

DC134

Deep Dive into "VMware Cloud on AWS" '18

ヴィエムウェア株式会社
ストラテジックアライアンス本部
スタッフテクニカルアライアンスマネージャ 大久 光崇

#vforumjp

vmware®

POSSIBLE
BEGINS
WITH YOU

免責事項

- このセッションには、現在開発中の製品/サービスの機能が含まれている場合があります。
- 新しいテクノロジーに関するこのセッションおよび概要は、VMware が市販の製品/サービスにこれらの機能を搭載することを約束するものではありません。
- 機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述してはなりません。
- 技術的な問題および市場の需要により、最終的に出荷される製品/サービスでは機能が変わる場合があります。
- ここで検討されているまたは提示されている新しいテクノロジーまたは機能の価格およびパッケージは、決定されたものではありません。

Agenda

はじめに

Elastic vSAN

ストレッチ クラスタ

POC からの教訓

おわりに

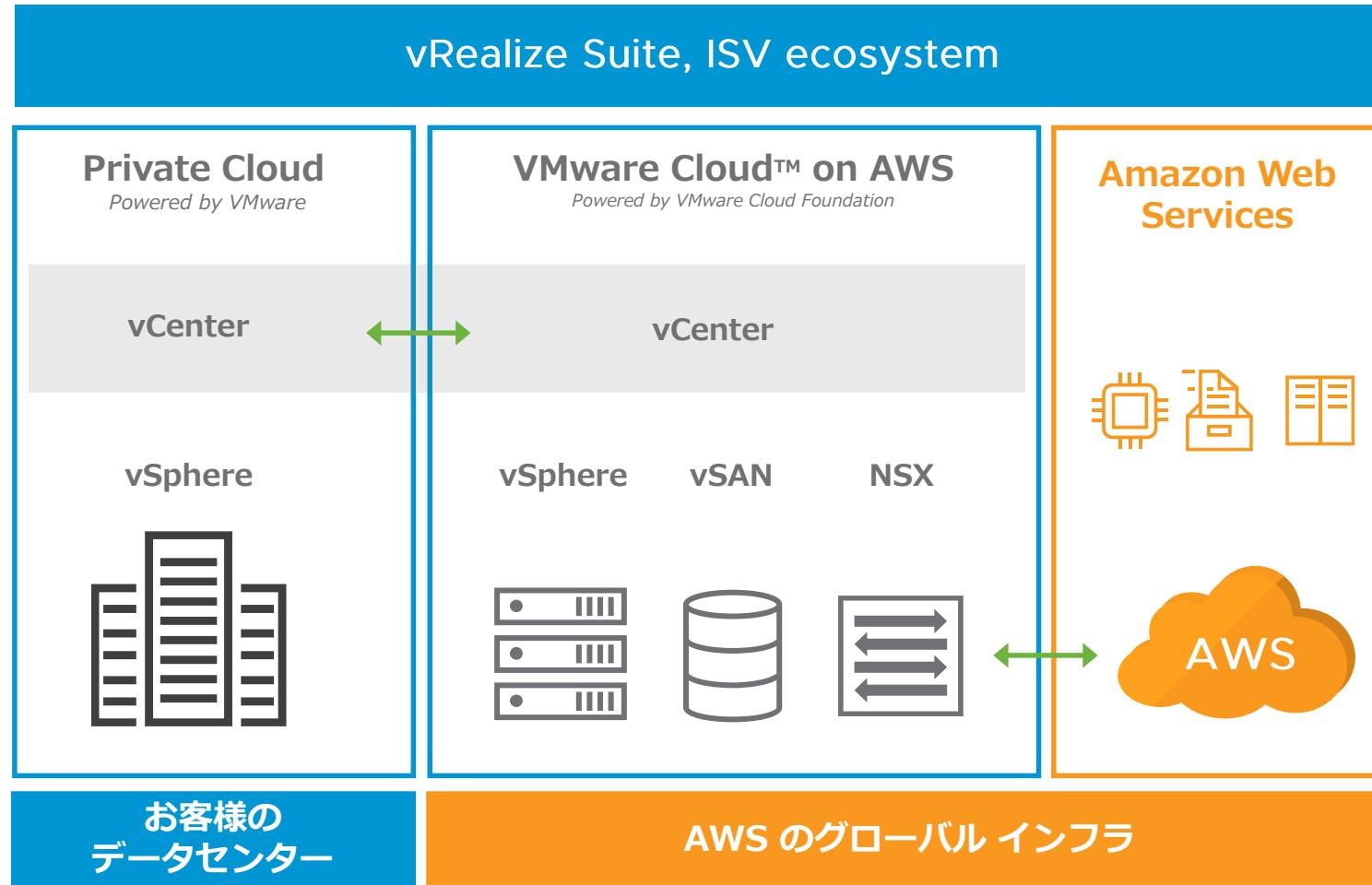


はじめに

Special Hardware and Software World
in the VMware Cloud™ on AWS

VMware Cloud on AWS 概要

世界で最もパワフルなクラウド テクノロジーの共演

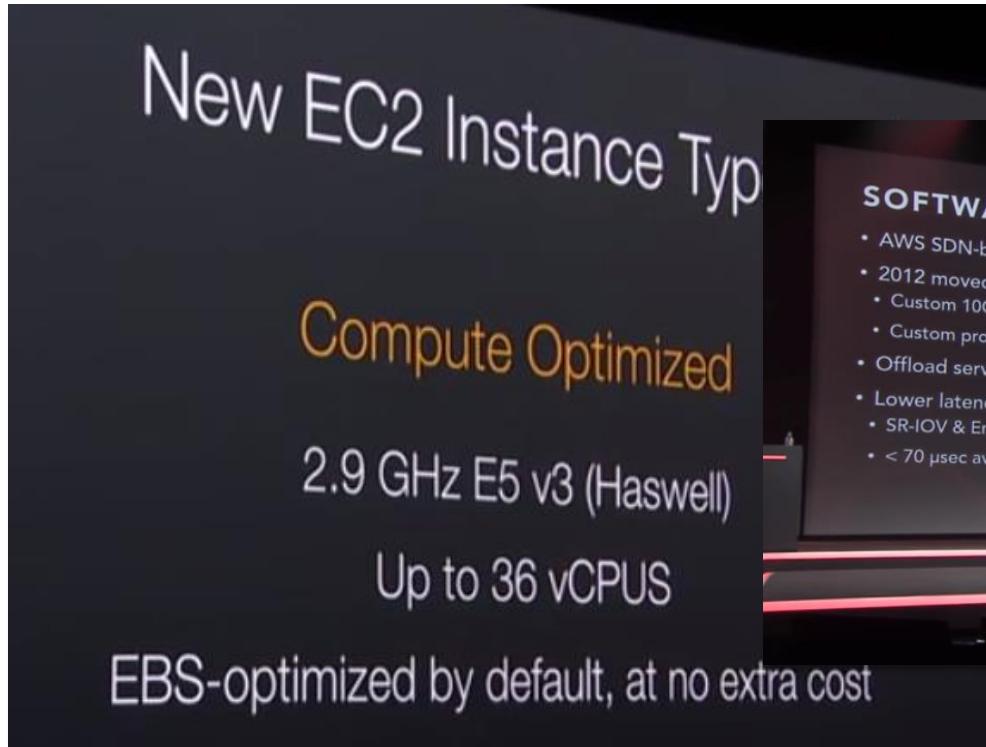


ハイライト

- AWS ベアメタル上で実行される VMware SDDC
- VMware が販売、運用、サポートを提供
- コンテナと仮想マシンのサポート
- オンデマンドのキャパシティと柔軟な利用
- オンプレミスの SDDC との完全な運用の一貫性
- ワークロードのシームレスな移行
- AWS のネイティブ サービスへの直接アクセス
- AWS のグローバルなフットプリントを基盤とした可用性の高いサービスの利用
- パートナーエコシステムとの連携

サーバーはコモディティ? クラウドでしか手に入らないパーツも登場

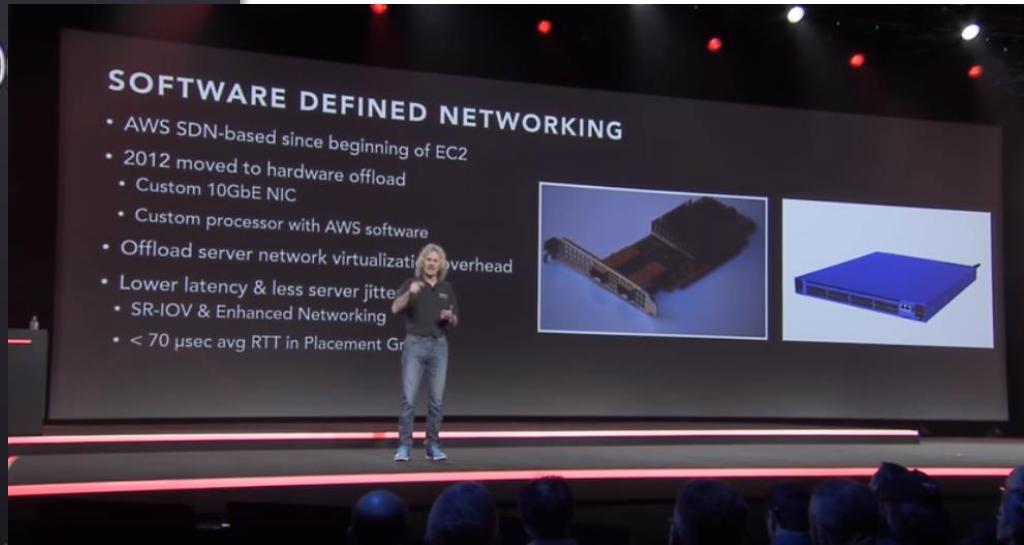
AWS 専用 Intel プロセッサ



AWS re:Invent 2014

AWS re:Invent 2014 | Day 2 Keynote with Werner Vogels
<https://youtu.be/ZPbM2qGfH3s?t=4895>

Elastic Network Adapter
(AWS's own ASIC)



AWS re:Invent 2016

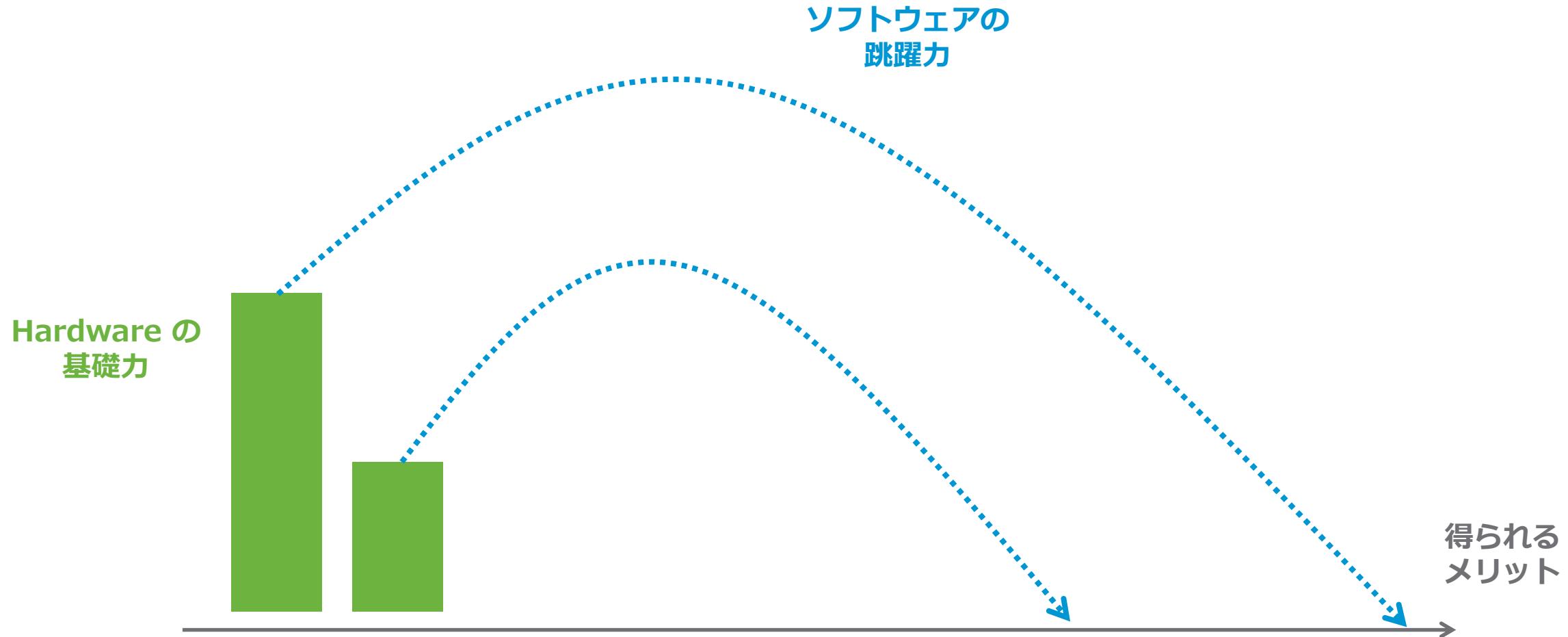
AWS re:Invent 2016: Tuesday Night Live with James Hamilton
<https://youtu.be/AyOAjFNPAbA?t=1824>



AWS re:Invent 2018

Software x Hardware

And Operational Excellence



AWS 用語

基本を抑える

用語	概要
リージョン	地理的に離れた領域
アベイラビリティ ゾーン	リージョン内に複数ある独立したロケーション
Amazon EC2	仮想マシン インスタンス、物理マシン インスタンスとしてコンピューティング性能を提供
Amazon VPC	論理的に切り離された仮想ネットワーク
AWS Direct Connect	AWS とお客様設備の間を専用線でプライベート接続
Amazon S3	安価かつ高い耐久性を持つオンラインストレージサービス
Amazon EBS	EC2 と組み合わせる永続的なブロックストレージボリューム
AWS Storage Gateway	標準的なストレージプロトコルから AWS のストレージサービスにアクセス

VMware 用語

もう基本なんですからっ

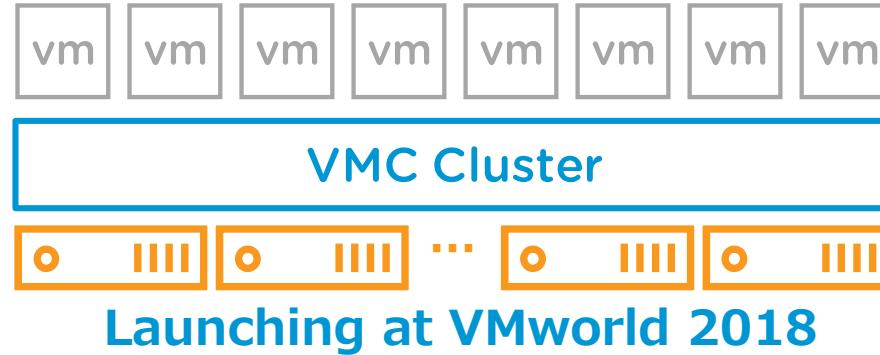
用語	概要
VMware vCenter®	仮想環境の統合管理サーバー
VMware ESXi™	安心・安全・高性能の鉄板ハイパーバイザによるサーバ仮想化
VMware vSAN™	カーネルにビルトインされたストレージ仮想化
VMware NSX®	迅速にネットワーク機能を提供するネットワーク仮想化



Elastic vSAN

Decoupled Compute and Storage Scaling

VMware Cloud on AWS のストレージ オプション



一貫した管理と運用を
各ストレージ オプションで提供



ローカル NVMe
with vSAN
(現在利用可能)

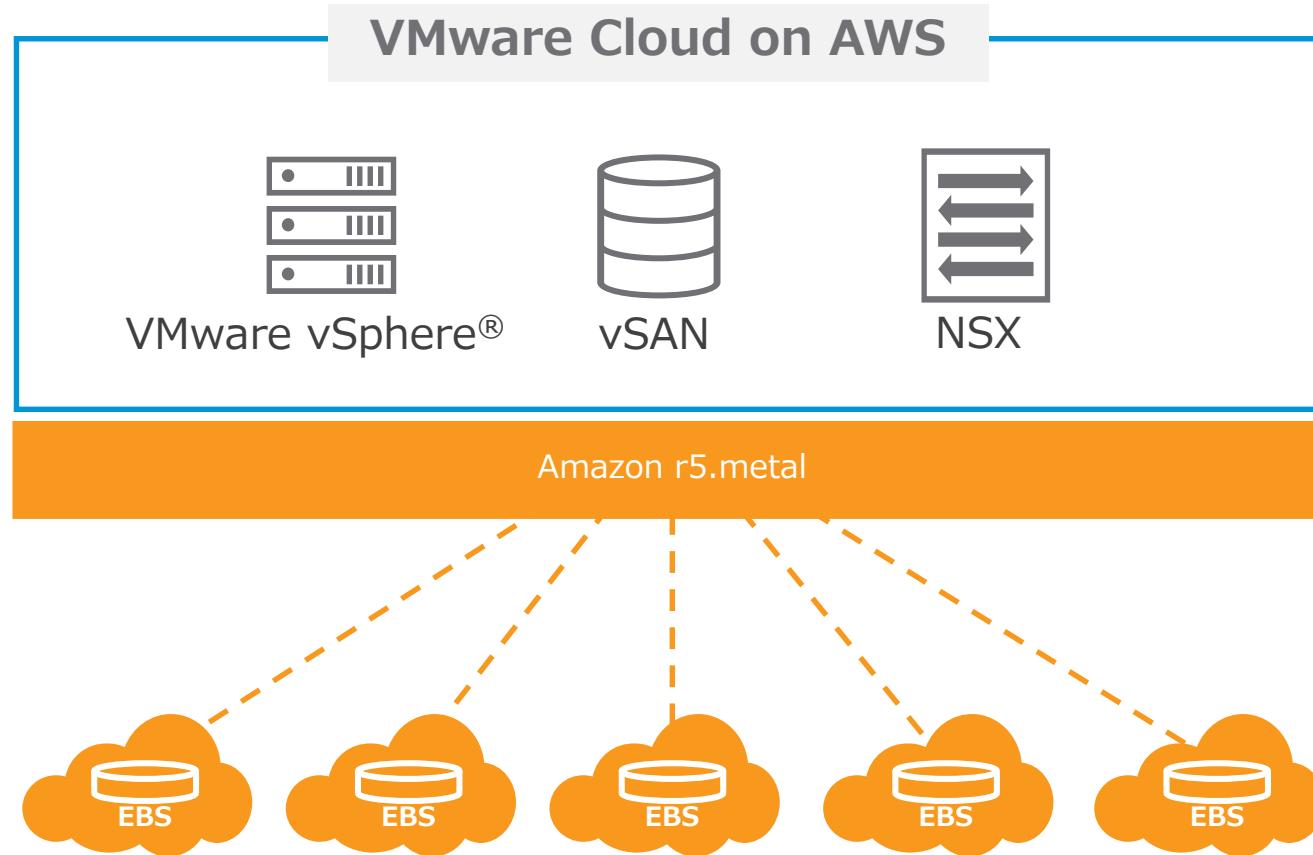


VMC にて制御された
外部ストレージ
(将来の機能)

幅広い価格/性能を提供するため様々なストレージ オプションを提供

高密度ストレージのワークロードに対応 新しい Amazon EC2 ベアメタル インスタンス

Developing



概要

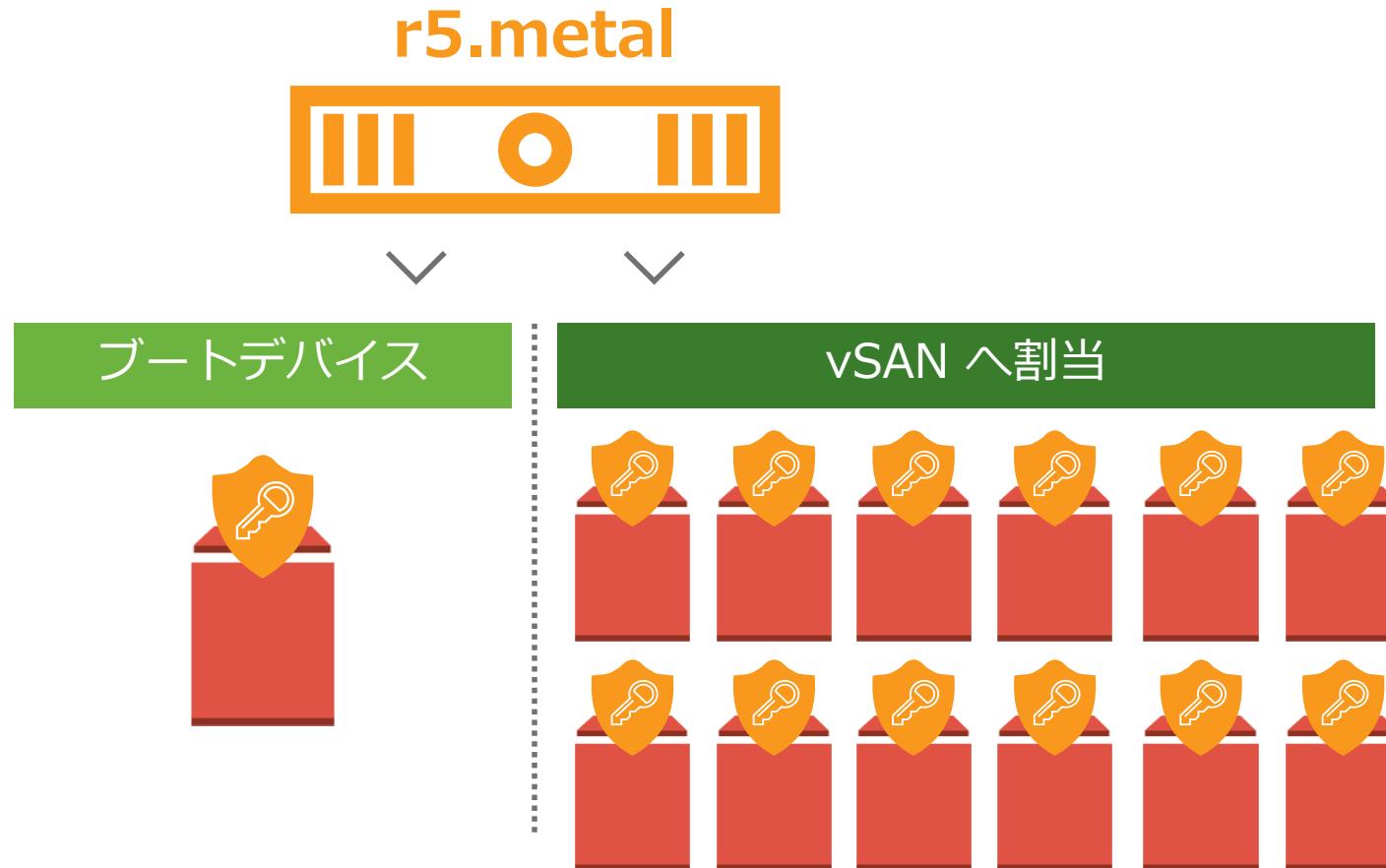
新しいディスクレスの
ホストインスタンス **r5.metal**

**Amazon Elastic Block
Storage (EBS)** を用いた
VMware vSAN

ストレージのスケーリングを可能にする新しいホスト

r5.metal の物理ホストの構成

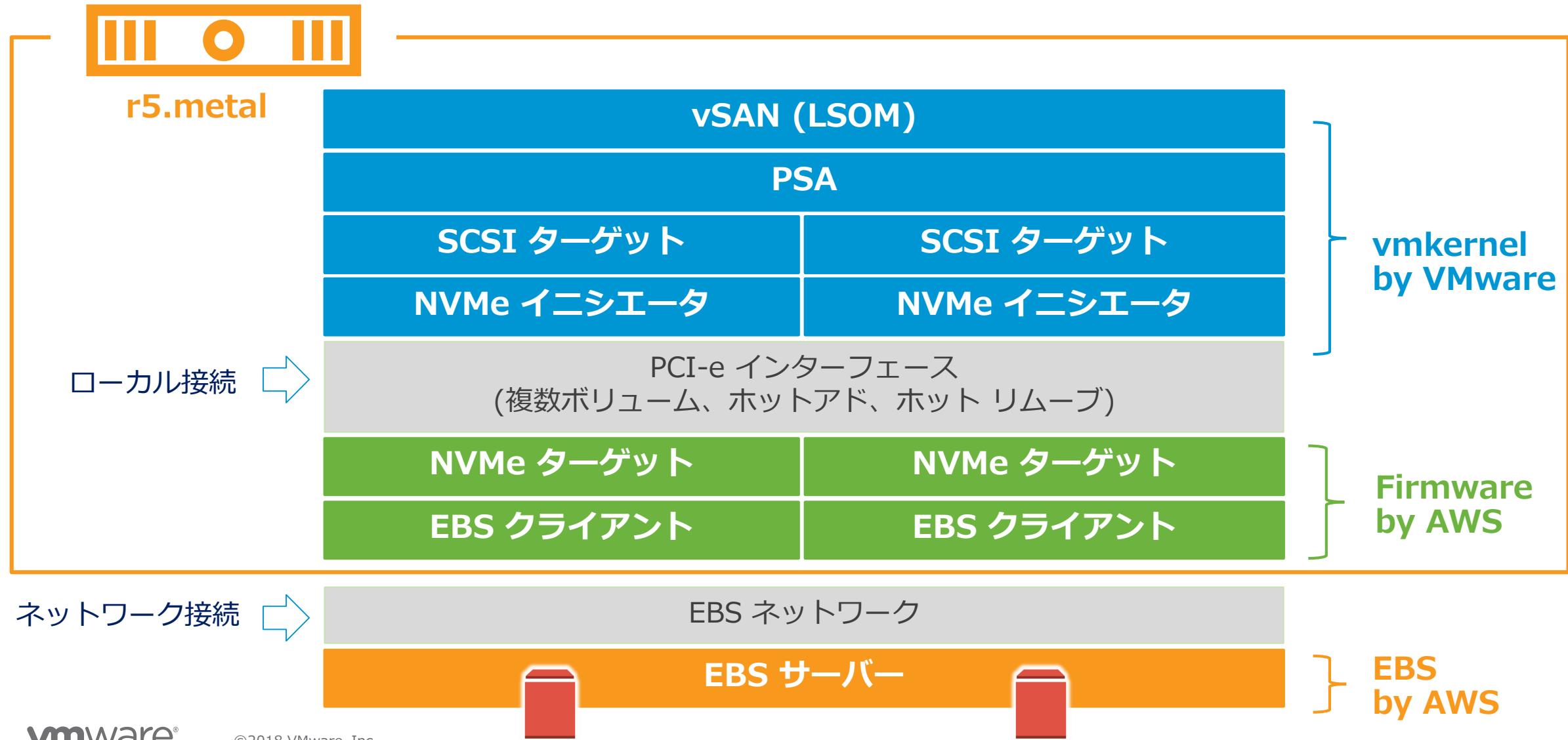
Developing



Item	Available
CPU	Skylake-SP
ソケット数/ホスト	2
コア数/ソケット	24
コア数/ホスト	48
メモリー	768 GB
ストレージ	EBS GP2 (汎用 SSD) -ディスク数可変-
NICs	1 x ENA

ストレージ アーキテクチャ

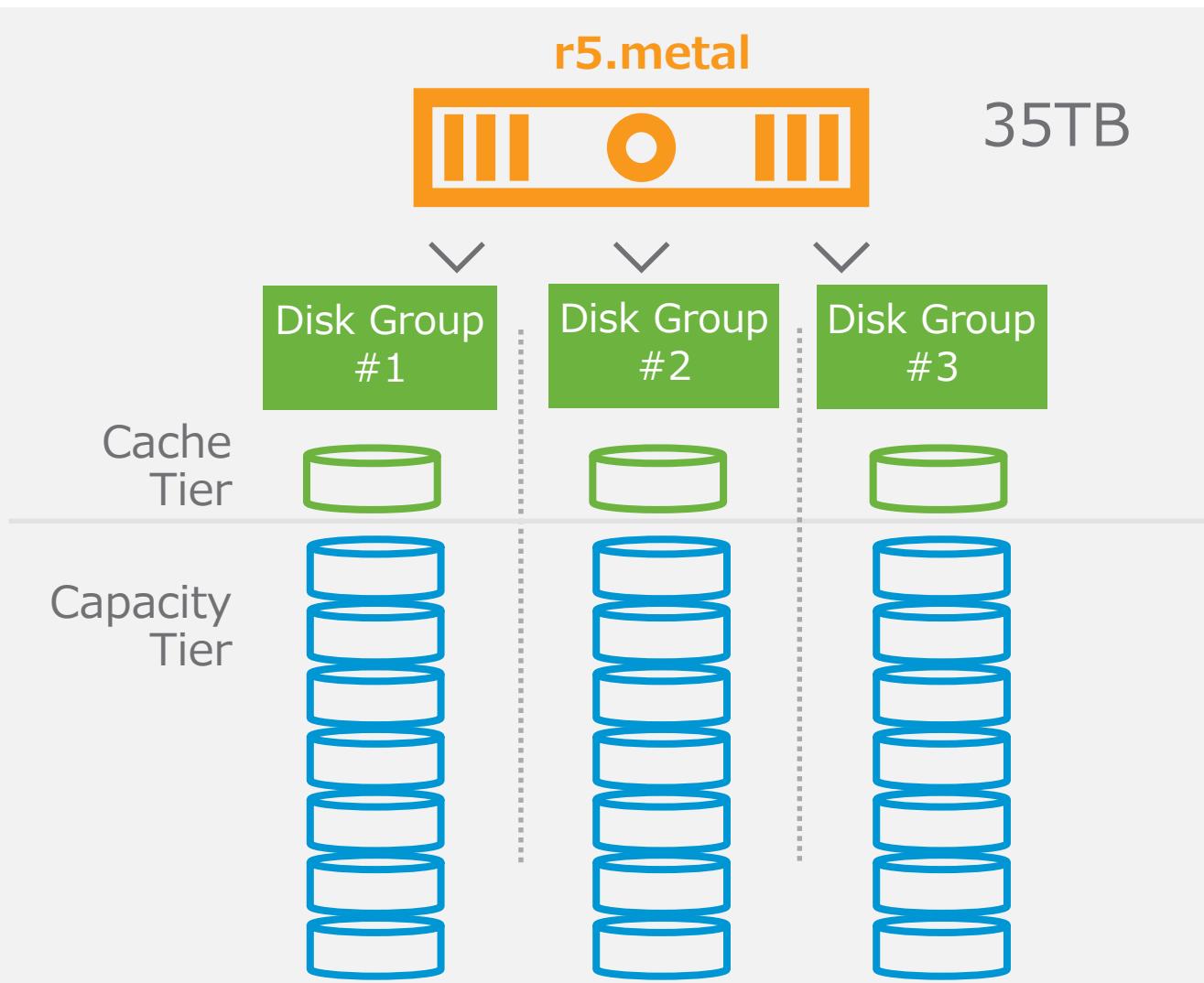
Developing



ホストのキャパシティを構成可能に

Elastic Cloud Storage

Developing



3 ディスク グループ / ホスト

3-7 キャパシティ ディスク / ディスクグループ

ホストあたり **15-35 TB** のキャパシティ

- ホストあたり約 10 TB のキャッシュ

vSAN ディスク タイプ	EBS ボリューム タイプ	ボリューム キャパシティ (GiB)	ベースライン/ バースト IOPS
キャッシュ	gp2	3,334	10,000
キャパシティ	gp2	1,667	5,001

ディスク
グループ
デフォルト
オブジェクト
ポリシー

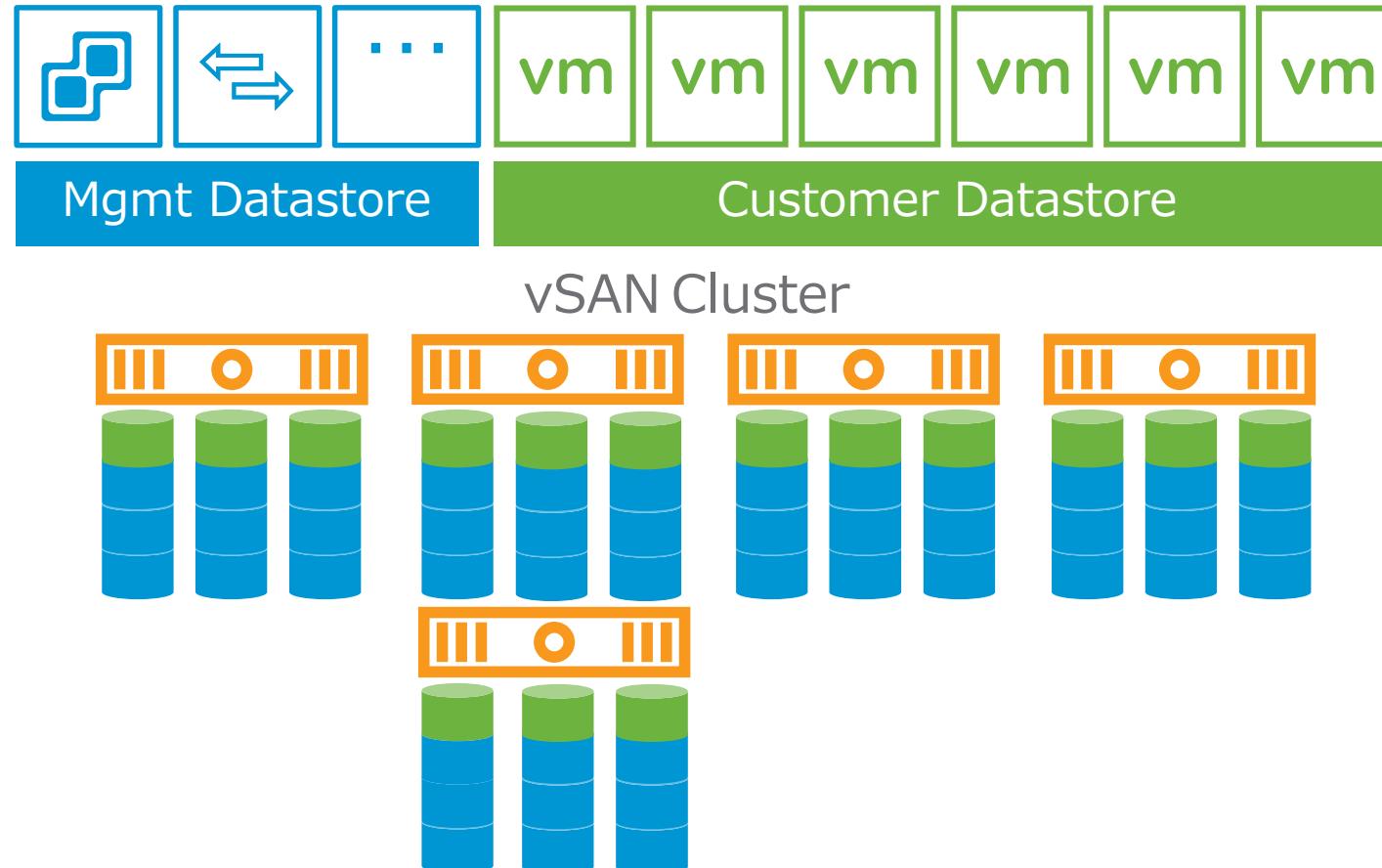
圧縮のみ
(重複排除なし)

RAID-5
FTT-1
Checksum
No Reservation
No Force Provisioning

問題/障害のあるホストの自動的なリプレイス

ホスト障害時の修復

Developing

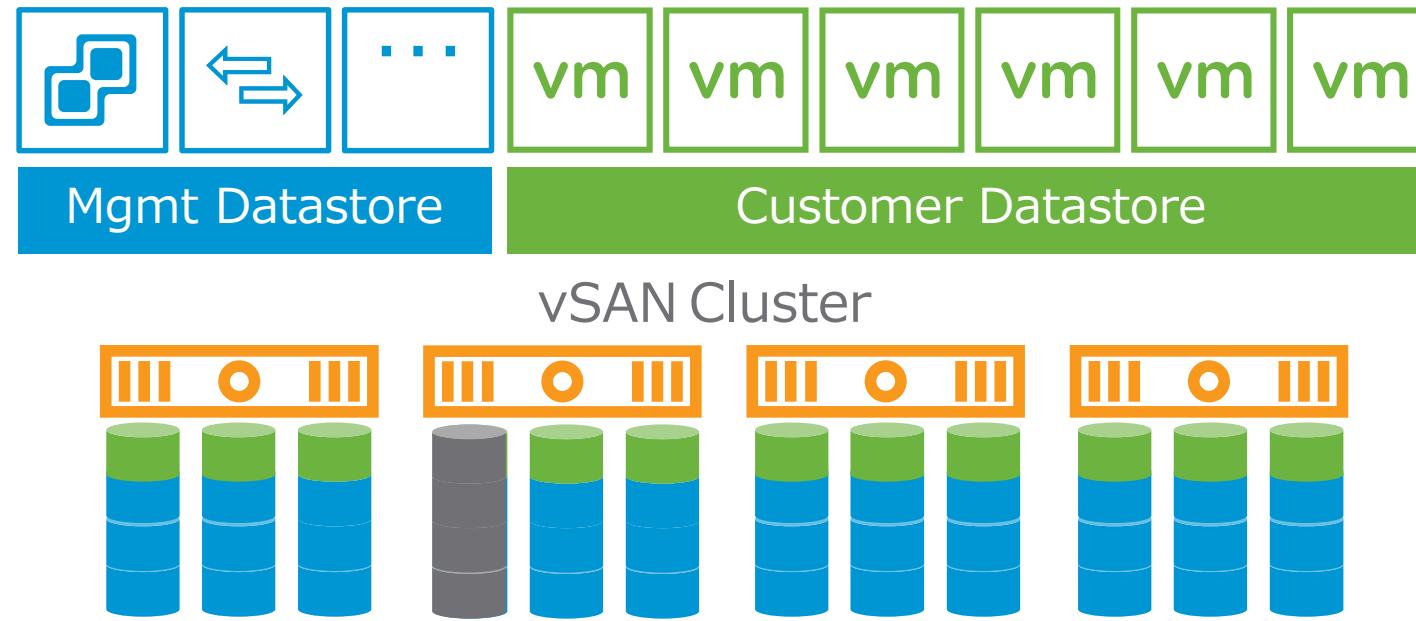


1. 問題発見
2. ホストの追加
3. ディスクグループの移動
4. 問題のあるホストの削除

障害のあるディスクグループの自動的なリプレイス

ディスク障害の修復

Developing



1. 問題の発見
2. ディスクグループの削除
3. 新しいディスクグループの作成
4. データのリビルド/リシンク

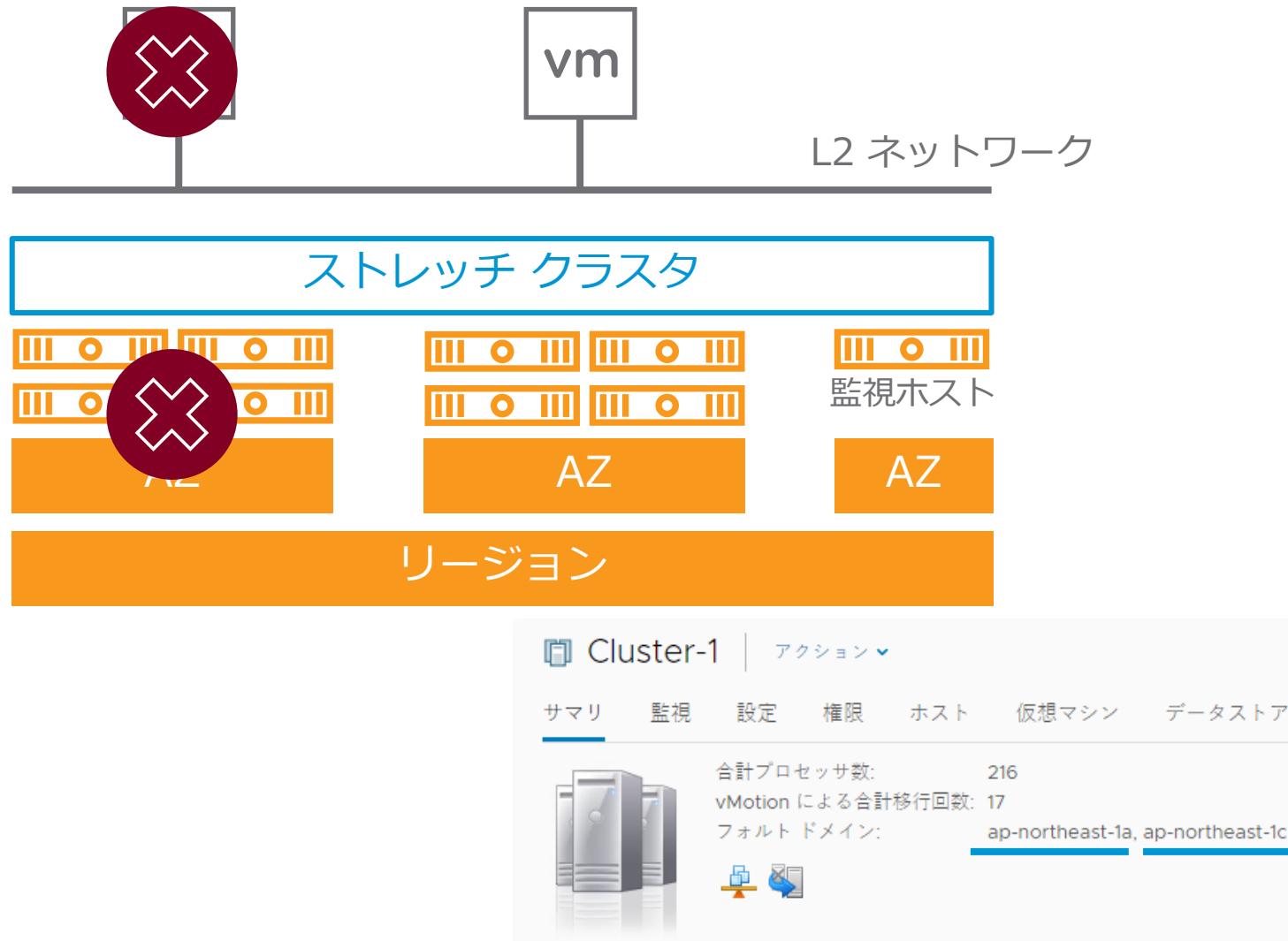


ストレッチ クラスタ

Multi AZ Availability

AWS アベイラビリティ ゾーン レベルの可用性

vSAN ストレッチ クラスタ



ゴール

データの回復性をより高めるために
vSAN ストレッチ クラスタを提供

ネストされたフォルト ドメイン
例) AZ 間の RAID-1, AZ 内での RAID-5

vSAN 監視ホストのライフサイクル管理

モチベーション

お客様と管理のワークロードに耐 AZ 故障の
回復性を提供するため

ストレッチ クラスタの構成

Easy to deploy

AWS リージョン Asia Pacific (Tokyo) 追加のリージョンが提供される予定です

デプロイ 単一ホスト 複数のホスト ストレッチ クラスタ [i](#)

SDDC 名 Multi-AZ-SDDC

ホスト数 6

ホスト キャパシティ 2 Sockets, 36 Cores, 512 GB RAM, 10.7 TB Storage

合計キャパシティ 12 Sockets, 216 Cores, 3 TB RAM, 64.2 TB Storage

1 クリック デプロイ

プロパティ としての
ストレッチ クラスタ

デプロイ時に決定

デプロイ後は通常クラスタへの
変更不可

最小 6 ホスト

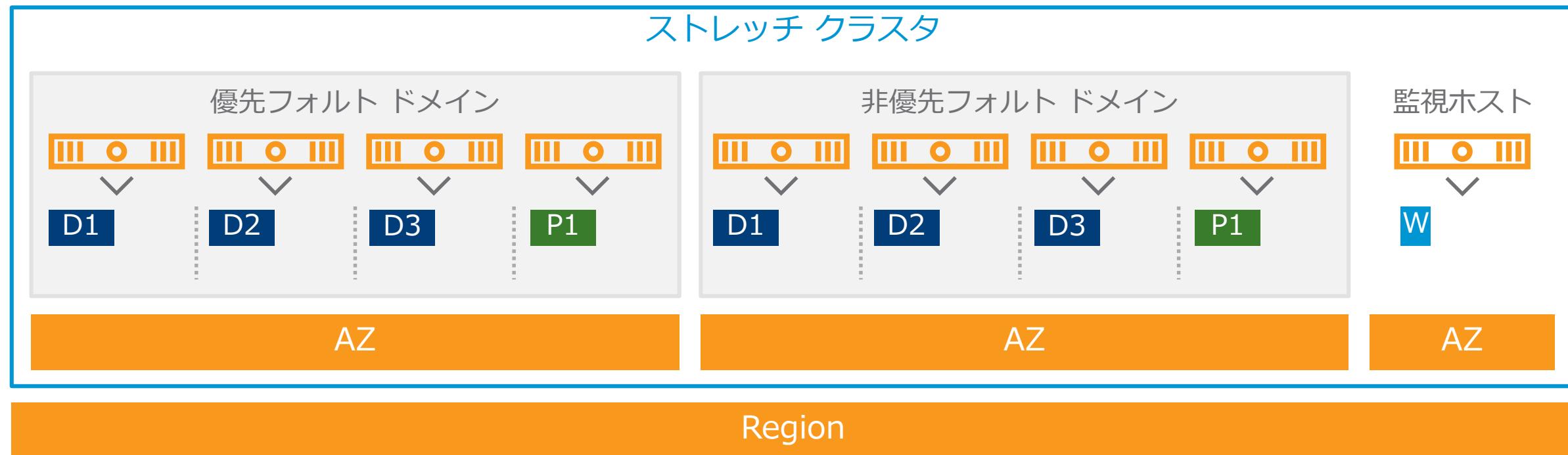
最大 16 ホスト

耐 AZ 障害の可用性を提供 仮想マシンストレージポリシー (SPBM)

SPBM: Storage Policy Based Management

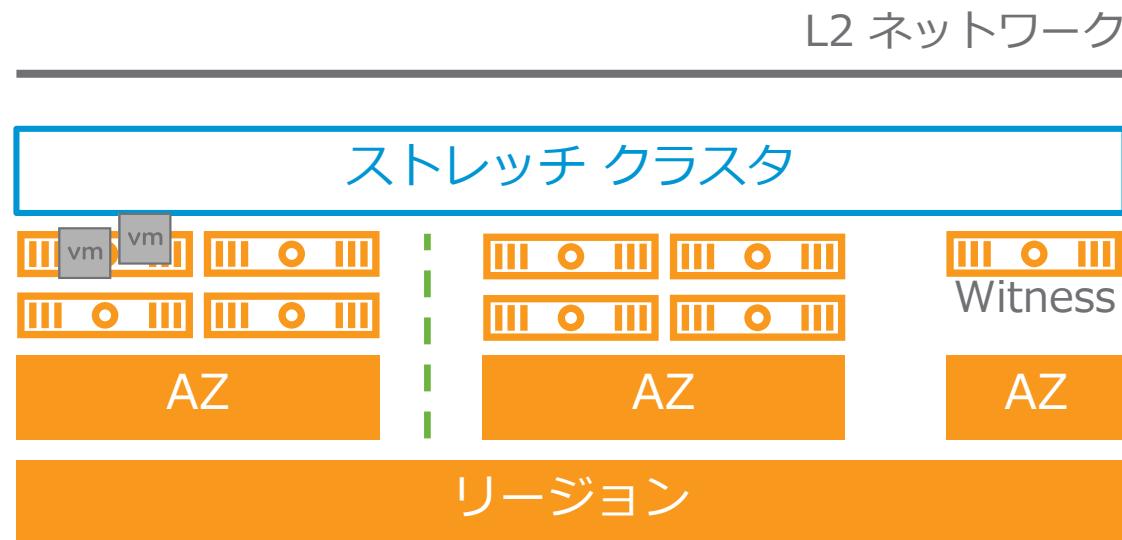


ストレッチ クラスタ



ワークロードの AZ アフィニティ

AZ を見切った DRS



AZ 内での DRS

HA は以前と同様にサポート

プロビジョニング時の意図を維持

AZ 越えの意図しない移動を回避

ストレッチ クラスタの注意点

- **デプロイ時のみ**構成可能:
 - シングル AZ からの**アップグレード**、シングル AZ への**ダウングレードは不可**
- 1 クラスタのみ (複数クラスタ対応は将来の予定)
- **AZ 間のネットワーク転送料金**が掛かる
- SDDC から出るネットワークは**片方の AZ** のみ
 - トロンボーン的な通信となる可能性あり
- ユーザーは 2 つの AZ を選択。
VMware がウィットネス ノードを 3 つめの AZ に配置

POC からの教訓

Lessons Learnt

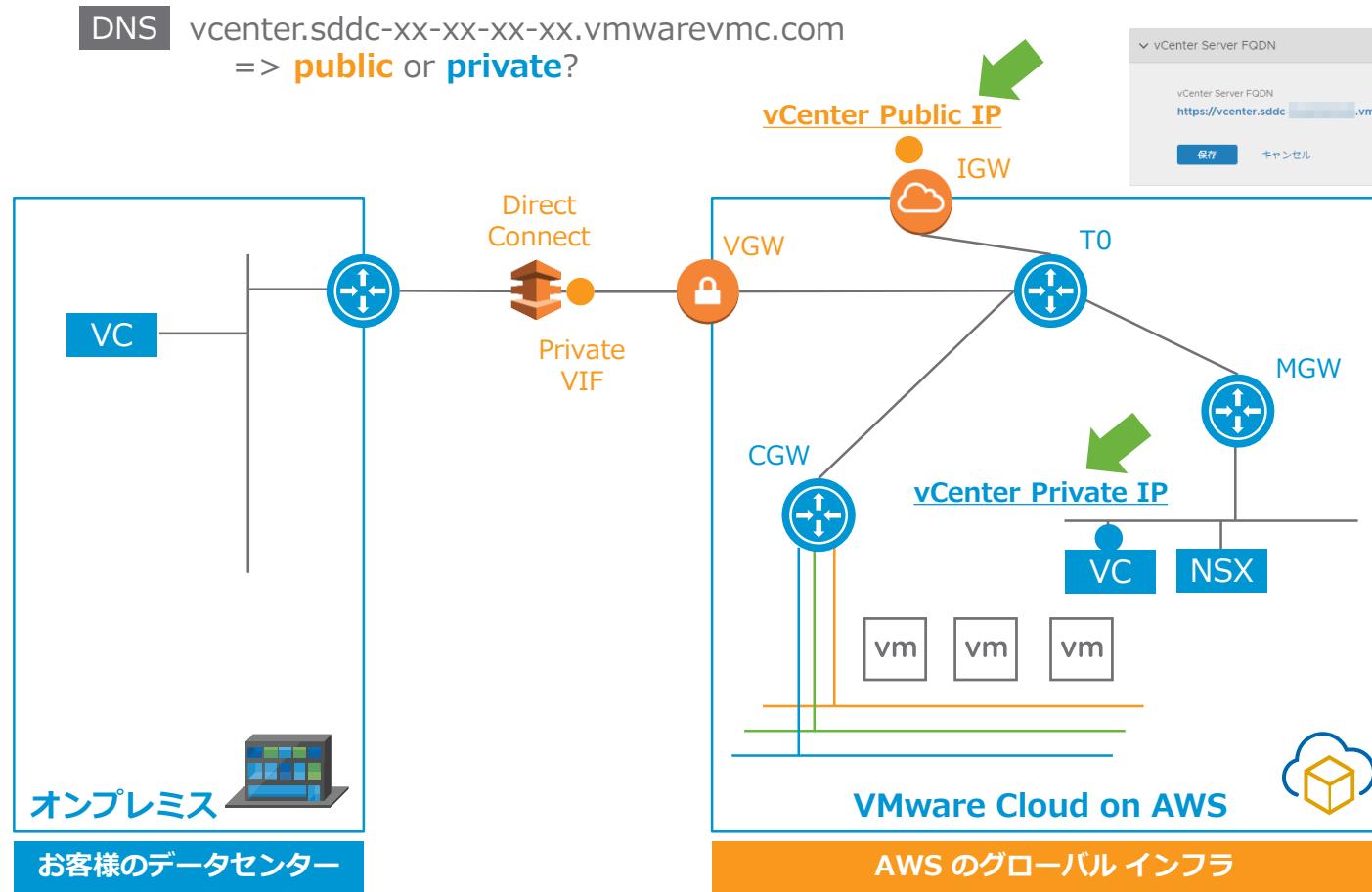
POC からの教訓

NSX-T SDDC における名前解決

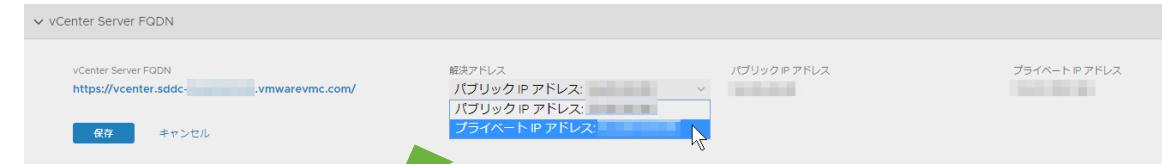
vCenter Server の名前解決

Public IP or Private IP ?

vCenter の Public IP から Private IP へは
NAT が設定済み (UI 上の表示なし)



vcenter.sddc-xx-xx-xx-xx.vmwarevmc.com の名前解決を
Public IP と **Private IP** のどちらにするか選択可能



Public DNS のエントリを変更

T0: Tier-0 Router

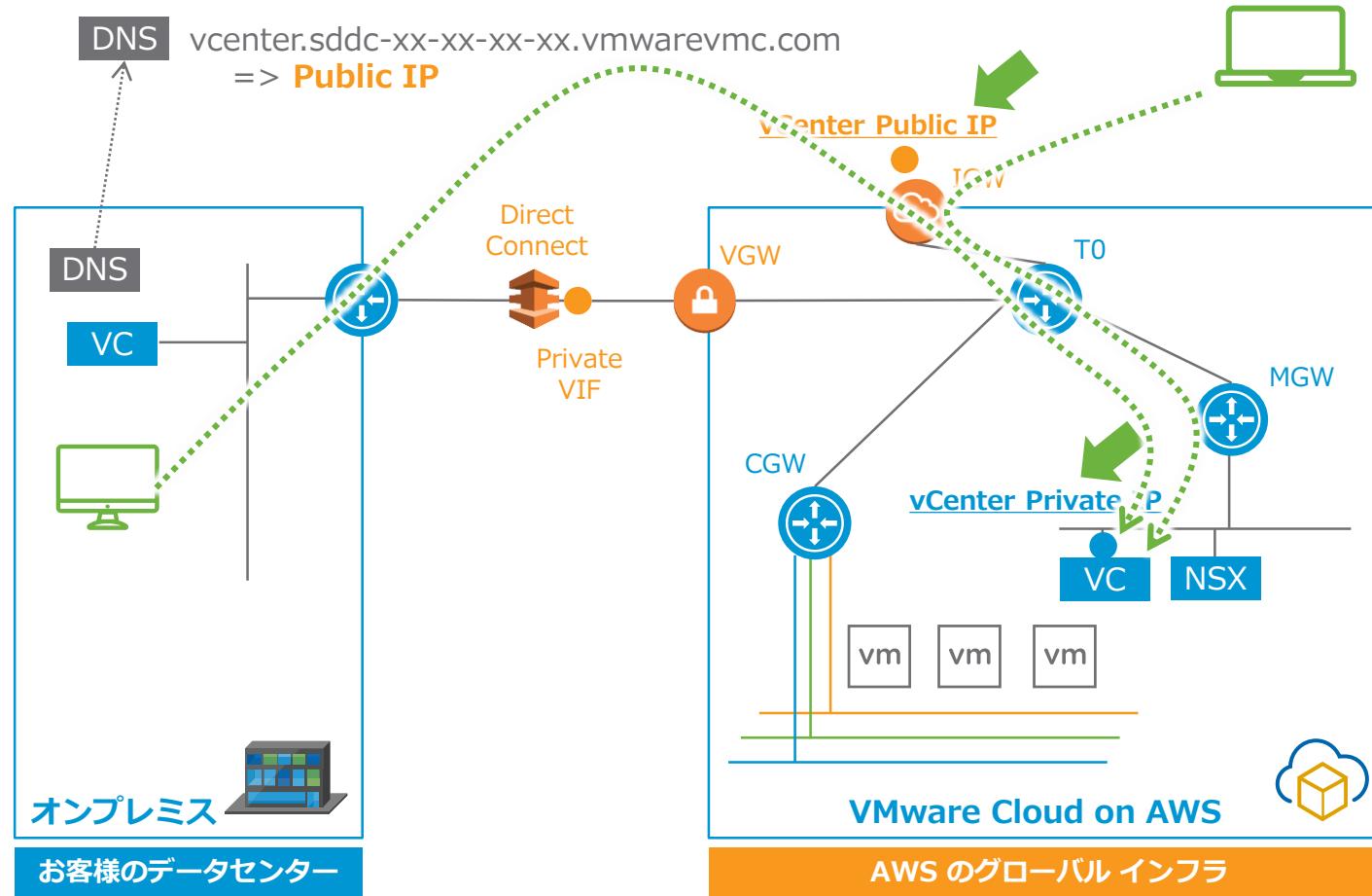
MGW: Management Gateway

CGW: Compute Gateway

VMC vCenter Server の名前解決

Public IP とする場合

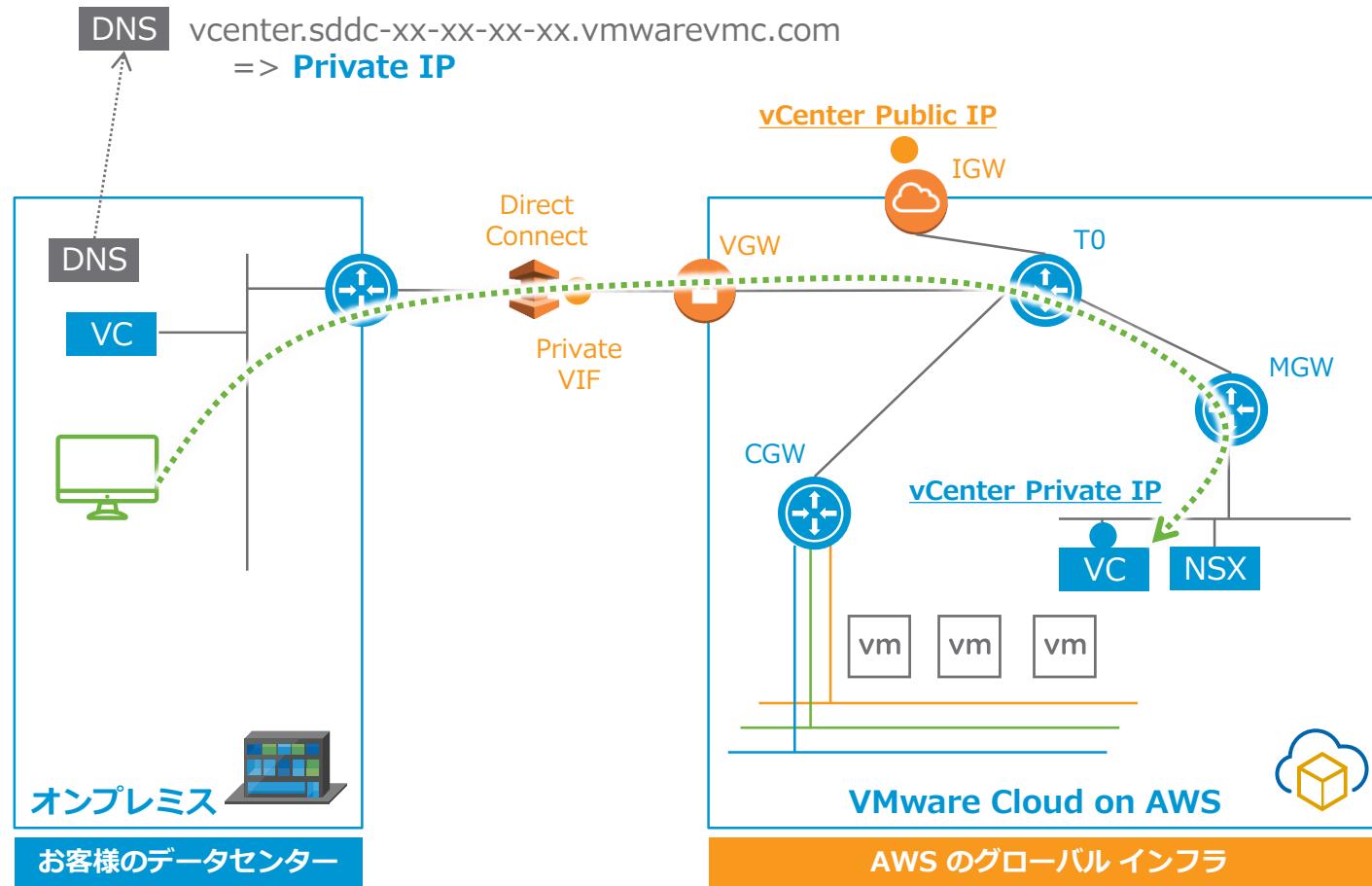
vCenter へ Internet 経由でアクセスする場合



VMC vCenter Server の名前解決

Public IP とする場合

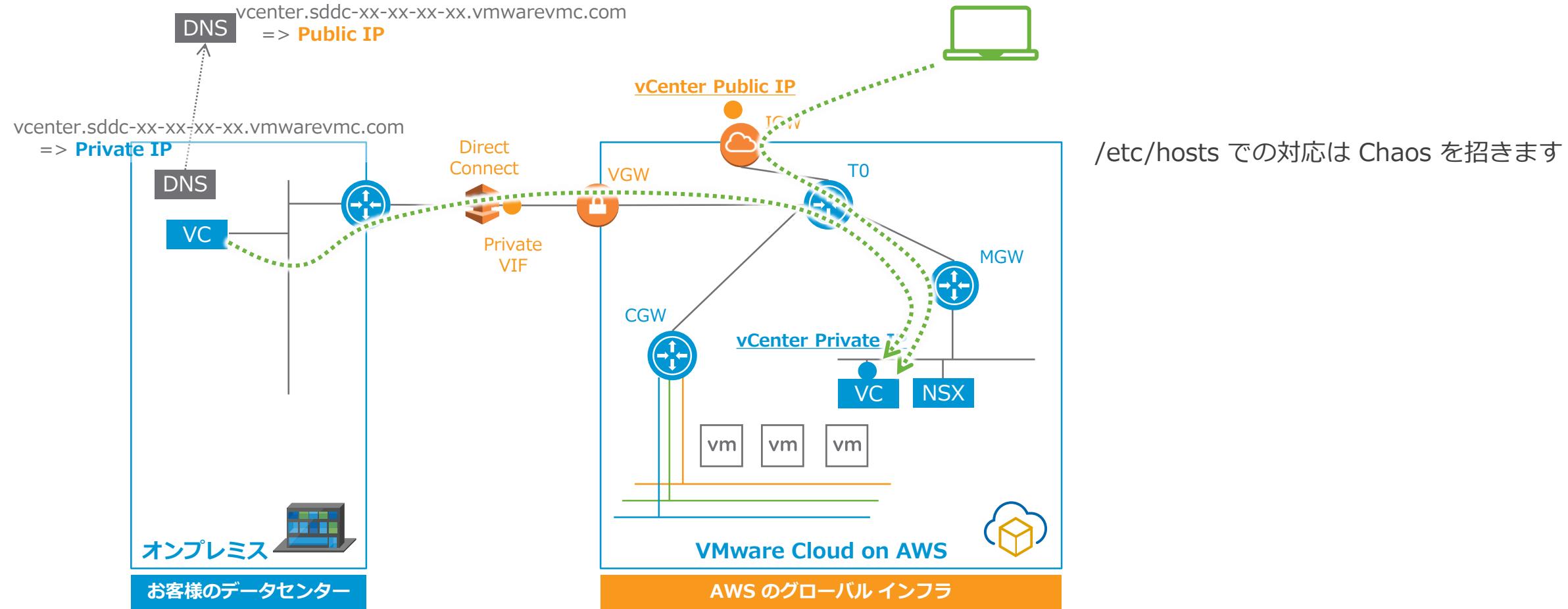
vCenter へ Direct Connect/VPN 経由でアクセスする場合



VMC vCenter Server の名前解決

Public IP と Private IP どちらも必要とする場合

Client PC からは Internet 経由、
Hybrid Linked Mode, Site Recovery, HCX の構成で Direct Connect/VPN を利用する場合



VMC SDDC における名前解決

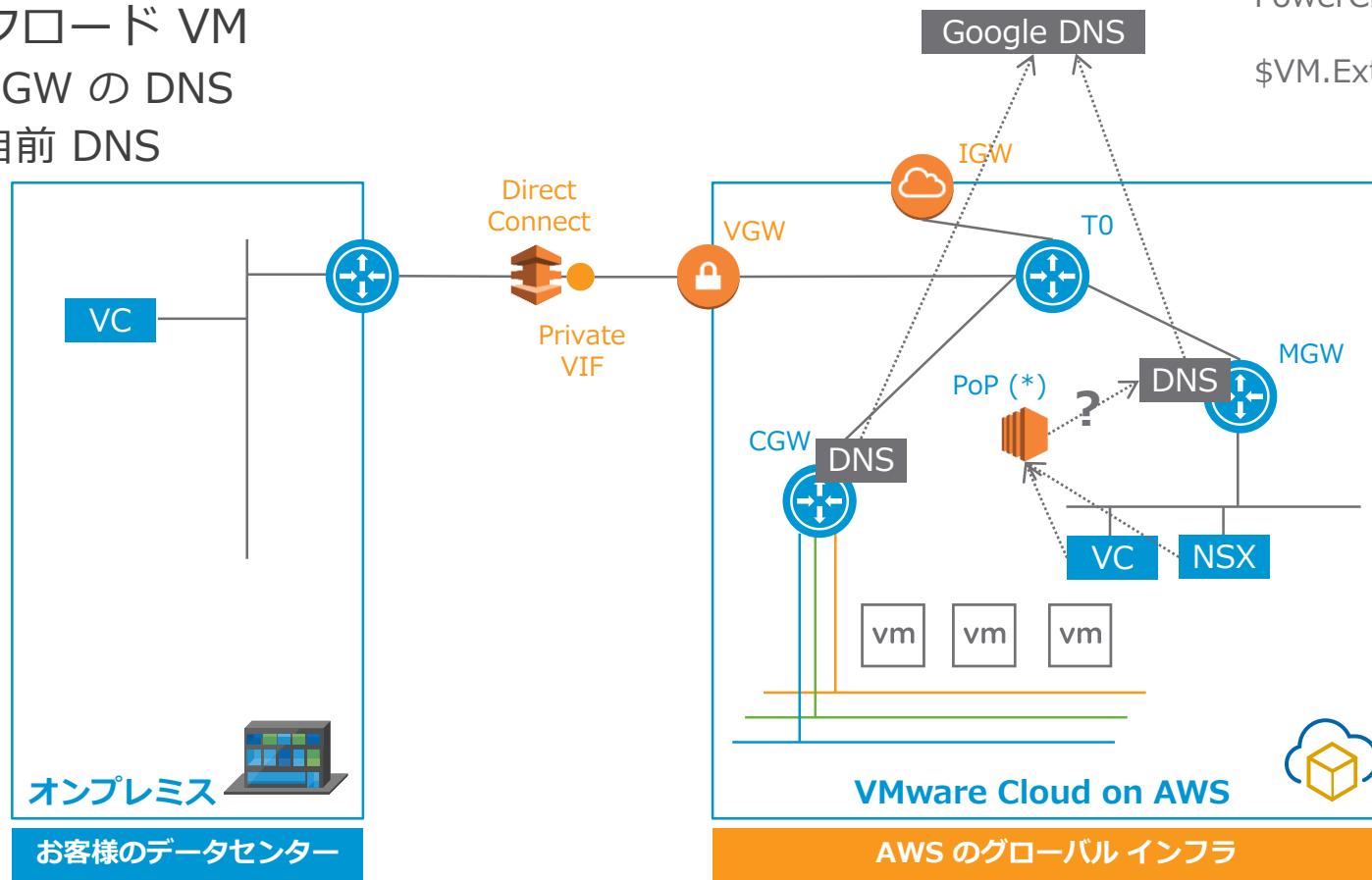
初期値は Google DNS へのフォワード

管理コンポーネント

- クッショングを経て MGW を DNS として利用

ワークロード VM

- CGW の DNS
- 自前 DNS



vCenter の DNS の設定値は以下の値を
PowerCLI や Managed Object Browser で確認可能

\$VM.ExtensionData.guest.ipStack[0].dnsConfig.ipAddress[0]

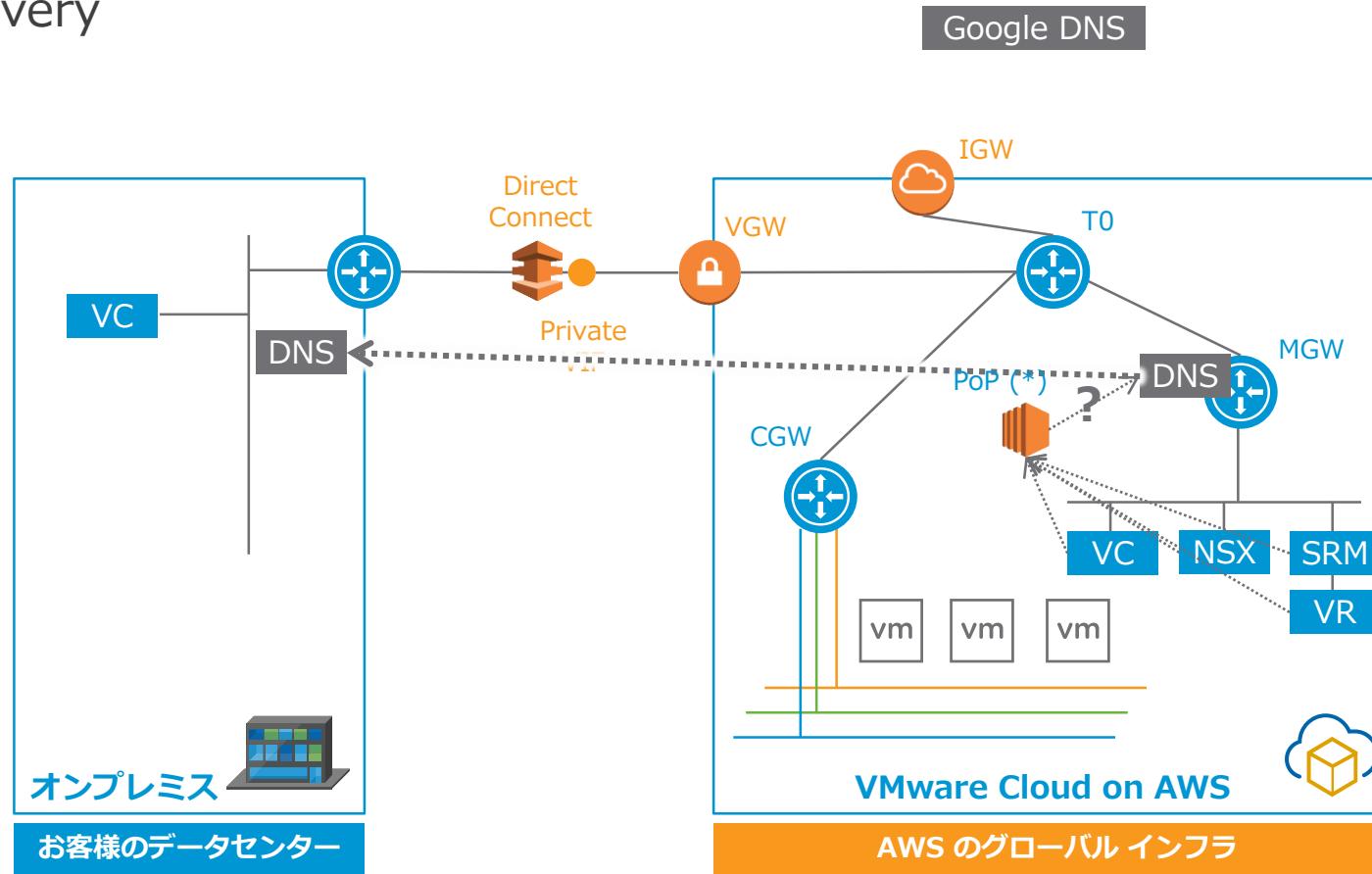
(*) PoP: Point of Presence

VMC SDDC における名前解決 - MGW 配下

オンプレミスの名前解決を可能に

オンプレミス側の名前解決が必要な場合は、MGW の DNS フォワード先をオンプレミスの DNS へ

- Hybrid Linked Mode
- Site Recovery

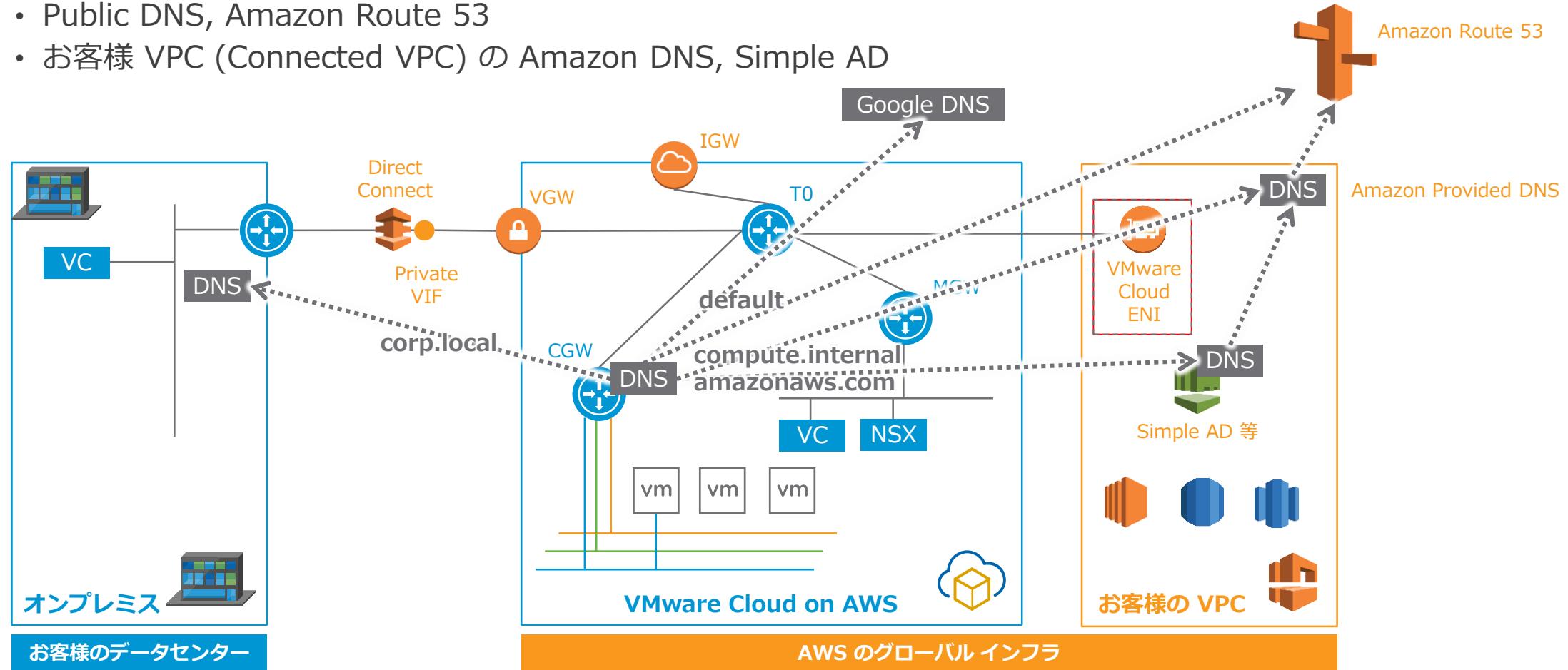


VMC SDDC における名前解決 – CGW 配下

ハイブリッド構成、セキュアな構成を視野に

CGW の DNS フォワーダーは FQDN 毎に設定可能 (5 つまで)

- ・オンプレミス DNS
- ・Public DNS, Amazon Route 53
- ・お客様 VPC (Connected VPC) の Amazon DNS, Simple AD



POC からの教訓

Amazon S3 連携

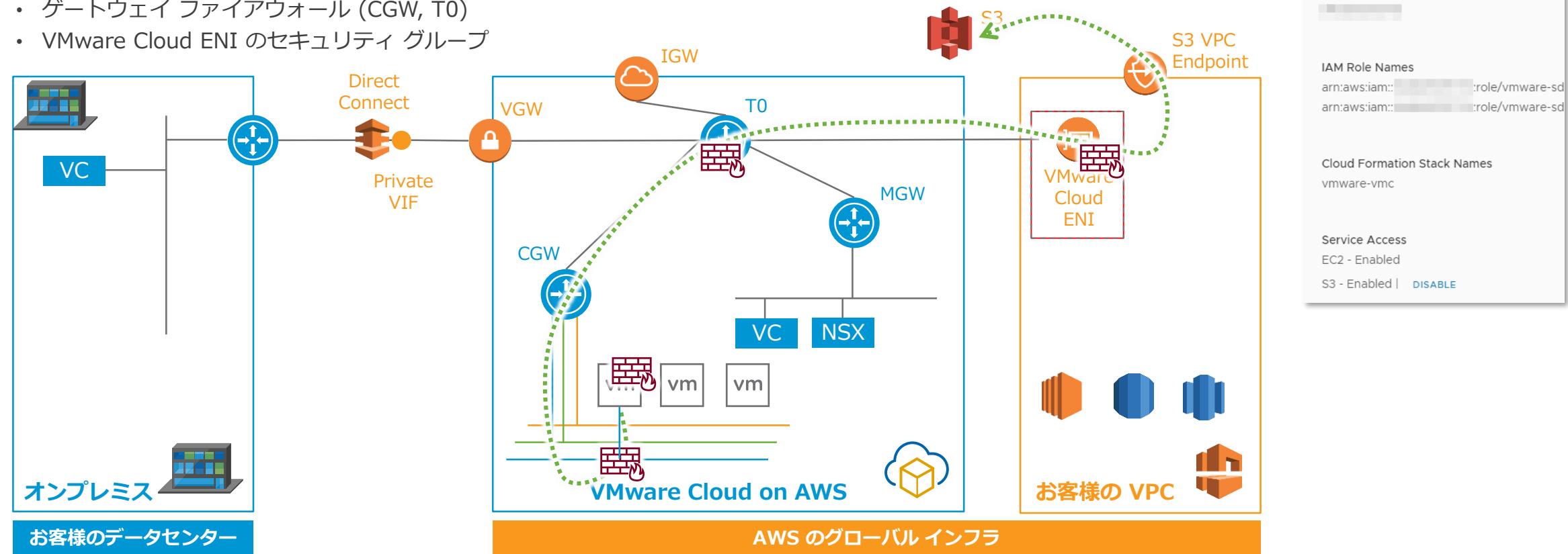
Amazon S3 の利用

コンピュート リソースからの S3 VPC エンドポイント 経由のアクセス

Networking & Security > Connected VPC > Service Access > S3 Enable (デフォルト)

各種 Firewall に注意

- Guest OS 内 (Windows Firewall, iptables/firewalld)
- 分散ファイアウォール
- ゲートウェイ ファイアウォール (CGW, T0)
- VMware Cloud ENI のセキュリティ グループ



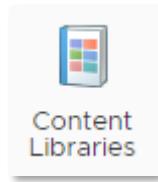
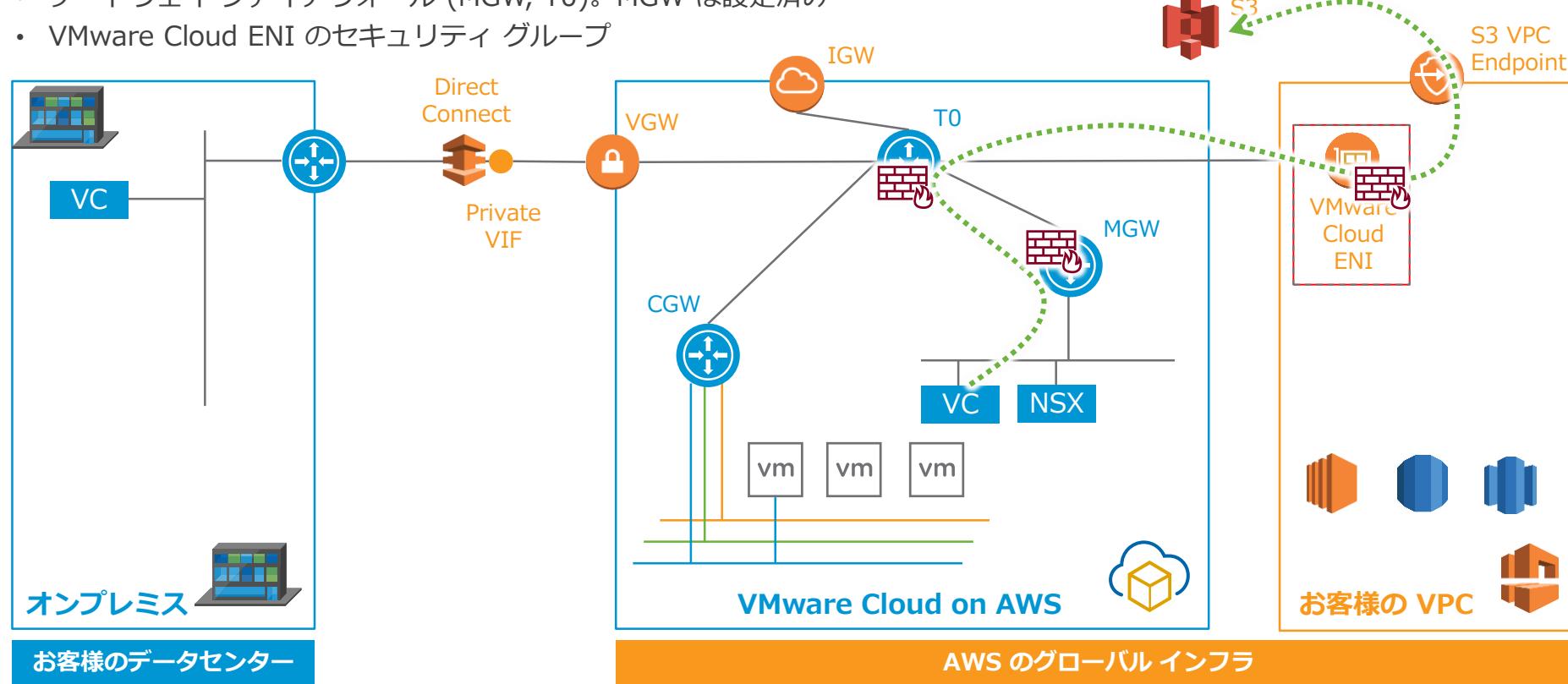
Amazon S3 の利用

管理リソースからの S3 VPC エンドポイント 経由のアクセス

Networking & Security > Connected VPC > Service Access > S3 Enable (デフォルト)

各種 Firewall に注意

- Guest OS 内 (Windows Firewall, iptables/firewalld)
- 分散ファイアウォール
- ゲートウェイ ファイアウォール (MGW, T0)。 MGW は設定済み
- VMware Cloud ENI のセキュリティ グループ



利用例:

S3 を購読先に設定した
コンテンツライブラリ

Connected Amazon VPC

AWS Account ID: [REDACTED]

IAM Role Names:
arn:aws:iam::[REDACTED]:role/vmware-sd
arn:aws:iam::[REDACTED]:role/vmware-sd

Cloud Formation Stack Names: vmware-vmc

Service Access:
EC2 - Enabled
S3 - Enabled | DISABLE

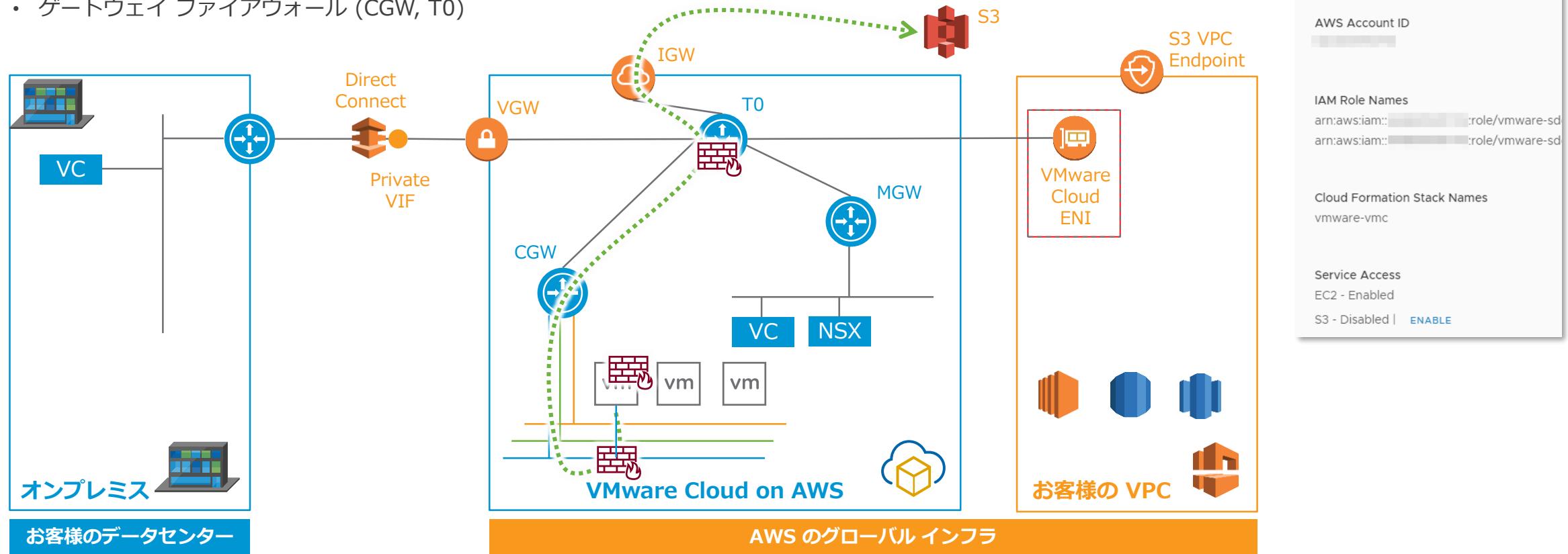
Amazon S3 の利用

インターネット経由のアクセス

Networking & Security > Connected VPC > Service Access > S3 Disable

各種 Firewall に注意

- Guest OS 内 (Windows Firewall, iptables/firewalld)
- 分散ファイアウォール
- ゲートウェイ ファイアウォール (CGW, T0)



その他の VPC のサービス, EC2, RDS, Redshift etc.

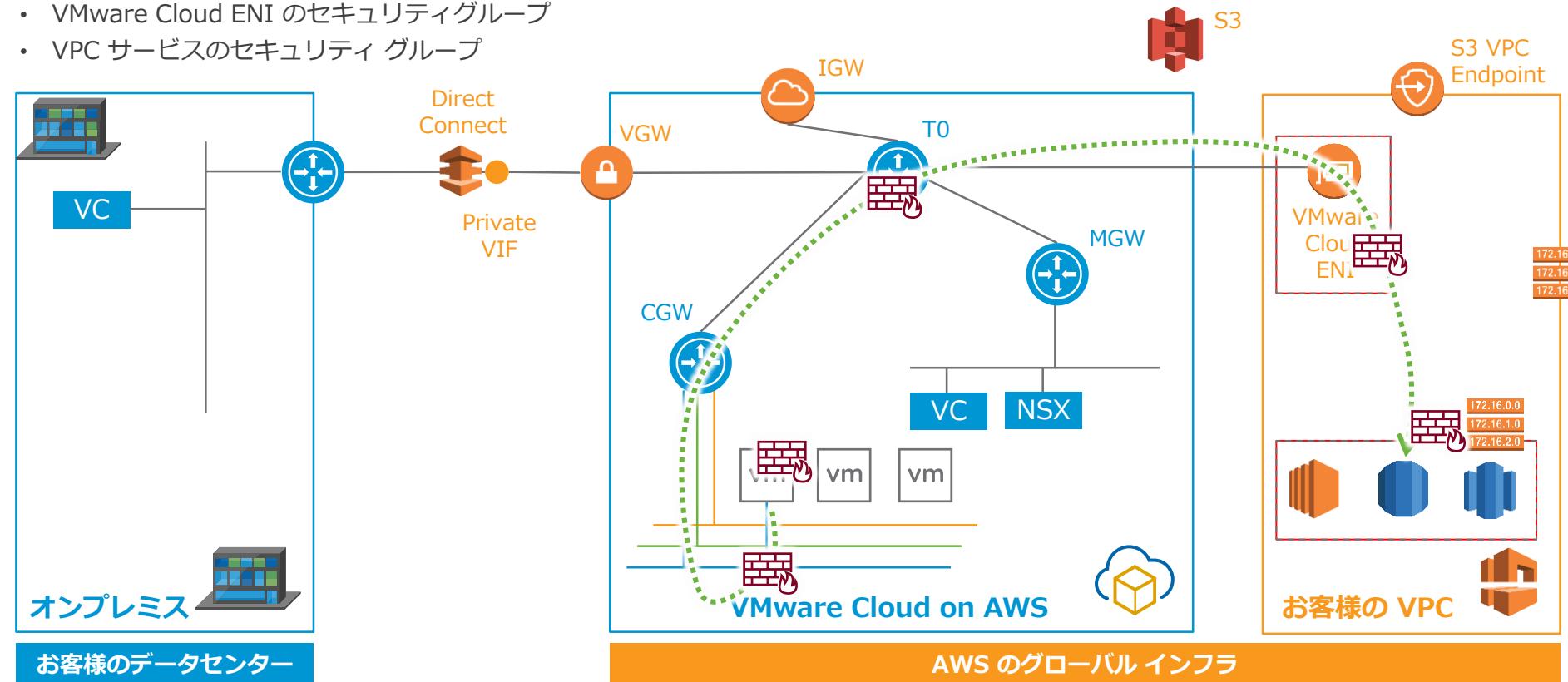
VPC 側のルート テーブルとセキュリティ グループに注意

ルート テーブル

- デフォルトのルート テーブルにはオーバーレイ ネットワークのルーティング情報が自動的に設定される
- デフォルト以外のルート テーブルを利用している際は、手動で適切に入力

セキュリティ グループ

- VMware Cloud ENI のセキュリティ グループ
- VPC サービスのセキュリティ グループ

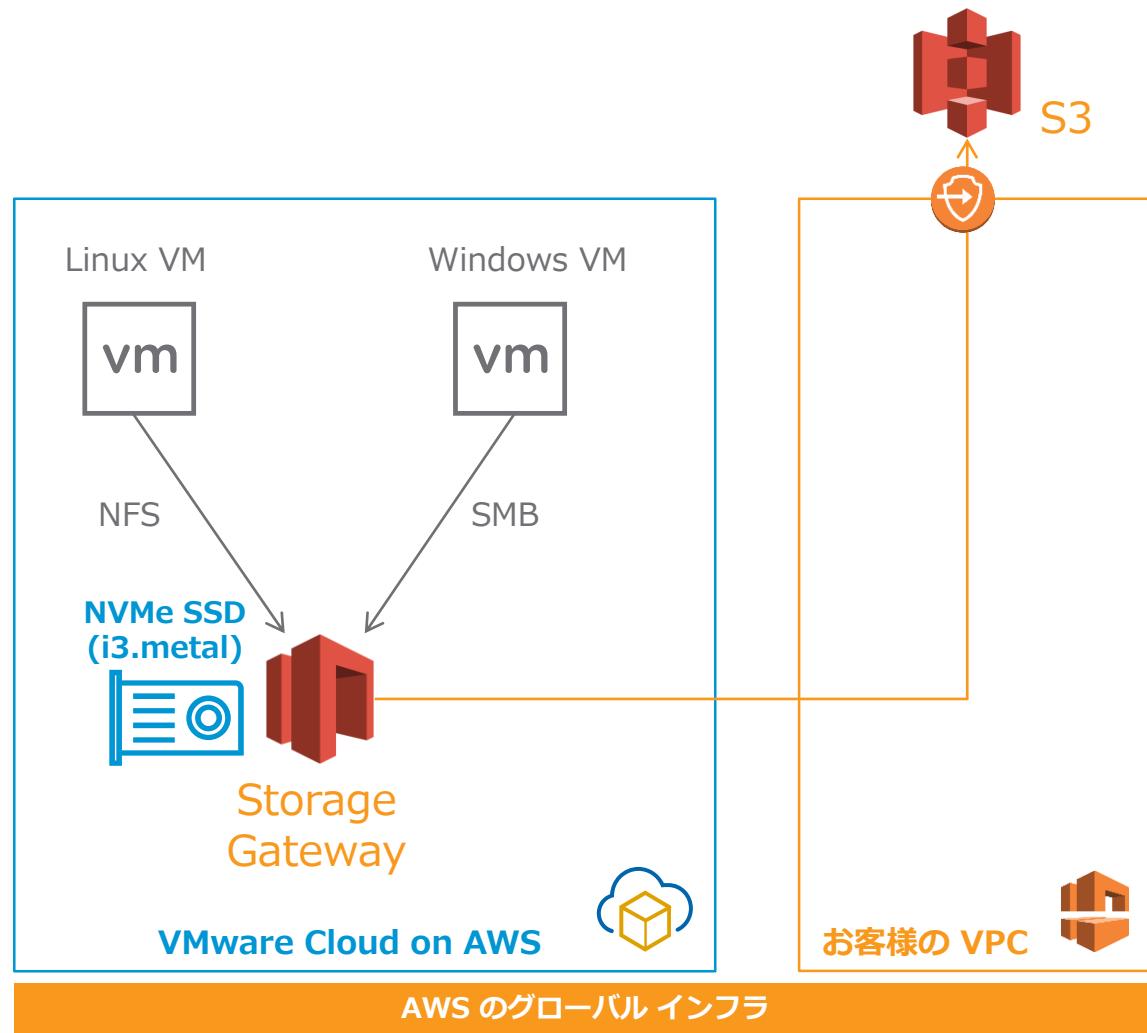


POC からの教訓

AWS Storage Gateway on VMware Cloud on AWS

AWS Storage Gateway

Amazon S3 をバックエンドとしたストレージ サービス



様々なサービスに対応

- ・ **ファイル ゲートウェイ (NFS/SMB)**
- ・ ボリューム ゲートウェイ (iSCSI)
- ・ テープゲートウェイ (iSCSI VTL)

格納容量無制限

- ・ 容量無制限の **Amazon S3** がバックエンド
- ・ Storage Gateway のディスクは**キャッシュ**

安価

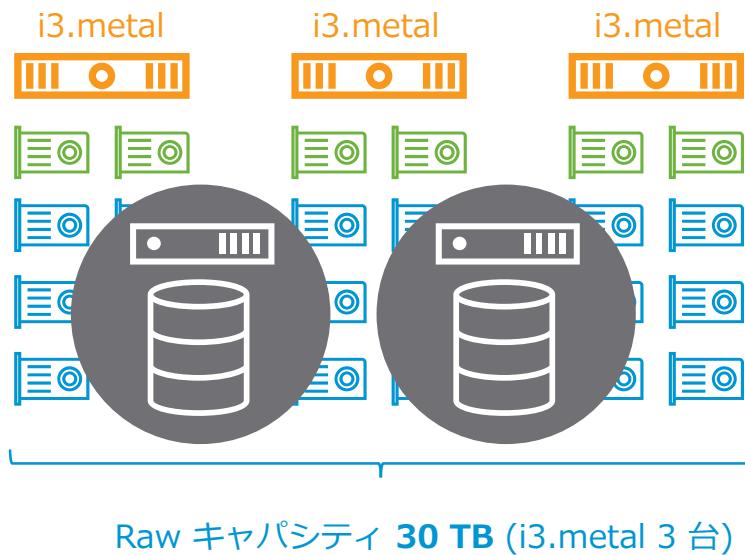
- ・ Amazon S3 の価格に準じる

プラットフォーム

- ・ Amazon EC2
- ・ **VMware**

ロックなし

貴重な NVMe SSD ストレージを大切に ファイル サーバーの置き換え



i3.metal インスタンス 3 台で Raw 30 TB

- 高価で高速な NVMe SSD

ファイルサーバーをそのまま移行すると
ストレージの**容量が不足しがち**

- ファイルサーバー: 数十 GB – 数 TB

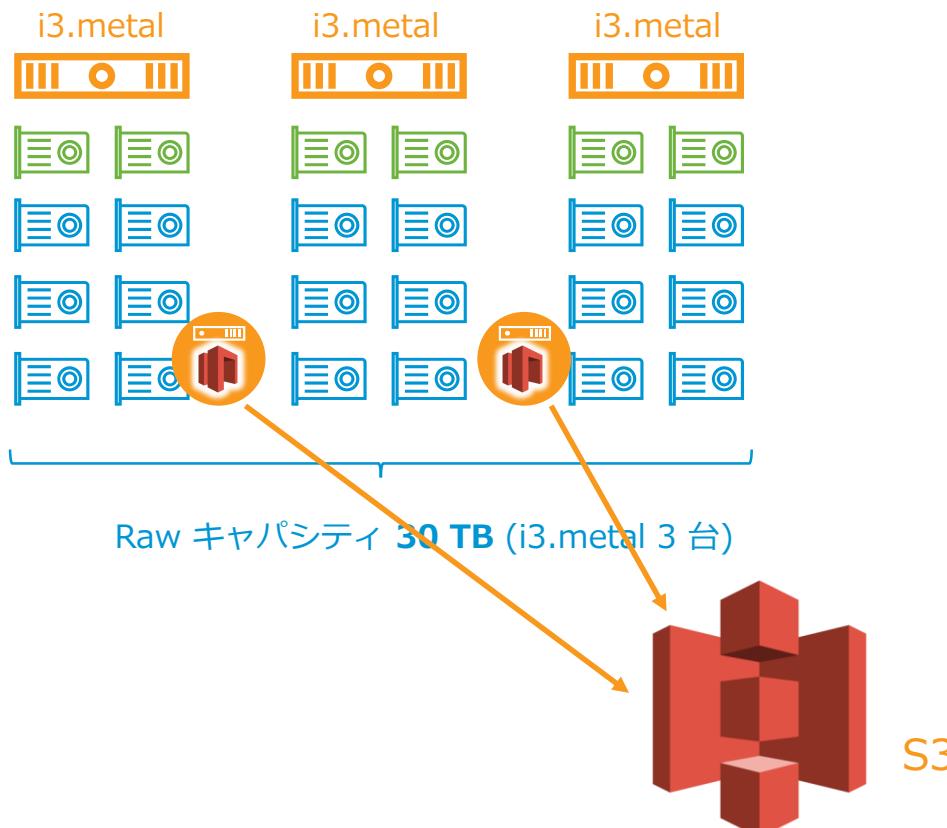
Storage Gateway に置き換え

- 高速な NVMe SSD キャッシュ
- 容量無制限
- vSAN データストアの容量節約

注意点

- ファイル ロックの必要性
- 高度なファイルサーバーの機能の要件
 - ユーザー権限
 - セルフ バックアップ / リストア

貴重な NVMe SSD ストレージを大切に ファイル サーバーの置き換え



i3.metal インスタンス 3 台で Raw 30 TB
• 高価で高速な NVMe SSD

ファイルサーバーをそのまま移行すると
ストレージの**容量が不足しがち**

- ファイルサーバー: 数十 GB – 数 TB

Storage Gateway に置き換え

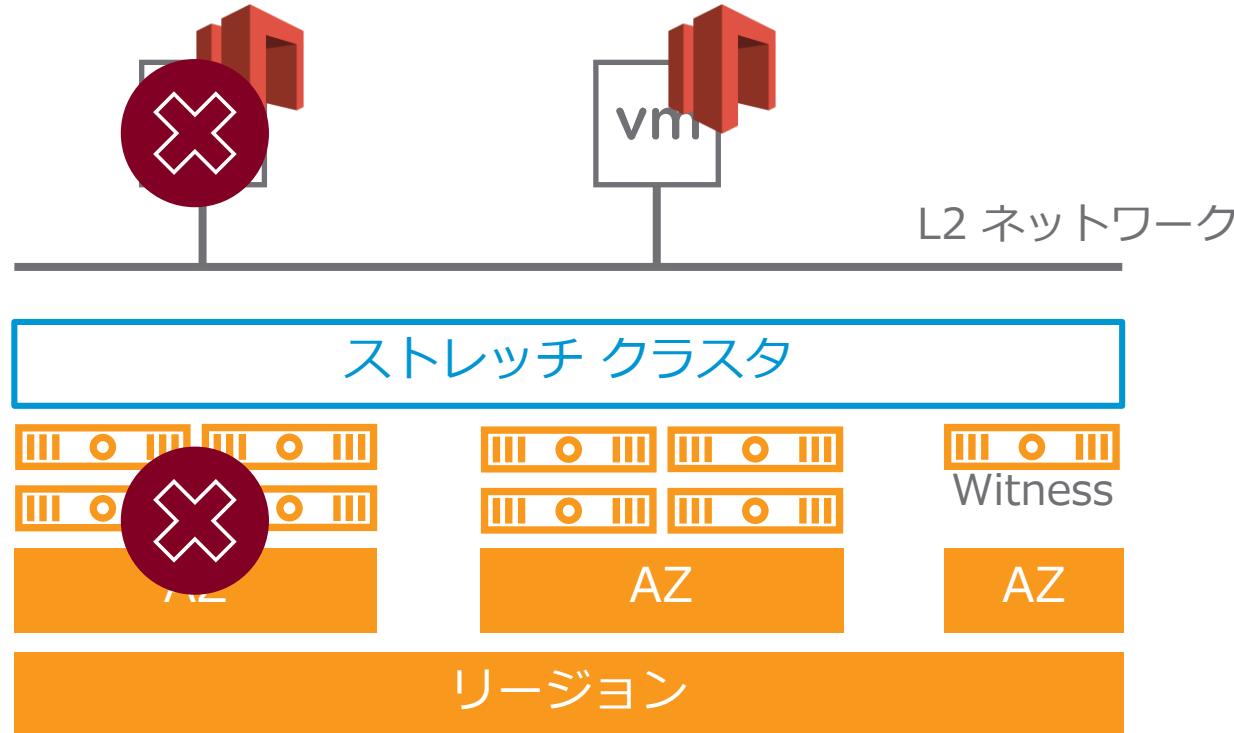
- 高速な NVMe SSD キャッシュ
- 容量無制限
- vSAN データストアの容量節約

注意点

- ファイル ロックの必要性
- 高度なファイルサーバーの機能の要件
 - ユーザー権限
 - セルフ バックアップ / リストア

Multi-AZ 対応した Storage Gateway

Power of AWS and VMware



AWS と VMware の共演による
Multi-AZ 対応の Storage Gateway

- **AWS Storage Gateway**
- VMware Cloud on AWS 上での **vSAN** ストレッチ クラスタ
- **AZ 間を貫く L2 ネットワーク**を実現する **NSX** オーバーレイ ネットワーク
- **セキュアな経路**を確保する **VMware Cloud ENI** と **VPC エンドポイント**

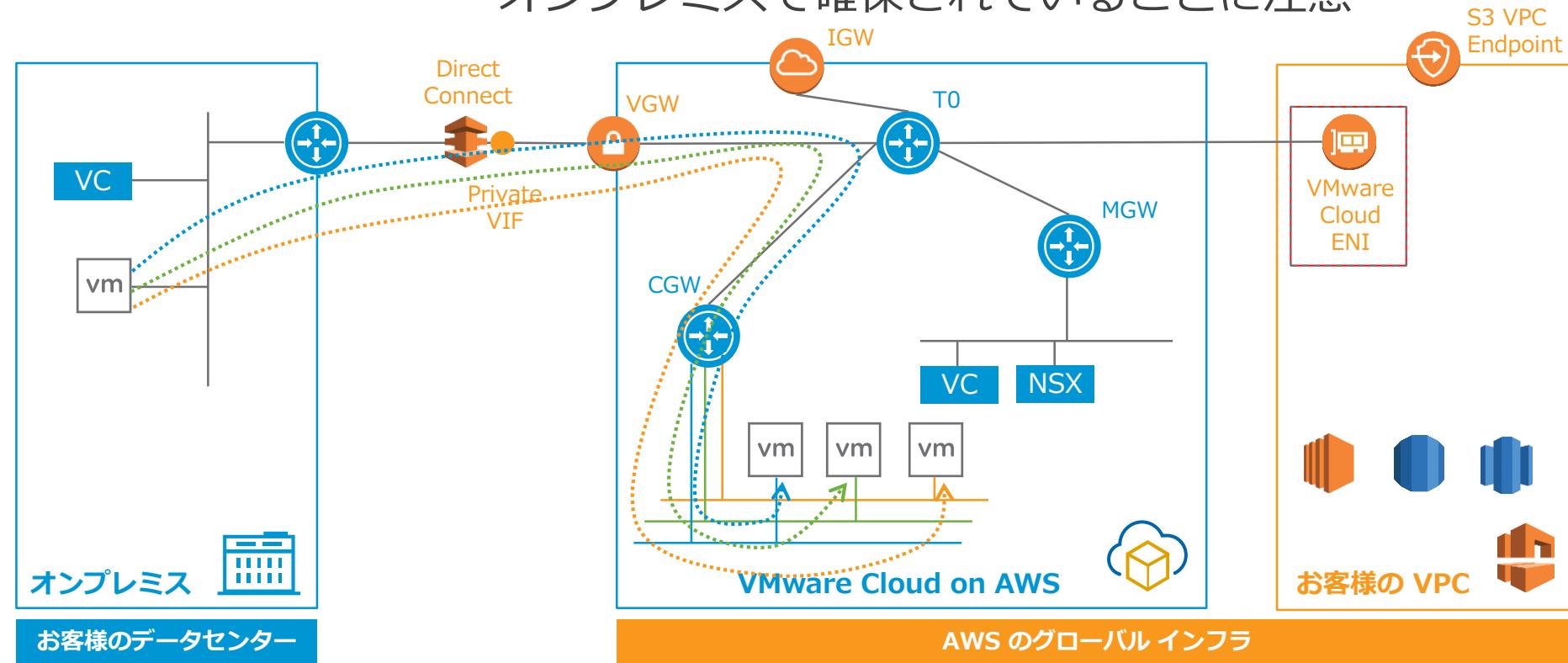
POC からの教訓

NSX-T with AWS Direct Connect

Direct Connect

Overlay network routing support

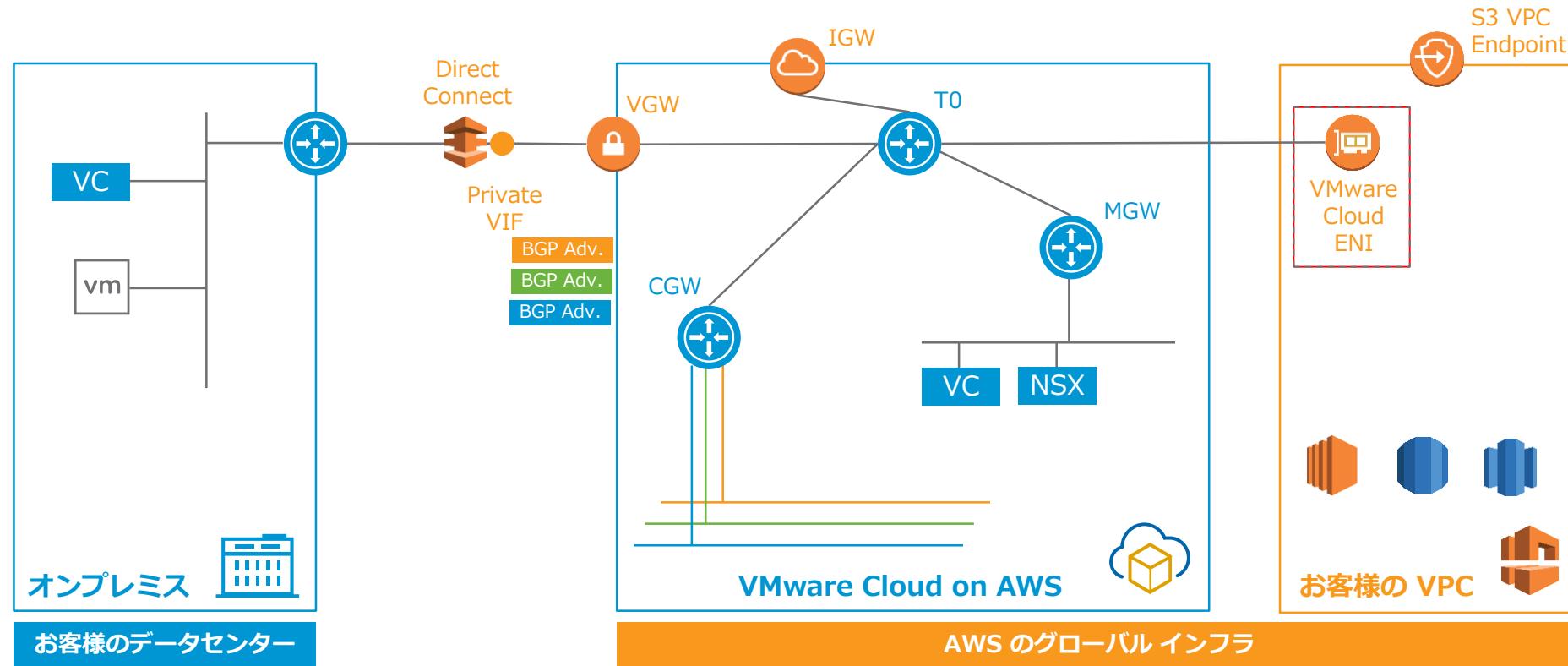
オンプレミスから **Direct Connect** 経由で VMC 側の**オーバーレイ ネットワーク**にアクセス可能
動的に作成可能なオーバーレイ ネットワークへの経路情報が
オンプレミスで確保されていることに注意



Need to be careful to advertisement

論理ネットワークの作成と同時にネットワークを Advertise 開始

- ・デフォルトで作成される論理ネットワーク (192.168.1.0/24) に注意

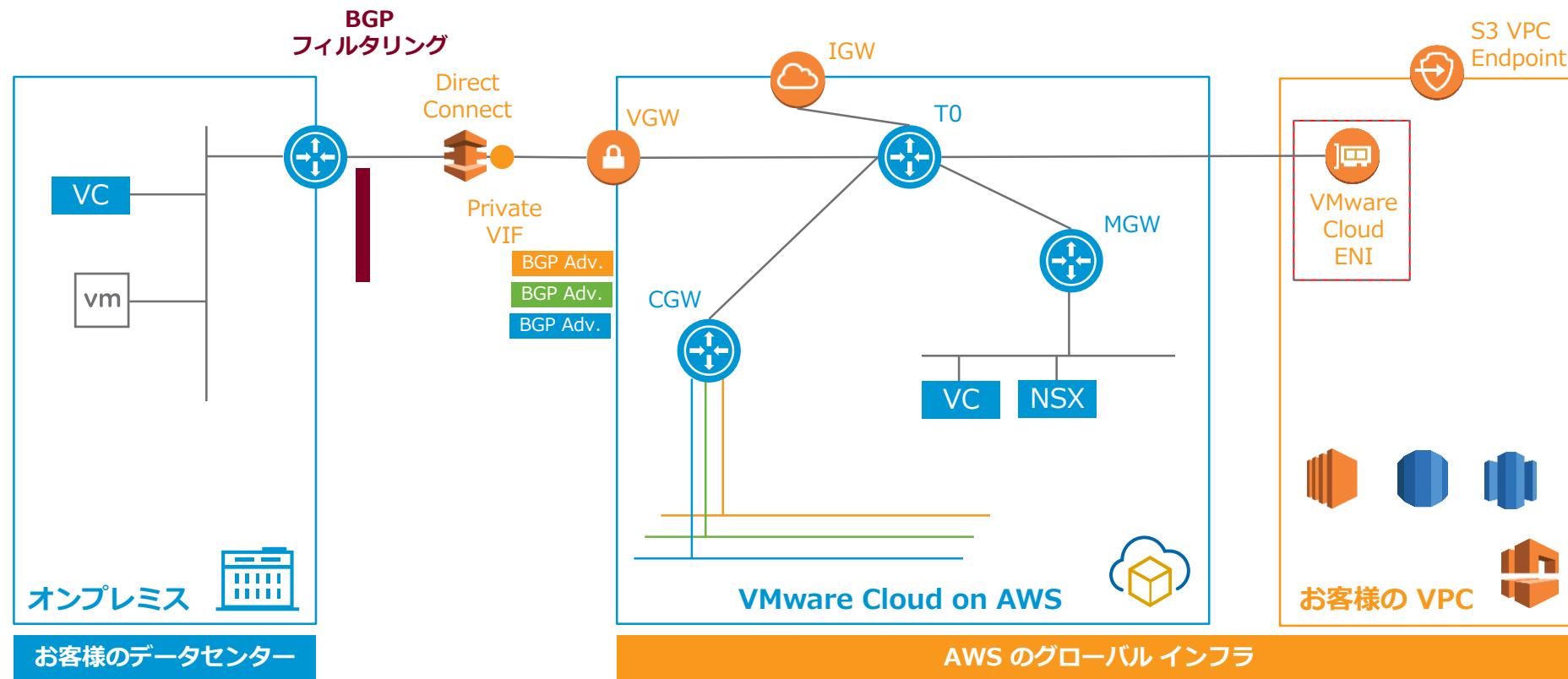


Need to be careful to advertisement

論理ネットワークの作成と同時にネットワークを Advertise 開始

- デフォルトで作成される論理ネットワーク (192.168.1.0/24) に注意

必要に応じてオンプレミス側のルーターで BGP ルート フィルタリングを実施



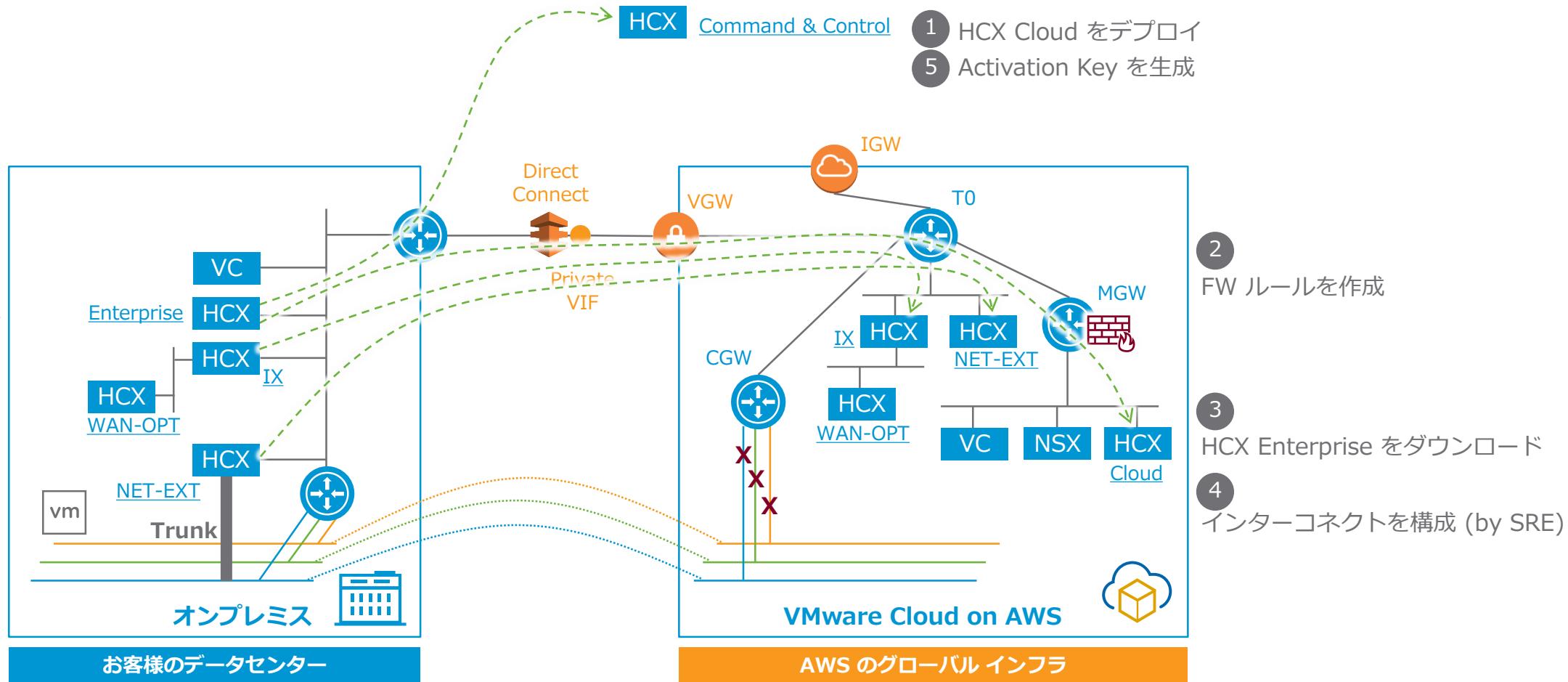
POC からの教訓

NSX-T with HCX

HCX のデプロイから利用まで

A long way to go

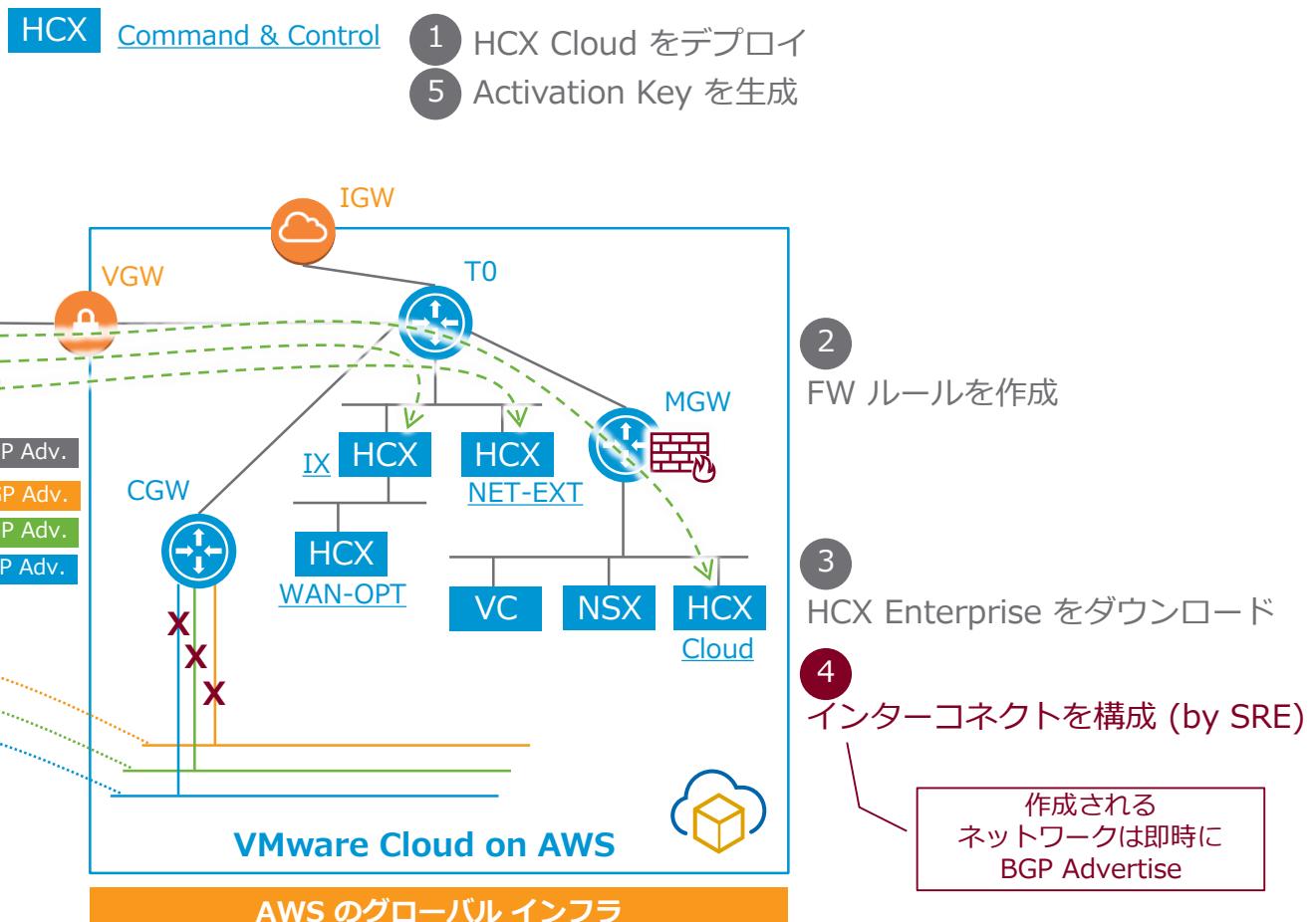
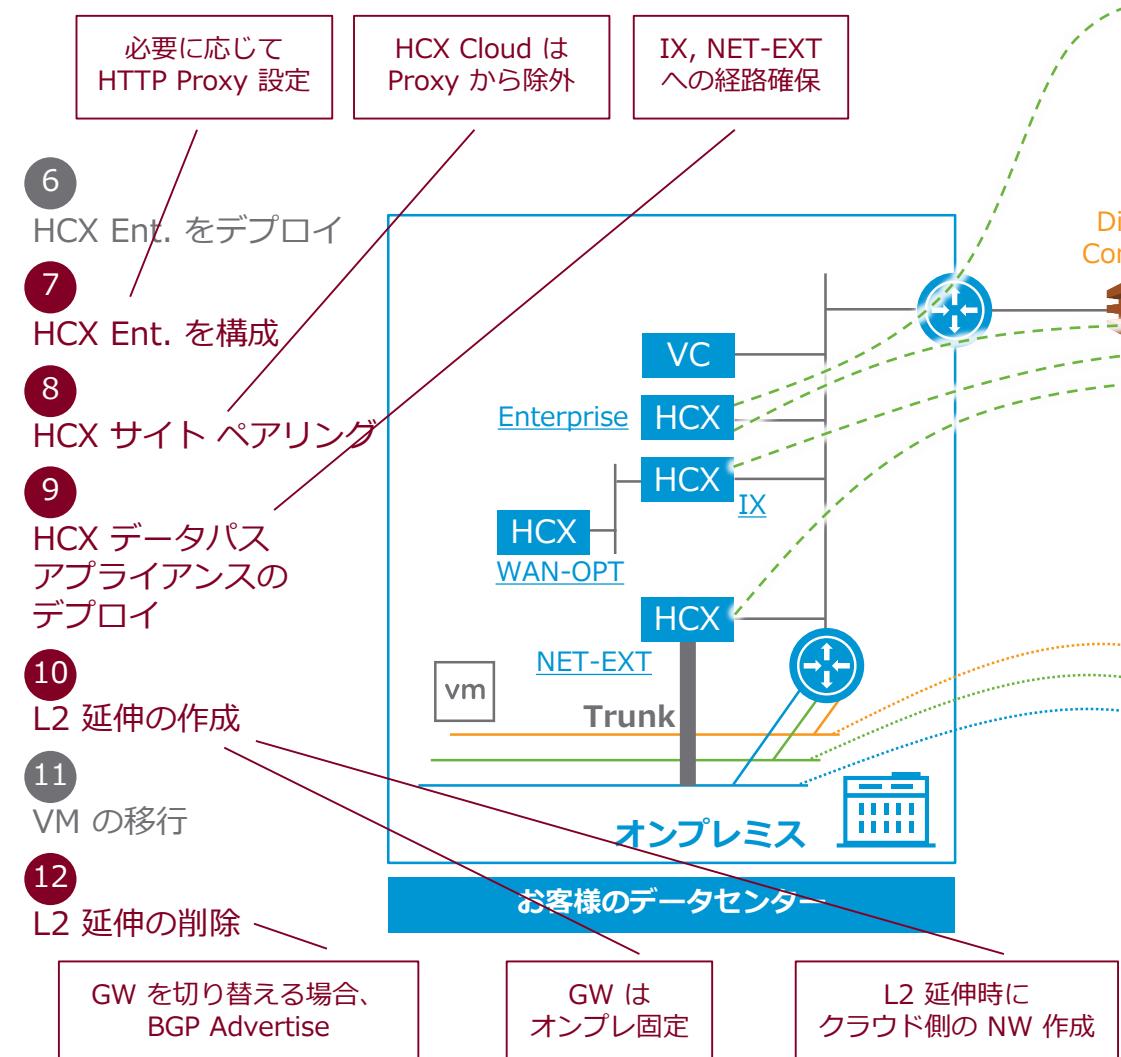
- 6 HCX Ent. をデプロイ
- 7 HCX Ent. を構成
- 8 HCX サイトペアリング
- 9 HCX データパス アプライアンスの デプロイ
- 10 L2 延伸の作成
- 11 VM の移行
- 12 L2 延伸の削除



東京リージョンオープン時は異なる手順になる可能性があります

ハマリどころ

Enjoy the journey



東京リージョンオープン時は異なる手順になる可能性があります

A silhouette of a person standing in a modern building with large windows overlooking a city skyline, holding a tablet.

おわりに

Open the Door to VMware Cloud on AWS

BRIDGING ACROSS SILOS OF INNOVATION





Build up Your Team

VMware SDDC

Application

Networking

Amazon Web
Services



Build up Your Skills

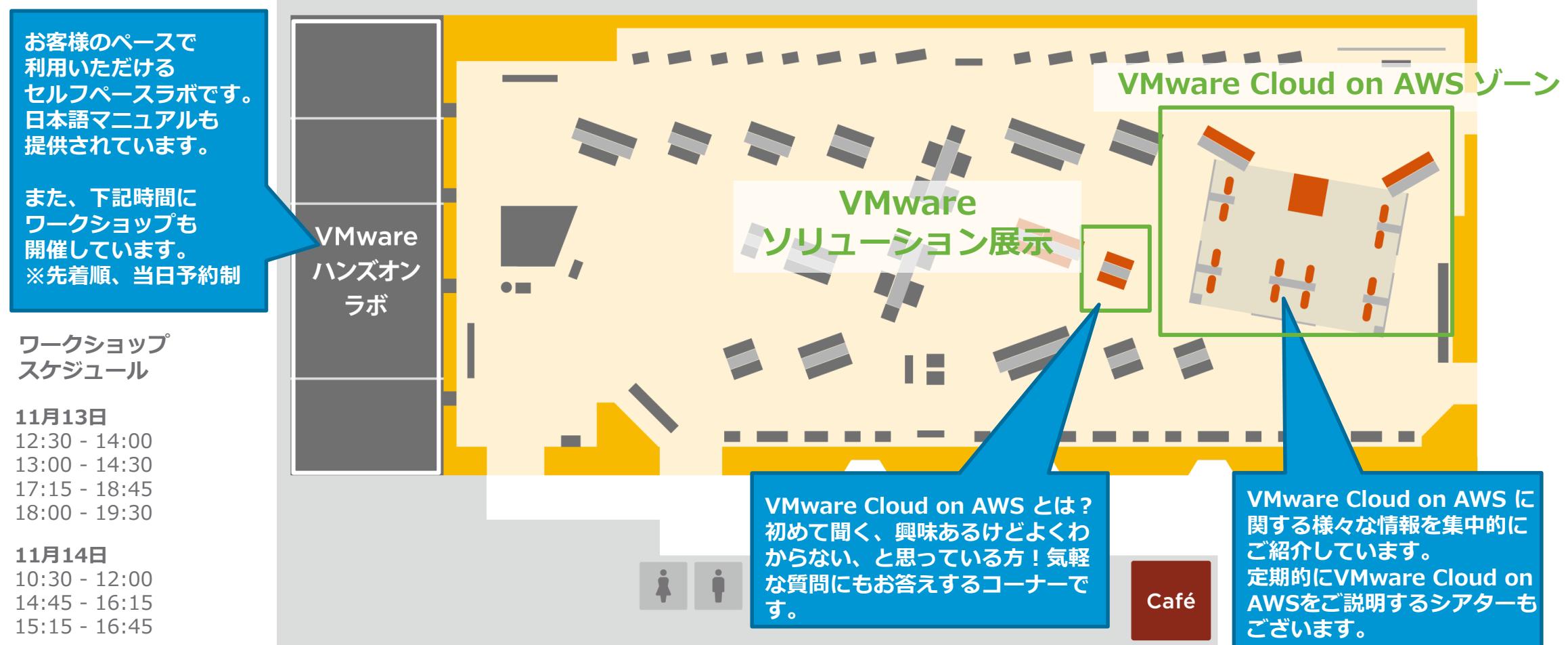
VMware SDDC

Application

Networking

Amazon Web
Services

本セッションに関連する展示・ハンズオンラボのご紹介





“1 ノード SDDC から
お気軽にお試し下さい”

Bridge across On-Premises and Clouds



ご清聴、ありがとうございました。