CITRIX SYSTEMS, INC.

Citrix Application Delivery Management Service

Data Governance Overview

November 2, 2021

This information is provided "AS-IS" without warranties of any kind (express or implied) and is subject to change at Citrix's discretion.

Contents

Abstract

This document communicates the data collected and stored in cloud as part of Citrix Application Delivery Management (ADM) service. The audience for this information is Security Officers, Compliance Officers, Information Auditors, Network Infrastructure and Operations administrators, and line-of-business owners using this service or involved in approving the use of this service within their respective organization.

For more information about data protection practices at Citrix, please see the Citrix Cloud Services Data Protection Overview.

Categories of Data Processed

During the performance of services, different types of data are processed by our Cloud Services. For our data handling practices, we classify this data into two categories: customer content and logs.

- **Customer Content** means any data uploaded to Customer's account for storage or data in Customer's computing environment to which Citrix is provided access in order to perform Services.
- **Logs** include records of Services, including, but not limited to:
  - Data and information on performance, stability, usage, security, support
  - Technical information about devices, systems

ADM Service Overview

Citrix Application Delivery Management (ADM) Service provides centralized network management, analytics, and automation as a service from the cloud to support virtualized or containerized applications deployed across public clouds and on-premises datacenters. From a single platform, administrators can view, automate, and manage network services across their entire infrastructure. The ADM Service enables IT operations and DevOps teams to focus on managing end-to-end application delivery, while letting Citrix take care of the operation, updates, and monitoring of the service.

The ADM Service is part of Citrix Cloud services portfolio, and it uses Citrix Cloud as the platform for signup, onboarding, authentication, administration, and licensing.

Data Access

Methods for data collection, storage, and transmission

The ADM Service collects data and information from the Citrix ADC instances. These instances are deployed in the customer's premises and data is transmitted from ADM Service agent (deployed in the customer's premise) securely over an SSL channel encrypted using TLS 1.2 protocol[1] to the cloud

[1] Note: All ADM Endpoints for UI/API access as well as Service URLs for Agent communications are graded "A" as per Qualys SSL Labs)

service. Data is stored in Relational database with multi-tenant data isolation at the database layer and as files in Elastic File System (EFS) hosted in AWS cloud in the United States, EMEA (Frankfurt) and APJ (Sydney) – depending on the Point of Presence (POP) chosen by the customer. All PoPs are hosted in AWS Commercial regions.

Customer onboarding for CAS & ADM service is independent, but both these services are available in US, EU and APAC region. CAS data of EU customers will go to CAS PoP in EU. For all other customers CAS data will go to CAS PoP in US. Listed below are the use cases delivered from CAS:

- App Dashboard / Intelligent App Analytics(Rule based indicators)
- Intelligent Infra Analytics(Rule based indicators)
- Detail Web Transactions
- Service Graph
- Distributed Tracing
- App Security Analytics
- Behaviour Based Violations
- Network Violations
- Bot Security Violations
- API Security

Passwords, SNMP community strings, SSL certificates, and ADC config backup are encrypted using a unique per tenant AES 256 key, and stored securely in the database.

Customer Content

Citrix ADM Service collects information from various sources:

1. Citrix ADC
2. Citrix Gateway
3. Citrix Web App Firewall (WAF) and Bot Management
4. Citrix SD-WAN

ADM Service also collects information about administrator's session and activity details in addition to the information mentioned below.

Logs

Logs are used to facilitate the provisioning of software updates, license authentication, support, analytics and other purposes consistent with Citrix User Agreements.

Metadata and telemetry Logs collected include:

- ADM Service agent hypervisor or public cloud platform or both agent hypervisor and public cloud platform
- agent's geographical location
- Citrix ADC version
- Citrix ADC product type
- licensing info (Express and subscription)
- usage of cloud service by the ADM Service admin (thereby improving the admin user experience).

Collected Customer Content and Logs

The Customer Content and Logs collected include the following artifacts:

- Event Management **(Login > Infrastructure > Events)**
    - SNMP traps providing alerts on state and performance of the ADC network
    - Syslog of Web transactions traversing through ADC network and ADC network state information.
    - SMS server, Slack and PagerDuty profile details for triggering SMS/Slack notifications of events
    - SMTP server details for email configuration
    - ServiceNow profile details for creating tickets in ServiceNow
- SSL Certificate Management **(Login > Infrastructure > SSL Dashboard)**
    - SSL certificates, SSL key, SSL CSR, CA issuer, signature algorithms of the Web apps optimized by the Citrix ADC instance
- Configuration Audit **(Login > Infrastructure > Configuration > Configuration Audit)**
    - Data Tracking for Citrix ADC Configuration Audit changes pertaining to the ADC instances, which include Web app server IP address and Citrix ADC IP address details
- Configuration Jobs **(Login > Infrastructure > Configuration > Configuration Jobs)**
    - Citrix ADC Configuration details, instance IP address, and Web app server IP address details
- StyleBooks **(Login > Applications > Configuration > StyleBooks)**
    - Citrix ADC configurations stored as a template, which include Web app server IP address details
- Instance Management **(Login > Infrastructure > Instances)**
    - IP address of the ADC instances, ADC instance type, ADC config backup, ADC critical events, geolocation of the datacenter where the ADC instance is deployed (if configured)
- Infrastructure Analytics **(Login > Infrastructure > Infrastructure Analytics)**
    - IP address of the ADC instances, ADC instance type, ADC critical events, number of app associated, geolocation of the datacenter where the ADC instance is deployed (if configured)
- Applications **(Login > Applications)**
    - App Dashboard: applications URL, request method, response code, total Bytes, Web app server details, virtual server IP addresses, client details, browser, client OS, client device, SSL protocol, SSL cipher strength, SSL key strength, ADC instance IP address, timestamp of server flaps, response content type
- Analytics (AppFlow/ Logstream)
    - Web Insights **(Login > Applications)**: virtual server IP address, clients, URLs, browsers, operating systems, requests methods, response statuses, domains, Web app server IP address, SSL certificates, SSL cipher negotiated, SSL key strength, SSL protocol, SSL failure frontend.
    - HDX Insight **(Login > Gateway)**: ICA user details, ICA application details, VDA server details, desktop details in HDX Insight, geolocation details of app client, HDX active session details, VPN licenses for HDX, client ADC IP address, client type and version
    - Gateway Insight **(Login > Gateway)**: user details, application details, browsers, operating

systems, session modes, Gateway licenses, AAA server details, AAA policy configured on Gateway.

- Security Violations **(Login >Security)**: client IP, URL, security violations (WAF and Bot), attack geolocation, attack timestamp, transaction ID, WAF and ADC security configuration status.
- API Analytics (**Login > Security > API Gateway**): Information on API Instances, API Endpoints, total bandwidth, API performance information, total request, response time, errors. Ability to drill down further into each API Instance to get visibility into individual API endpoints, performance. Security related to Auth success, failures; Rate-limiting, SSL cipher, protocol information and SSL errors.

- Security Advisory **(Login > Infrastructure > Instance Advisory > Security Advisory)**
    - Version scan: This scan needs ADM service to compare the version of an ADC instance with the versions and builds on which the fix is available. This version comparison helps ADM service security advisory identify whether the ADC is vulnerable to the CVE. The underlying logic for this scan is if a CVE is fixed on ADC release and build xx.yy, all the ADC instances on builds lesser than xx.yy build are considered vulnerable. Version scan is supported today in security advisory.
    - Configuration scan: This scan needs ADM service to match a pattern specific to the CVE scan with ADC config file (nsconf). If the specific config pattern is present in the ADC ns.conf file, the instance is considered vulnerable for that CVE. This scan is typically used in conjunction with version scan.
      Config scan is supported today in security advisory.
    - Custom scan: This scan needs Citrix Application Delivery and Management to connect with the managed ADC instance, push a script to it, and run the script. The script output helps Citrix Application Delivery and Management identify whether the ADC is vulnerable to the CVE. Examples include specific shell command output, specific CLI command output, certain logs, and existence or content of certain directories or files. Security Advisory also uses custom scans for multiple config patterns matches, if config scan cannot help with the same. For CVEs that require custom scans, the script runs every time your scheduled or on-demand scan runs. Learn more about the data collected and options for specific custom scans in the Security Advisory documentation for that CVE.

Security

The Citrix Services Security Exhibit describes in-depth the security controls applied to Citrix Cloud Services, including access and authentication, system development and maintenance, security program management, asset management, encryption, operations management, HR security, physical security, business continuity, and incident management.

The security of Citrix Cloud products is controlled by encryption and key management policies. Refer to the Security Development Processes whitepaper for more details on how Citrix employs security throughout its product development lifecycle.

Data retention policy for ADM Service

Data such as statistical measures, dashboards, reports, alerts, events, Logs[2] within the ADM service as well as login details are retained for the period the customer subscribes to the service. The user account then converts to an Express account where the user can manage only two virtual servers, two config jobs, two StyleBooks packs. The Express account has a capacity of 500 MB or 1-day of Analytics/Reporting data, whichever limit the account reaches first. If an ADM Express account is not used, or the customer does not log in to the account for more than 30 days, the account and all associated Customer Content are automatically deleted.

For more information about data retention and deletion for Citrix Cloud Services accounts, please see the Citrix Cloud Services Data Protection Overview.

Note: All Analytics data in ADM Service is retained for a maximum period of 30 days.

Third-party services used in ADM Service

ADM Service is hosted within Amazon Web Service (AWS) datacenters in the United States, EMEA (Frankfurt) and APJ (Sydney) regions – depending on the Point of Presence (POP) chosen by the customer.

Currently, the ADM Service uses services and APIs from various third-party technologies:

- Services used for product functionality
    - Google Maps, AWS EFS, AWS RDS, AWS Elastic Cache, AWS ALB, AWS Route 53, AWS EKS, AWS Secret Manager, AWS ECR repository, AWS MSK.
- Third-party services and tools used for monitoring and operating ADM Service include:
    - PagerDuty for on-call rotation
    - Log analysis with Splunk
    - Fluentd for log aggregation
    - Slack for communication and alerting
    - AWS Cloudwatch, SQS
    - S3 as storage area in AWS –for storing core files and metrics
    - Prometheus and Grafana for monitoring (in case of Honeycomb deployment)

References

[2] Logs may be retained by Citrix and the third-party services used to support this Service for other purposes as described in the Citrix Services Security Exhibit. These will be deleted when no longer needed for a legitimate purpose.

Citrix Cloud Technical Security Overview
https://docs.citrix.com/en-us/citrix-cloud/overview/secure-deployment-guide-for-the-citrix-cloud-platform.html

Citrix Cloud Technical and organizational data security measures
https://www.citrix.com/about/legal/security-compliance/

Citrix Services Security Exhibit
https://www.citrix.com/buy/licensing/citrix-services-security-exhibit