ThousandEyes
テクニカル ワークショップ
後編

サウザンドアイズ

ThousandEyes is
now part of Cisco.

本日の内容

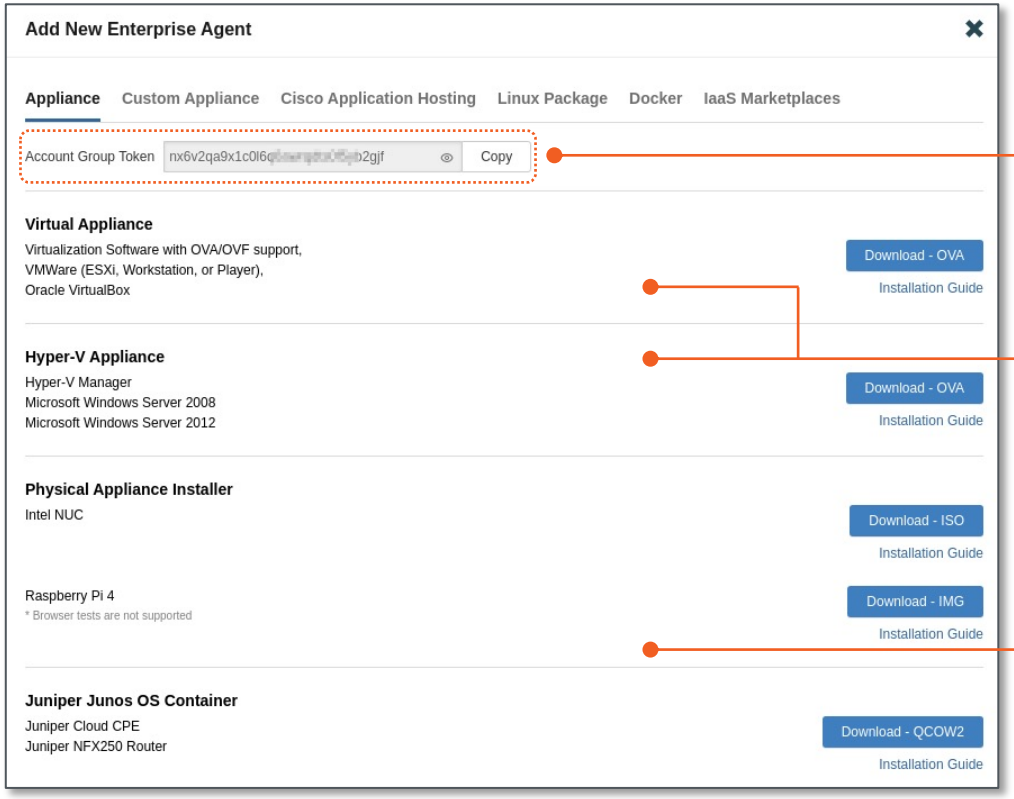
- Enterprise エージェント
- ネットワークテスト
- Webプロキシ環境の可視化
- オンラインビデオ会議の監視
- DNSサービスの監視
- インターネットにあるサービスの経路監視 (BGP)*
- ThousandEyes API *
- Q&A

Enterprise エージェント
（社内エージェント）

Enterprise エージェント

- ユーザーの選んだ場所にインストールできる「マイ・エージェント」
- 仮想システムや物理サーバーで動作可能
  - 仮想アプライアンスは ESXi, Hyper-V, QEMU/KVM, Virtualbox などをサポート
  - Linux サーバーのパッケージ (RHEL/CentOS, Ubuntu)、Linuxコンテナ（Docker）
  - 物理アプライアンスは Intel NUCとRaspberry Pi 4 を正式サポート
- Cisco ハードウェア (2020/03)
  - Cisco 1000 ASR
  - Cisco 4000 ISR
  - Cisco Cat 9000
  - Cisco Cat 9300 (OSに組み込み)
- Enterpriseエージェントの機能はCloudエージェントと同じ

Enterprise エージェントのインストール：アプライアンス



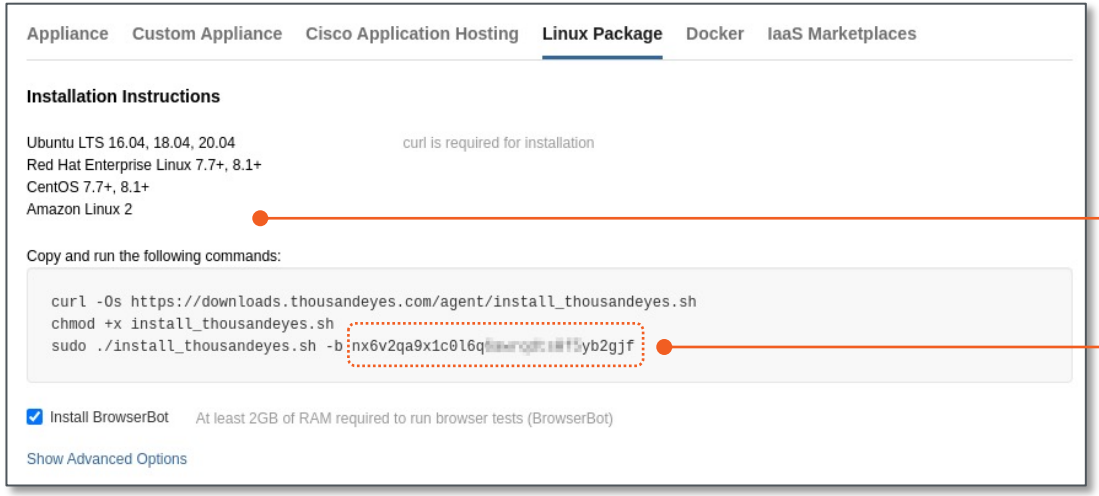
アカウントのトークン
エージェントをこのアカウントに紐付ける

仮想アプライアンス
ローメンテナンスのエージェント
ESXi, QEMU/**KVM**,
Hyper-V, Player, Virtualbox

物理アプライアンス
ローメンテナンスのエージェント
Intel NUC, Raspberry Pi 4

(RasPi はBrowser系の監視テスト：
Pageload, Transactionテストをサポートしません)

Enterprise エージェントのインストール：Linux のパッケージ



Linux のパッケージ
Ubuntu, RHEL, CentOS のサーバーに
エージェントをインストール

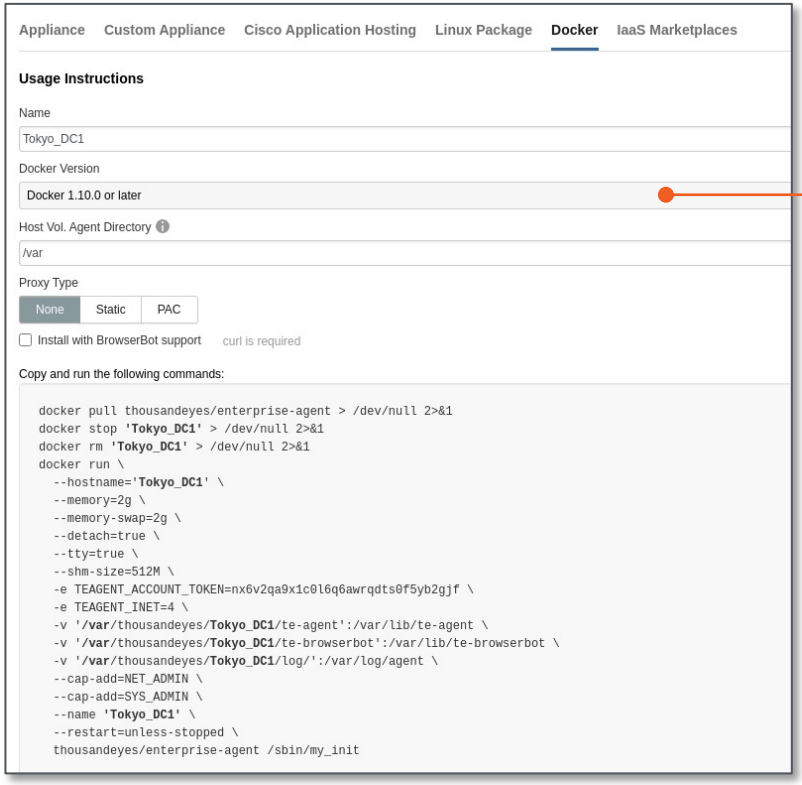
アカウントのトークン

エージェントの動作環境は
アプライアンスと同じ：

vCPU x 2
エージェント用メモリ 2GB
エージェント用ストレージ 20GB

- Linuxの設定でインターフェイスやVRFを複数使うことが可能
- サーバーOSのメンテナンスとハードニングはお客様が担当

Enterprise エージェントのインストール：Linux コンテナ



Docker を使ったインストール
LinuxのDistributionの制限は無し
(サーバーOSのメンテナンスとハードニングはお客様が担当)

エージェントの動作環境は同じ：

vCPU x 2
エージェント用メモリ 2GB
エージェント用ストレージ 20GB

Enterprise エージェントのインストール：Cisco ルーター

Appliance | Custom Appliance | **Cisco Application Hosting** | Linux Package | Docker | IaaS Marketplaces

Cisco IOS XE Docker Appliance

Catalyst 9000 Series Switches

* Browser tests are not currently supported. SSD not required.

Download - TAR

Installation Guide

Copy, adapt, and run the following commands:

```
Device> enable
Device# app-hosting install appid DESIRED_APP_ID package https://downloads.thousandeyes.com/enterprise-agent/tho
usandeyes-enterprise-agent-3.0.cat9k.tar
Device# configure terminal
Device(config)# app-hosting appid DESIRED_APP_ID
Device(config-app-hosting)# app-vnic AppGigabitEthernet trunk
Device(config-config-app-hosting-trunk)# vlan DESIRED_VLAN guest-interface 0
Device(config-config-app-hosting-vlan-access-ip)# guest-ipaddress DESIRED_IP netmask DESIRED_NETMASK
Device(config-config-app-hosting-vlan-access-ip)# exit
Device(config-config-app-hosting-trunk)# exit
Device(config-app-hosting)# app-default-gateway GATEWAY_IP guest-interface 0
Device(config-app-hosting)# name-server0 NAMESERVER1_IP
Device(config-app-hosting)# name-server1 NAMESERVER2_IP
Device(config-app-hosting)# app-resource docker
Device(config-app-hosting-docker)# prepend-pkg-opts
Device(config-app-hosting-docker)# run-opts 1 "-e TEAGENT_ACCOUNT_TOKEN=nx6v2qa9x1c0l6q6awrqdts0f5yb2gjf"
Device(config-app-hosting-docker)# run-opts 2 "--hostname DESIRED_AGENT_HOSTNAME"
Device(config-app-hosting-docker)# exit
Device(config-app-hosting)# exit
Device(config)# exit
Device# write memory
Device# app-hosting activate appid DESIRED_APP_ID
Device# app-hosting start appid DESIRED_APP_ID
Device#
```

Cisco IOS XE KVM Appliance

Integrated Services Router (ISR)
Aggregation Services Router (ASR)

Download - Cisco OVA

Installation Guide

Catalyst 9000 Series Switches

* Full test suite supported. SSD required.

Download - TAR

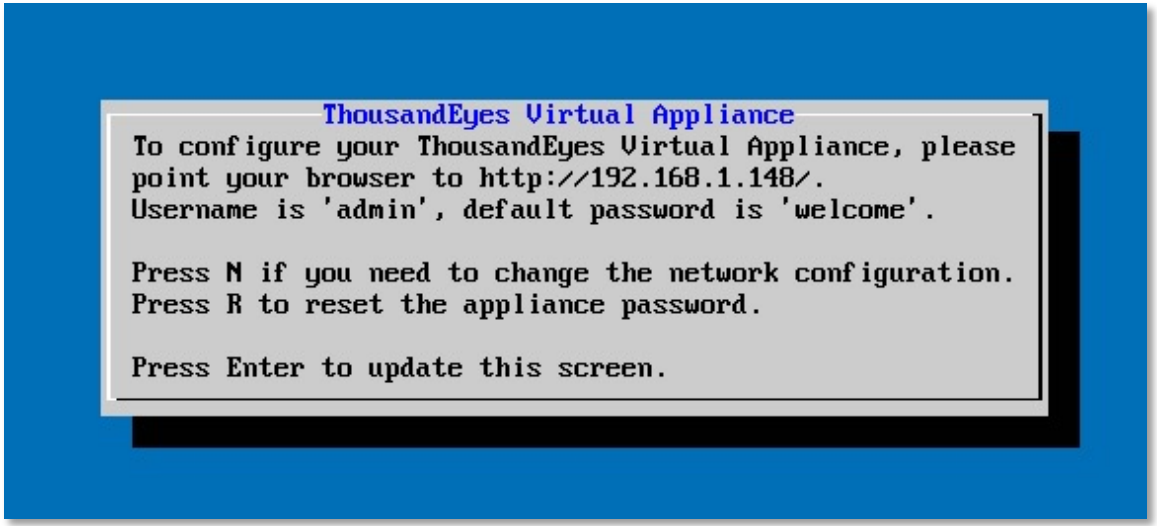
Installation Guide

現在のサポート状況

- ISR 4000
- ASR 1000
- Catalyst 9000
- Catalyst 9300
- Catalyst 9400 (2021/4 予定)
- Catalyst 9500 (2021/8 予定)
- Catalyst 9600 (2021/8 予定)
- Catalyst 8200 (2021/8 予定)
- Catalyst 8300 (2021/8 予定)

Enterprise エージェントの起動 (アプライアンス型)

- 仮想アプライアンスの電源をON
- 起動後、エージェントを設定をするURLとログイン情報が表示



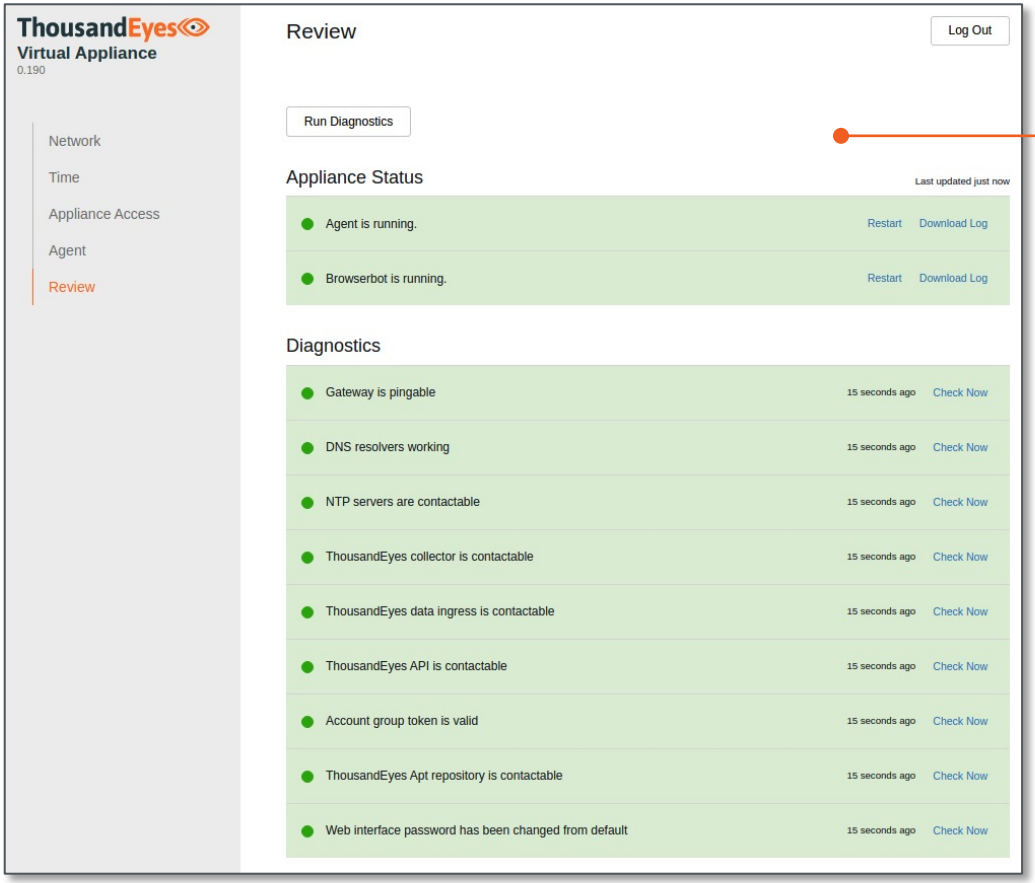
コンソール画面表示内容：

- WebUIのURL
- ユーザー名 (admin)
  パスワード (welcome)
- ネットワークの設定
- パスワードリセット

Enterprise エージェントの初期設定 (アプライアンス型)

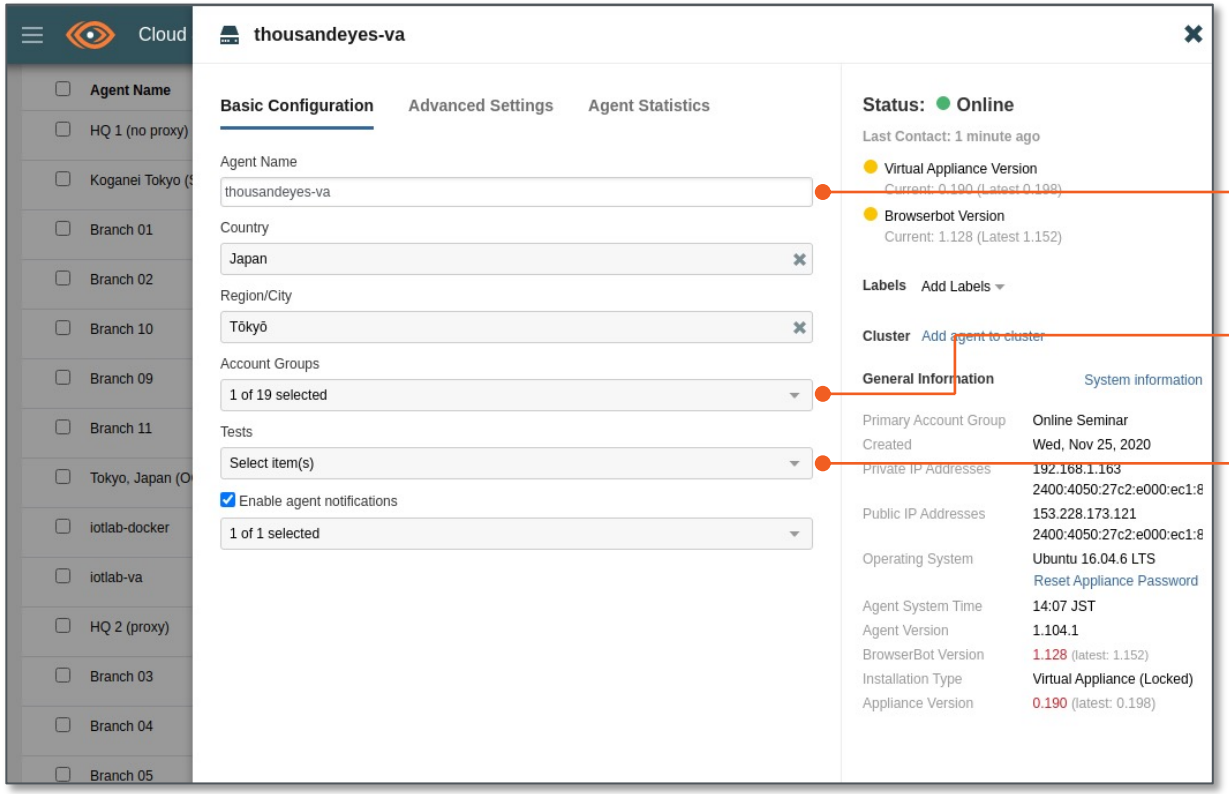
1. Self-signed デジタル証明書の警告は無視 ☺
2. ディフォルトのパスワードの変更
3. アカウントに紐付けるトークンを設定
4. Status 状態の確認
5. 追加設定 (optional) :
   - DNS サーバー
   - Proxy サーバー
   - Proxy 用のデジタル証明書のインストール
   - ソフトウェアのアップデートに使う Proxy サーバーの設定
   - クラウドアプリから設定の仕上げ

Enterprise エージェントの設定確認画面



この画面の項目が
全て緑色になればエージェントの設定完了

クラウドアプリからエージェントの設定

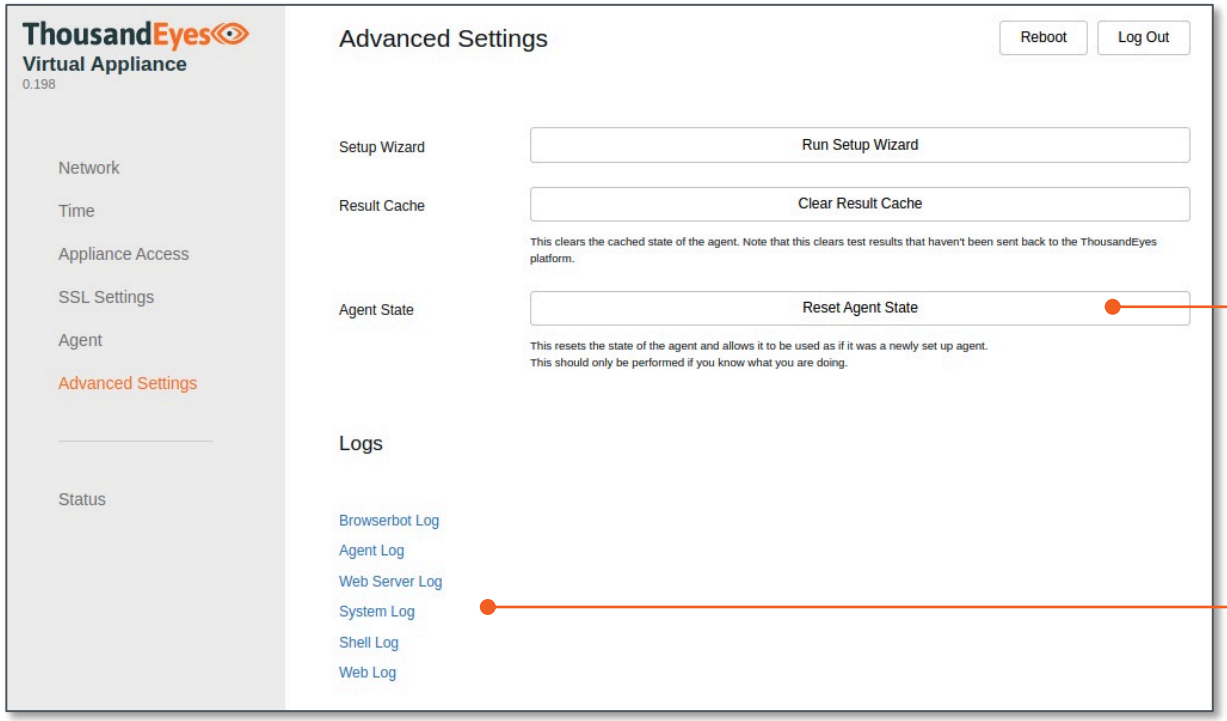


ディフォルトの仮想エージェント名
(もっと分かりやすい名前に変更)

このエージェントを使える
アカウントグループを指定

新しいエージェントを
設定済みの監視テストに追加

Enterprise エージェントを別のアカウントで使うには



エージェントを
現在のアカウントから削除
(ネットワーク設定は残ります)

エージェントのトラブルシュートに
役立つログがここから取得できます

Enterprise エージェントに関する資料

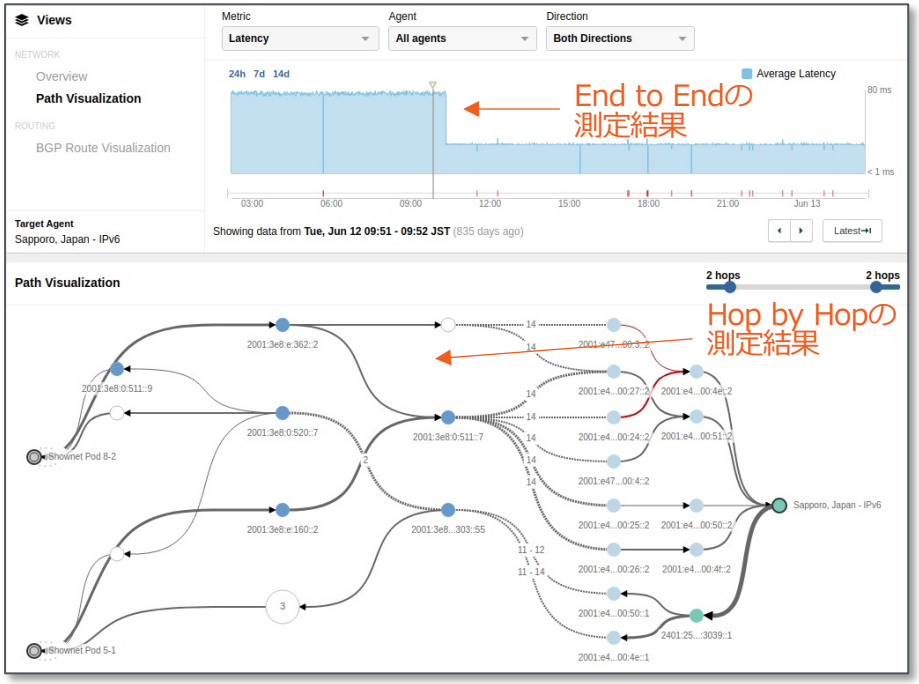
- 物理サーバーへのインストール（日本語）
- 仮想サーバーへのインストール（日本語）
- 仮想サーバーへのインストール (mp4 ビデオ, 2MB）
- Enterpriseエージェントの設定方法（日本語）
- Enterprise Agent に関するオンラインマニュアル

ネットワークテスト

Agent to Server テスト
エージェントとサービス間の可視化

ネットワーク テストとは？

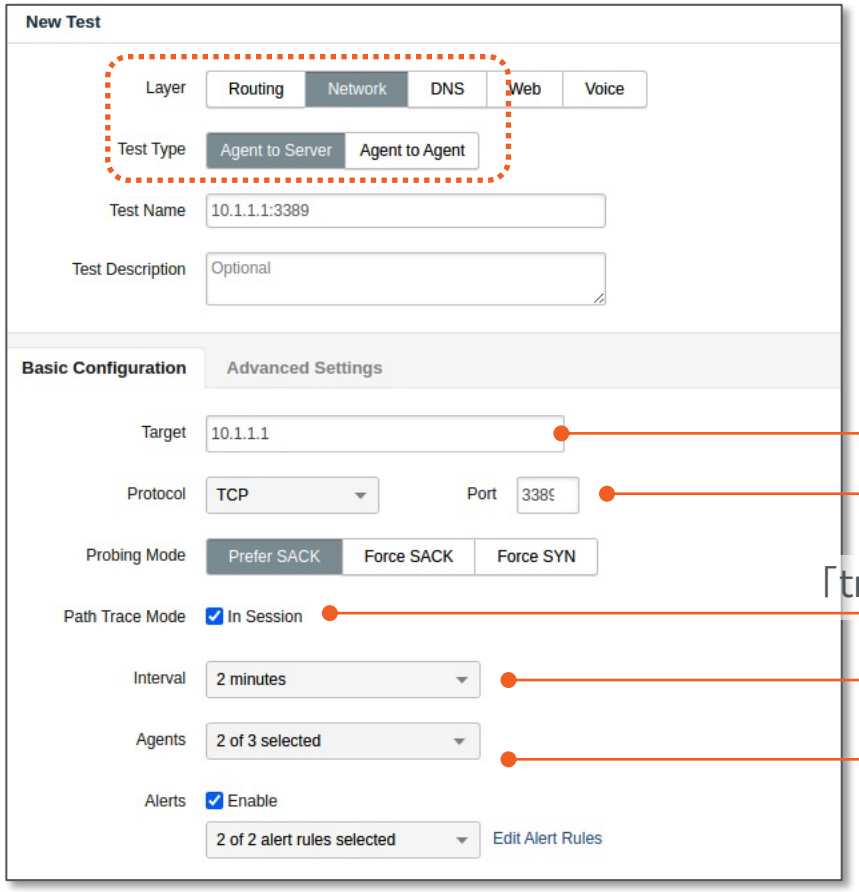
- アプリケーションサービスとエージェント間の可視化と品質測定
- ネットワークパスの可視化
  - マルチパスの検知
- ネットワークパスの品質測定
  - End to End
  - Hop by Hop
  - 双方向（上り+下り）
- アプリケーションの死活監視



Agent to Server テスト

- Serverとは TCP/ICMP に応答する送信先ホスト
  - TCP：imap/pop, rdp, proxy のポート など
  - ICMP：TCPに反応しないIPインターフェイス
- Agentは Cloud、Enterprise、Endpoint エージェント
- 任意のTCPポート、ICMPをテストに使用可能
- ICMPよりもTCPが優れた可視性を提供 (マルチパスの検知)

Agent to Server テスト設定



ターゲット（IP,ドメイン名）

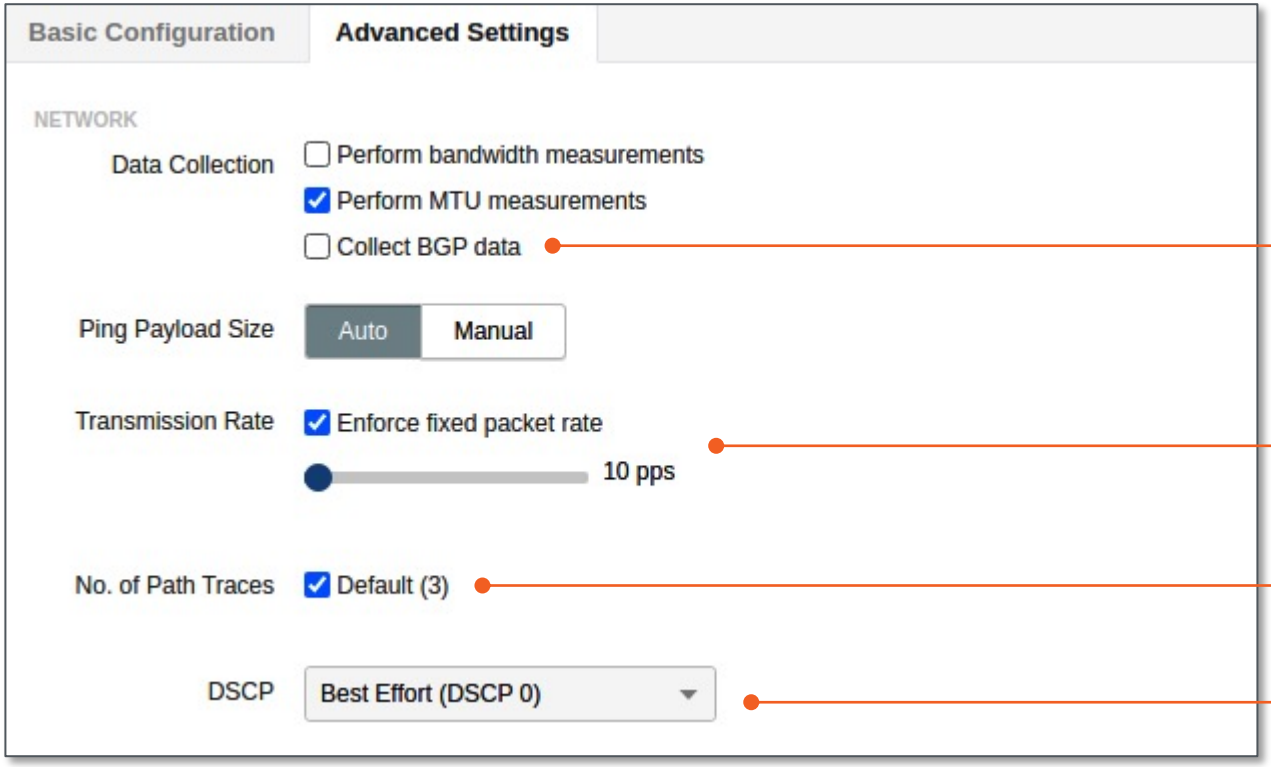
TCP/ポート番号、ICMP

「tracerouteを止めるFirewall」対策

テストの実行間隔

テストを実行するエージェント

Agent to Server テスト設定



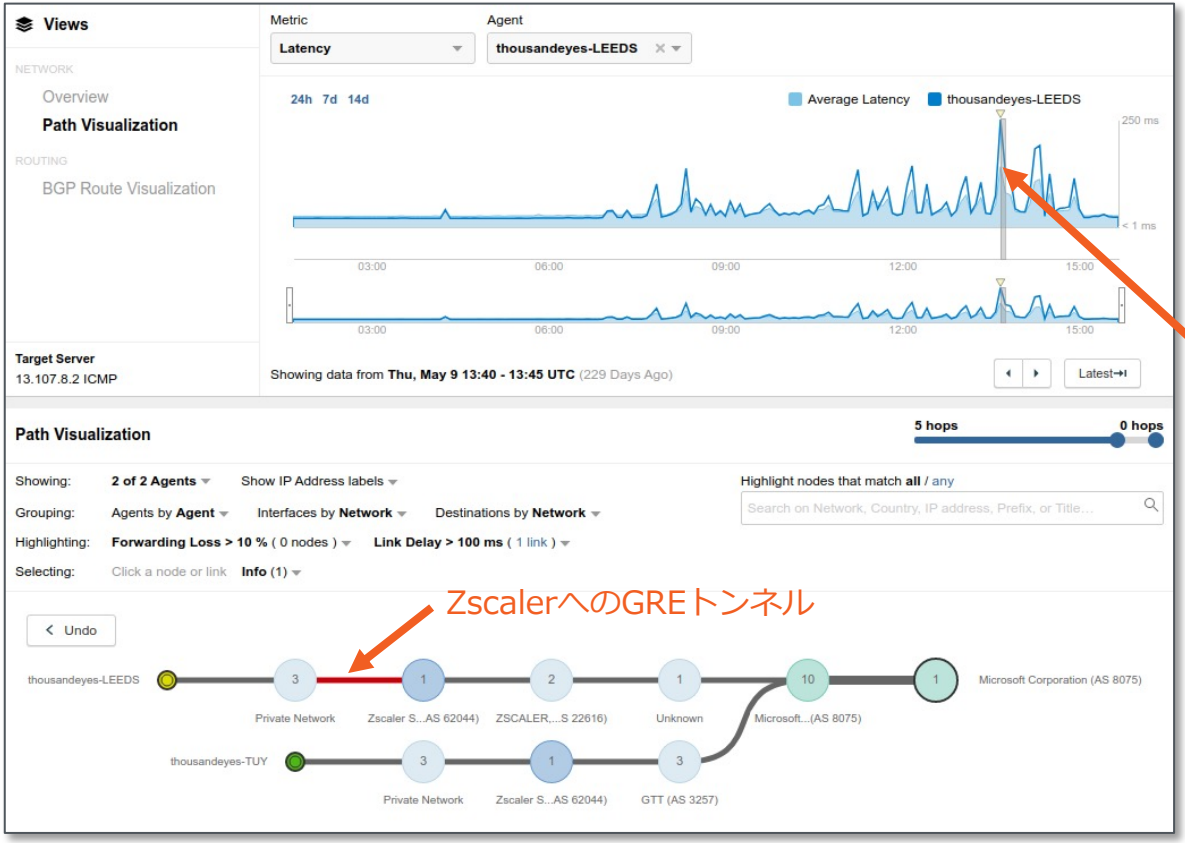
ターゲットの
経路データの取得

End-to-End
トラフィックの
送信レート

検出する
マルチパスの数

DSCPの値を設定

監視例 (1)：Zscalerを経由するMS Skypeへのパス



スナップショット

最大100msのRTTが推奨される
MS Skypeのトラフィックに
250ms以上の遅延が発生

監視テストはICMPを使った
Agent to Server テスト

ネットワークテスト

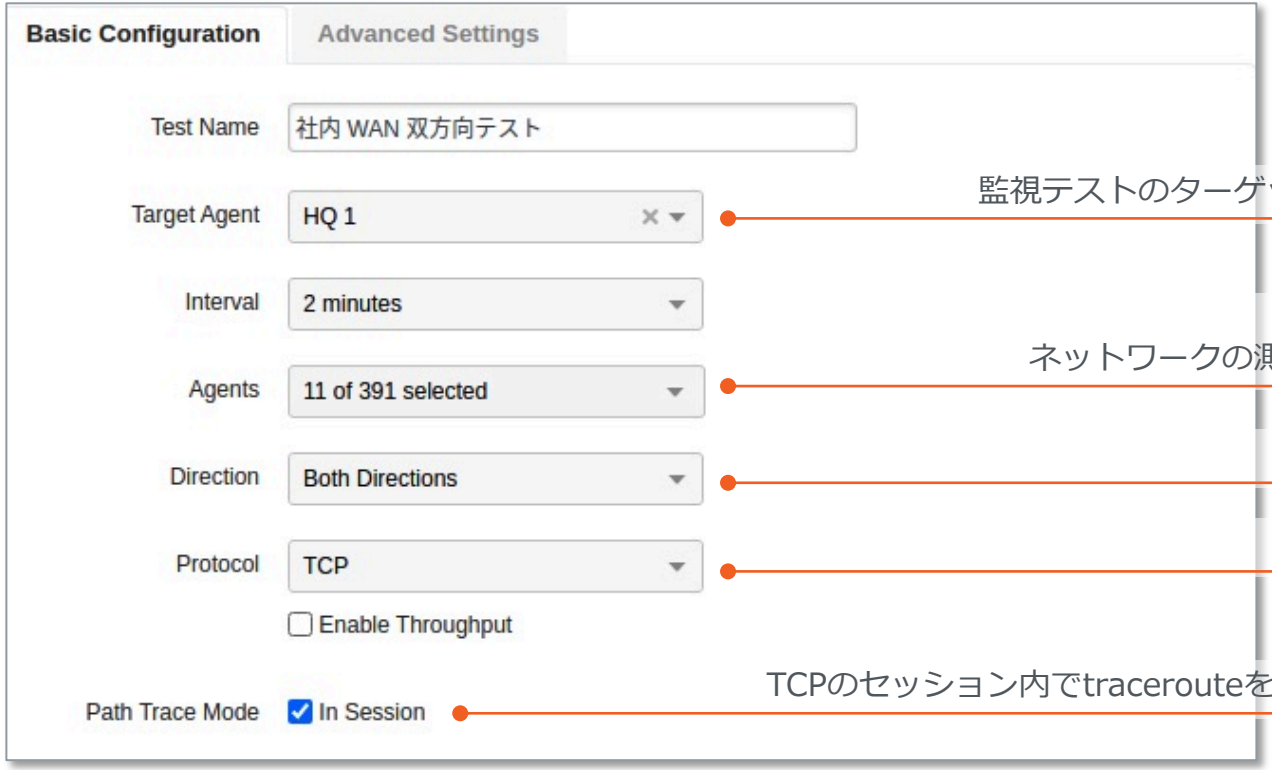
Agent to Agent テスト
エージェント間の可視化

Agent to Agent テスト

- エージェント間（ネットワーク間）のネットワーク測定
- 双方向のネットワークパスの品質測定と可視化
- 任意のTCP/UDPポートをテスト用に使用可能
- ICMPよりもTCPが優れた可視性を提供（マルチパスを検知）
- 環境によってはネットワークの設定変更が必要
  - 双方向テストではFirewallに外部から社内エージェント宛のルールを追加
  - 社内エージェント宛のNAT設定の変更

★ Endpointエージェントを使った Agent-to-Agent テストは不可

Agent to Agent テストの設定



監視テストのターゲットとなるエージェント (1台)

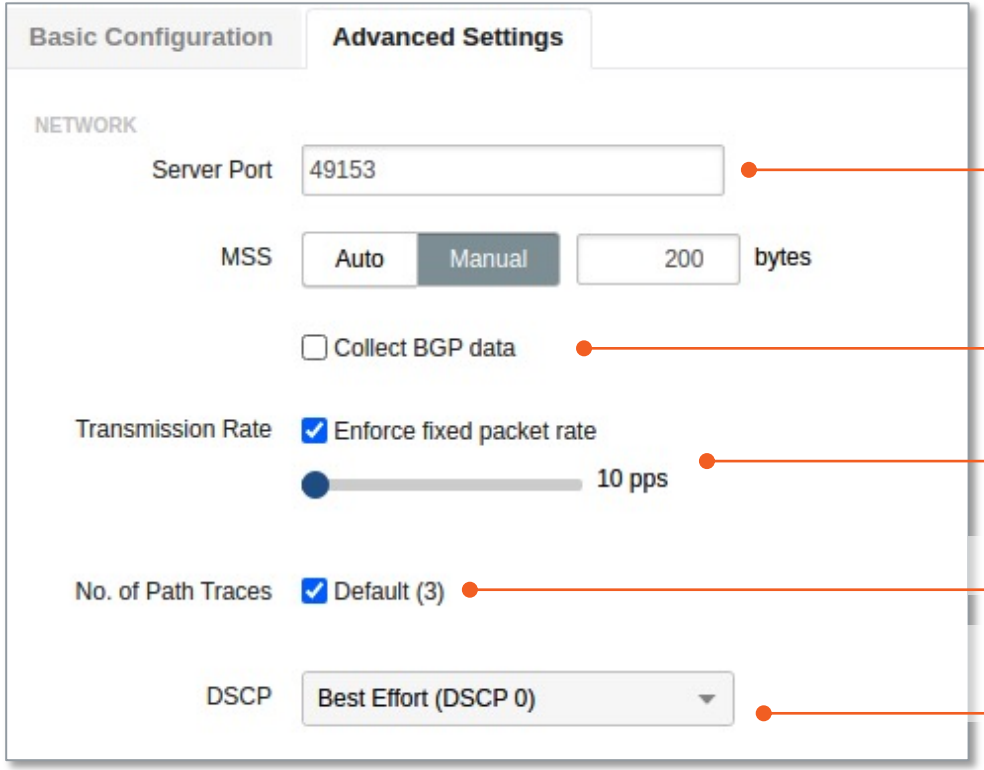
ターゲットのエージェントと
ネットワークの測定をするエージェント (複数)

測定トラフィックの方向

TCP/UDP

TCPのセッション内でtracerouteを実行するモード (IPS/FW 対策)

Agent to Agent テストの設定



TCP/UDP 受信ポート

ターゲットの経路情報の取得
プライベートIPでは必要なし

測定トラフィックの速度

検知するマルチパスの数

DSCPの設定
(ルーターホップ毎にDSCPが見える)

Agent to Agent の監視テスト例 (1)

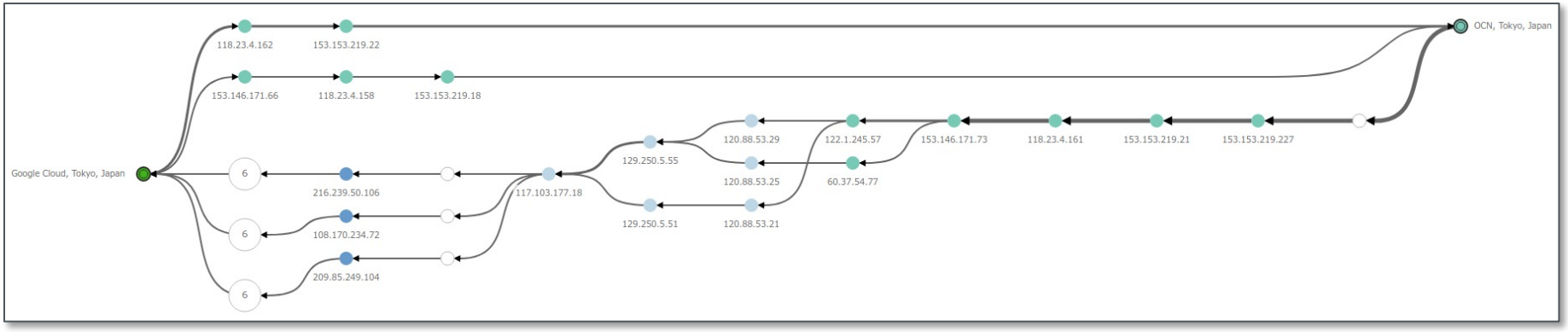
Agent to Agent テストを使った支店・本社WANの双方向品質監視
ISPのピアリングが変更して、ネットワークの遅延が大きく変わる

共有リンク

Agent to Agent の監視テスト例 (2)

上りと下りの経路が異なるネットワークパス

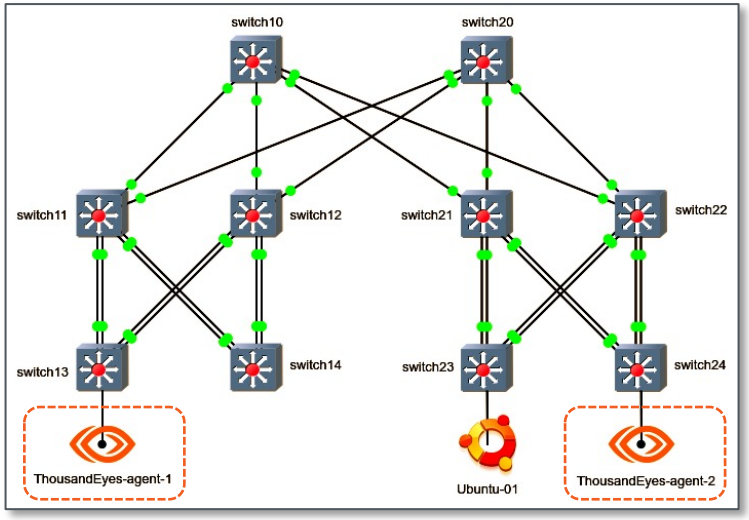
双方向の監視テストを実行して分かる 非対称ルーティング

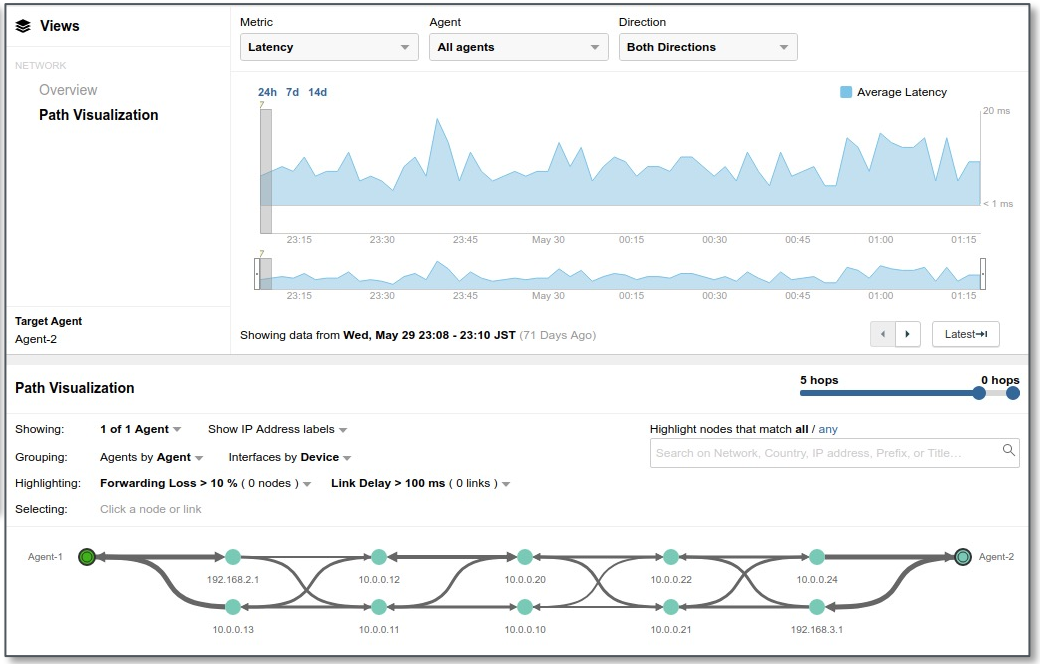


共有リンク

監視例 (3)：データセンターLANの監視

IP/Clos ネットワークのアプリケーションパスの可視化
Agent-to-Agentの双方向テストを使い多数のパスのある
ネットワークのアプリケーションパスを可視化



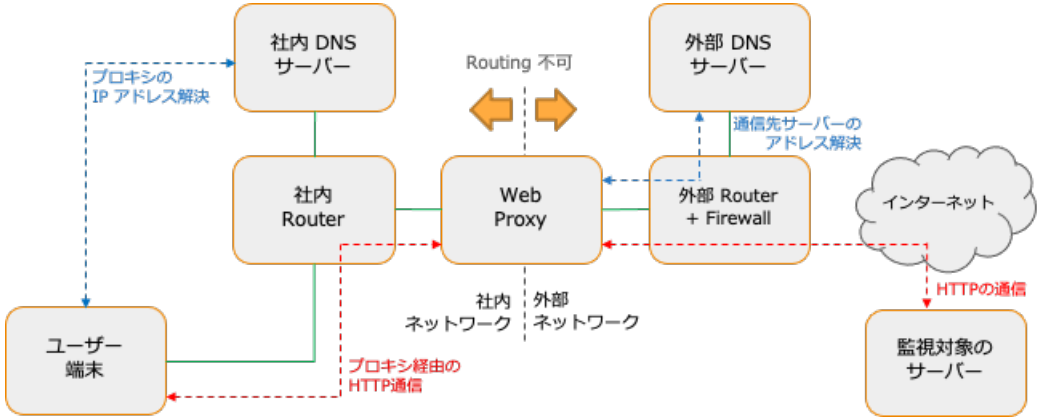


スナップショットの共有リンク

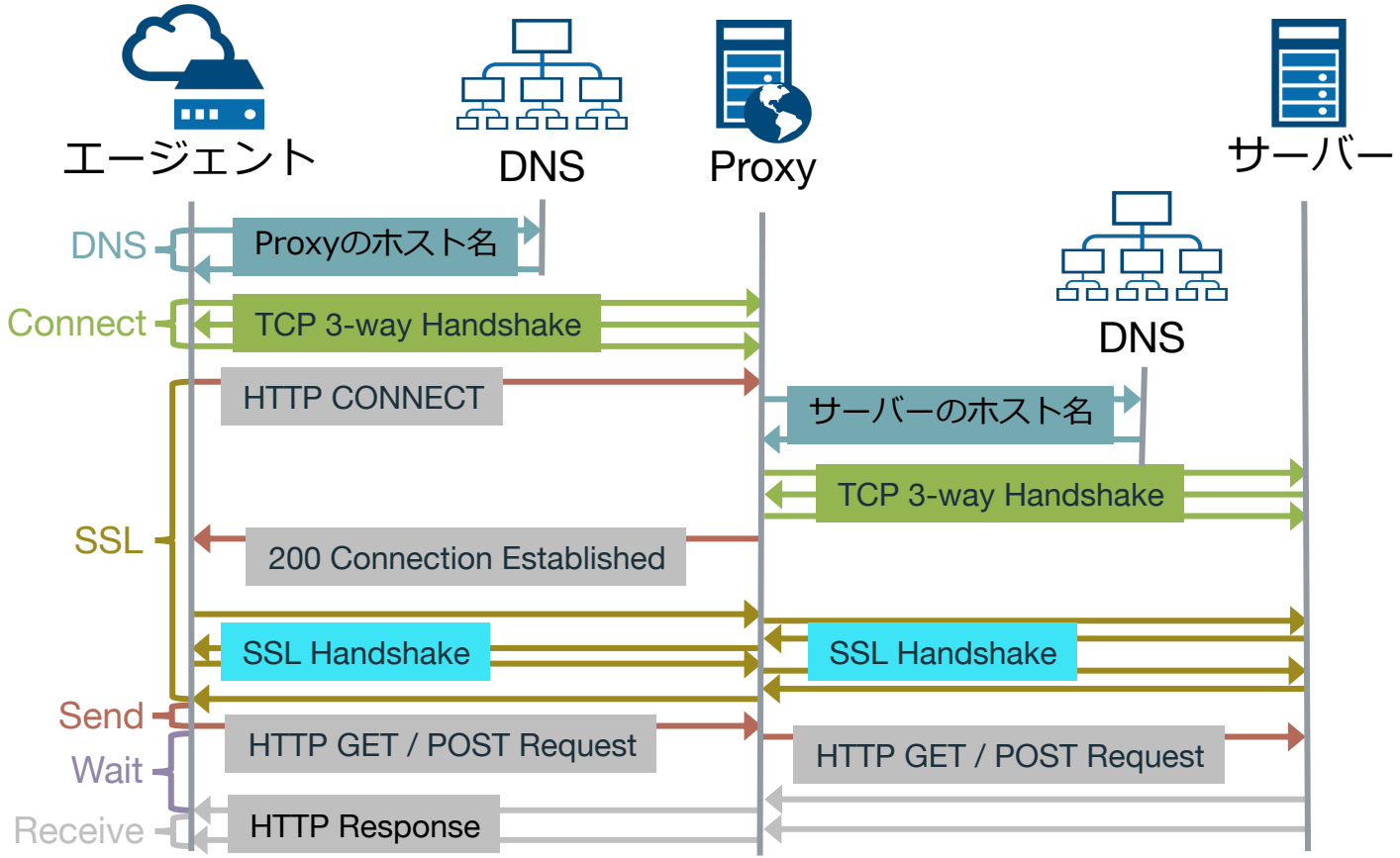
Web プロキシ環境の可視化

Web プロキシ

1. 社内ネットワークからインターネットへのWeb アプリのトラフィック制御を実行
2. Web プロキシの種類：
   a. ユーザー端末にプロキシの設定をする Explicit 構成（最も一般的構成）
   b. プロキシ指定をしていないクライアントのトラフィックを外部デバイスがプロキシにリダイレクトする Transparent 構成
   a. 社内ネットワークと外部ネットワークの通信は全てプロキシを経由する構成 (**下の図**)



Web プロキシを使ったHTTPの動作



エージェントに３種類のプロキシ設定が可能

1. エージェントのWebUIから固定・PACファイルの設定

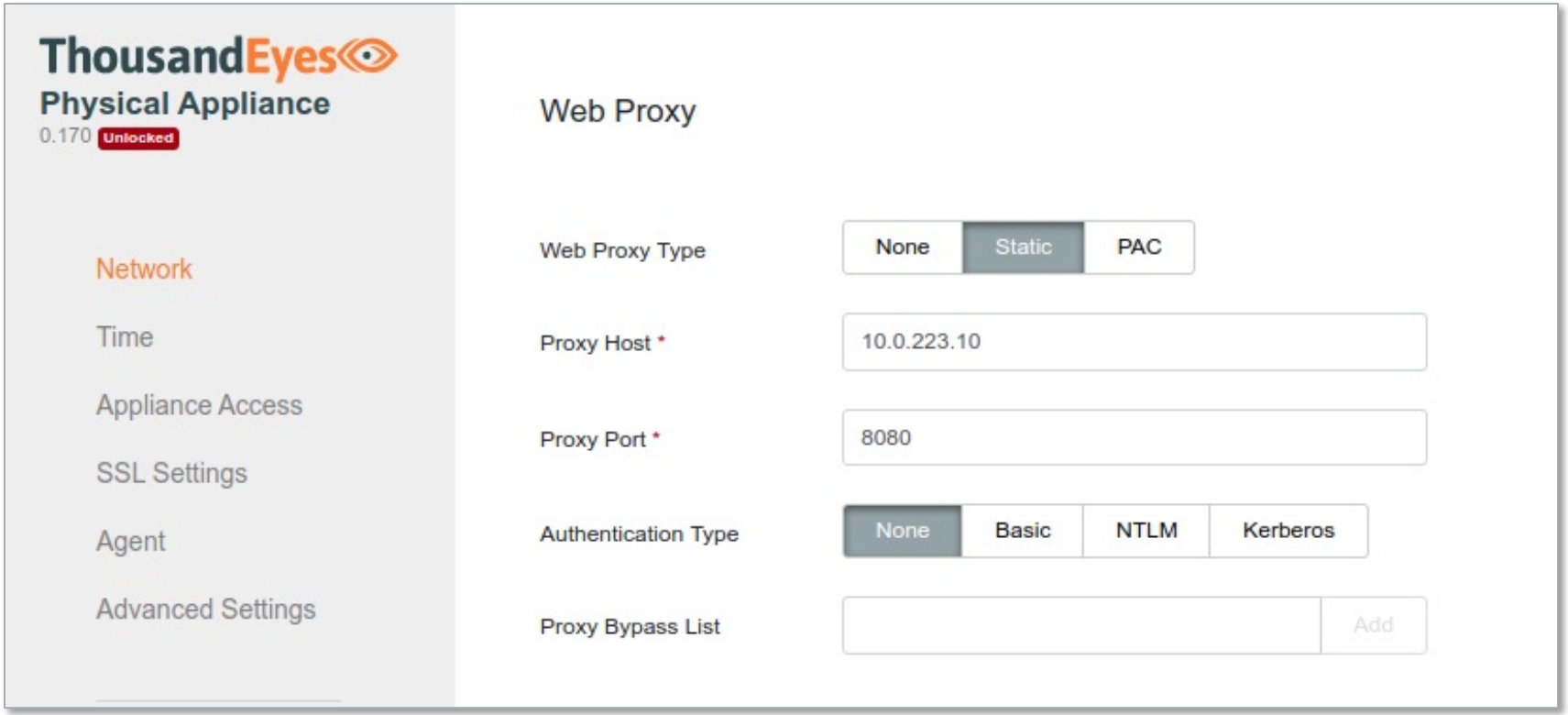
   - 監視テスト内でプロキシ設定を変更しない限りすべての通信 (監視テスト、ThousandEyesとの通信) はプロキシ経由で実行
   - プロキシを経由しないとインターネットに抜けられない環境ではエージェントのWebUIから初期設定の際にプロキシを設定

2. ThousandEyesのクラウドアプリからプロキシの設定

3. 監視テスト毎のプロキシ設定

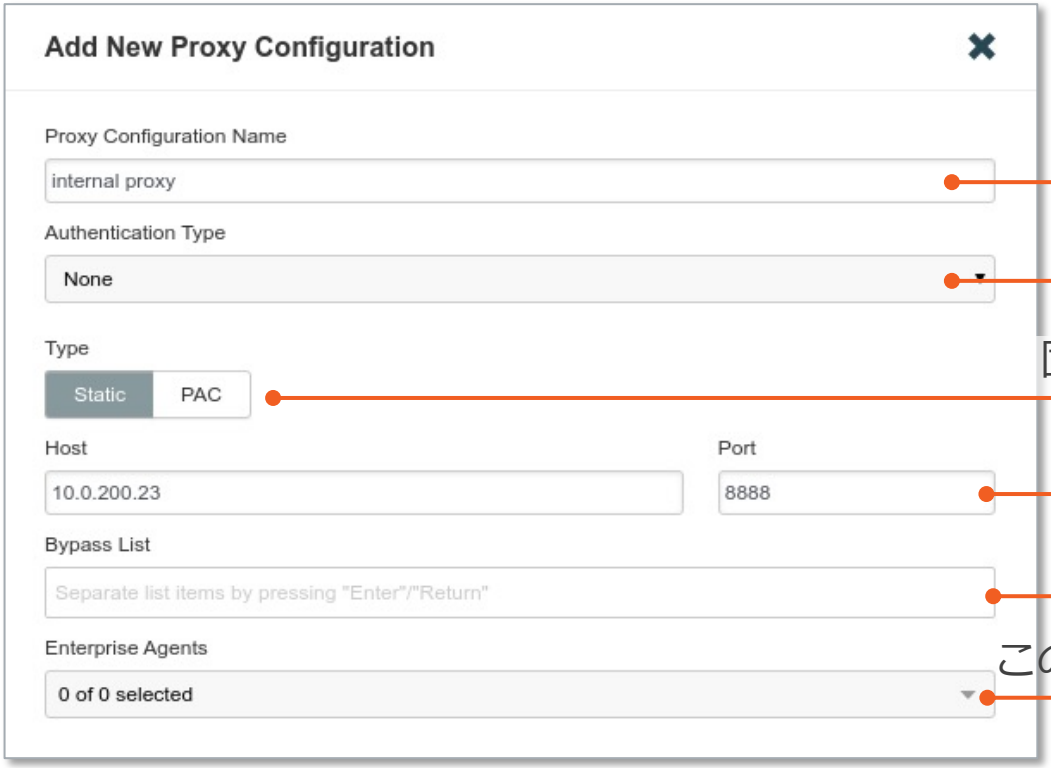
   - テスト毎に異なるプロキシ有り・無しの実行が可能
   - 但しThousandEyesとの通信は1と２で設定したプロキシを経由する

1. エージェントのWebUIからWebプロキシの設定



2.クラウドアプリのUIからWebプロキシの設定

Cloud & Enterprise Agents > Agent Settings > Proxy Settings



このプロキシ構成の名前

認証の設定

固定プロキシ・PACファイルの選択

固定プロキシの設定

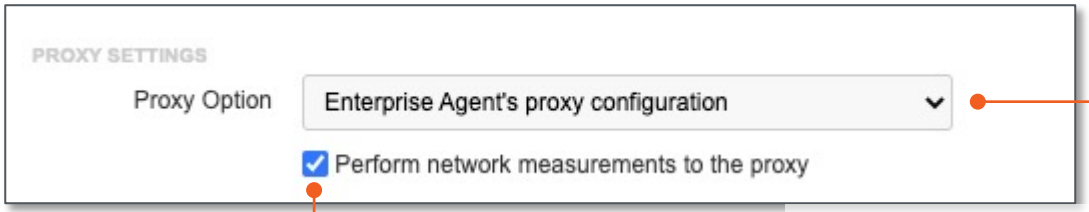
プロキシを経由しないターゲット

このプロキシ設定を使うエージェント

3. 監視テストのプロキシ設定

HTTP / Page Load / Transaction テストの設定画面の Advanced Setting から

a) 監視テストが使用するプロキシの選択と
b) エージェント ⇄ プロキシ間のネットワーク品質測定の設定が可能



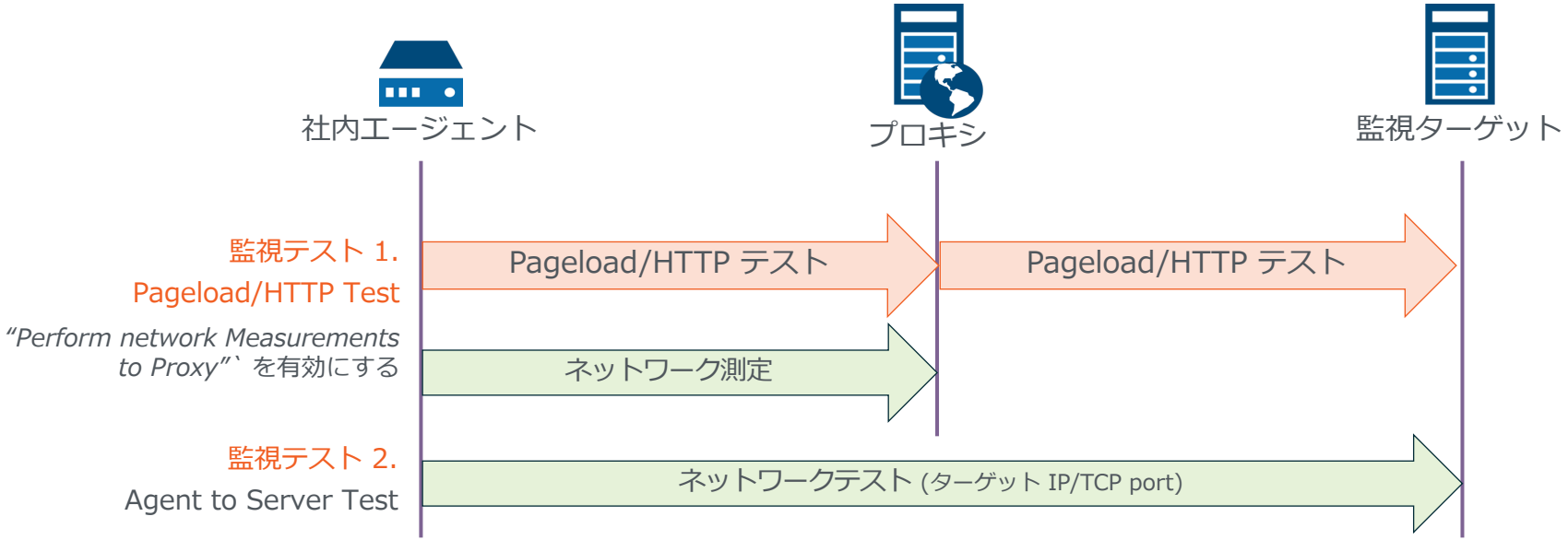
監視テストの実行に使われる
Proxyサーバーの選択

エージェントとProxyサーバー間の
ネットワーク品質測定を実行する

c) 特定の監視テストだけプロキシをバイパスする設定も可能

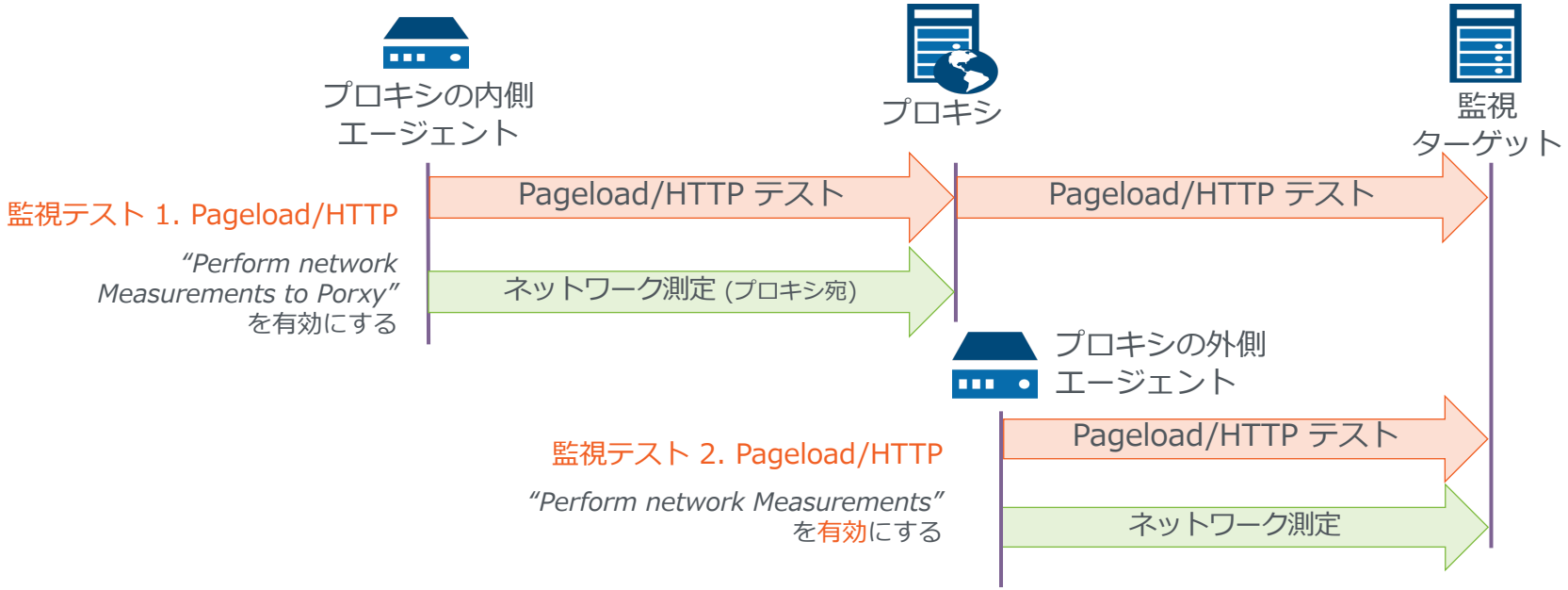
Webプロキシを使ったパスの可視化

(監視ターゲットにエージェントからtracerouteが可能な場合)



1. プロキシを経由するWebアプリのレスポンスとプロキシまでのネットワークパスの品質測定をする HTTP/PageLoad テスト
2. エージェントと監視対象のサーバー間のネットワークの可視化と品質を直接測定する Agent to Server ネットワークテスト

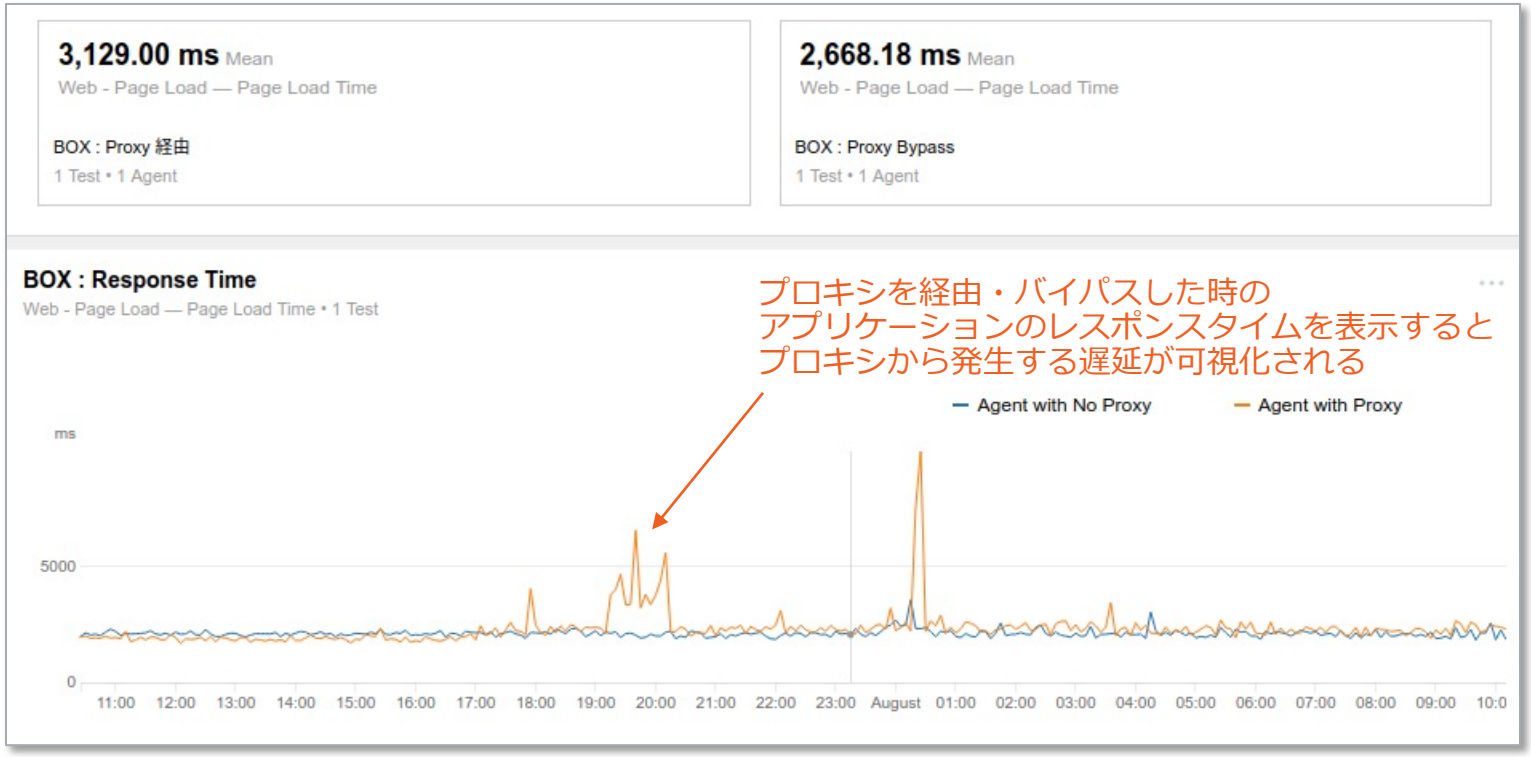
Webプロキシを使ったパスの可視化
(監視ターゲットにエージェントからtracerouteが不可能な場合)



- Proxy経由以外は外部ネットワークに通信不可であるネットワークでは、プロキシを境界線として、プロキシの両側を別に測定する。
- 一般的にはこの方法の監視テストを推奨します。

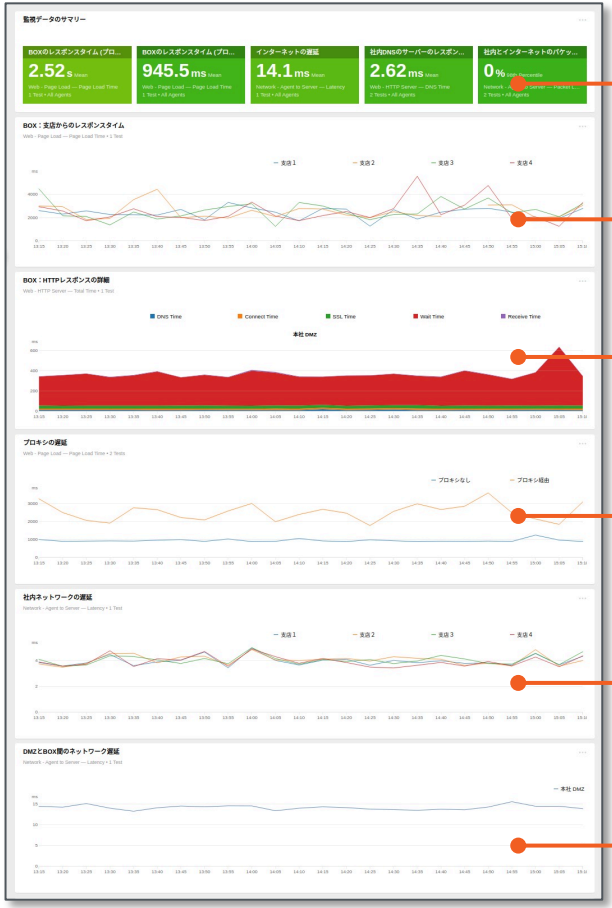
Webプロキシの負荷を監視

レポートやマルチテストViewの機能を使い、プロキシから発生する遅延を監視



Webプロキシ環境の監視レポート

共有リンク



全体のステータス

支店のアプリのレスポンス

レスポンスタイムの詳細

プロキシから発生した遅延

プロキシへの遅延

プロキシの外側から
Webアプリのレスポンス

関係資料

HTTPプロキシを使用したパフォーマンスの測定

Zscaler Web Secure Gatewayの監視

Installing Enterprise Agents in Proxy Environments

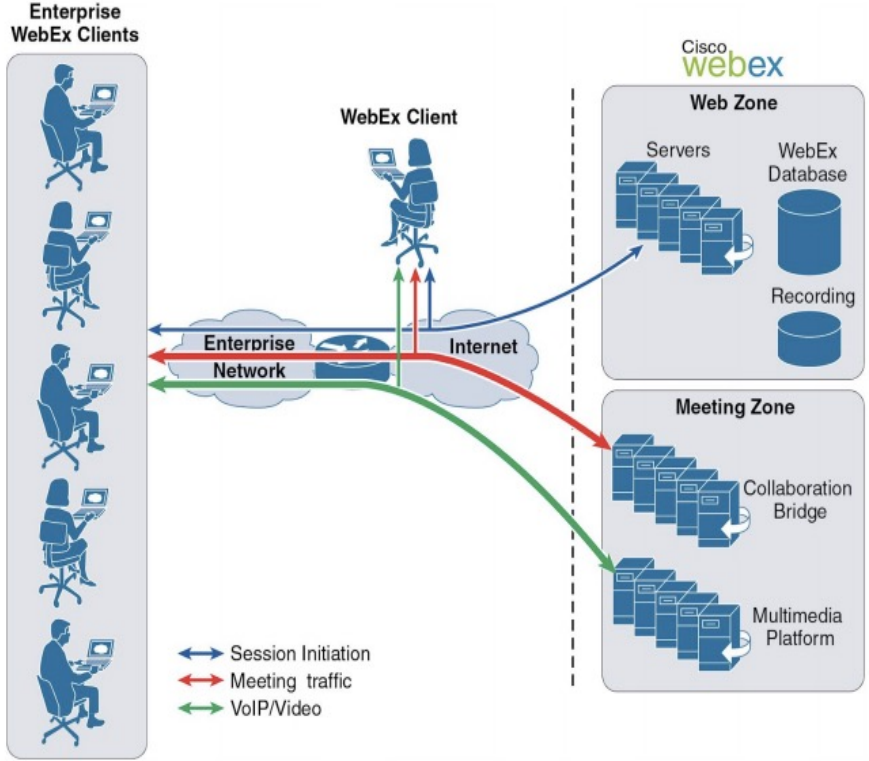
Configuring an Enterprise Agent to Use a Proxy Server

Measuring Performance with HTTP Proxies

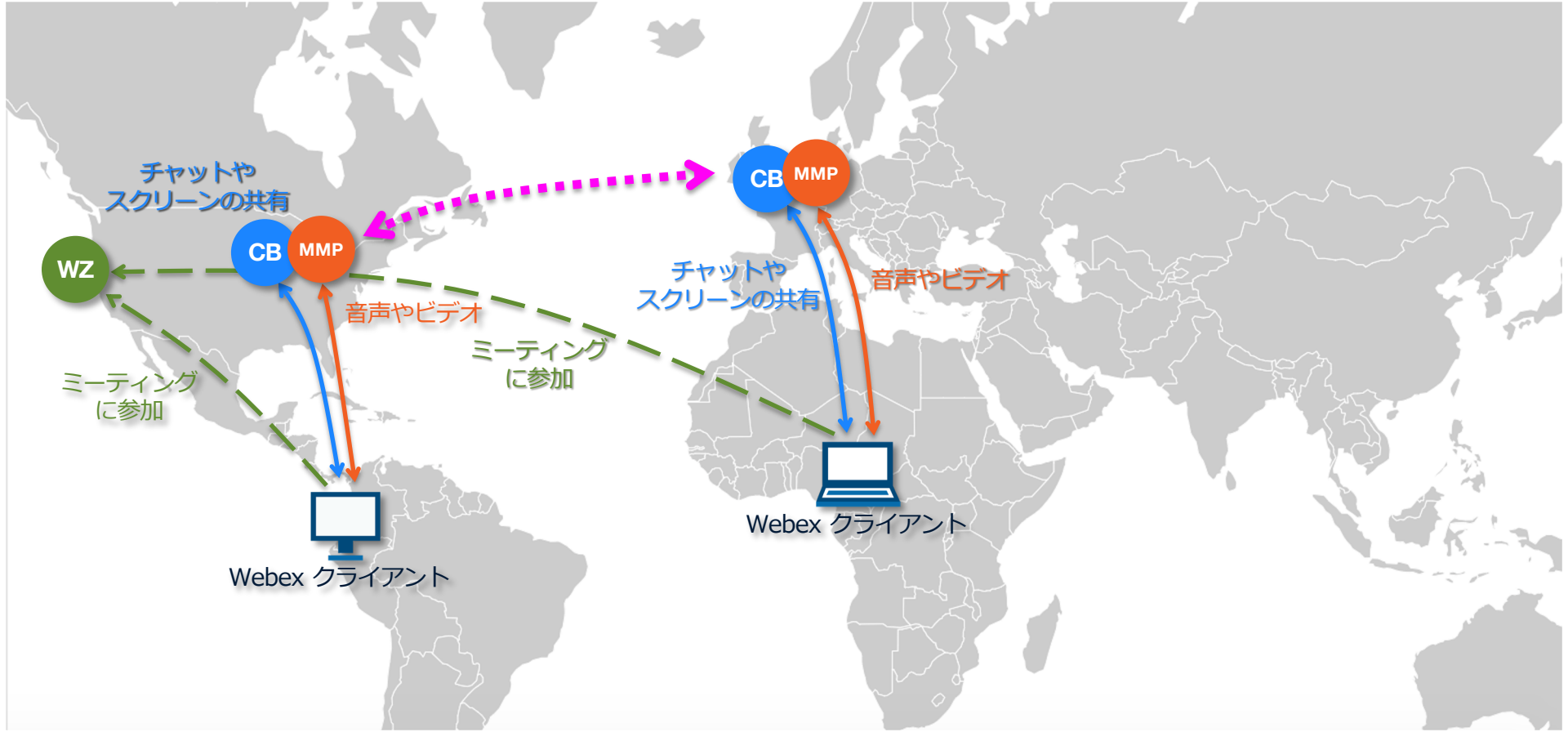
オンラインビデオ会議の監視
Webex

Webex のアーキテクチャ

1. Webexデータセンターは、WebゾーンとMeetingゾーンに分割
2. ユーザーは初めにWebゾーンに接続。Webゾーンは認証、スケジューリング、課金、レポート、レコーディングなどのタスクを処理
3. Meetingゾーンにはチャットやデスクトップ共有などの通信処理をするコラボレーションブリッジ (CB)、会議の音声やビデオストリームの処理するマルチメディア プラットフォーム (MMP)がある
4. WebゾーンのDCはお客様の本社に近いロケーション、会議ゾーンは接続するユーザーに近いDCが選択される



グローバルに分散された会議



Webexの監視ターゲット

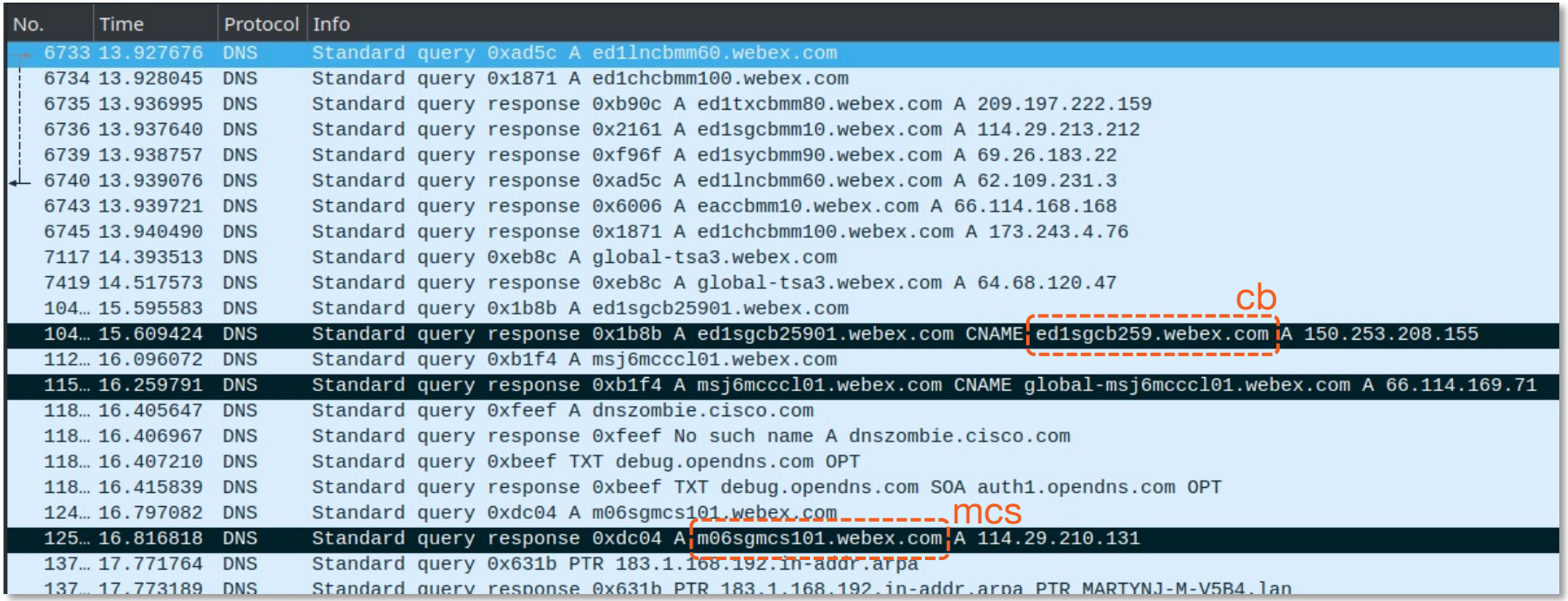
1. MMPやCBは共に数が10,000ノードを超える (2020/4月)
2. Webexのクライアントが接続するMMP/CBは動的に選択されるため、事前に監視ターゲットを選択することは難しい
3. 何処のDCのCB/MMPが選択されるかはパケットキャプチャやDNSのリクエストから確認

CB/MMPのドメイン名:

cb.webex.com のホスト名が Collaboration Bridge、

mcs.webex.com のホスト名が Multimedia Platform

監視テストのターゲットをキャプチャ



Collaboration Bridge (cb) : **ed1sgcb259.webex.com**
Multimedia Platform (mmp) : **m06sgmcs101.webex.com**

監視テストに使える
日本国内Webex DCの監視ターゲット

パケットキャプチャやDNSのログにアクセスできない場合、
以下の日本国内にあるWebEx DC内のサーバー宛に監視テストを設定

サービスの種類	ドメイン名のフォーマット	ドメイン名
Multimedia Platform	*jpmcs*.webex.com	m06jpmcs113.webex.com m06jpmcs201.webex.com m06jpmcs212.webex.com
Collaboration Bridge	*jp2cb*.webex.com	ed1jp2cb53201.webex.com ed1jp2cb52202.webex.com

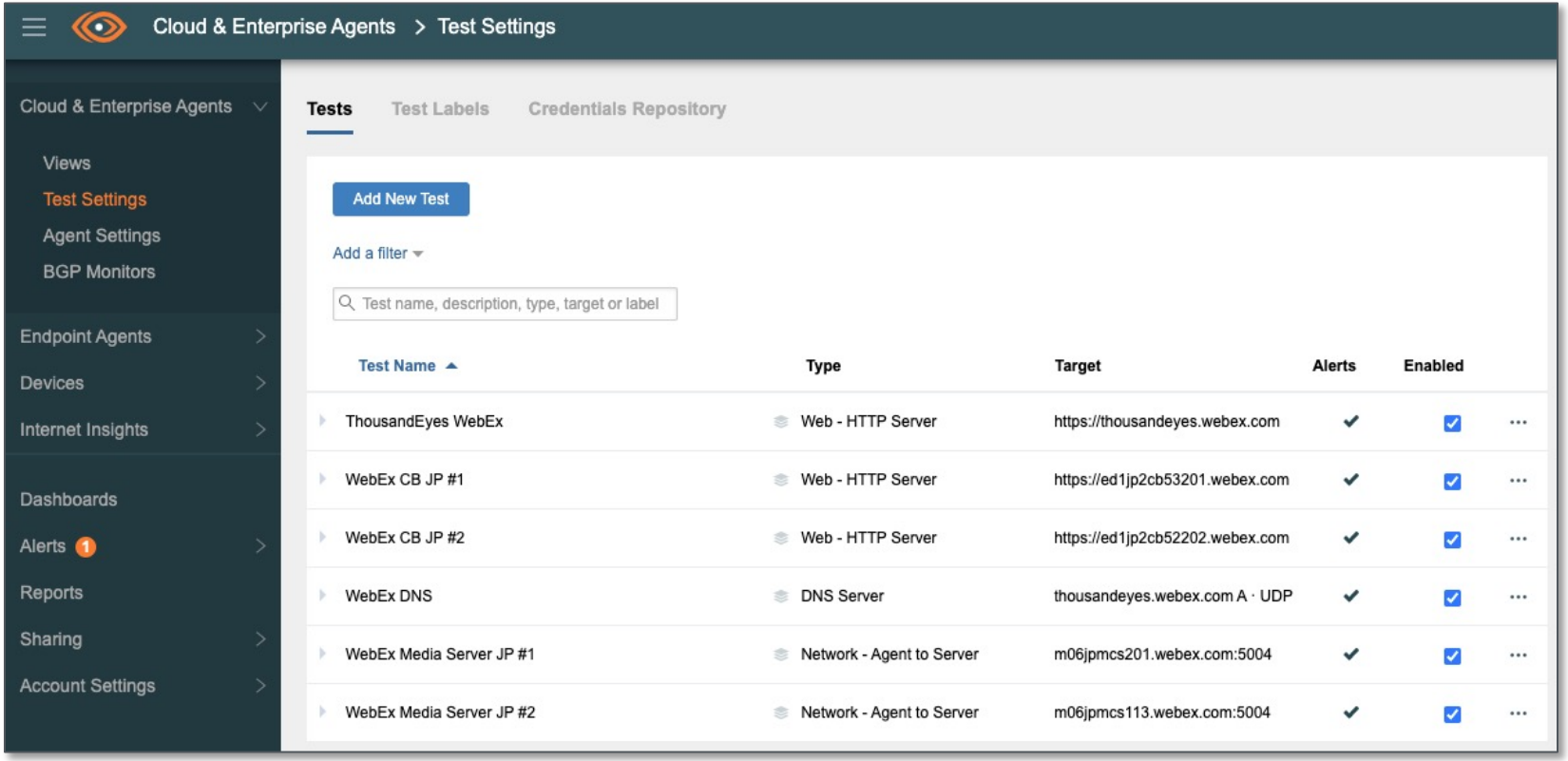
Webexの監視テストの設定例

テストの種類	ターゲット	エージェント	間隔	パラメター
DNS Server (ローカル DNS サーバー)	**<会社名>**.webex.com IN,A	Enterprise	5分間	Path Trace : In Session No. of Path Traces : 5 Transmission Rate : 10 pps Send recursive queries : **ENABLE**
HTTP テスト (WebZone)	https://**<会社名>**.webex.com	Enterprise + Cloud	2-5分間隔	HTTP interval : 2 min No. of Path Traces : 5 Path Trace : In Session Transmission Rate : 10 pps
HTTP Server * (Collaboration Bridge)	https://ed1jp2cb53201.webex.com + https://ed1jp2cb52202.webex.com	Enterprise エージェント + Cloud エージェント	2分間	No. of Path Traces : 5 Path Trace : In Session Transmission Rate : 10 pps
Agent to Server * (Multimedia Platform)	m06jpmcs113.webex.com + m06jpmcs201.webex.com	Enterprise エージェント + Cloud エージェント	1-2分間	**TCP port 5004** Path Trace : In Session No. of Path Traces : 5 Transmission Rate : 10 pps DSCP : EF (DSCP 46)

* CBとMMPの監視テストは、傷害の際にサーバーとネットワーク問題の切り分けのために2台ずつ監視テストを設定します

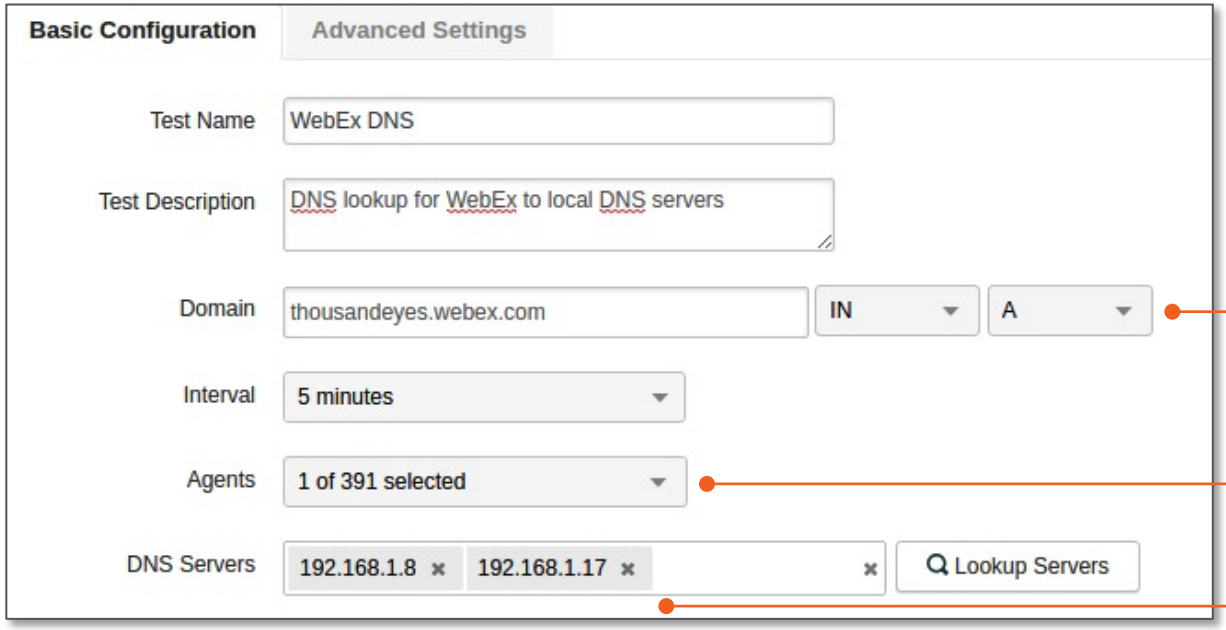
Webex監視テストの設定例

- Webex監視に必要な監視テストの一覧



Webex監視テストの設定例：DNSサーバー

- DNSサーバーテストの基本設定



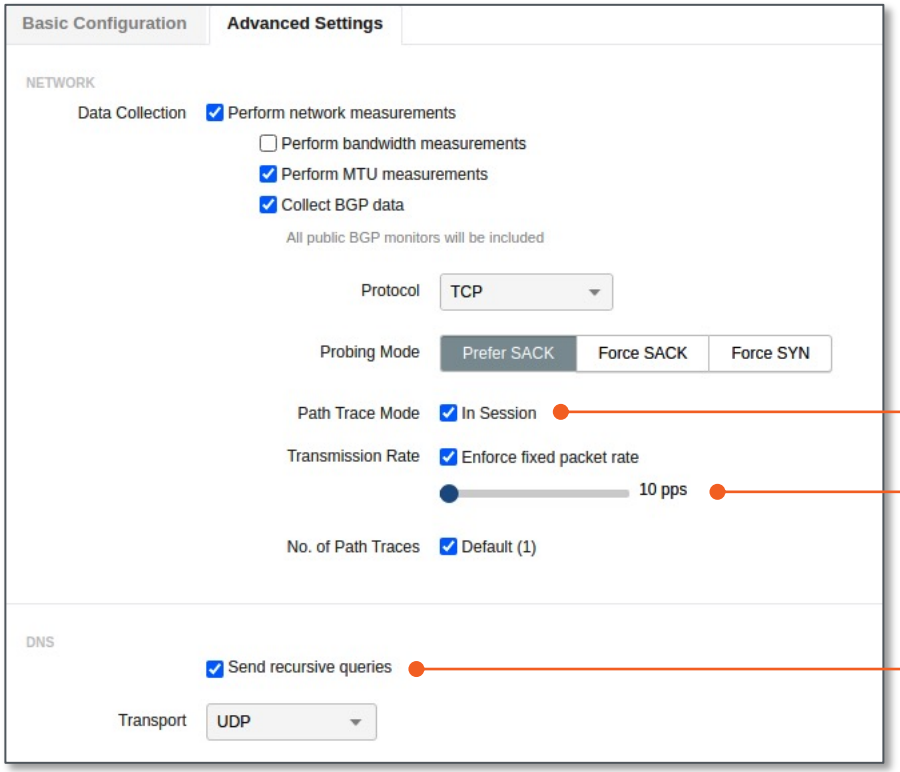
お客様にアサインされた
Webex URL

社内Enterpriseエージェント

社内DNSサーバー

Webex監視テストの設定例：DNSサーバー

- DNSサーバーテストのアドバンス設定



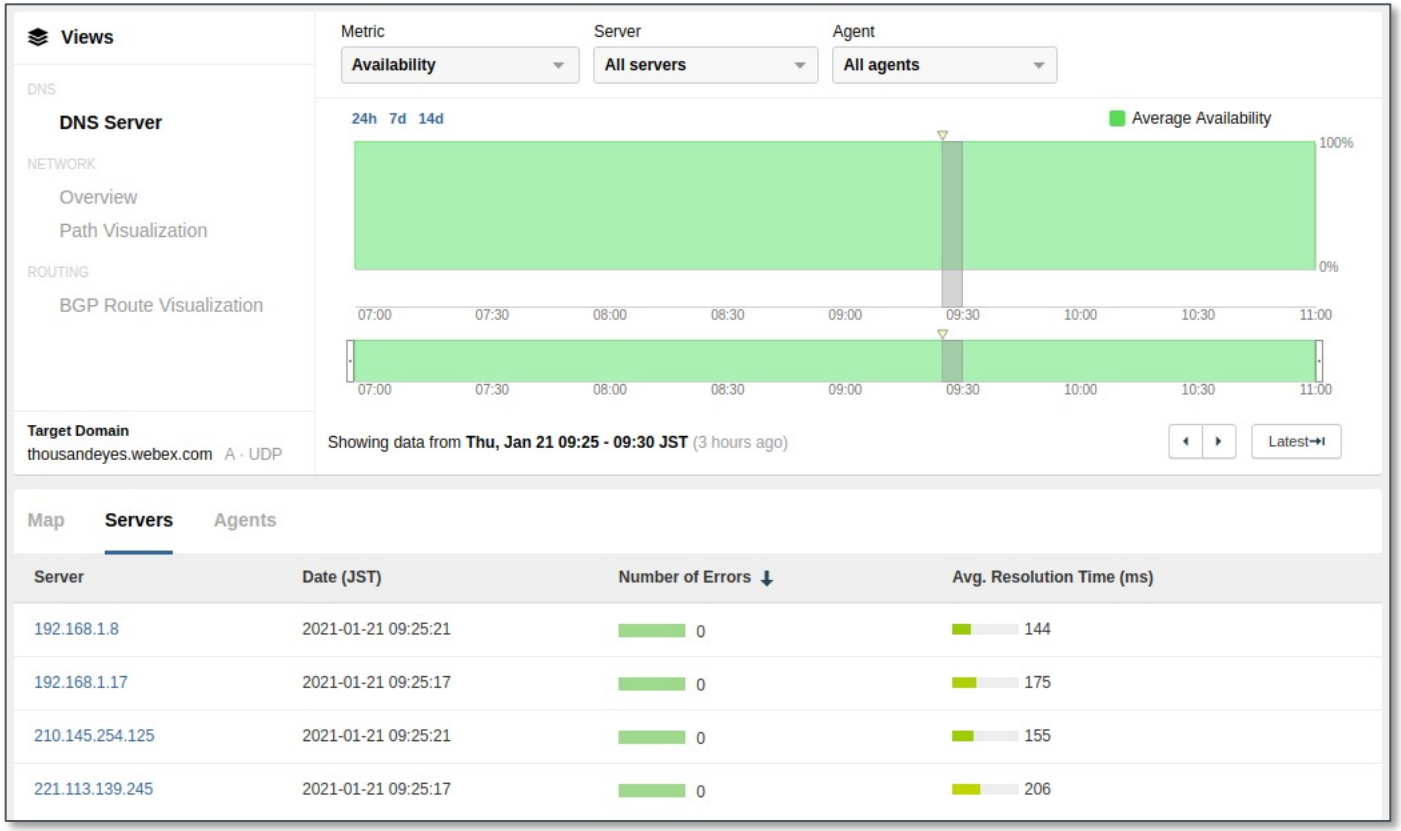
サーバーと接続したTCPセッション内での
End to Endのネットワーク品質測定を実行

サーバーに優しい送信レート

IPアドレスを解決するまで
DNSクエリを続けるように設定

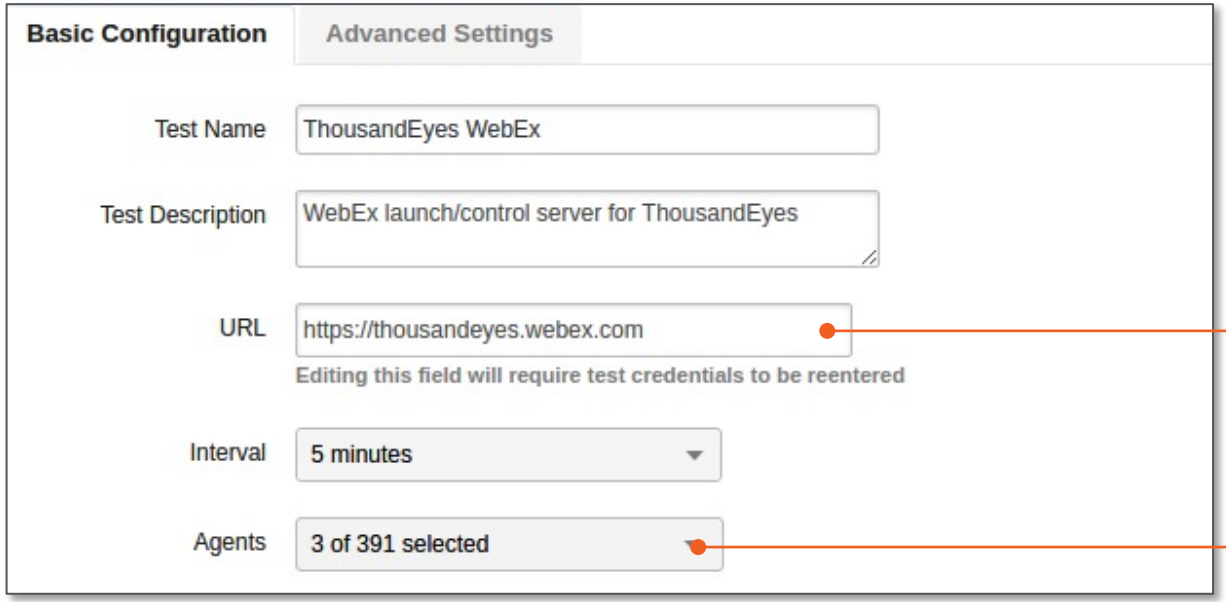
Webex：ローカルDNSサーバーの監視例

共有リンク



Webex監視テストの設定例：WebZone

- HTTPサーバーテストの基本設定

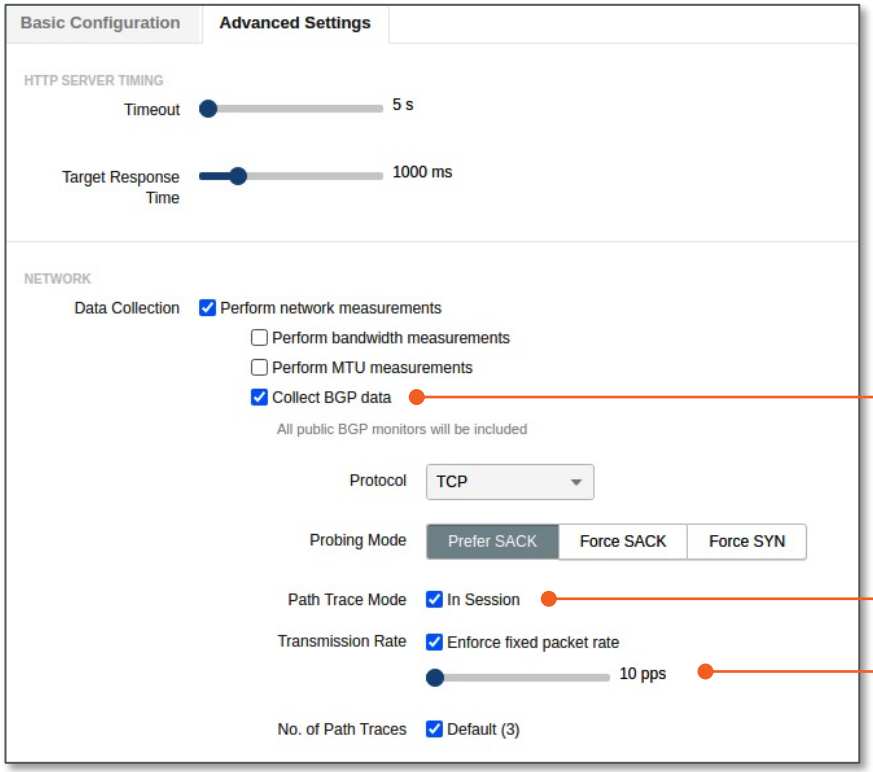


1）お客様のWebex URL
2）Collaboration Bridge

社内Enterpriseエージェント
+ Cloud エージェント

Webex監視テストの設定例：WebZone

- HTTPサーバーテストのアドバンス設定

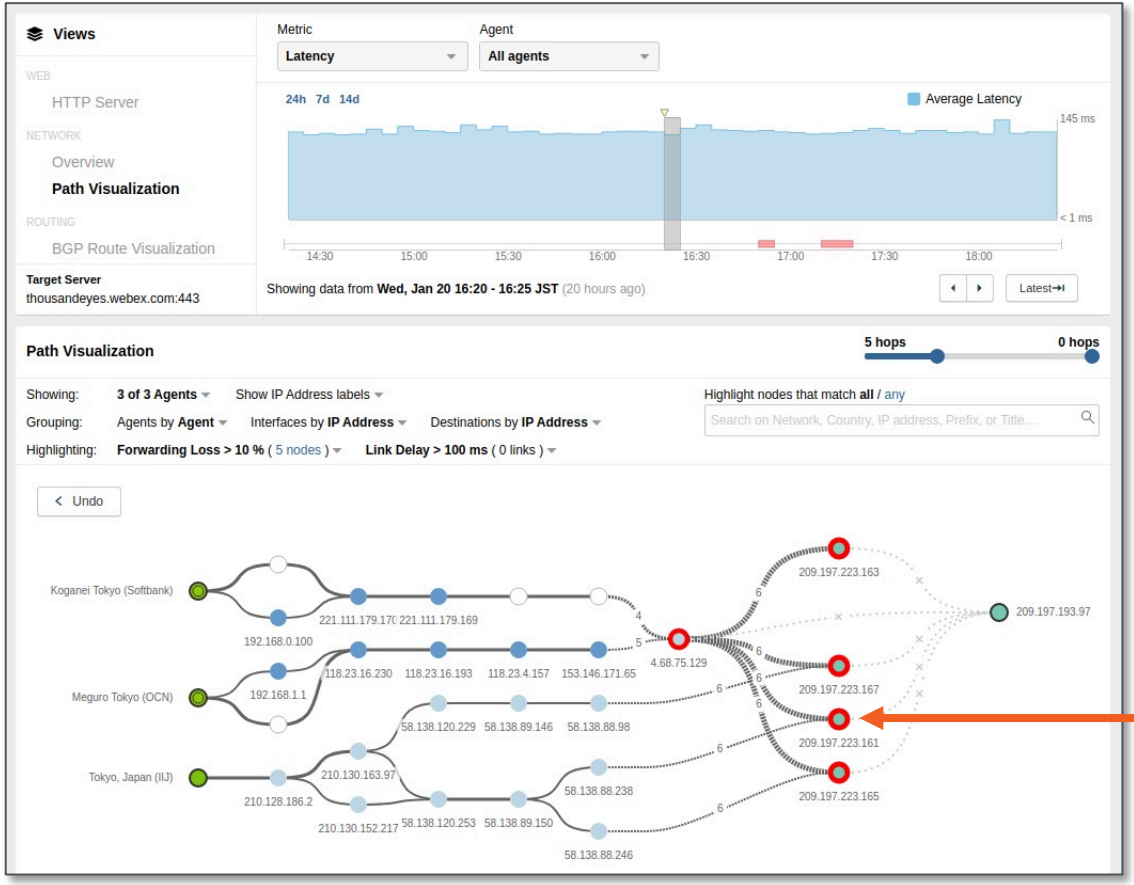


BGPの経路データを取得する

サーバーと接続したTCPセッション内での
End to Endのネットワーク品質測定を実行

サーバーに優しい送信レート

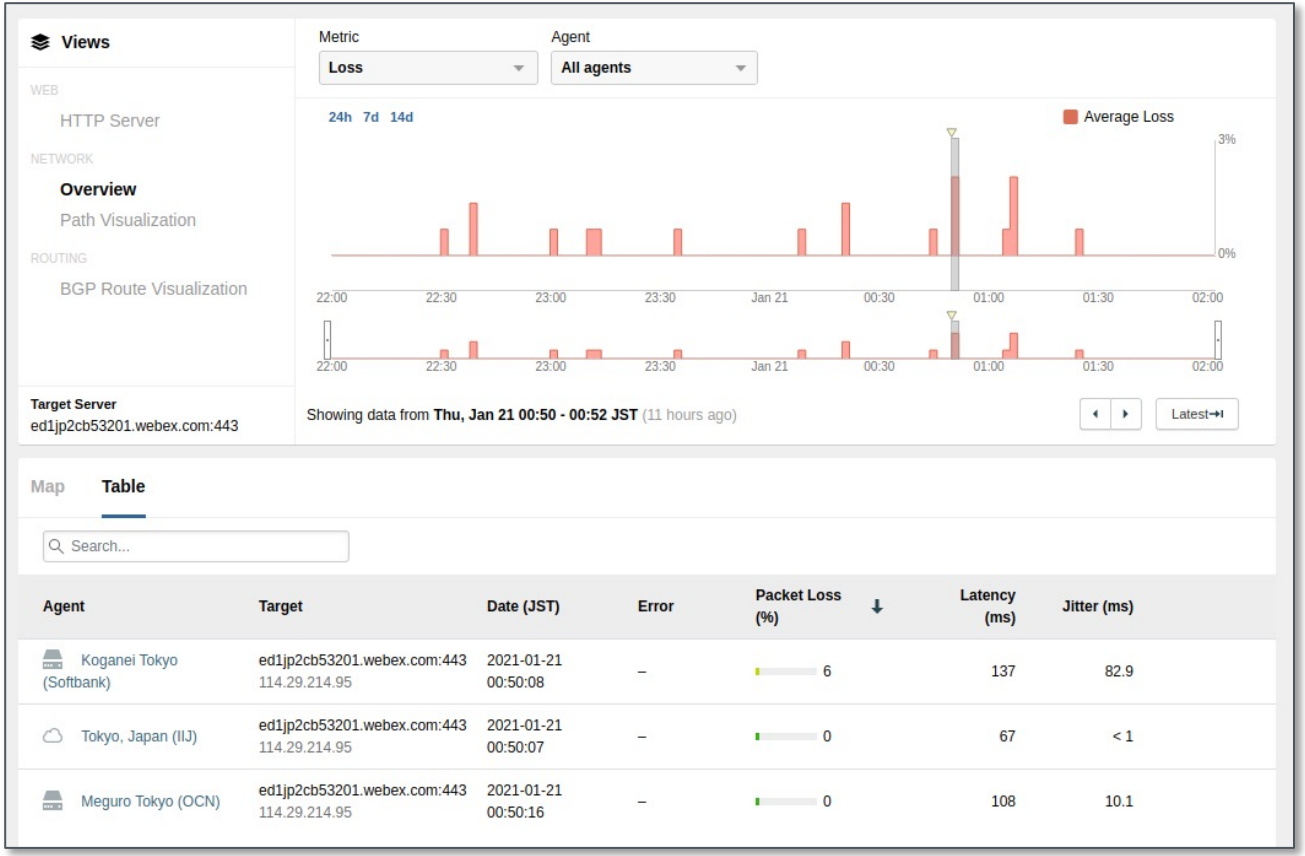
Webex WebZone の監視例



[共有リンク]

Webex DC内では
ICMPパケット
がブロックされている

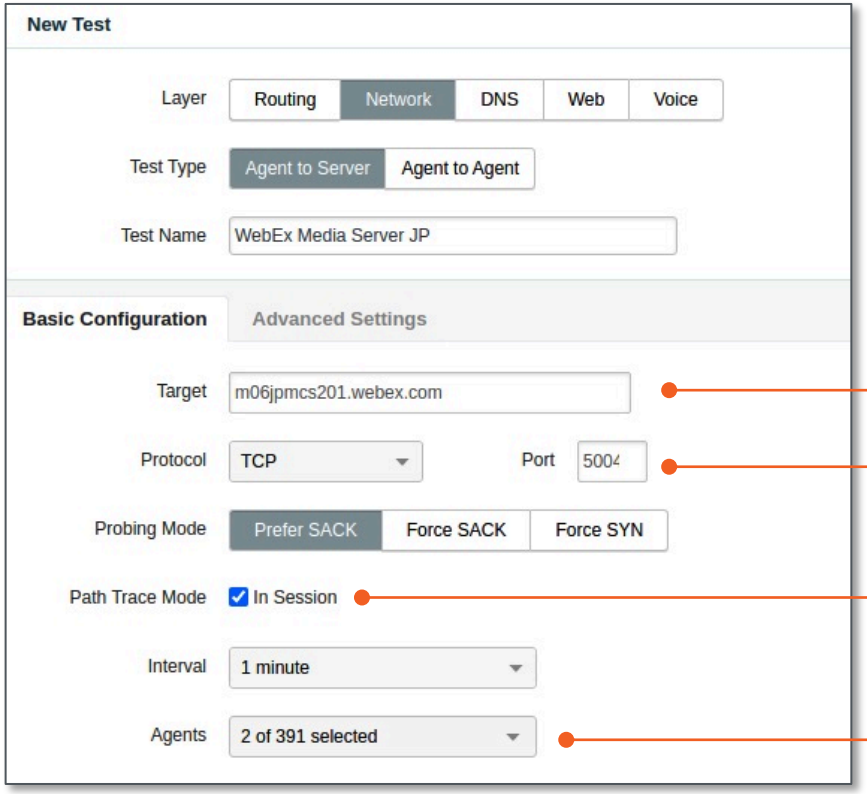
国内 Collaboration Bridge の監視例



共有リンク

Webex監視テストの設定例：Multimediaサーバー

- メディアサーバーへのネットワークテストの基本設定



監視対象のメディアサーバーのドメイン名

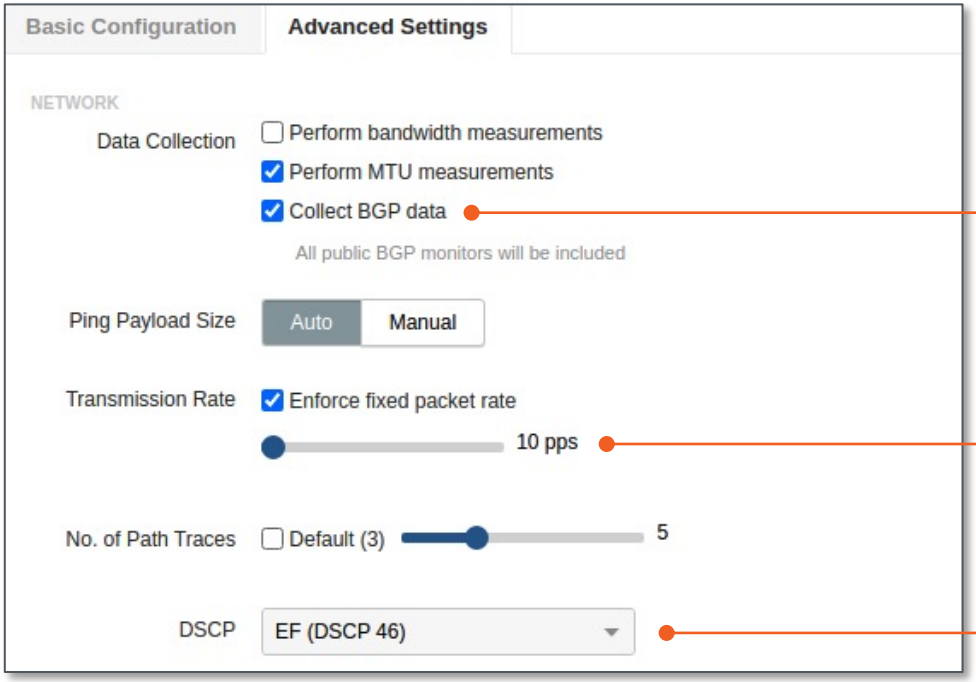
TCP ポート 5004

サーバーと接続したTCPセッション内での
End to Endのネットワーク品質測定を実行

社内Enterpriseエージェント+ Cloud エージェント

Webex監視テストの設定例：Multimediaサーバー

- メディアサーバーへのネットワークテストのアドバンス設定

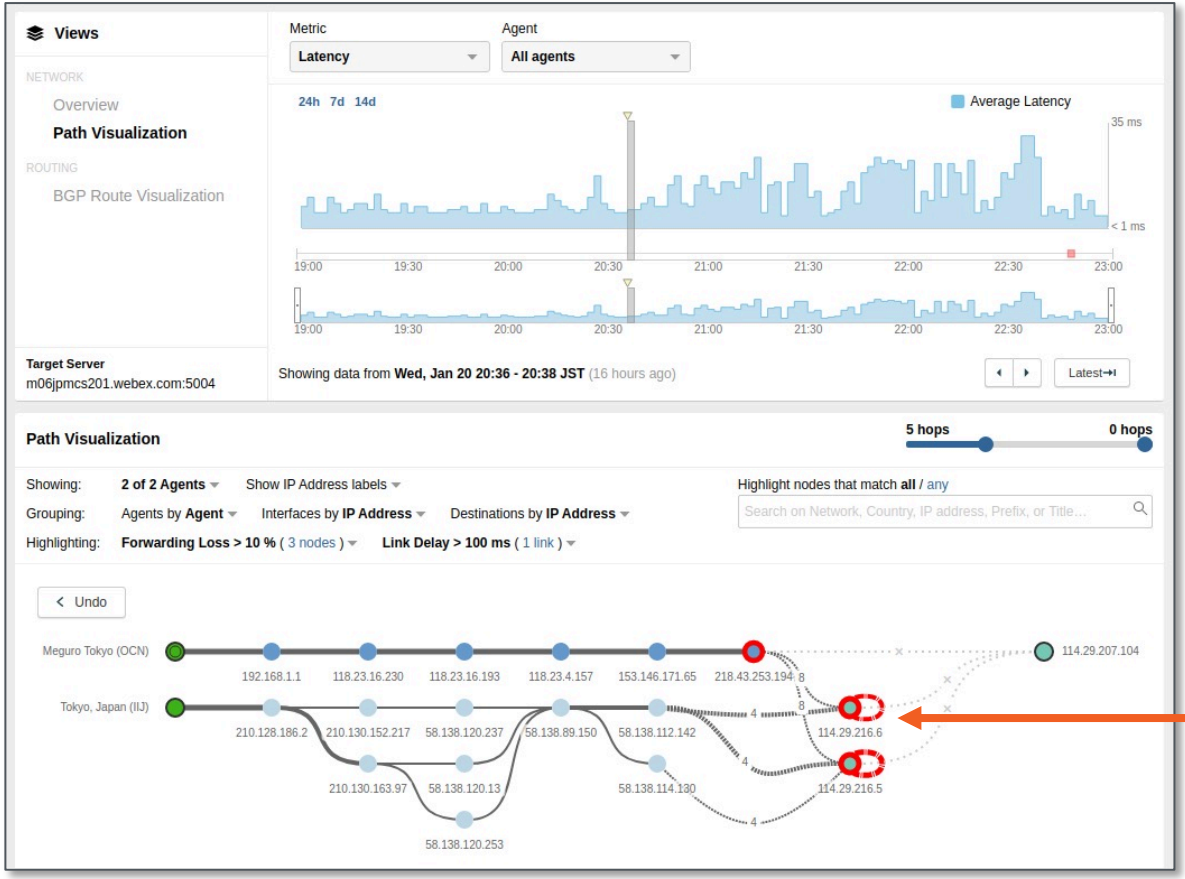


BGPの経路データを取得する

サーバーに優しい送信レート

DSCPの設定 (EF, DSCP 46)

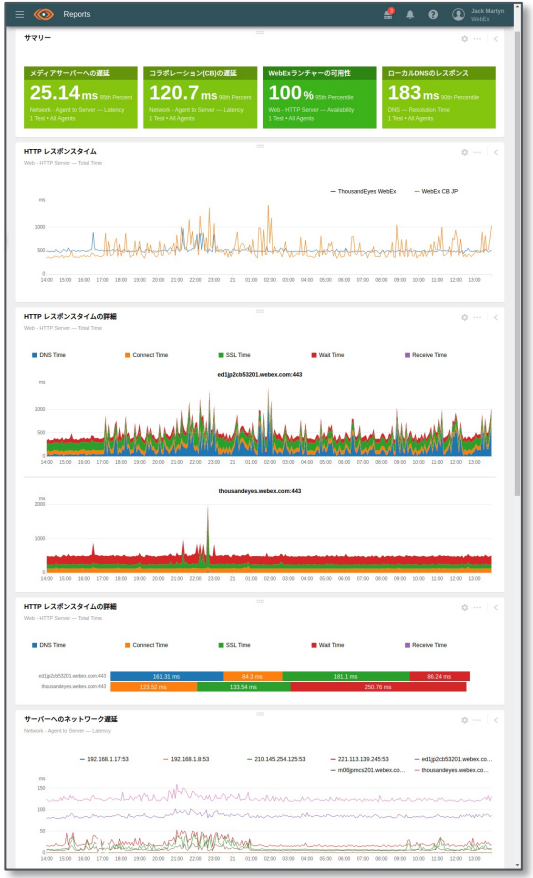
国内 Multimedia サーバーの監視例



[共有リンク]

WebEx DCがICMPパケットをブロックしている

Webexの監視レポート例



[共有リンク]

オンラインビデオ会議の監視
Microsoft Teams

Microsoft Teams

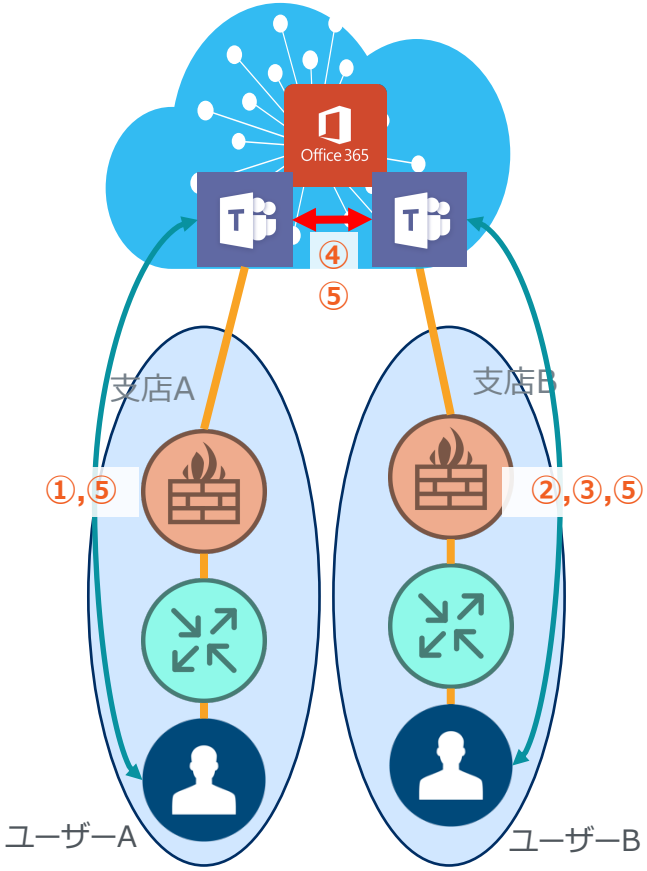
- Teamsに対するMicrosoft社の推奨環境：

1. プロキシやDPIなど遅延に影響する機器はバイパスする
2. 自社ネットワークに一番近いMicrosoftエッジへのパスを使う
3. ボイスやビデオのトラフィックにはUDPを使う
4. DNSはローカルのネットワークで解決する
5. 事前にOffice 365への遅延、ロス、ジッターや必要になる帯域などを測定・計算する

Teamsのコールフロー

- コールフロー

1. 社員AがOffice365のTeamsに接続 (TCP/443)、社員Bへの通話の招待状を送信
2. Office365のTeamsが社員Bに社員Aからの通話招待を通知
3. 社員BがOffice365のTeamsに接続 (TCP/443)、通話の招待に回答
4. 社員Aと社員BのTeamsが直接接続の通信は不可であることを検知、Office 365のTeamsの**トランスポートリレー**を使い接続する
5. Office 365のTeamsのトランスポートリレーを使った会話の開始



Teamsのエッジノード

- Teams の制御ノード
  - Teamsクライアントとコールのシグナリングを処理
  - https://teams.microsoft.com
  - IP Anycastで運用 (現在 52.113.194.131)
  - Office365のバックエンドとのコミュニケーション

- トランスポートリレー
  - world.tr.teams.microsoft.com, IP Anycast (現在 13.107.64.2)
  - カンファレンスのメディア通信を複数のユーザーにリレーする
  - UDP/3479 (音声), UDP/3480 (ビデオ), UDP/3481 (画面)
  - UDPの通信が最適。不可の場合はTCP/443にフォールバック
  - UDP/TCPやIPv4/IPv6のクライアントをブリッジ接続できる！

監視テストの内容

1. Teamsのエッジノードの監視

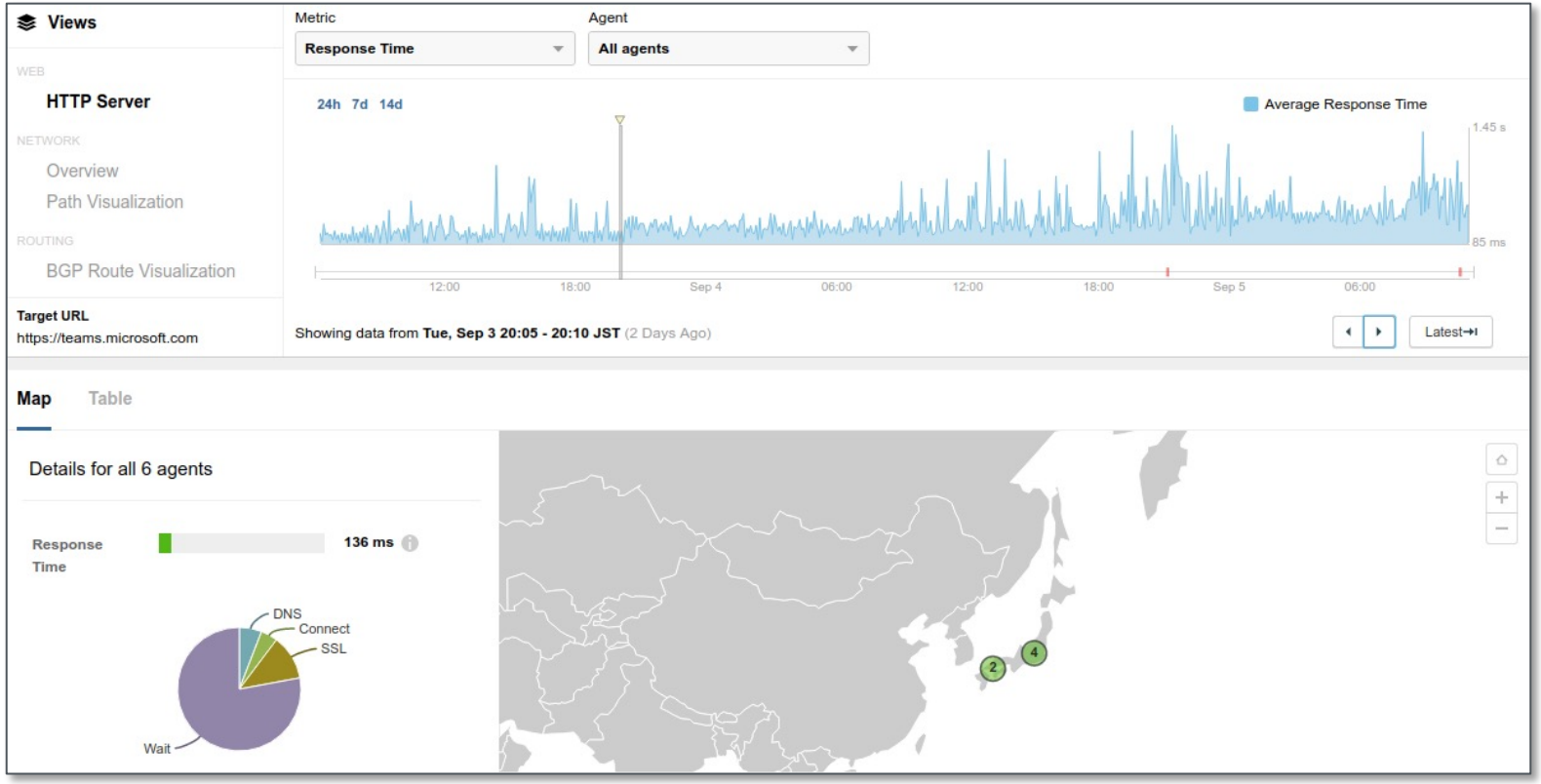
   - 社内EnterpriseエージェントとCloudエージェントからHTTPテストを実行
   - ターゲットは **https://teams.microsoft.com**
   - テスト間隔は5分以内

2. トランスポートリレーの監視

   - 社内EnterpriseエージェントとCloudエージェントから Agent to Server テストを実行
   - ターゲットは **world.tr.teams.microsoft.com**、tcp/443
   - テスト間隔は2分以内、DSCPの設定：音声は 46、ビデオなら 34

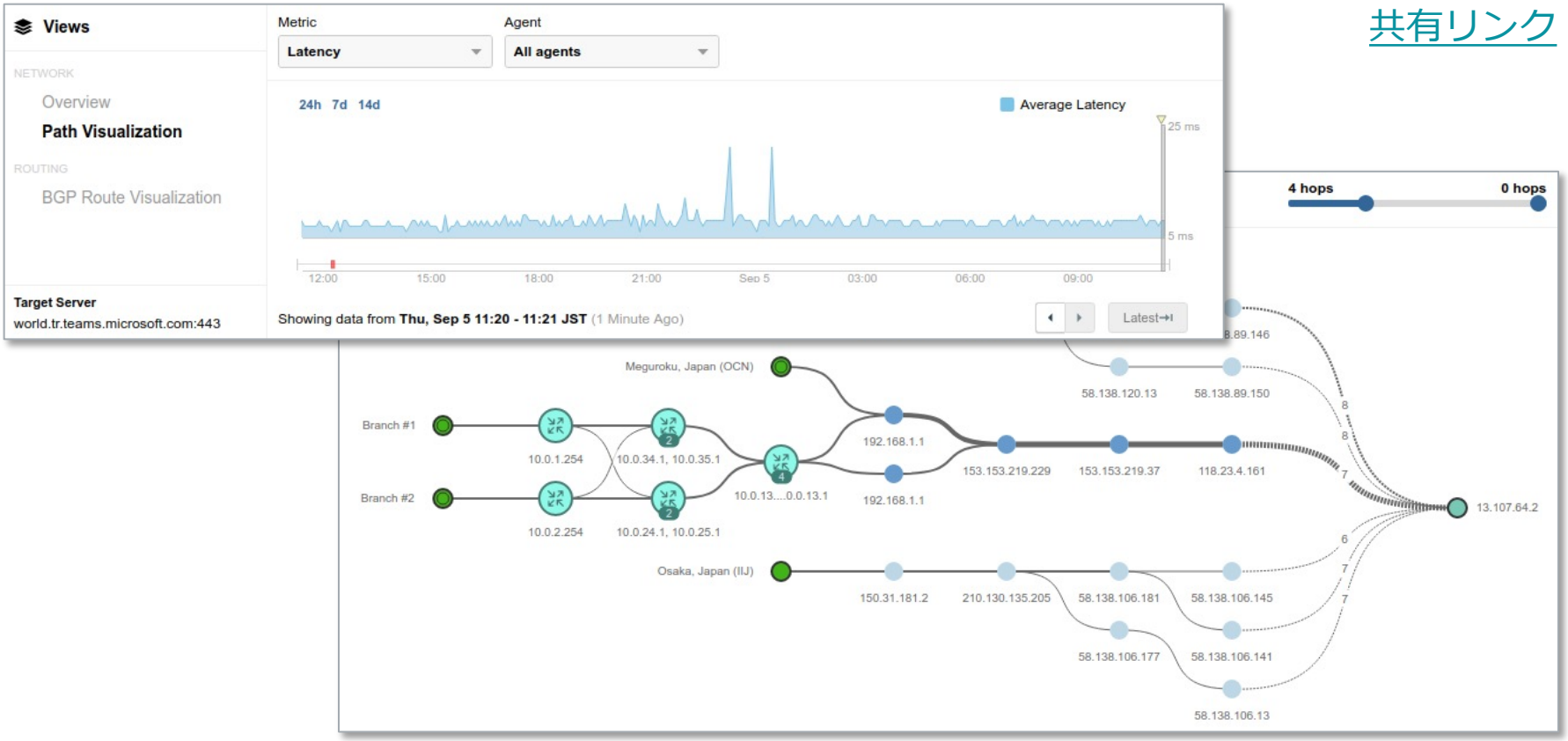
監視テストの実行例：Teamsのエッジノード

共有リンク



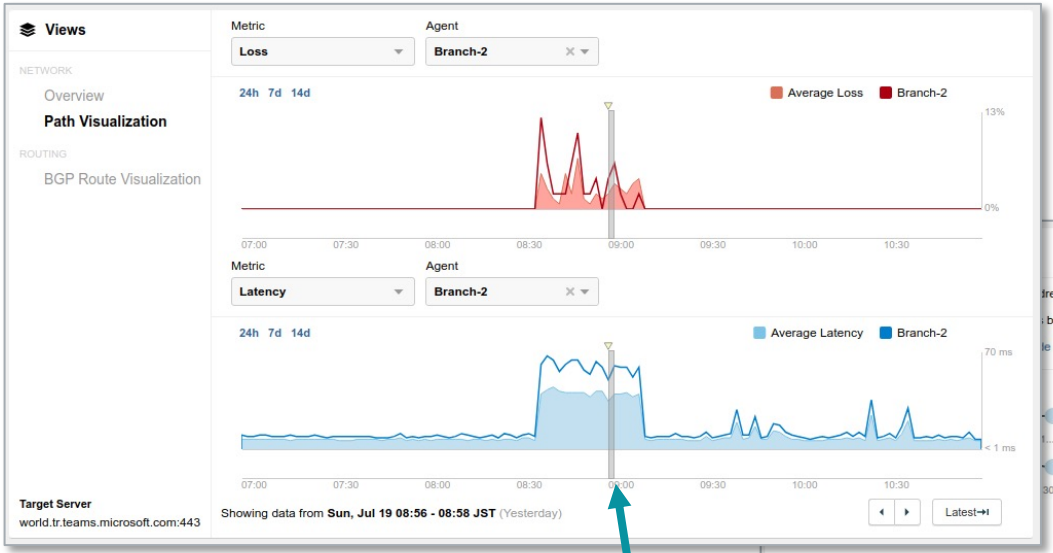
監視テストの実行例：トランスポートリレー (1)

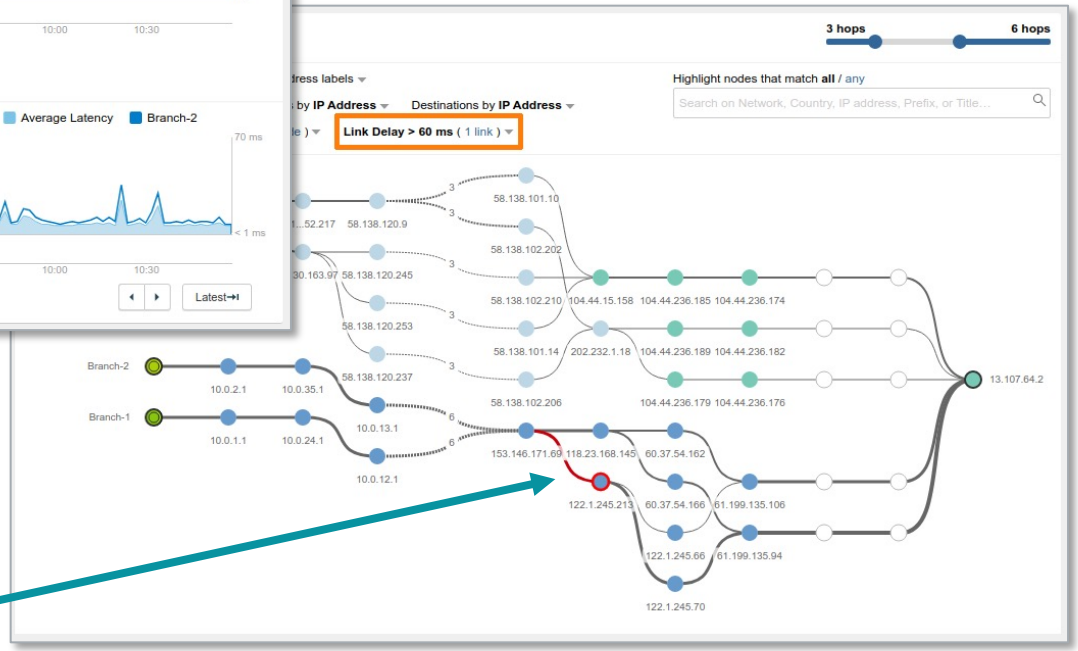
共有リンク



監視テストの実行例：トランスポートリレーの障害 (2)

共有リンク





トランスポートリレーへの
ネットワークパス上のルーターにて
大きな遅延とロスが発生

MS Teams のアラート設定

- Teamsが正常に動作するためのネットワーク環境：

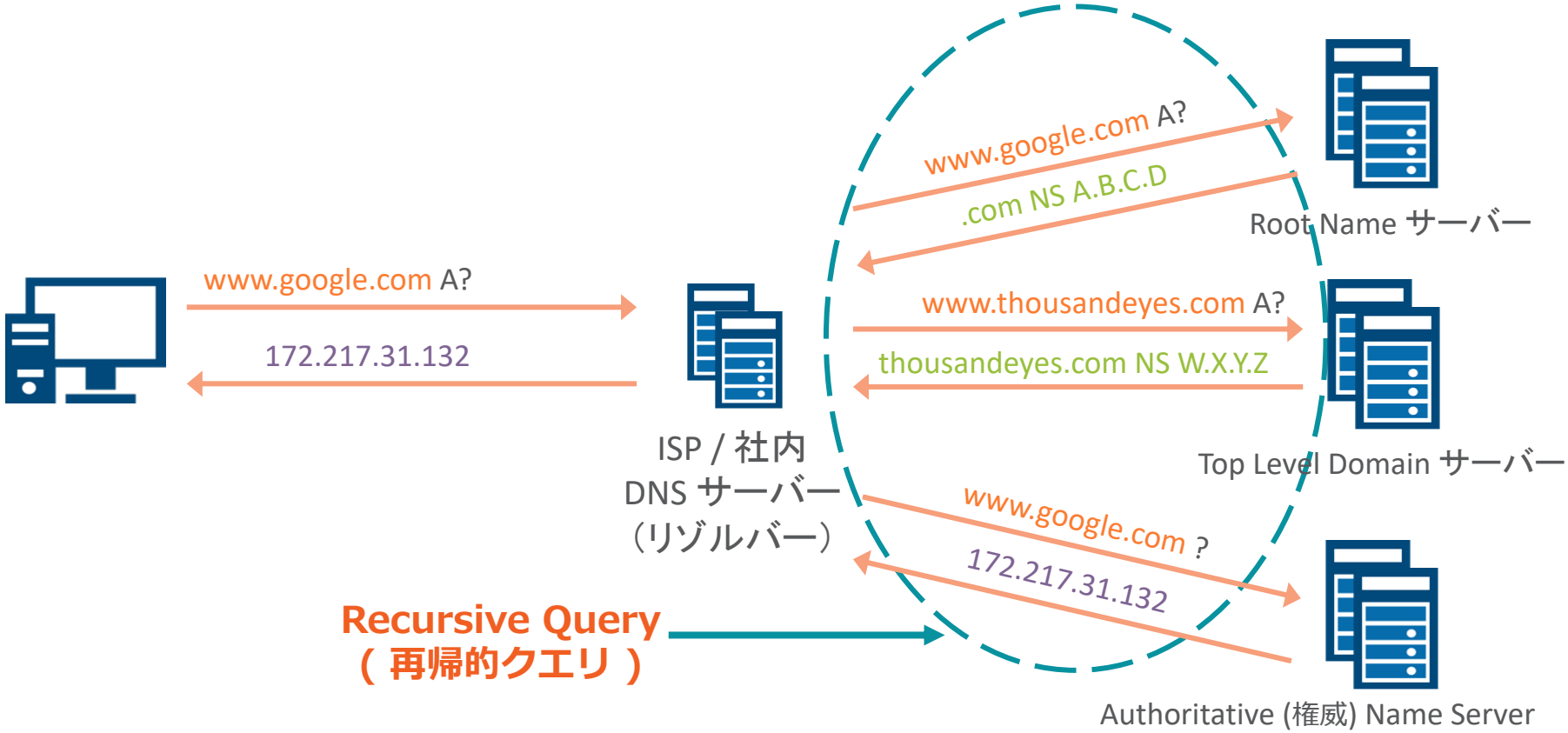
  https://docs.microsoft.com/ja-jp/microsoftteams/prepare-network

- 下のMicrosoftの推奨値を使い、トランスポートリレーの監視テストにアラートを設定：

監視データ	ThousandEyes のアラート設定	推奨値
遅延 (往復時間)	Network Latency	100 ミリ秒以下
パケット損失	Network Packet Loss	1% 以下
パケット到着間ジッター	Network Jitter	30 ミリ秒以下

DNS サービスの監視

DNSの基礎知識



DNS レコード

DNSに格納されている情報を「レコード」と呼ぶ。
レコードは格納する情報によって種類が分類分けされている。

監視テストによく使うDNSレコード：

Aレコード	ドメイン名からIPv4アドレス
AAAAレコード	ドメイン名からIPv6アドレス
PTRレコード	IPアドレスからドメイン名
NSレコード	DNSサーバーのドメイン名
MXレコード	メールサーバーのドメイン名
CNAMEレコード	ドメイン名の別名

DNSのアドレス解決 (Mac OS, Linux)

```
$ dig @8.8.8.8 outlook.office.com
```

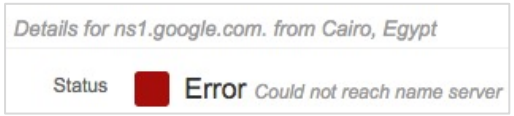
8.8.8.8 (Google) のDNSリゾルバーに
outlookoutlook.office.comのアドレス解決をリクエスト、
以下はサーバーからのレスポンス

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23367
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;outlook.office.com.    IN   A

;; ANSWER SECTION:
outlook.office.com.                     8     IN    CNAME    substrate.office.com.
substrate.office.com.                   205   IN    CNAME    substrate.ms-acdc.office.com.
substrate.ms-acdc.office.com.           8     IN    CNAME    afd-k.office.com.
afd-k.office.com.                       54    IN    CNAME    outlook-office-com.k-0002.k-
msedge.net.
outlook-office-com.k-0002.k-msedge.net. 48    IN    CNAME    k-0002.k-msedge.net.
k-0002.k-msedge.net.                    48    IN    A        13.107.18.11
```

qr：サーバーからの回答
rd：再帰的クエリの要求
ra：サーバーは再帰的クエリをサポート

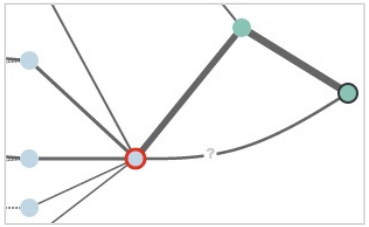
DNS 監視テストのユースケース

サーバーの可用性とレスポンスタイム



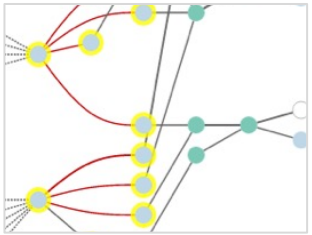
データの正確性

DNSサーバーへのネットワークの品質



クエリーのトレース

CDN/DNSの動作確認



DNSSECバリデーション

DNSの運用管理者

DNSサーバーの種類	運用・管理者	監視の必要
ルートサーバー	VeriSign, NASA, Internet Systems Consortium, US Defence Agency, ICANN, WIDE Project, JPRS	X
トップレベルドメイン	ICANN/IANAとその配下の公式レジストラ	X
権威DNSサーバー	SaaS、IaaSや **自社のWebアプリ管理者**	DNS Server テスト
社内DNSサーバー（ローカル IP アドレス、DNS キャッシュ）	**社内IT**	DNS Server テスト

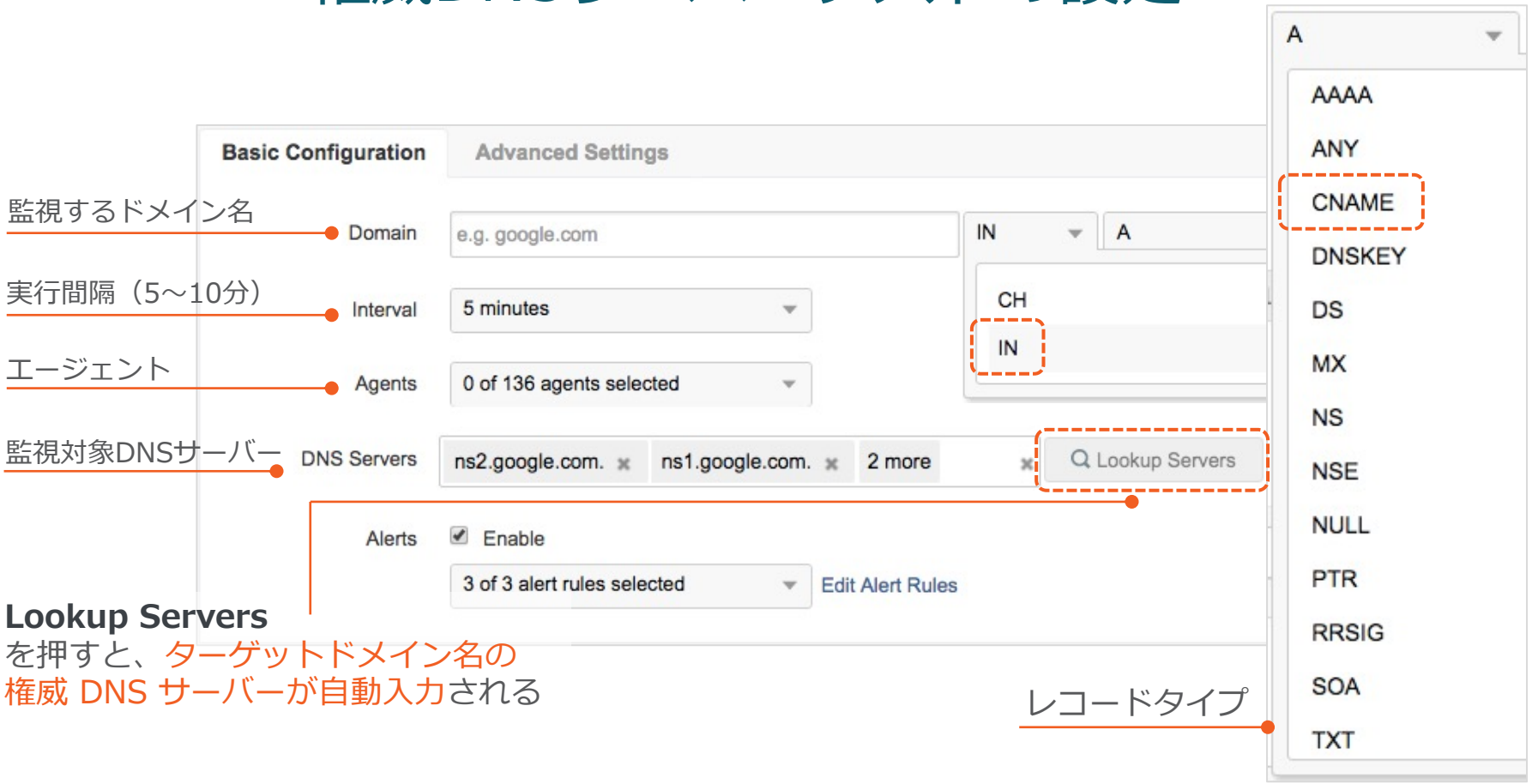
監視する必要あり

権威 DNS サーバーの監視

DNS サーバーの監視

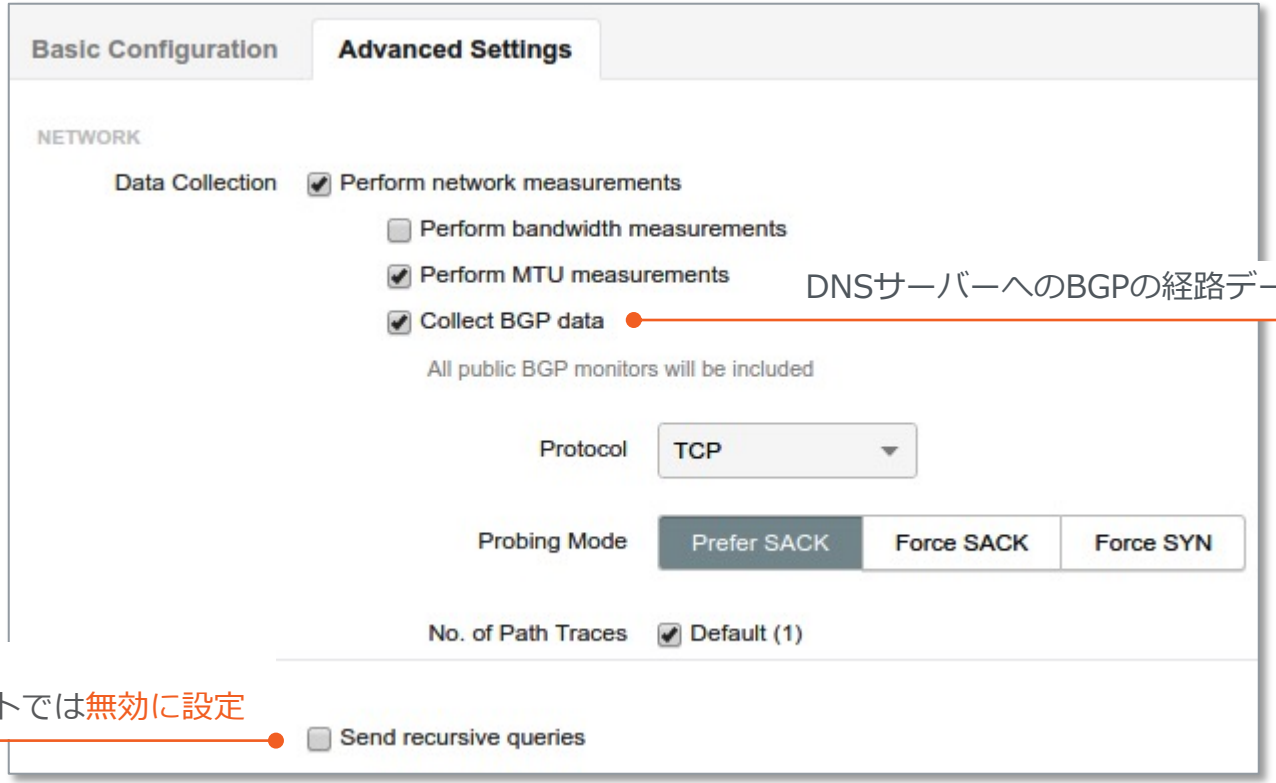
- 権威DNSサーバーの監視内容
  - **権威DNSサーバーの可用性**
  - 名前解決のレスポンスタイムの監視
  - 権威DNSサーバーへのネットワークパスの品質監視
  - 正しいIPアドレスのマッピングの確認（セキュリティ）
- 社内DNSサーバー
  - 社内サーバーの可用性
  - **ユーザーが体験しているレスポンスタイムの監視**
  - ユーザーからDNSサーバーへのネットワークパスの品質監視
  - 正しいIPアドレスのマッピングの確認（セキュリティ）

権威DNSサーバーテストの設定



Lookup Servers
を押すと、ターゲットドメイン名の
権威 DNS サーバーが自動入力される

権威DNSサーバーテストの設定



DNSサーバーへのBGPの経路データの取得

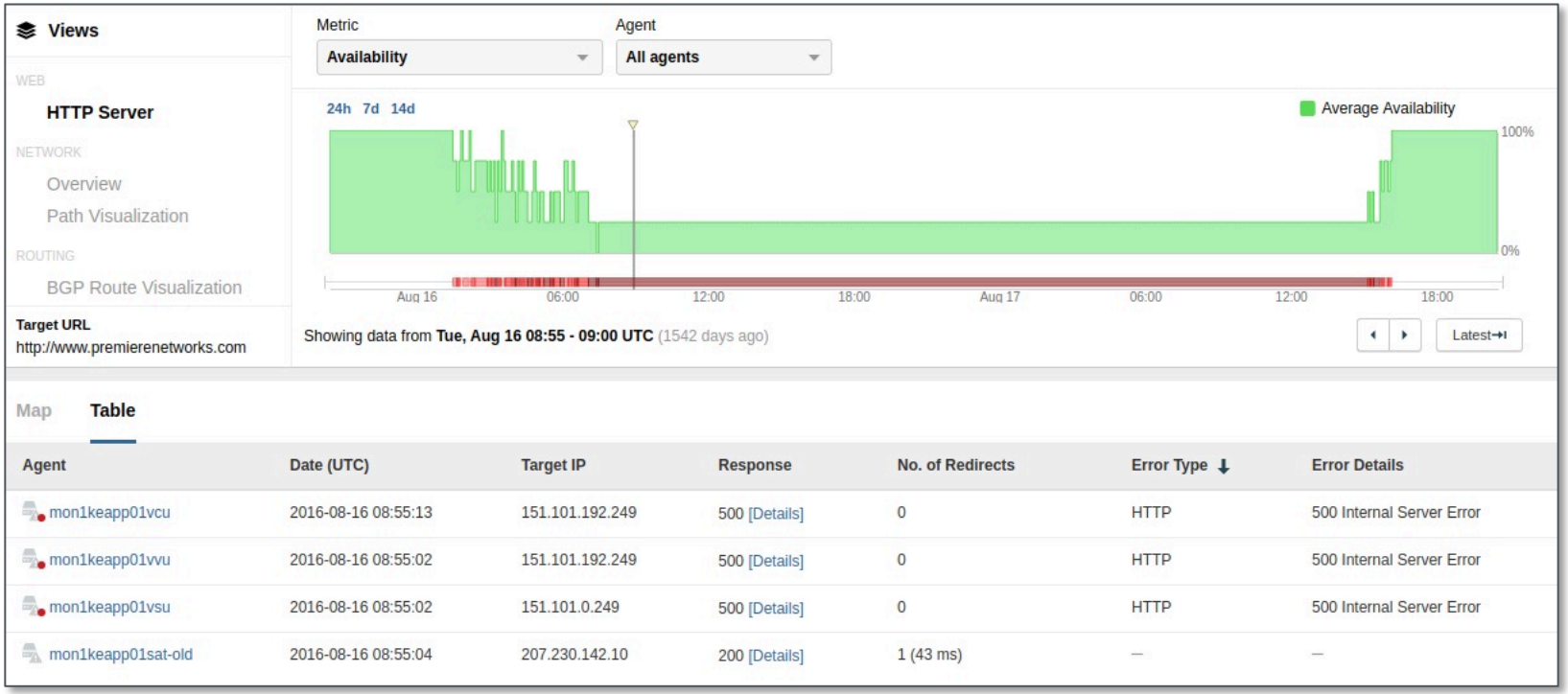
再帰クエリ
権威サーバーのテストでは無効に設定

権威DNSサーバーの監視例 (1)

CDNへのステアリングに問題

共有リンク

DNSを使いCDNに誘導された後、ホスティングされているべきWebサービスが無かった！

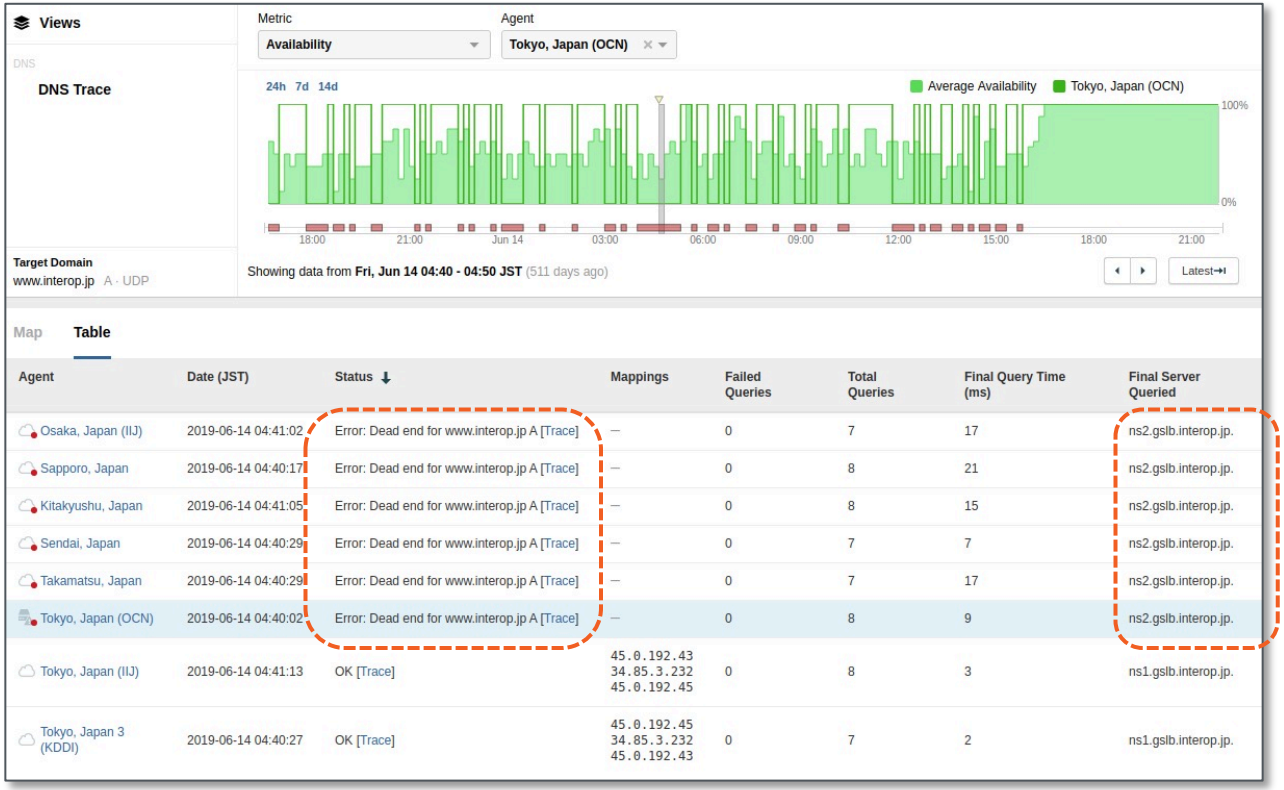


Agent	Date (UTC)	Target IP	Response	No. of Redirects	Error Type	Error Details
mon1keapp01vcu	2016-08-16 08:55:13	151.101.192.249	500 [Details]	0	HTTP	500 Internal Server Error
mon1keapp01vvu	2016-08-16 08:55:02	151.101.192.249	500 [Details]	0	HTTP	500 Internal Server Error
mon1keapp01vsu	2016-08-16 08:55:02	151.101.0.249	500 [Details]	0	HTTP	500 Internal Server Error
mon1keapp01sat-old	2016-08-16 08:55:04	207.230.142.10	200 [Details]	1 (43 ms)	–	–

権威DNSサーバーの監視例 (2)

DNS Traceテストを使ったDNSサーバーの問題解析　　共有リンク

ロードバランスされたDNSサーバーの１台 (ns2.gslb.interop.jp) の問題



Agent	Date (JST)	Status	Mappings	Failed Queries	Total Queries	Final Query Time (ms)	Final Server Queried
Osaka, Japan (IIJ)	2019-06-14 04:41:02	Error: Dead end for www.interop.jp A [Trace]	–	0	7	17	ns2.gslb.interop.jp.
Sapporo, Japan	2019-06-14 04:40:17	Error: Dead end for www.interop.jp A [Trace]	–	0	8	21	ns2.gslb.interop.jp.
Kitakyushu, Japan	2019-06-14 04:41:05	Error: Dead end for www.interop.jp A [Trace]	–	0	8	15	ns2.gslb.interop.jp.
Sendai, Japan	2019-06-14 04:40:29	Error: Dead end for www.interop.jp A [Trace]	–	0	7	7	ns2.gslb.interop.jp.
Takamatsu, Japan	2019-06-14 04:40:29	Error: Dead end for www.interop.jp A [Trace]	–	0	7	17	ns2.gslb.interop.jp.
Tokyo, Japan (OCN)	2019-06-14 04:40:02	Error: Dead end for www.interop.jp A [Trace]	–	0	8	9	ns2.gslb.interop.jp.
Tokyo, Japan (IIJ)	2019-06-14 04:41:13	OK [Trace]	45.0.192.43 34.85.3.232 45.0.192.45	0	8	3	ns1.gslb.interop.jp.
Tokyo, Japan 3 (KDDI)	2019-06-14 04:40:27	OK [Trace]	45.0.192.45 34.85.3.232 45.0.192.43	0	7	2	ns1.gslb.interop.jp.

社内 DNS サービスの監視

社内 DNS サーバーの設定

- 権威DNSサーバーの監視内容
  - **サーバーの可用性**
  - 名前解決のレスポンスタイムの監視
  - サーバーへのネットワークパスの品質監視
  - 正しいIPアドレスのマッピングの確認（セキュリティ）

- 社内DNSサーバー
  - **社内サーバーの可用性**
  - **ユーザーが体験しているレスポンスタイムの監視**
  - ユーザーからDNSサーバーへのネットワークパスの品質監視
  - 正しいIPアドレスのマッピングの確認（セキュリティ）

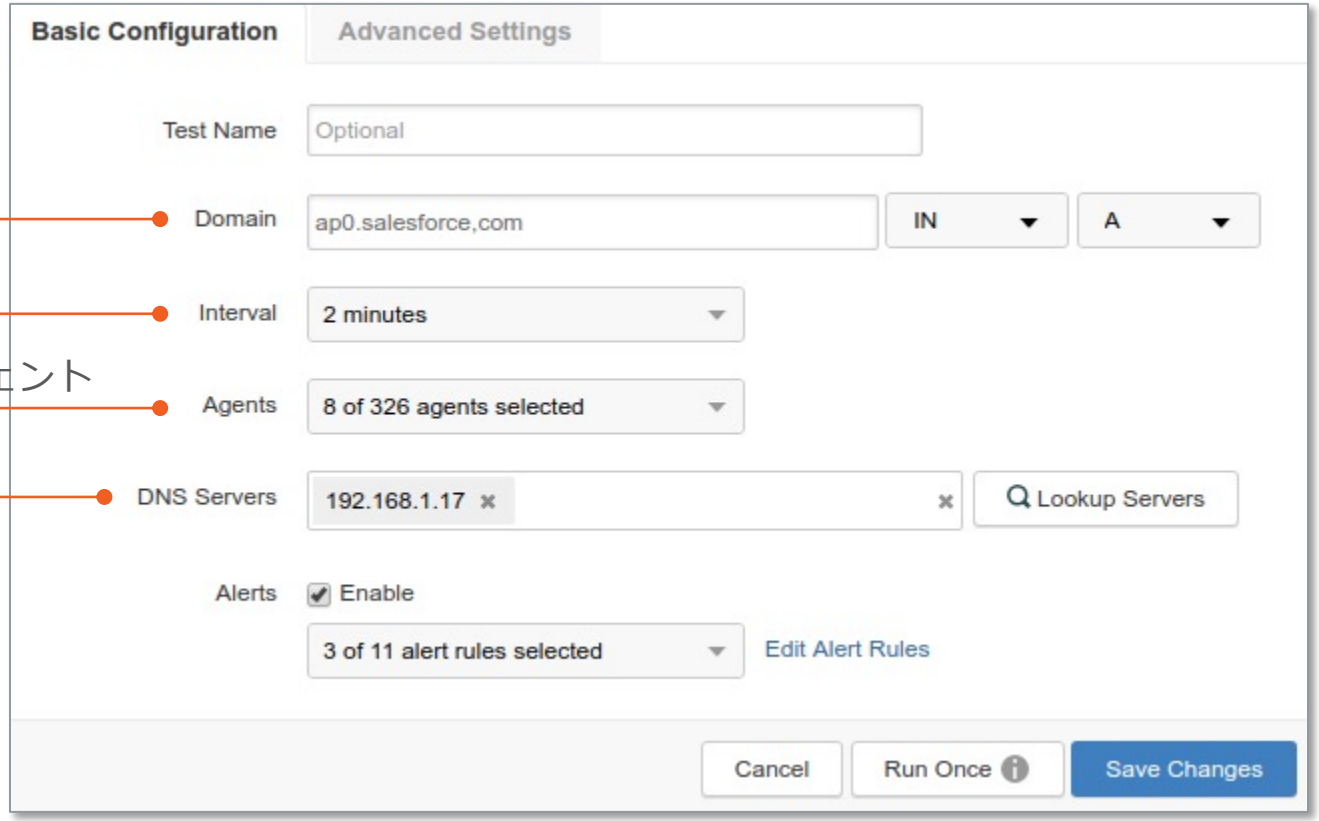
Web アプリケーションの DNS 監視
社内 DNS サーバーテストの設定

監視するドメイン名

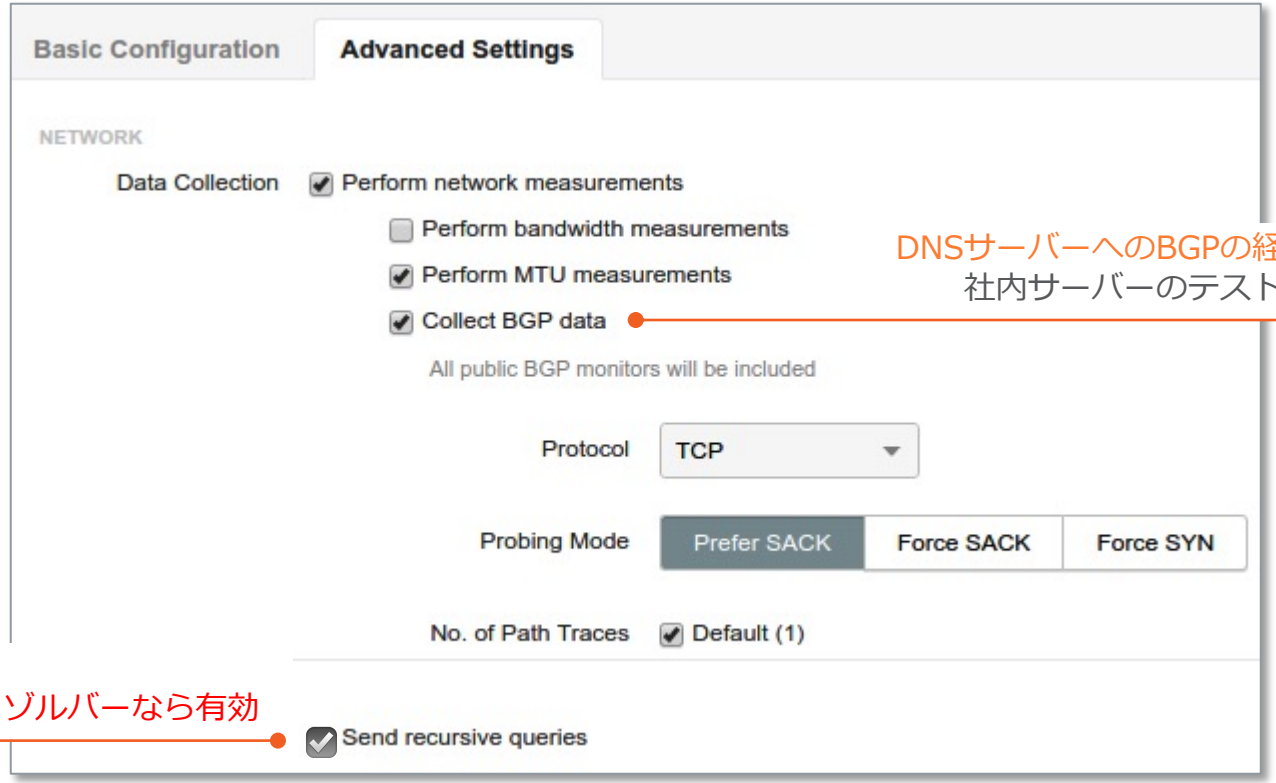
間隔（2～5分）

社内Enterpriseエージェント

社内DNSサーバー



DNSサーバーテストの設定



DNSサーバーへのBGPの経路データ
社内サーバーのテストでは無効

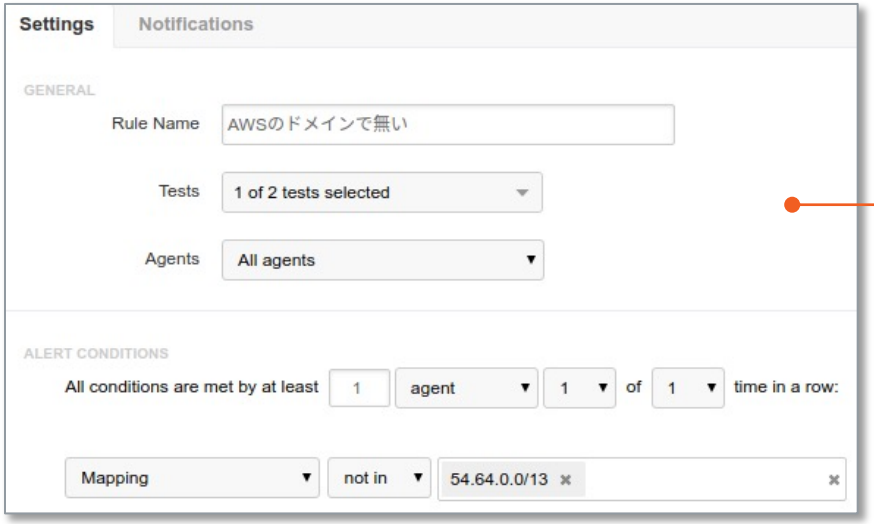
再帰クエリ
DNSサーバーがリゾルバーなら有効

DNSのアラート設定

- 可用性とレスポンスタイム
  - サーバーの問題やレスポンスの劣化はアラートでリアルタイムに通知
- DNSハイジャックの検知
  - アタッカーがDNSのレスポンスに偽りのリソースレコードを埋め込む
  - 正常でないIPアドレスの解決を管理者にアラート

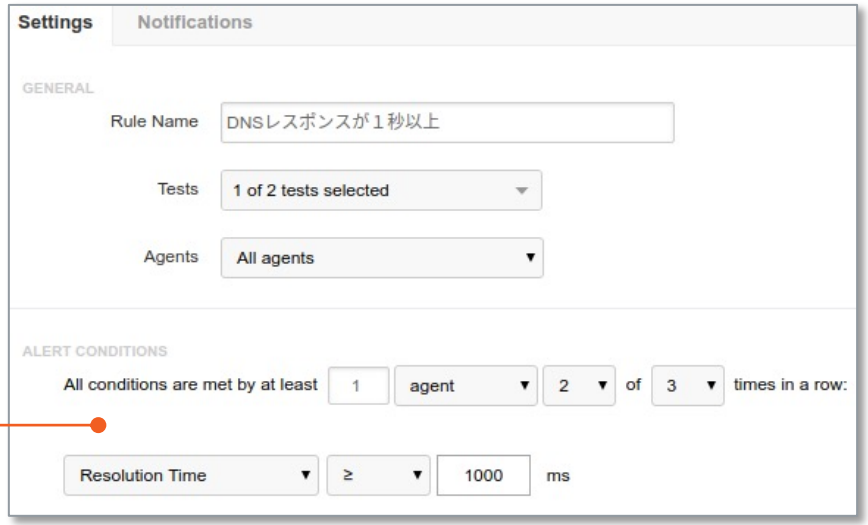
- DNSサーバーへのネットワークパス上のパケットロスを通知
- BGPのアラート：DNSサーバーへの経路の変化

DNSカスタムアラートの設定例



1回でもDNSのレスポンスが
AWSのIPブロックでなかったらアラートする

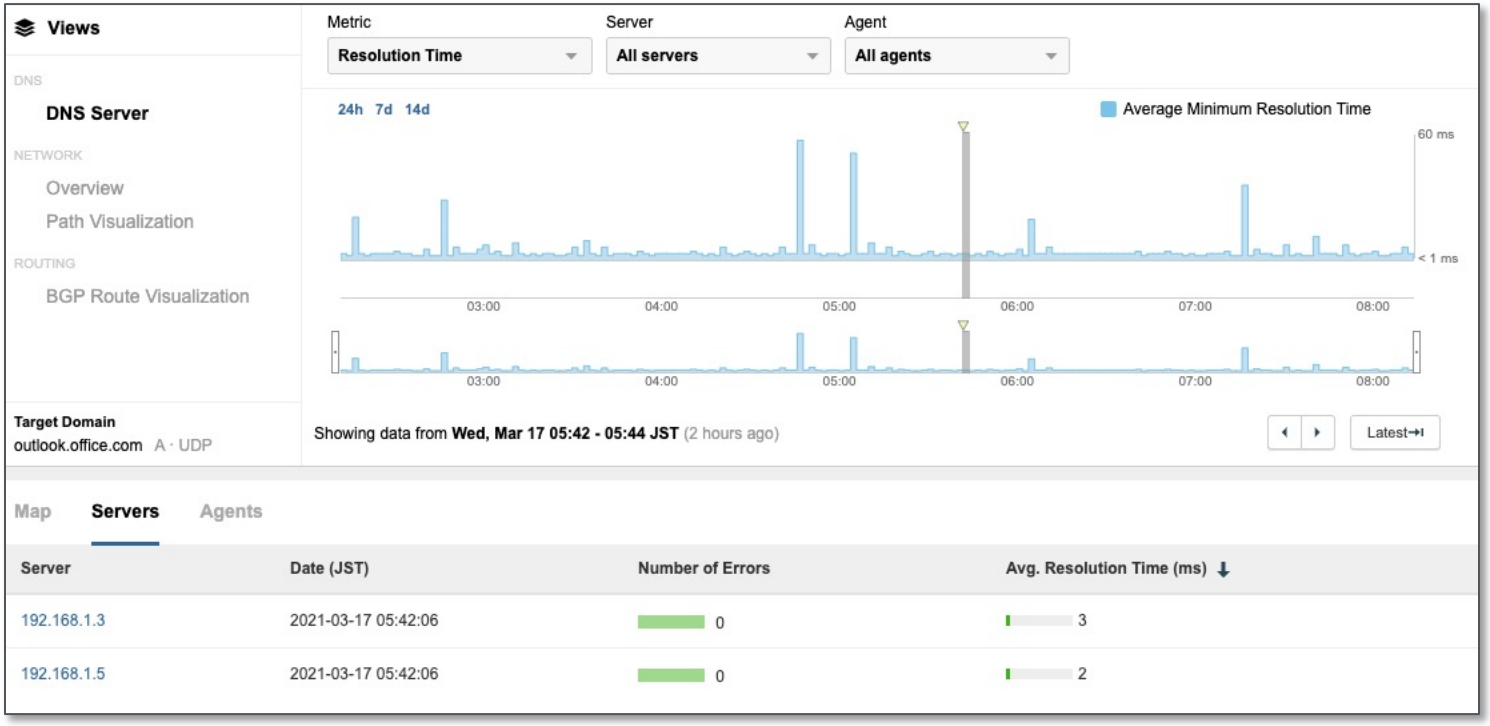
DNSサーバーからのレスポンスが3回に2回
1秒以上であったらアラートする



社内DNSサーバーの監視例

社内DNSサーバーの可用性、レスポンスとネットワークパスの品質測定

共有リンク

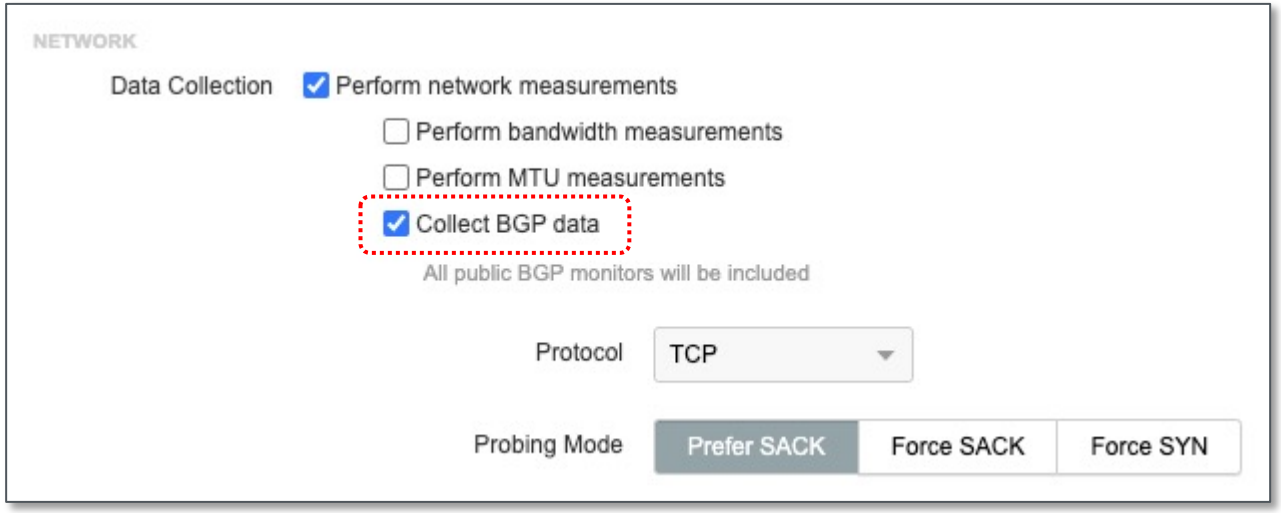


インターネットにある
サービスの経路監視 (BGP)

BGP 経路の可視化

- BGP Route Visualization は全ての監視テストの一部
- 監視テストのターゲットが属するIPプリフィックスがBGPでどのように変動しているか、世界100箇所以上のISPのルーティングテーブルデータから監視する。
  - 各ISPからのReachableであるか
  - インターネットのどこかでPath Changeが発生しているか
  - サービスのプリフィックスがハイジャックされてはいないか
  - サービスのプリフィックスがブラックホールされてはいないか
- 経路に異常があると管理者にアラートで通知
- BGPの経路データは Route Views Project から取得
  - http://www.routeviews.org/routeviews/

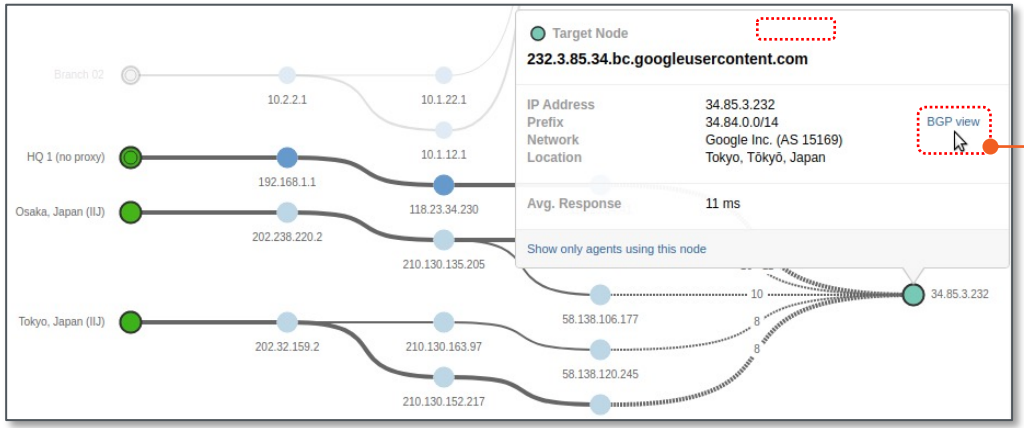
監視テストのBGPデータ監視設定



- 監視テストの Advanced Settings > Collect BGP data
  をチェックすれば監視しているサービスのIPプリフィックスが自動に監視される。
- 設定した監視ターゲットがCDNのサービスを使うことで多数のIPアドレスに
  リゾルブされる場合、このオプションが外れることがあるが、強制的にチェック
  できる。

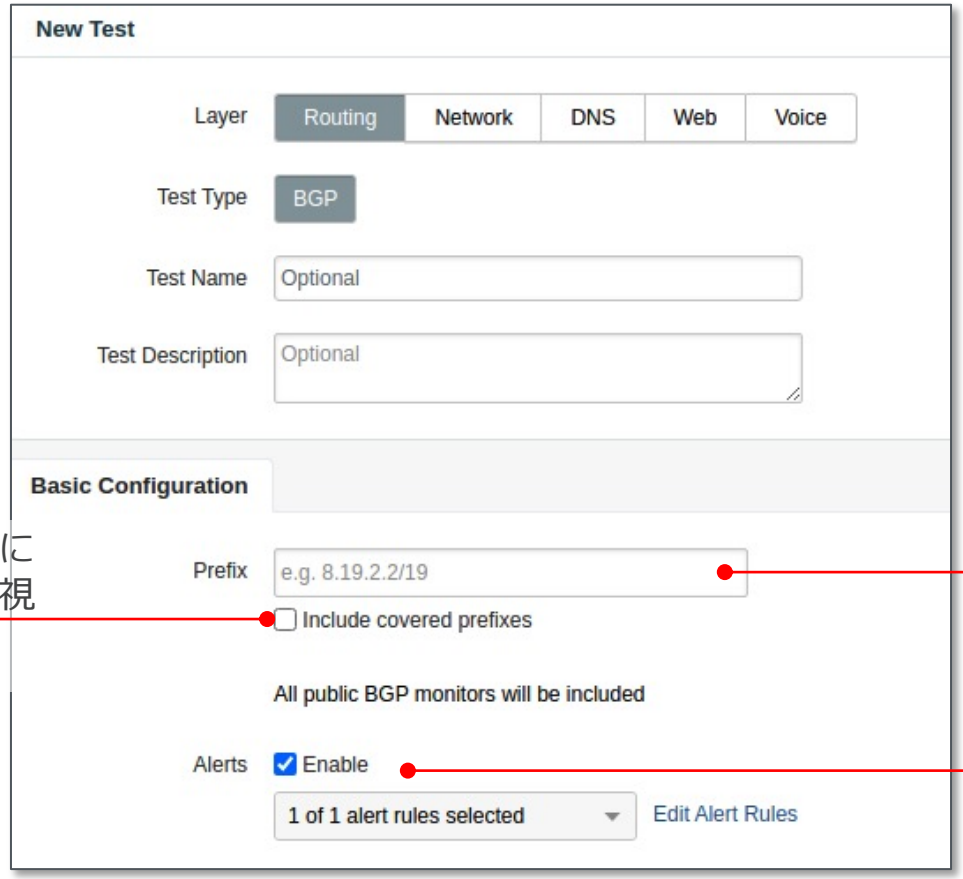
BGP 経路の可視化の使い方

- 監視ターゲットの経路を監視するサービスであり、巨大なIPアドレススペースを持つプロバイダーの経路を全て監視するような機能ではない。
- CDNを使ったサービスではロケーションによって異なるサーバー・IPにDNSで誘導される。正しいIPプリフィックスをUIで追いかけるには、Path Visualizationの画面からターゲットデータに表示される BGP View のリンクを使う：



ここをクリックすれば
追いかけやすい

(単独の) BGP 監視テスト



指定したプリフィックスに
含まれるサブネットの監視
(/19~/23 まで)

監視するプリフィックス
(CIDR表記)

アラートの設定

BGPの可視化：記号の意味

BGP モニター

Public/Private BGP モニター
ターゲットの経路情報あり

隠れたASホップ数

視覚化のために簡略化されたパス。
数字は隠れたASホップを表す。
クリックしてパスを展開。

BGP モニター

Public/Private BGP モニター
ターゲットの経路情報がない

リンクの太さ

BGPピアリングを通過する
経路の数を回線の太さで示す

トランジットAS

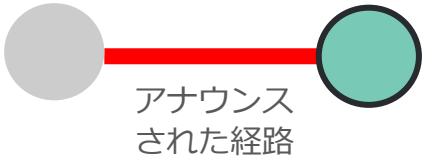
トランジットAS
中央にASNを表示

消去された経路

ターゲットのプリフィックスが
消去された

Origin AS

ターゲットのOrigin AS
中央にASNを表示



アナウンス
された経路

ターゲットのプリフィックスが
新しくアナウンスされた

ThousandEyesを使った Office 365 の (BGP) 障害解析例

2019年11月20日 障害発生

「Microsoft 365」で障害発生　「Teams」「Skype」など利用しづらい状況　アップデートが影響か

2019年11月20日 12時15分 公開　[ITmedia]

印刷　179　Share　B!　5

米Microsoftは11月20日午前10時53分（日本時間）、「Microsoft 365」に含まれる複数のクラウドサービスが利用しづらい障害が発生していると発表した。最近行ったネットワークアップデートが影響している可能性があるという。

- 「Microsoft 365」の障害が解消　「Teams」など全サービス復旧

Microsoft 365 Status @MSFT365Status · 2019年11月20日
We're investigating an issue preventing access to Microsoft 365 services. We'll provide additional details shortly on status.office.com.

Microsoft 365 Status
@MSFT365Status

We've identified that multiple Microsoft 365 services are affected and we're actively looking for the swiftest means of restoring access. Please refer to status.office.com for details, or MO196220 in the admin portal, if accessible.

♡ 233　10:53 - 2019年11月20日

298人がこの話題について話しています

該当するサービスは「Exchange Online」「SharePoint Online」「Microsoft Teams」「Skype for Business」「Yammer」など。

Microsoft 365のユーザー管理や契約形態の変更ができる管理者向けツール「Microsoft 365 Admin Center」も利用しづらい状況になっている。

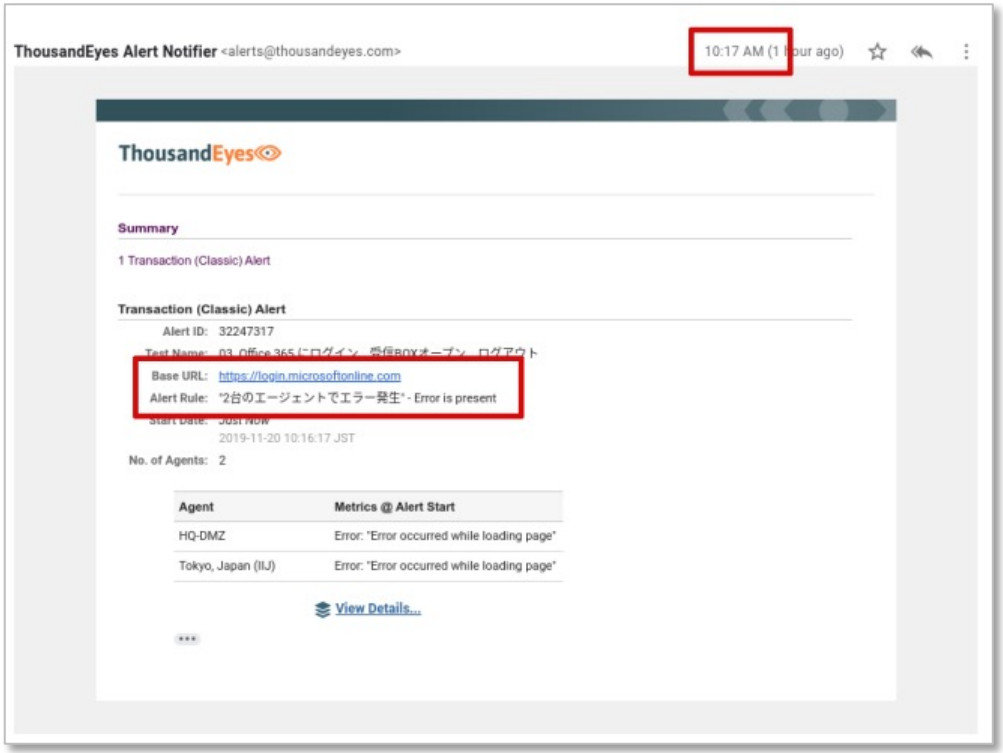
米Microsoftによる発表

同社は「最近のネットワークアップデートが、ユーザーのアクセス失敗に影響している可能性がある。当社はこの更新を元に戻したので、サービスは回復の傾向がみられる。今後も問題の原因を検証し続ける」と説明している。

すでに復旧済みだが、19日には日本、インド、オーストラリアなどで「Office 365」のメール機能が利用しづらい障害が発生していた。

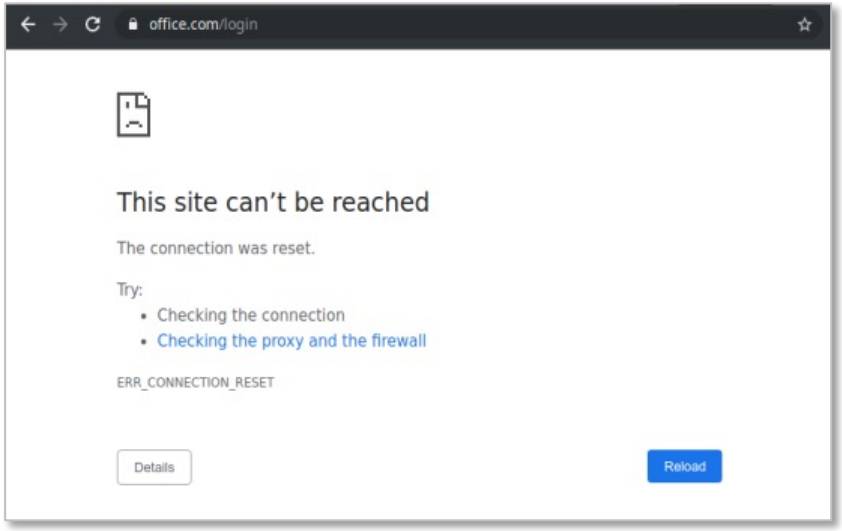
https://www.itmedia.co.jp/news/articles/1911/20/news088.html

障害発生直後にアラート通知 (2019年11月20日)



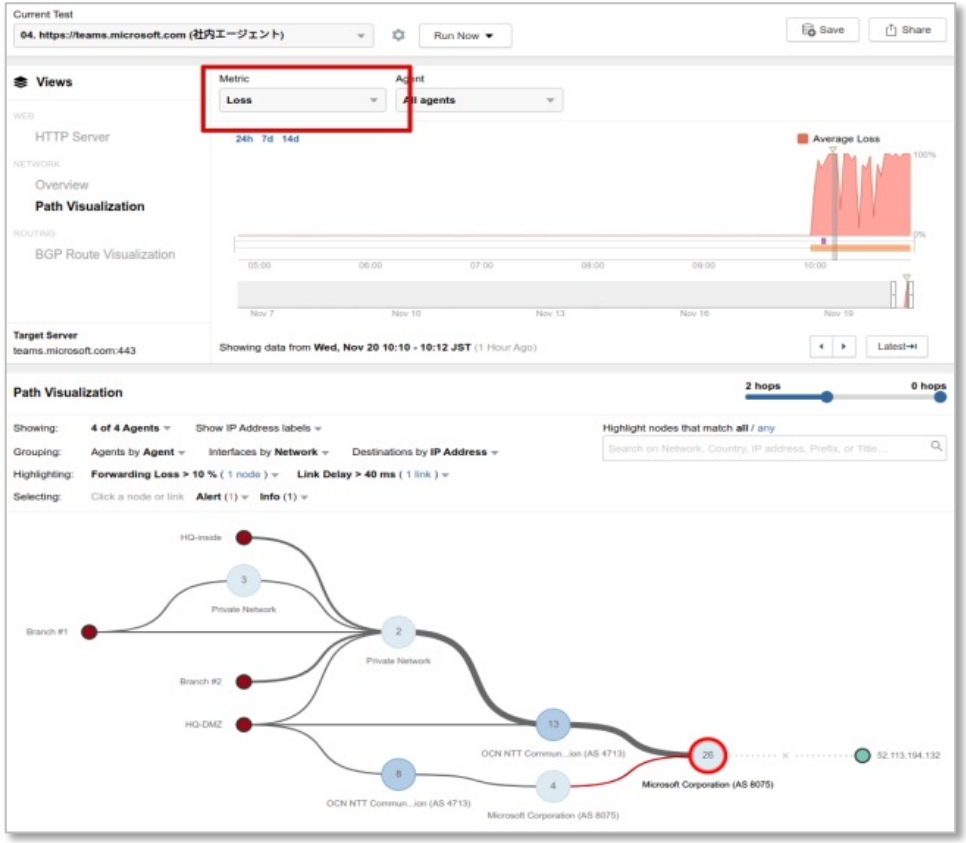
メールでアラート通知

共有リンク



実際ブラウザーのアクセスも不可

Office 365 の障害解析 (2019年11月20日)



10:00am
TeamsやOutlookへの通信でMicrosoft社のネットワーク内でほぼ100%のパケットロスが発生

10:00am
障害が発生する直前に Microsoft社のサービスが属する複数のネットワークへの経路の変動を確認

11:30am
日本国内のTeamsへの経路とサービスの復旧

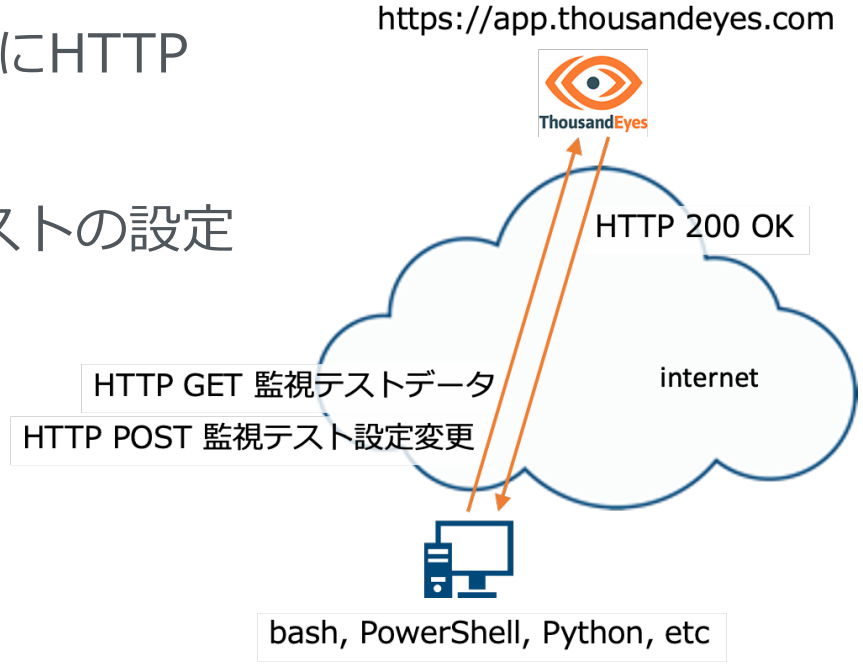
今回の障害は、Microsoft社のBGPルーティングの問題が原因で複数のサービスに影響を及ぼしたと考察

【共有リンク】
https://cmkyaz.share.thousandeyes.com/

ThousandEyes API

ThousandEyesのAPI

- RESTful API
- アプリケーションからAPIのURIにHTTP GET/POSTの通信を実行
- 監視データの読み取りや監視テストの設定変更が可能

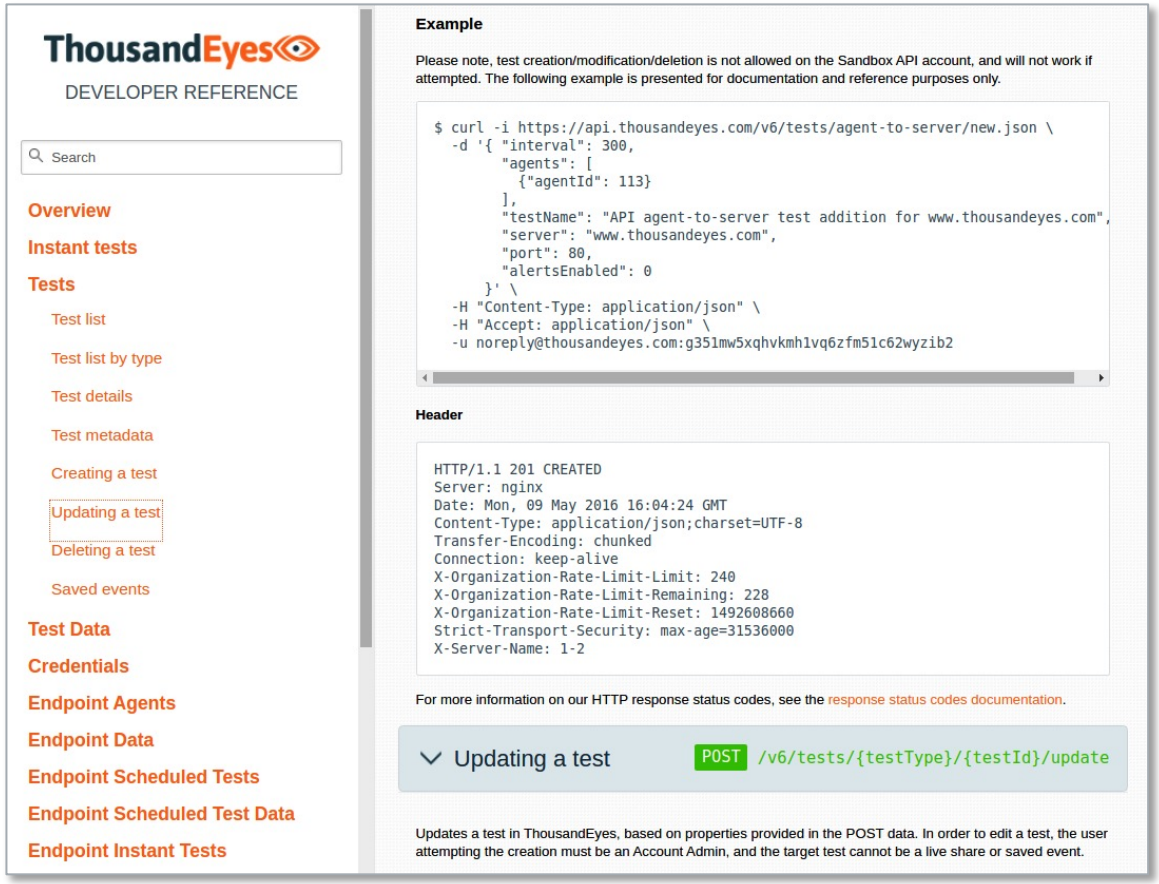


ThousandEyes APIのユースケース

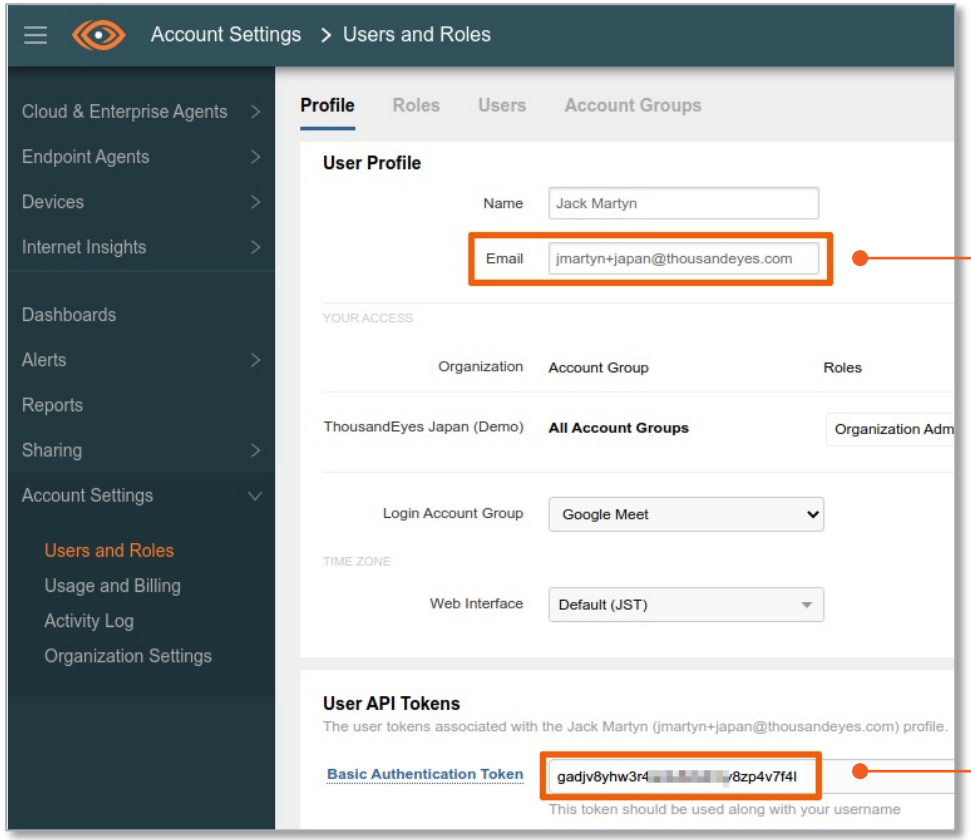
- 同じオペレーションを多数繰り返して実行する際
  - 監視ターゲットだけが違う監視テストをExcelファイルから数百個設定
  - APIを使いテンプレート化された複雑なレポートを自動設定
- 自動運用
  - アラートで障害を検知した時、自動にスナップショットを保存
  - 外部アプリと連携、監視テストの自動作成と設定変更

APIのオンラインマニュアル

https://developer.thousandeyes.com/



APIとの認証に必要なデータ



ユーザー名
（ログインに使ったメールアドレス）

API トークン

Q&A タイム

Thrive in a connected world™

ThousandEyes is
now part of Cisco.