Solution Category: Cloud Governance
Deployment Model: SaaS outside AWS
Go Live Production Date: May, 2018
Available On Marketplace: No

About Citrix

Citrix (NASDAQ:CTXS) aims to power a world where people, organizations and things are securely connected and accessible to make the extraordinary possible. We help customers reimagine the future of work by providing the most comprehensive secure digital workspace that unifies the apps, data and services people need to be productive, and simplifies IT’s ability to adopt and manage complex cloud environments. With 2017 annual revenue of $2.82 billion, Citrix solutions are in use by more than 400,000 organizations including 99 percent of the Fortune 100 and 98 percent of the Fortune 500.

Problem Statement

Citrix operates large scale AWS deployment with over 100 AWS accounts and organizations. These accounts and subscriptions contain more than 1,000,000 configurable assets.

Citrix Cloud Security team relied on several open source frameworks to perform AWS compliance verification. Namely Cloud Custodian and Scout2. For AWS Compliance, Citrix created their in-house tool. As the cloud compliance program was maturing, certain challenges began to emerge.

- Each product division wanted to customize policies slightly to fit their risk profile
- Lack of exception handling process
- Some tools caused API throttling issues for production application during scanning
- Many compliance policies between AWS and other cloud providers were duplicate especially those that related to tagging policy.

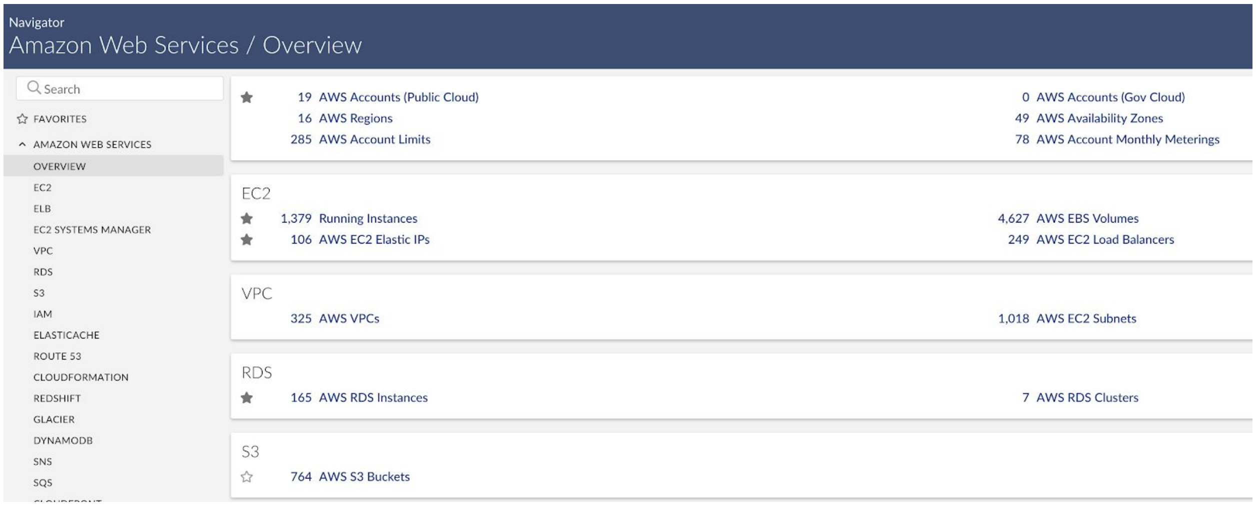
Cloudaware Modules Deployed

- Cloudaware CMDB
- Cloudaware Compliance Engine
- Cloudaware Incident Management

Solution

Cloudaware is a modular, SaaS based cloud management platform. Our CMDB uses collectors which in turn leverage AWS Config, AWS CloudTrail and service specific API calls to build complete inventory of all customer AWS infrastructure. Citrix used automatically generated CloudFormation StackSets and AWS Organizations where possible to create cross-account IAM role which allowed Cloudaware CMDB collectors to start harvesting information about current state of Citrix AWS infrastructure and populate CMDB.

In addition to supporting AWS, Cloudaware CMDB also supports other cloud providers and provides integrations for on premises infrastructure. This allowed Citrix to create a single pane of glass for all of their infrastructure regardless of where it was hosted.



Navigator
Amazon Web Services / Overview

19	AWS Accounts (Public Cloud)	0	AWS Accounts (Gov Cloud)
16	AWS Regions	49	AWS Availability Zones
285	AWS Account Limits	78	AWS Account Monthly Meterings

EC2

1,379	Running Instances	4,627	AWS EBS Volumes
106	AWS EC2 Elastic IPs	249	AWS EC2 Load Balancers

VPC

325	AWS VPCs	1,018	AWS EC2 Subnets

RDS

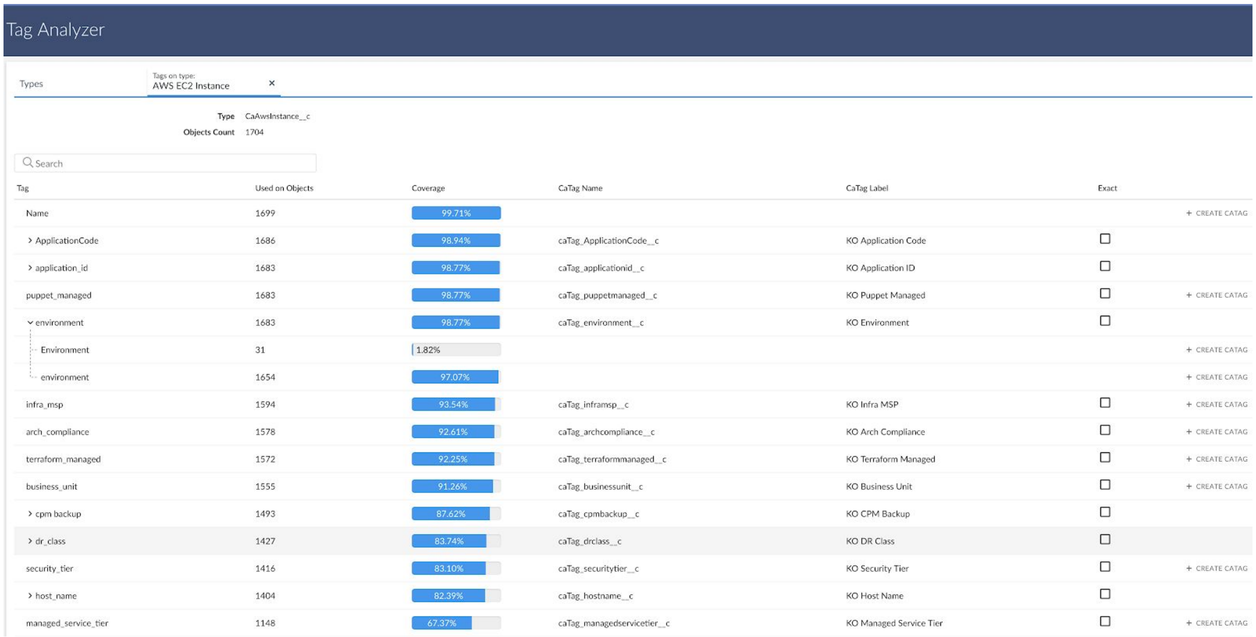
165	AWS RDS Instances	7	AWS RDS Clusters

S3

764	AWS S3 Buckets

Tagging

Particular area importance for Citrix was enforcing consistent tagging standards across their infrastructure. Using our Tag Analyzer which is part of the CMDB, Citrix was able to better understand and correct deviations in their tagging coverage.

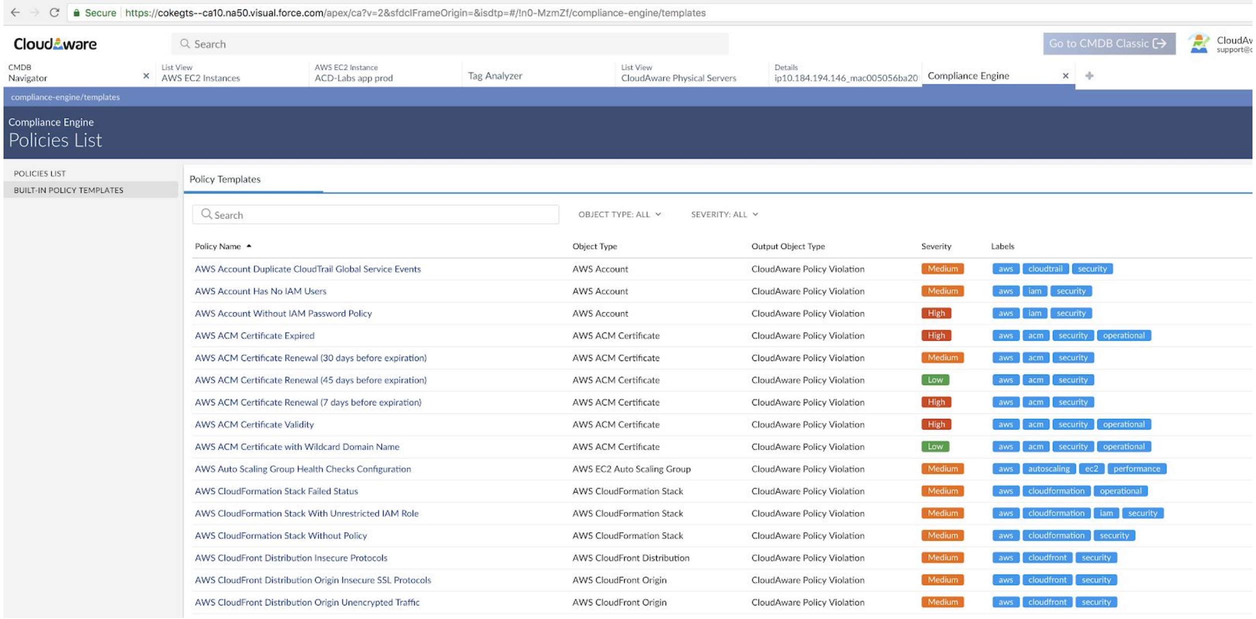


Type CaAwsInstance__c
Objects Count 1704

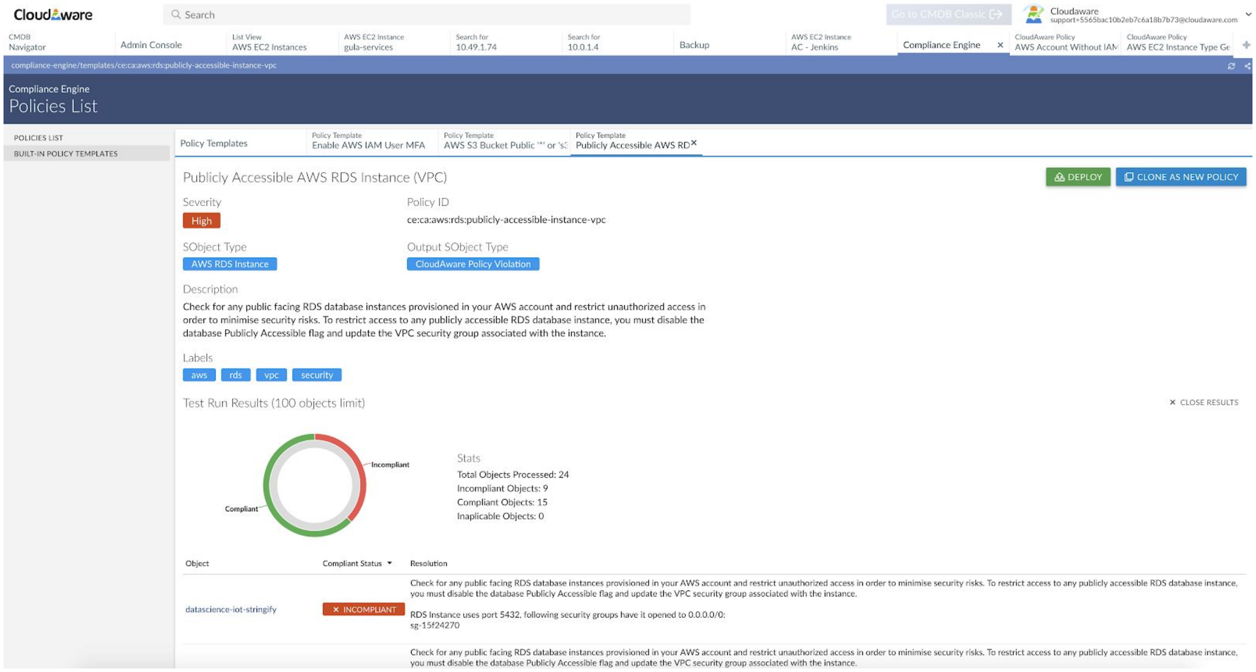
Tag	Used on Objects	Coverage	CaTag Name	CaTag Label	Exact	
Name	1699	99.71%				+ CREATE CATAG
› ApplicationCode	1686	98.94%	caTag_ApplicationCode__c	KO Application Code	□	
› application_id	1683	98.77%	caTag_applicationid__c	KO Application ID	□	
puppet_managed	1683	98.77%	caTag_puppetmanaged__c	KO Puppet Managed	□	+ CREATE CATAG
⌄ environment	1683	98.77%	caTag_environment__c	KO Environment	□	
Environment	31	1.82%				+ CREATE CATAG
environment	1654	97.07%				+ CREATE CATAG
infra_msp	1594	93.54%	caTag_inframsp__c	KO Infra MSP	□	+ CREATE CATAG
arch_compliance	1578	92.61%	caTag_archcompliance__c	KO Arch Compliance	□	+ CREATE CATAG
terraform_managed	1572	92.25%	caTag_terraformmanaged__c	KO Terraform Managed	□	+ CREATE CATAG
business_unit	1555	91.26%	caTag_businessunit__c	KO Business Unit	□	+ CREATE CATAG
› cpm backup	1493	87.62%	caTag_cpmbackup__c	KO CPM Backup	□	
› dr_class	1427	83.74%	caTag_drclass__c	KO DR Class	□	
security_tier	1416	83.10%	caTag_securitytier__c	KO Security Tier	□	+ CREATE CATAG
› host_name	1404	82.39%	caTag_hostname__c	KO Host Name	□	
managed_service_tier	1148	67.37%	caTag_managedservicetier__c	KO Managed Service Tier	□	+ CREATE CATAG

Compliance Engine

Cloudaware Compliance engine is a collection of over 300 cloud configuration policies and is a superset of policies available from frameworks such as Scout2, CloudCustodian, CloudConformity and other commercial products.



Policy Name ▲	Object Type	Output Object Type	Severity	Labels
AWS Account Duplicate CloudTrail Global Service Events	AWS Account	CloudAware Policy Violation	Medium	aws cloudtrail security
AWS Account Has No IAM Users	AWS Account	CloudAware Policy Violation	Medium	aws iam security
AWS Account Without IAM Password Policy	AWS Account	CloudAware Policy Violation	High	aws iam security
AWS ACM Certificate Expired	AWS ACM Certificate	CloudAware Policy Violation	High	aws acm security operational
AWS ACM Certificate Renewal (30 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	Medium	aws acm security
AWS ACM Certificate Renewal (45 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	Low	aws acm security
AWS ACM Certificate Renewal (7 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	High	aws acm security
AWS ACM Certificate Validity	AWS ACM Certificate	CloudAware Policy Violation	High	aws acm security operational
AWS ACM Certificate with Wildcard Domain Name	AWS ACM Certificate	CloudAware Policy Violation	Low	aws acm security operational
AWS Auto Scaling Group Health Checks Configuration	AWS EC2 Auto Scaling Group	CloudAware Policy Violation	Medium	aws autoscaling ec2 performance
AWS CloudFormation Stack Failed Status	AWS CloudFormation Stack	CloudAware Policy Violation	Medium	aws cloudformation operational
AWS CloudFormation Stack With Unrestricted IAM Role	AWS CloudFormation Stack	CloudAware Policy Violation	Medium	aws cloudformation iam security
AWS CloudFormation Stack Without Policy	AWS CloudFormation Stack	CloudAware Policy Violation	Medium	aws cloudformation security
AWS CloudFront Distribution Insecure Protocols	AWS CloudFront Distribution	CloudAware Policy Violation	Medium	aws cloudfront security
AWS CloudFront Distribution Origin Insecure SSL Protocols	AWS CloudFront Origin	CloudAware Policy Violation	Medium	aws cloudfront security
AWS CloudFront Distribution Origin Unencrypted Traffic	AWS CloudFront Origin	CloudAware Policy Violation	Medium	aws cloudfront security


Cloudaware
Search
Go to CMDB Classic
Cloudaware
support+5565bac10b2eb7c6a18b7b73@cloudaware.com
CMDB Navigator
Admin Console
List View AWS EC2 Instances
AWS EC2 Instance gula-services
Search for 10.49.1.74
Search for 10.0.1.4
Backup
AWS EC2 Instance AC - Jenkins
Compliance Engine
CloudAware Policy AWS Account Without IAM
CloudAware Policy AWS EC2 Instance Type Ge
compliance-engine/templates/ce:ca:aws:rds:publicly-accessible-instance-vpc
Compliance Engine
Policies List
POLICIES LIST
BUILT-IN POLICY TEMPLATES
Policy Templates
Policy Template Enable AWS IAM User MFA
Policy Template AWS S3 Bucket Public '*' or 's3
Policy Template Publicly Accessible AWS RD
DEPLOY
CLONE AS NEW POLICY
CLOSE RESULTS
Incompliant
Compliant

Publicly Accessible AWS RDS Instance (VPC)

Severity: High

Policy ID: ce:ca:aws:rds:publicly-accessible-instance-vpc

SObject Type: AWS RDS Instance

Output SObject Type: CloudAware Policy Violation

Description

Check for any public facing RDS database instances provisioned in your AWS account and restrict unauthorized access in order to minimise security risks. To restrict access to any publicly accessible RDS database instance, you must disable the database Publicly Accessible flag and update the VPC security group associated with the instance.

Labels: aws, rds, vpc, security

Test Run Results (100 objects limit)

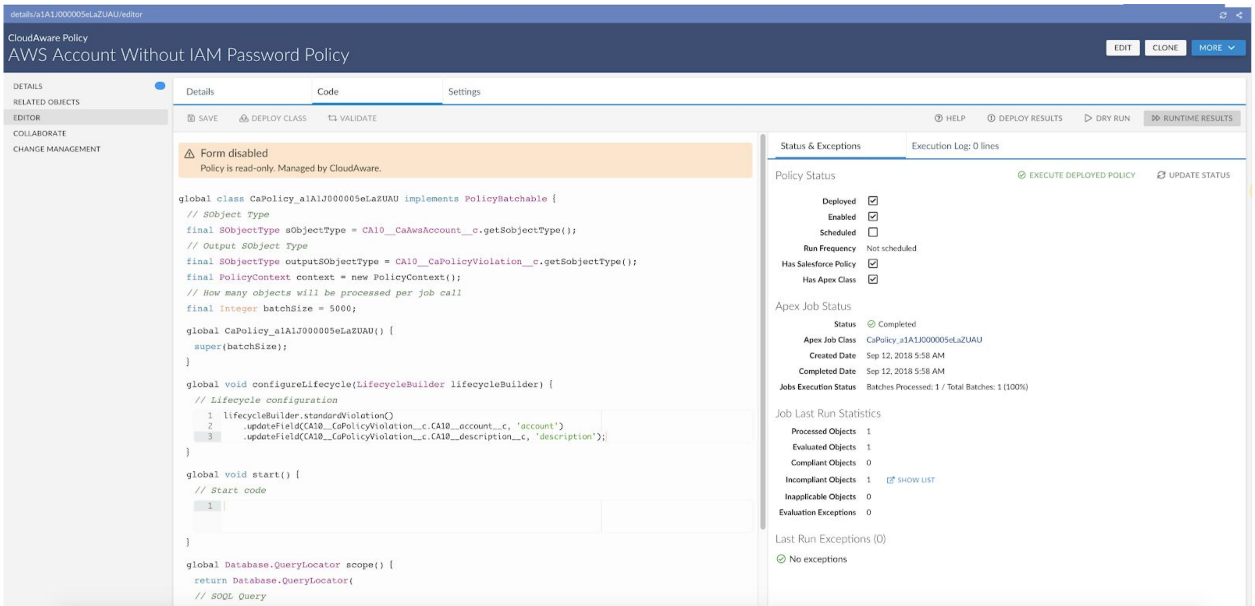
Stats
Total Objects Processed: 24
Incompliant Objects: 9
Compliant Objects: 15
Inaplicable Objects: 0

Object	Compliant Status	Resolution
datascience-iot-stringify	✕ INCOMPLIANT	Check for any public facing RDS database instances provisioned in your AWS account and restrict unauthorized access in order to minimise security risks. To restrict access to any publicly accessible RDS database instance, you must disable the database Publicly Accessible flag and update the VPC security group associated with the instance. RDS Instance uses port 5432, following security groups have it opened to 0.0.0.0/0: sg-15f24270
		Check for any public facing RDS database instances provisioned in your AWS account and restrict unauthorized access in order to minimise security risks. To restrict access to any publicly accessible RDS database instance, you must disable the database Publicly Accessible flag and update the VPC security group associated with the instance.

Cloudaware Compliance Engine has several key differentiators from other similar solution available on the market.

1. Extremely rich library of policies
2. Multi-cloud policies
3. Ability to author new and clone existing policies using Java programming language
4. Customize policies for specific accounts, VPCs, etc.
5. Ability to create policies that evaluate non-AWS attributes available in CMDB
6. Reduce number of API calls made to AWS by collecting once and running evaluations against CMDB, not against AWS inventory.
7. Integrate with 3rd party ticketing systems such as JIRA, ServiceNow, ServiceCloud, etc.
8. Automate exception handling processes.

Sample policy interface:



Form disabled

Policy is read-only. Managed by CloudAware.

```
global class CaPolicy_a1A1J000005eLaZUAU implements PolicyBatchable {
 // SObject Type
 final SObjectType sObjectType = CA10__CaAwsAccount__c.getSobjectType();
 // Output SObject Type
 final SObjectType outputSObjectType = CA10__CaPolicyViolation__c.getSobjectType();
 final PolicyContext context = new PolicyContext();
 // How many objects will be processed per job call
 final Integer batchSize = 5000;

 global CaPolicy_a1A1J000005eLaZUAU() {
  super(batchSize);
 }

 global void configureLifecycle(LifecycleBuilder lifecycleBuilder) {
  // Lifecycle configuration
  lifecycleBuilder.standardViolation()
      .updateField(CA10__CaPolicyViolation__c.CA10__account__c, 'account')
      .updateField(CA10__CaPolicyViolation__c.CA10__description__c, 'description');
 }

 global void start() {
  // Start code

 }

 global Database.QueryLocator scope() {
  return Database.QueryLocator(
  // SOQL Query
```

Policy Status

Deployed	☑
Enabled	☑
Scheduled	☐
Run Frequency	Not scheduled
Has Salesforce Policy	☑
Has Apex Class	☑

Apex Job Status

Status	✓ Completed
Apex Job Class	CaPolicy_a1A1J000005eLaZUAU
Created Date	Sep 12, 2018 5:58 AM
Completed Date	Sep 12, 2018 5:58 AM
Jobs Execution Status	Batches Processed: 1 / Total Batches: 1 (100%)

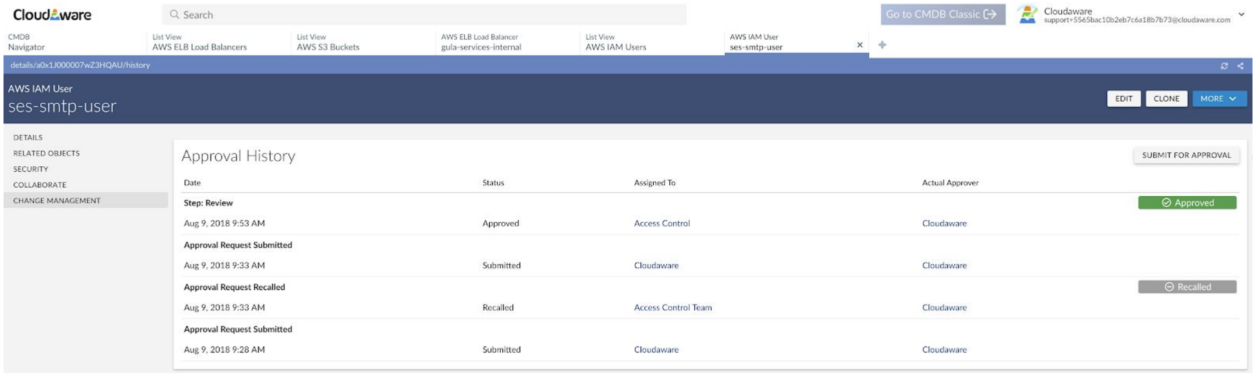
Job Last Run Statistics

Processed Objects	1
Evaluated Objects	1
Compliant Objects	0
Incompliant Objects	1
Inapplicable Objects	0
Evaluation Exceptions	0

Last Run Exceptions (0)

✓ No exceptions

Exception Handling:



Approval History

Date	Status	Assigned To	Actual Approver	
Step: Review				Approved
Aug 9, 2018 9:53 AM	Approved	Access Control	Cloudaware	
Approval Request Submitted				
Aug 9, 2018 9:33 AM	Submitted	Cloudaware	Cloudaware	
Approval Request Recalled				Recalled
Aug 9, 2018 9:33 AM	Recalled	Access Control Team	Cloudaware	
Approval Request Submitted				
Aug 9, 2018 9:28 AM	Submitted	Cloudaware	Cloudaware	

Incident Management

Cloudaware Incident Management allows customers to route policy violations to the appropriate teams.

This feature proved critical to Citrix because it has so many different engineering teams who use different ticketing systems. Cloudaware was able to route policy violations to the appropriate team and create tickets in in different JIRA instances, ServiceNow implementations, etc.

Incident Management module also provides sophisticated stateful integration with third party ticketing systems such as JIRA, ServiceNow, etc. and can not only open tickets but also close them and update them depending on the lifecycle of the violation. Citrix integrated Cloudaware Incident Management with its own in-house ticketing system using our outbound incident API. This allowed all the compliance engine policy violations to flow into Citrix’s systems of action.

Results

- Cloudaware now automatically validates against over 300 compliance policies derived from AWS, industry and internal best practices.
- Each product division maintains shares base set compliance and governance policies while having the option of creating their own department specific policies.
- Each product division can have custom exception handling and routing logic.
- Reduced administrative overhead by allowing users consistent and low friction process to request exemptions e.g. some S3 buckets are meant to be public after all.
- Eliminated issues with AWS API throttling during compliance checks because checks are ran against CMDB that in turn leverages CloudTrail and AWS Config to minimize “Describe*” API calls.
- One policy can now be applied to resources both in AWS and other cloud providers
- Removed the need to maintain in-house AWS compliance tool.