integrations
- Global settings

Evaluation results

2021-10-13 8:57:34 AM 2021-10-13 8:57:34 AM View docs

You are 100% compliant.
Congratulations! Your latest scan came back completely compliant.

Services: All Search Download report

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

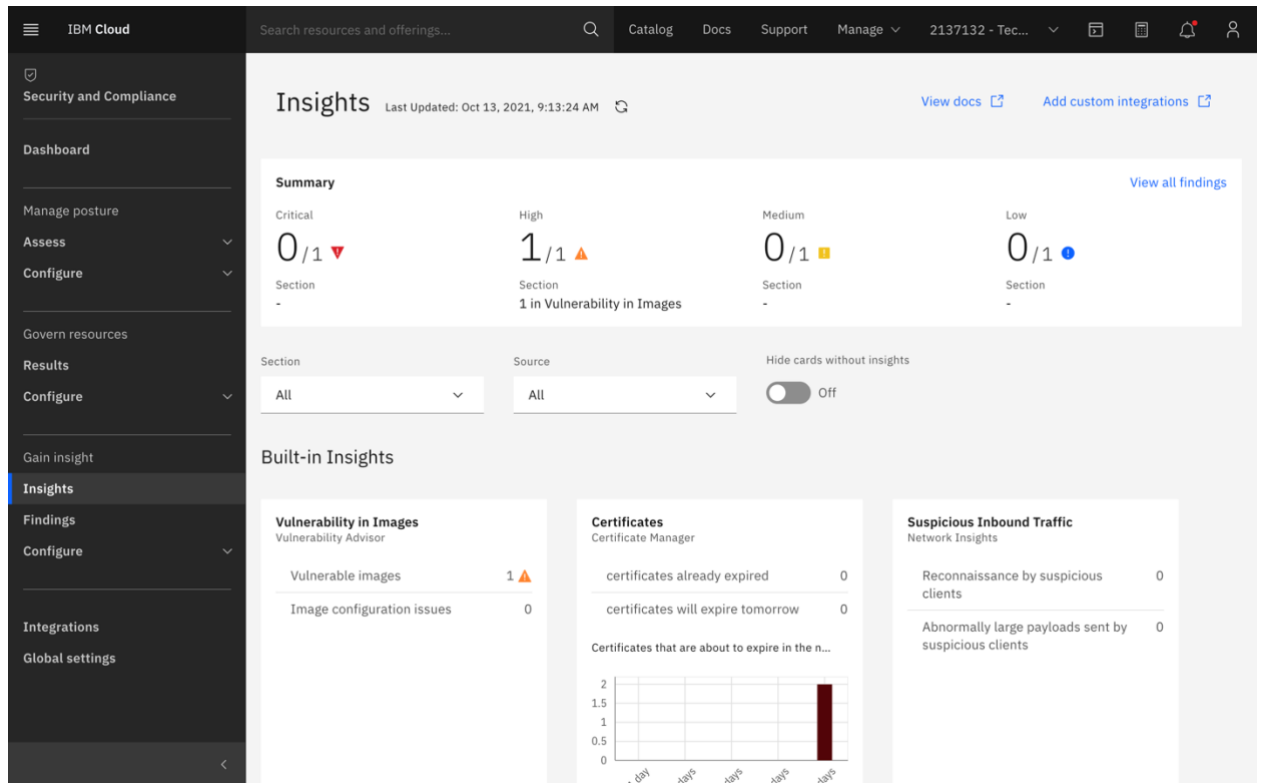
Items per page: 25 1-1 of 1 item 1 1 of 1 page

7. Say: “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

Hybrid Cloud Ecosystem – Ecosystem Labs



9. Say: “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 DEMO STEPS