ホワイトペーパー

DDIでInfobloxを選ぶ理由:

今こそBINDとMicrosoftから移行する時です

目次

多くの組織では、信頼性の高い接続とインターネットへのアクセスを可能にするコアサービスは、無料ベースで、表面上は無料製品になっています。価格は魅力的かもしれませんが、これらの製品には機能の制限があったり、管理に非効率性があることで、隠れたコストを伴うことがよくあります。今日のネットワークで発展と変化を計画する場合、「無料」のために生じる制限と、ネットワークを次のレベルに引き上げるためのコアサービスのあり方を考慮することが不可欠です。

DNS、DHCP、IPAM の歴史

当初、DNS は Web サイトやアプリケーションにアクセスするための便利な方法であり、DHCP は事実上ほとんど知られていませんでした。これらは通常、DNS や DHCP を理解している人によって管理され、BIND/DHCPD や Microsoft DNS/DHCP などの「無料」システムに依存していました。場合によっては、スプレッドシートが重要なプロトコルサービス（DNS と DHCP）を維持するための土台となることがありました。これらのシステムは、多くの場合、少人数の専任チームによって維持管理される一連の「DIY」ツールによって進化しました。そのため、その専任者が他の役割や他の組織に異動した際には、運営上や計画上の意思決定が妨げられました。

IP アドレス管理（IPAM）は後に拡張され、DNS と DHCP を管理する担当者から切り離されることがありました。リソースを割り当ててネットワークを定義するチームは、名前とアドレスを管理し定義する担当者とは別でした。

これらのシステムのビジネスへの影響や信頼性は、IT 戦略全体の中で無視されることが多く、どのグループ（運用、システム、ネットワーク）がその維持を担当するかについて一貫したルールが存在することはほとんどありませんでした。DNS、DHCP、IPAM を組み合わせた（「DDI」）という概念が採用されるようになったのはつい最近のことです。

最新のネットワークにおける DDI

過去 20 年間の驚異的な成長とネットワークとモビリティへの依存、そしてモバイルデバイスが爆発的に使用されるようになり、DNS は常に機能する「ダイヤルトーン」サービスであることが期待されています。

認証、データベース、その他のバックエンドリソースへのアクセスが不可欠であるため、IPv6、IoT、その他ほとんどすべてのものは現在、DDI をネットワークの中核に据えています。そのため、極めて高い信頼性、統合性、結果責任に対する追加の要件が追加されています。これらは、元々の設計モデルの一部として完全には考慮されていませんでした。

無料またはオープンソースのソリューションは必要なサービスを提供できますが、保守に多大な労力がかかる可能性があり、今日の最新のネットワークでは「エンタープライズグレード」とみなされるほどの堅牢性には欠けています。

企業はまた、特にクラウドや仮想空間において、より自動化された環境に移行しつつあります。ただし、これらの既存のソリューションを、期待される自動化レベルに適応させるには、さらに多くのカスタマイズが必要になります。IPv6 が普及するにつれて、電話で IP アドレスを読み上げる時代は終わり、この複雑さや問題はさらに増大するでしょう。これらのますます複雑化する環境を適切に管理するには、サポート可能でスケーラブルな集中管理型の DDI ソリューションが不可欠です。

簡単に言うと、DDI サービスがダウンしたり、変更の実装に時間がかかりすぎたりすると、ビジネス機能に悪影響が生じ、最終的には生産性と利益の損失につながります。

経営幹部レベルの優先事項

最近の KPMG レポートでは、CIO 向けの経営戦略上の優先事項として次の 5 つが挙げられています。

- 市場投入までのスピードの向上
- ビジネスのデジタル化
- よりデータ主導型になる
- 社会的信頼の構築
- 破壊的テクノロジーの導入

DDI の分野では、これらは「ビジネスの保護」、「ビジネスのスピード向上」、あるいは「会社の評判の維持」などの取り組みへと発展する可能性があります。

また、このような取り組みに対処するために DDI インフラストラクチャを再設計する場合、点と点を結び、従来のソリューションと最新の統合ソリューションの限界を確認するのにそれほど労力はかかりません。

データに対するすべての攻撃進路を適切に保護し、軽減する場合にのみ、ビジネスを保護することができます。DNS は現在、アプリケーションレイヤー攻撃（DDoS）の 78%、マルウェア配布、コマンドアンドコントロール、データ流出の 91%の主なチャネルとなっています。

会社の評判を高め、よりデータ駆動型のビジネスへの進展を示すことは、ネットワークの中核で、インフラのコンプライアンスと保護、マルウェアの軽減、集中型の脅威封じ込めと運用モデルに対応できるシステムを使用している場合にのみ達成できます。

また、このようなビジネスのスピードを発揮することができるのは、クラウドベースのインフラストラクチャが要求する急速かつ変動する成長をサポートできるレベルまで DDI が自動化されている場合にのみ実現可能です。

次世代データセンターを実現するまでの道のりは困難な場合があります。従来の DNS インフラやスプレッドシートでの IP アドレス管理では、ワークロード・プロビジョニングの効率化、可視化、自動化を実現できず、IT 部門はコアネットワークサービスのプロビジョニングに手作業と時間のかかるプロセスを余儀なくされていました。真のデータセンター変革ではストレージとコンピューティングの自動化だけではなく、迅速に中央管理され、拡張性の高いデータセンターを実現するためのネットワークの自動化も必要です。

すべてのデバイスがどこにあるのか、何をしているのか、誰と通信しているのか、時間の経過とともにどのように変化しているのか、手元にある限られたリソースの中でどこに注力すべきかを把握する必要があります。

理想的なシステム

今日の環境における DDI は、次のような多くの重要な基準を満たす必要があります。

- 信頼できる稼働時間（アップタイム）
- 変更のしやすさ
- エンドポイントとトポロジのリアルタイムでの可視化
- 自動化システムへの統合
- 冗長性や迅速な復旧時間

つまり、理想的なシステムは集中管理され、保守に必要なリソースが最小限で、導入と拡張が容易である必要があります。また、安定性と安全性が高く、様々なニーズに対応できる必要もあります。これらには、高位レベルの管理者、サイト / デスクトップサポート、自動化タスク、ネットワーク計画、セキュリティフォレンジックなどが含まれことがあります。

計画の立案・実行とフォレンジックについては、「信頼できる一つの情報源」が鍵となります。競合する可能性のある複数のシステムや 同期していないシステムを検索するのではなく、デバイスやネットワークの情報を 1 か所で検索できるシステムが必須です。

これは、過去の成長パターン、DNS の使用状況と傾向の可視性、DHCP リース履歴、デバイス履歴にまで及びます。これらはすべて、セキュリティインシデントへの迅速な対応、ネットワークの問題へのトラブルシューティング、一般的な容量プラニングを実現するための鍵となります。

理想的なソリューションでは、より大きなエコシステムの一部として他のシステムと通信し、相互に動的に情報交換もできます。自動化は今や欠かすことができません。

この例には次のようなものがあります。

- 潜在的に悪意があるとしてフラグが付けられた DNS レコードをクエリすると、DNS は応答ポリシーゾーンを介してこれを「取得」できます。この一致がデバイススキャナに送信され、問題のシステムを自動的にスキャンして潜在的な問題がないか確認し、必要に応じて警告を発し、そのシステムを隔離できます。
- DHCP リースログをサードパーティのログシステムに送信して、使用傾向とイベントの相関関係を 追跡できます。
- 新しく作成された VM の IP 割り当てと再利用のための自動システムにより、プロビジョニング時間をこれまで要していた数日や数時間から数分に短縮できます。
- 悪意のあるエンドポイントにフラグを付けるエンドポイントセキュリティシステムを使用すると、この情報をセキュリティポリシーに自動的にプッシュして、クライアントがそのエンドポイントにアクセスするのを防ぐことができます。

もちろん、これらは、システム間の自動交信によって変更が容易になり、エンドポイントとトポロジをリアルタイムで可視化でき、自動化システムに統合できる多くの例のうちのほんの一部にすぎません。

Infoblox の利点

レガシーシステムは拡張できません

BIND は DNS とインターネットに関して業界標準になりましたが、適切に実装して運用するには高度な知識とスキルが必要です。単純なタスクを適切に実行するには、手作業での複数の手順を必要とします（たとえば、レコードが追加 / 変更 / 削除されるときにゾーンのシリアル番号を割り当てする必要があります）。DNSSEC などのもっと複雑な構成や機能を実装する場合、予測できない動作や DNS が完全に停止しまう可能性が生じるという落とし穴があります。

さらに、BIND は DNS をサポートしますが、動作の監視と管理を可能にする統合レポートを提供しておらず、IP アドレス管理との統合も提供していないため、ネイティブ DNS レコードと IPAM に表示されるレコードの間で一致しないという可能性があります。BIND は自動化を念頭に開発されていないため、DDI システムが提供する DNS レコード変更の単純な自動化のための堅牢な API は含まれていません。

IPAM と DNS の統合

IPAM を DNS に統合して、両方のシステムを正確に同期させておくことが重要です。新しいデバイスがネットワーク上に展開されると、最初に IP アドレスが割り当てられ、次に通常はその直後にホストを DNS に追加する要求が続きます。DNS と IPAM を統合することにより、このプロセスは 1 つのステップになり、IP の割り当てと同時に DNS レコードが作成されます。これにより、効率が向上するだけでなく、データが転記または中継されないため、エラーの可能性も減少します。IPv6 の普及が進むにつれて、IPAM と DNS の統合の必要性は高まるばかりです。

DNS と IPAM の精度をさらに向上させるために、検出機能を追加できます。検出機能を IPAM に統合することで、IPAM は、ほとんど人間の行為に依存するシステムから、ネットワーク管理者やセキュリティ運用者に、ネットワーク上にその瞬間に何があるのかをリアルタイムのビューを提供する「権威ある IPAM」に生まれ変わります。レポートソリューションと組み合わせると、IP アドレスの履歴を長期にわたって追跡できるため、セキュリティイベントを適切に分析するために非常に重要なものになります。

Infoblox DDI を使用すると、次の方法でこれらの問題の多くに対処する最新の DNS サービスを得られます。

- DNS、DHCP、IP アドレス管理、その他のコアネットワーク・サービスを単一のプラットフォームに統合し、共通のコンソールから管理
- ハイブリッドおよびパブリッククラウド、仮想およびプライベートクラウド環境向けの統合機能により、多様なインフラストラクチャ全体で DDI 機能を中央で一元調整
- 容量プラニング、資産管理、コンプライアンス管理、監査のための豊富な統合レポート機能と分析機能へのアクセス
- Infoblox Grid と連携して、RESTful API を通じて他の IT システムとシームレスに統合することで、IT の効率と自動化を促進

Infoblox for DNS と Microsoft DNS の比較

Microsoft Active Directory で使用する DNS ソリューションを選択する場合、多くの管理者は単に「Windows Server に付属しているもの」を選択しますが、Microsoft DNS 以外を使用する理由がいくつかあります。

- **セキュリティ :** 組織は、インターネット攻撃にさらされている外部 DNS の偽の情報に最適なソリューションを求めています。サードパーティの DNS ソリューションでは、セキュリティを念頭に一から設計・構築されているものが利用できます。組織の内部 DNS 構造も同時に、悪意のある脅威、マルウェア、フィッシング、データ流出にさらされています。
- **可視性と単一ビュー :** ほとんどの組織では、異機種環境の様々な技術が混在しています。効率的なコンプライアンスと管理には、正確で 1 か所での可視性が不可欠です。
- **運用の効率化 :** 手作業でのスプレッドシート管理に対して、自動化とワークフローを活用して、運用コストを最適化します。
- **インテリジェントサービス :** DNS ベースでトラフィック制御、ネットワーク負荷分散、サービス監視を統合して、組織に大きな価値をもたらします。Microsoft IPAM のギャップにより、ネットワークトポロジの現状と Microsoft Active Directory（AD）に含まれる情報との間に不整合が生じます。そのため、ユーザー認証やファイルの可用性といった基本的なサービスが完全に停止する可能性があります。

Infoblox IPAM は、Microsoft AD サイトとサービスをシームレスに統合することもでき、AD 管理者とネットワーク管理者の両方に対してこのギャップを埋めることもできます。さらに、Infoblox は Microsoft フォレストにまたがり、Microsoft 環境全体を一元管理する GUI に取り込んで、これまでにない可視性を提供し、運用効率とサービス稼働時間を向上させます。

詳細については、グループポリシー MVP の Jeremy Moskowitz が執筆した「Microsoft DNS と Microsoft 製品以外の DNS の比較 : 事実とフィクション（Microsoft vs Non-Microsoft DNS: Facts vs Fiction）」を参照してください。

Infoblox と他の製品やエコシステムとの統合

Infoblox は、最先端のセキュリティと管理の様々な技術ともシームレスに統合できます。オープン API 経由でインテリジェントな自動化を実現し、クラウド環境とオンプレミス環境の両方でワークロードをサポートします。当社の製品は、高度な脅威インテリジェンスとエコシステムの統合を備えたコンテキスト認識型セキュリティで構成されています。

より大きなセキュリティエコシステムの一部として、Infoblox は REST と PERL API もサポートしています。また、イベントベースのアウトバウンド API もサポートし、セキュリティインフラストラクチャの他のシステムと相互に交信して、IPAM に追加されたネットワークをスキャン対象として追加したり、エンドデバイスが RPZ ルール（Threat Insight を含む）などに一致するクエリを送信した場合にデバイススキャンや検疫をトリガーしたりできます。さらに、Infoblox は Cisco ISE、McAfee、その他 20 社以上とも統合されており、その数は増え続けています。

結論

やるべきこと

BIND/DHCPD、Microsoft DNS/DHCP、スプレッドシートなどの「無料」システムは、最新ネットワークのニーズに適切に対応できません。時間をかけてコアの弱点を調査し、統合 IPAM システムに移行する計画を立ててください。

既存のワークフローと IPAM プロセスを特定し、以下において改善できる点を検討します。

- 信頼できる稼働時間（アップタイム）
- 変更のしやすさ
- エンドポイントとトポロジのリアルタイムでの可視化
- 自動化システムへの統合
- 冗長性や迅速な復旧時間

また、Infoblox は市場で 50% 以上のシェアと 8,000 社以上の顧客を有するマーケットリーダーであり、この決断を支援するために多くのリソースを用意しています：https://www.infoblox.com/resources/?category=Whitepaprs

次のステップ

導入アーキテクチャの推奨については、Infoblox セールスチームにお問い合わせください。

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