

商用サービスインフラにおけるSONiCスイッチ障害交換運用の実際

JANOG54 (2024/07/05)

三井情報株式会社

- 背景説明(説明対象の商用サービス、なぜSONiC?)
- 構築時に遭遇した問題の数々
- ZTPによるSONiCスイッチの交換運用
- まとめ

松本 直樹

□ 三井情報株式会社

- ソリューション第二技術本部 イノベーション推進部 第二技術室
- ITインフラ関連の研究開発 + PoC案件対応
- 2002年 新卒入社～ （当時はネクストコム株式会社）
- 基本的にはNWエンジニア 主にFirewallやSLB、WebProxy等

□ 出身：千葉県

□ 趣味：子供と散歩、捕食系動画の鑑賞



芹田 大輔

□ 三井情報株式会社

- ソリューション第二技術本部 イノベーション推進部 第二技術室
- L2/L3スイッチのネットワーク設計、構築、技術支援業務
- 2001年～（当時はアダムネット株式会社）
- L2/L3スイッチを取り扱うNWエンジニア

□ 出身：秋田県

□ 趣味：猫に世話をしてもらうこと



背景説明

サービス提供・運用をしているものの体制は少人数...



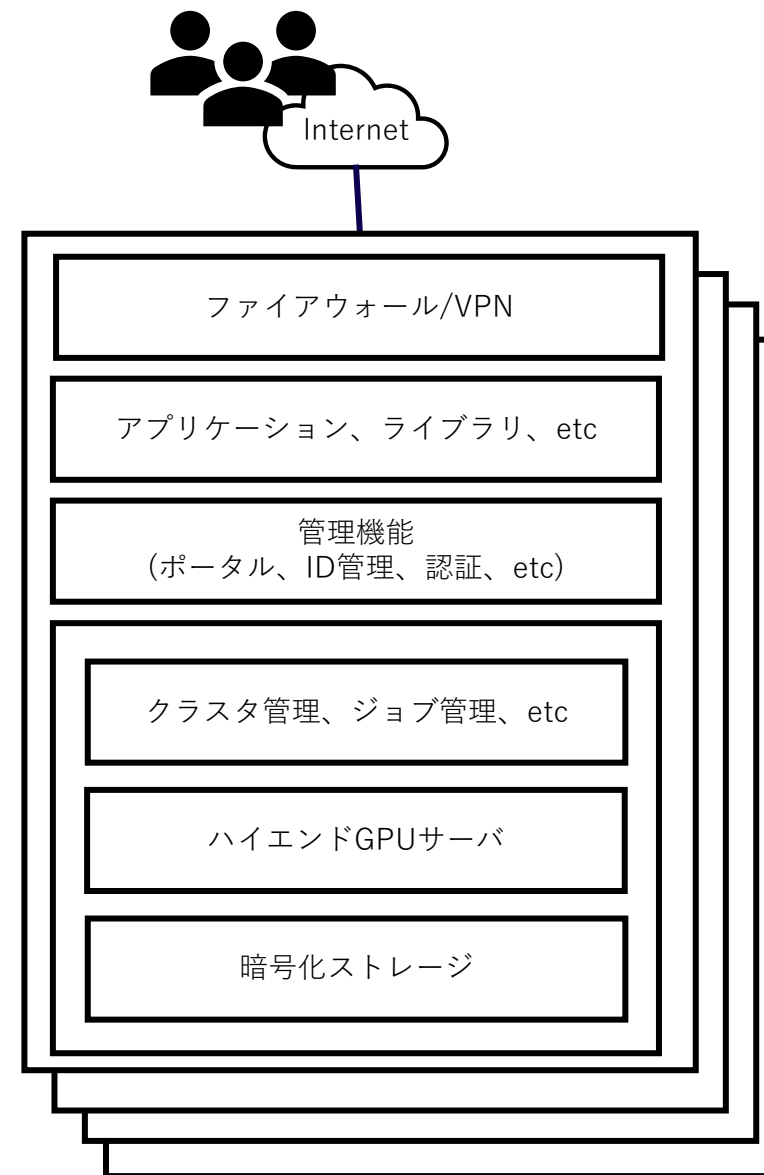
運用効率化・自動化等に取り組んで
自分達に**心と時間の余裕**を作りたい

研究開発っていうなら
社外発表の一つもやれ！



- ⇒ JANOGにはNW運用現場の第一線で活躍されている方が多いらしいので、SONiCやIP Clos Nwやら運用する上での色々知っている人に会えるかも！
- ⇒ 設計構築時からSONiCをちゃんと使うための参考情報が得られなかった...。我々の実践結果や取組のGood/Badが、実は皆さんのお役に立てるかも！？

- 今年2月にサービスインしたばかりの創薬AI向けGPU計算リソース提供サービス
- プールしているハイエンドGPUサーバ・ストレージ領域を顧客テナント毎に割り付けてVPN越しに利用頂くイメージ
- GPUサーバ利用界限で必要なVMや運用管理機能等を提供するコンテナ等動作させるVM/コンテナ基盤やNFS/Lustreストレージが動作

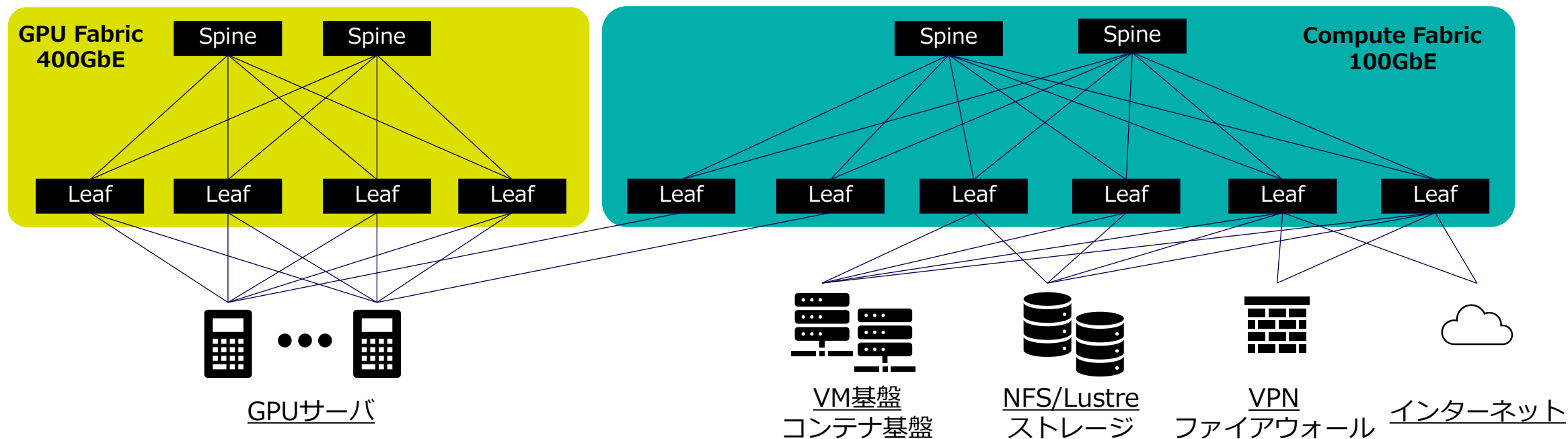


詳しくは

三井情報、創薬支援サービス「Tokyo-1」のIT環境を導入し、製薬会社による利用開始
<https://www.mki.co.jp/news/solution/20240208-1.html>

SONiCによるEthernetファブリック

2層IP Clos NetworkのVXLAN/EVPNによるL2/L3VPNマルチテナントNWを提供



なぜSONiCを選択したのか

我々が求めるITサービス向けNWインフラの要件

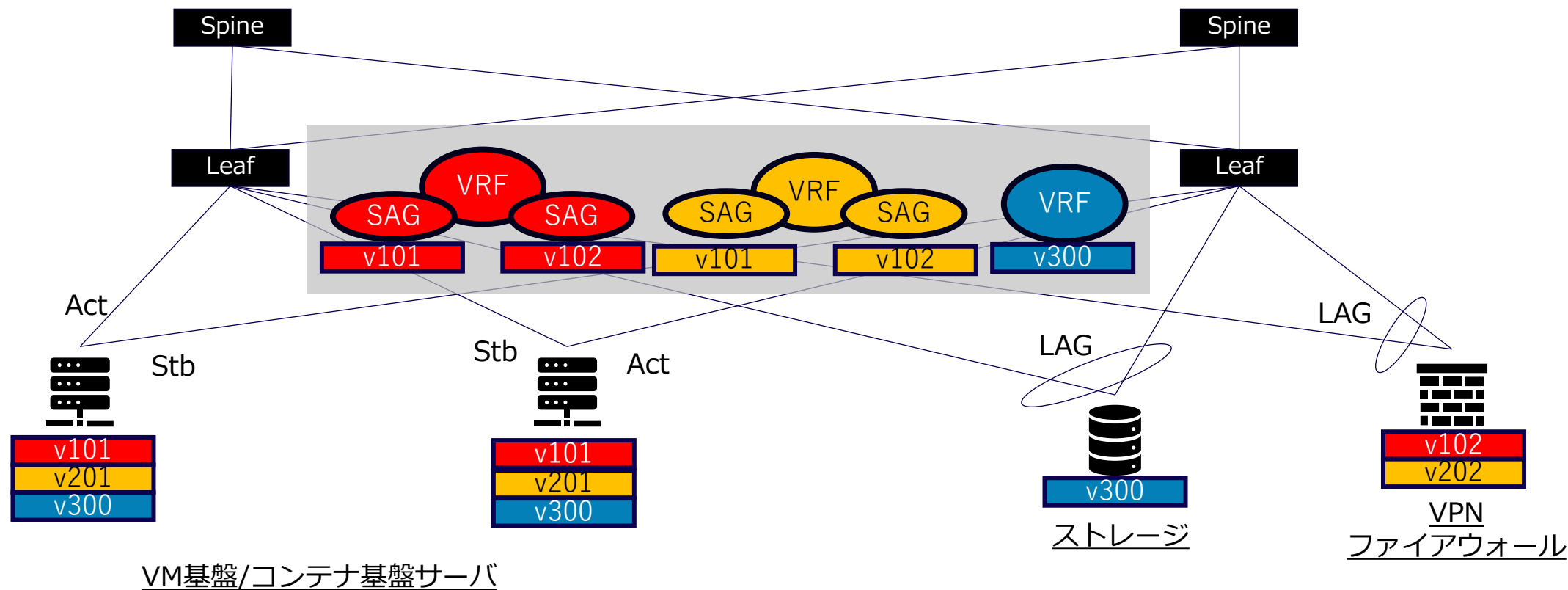
- ✓ ネットワーク帯域幅、接続要件の変更や拡張が柔軟・容易であること
- ✓ 構成する機器のベンダーロックインを回避しやすいこと
- ✓ マルチテナントを実現しやすく様々な通信特性やユースケースに柔軟であること

上記を満たすべく採用した構成や技術

- ✓ NW機器同士が疎結合なIP Clos NetworkデザインのSpine/Leaf構成
- ✓ オープンスタンダードなBGP、EVPN/VXLANを採用した
アンダーレイ/オーバーレイネットワーク
- ✓ マルチベンダで調達しやすいホワイトボックススイッチ製品

これらが実現でき、特定メーカーに縛られない
オープンなNOSとして**SONiC**を選択

構築時に遭遇した問題の数々



- VM基盤サーバやストレージを接続するため、Act/Stbの非LAG(RoCEv2対応NICの仕様に因る)やLAG+EVPNMHでL2可用性設計。
- L3では、VRFやSAG(Static Anycast Gateway)、ACLsの機能も使用。

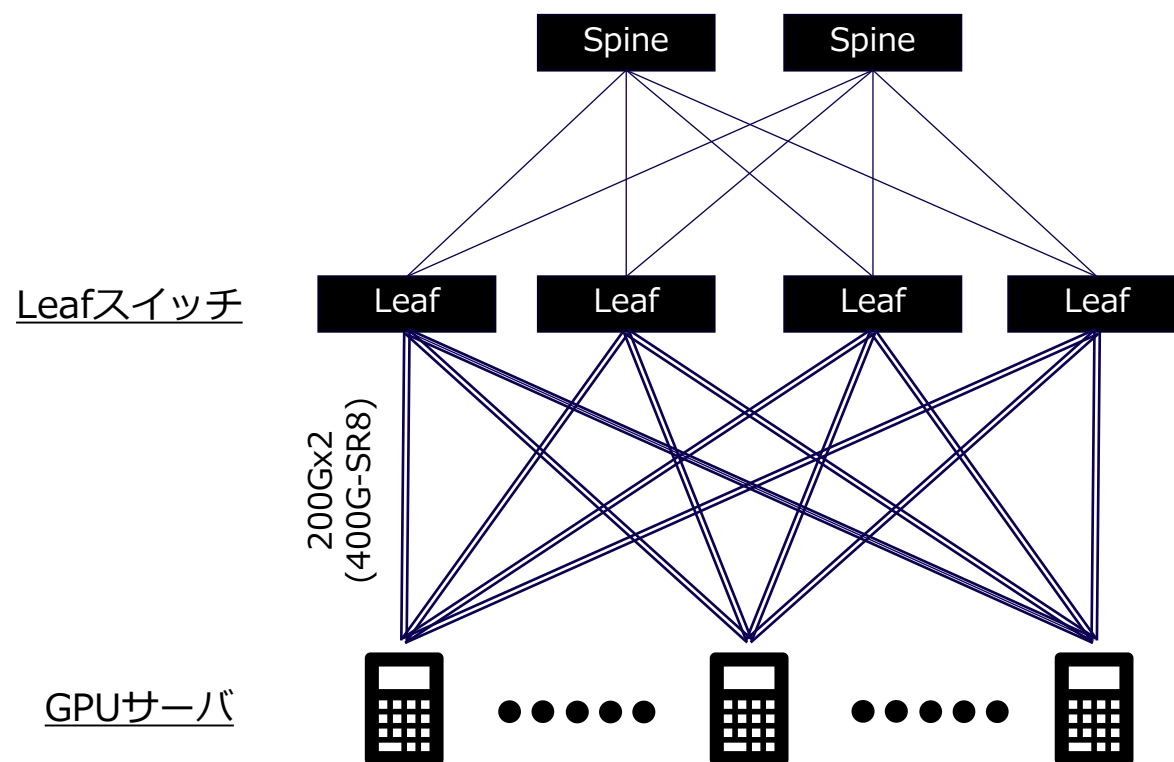
サービス全断しかねない致命的な通信トラブルに遭遇

- 試験でLeafスイッチ再起動の度に不特定多数の通信断(復旧もしない)に見舞われる。致命的な通信断で、幾度もVM基盤の再構築をSV担当者に依頼するハメに...
- SAGのIPアドレスを使った疎通確認が役に立たず。
どこからどこへパケットが飛んでるのか客観的にはサッパリ。。。
※採用したSONiCの仕様でVLAN I/FにSAGを使うと仮想アドレスしか設定できず。
- ベンダーさんからは、VNIをたくさん設定していると起動時に全VNI認識するまで分単位で時間かかるというお話が聞けたが、これが原因というわけではなかった。
- SONiCのアーキテクチャにも少し踏み込んでみて暫定対処を模索。

Leafスイッチ起動時はダウンリンク(=サーバ接続)を
Shutdown状態で起動させて、暫く時間たってから
ダウンリンクをUpさせるとうまくいく

↑
原因はわからないものの、**ワークアラウンド**を確立した

今度はGPUファブリックで



AOC接続検証時の写真

- GPUサーバとLeafスイッチ間の1対向を内部的にBreakoutしてスイッチ上で200GbEインタフェースx2に見せかける謎の設計をする必要があった。

- Leafスイッチを再起動する度にGPUサーバの400G(200Gx2)接続が徐々にリンクアップしなくなる事象が発覚した。
- GPUサーバでNICのファームウェアリセット(?)のコマンドを発見！！が、実行を試みるもサーバOS自体が再起動を始めた…。
- 今なお、トランシーバのメーカーさんにてトラブルシューティング中...

GPUサーバ側で物理的にトランシーバを抜き差しすれば
復旧することを見



データセンターの方に物理的な挿抜を施して頂く
ワークアラウンドを確立した

根本解決はできておらず、スイッチ1台を停止・起動するだけでも、色々対処を施さないとサービスに重大な影響を与えてしまう状況。

とても変更や拡張が柔軟・容易なネットワークとは呼べない。

ワークアラウンドだけは手動運用で対処するにしても、運用上で発生する作業の自動化・効率化を推進しないと運用体制が厳しい...

やった方が良く考えていること

⇒ ネットワーク機器の交換や追加に際しては、
周辺機器等に求められる操作や作業を含め極力自動化していく。

今回はこちらにフォーカス！

⇒膨大なログや状態表示からどんな状態ならば正常と見なしてよいか、
その確認手段や判断条件を含めて自動化前提で実装していく。

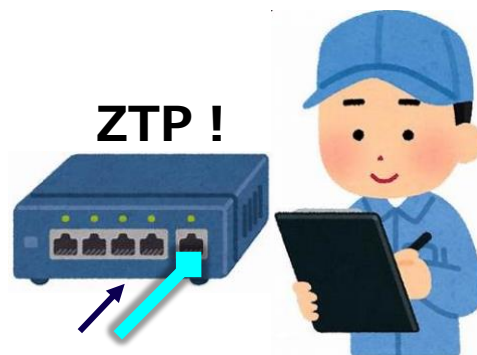
ZTPによるSONiCスイッチの交換運用

⇒ ネットワーク機器の交換や追加に際しては、
周辺機器等に求められる操作や作業を含め極力自動化していく。

SONiCスイッチの障害機を予備機に交換する一連の手続きの中に
ZTP(Zero Touch Provisioning)を本番環境に導入すべく検証を実施。



①物理交換作業
⇒カスタマエンジニア

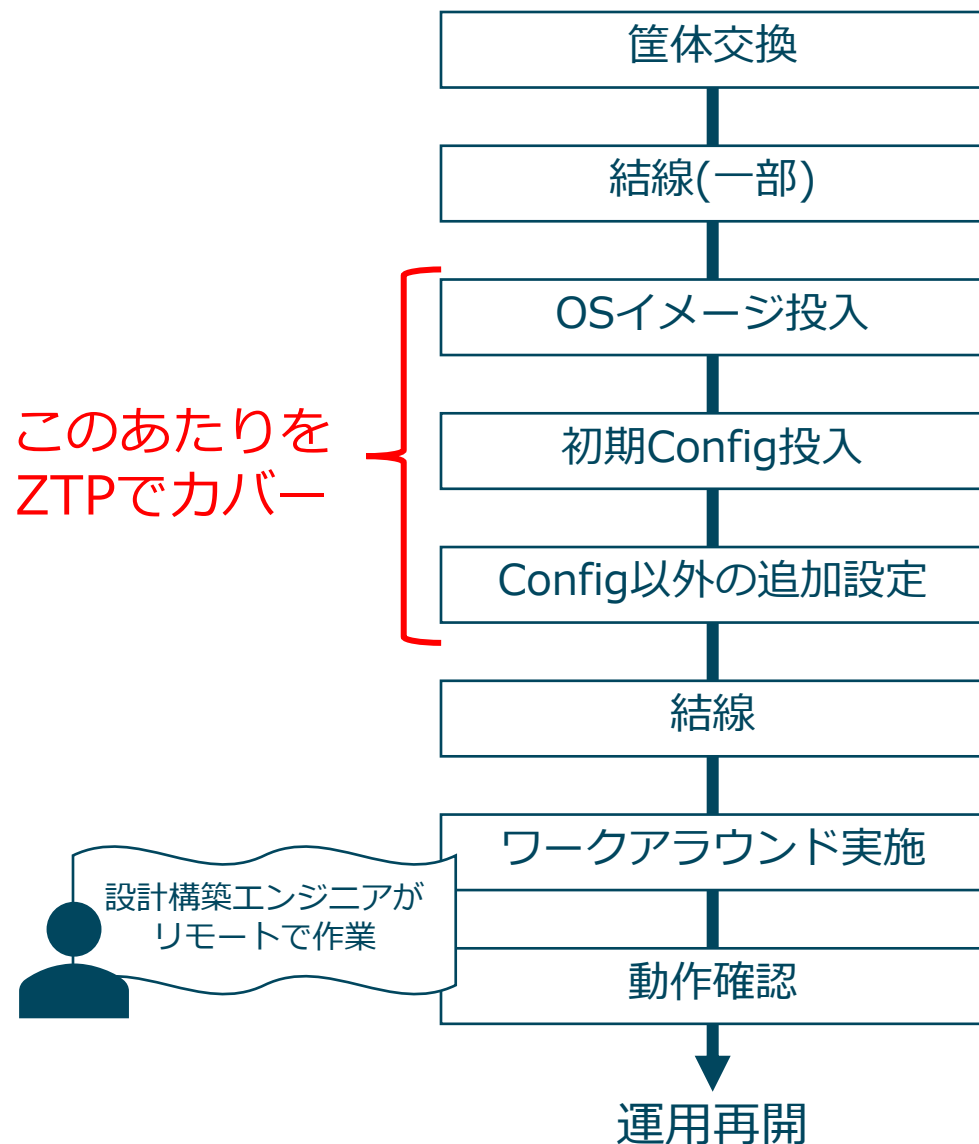


②初期化/設定復旧/諸々操作
⇒カスタマエンジニア+ZTP



③スイッチ起動時問題の
ワークアラウンドなど複雑な作業
⇒設計構築エンジニア+スクリプト

SONiCスイッチの機器交換の流れ



この運用が実現できるなら、

- ✓ 現地に物理作業できる要員が居るだけで良い。
- ✓ SONiCの巨大なOSファイル(1GB超)の端末受け渡しが必要なし。
- ✓ 設定情報の端末持ち出しは必要なし。
- ✓ 操作の抜け/誤りが無くなる。

※SONiCは設定操作の体系がややこしい

メリットしかなかった...

必要となった機材

□ ONIEが導入されたホワイトボックススイッチ予備機

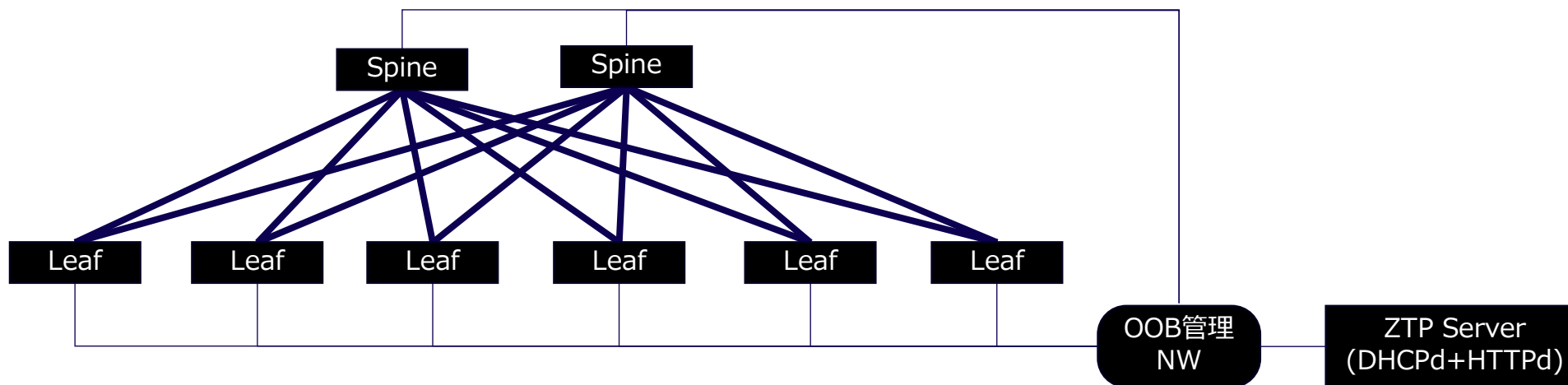
□ ZTPサーバ

Ubuntu Server、ISC DHCPとApache HTTP Server導入。

※予備機の管理ポートMACアドレスに紐づけたDHCPサーバのIPアドレス払い出し設定済み

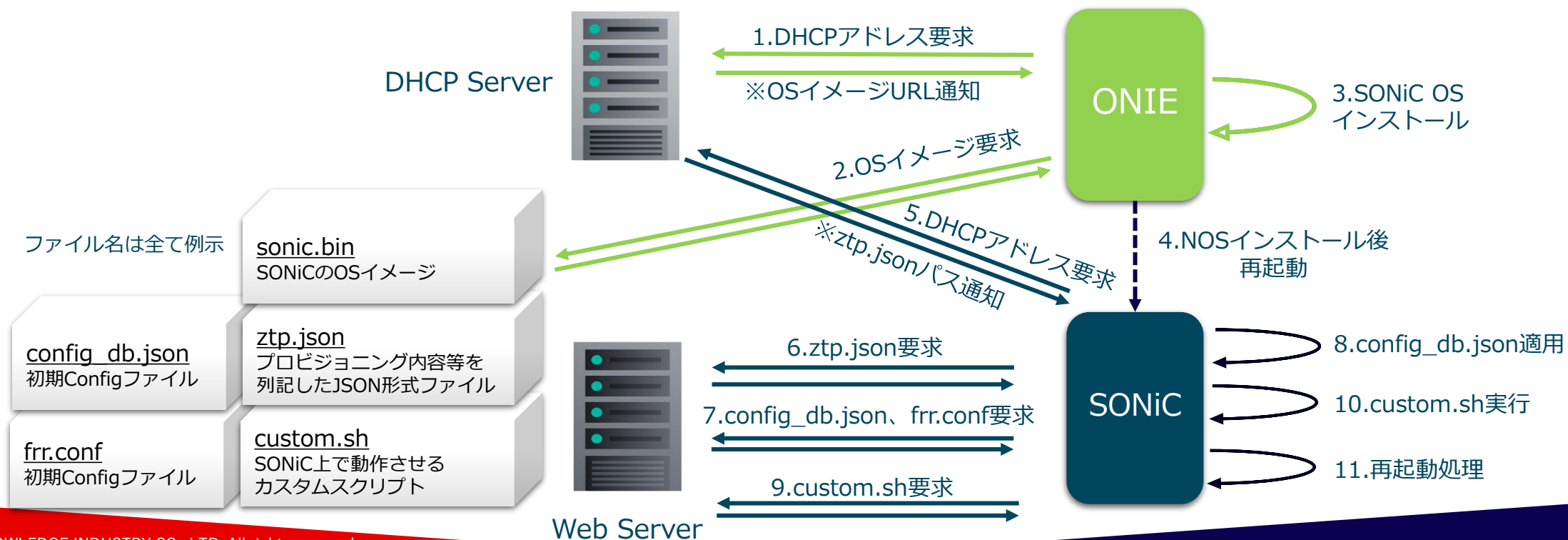
□ DHCPリレーエージェント (必要なNW構成の場合のみ)

※本番環境ではスイッチのOOB管理セグメントとZTPサーバ動作セグメント間にある
ファイアウォールがDHCPリレー予定



SONiCスイッチにおけるZTP動作

- SONiCのOSイメージ自体の導入はONIEのNOS(Network OS)インストールの仕組みで行い、SONiCのZTP同様DHCPの仕組みを利用する。
- SONiCのZTPは、DHCPオプションとWebサーバによって実現。
Webサーバから取得させるztp.jsonファイルの記述で様々なプロビジョニング内容を指示できる。
※config_db.jsonファイルの取得、任意スクリプトファイルの取得・実行など
- ZTPの完了はフラグで管理されているため、再起動処理を挟むことも可能。



DHCPサーバ設定(dhcpd.conf抜粋)

```
# per host
host leaf001 {
    hardware ethernet ab:cd:ef:01:02:03;
    fixed-address 10.1.1.11;
    # ---- for ONIE ----
    option default-url = "http://10.1.1.201/sonic/os/leaf001_sonic.bin";
    # ---- for SONiC ----
    option bootfile-name "http:// 10.1.1.201 /sonic/ztp/leaf001_ztp.json";
}
```

leaf001_ztp.json

```
"01-download":  
  "url":  
    "source": "http://10.1.1.201/sonic/config/leaf001_config_db.json",  
    "destination": "/home/admin/config_db.json"  
  "url":  
    "source": "http:// 10.1.1.201/sonic/config/leaf001_frr.conf",  
    "destination": "/etc/sonic/frr/frr.conf"  
"02-provisioning-script":  
  "url": "http:// 10.1.1.201/sonic/ztp/leaf001_install1.sh"  
  "reboot-on-success": true  
"03-provisioning-script":  
  "url": "http:// 10.1.1.201/sonic/ztp/leaf001_install2.sh"
```

leaf001_install1.sh

```
#!/bin/bash  
#mac change  
DUT_MAC=`show platform syseeprom | grep 'Base MAC Address' | awk '{print $6}'`  
jq --arg dut_mac $DUT_MAC '.DEVICE_METADATA.localhost += {"mac": $dut_mac}'  
/home/admin/config_db.json > /home/admin/config_db.json2  
cp /home/admin/config_db.json2 /etc/sonic/config_db.json
```

Config上の予備機のMACアドレス書換処理

leaf001_install2.sh

```
#!/bin/bash  
# Rewrite rsyslog.conf.j2  
sed -i.org -e 's/¥*¥.¥*/¥*¥. INFO/g' /usr/share/sonic/templates/rsyslog.conf.j2  
systemctl restart rsyslog-config  
# Modify User-Account  
echo admin:$(LANG=C perl -e 'print crypt("MyPaSsWoRd", "salt"), "¥n")' | chpasswd -e
```

config_db.json上に保存されない類の雑多な設定群の反映

躰いた点① ベースMACアドレス

config_db.json : 障害交換前のスイッチから保存したコンフィグファイル。旧機器のMACアドレスが記載。

DHCPサーバ : 予備機向けに動作するように予備機のMACアドレスで設定を準備。



旧機器のMACアドレスが含まれたconfig_db.jsonを読み込んで起動すると、再起動時に意図したアドレス払い出しができない。



スクリプトで自機のベースMACアドレスを抽出、config_db.jsonのMETADATAを書換。

```
#mac change
DUT_MAC=`show platform syseeprom | grep 'Base MAC Address' | awk '{print $6}'`
jq --arg dut_mac $DUT_MAC '.DEVICE_METADATA.localhost += {"mac": $dut_mac}' /home/admin/config_db.json >
/home/admin/config_db.json2
cp /home/admin/config_db.json2 /etc/sonic/config_db.json
```

躓いた点② 対話型コマンドを使った設定の代替

カスタムスクリプトで管理者パスワードの変更をpasswordコマンドでそのままやらせてみた。



対話型コマンドなので、

```
password admin  
MyPaSsWoRd  
MyPaSsWoRd
```

と書いてみたが成功するはずもなく。



SONiC Wikiに掲載されていたワンライナーで実行できるスクリプトで実装できた。

```
# Modify User-Account  
echo admin:$(LANG=C perl -e 'print crypt( "MyPaSsWoRd", "salt"), "¥n"') | chpasswd -e
```

参考 : [How to Change the Password · sonic-net/SONiC Wiki · GitHub](#)

躓いた点③ ワークアラウンド(ダウンリンクポートのNo Shutdown)の適用

前半に説明した致命的な通信トラブルのワークアラウンドもZTPで処理できればと思い、ZTPカスタムスクリプト末尾でダウンリンクポートのNo shutdown手順を追加してみた。



効果なし（通信断発生）



SONiCを構成する各コンテナが起動するのはZTPのシーケンスが完了してから(?)だった。



VNI/RemoteVTEP等、BGP/FRRが起動した後の話なのでZTPの中で組み込むことは諦めた。

⇒ZTP完了後に別途自動化処理を実行することとも考慮したが、
今後の改修・改善を待つことにして手作業での対応、と整理。

□ZTPによるスイッチ交換手順の自動化

⇒期待値はクリア。リハーサルまで実施して問題無し
(まだ本番環境で障害は発生していない)

カスタムスクリプトには様々な書式があり、色々な処理を実装できそう。

正常状態確認、疎通確認、etc...

□構築時にあった諸々障害への対応負担(ワークアラウンド実施等)

⇒ZTPの自由度からワークアラウンドの手順も実装できるかと思いきや実装不可。

まとめ

- 我々の知見や経験不足のためか、構築で色々と問題発生。
構築時に根本解決できず、その対処を運用へ先送りしてしまった。
- ZTPを本格的に使うのは始めてだったが、運用負担を減らすために、
ZTPによるスイッチ交換の自動化をSONiC向けのノウハウを獲得しつつ、
本番導入Readyな状態まで到達させることができた。
- SONiCはディストリビューション固有/独自の部分を除けば、
ソースコードやアーキテクチャ情報は広く開示されている。
柔軟性が高くZTP等の機能は様々な可能性を感じる一方、
トラブル発生時にも我々SIer自身が深くSONiCを理解することが求められる 😞

- 商用利用においてスイッチ機器交換にはどんな手法や手段を皆さんご検討・採用されているのでしょうか？
- 我々が運用する商用サービスではスイッチ障害は運用フェーズでまだ発生しておらず、スイッチの障害交換を本番で行ったことはまだありません....

よくありそうなIP Clos Networkを採用したマルチテナントNW設計ですが商用サービス等でZTPの有無に限らず、いざスイッチ交換しようとしたら、どんな事が起きるのか/問題があったのか是非情報共有させください。

- ホワイトボックススイッチ製品とSONiCを始めとするNOS製品の組み合わせは、機能がこなれていなかったり、単一メーカーによるサポートが望めないケースも多く、商用利用にはハードルが高いはず。
そういった品質・サポート面の課題をどの様に乗り越え商用に導入されました？



ナレッジでつなく、未来をつくる
Unite Knowledge, Ignite the Future.