

徹底解説！ 進化を続ける VMware Cloud on AWS ～大阪リージョンを活用した災害対策とネットワーク 接続のベストプラクティス～

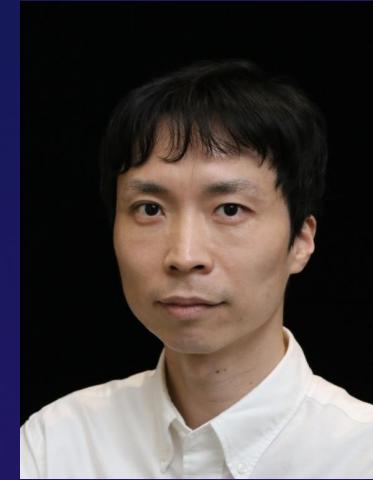
豊田 真行

ISVパートナー本部 シニアパートナーソリューションアーキテクト
アマゾン ウェブ サービス ジャパン合同会社

自己紹介

豊田 真行 (Masayuki Toyoda)

アマゾン ウェブ サービス ジャパン合同会社
ISVパートナー本部
シニアパートナーソリューションアーキテクト



好きな AWS サービス：



VMware Cloud on AWS



Amazon EventBridge



本セッションの対象と注意点

✓ 話すこと

- VMware Cloud on AWS のネットワーク接続のベストプラクティス
- VMware Cloud on AWS を活用した災害対策
- VMware Cloud on AWS に関するアップデート情報

✓ 話さないこと

- VMware ソフトウェア・コンポーネント (vSphere, vSAN, NSX) の基礎知識
- VMware Cloud on AWS の基本アーキテクチャ
 - 「AWS Black Belt Online Seminar – VMware Cloud on AWS」をご覧ください。
<https://aws.amazon.com/jp/blogs/news/webinar-bb-vmwarecloudonaws-2021/>

注意点

- 本セッションはセッション収録時点のサービス内容についてご説明しています。
最新の情報は AWS 公式ウェブサイト (<http://aws.amazon.com>) 及び
VMware 公式ウェブサイト (<https://www.vmware.com/jp/products/vmc-on-aws.html>) をご確認ください。



Agenda

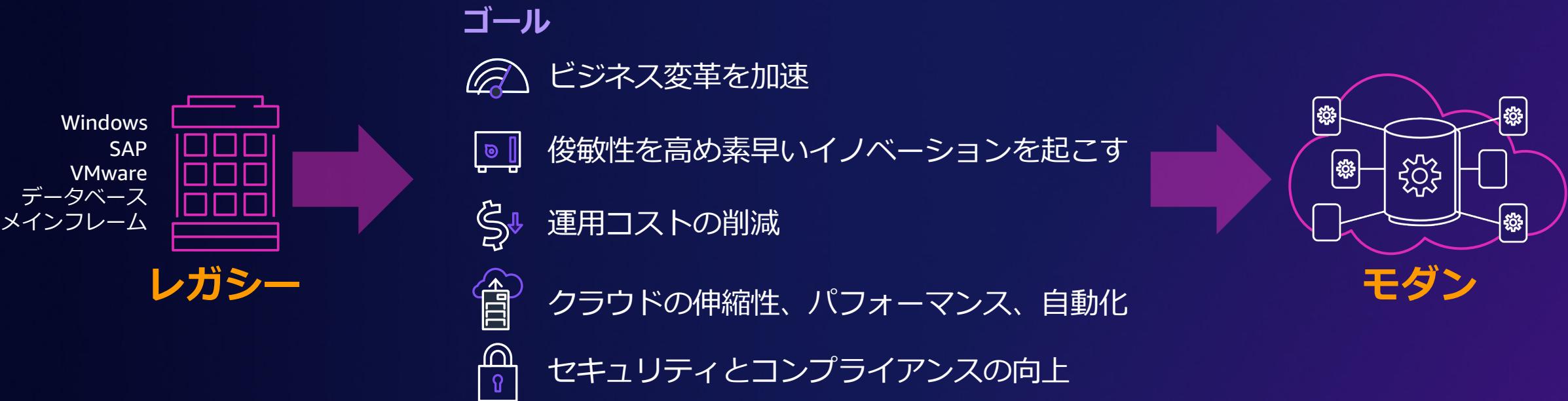
1. はじめに (VMware Cloud on AWS の概要)
2. コストを最適化した災害対策の実現
3. 大阪 / 東京リージョンのネットワーク接続構成
4. ネイティブ AWS サービスとの様々な接続要件におけるネットワークデザイン
5. 最新アップデート

はじめに



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

レガシーアプリケーションやデータは クラウドに移行し始めている

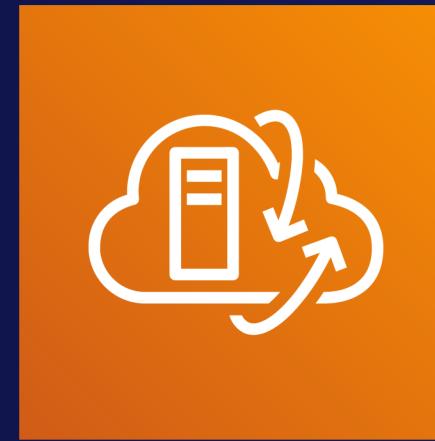


>50% の企業のワークフローとデータが 12か月以内に
パブリッククラウドに移行すると見込まれている

AWS のツール、プログラム、サービス



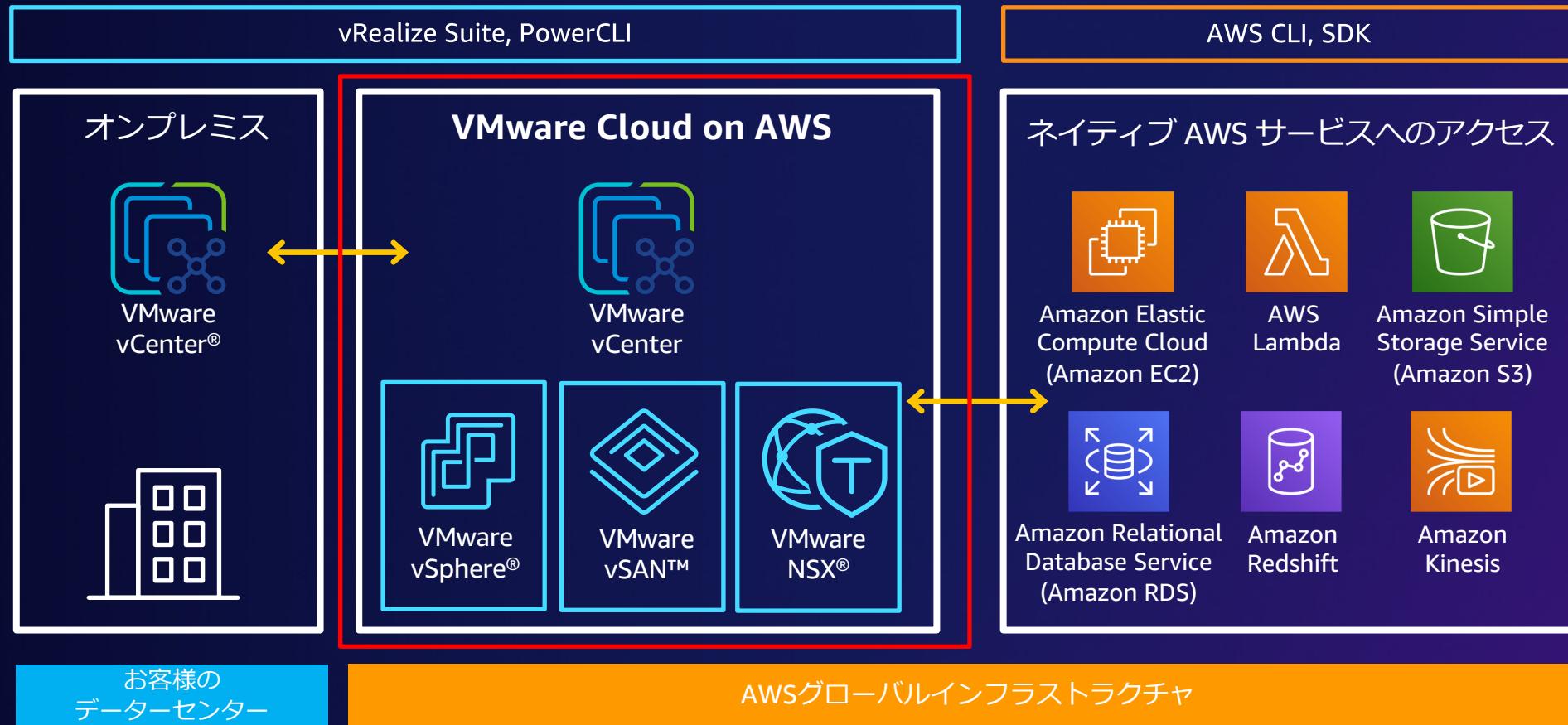
- ✓ 目的に特化した AWS および パートナー製品
- ✓ インセンティブ プログラム
- ✓ サードパーティーオファリング
- ✓ 無料のリソース
- ✓ AWS プロフェッショナルサービス
- ✓ 認定パートナーサービス



VMware Cloud on AWS

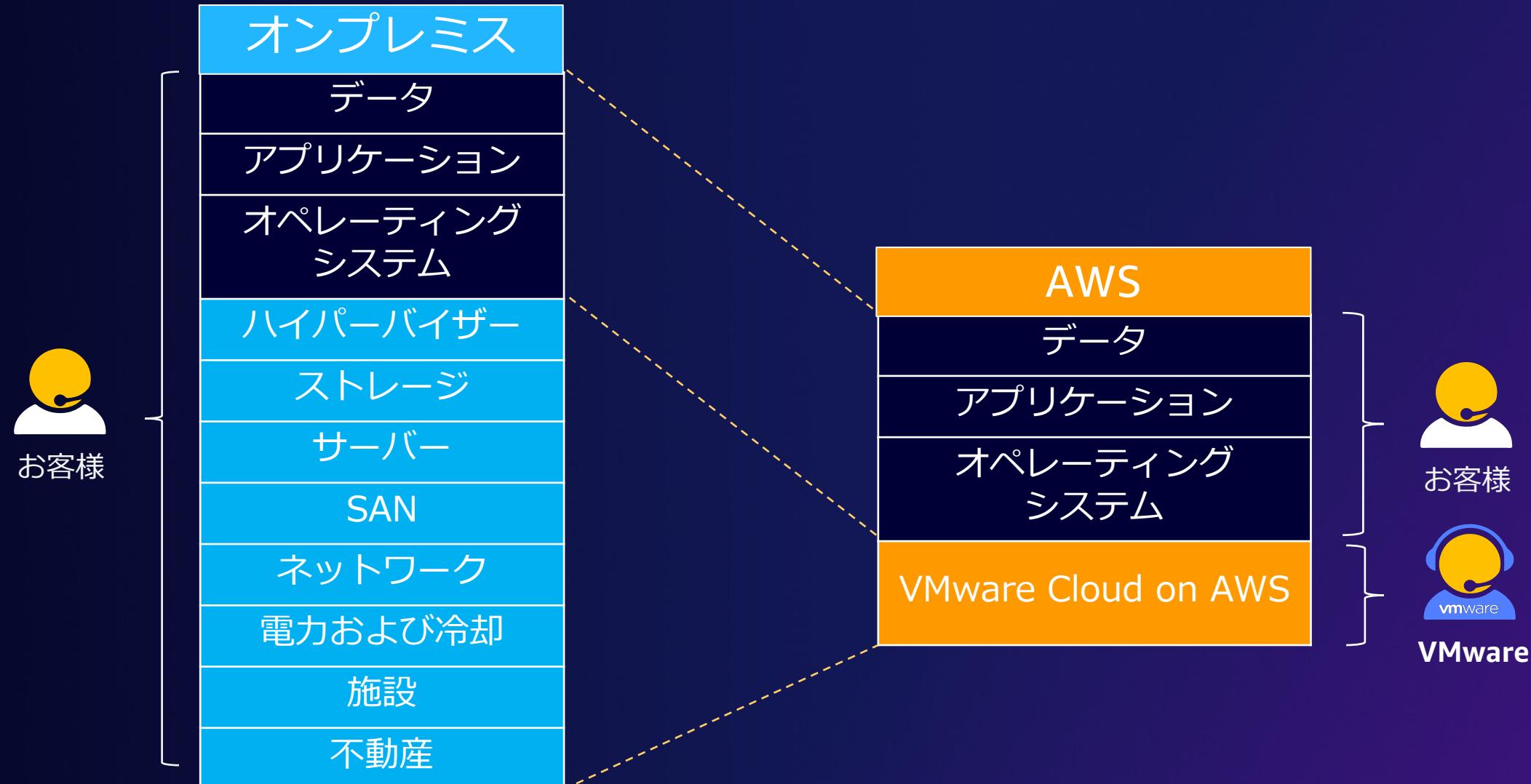
VMware Cloud on AWS

VMware と AWS により共同開発されたイノベーション



共同開発ならではの VMware による"フルマネージドサービス"

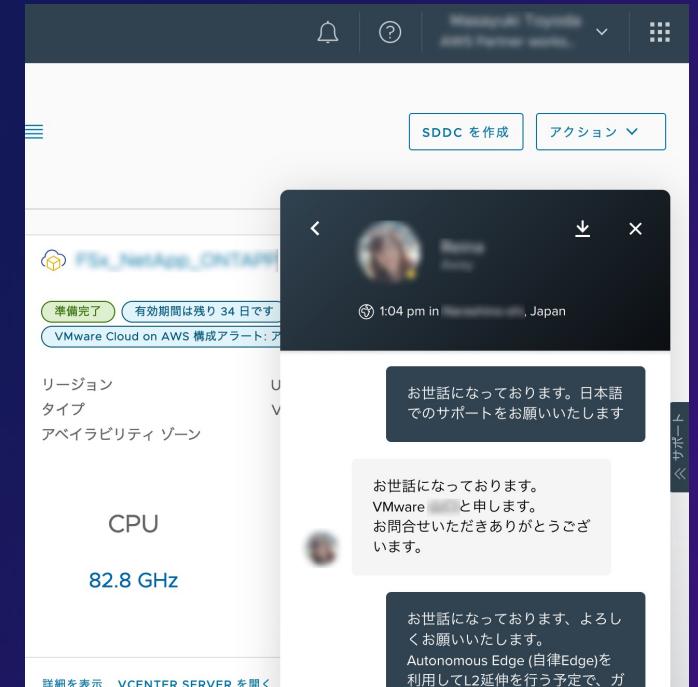
お客様はゲスト OS から上のレイヤーに注力出来る



共同開発ならではの VMware による"フルマネージドサービス"

VMware による高品質なサポート

- VMware Cloud on AWS は L1 から VMware の直接サポート
- VMware が単一のサポート窓口を提供
- 日本語でのサポート（※日本時間帯のみ）



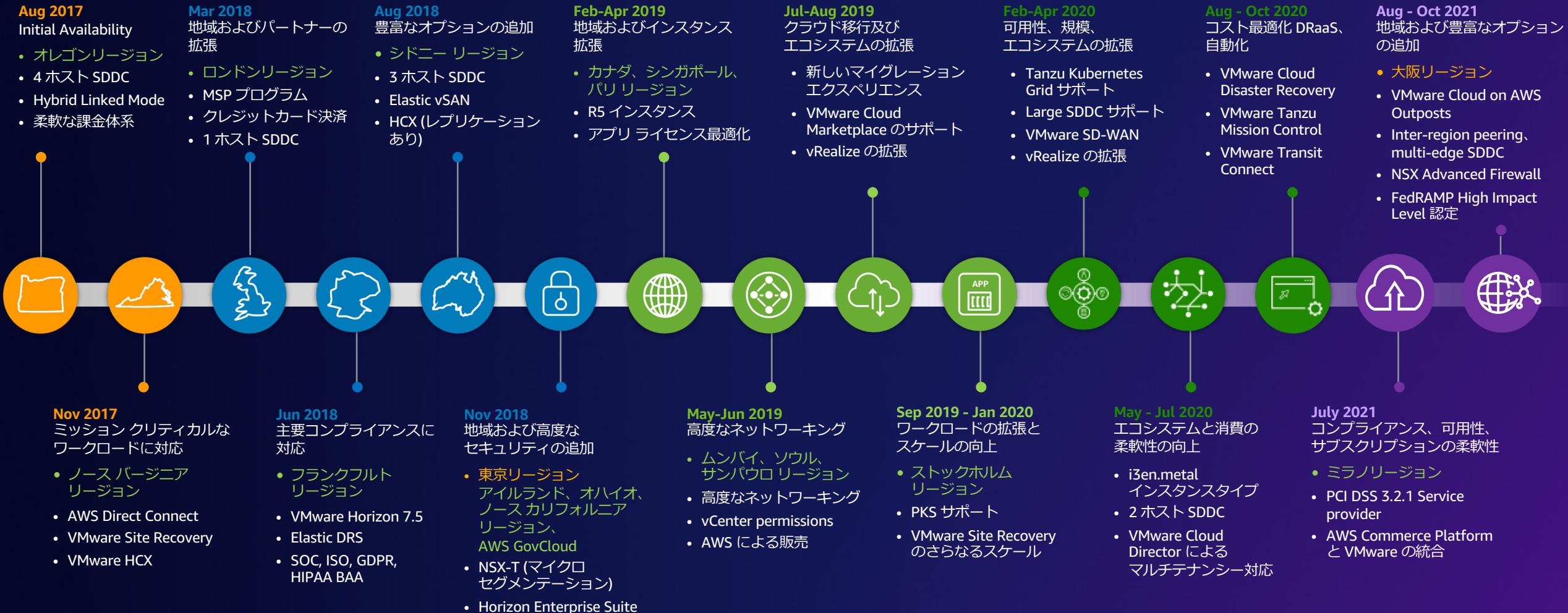
SDDC スタック以下のパッチ適用や障害対応は VMware が実施※

- お客様はインフラにかける時間が削減でき、イノベーションへ注力が可能に

※ VMware Cloud on AWS における責任共有モデルの詳細は下記を参照
<https://docs.vmware.com/en/VMware-Cloud-on-AWS/solutions/VMware-Cloud-on-AWS.39646badb412ba21bd6770ef62ae00a2/GUID-31CC90E5EB22075B2313FA674D567F2A.html>



お客様のニーズに基づいた機能を継続的にリリース



VMware Cloud on AWS は 20 のリージョンで利用可能

- ◆ 米国東部 (バージニア北部)
- ◆ 米国西部 (北カリフォルニア)
- ◆ 米国西部 (オレゴン)
- ◆ 欧州 (アイルランド)
- ◆ アジアパシフィック (東京)
- ◆ 南米 (サンパウロ)
- ◆ アジアパシフィック (シンガポール)
- ◆ アジアパシフィック (シドニー)
- ◆ GovCloud (米国西部) *1 **NEW**
- ◆ 欧州 (フランクフルト)
- ◆ アジアパシフィック (ソウル)
- ◆ アジアパシフィック (ムンバイ)
- ◆ 米国東部 (オハイオ)
- ◆ カナダ (中部)
- ◆ 欧州 (ロンドン)
- ◆ 欧州 (パリ)
- ◆ アジアパシフィック (大阪) **NEW**
- ◆ GovCloud (米国東部) *1
- ◆ 欧州 (ストックホルム)
- ◆ 欧州 (ミラノ) **NEW**



*1 GovCloud は米国政府関係企業用です

大阪リージョンで VMware Cloud on AWS の提供開始

大阪リージョンでの新たな活用シーン

クラウド移行



データセンターの拡張



災害対策



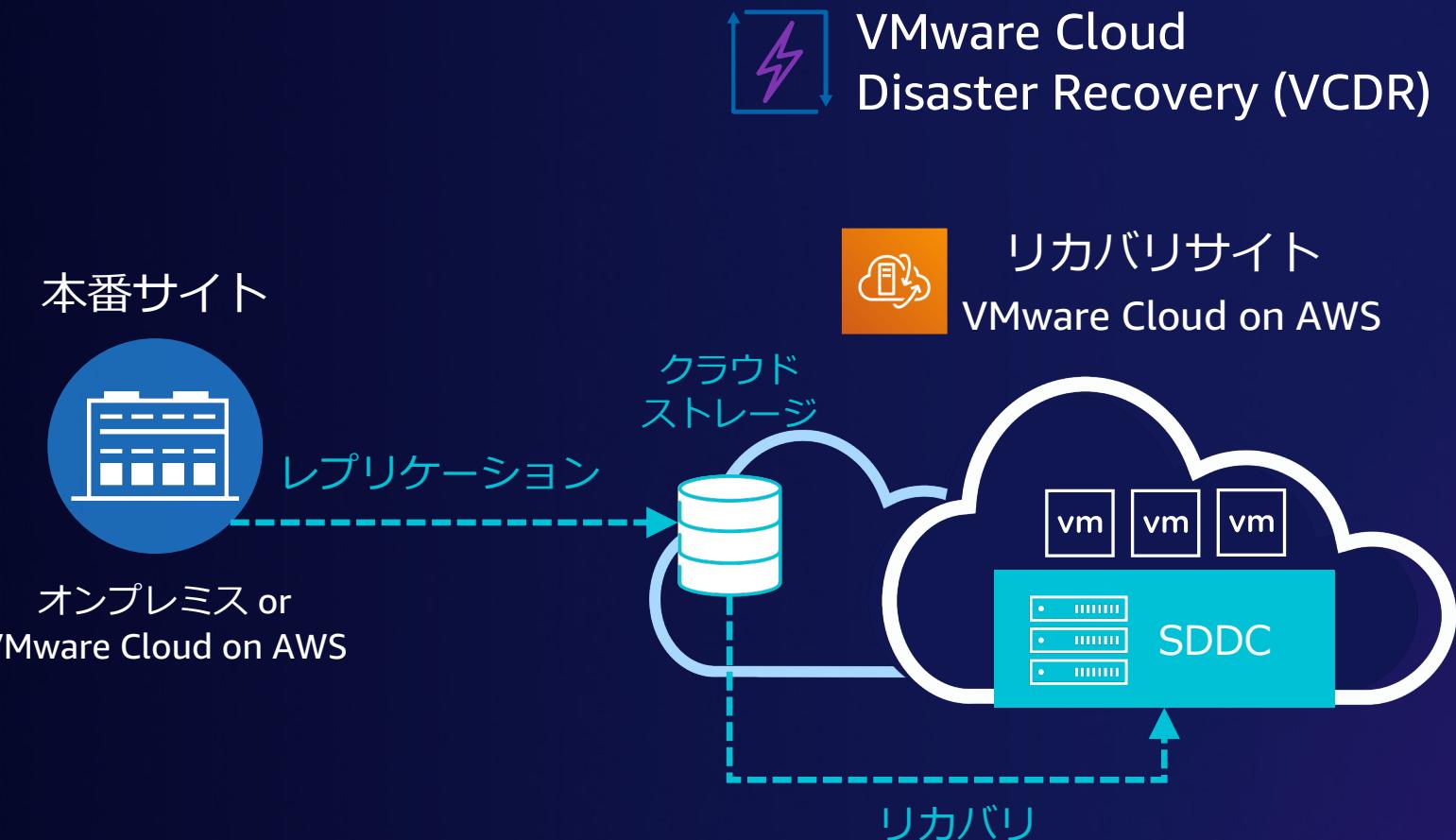
西日本地域のお客様に
従来より低遅延でサービスを提供が可能に

大阪リージョンと東京リージョンを
組み合わせ、広域災害に対する
災害対策を日本国内で実現

コストを最適化した災害対策の実現

VMware Cloud Disaster Recovery

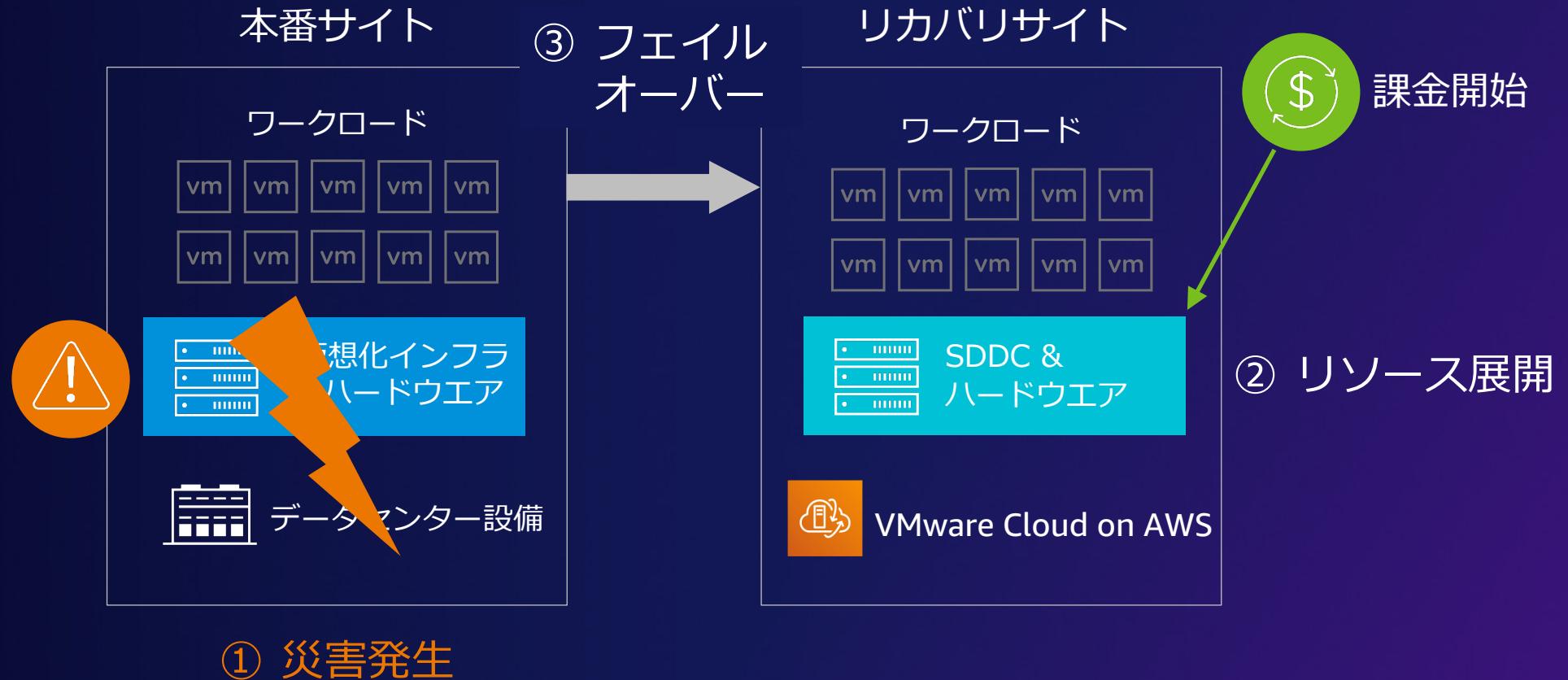
クラウドの利点を最大限に活かした災害対策ソリューション



- クラウドを活用した災害対策ソリューション (DRaaS)
 - 大規模な初期投資不要
 - 仮想マシンとストレージ容量による従量課金
 - クラウドにリカバリ可能 (クラウドストレージの活用)
- VMware Cloud on AWS の活用
 - リカバリサイトに VMware Cloud on AWS を利用
 - フェイルオーバーと同時に SDDC を展開可能 (SDDC の事前展開も可能)

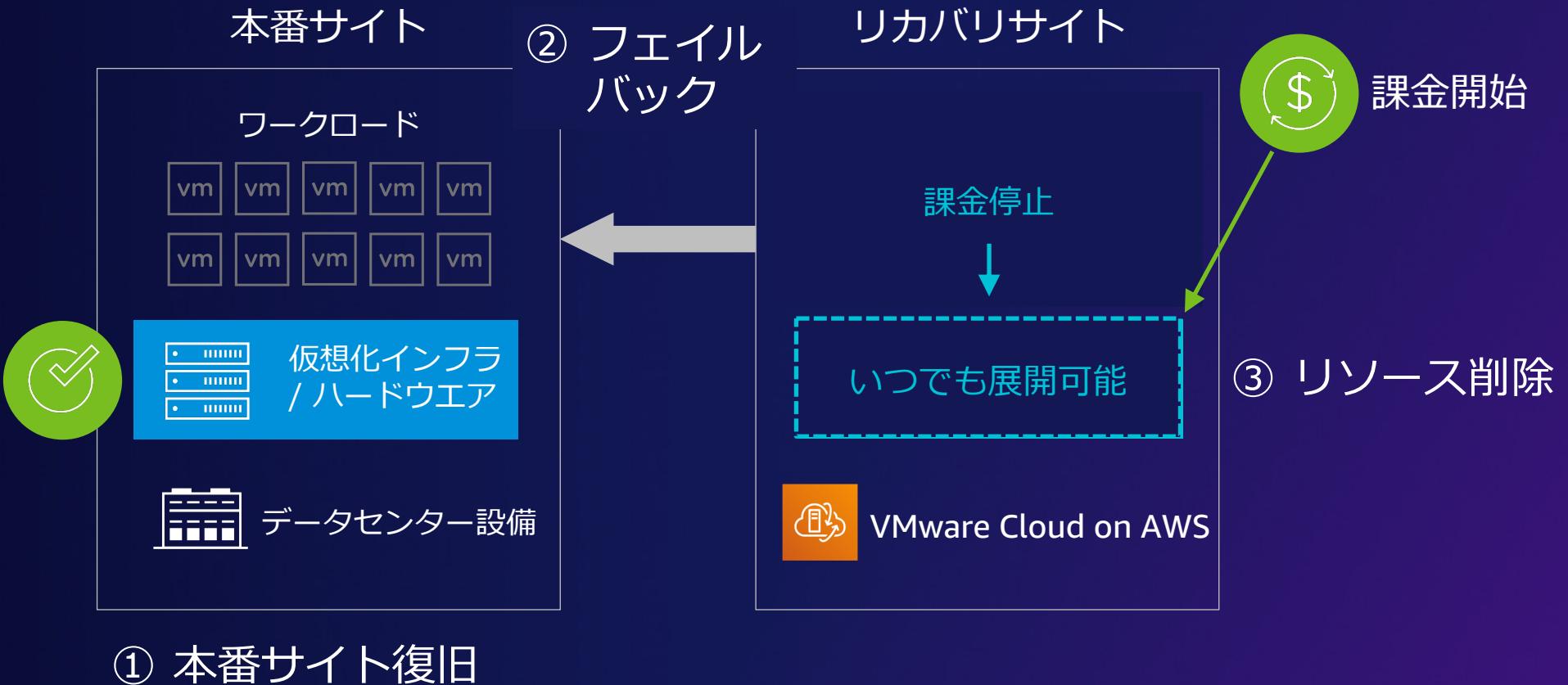
フェイルオーバーの動作

必要な時だけリソースを展開してコストを最適化



フェイルレバッくの動作

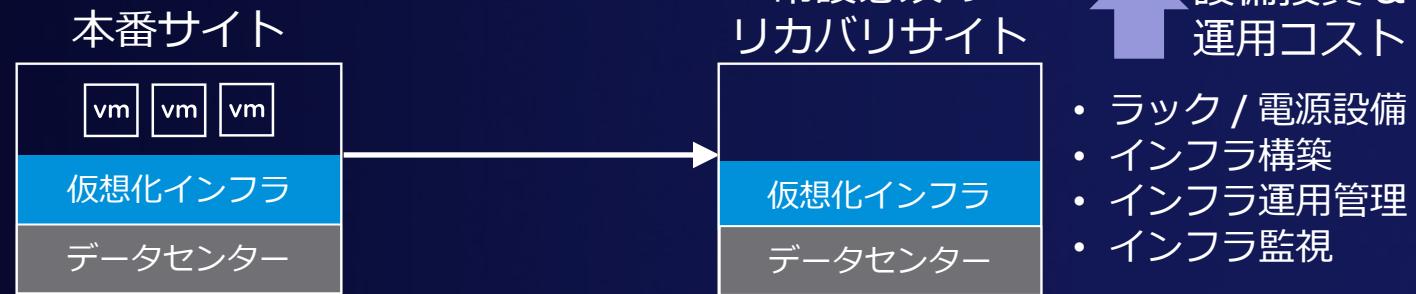
必要な時だけリソースを展開してコストを最適化



大規模な設備投資が不要に

クラウドのメリット（従量課金 / オンデマンド）を最大限に活かしてコストを最適化

従来の災害対策ソリューション



常設不要なリカバリサイト

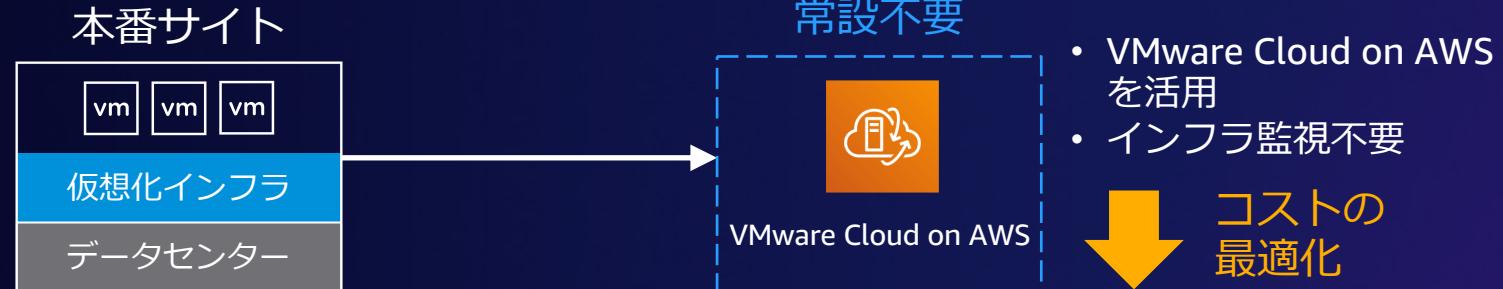
- ・VMware Cloud on AWS の活用により、フェイルオーバー実行と同時にリカバリサイトの展開が可能

従量課金によるコストの最適化

- ・必要時だけリカバリサイトを展開できるので、従来のソリューションと比べて大幅なコスト削減が可能
- ・利用量に応じた従量課金により、大規模な設備投資を回避



VMware Cloud Disaster Recovery



クラウドリソースの利用方法が選択可能

オンデマンド展開

On-demand

- ・フェイルオーバー時のみ SDDC（ホスト）を展開する方式
- ・**コスト抑制** を重視する要件に最適
- ・リカバリサイトのコスト削減が可能

事前展開

Pilot Light

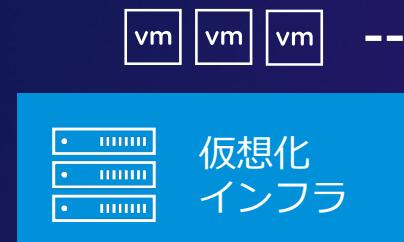
- ・予め必要最小限の SDDC（ホスト）を展開しておく方式
- ・**RTO の短縮化** を重視する要件に最適
- ・平常時はハイブリッドクラウドとして活用可能

本番サイト



リカバリサイト

本番サイト

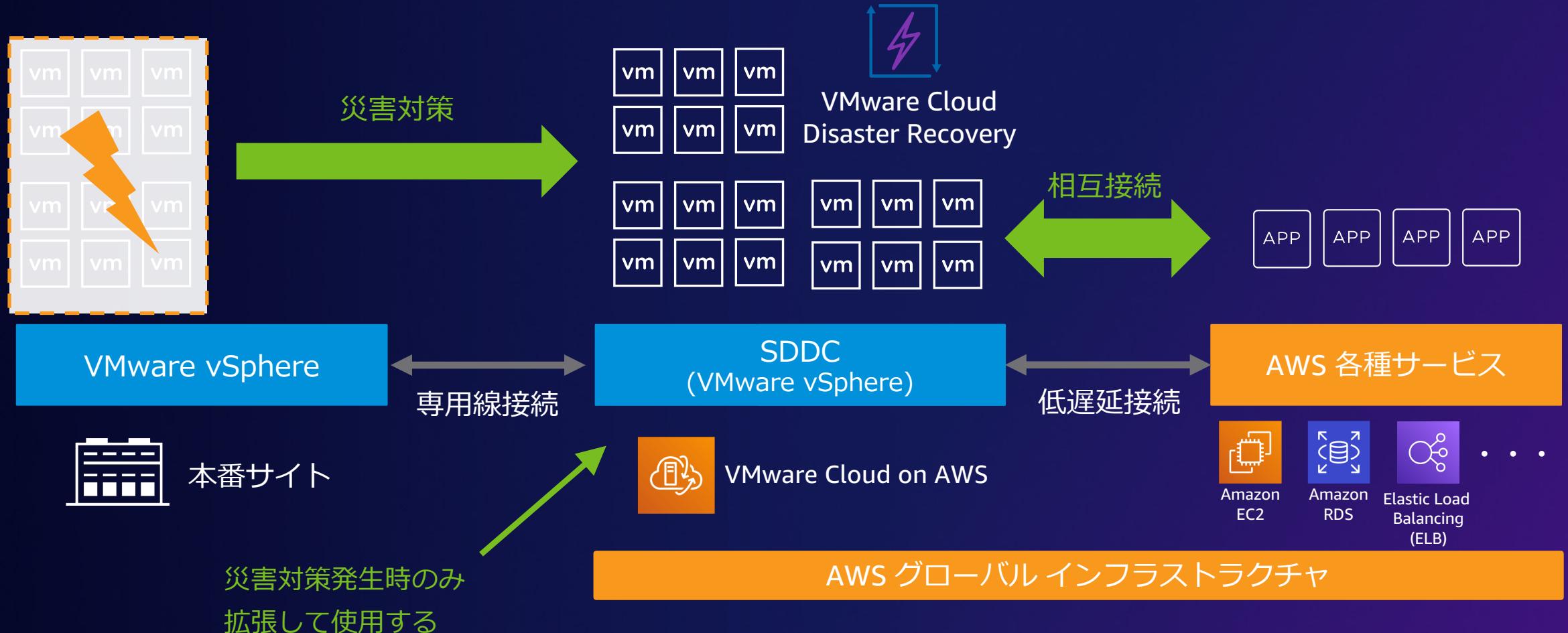


リカバリサイト



クラウドを活用した災害対策

Pilot Light（事前展開）オプション利用時もクラウドのメリットを最大限に活用



シンプルなオペレーションによって運用の最適化を実現



DR プランの事前定義により
有事のオペレーションを極小化

- 保護サイトやリカバリサイト、リソースなどの構成を事前に定義
- 有事の際には DR プランを実行するだけで操作が完了

運用の最適化

- オペレーションの定型化により属人化を回避
- シンプルなオペレーションによりヒューマンエラーを削減

直感的でわかりやすいユーザーアンターフェース

vmw VMware Cloud DR Dashboard Sites Protection groups DR plans Monitor

Dashboard

Global summary

Show setup guide

System health	Cloud backup	Protected sites	Recovery SDDC	Protected VMs	DR plans
	1 14.5 GiB Calculated every 12h	1 1	1	4 VMs	5

Sites

cloud-backup-1		14.5 GiB backup size
Demo-Lab-SDDC-Alpha		1 cluster 1 connector
OnPremises-Lab-IAD		1 vCenter 2 connectors
Demo-Lab-SDDC-Charlie		2 hosts 20.7 TiB storage

Topology

The diagram illustrates the network topology. It shows four main components: 'OnPremises-Lab-IAD' (represented by a blue circle with a cluster icon), 'cloud-backup-1' (represented by a blue circle with a cloud icon), 'Demo-Lab-SDDC-Alpha' (represented by a blue circle with a cloud icon), and 'Demo-Lab-SDDC-Charlie' (represented by a purple circle with a cube icon). Dashed arrows indicate bidirectional connections between 'OnPremises-Lab-IAD' and both 'cloud-backup-1' and 'Demo-Lab-SDDC-Alpha'. Additionally, there is a direct connection between 'cloud-backup-1' and 'Demo-Lab-SDDC-Charlie'.

災害対策は高い信頼性を維持することが基本

「いざと言う時に動作しない」を避けるための対策が必要

フェイルオーバー失敗の原因

- フェイルオーバーしたらハードウェアが故障していたため、復旧作業に時間がかかった
- バックアップしておいたデータが破損していたため、戻せなかつた
- 操作手順書が古いままで更新されておらず、操作ミスが発生した

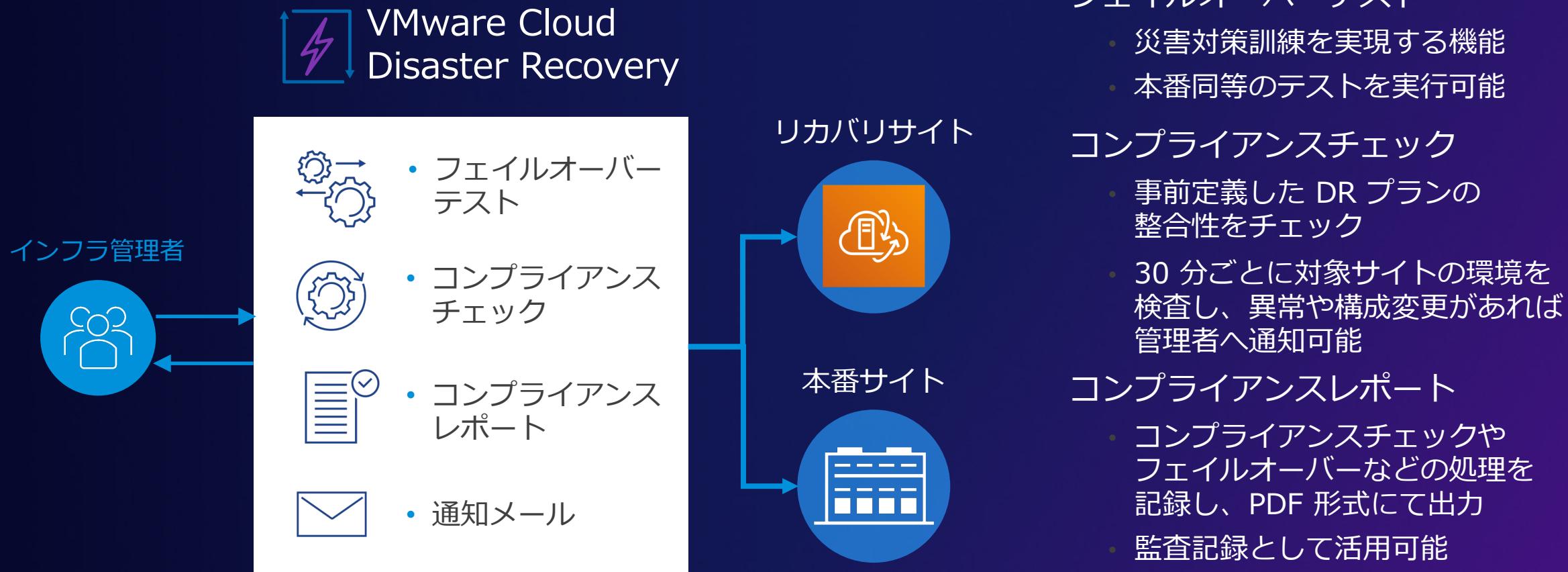


望ましい対策

- 定期的な災害対策訓練の実施
- リカバリサイトの健全性チェックと環境維持
- 操作手順と実環境の整合性の維持

安全で確実な災害対策を実現

フェイルオーバーの信頼性を高める機能によって、確実にビジネスを継続



コンプライアンスチェックとフェイルオーバーテスト

vwm VMware Cloud DR

Dashboard Sites Protection groups DR plans Monitor

SDDC-Alpha-VCDR-RPI

Summary Reports

Plan

SDDC-Alpha-VCDR-RPI

Demo-Lab-SDDC-Alpha → Demo-Lab-SDDC-Charlie

SDDC Alpha to Charlie VCDR RPI

Ready

Continuous compliance

All 20 checks passed with no issues! 16m ago

Protected site

- ✓ Connection to source site
- ✓ Protected groups replication schedule
- ✓ Networks exist on source site
- ✓ Resource pools exist on source site
- ✓ Folders exist on source site
- ✓ All clusters are protected on the source site
- ✓ Firewall rules created automatically exist in protected SDDC

Recovery site

- ✓ Connection to failover site
- ✓ vCenter server registered in failover site
- ✓ Datastores exist on failover site
- ✓ Protection groups can be recovered in failover site
- ✓ Networks exist on failover site
- ✓ Resource pools exist on failover site
- ✓ Folders exist on recovery site

Orchestration

- ✓ IP address mapping
- ✓ Recovery steps
- ✓ Script server recovered before script actions

Create PDF report OK

コンプライアンスチェック

OnPremises-VCDR-RP1

Summary **Reports**

<p>Plan</p> <p>OnPremises-VCDR-RP1</p> <p>OnPremises-Lab-1AD ➔ Demo-Lab-SDDC-Charlie</p> <p>DR Plan for Protection Group VMs to Failover from Protected OnPremises to Recovery Charlie</p>	<p>Protected groups</p> <p>OnPremises-VCDR-PG1</p>	<p>Continuous compliance</p> <p>19 / 19 checks passed 28m ago</p> <p>Show</p>
--	--	---

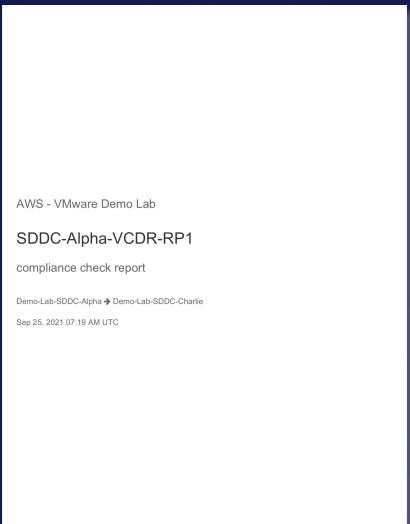
Test finished with no errors

Success

Step

Step	Timestamp	Duration	Progress
✓ Step 1. Prepare cloud storage resources to run VMs for step Recover all remaining VMs, files, and groups	Sep-28 05:45 pm < 1m		Finished
✓ 1. Prepare cloud storage resources to run VMs	[Log]		Finished
✓ Step 2. Recover all remaining VMs, files, and groups	Sep-28 05:45 pm < 1m		Finished
✓ 1. Duplicate protection group snapshot OnPremises-VCDR-PG1 - Every 4 hours - 2021-09-28T08:00 UTC into a snapshot with unlimited retention	[Log]	Sep-28 05:45 pm < 1m	Finished
✓ 2. Recover 1 VMs	[Log]	Sep-28 05:45 pm < 1m	Finished
✓ Step 3. Migrate to SDDC datastore VMs recovered in step Recover all remaining VMs, files, and groups	Sep-28 05:46 pm < 1m		Finished
✓ 1. Migrate 1 VMs to SDDC datastore	[Log]	Sep-28 05:46 pm < 1m	Finished
✓ Step 4. Release cloud storage resources for step Recover all remaining VMs, files, and groups	Sep-28 05:47 pm < 1m		Finished
✓ 1. Release cloud storage resources	[Log]	Sep-28 05:47 pm < 1m	Finished

フェイルオーバーテスト



コンプライアンスチェックレポート (PDF)

AWS - VMware Demo Lab		Since
Protected site		
✓ Folders exist on source site	Sep 15, 2021 03:23 PM UTC	
✗ Connection to source site	Sep 15, 2021 03:25 PM UTC	
✗ Replication rules on source site	Sep 15, 2021 03:26 PM UTC	
All clusters are protected on the source site	Jun 18, 2021 16:45 AM UTC	
Firewall rules created automatically exist in protected SDDC	Sep 22, 2021 05:55 AM UTC	
✓ Protected groups replication schedule	Aug 18, 2021 15:48 PM UTC	
✓ Networks exist on source site	Sep 15, 2021 03:26 PM UTC	
Recovery site		Since
✓ Networks exist on fallover site	Aug 25, 2021 01:48 PM UTC	
✗ Recovery points exist on recovery site	Aug 25, 2021 01:49 PM UTC	
✓ vCenter server registered in fallover site	Aug 25, 2021 01:49 PM UTC	
✗ Connection to fallover site	Aug 25, 2021 01:51 PM UTC	
✓ Protection groups can be recovered in fallover site	Aug 25, 2021 01:51 PM UTC	
✓ Folders exist on recovery site	Aug 25, 2021 01:52 PM UTC	
✓ Databases exist on fallover site	Aug 25, 2021 01:52 PM UTC	
Orchestration		Since
✗ IP address mapping	Aug 18, 2021 16:48 PM UTC	
✓ Recovery steps	Jun 18, 2021 16:48 PM UTC	
✗ Script server recovered before script actions	Jun 18, 2021 16:49 PM UTC	
Other		Since
✓ VMC refresh token valid	Aug 25, 2021 01:50 PM UTC	
✓ VMC folder structure for file recovery is valid	Aug 25, 2021 01:50 PM UTC	
✓ VMC proxy is running and reachable	Aug 25, 2021 01:50 PM UTC	

コンプライアンスチェックレポート (PDF)

AWS - VMware Demo Lab

Report contents

- Plan summary
- Plan configuration
- Failover runtime log
- Failover action log
- Env log

Plan summary

Plan name: SDDC-Alpha-VCDR-RP1

Description: SDDC Alpha to Charlie VCDR RP1

Protected site: Demo-Lab-SDDC-Alpha

Recovery Site: Demo-Lab-SDDC-Charlie

Test Site: cloud-backup-1

Protection groups: Alpha-SDDC-VCDR-PG1

Test failover

Result	Status
Success	Success

Started: Sep 16, 2021 15:38 PM UTC
Ended: Sep 16, 2021 15:39 PM UTC

Time to recovery: 38 seconds

Test status	Task successfully completed.
Errors	none

Clean up started: Sep 16, 2021 15:41 PM UTC
Clean up ended: Sep 16, 2021 15:41 PM UTC
Clean up status: Task has been cleaned.
Clean up errors: none

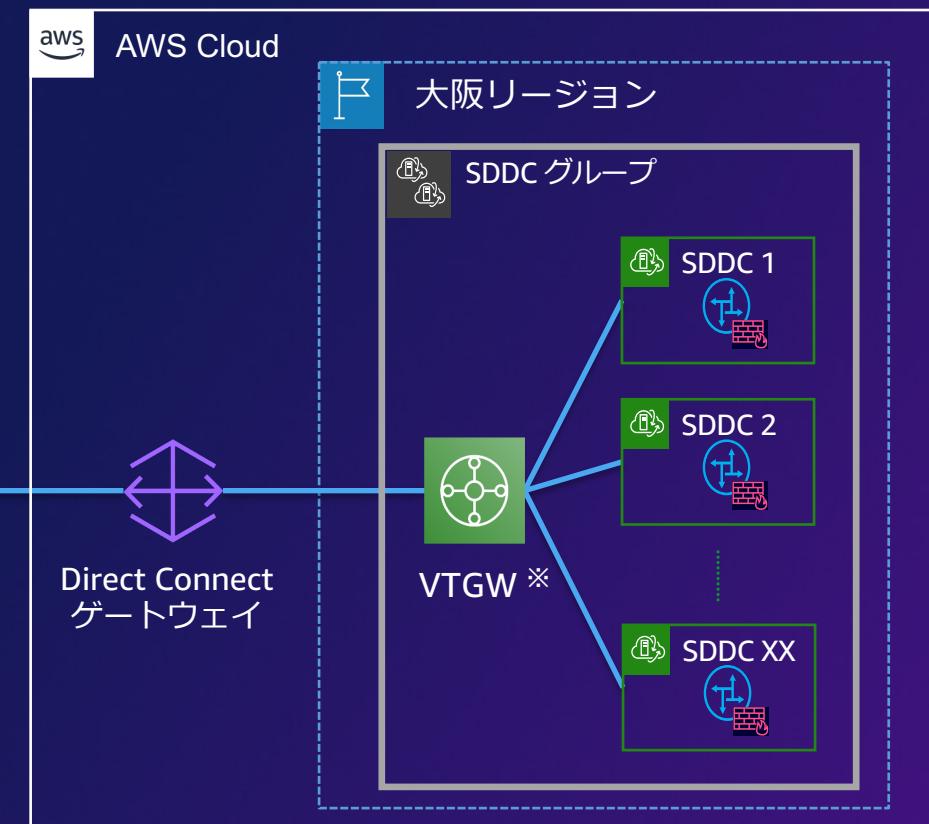
Vmware Cloud Disaster Recovery

フェイルオーバーテストレポート (PDF)

大阪 / 東京リージョンのネットワーク 接続構成

大阪リージョンとの AWS Direct Connect 接続

- 全世界の Direct Connect ポートケーションから Direct Connect ゲートウェイ経由で接続可能
- 大阪の **Equinix OS1** を利用する事で、東京の災害の影響を受けず直接大阪リージョンへ到達する
- VMware Transit Connect** 利用により Direct Connect ゲートウェイ経由でのオンプレミスとの接続が可能※

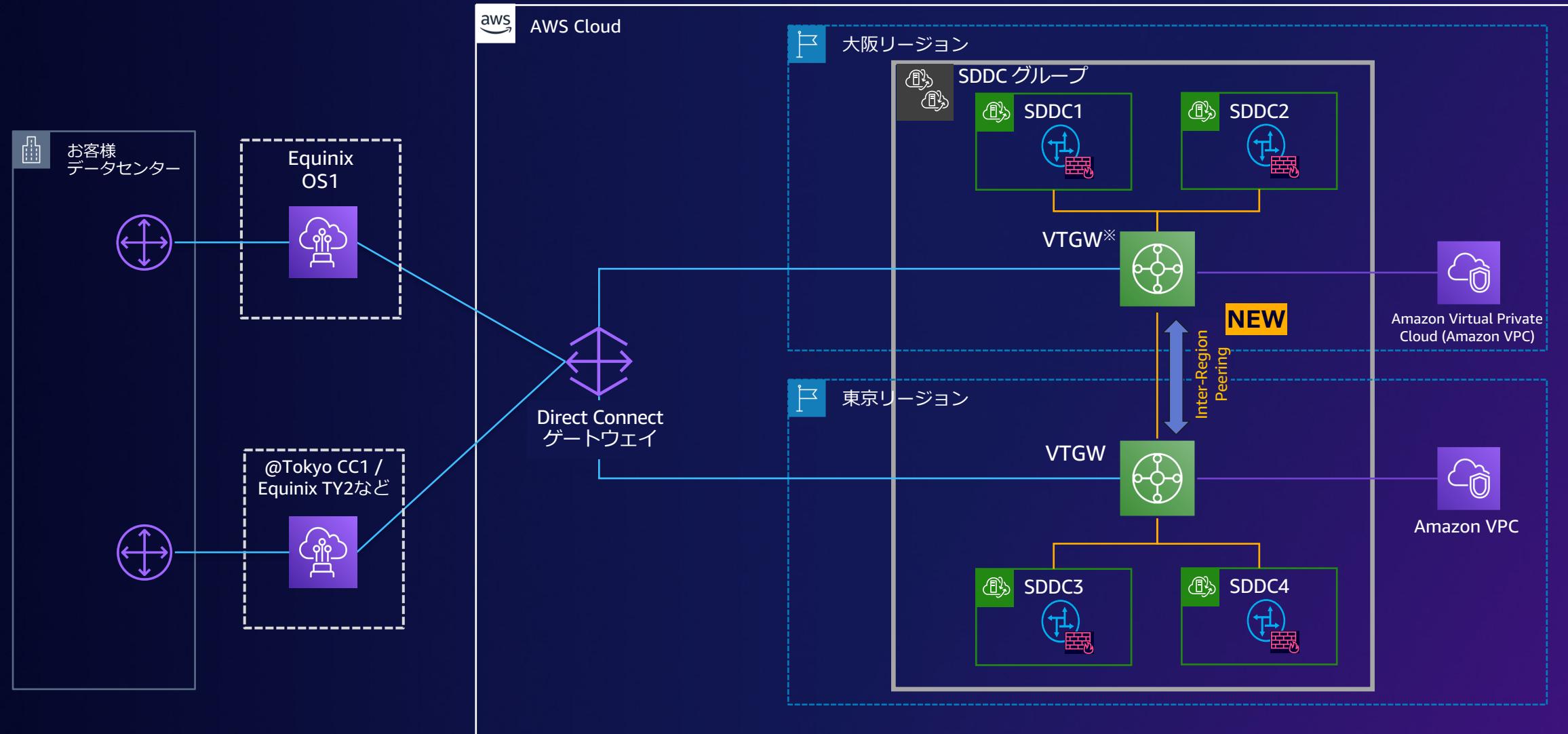


※ VTGW: VMware Transit Connect サービスにおける AWS Transit Gateway 機能の総称

※ VMware Transit Connect は収録日時点で大阪リージョンでは未サポート
最新のサポート状況:

<https://docs.vmware.com/jp/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started//GUID-19FB6A08-B1DA-4A6F-88A3-50ED445CFFCF.html>

大阪 / 東京リージョンのネットワーク接続構成パターン※



※ VTGW: VMware Transit Connect サービスにおける AWS Transit Gateway 機能の総称

※ VMware Transit Connect は収録日時点で大阪リージョンでは未サポート

最新のサポート状況:

<https://docs.vmware.com/jp/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started//GUID-19FB6A08-B1DA-4A6F-88A3-50ED445CFFCF.html>

リージョン間の SDDC の接続 (SDDC グループの作成)

The screenshot shows the VMware Cloud interface with the following details:

- Header:** VMware Cloud logo, user name (Masayuki T... AWS Partner...), and a bell icon.
- Left Sidebar:** Navigation menu with options: 開始 (Start), Inventory, サブスクリプション (Subscription), アクティビティ ログ (Activity Log), ツール (Tools), デベロッパー センター (Developer Center), and 通知設定 (Notification Settings).
- Top Bar:** Buttons for SDDC を作成 (Create SDDC) and アクション (Actions).
- Content Area:**
 - Section:** インベントリ (Inventory) with tabs: SDDC and SDDC グループ (selected).
 - SDDC Group List:** Two entries are shown:
 - 接続済み (Connected)
説明 (Description)
メンバー (Members): 1
詳細表示 (Details)
 - 接続済み (Connected)
説明 (Description)
メンバー (Members): 0
詳細表示 (Details)
 - Action Bar:** Buttons for 期間サブスクリプションを購入 (Purchase Period Subscription) and ユーザーを招待 (Invite User), and a large blue button labeled SDDC グループの作成 (Create SDDC Group) which is highlighted with a red box.
- Bottom Right:** Support icon (サポート) and a back arrow icon.

リージョン間の SDDC の接続 (SDDC グループの作成)

VMware Cloud

開始 Inventory サブスクリプション アクティビティ ログ ツール デベロッパー センター 通知設定

VMware Cloud

SDDC グループの作成

異なるリージョンのSDDCをグループに含める

1. 名前と説明
名前 : SDDC Group

2. メンバーシップ
グループに属する SDDC を選択

名前	SDDC ID	場所	バージョン	管理 CIDR
<input checked="" type="checkbox"/> SDDC N.California	4b442fe0-99d8-4d54-8507-	US West (N. California)	1.16.0.12	10.3.0.0/16
<input checked="" type="checkbox"/> SDDC Tokyo	6b95728a-6aea-49b0-bd5b-	Asia Pacific (Tokyo)	1.16.0.12	10.2.0.0/16
<input type="checkbox"/>	8ba64511-1b99-45ee-8735-	US East (N. Virginia)	1.16.0.11	10.2.0.0/16
2				

ページあたりのアイテム数 100 1 - 3 / 3 アイテム

次へ

3. 確認
グループの作成前に要件を確認して承認

ダーク

リージョン間の SDDC の接続 (SDDC グループの作成)

The screenshot shows the VMware Cloud interface with the following details:

- Header:** vmw VMware Cloud
- Top Bar:** Includes a bell icon, a question mark icon, and a dropdown menu.
- Left Sidebar:** Contains links for 開始 (Start), Inventory, Subscriptions, Activity Log, Tools, DevOps Center, and Notifications.
- Current View:** "SDDC グループの作成" (Create SDDC Group) screen.
- Form Fields:**
 - 1. 名前と説明:** Name: SDDC Group
 - 2. メンバーシップ:** Member: 2
 - 3. 確認:** Confirmation section asking to review before creation.
- Checklist:** A checkbox is checked, indicating "Groups with VMware Transit Connect will incur charges based on connection and data transfer." This checkbox is highlighted with a red border.
- Information Box:** A tooltip explains that a firewall rule will be created for the group's SDDC connections. It includes a "Details" link.
- Bottom Button:** A large blue button labeled "グループの作成" (Create Group) is highlighted with a red border.



リージョン間の SDDC の接続 (SDDC グループの作成)

The screenshot shows the VMware Cloud interface with the following details:

- Header:** VMware Cloud logo, navigation icons (Bell, Help, Search), and a dropdown menu.
- Left Sidebar:** Navigation links including 開始 (Start), Inventory, Subscriptions, Activity Log, Tools, Developer Center, and Notifications.
- Top Bar:** Buttons for SDDC を作成 (Create SDDC) and アクション (Actions).
- Section Header:** インベントリ (Inventory).
- Tab Selection:** SDDC グループ (SDDC Group) is selected.
- SDDC Group List:** A list of SDDC groups. The first item is highlighted with a red box and contains the following information:
 - SDDC Group:** SDDC Group
 - Status:** 接続済み (Connected)
 - Description:** 説明 (Description)
 - Members:** メンバー (2)
 - Details:** 詳細表示 (Details)
- Other Groups:** Two other SDDC groups are listed:
 - 説明 (Description) - Members: 1
 - 説明 (Description) - Members: 0
- Bottom Left:** ダーク (Dark) mode switch.



リージョン間の SDDC の接続 (SDDC グループの作成)

The screenshot shows the VMware Cloud interface with the following details:

- Header:** VMware Cloud logo, navigation icons (Bell, Help, etc.), and a dropdown menu.
- Left Sidebar:** Navigation links including 開始, Inventory, サブスクリプション, アクティビティ ログ, ツール, デベロッパー センター, and 通知設定.
- Current View:** SDDC Group page.
- Top Navigation:** サマリ, vCenter Server の関連付け, Direct Connect, 外部 VPC, 外部 TGW, ルーティング, and サポート (highlighted with a red box).
- Support Information:** グループ ID: 1ec92e54-1461-621a-88ee-1b1e18, 作成日: 2022年2月21日月曜日 7時09分48秒 GMT+00:00.
- VMware VTGW:** A table showing two entries:

TGW ID	場所
tgw-06c49b6b288	Asia Pacific (Tokyo)
tgw-0435b771917c	US West (N. California)

Two yellow arrows point to the TGW IDs in the first row.
- Bottom Left:** ダーク mode switch.

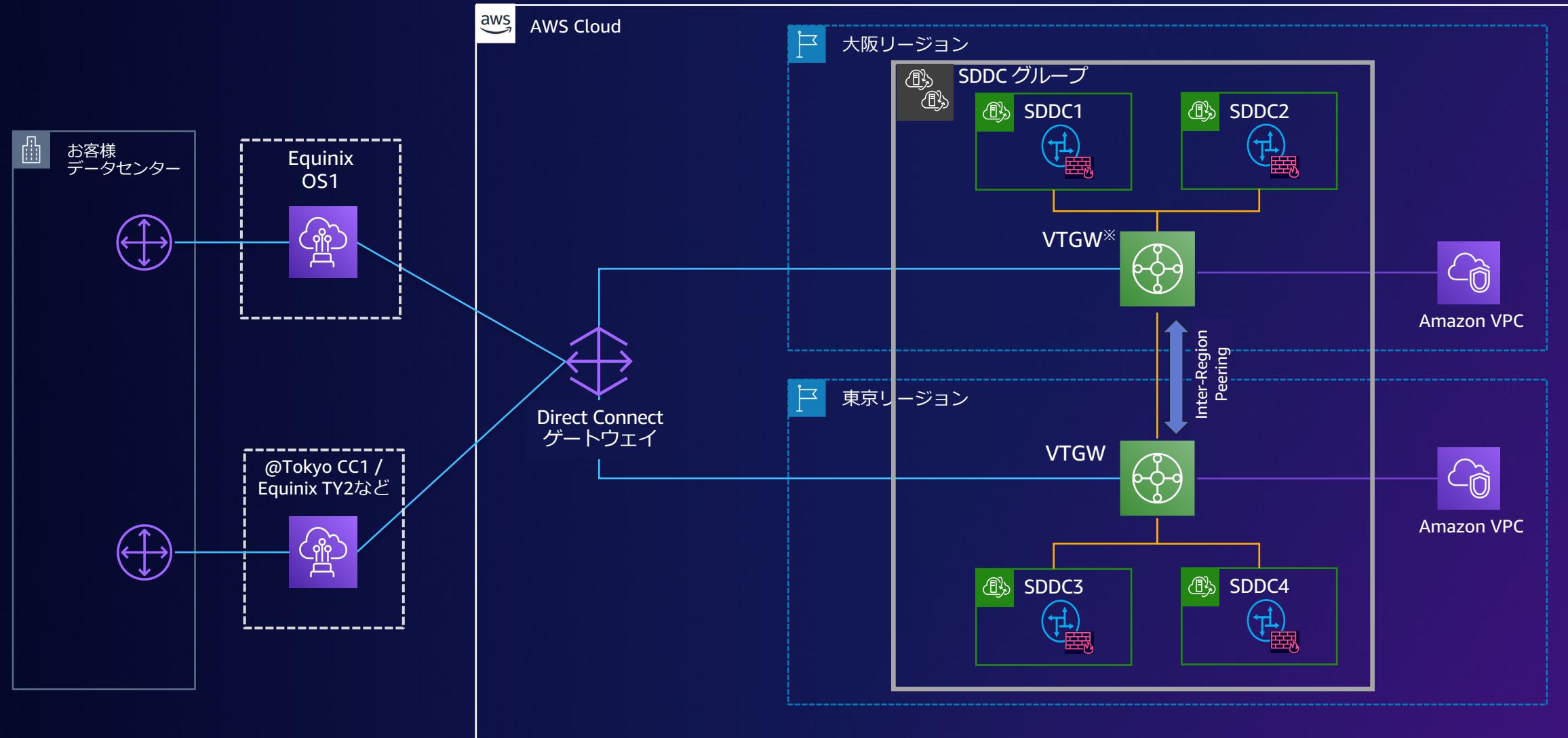


リージョン間の SDDC の接続 (SDDC グループの作成)

The screenshot shows the VMware Cloud interface with the following details:

- Left Sidebar:** Includes links for 開始 (Start), Inventory, Subscriptions, Activity Log, Tools, Developer Center, and Notifications.
- Top Bar:** Shows the VMware Cloud logo, a bell icon, a help icon, and a dropdown menu.
- SDDC Group Page:** The title is "SDDC Group". The tab "ルーティング" (Routing) is selected and highlighted with a red box.
- Route Table:** Members - Asia Pacific (Tokyo) is selected. The last update was on February 21, 2022, at 7:24:16 GMT+00:00.
- Table Headers:**宛先 (Destination), ターゲット (Target), 場所 (Location), and タイプ (Type).
- Table Data:** The table lists route entries for three subnets in Asia Pacific (Tokyo) and three in US West (N. California). All routes point to SDDC endpoints.
- Annotations:**
 - A blue box highlights the text "東京リージョンの SDDC の管理サブネット、及び 論理ネットワークのサブネット" (Management and logical subnets for the Tokyo region's SDDC).
 - A blue box highlights the text "N. California リージョンの SDDC の管理サブネット、及び 論理ネットワークのサブネット" (Management and logical subnets for the N. California region's SDDC).
- Page Footer:** Includes the AWS logo, copyright notice (© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.), and page navigation controls.

大阪 / 東京リージョンのネットワーク接続構成パターン※



※ VTGW: VMware Transit Connect サービスにおける AWS Transit Gateway 機能の総称

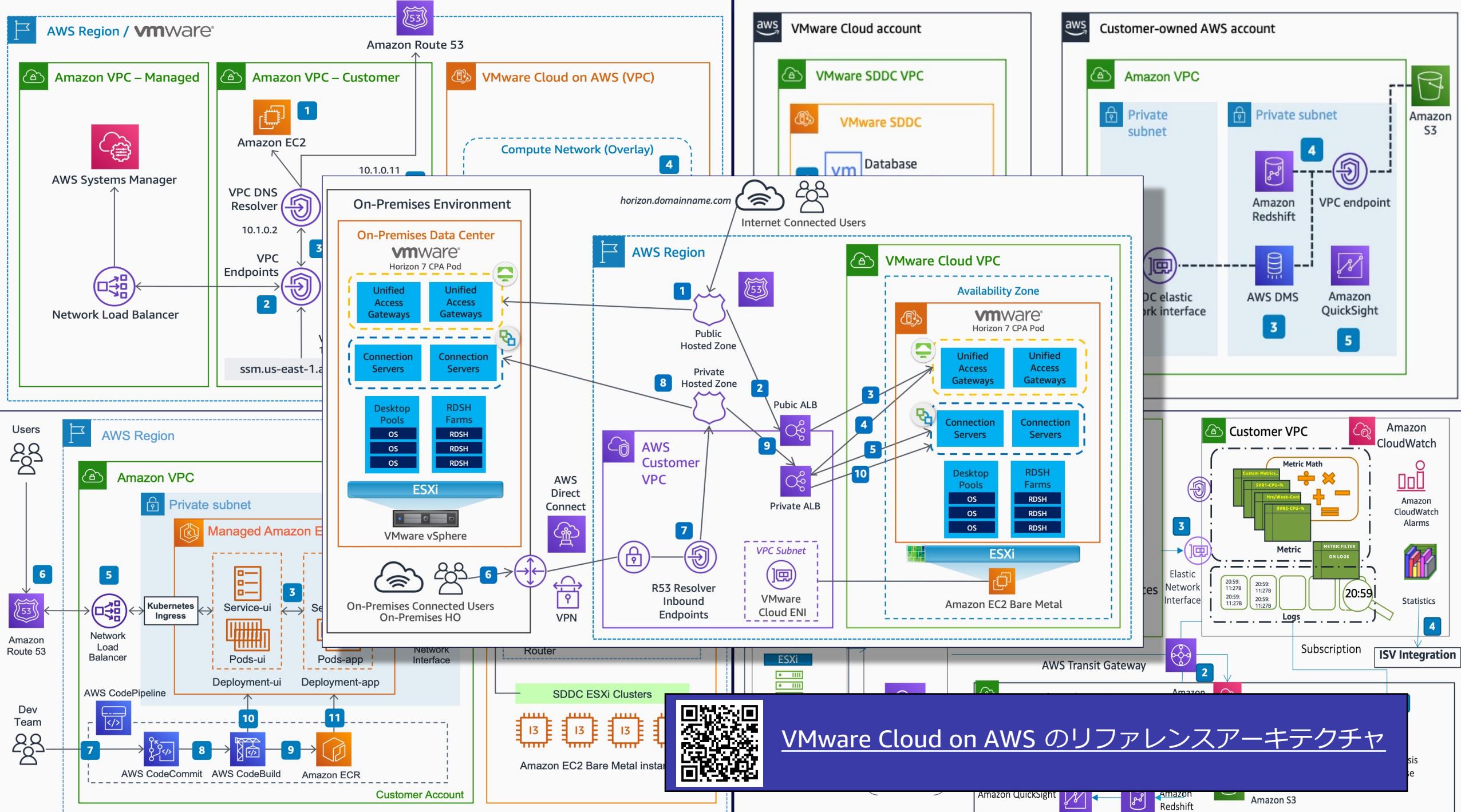
※ VMware Transit Connect は収録日時点で大阪リージョンでは未サポート

最新のサポート状況:

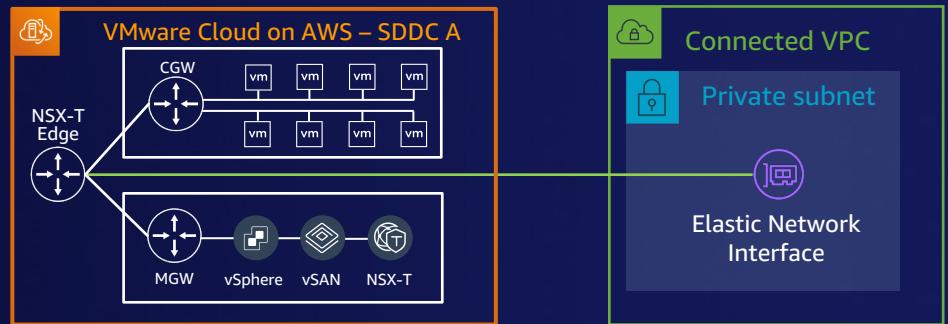
<https://docs.vmware.com/jp/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started//GUID-19FB6A08-B1DA-4A6F-88A3-50ED445CFFCF.html>

ネイティブ AWS サービスとの様々な 接続要件におけるネットワークデザイン

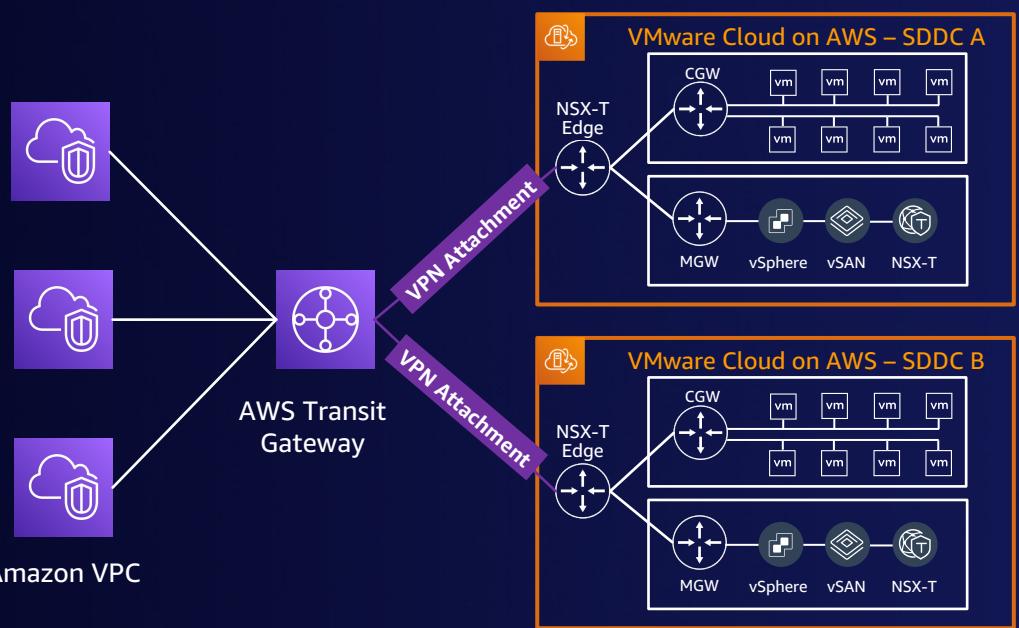




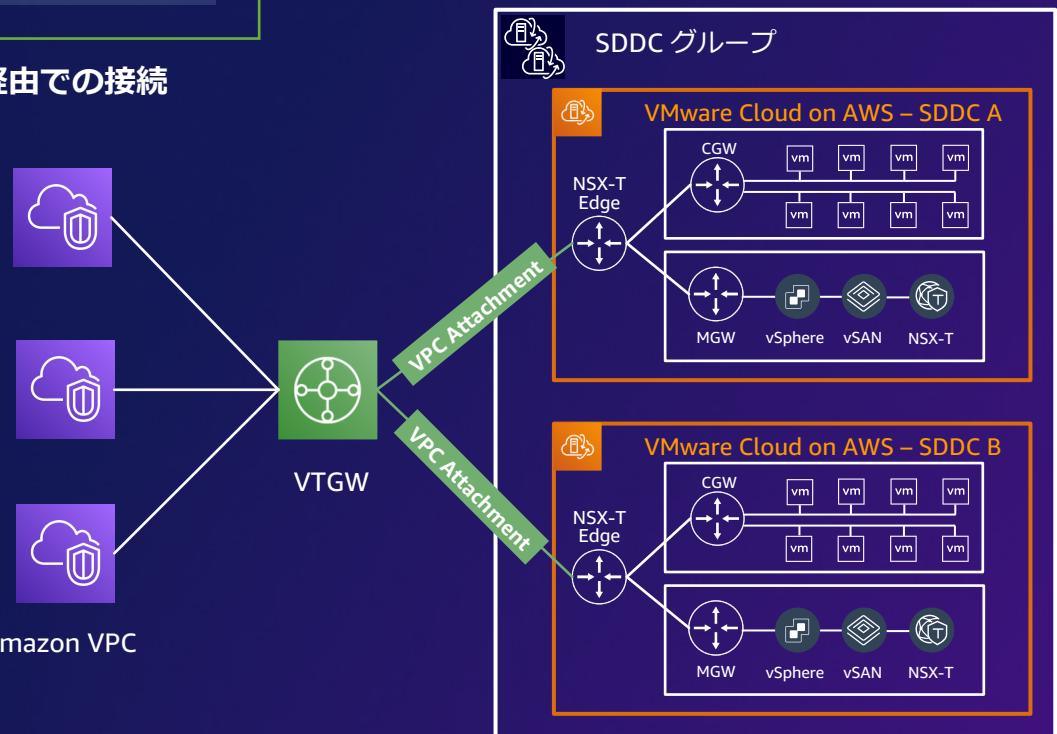
Amazon VPC との接続パターン



Elastic Network Interface (ENI) 経由での接続
(1:1 の接続)

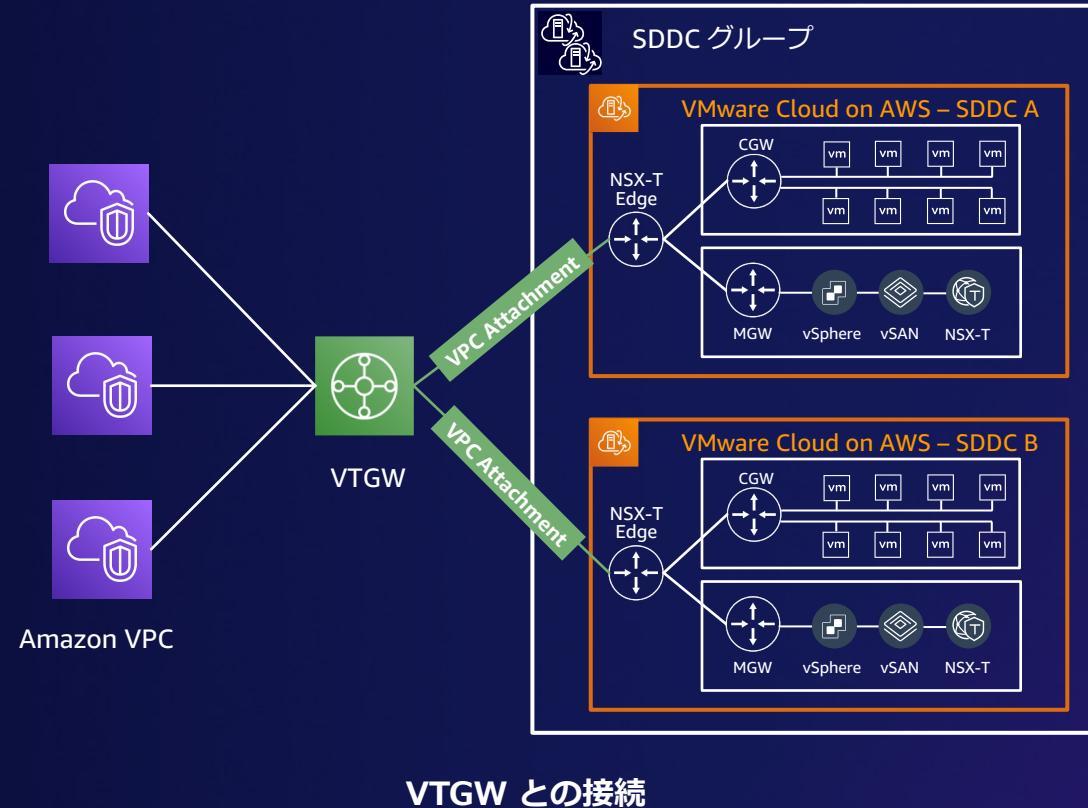


AWS Transit Gateway との接続 (注: VPN アタッチメント)

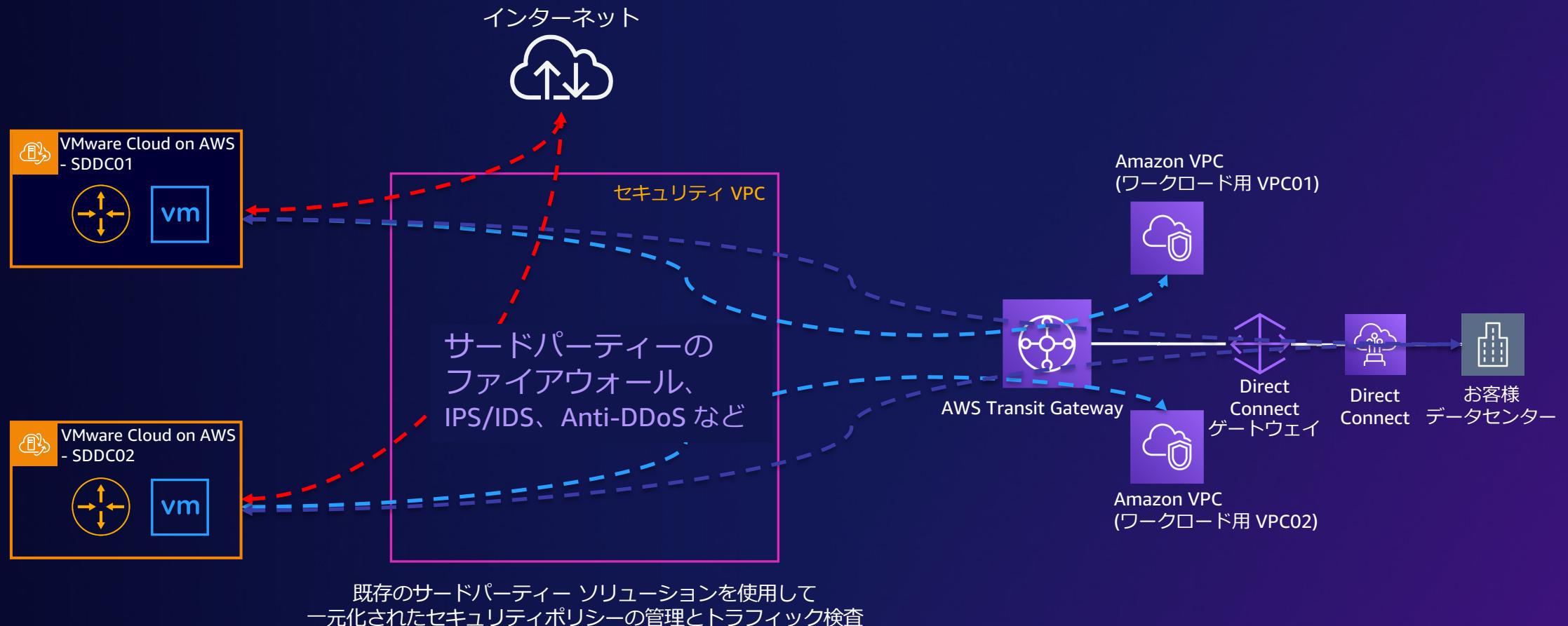


VTGW との接続

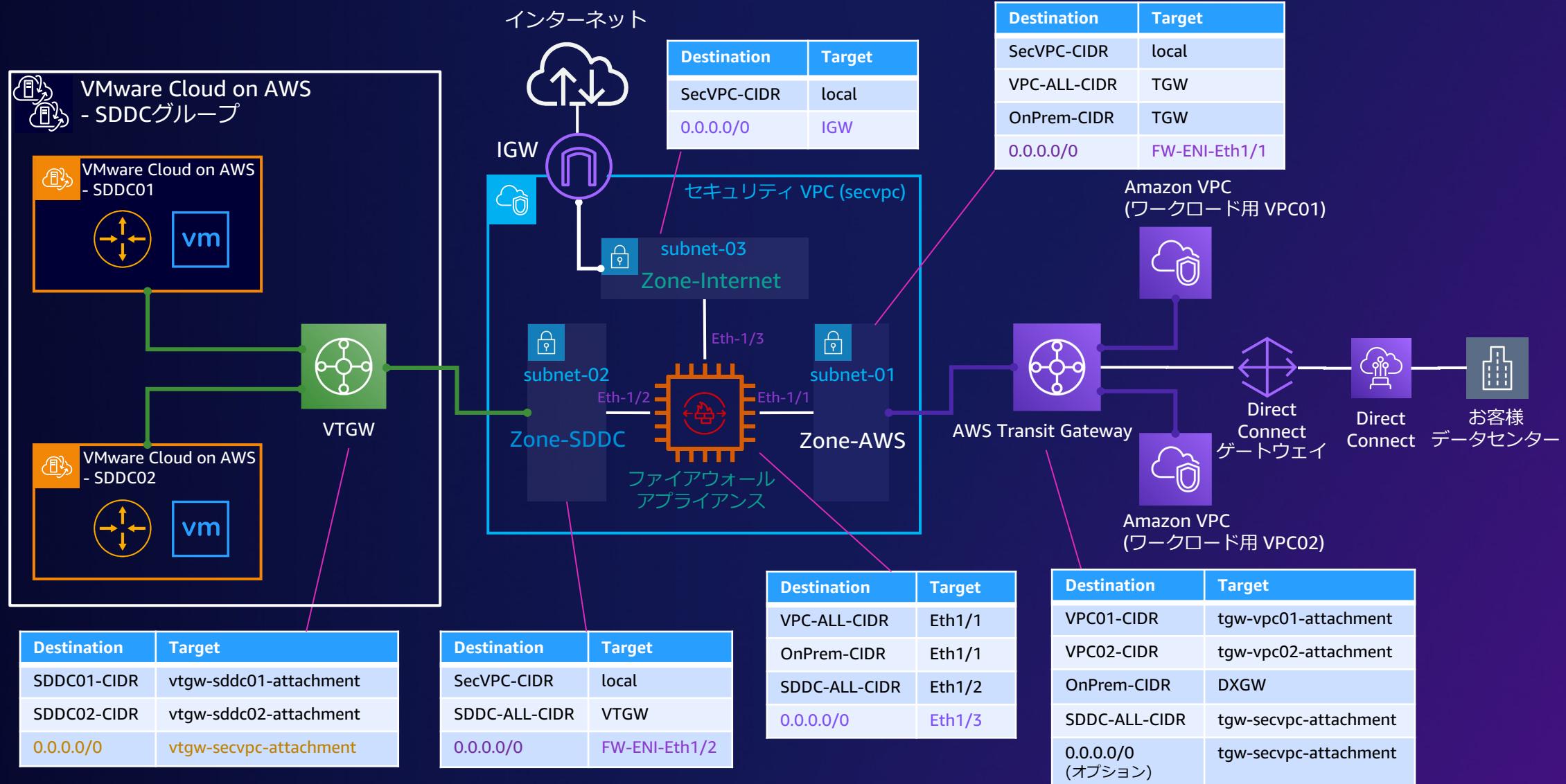
Amazon VPC との接続パターン



サードパーティのファイアウォールアライアンスとの連携



VTGW を使用したセキュリティ VPC アーキテクチャ



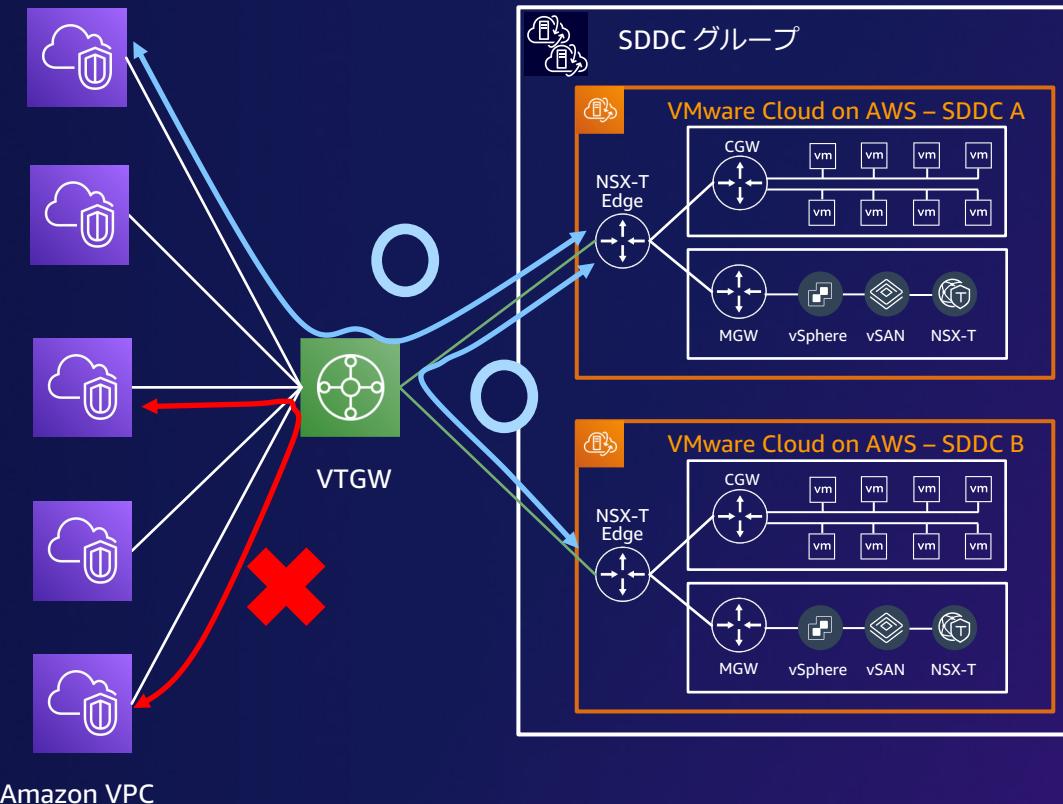
アーキテクチャのキーポイント

- VTGW に static のデフォルトルートを設定し、SDDC からのすべてのトラフィックがセキュリティ VPC を通過するように強制する。
- ファイアウォールに接続されているすべての ENI (管理インターフェイスを除く) で、「送信元/宛先チェック」を無効にする。
- SDDC からインターネット向けのアクセスを行うために、ファイアウォールで送信元ネットワークアドレス変換 (SNAT) ルールが必要です。このルールは、インターネットに転送される前にパブリック EIP にマッピングされます。
- vCenter / HCX などの SDDC 管理コンポーネントへのアクセスもセキュリティ VPC を通過するように強制されます。このアーキテクチャにより、誤ってインターネットに公開されるのを防ぐことができます。

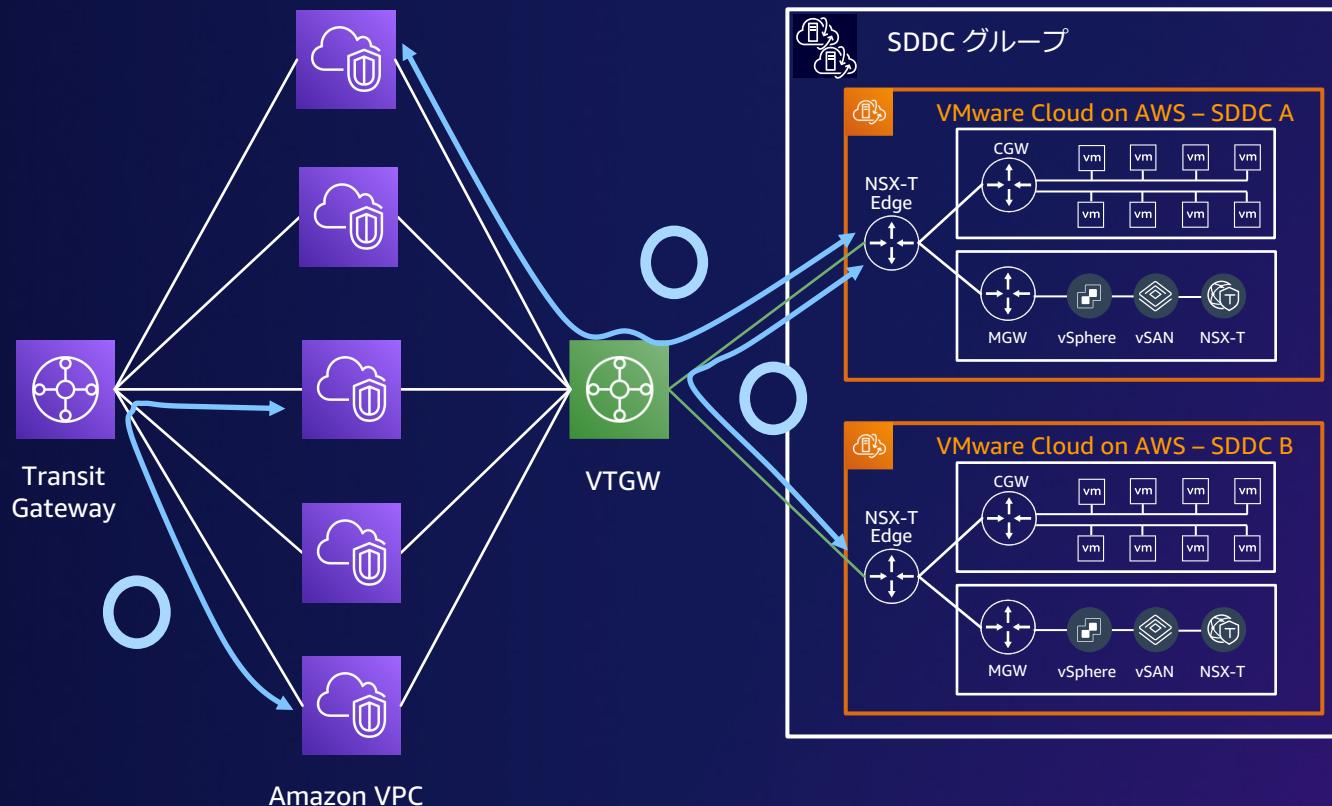
The image displays three screenshots from the AWS CloudFormation console illustrating the architecture's key points:

- Top Screenshot:** Shows the "Transit Gateway Attachment" page. A route for "0.0.0.0/0" is highlighted with a red box, indicating it强制所有 traffic through the security VPC.
- Middle Screenshot:** Shows the "Details" page for a Network Interface (eni-0700200ce92f). The "Source/dest. check" field is highlighted with a red box and a red arrow, showing it is set to "False".
- Bottom Screenshot:** Shows the "Summary" page for an Elastic IP (eipalloc-0ee1ed63b58600b24). A red box highlights the "Allocated IPv4 address" and "Type" fields. A red arrow points from the "Allocation ID" field to the "Private IP address" field, which is also highlighted with a red box, illustrating how a public IP is mapped to a private IP on the interface.

VTGW 経由のトラフィック

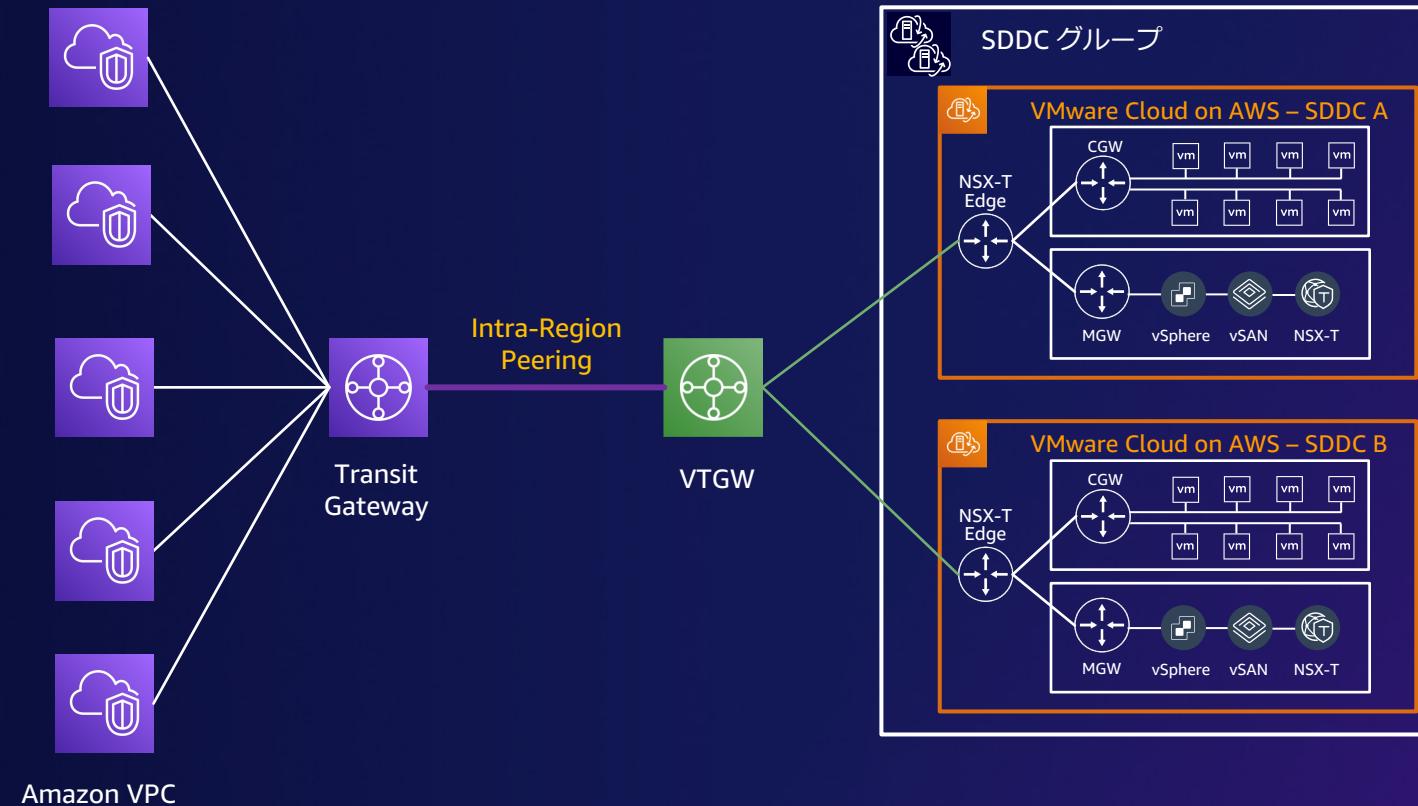


VTGW 経由のトラフィック



Intra-Region Peering for VMware Cloud on AWS

VTGW と AWS Transit Gateway のリージョン内ピアリングにより管理と接続を簡素化



Intra-Region Peering for VMware Cloud on AWS

VMware Cloud

VMware Cloud

Matayuki Toyoda
AWS - VMware Dev...

アクション

開始

Inventory

サブスクリプション

アクティビティ ログ

ツール

デベロッパー センター

通知設定

US-EAST

サマリ vCenter

TGW の追加

01519

外観 TGW の追加

外部トランジット ゲートウェイを SDDC グループに接続するには、次の情報を指定します。

AWS アカウント ID [i](#)

tgw-Oe 657622566485

TGW ID [i](#)

TGW の場所 [i](#)

US East (N. Virginia)

VMC on AWS リージョン [i](#)

US East (N. Virginia)

ルート [i](#)

10.1.1.0/24

SDDCと同じ
リージョンが指定可能

プリフィックスは、カンマ、スペースまたは改行で区切ることができます

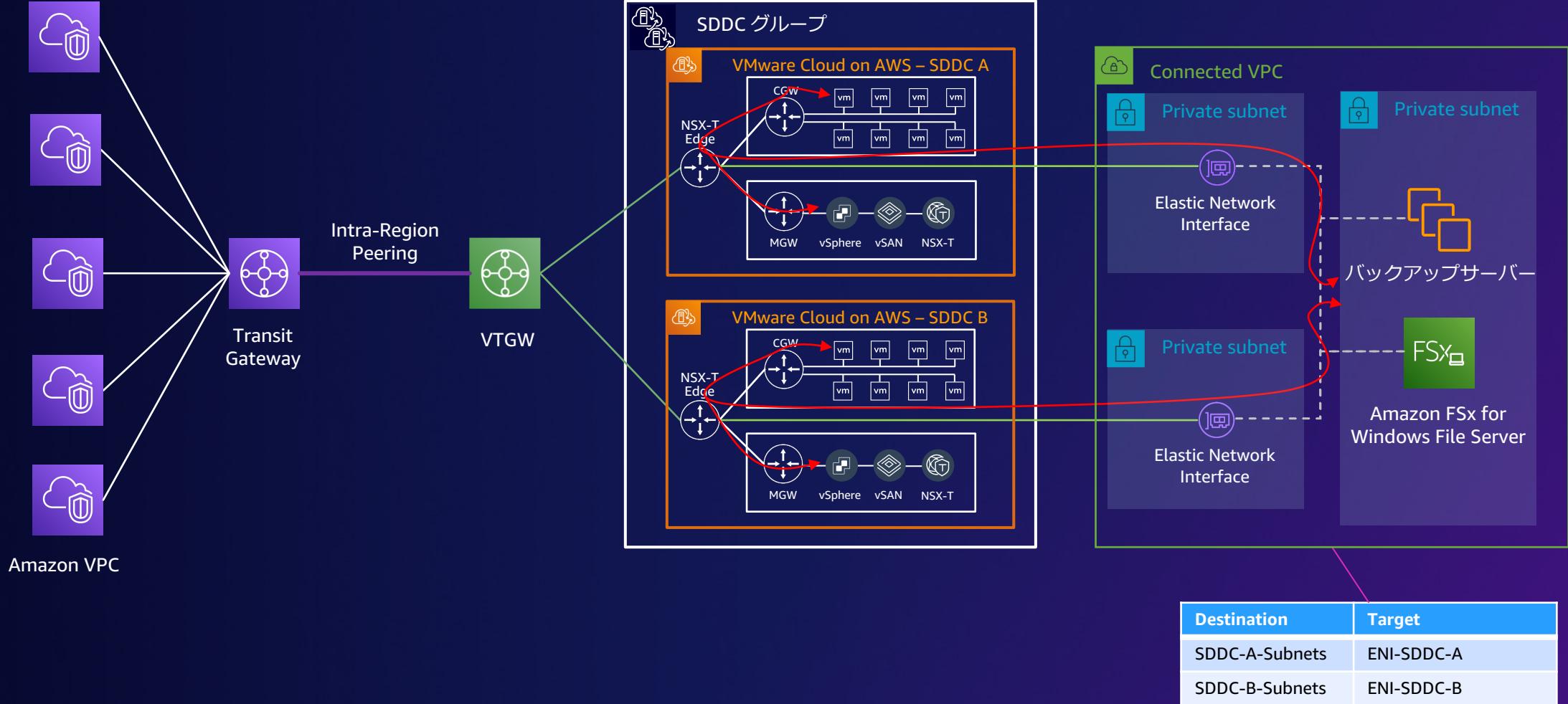
合計: 1、無効: 0

キャンセル

追加

The screenshot shows the VMware Cloud on AWS interface with a modal dialog titled "External TGW の追加". The dialog is used to connect an external Transit Gateway (TGW) to a Service Delivery Data Center (SDDC) group. It requires specifying the AWS Account ID (657622566485), TGW ID (tgw-Oe), and the location (US East (N. Virginia)). A note on the right side of the dialog states "SDDCと同じリージョンが指定可能" (The same region can be specified for SDDC). The "TGW の場所" (Location) and "VMC on AWS リージョン" (Region) dropdowns are highlighted with a red box. Below the dropdowns, there is a "ルート" (Route) section containing a single entry: "10.1.1.0/24". At the bottom of the dialog, there are "キャンセル" (Cancel) and "追加" (Add) buttons.

VTGW と ENI 接続を組み合わせた接続パターン



アーキテクチャのキーポイント

- SDDC 間で IP アドレスの重複がないようネットワークセグメントの設計を行う。
- ENI が作成されるサブネットには SDDC 毎に 17 個の ENI が作成される。
SDDC 毎に専用の /26 CIDR ブロックの用意が推奨
- ENI が作成される Connected VPC では、メインルートテーブルを利用する。
(カスタムルートテーブルの使用はサポートされません)

The screenshot displays two main sections of the VMware Cloud on AWS interface:

- ネットワークインターフェイス (34) 情報**: A table listing 34 network interfaces. The columns include Name, ネットワークインターフェイス ID, サブネット ID, VPC ID, and アベイラビリティゾーン. Most entries have "vpc-0f79fe4622af" as the VPC ID and "ap-northeast-1" as the availability zone.
- ルートテーブル (1) 情報**: A table showing a single route table named "rtb-03095870e775...". It has one entry for "subnet-0e7380c039a..." with "vpc-0f79fe4622af" as the VPC ID. The "メイン" (Main) column is highlighted with a red box and contains the value "はい" (Yes).
- ルート (5)**: A detailed view of the routes in the route table. The table includes columns for 送信先 (Destination), ターゲット (Target), ステータス (Status), and 伝播済み (Propagated). The first four rows (with destinations 192.168.1.0/24, 10.2.0.0/16, 172.16.1.0/24, and 10.3.0.0/16) are highlighted with red boxes.

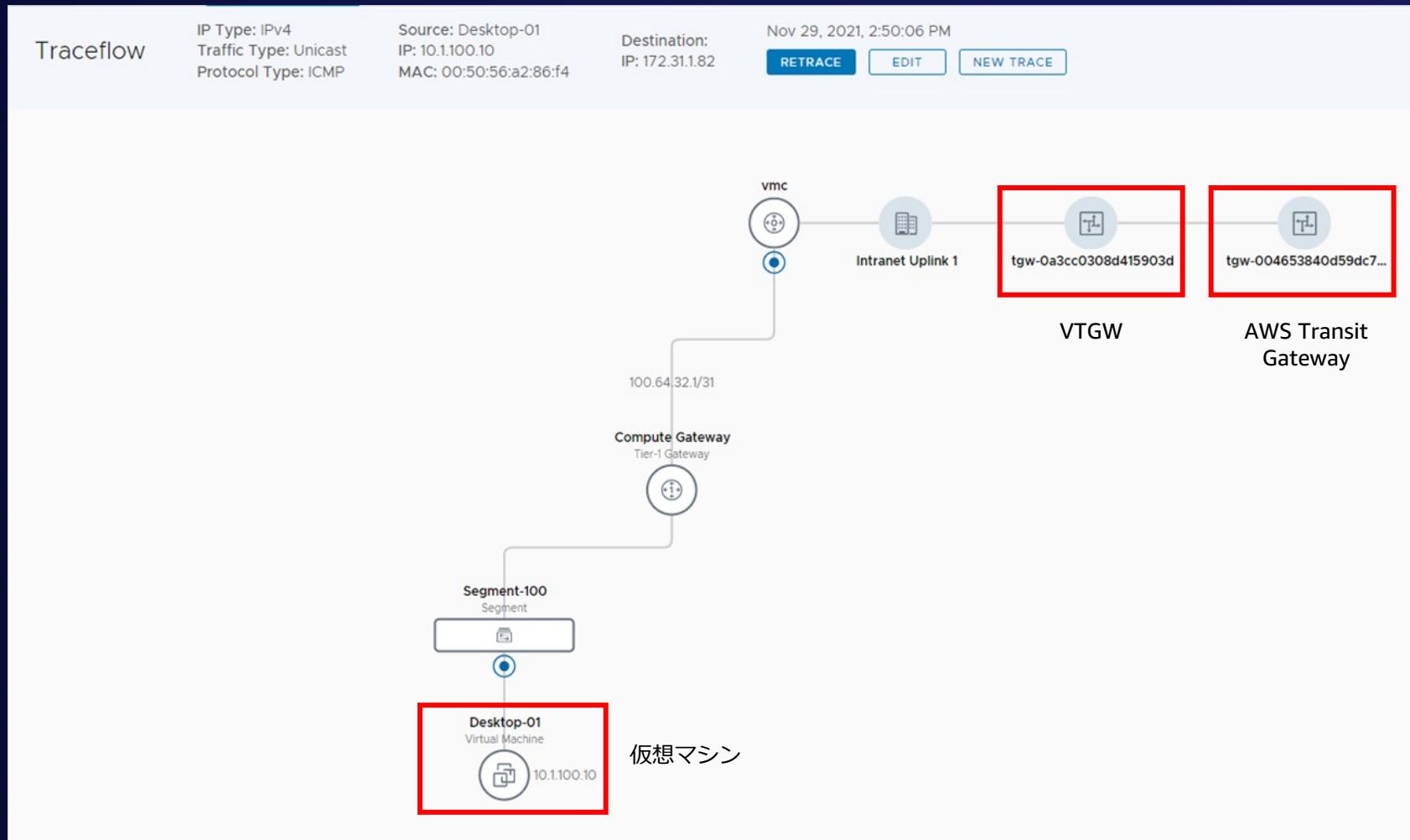
Software-Defined Data Center (SDDC) の展開と管理:

<https://docs.vmware.com/jp/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-BC0EC6C5-9283-4679-91F8-87AADFB9E116.html>

NEW

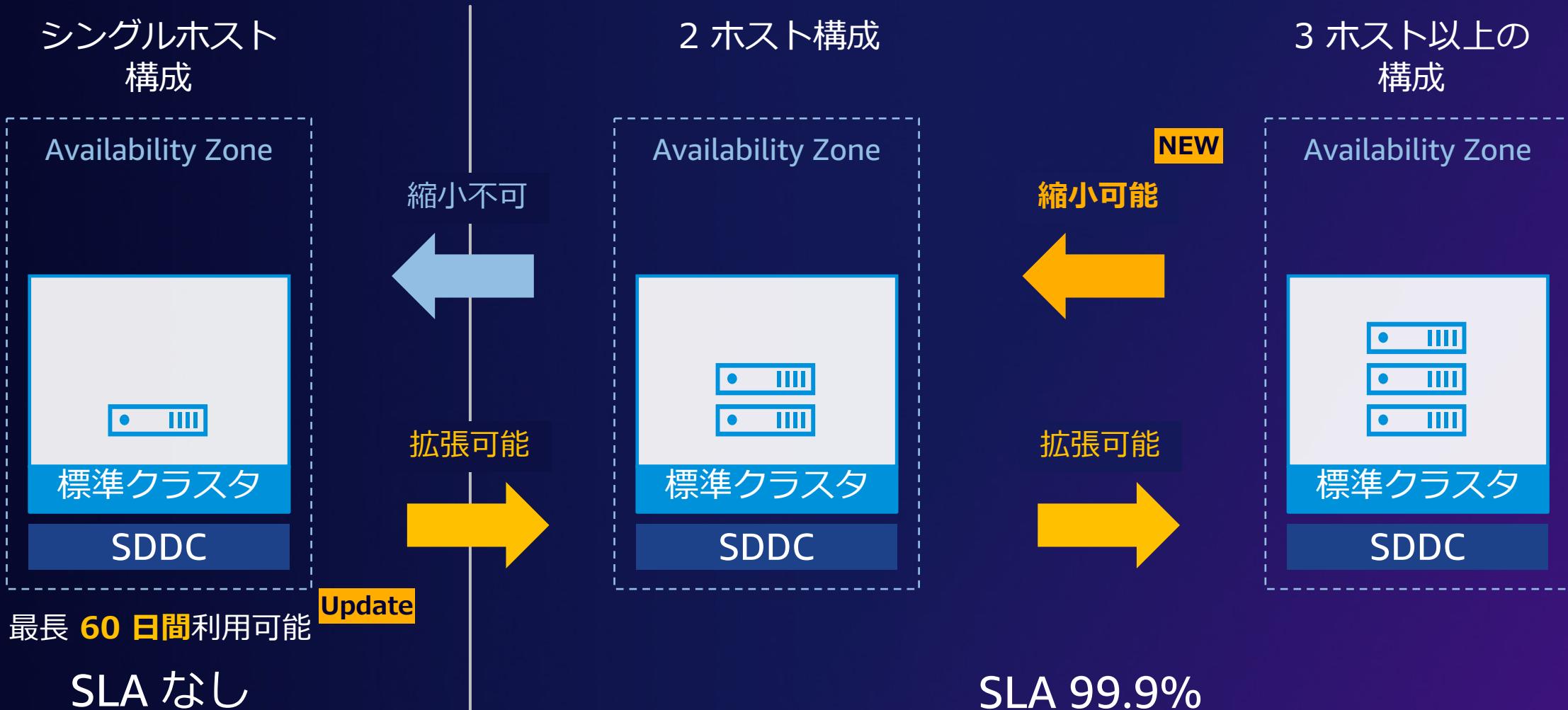
NSX Traceflow

NSX Manager UI で利用可能な拡張トラブルシューティング

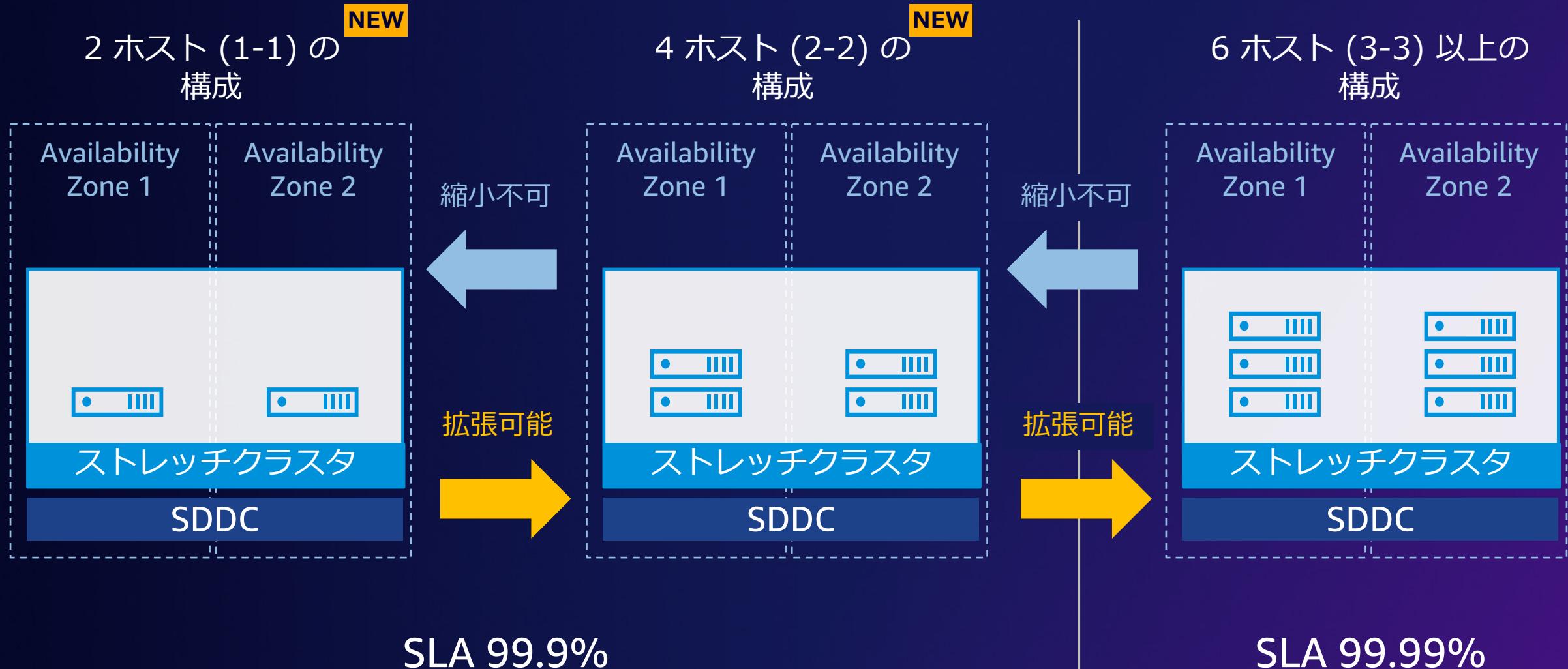


その他最新アップデート

標準クラスタのアップデート

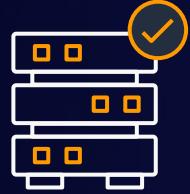


ストレッチクラスタの柔軟なホスト構成



VMware Cloud on AWS Outposts

- VMware Cloud on AWS をオンプレミスに導入



AWS のデータセンターと同じ
AWS が設計した
インフラストラクチャ
(AWS Nitro システム
上に構築)



VMware と AWS による
フルマネージドサービス

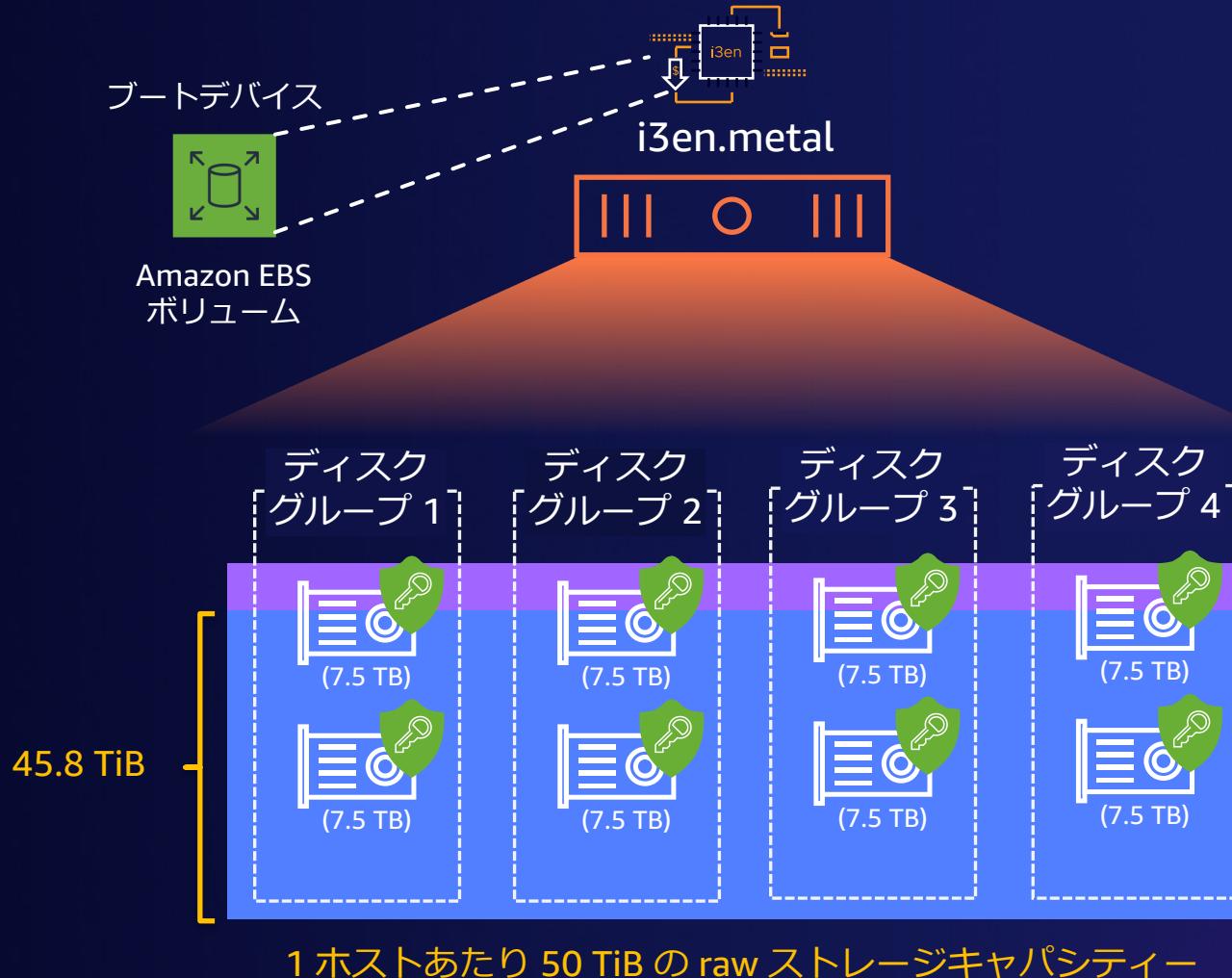


vCenter を使用した
操作の一貫性
同じ API とツール



VMware Cloud on AWS Outposts

ラック内のコンピューティングとストレージ



CPU

48 の物理 CPU コア

96 論理コア (ハイパースレッディング有効)

Memory

768 GB RAM

■ キャッシュ階層

■ キャパシティー階層

最小 3 ノード ~ 8 ノードまで選択可能
(上記に加えて、修復 / EDRS スケールアウト / LCM 用の
Dark Capacity が付属)

VMware Cloud on AWS Outposts:

<https://aws.amazon.com/jp/vmware/outposts/>



Amazon FSx for NetApp ONTAP 統合（プレビュー）

- Amazon FSx for NetApp ONTAP を NFS データストアとして利用が可能に
- SDDC クラスターに依存しないストレージ環境の拡張
- ONTAP のデータ管理機能の活用
- ストレージ容量を多く必要とする環境での大幅なコスト削減を実現

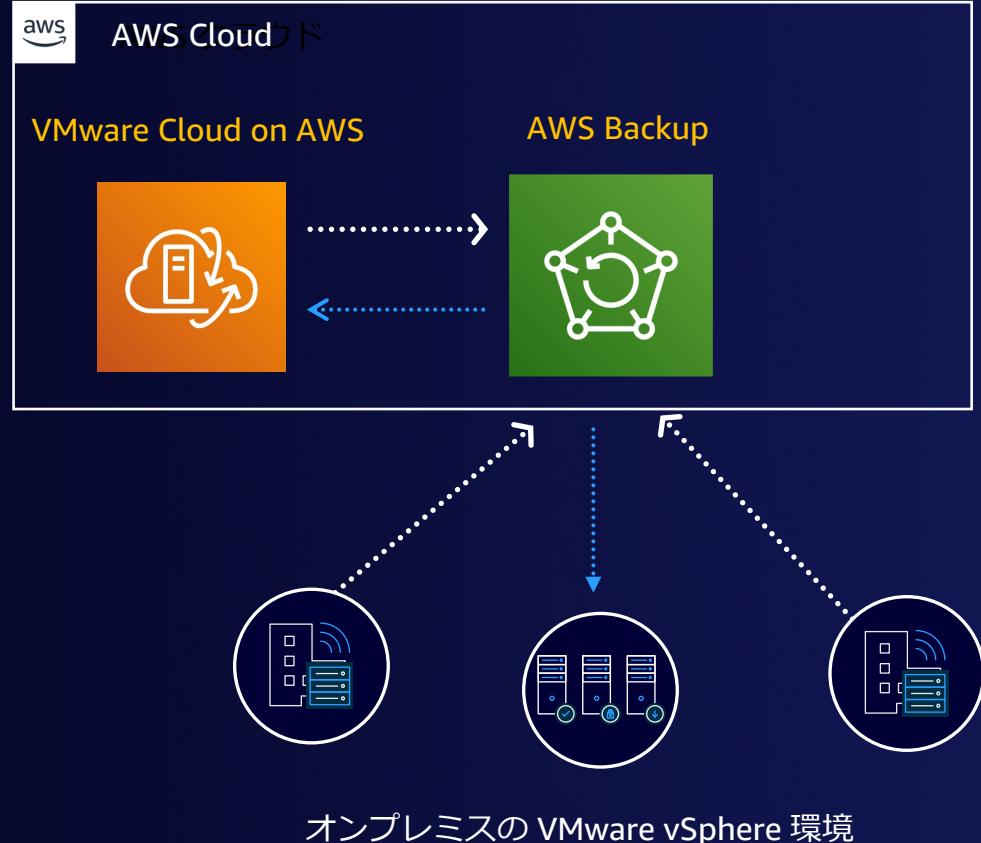


VMware Cloud on AWS

Amazon FSx for NetApp
ONTAP

AWS Backup の VMware Cloud on AWS サポート

NEW



- **VMware Cloud on AWS** とオンプレミスの VMware 環境※ のバックアップ、リストアをサポート
- VMware Tools のファイルシステム静止を使用し、アプリケーションの整合性のある VM のバックアップを作成
 - ファイルシステム静止と互換性がない場合は、クラッシュ整合性のあるバックアップを作成
- バックアップ ゲートウェイ仮想アプライアンスをクラスタ内に OVF テンプレートを使用してデプロイ

※ VMware ESXi 6.7 および 7.0 をサポート

まとめ

- ・ 大阪リージョンでも VMware Cloud on AWS の提供が開始され活用シーンが増えている
- ・ 大阪・東京リージョンのネットワーク接続構成
 - VTGW 利用により、Direct Connect ゲートウェイ経由でオンプレミスから大阪リージョンと接続が可能
 - リージョン間の SDDC の接続もコンソールから容易に設定が可能
- ・ VMware Cloud on AWS を活用した災害対策 (VMware Cloud Disaster Recovery)
 - クラウドのメリットを最大限に活かしたコストの最適化が可能
 - RTO の短縮化を目的にした、必要最小限のリソースを確保しておくオプションも選択可能
- ・ ネイティブ AWS サービスとの接続のネットワークデザイン
 - VTGW、AWS Transit Gateway を組み合わせる
 - ENI 接続も組み合わせる事でアウトバウンドトラフィックも抑えた接続が可能
- ・ よりコストを抑えてフレキシブルに利用できるアップデートを継続的にリリース

AWS のイノベーションと経験



スケール



信頼性



セキュリティ



アジャイル
アプリケーション開発



パフォーマンス



高度なデータ分析

10 年以上

数千の移行とモダナイゼーションプロジェクト実績

追加のリソース



[VMware Cloud on AWS](#)

VMware Cloud on AWS 製品ページ



[VMware Cloud on AWS リソース](#)

VMware Cloud on AWS のリファレンスアーキテクチャ、動画など



[Amazon Web Services ブログ](#)

VMware Cloud on AWS 関連のブログ（日本語）



[SDDC Deployment and Best Practices Guide](#)

VMware Cloud on AWS のリファレンス デプロイメントガイド

Thank you!

Masayuki Toyoda

 masayuki-toyoda



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.