Zoom Video Communications, Inc.

Global Infrastructure and Security Guide

January 2016

Contents

1. Overview

The Zoom Cloud is a proprietary global network that has been built from the ground up to provide quality communication experiences to our users. Our engineering team, with over 900 years of online collaboration experience, has focused on providing industry-leading customer satisfaction. Zoom's cloud platform is a powerful and reliable base for real-time audio, video, and collaboration.

Zoom provides users with:

- Phenomenal audio and video quality
- Industry-leading web collaboration toolkit
- Stringent security standards and implementation
- Reliable firewall traversal
- Simple signup and setup
- Intuitive web portal for site, user, and meeting management

2. Reliable Service Infrastructure

2.1 High Quality

Zoom has a geographically dispersed presence allowing our users to connect directly to the Zoom Cloud though a locally-designated point of presence. No matter where you are in the world, a local on-ramp to the Zoom Cloud will allow for a high quality audio, video, and collaboration services.

2.2 High Availability

The Zoom Cloud is fully redundant at each of our global points of presence. If there is a failure at one of our data centers, traffic will automatically be redirected to a fully-functioning point of presence. All servers and network devices have redundant components and multiple network paths to avoid single points of failure.

2.3 Distributed Network

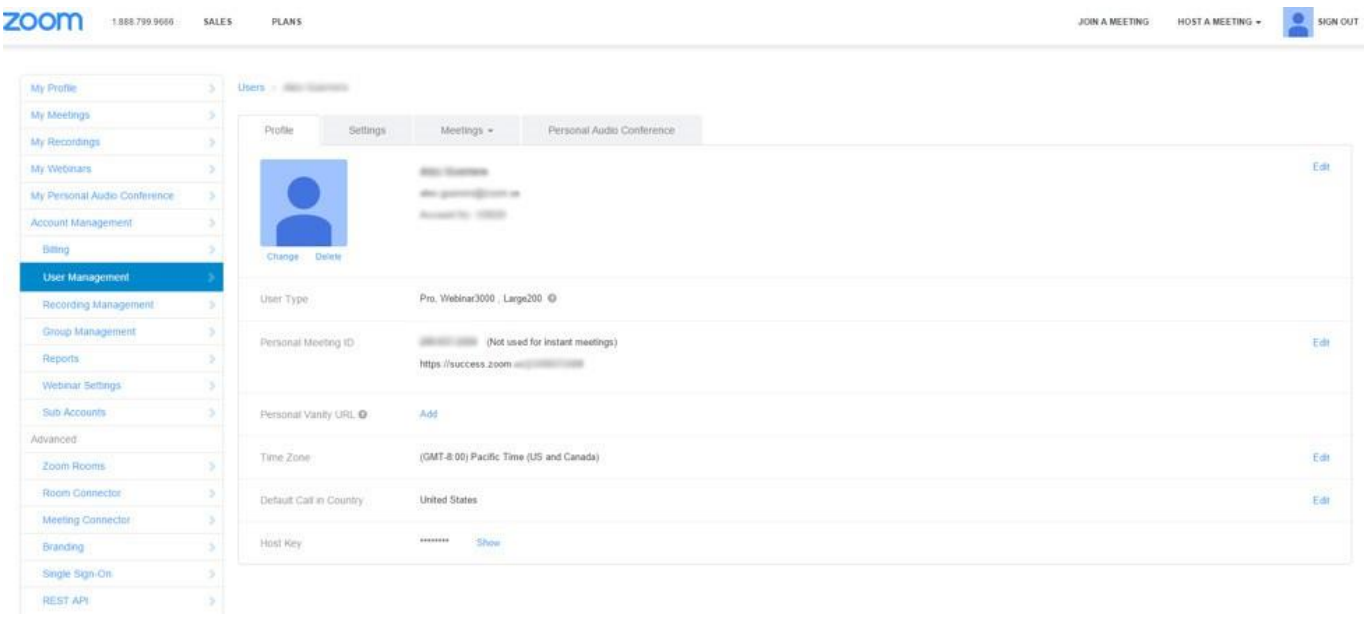
Zoom's cloud runs on a distributed network of low-latency multimedia routers. All session data originating from a host device and arriving at the participants' devices is dynamically switched.

3. Supported Endpoints

- There are various clients and endpoints for connecting to the Zoom cloud for real-time collaboration. Desktop: Zoom has desktop clients that run on PC, Mac, and Linux operating systems.
- Mobile: Zoom has mobile clients that run on iOS, Android, and BlackBerry.
- H.323/SIP: Any traditional H.323 or SIP conference room endpoint can connect to Zoom meetings.
- Zoom Rooms: Users can set up their own Zoom-enabled conference room that connects directly to the Zoom Cloud for real-time collaboration. This software-defined video conference room system supports video and audio, wireless content sharing, and integrated calendaring.
- PSTN: Public Switched Telephone Network (PSTN) is traditional telephony networks that are utilized for Audio conferencing. Zoom partners with the leading telephony service providers across the globe to provide the clearest, most localized audio experience.

4. Management - Administrative Console and Set Up

Management of sites, hosts, and meetings can be easily achieved from anywhere in the world through the Zoom portal accessed via https://zoom.us/signin. Our secure and redundant systems will backup your settings to ensure that all service settings are available, even in the case of a site service failure. Users can also customize their site and setup with Zoom's Rest API.



5. Monitoring and Reporting

5.1 Zoom Cloud Monitoring

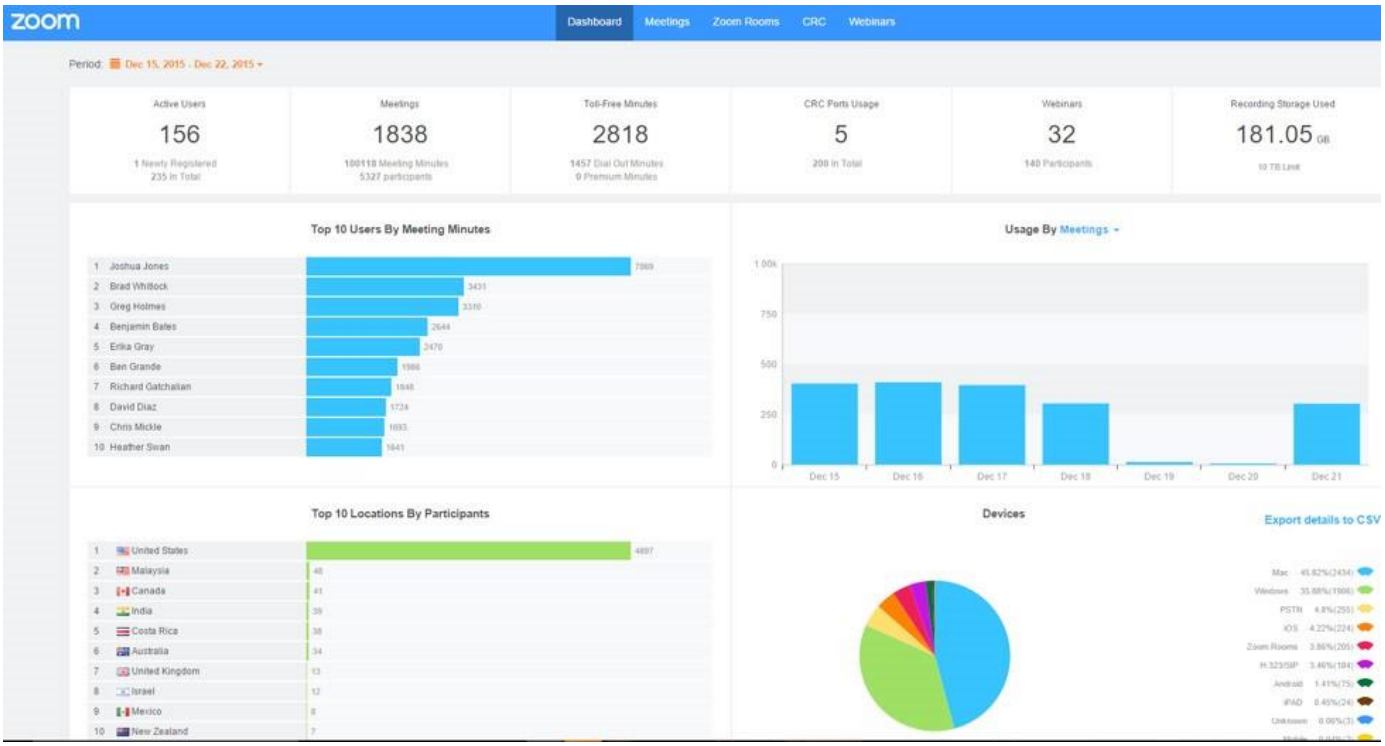
Zoom's global network operations utilizes industry-leading tools to monitor the health and performance of the Zoom Cloud. Network health is monitored with traditional monitoring tools while leading-edge analytics are used to predict problems before they occur.

We integrate all standalone monitoring tools, including but not limited to network, security, platform, systems, and applications into a centralized management platform to accomplish the following:

- Log collections go through filters and are archived. Analytics identify issues and assign each issue to a group based on severity. Reports are generated for future optimization.
- Auto-recovery and auto-failover for critical incident messages are identified in logs.
- Data and log usages trend analytics: to reflect our architectural adjustments.
- Automatic incident management.
- Network traffic analysis.
- Application services quality analysis tool provided by Pingdom.

5.2 Usage Reporting

Usage reporting can be accessed through the Zoom Cloud portal. This allows our account administrators to access reports that will let them analyze usage of Zoom services such as meetings, telephony, and webinars.



6. Security Features

6.1 Overview

The security of the Zoom cloud is of the utmost importance. We have considered all levels of the Zoom Cloud architecture to ensure that all meetings are completely secure.

All of the Zoom endpoints and clients have signed certificates that facilitate secure communication with certificates on Zoom servers. This secure communication eliminates the possibility of eavesdropping on Zoom-based communications.

The Zoom service supports full firewall traversal, allowing all clients and endpoints behind firewalls to connect to Zoom Cloud services.

All session data originating from the host's device and arriving at the participants' devices is dynamically switched and never stored persistently through the Zoom communications infrastructure.

- Log collections go through filters and are archived. Analytics identify issues and assign each issue to a group based on severity. Reports are generated for future optimization.
- Auto-recovery and auto-failover for critical incident messages are identified in logs.
- Data and log usages trend analytics: to reflect our architectural adjustments.
- Automatic incident management.
- Network traffic analysis.
- Application services quality analysis tool provided by Pingdom.

6.2 Authentication and Encryption

Zoom's sign in and join pages (https://zoom.us/signin and https://zoom.us/join) use TLS 1.2 connections with 256 bit encryption. With username and passwords encrypted, meetings will not be susceptible to breaches. Real time traffic is also encrypted with same standard and is never stored.

6.3 Firewall Traversal

The Zoom service supports full firewall traversal. This allows all clients and endpoints behind firewalls to connect to Zoom Cloud services. This is done securely with the use of certificates and encryption.