Zerto
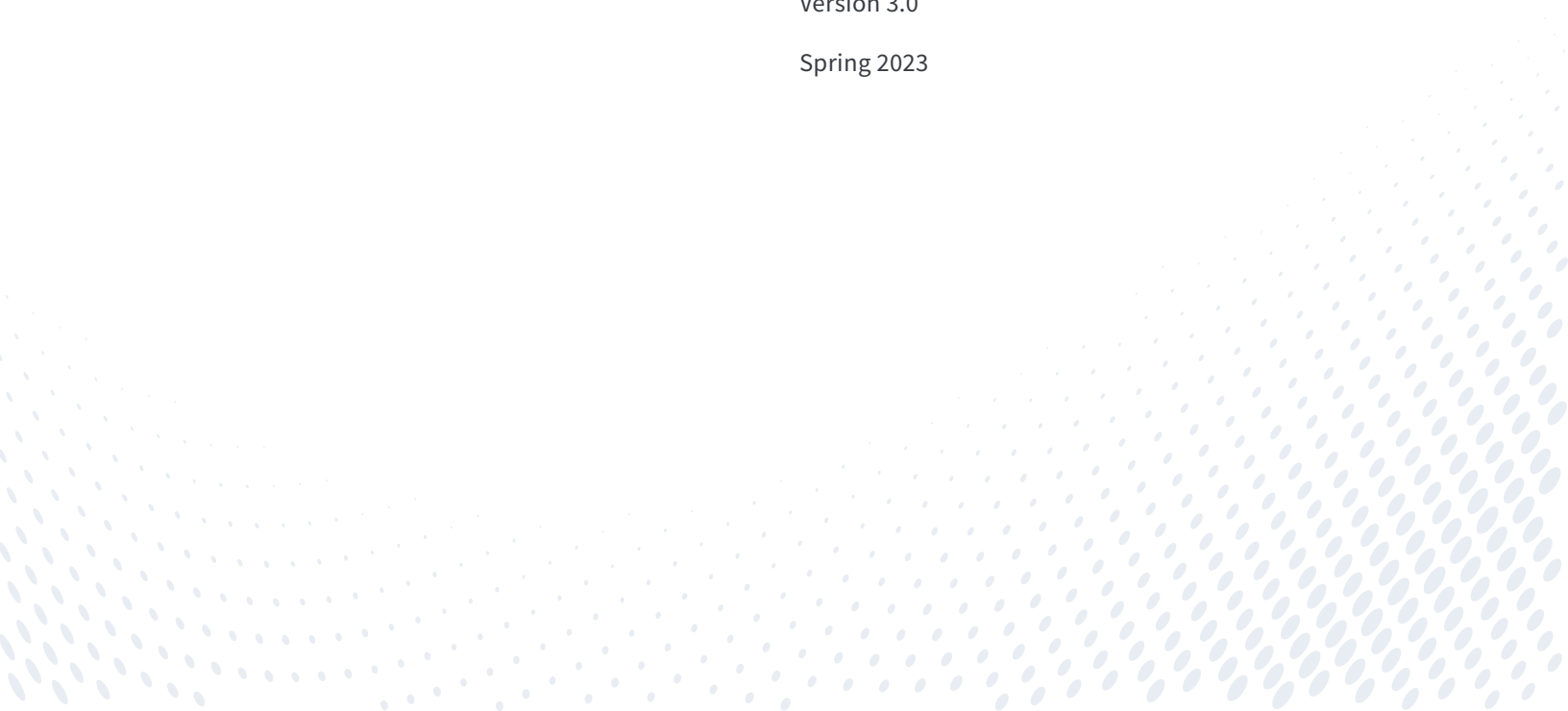
a Hewlett Packard
Enterprise company

Zerto Analytics
Secure Architecture

Version 3.0

Spring 2023

Contents

Introduction

It is important to keep safe what keeps you protected. That is why at Zerto, a Hewlett Packard Enterprise company, we ensure customers can rely on Zerto's ability to not only keep their applications secure, but that we keep our software secure too.

This is why Zerto provides best-in-class secure communication between the Zerto Virtual Manager (ZVM), our control plane, and the Zerto Analytics datastore, which ensures a timely and accurate collection of analytics data. Data transmitted to Zerto Analytics is securely stored and can be viewed and exported only by an authorized user. The data is also used by the analytics engine to generate advanced guidance and analysis.

This whitepaper details the secure architecture that provides the path to transmit, the datastore where the data is maintained, and access of that data.

Zerto Analytics overview

Every day, businesses of all sizes face complex decisions. In order to generate greater overall efficiency, it teams need to evolve based on more informed decision-making. Zerto Analytics enables out of the box real-time and historical analysis of all your virtual infrastructure protected with Zerto, whether they are virtual machines on-premises, in the cloud, or run using containers and Kubernetes.

Zerto Analytics provides the following benefits:

1. Data and guidance for collaboration with peers to troubleshoot and solve problems
2. Guidance to make recommendations to optimize and plan environment resources efficiently
3. Understanding regarding future resource needs based on patterns in data history

Zerto Analytics delivers unrivaled visibility across all sites protected with Zerto. It ingests metrics of Virtual Protection Groups (VPGs) such as average RPO, storage consumption, and network performance. It provides real-time information based on real-time replication. All the collected data is aggregated and consolidated into a simple, easy-to use web interface that runs as software-as-a-service (SaaS). The ZVM sends data once every minute to monitor environments in real time. The data is compressed and throttled to minimize the amount of bandwidth consumed.

Get started with Zerto Analytics

Enabling Zerto Analytics is simple:

1. In the Zerto Virtual Manager, go to Settings > About and check "Enable Zerto SaaS features. Includes Zerto Analytics, Zerto Mobile App and Remote Upgrade"
2. Go to the myZerto portal at zerto.com/myzerto and login using your credentials.
3. Click on the Zerto Analytics tab
4. Begin monitoring environment health across all protected on-premises and cloud sites in one intelligent dashboard

Zerto Analytics architecture

Understanding the Zerto Analytics architecture starts with understanding the transfer of data. The ZVM communicates with the following URLs to transfer data over HTTPS TLS 1.2:

1. Google Analytics → google-analytics.com

2. Zerto Analytics → receiver DNS address zerto-mobile-data.zerto.com

3. Upgrade Manager → zerto-msgs-for-sites.SaaS.zerto.com

4. Remote Log Collection (RLC)→ zerto-msgs-for-sites.SaaS.zerto.com

5. Zerto Cloud Appliance (ZCA) Auto Update → zerto-msgs-for-sites.SaaS.zerto.com

6. CallHome → autologs.zerto.com

Collected metadata is stored in the Zerto Analytics backend, hosted by Zerto on AWS in the us-east-1 (N. Virginia) region. All communication to and from the cloud is encrypted (HTTPS) using TLS 1.2. Furthermore, the data is isolated in the SaaS backend and accessible only within the backend itself via VPN from Zerto. End users are authenticated against AWS Cognito's IAM service.

Transmission and storage of deployment metadata

ZVMs transmit current site status and all relevant metadata over secured HTTPS to the SaaS backend in short (~1 minute) intervals. The SaaS backend collects data from all transmitting sites and stores it in an Amazon S3 bucket. The S3 bucket is secured inside an internal protected network, an Amazon Virtual Private Cloud (VPC), and is accessible only within the backend itself and via VPN from a limited set of authorized Zerto users. The transmitted data is kept in Zerto Analytics for ninety (90) days to support ninety (90) days of report history.
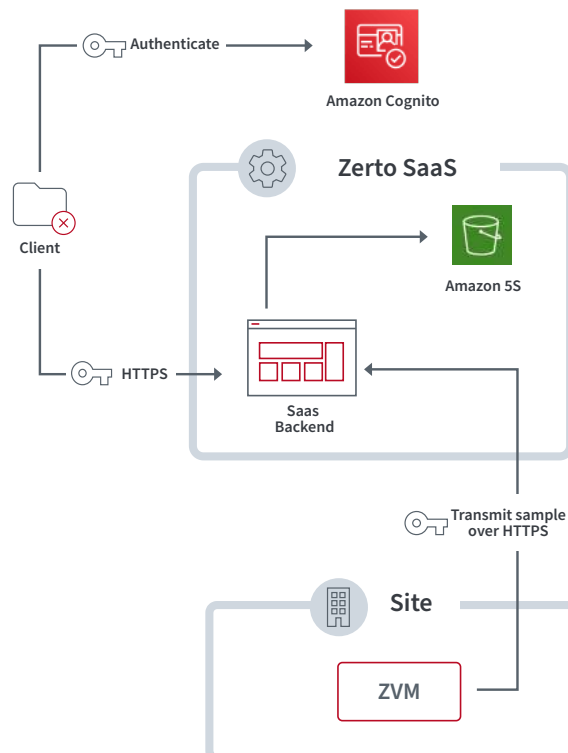
User authentication and authorization

Before sending any request to the backend, a client (browser/mobile/RESTful client) must obtain a security token which securely identifies the user. The security token is achieved by authenticating the user against the Amazon Cognito service. Each client request contains a security token. For each request, the backend validates the security token and authorizes execution of the request according to the user's identity which is part of the security token's payload.

Reporting historical data

For each client request, the backend gets the latest data from the relevant samples as stored in the S3 bucket and then relevant data is sent to the client.

What data Zerto Analytics collects

The Zerto Analytics dashboard utilizes several metrics to deliver detailed monitoring and reporting of all applications protected using Zerto. Metadata includes alerts, tasks, sites, VPGs, VMs, and more. There is no personal identifiable information (PII) stored or retained ever.

A complete list of all data collected by Zerto Analytics can be found here.

Summary

Zerto Analytics delivers a robust range of insights for solving enterprise-grade problems. To ensure a secure adoption of Zerto Analytics, customers need to know every piece of data that is collected from their environment. This whitepaper described the secure architecture that provides the path to transmit, the datastore where the data is housed, and access of that data. With this information, enterprises can feel confident using Zerto Analytics to troubleshoot problem areas, optimize resource efficiency, and plan to evolve into a data-driven enterprise.

RITM0087060