

Citrix Case Study

citrix

Solution Category: Cloud Governance

Deployment Model: SaaS outside AWS

Using Cloudaware: Since 2018

Available On Marketplace: Yes

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. Citrix helps 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 2021 annual revenue of \$3.22 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 250 AWS accounts and organizations. These accounts and subscriptions contain more than 1,500,000 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, specific 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 applications during scanning
- Many compliance policies between AWS and other cloud providers were duplicated, especially those related to a tagging policy.

Clouware Modules Deployed

- Clouware CMDB
- Clouware Compliance Engine
- Clouware Incident Management

Solution

Clouware is a modular SaaS-based cloud management platform. Our CMDB uses collectors, which leverage AWS Config, AWS CloudTrail, and service-specific API calls to build a complete inventory of all customer AWS infrastructure.

Citrix used automatically generated CloudFormation StackSets and AWS Organizations where possible to create a cross-account IAM role which allowed Clouware CMDB collectors to start harvesting information about the current state of Citrix AWS infrastructure and populate CMDB.

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

CMDB / Navigator
Amazon Web Services

Navigator / AWS

Search in navigator

AMAZON WEB SERVICES			
AWS Accounts	15	AWS S3 Buckets	138
AWS EC2 Instances	130	AWS ELB Load Balancers	13
AWS RDS Instances	4	AWS RDS Clusters	0
AWS EBS Volumes	188	AWS Redshift Clusters	2
		AWS DynamoDB Tables	7
		AWS ElastiCache Clusters	0
		AWS Elasticsearch Domains	0
		AWS EMR Clusters	0

AI & MACHINE LEARNING	ANALYTICS	APPLICATION INTEGRATION	BLOCKCHAIN
Rekognition	Athena CloudSearch Data Pipeline EMR Elasticsearch Glue Kinesis MSK	MQ SNS SQS Step Functions	Managed Blockchain
COMPUTE	COST MANAGEMENT	CUSTOMER ENGAGEMENT	DATABASE
Batch EC2 ECR ECS EKS Elastic Beanstalk Lambda Lightsail	Budgets Cost Explorer Savings Plans	SES	DAX DynamoDB DynamoDB Streams ElastiCache RDS Redshift
DEVELOPER TOOLS	END USER COMPUTING	INTERNET OF THINGS	MACHINE LEARNING
CodeBuild CodeCommit CodeDeploy CodePipeline	AppStream WorkSpaces	IoT Core	Kendra SageMaker

Tagging

The particular area of importance for Citrix was enforcing consistent tagging standards across their infrastructure. Using Cloudaware Tag Analyzer which is part of the CMDB, Citrix could better understand and correct deviations in their tagging coverage.

Tag Analyzer

Types: Tag on type: AWS EC2 Instance X

Type: CaAwsInstance_c
Objects Count: 1704

Search:

Tag	Used on Objects	Coverage	CaTag Name	CaTag Label	Exact
Name	1699	99.71%			<input type="checkbox"/>
> ApplicationCode	1686	98.94%	caTag_ApplicationCode_c	KO Application Code	<input type="checkbox"/>
> application_id	1683	98.77%	caTag_applicationid_c	KO Application ID	<input type="checkbox"/>
puppet_managed	1683	98.77%	caTag_puppetmanaged_c	KO Puppet Managed	<input type="checkbox"/>
> environment	1683	98.77%	caTag_environment_c	KO Environment	<input type="checkbox"/>
Environment	31	1.82%			<input type="checkbox"/>
> environment	1654	97.07%			<input type="checkbox"/>
infra_msp	1594	93.54%	caTag_infra_msp_c	KO Infra MSP	<input type="checkbox"/>
arch_compliance	1578	92.61%	caTag_archcompliance_c	KO Arch Compliance	<input type="checkbox"/>
terraform_managed	1572	92.25%	caTag_terraformmanaged_c	KO Terraform Managed	<input type="checkbox"/>
business_unit	1555	91.26%	caTag_businessunit_c	KO Business Unit	<input type="checkbox"/>
> cpm backup	1493	87.62%	caTag_cpmbackup_c	KO CPM Backup	<input type="checkbox"/>
> dr_class	1427	83.74%	caTag_drclass_c	KO DR Class	<input type="checkbox"/>
security_tier	1416	83.10%	caTag_securitytier_c	KO Security Tier	<input type="checkbox"/>
> host_name	1404	82.39%	caTag_hostname_c	KO Host Name	<input type="checkbox"/>
managed_service_tier	1148	67.37%	caTag_managedservicetier_c	KO Managed Service Tier	<input type="checkbox"/>

Compliance Engine

Cloudaware Compliance Engine is a collection of over 450 cloud configuration policies and industry benchmarks available from CIS and other frameworks such as Scout2, CloudCustodian, CloudConformity, etc.

Compliance Engine

Built-in Policy Templates Library

POLICY MANAGEMENT

- POLICY LIST
- TEMPLATES LIBRARY

CIS BENCHMARKS

- AWS FOUNDATIONS V1.2.0
- AWS FOUNDATIONS V1.4.0
- AZURE FOUNDATIONS V1.0.0
- AZURE FOUNDATIONS V1.1.0
- GCP FOUNDATIONS V1.0.0

SETUP

- OUTPUT OBJECTS
- UTILITY CLASSES

Policy Templates

Search:

OBJECT TYPE: NONE SELECTED | SEVERITY: NONE SELECTED | LABELS: NONE SELECTED

Policy Name	Object Type	Output Object Type	Severity	Labels	Deployed
<input type="checkbox"/> AWS Account Duplicate CloudTrail Global Service Events	AWS Account	CloudAware Policy Violation	Medium	aws, cloudtrail, security	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS Account Has No IAM Users	AWS Account	CloudAware Policy Violation	Medium	aws, iam, security, hipaa-access-control	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS Account Without IAM Password Policy	AWS Account	CloudAware Policy Violation	High	aws, iam, security, hipaa-access-control, FFIEC-IT-C-15-Ba	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS ACM Certificate Expired	AWS ACM Certificate	CloudAware Policy Violation	High	aws, acm, security, operational, hipaa-encryption, ISO-27001-CC1.1	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS ACM Certificate Renewal (30 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	Medium	aws, acm, security	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS ACM Certificate Renewal (45 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	Low	aws, acm, security	<input type="checkbox"/>
<input type="checkbox"/> AWS ACM Certificate Renewal (7 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	High	aws, acm, security	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS ACM Certificate Validity	AWS ACM Certificate	CloudAware Policy Violation	High	aws, acm, security, operational, hipaa-encryption, ISO-27001-CC1.1	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS ACM Certificate with Wildcard Domain Name	AWS ACM Certificate	CloudAware Policy Violation	Low	aws, acm, security, operational	<input type="checkbox"/>
<input type="checkbox"/> AWS API Gateway REST API public access	AWS API Gateway API	CloudAware Policy Violation	Medium	aws, apigateway, security	<input type="checkbox"/>
<input type="checkbox"/> AWS API Gateway REST API Stage Not Integrated With AWS WAF	AWS API Gateway Stage	CloudAware Policy Violation	Medium	aws, apigateway, security	<input type="checkbox"/>
<input type="checkbox"/> AWS Athena Encryption at Rest	AWS Athena Work Group	CloudAware Policy Violation	Low	aws	<input type="checkbox"/>
<input type="checkbox"/> AWS Auto Scaling Group Health Checks Configuration	AWS EC2 Auto Scaling Group	CloudAware Policy Violation	Medium	aws, autoscaling, ec2, performance, hipaa-auditing	<input type="checkbox"/>
<input type="checkbox"/> AWS CloudFormation Stack Contains Sensitive Data	AWS CloudFormation Stack	CloudAware Policy Violation	High	aws, cloudformation, security, hipaa-auditing	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS CloudFormation Stack Failed Status	AWS CloudFormation Stack	CloudAware Policy Violation	Medium	aws, cloudformation, operational	<input type="checkbox"/>
<input type="checkbox"/> AWS CloudFormation Stack With Unrestricted IAM Role	AWS CloudFormation Stack	CloudAware Policy Violation	Medium	aws, cloudformation, iam, security, hipaa-access-control	<input checked="" type="checkbox"/>
<input type="checkbox"/> AWS CloudFormation Stack Without Policy	AWS CloudFormation Stack	CloudAware Policy Violation	Medium	aws, cloudformation, security	<input checked="" type="checkbox"/>

Compliance Engine
Built-in Policy Templates Library

POLICY MANAGEMENT
POLICY LIST
TEMPLATES LIBRARY

CIS BENCHMARKS
AWS FOUNDATIONS V1.2.0
AWS FOUNDATIONS V1.4.0
AZURE FOUNDATIONS V1.0.0
AZURE FOUNDATIONS V1.1.0
GCP FOUNDATIONS V1.0.0

SETUP
OUTPUT OBJECTS
UTILITY CLASSES

Policy Templates Policy Template
Publicly Accessible AWS RD^x

Publicly Accessible AWS RDS Instance (VPC) Deployed CLONE AS NEW POLICY

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

SObject Type AWS RDS Instance Output SObject Type CloudAware PolicyViolation

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 hipaa-access-control

Policy Code TEST RUN

```
global class NewPolicy implements PolicyBatchable {
    // SObject Type
    final SObjectType sObjectType = CA10_CaAwsDbInstance_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 = 100;

    global NewPolicy() {
        super(batchSize);
    }

    global void configureLifecycle(LifecycleBuilder lifecycleBuilder) {
        // Lifecycle configuration
        1 lifecycleBuilder
        2     .standardViolation()
        3     .updateField(CA10_CaPolicyViolation_c.CA10_account_c, 'account')
        4     .updateField(CA10_CaPolicyViolation_c.CA10_awsAccountId_c, 'accountId')
        5     .updateField(CA10_CaPolicyViolation_c.CA10_awsDbInstanceArn_c, 'dbInstanceArn')
```

Cloudaware Compliance Engine has several key differentiators from other similar solutions 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-cloud attributes available in CMDB
6. Reduce the number of API calls made to the cloud by collecting once and running evaluations against CMDB, not against cloud inventory
7. Integrate with third-party ticketing systems such as JIRA, ServiceNow, ServiceCloud, etc.
8. Automate exception handling processes

Sample policy interface:

The screenshot displays the CloudAware Policy interface for a policy named "AWS Account Without IAM Password Policy". The interface is divided into several sections:

- Header:** Shows the policy name and navigation buttons: EDIT, CLONE, MORE.
- Left Sidebar:** Contains navigation options: DETAILS, RELATED OBJECTS, EDITOR, COLLABORATE, and CHANGE MANAGEMENT.
- Code Editor:** Displays the Apex class code for `CaPolicy_a1A1J000005eLz2UAU`. The code includes lifecycle configuration and a `start()` method. A message at the top of the editor states: "Form disabled. Policy is read-only. Managed by CloudAware."
- Right Panel:** Shows the "Status & Exceptions" section with the following details:
 - Policy Status:** Deployed (checked), Enabled (checked), Scheduled (unchecked), Run Frequency: Not scheduled, Has Salesforce Policy (checked), Has Apex Class (checked).
 - Apex Job Status:** Status: Completed, Apex Job Class: CaPolicy_a1A1J000005eLz2UAU, 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 (with a "SHOW LIST" link), Inapplicable Objects: 0, Evaluation Exceptions: 0.
 - Last Run Exceptions (0):** No exceptions.