aws marketplace

In cooperation with CYBRARY

Barracuda®

Getting Started Guide:

Barracuda Cloud Security Guardian in AWS

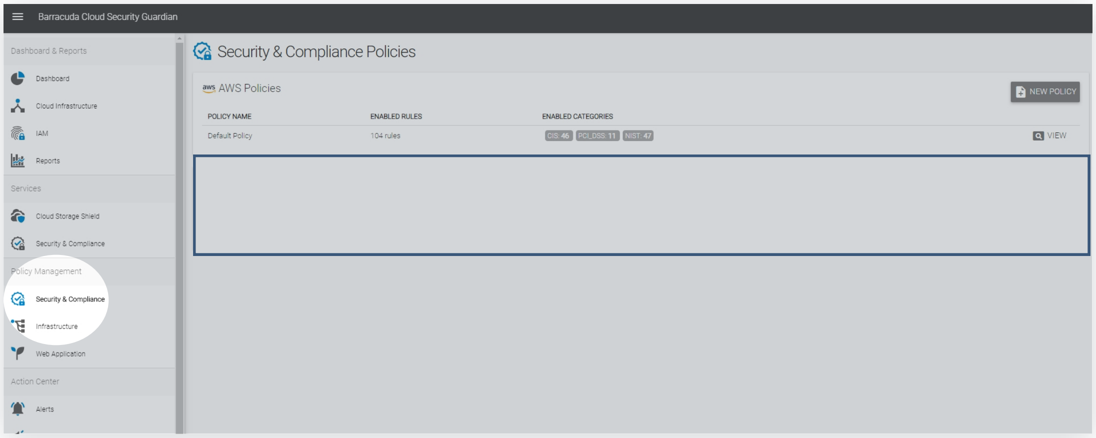
The **Barracuda Cloud Security** Guardian in AWS solution runs on AWS and offers the following key benefits:

- **Discovery and Visualization**
- **Policy Definition**
- **Compliance Assessment**
- **Control Implementation**
- **Automated Remediation**

Create a New Policy in Barracuda Cloud Security Guardian

Step 1 Log into the Barracuda Cloud Security Guardian dashboard (if not already logged in).

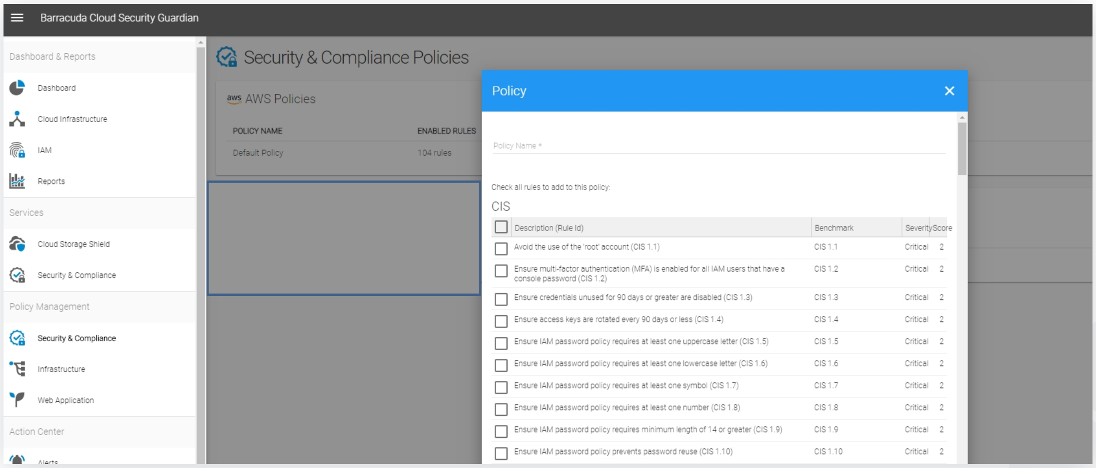
Step 2 On the left-side, select the **Security & Compliance** option, located under the Policy Management area.



POLICY NAME	ENABLED RULES	ENABLED CATEGORIES	
Default Policy	104 rules	CIS: 46 PCI_DSS: 11 NIST: 47	VIEW

Step 3 Click the **New policy** button.

Step 4 Complete the Policy Name field.



Policy Name *

Check all rules to add to this policy:

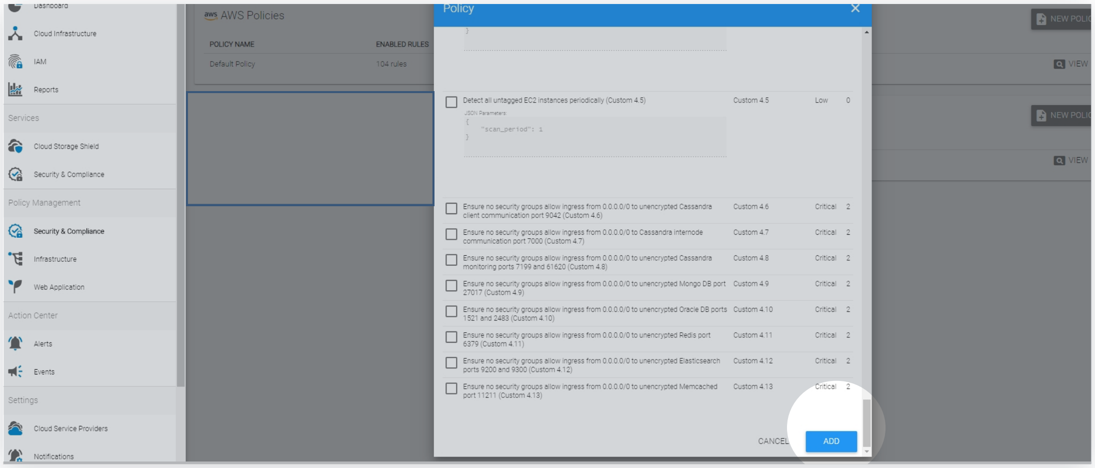
CIS

□	Description (Rule Id)	Benchmark	Severity	Score
□	Avoid the use of the 'root' account (CIS 1.1)	CIS 1.1	Critical	2
□	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (CIS 1.2)	CIS 1.2	Critical	2
□	Ensure credentials unused for 90 days or greater are disabled (CIS 1.3)	CIS 1.3	Critical	2
□	Ensure access keys are rotated every 90 days or less (CIS 1.4)	CIS 1.4	Critical	2
□	Ensure IAM password policy requires at least one uppercase letter (CIS 1.5)	CIS 1.5	Critical	2
□	Ensure IAM password policy requires at least one lowercase letter (CIS 1.6)	CIS 1.6	Critical	2
□	Ensure IAM password policy requires at least one symbol (CIS 1.7)	CIS 1.7	Critical	2
□	Ensure IAM password policy requires at least one number (CIS 1.8)	CIS 1.8	Critical	2
□	Ensure IAM password policy requires minimum length of 14 or greater (CIS 1.9)	CIS 1.9	Critical	2
□	Ensure IAM password policy prevents password reuse (CIS 1.10)	CIS 1.10	Critical	2

Steps 5-7 of 14

Step 5 Select the policy items you wish to add by marking the checkboxes to the left of each item.

Step 6 Once you have selected all policy items that you want, click the **Add** button at the bottom of the pop-up window to save the new policy.

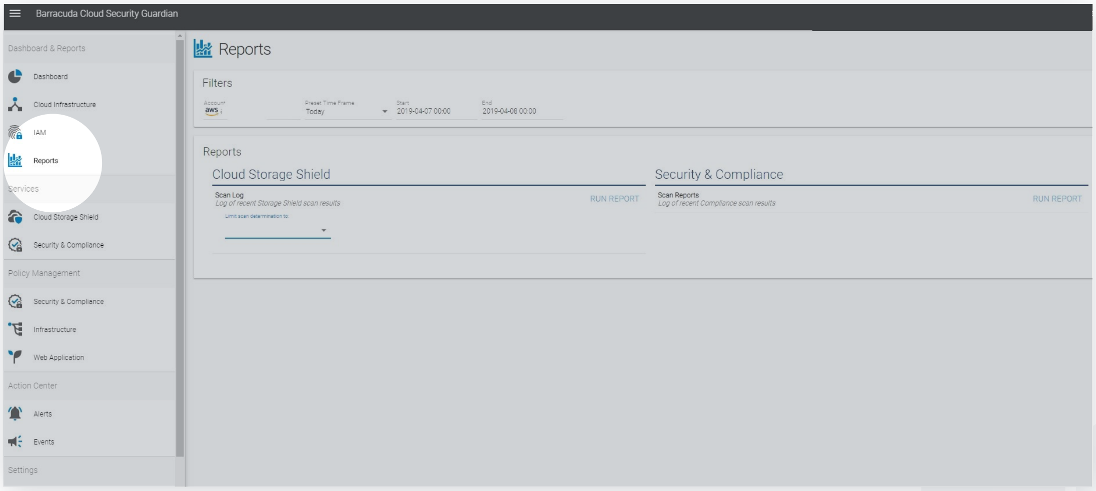


□ Detect all untagged EC2 instances periodically (Custom 4.5)	Custom 4.5	Low	0
□ Ensure no security groups allow ingress from 0.0.0.0/0 to unencrypted Cassandra client communication port 9042 (Custom 4.6)	Custom 4.6	Critical	2
□ Ensure no security groups allow ingress from 0.0.0.0/0 to Cassandra internode communication port 7000 (Custom 4.7)	Custom 4.7	Critical	2
□ Ensure no security groups allow ingress from 0.0.0.0/0 to unencrypted Cassandra monitoring ports 7199 and 61620 (Custom 4.8)	Custom 4.8	Critical	2
□ Ensure no security groups allow ingress from 0.0.0.0/0 to unencrypted Mongo DB port 27017 (Custom 4.9)	Custom 4.9	Critical	2
□ Ensure no security groups allow ingress from 0.0.0.0/0 to unencrypted Oracle DB ports 1521 and 2483 (Custom 4.10)	Custom 4.10	Critical	2
□ Ensure no security groups allow ingress from 0.0.0.0/0 to unencrypted Redis port 6379 (Custom 4.11)	Custom 4.11	Critical	2
□ Ensure no security groups allow ingress from 0.0.0.0/0 to unencrypted Elasticsearch ports 9200 and 9300 (Custom 4.12)	Custom 4.12	Critical	2
□ Ensure no security groups allow ingress from 0.0.0.0/0 to unencrypted Memcached port 11211 (Custom 4.13)	Custom 4.13	Critical	2

JSON Parameters:

```
{
    "scan_period": 1
}
```

Step 7 Next, click on **Reports** on the left-side of the dashboard.



Account: aws

Preset Time Frame: Today

Start: 2019-04-07 00:00

End: 2019-04-08 00:00

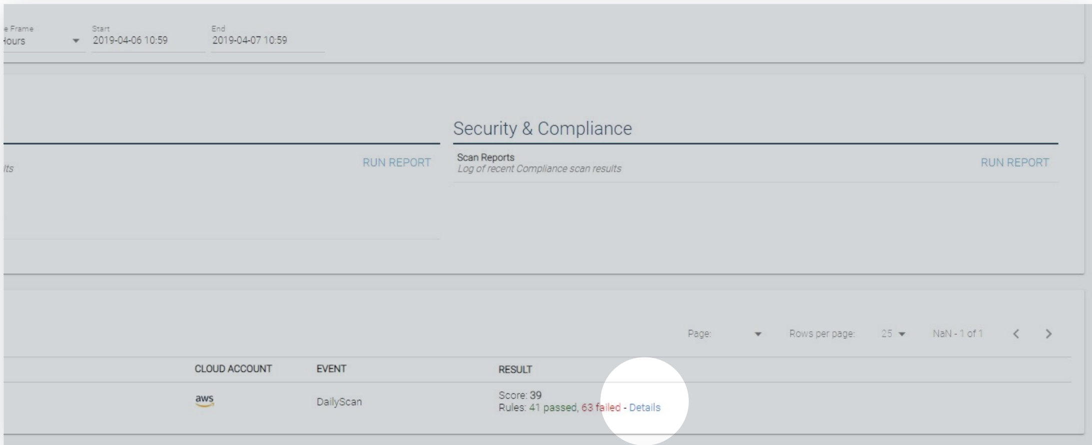
Scan Log
Log of recent Storage Shield scan results

Scan Reports
Log of recent Compliance scan results

Steps 8-11 of 14

Step 8 Select Security & Compliance and then Run Report.

Step 9 Next, click the **Details** option to view the results of the scan.



Start 2019-04-06 10:59

End 2019-04-07 10:59

Security & Compliance

Scan Reports
Log of recent Compliance scan results

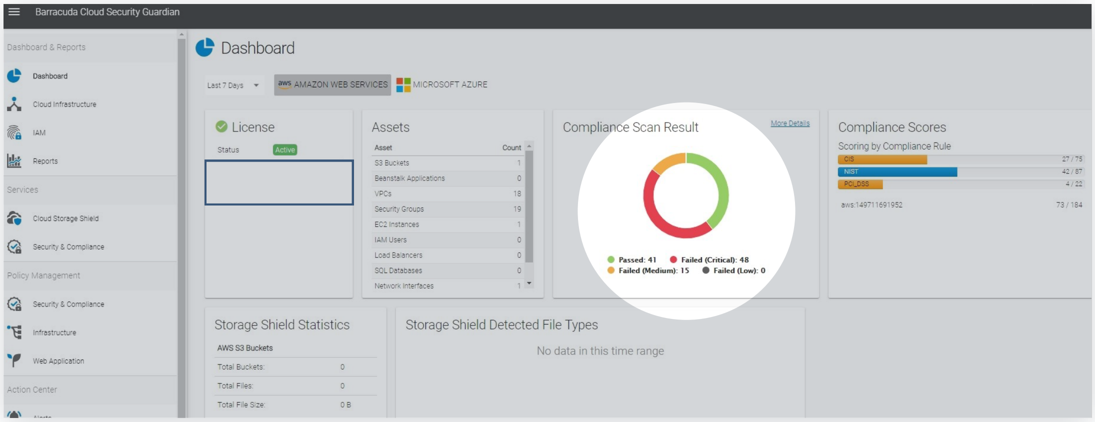
CLOUD ACCOUNT	EVENT	RESULT
aws	DailyScan	Score: 39 Rules: 41 passed, 63 failed - Details

Step 10 Now we want to fix some of the issues.

Step 11 Click back on the **Dashboard** option on the left-side menu.

Steps 12-14 of 14

Step 12 On the Dashboard screen, you should see data under the Compliance Scan Result area. If you do not, you may need to change the filter for the time range.



License

Status: Active

Assets

Asset	Count
S3 Buckets	1
Beanstalk Applications	0
VPCs	18
Security Groups	19
EC2 Instances	1
IAM Users	0
Load Balancers	0
SQL Databases	0
Network Interfaces	1

Compliance Scan Result

● Passed: 41 ● Failed (Critical): 48
● Failed (Medium): 15 ● Failed (Low): 0

Compliance Scores

Scoring by Compliance Rule

CIS	27 / 75
NIST	42 / 87
PCI_DSS	4 / 22
aws:149711691952	73 / 184

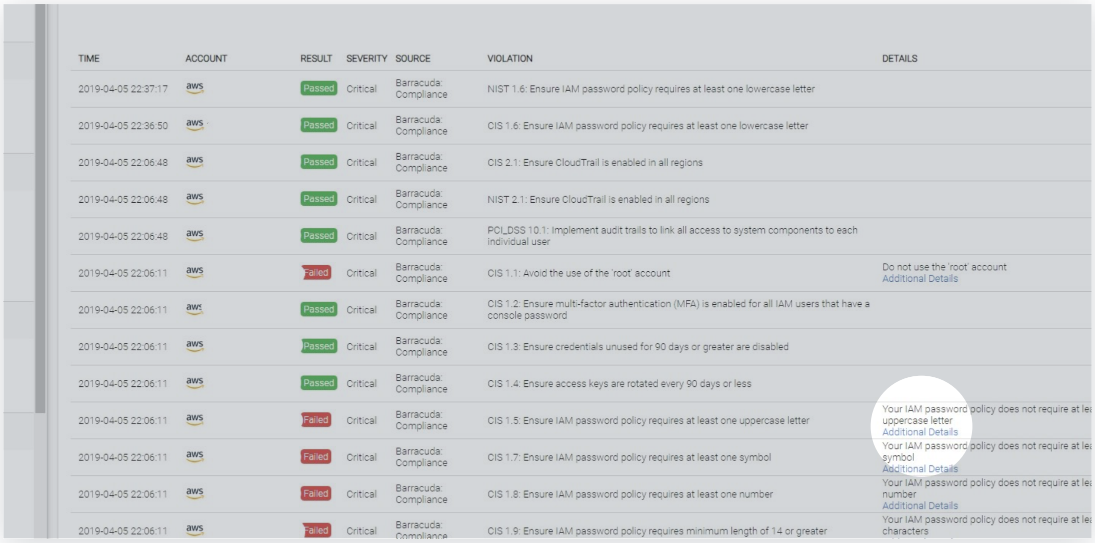
Storage Shield Statistics

AWS S3 Buckets	
Total Buckets:	0
Total Files:	0
Total File Size:	0 B

Storage Shield Detected File Types

No data in this time range

Step 13 Click the **More Details** option.



TIME	ACCOUNT	RESULT	SEVERITY	SOURCE	VIOLATION	DETAILS
2019-04-05 22:37:17	aws	Passed	Critical	Barracuda: Compliance	NIST 1.6: Ensure IAM password policy requires at least one lowercase letter	
2019-04-05 22:36:50	aws	Passed	Critical	Barracuda: Compliance	CIS 1.6: Ensure IAM password policy requires at least one lowercase letter	
2019-04-05 22:06:48	aws	Passed	Critical	Barracuda: Compliance	CIS 2.1: Ensure CloudTrail is enabled in all regions	
2019-04-05 22:06:48	aws	Passed	Critical	Barracuda: Compliance	NIST 2.1: Ensure CloudTrail is enabled in all regions	
2019-04-05 22:06:48	aws	Passed	Critical	Barracuda: Compliance	PCI_DSS 10.1: Implement audit trails to link all access to system components to each individual user	
2019-04-05 22:06:11	aws	Failed	Critical	Barracuda: Compliance	CIS 1.1: Avoid the use of the 'root' account	Do not use the 'root' account Additional Details
2019-04-05 22:06:11	aws	Passed	Critical	Barracuda: Compliance	CIS 1.2: Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	
2019-04-05 22:06:11	aws	Passed	Critical	Barracuda: Compliance	CIS 1.3: Ensure credentials unused for 90 days or greater are disabled	
2019-04-05 22:06:11	aws	Passed	Critical	Barracuda: Compliance	CIS 1.4: Ensure access keys are rotated every 90 days or less	
2019-04-05 22:06:11	aws	Failed	Critical	Barracuda: Compliance	CIS 1.5: Ensure IAM password policy requires at least one uppercase letter	Your IAM password policy does not require at lea uppercase letter Additional Details
2019-04-05 22:06:11	aws	Failed	Critical	Barracuda: Compliance	CIS 1.7: Ensure IAM password policy requires at least one symbol	Your IAM password policy does not require at lea symbol Additional Details
2019-04-05 22:06:11	aws	Failed	Critical	Barracuda: Compliance	CIS 1.8: Ensure IAM password policy requires at least one number	Your IAM password policy does not require at lea number Additional Details
2019-04-05 22:06:11	aws	Failed	Critical	Barracuda: Compliance	CIS 1.9: Ensure IAM password policy requires minimum length of 14 or greater	Your IAM password policy does not require at lea characters

Step 14 You can now review the alerts from the scan and fix any issues.

Complete

aws marketplace

In cooperation with CYBRARY

Thank you.

For more information, visit **https://amzn.to/2LUJQbE**