

Z 解体 真書

Chapter 1

ゼットスケーラー株式会社

エバンジェリスト&アーキテクト

高岡 隆佳

Zアーキテクチャを6つの切り口から紹介



1. Z構成要素

Zscaler = Zenith of Scalability (天井知らずの拡張性)



CENTRAL
AUTHORITY



脅威インテリジェンス
ポリシー管理



ZSCALER
ENFORCEMENT
NODE

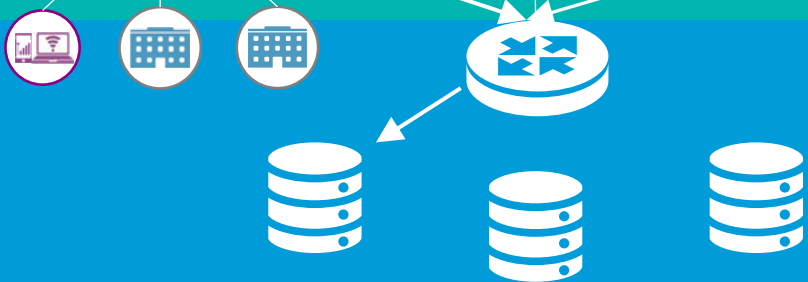


全パケットの
インライン高速処理

>150DCs



NANOLOG



匿名化/圧縮されたログを
指定パスに保存・送信

Central Authority(CA)



||



- “Control Plane”
- Zクラウド全体を管理 (CA of CA)
- 管理者コンソール
- ユーザ設定ポリシー
- 企業アカウントごとのユニークID
(ZEN/Nanolog用)
- 4DCに配備

UX重視の管理コンソール

完全日本語対応UI



推奨設定の表示



効果の分かるレポート



初めての方でも直感的に設定・運用可能な管理コンソール

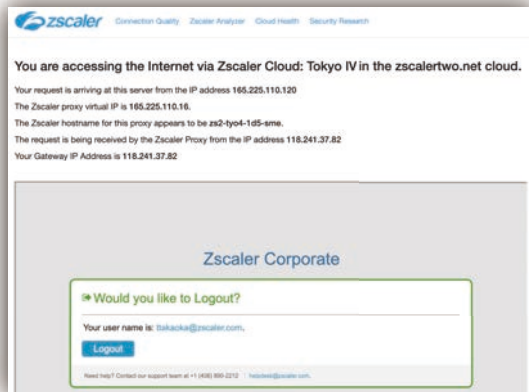
Zscaler Enforcement Nodes(ZEN)



- “Data Plane”
- 通信の高速処理、ポリシー実行
- ユーザ通信受信時、CAからポリシーをロード（200msec）
- μ sec単位でのプロキシ処理実行
- ハードディスクへの書込みは一切なし
- ログの圧縮処理と転送
- 150DCに配備
(各サイトによってノード数は異なる)

UX重視の運用ツール

プロキシ接続テスト



zscaler Connection Quality Zscaler Analyzer Cloud Health Security Research

You are accessing the Internet via Zscaler Cloud: Tokyo IV in the zscalertwo.net cloud.

Your request is arriving at this server from the IP address 165.225.110.120
The Zscaler proxy virtual IP is 165.225.110.16.
The Zscaler hostname for this proxy appears to be zs2-tyo4-1d5-sme.
The request is being received by the Zscaler Proxy from the IP address 118.241.37.82
Your Gateway IP Address is 118.241.37.82

Zscaler Corporate

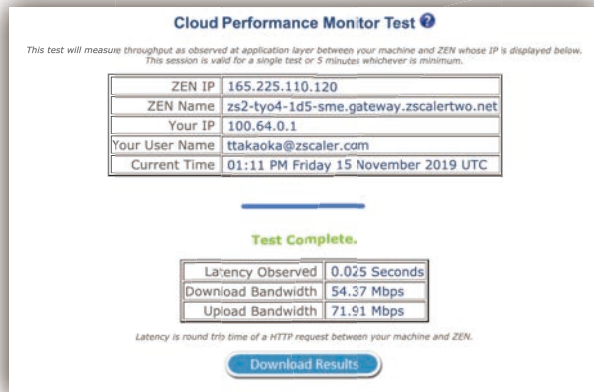
Would you like to Logout?

Your user name is: ttakaoka@zscaler.com.

Logout

Need help? Contact our support team at +1 (888) 859-2212 | helpdesk@zscaler.com.

遅延確認ツール



Cloud Performance Monitor Test

This test will measure throughput as observed at application layer between your machine and ZEN whose IP is displayed below.
This session is valid for a single test or 5 minutes whichever is minimum.

ZEN IP	165.225.110.120
ZEN Name	zs2-tyo4-1d5-sme.gateway.zscalertwo.net
Your IP	100.64.0.1
Your User Name	ttakaoka@zscaler.com
Current Time	01:11 PM Friday 15 November 2019 UTC

Test Complete.

Latency Observed	0.025 Seconds
Download Bandwidth	54.37 Mbps
Upload Bandwidth	71.91 Mbps

Latency is round trip time of a HTTP request between your machine and ZEN.

Download Results

サービス状態確認



これらの運用ツール、サイトはウェブにて公開されています。

クラウドサービスだからこそ、問題発生時はこれらの可視化が重要です



- “Statistics Plane”
- ログルータとNanologクラスタから構成
- 指定された地域のNanologへ保存
- 保存期間は6ヶ月
- オンプレSIEMへの転送には受信用VMが必要 (NSS)

ログの肥大化を防ぐ技術



平文でのログ出力

重複排除

匿名化

圧縮

ログサイズ : **1/50** Nanolog™



Thank You

NEXT STEPS