Interop Tokyo 2017における ShowNet運用監視について

Zabbix Conference Japan 2017
ShowNet NOC Team
鈴木 孝規

SHOWNET
INHERIT THE INTENTION

自己紹介

- 所属
  - ニュータニックス・ジャパン合同会社
  - シニア ソリューション アーキテクト

- ShowNet 2015～2017 NOCチームメンバー
  - モニタリング担当（2016～2017）
  - 無線LAN担当（2015～2016）

SHOWNET
INHERIT THE INTENTION

アジェンダ

- ShowNetの概要
- ShowNet運用監視の考慮点
- ShowNet監視の取り組み
- ShowNetを監視するツール群

SHOWNET
INHERIT THE INTENTION

ShowNetの概要

ShowNetとは？

1. **最新鋭の技術、機器を集め構築される近未来ネットワーク**
   - 新技術の相互接続
   - 提供された機器を使い実ネットワークを構築
2. **世界最大のライブデモンストレーション**
   - 2年後、３年後に業界に浸透する技術に先駆けて挑戦
   - 世界、国内で初披露(実稼働)される新製品も導入
   - Interop Tokyoが唯一、開催当初のスピリットを継承
3. **コントリビューション(機器、技術提供）によって構築されます**
   - 産学官から集まったNOCチームメンバーと、機器やサービスをご提供頂く
   - コントリビュータのみなさま、一般から公募するボランティア(STM)の
   - 三位一体で構築

SHOWNET
INHERIT THE INTENTION

ShowNetの目的

- **未来のネットワークのデモンストレーション**
  - 相互接続性検証 ＝ Interopの理念
  - 使っただけ/動かしただけでなく、**どう使うか**を見せる
- **実サービスネットワーク**
  - 出展社、来場者への接続性提供
    - 対外接続性、バックボーン、ディストリビューション、Wifi、CGN、DHCP、DNSなどなど

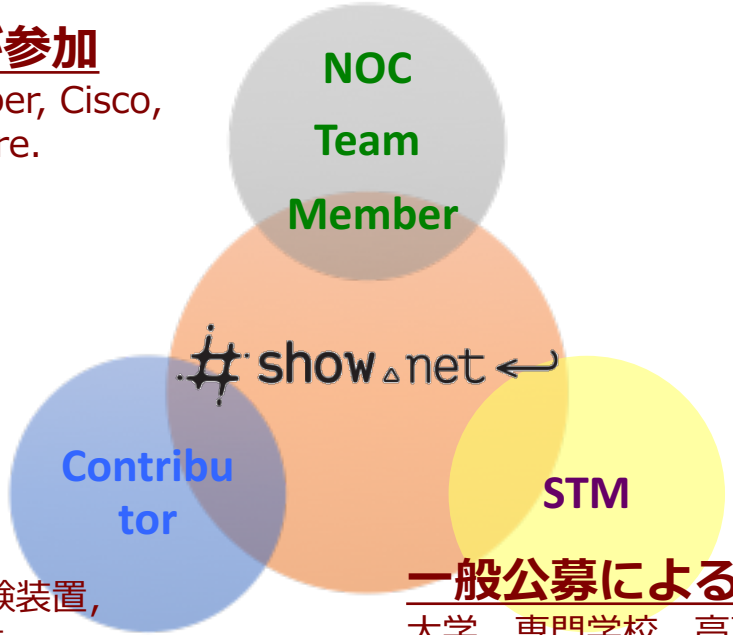
- I know it works because I saw it at Interop -

SHOWNET
INHERIT THE INTENTION

ShowNetの構成要素

3つの要素が、協力、調和することで、ShowNetは構築、運営されています！

産学界から様々な人材が参加
東大, JAIST, NTT Com, Juniper, Cisco,
さくらインターネット and more.

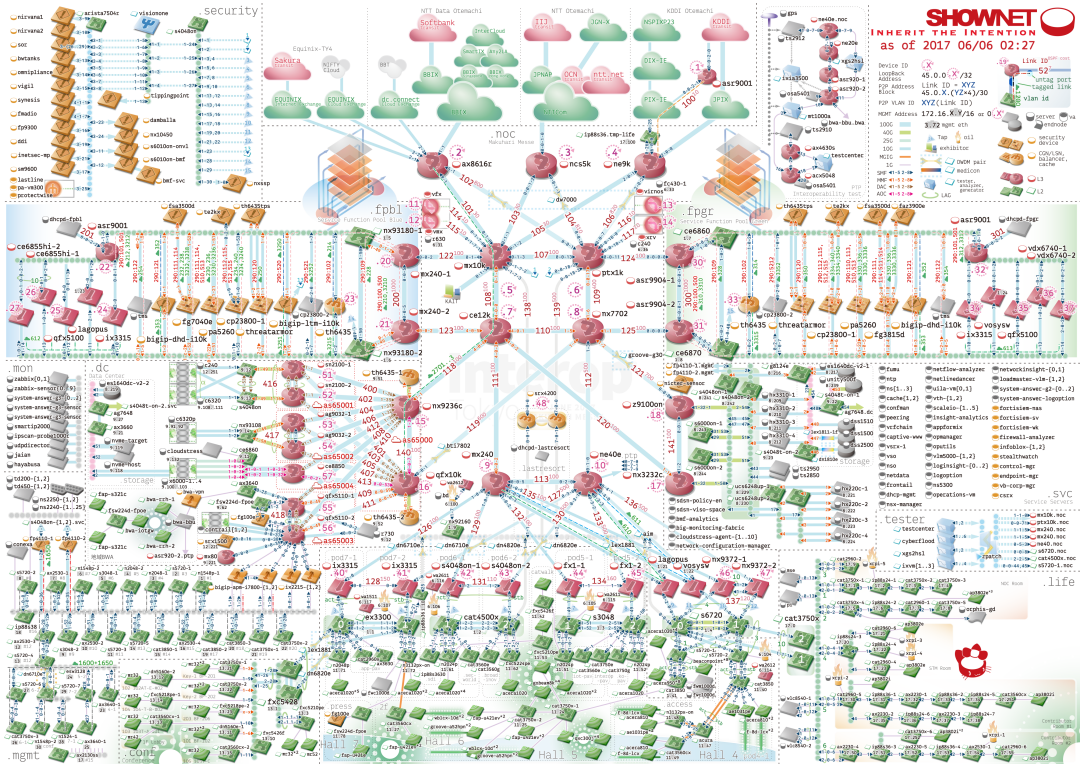


ShowNet機材提供企業
各種ネットワーク機器，負荷試験装置，
ソフトウェア, そして人材の提供

一般公募によるボランティアスタッフ
大学，専門学校，高専，企業(ISP, SIer…)など多種多様

SHOWNET
INHERIT THE INTENTION

2017年トポロジ図



SHOWNET
INHERIT THE INTENTION

ネットワークの規模

- コントリビューション総額：￥8,690,349,399-
- 動員数（のべ）　：**441名**
  - NOCチームメンバー　：27名
  - NOCチームアドバイザリーメンバー　：15名
  - STM/CTM　：31名
  - コントリビュータ　：367名
- NOCラックの電源総使用量：
  - 100V:148.0kw　200V:82.0kw
- UTP利用線長総計：25.1km（光ファイバ総延長：4.2km）
- NOCラック総コンセント数：約350個

各分野ごとのトピック

- 対外接続
  - ピアリングポータルによるIX Peer
- 伝送
  - 一芯多重伝送
- 相互接続検証
  - PTP
  - 地域BWA
- L2/L3
  - Service Chaining
- 出展社収容
  - 多様な回線を活用した死活監視
- セキュリティ
  - 大規模ネットワークにおけるインラインセキュリティ
  - EDRとの連携
- テスタ
  - 大規模に変化するネットワークを見越した負荷試験
  - 網内のセキュリティ検査
- Wireless
  - 機器特性を生かした無線設計
  - ネットワークサービスとしてのCaptive Portal
- モニタリング
  - ネットワーク構築の段階に応じた効率的な監視
  - リアルタイムネットワークテレメトリによる可視化
- データセンタ
  - 大規模仮想化基盤の導入
  - IPファブリックによる柔軟なネットワーク構成
  - マルチクラウドファブリック
- ファシリティ
  - アグリゲーション・クイックデプロイ

SHOWNET
INHERIT THE INTENTION

ShowNet運用監視の考慮点

Inherit the Intention

- Interop Tokyo 2016
  - モニタリングツールのInteroperability
  - API/クラウドを用いた通知連携、ChatOps
  - センサーを用いた温度や電力などのファシリティ常時監視
  - モニタリングチームによる監視、他チームへの通知

- Interop Tokyo 2017
  - ネットワークテレメトリのための全パケットキャプチャ
  - 機械学習を取り入れた早期異常検知と効率的な運用

SHOWNET
INHERIT THE INTENTION

ShowNetの特色

- 短期間でやることが大きく変わる
  - ホットステージ初期：物理構築
  - ホットステージ中期：機器の設定
  - ホットステージ後期：障害試験／負荷試験／引っ越し
  - 会期：システム／ネットワーク／セキュリティ運用

- 同じログが欲しい機器が大量にある
  - ルーターなどに設定できるログの宛先は限界がある

ShowNetモニタリングチームの方針

1. 可能な限り全ての機器から全てのログを集める
   - SNMP, SNMP Trap, Syslog, NetFlow, sFlow, IPFIX, 全トラフィックのパケット
2. チームごとの稼働状況を見る
   - Facility, External, L2/L3, DC, PTP, Wifi, Conf, MultiCloud, BWA, Security, Server, Storage, Ticket Management System
3. 人と機器のログを突き合わせて現状を把握する
   - 人:「設定完了、正常稼働してます」 → 機器:「error: xxxx」
   - 人:「通信できない」 → 機器:「no log]

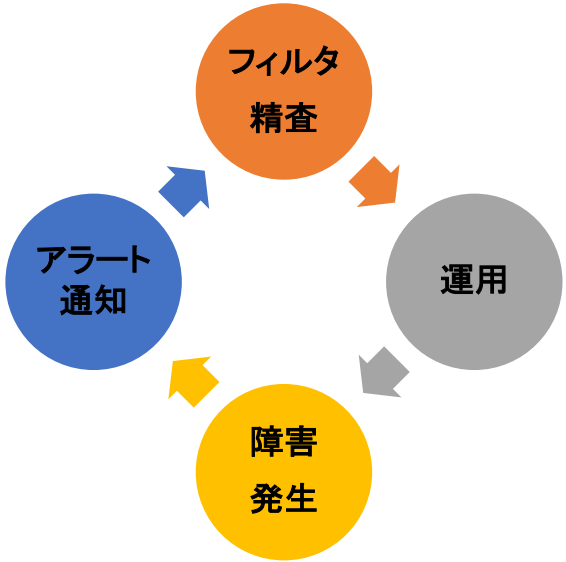
ShowNet監視の取り組み

ログ監視と通知 – ノイズとの闘い

- 運用監視UIはZabbixからのSlack通知
  - alertチャンネルから通知が来ると該当箇所を確認

- よく見かけるログ
  - Interface UP/Down
  - High Voltage
  - Packet Discarded
  - BGP Peer Down, OSPF Neighbor Down
  - Storm Detected
  - CPU/Memory/Disk alert

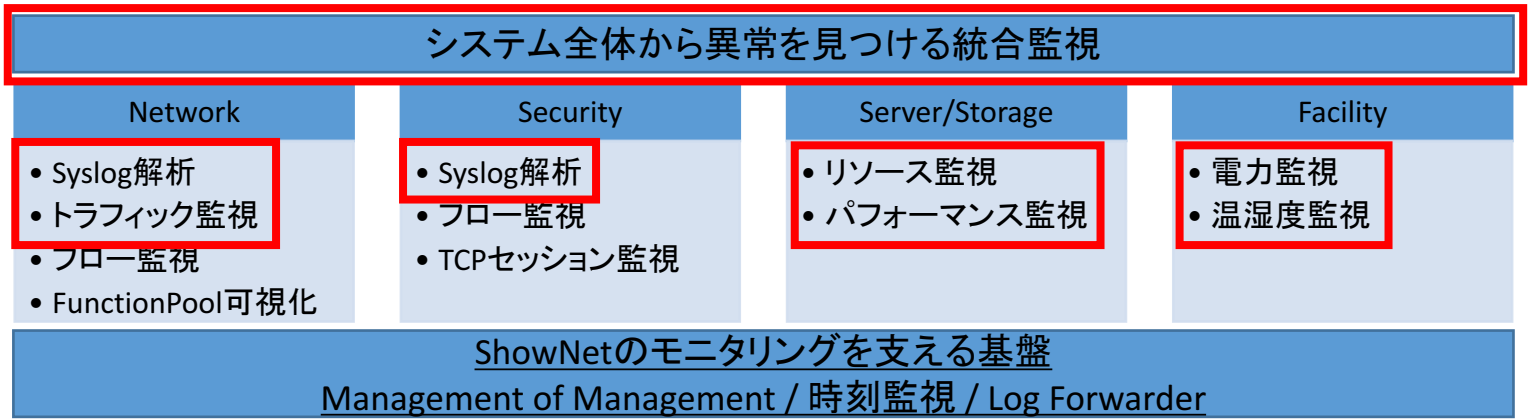
- 何を通知するかが毎日変わる
  - 日々、変化する環境ではフィルタの精査が重要
  - 失敗するとスマートフォンが鳴りやまない



SHOWNET
INHERIT THE INTENTION

ShowNetモニタリングの見どころ

1. 効率的なログ分析と機械学習による異常検知
2. 統合監視と個別監視/環境監視による広範囲のモニタリング機構
3. リアルタイムネットワークテレメトリによる可視化



Wide & Deep Monitoring

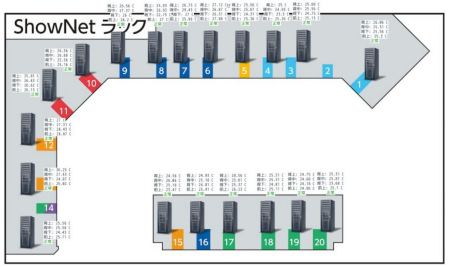
Zabbix

SHOWNET INHERIT THE INTENTION

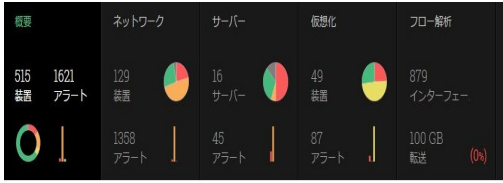
統合監視と個別監視/環境監視による広範囲のモニタリング機構

- 課題
  - 監視項目が多岐にわたり一つのツールでカバーできない
    - ネットワークトラフィック、xFlow、SNMP、Syslog
    - サーバ/ストレージリソース、HTTPコンテンツ、温度、電力
  - どのログをいつ見ればいいかわからない、ノイズだらけ
    - 常時構築、常時検証、常時運用
- 対策
  1. 統合管理ツール等による全体把握
     - Syslog, SNMP / SNMP Trap, xFlowのトータル管理
     - 1時間毎のコンフィグバックアップと差分表示による設定漏れ防止
  2. 対象ネットワークスキャンツールや気圧/温湿度センサーを利用し統合管理ツールへ情報集約
  3. 通知は統合管理ツールを経由してSlack通知
     1. フェーズ別での通知ポリシーの見直し
     2. 必要なときに必要なログがすぐに見れる環境

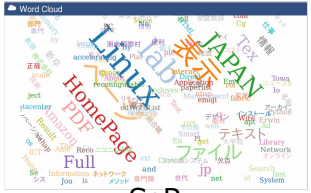
Appformix



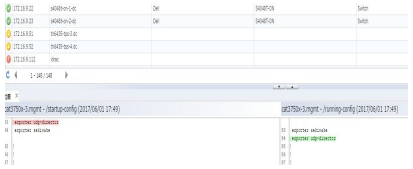
Zabbix



OpManager



SoR



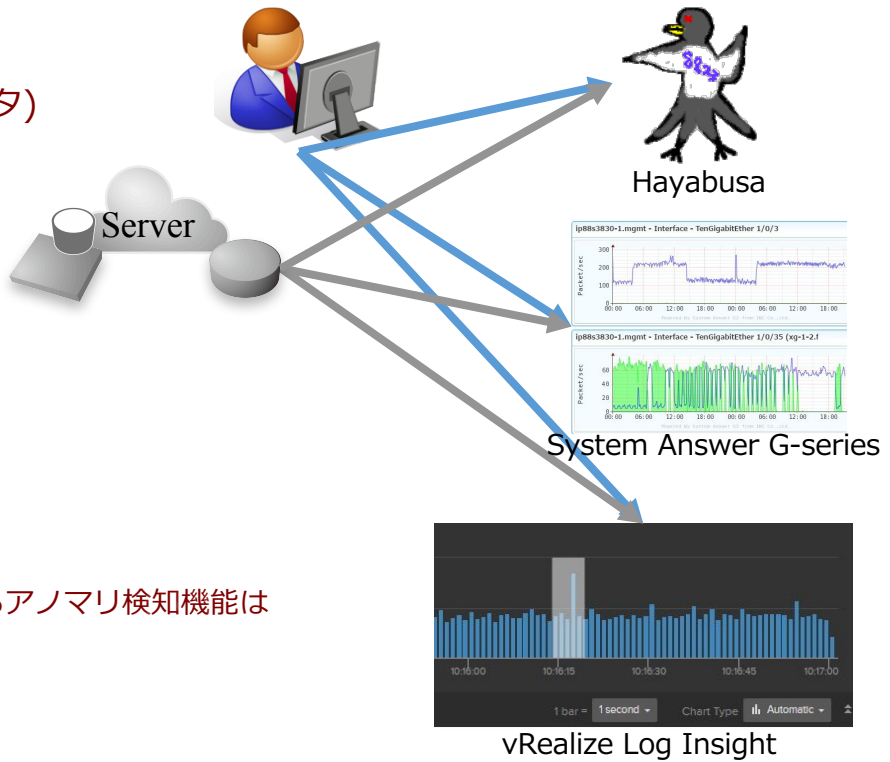
NetLine Dancer

SHOWNET
INHERIT THE INTENTION

効率的なログ分析と機械学習による異常検知

- 課題
  - 構築中の大量ログの分析(数字はHotStage中のデータ)
    - 最大Syslog数: 176,194,490件 / Day
    - 最大SNMP Trap数: 840件 / Day
    - 最大TCPコネクション数: 63,722,303 / Day

- 対策
  1. 問題が予測できるところは従来技術を適用
     - 知見のある所は従来技術の方がミスが起こりにくい
     - 時間を自由自在に切り替えることで異常値を発見
  2. 機械学習を取り込んだ監視ツール
     - ログをすべて見ることは不可能な規模では機械学習によるアノマリ検知機能は有効
     - 機械学習の結果が正しかったかどうかの検証は必須
     - 変化の多いShowNetでは最終判断は人間



SHOWNET INHERIT THE INTENTION

ログから見たShowNetの規模

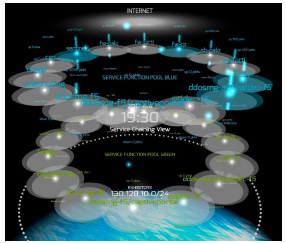
- ShowNet構築期間のSyslog
  - Syslog 19,377 /sec
  - Syslog 176,194,490件 / Day

- ShowNet初日の記録(2017/6/7)
  - Syslog数 71,234,562
  - TCPコネクション数 38,008,884
    - Syn 98.22%
  - xFlow数 1,025,572
    - NetFlow 99.32%

リアルタイムネットワークテレメトリによる可視化

- 課題
  - 従来技術だけではリアルタイムな情報が取れない
  - xFlowはサンプリングしないと負荷が高くスイッチやルーターで全フローを出すのは困難
  - 仮想スイッチやサービスチェイニングは既存の管理手法では見えにくい
  - リアルタイム性を高めるほど重要になる時刻同期

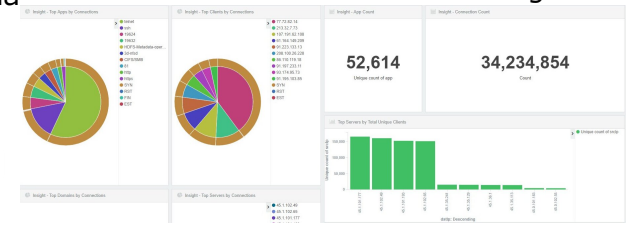
- 対策
  1. 新たなデータ取得方法
     - APIを使ったリアルタイムデータ取得、エンドユーザーレスポンス監視
     - TAPからの全パケットをキャプチャして可視化
     - 専用サーバーによる1:1 NetFlow Generation
  2. サービスチェイニングの実装に合わせた可視化
     - 既存ツールの限界を超えるShowNetカスタマイズされたFunctionPool可視化
  3. 時刻監視システムによる常時監視
     - 仮想サーバーやネットワーク機器は時刻同期がはずれても気付きにくいので外部システムから強制的に同期状態を確認
     - 最終的にはPTPとの連携でマイクロ秒オーダーのログ記録を実現



NXS-TVL

Uila

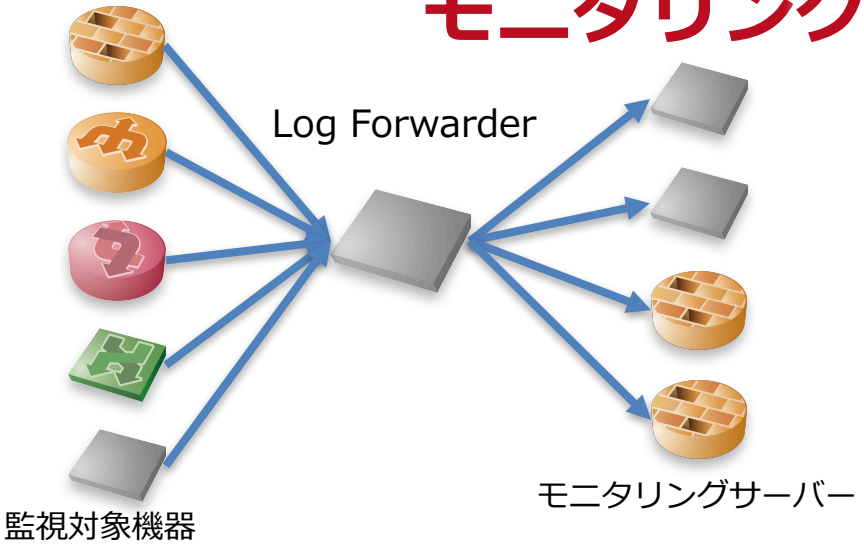

vRealize Network Insight

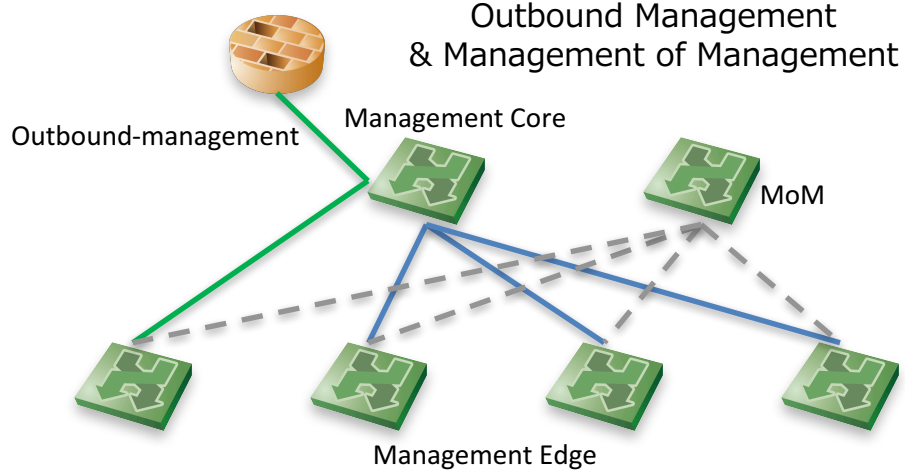


VCF-Center Insight Analytics

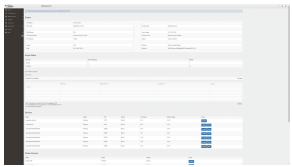
SHOWNET
INHERIT THE INTENTION

モニタリングを支える基盤技術





全機器のログを集約して転送するログフォワーダー



UDP Director

Jaian

管理対象デバイスのIPアドレス台帳

SmartIP2000

ログで最も大切な時刻の監視

TS-2850 Time Server

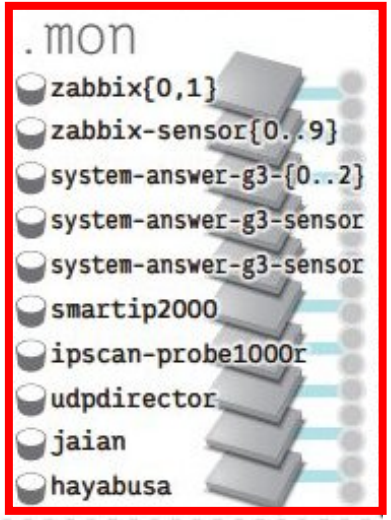
SHOWNET
INHERIT THE INTENTION

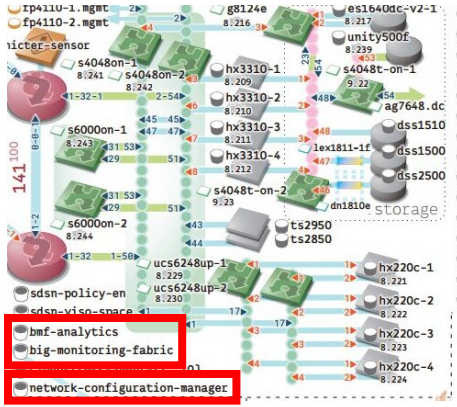
Zabbix at ShowNet

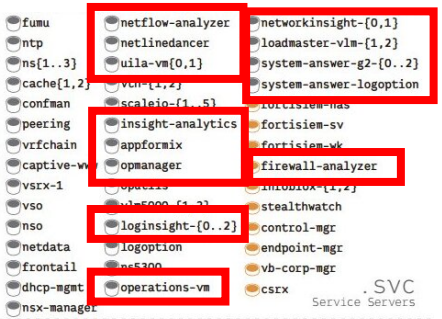
- 管理対象
  - 全機器からのSyslog, SNMP, SNMP Trap
- 対象外
  - xFlow, 生パケット、L1情報
- 役割
  - 統合監視（他の管理ソフトウェアの監視含む）
  - 温湿度監視
  - Slack通知の唯一のインタフェース
  - ルーティングテーブルの状態監視（カスタムスクリプト）
- あると嬉しかった機能
  - ウィザード形式で誰でもしきい値を変更できる機能
  - WebUIからのカスタムスクリプト編集機能

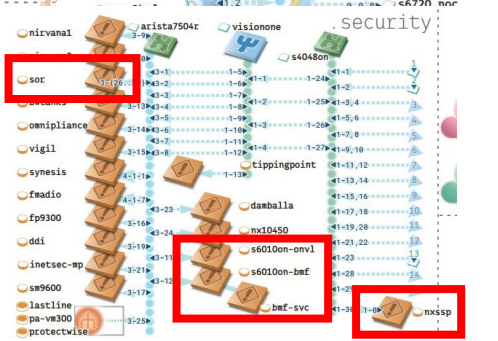
ShowNetを監視するツール群

ShowNetの監視システム群





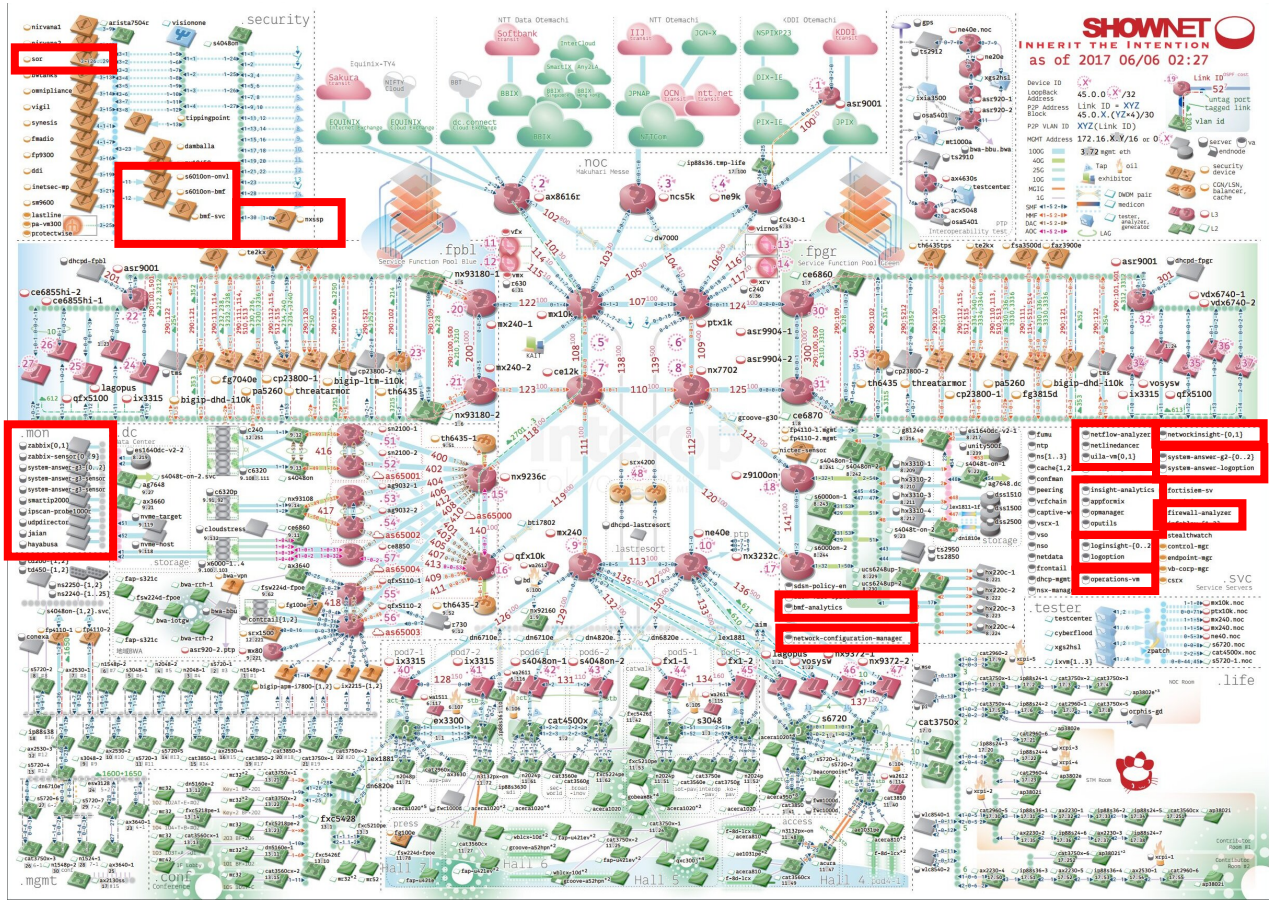




ハードウェアは基本的に.mon
タップからパケットを見る製品は.security
ソフトウェアは.svc

SHOWNET
INHERIT THE INTENTION

ShowNetを監視するツール群



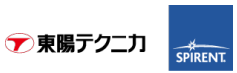
SHOWNET
INHERIT THE INTENTION

役割別コントリビューション一覧

- 統合管理製品
  - Zabbix Japan様 Zabbix
  - IBC様 SystemAnswer Series
  - ゾーホージャパン様 OpManager
- ネットワーク監視
  - 富士通九州ネットワークテクノロジーズ様 NXS-TVL
  - VMware様 vRealize Network Insight
  - ViaScope様 SmartIP2000 / Probe1000R
  - Dell EMC様 Pluribus VCF Center
- Syslog監視
  - VMware様 vRealize Log Insight
  - JAIST様 Hayabusa
- xFlow監視
  - ゾーホージャパン様 Netflow Analyzer
  - Cisco様 StealthWatch
  - Dell EMC様 BigSwitch BMF Analytics
- コンフィグ管理
  - ロジックベイン様 Net LineDancer
  - ゾーホージャパン様 Network Configuration Manager
- 温湿度監視、電力監視
  - Zabbix Japan様 温湿度気圧センサー
  - IBC様 無線温度センサー
  - Panduit様 無線温度センサー
- ハイパーバイザー監視
  - VMware様 vRealize Operations
  - Juniper様 Appformix
- エンドユーザーレスポンス監視
  - 東陽テクニカ様 Uila
- HTTPコンテンツモニタリング
  - 慶応義塾大学 西研究室様 SoR
- Firewall監視
  - ゾーホージャパン様 FireWall Analyzer
- 時刻監視
  - セイコーソリューションズ様 Time Server TS-2850
- ログ転送
  - Cisco様 StealthWatch UDPDirector
  - JAIST様 JAIan

SHOWNET
INHERIT THE INTENTION

Monitoring Contoribution



SHOWNET
INHERIT THE INTENTION


SHOWNET
INHERIT THE INTENTION