

VMware Cloud on AWS の ネットワークおよびセキュリティ

2023 年 7 月 14 日

SDDC バージョン 1.22

VMware Cloud on AWS

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴィエムウェア株式会社
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

Copyright © 2017-2023 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

VMware Cloud on AWS のネットワークとセキュリティについて 5

1 NSX ネットワークの概念 6

NSX でサポートされる機能 13

2 [ネットワークとセキュリティ] ダッシュボードの使用 16

3 NSX を使用した VMware Cloud on AWS のネットワークとセキュリティの構成 18

組織のメンバーへの NSX サービス ロールの割り当て 19

NSX Manager による SDDC ネットワーク管理 20

NSX Manager を開く 22

LDAP ID ソースからの NSX ロールの割り当て 25

SDDC とオンプレミス データセンターの間の AWS Direct Connect の設定 26

AWS Direct Connect への接続のセットアップ 27

SDDC の管理およびコンピューティング ネットワーク トラフィック用のプライベート仮想インターフェイスに対する Direct Connect の構成 28

AWS サービスにアクセスするためのパブリック仮想インターフェイスに対する Direct Connect の構成 33

Direct Connect の MTU の指定 33

SDDC とオンプレミス データセンターの間の VPN 接続の設定 34

ルートベースの VPN の作成 35

ポリシー ベース VPN の作成 40

IPsec VPN の証明書ベースの認証の構成 45

レイヤー 2 VPN および拡張ネットワーク セグメントの構成 46

VPN トンネルのステータスと統計情報の表示 50

IPsec VPN 設定リファレンス 51

VMware Cloud on AWS における VPN の問題のトラブルシューティング 53

管理ゲートウェイのネットワークおよびセキュリティの構成 55

vCenter Server の FQDN 解決アドレスの設定 55

HCX FQDN 解決アドレスの設定 56

管理ゲートウェイのファイアウォール ルールの追加または変更 56

コンピューティング ゲートウェイのネットワークおよびセキュリティを構成 60

ネットワーク セグメントの作成または変更 61

コンピューティング ゲートウェイのファイアウォール ルールの追加または変更 67

分散ファイアウォール ルールの追加または変更 70

DNS サービスの構成 75

VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理 77

VMware Transit Connect を通じて学習およびアドバタイズされたルートの表示 97

アップリンクに関する統計情報の表示と設定の管理	98
VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加	99
Tier-1 ゲートウェイへの VPN の接続	102
SDDC ネットワークでの IPv6 の有効化と使用	106
トラフィック グループを使用したマルチエッジ SDDC の構成	108
接続中の Amazon VPC の AWS 管理対象プリフィックス リスト モードの有効化	112
アップリンクへのルートの集約とフィルタリング	114
インベントリ グループの操作	116
コンテキスト プロファイルについて	117
ワークロード接続の管理	117
コンピューティング ネットワーク セグメントへの仮想マシンの接続またはワークロード仮想マシンの分離	117
パブリック IP アドレスの要求またはリリース	118
NAT ルールの作成または変更	119
コンピューティング ネットワークと管理ネットワーク間のトラフィックを管理するためのファイアウォール ルールの作成	123
4 監視およびトラブルシューティング機能の設定	125
IPFIX の設定	125
ポート ミラーリングの設定	126
接続中の VPC 情報の表示と接続中の VPC に関する問題のトラブルシューティング	127
5 NSX イベントとアラームの操作	130
VMware Cloud on AWS の NSX アラーム カタログ	131
6 NSX Advanced Firewall 機能について	133

VMware Cloud on AWS のネットワークとセキュリティについて

『VMware Cloud on AWS のネットワークおよびセキュリティ』ガイドには、VMware Cloud on AWS の NSX ネットワークおよびセキュリティの設定に関する情報が記載されています。

対象読者

本書は、VMware Cloud on AWS を使用して、ワークロードをオンプレミスに移行してクラウドで安全に実行するためのネットワークおよびセキュリティ インフラストラクチャを備えた SDDC を構築する方を対象としています。本書は、オンプレミス環境で vSphere を使用したことがあり、NSX または別のネットワーク ソリューションを使用した IP ネットワークの基礎に精通している方を対象としています。vSphere や Amazon Web Services について熟知している必要はありません。

NSX ネットワークの概念

1

VMware Cloud on AWS では、NSX を使用して SDDC ネットワークを作成および管理します。NSX は、クラウドネイティブのアプリケーション環境を構築する俊敏性に優れた Software-Defined Infrastructure を提供します。

『VMware Cloud on AWS Networking and Security』ガイドでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用して SDDC ネットワークを管理する方法について説明します。NSX Manager Web ユーザー インターフェイスを使用してこれらのネットワークを管理することもできます。SDDC バージョン 1.22 以降では、[2 章 \[ネットワークとセキュリティ\] ダッシュボードの使用](#)を試すことができます。これにより、SDDC ネットワークの表示が簡素化され、関連する NSX Manager の機能へのリンクも提供されます。

NSX Manager は、[ネットワークとセキュリティ] タブにある機能のスーパーセットをサポートしています。NSX Manager の使い方の詳細については、『NSX Data Center 管理ガイド』の [NSX Manager](#) を参照してください。VMware Cloud on AWS SDDC 内の NSX Manager には、インターネットに接続できる任意のブラウザから接続可能なパブリック IP アドレスでアクセスできます。これには、VPN または AWS Direct Connect を介して内部ネットワークからアクセスすることもできます。詳細については、[NSX Manager を開く](#)を参照してください。

NSX Manager Web ユーザー インターフェイスのレイアウトとナビゲーションは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブと似ています。どちらのツールを使用しても、このドキュメントのほとんどの手順を完了できます。[ネットワークとセキュリティ] タブには、VPN、NAT、DHCP などの NSX の [ネットワーク] 機能とファイアウォールなどの NSX の [セキュリティ] 機能が組み合わされています。手順で NSX Manager を使用する必要がある場合は、該当する手順の前提条件に、その旨を注記しています。

SDDC ネットワーク トポロジー

SDDC を作成すると、管理ネットワークが含まれます。単一ホストの評価版 SDDC には、小規模なコンピューティングネットワークも含まれます。SDDC を作成するときに、ユーザーが管理ネットワーク CIDR ブロックを指定します。SDDC を作成した後、管理ネットワーク CIDR ブロックは変更できません。詳細については、[VMC コンソールからの SDDC の展開](#)を参照してください。管理ネットワークには 2 つのサブネットがあります。

アプライアンスのサブネット

このサブネットは、vCenter Server、NSX、および SDDC 内の HCX アプライアンスによって使用されます。SRM などのアプライアンススペースのサービスを SDDC に追加すると、このサブネットにも接続されます。

インフラストラクチャ サブネット

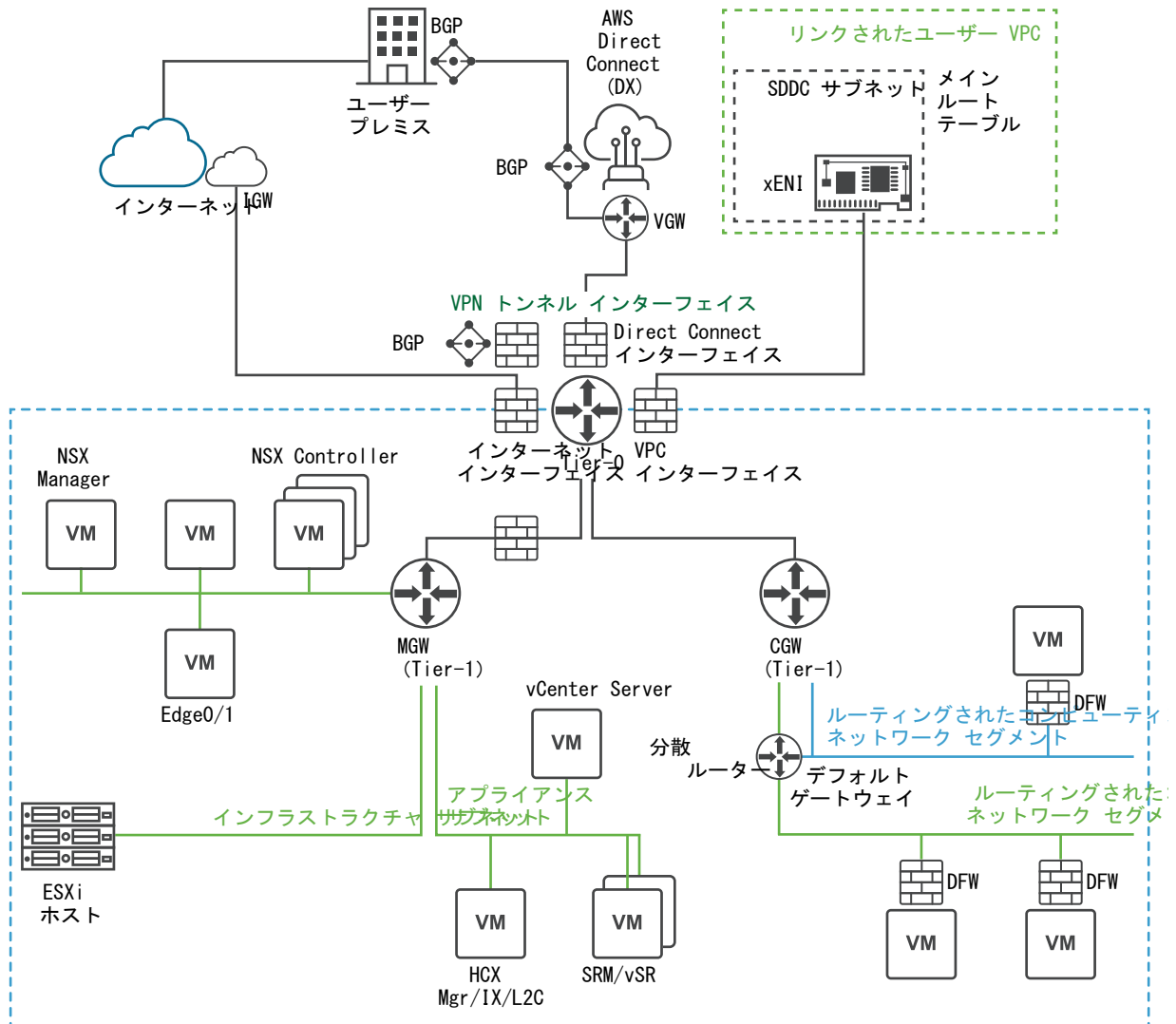
このサブネットは、SDDC 内の ESXi ホストによって使用されます。

コンピューティング ネットワークには、ワークロード仮想マシンに対応する任意の数の論理セグメントが含まれています。論理セグメントの現在の制限については、[VMware 構成の上限](#)を参照してください。単一ホストによる SDDC スタータ構成では、1つのルーティング セグメントを持つコンピューティング ネットワークを作成します。これよりも多くのホストを含む SDDC 構成では、ニーズを満たすだけのコンピューティング ネットワーク セグメントを作成する必要があります。適用される制限については、[VMware 構成の上限](#)を参照してください。

SDDC ネットワークには、次の 2 つの概念的階層があります。

- Tier 0 は、North-South トラフィック（SDDC に出入りするトラフィック、または管理ゲートウェイとコンピューティング ゲートウェイ間のトラフィック）を処理します。デフォルト構成では、各 SDDC に 1 つの Tier-0 ルーターがあります。SDDC が SDDC グループのメンバーである場合は、SDDC を再構成して、SDDC グループ トラフィックを処理する Tier-0 ルーターを追加できます。[トラフィック グループを使用した マルチエッジ SDDC の構成](#)を参照してください。
- Tier 1 は East-West トラフィック（SDDC 内のルーティング ネットワーク セグメント間のトラフィック）を処理します。デフォルト構成では、各 SDDC に 1 つの Tier-1 ルーターがあります。必要に応じて、追加の Tier-1 ゲートウェイを作成し、構成することができます。[VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加](#)を参照してください。

図 1-1. SDDC ネットワーク トポロジー



NSX Edge アプライアンス

デフォルトの NSX Edge アプライアンスは、アクティブ/スタンバイ モードで実行される仮想マシンのペアとして実装されます。このアプライアンスは、デフォルトの Tier 0 ルーターと Tier 1 ルーターを実行するプラットフォームであり、あわせて IPsec VPN 接続と BGP ルーティング マシンの機能を備えています。すべての North-South トラフィックはデフォルトの Tier 0 ルーターを通過します。アプライアンス経由で East-West トラフィックが送信されるのを防ぐため、各 Tier 1 ルーターのコンポーネントは、SDDC 内の宛先のルーティングを処理するすべての ESXi ホストで実行されます。

SDDC グループ メンバー、SDDC グループに接続された Direct Connect Gateway、HCX Service Mesh、または接続中の VPC にルーティングされるこのトラフィックのサブセット用にさらにバンド幅が必要な場合は、トラフィック グループを作成して SDDC を再構成し、各グループに追加の TO ルーターが作成されるマルチエッジにします。詳細については、[トラフィック グループを使用したマルチエッジ SDDC の構成](#)を参照してください。

注： VPN トラフィックとプライベート VIF への DX トラフィックは、デフォルトの TO を介して通過する必要があります。デフォルト以外のトラフィック グループにルーティングすることはできません。また、NAT ルールは常にデフォルトの TO ルーターで実行されるため、追加の TO ルーターは NAT ルールの影響を受けるトラフィックを処理できません。これには、SDDC のネイティブ インターネット接続との間のトラフィックが含まれます。また、これには Amazon S3 サービスへのトラフィックも含まれ、このサービスは NAT ルールを使用し、デフォルトの TO を経由する必要があります。

管理ゲートウェイ (MGW)

管理ゲートウェイは、vCenter Server のルーティングとファイアウォーリング、および SDDC で実行するその他の管理アプライアンスを処理する Tier 1 ルーターです。管理ゲートウェイのファイアウォール ルールは MGW で実行され、管理仮想マシンへのアクセスを制御します。新しい SDDC では、インターネット接続は [概要] タブで [未接続] というラベルが付けられ、信頼されている送信元からのアクセスを許可する管理ゲートウェイのファイアウォール ルールを作成するまでブロックされた状態になります。[管理ゲートウェイのファイアウォール ルールの追加または変更](#)を参照してください。

コンピューティング ゲートウェイ (CGW)

CGW は、ルーティングされたコンピューティング ネットワーク セグメントに接続されたワークロード仮想マシンのネットワーク トラフィックを処理する Tier 1 ルーターです。コンピューティング ゲートウェイのファイアウォール ルールと NAT ルールは、Tier 0 ルーターで実行されます。デフォルトの構成では、これらのルールはコンピューティング ネットワーク セグメントとの間のすべてのトラフィックをブロックします ([コンピューティング ゲートウェイのネットワークおよびセキュリティを構成](#)を参照)。

SDDC と接続中の VPC の間のルーティング

SDDC を作成すると、当社では、SDDC の作成時にユーザーが指定した AWS アカウントが所有する選択した VPC に、17 の AWS Elastic Network Interface (ENI) を事前に割り当てます。当社では、これらの ENI のそれぞれに、SDDC 作成時に指定したサブネットの IP アドレスを割り当て、SDDC クラスター Cluster-1 内の各ホストをこれらの ENI の 1 つに接続します。アクティブな NSX Edge アプライアンスが実行されている ENI に追加の IP アドレスが割り当てられます。

接続中の VPC と呼ばれるこの構成は、SDDC 内の仮想マシン間のネットワーク トラフィック、および接続中の VPC のプライマリ CIDR ブロック内にあるアドレスを使用するネイティブ AWS インスタンス/サービスをサポートします。デフォルトの CGW に接続されているルーティング ネットワーク セグメントを作成または削除すると、メイン ルート テーブルが自動的に更新されます。接続中の VPC で管理対象プリフィックス リスト モードが有効になっている場合、メイン ルート テーブルと、管理対象プリフィックス リストを追加したカスタム ルート テーブルも更新されます。

接続中の VPC（または [SERVICES]）インターフェイスは、接続中の VPC のプライマリ CIDR 内の宛先へのすべてのトラフィックに使用されます。デフォルト構成を使用する場合、SDDC と通信する AWS サービスまたはインスタンスは、接続中の VPC のメイン ルート テーブルに関連付けられたサブネット内にある必要があります。AWS 管理対象プリフィックス リスト モードが有効になっている場合（「[接続中の Amazon VPC の AWS 管理対象プリフィックス リスト モードの有効化](#)」を参照）、接続中の VPC 内のカスタム ルート テーブルを使用する AWS サービス/インスタンスが SERVICES インターフェイスを介して SDDC ワークロードと通信できるようにするには、これらのカスタム ルート テーブルに管理対象プリフィックス リストを手動で追加できます。

障害からのリカバリ、または SDDC のメンテナンスで、SDDC 内の NSX Edge アプライアンスを別のホストに移動すると、アプライアンスに割り当てられた IP アドレスが新しい ENI（新しいホストの ENI）に移動され、メイン ルート テーブルおよび管理対象プリフィックス リストを使用するカスタム ルート テーブルが更新されて、変更が反映されます。メイン ルート テーブルを置き換えた場合、またはカスタム ルート テーブルを使用しているが、管理対象プリフィックス リスト モードが有効になっていない場合、その更新は失敗し、SDDC ネットワークと接続中の VPC 間でネットワーク トラフィックをルーティングできなくなります。VMware Cloud コンソールを使用して接続中の VPC の詳細情報を表示する方法については、[接続中の VPC 情報の表示と接続中の VPC に関する問題のトラブルシューティング](#)を参照してください。

VMware Cloud on AWS には、接続中の VPC、他の VPC、および VMware Managed Transit Gateway へのルートを集約するのに役立ついくつかの機能があります。「[接続中の Amazon VPC の AWS 管理対象プリフィックス リスト モードの有効化](#)」を参照してください。

SDDC ネットワーク アーキテクチャとそれをサポートする AWS ネットワーク オブジェクトの詳細については、VMware Cloud Tech Zone の記事、[VMware Cloud on AWS: SDDC ネットワーク アーキテクチャ](#)を参照してください。

予約されたネットワーク アドレス

SDDC コンピューティング ネットワークでは、特定範囲の IPv4 アドレスを使用できません。そのいくつかは、SDDC ネットワーク コンポーネント内部で使用されます。これらのアドレスのほとんどは、他のネットワーク上の規約でも予約されています。

表 1-1. SDDC ネットワークの予約済みアドレスの範囲

<ul style="list-style-type: none"> ■ 10.0.0.0/15 ■ 172.31.0.0/16 	これらの範囲は SDDC 管理サブネットに予約済みですが、オンプレミス ネットワークや SDDC コンピューティング ネットワーク セグメントで使用できます。
<ul style="list-style-type: none"> ■ 169.254.0.0/19 ■ 169.254.64.0/24 ■ 169.254.101.0/30 ■ 169.254.105.0/24 ■ 169.254.106.0/24 	RFC 3927 では、169.254.0.0/16 はすべてリンク ローカル範囲で、1つのサブネットを超えてルーティングすることはできません。ただし、これらの CIDR ブロックを除き、ユーザーの仮想トンネル インターフェイスには 169.254.0.0/16 アドレスを使用できます。 ルートベースの VPN の作成 を参照してください。
192.168.1.0/24	これは、シングルホスト スタータ SDDC のデフォルトのコンピューティング セグメント CIDR であり、他の構成では予約されません。

注： SDDC バージョン 1.20 以前では、[RFC 6598](#) に即したキャリアグレード NAT 用に 100.64.0.0/16 も予約されています。1.22 より前のバージョンの SDDC では、この範囲のアドレスを使用しないでください。以前の SDDC ネットワークにおける 100.64.0.0/16 アドレス範囲の使用の詳細については、VMware ナレッジベースの記事 [KB76022](#) を参照してください。SDDC バージョン 1.22 における予約済みアドレスの範囲の変更の詳細については、VMware ナレッジベースの記事 [KB92322](#) を参照してください。

SDDC ネットワークには、[RFC 3330](#) に列挙された特別な IPv4 アドレス範囲の使用規則も適用されます。

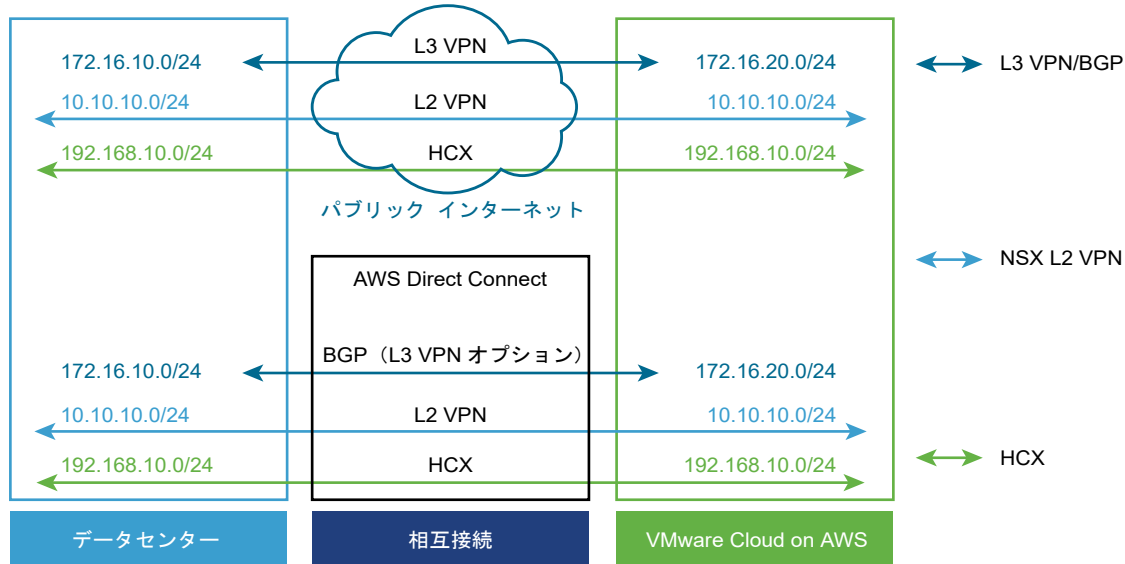
SDDC ネットワークでのマルチキャストのサポート

SDDC ネットワークでは、レイヤー 2 マルチキャスト トラフィックは、トラフィックが発生したネットワーク セグメント上のブロードキャスト トラフィックとして扱われます。そのセグメントを超えてルーティングされることはありません。IGMP スヌーピングなどのレイヤー 2 マルチキャスト トラフィック最適化機能はサポートされません。レイヤー 3 マルチキャスト (Protocol Independent Multicast など) は、VMware Cloud on AWS ではサポートされません。

クラウド SDDC へのオンプレミス SDDC の接続

オンプレミス データセンターを VMware Cloud on AWS SDDC に接続する場合、パブリック インターネットを使用する VPN または AWS Direct Connect を使用する VPN を作成するか、単純な AWS Direct Connect をそのまま使用できます。また、SDDC グループを利用して、VMware Transit Connect と AWS Direct Connect Gateway を使用し、VMware Cloud on AWS SDDC のグループとオンプレミスの SDDC の間に一元的な接続を提供することもできます。「[VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理](#)」を参照してください。

図 1-2. オンプレミス データセンターへの SDDC 接続



レイヤー 3 (L3) VPN

レイヤー 3 VPN は、パブリック インターネットまたは AWS Direct Connect を介して、オンプレミス データセンターと VMware Cloud on AWS SDDC との間の安全な接続を提供します。これらの IPsec VPN は、ルートベースまたはポリシーベースにすることができます。オンプレミス エンドポイントの場合は、[IPsec VPN 設定リファレンス](#)に表示されている設定をサポートする任意のデバイスを使用できます。

レイヤー 2 (L2) VPN

Layer 2 VPN は、オンプレミス データセンターと SDDC にまたがるように拡張またはストレッチされたネットワークに対して単一の IP アドレス空間を提供し、SDDC へのオンプレミスのワークロードのホットまたはコールド移行を可能にします。任意の SDDC に 1 つの L2VPN トンネルのみを作成できます。トンネルのオンプレミス エンドには NSX が必要です。オンプレミス データセンターでまだ NSX を使用していない場合は、スタンドアロン NSX Edge アプライアンスをダウンロードして必要な機能を提供できます。L2 VPN は、オンプレミス データセンターを SDDC に、パブリック インターネットまたは AWS Direct Connect 経由で接続できます。

AWS Direct Connect (DX)

AWS Direct Connect は、AWS が提供するサービスで、オンプレミス データセンターと AWS サービス間に、高速で遅延の小さい接続を作成します。AWS Direct Connect を構成すると、VPN はパブリック インターネットではなく DX 経由でトラフィックをルーティングできます。DX は境界ゲートウェイ プロトコル (BGP) ルーティングを実装するため、DX を構成するときに、オプションで管理ネットワークに L3VPN を使用できます。DX トラフィックは暗号化されません。このトラフィックを暗号化する場合は、DX およびプライベート IP アドレスを使用する IPsec VPN を構成します。

VMware HCX

マルチクラウド アプリケーション モビリティ ソリューションの VMware HCX は、すべての SDDC に無償で提供されます。これを利用して、オンプレミス データセンターと SDDC 間でワークロード仮想マシンを簡単に

移行できます。HCX のインストール、構成、および使用方法の詳細については、[HCX チェックリストによるハイブリッド移行](#)を参照してください。

内部トラフィックと外部トラフィックの MTU に関する考慮事項

SDDC 内部のネットワーク トラフィック（接続中の VPC との間のトラフィックを含む）では、最大 8,900 バイトの MTU がサポートされます。管理アプライアンス インターフェイスでは MTU 値 1500 が使用されるため、通常、管理ゲートウェイへのトラフィックは 1,500 バイトに制限されます。その他の MTU のデフォルト値は、「[VMware 構成の上限](#)」に記載されています。次のガイドラインは、SDDC ネットワーク全体の MTU 値に適用されます。

- SDDC グループと DX は同じインターフェイスを共有するため、両方の接続が使用中の場合は、使用する MTU 値 (8,500 バイト) を引き下げる必要があります。
- 同じセグメント上のすべての仮想マシン NIC とインターフェイスに同じ MTU を指定する必要があります。
- エンドポイントで PMTUD がサポートされていて、パス内のファイアウォールで ICMP トラフィックが許可されている限り、セグメント間では異なる MTU が使用される可能性があります。
- レイヤー 3 (IP) MTU は、基盤となるレイヤー 2 接続でサポートされる最大パケット サイズ (MTU) からプロトコル オーバーヘッドを差し引いた値以下にする必要があります。VMware Cloud on AWS では、これは NSX セグメントであり、最大 8,900 バイトの MTU を指定したレイヤー 3 パケットがサポートされます。

SDDC ネットワークのパフォーマンスについて

SDDC ネットワークのパフォーマンスの詳細については、VMware Cloud Tech Zone Designlet の「[Understanding VMware Cloud on AWS Network Performance](#)」を参照してください。

次のトピックを参照してください。

- [NSX でサポートされる機能](#)

NSX でサポートされる機能

NSX は、広範なネットワーク ソリューションおよびセキュリティ ソリューションをサポートしています。

NSX は、大規模なさまざまなデータセンター環境を特にサポートするように設計されており、コンテナとクラウドに堅牢性をもたらします。

注： NSX の構成の上限は、[VMware 構成の上限](#)に含まれるようになりました。

ネットワークと接続の機能

NSX は、SDDC で実行されているワークロードに必要なすべてのネットワーク機能を提供します。これらの機能により、次のことが可能になります。

- ネットワーク（L2、L3、および分離）を展開し、そこに配置されるワークロードのサブネットとゲートウェイを定義します。
 - L2VPN は、オンプレミスの L2 ドメインを SDDC に拡張して、IP アドレスを変更しなくてもワークロードを移行できるようにします。
 - ルートベースの IPsec VPN は、オンプレミス ネットワーク、VPC、またはその他の SDDC に接続できます。ルートベースの VPN は BGP を使用して、ネットワークが利用可能になったときに新しいルートを学習します。
 - ポリシーベースの IPsec VPN も、オンプレミス ネットワーク、VPC、またはその他の SDDC との接続に使用できます。
 - 分離されたネットワークにはアップリンクがないため、アクセスできるのは接続されている仮想マシンのみです。
- AWS Direct Connect (DX) を使用して、広帯域、低遅延の接続を介してオンプレミス ネットワークと SDDC ネットワーク間でトラフィックを送信します。ルートベースの VPN を DX トラフィックのバックアップとして使用することもできます。
- ネットワーク セグメントに対してネイティブ DHCP を選択的に有効にするか、DHCP リレーを使用してオンプレミスの IP アドレス管理ソリューションとリンクします。
- 複数の DNS ゾーンを作成し、ネットワーク サブドメインごとに異なる DNS サーバを使用できるようにします。
- ワークロードの配置先となるホストで実行中の NSX カーネル モジュールで管理されている分散ルーティングを利用して、ワークロードの相互通信を効率的に行うことができます。

セキュリティ機能

NSX セキュリティ機能には、ネットワーク アドレス変換 (NAT) 機能および高度なファイアウォール機能が含まれています。

- 送信元 NAT (SNAT) は SDDC 内のすべてのワークロードに自動的に適用されて、インターネット アクセスが有効になります。安全な環境を実現するためにインターネット アクセスは Edge ファイアウォールでブロックされますが、管理アクセスを許可するようにファイアウォール ポリシーを変更することができます。また、ワークロード用のパブリック IP アドレスを要求し、それらに対してカスタム NAT ポリシーを作成することもできます。
- Edge ファイアウォールは、管理ゲートウェイとコンピューティング ゲートウェイで実行されます。これらのステートフル ファイアウォールは、SDDC との間で送受信されるすべてのトラフィックを調べます。
- 分散ファイアウォール (DFW) は、すべての SDDC ホストで実行されるステートフル ファイアウォールです。SDDC 内のトラフィックを保護し、マイクロセグメンテーションを有効にして、ワークロード間のトラフィックを詳細に制御できるようにします。

ネットワーク運用ツール

NSX には、一般的なネットワーク運用管理ツールもいくつか用意されています。

- ポート ミラーリングは、送信元から SDDC またはオンプレミス ネットワーク内の宛先アプライアンスにミラーリング済みのトラフィックを送信できます。
- IPFIX は、トラフィック フローを IPFIX コレクタに送信することによって、セグメント固有のネットワーク トラフィック分析をサポートします。

[ネットワークとセキュリティ] ダッシュボードの使用

2

[ネットワークとセキュリティ] ダッシュボードは、レガシーの [ネットワークとセキュリティ] ビューに代わる、簡素化されたダッシュボードです。このダッシュボードには、SDDC のネットワークとセキュリティのステータスおよび NSX Manager のネットワーク管理機能へのリンクが 1 ページで表示されます。

重要： レガシーの [ネットワークとセキュリティ] ビューは SDDC バージョン 1.22 で廃止され、今後のリリースでは削除される予定です。それまでは、[ネットワークとセキュリティ] ダッシュボード バナーの [ビューの切り替え] をクリックして、レガシーの [ネットワークとセキュリティ] ビューに一時的に戻すことができます。

ダッシュボード ビュー内の情報

ダッシュボード ビューには、SDDC 接続、管理ゲートウェイとコンピューティング ゲートウェイ、およびクラウドプロバイダに関する情報が表示されます。

VPN

このカードには、SDDC 内の VPN に関する情報が表示されます。パブリック インターネットまたは AWS Direct Connect 経由で SDDC への安全な接続を提供するように VPN を構成します。ルートベースの IPsec VPN とポリシーベースの VPN がサポートされます。どちらのタイプの VPN でも、インターネット経由で SDDC に接続できます。ルートベースの VPN は、AWS Direct Connect 経由で SDDC に接続することもできます。レイヤー 2 VPN を構成することもでき、これは、ワークロードの移行に特に役立ちます。VPN タイプとその構成方法の詳細については、[SDDC とオンプレミス データセンターの間の VPN 接続の設定](#)を参照してください。

Direct Connect

このカードには、SDDC の Direct Connect 接続(存在する場合)のステータスが表示されます。AWS Direct Connect (DX) は、AWS が提供するサービスで、オンプレミス データセンターと AWS サービス間に、高速で遅延の小さい接続を作成します。AWS Direct Connect を構成すると、VPN はパブリック インターネットではなく DX 経由でトラフィックをルーティングできます。DX は境界ゲートウェイ プロトコル (BGP) ルーティングを実装するため、DX を構成するときに、オプションで管理ネットワークに L3VPN を使用できます。DX トラフィックは暗号化されません。このトラフィックを暗号化する場合は、DX およびプライベート IP アドレスを使用する IPsec VPN を構成します。AWS Direct Connect の詳細については、[SDDC とオンプレミス データセンターの間の AWS Direct Connect の設定](#)を参照してください。

中継接続

この SDDC が SDDC グループのメンバーである場合、このカードにはグループの VMware Transit Connect 接続のステータスが表示されます。SDDC 展開グループは、VMware Transit Connect を使用して、グループ内の SDDC 間にバンド幅が大きく、遅延の小さい接続を提供します。SDDC グループには、所有する VPC を含めることができます。「[VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理](#)」を参照してください。

管理ゲートウェイ

このカードには、SDDC の管理ゲートウェイ (MGW) とサブネットのステータスが表示されます。管理ゲートウェイは、vCenter Server のルーティングとファイアウォーリング、および SDDC で実行するその他の管理アプライアンスを処理する Tier 1 ルーターです。管理ゲートウェイのファイアウォール ルールは MGW で実行され、管理仮想マシンへのアクセスを制御します。デフォルトの構成では、これらのルールは管理ネットワークへのすべての受信トラフィックをブロックします。詳細については、[管理ゲートウェイのネットワークおよびセキュリティの構成](#)を参照してください。

デフォルトのコンピューティング ゲートウェイ

このカードには、SDDC のコンピューティング ゲートウェイとコンピューティング ネットワーク セグメントのステータスが表示されます。SDDC コンピューティング ネットワークには、1 つ以上のセグメントが含まれています。DNS、DHCP、およびワークロード仮想マシンのネットワーク トラフィックを管理するセキュリティ (ゲートウェイ ファイアウォールと分散ファイアウォール) サービスがサポートされます。詳細については、[コンピューティング ゲートウェイのネットワークおよびセキュリティを構成](#)を参照してください。

クラウド プロバイダ

このカードには、SDDC の [接続中の VPC] 画面で使用可能な情報のスーパーセットが表示されます。

NSX を使用した VMware Cloud on AWS のネットワークとセキュリティの構成

3

このワークフローに沿って、SDDC の NSX のネットワークとセキュリティを構成します。

手順

1 組織のメンバーへの NSX サービス ロールの割り当て

組織内のユーザーに NSX サービス ロールを付与して、SDDC で NSX 機能を確認または設定できるようにします。

2 NSX Manager による SDDC ネットワーク管理

NSX Web ユーザー インターフェイスまたは VMware Cloud コンソールの [ネットワークとセキュリティ] タブのいずれかを使用して、SDDC ネットワークを管理できます。

3 SDDC とオンプレミス データセンターの間の AWS Direct Connect の設定

AWS Direct Connect の使用はオプションです。オンプレミス ネットワークと SDDC ワークロードの間のトラフィックをパブリック インターネットによる接続よりも高速、低遅延にする必要がある場合は、AWS Direct Connect を使用するように VMware Cloud on AWS を構成します。

4 SDDC とオンプレミス データセンターの間の VPN 接続の設定

VPN を構成して、パブリック インターネットまたは AWS Direct Connect 経由で SDDC に安全な接続を提供します。ルートベースの IPsec VPN とポリシーベースの VPN がサポートされます。どちらのタイプの VPN でも、インターネット経由で SDDC に接続できます。ルートベースの VPN は、AWS Direct Connect 経由で SDDC に接続することもできます。

5 管理ゲートウェイのネットワークおよびセキュリティの構成

管理ネットワークと管理ゲートウェイは、SDDC でほぼ事前構成されています。ただし、vCenter Server や HCX などの管理ネットワーク サービスへのアクセスを構成し、管理ネットワークと他のネットワーク（オンプレミス ネットワークやその他の SDDC ネットワークなど）間のトラフィックを許可するための管理ゲートウェイ ファイアウォール ルールを作成する必要があります。

6 コンピューティング ゲートウェイのネットワークおよびセキュリティを構成

コンピューティング ゲートウェイ ネットワークには、1 つ以上のセグメントを含むコンピューティング ネットワークと、ワークロード仮想マシンのネットワーク トラフィックを管理する DNS 構成、DHCP 構成、セキュリティ構成（ゲートウェイ ファイアウォールおよび分散ファイアウォール）が含まれます。また、オンプレミス ネットワークと SDDC ワークロード ネットワークにまたがる単一のブロードキャスト ドメインを提供するレイヤー 2 VPN と拡張ネットワークが含まれる場合もあります。

7 VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加

すべての新しい VMware Cloud on AWS SDDC に、コンピューティング ゲートウェイ (CGW) という名前のデフォルトの Tier-1 ゲートウェイが含まれています。必要に応じて、追加のカスタム Tier-1 ゲートウェイを作成し、構成することができます。各 Tier-1 ゲートウェイは、SDDC Tier-0 ゲートウェイと任意の数のコンピューティング ネットワーク セグメントの間に配置されます。

8 SDDC ネットワークでの IPv6 の有効化と使用

SDDC バージョン 1.22 以降では、新しい SDDC でデュアル スタック (IPv4 および IPv6) ネットワークを有効にすることができます。

9 トラフィック グループを使用したマルチエッジ SDDC の構成

デフォルトの構成では、Software-Defined Data Center (SDDC) ネットワークにシングル エッジ (TO) ルーターがあり、このルーターを通じて、すべての North-South トラフィック フローが流れます。このエッジはデフォルトのトラフィック グループをサポートしますが、これは構成できません。SDDC グループ メンバー、SDDC グループに接続された Direct Connect Gateway、VMware HCX Service Mesh、または接続中の VPC にルーティングされるこのトラフィックのサブセット用にさらにバンド幅が必要な場合は、トラフィック グループを作成して SDDC を再構成し、各グループに追加の TO ルーターが作成されるマルチエッジにします。

10 接続中の Amazon VPC の AWS 管理対象プリフィックス リスト モードの有効化

AWS 管理対象プリフィックス リスト モードを使用すると、マルチエッジ SDDC でルート テーブルの管理を簡素化し、任意の SDDC でカスタムのルート テーブルとルート集約のサポートを使用できるようになります。

11 アップリンクへのルートの集約とフィルタリング

ルート集約と出力方向フィルタリングを使用して、Direct Connect、VMware Transit Connect、接続中の VPC などの SDDC ネットワーク アップリンクにアダプタイズされる一連のルートを制御します。これは、VPC ルート テーブル内のエントリ数を削減する場合や、アップリンクにアダプタイズされる一連のルートを制限する場合に必要になります。

12 インベントリ グループの操作

VMware Cloud on AWS のネットワーク管理者は、NSX インベントリ オブジェクトを使用して、ファイアウォール ルールで使用するサービス、グループ、コンテキスト プロファイル、および仮想マシンのコレクションを定義できます。

13 ワークロード接続の管理

デフォルトでは、ルーティング セグメントまたは MON が有効な HCX 拡張ネットワーク上のワークロード仮想マシンがインターネットに接続できます。NAT ルール、コンピューティング ゲートウェイのファイアウォール ルール、分散ファイアウォール ルール、さらには VPN 接続、DX 接続、または VTGW 接続によってアダプタイズされるデフォルト ルートのすべてで、インターネット アクセスをきめ細かく制御できます。

組織のメンバーへの NSX サービス ロールの割り当て

組織内のユーザーに NSX サービス ロールを付与して、SDDC で NSX 機能を確認または設定できるようにします。

組織のメンバーが組織の資産上で持つ権限を指定する組織ロールとは異なり、サービス ロールは、組織が使用する VMware Cloud Services にアクセスする際に組織のメンバーが持つ権限を指定します。すべてのサービス ロールは、組織の所有者権限を持つユーザーによって割り当ておよび変更できます。削除が制限された管理者や NSX Cloud 監査者など、制限付きロールを組織メンバーのロールとともに割り当てて、変更を防止する必要があります。VMware Cloud on AWS で使用可能なサービス ロールの詳細については、『VMware Cloud on AWS スタート ガイド』の [Assign a VMware Cloud on AWS Service Role to an Organization Member](#) を参照してください。

新しいサービス ロールを有効にするには、ユーザーはログアウトしてから再度ログインする必要があります。

前提条件

組織のメンバーにサービス ロールを割り当てるには、組織の所有者である必要があります。

手順

- 1 <https://vmc.vmware.com> から VMware Cloud コンソール にログインします。
- 2 サービス アイコンをクリックし、[ID とアクセスの管理] を選択します。
- 3 ユーザーを選択し、[ロールの編集] をクリックします。
- 4 [サービス ロールの割り当て] で [VMware Cloud on AWS] サービス名を選択します。
- 5 割り当てる NSX サービス ロールを選択します。

次の NSX サービス ロールを使用できます。

NSX Cloud 監査者

このロールは、NSX サービスの設定とイベントを表示できますが、サービスに変更を加えることはできません。

NSX Cloud 管理者

このロールは、NSX サービスの展開と管理に関連するすべてのタスクを実行できます。

注： 組織ユーザーに複数のサービス ロールが割り当てられている場合、最も権限が許容されたロールに対して権限が付与されます。たとえば、NSX Cloud 管理者と NSX Cloud 監査者の両方のロールを持つ組織メンバーには、NSX Cloud 監査者ロールに付与される権限が含まれる、すべての NSX Cloud 管理者権限が付与されます。

- 6 [保存] をクリックして、変更内容を保存します。

次のステップ

変更を有効にするために、ロールを変更されたユーザーがログアウトしてから再度ログインします。

NSX Manager による SDDC ネットワーク管理

NSX Web ユーザー インターフェイスまたは VMware Cloud コンソール の [ネットワークとセキュリティ] タブのいずれかを使用して、SDDC ネットワークを管理できます。

NSX Manager は、[ネットワークとセキュリティ] タブにある機能のスーパーセットをサポートしています。NSX Manager の使い方の詳細については、『NSX Data Center 管理ガイド』の [NSX Manager](#) を参照してください。

NSX Manager へのアクセス

ローカル NSX Manager には、Direct Connect または VPN を使用してプライベート IP アドレスでアクセスするか、任意のブラウザを使用してインターネット経由によってパブリック IP アドレスでアクセスできます。[NSX Manager を開く](#)を参照してください。

注： 多くの NSX ワークフローは、「管理者権限で NSX Manager にログインする」という指示から始まります。[ネットワークとセキュリティ] タブを使用するか [NSX Manager を開く] をクリックして [インターネット経由のアクセス] を選択した場合、この手順は省略できます。いずれの場合でも、VMware Cloud on AWS 組織ロールに含まれる権限によって SDDC NSX Manager にアクセスできます。[NSX Cloud 管理者] ロールには、NSX への管理者アクセス権があります。[NSX Cloud 監査者] には、NSX に対する読み取り専用アクセス権があります。サービス ロールとその割り当て方法の詳細については、[組織のメンバーへの NSX サービス ロールの割り当て](#)を参照してください。

[NSX Manager を開く] をクリックし、内部ネットワーク経由で NSX にログインする場合、ロールは組織ロールではなく NSX の認証情報によって決まります。

ワークフローのナビゲーション

[ネットワークとセキュリティ] タブには VPN、NAT、DHCP などの NSX の [ネットワーク] 画面の機能、ファイアウォールなどの [セキュリティ] 画面の機能、および [インベントリ]、[プランとトラブルシューティング]、[システム] など、他の NSX 画面の機能がまとめられています。このドキュメント内の NSX ユーザー インターフェイス項目の参照は、NSX Manager Web ユーザー インターフェイスと VMware Cloud コンソールの [ネットワークとセキュリティ] タブの両方に適用されます。

この表を使用して、本書で扱うワークフローの開始点と [ネットワークとセキュリティ] タブおよび NSX Manager の適切な項目との対応を確認してください

表 3-1. SDDC ネットワーク管理ワークフロー

ワークフロー	[ネットワークとセキュリティ] タブ	NSX
概要	概要	概要
ネットワーク セグメントの作成または変更	[ネットワーク] - [セグメント]	[ネットワーク] - [接続] - [セグメント]
SDDC とオンプレミス データセンターの間の VPN 接続の設定	[ネットワーク] - [VPN]	[ネットワーク] - [ネットワーク サービス] - [VPN]
NAT ルールの作成または変更	[ネットワーク] - [NAT]	[ネットワーク] - [ネットワーク サービス] - [NAT]
VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加	[ネットワーク] - [Tier-1 ゲートウェイ]	[ネットワーク] - [接続] - [Tier-1 ゲートウェイ]
トラフィック グループを使用したマルチエッジ SDDC の構成	[ネットワーク] - [Transit Connect]	[ネットワーク] - [Cloud Services] - [Transit Connect]
SDDC とオンプレミス データセンターの間の AWS Direct Connect の設定	[システム] - [Direct Connect]	[ネットワーク] - [Cloud Services] - [Direct Connect]
接続中の VPC 情報の表示と接続中の VPC に関する問題のトラブルシューティング	[システム] - [接続中の VPC]	[ネットワーク] - [Cloud Services] - [接続中の VPC]

表 3-1. SDDC ネットワーク管理ワークフロー（続き）

ワークフロー	[ネットワークとセキュリティ] タブ	NSX
パブリック IP アドレスの要求またはリリース	[システム] - [パブリック IP アドレス]	[ネットワーク] - [Cloud Services] - [パブリック IP アドレス]
DNS サービスの構成	[システム] - [DNS]	[ネットワーク] - [IP 管理] - [DNS]
セグメントの DHCP プロパティの構成	[システム] - [DHCP]	[ネットワーク] - [IP 管理] - [DHCP]
管理ゲートウェイのファイアウォール ルールの追加または変更、コンピューティング ゲートウェイのファイアウォール ルールの追加または変更	[セキュリティ] - [ゲートウェイ ファイアウォール]	[セキュリティ] - [ゲートウェイ ファイアウォール]
分散ファイアウォール ルールの追加または変更	[セキュリティ] - [分散ファイアウォール]	[セキュリティ] - [分散ファイアウォール]
6 章 NSX Advanced Firewall 機能について	[セキュリティ] - [分散 IDS/IPS]	[セキュリティ] - [分散 IDS/IPS]
インベントリ グループの操作	[インベントリ]	[インベントリ]
4 章 監視およびトラブルシューティング機能の設定	[ツール]	[プランとトラブルシューティング]

NSX Manager を開く

SDDC バージョン 1.16 以降では、インターネットに接続可能な任意のブラウザから接続できるパブリック IP アドレスで SDDC NSX Manager にアクセスできます。SDDC の [サマリ] 画面で [NSX Manager を開く] をクリックします。

SDDC NSX Manager には、管理ネットワーク上のプライベート IP アドレスも割り当てられます。管理ネットワークは、管理ゲートウェイ (MGW) によって保護されています。デフォルトでは、MGW は、NSX を含め、すべての管理ネットワーク送信元からのすべての宛先へのトラフィックをブロックします。ローカル NSX Manager にプライベート IP アドレスでアクセスするには、信頼されている送信元からの安全なトラフィックのみを許可する管理ゲートウェイ ファイアウォール ルールを追加する必要があります。次のいずれかの接続タイプを使用して、プライベート IP アドレスで SDDC NSX Manager に接続できます。

- **SDDC とオンプレミス データセンターの間の AWS Direct Connect の設定**

このオプションによって、企業と SDDC の間で専用接続が提供されます。IPsec VPN と組み合わせることで、トラフィックを暗号化できます。

- **SDDC とオンプレミス データセンターの間の VPN 接続の設定**

このオプションによって、企業と SDDC の間に暗号化された接続が提供されます。

Direct Connect または VPN を使用できない場合は、パブリック IP アドレスを使用して、インターネット経由でローカル NSX Manager にアクセスできます。ローカル NSX Manager のパブリック IP アドレスへのトラフィックは、すべて暗号化されて認証されます。このため、その接続やトラフィックがプライベート ネットワークの外部で改ざんされるリスクが最小限に抑えられます。SDDC の [設定] タブには、ローカル NSX Manager に接続するための接続と認証に関する詳細情報が表示されます。

注： VMware Tanzu Kubernetes Grid が有効になっている SDDC の場合、NSX Manager で[ロード バランサ] タブを表示できます。このロード バランサのサービスは、Tanzu Kubernetes Grid ワークロードでのみ使用できます。詳細については、VMware のナレッジベースの記事 [86368](#) を参照してください。

前提条件

この操作は、[NSX Cloud 管理者] または [NSX Cloud 監査者] の組織ロールを持つユーザーに限定されています。サービス ロールとその割り当て方法の詳細については、[組織のメンバーへの NSX サービス ロールの割り当て](#)を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 SDDC カードの [NSX Manager を開く] ボタンをクリックして、ローカル NSX Manager をデフォルトのパブリック IP アドレスで開きます。

NSX へのログインには、VMware Cloud on AWS の認証情報が使用されます。

- 4 SDDC に VPN または DX 接続が含まれていて、NSX Manager にプライベート IP アドレスでアクセスする場合は、VPN または DX からローカル NSX Manager への HTTPS トラフィックを許可する管理ゲートウェイ ファイアウォール ルールを作成します。そのうえで、ブラウザを使用して、[設定] タブに表示されたいずれかの [NSX Manager の URL] への接続を開きます。

- a [NSX Manager を開く] ボタンをクリックするか、[ネットワークとセキュリティ] タブを開いてファイアウォール ルールを作成します。

管理ゲートウェイ ファイアウォール ルールの作成方法の詳細については、[管理ゲートウェイのファイアウォール ルールの追加または変更](#)を参照してください。このルールには以下のパラメータを使用します。

管理ゲートウェイ ファイアウォール ルール プロパティ	値
送信元	<p>オンプレミス データセンターの IP アドレスまたは CIDR ブロック。</p> <p>重要： ファイアウォール ルールの送信元アドレスとして [任意] を選択できますが、このファイアウォール ルールの送信元アドレスとして [任意] を使用すると、NSX Manager に対する攻撃が可能になり、SDDC が侵害される可能性があります。ベスト プラクティスとして、信頼できる送信元アドレスからのアクセスのみを許可するには、このファイアウォール ルールを構成します。</p>
宛先	[NSX Manager] システム定義のグループ。
サービス	HTTPS (TCP 443)
操作	Allow

- b ブラウザを使用して、NSX への接続を開きます。

[設定] タブの [NSX Manager の URL] を展開して、使用できる URL とアカウントを表示します。

インターネット経由での NSX Manager へのアクセス

この URL には、ローカル NSX Manager のパブリック IP アドレスが含まれています。このアドレスは、[NSX Manager を開く] ボタンをクリックすると使用されます。

内部ネットワーク経由での NSX Manager へのアクセス

これは、管理サブネット上の NSX Manager の [プライベート IP] アドレスです。4.a に示すような管理ゲートウェイ ファイアウォール ルールでは、このアドレスへのトラフィックが許可されます。

必要なファイアウォール ルールが作成されていても、内部ネットワーク経由で NSX Manager にアクセスできない場合は、一時的なネットワーク問題が原因である可能性があります。[再試行] をクリックして内部ネットワーク経由のアクセスを再試行するか、ブラウザを開いてパブリック URL で NSX Manager に接続します。NSX のプライベート URL とパブリック URL は、SDDC コンソールの [設定] 画面に一覧表示されます。

内部ネットワーク経由でアクセスする URL (VMware Cloud Services を使用してログイン)

ブラウザでこの URL を開き、VMware Cloud on AWS の認証情報を使用して NSX Manager にログインします。

内部ネットワーク経由でアクセスする URL (NSX Manager 認証情報を使用してログイン)

ブラウザでこの URL を開き、[NSX Manager 管理者ユーザー アカウント] の認証情報（NSX のデプロイおよび管理に関連するすべてのタスクを実行する場合）、または [NSX Manager 監査ユーザー アカウント] の認証情報（NSX サービスの設定とイベントを表示する場合）を使用してログインします。

- c （オプション） 内部ネットワークを使用するように NSX Manager のデフォルト アクセスを変更します。

NSX Manager に内部ネットワーク経由でアクセスするように構成すると、SDDC の [設定] タブを開き、[[NSX Manager] ボタンのデフォルト アクセス] を [インターネット経由（パブリック）] から [内部ネットワーク経由（プライベート）] に変更できます。この変更を行った後で [NSX Manager を開く] ボタンをクリックすると、ローカル NSX Manager は内部ネットワーク上のプライベート IP アドレスで開きます。

LDAP ID ソースからの NSX ロールの割り当て

管理ユーザー アカウントが LDAP ID ソース（Active Directory または OpenLDAP）で維持されている場合は、NSX Manager でアカウントまたは LDAP グループに割り当てるロールで LDAP ユーザーが NSX にアクセスできるように SDDC NSX Manager を構成します。

ほとんどの場合、LDAP サービスの設定後に必要な操作は、NSX Manager がポート 389 (LDAP) または 636 (LDAPS) 上の任意のドメイン コントローラを参照するように指定することのみです。

Active Directory (AD) を使用し、Active Directory フォレストが複数のサブドメインから構成されている場合は、Active Directory グローバル カタログ (GC) で NSX Manager をポイントし、NSX で各サブドメインを代替ドメイン名として構成する必要があります。グローバル カタログ サービスは通常、プライマリ Active Directory ドメイン コントローラで実行されます。これは、すべてのプライマリ ドメインとセカンダリ ドメインの最も重要な情報の読み取り専用コピーです。GC サービスは、ポート 3268（プレーンテキスト）と 3269（TLS を介した LDAP、暗号化）で実行されます。

たとえば、プライマリ ドメインが example.com で、サブドメインに americas.example.com と emea.example.com がある場合は、次のことを行う必要があります。

- 1 ポート 3268 で LDAP プロトコルを使用するか、ポート 3269 で LDAPS プロトコルを使用するように NSX Manager を構成します。
- 2 NSX LDAP 構成に代替ドメイン名 americas.example.com と emea.example.com を追加します。

サブドメインのいずれかのユーザーは、適切なドメインを含むログイン名でログインする必要があります。たとえば、emea.example.com ドメインのユーザー john は、ユーザー名 john@emea.example.com でログインする必要があります。

前提条件

SDDC NSX Manager は、LDAP を介した Active Directory や OpenLDAP などのディレクトリ サービスを使用してユーザーを認証し、管理ゲートウェイ ファイアウォールを介して LDAP ID ソースにアクセスできるように構成する必要があります。『NSX 管理ガイド』の「LDAP ID ソース」を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。

- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [NSX Manager を開く] をクリックします。ローカル NSX Manager をデフォルトのパブリック IP アドレスで開きます。NSX へのログインには、VMware Cloud on AWS の認証情報が使用されます。VMware Cloud コンソールから NSX Manager への接続時に必要になる可能性のあるファイアウォール ルールの詳細については、「[NSX Manager を開く](#)」を参照してください。
- 3 NSX Manager LDAP ID ソースから NSX ロールを割り当てます。

NSX Manager ユーザー インターフェイスで、[システム] - [ユーザー管理] の順にクリックします。[ユーザーロールの割り当て] タブで、[LDAP ユーザーのロールを追加] をクリックし、検索する LDAP ドメインを選択します。

4 LDAP ユーザーまたはグループの NSX ロールを指定します。
 - a LDAP ディレクトリを検索するにはユーザー名またはグループ名の最初の数文字を入力して、表示されたリストからユーザーまたはグループを選択します。
 - b [ロール/範囲の設定] 画面で、NSX ロールをユーザーまたはグループに割り当てます。

次のいずれかの NSX ロールを割り当てることができます。

クラウド管理者

このロールは、NSX サービスの展開と管理に関連するすべてのタスクを実行できます。

クラウド オペレータ

このロールは、NSX サービスの設定とイベントを表示できますが、サービスに変更を加えることはできません。

その他のロールをここで割り当ててはできません。

- c [適用] をクリックします。
- d [保存] をクリックします。

結果

NSX ロールを持つ LDAP グループ メンバーは、このワークフローを使用して、NSX Manager のプライベート URL に LDAP 認証情報でログインできます。

SDDC の [設定] タブで、[NSX 情報] に移動して、[NSX Manager の URL] を展開します。[プライベート URL (NSX Manager 認証情報を使用してログイン)] に表示されるリンクをクリックして、LDAP 認証情報を入力します。

SDDC とオンプレミス データセンターの間の AWS Direct Connect の設定

AWS Direct Connect の使用はオプションです。オンプレミス ネットワークと SDDC ワークロードの間のトラフィックをパブリック インターネットによる接続よりも高速、低遅延にする必要がある場合は、AWS Direct Connect を使用するように VMware Cloud on AWS を構成します。

オンプレミス データセンターとの間のトラフィックに対して AWS Direct Connect を利用するように VMware Cloud on AWS SDDC を設定するには、いくつかの方法があります。

プライベート VIF への Direct Connect を構成します。

AWS Direct Connect (DX) は、オンプレミス ネットワーク インフラストラクチャと Amazon VPC の仮想インターフェイス (VIF) の間の専用ネットワーク接続を提供します。プライベート VIF は、SDDC への直接プライベート アクセスを提供します。オンプレミス データセンターと VMware Cloud on AWS SDDC との間で VPN、HCX、vMotion などのワークロードおよび管理トラフィックを送信する場合は、プライベート VIF 上に DX を構成します。DX 接続は、ネットワーク通信用のプライベート パスを提供し、BGP を使用して SDDC とオンプレミス データセンター間のルートをアドバタイズします。現在の VIF のプロビジョニング手順は、選択した DX 接続のタイプによって異なります。

Direct Connect Gateway (DXGW) を SDDC グループの VMware Managed Transit Gateway に関連付けます。

VMware Cloud on AWS 組織に SDDC グループを作成した場合は、AWS Transit VIF を使用してそのグループの DXGW に接続し、オンプレミス データセンターとグループ内のすべての SDDC 間の DX 接続を提供することができます。「[SDDC グループへの Direct Connect Gateway の接続](#)」を参照してください。

パブリック VIF を介した AWS サービスへのアクセス

DX を使用して AWS サービスにアクセスするだけの場合は、パブリック VIF を介してそうすることができます。パブリック VIF は SDDC に対して透過的であり、SDDC 自体における構成は必要ありません。パブリック VIF を使用して、プライベート VIF または Direct Connect Gateway を必要とする同じ種類の SDDC トラフィック (vMotion など) を送信することはできません。SDDC が配置されているリージョンで AWS ルートを学習するようにパブリック VIF が構成されている場合、SDDC からオンプレミス データセンター内のパブリック IP アドレスへの接続は、そのリージョンの AWS ルートに含まれ、DX を経由します。このような構成では、パブリック VIF 経由の VPN 接続により、SDDC への安全なプライベート接続が提供されます。

AWS Direct Connect への接続のセットアップ

AWS Direct Connect への接続をセットアップするには、AWS コンソールから発注し、VMware Cloud on AWS が使用可能なリージョンに Direct Connect 接続を作成します。

接続タイプ

AWS は、次の 3 種類の Direct Connect 接続を提供しています。

専用接続

専用接続は、複数のプライベート/パブリック仮想インターフェイス (VIF) と 1 つの中継 VIF をサポートする単一ユーザー専用の物理的イーサネット ポートを提供します。

専用接続を注文するには、AWS Direct Connect パートナー プログラムのメンバーに、SDDC と同じリージョンの AWS Direct Connect ロケーションに回線のプロビジョニングを依頼します。この要求を行う際は、(顧客管理) AWS アカウントを使用してください。回線のプロビジョニング後、NSX の [Direct Connect] 画面の [AWS アカウント ID] フィールドに表示されるアカウントで、SDDC にホスト型プライベート VIF を作成します。SDDC グループのメンバーである SDDC では、アカウントに Direct Connect Gateway (DXGW) を作成して、そこに DXGW から中継 VIF を接続できます。[VMware Transit Connect による SDDC 展開グループの作成と管理](#)を参照してください。

ホスト型接続

ホスト型接続は複数のユーザーによって共有され、AWS Direct Connect パートナーによってユーザーの AWS アカウントにプロビジョニングされる回路です。回線のプロビジョニング後、NSX の [Direct Connect] 画面の [AWS アカウント ID] フィールドに表示されるアカウントで、SDDC にホスト型プライベート VIF を作成します。ホスト型接続の速度が 1Gbps 以上であり、SDDC グループのメンバーである SDDC の場合は、ユーザー アカウントに Direct Connect Gateway (DXGW) を作成して、そこに DXGW から中継 VIF を接続することもできます。[VMware Transit Connect による SDDC 展開グループの作成と管理](#)を参照してください。

ホスト型 VIF

ホスト型 VIF はホスト型接続に似ていますが、作成できるのはパートナーが管理する VIF 1 つのみです。ホスト型プライベート VIF は、NSX の [Direct Connect] 画面の [AWS アカウント ID] フィールドに表示されるアカウント番号を使用して AWS パートナーが作成します。各ユーザーの AWS アカウントにはプロビジョニングされません。

Direct Connect の VMware Cloud on AWS との使用の詳細については、VMware Designlet の [VMware Cloud on AWS SDDC Connectivity With Direct Connect Private VIF](#) を参照してください。接続タイプとセットアップ方法の詳細については、[AWS Direct Connect パートナー企業、開始方法 AWS Direct Connect の使用](#)を参照してください。

SDDC の管理およびコンピューティング ネットワーク トラフィック用のプライベート仮想インターフェイスに対する Direct Connect の構成

DX を介したプライベート VIF を作成し、プライベート IP アドレスを使用して、オンプレミス ネットワークと SDDC のワークロード、ESXi 管理、および管理アプライアンス間の直接接続を提供します。

SDDC に接続する Direct Connect (DX) 回線それぞれに対してプライベート仮想インターフェイス (VIF) を 1 つ作成します。各プライベート VIF は個別の BGP セッションを確立します。これは、アクティブ/スタンバイ設計またはアクティブ/アクティブ (ECMP を含む) 設計で使用することも、プライベート ネットワーク セグメントに使用することもできます。DX の冗長性が必要な場合は、異なる DX 回線でプロビジョニングされた個別のプライベート VIF を SDDC に接続します。

高可用性を確保するために複数のプライベート VIF を個別の DX 回線を介して SDDC に接続する場合は、すべての DX 回線を同じ AWS アカウントで作成し、異なる [AWS Direct Connect ロケーション](#)に提供する必要があります。この操作を行うと、AWS は冗長性を高めるために DX 接続に個別の内部ネットワーク パスを利用しようとします。AWS ドキュメントの [High resiliency](#) および [Active/Active and Active/Passive Configurations in](#)

[AWS Direct Connect](#) を参照してください。すべてのプライベート VIF にアダプタイズされるネットワーク セグメント数の制限については、[VMware Configuration Maximums](#) を参照してください。柔軟性を高めるためのルート集約がサポートされていますが、すべての VIF には、SDDC によってアダプタイズされた同じネットワークがあります。

重要： DX プライベート仮想インターフェイスまたは SDDC グループを SDDC に接続すると、SDDC 内の他のルーティング構成に関係なく、ESXi ホスト上で SDDC ネットワーク外の宛先行きのすべての送信トラフィックは、そのインターフェイス経由でルーティングされます。vMotion トラフィックと vSphere Replication トラフィックも同様です。受信トラフィックと送信トラフィックのパスが対称になるように、ESXi ホストへの受信トラフィックも同じパス経由でルーティングされるようにする必要があります。VMware Transit Connect と VMware Managed Transit Gateway (VTGW) の詳細については、『VMware Cloud on AWS Operations Guide』の [VMware Transit Connect を使用した SDDC 展開グループの作成と管理](#) を参照してください。

ルートベースの VPN から学習したルートは、BGP を介して他のルートベースの VPN にアダプタイズされますが、SDDC は自身のネットワークのみを SDDC グループにアダプタイズします。VPN から学習したルートはアダプタイズされません。BGP 経由でアダプタイズおよび学習されるルートの制限をはじめ、AWS によって課される Direct Connect に関する制限の詳細については、『AWS Direct Connect ユーザー ガイド』の [AWS Direct Connect のクォータ](#) を参照してください。

この方法で作成したプライベート VIF は、その VIF を作成したリージョン内の任意の組織の SDDC に接続できます。プライベート VIF は、DX 回線と同じリージョンに作成し、その同じリージョン内の SDDC に接続する必要があります。SDDC に接続した後で VIF を分離したり、別の SDDC に再割り当てしたりすることはできません。代わりに、その VIF を削除して新しい VIF を作成する必要があります。SDDC を削除すると、接続されている VIF がすべて削除されます。

前提条件

- [仮想インターフェイスの前提条件](#)に記載されている仮想インターフェイスの前提条件を満たしていることを確認します。
- ルートベースの VPN を Direct Connect のバックアップとして使用する場合は、手順 6 に示すように [Direct Connect のバックアップとして VPN を使用] スイッチを [有効] に設定する必要があります。ポリシーベースの VPN を使用して別の接続をバックアップすることはできません。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

4 AWS コンソールにログインし、[ホスト仮想インターフェイスの作成](#)で説明されている「ホストされたプライベート仮想インターフェイスを作成する」の手順を実行します。

ホストされている VIF を使用している場合は、AWS Direct Connect パートナー企業と連携し、[Direct Connect] 画面の [AWS アカウント ID] フィールドに表示されているアカウントで VIF を作成し、この手順の[手順 5](#)にスキップします。専用の接続またはホストされた接続を使用している場合は、最初に次の手順を実行します。

- a [仮想インターフェイス タイプ] に対し、[プライベート] を選択し、[仮想インターフェイス名] を組み立てます。
- b [仮想インターフェイス所有者] フィールドに対し、[他の AWS アカウント] を選択し、NSX [Direct Connect] 画面の [AWS アカウント ID] を使用します。
- c [VLAN] に対し、AWS Direct Connect パートナー企業が提供する値を使用します。
- d [BGP ASN] に対し、この接続が終了するオンプレミス ルーターの ASN を使用します。

この値を、NSX [Direct Connect] 画面に表示されている [BGP ローカル ASN] と同じにすることはできません。

- e [詳細設定] を展開し、次の項目を選択します。

[アドレス ファミリ]	IPv4 の選択
[ルーター ピア IP]	この接続のオンプレミス側（ルーター）の IP アドレスを指定するか、空白のままにして AWS がアドレスを自動的に割り当てられるようにします。このアドレスは、後でルーターで設定する必要があります。
[Amazon のルーター ピア IP]	この接続の AWS 側の IP アドレスを指定するか、空白のままにして AWS がアドレスを自動的に割り当てられるようにします。このアドレスは、後でルーターで設定する必要があります。
[BGP 認証キー]	値を指定するか、空白のままにして AWS がキーを生成できるようにします。このキーは、後でルーターで設定する必要があります。
[ジャンボ MTU (MTU サイズ 9001)]	すべての SDDC ネットワークのデフォルトの MTU は 1,500 バイトです。このプライベート VIF への DX トラフィックを有効にして、より高い MTU を使用するには、[ジャンボ MTU (MTU サイズ 9001)] の [有効] を選択します。VIF を作成したら、NSX の [グローバル構成] 画面を開き、[イントラネット アップリンク] でより高い [MTU] の値を設定する必要もあります。詳細については、 Direct Connect の MTU の指定 を参照してください。接続プロパティでこれを有効にすると、すぐに使用しない場合でも、SDDC ネットワークでジャンボ フレームを必要に応じて利用しやすくなります。

インターフェイスが作成されると、受け入れの準備ができたことが AWS コンソールから報告されます。

- 5 [NSX Manager] または VMC コンソールの [ネットワークとセキュリティ] タブを開きます。[Direct Connect] をクリックし、[接続] をクリックして仮想インターフェイスを受け入れます。

新しい VIF は、受け入れられる前は組織内のすべての SDDC に表示されます。VIF を受け入れると、他の SDDC には表示されなくなります。

BGP セッションが有効になるまでに、最長 10 分かかる場合があります。接続が準備できると、[状態] が [接続済み]、[BGP ステータス] が [UP] と表示されます。

- 6 (オプション) ルートベース VPN を Direct Connect のバックアップとして構成します。

デフォルトの設定では、DX と VPN の両方によって BGP にアドバタイズされるすべてのルート上のトラフィックには、デフォルトでルートベースの VPN が使用されます。DX と VPN の両方によってアドバタイズされるルートが、デフォルトでは DX を使用し、DX が使用できないときは VPN にフェイルオーバーするようにするには、[Direct Connect] をクリックし、[Direct Connect のバックアップとして VPN を使用] スイッチを [有効] に設定します。

注： この設定には、ルートベース VPN が必要です。ポリシーベース VPN を Direct Connect のバックアップとして使用することはできません。SDDC グループのメンバーである SDDC では、DX プライベート VIF とグループの VMware Managed Transit Gateway (VTGW) の両方がアドバタイズするルートを通過するトラフィックは、VTGW を介してルーティングされます。

ルーティング設定の更新には約 1 分かかります。操作が完了すると、DX と VPN の両方によって通知されるルートは、DX 接続がデフォルトになり、DX が使用できない場合にのみ VPN が使用されます。DX と VPN の両方がアドバタイズする同等のルートは、VPN 接続に優先順位を付けます。

結果

ルートが学習されてアドバタイズされると、[アドバタイズされた BGP ルート] と [学習された BGP ルート] のリストが表示されます。更新アイコンをクリックすると、これらのリストが更新されます。SDDC 内のすべてのルーティングされたサブネットは、管理ネットワーク サブネットの次のサブセットとともに、BGP ルートとしてアドバタイズされます。

- サブネット 1 には、ESXi ホスト vmks およびルーター インターフェイスで使用されるルートが含まれます。
- サブネット 2 には、マルチ AZ のサポートと AWS 統合に使用されるルートが含まれます。
- サブネット 3 には管理仮想マシンが含まれます。

切断されたネットワークと拡張ネットワークはアドバタイズされません。カスタム T1 に接続されたネットワークはアドバタイズされません。ルート フィルタリングが有効になっている場合は、デフォルト CGW に接続されたネットワークもアドバタイズされません。

DX に定義および適用されたルート集約は、定義に従ってアドバタイズされます ([アップリンクへのルートの集約とフィルタリング](#)を参照してください)。

プライベート VIF に実際にアドバタイズされる CIDR ブロックは、管理サブネットの CIDR ブロックによって決まります。ある SDDC で、デフォルト管理ネットワーク CIDR がブロック サイズ /16、/20、/22 の 10.2.0.0 である場合、これらのルートの CIDR ブロックは次の表のようになります。

表 3-2. デフォルトの管理ゲートウェイ CIDR 10.2.0.0 についてアドバタイズされるルート

管理ゲートウェイ CIDR	サブネット 1	サブネット 2	サブネット 3
10.2.0.0/23	10.2.0.0/24	10.2.1.0/26	10.2.1.128/25
10.2.0.0/20	10.2.0.0/21	10.2.8.0/23	10.2.12.0/22
10.2.0.0/16	10.2.0.0/17	10.2.128.0/19	10.2.192.0/18

次のステップ

オンプレミスの vMotion インターフェイスが Direct Connect を使用するように構成されていることを確認します。[Direct Connect を使用するための vMotion インターフェイスの設定](#)を参照してください。

Direct Connect を使用するための vMotion インターフェイスの設定

Direct Connect 接続をオンプレミスのデータセンターとクラウドの Software-Defined Data Center (SDDC) 間で使用する場合は、オンプレミスのホストに vMotion インターフェイスを構成して、Direct Connect の接続を経由する vMotion トラフィックをルーティングする必要があります。

前提条件

Direct Connect を構成し、プライベート仮想インターフェイスを作成します。

手順

- 1 オンプレミス環境の各ホストで vMotion インターフェイスを構成するには、次の方法のいずれかを選択します。

オプション	説明
デフォルト ゲートウェイのオーバーライド (vSphere 7.0 以降)	各ホストの vMotion トラフィックに使用する VMkernel アダプタを編集し、デフォルト ゲートウェイをオーバーライドするオプションを選択します。Direct Connect 接続のオンプレミス側にトラフィックをルーティングできるオンプレミスの vMotion サブネットに IP アドレスを入力します。 VMkernel アダプタ構成の編集 を参照してください。
vMotion TCP/IP スタックの設定	各ホストで、次の操作を実行します。 <ol style="list-style-type: none"> a 既存の vMotion VMkernel アダプタを削除します。 b 新規の VMkernel アダプタを作成し、vMotion TCP/IP スタックを選択します。ESXi ホストの vMotion TCP/IP スタックへの vMotion トラフィックの配置を参照してください。 c Direct Connect 接続のオンプレミス側にトラフィックをルーティングできるオンプレミスの vMotion サブネットに IP アドレスを使用するためにルーティングを変更するには、ホストの vMotion TCP/IP スタックを編集します。ホスト上の TCP/IP スタック構成の変更を参照してください。

- 2 (オプション) vmkping を使用して、オンプレミスのホストとクラウド SDDC ホスト間の接続をテストします。

詳細については、VMware のナレッジベースの記事 [1003728](#) を参照してください。

AWS サービスにアクセスするためのパブリック仮想インターフェイスに対する Direct Connect の構成

オンプレミスのワークロードに AWS EC2 のインスタンスおよびサービスへのアクセス権が必要な場合は（DX 接続経由の S3 など）、VPC のそのトラフィック用のパブリック仮想インターフェイスを構成します。

DX 上の SDDC 管理トラフィックとワークロード トラフィックでは、プライベート VIF または DX ゲートウェイを使用する必要があります。ただし、オンプレミスのワークロードから AWS サービスにアクセスする必要がある場合や、何らかの目的でグローバルの AWS バックボーンに接続する必要がある場合は、オンプレミスのデータセンターからパブリック VIF への DX 接続を作成できます。

前提条件

- [仮想インターフェイスの前提条件](#)に記載されている仮想インターフェイスの前提条件を満たしていることを確認します。

手順

- 1 AWS コンソールにログインします。[ホスト仮想インターフェイスの作成](#)で示されている、ホストされたパブリック仮想インターフェイスを作成する手順を完了します。
 - a [インターフェイス所有者] フィールドで、[My AWS アカウント] を選択します。
 - b [ルーター ピア IP アドレス] と [Amazon のルーター ピア IP アドレス] を指定します。
 - c [BGP キーの自動生成] を選択し、AWS 基盤でアドバタイズするすべてのオンプレミス ルートを [アドバタイズするプリフィックス] に指定します。

インターフェイスが作成されると、受け入れの準備ができたことが AWS コンソールから報告されます。

- 2 [NSX Manager] または VMC コンソールの [ネットワークとセキュリティ] タブを開きます。[Direct Connect] をクリックし、[接続] をクリックして仮想インターフェイスを受け入れます。

新しい VIF は、受け入れられる前は組織内のすべての SDDC に表示されます。VIF を受け入れると、他の SDDC には表示されなくなります。

BGP セッションが有効になるまでに、最長 10 分かかる場合があります。接続が準備できると、[状態] が [接続済み]、[BGP ステータス] が [UP] と表示されます。

Direct Connect の MTU の指定

すべての SDDC ネットワークのデフォルトの最大転送ユニット (MTU) は 1,500 バイトです。Direct Connect とプライベート VIF の使用時には、SDDC アップリンクにより大きな MTU（最大 8,900 バイト）を構成できます（DX 接続でサポートされている場合）。

VIF を作成する際に、DX を有効にして、使用する MTU を引き上げることができます。この操作を行う場合は、NSX の [グローバル構成] 画面を開き、[イントラネットの MTU 値] の設定値を大きくする必要があります。

この大きな（ジャンボ）MTU 値は、プライベート VIF および構成済みの SDDC グループ接続を介した DX 接続にのみ適用されます。DX 経由で接続されているかどうかにかかわらず、すべての VPN は、他の設定に関係なく MTU 値 1500 を使用します。ワークロード仮想マシンがより大きな MTU を利用できるようにするには、DX 接続を使用するワークロード仮想マシン、およびワークロードの接続パスに従うその他のインターフェイスで [イントラネットの MTU 値] と同じ MTU が使用されていることを確認してください。

セグメント上のすべてのネットワーク インターフェイスを同じ MTU 値に設定する必要があります。そうしないと、通信の問題が発生する可能性があります。通常、Path MTU Discovery (PMTUD) が有効で、ネットワーク間で ICMP トラフィックが許可されている限り、セグメントごとに異なる MTU 値を使用できます。SDDC グループが構成されている場合は、イントラネット インターフェイス MTU を 8,500 バイト (SDDC グループ トラフィックでサポートされる最大値) を上回る値に設定しないでください。SDDC グループに属していて DX 接続も使用する SDDC では、DX プライベート VIF と SDDC グループ接続の両方で同じイントラネット インターフェイスを共有するため、すべてのトラフィックに使用可能な最大 MTU は 8,500 バイトです。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。 [NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [グローバル構成] 画面で、鉛筆アイコン (✎) をクリックし、[イントラネット アップリンク] フィールドで [MTU] 値を高く設定して、[保存] をクリックします。

設定する値は、すべての DX 仮想インターフェイスの最小 MTU 値以下にする必要があります。これは、ジャンボ MTU をサポートしていない VIF があると、実質的にはすべての DX 接続が MTU 値 1500 に制限されるため、すべての VIF を同一の MTU 値 (デフォルトでは 1500、ジャンボでは 9001) に設定する必要があるという意味です。ネットワーク内で MTU サイズを混在させると、パケットの断片化やその他の問題が発生し、ネットワーク パフォーマンスが低下する場合があります。

注： Geneve (Generic Network Virtualization Encapsulation) ヘッダーの余地を残しておくため、SDDC のイントラネットの MTU は、上限が 8,900 バイトに設定されています。これは VIF でのパケットの断片化を防ぐためです。

SDDC とオンプレミス データセンターの間の VPN 接続の設定

VPN を構成して、パブリック インターネットまたは AWS Direct Connect 経由で SDDC に安全な接続を提供します。ルートベースの IPsec VPN とポリシーベースの VPN がサポートされます。どちらのタイプの VPN でも、インターネット経由で SDDC に接続できます。ルートベースの VPN は、AWS Direct Connect 経由で SDDC に接続することもできます。

レイヤー 2 VPN を構成することもでき、これは、ワークロードの移行に特に役立ちます。

IPsec VPN の詳細については、VMware Designlet の [VMware Cloud on AWS SDDC Connectivity With IPsec VPN](#) を参照してください。

次に参照するドキュメント

- [ルートベースの VPN の作成](#)

ルートベースの VPN では、IPsec トンネル インターフェイスが作成され、SDDC ルーティング テーブルで指定されたとおりにトラフィックがルーティングされます。ルートベースの VPN では、複数のサブネットに対する、回復性と安全性が確保されたアクセスが提供されます。ルートベースの VPN を使用すると、新しいネットワークが作成されたときに新しいルートが自動的に追加されます。

- [ポリシー ベース VPN の作成](#)

ポリシーベースの VPN では、IPsec トンネルと、トラフィックによるトンネルの使用方法を指定するポリシーが作成されます。ポリシーベースの VPN を使用する場合は、新しいルートを追加するときに、ネットワークの両端でルーティング テーブルを更新する必要があります。

- [IPsec VPN の証明書ベースの認証の構成](#)

証明書ベースの VPN では、IKE ネゴシエーション時にプリシェアード キーではなくデジタル証明書を使用します。

- [レイヤー 2 VPN および拡張ネットワーク セグメントの構成](#)

VMware Cloud on AWS のレイヤー 2 仮想プライベート ネットワーク (L2VPN) を使用して、オンプレミス ネットワークを SDDC の 1 つ以上の VLAN ベースのネットワークに拡張できます。この拡張ネットワークは、単一のブロードキャスト ドメインを持つ単一のサブネットです。この拡張ネットワークでは、クラウド SDDC に対して、仮想マシンを、その IP アドレスを変更せずに移行できます。

- [VPN トンネルのステータスと統計情報の表示](#)

SDDC NSX Manager には、IPsec VPN セグメントと L2VPN セグメントのステータスと統計情報が表示されます。

- [IPsec VPN 設定リファレンス](#)

IPsec VPN のオンプレミス側の設定は、その VPN の Software-Defined Data Center (SDDC) 側で指定した設定と同じにする必要があります。

- [VMware Cloud on AWS における VPN の問題のトラブルシューティング](#)

VPN の問題には、認証エラー (IKE フェーズ 1 およびフェーズ 2) や接続 (ピアが応答しない) の問題が含まれる場合があります。

ルートベースの VPN の作成

ルートベースの VPN では、IPsec トンネル インターフェイスが作成され、SDDC ルーティング テーブルで指定されたとおりにトラフィックがルーティングされます。ルートベースの VPN では、複数のサブネットに対する、回復

性と安全性が確保されたアクセスが提供されます。ルートベースの VPN を使用すると、新しいネットワークが作成されたときに新しいルートが自動的に追加されます。

注： このトピックでは、SDDC のデフォルトのパブリック IP アドレスまたはプライベート IP アドレスに接続するルートベース VPN の作成方法について説明します。追加の Tier-1 ゲートウェイが配置された SDDC (VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加を参照) がある場合は、[NSX Manager を開く] をクリックし、これらのゲートウェイを終端とする VPN サービスを追加できます。『NSX Data Center 管理ガイド』の VPN サービスの追加を参照してください。

VMware Cloud on AWS では、Tier-1 ゲートウェイに対する VPN サービスは BGP をサポートしていません。

VMware Cloud on AWS SDDC 内のルートベースの VPN では、IPsec プロトコルを使用してトラフィックが保護され、ネットワークが追加および削除されたときにはボーダー ゲートウェイ プロトコル (BGP) を使用してルートが検索、伝達されます。ルートベースの VPN を作成するには、ローカル (SDDC) およびリモート (オンプレミス) のエンドポイントの BGP 情報を構成してから、トンネルの SDDC 側のトンネル セキュリティ パラメータを指定します。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。NSX Manager による SDDC ネットワーク管理を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 (オプション) デフォルトのローカル自律システム番号 (ASN) を変更します。

SDDC のルートベースのすべての VPN は、デフォルトでは ASN 65000 に設定されます。ローカル ASN には、リモート ASN とは別の値を使用してください (同一のローカル ASN とリモート ASN が求められる iBGP は、SDDC ネットワークではサポートしていません)。デフォルトのローカル ASN を変更するには、[ローカル ASN の編集] をクリックし、64521 から 65534 (或いは 4200000000 から 4294967294) の範囲で新しい値を入力して、[適用] をクリックします。

注： この値を変更すると、この SDDC 内のすべてのルートベースの VPN に影響が及びます。

- 5 [VPN] - [ルート ベース] - [VPN の追加] の順にクリックして、新しい VPN に [名前] とオプションの [説明] を指定します。
- 6 ドロップダウン メニューから [ローカル IP アドレス] を選択します。
 - 現在の SDDC が SDDC グループのメンバーの場合、または AWS Direct Connect を使用する構成になっている場合は、VPN でインターネット経由の接続ではなく、その接続を使用できるように、プライベート IP アドレスを選択します。Direct Connect または VMware Managed Transit Gateway

(VTGW) 経由の VPN トラフィックは、より高い MTU がリンクでサポートされていても、デフォルト MTU の 1,500 バイトが上限になるので注意してください。[SDDC の管理およびコンピューティング ネットワーク トラフィック用のプライベート仮想インターフェイスに対する Direct Connect の構成](#)を参照してください。

- インターネット経由で VPN を接続する場合は、パブリック IP アドレスを選択します。

7 [リモート パブリック IP アドレス] には、オンプレミスの VPN エンドポイントのアドレスを入力します。

これは、この VPN に対する IPsec 要求を開始したり、それに応答したりするデバイスのアドレスです。このアドレスは、次の要件を満たす必要があります。

- 別の VPN でまだ使用されていないアドレスである必要があります。VMware Cloud on AWS はすべての VPN 接続に同じパブリック IP アドレスを使用するため、特定のリモート パブリック IP アドレスに対して作成できる VPN 接続（ルートベース、ポリシーベース、または L2VPN）は 1 つのみとなります。
- [手順 6](#) でパブリック IP アドレスを指定した場合は、インターネット経由でアクセスできる必要があります。
- [手順 6](#) でプライベート IP アドレスを指定した場合、VTGW または Direct Connect 経由でプライベート VIF にアクセスできるように設定してください。

デフォルト ゲートウェイ ファイアウォール ルールでは、VPN 接続を経由した受信トラフィックと送信トラフィックが許可されますが、VPN トンネル経由のトラフィックを管理するにはファイアウォール ルールを作成する必要があります。

8 [BGP ローカル IP アドレス/プリフィックス長] の場合、169.254.0.0/16 サブネット内で /30 サイズの CIDR ブロックのネットワーク アドレスを入力します。

この範囲内の一部のブロックは、[予約されたネットワーク アドレス](#)にあるように予約済みです。既存のネットワークとの競合が原因で、169.254.0.0/16 サブネットのネットワークを使用できない場合は、BGP サービスからここで選択したサブネットへのトラフィックを許可するファイアウォール ルールを作成する必要があります。[コンピューティング ゲートウェイのファイアウォール ルールの追加または変更](#)を参照してください。

[BGP ローカル IP アドレス/プリフィックス長] はローカル サブネットと、その内部の IP アドレスの両方を指定します。したがって、/30 の範囲の 2 番目または 3 番目のアドレスで、/30 サフィックスを含む値を入力してください。たとえば、[BGP ローカル IP アドレス/プリフィックス長] が 169.254.32.1/30 では、ネットワーク 169.254.32.0 が作成され、169.254.32.1 がローカル BGP IP（別名、仮想トンネル インターフェイス (VTI)）として割り当てられます。

9 [BGP リモート IP アドレス] の場合、[手順 8](#) で指定した範囲で残った IP アドレスを入力します。

たとえば、[BGP ローカル IP アドレス/プリフィックス長] に 169.254.32.1/30 を指定した場合、[BGP リモート IP アドレス] には 169.254.32.2 を使用します。この VPN のオンプレミス側を構成するときは、[BGP リモート IP アドレス] に指定した IP アドレスを、そのローカル BGP IP アドレスまたは VTI アドレスとして使用します。

10 [BGP ネイバー ASN] には、オンプレミス VPN ゲートウェイの ASN を入力します。

11 [認証モード] を選択します。

- PSK 認証の場合は、[プリシェアード キー] 文字列を入力します。キーの最大長は 128 文字です。このキーは、VPN トンネルの両側で同一である必要があります。
- 証明書ベースの認証については、[IPsec VPN の証明書ベースの認証の構成](#)を参照してください。

12 [リモート プライベート IP アドレス] を指定します。

[リモート パブリック IP アドレス] を IKE ネゴシエーションのリモート ID として使用する場合は、空のままにします。オンプレミス VPN ゲートウェイが NAT デバイスの背後にある場合や、そのローカル ID に別の IP アドレスを使用する場合は、ここにその IP アドレスを入力する必要があります。

13 [トンネルの詳細パラメータ] を構成します。

パラメータ	値
[IKE プロファイル] - [IKE 暗号化]	オンプレミス VPN ゲートウェイでサポートされているフェーズ 1 (IKE) 暗号を選択します。
[IKE プロファイル] - [IKE ダイジェスト アルゴリズム]	<p>オンプレミス VPN ゲートウェイでサポートされているフェーズ 1 ダイジェスト アルゴリズムを選択します。ベスト プラクティスは、[IKE ダイジェスト アルゴリズム] と [トンネル ダイジェスト アルゴリズム] の両方に同じアルゴリズムを使用することです。</p> <p>注： [IKE 暗号化] に GCM ベースの暗号を指定する場合は、[IKE ダイジェスト アルゴリズム] を [なし] に設定します。ダイジェスト機能は GCM 暗号に不可欠です。GCM ベースの暗号を使用する場合は IKE V2 を使用する必要があります。</p>
[IKE プロファイル] - [IKE バージョン]	<ul style="list-style-type: none"> ■ IKEv1 プロトコルを開始して受け入れる場合は、[IKE V1] を指定します。 ■ IKEv2 プロトコルを開始して受け入れる場合は、[IKE V2] を指定します。GCM ベースの [IKE ダイジェスト アルゴリズム] を指定した場合は、IKEv2 を使用する必要があります。 ■ IKEv1 または IKEv2 を受け入れてから IKEv2 を開始する場合は、[IKE FLEX] を指定します。IKEv2 の開始に失敗した場合、IKE FLEX は IKEv1 にフォールバックしません。
[IKE プロファイル] - [Diffie Hellman]	オンプレミス VPN ゲートウェイでサポートされている Diffie-Hellman グループを選択します。この値は、VPN トンネルの両側で同一にする必要があります。グループ番号が大きいほど、保護は強化されます。グループ 14 以上を選択することをお勧めします。
[IPSec プロファイル] - [トンネル暗号化]	オンプレミス VPN ゲートウェイでサポートされているフェーズ 2 Security Association (SA) 暗号を選択します。
[IPSec プロファイル][トンネル ダイジェスト アルゴリズム]	<p>オンプレミス VPN ゲートウェイでサポートされているフェーズ 2 ダイジェスト アルゴリズムを選択します。</p> <p>注： [トンネルの暗号化] に GCM ベースの暗号を指定する場合は、[トンネル ダイジェスト アルゴリズム] を [なし] に設定します。ダイジェスト機能は GCM 暗号に不可欠です。</p>
[IPSec プロファイル] - [Perfect Forward Secrecy]	オンプレミス VPN ゲートウェイの設定に合わせて有効または無効にします。Perfect Forward Secrecy を有効にすると、プライベート キーが盗み取られたとしても、記録された（過去の）セッションが復号されることを回避できます。
[IPSec プロファイル] - [Diffie Hellman]	オンプレミス VPN ゲートウェイでサポートされている Diffie-Hellman グループを選択します。この値は、VPN トンネルの両側で同一にする必要があります。グループ番号が大きいほど、保護は強化されます。グループ 14 以上を選択することをお勧めします。

パラメータ	値
[DPD プロファイル] - [DPD ブローブ モード]	<p>[定期]または[オンデマンド]のいずれか。</p> <p>定期 DPD ブローブ モードの場合、指定した DPD ブローブ間隔が経過するたびに DPD ブローブが送信されます。</p> <p>オンデマンド DPD ブローブ モードの場合、アイドル期間の経過後にピア サイトから IPsec パケットが受信されないと、DPD ブローブが送信されます。使用されるアイドル期間は [DPD ブローブ間隔] の値によって決まります。</p>
[DPD プロファイル] - [再試行回数]	許可される再試行回数の整数。1~100 の範囲の値が有効です。デフォルトの再試行回数は 10 です。
[DPD プロファイル] - [DPD ブローブ間隔]	<p>DPD ブローブの送信の間に NSX IKE デーモンが待機する秒数。</p> <p>定期 DPD ブローブ モードの場合、有効な値は 3~360 秒の間です。デフォルト値は 60 秒です。</p> <p>オンデマンド ブローブ モードの場合、有効な値は 1~10 秒の間です。デフォルト値は 3 秒です。</p> <p>定期 DPD ブローブ モードを設定した場合、IKE デーモンは DPD ブローブを定期的に送信します。ピア サイトが 0.5 秒以内に応答すると、構成した DPD ブローブ間隔の経過後に次の DPD ブローブが送信されます。ピア サイトが応答しない場合は、0.5 秒待機した後に DPD ブローブが再送信されます。リモート ピア サイトが応答しない場合、応答が受信されるか再試行回数に到達するまで、IKE デーモンは DPD ブローブの再送信を繰り返します。ピア サイトの非活動が宣言されるまで、IKE デーモンは [再試行回数] プロパティに指定された最大回数に達するまで、DPD ブローブを再送信します。ピア サイトが非活動と宣言されると、NSX は、非活動ピアのリンクで Security Association (SA) を解除します。</p> <p>オンデマンド DPD モードを設定すると、構成した DPD ブローブ間隔の経過後、ピア サイトから IPsec トラフィックが受信されない場合にのみ、DPD ブローブが送信されます。</p>
[DPD プロファイル] - [管理ステータス]	DPD プロファイルを有効または無効にするには、[管理ステータス] トグルをクリックします。デフォルトでは、この値は [有効] に設定されます。DPD プロファイルを有効にすると、DPD プロファイルを使用する IPsec VPN サービスのすべての IPsec セッションに、その DPD プロファイルが使用されます。
[TCP MSS クランプ]	[TCP MSS クランプ] を使用して IPsec 接続時の TCP セッションの最大セグメント サイズ (MSS) ペイロードを削減するには、このオプションを [有効] に切り替えて、[TCP MSS の方向] を選択し、必要に応じて [TCP MSS 値] を選択します。『NSX Data Center 管理ガイド』の TCP MSS クランプの理解 を参照してください。

14 (オプション) [BGP の詳細パラメータ] で、オンプレミス ゲートウェイで 사용되는ものに対応する BGP の [シークレット] を入力します。

15 (オプション) VPN にタグを付けます。

NSX オブジェクトのタグgingについて詳しくは、『NSX Data Center 管理ガイド』の[オブジェクトへのタグの追加](#)を参照してください。

16 [保存] をクリックします。

結果

VPN の作成プロセスには数分かかることがあります。ルートベース VPN が使用可能になると、トンネルのステータスと BGP セッションの状態が表示されます。次のアクションを実行して、VPN のオンプレミス側のトラブルシューティングと設定を行うことができます。

- [設定のダウンロード] をクリックし、VPN 構成の詳細を含むファイルをダウンロードします。これらの詳細を使用して、この VPN のオンプレミスのエンドを構成できます。
- [統計情報の表示] をクリックし、この VPN のパケット トラフィックの統計情報を表示します。[VPN トンネルのステータスと統計情報の表示](#)を参照してください。
- [ルートの表示] をクリックし、この VPN でアドバタイズ済みのルートおよび学習済みのルートの表示を開きます。
- [ルートのダウンロード] をクリックし、[アドバタイズされたルート] または [学習されたルート] のリストを CSV 形式でダウンロードします。

次のステップ

必要に応じて、ファイアウォール ルールを作成または更新します。ルート ベース VPN を経由するトラフィックを許可するには、[適用先] フィールドで [VPN トンネル インターフェイス] を指定します。[すべてのアップリンク] オプションには、ルーティングが設定された VPN トンネルは含まれません。

ポリシー ベース VPN の作成

ポリシーベースの VPN では、IPsec トンネルと、トラフィックによるトンネルの使用方法を指定するポリシーが作成されます。ポリシーベースの VPN を使用する場合は、新しいルートを追加するときに、ネットワークの両端でルーティング テーブルを更新する必要があります。

注： このトピックでは、SDDC のデフォルトのパブリック IP アドレスまたはプライベート IP アドレスに接続するポリシーベース VPN の作成方法について説明します。追加の Tier-1 ゲートウェイが配置された SDDC ([VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加](#)を参照) がある場合は、[NSX Manager を開く] をクリックし、これらのゲートウェイを終端とする VPN サービスを追加できます。『NSX Data Center 管理ガイド』の [VPN サービスの追加](#)を参照してください。

VMware Cloud on AWS では、Tier-1 ゲートウェイに対する VPN サービスは BGP をサポートしていません。

VMware Cloud on AWS SDDC 内のポリシーベースの VPN では、IPsec プロトコルを使用してトラフィックが保護されます。ポリシーベースの VPN を作成するには、ローカル (SDDC) エンドポイントを構成してから、一致するリモート (オンプレミス) エンドポイントを構成します。すべてのポリシーベースの VPN では、ネットワークごとに新しい IPsec Security Association (SA) を作成する必要があるため、管理者は、新しいポリシーベースの VPN が作成されるたびに、オンプレミスと SDDC のルーティング情報を更新する必要があります。VPN のいずれかの両端のネットワークの数が少ない場合、またはオンプレミスのネットワーク ハードウェアで BGP (ルートベースの VPN に必要) がサポートされていない場合は、ポリシーベースの VPN を選択することをお勧めします。

重要： SDDC にポリシーベース VPN 接続と別の接続 (ルートベース VPN、DX、VTGW など) が両方含まれる場合、これらのいずれかの接続がデフォルト ルート (0.0.0.0/0) を SDDC にアドバタイズすると、ポリシーベース VPN 経由の接続は失敗します。これらの他の接続のいずれもデフォルト ルートをアドバタイズしない場合、VPN のポリシーに一致するすべてのトラフィックは、他の接続によってより具体的なルートが提供されても、VPN を通ります。重複する場合は、ポリシーベースの VPN ポリシーの一致よりもルートベースの VPN ルートが優先されます。

手順

- 1 <https://vmc.vmware.com> から VMware Cloud コンソール にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。 [NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [VPN] - [ポリシー ベース] - [VPN の追加] の順にクリックして、新しい VPN に [名前] とオプションの [説明] を指定します。
- 5 ドロップダウン メニューから [ローカル IP アドレス] を選択します。
 - 現在の SDDC が SDDC グループのメンバーの場合、または AWS Direct Connect を使用する構成になっている場合は、VPN でインターネット経由の接続ではなく、その接続を使用できるように、プライベート IP アドレスを選択します。Direct Connect または VMware Managed Transit Gateway (VTGW) 経由の VPN トラフィックは、より高い MTU がリンクでサポートされていても、デフォルト MTU の 1,500 バイトが上限になるので注意してください。 [SDDC の管理およびコンピューティング ネットワーク トラフィック用のプライベート仮想インターフェイスに対する Direct Connect の構成](#) を参照してください。
 - インターネット経由で VPN を接続する場合は、パブリック IP アドレスを選択します。

- 6 オンプレミス ゲートウェイの [リモート パブリック IP アドレス] を入力します。

このアドレスは、別の VPN でまだ使用されていないアドレスである必要があります。VMware Cloud on AWS はすべての VPN 接続に同じパブリック IP アドレスを使用するため、特定のリモート パブリック IP アドレスに対して作成できる VPN 接続 (ルートベース、ポリシーベース、または L2VPN) は 1 つのみとなります。 [手順 5](#) でパブリック IP アドレスを指定した場合は、このアドレスにインターネット経由でアクセスできる

必要があります。プライベート IP アドレスを指定した場合は、プライベート VIF への Direct Connect 経由でそのアドレスにアクセスできる必要があります。デフォルト ゲートウェイ ファイアウォール ルールでは、VPN 接続を経由した受信トラフィックと送信トラフィックが許可されますが、VPN トンネル経由のトラフィックを管理するにはファイアウォール ルールを作成する必要があります。

7 この VPN が接続できる [リモート ネットワーク] を指定します。

このリストには、オンプレミス VPN ゲートウェイによってローカルと定義されたすべてのネットワークが含まれている必要があります。各ネットワークは CIDR 形式で入力し、複数の CIDR ブロックはカンマで区切ります。

8 この VPN が接続できる [ローカル ネットワーク] を指定します。

このリストには、SDDC 内のすべてのルーティングされたコンピューティング ネットワーク、および管理ネットワークとアプライアンス サブネット (ESXi ホスト以外の、vCenter Server などの管理アプライアンスを含む管理ネットワークのサブセット) が含まれます。また、コンピューティング ゲートウェイ DNS ネットワーク (コンピューティング ゲートウェイ DNS サービスによって転送される要求の送信元を明らかにするための単一の IP アドレス) も含まれます。

9 [認証モード] を選択します。

- PSK 認証の場合は、[プリシェアード キー] 文字列を入力します。キーの最大長は 128 文字です。このキーは、VPN トンネルの両側で同一である必要があります。
- 証明書ベースの認証については、[IPsec VPN の証明書ベースの認証の構成](#)を参照してください。

10 (オプション) オンプレミス ゲートウェイが NAT デバイスの背後にある場合は、そのゲートウェイのアドレスを [リモート プライベート IP アドレス] として入力します。

この IP アドレスは、オンプレミス VPN ゲートウェイによって送信されるローカル ID (IKE ID) と一致する必要があります。このフィールドが空の場合は、[リモート パブリック IP アドレス] フィールドがオンプレミス VPN ゲートウェイのローカル ID との照合に使用されます。

11 [トンネルの詳細パラメータ] を構成します。

パラメータ	値
[IKE プロファイル] - [IKE 暗号化]	オンプレミス VPN ゲートウェイでサポートされているフェーズ 1 (IKE) 暗号を選択します。
[IKE プロファイル] - [IKE ダイジェスト アルゴリズム]	<p>オンプレミス VPN ゲートウェイでサポートされているフェーズ 1 ダイジェスト アルゴリズムを選択します。ベスト プラクティスは、[IKE ダイジェスト アルゴリズム] と [トンネル ダイジェスト アルゴリズム] の両方に同じアルゴリズムを使用することです。</p> <p>注： [IKE 暗号化] に GCM ベースの暗号を指定する場合は、[IKE ダイジェスト アルゴリズム] を [なし] に設定します。ダイジェスト機能は GCM 暗号に不可欠です。GCM ベースの暗号を使用する場合は IKE V2 を使用する必要があります。</p>

パラメータ	値
[IKE プロファイル] - [IKE バージョン]	<ul style="list-style-type: none"> ■ IKEv1 プロトコルを開始して受け入れる場合は、[IKE V1] を指定します。 ■ IKEv2 プロトコルを開始して受け入れる場合は、[IKE V2] を指定します。GCM ベースの [IKE ダイジェスト アルゴリズム] を指定した場合は、IKEv2 を使用する必要があります。 ■ IKEv1 または IKEv2 を受け入れてから IKEv2 を開始する場合は、[IKE FLEX] を指定します。IKEv2 の開始に失敗した場合、IKE FLEX は IKEv1 にフォールバックしません。
[IKE プロファイル] - [Diffie Hellman]	オンプレミス VPN ゲートウェイでサポートされている Diffie-Hellman グループを選択します。この値は、VPN トンネルの両側で同一にする必要があります。グループ番号が大きいほど、保護は強化されます。グループ 14 以上を選択することをお勧めします。
[IPSec プロファイル] - [トンネル暗号化]	オンプレミス VPN ゲートウェイでサポートされているフェーズ 2 Security Association (SA) 暗号を選択します。
[IPSec プロファイル][トンネル ダイジェスト アルゴリズム]	<p>オンプレミス VPN ゲートウェイでサポートされているフェーズ 2 ダイジェスト アルゴリズムを選択します。</p> <p>注： [トンネルの暗号化] に GCM ベースの暗号を指定する場合は、[トンネル ダイジェスト アルゴリズム] を [なし] に設定します。ダイジェスト機能は GCM 暗号に不可欠です。</p>
[IPSec プロファイル] - [Perfect Forward Secrecy]	オンプレミス VPN ゲートウェイの設定に合わせて有効または無効にします。Perfect Forward Secrecy を有効にすると、プライベート キーが盗み取られたとしても、記録された（過去の）セッションが復号されることを回避できます。
[IPSec プロファイル] - [Diffie Hellman]	オンプレミス VPN ゲートウェイでサポートされている Diffie-Hellman グループを選択します。この値は、VPN トンネルの両側で同一にする必要があります。グループ番号が大きいほど、保護は強化されます。グループ 14 以上を選択することをお勧めします。
[DPD プロファイル] - [DPD ブローブ モード]	<p>[定期]または[オンデマンド]のいずれか。</p> <p>定期 DPD ブローブ モードの場合、指定した DPD ブローブ間隔が経過するたびに DPD ブローブが送信されます。</p> <p>オンデマンド DPD ブローブ モードの場合、アイドル期間の経過後にピア サイトから IPsec パケットが受信されないと、DPD ブローブが送信されます。使用されるアイドル期間は [DPD ブローブ間隔] の値によって決まります。</p>
[DPD プロファイル] - [再試行回数]	許可される再試行回数の整数。1~100 の範囲の値が有効です。デフォルトの再試行回数は 10 です。

パラメータ	値
[DPD プロファイル] - [DPD ブローブ間隔]	<p>DPD ブローブの送信の間に NSX IKE デーモンが待機する秒数。</p> <p>定期 DPD ブローブ モードの場合、有効な値は 3~360 秒の間です。デフォルト値は 60 秒です。</p> <p>オンデマンド ブローブ モードの場合、有効な値は 1~10 秒の間です。デフォルト値は 3 秒です。</p> <p>定期 DPD ブローブ モードを設定した場合、IKE デーモンは DPD ブローブを定期的に送信します。ピア サイトが 0.5 秒以内に応答すると、構成した DPD ブローブ間隔の経過後に次の DPD ブローブが送信されます。ピア サイトが応答しない場合は、0.5 秒待機した後に DPD ブローブが再送信されます。リモート ピア サイトが応答しない場合、応答が受信されるか再試行回数に到達するまで、IKE デーモンは DPD ブローブの再送信を繰り返します。ピア サイトの非活動が宣言されるまで、IKE デーモンは [再試行回数] プロパティに指定された最大回数に達するまで、DPD ブローブを再送信します。ピア サイトが非活動と宣言されると、NSX は、非活動ピアのリンクで Security Association (SA) を解除します。</p> <p>オンデマンド DPD モードを設定すると、構成した DPD ブローブ間隔の経過後、ピア サイトから IPsec トラフィックが受信されない場合にのみ、DPD ブローブが送信されます。</p>
[DPD プロファイル] - [管理ステータス]	<p>DPD プロファイルを有効または無効にするには、[管理ステータス] トグルをクリックします。デフォルトでは、この値は [有効] に設定されます。DPD プロファイルを有効にすると、DPD プロファイルを使用する IPsec VPN サービスのすべての IPsec セッションに、その DPD プロファイルが使用されます。</p>
[TCP MSS クランプ]	<p>[TCP MSS クランプ] を使用して IPsec 接続時の TCP セッションの最大セグメント サイズ (MSS) ペイロードを削減するには、このオプションを [有効] に切り替えて、[TCP MSS の方向] を選択し、必要に応じて [TCP MSS 値] を選択します。『NSX Data Center 管理ガイド』の TCP MSS クランプの理解を参照してください。</p>

12 (オプション) VPN にタグを付けます。

NSX オブジェクトのタギングについて詳しくは、『NSX Data Center 管理ガイド』の[オブジェクトへのタグの追加](#)を参照してください。

13 [保存] をクリックします。

結果

VPN の作成プロセスには数分かかることがあります。ポリシーベースの VPN が使用可能になると、次のアクションを実行して、VPN のオンプレミス側のトラブルシューティングと設定を行うことができますようになります。

- [設定のダウンロード] をクリックし、VPN 構成の詳細を含むファイルをダウンロードします。これらの詳細を使用して、この VPN のオンプレミスのエンドを構成できます。
- [統計情報の表示] をクリックし、この VPN のパケット トラフィックの統計情報を表示します。[VPN トンネルのステータスと統計情報の表示](#)を参照してください。

次のステップ

必要に応じて、ファイアウォール ルールを作成または更新します。ポリシー ベース VPN を経由するトラフィックを許可するには、[適用先] フィールドで [インターネット インターフェイス] を指定します。

IPsec VPN の証明書ベースの認証の構成

証明書ベースの VPN では、IKE ネゴシエーション時にプリシェアード キーではなくデジタル証明書を使用します。

ルートベースまたはポリシーベースの VPN で証明書ベースの認証を使用できます。

IPsec VPN に対する証明書ベースの認証では、各エンドポイントが IKE ネゴシエーション時に証明書を提示します。両方のエンドポイントで共通の認証局 (CA) を共有する必要があります。各エンドポイントは、IP アドレスや CIDR ではなく、ピア証明書の属性 (DN、E メール ID、証明書内の IP アドレスなど) をリモート ID として使用して構成されます。

前提条件

NSX Manager に必要なサーバ証明書または CA 証明書がない場合は、証明書をインポートします。[自己署名証明書または CA 署名付き証明書のインポート](#)および[CA 証明書のインポート](#)を参照してください。

証明書をインポートする場合は、インポートを許可する管理ゲートウェイのファイアウォール ルールを作成する必要があります。ルールで使用する送信元アドレスとポート番号を認証局に確認してください。

手順

- 1 SDDC ゲートウェイでローカル VPN エンドポイントを構成し、その証明書を選択します。

SDDC コンピューティング ゲートウェイ (T0) には、デフォルトでローカル エンドポイントがプロビジョニングされます。VPN をカスタム T1 ゲートウェイに接続する場合は、そのゲートウェイに[ローカル エンドポイントを追加する](#)必要があります。

ローカル エンドポイントに関連する証明書から派生するローカル ID は、証明書に含まれている X509v3 拡張機能によって異なります。ローカル ID は、X509v3 拡張機能の Subject Alternative Name (SAN) または識別名 (DN) のいずれかになります。[ローカル ID] は不要です。指定した ID は無視されます。ただし、リモート VPN ゲートウェイの場合は、ピア VPN ゲートウェイでローカル ID をリモート ID として構成する必要があります。

- 証明書に X509v3 Subject Alternative Name がある場合、SAN 文字列の 1 つがローカル ID 値として取得されます。

証明書に複数の SAN フィールドがある場合は、次の順序でローカル ID を選択します。

順序	SAN フィールド
1	IP アドレス
2	DNS
3	メール アドレス

たとえば、構成されたサイトの証明書に次の SAN フィールドがあるとしします。

```
X509v3 Subject Alternative Name:
DNS:Site123.vmware.com, email:user1@company.com, IP Address:1.1.1.1
```

この場合、IP アドレス 1.1.1.1 がローカル ID として使用されます。IP アドレスが使用できない場合は、DNS 文字列が使用されます。IP アドレスと DNS が使用できない場合は、メール アドレスが使用されます。

- 証明書に X509v3 Subject Alternative Name が存在しない場合、識別名 (DN) がローカル ID 値として使用されます。

たとえば、証明書に SAN フィールドがなく、次の DN 文字列があるとしします。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123
```

この場合、DN 文字列がローカル ID として自動的に使用されます。ローカル ID はリモート サイトのピア ID になります。

2 VPN の証明書ベースの認証を構成します。

- [認証モード] ドロップダウン メニューから [証明書] を選択します。
- [リモート プライベート IP アドレス/リモート ID] テキスト ボックスに、ピア サイトを識別する値を入力します。

リモート ID は、ピア サイトの証明書で使用される識別名 (DN)、IP アドレス、DNS、またはメール アドレスにする必要があります。

注： たとえば、次のようにピア サイトの証明書で識別名 (DN) にメール アドレスが含まれている場合、

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

次の形式で [リモート ID] の値を入力します。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com
```

レイヤー 2 VPN および拡張ネットワーク セグメントの構成

VMware Cloud on AWS のレイヤー 2 仮想プライベート ネットワーク (L2VPN) を使用して、オンプレミス ネットワークを SDDC の 1 つ以上の VLAN ベースのネットワークに拡張できます。この拡張ネットワークは、単一のブロードキャスト ドメインを持つ単一のサブネットです。この拡張ネットワークでは、クラウド SDDC に対して、仮想マシンを、その IP アドレスを変更せずに移行できます。

データセンターの移行に加えて、ディザスタ リカバリ、または必要に応じてクラウド コンピューティング リソース への動的アクセス（別名「クラウド バースト」）に拡張 L2VPN ネットワークを使用できます。

VMware Cloud on AWS は NSX を使用して、クラウド SDDC 内で L2VPN サーバを提供します。L2VPN クライアント機能は、オンプレミスの NSX Edge によって提供されます。L2VPN の制約については、[VMware 構成の上限](#)を参照してください。

VMware Cloud on AWS の L2VPN 機能は、VLAN ネットワークの拡張をサポートします。NSX サーバへの L2VPN 接続は IPsec トンネルを使用します。L2VPN の拡張ネットワークは、仮想マシン ネットワークを拡張してワークロードのトラフィックを伝送するためにのみ使用されます。このネットワークは移行トラフィック（ESXi の管理または vMotion）に使用される VMkernel ネットワークから独立しています。VMkernel ネットワークでは、個別の IPsec VPN または Direct Connect 接続が使用されます。

重要： L2VPN クライアントおよびサーバを構成し、クライアントに割り当てられたトンネル ID を指定する拡張ネットワークを作成するまで、L2VPN トンネルは起動できません。

手順

1 SDDC でのレイヤー 2 VPN トンネルの設定

ローカル (SDDC) とリモート (オンプレミス) の IP アドレスを指定して、レイヤー 2 VPN トンネルの SDDC 側を作成します。

2 レイヤー 2 VPN の拡張セグメントの構成

拡張ネットワークには、オンプレミス ネットワークとクラウド SDDC 内のネットワーク間をセキュアな通信トンネルで接続する、レイヤー 2 仮想プライベート ネットワーク (L2VPN) が必要です。

3 オンプレミス NSX Edge のインストールと構成

L2VPN のオンプレミス側は、NSX Edge アプライアンスである必要があります。L2VPN を作成するには、このアプライアンスおよび関連するオンプレミスの vSphere ネットワークを構成する必要があります。

SDDC でのレイヤー 2 VPN トンネルの設定

ローカル (SDDC) とリモート (オンプレミス) の IP アドレスを指定して、レイヤー 2 VPN トンネルの SDDC 側を作成します。

注： このトピックでは、SDDC のデフォルトのパブリック IP アドレスまたはプライベート IP アドレスに接続するレイヤー 2 VPN の作成方法について説明します。追加の Tier-1 ゲートウェイが配置された SDDC（[VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加](#)を参照）がある場合は、[NSX Manager を開く] をクリックし、これらのゲートウェイを終端とする VPN サービスを追加できます。『NSX Data Center 管理ガイド』の [VPN サービスの追加](#)を参照してください。

VMware Cloud on AWS では、オンプレミス環境と SDDC の間で 1 つのレイヤー 2 VPN トンネルがサポートされます。

手順

1 <https://vmc.vmware.com> から VMware Cloud コンソール にログインします。

2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。

3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [VPN] - [レイヤー 2] の順にクリックします。
- 5 [VPN トンネルの追加] をクリックします。
- 6 VPN パラメータを構成します。

オプション	説明
ローカル IP アドレス	<ul style="list-style-type: none"> ■ この SDDC で AWS Direct Connect を構成していて、それを VPN で使用する場合は、プライベート IP アドレスを選択します。SDDC の管理およびコンピューティング ネットワーク トラフィック用のプライベート仮想インターフェイスに対する Direct Connect の構成を参照してください。 ■ VPN をインターネット経由で SDDC に接続する場合は、パブリック IP アドレスを選択します。
リモート パブリック IP アドレス	オンプレミス L2VPN ゲートウェイのリモート パブリック IP アドレスを入力します。L2VPN の場合、これは常にスタンドアローンの NSX Edge アプライアンスです (オンプレミス NSX Edge のインストールと構成 を参照)。
リモート プライベート IP アドレス	オンプレミスのゲートウェイが NAT の背後に構成されている場合は、リモートのプライベート IP アドレスを入力します。

注： 最大セグメント サイズ (MSS) を削減するために、SDDC バージョン 1.15 以降のレイヤー 2 VPN では TCP TMSS クランプが常に有効になります。

- 7 (オプション) VPN にタグを付けます。

NSX オブジェクトのタグgingについて詳しくは、『[NSX Data Center 管理ガイド](#)』の[オブジェクトへのタグの追加](#)を参照してください。

- 8 (オプション) [説明] を追加します。
- 9 [保存] をクリックします。

SDDC 環境によっては、レイヤー 2 VPN の作成プロセスに数分かかる場合があります。レイヤー 2 VPN トンネルが使用可能になると、ステータスが [UP] に変わります。

レイヤー 2 VPN の拡張セグメントの構成

拡張ネットワークには、オンプレミス ネットワークとクラウド SDDC 内のネットワーク間をセキュアな通信トンネルで接続する、レイヤー 2 仮想プライベート ネットワーク (L2VPN) が必要です。

このトンネルの両端に ID が設定されています。クラウド SDDC およびトンネルのオンプレミス側でトンネル ID が一致する場合は、2 つのネットワークが同じブロードキャスト ドメインに属します。拡張ネットワークは、デフォルト ゲートウェイとしてオンプレミス ゲートウェイを使用します。DHCP および DNS などの他のネットワーク サービスもオンプレミスで提供されます。

論理ネットワークは、ルーティングから拡張ネットワークへ、または拡張ネットワークからルーティングへ変更できます。たとえば、論理ネットワークを拡張ネットワークとして設定し、オンプレミス データセンターからクラウド SDDC へ仮想マシンの移行することができます。移行が完了したら、ルーティングに変更して、仮想マシンに VMware Cloud on AWS ネットワーク サービスの使用を許可することができます。

前提条件

レイヤー 2 VPN トンネルが使用可能であることを確認します。[SDDC でのレイヤー 2 VPN トンネルの設定](#) を参照してください。

手順

- 1 <https://vmc.vmware.com> から VMware Cloud コンソール にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 L2VPN トンネルのトンネル ID にバインドされた拡張セグメントを作成するには、[ネットワーク セグメントの作成または変更](#)の手順を実行します。
- 5 [保存] をクリックします。
- 6 [設定のダウンロード] をクリックして、ピアコードなどの、リモート側の VPN 構成のオンプレミスを設定するときに必要な情報を含むファイルをダウンロードします。
- 7 L2VPN のクライアント側を構成します。

[オンプレミス NSX Edge のインストールと構成](#)を参照してください。

オンプレミス NSX Edge のインストールと構成

L2VPN のオンプレミス側は、NSX Edge アプライアンスである必要があります。L2VPN を作成するには、このアプライアンスおよび関連するオンプレミスの vSphere ネットワークを構成する必要があります。

互換性がある NSX のバージョンをオンプレミス データセンターにインストールしている場合は、SDDC に接続する L2VPN のオンプレミス (クライアント) 側として既存の NSX Edge アプライアンスを使用できます。必要に応じて、L2VPN クライアントとして使用するスタンドアローン NSX Edge をダウンロードし、展開できます。

次の表に、互換性のある SDDC とオンプレミスのバージョンを示します。SDDC で実行されている NSX のバージョンを確認するには、『VMware Cloud on AWS Operations Guide』で [VMware Cloud on AWS とコンポーネント リリースの関連付け](#)を参照してください。

表 3-3. L2VPN の相互運用性

L2VPN サーバ バージョン (SDDC バージョン)	L2VPN クライアント バージョン (オンプレミス Edge)
4.1.0 (SDDC 1.22)	4.0.1.1, 3.2.2
4.0.1(SDDC 1.19, 1.20)	3.1.1, 3.2.1,4.0.0.1
3.1.5(SDDC 1.17, 1.18)	3.1.1

手順

- 1 (オプション) スタンドアローンの NSX Edge をダウンロードします。

互換性がある NSX のバージョンをオンプレミス データセンターにインストールしていない場合は、現在の L2VPN のオンプレミス エンドポイントとして使用するスタンドアローンの NSX Edge アプライアンスをダウンロードして構成できる場合があります。L2VPN のサーバ側を構成したら、[リモート L2 VPN クライアントの構成] 画面の手順に従って、[NSX Edge for VMware ESXi] を OVF ファイルとしてダウンロードします。

- 2 NSX Edge をインストールして構成します。

オンプレミスの vCenter Server に自律エッジをインストールして構成する方法の詳細については、『NSX Data Center 管理ガイド』の [L2 VPN クライアントとしての自律エッジの追加](#)を参照してください。

VPN トンネルのステータスと統計情報の表示

SDDC NSX Manager には、IPsec VPN セグメントと L2VPN セグメントのステータスと統計情報が表示されます。

VPN 操作のステータスは、[VPN] 画面に表示されます。この画面は、[ネットワークとセキュリティ] タブにあります。また、VPN 操作に関するログ メッセージは、オプションの SDDC 統合サービスである VMware Aria Operations for Logs にも送信されます。詳細については、[VMware Aria Automation クラウド サービスの使用](#)および [VMware Aria Operations for Logs ドキュメント](#)を参照してください。


手順


- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [VPN] 画面で、[ルート ベース]、[ポリシー ベース]、または [レイヤー 2] をクリックして、選択したタイプの VPN を一覧表示します。

次のいずれかの操作を実行します。

- 情報アイコン  をクリックすると、ステータス メッセージが表示され、チャンネル (IKE フェーズ 1 ネゴシエーション) とトンネルのステータスに関するその他の情報を確認できます。
- 行を展開して VPN の詳細を表示してから、[統計情報を表示] をクリックしてトラフィックの統計情報を表示します。すべてのトンネル、または選択した VPN (0.0.0.0/0) によって使用されるトンネルについて、集計されたステータスと統計情報を取得できます。集計された統計情報を表示する際には、[統計情報] 列の [詳細情報の表示] をクリックすると、エラーの統計情報のリストを表示できます。

- 更新アイコン  をクリックすると、トンネルの統計情報が更新されます。トンネルが無効になった場合や再度有効になった場合は、VPN 関連のすべての統計情報が 0 にリセットされます。

次のステップ

VPN 接続の問題のトラブルシューティングについては、『NSX Data Center 管理ガイド』の [Virtual Private Network \(VPN\) のトラブルシューティング](#)を参照してください。

IPsec VPN 設定リファレンス

IPsec VPN のオンプレミス側の設定は、その VPN の Software-Defined Data Center (SDDC) 側で指定した設定と同じにする必要があります。

次の表は、SDDC IPsec VPN 設定の概要を示したものです。設定には変更可能なものと、変更できない固定的なものがあります。この情報を使用して、オンプレミスの VPN ソリューションを SDDC 内の VPN ソリューションと一致するように設定できるかどうかを確認してください。以下の表に記載されたすべての固定設定と、変更可能な任意の設定をサポートするオンプレミスの VPN ソリューションを選択します。

Diffie-Hellman グループが IPsec VPN のパフォーマンスとセキュリティに与える影響について

IPsec VPN 構成では、Diffie-Hellman (DH) グループを選択する必要があります。これは、IKE ネゴシエーションの両フェーズで、信頼されていないパスを介してエンドポイント間でプライベート キーを安全にやり取りする際に使用されます。DH グループ 19 ~ 21 は、グループ 14 ~ 16 に比べてセキュリティが大幅に強化され、暗号化時のリソース使用が少なくなります。NIST の [Guide to IPsec VPNs](#) (PDF) では、これらと IPsec VPN 構成の他の選択肢について非常に詳細に説明しています。

注： DH グループ 2 と 5 は NIST で非承認のため、古いオンプレミス デバイスとの互換性のために必要な場合にかぎり使用してください。

ベスト プラクティスとして、構成可能な設定は両フェーズで同じにする必要があります。

フェーズ 1 (IKE プロファイル) IPsec VPN 設定

表 3-4. 構成可能な設定

属性	使用可能な値	推奨値
プロトコル	IKEv1、IKEv2、IKE FLEX	IKEv2
暗号化アルゴリズム	AES (128、256)、AES-GCM (128、192、256)	AES GCM 暗号化のビット深度を大きくすると、解読が難しくなりますが、エンドポイント デバイスの負荷が増えます。
トンネル/IKE ダイジェスト アルゴリズム	SHA1、SHA2 (256、384、512)	[IKE 暗号化] に GCM ベースの暗号を指定する場合は、[IKE ダイジェスト アルゴリズム] を [なし] に設定します。ダイジェスト機能は GCM 暗号に不可欠です。GCM ベースの暗号を使用する場合は IKE V2 を使用する必要があります
Diffie Hellman (DH)	DH グループ 2、5、14 ~ 16、19 ~ 21	DH グループ 19 ~ 21 または 14 ~ 16

表 3-5. 固定設定

属性	値
ISAKMP モード	Main モード
ISAKMP/IKE SA ライフタイム	86,400 秒 (24 時間)
IPsec モード	トンネル
IKE 認証	PSK (Pre Shared Key)

フェーズ 2 (IPsec プロファイル) IPsec VPN 設定

構成可能な設定は、フェーズ 1 とフェーズ 2 で同じです。

表 3-6. 構成可能な設定

属性	使用可能な値	推奨値
プロトコル	IKEv1、IKEv2、IKE FLEX	IKEv2
暗号化アルゴリズム	AES (128、256)、AES-GCM (128、192、256)	AES GCM 暗号化のビット深度を大きくすると、解読が難しくなりますが、エンドポイント デバイスの負荷が増えます。
トンネル/IKE ダイジェスト アルゴリズム	SHA-1、SHA2(256、384、512)	[IKE 暗号化] に GCM ベースの暗号を指定する場合は、[IKE ダイジェスト アルゴリズム] を [なし] に設定します。ダイジェスト機能は GCM 暗号に不可欠です。GCM ベースの暗号を使用する場合は IKE V2 を使用する必要があります
Diffie Hellman (DH)	DH グループ 2、5、14 ~ 16、19 ~ 21	DH グループ 19 ~ 21 または 14 ~ 16

表 3-7. 固定設定

属性	値
トンネル モード	ESP (Encapsulating Security Payload)
SA ライフタイム	3600 秒 (1 時間)

オンプレミス IPsec VPN の設定

VPN 構成の詳細を含むファイルをダウンロードするには、VPN のステータス ページで [設定のダウンロード] をクリックします。これらの詳細を使用して、VPN のオンプレミスのエンドを構成できます。

注： VPN のオンプレミス側では、アイドル タイムアウト（たとえば、NSX の [セッション アイドル タイムアウト]）を構成しないでください。オンプレミスのアイドル タイムアウトを設定すると、VPN の切断が断続的に発生する可能性があります。

VMware Tech Zone の [IPsec VPN 構成リファレンス](#)では、エンドポイントの構成に関する詳細なアドバイスを提供しています。また、VMware {code} では、一般的なエンドポイント デバイスのサンプル構成ファイルが入手できます。

■ Palo Alto Networks のファイアウォール

VMware Cloud on AWS における VPN の問題のトラブルシューティング

VPN の問題には、認証エラー（IKE フェーズ 1 およびフェーズ 2）や接続（ピアが応答しない）の問題が含まれる場合があります。

IPsec VPN セッションまたはトンネルが停止すると、NSX アラームが発生し、停止アラームの理由が NSX Manager ユーザー インターフェイスの [アラーム] ダッシュボードまたは [VPN] 画面に表示されます。『NSX 管理ガイド』の「[IPsec VPN セッションまたはトンネルが停止したときのアラーム](#)」を参照してください。

■ VPN ピアが応答しない

「ピアが応答していません」というメッセージが表示されて VPN が停止した場合、ネットワークの停止、ファイアウォール ルールの欠落や構成ミスなど、さまざまな根本原因が考えられます。

■ VPN 認証エラー

通常、VPN 認証エラーは SDDC とオンプレミス VPN エンドポイント間の構成の不一致が原因で発生します。通常、これらのエラーにより作成時に VPN の起動が妨げられますが、いずれか 1 台のエンドポイントが再構成されたときに動作中の VPN を停止させる可能性もあります。

VPN ピアが応答しない

「ピアが応答していません」というメッセージが表示されて VPN が停止した場合、ネットワークの停止、ファイアウォール ルールの欠落や構成ミスなど、さまざまな根本原因が考えられます。

問題

作成後に新しい VPN が起動しない。またはいずれか 1 台のエンドポイントが更新または再構成された後、あるいはルート テーブルが変更された後に動作中の VPN が機能を停止する。

原因

ping などのコマンドを使用して到達可能性を検証できる他のエンドポイントとは異なり、VPN 自体の外部で VPN 接続を検証することはできません。IPsec では UDP を使用するため、ピアから応答を取得するか、または取得しません。ping の到達可能性は、ピアが ping を有効にしているかどうかによって異なり、多くのピアでは有効にしていません。

解決方法

- 1 VPN で構成されたリモート IP アドレスが、ピアがリッスンする IP アドレスと一致していることを確認します。
- 2 リモート（オンプレミス）サイトのすべてのファイアウォールが UDP ポート 500 へのトラフィックを許可するように構成されていることを確認します。リモート エンドポイントが NAT 処理されている場合、リモートサイトのファイアウォールは UDP ポート 4500 へのトラフィックを許可する必要があります。

- 3 IPsec VPN トラフィックでは複数のプロトコルを使用します。すべてのプロトコルをファイアウォール経由で許可する必要があります。

一般的に次の設定を行います。

- ESP (Encapsulating Security Payload) IP プロトコル 50
- AH (認証ヘッダー) - IP プロトコル 51
- ISAKMP (Internet Security Association and Key Management Protocol)、続いて IKE と IKE v2 (インターネット キー交換) を使用

- 4 両方のエンドポイントに同じ IKE バージョンが構成されていることを確認します。

- 5 それぞれの側が相互に到達できるようにルーティングが設定されていることを確認します。

これは traceroute を使用して検証できますが、多くのエンドポイントは標準の ICMP エコー (ping) または traceroute 要求に応答しないため、エンドツーエンドのパス検証が常に可能とは限りません。SDDC VPN の [ローカル IP アドレス] をパブリックとして構成すると、VPN トラフィックは常に SDDC インターネット ゲートウェイを通過します。それ以外の場合 (VPN の [ローカル IP アドレス] がプライベートの場合)、VPN トラフィックは SDDC の [イントラネット] アップリンクを通過します。VPN のリモート側が同じパスを介して応答トラフィックを送信していることを確認してください。

VPN 認証エラー

通常、VPN 認証エラーは SDDC とオンプレミス VPN エンドポイント間の構成の不一致が原因で発生します。通常、これらのエラーにより作成時に VPN の起動が妨げられますが、いずれか 1 台のエンドポイントが再構成されたときに動作中の VPN を停止させる可能性もあります。

問題

作成後に新しい VPN が起動しない。またはいずれか 1 台のエンドポイントが更新または再構成された後に動作中の VPN が機能を停止する。

原因

IKE ネゴシエーションには、次の 2 つのフェーズがあります。

- フェーズ 1 では、ピア エンドポイントが IKE Security Association (SA) を確立し、エンドポイント間の通信にセキュアなチャネルを提供します。
- フェーズ 2 では、エンドポイントが SA を使用して、VPN の作成時に入力したプリシェアード キーを通じてキー交換をネゴシエートします。

フェーズ 1 のエラーは、リモート ID とローカル ID の値に一貫性がない場合に発生する可能性があります。フェーズ 2 のエラーは、異なるプリシェアード キーがピアに構成されている場合に発生する可能性があります。

解決方法

- 1 各側のプリシェアード キーが同一であることを確認します。キー文字列の両端に空白があることを確認します。
- 2 プリシェアード キーで特殊文字を使用している場合は、(一方の側で特殊文字が正しく解釈されない場合に備えて) 特殊文字を含まないプリシェアード キーを試してください。

- 3 それぞれの側のリモート ID がピアで使用するローカル ID と一致していることを確認します。通常、これはパブリック IP アドレスですが、一方の側が NAT ルーターの背後にある場合は、代わりにプライベート IP アドレスを使用できます。プライベート IP アドレスは、ピアの構成のリモート ID として手動で入力する必要があります。この ID は認証の一部を形成するため、一致しない場合は認証エラーが発生します。
- 4 両方のエンドポイントに同じ IKE バージョンが構成されていることを確認します。VMware Cloud on AWS VPN には、IKEv1 または IKEv2 と互換性のある [IKE FLEX] バージョンも用意されています。
- 5 両方のエンドポイントに同じ IKE モードが構成されていることを確認します。VMware Cloud on AWS VPN では IKE アグレッシブモードがサポートされていません。

管理ゲートウェイのネットワークおよびセキュリティの構成

管理ネットワークと管理ゲートウェイは、SDDC でほぼ事前構成されています。ただし、vCenter Server や HCX などの管理ネットワーク サービスへのアクセスを構成し、管理ネットワークと他のネットワーク（オンプレミス ネットワークやその他の SDDC ネットワークなど）間のトラフィックを許可するための管理ゲートウェイ ファイアウォール ルールを作成する必要があります。

次に参照するドキュメント

手順

1 vCenter Server の FQDN 解決アドレスの設定

SDDC vCenter Server には、パブリック IP アドレスまたはプライベート IP アドレスで接続できます。プライベート IP アドレスは、SDDC VPN から解決できます。パブリック IP アドレスは、インターネットから解決できます。

2 HCX FQDN 解決アドレスの設定

VMware HCX には、パブリック IP アドレスまたはプライベート IP アドレスで接続できます。プライベート IP アドレスは、SDDC VPN から解決できます。パブリック IP アドレスは、インターネットから解決できます。

3 管理ゲートウェイのファイアウォール ルールの追加または変更

SDDC 管理インフラストラクチャの安全性とセキュリティを維持することが重要です。デフォルトでは、管理ゲートウェイはすべての管理ネットワーク送信元からのすべての宛先へのトラフィックをブロックします。

vCenter Server の FQDN 解決アドレスの設定

SDDC vCenter Server には、パブリック IP アドレスまたはプライベート IP アドレスで接続できます。プライベート IP アドレスは、SDDC VPN から解決できます。パブリック IP アドレスは、インターネットから解決できます。

前提条件

プライベート IP アドレスで SDDC vCenter Server にアクセスできるようにするには、SDDC をオンプレミス データセンターに接続する VPN を設定する必要があります。[ルートベースの VPN の作成](#)または[ポリシー ベース VPN の作成](#)を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 SDDC の [設定] タブに移動します。
- 4 [vCenter Server の FQDN] を展開して [編集] をクリックします。
- 5 [解決アドレス] の下で、[パブリック IP アドレス] または [プライベート IP アドレス] のいずれかを選択し、[保存] をクリックします。

HCX FQDN 解決アドレスの設定

VMware HCX には、パブリック IP アドレスまたはプライベート IP アドレスで接続できます。プライベート IP アドレスは、SDDC VPN から解決できます。パブリック IP アドレスは、インターネットから解決できます。

前提条件

プライベート IP アドレスで HCX にアクセスできるようにするには、SDDC をオンプレミス データセンターに接続する VPN を設定する必要があります。[ルートベースの VPN の作成](#)または[ポリシー ベース VPN の作成](#)を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 SDDC の [設定] タブに移動します。
- 4 [HCX FQDN] を展開して [編集] をクリックします。
- 5 [解決アドレス] の下で、[パブリック IP アドレス] または [プライベート IP アドレス] のいずれかを選択し、[保存] をクリックします。

管理ゲートウェイのファイアウォール ルールの追加または変更

SDDC 管理インフラストラクチャの安全性とセキュリティを維持することが重要です。デフォルトでは、管理ゲートウェイはすべての管理ネットワーク送信元からのすべての宛先へのトラフィックをブロックします。

SDDC 管理インフラストラクチャへのアクセスを構成する場合は、SDDC 管理ネットワークへの必要なアクセスのみを許可する管理ゲートウェイのファイアウォール ルールを作成することが重要です。管理ゲートウェイにアクセスするには、[SDDC とオンプレミス データセンターの間の AWS Direct Connect の設定](#)、[SDDC とオンプレミス データセンターの間の VPN 接続の設定](#)、またはその両方を実行します。企業と SDDC 間のプライベート接続を提供する Direct Connect を単独で使用するか、IPsec VPN と組み合わせて使用してトラフィックを暗号化できます。

Direct Connect、VMware Managed Transit Gateway、または VPN を使用できない場合は、パブリック DNS および vCenter Server のパブリック IP アドレスを使用してインターネット経由で直接 SDDC vCenter Server にアクセスできます。この操作を行う場合は、信頼されていない送信元が管理ネットワークにアクセスできないようにする管理ゲートウェイのファイアウォール ルールを作成する必要があります。VPN は、暗号化と認証プロトコルを使用してセキュリティを強化します。

管理ゲートウェイのファイアウォール ルールは、送信元アドレスと宛先アドレス、およびサービス ポートに基づいて、ネットワーク トラフィックに対して実行するアクションを指定します。送信元または宛先は、システム定義のインベントリ グループである必要があります。インベントリ グループの表示または変更の詳細については、[インベントリ グループの操作](#)を参照してください。

重要： デフォルトの管理ゲートウェイのファイアウォール ルールではすべてのトラフィックが拒否されるため、vCenter Server Appliance およびその他の管理仮想マシンとアプライアンスへのアクセスを提供するには、ユーザー定義の管理ゲートウェイのファイアウォール ルールを 1 つ以上作成する必要があります。パブリック インターネットを使用して管理ゲートウェイにアクセスする際に適切なセキュリティを提供するには、自分が所有または信頼する IP アドレスからのトラフィックのみを許可する管理ゲートウェイのファイアウォール ルールを構成し、送信元 IP アドレス範囲（内部と外部の両方）を常に可能な限り最小のセットに制限します。たとえば、CIDR ブロック 93.184.216.34/30 のアドレスからインターネットにアクセスする企業は、[管理ゲートウェイのファイアウォール ルールの例](#)に示すような管理先にアクセスするために 93.184.216.34/30 の [送信元] CIDR のトラフィックのみを許可する管理ゲートウェイのファイアウォール ルールを作成する必要があります。SDDC バージョン 1.22 以降では、[任意] または 0.0.0.0/0 を含む [送信元] からのトラフィックを許可する管理ゲートウェイのファイアウォール ルールを発行することはできません。SDDC 管理インフラストラクチャへの安全なアクセスの提供の詳細については、VMware ナレッジベースの記事 [KB84154](#) を参照してください。

次の 2 種類のファイアウォール ルールがあります。

- 事前定義されたファイアウォール ルールは、VMware Cloud on AWS によって作成および管理されます。これらのルールを変更または並べ替えることはできません。事前定義された管理ゲートウェイのファイアウォール ルールを次に示します。

表 3-8. 事前定義された管理ゲートウェイのファイアウォール ルール

名前	送信元	宛先	サービス	操作
デフォルトですべて拒否	任意	任意	任意	Drop

このルールはデフォルトの拒否モードで機能するため、許可されるのは、ユーザー定義のルールで明示的に許可されるトラフィックのみです。

- ユーザー定義のファイアウォール ルールは、指定した順序で処理され、常に事前定義されたルールの前に処理されます。これらのルールでは、送信元または宛先のいずれかをシステム定義のグループにする必要があります。使用可能なポートとサービスのリストは、VMware によって管理される制限付きのリストです。[送信元] がシステム定義のグループの場合は、[サービス] を [任意] に指定する必要があります。これらのルールには [任意] のアクションが必要であるため、通常、ルールの順序は重要ではありません。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [ゲートウェイ ファイアウォール] カードで、[管理ゲートウェイ] をクリックしてから、[ルールの追加] をクリックし、新しいルールの [名前] を入力します。
- 5 新しいルールのパラメータを入力します。

パラメータはデフォルト値に初期化されます ([送信元] と [宛先] は [任意] など)。パラメータを編集するには、パラメータ値の上にマウス カーソルを移動し、鉛筆アイコン (✎) をクリックしてパラメータ固有のエディタを開きます。

オプション	説明
送信元	<p>送信元アドレス (CIDR ブロックまたは管理グループ名) の任意の組み合わせを入力します。</p> <p>重要： ファイアウォール ルールの送信元アドレスとして [任意] を選択できますが、宛先が [vCenter Server] の場合は、送信元アドレスとして [任意] またはワイルドカード 0.0.0.0/0 を使用できません。これらを使用すると、vCenter Server に対する攻撃が可能になり、SDDC が侵害される可能性があります。</p> <p>[システム定義のグループ] を選択し、次の送信元オプションのいずれかを選択します。</p> <ul style="list-style-type: none"> ■ [ESXi] を選択すると、SDDC の ESXi ホストからのトラフィックを許可します。 ■ [NSX Manager] を選択すると、SDDC の NSX アプライアンスからのトラフィックを許可します。 ■ [vCenter Server] を選択すると、SDDC の vCenter Server からのトラフィックを許可します。 ■ SDDC で有効なその他の統合サービス。 <p>[ユーザー定義のグループ] を選択すると、自分が定義した管理グループを使用できます。 インベントリ グループの操作 を参照してください。</p>
宛先	<p>任意の宛先アドレスまたはアドレスの範囲へのトラフィックを許可するには、[任意] を選択します。</p> <p>[システム定義のグループ] を選択し、次の宛先オプションのいずれかを選択します。</p> <ul style="list-style-type: none"> ■ [ESXi] を選択すると、SDDC の ESXi 管理へのトラフィックを許可します。 ■ [NSX Manager] を選択すると、SDDC の NSX アプライアンスへのトラフィックを許可します。 ■ [vCenter Server] を選択すると、SDDC の vCenter Server へのトラフィックを許可します。 ■ SDDC で有効なその他の統合サービス。
サービス	<p>ルールが適用されるサービス タイプを選択します。サービス タイプのリストは、対象の [送信元] と [宛先] によって異なります。</p>
操作	<p>新しい管理ゲートウェイのファイアウォール ルールでは [許可] アクションのみ設定できます。</p>

新しいルールはデフォルトで有効になります。トグル ボタンを左にスライドして無効にします。

- 6 [発行] をクリックして、ルールを作成します。

新しいルールには、ルールによって生成されるログ エントリで使用される、整数の [ID] 値が付与されます。

ファイアウォール ルールは、一番上から順に適用されます。デフォルトの [ドリップ] ルールが最下位にあり、その上のルールは常に [許可] ルールであるため、管理ゲートウェイ ファイアウォール ルールの順序はトラフィック フローに影響を与えません。

例：管理ゲートウェイのファイアウォール ルールの作成

オンプレミスの ESXi ホストから SDDC の ESXi ホストへの vMotion トラフィックを許可する管理ゲートウェイ ファイアウォール ルールを作成するには、次の手順を行います。

- 1 SDDC への vMotion トラフィックを許可するオンプレミス ESXi ホストが含まれた、管理インベントリ グループを作成します。
- 2 送信元に ESXi、宛先にオンプレミスの ESXi ホストを指定して、管理ゲートウェイ ルールを作成します。
- 3 また、送信元にオンプレミスの ESXi ホスト グループ、宛先に vMotion サービスを有効にした ESXi を指定して、別の管理ゲートウェイを作成します。

次のステップ

[デフォルトですべて拒否] ルール以外のルールの場合、[ルールのヒットの統計] および [フローの統計] を表示できます。



- 歯車アイコン  をクリックして、ルールのログ設定を表示または変更します。ログのエントリは、VMware VMware Aria Operations for Logs サービスに送信されます。『VMware Cloud on AWS Operations Guide』の [Using VMware Aria Operations for Logs](#) を参照してください。
- グラフ アイコン  をクリックして、ルールのヒットおよびフローの統計情報を表示します。

表 3-9. ルールのヒットの統計

ポピュラリティ インデックス	過去 24 時間にルールがトリガーされた回数。
ヒット カウント	ルールが作成されてからトリガーされた回数。

表 3-10. フローの統計

パケット数	このルールの対象となるパケット フローの合計。
バイト数	このルールの対象となるバイト フローの合計。

統計情報は、ルールが有効になるとすぐに集計が開始されます。

管理ゲートウェイのファイアウォール ルールの例

一部の一般的なファイアウォール ルールの設定には、インターネットからの vSphere Client へのアクセスの提供、管理 VPN トンネルを経由した vCenter Server へのアクセスの許可、およびリモート コンソール アクセスの許可が含まれます。

一般的に使用されるファイアウォール ルール

次の表は、一般的に使用されるファイアウォール ルールのサービス、ソースおよびターゲットの設定を示しています。

表 3-11. 一般的に使用されるファイアウォール ルール

使用事例	サービス	送信元	宛先
vCenter Server へのインターネットからのアクセスの提供。 一般的な vSphere Client アクセスおよび vCenter Server の監視に使用します。	HTTPS	オンプレミス データセンターからの IP アドレスまたは CIDR ブロック 重要： ファイアウォール ルールの送信元アドレスとして [任意] を選択できますが、宛先が [vCenter Server] の場合は、送信元アドレスとして [任意] またはワイルドカード 0.0.0.0/0 を使用できません。これらを使用すると、vCenter Server に対する攻撃が可能になり、SDDC が侵害される可能性があります。	vCenter Server
vCenter Server への VPN トンネルを経由したアクセスの提供。 管理ゲートウェイ VPN、ハイブリッド リンク モード、コンテンツライブラリに必要です。	HTTPS	オンプレミス データセンターからの IP アドレスまたは CIDR ブロック	vCenter Server
Active Directory、Platform Services Controller、コンテンツ ライブラリなどのオンプレミス サービスへの、クラウド vCenter Server からのアクセスの提供。	任意	vCenter	オンプレミス データセンターからの IP アドレスまたは CIDR ブロック
コールド移行、オンプレミスの仮想マシンからのクローン作成、スナップショットの移行、レプリケーションなどのネットワーク ファイル コピー トラフィックを含むプロビジョニング操作。	プロビジョニング	パブリックまたは VPN トンネルで接続されたオンプレミス データセンターからの IP アドレスまたは CIDR ブロック	ESXi 管理
VMRC リモート コンソール アクセス。 VMware Aria Automation に必要です。	リモート コンソール	パブリックまたは VPN トンネルで接続されたオンプレミス データセンターからの IP アドレスまたは CIDR ブロック	ESXi 管理
VPN を経由した vMotion トラフィック。	任意	ESXi 管理	オンプレミス データセンターからの IP アドレスまたは CIDR ブロック

コンピューティング ゲートウェイのネットワークおよびセキュリティを構成

コンピューティング ゲートウェイ ネットワークには、1 つ以上のセグメントを含むコンピューティング ネットワークと、ワークロード仮想マシンのネットワーク トラフィックを管理する DNS 構成、DHCP 構成、セキュリティ構成（ゲートウェイ ファイアウォールおよび分散ファイアウォール）が含まれます。また、オンプレミス ネットワー

クと SDDC ワークロード ネットワークにまたがる単一のブロードキャスト ドメインを提供するレイヤー 2 VPN と拡張ネットワークが含まれる場合もあります。

次に参照するドキュメント

手順

1 ネットワーク セグメントの作成または変更

ネットワーク セグメントは、SDDC コンピューティング ネットワークのワークロード仮想マシンによって使用される論理ネットワークです。

2 コンピューティング ゲートウェイのファイアウォール ルールの追加または変更

デフォルトでは、コンピューティング ゲートウェイは SDDC コンピューティング ネットワークとの間のトラフィックをブロックします。必要に応じて、トラフィックを許可するコンピューティング ゲートウェイのファイアウォール ルールを追加します。

3 分散ファイアウォール ルールの追加または変更

分散ファイアウォール ルールは、仮想マシン (vNIC) レベルで適用され、SDDC 内の East-West トラフィックを制御します。

4 DNS サービスの構成

VMware Cloud on AWS DNS 転送サービスは、DNS ゾーン内で実行されます。これにより、ゾーン内のワークロード仮想マシンは、完全修飾ドメイン名を IP アドレスに解決できるようになります。

5 VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理

SDDC 展開グループは、VMware Transit Connect を使用して、グループ内の SDDC 間にバンド幅が大きく、遅延の小さい接続を提供します。SDDC グループには、所有する VPC を含めることができます。AWS Direct Connect Gateway (DXGW) を追加し、グループ メンバーとオンプレミス SDDC の間の接続を提供することもできます。

6 VMware Transit Connect を通じて学習およびアドバタイズされたルートの表示

SDDC グループのメンバーである SDDC では、[Transit Connect] 画面を開き、グループ用に作成された VMware Transit Connect インスタンスによって学習およびアドバタイズされたルートを表示できます。

7 アップリンクに関する統計情報の表示と設定の管理

[グローバル構成] 画面には、SDDC ネットワーク アップリンクのトラフィック統計情報を表示できるコントロールと、その最大伝送可能単位 (MTU) およびユニキャスト リバース パス転送 (URPF) の設定を管理できるコントロールがあります。

ネットワーク セグメントの作成または変更

ネットワーク セグメントは、SDDC コンピューティング ネットワークのワークロード仮想マシンによって使用される論理ネットワークです。

VMware Cloud on AWS は、3 種類のネットワーク セグメント (ルーティング、拡張、および切断) をサポートしています。

- ルーティング ネットワーク セグメント (デフォルト タイプ) は、SDDC 内の他の論理ネットワークと接続したり、SDDC ファイアウォールを介して外部ネットワークに接続したりします。

- 拡張ネットワーク セグメントは、既存の L2VPN トンネルを拡張し、SDDC とオンプレミス ネットワークにまたがる単一の IP アドレス空間を提供します。
- 切断されたネットワーク セグメントには、アップリンクがありません。接続されている仮想マシンのみがアクセスできる、分離されたネットワークが提供されます。切断されたセグメントは、VMware HCX で必要になると作成されます (VMware HCX スタート ガイドを参照)。自分で作成したり、他のセグメント タイプに変換したりすることもできます。

SDDC あたりのセグメント数の制限、およびセグメントあたりのネットワーク接続数の制限については、[VMware 構成の上限](#)を参照してください。

単一ホスト スタータ SDDC が、sddc-cgw-network-1 という名前の単一ルーティング ネットワーク セグメントを使用して作成されます。マルチホスト SDDC はデフォルトのネットワーク セグメントなしで作成されるため、ワークロード仮想マシン用に少なくとも 1 つ作成する必要があります。セグメントを作成する場合は、まず、いくつかの基本的なパラメータを構成し、そのセグメントで DHCP 要求を処理する方法を指定します。セグメントが作成された後、さらにオプションの手順を実行して、セグメント プロファイルの指定と DHCP の静的バインドの作成を行うことができます。

注：


手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [セグメント] 画面を開きます。

新しいセグメントを作成するには、[セグメントの追加] をクリックし、新しいセグメントの [名前] と、必要に応じて [説明] を入力します。IPv6 セグメントまたはデュアルスタック セグメントの作成の詳細については、[SDDC ネットワークでの IPv6 の有効化と使用](#)を参照してください。

セグメントを削除または変更するには、その  ボタンをクリックして、[編集] を選択します。セグメント タイプを含む、すべてのセグメント プロパティを変更できます。また、セグメントの DHCP 構成を編集したり、削除したりすることもできます。

重要： 仮想マシンまたは VIF が接続されている場合、どのタイプのセグメントも無効にしたり、削除したりすることはできません。セグメントを削除する前に、接続されている仮想マシンと VIF を切断します。

- 5 [接続されたゲートウェイ] ドロップダウンでセグメント タイプおよび接続されたゲートウェイを指定し、必要な構成パラメータを入力します。

デフォルト構成で [接続されたゲートウェイ] として選択できるのは、コンピューティング ゲートウェイのみです。SDDC で追加の Tier-1 ゲートウェイを作成する方法については、[VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加](#)を参照してください。セカンダリ Tier-1 ゲートウェイに接続されているセグメントで構成されたネットワークは、デフォルトでは、Direct Connect、SDDC グループ (VTGW)、または ESXi 管理ホストにアドバタイズされません。接続を確立するには、これらのネットワークを含むルート集約を定義します

パラメータの要件は、セグメントのタイプによって異なります。

表 3-12. ルーティングされたセグメントの構成パラメータ

パラメータ	値
VPN トンネル ID	ルーティングされたセグメント タイプまたは切断済みのセグメント タイプの場合はなし。
サブネット	セグメントの IPv4 CIDR ブロックを指定します。このブロックは、管理ネットワーク、 予約されたネットワーク アドレス に示されているいずれかの CIDR ブロック、または接続中の Amazon VPC のいずれかのサブネットと重複してはなりません。ブロックのいずれかの部分がパブリック IP アドレス空間にある場合は、IANA またはその他の地域のインターネット レジストリによって使用が割り当てられている必要があります。
uRPF モード	[厳密] を選択して、 RFC3704 で定義されているユニキャスト リバース パス フォワーディング (URPF) 厳密モードを適用するか、[なし] を選択して、このサブネットに対して URPF を無効にします。
DHCP 構成の設定	ルーティングされたセグメントでは、コンピューティング ゲートウェイの DHCP サーバがデフォルトで使用されます。セグメントを作成または更新するときは、DHCP リレーなどのセグメントごとの DHCP 構成を指定できます。 セグメントの DHCP プロパティの構成 を参照してください。
ドメイン名	(オプション) 完全修飾ドメイン名を入力します。セグメント上の静的バインドでは、このドメイン名が自動的に継承されます。
タグ	NSX オブジェクトのタグgingについて詳しくは、『NSX Data Center 管理ガイド』の オブジェクトへのタグの追加 を参照してください。

表 3-13. 拡張セグメントの構成パラメータ

パラメータ	値
VPN トンネル ID	既存の L2VPN トンネルのトンネル ID を指定します。ルーティングされたセグメント タイプまたは切断済みのセグメント タイプの場合はなし。まだ L2VPN を作成していない場合は、 SDDC でのレイヤー 2 VPN トンネルの設定 を参照してください。
サブネット	拡張セグメントの場合はなし。
uRPF モード	[厳密] を選択して、 RFC3704 で定義されているユニキャスト リバース パス フォワーディング (URPF) 厳密モードを適用するか、[なし] を選択して、このサブネットに対して URPF を無効にします。

表 3-13. 拡張セグメントの構成パラメータ（続き）

パラメータ	値
ドメイン名	（オプション）完全修飾ドメイン名を入力します。セグメント上の静的バインドでは、このドメイン名が自動的に継承されます。
タグ	NSX オブジェクトのタグgingについて詳しくは、『NSX Data Center 管理ガイド』の オブジェクトへのタグの追加 を参照してください。


表 3-14. 切断済みのセグメントの構成パラメータ

パラメータ	値
VPN トンネル ID	ルーティングされたセグメント タイプまたは切断済みのセグメント タイプの場合はなし。
サブネット	セグメントの IPv4 CIDR ブロックを指定します。このブロックは、管理ネットワーク、 予約されたネットワーク アドレス に示されているいずれかの CIDR ブロック、または接続中の Amazon VPC のいずれかのサブネットと重複してはなりません。ブロックのいずれかの部分がパブリック IP アドレス空間にある場合は、IANA またはその他の地域のインターネット レジストリによって使用が割り当てられている必要があります。
ドメイン名	（オプション）完全修飾ドメイン名を入力します。セグメント上の静的バインドでは、このドメイン名が自動的に継承されます。
uRPF モード	[厳密] を選択して、 RFC3704 で定義されているユニキャスト リバース パス フォワーディング (URPF) 厳密モードを適用するか、[なし] を選択して、このサブネットに対して URPF を無効にします。
タグ	NSX オブジェクトのタグgingについて詳しくは、『NSX Data Center 管理ガイド』の オブジェクトへのタグの追加 を参照してください。

6 [保存] をクリックしてセグメントを作成または更新します。

セグメント構成を続行する場合は、[はい] をクリックします。[いいえ] をクリックした場合でも、後で必要に応じてセグメントを編集できます。

要求されたセグメントが、システムによって作成されます。この操作は、完了までに最大で 15 秒ほどかかることがあります。セグメントの [ステータス] が [Up] に移行すると、そのセグメントが使用可能になります。セグ

メントの [ステータス] が [Down] の場合は、情報アイコン  をクリックして、問題の原因に関する詳細情報を表示できます。

7 （オプション） [セグメント プロファイル] をクリックして、セグメントのプロファイルを表示します。

すべてのセグメントには、IP アドレス検出、MAC 検出、および関連するセキュリティ制御の処理方法を指定する読み取り専用プロファイルがあります。主な設定は次のとおりです。

- 無作為検出モードはサポートされていません。
- MAC ラーニングはサポートされていません。セグメントに接続されている NIC で使用できる MAC アドレスは 1 つのみです。
- BPDU フィルタリングが有効です。

- IP アドレス検出（動的メンバーシップを使用してグループに追加された IP アドレスに影響する）は、[初回使用時に信頼する] に設定されます。検出には ARP と DHCP スヌーピング、および VMware Tools が使用されます。『NSX Data Center 管理ガイド』の [IP アドレス検出セグメント プロファイルの理解](#) を参照してください。

IPv6 セグメントまたはデュアルスタック セグメントのプロファイルの詳細については、[SDDC ネットワークでの IPv6 の有効化と使用](#) を参照してください。

8 （オプション）[DHCP 静的バインド] を構成します。

- [設定] をクリックして、セグメント上の仮想マシンの静的バインドを指定します。

[IPv4 静的バインドの追加] をクリックして、バインドの [名前] を入力し、セグメントに含まれる IPv4 アドレスと MAC アドレスを指定します。指定された MAC アドレスを持つ仮想マシンがパワーオンされ、セグメントに接続されると、指定されたアドレスを受信します。[保存] をクリックしてバインドを作成した後、別のバインドを追加するか、または [適用] をクリックして、指定された静的バインドをセグメントに適用します。

- [DHCP オプション] をクリックして、DHCP クラスレス スタティック ルート（オプション 121）と一般オプションを指定します。

- IPv4 用の DHCP の各クラスレス スタティック ルート オプションでは、宛先が同じ複数のルートを設定できます。各ルートには、宛先サブネット、サブネット マスク、ネクスト ホップ ルーターが含まれます。DHCPv4 のクラスレス スタティック ルートについては、[RFC 3442](#) を参照してください。DHCPv4 サーバでは、最大 127 個のクラスレス スタティック ルートを追加できます。
- 一般オプションを追加するには、オプションのコードを選択して、オプションの値を入力します。バイナリ値の場合、値は Base-64 エンコード形式にする必要があります。

次のステップ

セグメントが作成され、ステータスが [成功] になった後、[統計情報の表示] をクリックすると、セグメントへのネットワーク トラフィックとセグメントからのネットワーク トラフィックの統計情報を表示できます。[関連グループの表示] をクリックすると、このセグメントを含むグループのリストを表示できます。詳細については、『NSX Data Center 管理ガイド』の [グループの追加](#) を参照してください。

セグメントの DHCP プロパティの構成

DHCP 構成は、セグメントごとのプロパティです。デフォルト構成の場合、コンピューティング ゲートウェイの DHCP サーバは、ルーティングされたすべてのセグメントにある仮想マシンからの DHCP 要求を処理します。ワークロード ネットワークに別の DHCP サーバを使用するには、DHCP リレーを使用するようにセグメントを構成します。また、独自のローカル DHCP サーバを使用するようにセグメントを構成することもできます。

セグメントごとの DHCP 構成は、[ネットワーク セグメントの作成または変更](#)のセグメント作成/更新ワークフロー ドキュメントに含まれています。詳細については、『NSX 管理ガイド』の [DHCP](#) を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。

- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。 [NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [セグメント] 画面を開きます。

[DHCP タイプ] を選択して、構成の詳細を指定します。『NSX 管理ガイド』の [セグメントでのセグメントの DHCP サーバの構成](#) を参照してください。

注： セグメント内の仮想マシンからの DHCP 要求は、セグメントのゲートウェイ アドレスを送信元 IP アドレスとして使用します。この CGW ファイアウォール経由のトラフィックを許可するには、この送信元アドレスを持つパケットがリモート DHCP サーバに到達できるようにするルールを作成します。セグメント オブジェクトをグループ メンバーとして含めると、ゲートウェイ IP アドレスはグループに含まれません。IP アドレスとしてグループに追加する必要があります。関連情報については、VMware のナレッジベースの記事 [KB79595](#) を参照してください。

DHCP プロファイルの作成または変更

DHCP プロファイルでは、DHCP サーバのタイプと構成を指定します。デフォルトのプロファイルを使用することも、必要に応じて別のプロファイルを作成することもできます。

DHCP プロファイルを使用すると、SDDC ネットワーク内の任意の場所に DHCP リレー サーバの DHCP サーバを構成できます。『NSX-T Data Center 管理ガイド』の [DHCP プロファイルの追加](#) を参照してください。

手順

- 1 <https://vmc.vmware.com> から VMware Cloud コンソール にログインします。
- 2 [ネットワークとセキュリティ] - [DHCP] の順に選択します。
- 3 [DHCP プロファイルの追加] をクリックして、プロファイルの [名前] を入力します。

[プロファイル タイプ] を選択して、必要な構成パラメータを指定します。

- [DHCP サーバ] の場合、IPv4 [サーバの IP アドレス] を指定し、必要に応じて [リース時間] を変更します。
- [DHCP リレー] では、[サーバの IP アドレス] としてターゲット DHCP サーバのアドレスを指定します。ターゲット DHCP サーバがオンプレミスの場合は、オンプレミスのファイアウォールで DHCP トラフィック（ポート 67 および 68）がこのアドレスに到達できることを確認してください。リース時間は、ターゲット サーバの構成によって制御されます。

いずれのタイプの DHCP プロファイルにもタグ付けが可能です。

- 4 [保存] をクリックしてプロファイルを作成します。

新しいプロファイルは、ルーティングされたセグメントの DHCP 構成を指定するときに使用できます。 [ネットワーク セグメントの作成または変更](#) を参照してください。[使用場所] 列には、このプロファイルが指定されたセグメントが表示されます。

コンピューティング ゲートウェイのファイアウォール ルールの追加または変更

デフォルトでは、コンピューティング ゲートウェイは SDDC コンピューティング ネットワークとの間のトラフィックをブロックします。必要に応じて、トラフィックを許可するコンピューティング ゲートウェイのファイアウォール ルールを追加します。

デフォルトのコンピューティング ゲートウェイおよび作成する追加の Tier-1 ゲートウェイのファイアウォール ルールは、指定された送信元から指定された宛先およびサービスへのネットワーク トラフィックに対して実行するアクションを指定します。アクションは次のいずれかになります。

- 許可（一致するトラフィックを許可する）
- ドロップ（一致するトラフィックを通知なしにドロップする）
- 拒否（一致するトラフィックをドロップして送信元に通知する）

物理ネットワーク インターフェイスのリストからの選択、または [すべてのアップリンク] という一般的な指定（ゲートウェイから VPC インターフェイス、インターネット インターフェイス、またはイントラネット (Direct Connect) インターフェイスに向かうすべてのトラフィックに適用される）にルールを適用できます。

注： [すべてのアップリンク] に適用されるファイアウォール ルールは、仮想インターフェイスであって物理アップリンクではない [VPN トンネル インターフェイス] (VTI) には適用されません。[VPN トンネル インターフェイス] は、ルートベースの VPN で行われるワークロード仮想マシンの通信を管理する、任意のファイアウォール ルールの [適用先] パラメータで明示的に指定する必要があります。

ファイアウォールを通過するすべてのトラフィックは、ルール テーブルに表示されている順序でルールによって評価されます。最初のルールに一致するトラフィックは、そのアクション（許可、ドロップ、または拒否）に従い、評価は停止します。最初のルールに一致しないトラフィックは後続のルールに渡されます。一致すると、ルール アクションの指定に従ってトラフィックが許可、ドロップ、または拒否され、ルールの評価は停止します。ユーザー定義のルールに一致しないトラフィックは、デフォルト ルールによって処理されます。

次の 2 種類のファイアウォール ルールがあります。

- 事前定義されたファイアウォール ルールは、VMware Cloud on AWS によって作成されます。2 つの事前定義されたコンピューティング ゲートウェイのファイアウォール ルールを次に示します。

表 3-15. 事前定義されたコンピューティング ゲートウェイのファイアウォール ルール

名前	送信元	宛先	サービス	適用先	操作
デフォルトの VTI ルール	任意	任意	任意	VPN トンネル インターフェイス	ドロップ *
デフォルトのアップリンク ルール	任意	任意	任意	すべてのアップリンク	Drop

* [デフォルトの VTI ルール] は、ワークロード仮想マシンがルートベースの VPN を介して通信できるように、（仮想トンネル インターフェイス経由の）ルートベースの VPN トラフィックをすべてドロップし、このルールを [許可] に変更してトラフィックを許可するか、ルール階層の下位に移動して、より許可度の高いルールの後ろに配置します。[デフォルトのアップリンク ルール] を変更または並べ替えることはできません。

- ユーザー定義のファイアウォール ルールは、指定した順序で処理され、常に [デフォルトのアップリンク ルール] の前に処理されます。

前提条件

コンピューティング ゲートウェイのファイアウォール ルールでは、送信元と宛先の値についてインベントリ グループを指定する必要があります。インベントリ グループの操作を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。NSX Manager による SDDC ネットワーク管理を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [ゲートウェイ ファイアウォール] 画面で、[コンピューティング ゲートウェイ] をクリックします。
- 5 ルールを追加するには、[ルールの追加] をクリックし、新しいルールの [名前] を入力します。
- 6 新しいルールのパラメータを入力します。

パラメータはデフォルト値に初期化されます ([送信元] と [宛先] は [すべて] など)。パラメータを編集するには、パラメータ値の上にマウス カーソルを移動し、鉛筆アイコン (✎) をクリックしてパラメータ固有のエディタを開きます。

オプション	説明
送信元	[送信元] 列の [任意] をクリックし、送信元ネットワーク トラフィックのインベントリ グループを選択するか、[グループの追加] をクリックして、このルールで使用する新しいユーザー定義のインベントリ グループを作成します。[保存] をクリックします。
宛先	[宛先] 列の [任意] をクリックし、宛先ネットワーク トラフィックのインベントリ グループを選択するか、[グループの追加] をクリックして、このルールで使用する新しいユーザー定義のインベントリ グループを作成します。[保存] をクリックします。
サービス	[サービス] 列の [任意] をクリックして、リストからサービスを選択するか、[サービスの追加] をクリックして、このルールで使用する新しいユーザー定義のサービスを作成します。[保存] をクリックします。

オプション	説明
適用先	<p>ルールを適用するトラフィックのタイプを定義します。</p> <ul style="list-style-type: none"> ■ ルートベースの VPN 上のトラフィックにルールを適用する場合は、[VPN トンネル インターフェイス] を選択します。 ■ リンクされた Amazon VPC 接続上のトラフィックにルールを適用する場合は、[VPC インターフェイス] を選択します。 ■ パブリック IP エンドポイントを使用するポリシーベースの VPN を介したトラフィックを含む、SDDC のインターネット ゲートウェイを介したトラフィックにルールを適用する場合は、[インターネット インターフェイス] を選択します。 ■ AWS Direct Connect、VMware Transit Connect、およびプライベート IP アドレスを使用するポリシーベースの VPN を介したトラフィックをルールで許可する場合は、[イントラネット インターフェイス] を選択します。 ■ [VPC インターフェイス]、[インターネット インターフェイス]、[イントラネット インターフェイス] にルールを適用し、[VPN トンネル インターフェイス] に適用しない場合は、[すべてのアップリンク] を選択します。 <p>注： [VPN トンネル インターフェイス] はアップリンクとして分類されていません。</p>
操作	<ul style="list-style-type: none"> ■ すべての L3 トラフィックがファイアウォールを通過できるようにするには、[許可] を選択します。 ■ [ドロップ] を選択すると、指定した [送信元]、[宛先]、[サービス] に一致するパケットをドロップします。これは、送信元または宛先のシステムに通知されない、サイレント アクションです。パケットがドロップされると、再試行のしきい値に到達するまで、接続が再試行されます。 ■ [拒否] を選択すると、指定した [送信元]、[宛先]、[サービス] に一致するパケットを拒否します。このアクションは、「宛先への到達不能メッセージ」を送信者に返します。TCP パケットの場合、応答には TCP RST メッセージが含まれます。UDP、ICMP、およびその他のプロトコルの場合、応答には「管理上禁止」のコード（9 または 10）が含まれます。接続を確立できない場合、すぐに送信者に通知されます（再試行は行われません）。

新しいルールはデフォルトで有効になります。トグル ボタンを左にスライドして無効にします。

7 [発行] をクリックして、ルールを作成します。

新しいルールには、ルールによって生成されるログ エントリで使用される、整数の [ID] 値が付与されます。

次のステップ

既存のファイアウォール ルールを使用して、これらの任意のアクションのいずれか、またはすべてを実行できます。



- 歯車アイコン  をクリックして、ルールのログ設定を表示または変更します。ログのエントリは、VMware VMware Aria Operations for Logs サービスに送信されます。『VMware Cloud on AWS Operations Guide』の [Using VMware Aria Operations for Logs](#) を参照してください。
- グラフ アイコン  をクリックして、ルールのヒットおよびフローの統計情報を表示します。

表 3-16. ルールのヒットの統計

ポピュラリティ インデックス	過去 24 時間にルールがトリガーされた回数。
ヒット カウント	ルールが作成されてからトリガーされた回数。

表 3-17. フローの統計

パケット数	このルールの対象となるパケット フローの合計。
バイト数	このルールの対象となるバイト フローの合計。

統計情報は、ルールが有効になるとすぐに集計が開始されます。

- ファイアウォール ルールを並べ替えます。

[新しいルールの追加] ボタンから作成されたルールは、ルールの一覧の一番上に配置されます。ファイアウォール ルールは、一番上から順に適用されます。リスト内のルールの位置を変更するには、ルールを選択して新しい位置にドラッグします。[公開] をクリックして変更を公開します。

分散ファイアウォール ルールの追加または変更

分散ファイアウォール ルールは、仮想マシン (vNIC) レベルで適用され、SDDC 内の East-West トラフィックを制御します。

分散ファイアウォールを通過するすべてのトラフィックに、このルール テーブルのルールが上から順に適用されます。上位のルールで許可されたパケットが、その下のルールに順次渡されていきます。いずれかのルールでパケットがドロップされるか拒否されるまで、またはすべてのトラフィックが許可されるデフォルト ルールに適合するまで、ルールの適用が続けられます。

注目: SDDC バージョン 1.20、1.20v2、または 1.20v3 では、FQDN 属性を指定したコンテキスト プロファイルが分散ファイアウォール ルールに使用されている場合に、DNS サーバからの応答で CNAME レコードを受信すると、PSOD エラーが発生する可能性があります。詳細については、VMware ナレッジベースの記事 [KB91654](#) を参照してください。

分散ファイアウォール ルールは、ポリシー別にグループ化されます。ポリシーはカテゴリごとに分類されます。各カテゴリには、評価の優先順位があります。優先順位の高いカテゴリのルールは、優先順位の低いカテゴリのルールよりも先に評価されます。

表 3-18. 分散ファイアウォール ルールのカテゴリ

カテゴリ評価の優先順位	カテゴリ名	説明
1	イーサネット	レイヤー 2 のすべての SDDC ネットワーク トラフィックに適用します。 注: このカテゴリのルールでは、送信元と宛先として MAC アドレスが必要です。IP アドレスは受け入れられますが、無視されます。
2	緊急	検疫ルールと許可ルールに使用します。
3	インフラストラクチャ	共有サービスへのアクセスを定義します。グローバル ルール、Active Directory、DNS、NTP、DHCP、バックアップ、管理サーバ。
4	環境	本番環境ゾーン、開発ゾーン、または特定のビジネス目的専用のゾーンなどのセキュリティ ゾーン間のルール。
5	アプリケーション	アプリケーション、アプリケーション層、またはマイクロサービス間のルール。

分散ファイアウォールの専門用語の詳細については、『NSX Data Center 管理ガイド』の[セキュリティに関する用語](#)を参照してください。

前提条件

分散ファイアウォール ルールは、ソースおよびターゲットとしてインベントリ グループを必要とします。また、サービス（事前定義されたサービスまたは SDDC 用に定義したカスタム サービス）に適用する必要があります。これらのグループやサービスはルールの作成中に作成できますが、事前にこのような操作を行っておくと、プロセスを高速化できます。[インベントリ グループの操作](#)を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [分散ファイアウォール] 画面を開きます。

[カテゴリ固有のルール] をクリックしてカテゴリを選択すると、そのカテゴリのポリシーとルールを表示および修正できます。[すべてのルール] をクリックすると、すべてのポリシーとカテゴリのルールを表示できます（修正はできません）。

- 5 （オプション）デフォルトの接続方法を変更します。

分散ファイアウォールには、レイヤー 2 およびレイヤー 3 のすべてのトラフィックに適用されるデフォルト ルールが含まれています。これらのルールは、カテゴリ内の他のすべてのルールの後に評価され、前のルールに一致しないトラフィックがファイアウォールを通過することを許可します。これらのルールのいずれかまたは両方を変更して制約を厳しくすることはできますが、どちらのルールも無効にすることはできません。

- [デフォルトのレイヤー 2 のルール] を変更するには、[イーサネット] カテゴリの [デフォルト レイヤー 2 のセクション] を展開して、そのルールの [アクション] を [ドロップ] に変更します。
- [デフォルトのレイヤー 3 のルール] を変更するには、[アプリケーション] カテゴリの [デフォルトのレイヤー 3 のセクション] を展開して、そのルールの [アクション] を [ドロップ] または [拒否] に変更します。

[発行] をクリックして、ルールを更新します。

- 6 ポリシーを追加するには、該当のカテゴリを開いて [ポリシーの追加] をクリックし、新しいポリシーの [名前] を指定します。

そのカテゴリのポリシー リストの一番上に新しいポリシーが追加されます。既存のポリシーの前後にポリシーを追加するには、ポリシー行の先頭の縦方向の省略記号ボタンをクリックしてポリシー設定メニューを開き、[ポリシーを上追加] または [ポリシーを下追加] をクリックします。

デフォルトでは、[適用先] 列は [DFW] に設定され、このルールがすべてのワークロードに適用されます。このルールやポリシーは、選択したグループにも適用できます。[適用先] は、ルールごとの適用範囲を定義し、主にホスト リソース消費の最適化に使用します。他のテナントやゾーンに定義したポリシーに干渉することなく、特定のゾーンやテナントの目標ポリシーを定義する際に便利です。

注： IP アドレス、MAC アドレス、または Active Directory グループのみからなるグループは、[適用先] テキスト ボックスで使用できません。


- 7 ルールを追加するには、ポリシーを選択して [ルールの追加] をクリックし、ルールの [名前] を入力します。
- 8 新しいルールのパラメータを入力します。

パラメータはデフォルト値に初期化されます ([送信元] と [宛先] は [すべて] など)。パラメータを編集するには、パラメータ値の上にマウス カーソルを移動し、鉛筆アイコン (✎) をクリックしてパラメータ固有のエディタを開きます。

オプション	説明
送信元	[送信元] 列の [任意] をクリックし、送信元ネットワーク トラフィックのインベントリ グループを選択するか、[グループの追加] をクリックして、このルールで使用する新しいユーザー定義のインベントリ グループを作成します。[保存] をクリックします。
宛先	[宛先] 列の [任意] をクリックし、宛先ネットワーク トラフィックのインベントリ グループを選択するか、[グループの追加] をクリックして、このルールで使用する新しいユーザー定義のインベントリ グループを作成します。[保存] をクリックします。
サービス	[サービス] 列の [任意] をクリックし、リストからサービスを選択します。[保存] をクリックします。
適用先	ルールは、そのルールが含まれているポリシーの [適用先] の値を継承します。
操作	<ul style="list-style-type: none"> ■ すべての L2 および L3 トラフィックがファイアウォールを通過できるようにするには、[許可] を選択します。 ■ [ドロップ] を選択すると、指定した [送信元]、[宛先]、[サービス] に一致するパケットをドロップします。これは、送信元または宛先のシステムに通知されない、サイレント アクションです。パケットがドロップされると、再試行のしきい値に到達するまで、接続が再試行されます。 ■ [拒否] を選択すると、指定した [送信元]、[宛先]、[サービス] に一致するパケットを拒否します。このアクションは、「宛先への到達不能メッセージ」を送信者に返します。TCP パケットの場合、応答には TCP RST メッセージが含まれます。UDP、ICMP、およびその他のプロトコルの場合、応答には「管理上禁止」のコード (9 または 10) が含まれます。接続を確立できない場合、すぐに送信者に通知されます (再試行は行われません)。

新しいルールはデフォルトで有効になります。トグル ボタンを左にスライドして無効にします。

- 9 (オプション) 詳細設定の構成。

ルールの方向またはログの動作を変更するには、歯車アイコン  をクリックして [設定] ページを開きます。

方向

デフォルトでは、この値は [In/Out] であり、すべての送信元および宛先にこのルールを適用します。これを [In] に変更して、ルールを送信元からの受信トラフィックのみに適用するか、[Out] にして、宛先への送信トラフィックのみに適用することができます。この値を変更すると、非対称ルーティングやその他のトラフィック異常が発生する可能性があるため、[方向] のデフォルト値の変更を行う前に、すべての送信元と宛先について予想される結果を理解しておく必要があります。

ログ

新しいルールのログは、デフォルトで無効になっています。ルール アクションのログを有効にするには、トグル ボタンを右にスライドします。

10 [発行] をクリックして、ルールを作成します。

新しいルールには、生成されるログ エントリ内のルールを識別するために使用される、整数の [ID] 値が付与されます。

次のステップ

既存のファイアウォール ルールを使用して、これらの任意のアクションのいずれか、またはすべてを実行できます。



- 歯車アイコン  をクリックして、ルールのログ設定を表示または変更します。ログのエントリは、VMware VMware Aria Operations for Logs サービスに送信されます。『VMware Cloud on AWS Operations Guide』の [Using VMware Aria Operations for Logs](#) を参照してください。
- グラフ アイコン  をクリックして、ルールのヒットおよびフローの統計情報を表示します。

表 3-19. ルールのヒットの統計

ポピュラリティ インデックス	過去 24 時間にルールがトリガーされた回数。
ヒット カウント	ルールが作成されてからトリガーされた回数。

表 3-20. フローの統計

パケット数	このルールの対象となるパケット フローの合計。
バイト数	このルールの対象となるバイト フローの合計。

統計情報は、ルールが有効になるとすぐに集計が開始されます。

- ファイアウォール ルールを並べ替えます。

[新しいルールの追加] ボタンから作成されたルールは、ポリシーのルールのリストの一番上に配置されます。各ポリシーのファイアウォール ルールは、一番上から順に適用されます。リスト内のルールの位置を変更するには、ルールを選択して新しい位置にドラッグします。[公開] をクリックして変更を公開します。

分散ファイアウォール ルールの管理

ファイアウォールを通過するトラフィックには、[すべてのルール] リストに表示されている順序でルールが適用されます。

[すべてのルール] リストの分散ファイアウォール ルールの順序は、ポリシーの順序付きリストと、各ポリシーのルールの順序付きリストを組み合わせたものになります。分散ファイアウォールのセクションとセクション内のルールは、順序を変更できます。また、既存の分散ファイアウォール構成の編集、ファイアウォール ルールまたはセクションの削除、クローンの作成などを実行できます。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。NSX Manager による SDDC ネットワーク管理を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [分散ファイアウォール] 画面を開きます。
- 5 (オプション) ポリシー設定を変更します。

ポリシー行の先頭にある縦方向の省略記号ボタンをクリックし、ポリシー内のすべてのルールに適用される一括アクションを実行できます。ポリシーにルールが含まれていると、これらの設定は変更できません。

- 6 (オプション) ポリシーの順序を変更します。

[ポリシーの追加] ボタンで作成されたポリシーは、ポリシーのリストの最上位に配置されます。各ポリシーのファイアウォール ルールは、一番上から順に適用されます。リスト内でポリシー（およびポリシーに含まれるすべてのルール）の位置を変更するには、そのポリシーを選択して新しい位置にドラッグします。[公開] をクリックして変更を公開します。

- 7 (オプション) ルールを複製またはコピーします。

ルール行の先頭にある  をクリックしてから、次をクリックします。

- [ルールを複製] では、このポリシーのルールのコピーを作成します。
- [ルールをコピー] では、別のポリシーに追加できるルールのコピーを作成します。

- 8 (オプション) ルールを追加または削除します。

ルール行の先頭にある  をクリックしてから、次をクリックします。

- [ルールの追加] では、このポリシーにルールを追加します。
- [ルールの削除] では、このポリシーからルールを削除します。

- 9 (オプション) 分散ファイアウォールの構成を保存するか、表示します。

VMware Cloud on AWS の分散ファイアウォールの構成は、オンプレミス NSX の [ファイアウォール ドラフト機能](#) に似ています。[アクション] - [表示] の順にクリックして、保存されている構成のリストを表示します。[アクション] - [保存] の順にクリックして、現在の構成を保存します。デフォルトでは、構成が自動的に保存されます。[アクション] - [設定] - [全般設定] をクリックし、[ドラフトを自動保存] を無効にします。

10 (オプション) Identity Firewall 設定の構成

このオプションは、NSX の Advanced Firewall 機能を有効にしている場合に使用できます。詳細については、[6 章 NSX Advanced Firewall 機能について](#)を参照してください。この機能を使用するには、この機能を 1 つ以上の SDDC クラスタに適用する必要があります。

- a [分散ファイアウォール] タブで [アクション] - [設定] - [全般設定] をクリックし、[Identity Firewall のステータス] を [有効化] に切り替えます。
- b [Identity Firewall の設定] タブをクリックし、この機能を使用する SDDC クラスタを選択します。

分散ファイアウォール除外リストの管理


分散ファイアウォールの除外リストを使用すると、分散ファイアウォールの対象範囲から除外するインベントリ グループを指定できます。除外対象グループのメンバーとの間の East-West ネットワーク トラフィックは、本来適用される分散ファイアウォール ルールの対象外になります。

分散ファイアウォールの除外リストを使用すると、特定のインベントリ グループを分散ファイアウォール ルールの適用対象外にすることができます。デフォルトでは、vCenter Server や NSX コントローラなどの管理仮想マシンおよびアプライアンスが除外リストに含まれます。リストを編集して、エントリを追加または削除できます。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [分散ファイアウォール] 画面を開きます。
- 5 [アクション] - [設定] - [除外リスト] の順にクリックし、[除外リスト] 画面を表示します。
 - 既存のグループを除外リストに追加するには、[グループの追加] をクリックし、既存の [グループ名] を選択します。
 - [除外リストの管理] でグループを作成するには、[グループの追加] をクリックし、[グループ名] を入力します。次に、[メンバーを設定] をクリックし、インベントリ グループの作成画面を開きます。この画面の使用方法の詳細については、[インベントリ グループの操作](#)を参照してください。
 - リストからグループを削除するには、グループ行の先頭にある  ボタンをクリックし、[削除] を選択します。
- 6 [適用] をクリックして、変更内容を保存します。

DNS サービスの構成

VMware Cloud on AWS DNS 転送サービスは、DNS ゾーン内で実行されます。これにより、ゾーン内のワークロード仮想マシンは、完全修飾ドメイン名を IP アドレスに解決できるようになります。

SDDC には、管理ゲートウェイとコンピューティング ゲートウェイのデフォルトの DNS ゾーンが含まれています。各ゾーンには、事前構成済みの DNS サービスが含まれています。

[DNS サービス] 画面の [DNS サービス] タブを使用すると、デフォルト ゾーンの DNS サービスのプロパティを表示したり、更新したりできます。任意のゾーンで追加の DNS ゾーンを作成するか、DNS サービスの追加プロパティを構成するには、[DNS ゾーン] タブを使用します。

VMware Cloud on AWS の DNS 構成オプションの詳細については、[DNS Strategies for VMware Cloud on AWS](#) を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [DNS] 画面を開きます。
 - 5 [DNS サービス] をクリックして [DNS サービス] 画面を開きます。
 - 6 DNS サービスのパラメータを表示または編集します。
- ほとんどのゲートウェイ DNS サービスのパラメータは読み取り専用です。ただし、縦方向の省略記号ボタンをクリックして、[DNS サーバの IP アドレスの編集] を選択し、このサービス用のサーバ IP アドレスを追加または変更することができます。
- 7 [保存] をクリックします。

DNS ゾーンの追加

SDDC ネットワーク内の各 DNS ゾーンは、ユーザーが自身で管理する DNS 名前空間を表します。

SDDC の DNS ゾーンは、次の 2 つのカテゴリに分類されます。

- デフォルト ゾーン：サーバは、ゾーン内のサブネット上のすべての SDDC 仮想マシンからの DNS クエリを待機します。
- FQDN ゾーン：サーバは、デフォルト ゾーンから転送された DNS 要求を待機します。

コンピューティング ゲートウェイおよび管理ゲートウェイは、それぞれ単一のデフォルト DNS ゾーンで構成されます。いずれかのゲートウェイにいずれかのタイプのゾーンを最大 4 つ追加することで、複数の DNS サーバとサブドメインを利用できる柔軟性を確保することができます。NSX による DNS ゾーンの実装方法の詳細については、『NSX Data Center 管理ガイド』の [DNS ゾーンの追加](#) を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。

- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。 [NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [DNS] 画面を開きます。
- 5 [DNS ゾーン] をクリックして [DNS ゾーン] 画面を開きます。
- 6 デフォルト ゾーンを追加するには、[DNS ゾーンの追加] - [デフォルトゾーンの追加] の順に選択します。
デフォルトの DNS ゾーンでは、管理ゲートウェイおよびコンピューティング ゲートウェイの DNS フォワーダの IP アドレスを追加または変更できます。デフォルト ゾーン内の仮想マシンからの DNS クエリが、いずれの FQDN ゾーンの基準とも一致しない場合は、デフォルトでこれらの IP アドレスに送信されます。
 - a 名前を入力し、必要に応じて説明を入力します。このゾーン内のトラフィックに適用される DNS ファイアウォール ルールを作成する場合は、この [名前] を使用します。
 - b 最大 3 台の DNS サーバの IP アドレスを入力します。指定するすべての DNS サーバは、構成が同一である必要があります。
 - c (オプション) [ソース IP] フィールドに IP アドレスを入力します。
- 7 FQDN ゾーンを追加するには、[DNS ゾーンの追加] - [FQDN ゾーンの追加] の順に選択します。
DNS 転送を有効にする 1 つ以上の FQDN を指定します。DNS フォワーダは、デフォルトの DNS ゾーンと、最大 5 つの FQDN DNS ゾーンに関連付けられています。ゾーン内の仮想マシンから DNS クエリを受信すると、DNS フォワーダはクエリ内のドメイン名と FQDN DNS ゾーンのドメイン名を比較します。一致が確認されると、FQDN DNS ゾーンで指定された DNS サーバにクエリが転送されます。一致が確認されない場合は、デフォルト DNS ゾーンで指定された DNS サーバにクエリが転送されます。
 - a 名前を入力し、必要に応じて説明を入力します。このゾーン内のトラフィックに適用される DNS ファイアウォール ルールを作成する場合は、この [名前] を使用します。
 - b ドメインの FQDN を入力します。これは、example.com などの完全修飾ドメイン名である必要があります。
 - c 最大 3 台の DNS サーバの IP アドレスを入力します。
 - d (オプション) [ソース IP] フィールドに IP アドレスを入力します。
- 8 (オプション) DNS ゾーンにタグを付けます。
NSX オブジェクトのタグgingについて詳しくは、『NSX Data Center 管理ガイド』の [オブジェクトへのタグの追加](#) を参照してください。
- 9 [保存] をクリックします。

VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理

SDDC 展開グループは、VMware Transit Connect を使用して、グループ内の SDDC 間にバンド幅が大きく、遅延の小さい接続を提供します。SDDC グループには、所有する VPC を含めることができます。AWS Direct

Connect Gateway (DXGW) を追加し、グループ メンバーとオンプレミス SDDC の間の接続を提供することもできます。

SDDC 展開グループ (SDDC グループ) は、組織の大規模な VMware Cloud on AWS リソースの管理を簡素化するために設計された論理エンティティです。組織に複数の SDDC があり、ワークロード間で広帯域、低遅延の接続が必要な場合、SDDC を 1 つの SDDC グループにまとめると、多くのメリットが得られます。グループ メンバー間のすべてのネットワーク トラフィックが VMware Transit Connect ネットワークを通過します。サブネットが追加または削除されると、グループ内にあるすべての SDDC のコンピューティング ネットワーク間のルーティングが VMware Transit Connect によって自動的に管理されます。グループ メンバーのワークロード間のネットワーク トラフィックは、コンピューティング ゲートウェイのファイアウォール ルールによって制御します。

[管理者] または [削除が制限された管理者] の VMC サービス ロールがあれば、どの組織のメンバーでも SDDC グループを作成したり、変更したりできます。

グループ メンバーシップ

SDDC グループは、組織レベルのオブジェクトです。1 つの SDDC グループに複数の組織の SDDC を含めることはできません。1 つの SDDC グループには、最大 3 つの AWS リージョンからのメンバーを含めることができます。SDDC がグループ メンバーシップの資格を得るには、いくつかの条件を満たす必要があります。

- 管理ネットワークの CIDR ブロックは、他のグループ メンバーの管理 CIDR ブロックと重複することはできません。
- 別の SDDC グループのメンバーであってはなりません。

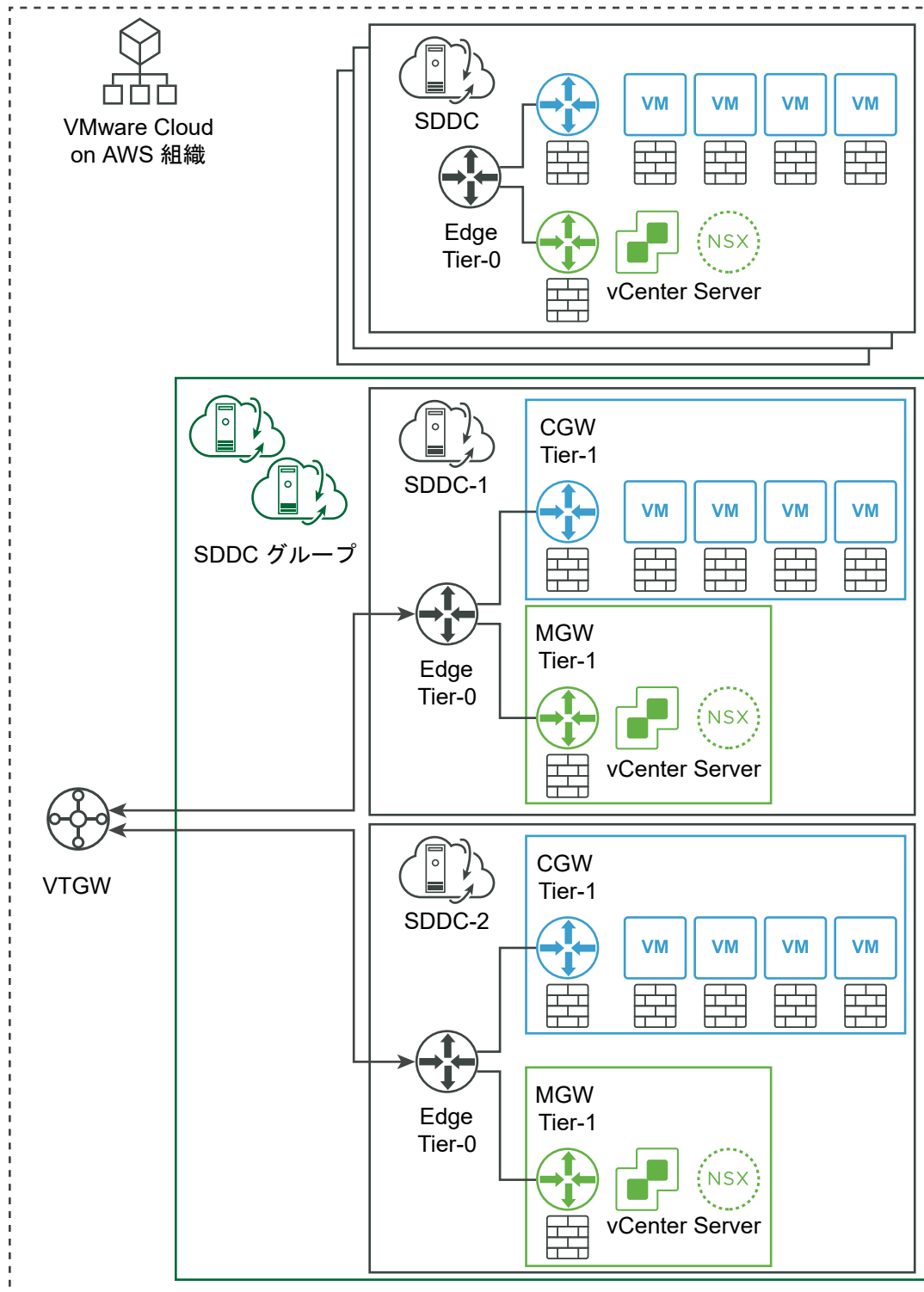
作成するグループ内のメンバーを 1 つだけにすることもできますが、ほとんどの場合、SDDC グループを実際に利用するには複数のメンバーが必要です。

注： VPN 接続経由のハイブリッド リンク モードは、SDDC グループと互換性がありません。ハイブリッド リンク モードを VPN 接続経由で使用するよう構成した SDDC を追加すると、接続が失敗し、その SDDC でハイブリッド リンク モードを使用できなくなります。SDDC がグループに追加された場合、DX 接続経由のハイブリッド リンク モードは影響を受けません。

VMware Transit Connect を使用した内部グループの接続

SDDC グループ メンバー間のピア接続には、VMware Managed Transit Gateway (VTGW) が必要です。これは、VMware が所有および管理している AWS リソースです。SDDC グループに最初のメンバーを追加すると、これらのリソースの 1 つが作成され、グループに割り当てられます。VTGW を作成および操作すると、VMware Cloud on AWS の請求で追加料金として課金されます。グループに複数のリージョン内のメンバーが含まれている場合、VTGW は、これらのリージョンのそれぞれに作成されます。

図 3-1. VMware Transit Connect がグループ内の SDDC を相互に接続

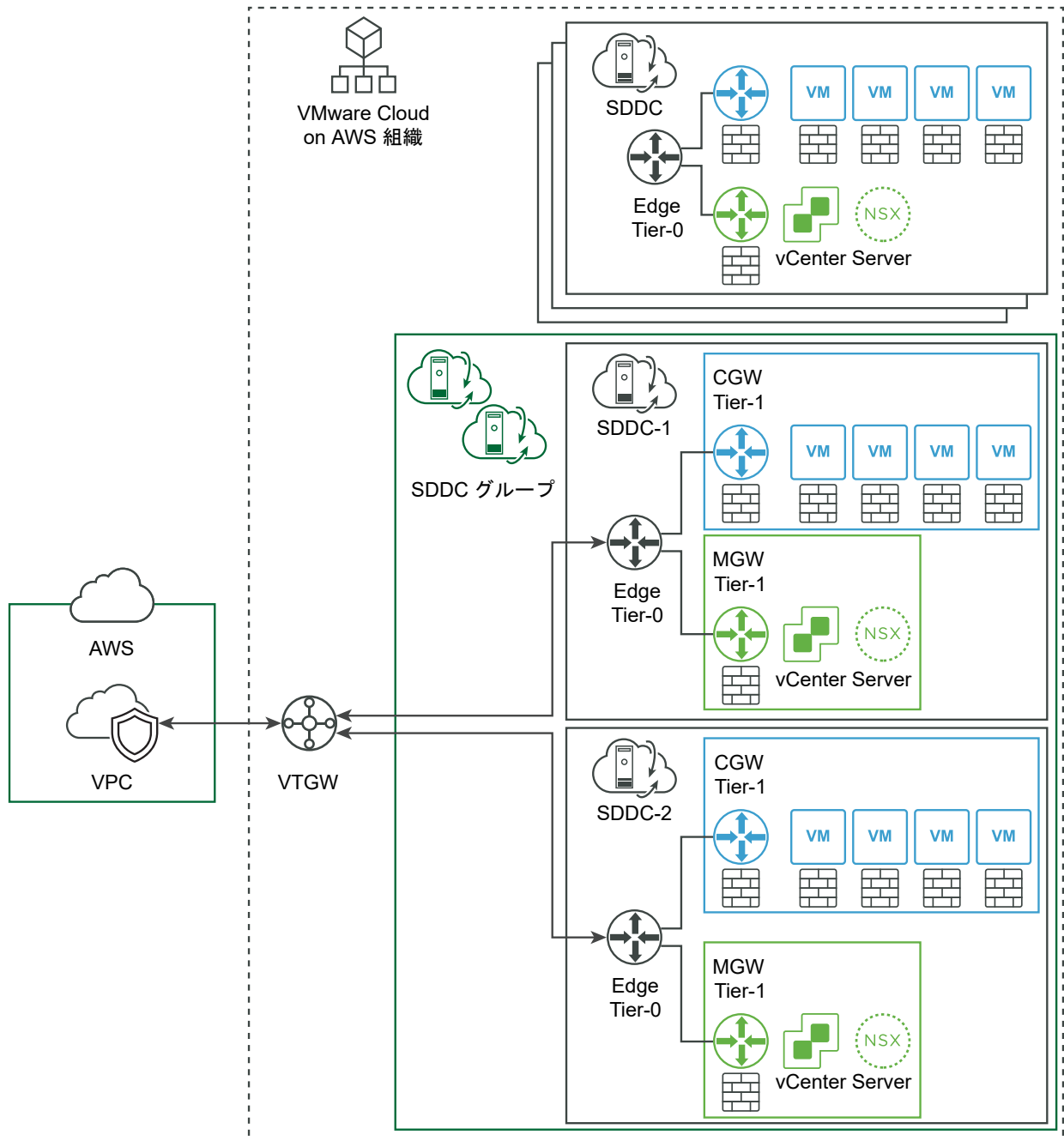


グループのメンバーは、必要に応じて追加したり、削除したりできます。すべてのメンバーが削除されるまで、グループを削除することはできません。グループを削除すると、グループの VMware Managed Transit Gateway も破棄されます。

SDDC グループへの VPC の接続

SDDC グループに VPC を接続すると、グループ内の SDDC とその VPC で実行される AWS サービスとの間でネットワーク接続を簡単に行えるようになります。最初に、VMware Cloud コンソールを使用して、VTGW (AWS リソース) を共有できるようにします。次に、AWS コンソールを使用して、共有リソースを受け入れ、SDDC グループに接続する VPC に関連付けます。接続された VPC への VTGW 接続は、マルチリージョン グループ内の複数のリージョンにまたがることはできません。

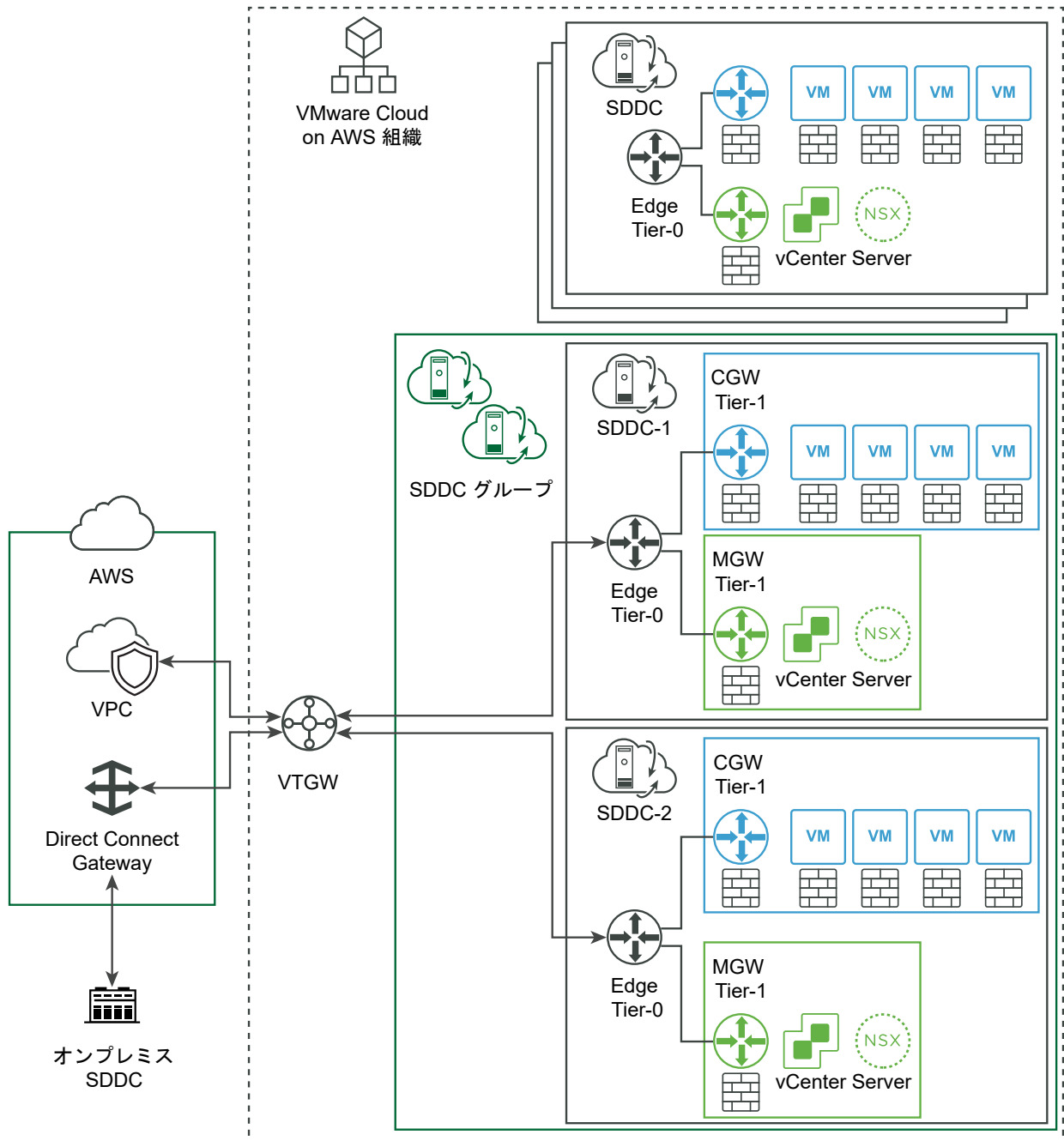
図 3-2. VMware Transit Connect を使用して VPC を SDDC グループに接続



AWS Direct Connect Gateway を使用した外部グループの接続

グループと外部のエンドポイント（オンプレミスの SDDC など）をネットワークで接続するには、グループ用に作成された VMware Managed Transit Gateway に AWS Direct Connect Gateway (DXGW) を関連付けます。Direct Connect (DX) 構成を使用すると、オンプレミスの SDDC をスタンドアローンの VMware Cloud on AWS SDDC に接続できますが、DXGW を VTGW に関連付けると、DX レベルの接続をすべての SDDC グループメンバーに対して行えるようになります。

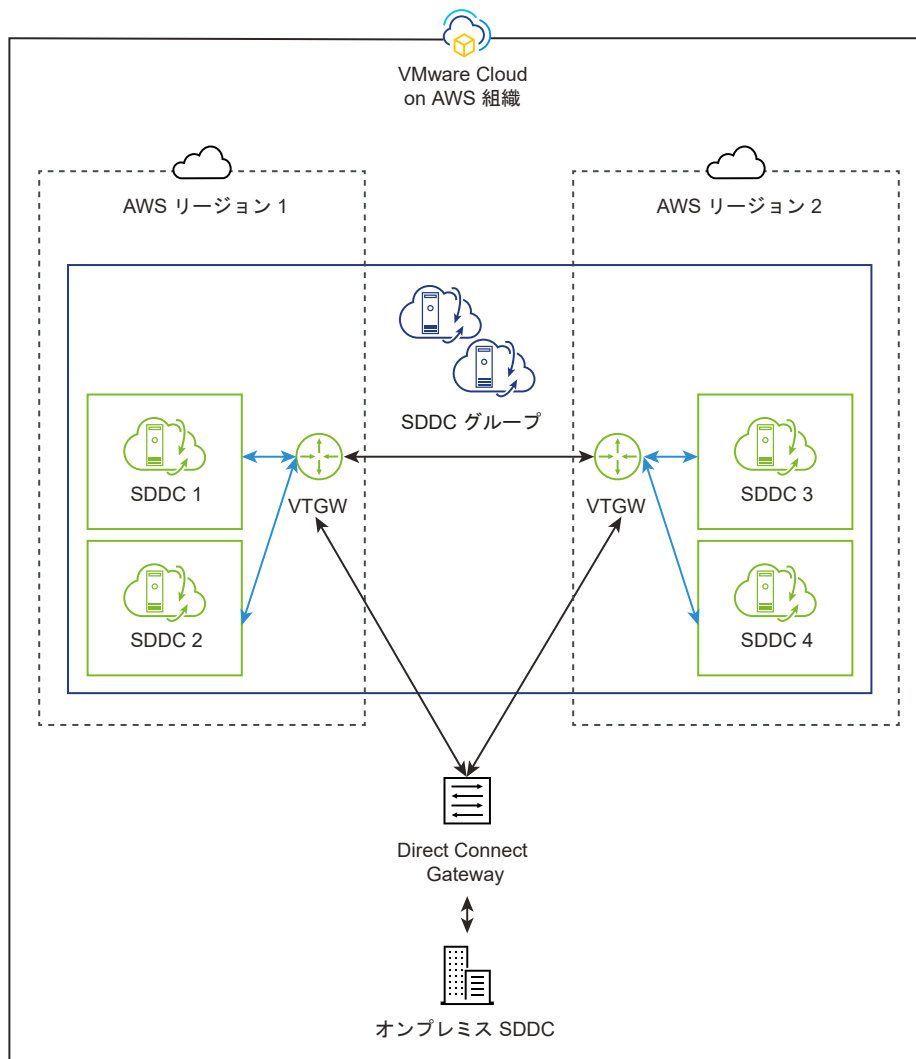
図 3-3. AWS Direct Connect Gateway が SDDC グループをオンプレミスの SDDC に接続



複数のリージョンからの SDDC のグループ化

マルチリージョン SDDC グループは、VPC およびオンプレミス データセンターへの接続を含む単一リージョン SDDC グループと同じ種類の接続を提供しますが、VPC への接続は複数のリージョンにまたがることはできません。1つのグループに複数のリージョンのメンバーが含まれている場合、グループ作成はこれらのリージョンのそれぞれに VTGW をプロビジョニングし、そのリージョン内のグループ メンバーに接続します。この VTGW は、グループ内の他の VTGW とピアリングされ、すべてのグループ メンバーを含む単一の IP アドレス空間が提供されます。グループへの VPC の関連付けは、VPC が占有するリージョン内でのみ有効です。他のリージョン内の SDDC グループ メンバーは、VTGW を介して VPC にアクセスできません。

図 3-4. マルチリージョン SDDC グループ



ルーティングおよびピアリング

SDDC グループ メンバーは、ローカル ネットワーク セグメントをアドバタイズします。これらのセグメントは、SDDC の Tier-0 ルーターのルート テーブルと、グループの VTGW に追加されます。メンバー SDDC によって学習およびアドバタイズされた VMware Transit Connect ルートのリストを表示またはダウンロードするには、NSX Manager またはレガシーの [ネットワークとセキュリティ] タブを開き、[Transit Connect] をクリックします。[VMware Transit Connect を通じて学習およびアドバタイズされたルートの表示](#)を参照してください。

VTGW インスタンス間のピアリングは、同一のリージョン内または異なるリージョン間でサポートされています。

グループ内のすべての SDDC によって学習およびアドバタイズされたルートを表示するには、[ルーティング] タブをクリックします。ドロップダウン コントロールを使用できます。[外部] を選択すると、メンバー間のルートが表示されます。[メンバー] を選択すると、メンバーと外部エンドポイント（VPC や Direct Connect Gateway など）の間のルートが表示されます。[外部] ルートは、VPC や DXGW のような外部エンドポイントから SDDC グループ メンバーを送信元とするトラフィックを送信します。[メンバー] ルートは、メンバー SDDC を送信元とするトラフィックを送信し、SDDC グループ メンバーと外部エンドポイントを含めます。

グループ内の SDDC では、グループ内の他の SDDC によってアドバタイズされたネットワークへのルートと、グループの DXGW を介してアドバタイズされたネットワークへのルートが学習されます。また、グループに接続されている任意の VPC の CIDR も学習します。AWS では、DXGW によってオンプレミスの SDDC などの外部エンドポイントにアドバタイズできるプリフィックスは 20 個という制限が課されています。このため、すべての SDDC グループ メンバーの CIDR ブロック プリフィックスは、その制限を超えない集約可能な範囲内に収まっている必要があります。

VMware Transit Connect では、次のようなルーティング ポリシーが適用されます。

- メンバー SDDC から送信されたトラフィックは、他のメンバー SDDC や、送信元の SDDC と同じリージョン内のグループに接続されている VPC と Direct Connect Gateway にルーティングできます。
- グループに接続されている VPC または Direct Connect Gateway から送信されたトラフィックは、送信元の SDDC と同じリージョンにあるグループ内の SDDC にもルーティングできます。
- VPC 間、または VPC と Direct Connect Gateway 間のトラフィックは、ブロックされます。

注： SDDC が SDDC グループのメンバーになると、既存の SDDC ネットワークのいくつかの側面が変わります。

- ルートベースの VPN によってアドバタイズされるルートは、VMware Transit Connect または DXGW によってアドバタイズされるルートよりも優先されます。ただし、ホストから SDDC ネットワーク外の宛先への送信トラフィックはすべて、SDDC 内の他のルーティング構成に関係なく、VTGW またはプライベート VIF にルーティングされます。vMotion トラフィックと vSphere Replication トラフィックも同様です。受信トラフィックと送信トラフィックのパスが対称になるように、ESXi ホストへの受信トラフィックも DXGW インターフェイス経由でルーティングされるようにする必要があります。
 - 同じルートが VTGW と DX を介してアドバタイズされる場合は、VTGW パスが推奨されます。これには、VTGW に接続された DXGW からのルートが含まれます。
 - グループ メンバー間のイントラネット トラフィックの最大 MTU は 8,500 バイトに制限されます。SDDC 内部または DX を介するトラフィックには、最大 8,900 バイトの MTU を使用できます。[「SDDC の管理およびコンピューティング ネットワーク トラフィック用のプライベート仮想インターフェイスの作成」](#)を参照してください。
-

SDDC グループの作成または変更

SDDC グループを作成するには、グループの名前と説明を入力してから、メンバーにする SDDC を組織から選択します。

前提条件

VMC コンソールにログインするときは、[管理者] または [削除が制限された管理者] の VMC サービス ロールが必要です。

手順

1 <https://vmc.vmware.com> から VMware Cloud コンソール にログインします。

2 [インベントリ] 画面で、[SDDC グループ] をクリックします。

3 [SDDC グループ] タブで [アクション] をクリックして、[SDDC グループの作成] を選択します。

グループの [名前] を入力し、オプションで [説明] を入力して [次へ] をクリックします。後でグループを編集して、これらの値を変更できます。

4 [メンバーシップ] グリッドで、グループ メンバーとして含める SDDC を選択します。

グリッドには、組織内のすべての SDDC のリストが表示されます。グループ内のメンバーシップの資格を得るには、SDDC が次の条件を満たす必要があります。

- 管理ネットワークの CIDR ブロックは、他のグループ メンバーの管理 CIDR ブロックと重複することはありません。
- 別の SDDC グループのメンバーであってはなりません。

メンバーの選択が終了したら、[次へ] をクリックします。後でグループを編集して、メンバーを追加または削除できます。

5 SDDC グループの作成時に発生するコストについて理解し、その責任を負うことを確認します。次に [グループの作成] をクリックして、SDDC グループとその VMware Transit Connect ネットワークを作成します。

[グループの作成] をクリックすると、課金が始まります。このプロセスは、開始後に一時停止やキャンセルを行うことはできません。グループ メンバーは、展開が完了するまでグループの VMware Transit Connect ネットワークを使用できません。通常、展開には約 15 分かかります。展開が完了すると、グループの [接続ステータス] が [保留] から [接続済み] に変化します。

6 (オプション) グループ名や説明を変更したり、グループ メンバーを追加または削除したりするには、[アクション] をクリックして [グループの編集] を選択します。

[接続ステータス] が [保留] の間は、グループを編集できません。

次のステップ

グループ内の SDDC、VPC、TGW/DGW インスタンスによって学習およびアドバタイズされたルートを表示するには、[ルーティング] タブをクリックします。ドロップダウン コントロールで [外部] を選択して、VPC や Direct Connect Gateway などの外部エンドポイントで使用するルートを表示します。メンバー SDDC で使用されるルートを表示するには、[メンバー] を選択します。

メンバーの SDDC 内でワークロード間のネットワーク トラフィックを許可するには、各メンバーにコンピューティング ゲートウェイの一連のファイアウォール ルールを作成する必要があります。詳細については、[SDDC グループメンバーのワークロード接続を有効にするためにコンピューティング ゲートウェイのファイアウォール ルールを追加](#)を参照してください。これは、新しいメンバーをグループに追加するたびに行う必要があります。

SDDC グループへの VPC の接続

AWS VPC を SDDC グループに接続するには、VMware Transit Connect を使用します。これにより、グループ内の SDDC とその VPC で実行される AWS サービスとの間でネットワーク接続を簡単に行うことができます。

VMware Transit Connect は SDDC グループ メンバー間のすべてのコンピューティングおよび管理ネットワーク トラフィックを処理しますが、外部 VPC または他の AWS オブジェクトから SDDC グループの VTGW にトラフィックを送信するように AWS ルート テーブルが自動的に設定されることはありません。この種の接続を必要とするネットワーク トポロジには、「セキュリティ VPC」（これを介して SDDC グループとインターネットとの間のすべてのトラフィックが検査用にルーティングされます）の作成および AWS オブジェクトと SDDC グループメンバー間の通信を有効にするための同様の要件が含まれます。この種のネットワーク トポロジでは、[手順 8](#) に示すように、SDDC グループの VTGW から VPC へのトラフィックの宛先ルートを定義する必要があります。

SDDC グループに VPC を接続するには、複数のステップを実行する必要があります。また、このプロセスでは、VMware Cloud コンソールと AWS コンソールの両方を使用する必要があります。最初に、VMware Cloud コンソールを使用して、VTGW（VMware で管理される AWS リソース）を共有できるようにします。次に、AWS コンソールを使用して、共有リソースを受け入れ、SDDC グループに接続する VPC に関連付けます。

手順

- 1 VMware Cloud コンソールの [インベントリ] 画面で [SDDC グループ] をクリックし、VPC を接続するグループの [名前] をクリックします。
- 2 グループの [外部 VPC] タブで [アカウントの追加] をクリックし、グループに接続する VPC を所有する AWS アカウントを指定します。

これにより、VTGW 用にそのアカウントで AWS リソースを共有できるようになります。

- 3 AWS コンソールで、[Resource Access Manager] - [Shared with me] の順に開き、共有 VTGW リソースを受け入れます。

リソースの [Name] の形式は `VMC-Group-UUID` で、[Pending] の [Status] です。リソース名をクリックしてリソースの [Summary] カードを開き、[Accept resource share] をクリックして受け入れを確定します。

- 4 VMware Cloud コンソールで、グループの [VPC 接続] タブに戻り、[手順 3](#) で受け入れたリソース共有の [ステータス] が [関連付け] から [関連付け済み] に変化するまで待ちます。

VPC リソースの関連付けには、最大で 10 分かかることがあります。VPC の関連付けが完了したら、VTGW を接続できます。

- 5 AWS コンソールの [Resource Access Manager] に戻り、共有 VTGW リソースのリソース ID を確認します。

これは、[Shared with me: Shared resources] に、`TGW-UUID` 形式の [Resource ID] と `ec2:TransitGateway` の [リソース タイプ] が表示されます。

6 Transit Gateway の接続を作成します。

- a 手順 5 で特定した [Transit Gateway ID] を選択し、VPC の [Attachment type] を指定して、SDDC グループに接続する [VPC ID] を選択します。
- b グループへの接続を必要とする各アベイラビリティ ゾーン (AZ) で [サブネット ID] を選択します。
AZ あたりの選択できるサブネットは 1 つのみですが、SDDC グループ メンバーはその AZ 内のすべての VPC サブネットと通信できます。
- c 「外部ストレージとしての Amazon FSx for NetApp ONTAP の構成」に記載されているように、VPC が FSx VPC の場合は、[DNS support] も選択する必要があります。
- d [Create Transit Gateway Attachment] をクリックして接続を作成します。

7 VMware Cloud コンソールで、グループの [外部 VPC] タブに戻り、共有 VPC 接続を [承諾] します。

VPC のステータスが [承諾の保留中] に変化したら、[承諾] をクリックして受け入れます。承諾プロセスが完了すると、ステータスが [使用可能] に変化します。承諾には、最大で 10 分ほどかかる場合があります。

8 VPC への追加のルートを構成します。


AWS コンソールで、共有 VTGW に接続されている VPC のすべてのサブネットに関連付けられ、SDDC グループとの通信が必要なルート テーブルを特定します。ルート テーブルの [ルート] タブで、[ルートの編集] をクリックし、SDDC グループ内のすべての CIDR を、手順 5 で特定した VTGW ID に設定したターゲットとともに宛先として追加します。SDDC グループの CIDR のリストは、SDDC グループの VMC コンソールの [ルーティング] タブで [ルート テーブル] ドロップダウンの [外部] を選択して確認できます。

ルートを手動で編集する代わりに、管理対象プリフィックス リストを作成して、VPC に関連付けられているメイン ルート テーブルに追加することを検討してください。共有プリフィックス リストを使用した外部 VPC および TGW オブジェクトのルーティングの簡素化を参照してください。

9 (オプション) VPC への追加の宛先ルートを構成します。

SDDC グループを作成すると、VPC のプライマリ CIDR とすべてのセカンダリ CIDR のルートがシステムによって作成されます。宛先を VPC 経由した外部にする必要がある場合 (セキュリティ VPC またはトランジット VPC で必要な場合など) は、接続された VPC にルーティングする追加の CIDR ブロックを定義できます。

グループの VTGW から外部 VPC へのルーティングを作成または変更するには、[外部 VPC] タブを開き、VPC を所有する [AWS アカウント ID] を選択し、行を展開します。ルートが指定されていない場合は、[ルート] 列の [ルートの追加] をクリックして [ルートの編集] 画面を開き、この VPC を [ターゲット] として使用する 1 つ以上のルートを追加します。それ以外の場合、[ルート] 列に最初のルートと追加ルートの数が表示されま

す。鉛筆アイコン () をクリックして [ルートの編集] 画面を開き、このリストを編集できます。各プリフィックスは、グループの VTGW から [VPC ID] 列にリストされている VPC へのルートを定義します。また、各プリフィックスは、グループの [ルーティング] タブに [ターゲット] として表示されます。接続された各 VPC に対して最大 100 個のルートを指定できます。

次のステップ

- AWS コンソールで、グループに追加した VPC と他のグループ メンバーとの間のトラフィックを管理するネットワーク ACL を作成します。VPC で実行している AWS サービスにアクセスする場合は、サービスの AWS セキュリティ ポリシーの変更が必要になる場合があります。S3 サービスの AWS セキュリティ ポリシー構成の例については、「[S3 エンドポイントを使用した S3 バケットへのアクセス](#)」を参照してください。

SDDC グループへの AWS Transit Gateway の接続

SDDC グループ メンバーが、グループ内の SDDC と任意のリージョン内の任意の VPC で実行されている AWS サービスの間のネットワーク接続を実行できるようにするには、AWS Transit Gateway を SDDC グループに接続します。

SDDC グループに AWS Transit Gateway (TGW) を接続するには、複数のステップを実行する必要があります。また、このプロセスでは、VMware Cloud コンソールと AWS コンソールの両方を使用する必要があります。VMware Cloud コンソールを使用して既存の TGW へのアクセス権を要求し、AWS コンソールを使用して SDDC グループの VTGW に接続します。VMware によって管理される AWS リソースである VTGW とは異なり、TGW はユーザーが自分で使用および管理できる純粋な AWS リソースです。AWS ドキュメントの [Getting started with transit gateways](#) を参照してください。

手順

- 1 VMware Cloud コンソールの [インベントリ] 画面で [SDDC グループ] をクリックし、AWS TGW を接続するグループの [名前] をクリックします。
- 2 グループの [外部 TGW] タブで、[TGW の追加] をクリックし、必要なパラメータと値の情報を指定します。

パラメータ	値
AWS アカウント ID	TGW を所有する AWS アカウント。
TGW ID	TGW の AWS ID。指定した AWS アカウントによって所有されている既存の TGW を使用するか、そのアカウント内で新しい TGW を作成することができます。
TGW の場所	TGW が配置されている AWS リージョン。
VMC on AWS リージョン	SDDC グループが存在する AWS リージョン。
ルート	このピアリング接続を介して到達可能な AWS リソースの宛先プリフィックス

[追加] をクリックして、TGW をグループの VTGW にピアとして追加します。[ステータス] 列が [PENDING_ACCEPTANCE] に変化したら、[手順 3](#) に進みます。

- 3 [手順 2](#) で指定した AWS アカウント ID の管理者認証情報を使用して AWS コンソールにログインします。
AWS コンソールで [Transit Gateway Attachments] に移動し、TGW ID が [手順 2](#) で指定した TGW ID と一致する TGW を選択し、[Accept Transit Gateway Attachment] をクリックします。
- 4 VMware Cloud コンソールで、グループの [外部 TGW] タブに戻り、TGW の [状態] が [関連付け済み] に変更されていることを確認します。

5 (オプション) AWS ルート テーブルを接続された TGW に関連付けます。

新しい TGW のピアリング セッションでは、TGW 接続を AWS ルート テーブルに関連付ける必要があります。一部の環境では、ルート テーブルがデフォルトで接続に関連付けられないため、AWS コンソールを使用してルーティング テーブルを接続に関連付ける必要があります。[Getting started with transit gateways](#) の「Add routes between the transit gateway and your VPCs」を参照してください。

6 CGW ファイアウォール ルールを作成して、TGW を経由するワークロード トラフィックを有効にします。

[SDDC グループ メンバーのワークロード接続を有効にするためにコンピューティング ゲートウェイのファイアウォール ルールを追加](#)を参照してください。

7 SDDC または AWS ルーティング テーブルで、追加の送信元ルートと宛先ルートを構成します。

グループの VTGW から外部 TGW へのルーティングを作成または変更するには、[外部 TGW] タブを開きます。TGW を所有する [AWS アカウント ID] を選択し、行を展開します。ルートが指定されていない場合は、

[ルート] 列に最初のルートと追加ルートが表示されます。鉛筆アイコン (✎) をクリックして [ルートの編集] 画面を開き、このリストを編集できます。または、[ルート] 列の [ルートの追加] をクリックして [ルートの編集] 画面を開きます。外部 TGW を介してネイティブ AWS サブネットへのルートを指定する CIDR プリフィックスを追加します。各プリフィックスは、グループの VTGW から [TGW ピアリング接続 ID] 列にリストされている外部 TGW へのルートを定義します。また、各プリフィックスは、グループの [ルーティング] タブに [ターゲット] として表示されます。接続された各 TGW に対して最大 100 個のルートを指定できます。

ルートを手動で編集する代わりに、管理対象プリフィックス リストを作成して、TGW に関連付けられているメイン ルート テーブルに追加することを検討してください。[共有プリフィックス リストを使用した外部 VPC および TGW オブジェクトのルーティングの簡素化](#)を参照してください。

次のステップ

トポロジの例と推奨されるワークフローについては、「[Getting Started with VMware Transit Connect Intra-Region Peering for VMware Cloud on AWS](#)」を参照してください。

共有プリフィックス リストを使用した外部 VPC および TGW オブジェクトのルーティングの簡素化

SDDC グループ接続を拡張して、所有および管理しているネイティブの AWS オブジェクト (VPC、Transit Gateway (TGW)、Direct Connect Gateway (DXGW) など) を含める場合は、VPC ルート テーブルまたは VMware Cloud on AWS 共有プリフィックス リストも編集してグループの VTGW とそれらのオブジェクト間の接続を確立し、維持する必要があります。

VMware Cloud on AWS ネットワークとネイティブの AWS オブジェクト間の接続のルート管理は、ネットワーク トポロジによって異なります。[SDDC グループへの VPC の接続](#)および [SDDC グループへの AWS Transit Gateway の接続](#)に示すように、TGW や VPC などのネイティブの AWS オブジェクトを含むすべてのトポロジでは、それらのオブジェクトから SDDC グループへのリターン パスを定義する必要があります。SDDC グループからネイティブの AWS オブジェクト (SDDC グループとインターネット間のすべてのトラフィックが検査用にルーティングされる「セキュリティ VPC」など) にトラフィックを送信するトポロジでは、それらの送信ルートを手動で構成する必要があります。そのためには、AWS の [Virtual Private Cloud ユーザー ガイド](#)の説明に従ってネイティブのルート テーブルを編集するか、VMware Cloud on AWS 共有プリフィックス リストを使用します。

共有プリフィックス リスト（VMware が管理し、AWS アカウントと共有するサブネット CIDR のリスト）は、ほとんどの SDDC グループに最適なオプションです。このリストでは、NSX Edge の移行またはフェイルオーバー時および SDDC グループのメンバーが追加/削除されるたびに、外部 VPC および TGW ルート テーブルが自動的に更新されるためです。詳細については、VMware Cloud Tech Zone の記事 [Understanding Shared Prefix Lists for SDDC Groups in VMC on AWS](#) を参照してください。

手順

- 1 VMware Cloud コンソールの [インベントリ] 画面で [SDDC グループ] をクリックし、VPC が接続されたグループの [名前] をクリックします。

- 2 グループ メンバーのサブネットおよび外部 AWS オブジェクトとの間のルートの手動メンテナンスの簡素化に使用できる共有プリフィックス リストを作成するには、グループの [ルーティング] タブを開き、[プリフィックス リストの作成] をクリックします。

外部 VPC のルート テーブルを手動で更新する場合は、この手順をスキップできます。

- a [プリフィックス リストの作成] カードで必要な値を入力し、[プリフィックス リストの作成] をクリックします。

[プレフィックス リスト名]	名前を入力します。
[VMC on AWS リージョン]	SDDC グループのメンバーが占有する AWS リージョンのリストからリージョンを選択します。
[AWS リージョン]	プリフィックス リストを作成するリージョン。最初は [VMC on AWS リージョン] の値と同じですが、プリフィックス リストを別のリージョンに作成するように変更できます。
[関連付ける AWS アカウント]	このリストには、SDDC グループに関連付けられている 12 桁の AWS アカウント ID が事前に入力されています。必要に応じて、アカウント ID を追加または削除できます。

[プリフィックス リストの作成] をクリックすると、プリフィックス リストの [ステータス] が [作成の実行中です] に変わります。

- b プリフィックス リストの [ステータス] が [作成済み] に変わったら、リソース共有を受け入れる権限を持つ AWS ID を使用し、[関連付けられた AWS アカウント] のいずれかを使用して AWS コンソールにログインします。

[Resource Access Manager] - [Shared with me] の順にクリックして、アカウントがアクセスできる AWS リソース共有のリストを表示します。リソースの [Name] の形式は `VMC-SHARED-PREFIX-LIST-ID` で、[Status] は [Pending] です。リソースの [Name] をクリックしてリソース共有の詳細カードを開き、[Accept resource share] をクリックして受け入れを確定します。


- c AWS コンソールで [Your VPCs] を開き、VPC を選択して、VPC のメイン ルート テーブルに 1 つ以上のプリフィックスを追加します。

[Add route] をクリックし、プリフィックス リスト ID を [Destination] として入力し、SDDC グループの VTGW を [Target] として指定します。

注： 各プリフィックス リストは、ルート テーブルへの追加の際に 1 つの [ルート] としてカウントされますが、多数のエントリがリストに含まれている場合があります。各エントリはルート テーブルの割り当てに含まれます。[AWS VPC ルート テーブルの割り当て](#)の説明を参照して、すべてのルートをプリフィックス リストに含めるための十分なキャパシティがルート テーブルにあることを確認してください。

VPC ルート テーブルにプリフィックス リストを追加すると、SDDC グループのメンバーからターゲット TGW または VPC オブジェクトへのすべてのルートが自動的に更新されます。

- 3 共有プリフィックス リストを変更または削除するには、グループの [ルーティング] タブを開きます。

- [プリフィックス リスト名] またはその [関連付けられた AWS アカウント] を変更するには、鉛筆アイコン () をクリックして、[プリフィックス リスト名の編集] または [AWS アカウントの関連付け] カードを開きます。

- プリフィックス リストを削除するには、リストを選択して、[プリフィックス リストの削除] をクリックします。リストに関連付けられているリソース（ルート テーブルなど）は、リストを削除する前に削除する必要があります。
- 4 この SDDC グループに対して（手動で、または共有プリフィックス リストから）プログラムされた現在の一連のルートを表示するには、グループの [ルーティング] タブを開きます。

[メンバー]（グループ内の SDDC とグループの VTGW および接続された VPC）、または [外部] エンドポイント（他のグループ内の SDDC）へのルートを表示できます。各リストは、オブジェクト タイプ（SDDC、VPC、または TGW）でフィルタリングできます。

SDDC グループ サポート情報の表示

SDDC グループのサポート情報には、作成日、グループ ID、および VTGW ID が含まれます。

SDDC グループのサポート情報は、SDDC グループの [サポート] タブに表示されています。また、VMware Aria Operations for Logs サービスを使用して、SDDC グループによってログに記録されたイベントを表示することもできます。type\:[SDDC_GROUP | SDDC_SHARE | EXTERNAL]) 形式の VMware Aria Operations for Logs 正規表現を指定すると、ストリーム内の SDDC グループ ログ エントリが返されます。

前提条件

VMC コンソールにログインするときは、[管理者] または [削除が制限された管理者] の VMC サービス ロールが必要です。

手順

- 1 <https://vmc.vmware.com> から VMware Cloud コンソール にログインします。
- 2 [インベントリ] 画面で、[SDDC グループ] をクリックします。
- 3 グループのカードの [詳細表示] をクリックし、グループの [サマリ] 画面を開きます。
- 4 [サポート] タブをクリックして、グループの [サポート情報] を表示します。

SDDC グループの削除

SDDC グループを削除するには、グループ内のすべてのメンバーを削除してから、グループを削除します。

グループからメンバーを削除すると、そのメンバーはグループの VTGW からは切断されますが、グループのプロパティに対してその他の変更が行われることはありません。SDDC グループを削除すると、グループの VMware Transit Connect ネットワークと、そのネットワークに関連付けられているルーティング情報が、その VTGW とともに破棄されます。

前提条件

VMC コンソールにログインするときは、[管理者] または [削除が制限された管理者] の VMC サービス ロールが必要です。

手順

- 1 <https://vmc.vmware.com> から VMware Cloud コンソール にログインします。
- 2 [インベントリ] 画面で [SDDC グループ] をクリックし、削除するグループをクリックします。

- 3 [名前] チェックボックスをクリックして、グループ内のすべての SDDC を選択し、[SDDC の削除] をクリックします。

SDDC を削除した場合の影響について理解していることを確認してから、[続行] をクリックして削除を実行します。削除は SDDC ごとに数分かかることがあります。

- 4 すべての SDDC が削除されたら、[アクション] - [グループの削除] の順にクリックして、グループとグループに関連付けられた AWS リソースを削除します。

グループを削除した場合の影響について理解していることを確認してから、[グループの削除] をクリックして、削除を実行します。

SDDC グループ メンバーのワークロード接続を有効にするためにコンピューティング ゲートウェイのファイアウォール ルールを追加

グループ内の SDDC ごとにコンピューティング ゲートウェイのファイアウォール ルールを作成する必要があります。これらのルールがないと、グループ メンバーで実行されているワークロードは、VMware Transit Connect を使用して相互に通信できません。

SDDC グループのすべてのメンバーは、同じ VMware Cloud on AWS 組織によって所有されるため、グループのメンバー間のネットワーク トラフィックを、East-West トラフィックとして安全に処理できます。送信元または宛先が外部の可能性がある North-South トラフィックとして処理されることはありません。ただし、SDDC コンピューティング ゲートウェイのデフォルトのファイアウォール ルールでは、外部トラフィックが拒否されるため、ファイアウォール ルールを作成し、トラフィックがグループ内の各 SDDC のコンピューティング ゲートウェイを通過できるようにする必要があります (SDDC グループは現在、メンバーの管理ゲートウェイを介してネットワーク トラフィックをルーティングする必要はありません)。

VMware Cloud on AWS では、コンピューティング ゲートウェイのファイアウォール ルールでの使用を目的としたインベントリ グループのセットが定義されています。これにより、グループ メンバー間のトラフィック全体を制御することができます。これらのグループには、VMware Transit Connect と、SDDC の AWS アカウント所有者が所有する AWS Transit Gateway で学習したルートのプリフィックス (CIDR ブロック) が含まれています。

[Transit Connect ユーザーの TGW プリフィックス]

ユーザーが所有する AWS Transit Gateway から学習したルート。

[Transit Connect の DGW プリフィックス]

グループの Direct Connect Gateway から学習されたルート。

[Transit Connect のネイティブ VPC プリフィックス]

グループの接続された VPC から学習されたルート。

[Transit Connect の他の SDDC プリフィックス]

グループ内の他の SDDC から学習されたルート。

グループ メンバーシップが変更され、新しいルートが学習されると、各グループのプリフィックスが自動的に追加、削除、更新されます。

詳細については、「[コンピューティング ゲートウェイのファイアウォール ルールの追加または変更](#)」および「[インベントリ グループの操作](#)」を参照してください。

手順

- 1 [コンピューティング ゲートウェイのファイアウォール ルールの追加または変更](#)で定義されているワークフローを使用して、必要なインベントリ グループとコンピューティング ゲートウェイ ファイアウォール ルールを作成します。

システム定義のインベントリ グループは、グループ メンバーおよび接続されている VPC の間の全体的な接続を作成するのに役立ちます。詳細なファイアウォール ルールを作成して、メンバー SDDC の個々のワークロード セグメントに適用する必要がある場合は、次の例に示すように、インベントリ グループを作成して、それらのセグメントを定義する必要があります。

- 2 [ゲートウェイ ファイアウォール] - [コンピューティング ゲートウェイ] の順にクリックしてから、[ルールの追加] をクリックします。

システム定義のインベントリ グループと、ユーザーが定義したコンピューティング グループを、[送信元] 画面と [宛先] 画面で選択できます。無制限のグループ接続を有効にするには、次のようなルールを追加します。これにより、他のグループ メンバーからこの SDDC への受信トラフィックが許可されます。

名前	送信元	宛先	サービス	適用先	操作
他の SDDC からの受信	[Transit Connect の他の SDDC プリ フィックス]	任意	任意	Direct Connect インターフェイス	Allow

ローカル ワークロード セグメントの CIDR ブロックを使用してインベントリ グループを作成した場合は、それらを使用して、このトラフィックに詳細な制御を適用する優先順位の高いルールを作成できます。

例：グループ メンバー間のワークロード トラフィックを許可する、ユーザー定義のインベントリ グループを使用する CGW ファイアウォール ルール

これらの例では、NSX Manager を使用してインベントリ グループとファイアウォール ルールを作成する方法を示します。このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

グループの作成

NSX Manager で、[インベントリ] - [コンピューティング グループ] の順にクリックしてから、[グループの追加] をクリックして 3 つのグループを作成します。グループには、任意の名前を使用できます。ここに示すのは、単なる例です。

- SDDC 独自のワークロード セグメント用のセグメント プリフィックスを含む、**ローカル ワークロード**という名前のグループ。
- グループ内の他の SDDC のワークロード セグメント用のセグメント プリフィックスを含む、**ピア ワークロード**という名前のグループ。
- グループ内の各 SDDC の vCenter Server のプライベート IP アドレスを含む、**ピア SDDC vCenter Server** という名前のグループ。

各グループについて、[コンピューティング メンバー] 列の [設定] をクリックして [メンバーの設定] ツールを開きます。このツールでは、[基準の追加] をクリックして、グループ メンバーの [IP アドレス] または [MAC アドレス] を入力できます。また、[アクション] - [インポート] の順にクリックして、これらの値をファイルからインポートすることもできます。

ルールの作成

手順 2 と同様に、[ゲートウェイ ファイアウォール] カードを開き、[コンピューティング ゲートウェイ] をクリックして、[ルールの追加] をクリックします。これにより、[送信元] および [宛先] に対して作成されたインベントリ グループを使用する新しいルールが作成されます。ルールには、任意の名前を使用できます。ここに示すのは、単なる例です。

名前	送信元	宛先	サービス
ローカル ワークロードからピア ワークロードへ	ローカル ワークロード	ピア ワークロード	ローカル ワークロードから他のグループ メンバーのワークロードへの送信トラフィック用
ピア ワークロードからローカル ワークロードへ	ピア ワークロード	ローカル ワークロード	他のグループ メンバーのワークロードからローカル ワークロードへの受信トラフィック用

コンピューティング ゲートウェイ ファイアウォールを通過する SDDC グループ メンバー トラフィックを管理するすべてのルールは、[すべてのアップリンク] に適用する必要があります。また、アクションとして [許可] を設定する必要があります。

SDDC グループへの Direct Connect Gateway の接続

SDDC グループの作成後、オンプレミスの SDDC をそのグループの Direct Connect Gateway に接続して、SDDC グループのすべてのメンバーへの DX 接続を提供することができます。

VMware Transit Connect は、SDDC グループ メンバー間のすべてのコンピューティングおよび管理ネットワーク トラフィックを処理します。多くの SDDC グループ メンバーは、オンプレミス データセンターへのネットワーク接続も必要になります。これらの接続を有効にするには、AWS Direct Connect Gateway をグループの VMware Managed Transit Gateway に関連付けます。

SDDC グループに Direct Connect Gateway を接続するには、複数のステップを実行する必要があります。また、このプロセスでは、VMware Cloud コンソールと AWS コンソールの両方を使用する必要があります。最初に、VMware Cloud コンソールを使用して、VTGW（AWS リソース）を共有できるようにします。次に、AWS コンソールを使用して、共有リソースを受け入れ、SDDC グループに接続する Direct Connect Gateway に関連付けます。既存の Direct Connect Gateway で許可されるプリフィックスのリストを変更する必要がある場合は、AWS コンソールも使用します。

前提条件

AWS Direct Connect Gateway を作成する必要があります。AWS ドキュメントの [Direct Connect ゲートウェイの作成](#) を参照してください。

手順

- 1 VMware Cloud コンソールの [インベントリ] 画面で [SDDC グループ] をクリックし、Direct Connect Gateway を接続するグループの [名前] をクリックします。

- 2 グループの [Direct Connect] タブで [アカウントの追加] をクリックし、グループに追加する Direct Connect Gateway を所有する AWS アカウントを指定します。

[Direct Connect Gateway の追加] 画面で、次の値を入力します。

オプション	説明
Direct Connect Gateway の接続 ID	AWS コンソールでゲートウェイ オブジェクトの [Direct Connect Gateway] 画面に表示される [ID] 値。
場所	このゲートウェイのために、追加の VTGW 接続を指定します。任意のリージョン内の単一の Direct Connect Gateway 接続で、マルチリージョン グループのすべてのメンバー間のトラフィックを処理できますが、推移的なルーティングはサポートされません。1つのグループに2つの異なるリージョンのメンバーが存在し、DXGW 接続が1つのみである場合、DXGW に接続されたリージョンの SDDC からのトラフィックだけが、オンプレミス データセンターにルーティングされます。[VTGW の場所] コントロールを使用して、DXGW を別のリージョン内の VTGW に関連付けます。
許可されたプリフィックス	指定された [VTGW の場所] の SDDC グループ メンバーのコンピューティング ネットワーク CIDR ブロックのカンマ区切りのリスト。

[OK] をクリックすると、指定されたゲートウェイについて、AWS の関連付けの提案が生成されます。

- 3 AWS コンソールで、ゲートウェイ オブジェクトの [Direct Connect Gateway] 画面を開き、関連付けの提案を受け入れます。

受け入れには、最大で 20 分ほどかかる場合があります。受け入れが完了すると、次のようになります。

- AWS コンソールの場合、ゲートウェイ オブジェクトの AWS [Direct Connect Gateway] 画面で、ゲートウェイの [状態] が [関連付け済み] になります。
- VMware Cloud コンソールの場合、グループの [Direct Connect] タブで、ゲートウェイの [状態] が [接続済み] になります。

- 4 Direct Connect Gateway と Direct Connect ロケーション (Direct Connect プロバイダ) の間に AWS Transit VIF を接続します。

AWS VPC ドキュメントの [Direct Connect Gateway へのトランジット ゲートウェイの接続](#)を参照してください。

- 5 (オプション) Direct Connect Gateway の場所を追加します。

複数リージョンの SDDC グループでは、任意のリージョン内の VTGW グループを Direct Connect Gateway に接続できます。グループの [Direct Connect Gateway] タブで、[場所の追加] をクリックして [Direct Connect Gateway の場所を追加] カードを開き、ゲートウェイに接続する AWS リージョンと1つ以上の [許可されたプリフィックス] を指定します。

次のステップ

Direct Connect Gateway とオンプレミスの SDDC 間のトラフィックを許可するために必要なファイアウォール ルールを作成します。

SDDC グループでの vCenter Server の関連付けの使用

SDDC 展開グループを含む組織は、それらの SDDC 内の vCenter Server システムを関連付けることで、管理者が、統合されたインベントリを同じ vSphere Client ビューで管理できるようにします。

SDDC グループで vCenter Server の関連付けを有効にすると、クラウド管理者は cloudadmin@vmc.local としてログインし、vSphere Client を使用してグループ内のすべての vCenter Server システムを管理できます。cloudadmin@vmc.local アカウントが、シングル サインオンを使用するようにこれらのシステムを構成している場合、そのシングル サインオン ドメイン内のアカウントを持つユーザーは、グループ内にある関連付けられたすべてのシステムにアクセスできます。

SDDC グループで vCenter Server の関連付けを有効にすると、そのグループに追加された SDDC 内の vCenter Server システムが自動的に関連付けられ、グループから削除された SDDC 内の vCenter Server システムの関連付けは自動的に解除されます。

前提条件

ネットワーク

この機能に必要な L3 ネットワークは、SDDC グループの作成時の一環としてすでに構成されている VMware Transit Connect によって提供されます。グループ内の関連付けられた各 vCenter Server は、グループの VMware Transit Connect ゲートウェイ経由のルートを使用して、プライベート IP アドレスにある他の関連付けられた vCenter Server インスタンスに到達できる必要があります。他のルーティング構成はサポートされていません。

関連付けられた SDDC グループ内の vCenter Server インスタンス間での vMotion を使用した仮想マシンの移行は機能しません。これは、VMware Transit Connect がグループ メンバー間に L3 接続のみを作成するためです。vMotion を使用して移行するには、L2 接続が必要です。

サービス ロール

この操作は、[管理者] または [削除が制限された管理者] の VMC サービス ロールを持つユーザーに限定されます。

vCenter Server の名前解決

グループ内の関連付けられた各 vCenter Server は、関連付けられた他の vCenter Server のホスト名と FQDN をプライベート IP アドレスに解決できる必要があります。「[vCenter Server の FQDN 解決アドレスの設定](#)」を参照してください。

ハイブリッド リンク モード

[VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理](#)で説明したように、SDDC が SDDC グループのメンバーである場合、VPN 接続でのハイブリッド リンク モードの使用はサポートされません。

重要： VMware Cloud Gateway を使用して、リンクされた SDDC グループ メンバーへの Direct Connect Gateway (DXG) 接続を介してハイブリッド リンク モードを構成することはできません。

VMware Cloud Disaster Recovery

26 より前のバージョンの VMware Cloud Disaster Recovery で保護されている SDDC では、vCenter Server の関連付けはサポートされません。

手順

- 1 <https://vmc.vmware.com> から VMware Cloud コンソール にログインします。

- 2 [インベントリ] 画面で、[SDDC グループ] をクリックします。

このページには、組織内のすべての SDDC グループが一覧表示されます。SDDC グループを作成するには、[SDDC グループの作成または変更](#)を参照してください。

- 3 [SDDC グループ] ページで SDDC グループのカードを選択し、[詳細表示] をクリックして、[vCenter Server の関連付け] タブを開きます。

このページには、グループ内のすべての SDDC、それらのバージョン、および vCenter Server の関連付けステータスが表示されます。

- 4 リスト内のすべての vCenter Server システムを関連付けるには、[すべての vCenter Server のリンク] をクリックします。

この操作により、[関連付け解除済み] ステータスのすべての vCenter Server システムが関連付けられます。SDDC グループ内の vCenter Server システムの関連付けは、1 回だけ実行するものです。これによりグループのプロパティが作成され、グループ内の vCenter Server システムは、故意に関連付けが解除されるまで、SDDC の一連のメンバーとは関係なく常に関連付けられた状態になります。グループ内のすべての vCenter Server について [すべての vCenter Server のリンク] を実行すると、SDDC がグループに追加されるたびに vCenter Server の関連付けが自動的に行われます。SDDC がグループから削除されると、関連付けられた vCenter Server システムは自動的に関連付けが解除されます。

- 5 (オプション) 関連付けられた vCenter Server システムには、共有 ID ソースを設定してください。

関連付けられた vCenter Server システムを、同じ ID ソースを使用するように構成すると、その ID ソースで定義されたユーザー アカウントは、ID ソースのアカウントに定義された権限を持つ、関連付けられたすべての vCenter Server システムにアクセスできます。構成の詳細については、VMware vSphere のドキュメントにある、[vCenter Single Sign-On による vSphere 認証](#)を参照してください。この手順を実行しない場合、cloudadmin@vmc.local は、VMware Cloud コンソールの [設定] タブにリストされている認証情報を使用して、関連付けられたすべての vCenter Server システムに対して認証を行うことができます。

- 6 リスト内のすべての vCenter Server システムの関連付けを解除するには、[すべての vCenter Server のリンク解除] をクリックします。

この操作により、[関連付け] ステータスのすべての vCenter Server システムの関連付けが解除されます。SDDC グループ内の vCenter Server システムの関連付けと同様、関連付けの解除は 1 回だけ実行するものです。これによりグループのプロパティが作成され、グループ内の vCenter Server システムは、故意に関連付けられるまで、関連付けがない状態になります。グループ内のすべての vCenter Server について [すべての vCenter Server のリンク解除] を実行すると、SDDC がグループに追加されても vCenter Server システムは関連付けがないままとなります。

VMware Transit Connect を通じて学習およびアドバタイズされたルートの表示

SDDC グループのメンバーである SDDC では、[Transit Connect] 画面を開き、グループ用に作成された VMware Transit Connect インスタンスによって学習およびアドバタイズされたルートを表示できます。

SDDC グループでは、グループ メンバー間のすべてのネットワーク トラフィックが VMware Transit Connect ネットワークを通過します。サブネットが追加または削除されると、グループ内にあるすべての SDDC のコンピューティング ネットワーク間のルーティングが VMware Transit Connect によって自動的に管理されます。

[Transit Connect] 画面と [SDDC グループ] 画面は、そのネットワークを経由するルートに関する情報を提供します。SDDC グループの作成や SDDC グループへの SDDC の追加については、「[VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理](#)」を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [Transit Connect] 画面を開くか、SDDC の [概要] 画面の [SDDC グループ] アイコンをクリックします。
[Transit Connect] 画面には、[学習されたルート]（グループ内の他の SDDC からこの SDDC によって学習されたルート）のリストと、[アドバタイズされたルート]（この SDDC がグループ内の他の SDDC にアドバタイズしたルート）のリストが表示されます。ダウンロード アイコンをクリックして、いずれかのリストを CSV 形式でダウンロードします。
集約された CIDR は、[アドバタイズされたルート] テーブルで [集約] とフラグ付けされます。除外された（アドバタイズされていない）セグメントの [ステータス] は [フィルタリング] になります。ルート集約とフィルタリングの詳細については、[アップリンクへのルートの集約とフィルタリング](#)を参照してください。

アップリンクに関する統計情報の表示と設定の管理

[グローバル構成] 画面には、SDDC ネットワーク アップリンクのトラフィック統計情報を表示できるコントロールと、その最大伝送可能単位 (MTU) およびユニキャスト リバース パス転送 (URPF) の設定を管理できるコントロールがあります。

デフォルト構成を次に示します。

- （接続先の VPC にトラフィックを転送する）[サービス] アップリンクの MTU は、8,900 バイトに設定されています。他のアップリンクの MTU は、1,500 バイトに設定されています。
- URPF は Strict モードで適用されます。パケットが SDDC アップリンクに転送されるのは、パケットを受信するインターフェイスによって、パケットの送信元への最適なりバース パスが提供される場合のみです。この条件を満たさないパケットはドロップされます。

これらの設定は、[グローバル構成] 画面で編集できます。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。

- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。 [NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [グローバル構成] 画面を開きます。

この画面には、各 SDDC アップリンクの [MTU] 設定と [URPF] 設定が表示されます。各アップリンクには [統計情報の表示] ボタンもあります。このボタンをクリックすると、アップリンクのトラフィック統計情報が表示されます。

- a MTU 設定と URPF 設定を管理します。


アップリンクの MTU 設定を変更するには、[編集] をクリックして新しい値を入力します。インターネット アップリンクには、[RFC3704](#) で定義されている URPF の Strict モードが必要です。別のアップリンクの URPF 設定を変更するには、[編集] をクリックして、次のいずれかの値を選択します。

[Strict]	URPF をこのアップリンクに Strict モードで適用します。
[なし]	このアップリンクに URPF を適用しません。

[保存] をクリックして変更内容を適用します。

- b [統計情報の表示] をクリックして、アップリンクのトラフィック統計情報を表示します。

アップリンクごとに収集される統計情報には、データ (KB 単位)、合計パケット数、ドロップされたパケッ

ト数などがあります。更新アイコン  をクリックすると、統計情報が更新されます。

- 5 (オプション) 出力方向フィルタリングを適用します。

CGW サブネットがアップリンクの BGP コンシューマにアダプタイズされる方法を制御するには、[出力方向フィルタリング] トグルを使用します。詳細については、[アップリンクへのルートの集約とフィルタリング](#) を参照してください。

VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加

すべての新しい VMware Cloud on AWS SDDC に、コンピューティング ゲートウェイ (CGW) という名前のデフォルトの Tier-1 ゲートウェイが含まれています。必要に応じて、追加のカスタム Tier-1 ゲートウェイを作成し、構成することができます。各 Tier-1 ゲートウェイは、SDDC Tier-0 ゲートウェイと任意の数のコンピューティング ネットワーク セグメントの間に配置されます。

追加の Tier-1 ゲートウェイを使用することにより、SDDC ネットワーク管理者は、VMware Cloud on AWS 組織内の特定のプロジェクト、テナント、またはその他の管理ユニットに固有の専用ワークロード ネットワーク キャパシティを確保することができます。

カスタム Tier-1 ゲートウェイを含む SDDC ネットワーク構成の詳細については、VMware Cloud Tech Zone Designlet の「[VMware Cloud on AWS Static Routing on Multiple CGWs \(T1s\)](#)」を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。 [NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [Tier-1 ゲートウェイ] - [Tier-1 ゲートウェイの追加] の順にクリックし、新しいゲートウェイに [名前] とオプションの [説明] を指定します。
- 5 ゲートウェイの [タイプ] を指定します。

タイプ	トラフィック パターン
[ルーティング]	セグメント トラフィックは、新しいゲートウェイを介してルーティングされます。
[分離]	セグメント トラフィックは、新しいゲートウェイを経由します。ローカル セグメントは相互に接続できます。セグメントはルーティング テーブルに追加されません。
[NAT 適用]	セグメント トラフィックの NAT ルールを作成するまで、セグメント トラフィックは新しいゲートウェイを経由できません (NAT ルールの作成または変更 を参照)。ローカル セグメントは相互に接続できます。セグメントはルーティング テーブルに追加されません。

- 6 (オプション) 新しいゲートウェイにタグを付けます。

NSX オブジェクトのタグgingについて詳しくは、『[NSX Data Center 管理ガイド](#)』の [オブジェクトへのタグの追加](#) を参照してください。

- 7 [保存] をクリックしてカスタム Tier-1 ゲートウェイを作成または構成します。
- 8 (オプション) カスタム Tier-1 ゲートウェイに DNS サービスを構成し、接続されたワークロードで使用する場合は、コンピューティング ゲートウェイのファイアウォール ルールを追加します。

カスタム Tier-1 ゲートウェイに接続されたワークロードでデフォルトのコンピューティング ゲートウェイの DNS フォワーダを使用する場合は、この手順をスキップできます。

コンピューティング ゲートウェイとは異なり、カスタム Tier-1 ゲートウェイには、接続されたワークロードからの DNS アクセスを許可するデフォルトのファイアウォール ルールがありません。このようなルールが必要になるのは、ゲートウェイの DNS サービスを作成し、ゲートウェイに接続されたワークロードでそのサービスをデフォルトのコンピューティング ゲートウェイの DNS フォワーダの代わりに使用する場合のみです。

名前	送信元	宛先	サービス	適用先	操作
ゲートウェイの DNS フォワーダ	[DNS サービス] タ ブに表示される [DNS サービスの IP アドレス]	任意	DNS-UDP	SDDC ネットワー クのデフォルト ル ートをアダプタイズ するインターフェイ ス。通常は次のいず れかです。 ■ インターネット インターフェイ ス ■ イントラネット インターフェイ ス ■ VPN トンネル インターフェイ ス	Allow

9 (オプション) ゲートウェイの DHCP サービスを構成します。

カスタム Tier-1 ゲートウェイのワークロードに対して DHCP アドレス割り当てを有効にする必要がない場合は、この手順をスキップできます。

[DHCP 構成の設定] をクリックして、[DHCP 構成] 画面を開きます。新しいゲートウェイのデフォルト DHCP 構成の [タイプ] は、[動的 IP アドレス割り当てなし] です。この構成内のゲートウェイは DHCP サービスを提供しません。DHCP サービスを提供するようにゲートウェイを設定する場合は、[DHCP サーバ] の [タイプ] を選択し、[DHCP サーバ プロファイル] を指定します。新しいプロファイルを作成することも、既存のプロファイルを使用することもできます。[セグメントの DHCP プロパティの構成](#)を参照してください。

10 (オプション) ゲートウェイのトラフィック QoS を構成します。

このカスタム Tier-1 ゲートウェイを通過するトラフィックの QoS 統計情報を取得する必要がない場合は、この手順をスキップできます。

[追加設定] をクリックし、トラフィックの制限について [入力方向 QoS プロファイル] と [出力方向 QoS プロファイル] を選択します。これらのプロファイルは、許可されたトラフィックの情報レートとバースト サイズの設定で使用されます。QoS プロファイルの作成の詳細については、[ゲートウェイ QoS プロファイルの追加](#)を参照してください。VMware Cloud on AWS は IPv6 をサポートしていないため、[ND プロファイル] および [DAD プロファイル] オプションは適用されません。

11 (オプション) ゲートウェイのスタティック ルートを構成します。

このオプションは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブでは使用できません。

任意のタイプのカスタム Tier-1 ゲートウェイにデフォルト以外のルートを作成できます。デフォルトのスタティック ルート (0.0.0.0/0) を構成できるのは、分離されたゲートウェイのみです。NSX Manager の [ネットワーク] タブで、[Tier-1 ゲートウェイ] をクリックします。Tier-1 ゲートウェイを作成または編集する場合は、[スタティック ルート] をクリックして、ゲートウェイのスタティック ルートとネクスト ホップを作成するか、変更します。

- 12 (オプション) 接続中の VPC または SDDC グループ内から新しいゲートウェイにアクセスできるようにする場合は、ルート集約を作成します。(分離されたゲートウェイには適用されません。)

ルーティングまたは NAT 処理されたカスタム Tier-1 ゲートウェイに接続されているネットワークは、集約プリフィックス リストにカスタム T1 ネットワークの NAT 処理またはルーティングされた IP アドレスを含むルート集約を定義し、その集約を [SERVICES] 接続エンドポイントに適用しない限り、接続中の VPC からアクセスできません。

注： NAT 処理された T1 のルート集約では、変換された (SNAT) IP アドレスを使用する必要があります。

また、この SDDC が SDDC グループのメンバーである場合は、同様のルート集約を定義し、その集約を [INTRANET] 接続エンドポイントに適用する必要があります。ルート集約には管理対象プリフィックス モードが必要であり、接続中の VPC のデフォルト構成では使用できません。[アップリンクへのルートの集約とフィルタリング](#)を参照してください。

Tier-1 ゲートウェイへの VPN の接続

VPN を Tier-1 ゲートウェイに接続する場合は、ゲートウェイのインターネット インターフェイスを介した IPsec VPN トラフィックを有効にするために、ゲートウェイに対する IPsec サービスと適切な NAT ルールを作成する必要があります。

SDDC バージョン 1.18 以降では、カスタム Tier-1 ゲートウェイを終端とする VPN を作成することもできます。この構成は、特定のテナントまたはワークグループへの専用 VPN アクセスを提供する必要がある場合に特に便利です。

詳細については、VMware Tech Zone の記事 [Understanding VPN to Customer Created NSX T1s in VMC on AWS](#) を参照してください。

前提条件

NAT が設定された、またはルーティングされた Tier-1 ゲートウェイを作成します。[VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加](#)を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。
- 4 (オプション) VPN エンドポイントのパブリック IP アドレスを要求します。

インターネットからこの VPN にアクセスするという一般的な場合では、ローカル エンドポイントはパブリック IP アドレスである必要があります。[パブリック IP アドレスの要求またはリリース](#)を参照してください。この例では、そのアドレスとして 93.184.216.34 を使用します。DX または VMware Transit Connect 経由でこの VPN にアクセスする場合は、SDDC コンピューティング ネットワークで使用可能な任意の IP アドレスを使用できます。

注： 管理 CIDR のサブネットをローカル エンドポイントとして使用することはできません。

5 Tier-1 ゲートウェイに VPN サービスを追加します。

[ネットワーク] - [VPN] の順にクリックします。[Tier-1] タブを開き、[VPN サービス] - [サービスの追加] - [IPsec] の順にクリックします。IPsec サービスに [名前] を指定し、ドロップダウン メニューから [Tier-1 ゲートウェイ] を選択します。[保存] をクリックしてサービスを作成します。

6 ローカル エンドポイントを作成します。

[ローカル エンドポイント] タブを開き、[ローカル エンドポイントの追加] をクリックします。新しいローカル エンドポイントに [名前] を指定し、オプションで [説明] を指定します。[VPN サービス] には、手順 5 で作成した IPsec サービスの名前を使用します。[IP アドレス] には、[手順 4](#) で要求したパブリック IP アドレス、または SDDC コンピューティング ネットワークで使用可能な任意のアドレスを使用します。[保存] をクリックしてローカル エンドポイントを作成します。

7 VPN を構成します。

[IPsec セッション] タブを開き、[IPsec セッションの追加] ドロップダウンで [ルート ベース] または [ポリシー ベース] を選択します。

- a [VPN サービス] には、手順 5 で作成した IPsec サービスの名前を使用します。ローカル エンドポイント には、手順 6 で作成したエンドポイントを使用します。
- b [リモート IP アドレス] には、オンプレミスの VPN エンドポイントのアドレスを入力します。
- c [事前共有キー] の文字列を入力します。

キーの最大長は 128 文字です。このキーは、VPN トンネルの両側で同一である必要があります。

8 [リモート ID] を指定します。

[リモート IP アドレス] を IKE ネゴシエーションのリモート ID として使用する場合は、空のままにします。オンプレミス VPN ゲートウェイが NAT デバイスの背後にある場合や、そのローカル ID に別の IP アドレスを使用する場合は、ここにその IP アドレスを入力する必要があります。

9 [トンネルの詳細パラメータ] を構成します。

パラメータ	値
[IKE プロファイル] - [IKE 暗号化]	オンプレミス VPN ゲートウェイでサポートされているフェーズ 1 (IKE) 暗号を選択します。
[IKE プロファイル] - [IKE ダイジェスト アルゴリズム]	<p>オンプレミス VPN ゲートウェイでサポートされているフェーズ 1 ダイジェスト アルゴリズムを選択します。ベスト プラクティスは、[IKE ダイジェスト アルゴリズム] と [トンネル ダイジェスト アルゴリズム] の両方に同じアルゴリズムを使用することです。</p> <p>注： [IKE 暗号化] に GCM ベースの暗号を指定する場合は、[IKE ダイジェスト アルゴリズム] を [なし] に設定します。ダイジェスト機能は GCM 暗号に不可欠です。GCM ベースの暗号を使用する場合は IKE V2 を使用する必要があります。</p>

パラメータ	値
[IKE プロファイル] - [IKE バージョン]	<ul style="list-style-type: none"> ■ IKEv1 プロトコルを開始して受け入れる場合は、[IKE V1] を指定します。 ■ IKEv2 プロトコルを開始して受け入れる場合は、[IKE V2] を指定します。GCM ベースの [IKE ダイジェスト アルゴリズム] を指定した場合は、IKEv2 を使用する必要があります。 ■ IKEv1 または IKEv2 を受け入れてから IKEv2 を開始する場合は、[IKE FLEX] を指定します。IKEv2 の開始に失敗した場合、IKE FLEX は IKEv1 にフォールバックしません。
[IKE プロファイル] - [Diffie Hellman]	オンプレミス VPN ゲートウェイでサポートされている Diffie-Hellman グループを選択します。この値は、VPN トンネルの両側で同一にする必要があります。グループ番号が大きいほど、保護は強化されます。グループ 14 以上を選択することをお勧めします。
[IPSec プロファイル] - [トンネル暗号化]	オンプレミス VPN ゲートウェイでサポートされているフェーズ 2 Security Association (SA) 暗号を選択します。
[IPSec プロファイル][トンネル ダイジェスト アルゴリズム]	<p>オンプレミス VPN ゲートウェイでサポートされているフェーズ 2 ダイジェスト アルゴリズムを選択します。</p> <p>注： [トンネルの暗号化] に GCM ベースの暗号を指定する場合は、[トンネル ダイジェスト アルゴリズム] を [なし] に設定します。ダイジェスト機能は GCM 暗号に不可欠です。</p>
[IPSec プロファイル] - [Perfect Forward Secrecy]	オンプレミス VPN ゲートウェイの設定に合わせて有効または無効にします。Perfect Forward Secrecy を有効にすると、プライベート キーが盗み取られたとしても、記録された（過去の）セッションが復号されることを回避できます。
[IPSec プロファイル] - [Diffie Hellman]	オンプレミス VPN ゲートウェイでサポートされている Diffie-Hellman グループを選択します。この値は、VPN トンネルの両側で同一にする必要があります。グループ番号が大きいほど、保護は強化されます。グループ 14 以上を選択することをお勧めします。
[DPD プロファイル] - [DPD ブローブ モード]	<p>[定期]または[オンデマンド]のいずれか。</p> <p>定期 DPD ブローブ モードの場合、指定した DPD ブローブ間隔が経過するたびに DPD ブローブが送信されます。</p> <p>オンデマンド DPD ブローブ モードの場合、アイドル期間の経過後にピア サイトから IPsec パケットが受信されないと、DPD ブローブが送信されます。使用されるアイドル期間は [DPD ブローブ間隔] の値によって決まります。</p>
[DPD プロファイル] - [再試行回数]	許可される再試行回数の整数。1~100 の範囲の値が有効です。デフォルトの再試行回数は 10 です。

パラメータ	値
[DPD プロファイル] - [DPD ブローブ間隔]	<p>DPD ブローブの送信の間に NSX IKE デーモンが待機する秒数。</p> <p>定期 DPD ブローブ モードの場合、有効な値は 3~360 秒の間です。デフォルト値は 60 秒です。</p> <p>オンデマンド ブローブ モードの場合、有効な値は 1~10 秒の間です。デフォルト値は 3 秒です。</p> <p>定期 DPD ブローブ モードを設定した場合、IKE デーモンは DPD ブローブを定期的に送信します。ピア サイトが 0.5 秒以内に応答すると、構成した DPD ブローブ間隔の経過後に次の DPD ブローブが送信されます。ピア サイトが応答しない場合は、0.5 秒待機した後に DPD ブローブが再送信されます。リモート ピア サイトが応答しない場合、応答が受信されるか再試行回数に到達するまで、IKE デーモンは DPD ブローブの再送信を繰り返します。ピア サイトの非活動が宣言されるまで、IKE デーモンは [再試行回数] プロパティに指定された最大回数に達するまで、DPD ブローブを再送信します。ピア サイトが非活動と宣言されると、NSX は、非活動ピアのリンクで Security Association (SA) を解除します。</p> <p>オンデマンド DPD モードを設定すると、構成した DPD ブローブ間隔の経過後、ピア サイトから IPsec トラフィックが受信されない場合にのみ、DPD ブローブが送信されます。</p>
[DPD プロファイル] - [管理ステータス]	<p>DPD プロファイルを有効または無効にするには、[管理ステータス] トグルをクリックします。デフォルトでは、この値は [有効] に設定されます。DPD プロファイルを有効にすると、DPD プロファイルを使用する IPsec VPN サービスのすべての IPsec セッションに、その DPD プロファイルが使用されます。</p>
[TCP MSS クランプ]	<p>[TCP MSS クランプ] を使用して IPsec 接続時の TCP セッションの最大セグメント サイズ (MSS) ペイロードを削減するには、このオプションを [有効] に切り替えて、[TCP MSS の方向] を選択し、必要に応じて [TCP MSS 値] を選択します。『NSX Data Center 管理ガイド』の TCP MSS クランプの理解を参照してください。</p>

10 (オプション) VPN にタグを付けます。

NSX オブジェクトのタグgingについて詳しくは、『NSX Data Center 管理ガイド』の[オブジェクトへのタグの追加](#)を参照してください。

11 [保存] をクリックして VPN を作成します。

12 CGW のインターネット インターフェイスを経由する IPsec VPN トラフィックを許可するコンピューティング ゲートウェイ ファイアウォール ルールを追加します。

[ゲートウェイ ファイアウォール] タブを開き、[コンピューティング ゲートウェイ] をクリックします。このルールは機能しますが、許容度が一般的に本番環境に期待されるよりも高くなっています。信頼できる、または制御している CIDR ブロックのみに [送信元] を制限することを検討してください。この例では、[手順 4](#) で取得したパブリック IP アドレス (93.184.216.34) を [宛先] アドレスとして使用しています。

名前	送信元	宛先	サービス	適用先	操作
VPN アクセス	任意	93.184.216.34	[IKE (NAT トラバース)], [IKE (鍵交換)], [IPSec VPN ESP] を含める必要があります	[インターネットインターフェイス]	Allow

13 VPN のパブリック IP アドレスに外部からアクセスできるように、NAT ルールを作成します。

[ネットワーク] - [NAT] - [インターネット] の順に移動します。[NAT ルールの追加] をクリックし、次のような NAT ルールを作成します。

名前	パブリック IP アドレス	サービス	パブリック ポート	内部 IP アドレス	ファイアウォール
VPN アクセス	93.184.216.34	すべてのトラフィック	任意	93.184.216.34	外部アドレスと一致

このルールでは、[パブリック IP アドレス] と [内部 IP アドレス] に対して同じアドレス（この例では、[手順 4](#) で要求されたパブリック IP アドレス）を使用する必要があります。ファイアウォールは、受信パケットを調べるときに外部アドレスを照合する必要があります。

SDDC ネットワークでの IPv6 の有効化と使用

SDDC バージョン 1.22 以降では、新しい SDDC でデュアル スタック (IPv4 および IPv6) ネットワークを有効にすることができます。

デュアル スタック SDDC ネットワークでは、カスタム T1 ゲートウェイに接続されたセグメントのワークロード通信で IPv6 がサポートされます。IPv6 は、AWS Direct Connect と VMware Transit Connect を介した SDDC 通信でもサポートされます。IPv6 はインターネット接続ではまだサポートされていません。また、SDDC 管理ネットワークや接続中の VPC でも使用することはできません。詳細および設計ガイドラインについては、VMware Cloud Tech Zone Designlet の「[Understanding IPv6 in VMware Cloud on AWS](#)」を参照してください。

サブネットの選択と SDDC の有効化

SDDC が作成されたら、SDDC の [アクション] メニューから [IPv6 の有効化] を選択し、IPv6 に対して SDDC を有効にすることができます。SDDC が IPv6 に対して有効になっている場合、[グローバル構成] 画面には [IPv4 と IPv6] の [L3 転送モード] が表示されます。

注： SDDC の IPv6 の有効化を元に戻すことはできません。必要に応じて、[L3 転送モード] を [IPv4] に変更できますが、基盤となる IPv6 ネットワークのサポートは SDDC の有効期間中も維持されます。

セグメント構成

IPv6 は、カスタム T1 ゲートウェイに接続されたセグメントのワークロード通信でのみサポートされます。デフォルトのコンピューティング ゲートウェイに接続されているセグメントで IPv6 を有効にすることはできません。セグメントは、デュアルスタックまたは IPv6 のみにすることができます。詳細については、VMware Tech Zone の記事 [Understanding Segments in VMC on AWS](#) を参照してください。

デュアル スタック セグメントまたは IPv6 のみのセグメントを作成する場合は、「[ネットワーク セグメントの作成または変更](#)」で説明されているいくつかの構成パラメータに注意してください。

接続されたゲートウェイ

カスタム T1 ゲートウェイである必要があります。

セグメント プロファイル

IP アドレス検出を vmc-adv-ipdiscovery-profile に設定する必要があります。これにより、IPv6 に対してネイバー検出 (ND) スヌーピング、DHCP スヌーピング、および VMware Tools が有効になります。

IPv6 とファイアウォール ルール

ゲートウェイ ファイアウォールおよび分散ファイアウォール インベントリ グループには、IPv6 アドレスを含めることができます。SDDC で NSX Advanced Firewall が有効になっている場合は、レイヤー 7 APP-ID でも IPv6 がサポートされます。IPv6 アドレスは、システム定義のサービスとカスタム サービスでサポートされます。一部のサービスには IPv6 固有のバリエーション (ICMPv6 など) があり、ファイアウォール ルールを記述する際にそれらを考慮する必要があります。

AWS Direct Connect および VMware Managed Transit Gateway 経由の North-South トラフィック

SDDC との間の IPv6 トラフィックは、AWS Direct Connect および VMware Transit Connect 経由でサポートされます。IPv6 ネットワークを外部エンドポイントにアダプタイズする場合は、[アップリンクへのルートの集約とフィルタリング](#)の説明に従って、アダプタイズされたルートの IPv6 ルート集約を構成する必要があります。集約プリフィックス リスト内のプリフィックスはすべて同じアドレス ファミリーに含まれている必要があります。

IPv6 over IPv4 VPN

「[ルートベースの VPN の作成](#)」に記載されているワークフローを使用して、IPv4 と IPv6 の両方をサポートする VPN を構成できます。[BGP ローカル IP アドレス/プリフィックス長] を IPv6 サブネット (サイズに適したオプションは /126 または /127) として、[BGP リモート IP アドレス] を同じサブネット上の IPv6 アドレスとして構成します。たとえば、[BGP ローカル IP アドレス/プリフィックス長] に cccc:dddd:100/126 を指定した場合、[BGP リモート IP アドレス] には cccc:dddd::100/101 を使用します。この VPN のオンプレミス側を構成するときは、[BGP リモート IP アドレス] に指定した IP アドレスを、そのローカル BGP IP アドレスまたは VTI アドレスとして 使用します。

詳細については、VMware Cloud Tech Zone Designlet の「[Understanding IPv6 in VMware Cloud on AWS](#)」を参照してください。

DNS サービス

SDDC バージョン 1.22 の DNS サービスでは IPv6 接続がサポートされていません。IPv6 のみのワークロードでは、SDDC ネットワーク内または IPv6 対応の接続オプションのいずれかを介して到達できる、ユーザー管理の IPv6 でアクセス可能な DNS サーバを使用する必要があります。SDDC IPv4 DNS サービスは、DNS 要求が IPv4 経由で行われる限り、IPv6 アドレスを解決できます。

トラフィック グループを使用したマルチエッジ SDDC の構成

デフォルトの構成では、Software-Defined Data Center (SDDC) ネットワークにシングル エッジ (TO) ルーターがあり、このルーターを通じて、すべての North-South トラフィック フローが流れます。このエッジはデフォルトのトラフィック グループをサポートしますが、これは構成できません。SDDC グループ メンバー、SDDC グループに接続された Direct Connect Gateway、VMware HCX Service Mesh、または接続中の VPC にルーティングされるこのトラフィックのサブセット用にさらにバンド幅が必要な場合は、トラフィック グループを作成して SDDC を再構成し、各グループに追加の TO ルーターが作成されるマルチエッジにします。

トラフィック グループは、関連付けマップを使用して、CIDR ブロックのプリフィックス リストを、SDDC 内のデフォルト以外のトラフィック グループをサポートする TO ゲートウェイの 1 つに関連付けます。プリフィックス リストはゲートウェイから独立し、送信元 IP アドレスで構成されます。これらのアドレスからのトラフィックは、関連付けられたトラフィック グループをサポートする TO Edge にルーティングされます。このプリフィックス リストは、いつでも作成および更新できますが、関連付けマップに含まれている場合は、削除できません。プリフィックス リストをトラフィック グループに関連付けることで、リスト内の CIDR ブロックからグループ用に作成された TO ルーターを介してすべてのトラフィックをルーティングします。

注： VPN トラフィックとプライベート VIF への DX トラフィックは、デフォルトの TO を介して通過する必要があります。デフォルト以外のトラフィック グループにルーティングすることはできません。また、NAT ルールは常にデフォルトの TO ルーターで実行されるので、追加の TO ルーターは SNAT ルールまたは DNAT ルールの影響を受けるトラフィックを処理できません。これには、SDDC のネイティブ インターネット接続との間のトラフィックが含まれます。また、これには Amazon S3 サービスへのトラフィックも含まれ、このサービスは NAT ルールを使用し、デフォルトの TO を経由する必要があります。プリフィックス リストを作成するときは、この制限に留意してください。

前提条件

- トラフィック グループを作成するには、事前に VMware Transit Connect™ を使用して、SDDC を VMware Managed Transit Gateway (VTGW) に接続しておく必要があります。「[VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理](#)」を参照してください。
- トラフィック グループの作成には、大規模な管理アプライアンスと 4 台以上のホストがある SDDC が必要です。SDDC の管理アプライアンスのサイズを中規模から大規模に変更する方法については、『VMware Cloud on AWS 運用ガイド』の「[SDDC 管理アプライアンスのアップサイジング](#)」を参照してください。SDDC に対するホストの追加方法については、[ホストの追加](#)を参照してください。
- 各トラフィック グループは、デフォルトの 2 台の Edge 仮想マシンに加えて、2 台の Edge 仮想マシンを展開します。Edge 仮想マシンは同じホストを共有できず、パフォーマンス要件を満たすことができないため、トラフィック グループごとに 2 台以上のホストと、管理クラスター (Cluster-1) 内のデフォルトのトラフィック グループ用にさらに 2 台のホストが必要になります。SDDC がサポートできるトラフィック グループの数は、管理ホストの数によって異なり、次のような式で表すことができます。

$$TG = (\text{mgmt-hosts} - 2) \mid \text{MAX}$$

ここで *TG* は、SDDC がサポートできるトラフィック グループの最大数、*mgmt-hosts* は、SDDC 管理クラス内のホストの数を表します。*TG* の計算値に関係なく、SDDC トラフィック グループのサポートの上限は、「[VMware Configuration Maximums](#)」(MAX) に示されている SDDC あたりのマルチエッジ SDDC トラフィック グループの最大数に設定されています。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 トラフィック グループを作成します。[トラフィック グループ] 画面の [トラフィック グループ] タブで [トラフィック グループの追加] をクリックして、新しいトラフィック グループの [名前] を入力します。次に [保存] をクリックして、トラフィック グループと、そのトラフィック グループ用の追加の TO ルーターを作成します。


新しい TO エッジの作成中、トラフィック グループの [ステータス] は [処理中] に遷移します。このプロセスの完了には、最大 30 分ほどかかる場合があります。プロセスが完了すると、トラフィック グループの [ステータス] は [成功] に遷移し、その関連付けマップを作成できるようになります。

- 5 プリフィックス リストを作成します。


マルチエッジ SDDC では、トラフィック グループ内で送信元ベースのルーティングが使用されます。このため、プリフィックス リストには、宛先アドレスではなく、送信元アドレスを含める必要があります。


- a [トラフィック グループ] 画面の [IP プリフィックス リスト] タブで [IP プリフィックス リストの追加] をクリックして、新しいプリフィックス リストの [名前] と、必要に応じて [説明] を入力します。
- b [設定] をクリックして [プリフィックスの設定] ウィンドウを表示した後、[プリフィックスの追加] をクリックして、SDDC ネットワーク セグメントの CIDR ブロックを入力します。このセグメントには、トラフィック グループに含め、追加のエッジを介してトラフィックがルーティングされるようにする、ワークロード仮想マシンの送信元アドレスが含まれます。

重要： ここでは、SDDC 管理 CIDR ブロックや、VPN のローカル IP アドレスを提供するセグメントの CIDR ブロックを使用することはできません。これらの CIDR のいずれかをプリフィックス リストに追加すると、関連付けマップでリストを使用できなくなります。



[追加] をクリックして、指定されたプリフィックスをリストに追加します。プリフィックスを追加するか、またはリストにすでにあるプリフィックスを編集するには、 をクリックして、プリフィックス エディタを開きます。

- c [適用] をクリックして、変更内容をプリフィックス リストに適用します。
- d プリフィックスの追加または編集が完了したら、[保存] をクリックして保存するか、またはプリフィックス リストを作成します。

- 6 プリフィックス リストをゲートウェイに関連付けます。[トラフィック グループ] 画面の [トラフィック グループ] タブで、使用するトラフィック グループを探します。次に、 をクリックして、[編集] を選択します。

[関連付けマップ] 領域にあるプラス アイコン  をクリックして、マッピングの [名前] を入力します。次に、[プリフィックス] ドロップダウンから既存のプリフィックス リストを選択します。[ゲートウェイ] ドロップダウンからゲートウェイを選択し、[保存] をクリックして関連付けマップを作成します。

- 7 (オプション) トラフィック グループを削除するには、最初にその関連付けマップを削除する必要があります。

- a [トラフィック グループ] 画面で対象のトラフィック グループを探します。 ボタンをクリックして、[編集] を選択します。
- b [関連付けマップ] の [ステータス] ラベルの右側にあるマイナス アイコン  をクリックして、削除するマップを選択します。次に、[保存] をクリックして、マップを削除します。
- c [編集の終了] をクリックして、[トラフィック グループ] 画面のトラフィック グループに戻ります。そのトラフィック グループの省略記号ボタンをクリックして、[削除] を選択します。

トラフィック グループを削除するには、最大 30 分ほどかかる場合があります。トラフィック グループを削除すると、トラフィック グループをサポートするために作成された TO ルーターが削除されます。HCX が使用されている場合は、表示はできて変更はできない独自の関連付けマップが作成されます。HCX によって作成された関連付けマップを削除するには、HCX をアンインストールする必要があります。『VMware HCX ユーザーガイド』の [VMware HCX のアンインストール](#) を参照してください。

例：トラフィック グループ追加後のルート テーブルの変更

この例では、トラフィック グループを作成し、それを 2 つのホスト ルート (/32) のプリフィックス リストに関連付けた場合の影響を簡単に示します。

初期設定

最初のトラフィック グループを追加することによって追加の TO ルーターを作成する前の時点で、デフォルトのトラフィック グループとコンピューティング ゲートウェイ (CGW) のルート テーブル エントリに次の値を仮定します。

表 3-21. デフォルト ルート

サブネット	ネクスト ホップ
0.0.0.0/0	インターネット ゲートウェイ
192.168.150.51/24	CGW
192.168.151.0/24	CGW
VTGW、DXGW サブネット	VTGW、DXGW 接続
管理 CIDR	MGW

表 3-22. デフォルトのトラフィック グループを含む CGW ルート

サブネット	ネクスト ホップ
0.0.0.0/0	デフォルトの TO
192.168.150.0/24	デフォルトの TO
192.168.151.0/24	デフォルトの TO

マルチエッジ構成

最初のトラフィック グループが作成されると、デフォルトの TO に新しいルートが追加されます。トラフィック グループに関連付けられたプリフィックス リストに次のエントリがあると仮定します。

```
192.168.150.100/32
192.168.151.51/32
```

デフォルトの TO、新しい TO、および CGW のルート テーブルは、次のようになります。

表 3-23. トラフィック グループを追加した後のデフォルトの TO ルート

サブネット	ネクスト ホップ
0.0.0.0/0	インターネット ゲートウェイ
192.168.150.0/24	CGW
192.168.150.100/32	新しい TO
192.168.151.0/24	CGW
192.168.151.51/32	新しい TO
VTGW、DXGW サブネット	VTGW、DXGW 接続
管理 CIDR	MGW

新しいルート（例の表では 192.168.150.100/32 および 192.168.151.51/32）は、新しい TO をネクスト ホップとして使用し、新しい TO は最長プリフィックス一致を使用して CGW にトラフィックをルーティングします。

表 3-24. 新しいトラフィック グループのルート

サブネット	ネクスト ホップ
0.0.0.0/0	デフォルトの TO
192.168.150.100/32	CGW
192.168.151.51/32	CGW
VTGW、DXGW サブネット	VTGW、DXGW 接続
管理 CIDR	MGW

CGW ルート テーブルが、新しい TO ルーターを新しいルートのネクスト ホップとして指定することによってトラフィック グループを作成するように更新されます。

表 3-25. 追加のトラフィック グループを含む CGW ルート

サブネット	ネクスト ホップ
0.0.0.0/0	デフォルトの TO
192.168.150.0/24	デフォルトの TO
192.168.150.100/32	新しい TO
192.168.151.0/24	デフォルトの TO
192.168.151.51/32	新しい TO

接続中の Amazon VPC の AWS 管理対象プリフィックス リスト モードの有効化

AWS 管理対象プリフィックス リスト モードを使用すると、マルチエッジ SDDC でルート テーブルの管理を簡素化し、任意の SDDC でカスタムのルート テーブルとルート集約のサポートを使用できるようになります。

VMware Cloud on AWS で接続中の VPC の AWS 管理対象プリフィックス リストを有効にすると、デフォルトのコンピューティング ゲートウェイ プリフィックスとユーザー自身が作成した他のプリフィックス リストが集約されて、ポピュレートされた AWS プリフィックス リストが作成されます。このリストは、[接続中の Amazon VPC] 画面に表示される [AWS アカウント ID] と共有されます。この AWS リソース共有を受け入れると、接続中の VPC ルート テーブルにプリフィックス リストを追加できるようになります。

VMware Cloud on AWS は、管理対象プリフィックス リストを使用して、接続中の VPC のメイン ルート テーブルを更新します。プリフィックス リストがルート テーブルに追加された場合は、ルート テーブル内の該当エントリが宛先 ENI を参照し、ENI に含まれる個々の CIDR はプリフィックス リストによって置き換えられます。プリフィックス リストは管理対象オブジェクトであるため、新しいセグメントまたは集約が構成されるたびに自動的に更新されます。また、アクティブ エッジ インスタンスのホストが変更されるたびに、そのプリフィックス リストのルート テーブル エントリが正しい ENI を参照するように更新されます。ユーザーが作成したカスタム ルート テーブルに接続中の VPC プリフィックス リストを追加する作業は、ユーザー自身が行います。管理対象プリフィックス リストの詳細については、VMware Cloud Tech Zone の記事 [Understanding Managed Prefix List Mode for Connected VPC in VMC on AWS](#) を参照してください。

注： マルチエッジ SDDC では、接続中の VPC の管理対象プリフィックス リストにデフォルトのトラフィック グループのプリフィックス リストからのエントリがポピュレートされます。NSX エッジを追加するたびにプリフィックス リストを手動で更新する必要があります。

接続中の VPC のメイン ルート テーブルを含むルーティング テーブルからプリフィックス リストを削除し、後でそれをリストアする場合は、その処理を手動で行う必要があります。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。

2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。

3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。 [NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

4 [接続中の VPC] をクリックして、[接続中の Amazon VPC] 画面を開きます。

この画面の [トラフィック グループ] テーブルに、デフォルトのトラフィック グループとアクティブな AWS ネットワーク インターフェイス ID が表示されます。

5 [AWS 管理対象プリフィックス リスト モード] を有効にします。

a [AWS 管理対象プリフィックス リスト モード] を [有効] に切り替えます。

メッセージを確認し、[有効化] または [キャンセル] をクリックします。[有効化] をクリックして [AWS 管理対象プリフィックス リスト モード] を [アクション保留中] に移行すると、管理対象プリフィックス リストを含む AWS リソース共有を受け入れるように求められます。

b リソース共有を受け入れる権限を持つ ID を使用して AWS コンソールにログインし、[Resource Access Manager] - [Shared with me] の順にクリックします。

リソースの [Name] の形式は `managed-prefix-list-resource-share-vpc-ID` で、[Status] は [Pending] です。リソースの [Name] をクリックしてリソースの [Summary] カードを開き、[Accept resource share] をクリックして受け入れを確定します。

c VMware Cloud コンソールで、[接続中の Amazon VPC] タブに戻り、[AWS 管理プリフィックス リスト モード] が [保留] から [有効] に変更されるまで待機します。

AWS リソースの関連付けには、最大で 10 分かかることがあります。

接続中の VPC のメイン ルート テーブルでは、管理ゲートウェイとコンピューティング ゲートウェイへの個々のルートがプリフィックス リストに置き換えられます。[トラフィック グループ] テーブルに、デフォルト トラフィック グループの [プリフィックス リスト ID]、[プリフィックス リスト名]、[プログラムされたルート テーブル] が追加されました。[プリフィックス リスト名] をクリックしてリストを表示します。

次のステップ

接続中の VPC のカスタム ルート テーブルにプリフィックス リストを追加します。これにより、そのカスタム ルート テーブルに関連付けられているサブネット内の AWS リソースが SDDC と通信できるようになります。

VMware Cloud on AWS は、追加のルート テーブルを自動的に検出し、正しい ENI を参照するようにプリフィックス リストを更新します。最初の更新後、プリフィックス リストで使用されている ENI と同じ ENI を参照するようにルート テーブルを手動で構成することができます。手動で更新しない場合は、新しいルート テーブルにプリフィックス リストが追加されたことが VMware Cloud on AWS によって検出されるたびに、この更新と以降の更新が自動的に実行されます。

注： 各プリフィックス リストは、ルート テーブルへの追加の際に 1 つの [ルート] としてカウントされますが、多数のエントリがリストに含まれている場合があります。各エントリはルート テーブルの割り当てに含まれます。

[AWS VPC ルート テーブルの割り当て](#)の説明を参照して、すべてのルートをプリフィックス リストに含めるための十分なキャパシティがルート テーブルにあることを確認してください。[アップリンクへのルートの集約とフィルタリング](#)を使用すると、Direct Connect、VMware Transit Connect、接続中の VPC などの SDDC ネットワーク アップリンクにアダプタイズされる一連のルートを制御できます。集約は、VPC ルート テーブル内のエントリ数を削減する場合に役立ちます。出力方向フィルタリングは、接続中の Amazon VPC（サービス アップリンク）およびその他のアップリンクにアダプタイズされる一連のルートを制限する場合に役立ちます。

VMware Cloud on AWS では、カスタム ルート テーブルでプリフィックス リストを検出すると（最大 10 分かかる場合があります）、アクティブな ENI を参照するようにそのエントリを更新し、更新したルート テーブルを [トラフィック グループ] テーブルに追加します。そのルート テーブルに対する以降の更新は、アクティブな ENI が変更されるとすぐに実行されます。

アップリンクへのルートの集約とフィルタリング

ルート集約と出力方向フィルタリングを使用して、Direct Connect、VMware Transit Connect、接続中の VPC などの SDDC ネットワーク アップリンクにアダプタイズされる一連のルートを制御します。これは、VPC ルート テーブル内のエントリ数を削減する場合や、アップリンクにアダプタイズされる一連のルートを制限する場合に必要になります。

バージョン 1.18 以降の SDDC では、NSX Manager を使用して、イントラネット アップリンクとサービス アップリンクへのルートを集約できます。SDDC バージョン 1.20 以降では、NSX Manager を使用して、これらのアップリンクにアダプタイズされる一連のルートをフィルタリングすることもできます。ルート集約とフィルタリングは、レガシー VMware Cloud コンソールの [ネットワークとセキュリティ] タブでは公開されません。

デフォルトの構成では、SDDC コンピューティング ネットワーク内のすべてのセグメントが、接続中の Amazon VPC と外部接続（AWS Direct Connect や VMware Transit Connect など）にアダプタイズされます。この方法でアダプタイズされる CIDR のリストを管理するには、これらのルートを集約し、必要に応じてフィルタリングします。フィルタリングされたルートは、選択したアップリンクにアダプタイズされません。管理サブネットは常にアダプタイズされます。集約とフィルタリングの両方が適用されると、通常は除外される CIDR が集約されたサブネットに含まれている場合でも、そのサブネットがアダプタイズされます。接続中の VPC にアダプタイズされている現在の一連のルートを表示またはダウンロードするには、NSX Manager の [ネットワーク] タブを開き、[接続中の VPC] - [アダプタイズ済み] の順にクリックします。[Transit Connect] にアダプタイズされている現在の一連のルートを表示またはダウンロードするには、[VMware Transit Connect を通じて学習およびアダプタイズされたルートの表示](#)を参照してください。

IPv6 を使用して SDDC グループのメンバー間で通信する場合のルート集約の要件の詳細については、[SDDC ネットワークでの IPv6 の有効化と使用](#)を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックします。
- 4 CGW サブネットの CIDR を集約します。
 - a NSX Manager の [ネットワーク] タブで、[グローバル構成] - [ルート集約] の順にクリックします。
 - b 集約する CIDR ブロックのプリフィックス リストを作成します。

[集約プリフィックス リスト] の下の [集約プリフィックス リストの追加] をクリックし、リストに [名前] を指定し、[設定] をクリックして [プリフィックスの設定] エディタを開きます。必要に応じてプリフィックスの CIDR を追加します。より広い範囲に収まるサブネットが含まれるすべての CIDR が正規化されます。たとえば、デフォルトの CGW セグメントに 192.168.1.0/24、192.168.5.0/24、および 192.168.22.0/24 が含まれている場合、集約は 192.168.0.0/16 としてアドバタイズされますが、個々のセグメントはアドバタイズされません。

- c 新しいプリフィックス リストを含むルート構成を追加します。

[ルート構成] で [ルート構成の追加] をクリックし、新しい構成の [名前] を指定します。作成した [集約プリフィックス リスト] を選択し、[接続エンドポイント] を選択します。

- このルーティング構成を Direct Connect および VMware Transit Connect に適用するには、[イントラネット] を選択します。
- このルーティング構成を接続中の VPC に適用するには、[サービス] を選択します。AWS 管理対象プリフィックス リストが接続中の VPC へのルートの集約に与える影響については、[接続中の Amazon VPC の AWS 管理対象プリフィックス リスト モードの有効化](#)を参照してください。

[インターネット] エンドポイントにルート構成を追加することはできません。

- d [保存] をクリックして新しい構成を作成します。

[集約] ルートは、[Transit Connect] 画面の [アドバタイズされたルート] テーブルおよび [接続中の Amazon VPC] タブの [アドバタイズ済み] 画面でフラグが付けられます。

- 5 (オプション) アップリンクに出力方向フィルタリングを適用します。

アップリンクに対して出力方向フィルタリングが有効になっている場合、指定されたアップリンクの BGP コンシューマにアドバタイズされるのは、集約された CIDR ブロックと重複しない CIDR ブロックのみです。構成済みの集約のサブネットであるデフォルトの CGW セグメントはアドバタイズされません。NSX Manager の [ネットワーク] タブでは、[イントラネット] アップリンクと [サービス] アップリンクに対する出力方向フィルタリングの適用を制御できます。必要に応じて、[グローバル構成] - [アップリンク] の順にクリックして、[出力方向フィルタリング] を切り替えます。

NSX Manager の [ネットワーク] タブで、[グローバル構成] - [ルート フィルタリング] の順にクリックします。アップリンクの [出力方向フィルタリング] を切り替えて、CGW サブネットがアップリンクの BGP コンシューマにアドバタイズされないようにします。

- このルーティング構成を Direct Connect および VMware Transit Connect に適用するには、[イントラネット] を選択します。

- このルーティング構成を接続中の VPC に適用するには、[サービス] を選択します。

注： サービス アップリンクにルート フィルタリングを適用する前に、[接続中の Amazon VPC の AWS 管理対象プリフィックス リスト モードの有効化](#)を行う必要があります。

アップリンクの [出力方向フィルタリング] をオフにすると、すべての CGW サブネットがアダプタイズされます。[インターネット] アップリンクに出力方向フィルタリングを適用することはできません。

デフォルト以外の CGW セグメントは選択したアップリンクにアダプタイズされませんが、集約内にある場合は到達可能なままです。[接続中の Amazon VPC] タブの [アダプタイズ済み] 画面では、除外された（アダプタイズされていない）セグメントの [ステータス] が [フィルタリング] になります。同じ画面で、除外されていない（アダプタイズされた）セグメントの [ステータス] は [成功] になります。集約を含むフィルタリングされたルートは、この画面と [Transit Connect] 画面で [集約] とフラグ付けされます（[VMware Transit Connect を通じて学習およびアダプタイズされたルートの表示](#)を参照）。

インベントリ グループの操作

VMware Cloud on AWS のネットワーク管理者は、NSX インベントリ オブジェクトを使用して、ファイアウォール ルールで使用するサービス、グループ、コンテキスト プロファイル、および仮想マシンのコレクションを定義できます。

ファイアウォール ルールは、多くの場合、次のような共通する特性を持つ仮想マシンのグループに適用されます。

- 命名規則に基づく名前（Windows 仮想マシンの場合は Win*、Photon 仮想マシンの場合は Photon* など）
- 特定の範囲または CIDR ブロック内の IP アドレス
- タグ

また、サービス タイプやネットワーク プロトコルなどの特性によって区別されるネットワーク サービスに適用することもできます。NSX の [インベントリ] 画面を使用すると、ファイアウォール保護に関して同様なニーズを持つ仮想マシンのグループを作成するプロセスを簡素化できます。また、組み込みのサービス リストに新しいネットワーク サービスを追加することで、これらのサービスをファイアウォール ルールに追加できるようになります。

VMware Cloud on AWS は、すべての新しい SDDC で管理グループとサービス インベントリを作成します。ワークロード仮想マシンとそのタグのリストも保持します。管理仮想マシンまたはコンピューティング仮想マシンで構成される独自のインベントリ グループを追加または変更できます。

NSX インベントリ グループを作成して使用方法の詳細については、『[NSX データセンター管理ガイド](#)』の「[インベントリ](#)」を参照してください。

サービスの追加

サービスを構成して、ポートやプロトコルのペアリングなど、一致するネットワーク トラフィックのパラメータを指定することができます。

グループの追加

グループには静的および動的に追加されたさまざまなオブジェクトが含まれています。これらは、ファイアウォール ルールの送信元または宛先として使用できます。

コンテキスト プロファイルについて

コンテキスト プロファイルは、NSX Advanced Firewall アドオンを有効にした SDDC でのみ使用可能な VMware Cloud on AWS アドオン機能です。

プロファイルには、コンテキスト プロファイルとレイヤー 7 アクセス プロファイルの 2 種類があります。プロファイルを使用すると、レイヤー 7 アプリケーション ID やドメイン名などの属性キー値のペアを作成できます。定義したプロファイルは、1 つ以上の分散ファイアウォール ルールとゲートウェイ ファイアウォール ルールで使用できます。

NSX Advanced Firewall アドオンのインストールと使用については、[6 章 NSX Advanced Firewall 機能について](#)を参照してください。コンテキスト プロファイルの詳細と VMware Cloud on AWS での使用方法については、[こちら](#)を参照してください。

ワークロード接続の管理

デフォルトでは、ルーティング セグメントまたは MON が有効な HCX 拡張ネットワーク上のワークロード仮想マシンがインターネットに接続できます。NAT ルール、コンピューティング ゲートウェイのファイアウォール ルール、分散ファイアウォール ルール、さらには VPN 接続、DX 接続、または VTGW 接続によってアダプタイズされるデフォルト ルートのすべてで、インターネット アクセスをきめ細かく制御できます。

ワークロード仮想マシンは、プライベート IP アドレスを使用して、同じ SDDC または SDDC グループ内の他のワークロードと通信できます。すべてのトラフィックに適用するカスタム NAT ルールが適用されない限り、ワークロード仮想マシンは、パブリック IP アドレスを使用するときに、[概要] 画面に表示される [送信元の NAT パブリック IP アドレス] を取得します。

ワークロード トラフィックは、ファイアウォール ルールの処理中に、いくつかの種類の特別な処理の対象となります。

- ワークロード間のトラフィックには、CGW ファイアウォール ルールは適用されません。
- ソース仮想マシンによる分散ファイアウォール ルールの処理では、宛先パブリック IP アドレスと宛先仮想マシンの送信元パブリック IP アドレスが使用され、IP ベースである必要があります。仮想マシン属性による分散ファイアウォール ルールは、ワークロード間のトラフィックには影響しません。
- vCenter Server パブリック IP アドレスに対するワークロード仮想マシン通信には、管理ゲートウェイファイアウォール ルールが適用されますが、ワークロード仮想マシン IP は、ファイアウォール ルールが適用される前にパブリック IP アドレスに変換されます。

注： ネットワーク セグメント上のすべての仮想マシンは、同じ MTU を使用する必要があります。SDDC 内部または DX 経由のトラフィックでは、MTU の上限は 8,900 バイトです。他のエンドポイントへのネットワーク トラフィックの最大 MTU は、これより小さくなる場合があります。[VMware 構成の上限](#)を参照してください。

コンピューティング ネットワーク セグメントへの仮想マシンの接続またはワークロード仮想マシンの分離

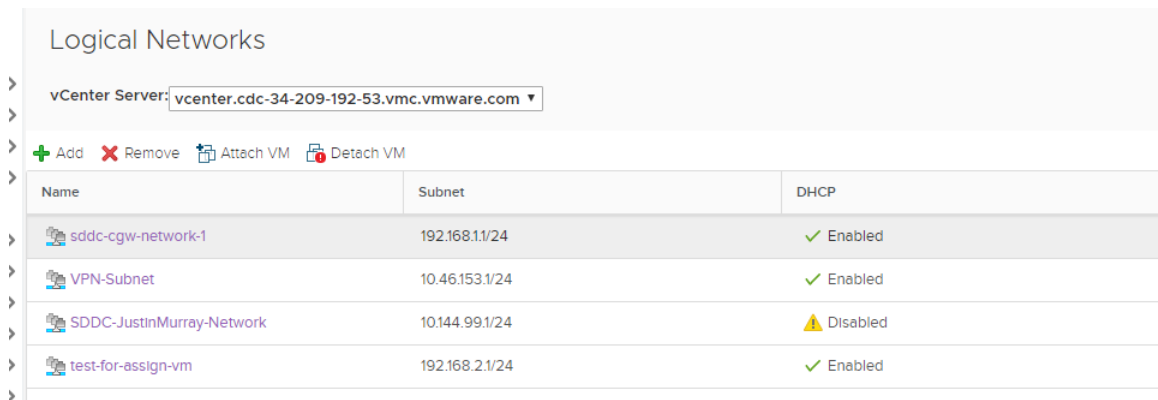
vSphere Client を使用して、コンピューティング ネットワーク セグメントへのワークロード仮想マシンの接続を管理します。

前提条件

SDDC コンピューティング ネットワークには、1 つ以上のセグメントが必要です。[ネットワーク セグメントの作成または変更](#)を参照してください。

手順

- 1 SDDC の vSphere Client にログインします。
- 2 [メニュー] - [グローバル インベントリ リスト] の順に選択します。
- 3 [論理ネットワーク] を選択します。
- 4 [vCenter Server] ドロップダウン メニューで、対象の論理ネットワークを管理する vCenter Server を選択します。
- 5 論理ネットワーク名の横をクリックして選択します。



Name	Subnet	DHCP
sddc-cgw-network-1	192.168.1.1/24	✓ Enabled
VPN-Subnet	10.46.153.1/24	✓ Enabled
SDDC-JustinMurray-Network	10.144.99.1/24	⚠ Disabled
test-for-assign-vm	192.168.2.1/24	✓ Enabled

- 6 仮想マシンの接続または切断のいずれかを選択します。
 - [仮想マシンの接続] をクリックし、選択したネットワークに仮想マシンを接続します。
 - 選択したネットワークから仮想マシンを切断するには、[仮想マシンの切断] をクリックします。
- 7 接続または切断する仮想マシンを選択し、[>>] をクリックします。[選択したオブジェクト] 列に移動して、[次へ] をクリックします。
- 8 各仮想マシンに対して、接続する仮想 NIC を選択し、[次へ] をクリックします。
- 9 [終了] をクリックします。

パブリック IP アドレスの要求またはリリース

インターネットからワークロード仮想マシンへのアクセスを許可するため、ワークロード仮想マシンに割り当てるパブリック IP アドレスを要求できます。VMware Cloud on AWS は、AWS から IP アドレスをプロビジョニングします。

ベスト プラクティスとして、使用されていないパブリック IP アドレスをリリースします。


前提条件

仮想マシンに、論理ネットワークから固定 IP アドレスが割り当てられていることを確認します。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。 [NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [パブリック IP アドレス] 画面を開きます。
- 5 新しいパブリック IP アドレスを要求するには、[新しい IP アドレスを要求] をクリックします。
必要に応じて、要求に関するメモを入力できます。
- 6 不要になったパブリック IP アドレスをリリースするには、、[IP アドレスのリリース] の順に選択します。
アドレスが NAT ルールによって使用されている場合は、パブリック IP アドレスのリリース要求は失敗します。
- 7 [保存] をクリックします。
しばらくすると、新しいパブリック IP アドレスがプロビジョニングされます。

次のステップ

パブリック IP アドレスがプロビジョニングされた後、パブリック IP アドレスから SDDC の仮想マシンの内部 IP アドレスにトラフィックを送るように NAT ルールを構成します。 [NAT ルールの作成または変更](#) を参照してください。

NAT ルールの作成または変更

ネットワーク アドレス変換 (NAT) は、パケット ヘッダー内の IP アドレスがゲートウェイの両側でどのように表示されるかを制御します。コンピューティング ゲートウェイで実行されるルールは、ゲートウェイに出入りするインターネット トラフィックをマッピングします。他の Tier-1 ゲートウェイで実行されるルールは、ゲートウェイと他の SDDC ネットワーク インターフェイス間のトラフィックをマッピングします。

NAT ルールは、コンピューティング ゲートウェイおよび作成した追加の Tier-1 ゲートウェイで実行されます。SDDC で追加の Tier-1 ゲートウェイを作成する方法については、[VMware Cloud on AWS SDDC へのカスタム Tier-1 ゲートウェイの追加](#) を参照してください。

SDDC のインターネット インターフェイス（コンピューティング ゲートウェイ）で実行される NAT ルールは、コンピューティング ネットワーク セグメントから送信されるパケットの内部送信元アドレスまたは内部宛先 IP アドレスを、パブリック インターネットで使用可能なアドレスにマッピングします。NAT ルールを作成するには、ワークロード仮想マシンまたはサービスの内部アドレスと、選択した外部 IP アドレスを指定します。[インターネット] インターフェイスで実行される NAT ルールには、パブリック IP アドレスが必要です。 [パブリック IP アドレスの要求またはリリース](#) を参照してください。

パケットの送信元アドレスと宛先アドレスを調べるファイアウォール ルールはこれらのゲートウェイで実行され、適用可能な NAT ルールによって変換された後のトラフィックを処理します。NAT ルールを作成する際に、仮想マシンの内部または外部 IP アドレスとポート番号を、その仮想マシンとの間のネットワーク トラフィックに影響するファイアウォール ルールに公開するかどうかを指定できます。

重要： SDDC のパブリック IP アドレスへの受信トラフィックは、常にユーザーが作成した NAT ルールによって処理されます。送信トラフィック（SDDC ワークロード仮想マシンからの応答パケット）は、アドバタイズされるルートに沿ってルーティングされ、SDDC ネットワークのデフォルト ルートが SDDC のインターネット インターフェイスを通過するときに、NAT ルールによって処理されます。ただし、デフォルト ルートの経由ルートが Direct Connect、VPN または VTGW 接続であるか、VPC へのスタティック ルートとして追加済みの場合、NAT ルールは受信トラフィックには実行されますが、送信トラフィックには実行されません。その結果、そのパブリック IP アドレスで仮想マシンがアクセス不能になる非同期パスが形成されます。たとえば、0.0.0.0/0 が BGP を介してアドバタイズされる場合、またはリモート ネットワークが 0.0.0.0/0 のポリシーベース VPN がある場合に、この非同期性が生じる可能性があります。デフォルト ルートがオンプレミス環境からアドバタイズされる場合は、オンプレミスのインターネット接続とパブリック IP アドレスを使用して、オンプレミス ネットワークで NAT ルールを構成する必要があります。

前提条件

- コンピューティング ゲートウェイ（[インターネット] インターフェイス）で NAT ルールを作成するには、この SDDC の仮想マシンで使用するパブリック IP アドレスを取得しておく必要があります。[パブリック IP アドレスの要求またはリリース](#)を参照してください。
- 仮想マシンは、ルーティングされたコンピューティング ネットワーク セグメントに接続する必要があります。仮想マシンの NAT ルールは、割り当てられたアドレスが静的アドレスの場合でも、動的 (DHCP) アドレスの場合でも作成できます。ただし、DHCP アドレス割り当てを使用する仮想マシンの NAT ルールは、ルールで指定されているアドレスと一致しない内部アドレスが仮想マシンに割り当てられると、無効になることがあります。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

4 [NAT] - [インターネット] の順にクリックして、デフォルトのコンピューティング ゲートウェイで実行される NAT ルールを追加します。

- a [NAT ルールの追加] をクリックし、ルールの [名前] を指定します。
- b [インターネット] NAT ルール オプションを構成します。

オプション	説明
パブリック IP アドレス	現在の SDDC 用にプロビジョニングされたパブリック IP アドレスのドロップダウン リストから選択します。 パブリック IP アドレスの要求またはリリース を参照してください。
サービス	<ul style="list-style-type: none"> ■ 指定した [内部 IP アドレス] に対する受信 (DNAT) トラフィックと送信 (SNAT) トラフィックの両方に適用するルールを作成するには、[すべてのトラフィック] を選択します。 ■ そのプロトコルとポートを使用するトラフィックにのみ適用する受信 (DNAT) ルールを作成するには、リスト内のサービスを 1 つ選択します。作成済みのカスタム サービス (インベントリ グループの操作を参照) もここに一覧表示されます。 <p>注： 複数の宛先ポートを使用するサービスには NAT ルールが適用されないため、これらのサービスはこのリストに表示されません。</p>
パブリック ポート	<p>[サービス] を [すべてのトラフィック] として指定した場合、デフォルトのパブリック ポートは [任意] になります。</p> <p>特定の [サービス] を選択すると、そのサービスに割り当てられたパブリック ポートにルールが適用されます。</p>
内部 IP アドレス	仮想マシンの内部 IP アドレスを入力します。このアドレスは、ルーティングされた SDDC ネットワーク セグメント上にある必要があります。
内部ポート	<p>選択した[サービス]で使用する内部ポートを表示します。カスタム ポートを使用するには、カスタム サービス (インベントリ グループの操作を参照) を追加し、NAT ルールでその [サービス] を選択します。</p> <p>[サービス] を [すべてのトラフィック] として指定した場合、デフォルトの内部ポートは [任意] になります。</p> <p>特定の [サービス] を選択すると、そのサービスに割り当てられたパブリック ポートにルールが適用されます。</p>
ファイアウォール	この NAT ルールが適用されるトラフィックをゲートウェイ ファイアウォール ルールにどのように公開するかを指定します。デフォルトでは、これらのファイアウォール ルールで、[内部 IP アドレス] と [内部ポート] の組み合わせを照合します。ファイアウォール ルールを [外部 IP アドレス] と [外部ポート] の組み合わせと照合するには、[外部アドレスと照合] を選択します。(分散ファイアウォール ルールは、外部アドレスやポートには適用されません。)

[すべてのトラフィック] に同じ [パブリック IP アドレス] と [内部 IP アドレス] を使用する NAT ルールを複数作成できます。その場合、各 [内部 IP アドレス] では、送信 (SNAT) トラフィックに [パブリック IP アドレス] が使用されますが、受信 (DNAT) トラフィックにはファースト マッチング ルールのみが使用されます。デフォルトの送信ルールが作成されますが、表示はされません。このルールは、[すべてのトラフィック] に適用される特定の NAT ルールと一致しないすべての [内部 IP アドレス] に使用されます。このルールに使用される IP は、[ネットワークとセキュリティ] [概要] ページの [デフォルト コンピューティング ゲートウェイ] に [送信元の NAT パブリック IP アドレス] として表示されます。

- c ルールの [優先順位] を選択します。

小さい値であるほど、このルールの優先順位は高くなります。

- d (オプション) [ログ] を切り替えてルールのアクションをログに記録します。
 - e 新しいルールは作成時にアクティブになります。[有効] を切り替えると無効になります。
 - f [保存] をクリックしてルールを作成します。
- 5 (オプション) 追加の Tier-1 ゲートウェイが作成されている場合は、[NAT] - [Tier-1 ゲートウェイ] の順にクリックして、そのゲートウェイで実行される NAT ルールを追加します。
- a ルールを実行する [ゲートウェイ] を選択します。
 - b [NAT ルールの追加] をクリックし、ルールの [名前] を指定します。
 - c [Tier-1 ゲートウェイ] NAT ルール オプションを構成します。

オプション	説明:
操作	<p>次のいずれかとします。</p> <p>SNAT</p> <p>送信元 NAT。パケット ヘッダーの送信元アドレスを変更します。Tier-1 ルーター上の送信元 NAT の設定を参照してください。</p> <p>DNAT</p> <p>宛先 NAT。パケット ヘッダーの宛先アドレスを変更します。Tier-1 ルーター上の宛先 NAT の設定を参照してください。</p> <p>必要に応じて、[変換ポート] を指定します。</p> <p>再帰</p> <p>非対称ルートを回避するためのステートレス NAT 構成。再帰 NAT を参照してください。</p> <p>SNAT なし</p> <p>送信元 NAT をオフにします。</p> <p>DNAT なし</p> <p>宛先 NAT をオフにします。</p>
一致	SNAT の場合は、使用する送信元アドレスを入力します。DNAT の場合は、使用する宛先アドレスを入力します。
変換	変換された SNAT または DNAT アドレスに使用する IPv4 アドレスまたは CIDR ブロックを入力します。
適用先	特定のインターフェイスまたはラベルを選択して、ルールを適用するトラフィックを定義します。
ファイアウォール	この NAT ルールが適用されるトラフィックをゲートウェイ ファイアウォール ルールにどのように公開するかを指定します。デフォルトでは、これらのファイアウォール ルールで、[内部 IP アドレス] と [内部ポート] の組み合わせを照合します。ファイアウォール ルールを [外部 IP アドレス] と [外部ポート] の組み合わせと照合するには、[外部アドレスと照合] を選択します。(分散ファイアウォール ルールは、外部アドレスやポートには適用されません。)

- d ルールの [優先順位] を選択します。
小さい値であるほど、このルールの優先順位は高くなります。
- e (オプション) [ログ] を切り替えてルールのアクションをログに記録します。
- f 新しいルールは作成時にアクティブになります。[有効] を切り替えると無効になります。
- g [保存] をクリックしてルールを作成します。

コンピューティング ネットワークと管理ネットワーク間のトラフィックを管理するためのファイアウォール ルールの作成

デフォルトの設定では、ファイアウォール ルールによって、コンピューティング ネットワーク上の仮想マシンは管理ネットワーク上の仮想マシンにアクセスできません。個々のワークロード仮想マシンが管理仮想マシンにアクセスできるようにするには、ワークロードおよび管理インベントリ グループを作成し、それらを参照する管理ゲートウェイ ファイアウォール ルールを作成します。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。 [NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。
- 4 管理ネットワーク用と、アクセスするワークロード仮想マシン用に 1 つずつ、コンピューティング インベントリ グループを作成します。

[インベントリ] 画面で、[グループ] - [コンピューティング グループ] の順にクリックし、2 つのグループを作成します。
 - [グループの追加] - [メンバーを設定] の順にクリックし、[IP アドレス] 画面を開き、[IP アドレスを入力] をクリックして、管理ネットワークの CIDR ブロックを入力します。[適用] をクリックし、[保存] をクリックしてグループを作成します。
 - [グループの追加] - [メンバーを設定] の順にクリックしてから、[メンバーシップ条件] - [条件の追加] の順にクリックし、vSphere インベントリ内の [仮想マシン] を指定します。[適用] をクリックし、[保存] をクリックしてグループを作成します。
- 5 コンピューティング グループからアクセスする管理ネットワークが含まれる管理グループを作成します。

[インベントリ] 画面で、[グループ] - [管理グループ] の順にクリックします。[メンバーを選択] 画面で、[IP アドレスを入力] をクリックし、管理ネットワークの CIDR ブロックを入力します。[適用] をクリックし、[保存] をクリックしてグループを作成します。

- 6 vCenter Server および ESXi への受信トラフィックを許可する管理ゲートウェイ ファイアウォール ルールを作成します。

管理ゲートウェイ ファイアウォール ルールの作成の詳細については、[管理ゲートウェイのファイアウォール ルールの追加または変更](#)を参照してください。たとえばワークロード仮想マシンが vSphere、PowerCLI、または OVFtool にのみアクセスする必要がある場合には、ポート 443 でのアクセスのみをルールで許可する必要があります。

表 3-26. ESXi および vCenter Server への受信トラフィックを許可する管理ゲートウェイ ルール

名前	送信元	宛先	サービス	操作
ESXi への受信	ワークロード仮想マシンのプライベート IP アドレス	ESXi	HTTPS (TCP 443)	Allow
vCenter Server のプライベート IP アドレスへの受信	ワークロード仮想マシンのプライベート IP アドレス	vCenter Server のプライベート IP アドレス	HTTPS (TCP 443)	Allow
vCenter Server のパブリック IP アドレスへの受信	NATted IP アドレスを持つワークロード仮想マシン	vCenter Server のパブリック IP アドレス	HTTPS (TCP 443)	Allow

監視およびトラブルシューティング機能の設定

4

NSX IPFIX およびポート ミラーリング機能を使用して、SDDC のネットワークとセキュリティの監視およびトラブルシューティングを行います。

SDDC の ESXi ホストはデフォルトでオーバーレイ ネットワークにアクセスできるため、SDDC で仮想マシン ワークロードとして展開されている監視およびトラブルシューティング アプリケーションと通信することが可能です。ただし、ESXi ホストと、ワークロード仮想マシンが接続されている論理セグメント間のトラフィックを許可するようにファイアウォールを構成する必要があります。[コンピューティング ネットワークと管理ネットワーク間のトラフィックを管理するためのファイアウォール ルールの作成](#)を参照してください。

■ IPFIX の設定

IPFIX (Internet Protocol Flow Information Export) は、トラブルシューティング、監査、または分析情報の収集に使用されるネットワーク フロー情報のフォーマットおよびエクスポートの標準です。

■ ポート ミラーリングの設定

ポート ミラーリングを使用すると、送信元からのすべてのトラフィックのレプリケーションとリダイレクトが可能になります。ミラーリングされたトラフィックは、Generic Routing Encapsulation (GRE) トンネル内でカプセル化されてコネクタに送信されるため、リモートの宛先に到達するまで、元のパケットの情報はすべて保持されます。

■ 接続中の VPC 情報の表示と接続中の VPC に関する問題のトラブルシューティング

接続されている Amazon VPC には、SDDC とそのすべてのネットワークが含まれています。この VPC に関する情報（アクティブな ENI、VPC サブネット、VPC ID など）は、[接続中の VPC] 画面で確認できます。

IPFIX の設定

IPFIX (Internet Protocol Flow Information Export) は、トラブルシューティング、監査、または分析情報の収集に使用されるネットワーク フロー情報のフォーマットおよびエクスポートの標準です。

論理セグメント上でフロー モニタリングを構成できます。その論理セグメントに接続されている仮想マシンからのすべてのフローがキャプチャされ、IPFIX コレクタに送信されます。コレクタ名は、各 IPFIX スイッチ プロファイルのパラメータとして指定します。

注： SDDC グループのメンバーである SDDC では、SDDC ネットワーク外のホストから宛先へのすべての送信トラフィックは、SDDC 内の他のルーティング構成に関係なく、VTGW またはプライベート VIF にルーティングされます。これには、IPFIX トラフィックとポート ミラーリングトラフィックが含まれます。[VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理](#)を参照してください。

前提条件

論理セグメントが設定済みであることを確認します。[ネットワーク セグメントの作成または変更](#)を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [IPFIX] 画面を開きます。

IPFIX の使用方法の詳細については、『NSX Data Center 管理ガイド』の[ネットワーク監視](#)を参照してください。

ポート ミラーリングの設定

ポート ミラーリングを使用すると、送信元からのすべてのトラフィックのレプリケーションとリダイレクトが可能になります。ミラーリングされたトラフィックは、Generic Routing Encapsulation (GRE) トンネル内でカプセル化されてコレクタに送信されるため、リモートの宛先に到達するまで、元のパケットの情報はすべて保持されます。

ポート ミラーリングは、次の場合に使用します。

- **トラブルシューティング：** トラフィックを分析して侵入を検出し、ネットワーク上のエラーをデバッグおよび診断します。
- **コンプライアンスとモニタリング：** 分析と修正を行うため、モニタリング対象のすべてのトラフィックをネットワーク アプライアンスに転送します。

ポート ミラーリングには、データが監視される送信元グループと、収集されたデータのコピー先となる宛先グループが含まれます。送信元グループのメンバーシップ条件では、Web グループやアプリケーション グループなど、ワークロードに基づいて仮想マシンをグループ化する必要があります。宛先グループのメンバーシップ条件では、IP アドレスに基づいて仮想マシンをグループ化する必要があります。ポート ミラーリングには1つの適用ポイントがあり、ここで SDDC 環境にポリシー ルールが適用されます。

ポート ミラーリングのトラフィックの方向は、入力方向、出力方向、双方向のいずれかです。

- 入力方向は、仮想マシンから論理ネットワークへの出力ネットワーク トラフィックです。
- 出力方向は、論理ネットワークから仮想マシンへの入力ネットワーク トラフィックです。
- 双方向は、仮想マシンから論理ネットワーク、および論理ネットワークから仮想マシンへのトラフィックです。デフォルトのオプションです。

注： SDDC グループのメンバーである SDDC では、SDDC ネットワーク外のホストから宛先へのすべての送信トラフィックは、SDDC 内の他のルーティング構成に関係なく、VTGW またはプライベート VIF にルーティングされます。これには、IPFIX トラフィックとポート ミラーリングトラフィックが含まれます。[VMware Transit Connect™ を使用した SDDC 展開グループの作成と管理](#)を参照してください。

前提条件

重要： ポート ミラーリングでは、多くのネットワーク トラフィックを生成できます。ベスト プラクティスとして、トラブルシューティングと修正が短時間で済むよう、ポート ミラーリングを使用するのは、同時に最大 6 台の仮想マシンまでとしてください。

IP アドレスおよび仮想マシンのメンバーシップ条件を満たすワークロード グループが使用可能であることを確認します。[インベントリ グループの操作](#)を参照してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#)を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [ポート ミラーリング] 画面を開きます。

ポート ミラーリングの使用法の詳細については、『NSX Data Center 管理ガイド』の[ネットワーク監視](#)を参照してください。

接続中の VPC 情報の表示と接続中の VPC に関する問題のトラブルシューティング

接続されている Amazon VPC には、SDDC とそのすべてのネットワークが含まれています。この VPC に関する情報（アクティブな ENI、VPC サブネット、VPC ID など）は、[接続中の VPC] 画面で確認できます。

VMware Cloud on AWS は、AWS アカウントのリンクと AWS CloudFormation を使用して、AWS アカウントへのアクセスに必要な権限を取得します。アカウントがリンクされている場合、VMware Cloud on AWS は IAM ロールを作成する CloudFormation テンプレートを実行し、いくつかの VMware アカウントにこれらのロールを引き継ぐための権限を付与します。ロール名は、SDDC の [接続中の VPC] 画面に一覧表示されます。これらのロールと権限の詳細は、『VMware Cloud on AWS Operations Guide』の [AWS のロールおよび権限](#) で公開されています。

これらのロールが、VMware Cloud on AWS に、ENI の作成、削除、割り当てと、VPC 内のルートテーブルの変更を行う権限を付与する場合を考えます。ロールでは、VMware Cloud on AWS が使用可能なリソースをマッピングし、SDDC 作成プロセスで提供できるように、アカウント内のサブネットと VPC の列挙も許可されます。これらの機能は、SDDC のアップグレードの際には必ず、SDDC の作成ワークフローの開始時に必要になります。また、SDDC の存続期間に、VPC とそのサブネットの検証が必要な場合や、ルート テーブルと ENI の調査や変更が必要な場合に必要になることもあります。組織のメンバーが IAM ロールの削除や変更、メイン ルート テーブルの変更などの操作を行って接続中の VPC の安全性を侵害した場合、SDDC の操作が次のような影響を受けることがあります。

- VMware Cloud on AWS で、SDDC 管理クラスタ内のホストの追加、置き換え、削除ができません。
- アップグレード中にルートが変更されたり、アクティブな NSX Edge でホストが変更されたりした場合でも、VMware Cloud on AWS でメインのルート テーブルを更新できません。これにより、SDDC とネイティブの AWS サービス間の接続が切断される可能性があります。詳細については、[SDDC と接続中の VPC の間のルーティング](#) を参照してください。
- 影響を受ける組織は、アカウントにリンクされた SDDC を展開できなくなります。

注： VMware Cloud on AWS CloudFormation テンプレートを再実行しても、既存の SDDC には影響しないため、[接続中の Amazon VPC] ページに表示されている IAM ロールが引き続き使用されます。既存の SDDC でこれらの症状のいずれかが発生している場合は、VMware のサポートに確認してください。

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。
- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。[NSX Manager による SDDC ネットワーク管理](#) を参照してください。

このワークフローでは、VMware Cloud コンソールの [ネットワークとセキュリティ] タブを使用することもできます。

- 4 [接続中の VPC] をクリックして、[接続中の Amazon VPC] 画面を開きます。

この画面には、次の情報が含まれます。

AWS アカウント ID

SDDC を作成したときに指定した AWS アカウント ID。

VPC ID

この VPC の AWS ID。

VPC サブネット

SDDC を作成したときに指定した VPC サブネットの AWS ID。

アクティブなネットワーク インターフェイス

この VPC で VMC によって使用される ENI の ID。

IAM ロールの名前

この VPC で定義されている AWS ID とアクセス管理ロール名。『VMware Cloud on AWS Operations Guide』の [AWS のロールと権限](#) を参照してください。

クラウド フォーメーション スタック名

SDDC の作成に使用される AWS Cloud フォーメーション スタックの名前

サービス アクセス

この VPC で有効になっている AWS サービスのリスト。

NSX イベントとアラームの操作

5

VMware Cloud on AWS SDDC の NSX Manager は、パフォーマンスとシステム操作に影響を与える可能性があるイベントに注意を促すアラームを提供します。アラームは、影響を受けるコンポーネント、イベントのタイプなど、詳細なイベント情報を提示し、修正アクションを推奨します。

アラームは、次のいずれかの状態になります。

状態	説明
開く	アラームはアクティブで未確認の状態になっています。
確認済み	ユーザーがアラームを確認しています。アラームはオープン状態のままですが、NSX Manager の通知には表示されなくなります。
抑止済み	ユーザーが指定した期間、このアラームの状態は報告されません。
解決	システムまたはユーザーの操作によってアラームが解決されています。アラームは最大 8 日間のアラーム テーブルに表示され、その後、自動的に削除されます（リソース要件のため、解決済みのアラームがこの期間よりも早く削除される場合があります）。 注： ユーザーがアラームの状態を「解決済み」に変更しても、アラームをトリガした状態が解決されていない場合は、新しいアラームインスタンスがインスタンス化されます。また、インターフェイスに表示される状態が更新される数分前に、イベントが解決されていることもあります。

VMware Cloud on AWS でサポートされているすべての NSX イベントとアラームのリストについては、[VMware Cloud on AWS の NSX アラーム カタログ](#)を参照してください。

前提条件

NSX のアラートとアラームへのアクセスは、VMware Cloud on AWS サービス ロールに基づいています。

表 5-1. サービス ロール別のアラームへのアクセス

VMware Cloud on AWS サービス ロール	イベントとアラームへのアクセス
NSX Cloud 管理者	アラームと定義の読み取りおよび変更
管理者	アラームと定義の読み取り
削除が制限された管理者	アラームと定義の読み取り
監査者	アラームと定義の読み取り
NSX Cloud 監査者	アラームと定義の読み取り

手順

- 1 <https://vmc.vmware.com> の VMware Cloud Services にログインします。

- 2 [インベントリ] - [SDDC] の順にクリックし、SDDC カードを選択して [詳細表示] をクリックします。
- 3 [NSX Manager を開く] をクリックし、SDDC の [設定] 画面に表示されている [NSX Manager 管理者ユーザー アカウント] を使用してログインします。
- 4 [ホーム] 画面に移動して、[アラーム] をクリックします。

注： 赤色の感嘆符 (!) が [アラーム] パネル ラベルの横に表示されている場合は、重要度が「重大」のアラームが1つ以上オープンしています。

[アラーム] パネルが表示され、[アクティブ アラーム]、[アラーム数が多い上位の機能]、[発生数別の上位のイベント] などのグラフィック ダッシュボードが表示されます。ダッシュボードの下には、現在のアラームのリストが表示されます。このリストは並べ替えが可能です。このテーブルでは、アクティブ アラームについて次の情報が表示されます。

- 影響を受ける機能
- イベント タイプ
- ノード
- エンティティ
- 重要度（重大、高、中）
- 前回レポートされた時間
- アラームの状態（オープン、抑止済み、解決済み、確認済み）

[アラーム] テーブルの各行を展開すると、詳細を表示できます。

- 5 ダッシュボードの右上隅にあるフィルタ アイコンをクリックすると、ダッシュボードに表示される結果をフィルタリングできます。

過去 24 時間、過去 48 時間、カスタム期間、オープン状態のすべてのアラームでフィルタリングできます。

- 6 テーブルの上にあるフィルタ テキスト ボックスをクリックすると、テーブルに表示される結果をフィルタリングできます。

アラームの状態、説明、エンティティ名、エンティティ タイプ、イベント タイプ、ノードなどのフィルタを指定するように求められます。

VMware Cloud on AWS の NSX アラーム カタログ

VMware Cloud on AWS では、NSX イベントのサブセットに対するアラームがサポートされます。

次の表に、アラーム メッセージや解決の推奨アクションなど、VMware Cloud on AWS で NSX アラームをトリガするイベントについて説明します。重要度が「低」より大きいイベントが発生すると、アラームがトリガされます。詳細については、『NSX 管理ガイド』の[イベントとアラームの操作](#)を参照してください。NSX でサポートされている一部のイベント、アラーム、および関連機能を VMware Cloud on AWS で使用することはできません。

分散ファイアウォール イベント

イベント名	重要度	ノードタイプ	アラートメッセージ	推奨アクション
DFW の CPU 使用率が非常に高い	重大	esx	DFW の CPU 使用率が非常に高くなっています。イベントの検出時:「トランスポート ノード <i>{entity_id}</i> の DFW の CPU 使用率が <i>{system_resource_usage}%</i> に達しています。これは、 <i>{system_usage_threshold}%</i> の超高しきい値に達しているか、超えています。」イベントの解決時:「トランスポート ノード <i>{entity_id}</i> の DFW の CPU 使用率が <i>{system_resource_usage}%</i> に達しています。これは、 <i>{system_usage_threshold}%</i> の超高しきい値を下回っています。」	このホストと他のホストの間で仮想マシン ワークロードのリバランシングを行うことを検討してください。最適化でのセキュリティ設計を確認してください。たとえば、ルールがデータセンター全体に適用されない場合は、適用先の構成を使用します。
DFW vMotion の障害	重大	esx	DFW vMotion に失敗し、ポートが切断されました。イベントの検出時:「宛先ホスト <i>{transport_node_name}</i> の DFW フィルタ <i>{entity_id}</i> の DFW vMotion でエラーが発生し、エンティティのポートが切断されました。」イベントの解決時:「宛先ホスト <i>{transport_node_name}</i> の DFW フィルタ <i>{entity_id}</i> の DFW 構成に成功し、DFW vMotion の障害で発生したエラーが解決されました。」	NSX Manager でホスト上の仮想マシンを確認します。NSX Manager ユーザー インターフェイスで、DFW 構成を手動で再度プッシュします。再プッシュされる DFW ポリシーは、DFW フィルタ <i>{entity_id}</i> で追跡できます。また、DFW フィルタが接続している仮想マシンを特定して再起動することも検討してください。
DFW セッション数が多い	重大	esx	DFW セッション数が多くなっています。イベントの検出時:「トランスポート ノード <i>{entity_id}</i> の DFW セッション数が <i>{system_resource_usage}%</i> に達しています。これは、 <i>{system_usage_threshold}%</i> のしきい値に達しているか、超えています。」イベントの解決時:「トランスポート ノード <i>{entity_id}</i> の DFW セッション数が <i>{system_resource_usage}%</i> に達しています。これは、 <i>{system_usage_threshold}%</i> のしきい値を下回っています。」	ホスト上で、ワークロードのネットワークトラフィックの負荷レベルを確認します。このホストと他のホストの間でワークロードをリバランシングすることを検討してください。

分散 IDS/IPS イベント

イベント名	重要度	ノードタイプ	アラートメッセージ	推奨アクション
NSX IDPS エンジンのメモリ使用率が高い	中	esx	NSX-IDPS エンジンのメモリ使用量が 75% 以上に達しています。イベントの検出時:「NSX-IDPS エンジンのメモリ使用率が <i>{system_resource_usage}%</i> になっています。これは、高しきい値の 75% に達しているか、超えています。」イベントの解決時:「NSX-IDPS エンジンのメモリ使用率が <i>{system_resource_usage}%</i> に達しています。これは、高しきい値の 75% を下回っています。」	このホストと他のホストの間で仮想マシン ワークロードのリバランシングを行うことを検討してください。

NSX Advanced Firewall 機能について

6

NSX Advanced Firewall サービスによって、SDDC で高度な NSX 機能を使用できます。

NSX Advanced Firewall サービスは、バージョン 1.16 以降の VMware Cloud on AWS SDDC で使用できます。このサービスに含まれる機能は次のとおりです。

- NSX レイヤー 7 コンテキスト プロファイル
- NSX 分散 IDS/IPS
- NSX Identity Firewall
- NSX 分散 FQDN フィルタリング。

SDDC で NSX Advanced Firewall アドオンを有効にするには、[アドオン] タブを開き、[NSX Advanced Firewall アドオン] カードで [有効化] をクリックします。アドオンが有効になると、NSX の高度なセキュリティ機能を SDDC で使用できるようになります。

これらの機能の詳細については、「NSX 製品のドキュメント」を参照してください。オンプレミス NSX での機能の動作と、VMware Cloud on AWS での動作には、操作上の違いがいくつかあります。たとえば、『NSX 製品のドキュメント』のほとんどの手順には NSX Manager に管理者権限でログインするように指示する手順が含まれています。[NSX Manager を開く] をクリックするか [ネットワークとセキュリティ] タブを開くと SDDC の NSX Manager に管理者権限でアクセスするため、この手順は VMware Cloud on AWS では不要になります。その他の違いについては、次のセクションを参照してください。

SDDC でのコンテキスト プロファイルの使用

[インベントリ] - [コンテキスト プロファイル] の順にクリックします。分散ファイアウォール ルールでコンテキスト プロファイルを指定するには、[分散ファイアウォール] グリッドの [プロファイル] 列の値を更新します。詳細については、『NSX 製品のドキュメント』の [レイヤー 7 ファイアウォール ルールのワークフロー](#) を参照してください。

VMware Cloud on AWS では、コンテキスト プロファイルは分散ファイアウォール ルールでの使用のみがサポートされます。管理ゲートウェイまたはコンピューティング ゲートウェイのファイアウォール ルールでは使用できません。

SDDC での Distributed IDS/IPS の使用

[セキュリティ] - [分散 IDS/IPS] をクリックします。詳細については、『NSX 製品のドキュメント』の [分散 IDS/IPS](#) を参照してください。

この機能を VMware Cloud on AWS で使用する場合は、次の操作上の違いを考慮してください。

クラスタ単位の有効化

この機能を使用するには、1 つ以上の SDDC クラスタで有効にします。[Distributed IDS/IPS] 画面で、[設定] タブをクリックし、[クラスタの侵入検知/防止を有効にする] で 1 つ以上のクラスタを選択します。現在、vMotion は仮想マシンの移行前にクラスタの IDS/IPS 有効化ステータスを確認しないため、すべてのクラスタでこの機能を有効にし、ワークロード仮想マシンへの IDS/IPS の適用に移行が影響を与えないようにすることを推奨します。

ホストへのアクセス権はなし

VMware Cloud on AWS は SDDC ホストにアクセスできないため、[ホストで Distributed IDS ステータスを確認](#)することができません。

ログ

VMware Cloud on AWS では、この機能によって生成されたイベントは VMware Aria Operations for Logs に記録されます。

SDDC での Identity Firewall の使用

[システム] - [Identity Firewall の Active Directory] をクリックして SDDC Active Directory ドメインを追加し、ユーザーベースの Identity Firewall ルールを作成できるようにします。この機能を VMware Cloud on AWS で使用する場合は、次の操作上の違いを考慮してください。

1 つ以上の SDDC クラスタの機能を有効化

この機能を使用するには、[分散ファイアウォール ルールの管理](#)の「Identity Firewall 設定の構成」の手順を実行して、機能を有効にし、1 つ以上の SDDC クラスタに適用する必要があります。

Active Directory アクセスを許可するファイアウォール ルールの作成

Active Directory を使用している場合は、管理ゲートウェイ ファイアウォール ルールを作成し、使用する Active Directory サーバに NSX がアクセスできるようにする必要があります。SDDC で Active Directory へのアクセスが中断された場合、この機能は動作しません。そのため、Active Directory サーバに変更が加えられた場合でも、ここで作成したファイアウォール ルールが有効なままであることが重要です。詳細については、『NSX 製品のドキュメント』の [Active Directory の追加](#)を参照してください。

ログ

VMware Cloud on AWS では、この機能によって生成されたイベントは VMware Aria Operations for Logs に記録されます。

SDDC での分散 FQDN フィルタリングの使用

VMware Cloud on AWS では、NSX FQDN フィルタリングは分散ファイアウォール ルールでの使用のみがサポートされます。管理ゲートウェイまたはコンピューティング ゲートウェイのファイアウォール ルールでは使用できません。この機能を使用するには、[特定のドメインのフィルタリング \(FQDN/URL\)](#)で説明されている DNS スヌーピングルールをポリシーの最初のルールとして追加します。また、FQDN フィルタリングをサポートするすべてのセグメントで、事前定義された [FQDNfiltering-spoofguard-profile] セグメント プロファイルを有効にする必要があります。セグメント プロファイルの SDDC ネットワーク セグメントへの適用については、[ネットワーク セグメントの作成または変更](#)を参照してください。

NSX Advanced Firewall アドオンの無効化

NSX Advanced Firewall アドオンを無効にする前に、アドオン機能を参照するすべてのファイアウォール ルールを削除する必要があります。これには以下が含まれます。

- コンテキスト プロファイルを含むすべての分散ファイアウォール ルール
- すべての Distributed IDS/IPS ルールおよびプロファイル
- すべての ID ベースのファイアウォール ルール

これらのオブジェクトを削除した後、アドオンを無効にできます。

- 1 SDDC の [アドオン] タブを開きます。
- 2 [NSX Advanced Firewall アドオン] カードで、[アクション] - [無効化] の順にクリックします。
- 3 無効の前に、削除が必要なオブジェクトのリストを確認します。オブジェクトが削除されたことを確認したら、[無効化の確認] をクリックします。

アドオンに対する請求は、無効化が完了するとただちに停止します。