ソリューションノート

TRINZIC X6 が、ハイブリッド、マルチクラウドネットワークにおける自動化、セキュリティ、稼働時間の課題を解決

NIOS 9.0.1

クラウドネットワークの利点が、ほぼすべての業界の組織を従来の物理的データセンターからハイブリッドおよびマルチクラウド環境へのデータプラットフォームやアプリケーションの移行へと導いています。

アプリケーションの稼働時間、弾力性、災害復旧、ワークフローの自動化、スケーラビリティ、アジリティ、そして潜在的なITコストにおける利点は、緊急ではなかったとしても、ビジネスインフラストラクチャを近代化する上で説得力のある理由の一つです。しかし、ハイブリッドおよびマルチクラウドへの移行の過程で、組織は職場の近代化の取り組みやクラウドの利点の達成を遅らせたり、さらには停滞させたりする無数の課題に直面します。統合ネットワークおよびセキュリティサービスのリーダーとして、Infoblox はこれらの課題を予測し、世界をリードする企業と協力して、クラウド移行の主要な障害を簡素化し解決するためのソリューションを理解・開発してきました。Infoblox は、NIOS 9.0.1 と Trinzic X6、Infoblox の専用物理およびソフトウェア・アプライアンス・プラットフォームを使用して、企業が一般的な落とし穴を回避し、クラウドの利点をより早く実現し、より優れた堅牢なソリューションを導入して、価値実現までの時間を短縮できるよう支援します。

ビジネスの課題

NIOS 9.0.1 では、Infoblox は、Trinzic X6 プラットフォームの一部として、3つのコスト削減を可能にする「サイト全体」ライセンス（以前は別売り）を含めることで、頻繁に発生するビジネス課題を解決し、職場の近代化を実現します。これには、クラウドプラットフォーム（CP）API 自動化、DNS ファイアウォール（DFW）、およびDNS トラフィックコントロール（DTC）によるグローバルサーバー負荷分散が含まれます。これらのソリューションは、サイロ化やマルチクラウド環境全体でワークロードの自動化と可用性を拡張し、レスポンスポリシーゾーン（RPZ）を活用して悪意のあるネットワークIPやドメインからのDNS解決をブロックすることにより、エッジで企業を保護します。また、遅延を排除し、災害復旧を実現することで、アプリケーションの稼働率とユーザーエクスペリエンスの向上といったビジネス上の課題に対応します。このソリューションノートでは、主なユースケース、ソリューションの仕組み、ハイブリッドなマルチクラウド環境における潜在的な優位性など、それぞれの特徴と機能を個別に検証します。

Trinzic X6 は、Cloud Platform（CP）API 自動化、DNS Firewall（DFW）、DNS Traffic Control（DTC）グローバルサーバー負荷分散の「サイト全体」ライセンスを含めることで、差し迫ったクラウド近代化の課題を解決します。

クラウドプラットフォーム（CP）自動化のためのAPI

使用例

- API DDI 自動化を拡張する
- API 呼び出しのバックホールを回避する
- DDIをマルチクラウド環境に拡張する
- ネットワークおよびクラウドチームのアクセス制御を簡素化する
- ネットワーク運用の複雑さを軽減する
- コストを削減し、強力な ROI を達成する

メリット

- **分散 API 処理：**CP ライセンスは DDI のパフォーマンスを向上させ、API の負荷をローカルに分散します。
- **委任管理とマルチテナンシー：**管理者は、特定のクラウドまたは自動化プロジェクトによるプログラム管理のために DDI オ

クラウドプラットフォーム（CP）自動化のためのAPI

クラウド環境における DDI インフラストラクチャの拡張と自動化

企業がクラウド導入を採用するにつれて、オーケストレーションと自動化の機能が重要になります。Infoblox CP API ライセンスは、API 処理を分散し、API 呼び出しと DNS/DHCP プロトコルサービスを各データセンターまたはクラウド環境にローカルに保つことで、データセンター展開のスケーラビリティと回復力を向上させます。このようなローカル展開（分散配置）により、企業は現在の分散型クラウド導入のニーズを最適化し、将来の導入トポロジーを現実化するアーキテクチャを用いて重要なネットワークサービスを拡張できます。

変化の理由：DNS と IPAM インフラストラクチャを近代化

重要な DDI（DNS、DHCP、IPAM）ネットワークサービスの自動化と配信は、現代の動的なインフラストラクチャにとって不可欠です。クラウド管理またはオーケストレーションプラットフォームの構成を変更するだけで、アプリケーションをオンプレミスのプライベートクラウド、オフプレミスのパブリッククラウド、またはハイブリッド環境に導入できます。同様に、アプリケーションを移動して、インフラストラクチャ・アズ・ア・サービス（IaaS）リソースをより有効に活用できます。したがって、DDI がこれらの環境において柔軟性を持ち、自動化され、分散されることが重要です。

プロビジョニングワークフローの一環として、各仮想マシン（VM）の計算、ストレージ、ネットワークの要件をプロビジョニングするために、サーバー／クラウドチーム間の統合が必要です。

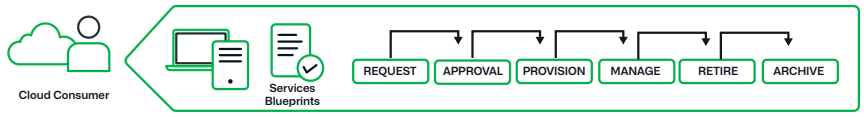

図 1：仮想マシン（VM）の作成は、サーバー／クラウドチームとネットワークチームを横断して、VM のプロビジョニング、管理、廃止を行います。

なぜ「今」なのか：ハイブリッド・マルチクラウドネットワーク向けにエンタープライズグレードの DDI を自動化・拡張

CP API ライセンスは、Infoblox Grid に直接統合された単一の Trinzic X6 プラットフォームで、DDI レコードの API 管理を通じて DNS および DHCP プロトコルを提供することにより、分散 DDI サービスの課題を解決します。VM がプロビジョニングされると、CP ライセンスは IP アドレスを割り当て、各 VM の DNS レコードを自動的に作成します。これにより、IP アドレスや個々の DNS レコードを手動でプロビジョニングすることによって生じるボトルネックが解消されます。CP ライセンスは、API の耐障害性、分散 API 処理、および権限委譲をさらに可能にします。

Infoblox は、RESTful API を使用して主要なクラウド管理プラットフォームと統合し、ワークロードの IP アドレス管理と自動 DNS プロビジョニングを提供することで俊敏性を向上させます。クラウドオーケストレーションプラットフォームは、API呼び出しを使用して、DNS および IP アドレスの自動化のためにネットワークサービスをプロビジョニングします。これらの API 呼び出しの処理は、VM のプロビジョニングにとって重要であり、単一障害点のないスケーラブルで回復力のあるソリューションが必要です。

ブジェクトを委任できます。また、テナントごとにオブジェクトをセグメント化して管理し、なおかつ一元化された可視性を維持することもできます。

- **耐障害性の向上：**APIの自動化はローカルアプライアンスレベルで行われるため、Grid Manager への接続が失われても、クラウドおよび仮想化の作成を継続できます。
- **Infoblox DDI との全面統合：**CP 機能は、Infoblox Grid 内の従来型 DDI アプライアンスと連携し、Infoblox Internal DNS Security をサポートします。
- **主要プラットフォームとの直接統合：**Infoblox は、VMware vRA/vRO、AWS EC2、GCP、Azure、OpenStack などのプラットフォームとの事前構築された統合を提供し、迅速な導入と価値実現のために最適化されています。

ハイブリッドクラウド導入における一元的な可視性と管理

Infoblox Grid のデータ同期および分散データベース機能により、DNS および DHCP プロトコルサポートを分散しながら、すべての DDI データを中央で簡単に管理できます。CP ライセンスは、DNS/DHCP を提供する同じ Infoblox メンバーで API 更新を可能にすることで、この概念をさらに一歩進めます。Infoblox Grid は、グリッド内のすべてのデータをほぼリアルタイムで双方向に同期し、Grid Manager および／または Trinzic X6 CP メンバーを通じて重要な DDI レコードを更新できる独自の機能を提供します。この機能により、企業は Infoblox Grid から DNS/DHCP プロトコルを提供するのと同様に、分散型で高可用性の API 処理の利点を享受できます。

クラウド管理プラットフォームによる API ハンドリングの改善

CP ライセンスがない場合、API 呼び出しは Infoblox Cloud Network Automation の展開の一部として Infoblox Grid Manager に送信されます。このアプローチは、Grid Managerとの通信が可能であればうまく機能します。しかし、クラウド管理プラットフォーム／オーケストレーターと Grid Manager をホストするプライマリデータセンター間のネットワーク接続が中断されると、DNS および IP アドレス管理に影響が及び、サービス停止のリスクが高まります。

Infoblox CP ライセンスは、従来のグリッドメンバーと同様に DNS と DHCP を提供しますが、IPAM レコードの同期と管理も可能です。これらの機能により、DNS/DHCP の変更がリアルタイムで行われる間、すべての API 呼び出しが同じデータセンターまたはクラウド環境内に維持されます。そのため、グリッドマネージャーへの接続が失われても、可用性と遅延の問題は解消されます。接続が再開されると、グリッドマネージャーとクラウドプラットフォームメンバー間でデータが自動的に同期されます。この同期手順により、集中化された可視性と管理を提供しながら、ローカルの耐障害性が保証されます。VM が複数の場所に展開されるスケールアウトされたクラウド環境では、ローカル API 機能によりシステム全体の信頼性が向上し、WAN 経由で送信する必要がある API 呼び出しによる遅延が回避されます。

分散型 DDI 管理とマルチテナンシーサポート

Infoblox CP ライセンスは委任モデルをサポートしており、組織は DDI をセグメント化して、ゾーン、サブゾーン、ネットワーク／サブネット、または範囲のレコード管理を組織内の特定の部門やプロジェクトに委任できます。Infoblox Cloud Network Automation と併用することで、CP ライセンスはネットワーク管理者が OpenStack、VMware vRA テナント、または AWS EC2 VPC に特化した DDI レコードの管理を委任および分離できるようにし、マルチテナント環境の管理を容易にします。

追加の CP ライセンスをオンデマンドで導入し、プロトコルと API の容量を増やすか、新しいクラウド環境のプロビジョニング時に重要なネットワークサービスを提供できます。この機能は、クラウド導入のスケーラビリティと弾力性を向上させると同時に、サービス提供までの全体的な時間を短縮します。CP 機能は、ハイブリッドおよびマルチクラウド展開で必要とされる、動的でスケーラブルな DDI サービスを提供するために不可欠です。

INFOBLOX を選ぶ理由：マルチクラウド企業向けに信頼性の高いDDI自動化、パフォーマンス、耐障害性を拡張

Infoblox の CP ライセンスは、信頼性が高くスケーラブルなクラウドネットワーク自動化のパフォーマンスと耐障害性を確保するために、エンタープライズグレードの DDI を最適化します。単一のコントロールプレーン管理により、物理リソースと仮想リソースの包括的な可視性を提供します。また、AWS、Azure、GCP、OpenStack、VMware などのプラットフォームとの強力な API 統合を活用し、ハイブリッド・マルチクラウドエンタープライズ全体で自動化を拡張します。

DNSファイアウォール（DFW）

エンタープライズの境界まで DNS を保護

Infoblox DNS Firewall は、レスポンスポリシーゾーン（RPZ）と threat intelligence サービス（マルウェアフィード）を利用して、マルウェアを検出、封じ込め、制御し、DNS を保護する Domain Name System（DNS）サービスです。このタイプのマルウェアは、侵入、データの持ち出し、その他の悪意のある行為のために、DNS を利用してコマンドアンドコントロール（C&C）サーバーやボットネットと通信します。RPZ は、クライアントがクエリを実行しているサーバーやサービスの評判を理解し、ネットワークユーザーやシステムが既知の悪意のあるインターネットの場所に接続することを防ぐためのポリシーやアクションを設定する方法を提供します。Infoblox は、物理アプライアンスおよびソフトウェアアプライアンス用の NIOS に DFW ライセンスを組み込むことで、オンプレミスサイト、データセンター、クラウドからネットワークエッジに至るまで、企業全体を保護する上で役立ちます。

変化する理由：DNS インフラストラクチャは攻撃を受けている

DNS インフラストラクチャへの攻撃は、世界中のあらゆる業界で毎日発生している何千件ものデータ侵害の主な原因であり続けています。DNS は、DNS キャッシュポイズニング、スプーフィング、セッションハイジャックなど、今日の次世代ファイアウォール（NGFW）の動作を回避したり、妨害したりするさまざまなボリューム型 DNS、DDoS、または DNS 増幅/リフレクション攻撃やエクスプロイトによって攻撃を受けます。ほとんどの NGFW は、DNS クエリと応答が送信されるプロトコルであるポート 53 をトラフィックが通過することを許可しているため、これらの脅威を識別または処理できません。

なぜ「今」なのか：データの持ち出しと悪意のある場所への接続を防止

DNS は、検出されていないマルウェアに感染したデバイスを介して無意識に、または悪意のある人物によって意図的に、ポート 53 を介して IP プロトコルをトンネリングすることにより、データ持ち出しの経路としてますます使用されるようになっています。さらに悪いことに、ほとんどのマルウェアは感染後 200 日以上検出されず、企業は顧客の機密データ、財務情報、知的財産、その他の重要な情報を失う危険にさらされています。

INFOBLOX を選ぶ理由：保護とパフォーマンスのためにネットワークとセキュリティを統合

Infoblox DFW は、業界をリードする DNS ベースのネットワークセキュリティ・ソリューションです。DFW を使用して、Infoblox はオンプレミスの展開からクラウドネットワークのエッジに至るまで、データを持ち出すマルウェアを封じ込めて制御することで、ネットワークとセキュリティを統合します。DFW は、DNS RPZ、Infoblox のオプションである BloxOne Threat Defense、Threat Insight、またはフォレンジックなサードパーティの侵害指標（IoC）フィードを統合して、マルウェアを検出、ブロック、リダイレクトします。Infoblox は、DFW をグリッド内のネットワーク IPAM データと組み合わせて、感染したデバイスを隔離し、修復を支援します。DHCP フィンガープリンティングと Identity Mapping を活用することで、管理者は感染したデバイスに関連付けられたユーザー名を取得し、サイバーキルチェーンの初期段階で脅威の影響を軽減できます。さらに、DFW は DNS リダイレクトを有効にし、管理者がドメインをブロックしたり、「ウォールドガーデン」やその他の指定された場所に転送したりできるようにします。DFW は、エコシステム・ライセンスをお持ちの顧客向けに、セキュリティエコシステム統合のトリガーとしても使用できます。また、DFW は Infoblox Reporting and Analytics と統合して、上位の RPZ ヒット、上位の悪意のあるホスト名、上位の悪意のあるユーザー、その他の多くのセキュリティメトリクスを含む、概要レポートと豊富なコンテキ

DNSファイアウォール（DFW）

使用例

- IOC 検出をネットワークエッジ（オンプレミスまたはクラウド）に導入する
- ハードウェアまたはソフトウェアアプライアンスでDFWを有効にしてください
- Infoblox および / またはサードパーティのフィードを使用した脅威保護を許可する
- DNS マルウェア保護の確保する
- 既存のセキュリティスタックを改善する

メリット

- **マルウェアの検出、封じ込め、制御：**ネットワークとセキュリティのツールおよびデータを組み合わせて、感染した通信や悪意のある通信を早期に検出できるようにします。
- **企業の DNS 脅威の影響を軽減：**RPZ とオプションの threat intelligence フィードを組み合わせて、オンプレミスからクラウド展開まで企業を保護します。
- **可視性、自動化、制御の向上：**管理者が豊富なコンテキストデータを確認し、脅威対応を自動化し、セキュリティ脅威をリダイレクトおよび修復できるようにします。
- **セキュリティエコシステムの統合を開始する：**広範なエコシステムの統合を通じて、脅威の認識、可視性、共有、対応を向上させます。
- **レポートとアナリティクスの統合：**豊富なネットワークデータの要約、フォレンジックおよび視覚化されたレポートをオンデマンドで取得します。
- 既存のセキュリティスタックを強化し、既存のセキュリティツールと統合の影響、価値、ROI を向上させます。

ストデータを提供します。最後に、DFW は DNS マルウェア保護において信頼できる基盤を提供し、顧客の既存のセキュリティスタックの効果と投資利益率（ROI）を向上させます。

ではその仕組みについて見ていきましょう。

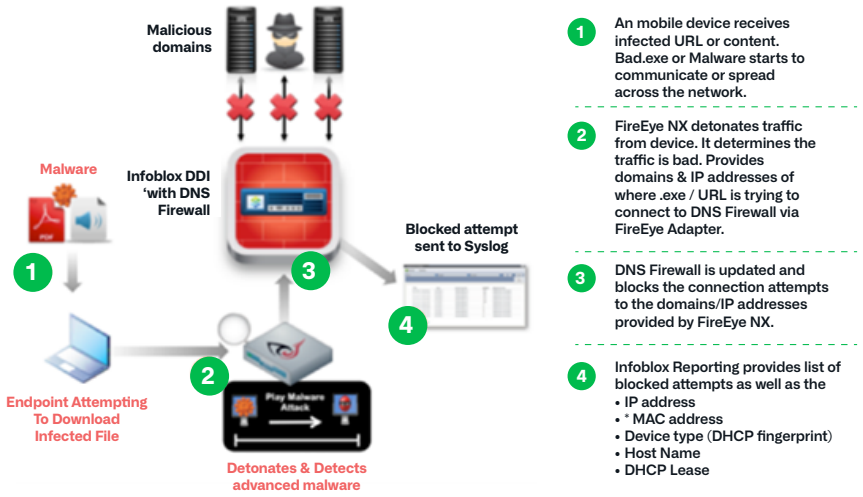

図 2：DNS ファイアウォールが悪意のある接続試行をブロックする仕組み。

DNSトラフィックコントロール（DTC）

トラフィック管理の改善、アプリケーションの稼働時間の向上、ユーザーエクスペリエンスの向上

Infoblox DTC ライセンスは、オンプレミスおよびハイブリッドのマルチクラウドネットワークに対して、ネットワークトラフィック管理、信頼性の高いアプリケーション稼働時間、サービスの弾力性、災害復旧（DR）を提供する統合型のグローバルサーバー負荷分散（GSLB）ソリューションです。DTC は、権威ある IPAM データを DNS および GSLB サーバーの正常性メトリック、GeoIP、拡張属性（EA またはユーザーメタタグ）と統合し、ユーザートラフィックを最適なサーバーにインテリジェントに誘導して、最大限の稼働時間とユーザーエクスペリエンスを実現します。

変化の理由：グローバルな近代化によるネットワーク環境の変化

地域およびグローバルな職場の近代化は、オンプレミスおよびハイブリッド、マルチクラウドの企業を変革しています。どこからでもクラウドアプリケーションに直接アクセスできることにより、迅速で効率的かつ常に利用可能な顧客体験への期待が高まっています。SD-WAN により、ローカルブランチから直接インターネットにアクセスすることが可能になります。5G 機能が出現し、IoT によりネットワークリソースへの接続需要が増加しています。組織が新しいプラットフォームや技術を採用するにつれて、これらの課題は拡大します。ユーザーは、特に e コマースや社内ポータルにおいて、リアルタイムのパフォーマンスを期待しています。レガシーアプリと最新アプリの管理は、特に合併や買収により、ますます複雑になっています。プライバシー規制は強化されており、遵守しない場合には厳しい罰則が科せられます。モバイルおよびリモートワーカーやブランチにおけるトレンドの変化、グローバル化、データセンターの統合、継続的なリソース制限、ならびに DNS、マルウェア、ステルス攻撃の拡大により、ネットワークトラフィック、稼働時間、ビジネス継続性を責任を持って持続可能な方法で管理するタスクを担当しているチームには、さらに大きな負担がかかっています。

DNSトラフィックコントロール（DTC）

使用例

- 社内外のオンプレミスおよびハイブリッドクラウドにおける費用対効果の良いグローバルトラフィック管理
- サブネット、GeoIP、拡張属性に基づくオンプレミスおよび SaaS アプリの稼働時間
- 壊滅的な障害後の弾力性を目的とした災害復旧（DR）
- ドメインゾーンの統合とサーバーおよびリソースの複製
- プライベート、ハイブリッド、マルチクラウド環境における API ベースのアプリケーション・スケーリング
- MS AD クライアントのサイトレベルの認識
- 全面統合型のレポート作成と分析

メリット

- **統合型 DNS/ グローバルサーバー負荷分散（GSLB）：**信頼性の高い IP アドレス管理（IPAM）を DNS と GSLB に統合し、独立した DNS プラットフォームに依存することなく、インターネットおよびイントラネットアプリケーションにおける「ファイブナイン」レベルの高可用性と稼働時間、パフォーマンスを提供します。
- **インテリジェントなグローバルトラフィック管理：**DNS ベースの GSLB を使用して、クライアントとサーバーの位置、サーバーの健全性と可用性に基づいて、ユーザートラフィックを最適なサーバーにインテリジェントに誘導します。

なぜ「今」なのか：手頃な価格で信頼性の高いグローバルな稼働時間と事業継続性

InfobloxのDTCは、他の競合するアプリケーションデリバリコントローラ（ADC）と比較して手頃な価格で、変化するグローバルトラフィック管理の課題を解決するソリューションを提供します。DTCは、信頼性の高いアプリケーションの稼働時間、パフォーマンス、シームレスなフェイルオーバーにより、ユーザーの高い満足度を実現します。簡単なユーザーインターフェースと堅牢なAPIを使用して、eコマース、顧客向けポータル、Web、社内のビジネスクリティカルなアプリケーション向けに、地理的に多様なオンプレミスおよびハイブリッドなマルチクラウド環境でネットワークトラフィックの負荷を分散します。また、壊滅的な事象が発生した場合に、通常の業務を復旧させるために、事業継続と災害復旧を提供します。

INFOBLOX を選ぶ理由：保護とパフォーマンスのためにネットワークとセキュリティを統合

Infoblox の DTC は、権威ある IPAM データを DNS と GSLB に統合し、ユーザートラフィックを最適なサーバーにインテリジェントに転送します。競合する ADC とは異なり、全面的に統合された DNS ソリューションであるため、レイヤー 2 およびレイヤー 3 プロトコルを追加するよりも高速で信頼性があります。複数の負荷分散アルゴリズムと柔軟で自動化されたヘルスチェックを実行し、サーバーの可用性を確保します。DTC は、変化するデータトラフィック量やビジネスニーズに対応する拡張性を備えています。最適な可視性を実現するために、DTC は、負荷分散ドメイン名（LBDN）、プールとサーバーの関係および属性を表示するシンプルなユーザーインターフェースとビジュアライザーを使用します。また、他の ADC とは異なり、LBDN、プール、サーバーをリアルタイムで本番前にテストし、稼働前の準備状況を確認できます。DTC は、GeoIP と EA データ（ユーザー定義のメタタグ）を使用して、アプリケーションの最適化とともに規制とプライバシーの遵守のために地域固有のゾーンへのトラフィックを制御できます。統合された Splunk ベースのレポートと分析ツールは、事前構築済みでカスタマイズ可能な DTC ダッシュボード、レポート、検索、アラート、自動レポート配布を提供し、このツールは別途利用可能です。最後に、DTC は Infoblox 検出ソースと統合し、IP サブネット、GeoIP、EA データに基づいてトポロジを自動的に更新します。API を使用すると、新しいサーバーインスタンスを迅速に追加し、新しいアプリのプロビジョニングや他のシステムとの統合、そして日常的なタスクの自動化を行うことができます。DTC は Grid に直接統合されているため、別のプラットフォームのソフトウェアを展開・構成して、更新管理を行う必要はありません。

- **DTC ビジュアライザー：** 負荷分散ドメイン名（LBDN）、プールとサーバーの関係および属性を 1 つの GUI で視覚化して表示します。
- **実稼働前テスト：**新規および更新された LBDN、プール、サーバーを迅速かつリアルタイムでテストし、本番運用開始前の準備が整っていることを確認します。
- **コンプライアンス：**GeoIP と拡張可能属性（EA）データを使用して、LBDN およびプールの地域固有のゾーンにトラフィックを制限し、プライバシーコンプライアンスへの対応を支援します。
- **統合レポートと分析：**Splunk ベースの事前構築済みでカスタマイズ可能なダッシュボード、レポート、検索、アラート、自動レポート配信を提供し、可視性と制御を強化します。
- **API の自動化：**新しいサーバーインスタンスの追加、新しいアプリの迅速なプロビジョニング、他のシステムとの統合、定期的な GSLB 管理タスクの自動化を通じて、時間とコストを節約可能。ウェブ GUI の機能を反映した、利便性と文書化に優れた API です。

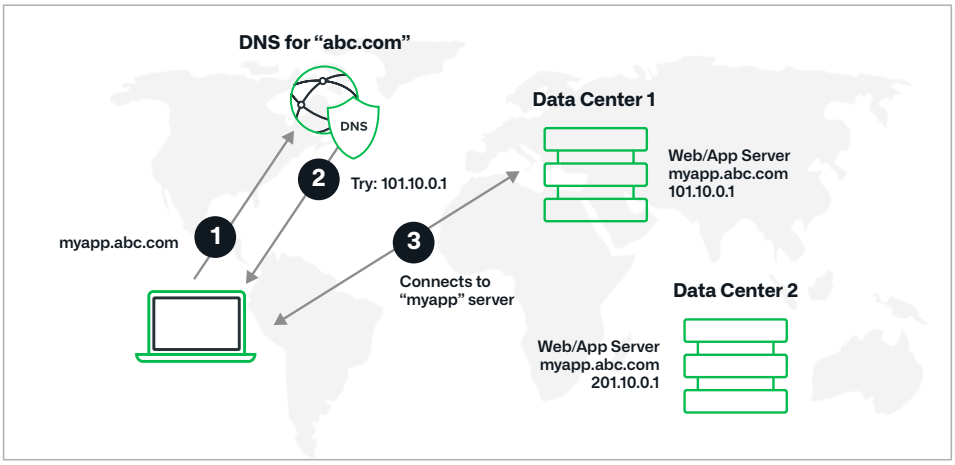

図3：DTCプロビジョニングの説明。1）アプリ展開の開始、2）会社のDNS接続、3）分散データセンターでのmyappサーバーのプロビジョニング。

要約と次のステップ

NIOS 9.0.1 と Trinzic X6 プラットフォームにより、Infoblox はクラウドの近代化における課題を解決する付加価値を提供します。これには、以前は個別に販売されていたクラウドプラットフォーム（CP）API 自動化、DNS ファイアウォール（DFW）、DNS トラフィック制御（DTC）グローバルサーバー負荷分散の「サイト全体」を対象としたライセンスが含まれています。これらのソリューションは、サイロやマルチクラウド環境全体にわたるワークロード自動化と耐障害性の拡張、悪意のあるネットワーク IP またはドメインからの DNS 解決を傍受・ブロックするレスポンスポリシーゾーン（RPZ）によるエッジまでのエンタープライズ保護、トラフィック管理の改善、アプリケーションの稼働時間およびユーザーエクスペリエンスの向上など、頻繁に発生するビジネス課題に対処します。詳細情報や製品トライアルのご希望については、Infoblox.com のアカウントチームにお問い合わせください。

お問い合わせ

追加の技術情報については、Infoblox サポートポータル（https://support.infoblox.com）にある『NIOS 9.0.1 リリースノート』（2023年8月21日から一般利用可能）をご覧ください。

Infoblox の NIOS または Trinzic X6 プラットフォーム、またはワークプレイスモダナイゼーションのためのハイブリッド・マルチクラウド統合の豊富なラインナップに関する具体的な回答は、Infoblox のアカウントチームにお問い合わせいただくか、Infoblox.com までご連絡ください。

Infoblox株式会社
〒107-0062 東京都港区南青山2-26-37
VORT外苑前I
3F

03-5772-7211
www.infoblox.com

バージョン：20230731v1