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

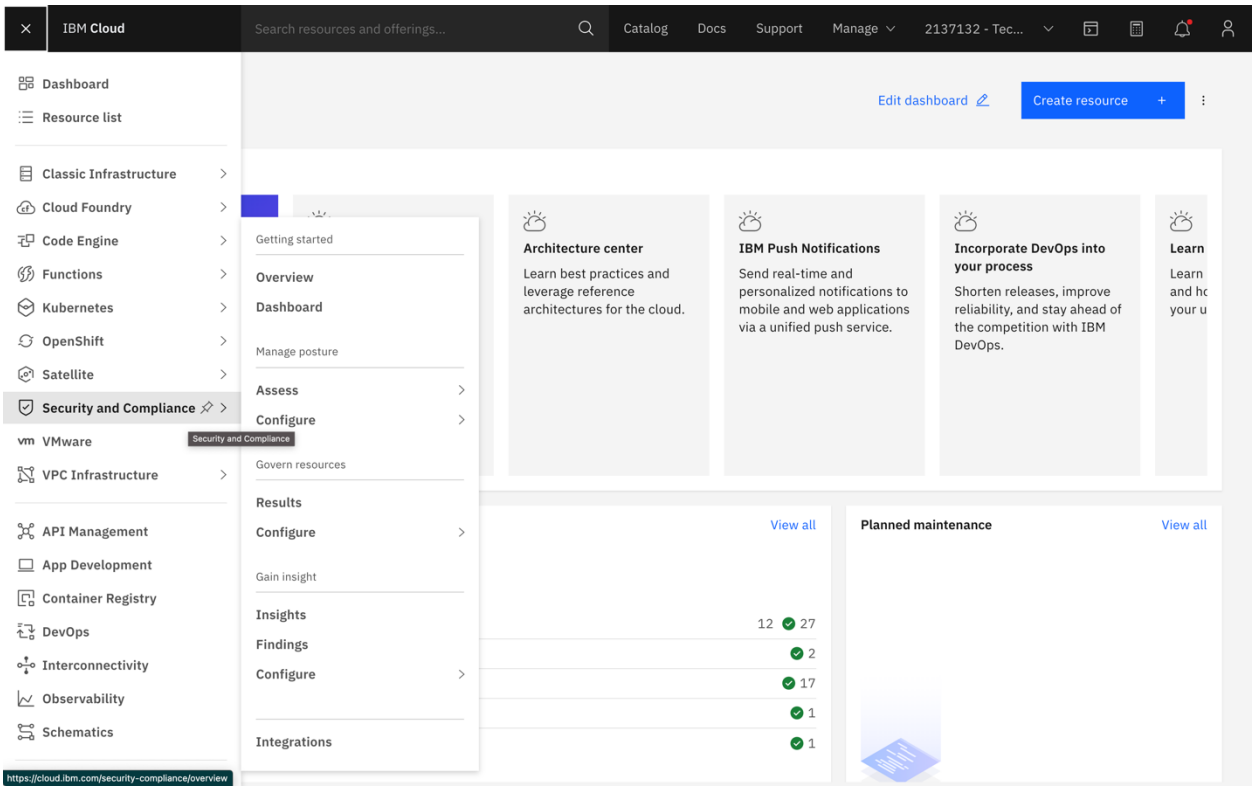
- Familiarize the audience with the Security & Compliance Center
- View scan results by pass/fail
- View scan results per resource instance
- View failing compliance controls and reason for failure

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

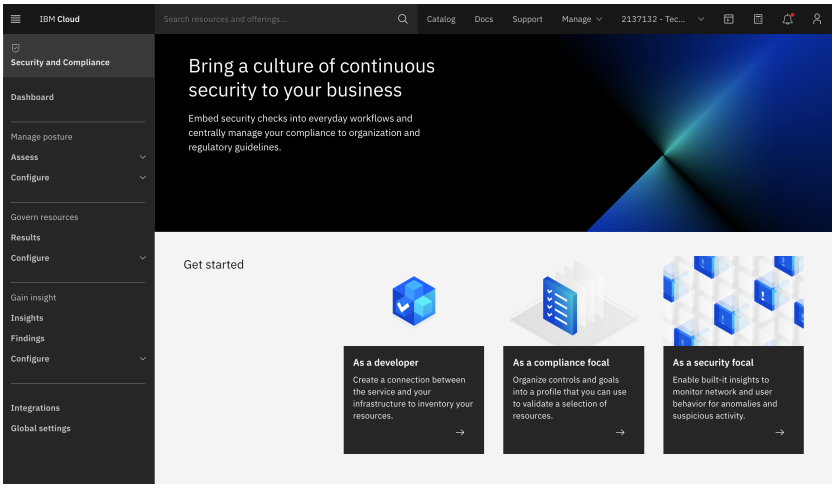
Steps

Dashboard

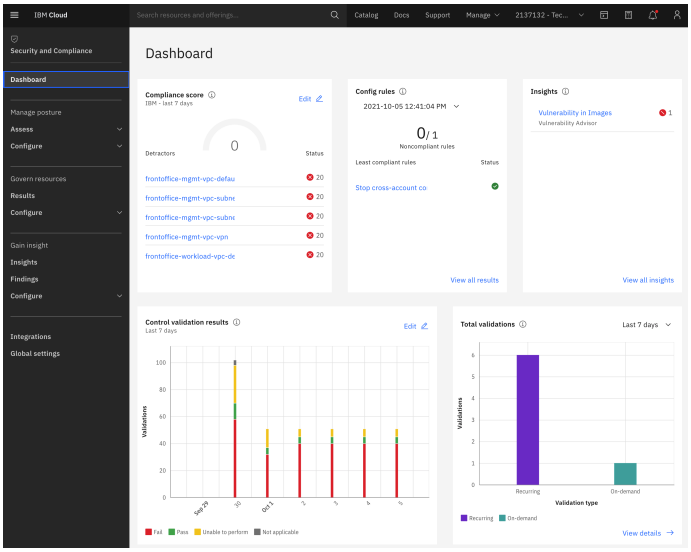
1. Log in to the IBM Cloud account – https://cloud.ibm.com
2. This is an account where the IBM Cloud for Financial Services Reference Architecture has been deployed and the Security and Compliance Center has been set up to monitor and manage the security posture of the deployment.
3. Click on the “Hamburger”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

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

environment.



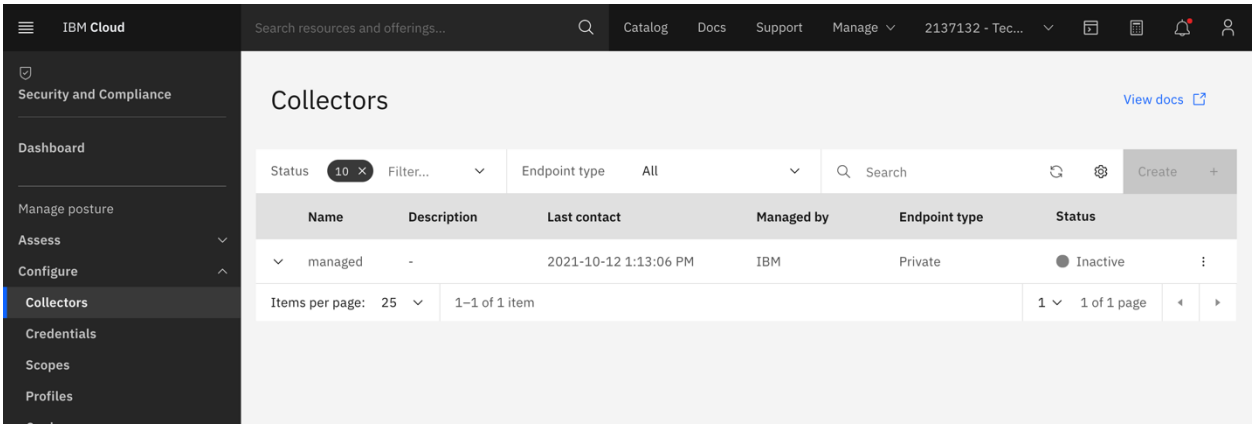
6. Navigate to the SCC Dashboard by clicking on the “Dashboard” link in the left-side menu.



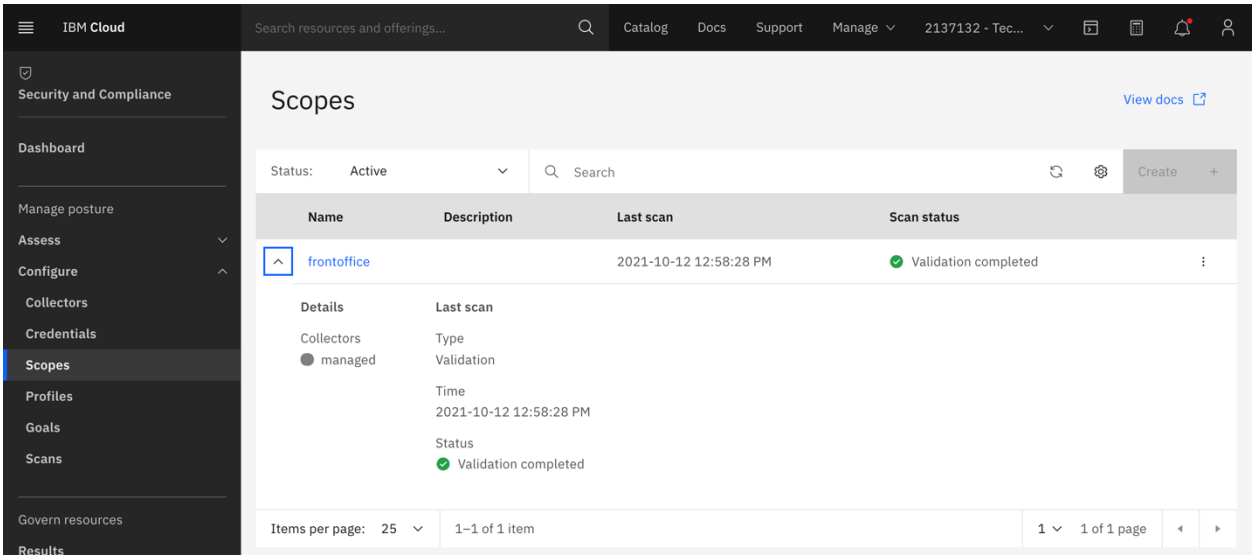
7. The dashboard gives an overview of all the current security posture and results of the threat detection. Let’s start by looking at how to manage the Security Posture.

Manage posture - Configure

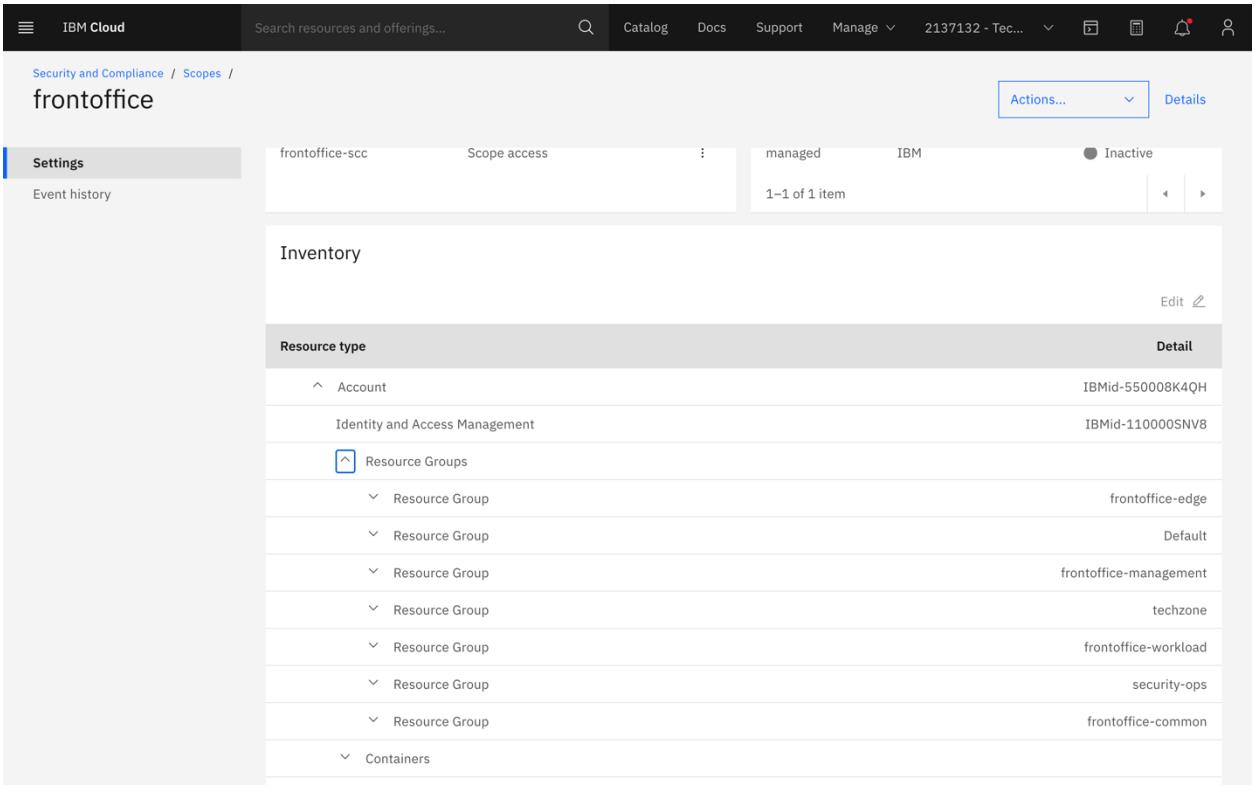
1. Click on “Configure” → “Collectors” under the “Manage Posture” section on the left menu.



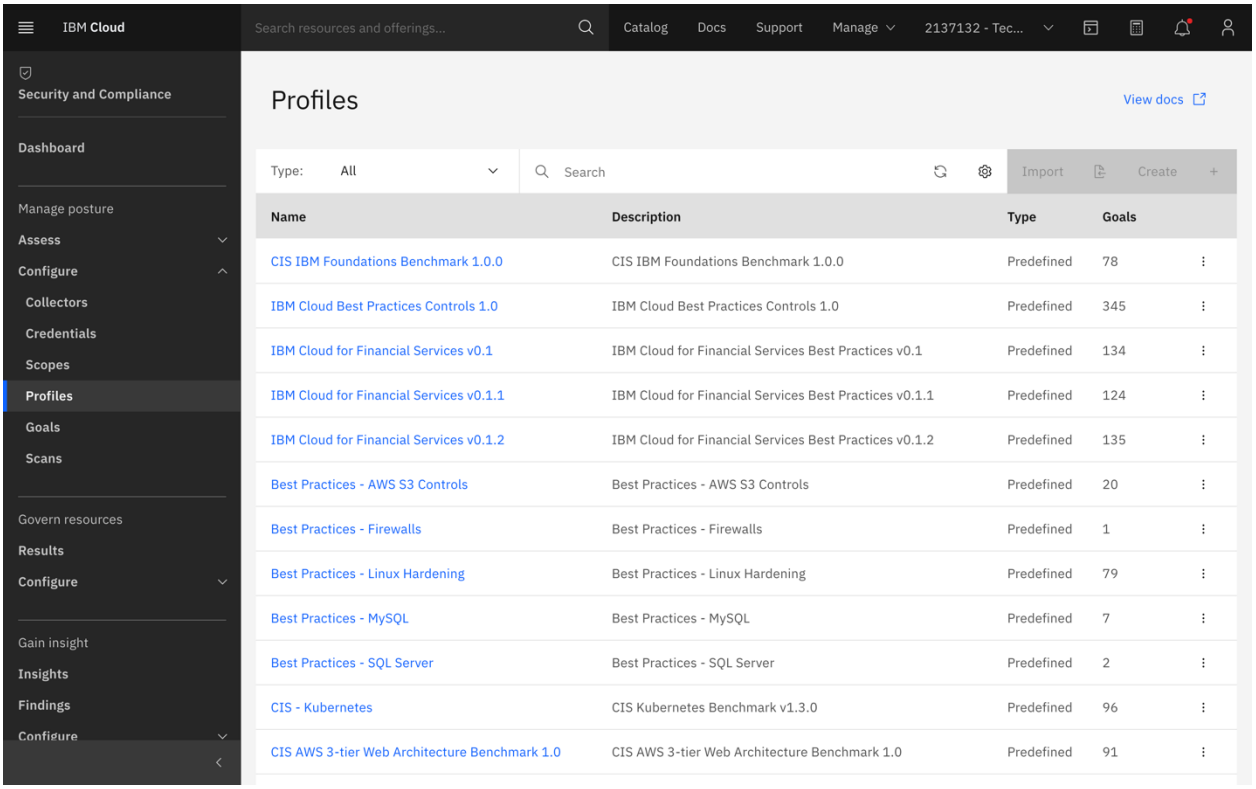
2. Before a scan can be run, a collector must be deployed. In this case, we have a provisioned an IBM-managed collector into the account and provided it with an API key that has the required permission to scan the resources within the account.
3. Click on “Configure” → “Scopes” under the “Manage Posture”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



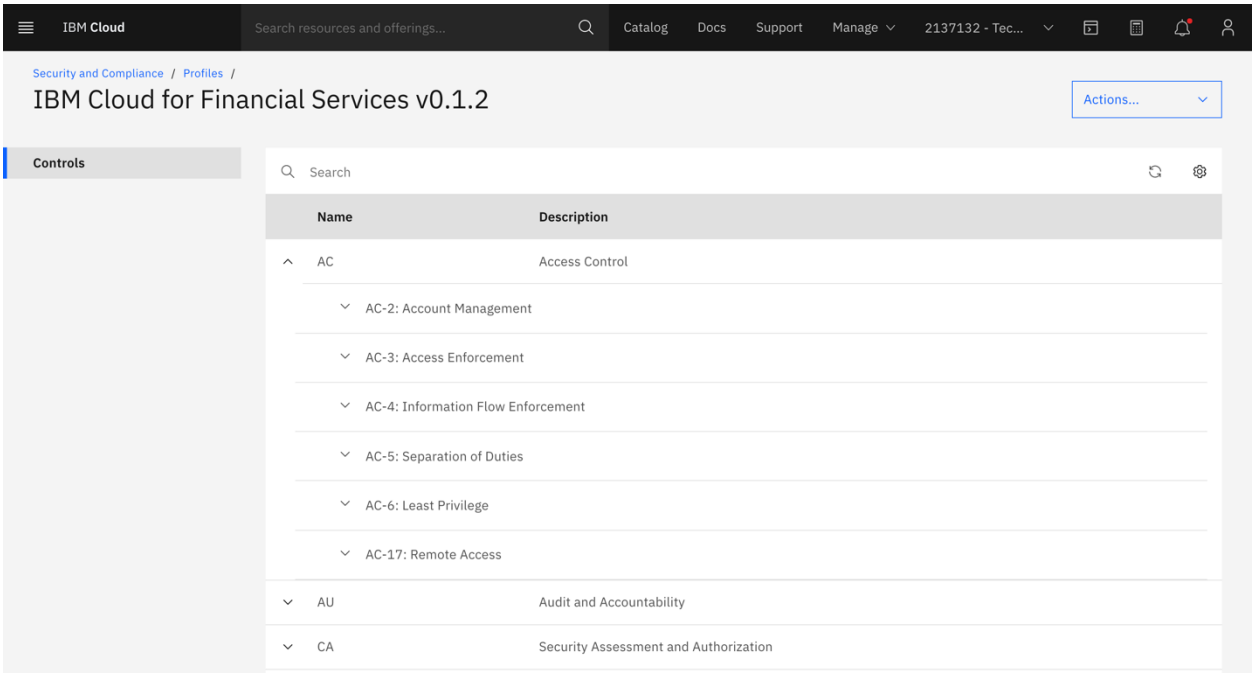
4. The next step is to define a scope. When the scope is created it is given a name and assigned a collector. The scope will then use the collector to discover the services available within the account.
5. Click on the name of the “frontoffice” scope to see the details.



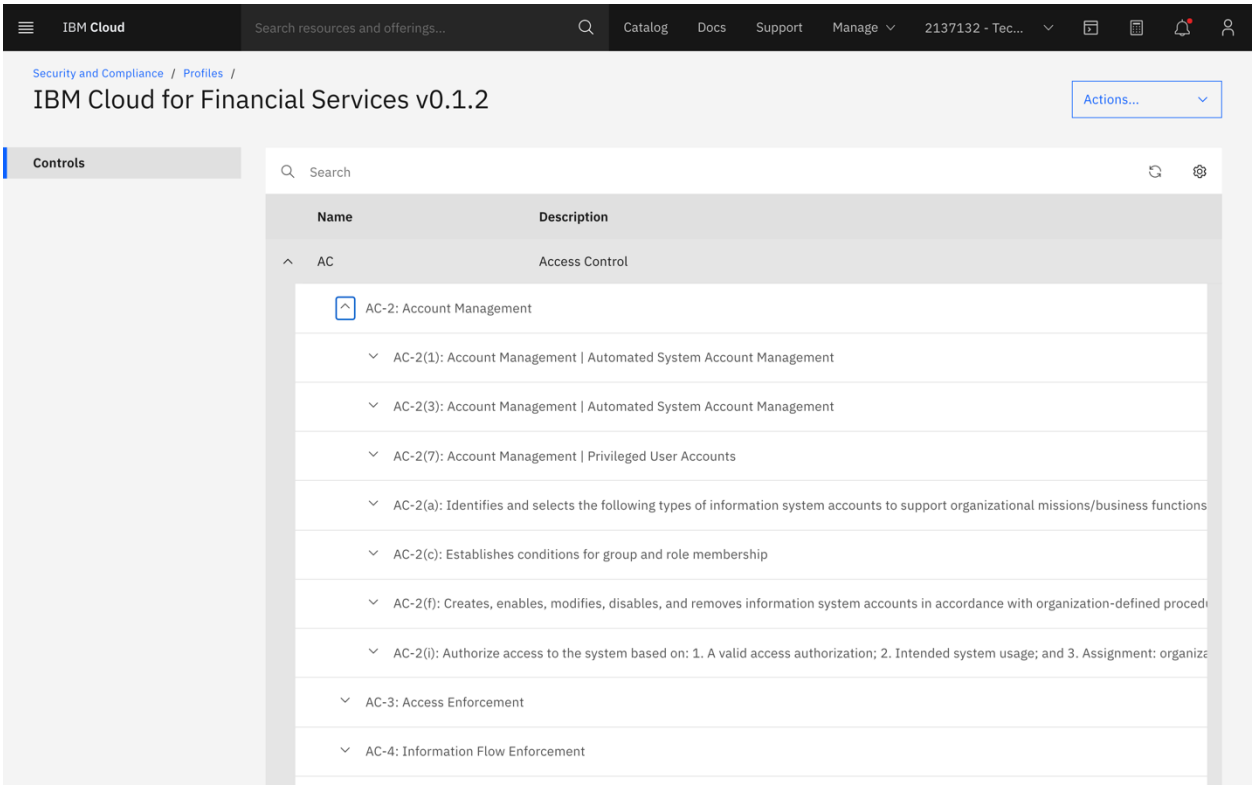
6. After the discovery scan runs, the inventory of resources are listed. At this point, if desired the list of resources can be pruned for this particular scope to include only a subset of the resources are included in the scan.
7. Click on “Configure” → “Profiles” under the “Manage Posture” section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



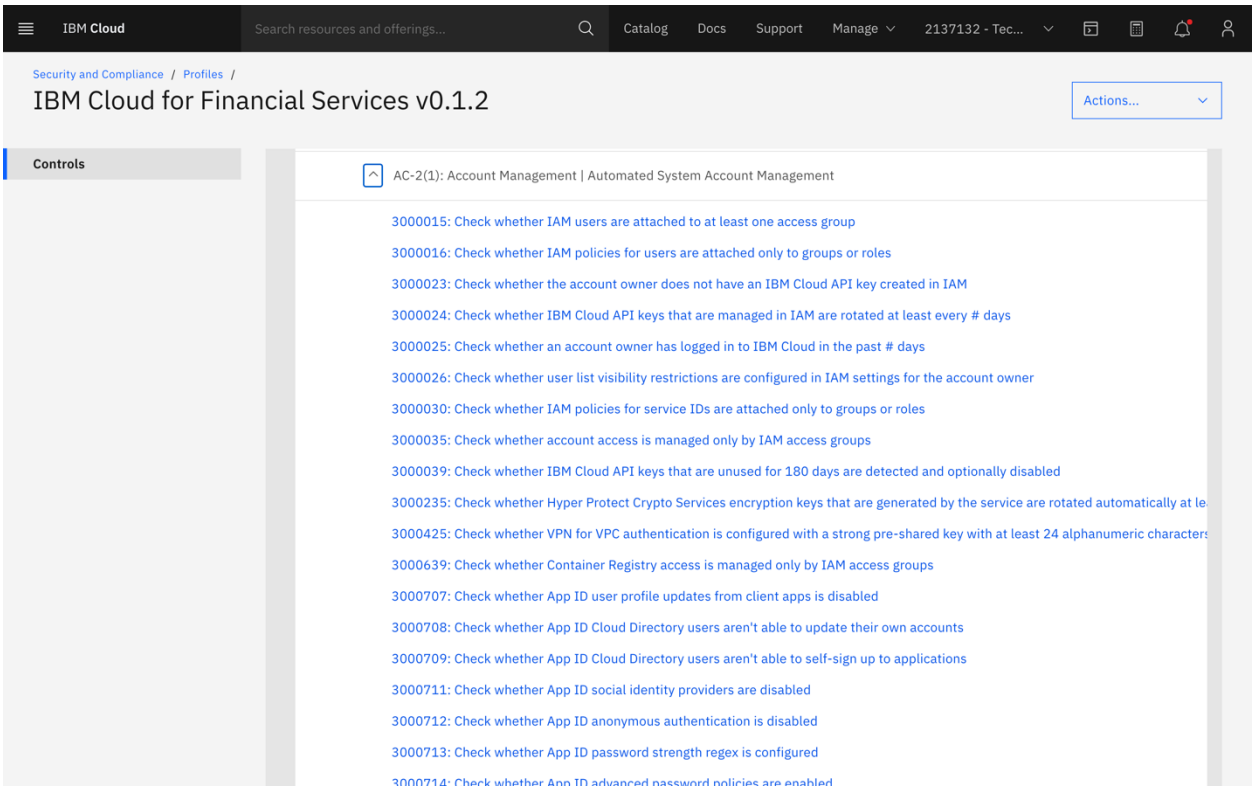
8. The next step is to determine the controls that will be evaluated against the scope to determine the current posture. The controls are grouped into Profiles. A number of profiles have been provided out of the box and custom profiles can be created to define a particular collection of controls.
9. 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.



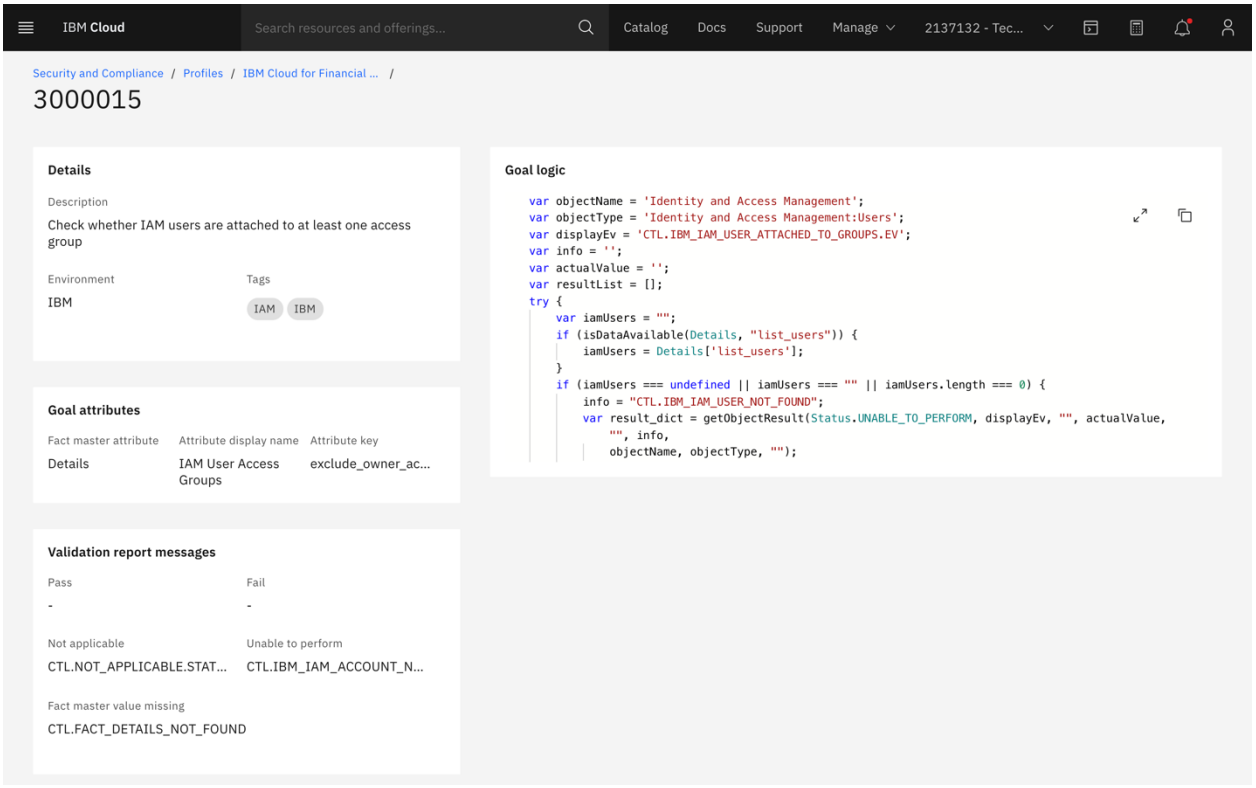
12. Within the control family a number of controls have been defined. The ‘AC’ control family defines the controls related to Access Control in the environment.
13. Expand the “AC-2” control.



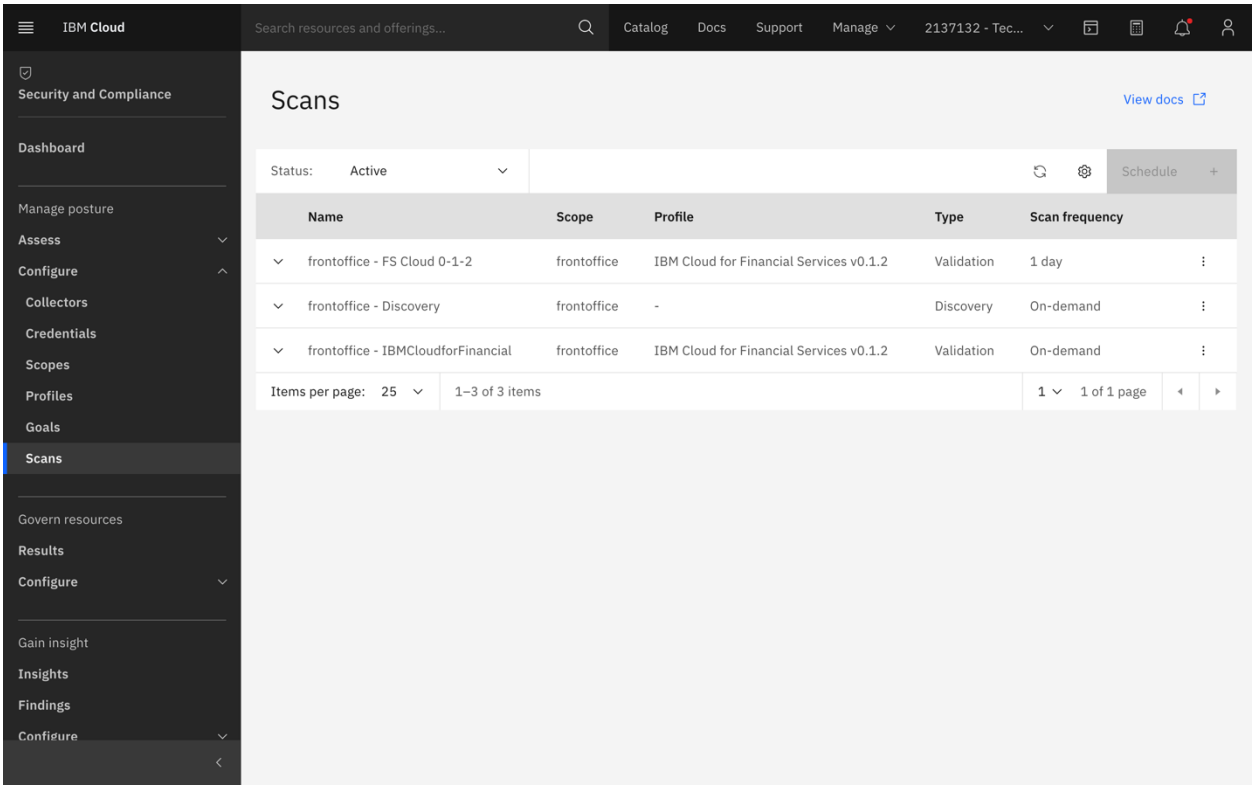
14. In this case, the ‘AC-2’ control is broken down into sub-parts.
15. Expand the “AC-2(1)” control.



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.



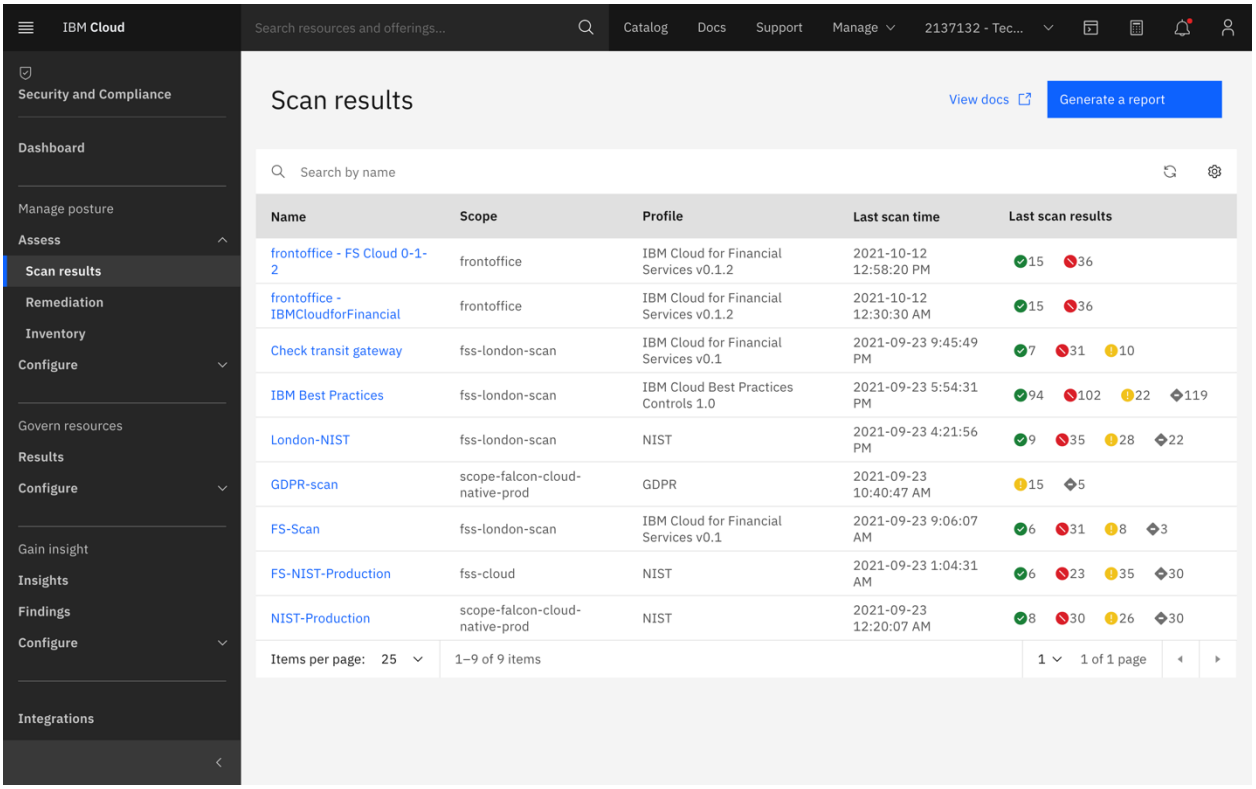
18. From this view we can see the details for the goal including the logic used to determine compliance.
19. Return to the main page of the Security and Compliance Center - https://cloud.ibm.com/security-compliance/overview . Click on “Configure” → “Scans” under the “Manage Posture” section on the left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



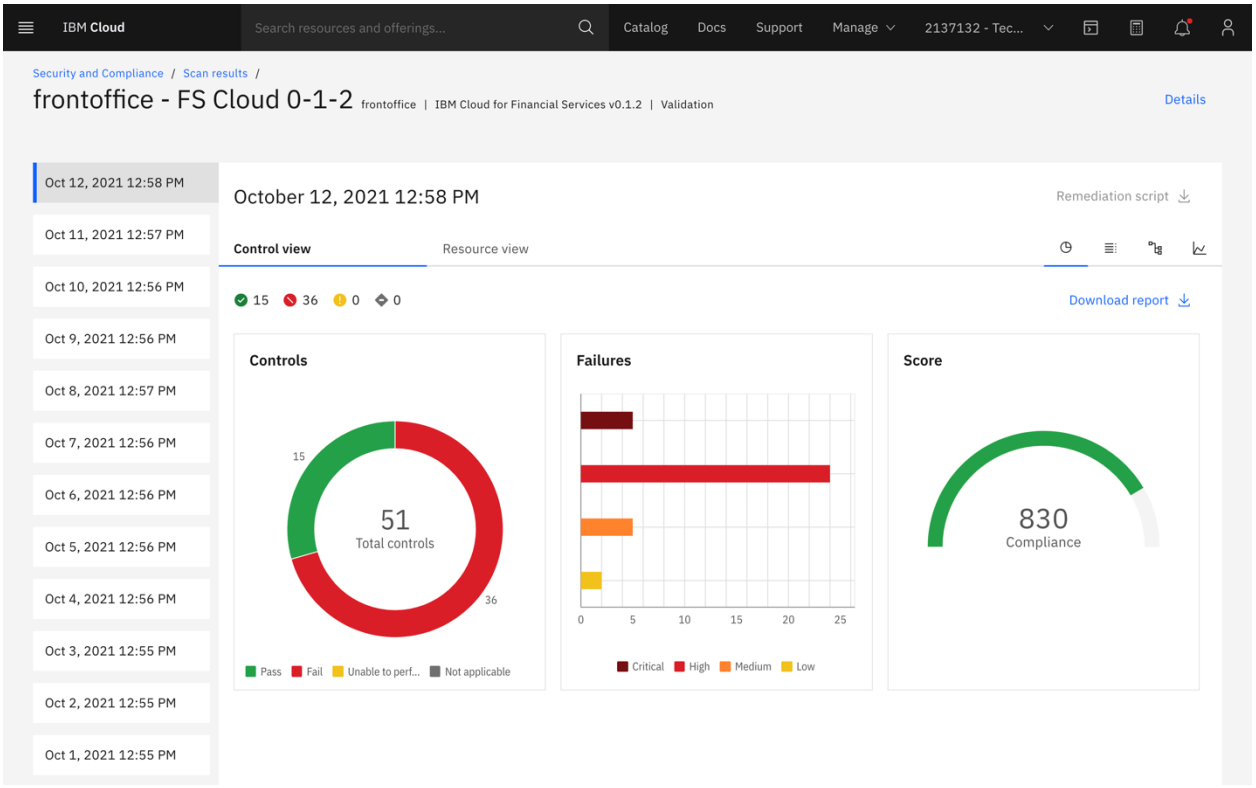
20. The last part of the configuration is to set up a scheduled scan. Here we've set up a scan that will run every day using the 'IBM Cloud for Financial Services v0.1.4' profile. It is also possible to run a scan on-demand against a particular profile.
21. Return to the Security and Compliance Center 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.



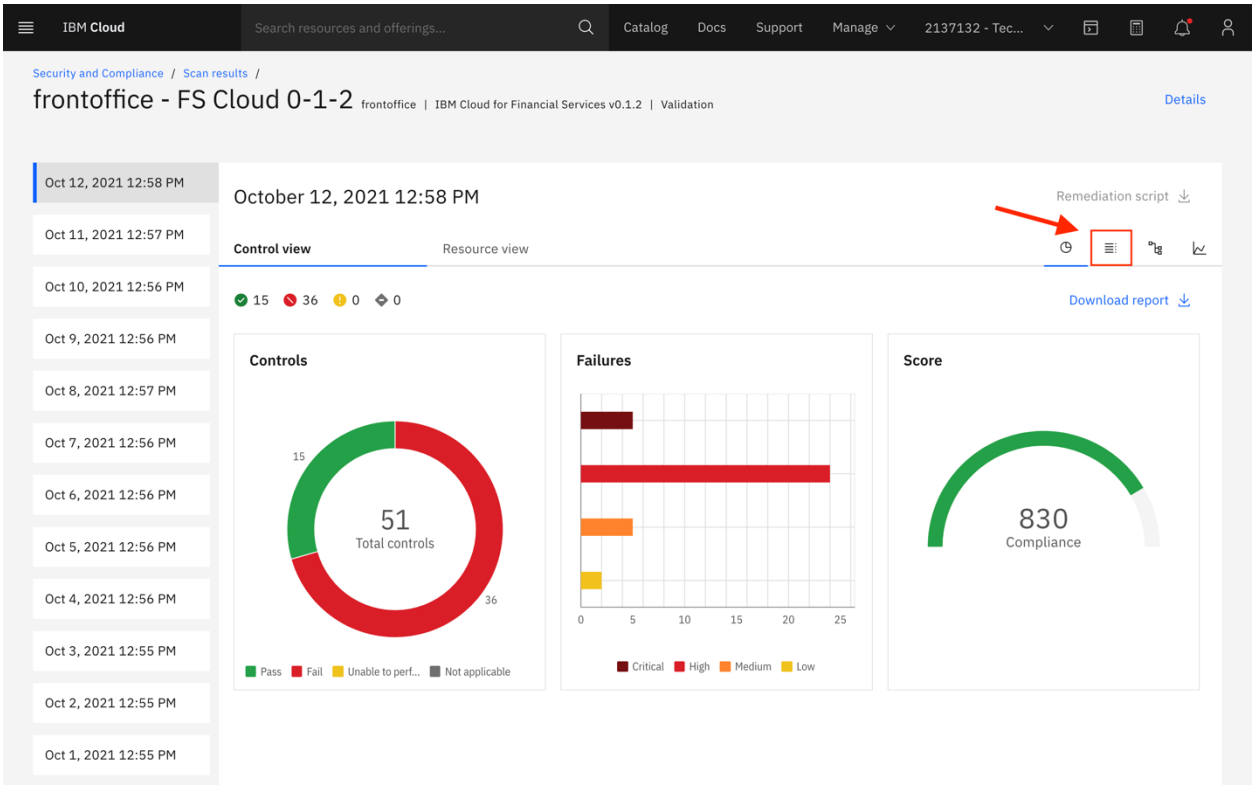
2. The results of the on-demand and scheduled scans against the defined scopes are all listed here. We can look at the results of the scan for our ‘frontoffice’ scope.
3. Click on the “frontoffice - FS Cloud 0-1-2” result.

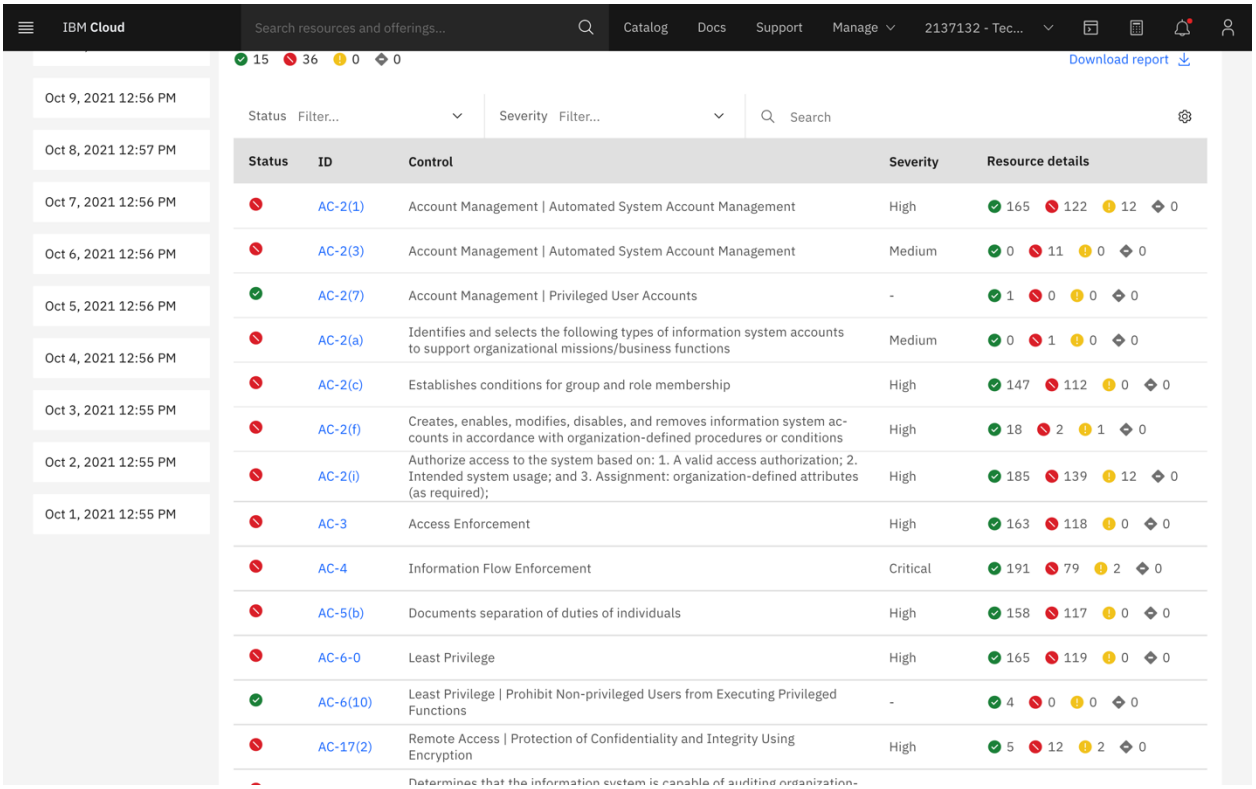


4. The initial view for the scan results shows the graphs for the Control view. Before getting into the specific results, it is important to understand what the values do and do not mean. The controls are measured by goals and if any one of the goals fail then the control fails. Often the same goal will 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.

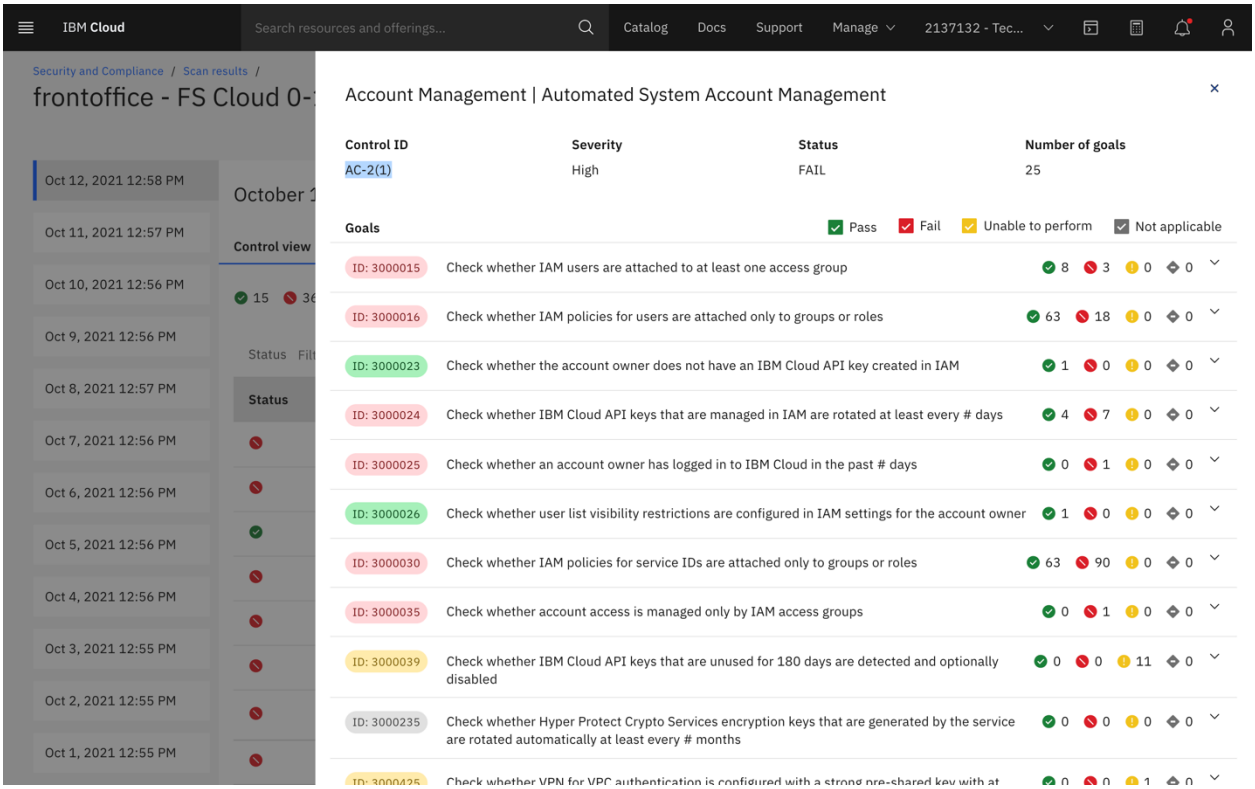
In this account, to accommodate the demo environment there are a couple of known exceptions to the FS controls. For example: some of the network ACLs are opened to allow VPN traffic and public gateways are attached to the OpenShift cluster subnets to allow access to external repositories.

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.

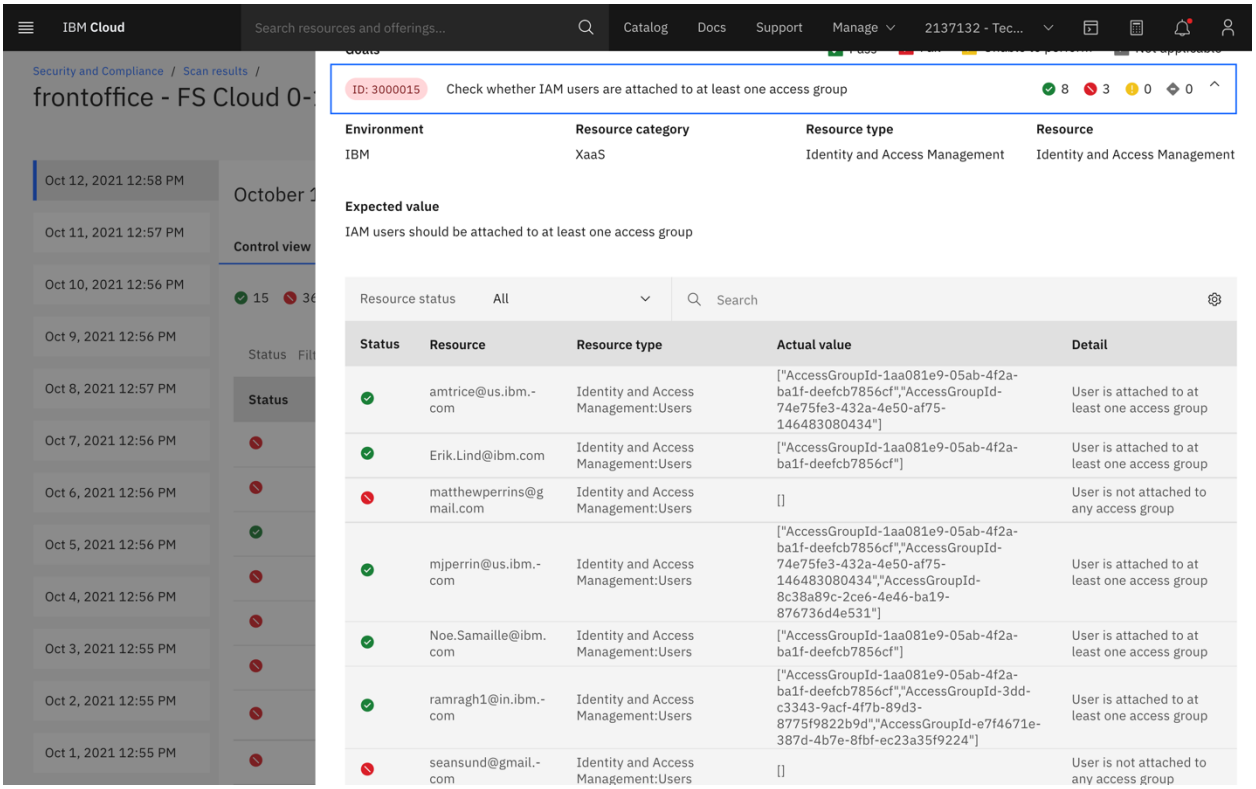

IBM Cloud
Search resources and offerings...
Catalog
Docs
Support
Manage
2137132 - Tec...
Security and Compliance / Scan results /
frontoffice - FS Cloud 0-1-2 frontoffice | IBM Cloud for Financial Services v0.1.2 | Validation
Details
Oct 12, 2021 12:58 PM
Oct 11, 2021 12:57 PM
Oct 10, 2021 12:56 PM
Oct 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
October 12, 2021 12:58 PM
Remediation script
Control view
Resource view
15 36 0 0
Download report
Controls
51
Total controls
15
36
Pass
Fail
Unable to perf...
Not applicable
Failures
0 5 10 15 20 25
Critical
High
Medium
Low
Score
830
Compliance


IBM Cloud
Search resources and offerings...
Catalog
Docs
Support
Manage
2137132 - Tec...
15 36 0 0
Download report
Status Filter...
Severity Filter...
Search
Status
ID
Control
Severity
Resource details
AC-2(1) Account Management | Automated System Account Management High 165 122 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 147 112 0 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) 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
AC-3 Access Enforcement High 163 118 0 0
AC-4 Information Flow Enforcement Critical 191 79 2 0
AC-5(b) Documents separation of duties of individuals High 158 117 0 0
AC-6-0 Least Privilege High 165 119 0 0
AC-6(10) Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions - 4 0 0 0
AC-17(2) Remote Access | Protection of Confidentiality and Integrity Using Encryption High 5 12 2 0

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.

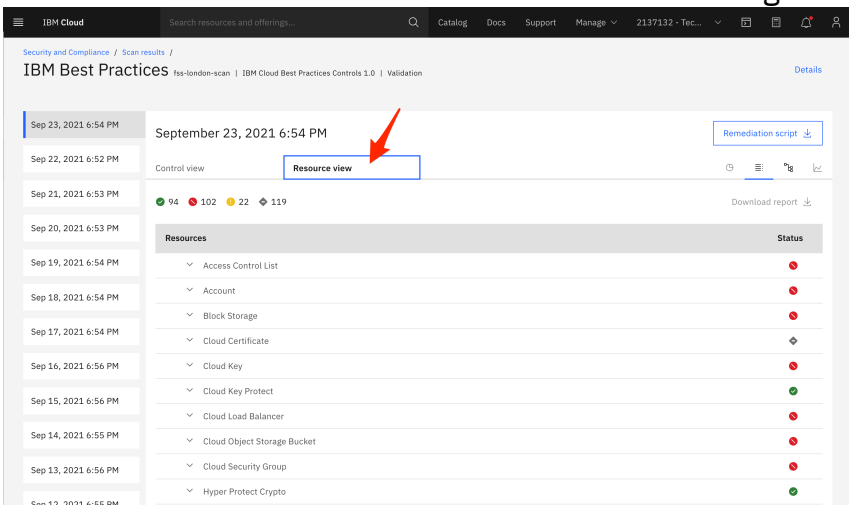


9. This view shows the goals associated with this control and the current state. We can look at the details of a goal to see the values that are causing the failure.
10. Click on goal “3000015”.

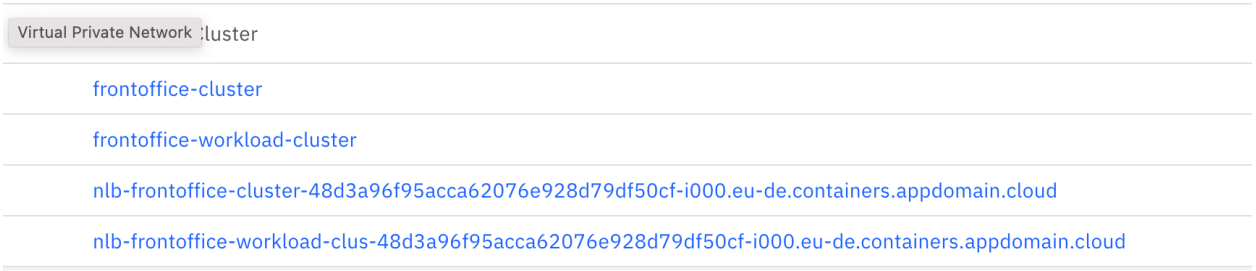


11. Goal 3000015 requires that every user is attached to an access group. The results show all of the users in the account and which ones are missing access groups.

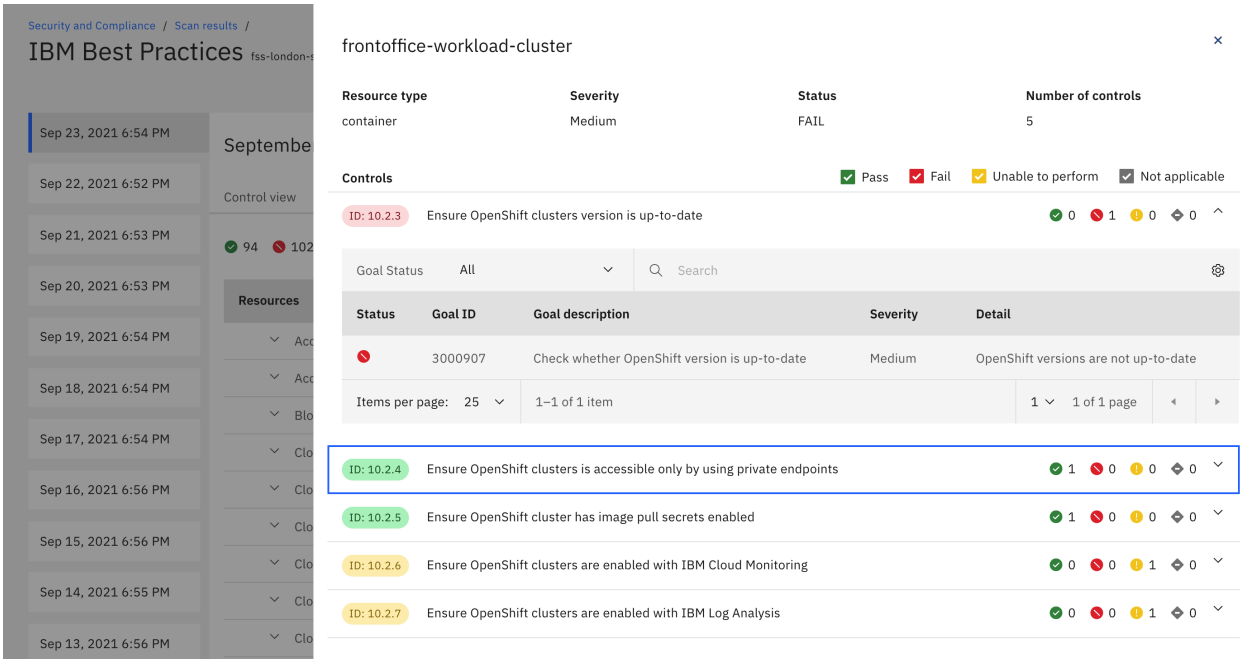
12. Click on the “Resource view” to list the resource categories.



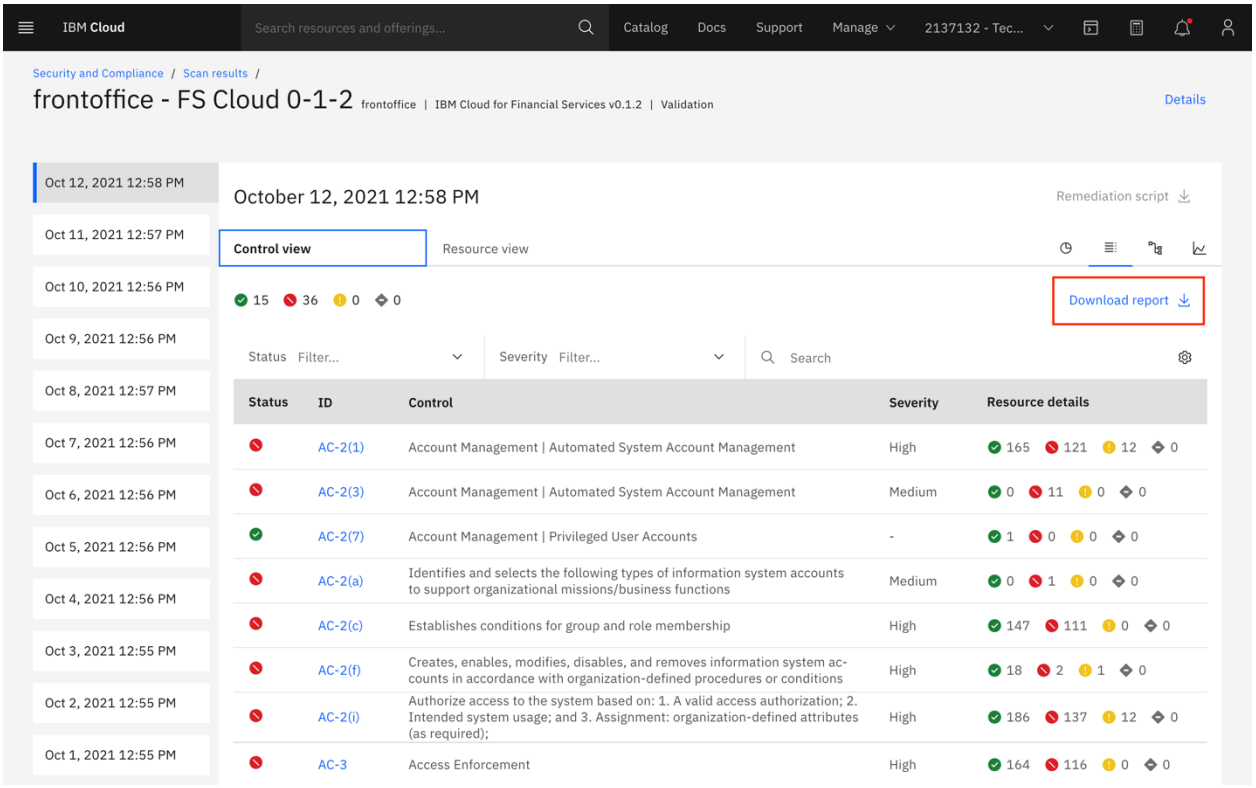
13. Expand the “OpenShift Cluster” item

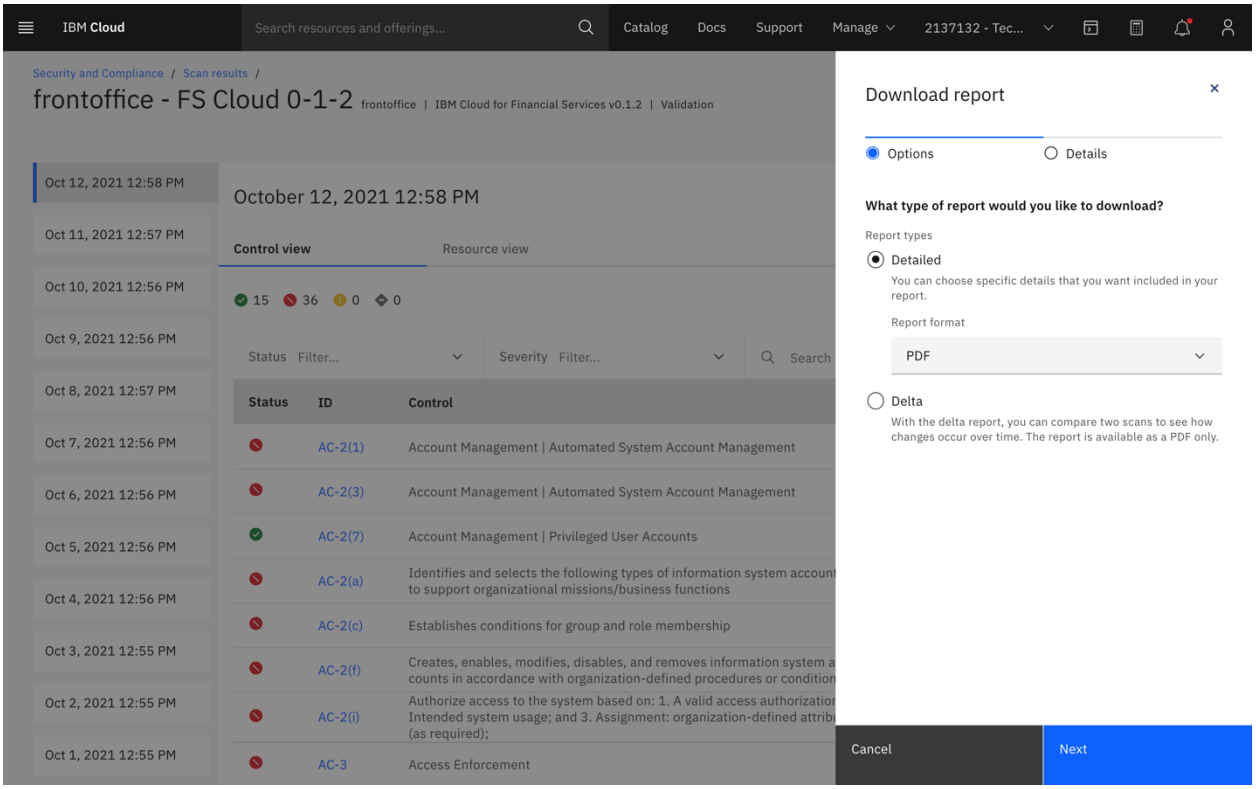


14. Click on the “frontoffice-workload-cluster” item, to see the controls that are scanned for this specific cluster and see the pass/fail status for each of the controls. Click on any of the controls to see details about that specific scan item.

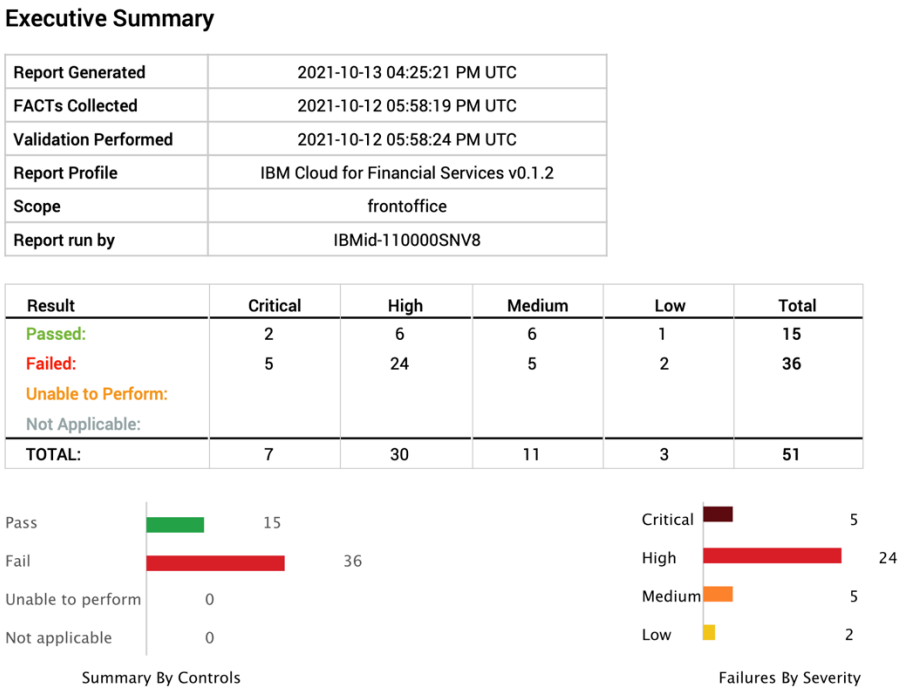


15. Click on the “Control view” tab again then click on “Download report”.


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
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
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
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 0 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) 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
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

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



Executive Summary

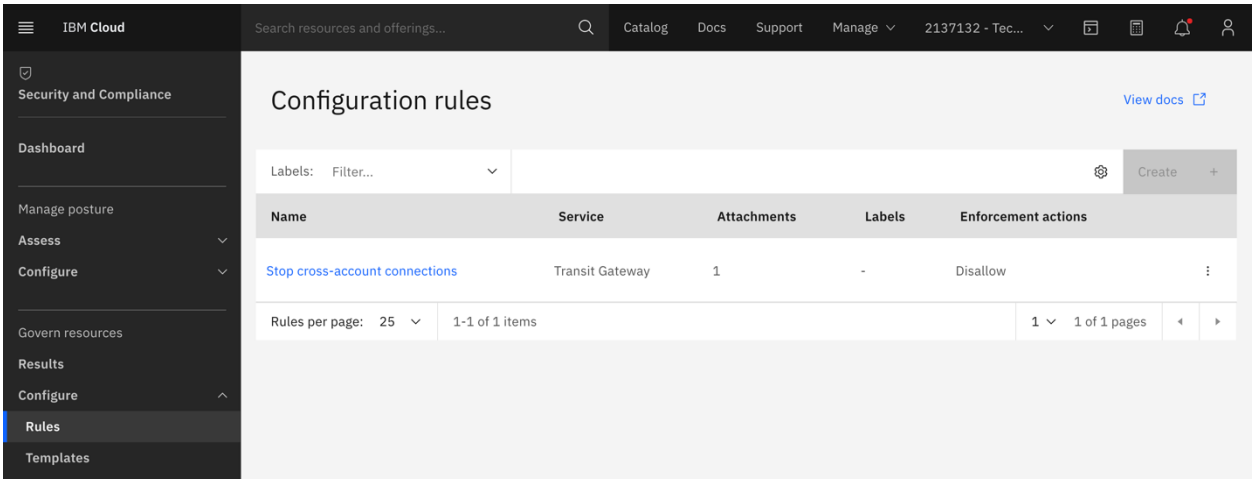
Report Generated	2021-10-13 04:25:21 PM UTC
FACTs Collected	2021-10-12 05:58:19 PM UTC
Validation Performed	2021-10-12 05:58:24 PM UTC
Report Profile	IBM Cloud for Financial Services v0.1.2
Scope	frontoffice
Report run by	IBMid-110000SNV8

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**

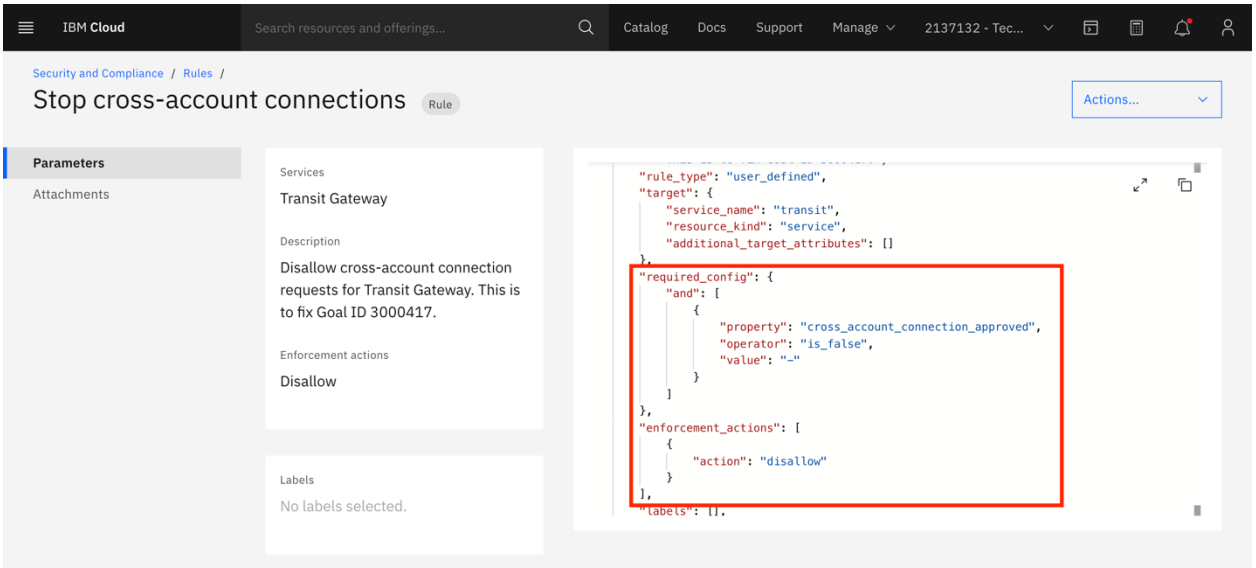
17. Return to the Security and Compliance Center overview page - https://cloud.ibm.com/security-compliance/overview

Govern resources

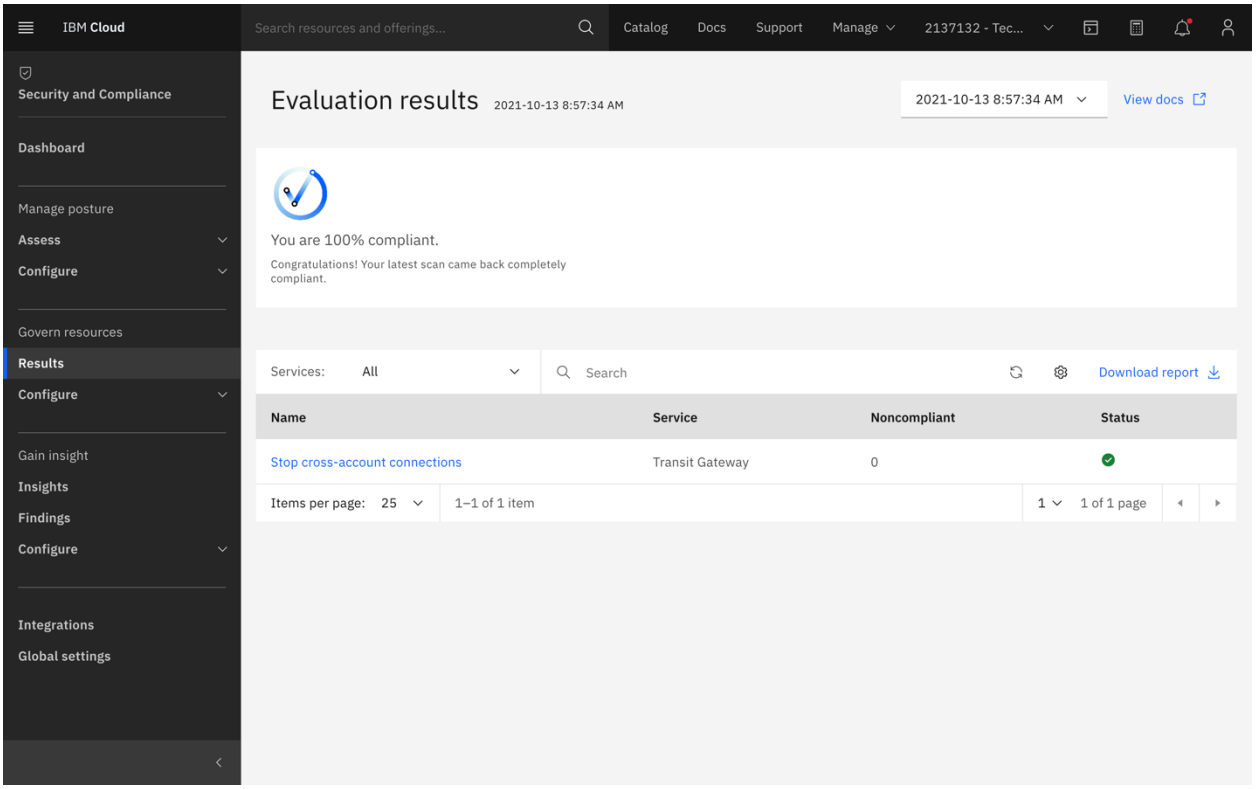
1. The Security and Compliance Center allows rules to define the constraints that should be placed on resources that are provisioned in the account.
2. Click on “Configure” → “Rules” under the “Govern resources” section on the left menu.



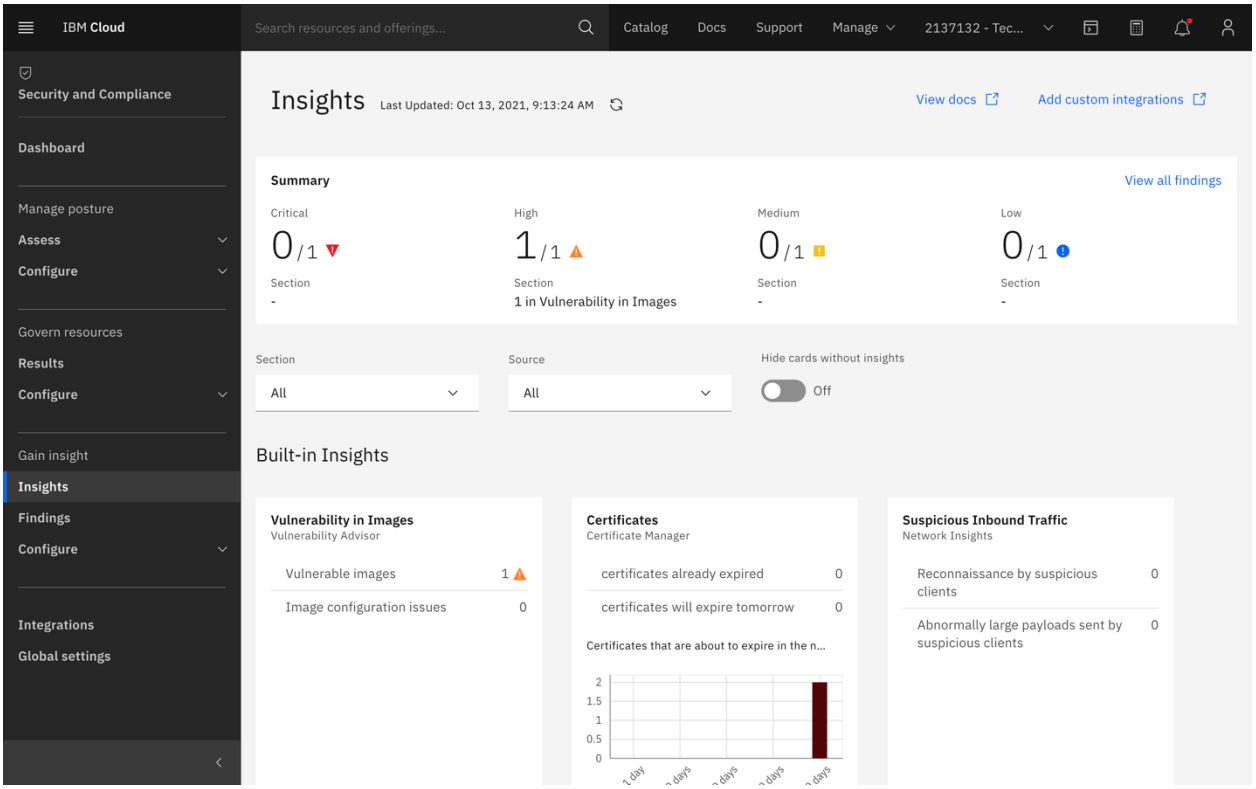
3. This page lists the rules that have been configured for this account.
4. Click on the “Stop cross-account connections” rule to see the details.



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.



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.



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