NSX を活用した
運用の変革に向けて

実用的なベスト プラクティス

ガイドブック

vmware

目次

概要

このホワイトペーパーは、クラウド、ネットワーク、およびセキュリティ担当の責任者とマネージャを対象に構成されています。また、NSX の運用を開始する際に、アーキテクチャ、エンジニアリング、および運用を担当するマネージャと担当者にも活用いただける内容になっています。

ネットワーク仮想化は、企業がスピード、俊敏性、およびセキュリティのメリットを実現するうえで大きな役割を果たしており、この 10 年間におけるコンピューティングの仮想化によるメリットと同等またはそれ以上のメリットをもたらしますが、ネットワーク仮想化のメリットを実現するためには、企業には、**人材**、**プロセス**、および**テクノロジー**にわたる運用計画の評価と実行が求められます。

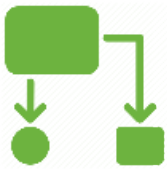
VMware は、NSX を導入されているお客様とのコミュニケーションを図り、ネットワーク仮想化の本番環境への導入状況を把握することで実際の環境に基づいた情報を、お客様が NSX の評価、導入、および運用開始をされる際にお役立ていただけるようご提供しており、お客様固有の環境に最も適したベスト プラクティスを活用いただくことが可能です。

このホワイトペーパーではさまざまなベスト プラクティスを取り扱いますが、NSX は、お客様環境の状態を問わず、最小限の変更を加えるだけで導入できます。運用も非常にシンプルです。

このガイドは 3 つのセクションで構成されており、それぞれの抑えておくべきポイントとベスト プラクティスを解説します。

人材

ネットワーク仮想化には、企業力を最大限に向上させる可能性があるほか、IT 部門の仕事のあり方を変革できる大きなメリットがあります。また、変化が伴うため、慎重に検討を重ね、企業の透明性と整合性を維持することが求められます。異なる役割と責任を持つメンバーで構成される部署を確立し、俊敏性の高い組織構造を実現することで、企業と従業員の双方にとって最大限の成果とメリットが期待できます。VMware は、組織構造、社内の取り組みやコミュニケーションに関する戦略、および役割と責任についての情報とガイダンスを提供します。



プロセス

アプリケーションのライフサイクル全体にわたり手動プロセスの自動化を行い、生産性の向上を図る上で、ネットワーク仮想化の導入は大きなきっかけとなります。アプリケーションおよびサービスのプロビジョニング、管理、監視の方法について、将来的に目指す状況を定義することで、現在使用しているプロセスや手法が不要になる場合があります。VMware は、自動化、プロセス管理、ツールのガイダンスや、注目すべきユース ケースを提供します。

テクノロジー

ネットワーク仮想化の主なメリットの 1 つは、ネットワークとセキュリティの機能を基盤となる物理ネットワーク インフラストラクチャから分離し、仮想化レイヤーで抽象化することです。これにより、将来に向けたインフラストラクチャの設計および管理をより適切に行うことができます。VMware は、アーキテクチャに関するベスト プラクティス、インフラストラクチャの段階的な実装、および新機能の定期的な導入についてのガイダンスを提供します。

これらのベスト プラクティスは、規定されたものでも画一的なものでもないため、固有の特性、目標、および優先順位を考慮して、お客様の環境に適したものを参照してください。「ビッグ バン」 方式の導入は行わずに、いくつかの小規模な環境から開始して、徐々に対象を拡大することをお勧めします。

企業によっては、プロジェクトの途中でその成果に満足し、最適なパフォーマンスを実現する前にプロジェクトを終了してしまうケースが見受けられます。このような場合、結果的には本来実現できるはずの成功を制限してしまうことになり兼ねません。目標とする状態を常に念頭に置いて、その実現に向けて継続的に改善に取り組むことをお勧めします。

人材

まず、人材について解説します。IT 部門の配下にある各部門、チーム、および個人は、アプリケーションとサービスの End-to-End での提供および管理を担当し、最終的には、ネットワーク仮想化およびセキュリティの運用開始を成功させる原動力となります。

組織構造に関する最初の検討事項

ネットワーク仮想化と NSX は、特別な組織がなくとも運用可能です。最適な組織構造は、企業によって異なります。NSX は、これまでサイロ化されていた組織から、さまざまなメンバーで構成される完全に連携の取れたクラウド チームにまで導入されており、厳密にサイロ化されたチームから完全な混成チームまで多岐にわたります。

理想的な組織構造はさまざまな要因で決まりますが、組織を構成する際は、次の点を考慮する必要があります。

- 部門や担当領域間の連携
- バリュー ストリームの成熟度
- 技術責任者のレベル
- スタッフの経験と専門知識
- 運用の経験と成熟度
- アウトソーシング利用の有無
- インフラストラクチャおよびアプリケーションの数量
- 既存環境への導入か、新規の導入か

VMware の推奨： 混成チーム構造の設計

実際のところ、生産性に最も優れたチームとは、緊密に連携し、協調性に優れ、自己解決力に優れたチームです。このような混成チームは、より効率的に機能することが実証されています。短いサイクルで機能し、迅速かつ詳細なフィードバックを蓄積できるため、知識を共有し、継続的に向上させることができます。チームは同じ場所で作業を行うのが理想的です。

VMware は、ドメイン （コンピューティング、ストレージ、ネットワーク、セキュリティなど） に基づくチームで構成される組織構造、および領域 （アーキテクチャ、開発と統合、運用、サポートなど） に基づくチームで構成される組織構造が成功することを確認しています。どちらの場合も、チームは物理インフラストラクチャと仮想インフラストラクチャの両方を担当します。

インフラストラクチャおよびアプリケーションを既存の企業ネットワークからクラウドに移行すると、担当者の移動も発生します。時間の経過とともに、クラウドを担当するスタッフが増えていき、既存の企業ネットワークを担当するスタッフが減っていきます。コミュニケーションやトレーニングの計画を策定し、この進化と新たなキャリア アップの機会に対する組織の理解と準備を支援することが重要です。同様に重要なこととして、組織が全体として成功するには、既存の企業ネットワークを担当しているスタッフとクラウドを担当しているスタッフの両方の貢献が不可欠だと伝える必要があります。

成果を評価する指標の共有

組織に関して、次に検討すべき重要な点は、目的、目標、指標、およびインセンティブが適切に定義された戦略を共有することです。チームはサービス指向のアプローチを採用し、ビジネス要件の定義から、SLA が保証された高品質の本番ワークロードの運用および管理まで、サービス デリバリのライフサイクル全体に共同で責任を持つ必要があります。

また、各チームは、組織にとって重要な要素に基づく、成果を評価する共通の指標を持っている必要があります。例として、市場投入までの時間、収益への影響、市場への対応速度、技術革新のペース、顧客のメリットと満足度などがあります。目標は外部に焦点を当て、ビジネスとサービス利用者を重視する必要があります。

成果を評価する指標は、チームが独自に策定し、追跡するようにします。ただし、指標は、共通の目標および目的に関連があり、それに沿ったものにします。組織の目標に沿っていることに加え、重要業績指標 （KPI） は、具体的かつ明確で、定量化および測定が可能である必要があります。KPI はシンプルなものにして、理解しやすく意味のある、基本的な数個のメトリックから測定を開始します。

KPI を選択したら、現在の状態を基準として設定し、文書化します。目標とする最終的な状態に対する進捗状況を定期的 （通常は月ごとまたは四半期ごと） に追跡し、評価します。これは、担当者や過去のパフォーマンスを批判するために行うのではなく、チームの成功と、チームがビジネスにもたらしている新たな価値を実証するために行うものだということを、チームに対して明確に示す必要があります。測定した KPI は、個人のパフォーマンスの確認と評価をより効果的かつ具体的に行い、有意義なものにするために利用することもできます。

責任の所在を明確にして積極的に行動する企業文化の確立

企業文化は、ネットワーク仮想化とセキュリティを成功させるための重要な基盤です。Software-Defined Data Center の原則を支援する文化があることが重要です。文化を変える場合、経営幹部や管理職からの指示で行うのは基本的に非常に困難です。チーム内で経験、スキル、および価値を共有することで、内部から自発的に変わっていくようにする必要があります。

成功を測定する共通の指標を確立することで、新しい文化が自然と出来上がって根付いていきます。その新しい文化の基盤は、ビジネスおよびユーザー中心の明確な目標、共有される責任とリスク、緊密な連携と協力、および相互の信頼と尊敬に基づくものになるでしょう。

チーム： セキュリティとネットワークの専門知識の連携

ネットワーク仮想化の主なメリットの 1 つは、ネットワークとセキュリティの機能を基盤となる物理ネットワーク インフラストラクチャから分離し、仮想化レイヤーで抽象化することです。この移行に伴い、次のような疑問が生じます。「ハイパーバイザーで実行される仮想ネットワークとセキュリティはどのチームが担当するのか」「ネットワーク仮想化により個人の責任はどのように変わるのか」このセクションでは、このような疑問に答えていきます。

既存のネットワークおよびセキュリティの担当者が、ネットワーク仮想化およびセキュリティを担当します。NSX は、ネットワークの専門知識を必要とするネットワークの概念とテクノロジーを基盤としています。必要な専門知識を持っているのはネットワーク チームだけです。物理ネットワークの場合と同様に、仮想ネットワークの設計、展開、および運用には、ネットワークとセキュリティの専門家が必要です。

物理ネットワークはなくなるわけではなく、これまでよりも大幅にシンプルかつ容易に管理できるようになります。物理ネットワークと論理ネットワークでチームを分けることは推奨しません。スピードと俊敏性を最大化するには、ネットワーク アーキテクト、ネットワーク エンジニア、および運用担当者が 1 つのチームに所属して、基盤となる物理ネットワークと、オーバーレイ方式の仮想ネットワークを担当する必要があります。

それでも、物理機器のラックへの設置や構成を担当するネットワーク エンジニアを配置し、別の担当者が仮想ネットワークを担当する場合もあるかもしれません。しかし、それらの担当者全員が同じチームのメンバーである必要があります。

ネットワークに関連する専門的な役割 （アーキテクト、エンジニア、運用担当者など） には、ネットワーク仮想化およびセキュリティが含まれるようになります。ネットワークおよびセキュリティ担当者のほとんどは、専門知識とスキルを強化するために新しいことを学習する必要があります。NSX では、ネットワーク サービスはハイパーバイザー レイヤーで実行されています。ネットワークの専門家は、サーバ仮想化と、それが論理ネットワーク サービスに及ぼす影響についてある程度理解している必要があります。

人材に関するベスト プラクティス： トレーニング

評価プロセスの初期段階で最も優先順位が高いのは、全員がネットワーク仮想化の原則を理解し、NSX と、NSX に関連する運用ツールと管理ツールのトレーニングを受けることです。それらのツールはクラウド エコシステムの一部です。そのために、VMware は、ハンズオン ラボ、ワークショップ、トレーニング コースなど、複数の方法を提供しています。これらのリソースは、主にサーバ仮想化の知識を持たないネットワークの専門家向けですが、ネットワーク仮想化を学習しようとしているサーバ仮想化の専門家にも適しています。また、個人がほかのチームやグループに対してベスト プラクティスを非公式に教える機会を設けるという形で、チーム内およびチーム間での知識の共有とトレーニングを目的とするプログラムを実施することもできます。

学習を促進する最善の方法の 1 つは、小規模のパイロット プロジェクトと評価を指定して開始することです。コンピューティング、ストレージ、ネットワーク、およびセキュリティにわたって、アーキテクチャ、エンジニアリング、運用など、必要となる専門的な分野をすべて含めるようにします。

複数部門が関与する小規模なチームから開始

リスクの低い取り組みとして、ネットワーク仮想化に向けて、複数部門が関与する小規模なチームから開始することも推奨します。サイロ化されたチームから混成チームに移行できる場合は、段階的に移行してください。複数部門が関与するチームには、主に 2 つのタイプがあります。最適なモデルを選択してください。

インキュベーション チーム	タイガー チーム
長期的に見て混成チームに移行できる場合は、インキュベーション チームのモデルを採用します。インキュベーション チームは、最終的には、組織構造または組織図内での常設チームとなります。また、このチームには専属のフルタイム従業員を配置してください。	長期的に見て混成チームに移行できない場合は、タイガー チームのモデルを採用します。タイガー チームは、必要に応じて結成したり解散したりします。メンバーは、公式にはほかのチームに所属したままで、タイガー チームの活動をパートタイムで行います。タイガー チームは、多くの場合、政府組織で使用されます。

複数部門が関与するチームは、通常、特定の 1 つのアプリケーション スタックか、または複数のアプリケーション スタックに対して、包括的に責任を持ちます。このチームには、コンピューティング、ストレージ、ネットワーク、およびセキュリティの専門家が必要であり、アーキテクチャ、エンジニアリング、および運用にわたる専門的なスキルが必要です。このチームは、設計、開発、テストから、導入および継続的な運用まで、すべてに対応できる必要があります （ネットワークとセキュリティに関する役割と責任の説明については付録を参照してください）。

初期チームのチェンジ エージェントの選択

初期のチームのメンバーとして、チェンジ エージェント、技術分野の専門家、エバンジェリスト、および尊敬されるリーダーを選択します。チームの一員として誰もが望む人材、人間関係の構築、コミュニケーション経路の確立、およびメンバー間の問題の発見と抑制に長けた人材、または、変化を実現させるようにほかのメンバーを促し、手本を示すことができる推進者を選択します。チームのメンバーが同じ場所にいない場合、プロジェクトの開始時に、数週間集まるようにします。

チームのメンバーは、チームの目標に沿って個人の目標を設定する必要があります。たとえば、チームのメンバーがインキュベーション チームの活動に 50 % の時間を費やす場合、個人の目標の約 50 % がインキュベーション チームの活動に該当するようにする必要があります。これは自明なことに感じられるかもしれませんが、複数部門が関与するチームの活動に費やした時間が、仕事の主要な部分としてではなく、あまり重要ではない作業のように扱われていることが実際にあります。これは、成功に向けた正しいやり方とは言えません。

ユーザーのベスト プラクティス： 予期しない事態の回避

導入の直前に予期しない事態が発生しないようにします。実際、ネットワークやセキュリティの運用担当者が加わるタイミングが遅すぎて、結果的にプロジェクトが大幅に遅れてしまった例があります。運用担当者は、ネットワーク仮想化とセキュリティが、監視、アラート、およびトラブルシューティングに与える影響を理解している必要があります。また、チームのプロセスおよびツールがどのように進化する必要があるかについては、このホワイトペーパー内で後述します。

成功と成長のチャンス

プロジェクトでネットワークとセキュリティを扱う場合、個人およびプロフェッショナルとしての可能性を説明します。インフラストラクチャの仮想化および自動化を行う場合、ネットワークおよびセキュリティ担当スタッフは、新しくて興味深いプロジェクトの作業により多くの時間を割けるようになります。より大きなメリットをビジネスにもたらす戦略的なイニシアティブに集中することができます。たとえば、VLAN、ロード バランサ、ファイアウォール ルールの構成などの定常作業ではなく、ビジネスに付加価値をもたらす新しいサービスの設計を行うことができます。ドメイン間のプロセスの自動化や、耐障害性、キャパシティ プランニング、またはその他の興味深いプロジェクトやイニシアティブの設計を行うことができます。

また、組織内のイノベーターと先進的な考えの持ち主には、ネットワークとセキュリティの変革に貢献できるチャンスがあるということを説明します。変革の推進者は、その結果からメリットを得ることができます。これは、IP ネットワークや、最近ではコンピューティングの仮想化を推進してキャリアを築いた人たちの場合と同様です。どちらの場合も、新しいスキルと知識を持つ新しいタイプの管理者が誕生しました。変革に関与することで、プロフェッショナルとしての経験を積み、労働市場でのチャンスを増やし、労働市場における自らの価値を向上させることができます。

サービスのユーザーとの積極的な関わりの促進

チームの活動を促進するには、サービスのユーザー （アプリケーション、ビジネス、インフラストラクチャの所有者など） と関わりを持ち、新しい機能について説明する方法もあります。積極的に参加してくれるように頼み、要件やフィードバックを収集します。ユーザーは、機能やユーザー使用環境の変更点を知りたいと考えています。ユーザーとの効果的な関わり方には、次の方法があります。

定期的な接点： 定期的にワークショップを開催して、最新情報を提供し、要件を確認し、フィードバックを収集します。

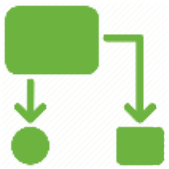
「説明するのではなく示す」： チームが定期的に新機能を開発およびリリースすることを確立し、伝達します。これによりユーザーとのやりとりが増えます。

組織内に成功を伝達することによる効果

一部のチーム メンバーおよびサービスのユーザーに対してプロジェクトを宣伝することに加え、事業部門全体または組織全体に対してプロジェクトを宣伝することも効果的です。目標は、一定数の人がプロジェクトを支援するようにして、物事を進めるための事実上の手段としてプラットフォームを確立することです。プロジェクトにおけるビジネスと IT の成果に関する興味深い話を共有します。プレゼンテーション、対話、論文、ブログ記事、ソーシャル メディア、E メール、デモを組み合わせることで、この取り組みを実行できます。チームの全員が、自分がプロジェクトのエバンジェリストであると考える必要があります。規模の大小に関わらず成功を誉めたたえることは、パフォーマンスに優れた組織の特徴です。これは、テクノロジーの変更管理における重要なベスト プラクティスです。

変化には困難が伴う： 共通の理解の特定

誰もが理解しているとおり、変化には困難が伴います。変化に時間のかかる分野や領域、変化がキャリアや生活に対して潜在的な脅威になると見なされている場所では特にそうです。これらの要因は、プロジェクトを進めていくうえで抵抗を生み出す場合があります。変革に対して、積極的に反対する人もいるかもしれません。最適なアプローチは、確実にコミュニケーションをとり、信頼できる支持を取り付け、組織の成功のために働くことを通じて、ネットワーク仮想化の可能性について、共通の理解を探ることです。率直でオープンな態度で、個人や組織のメリットについて進んで説明し、質問に答える必要があります。



プロセス

このセクションでは、ネットワーク仮想化が運用プロセスに与える影響と、既存のプロセスを分析して理解するために必要な手順について説明します。また、プロセスとツールを進化させてネットワーク仮想化およびセキュリティのメリットを最大限活用する方法を推奨します。

既存プロセスのインベントリ作成および分析

ネットワーク仮想化の主なバリュー プロポジション （価値提案） の 1 つに、アプリケーションのライフサイクルに関わる一般的に手動で行われているプロセスの自動化があります。これは、既存プロセスの総合的な評価を行い、ネットワーク仮想化によって既存のプロセスをどのように変化させるかを決定する大きなチャンスです。

重要なヒント： NSX のネットワーク仮想化とセキュリティを導入するにあたって、既存のプロセスを単純にすべて維持する必要はありません。既存のプロセスを維持すると、本来実現できたはずのメリットやコスト削減が実現できない場合があります。ネットワークとセキュリティに関する既存のすべてのプロセスを特定し、それらについて理解してください。ネットワーク仮想化が、次のプロセスに与える影響について理解してください。

- アプリケーションのプロビジョニング
- 構成管理
- 変更管理
- キャパシティ管理
- インシデントおよび問題管理

これらのプロセスが現在どのように機能しているか、全体を理解し、自動化とオーケストレーションによってどのように簡素化および効率化できるかを理解します。既存のプロセスまたは手順が大幅に効率化される場合や、プロセスが不要になる場合があります。

完全なインベントリを作成したら、これらのネットワークおよびセキュリティのプロセスを自動化する優先順位を決定します。短期間で効果を上げるには、少ない労力で大きなメリットを実現できる分野に集中することをお勧めします。一度に多数のプロセスを効率化しようとせず、まずは 1 つか 2 つを選択してください。

プロセスのベスト プラクティス： ベンチマーク

開始する前にベンチマークを実施することが重要です。プロセスの変更を行う前に、各プロセスに現在かかっている時間を、ベースラインとして記録しておきます。各プロセスに関連する作業にかかる労力およびサイクル時間を計算します。プロセスを自動化したあと、同じように測定します。そうすることで、達成した結果を比較し、伝達できます。パフォーマンスについて理解することで、チームは、目的 （プロビジョニング時間や問題を検出して分離するまでの時間の短縮など） を達成し、ユーザーのために適切な SLA を規定できます。

プロビジョニングおよび管理の自動化

現在のプロセスのインベントリを作成して評価したら、次に、アプリケーションまたはサービスのプロビジョニングおよび管理の自動化を検討します。組織は、ネットワーク仮想化および NSX の固有の自動化機能を使用して、スピード、標準化、一貫性、および監査性を実現できます。また、自動化することでダウンタイムを短縮し、手動構成によるエラーに関連するセキュリティ リスクを低減させることができます。自動化によって、開発とテストの生産性を向上させ、新しいアプリケーションの市場投入までの時間を短縮し、標準化された一貫性のある構成を提供し、エラーの数を削減して問題解決にかかる時間を短縮できます。

NSX には自動化ツールは必要ではありませんが、ほとんどのお客様はクラウドの自動化にツールと NSX API を組み合わせて使用しています。これらのツールと API を使用して、仮想ネットワーク向けの NSX の機能サービス（論理 L2 スイッチ、L3 ルーティング、ロード バランシング、ファイアウォール、および Edge サービス） のプロビジョニングおよび管理を自動化できます。NSX を使用しているほとんどの組織は、複数のサービスを自動化しています。

現在の一般的な状況： 物理ネットワークと VLAN は、現在でも、キーボードと CLI を使用して専用ハードウェアに手動でプロビジョニングされています。結果的に、アプリケーションを展開する際に、ネットワークの変更がクリティカル パスになります。ご存知のとおり、このような展開では、ネットワークの接続、パフォーマンス、可用性、およびセキュリティの準備が整うまで、数日また数週間以上かかる場合があります。

NSX による進化： 組織は NSX を使用して、ネットワーク仮想化およびセキュリティのプロビジョニング、構成、管理、および運用終了を自動化できます。NSX を使用することで、ネットワーク チームは、トラフィック ステアリングおよびネットワークの構成 （VLAN、VRF、VDC、QoS、ACL など） を伴う、多数の物理スイッチの構成を行う必要がなくなります。

基盤となる物理ネットワークの初期構成が完了したあとは、新規アプリケーションを展開したり、アプリケーションの要件が変化したりしても、ネットワークを継続的かつ頻繁に再構成する必要はありません。そのような変更はすべて、自動化ツールを使用して、論理ネットワーク領域で実行されるようになります。

プロセスのベスト プラクティス： IT の自動化への注力

VMware では、まずは IT の自動化を実現することで、サービスの要求に迅速に応えられるようにすることを推奨します。IT を自動化したあとは、セルフ サービスのポータルとサービス カタログを追加できます。それによって、アプリケーション開発者と品質管理担当のエンジニアは、ボタンを 1 つクリックするだけで、必要なものが一通りそろった環境にアクセスできるようになります。次に、NSX のお客様が使用している自動化ツールをいくつか紹介します。

ツールに関する検討事項

前述したように、初めに自動化を希望するタスクおよびプロセスを特定、理解、および文書化することが重要です。クラウド管理プラットフォームやオーケストレーション ツールなどの IT 自動化ツールは、それぞれ異なる機能を提供するため、これは重要なステップです。これらのツールはすべて、学習やセットアップのための先行投資が必要ですが、それだけの価値があります。

vRealize Suite および OpenStack を使用してネットワーク インフラストラクチャのプロビジョニング、管理、およびオーケストレーションを行うとします。初めは個別のタスクを自動化し、ツールを理解します。ツールについて学習したら、アプリケーション、ネットワーク、およびセキュリティが包括的にプロビジョニングおよび管理されるワークフローに移ることができます。ネットワークの運用担当者またはクラウド ネットワークの運用担当者は、ネットワーク自動化を促進するツールの評価および運用に関わる必要があります。

構成の標準化とカスタマイズ

組織は、テンプレートとポリシーを使用して、完全なアプリケーション スタックのコンピューティング、ストレージ、ネットワーク、およびセキュリティの構成を標準化できます。変更する必要がある場合は、テンプレートを修正して本番環境に適用します。そのテンプレートを使用しているすべてのワークロードには、変更が自動的に反映されます。監査とコンプライアンスのために、すべての変更の記録が維持されます。

設計によっては、静的な構成やカスタマイズ可能な構成を発行できます。静的な環境は、通常、本番環境での使用が認定されたスタック向けに使用されます。また、カスタマイズ可能な環境は、開発およびテスト用のサンドボックス環境向けです。カスタマイズ可能な環境は、ユーザーの要件の 80 % 以上に対応する場合もありますが、開発者または品質管理担当のエンジニアによって、必要に応じて変更されることがあります。ワークロードは、新しいネットワークを備えて起動するか、既存のネットワークに接続できます。

ブループリント プロセスの自動化の例

次に、標準化された 3 層アプリケーションのブループリント用に自動化できるタスクについて説明します。

ブループリントのテストと検証が終わったら、ユーザーが使用できるようにサービス カタログに発行されます。ユーザーがサービス アイテムをクリックすると、すべての接続、可用性、セキュリティを備えたアプリケーション スタック全体が数秒で展開されます。

この自動化されたサービスは、NSX を使用しない従来の物理ネットワークの何倍もの速さを実現します。従来は、ネットワークの展開に通常数日から数週間かかっていました。組織は、チケット発行を伴う複雑なワークフローによる長い作業時間と遅延、変更の確認と承認、冗長な要件の検出と検証、および手動構成を回避できます。

プロセスのベスト プラクティス： ロール ベースのアクセス

セルフ サービス ポータルへの役職に基づくロール ベースのアクセス制御を実装します。また、ビジネス グループに従ってリソースの予約と割り当てのポリシーを定義し、チャージバックのコストを追跡し、サービス レベル アグリーメント （SLA） を保証する必要があります。

グループによるセキュリティ ポリシーの自動化

NSX は、物理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では手動で行うタスクの多くをネイティブに自動化します。たとえば、NSX は、セキュリティ ポリシーを定義し、仮想化レイヤーの仮想マシンに適用する新しい方法を提供します。

従来のアプローチ： 従来は、セキュリティ チームは、IP アドレス、ポート、およびプロトコルに基づいて、手動でルールを作成していました。非常に面倒な 「5 タプル」 情報による管理です。

新しいアプローチ： 新しい方法では、セキュリティ ポリシーはセキュリティ グループに基づきます。仮想マシンのセットで構成されるセキュリティ グループを作成し、それらのワークロードに対してセキュリティ ポリシーを作成できます。グループに別の仮想マシンを追加する場合は、手作業なしで、新しいワークロードにセキュリティ ポリシーが自動的に適用されます。グループのメンバーシップは、セキュリティ タグまたはコンテキストを使用して動的に適用できます。NSX のセキュリティ ポリシーは、ファイアウォール、アンチウイルス、IPS などを含む場合があります。

セキュリティ グループは、動的または静的に設定できます。ワークロードに関する任意のメタデータがトリガとなるようにプログラミングできます。たとえば、ユーザー グループの ID、OS の特性、仮想マシンの名前とタグ、ウイルスの有無などの情報です。NSX は、物理トポロジーだけでなく、仮想化に関連するコンテキストに基づいて、適切なセキュリティ グループとポリシーを自動的に割り当てます。

事前に承認されたセキュリティ ポリシーは一元的にオーケストレーションおよび管理されるため、ルールの無秩序な拡大を抑制できるうえ、セキュリティが正確に一貫して適用されるようになります。このような新しいレベルの自動化によって、運用の複雑さと、ワークロード全体のセキュリティ ポリシーの管理にかかるコストが大幅に低下します。

多くのセキュリティ部門が、ネットワーク セキュリティ アプライアンスを独自に組み合わせて、それぞれの環境のニーズに対応しています。NSX の分散ファイアウォール機能に加え、組織は、NSX プラットフォームを活用して、VMware テクノロジー パートナーが提供する高度なネットワーク セキュリティ機能を自動化する必要があります。

ネットワーク セキュリティ部門では、複数のベンダーが提供する、まったく関連のないネットワーク セキュリティ サービスの連携が課題になることがありますが、NSX はこれを実現できます。NSX は、ネットワーク サービスを仮想 NIC のコンテキストに配信して、仮想ネットワーク トラフィックに適用するサービスの論理的なパイプラインを確立します。この論理パイプラインには、サードパーティ製のネットワーク サービスを適用できるので、物理サービスまたは仮想サービスの使用が可能です。企業は、NSX を使用して、NSX サービスの適用、連結、運用を利用するポリシーを作成できます。この機能によって、論理パイプラインでサービスを実行できます。

また、統合セキュリティ ツールは、NSX プラットフォームが提供する運用モデルからメリットを得ることができます。この統合によって、サーバ、ネットワーク、およびセキュリティ チームの業務の分離を維持しながら、プロビジョニングのスピード、管理効率、およびサービス品質を大幅に向上させることができます。

高度なセキュリティ機能は、Palo Alto Networks 社、Intel Security 社、Trend Micro 社、Symantec 社、Checkpoint 社などの VMware NSX パートナーとの連携を通じて利用できます。

最新ツールによるアプリケーション レベルの詳細情報の作成

ハイパーバイザーは、物理環境と仮想環境の境界という独自の理想的な場所に配置されています。NSX の仮想スイッチは、仮想マシンが送受信するすべてのパケットを認識するため、最高レベルの視認性とコンテキストを提供します。また、アプリケーション、仮想ネットワーク、物理ネットワークなどの間の流動的な関係に対して関連付けを行うこともできます。

NSX の独自の監視機能とトラブルシューティング機能を実証するシナリオの例を次に示します。

リアルタイムの概要	監視とトラブルシューティング	デバッグ
運用担当者は、任意の仮想マシンのネットワーク インターフェイスを選択し、すべてのフローと状態のリアルタイムの概要を確認できます。リモート ツールに完全なパケット キャプチャを構成し、仮想マシンの IP アドレスをさがす必要はありません。	NSX の統合 CLI および統合 API を利用すると、仮想ネットワークのあらゆる側面を把握できます。これにより、ネットワーク内のどこに問題があるか確認する必要がなくなるため、監視およびトラブルシューティングの作業が大幅に簡素化されます。さらに、トラブルシューティングを実行するために別のコンソールに切り替える必要がありません。	すべてのパケットが、仮想スイッチによってソフトウェアで処理されるため、従来のネットワークよりも視認性が向上します。ゲスト仮想マシンにアクセスできなくても、合成トランザクションを作成することができます。Traceflow のパケットを転送用パイプラインに追加して、データ パス内の問題 （過剰に制約の強い ACL ポリシーなど） をきめ細かにデバッグできます。

運用担当者は、データセンターのインフラストラクチャの管理とサポートのために、以前から多くのツールを使用しており、監視、トラブルシューティング、および変更管理の作業に、別々のツールを使用しています。ネットワークを仮想化すると、既存のツール セットと同じものを使用して、論理ネットワークの詳細な情報を確認できます。

仮想環境は絶えず変化しており、インフラストラクチャとアプリケーションがサーバ間で動的に移動し、ネットワークが自動的に再構成されます。そのため、仮想環境では、リアルタイムの監視ツールが重要です。

プロセスのベスト プラクティス： ツール

仮想環境と物理環境のコンピューティング、ストレージ、およびネットワーク インフラストラクチャ間のオブジェクトの関係を詳細に確認できる、VMware またはサードパーティ製のツールを特定します。インフラストラクチャ ドメイン間で関連付けを行うと、問題の範囲を特定のドメインに迅速に狭めることができるので、ドメイン固有の複数のツールを使用する必要性が低減します。

通常、vRealize Operations、Arkin、Riverbed などの最新のツールを使用することが最適な選択肢です。これらのツールは仮想環境および物理環境向けに設計されています。これらのツールでは、トポロジー、アプリケーションの健全性、使用率、およびキャパシティを End-to-End で確認できます。

単一のベンダーを使用することで最適な視認性を得られるとはかぎりません。現在の物理ネットワークのように、最適な監視、アラート、およびトラブルシューティングを実現するために複数のツールを使用することが適している場合もあります。たとえば、トラフィック フロー分析 （SolarWinds、NetQoS など）、パケット分析 （Wireshark、SteelCentral など）、アラート （Netcool、OpenNMS） に、それぞれ異なるツールを使用しているかもしれません。

仮想ネットワークでは、標準的なプロトコル （SNMP と API、SPAN / L3 SPAN、NetFlow / IPFIX、ポート ミラーリング、Syslog を通じたパケットとバイト数の統計情報など） 経由で、物理ネットワークと同レベルのインストルメンテーションを提供します。これにより、組織は、監視、アラート、およびトラブルシューティング用の既存のツールをまず使用し、その後、前述のものを含む最新ツールに移行できます。

プロセスのまとめ

ネットワーク仮想化と NSX により、現在の環境を評価し、先へ進むための、効率的で優れた方法を定義することができます。すべてのプロセスを見直すのは困難です。身動きが取れない状況にならないように、プロセスを段階的に自動化していきましょう。無駄なく継続的に改善していく手法は、前進するためのすばらしい方法です。

テクノロジー

このセクションでは、ネットワーク仮想化および NSX を計画、導入、および運用開始する際の、アーキテクチャおよびインフラストラクチャに関する検討事項について説明します。マイクロセグメンテーションおよびディザスタ リカバリについての実用的な事例についても説明します。

シンプルな物理ネットワークの設計

NSX では、物理ネットワーク アーキテクチャは接続性とパフォーマンスについて設計するだけです。現在すでに使用している L2 ファブリック、または Leaf-Spine アーキテクチャに基づく L3 ファブリックのようにシンプルです。初めは前者を使用し、その後、後者に移行していきましょう。

NSX では、L2 の境界の場所に関する厳しい要件はありません。物理ネットワークに対する構成変更は、ホスト間の接続性を提供するだけなので、あまり頻繁には発生しません。そのため、手作業による構成ミスを避けることができます。

ネットワークのサービスとトポロジーを物理ハードウェアから分離することで、L3 Spine-Leaf ファブリックを広範囲に使用できるようになりました。これにより、同じ論理ネットワーク、セキュリティ、および管理モデルを持つ共通のプラットフォームを構築できます。

仮想マシンのように仮想ネットワーク トポロジーを物理トポロジーから抽象化することで、NSX は、ネットワーク アーキテクチャの変更をより実現しやすくしました。NSX を利用すると、ネットワークの設計者は、Top-of-Rack スイッチ間でノンブロッキング ECMP を利用して L3 ルーティングを行う Spine-Leaf アーキテクチャに容易に移行できます。

基盤となる物理ネットワークは、仮想ネットワークとは独立して進化します。物理ネットワークのアーキテクチャは、スケーラビリティ、スループット、および堅牢性を基準として設計されます。単一のデバイスまたはリンクの障害は、アプリケーションの接続性に影響を与えません。

ECMP L3 ファブリックの設計では、構成が均一になり、デバイスの相互運用性が向上します。ハードウェアのアップグレード （新しいスイッチの展開など） は、NSX から分離できます。これにより、仮想ネットワークで実行中のワークロードに対する影響を回避できます。NSX は任意のベンダーのスイッチをサポートします。各スイッチは相互接続が可能です。

ネットワーク仮想化オーバーレイと Spine-Leaf アーキテクチャを組み合わせると、耐障害性と運用効率を向上させ、帯域幅をより効率的に使用し、データセンター内の増え続ける East-West 通信を処理するための拡張性を実現することができます。一方で、L2 ブロードキャスト ドメインの範囲が狭くなり、ネットワークの安定性が向上します。

ネットワーク仮想化の段階的な実装

NSX によるネットワーク仮想化は、二者択一を迫るものではありません。NSX の仮想ネットワークでは、基盤となる物理ネットワークを変更する必要はありません。ネットワーク仮想化は、物理ネットワーク上に展開された既存のアプリケーションと、透過的に共存できます。

IT 組織は、ハイパーバイザー ノードを NSX プラットフォームに追加するだけでネットワークを部分的に仮想化できる柔軟性が得られます。また、NSX のソフトウェア ゲートウェイまたは Top-of-Rack スイッチ （VMware パートナーが提供するハードウェア） を使用すると、仮想ネットワークと物理ネットワークをシームレスに相互接続できるようになります。ゲートウェイを使用することで、仮想ネットワークに接続しているワークロードのインターネット アクセスをサポートしたり、レガシー VLAN やベアメタル ワークロードを仮想ネットワークに直接接続したりすることができます。

テクノロジーのベスト プラクティス： 単一のプロジェクトでの開始

ネットワーク仮想化とセキュリティは段階的に導入する必要があります。単一のユースケースとアプリケーションのセットを対象に開始することを推奨します。リスクとメリットの面で新しい機能の利用に適したワークロードを特定してください。最初の実装では、リスクは低いが、環境内で NSX を検証するのに十分な複雑性を有するワークロードを選択します。

実装するユースケースによって、仮想ネットワークで自動化する NSX の機能サービスの大部分が決まります。たとえば、ネットワークのプロビジョニングを自動化する場合、論理 L2 スイッチ、L3 ルーティング、および Edge サービスから始める場合があります。マイクロ セグメンテーションを実装する場合、論理ファイアウォールから始めます。

NSX の新しい機能をお客様の環境に継続的に導入するための戦略と方法を定義します。事業部門にわかるように一定の間隔で導入し、事業部門がプロジェクトを進めるうえで導入のタイミングを把握できるようにします。定期的に機能をリリースすることで、ユーザーがより使用するようになり、サービスが浸透し、ユーザーの満足度が向上します。意図的に広く普及させようとするのではなく、サービスが自然に利用されるようにします。

テクノロジーのベスト プラクティス： ワークショップ

組織内の事業部門および技術部門と連携し続けることは、ネットワーク仮想化などの取り組みを成功に導くためのいい方法です。ユーザーが参加する定期的なワークショップを開催し、ネットワーク仮想化およびセキュリティの利用可能なサービスについて関係者に情報を提供して教育し、ロードマップの計画についても最新情報を知らせることを検討してください。アプリケーションとインフラストラクチャの所有者に協力を要請し、将来のリリースの要件と、すでに本番環境で利用できる機能のフィードバックを伝えてもらうようにします。

ユースケース： アプリケーションの境界に従ったセグメント

NSX のお客様のほとんどが早期に実装して運用を開始している主なユースケースの 1 つは、マイクロ セグメンテーションです。マイクロ セグメンテーションは、長年にわたって、セキュリティ アーキテクチャのベスト プラクティスと考えられてきました。攻撃者がネットワークに不正にアクセスすると、セグメント化によって攻撃者の動作を制限し、データ侵害を防ぐことができます。ただし、マイクロ セグメンテーションは、これまで広く普及してきたわけではありません。これは、従来の物理ネットワークにはアーキテクチャ上の制限があり、マイクロ セグメンテーションを利用するのが困難であったためです。

NSX は、ネイティブな分離とセグメント化の機能を提供して、マイクロ セグメンテーションを運用上実現可能にします。高度なサービスを挿入し、サードパーティ製セキュリティ アプライアンスで NSX の運用モデルを活用できるようにします。

分離は、ほとんどのネットワーク セキュリティの基盤です。コンプライアンスや封じ込めのため、または開発環境、テスト環境、本番環境の相互作用を防ぐために分離を行います。仮想ネットワークは、明示的に相互接続しないかぎり、デフォルトでほかの仮想ネットワークや基盤となる物理ネットワークから分離されています。運用担当者は、物理サブネット、VLAN、ACL、およびファイアウォール ルールを取り扱う必要はありません。

分離に関連して、マルチ ティア仮想ネットワーク内で各階層に適用されるのがセグメント化です。従来、ネットワークのセグメント化は、物理ファイアウォールまたはルータの機能であり、ネットワーク セグメントやネットワーク階層の間でトラフィックを許可または拒否するためのものでした。たとえば、ルータおよびファイアウォールは、Web 層、アプリケーション層、およびデータベース層の間でのトラフィックをセグメント化します。

現在の課題： セグメント化を構成するための従来のプロセスは時間のかかる手作業で、人的ミスが発生しやすく、結果的にセキュリティ侵害につながる可能性があります。実装には、デバイス構成の構文、ネットワークのアドレス設定、アプリケーション ポート、およびプロトコルに関する、詳細な専門知識が必要です。

ネットワーク仮想化ソリューション： NSX では、仮想化レイヤーにセキュリティ ポリシーが適用されます。East-West トラフィックを迂回させるためにさまざまな手段をとる必要がなくなります。パケットが最初の仮想ネットワーク ポートに到着する前に、セキュリティが透過的に適用されます。最初から保護されているため、遅延の影響を受けやすい East-West トラフィックは、遅延を最小に抑えるパスで宛先に直接送信されます。

統合管理とサービスの分散型の実装を組み合わせることで、非常に詳細なポリシーを、実際に運用可能な形ですべての仮想インターフェイスに適用できます。たとえば、3 層アプリケーションの同じ階層にある仮想マシンが、ほかの階層の仮想マシンと通信することはできるが同じ階層内の仮想マシンとは通信できないようにすることもできます。実際には、各ワークロードは、それぞれのセキュリティ ポリシーでラッピングされます。

NSX では、インフラストラクチャの低レベルの構成要素 （IP アドレス、アプリケーション ポート、プロトコルなど）ではなく、ビジネスの高レベルの構成要素 （アプリケーション、ユーザー、グループなど） に基づいてセキュリティ ポリシーを設定できます。セキュリティ ポリシーは、人間による解釈を介在させずに、より正確に企業のポリシーに合わせて適用できます。

ワークロードの可搬性と復元性のための設計

従来の物理ネットワーク トポロジーとアドレス空間では、アプリケーションが移動したときに IT 部門が IP アドレスを変更する必要があります。場合によっては、IP アドレスがアプリケーションにハードコーディングされており、コードの変更と回帰テストが必要になるため、さらにコストが高くなります。

NSX では、ワークロードが VLAN と IP アドレスから切り離されます。また、データセンター ファブリックでワークロードの可搬性と配置が制限されることはありません。NSX を使用すると、ワークロードの配置は、物理トポロジーと、特定の場所で物理ネットワーク サービスが利用可能であるかどうかに依存しません。

ネットワークの観点から仮想マシンに必要なものは、その物理的な場所を問わず、すべて NSX から提供されます。ワークロードは、運用担当者が IP アドレスを再割り当てする必要なく、サブネット、アベイラビリティ ゾーン、またはデータセンター間を自由に移動できます。ワークロードが移動すると、ワークロードのすべてのネットワーク サービスとセキュリティ サービスも合わせて自動的に移動します。人的操作は不要です。

組織は、NSX のワークロードの可搬性と配置を利用して次のことができます。

- アプリケーションの迅速なプロビジョニング
- 新しいデータセンターへのワークロードの移行
- 基盤となる物理インフラストラクチャの更新

ユースケース： ネットワーク仮想化によるサーバ リソース使用率の向上

組織は、NSX を使用して、データセンター内の別の場所または別のデータセンターで利用できるサーバ キャパシティにアクセスすることもできます。これにより、サーバのリソース使用率と統合率を大幅に向上できます。これらのユースケースはすべて、運用コストを大幅に削減し、俊敏性を向上させます。また、ネットワーク仮想化と NSX への投資の全体的なメリットを向上させます。

従来のネットワーク トポロジーでは、各クラスタまたはポッドに専用のサーバ キャパシティが割り当てられます。別のポッドやクラスタからアクセスするためにネットワークを再構成するには時間がかかりすぎ、人的エラーも発生しやすくなります。そのため、利用できるサーバ キャパシティが無駄になってしまいます。このような、容易に利用できないサーバ キャパシティのことを 「ダーク サーバ キャパシティ」 と呼ぶことがあります。実際には、従来のネットワーク トポロジーおよび機器が複雑であるため、利用可能なサーバ キャパシティを IT 組織が効率的に使用する能力が制限されます。

NSX を利用すると、ネットワークを拡張して、利用可能なキャパシティがデータセンターのどこにあってもアクセスできるようになります。既存の物理インフラストラクチャに手を加える必要はありません。たとえば、別のサブネットやアベイラビリティ ゾーンにあるサーバに仮想マシンを 1 台追加したい場合、仮想マシンを起動して論理スイッチに接続するだけです。それらの 2 つのワークロードは、物理ネットワーク上の複数のサブネットおよびアベイラビリティ ゾーンにわたっていても、L2 の隣接関係を持ちます。

ユースケース： ディザスタ リカバリ

NSX を使用して、既存のディザスタ リカバリ ソリューションを補完できます。ネットワークに対する従来のアプローチでは、ディザスタ リカバリ用のバックアップ サイトを利用するには、コストと機能の折り合いを付ける必要がありました。多くの組織は、ネットワークのトポロジーとサービスをセカンダリ サイトに忠実に再現するよりも、「必要最低限」 のソリューションを選択しています。コストを削減するために、プライマリ データセンターと比べて機能が制限されることを受け入れているのが実情です。

NSX では、妥協のないディザスタ リカバリを実現できます。仮想マシンのスナップショットを取得するだけではなく、NSX は、ネットワークおよびセキュリティを含む、アプリケーション アーキテクチャ全体のスナップショットを取得します。スナップショットのコピーをスタンバイ状態のディザスタ リカバリ サイトに送信することができます。ディザスタ リカバリ サイトでは任意のハードウェアを使用することができ、機能が制限されることはありません。

災害が発生した場合も、仮想マシンを起動するだけです。接続するネットワークは、リカバリ サイトですでに実行されています。ワークロードおよびセキュリティ アプライアンスに新しい IP アドレスを再構成する必要がないため、目標復旧時間 （RTO） を大幅に短縮できます。

テクノロジーに関する検討事項のまとめ

ネットワーク仮想化と NSX は、既存のテクノロジー環境に、非常に大きな柔軟性を新たにもたらします。それによって、複数の有益なユースケースを実現できるようになります。あらゆる可能性を試して対応しきれない状態になるのではなく、まずはサービス品質に集中し、最初のユースケースの導入範囲を拡大していきます。それから、2 番目のユースケースを選択して運用を開始します。チームのメンバーやユーザーが品質レベルに満足してから、新しい機能を提供するようにします。

次のステップ

ネットワーク仮想化およびセキュリティの運用を開始することは、一連のプロセスと考える必要があります。このプロセスでは、組織の Software-Defined Data Center への移行が進み、ビジネスに対する価値が大きくなるにつれて、成熟度が増し、洗練されていきます。

組織と個々のチーム メンバーは、ネットワーク仮想化と NSX がもたらす運用上のメリットを最大限実現する方法と、IT 部門のほかのメンバーにどのようにメリットをもたらすかという点について、さまざまな方法で学習することができます。

ステップ 1： 学習機会の提供

初めに行う必要があるのは、組織と個人に対して学習の機会を提供することです。正式なもの （ワークショップ、トレーニング コース、ハンズオン ラボ、プログラムなど） や気軽な雰囲気のもの （ランチ セミナー、コーチング、メンター制度など） など、さまざまな種類の教育やトレーニングを組み合わせて利用できます。学習の動機付けとして、トレーニングや学習の目標を個人の目標に含める方法を検討します。

初めに、チームは VMware のハンズオン ラボ （labs.hol.vmware.com） や、VMware の教育サービス （vmware.com/jp/education） を通じて利用できる、インストラクターが指導するワークショップおよびトレーニング コースに参加できます。また、VMware では、監視とトラブルシューティングに焦点を当てた、NSX の運用ガイドも提供しています。

ステップ 2： 変革サービスの採用

外部の視点でネットワーク仮想化および NSX への移行を確認することで、プロセスにかかる時間を大幅に短縮できます。VMware は、運用変革サービスおよびワークショップ （vmware.com/jp/consulting） を提供しています。たとえば、サービスとしてのネットワーク （NaaS） の計画は、新しいネットワークおよびセキュリティの運用モデルのビジョン、目標、および目的を明確に特定するのに役立ちます。NaaS の調査は、新しい運用モデルを実現して期待する目標や成果を達成するために強化または作成する必要がある、運用機能および組織の能力を特定するのに役立ちます。

ステップ 3： シンプルなパイロット プロジェクトの実施

NSX とその運用開始方法について学習する優れた方法の 1 つは、単一のユースケースといくつかのワークロードを使用して、本番環境でパイロット プロジェクトを実施することです。比較的リスクが低く、NSX の運用開始について学習した成果を最大化できる程度の複雑性を持つワークロードを選択します。

まずは、VMware またはパートナーの営業担当者にお問い合わせください。

付録

最終的なパフォーマンス特性

次の表に、ユーザー、プロセス、およびテクノロジーについて、NSX の導入完了時点での特性をまとめています。お客様の計画に合わせてガイドとしてご使用ください。

項目	現在 / 開始時の状態	将来 / 最終的な状態
組織構造	• 厳格な境界でサイロ化され、負荷の高いプロセスが必要 • 正式なリクエストの手順 • グループ間のコミュニケーション不足 • グループ間の責任の押し付け合い • グループごとに目標、目的、およびインセンティブが異なる	• グループ間でも即座のやりとりが可能 • オープンなコミュニケーション • 迅速なフィードバック ループ • 協調性に優れている • 目標および KPI の共有 • リスクおよび責任の共有
人材	• 専門分野に特化 • 特定のドメインに限定された専門知識 • CLI およびスクリプトの使用 • 広く普及している知識 • 限定的なキャリア パス • ハードウェア インフラストラクチャ中心	• 複数のドメイン、複数の分野に精通 • 複数ドメインの専門知識 • API および自動化ツールの使用 • 継続的な学習 • 戦略的プロジェクトでビジネスに影響を与えるチャンス • サービスおよびアプリケーション中心
プロセス	• 手作業であり、ミスが発生しやすい • 煩雑なチケット システム • 調整と引き継ぎ • 複雑さとボトルネック • サービスが開始されるまで待つ必要がある • 高い運用コスト • インフラストラクチャ中心	• 自動化、標準化、一貫性、および監査性 • 手作業によるミスのリスクが低い • 対応時間が短い / SLA を設定 • リアルタイムのやりとり • 運用コストの削減 • サービスまたはアプリケーション中心
ツール	• レガシー、ドメイン固有 • サイロ化され、複数のツールを使用 • 物理環境のみに対応したインストルメンテーション • インフラストラクチャ中心 • サービスの問題の分離が困難 • コンポーネントごとの CLI	• ドメイン間の最新のツール • 仮想環境および物理環境向けに設計されたインストルメンテーション • アプリケーション中心 • インフラストラクチャおよびサービスの統合監視 • サービスの問題の分離が容易 • インフラストラクチャのインストルメンテーション用の統合 CLI および API

項目	現在 / 開始時の状態	将来 / 最終的な状態
アーキテクチャ	• 従来の 3 層アーキテクチャの制限 • ワークロードによる制約 • ボトルネックとなるファイアウォール • オーバーサブスクライブ状態のコア • リンクのパフォーマンス • 場所に制限された統合サービス	• ノンブロッキング ECMP を利用する Spine-Leaf ファブリック • 分離と抽象化によるオーバーレイ • ワークロードの可搬性 • ネイティブの分離とセグメント化 • 拡張性と対障害性 • 分散サービス
インフラストラクチャ	• 物理インフラストラクチャを基盤とし、変更に時間がかかる • インフラストラクチャに縛られたセキュリティ • 機能に制限のある 「必要最低限」 のディザスタ リカバリ • ポリシーを人間が解釈 • インフラストラクチャ中心のポリシー • インフラストラクチャの低レベルの構成要素を利用 • 分断化された管理 • ハードウェア ベンダーによる囲い込み • サービス チェーン機能の実行が困難	• オーバーレイ方式の仮想インフラストラクチャ、動的に変更可能 • アプリケーション中心のセキュリティ • 妥協のないディザスタ リカバリ • 機械が読み取れるセキュリティ ポリシー • ビジネス中心のポリシー • ビジネスの高レベルの構成要素を利用 • 統合管理 • 価格性能比が優れた選択肢 • サービス チェーン機能の実行が容易

クラウドのネットワークとセキュリティに関する役割

次の説明は、クラウドのネットワークおよびセキュリティ担当スタッフの役割と責任を定義するうえで役立ちます。クラウドにおけるこれらの役割は、すでにチームにいる、「従来の」 ネットワークおよびセキュリティの専門家が担います。

中堅・中小企業では、1 人の担当者がこれらの複数の役割を担当することも一般的です。たとえば、1 人のネットワーク エンジニアがネットワークのアーキテクチャ、開発、運用の責任者になる場合もあります。すべての企業が、これらの各役割に異なる担当者を割り当てる必要はありません。

一方で、大規模企業では、同一または類似の役割に複数の担当者を割り当てることも一般的です。たとえば、複数のクラウド ネットワーク アーキテクトまたはクラウド ネットワーク エンジニアがいる多国籍企業も多数あります。

クラウドのネットワークに関する役割

クラウド ネットワーク アーキテクト （CNA） は、End-to-End のクラウド ネットワーク アーキテクチャおよびサービス ベースの利用モデル （サービスとしてのネットワーク） に従った標準の開発を担当します。CNA には次の役割があります。

- 技術上および運用上のネットワークの要件を決定する
- アプリケーションの要件 （キャパシティ、パフォーマンスなど） に対応する物理ネットワークおよび論理ネットワークを設計する
- 開発、検証、テストを行い、要件に対応していることを確認する
- クラウド ネットワーク ソリューションの計画と実装を主導する

クラウド ネットワーク エンジニア （CNE） は、ネットワーク サービスおよびインフラストラクチャの詳細な設計、ネットワーク機能の開発およびテスト、キャパシティのプロビジョニング、およびネットワーク構成の定義を担当します。CNE には次の役割があります。

- 利用者の要件と関連するサービス レベルを達成する
- 要件を論理的なブループリントと構成のテンプレートに変換する
- 定常作業 （連携、展開、監視、コンプライアンスなど） 用に、カスタムのワークフローとスクリプトを設計、開発、およびテストする
- トラブルシューティングを支援してレベル 2 およびレベル 3 のサポートを提供し、解決策を提案し、修正をリクエストする

クラウド ネットワーク オペレータ （CNO） は、導入後の運用、アプリケーションの運用上の要件 （パフォーマンス、キャパシティなど） の実現、およびクラウド ネットワーク インフラストラクチャ、ツール、プラットフォームの維持に関して、すべての側面を包括的に担当します。CNO には次の役割があります。

- プロビジョニング、管理、監視、アラート、およびトラブルシューティングの自動化を実行および制御する
- クラウド ネットワーク インフラストラクチャをプロアクティブに監視し、サービスに影響が及ぶ前に対応する
- トラブルシューティングと根本原因分析を行い、CNE が提案する解決策と修正を適用する
- レベル 2 およびレベル 3 サポートを提供し、インシデント、問題、およびエスカレーションを管理する

クラウドのセキュリティに関する役割

クラウド セキュリティ アーキテクト （CSA） は、クラウド セキュリティ インフラストラクチャの設計およびサポートに関するすべての側面を包括的に担当します。対象は、ネットワーク セキュリティの仮想化、自動化、オーケストレーション、および監視の全体にわたります。CSA には次の役割があります。

- クラウド インフラストラクチャおよびアプリケーションのセキュリティ リスクを評価し、セキュリティ戦略およびセキュリティ ソリューションに関する正式なガイダンスを提供する
- クラウドのセキュリティ要件および目標に対応するために必要な技術上のセキュリティ ポリシー、プロセス、および監査機能を決定する
- クラウド セキュリティ ソリューションを検証するための検証テストを開発し、それらを実装するための計画およびガイドを提供する
- 脅威およびリスクを低減する戦略に関する包括的な知識を維持管理する

クラウド セキュリティ エンジニア （CSE） は、セキュリティ ポリシーを監査可能なセキュリティ制御に変換することを担当します。CSE には次の役割があります。

- クラウドのセキュリティ制御を実現する物理ソリューションおよび論理ソリューションを設計および実装する
- クラウドのセキュリティ プロセス （制御、監視、および監査） のオーケストレーションおよび自動化を実行する
- 要件およびサービス レベルを達成するクラウドのセキュリティ サービスとツールを統合および実装する
- エスカレーションに対応し、セキュリティ侵害を調査し、修正ソリューションを推奨および実装する

クラウド セキュリティ オペレータ （CSO） は、組織のポリシーおよびリスク評価に必要とされる特定のセキュリティ制御の理解、実装、適用、検証、および維持を担当します。CSO には次の役割があります。

- セキュリティ上の異常、脆弱性、脅威を監視、検出、および分析する
- セキュリティ ログを管理し、標準的なログでコンプライアンスを確保し、セキュリティ監査を支援する
- インシデントが発生した際に、クラウド セキュリティの問題を調査、診断、および解決する
- セキュリティ ソリューションを実装し、脆弱性を修正する

ヴイエムウェア株式会社 〒105-0013 東京都港区浜松町1-30-5 浜松町スクエア 13F www.vmware.com/jp