Citrix Application Delivery Management
Data Governance Document

Dec 9, 2019
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>2</td>
</tr>
<tr>
<td>ADM Service Overview</td>
<td>2</td>
</tr>
<tr>
<td>Customer Content</td>
<td>2</td>
</tr>
<tr>
<td>Methods for data collection, storage, and transmission</td>
<td>3</td>
</tr>
<tr>
<td>Logs</td>
<td>4</td>
</tr>
<tr>
<td>Secure access to Customer Content and Logs</td>
<td>4</td>
</tr>
<tr>
<td>Data retention policy for ADM Service</td>
<td>4</td>
</tr>
<tr>
<td>Third-party services used in ADM Service</td>
<td>4</td>
</tr>
<tr>
<td>References</td>
<td>5</td>
</tr>
</tbody>
</table>

**Citrix Cloud Technical Security Overview**


**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
Abstract
This document is intended to communicate 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, or both using this service and involved in approving the use of this service within their respective organizations.

The following terms are used in this article:
- **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.
- **Log** means a record of events related to the Services, including records that measure performance, stability, usage, security, and support.

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. 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.

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

Customer Content
Citrix ADM Service collects information from various sources:
1. Citrix ADC
2. Citrix Gateway
3. Citrix Web App Firewall(WAF)
4. Citrix SD-WAN
ADM Service also collects information about administrator’s session and activity details in addition to the information mentioned below.

The Customer Content and Logs collected include the following artifacts:
- **Event Management** *(Login > Networks > 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 > Networks > SSL Dashboard)
  o SSL certificates, SSL key, SSL CSR, CA issuer, signature algorithms of the Web apps
  optimized by the Citrix ADC instance
• Configuration Audit (Login > Networks > Configuration Audit)
  o 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 > Networks > Configuration Jobs)
  o Citrix ADC Configuration details, instance IP address, and Web app server IP address
details
• StyleBooks (Login > Applications > StyleBooks)
  o Citrix ADC configurations stored as a template, which include Web app server IP address
details
• Instance Management (Login > Networks > Instances)
  o 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 > Networks > Infrastructure Analytics)
  o 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)
  o 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) (Login > Networks > Analytics)
  o Web Insights: 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.
  o HDX Insight: 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
  o Gateway Insight: user details, application details, browsers, operating systems,
    session modes, Gateway licenses, AAA server details, AAA policy configured on
    Gateway.
  o Security Insight: client IP, URL, security violations, attack geolocation, attack
    timestamp, transaction ID, WAF and ADC security configuration status

Methods for data collection, storage, and transmission
The data and information that ADM Service collects comes 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* to
the cloud service. Data is stored in Relational database with multi-tenant data isolation at the database
layer and also as files in Elastic File System (EFS) hosted in AWS cloud in the United States.

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

*Note: All ADM Endpoints for UI/API access as well as Service URLs for Agent communications are graded “A” as per Qualys SSL Labs)

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

Secure access to Customer Content and Logs
Citrix has implemented reasonable physical, technical, and organizational measures to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, destruction, or damage to personal data. Citrix uses industry-standard efforts to safeguard the confidentiality of personal data, including encryption and physical and logical access controls.

Data retention policy for ADM Service
Customer Content such as statistical measures, dashboards, reports, alerts, events, Logs¹, and analytics data within the ADM service as well as login details are retained for the period the customer subscribes to the service, plus an additional period of 60 days. After this grace period, the user account converts to an Express account where the user can manage only two virtual servers, two config jobs, two StyleBooks packs. In addition, 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.

Third-party services used in ADM Service
ADM Service is hosted within Amazon Web Service (AWS) datacenters in the United States.

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
- Third-party services and tools used for monitoring and operating ADM Service include:
  - PagerDuty for on-call rotation
  - Log analysis with Splunk
  - Slack for communication and alerting
  - AWS Cloudwatch, SQS
  - S3 as storage area in AWS –for storing core files and metrics
  - Storage Account area in Azure – for storing SW images

¹ 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.
Prometheus and Grafana for monitoring (in case of Honeycomb deployment)

References

Citrix Cloud Technical Security Overview

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