INFOBLOX® NIOS DDI リファレンスアーキテクチャとベストプラクティス

INFOBLOX NIOS DDI と INFOBLOX THREAT DEFENSE™ 製品を活用したDNS／DHCP サービス導入によるシンプルさ・セキュリティ・スケーラビリティの実現

目次

概要 3
会社紹介 5
サイジングに関する重要な注記 5
コントロールプレーン 6
外部権威 DNS 7
ローカルフォワーディング 8
内部 DNS 8
DHCP 9
リモートオフィス 9
クラウド 10
レポーティング 11
ネットワーク検出 11
外部システムおよびエコシステムの統合 11

概要

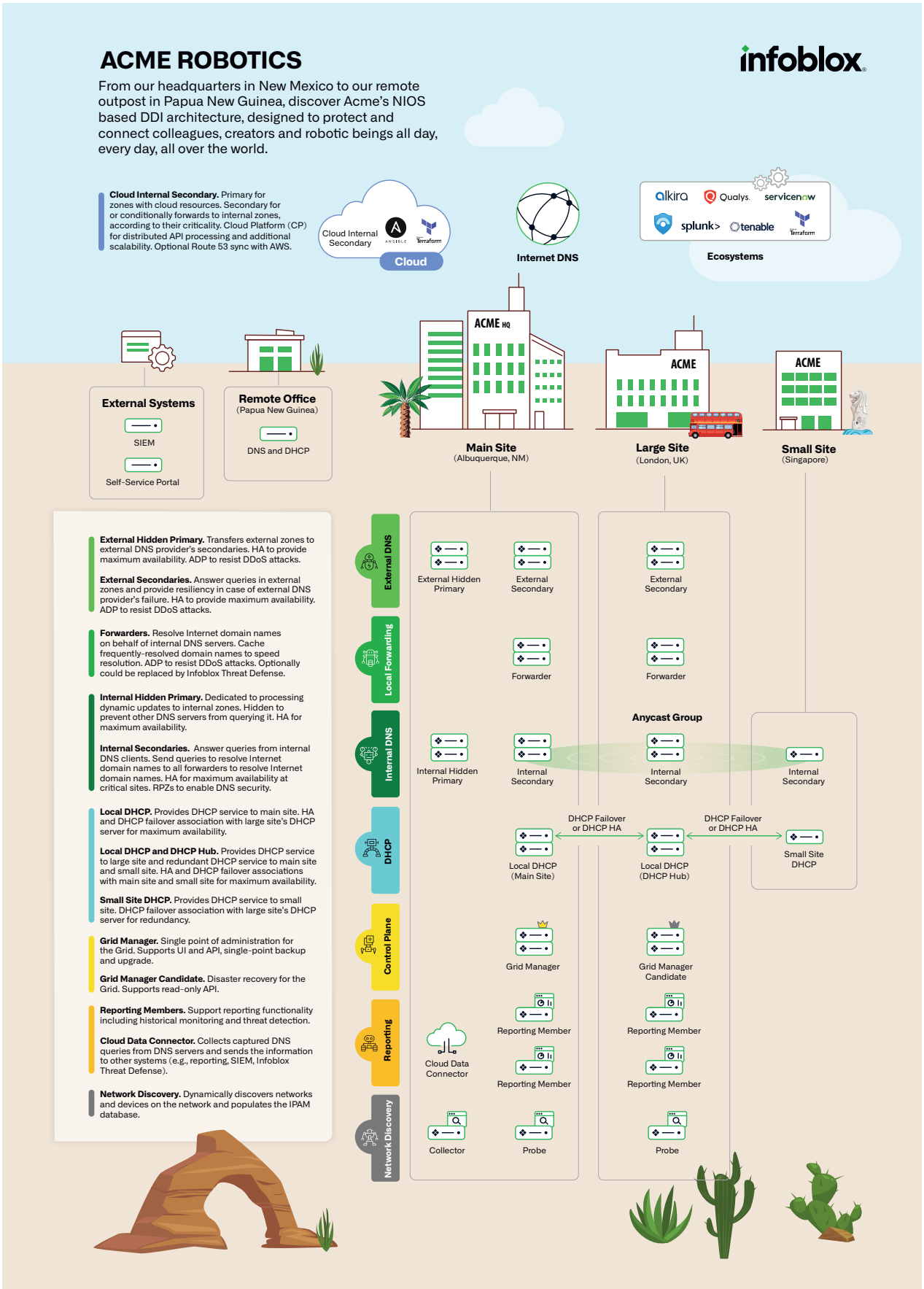
本ガイドは、Cricket Liu 氏と Infoblox® Architecture Review Board（ARB）が執筆したホワイトペーパーを基に作成されており、Infoblox のソリューションアーキテクトが設計した複雑な構成を審査する社内チームの協働の成果を示すものです。ARB に加えて、Infoblox 全社の技術専門家が専門知識を提供し、当社のソリューションが堅牢で革新的であり、業界のベストプラクティスに準拠した設計が実現されるよう支援しています。

NIOS アプライアンスは、DNS（Domain Name System）や DHCP（Dynamic Host Configuration Protocol）といったネットワークサービスの提供に最適なプラットフォームであり、それらに加えてセキュリティ機能も効率的かつ信頼性の高い方法でサポートするアーキテクチャを提示しています。本ガイドでは、これらのホワイトペーパーの内容を拡張し、情報技術分野における新たな動向を幅広くご紹介します。

- 重要なセキュリティツールとしてのDNSの活用
- パブリッククラウドおよびクラウドコンピューティングの台頭
- ServiceNow などのサービスによって推進されるセルフサービス型 IT の重要性の高まり
- 小規模なリモートオフィスの増加を伴う企業ネットワークの拡張
- セキュリティ情報およびイベント管理（SIEM）システムやその他のセキュリティ技術との統合の必要性

これらの新しい動向をどのようにサポートできるかを示すために、ある企業とその企業ネットワークのケーススタディを紹介し、業界のベストプラクティスに基づいてその要件を満たす DNS、DHCP、IP アドレス管理（DDI）アーキテクチャを設計します。設計では、可用性、パフォーマンス、セキュリティ、災害復旧、クラウドベースのコンピューティングやアプリケーションのサポート、社内およびクラウドベースのシステムとの統合といった企業の要件を考慮します。

この資料を読みながら、御社の DDI インフラストラクチャが、同等の弾力性、パフォーマンス、セキュリティを備えているか、また、本資料の設計内容の中に応用できる要素があるかどうかをぜひご検討ください。


ACME ROBOTICS
infoblox.
From our headquarters in New Mexico to our remote outpost in Papua New Guinea, discover Acme's NIOS based DDI architecture, designed to protect and connect colleagues, creators and robotic beings all day, every day, all over the world.
Cloud Internal Secondary. Primary for zones with cloud resources. Secondary for or conditionally forwards to internal zones, according to their criticality. Cloud Platform (CP) for distributed API processing and additional scalability. Optional Route 53 sync with AWS.
Cloud Internal Secondary
Cloud
Internet DNS
alkira
Qualys.
servicenow
splunk>
tenable
Terraform
Ecosystems
External Systems
SIEM
Self-Service Portal
Remote Office
(Papua New Guinea)
DNS and DHCP
ACME HQ
Main Site
(Albuquerque, NM)
ACME
Large Site
(London, UK)
ACME
Small Site
(Singapore)
External Hidden Primary. Transfers external zones to external DNS provider's secondaries. HA to provide maximum availability. ADP to resist DDoS attacks.
External Secondaries. Answer queries in external zones and provide resiliency in case of external DNS provider's failure. HA to provide maximum availability. ADP to resist DDoS attacks.
Forwarders. Resolve Internet domain names on behalf of internal DNS servers. Cache frequently-resolved domain names to speed resolution. ADP to resist DDoS attacks. Optionally could be replaced by Infoblox Threat Defense.
Internal Hidden Primary. Dedicated to processing dynamic updates to internal zones. Hidden to prevent other DNS servers from querying it. HA for maximum availability.
Internal Secondaries. Answer queries from internal DNS clients. Send queries to resolve Internet domain names to all forwarders to resolve Internet domain names. HA for maximum availability at critical sites. RPZs to enable DNS security.
Local DHCP. Provides DHCP service to main site. HA and DHCP failover association with large site's DHCP server for maximum availability.
Local DHCP and DHCP Hub. Provides DHCP service to large site and redundant DHCP service to main site and small site. HA and DHCP failover associations with main site and small site for maximum availability.
Small Site DHCP. Provides DHCP service to small site. DHCP failover association with large site's DHCP server for redundancy.
Grid Manager. Single point of administration for the Grid. Supports UI and API, single-point backup and upgrade.
Grid Manager Candidate. Disaster recovery for the Grid. Supports read-only API.
Reporting Members. Support reporting functionality including historical monitoring and threat detection.
Cloud Data Connector. Collects captured DNS queries from DNS servers and sends the information to other systems (e.g., reporting, SIEM, Infoblox Threat Defense).
Network Discovery. Dynamically discovers networks and devices on the network and populates the IPAM database.
External DNS
Local Forwarding
Internal DNS
DHCP
Control Plane
Reporting
Network Discovery
External Hidden Primary
External Secondary
External Secondary
Forwarder
Forwarder
Anycast Group
Internal Hidden Primary
Internal Secondary
Internal Secondary
Internal Secondary
DHCP Failover or DHCP HA
DHCP Failover or DHCP HA
Local DHCP (Main Site)
Local DHCP (DHCP Hub)
Small Site DHCP
Grid Manager
Grid Manager Candidate
Reporting Member
Reporting Member
Cloud Data Connector
Reporting Member
Reporting Member
Collector
Probe
Probe

会社紹介

当社は最近、ACME Robotics という多国籍企業から、新たな DNS アーキテクチャの設計を依頼を受けました。ACME 社は、多様な機能を備えたロボットデバイスを提供する著名な企業です。ACME Robotics 社は製造、マーケティング、流通を手がけ、販売およびサポート体制を整えています。

同社の市場は世界中に広がっていますが、特にアメリカ南西部に集中しています。

この会社には、企業ネットワークに接続された 4 種類の拠点があります。

1. ニューメキシコ州アルバカーキにあるACMEの本社には、最も多くのユーザー（約2,000人）がいます。本社には、会社の主要なデータセンターもあります。
2. イギリス、ロンドンにある大規模なサイトには、約500人の現地ユーザーがいます。
3. シンガポールを含む小規模拠点では、通常 100 人以下のユーザーが利用しています。小規模拠点は地理的な地域ごとに分類され、それぞれが地域事務所の支援を受けています。各小規模拠点は、それぞれを管轄する地域事務所を経由して、企業ネットワークに接続されています。
4. リモートサイトは通常、24人未満のユーザーをサポートします。リモートサイトは、VPNまたはSD-WAN接続を介してインターネットおよび企業ネットワークに接続されます。

同社は、製品のマーケティングに活用している強力なオンラインプレゼンスを有しており、これをサポートするために、AWS と Azure の 2 つのパブリッククラウドを使用しています。各クラウドで複数のアプリケーションが稼働しており、一部は内部リソースへのアクセスが必要となります。クラウドでのプロビジョニングは、アプリケーションに応じて Terraform または Ansible によって自動化されます。

同社は、従業員が DNS や DHCP を含む IT 変更をリクエストできるように ServiceNow を使用しています。社内に SIEM を導入しており、業界の特性により、パッシブ DNS（pDNS）データの収集とアーカイブが義務付けられています。

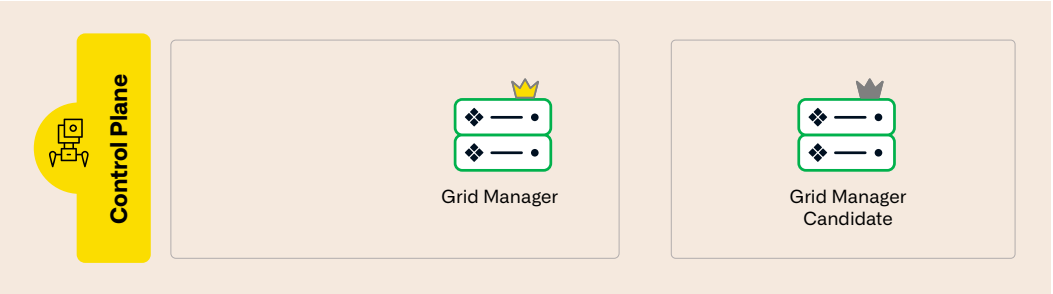
同社の IT サポート体制は、本社と大規模拠点に分散して配置されています。各地域オフィスには 1 名の IT 担当者が常駐しており、主にデスクトップやノートパソコンのローカルサポートを提供するほか、本社スタッフに代わって「目と手」としてリモート対応も行います。

従業員による私物デバイスの持ち込みを許可していますが、ゲストネットワークに分離されています。従業員 1 人あたりのデバイス数と、それに伴うトランザクション負荷は、あらかじめ設計に織り込まれています。

サイズに関する重要な注意点

本ドキュメントでは、アーキテクチャにおける重要な要素である「サイジング（規模の見積もり）」については扱っていません。企業の要求に応えるだけのパフォーマンスを DNS や DHCP サーバーが発揮するには、各サーバーのトランザクションレートを測定するか、適切な見積もりを行ったうえで、それに見合うアプライアンスを選定する必要があります。さらに、予期せぬ負荷の急増（例：拠点での停電とその後の復旧など）に対応するため、十分な「ヘッドルーム」（余剰サーバー容量）を設計段階で確保する必要があります。最後に、将来的な成長も見据えた見積もりと計画が求められます。たとえば、大規模な人員採用や他社の買収、合併といった計画がある場合、DNS と DHCP への負荷に大きな影響を及ぼす可能性があります。

コントロールプレーン



ここからは、DDI のコントロールプレーンについて説明します。本設計では、米国アルバカーキの本社に Grid Manager（GM）、英国ロンドンの大規模拠点に Grid Manager 候補（GMC）を配置しています。

Infoblox NIOS グリッドにおいて GM は、管理者が利用するウェブベースのユーザーインターフェースと、開発者が DDI タスクを自動化するために使用する API の両方を提供します。[1]GM は、グリッド内のすべての Infoblox メンバーとの通信および同期を管理します。[2]これらのアプライアンスは DNS や DHCP をはじめとする各種サービスを提供します。GM は重要な役割を担っているため、常に同一の物理サイトに Virtual Router Redundancy Protocol（VRRP）による高可用性（HA）構成のアプライアンスペアとして配備する必要があります。GM は、Advanced DNS Protection（ADP）のルールや Threat Insight モジュールの更新、管理にも使用できます。

GMC は GM のレプリカであり、リアルタイムで GM と同期されています。GM の役割を担う両方のアプライアンスが故障した場合でも、管理者は簡単なコマンドで GMC を GM に切り替える（または昇格させる）ことができます。切り替え後の GM は、グリッド内の他のアプライアンスに通知し、従来の GM の業務を引き継ぎます。GM と同様に、GMC も常に同一の物理サイトにおいて VRRP 高可用性（HA）構成のアプライアンスペアとして配備することが推奨されます。

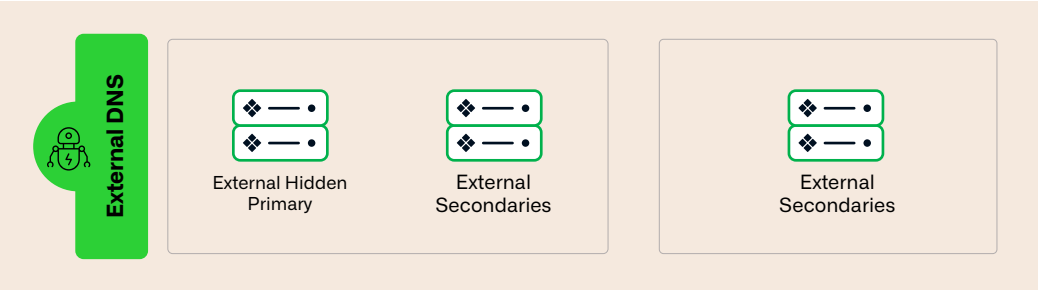
Infoblox Gridsは多くのGMCの指定をサポートしていますが、この会社はロンドンを災害復旧サイトとして特定しているため、そこでのみGMCをホストします。

本ドキュメントではサイジングの詳細には触れないと述べましたが、GMC のサイジングについては補足が必要です。GMC は、読み取り専用 API 呼び出しを処理できる（非常に便利な）機能を備えており、たとえば ACME が使用している ServiceNow との統合を支援する際などに役立ちます。GMC のサイジングを行う際には、GM にかかる負荷と、GMC が読み取り専用 API 呼び出しを処理することによって受ける負荷の両方を必ず考慮してください。災害などで GMC を GM に昇格させる場合、その GMC は、GM としての負荷に加え、GMC 時代の負荷もすべて処理できる必要があります。あるいは、1 台以上の GMC を追加し、それらを読み取り専用 API 呼び出し専用の処理に特化させるという選択肢もあります。

1 一部の例外を除き、詳細については「クラウド」セクションを参照してください。

2 注意：「アプライアンス」という用語は、物理アプライアンスと仮想アプライアンスの両方を指します。後者は、ほぼすべての仮想化プラットフォームおよびパブリッククラウドで走ります。

外部権威 DNS



外部の権威 DNS サーバーは、企業のゾーン情報をインターネット上に公開し、顧客やパートナーがメール送信、Web サイトの閲覧、インターネット向けアプリケーションの利用などを行えるようにします。これらのサーバーは可用性が企業の収益や顧客満足度、そして評判に直結するため、極めて重要な役割を担っています。

外部権威 DNS のインフラストラクチャは、3 台のサーバーで構成されています。アルバカーキ本社に配置された非公開のプライマリサーバーと、同じく本社とロンドンの大規模拠点にそれぞれ 1 台ずつのセカンダリサーバーで構成されています。各サーバーは、VRRP による高可用性（HA）構成のアプライアンスペアで運用されています。この構成により、たとえば BIND にバグや脆弱性が見つかった場合や、企業の成長に伴ってより大規模なアプライアンスが必要になった場合でも、DNS サーバーをダウンタイムなしでアップグレードできます。

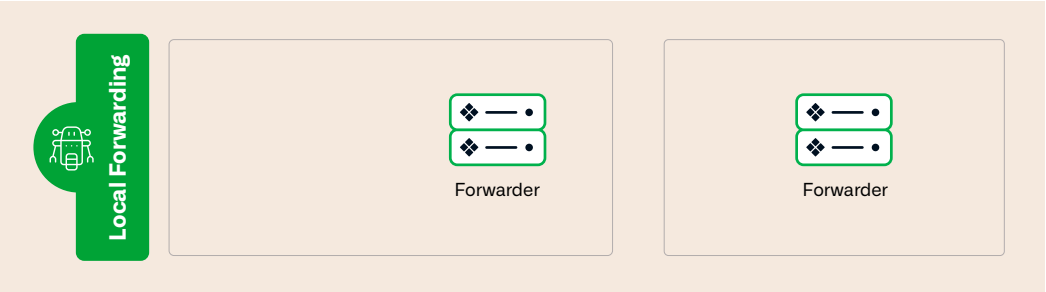
拡張された外部権威 DNS インフラストラクチャには、インターネットベースの DNS ホスティングプロバイダーが運用する DNS サーバーも含まれています。Cloudflare や、Neustar が提供する UltraDNS などのプロバイダーは、インターネット上に多数の DNS サーバーを分散配置しており、こうした広範なインフラは企業が自ら管理・運用するには困難かつ高コストです。ただし、こうしたホスティングプロバイダーもサービス停止に見舞われることがあります。[3]そのため、自社ネットワークと他の拠点にセカンダリ DNS サーバーを 2 台運用することは、コストを抑えつつ冗長性を確保する効果的な対策となります。もちろん、これは予想されるクエリ負荷に依存します。セカンダリサーバーの数が多くなる場合は、Anycast を活用することで特に高い効果が期待できます。

非公開のプライマリ DNS サーバーは外部ゾーンの権威データを保持していますが、インターネット上の DNS サーバーからのクエリには応答しません。その代わりに、この DNS サーバーはゾーン情報を DNS ホスティングプロバイダーに同期・複製します。

インターネットと直接通信する際の危険に対する追加の保護として、外部の権威 DNS サーバーは ADP を使用します。ADP は、DNS サーバーに対するさまざまな攻撃を検出し、軽減し、警告を発します。

3 例として、2016 年 10 月に発生した Dyn に対する DDoS 攻撃があります（https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn を参照）。

ローカルフォワーディング

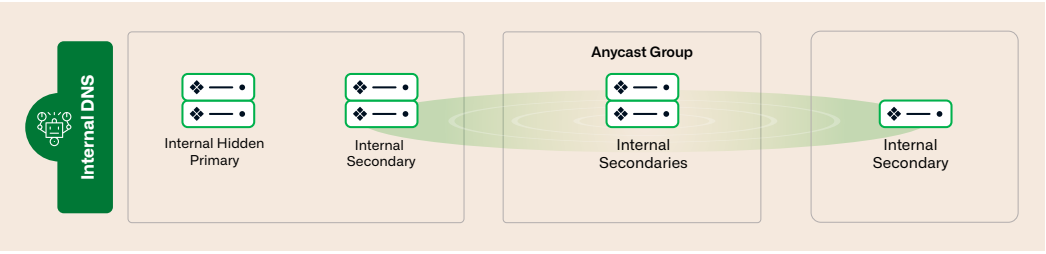


ローカルフォワーダーは、キャッシュフォワーダーとも呼ばれ、インターネット上のDNSサーバーに問い合わせることにより、内部DNSサーバーに代わってインターネットドメイン名を解決するように指定された内部DNSサーバーです。社内の一部の DNS サーバーのみがインターネット上の DNS サーバーと直接通信できるように制限することで、会社は、不正な形式の応答によって引き起こされるバッファオーバーランなどの潜在的な脆弱性へのリスクを低減しています。

同社にはフォワーダーが 2 台あり、1 台は本社に、もう 1 台は災害復旧用に指定された大規模拠点に配置されています。いずれも VRRP による高可用性（HA）構成のペアです。災害復旧用として位置付けられてはいるものの、大規模拠点のフォワーダーは、本社のフォワーダーが利用可能な状態であっても使用されており、冗長性に加えてスループットの向上にも貢献しています。内部 DNS サーバーは、クエリを送信する際の往復時間に基づいてフォワーダーを選択し、往復時間がほぼ同じであればランダムに選びます。したがって、内部 DNS サーバーは応答性に応じて両方のフォワーダーを活用します。これにより、両フォワーダー間の負荷が自然に分散される傾向があります。

インターネットとの直接通信に伴うリスクに対する追加の防御手段として、フォワーダーには ADP（Advanced DNS Protection）が導入されています。ADP は、DNS サーバーを標的とするさまざまな攻撃や、特定の有名な DNS トンネリングツールによって発生する大量トラフィックを検出・遮断します。低速かつ低頻度な DNS トンネリングに対しては、これらのアプライアンスに Threat Insight を導入することで対応可能です。Threat Insight の機能は、Infoblox ポータルと Infoblox DNS Forwarding Proxy（DFP）経由でも利用可能です。NIOS を使用した展開では、Threat Insight は応答ポリシーゾーン（RPZ）を使って適用を行います。

内部 DNS



DNS は非常に重要なネットワークサービスであるため、同社のすべての内部拠点にローカル DNS サーバーが必要です。本社には HA 構成の DNS サーバーが 2 組あり、そのうちの 1 組は内部ゾーンの非公開のプライマリとして機能しています。非公開のプライマリとは、クライアントからの問い合わせには応答せず、自身が管理するゾーンに対する動的更新の処理に特化したサーバーです。もう一方のサーバーはクライアントからのクエリを処理し、内部ゾーンのセカンダリとして機能します。他のドメイン名の解決には、フォワーダーのいずれかに問い合わせを行います。

同社の大規模拠点にも、セカンダリ DNS サーバーとして機能する HA 構成のサーバーペアが配備されています。小規模拠点には、HA 構成ではない単体のアプライアンスが設置されてい

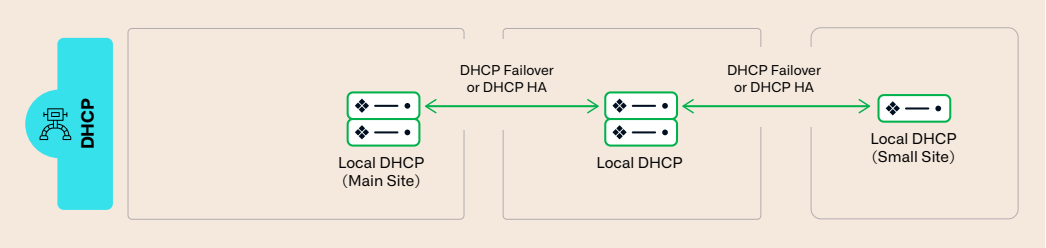
ます。DNS サービスのさらなる冗長性を確保するため、本社・大規模拠点・小規模拠点のすべての DNS サーバーは、いずれかの Anycast グループに属しています。グループ A の DNS サーバーには 1 つの仮想 IP アドレスが割り当てられており、グループ B のサーバーには異なる仮想 IP アドレスが割り当てられています。内部デバイス[4]は、まず 1 つ目の仮想 IP アドレスに DNS クエリを送信し、応答がない場合には 2 つ目に切り替えるようにスタブリゾルバが設定されています。この設定により、内部デバイスは最初のクエリを応答可能な DNS サーバーに確実に送信できるようになります。

すべての社内向けリカーシブ DNS サーバーには、RPZ（Response Policy Zone：応答ポリシーゾーン）が適用されています。RPZ は、Infoblox を含むインターネット上の RPZ プロバイダーから配信されており、悪用が確認されているドメイン名や、インターネット上で悪意のある動作が確認された権威 DNS サーバーの IP アドレスなど、脅威に関するリアルタイムの情報が含まれています。これにより、DNS クライアントが悪意あるドメインを解決するのを防ぐと同時に、解決を試みたデバイスを即座に特定できるため、企業の IT セキュリティチームは感染端末を迅速に発見、隔離することが可能になります。Threat Insight によって DNS トンネルが検出されると、それに応じて RPZ の 1 つが動的に構成されることがあります。

同社は地理的要因に基づいたアプリケーションも社内で運用しており、企業ネットワーク内のどのユーザーでもそれらのアプリケーションを利用できます。あわせて、負荷分散と冗長性の確保も求められています。Infoblox DNS Traffic Control（DTC）は、クライアントの位置、サーバーの可用性、ネットワークトポロジに基づいて DNS トラフィックをインテリジェントに制御し、アプリケーションの応答時間とパフォーマンスを最適化する負荷分散ソリューションです。DTC は、社内の権威 DNS サーバー上に構成されています。

リモートオフィス向けの DNS については、「リモートオフィス」という別セクションで詳しく説明します。

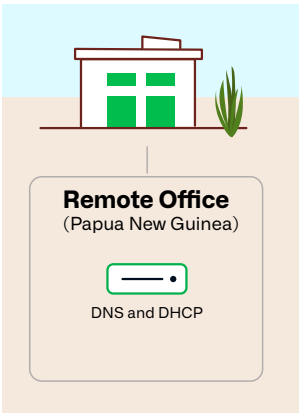
DHCP



DNS と同様に、DHCP も重要なネットワークサービスであるため、すべての社内サイトにはローカル DHCP サーバーが必要です。DHCP は DNS と同様に、本社と大規模拠点では HA（高可用性）構成のペアで、小規模サイトでは単一のアプライアンスによって提供されます。ただし、さらなる冗長性を確保するため、DHCP サーバーはフェイルオーバー構成で設定されています。各 DHCP サーバーには対になるピアが存在し、リースプールに関する情報を共有しており、どちらのサーバーからでもクライアントにリースを提供できるようになっています。この構成により、単一アプライアンスしかない拠点でも、冗長な DHCP サービスを実現できます。これらの DHCP サーバーは、内部ゾーンの非公開のプライマリ DNS サーバーに対して、動的 DNS（DDNS）を用いてレコードの更新を行います。

リモートオフィス

同社のリモートオフィスは、定義上小規模であり、それぞれ少人数の従業員しか常駐していません。しかし、リモートオフィスの数は多く、インターネットや他の社内ネットワークとの接続は依然として重要です。ほとんどのリモートオフィスには高速インターネット接続がありますが、社内ネットワークとの専用接続は



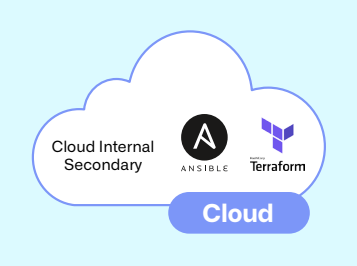
4 リモートオフィスにいる方を除く：構成については「リモートオフィス」セクションを参照してください。

なく、代わりに VPN を通じて DNS と DHCP サービスのトラフィックを社内ネットワークへ送信します。このようなケースに対応するため、同社は Infoblox のクラウドマネージドDDI ソリューションである Infoblox Universal DDI™ を使用して、リモートオフィスに DNS および DHCP を提供しています。各クラウド管理アプライアンスである NIOS-X は、リモートオフィスに対して DNS と DHCP のサービスを提供します。リモートオフィスの DNS サーバーは、同社の Anycast インフラストラクチャには含まれておらず、リモートオフィス内のクライアントはまずローカルの DNS サーバーに問い合わせを行い、それが利用できない場合には Anycast グループの 2 つの IP アドレスにフォールバックします。

冗長性のある DHCP を提供するため、各リモートオフィスの DHCP サーバーは、近隣のリモートオフィスの DHCP サーバーと高度なアクティブ／パッシブ構成で連携しています。これにより、両方のサーバーがそれぞれのリモートオフィスのクライアントに DHCP を提供できるようになり、リモートオフィスにおいても冗長な DHCP サービスを実現できます。

業務を完全にインターネットに依存するオフィス向けの代替策として、NIOS-X as a Service があります。これは、Infoblox が提供するマネージド型のクラウドベース DDI ソリューションです。これらの重要なネットワークサービスをクラウドでホストすることで、スケーラビリティ、柔軟性、そしてセキュリティが強化され、オンプレミスのハードウェアは不要となります。NIOS-X as a Service は、他の Infoblox ソリューションとシームレスに統合され、ネットワーク管理とセキュリティに対して統一されたシンプルなアプローチを提供し、信頼性が高く効率的なネットワーク運用を実現します。

クラウド



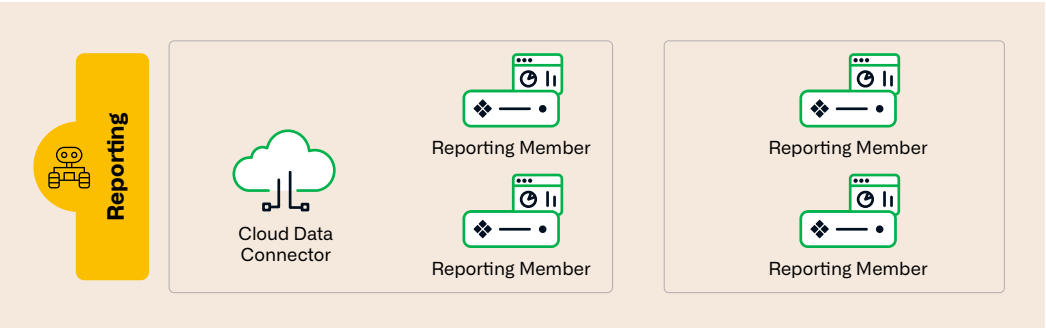
同社は、社内とインターネット向けのアプリケーションをサポートするために、複数のパブリッククラウドを活用しています。各クラウドには、クラウドアプリケーションやワークロードが内部ゾーンのドメイン名を解決するために必要な、セカンダリとして構成された 1 台以上の仮想クラウドプラットフォームアプライアンスがホストされています。これは、内部 DNS サーバーへのクエリ転送に条件付きフォワーディングを使う方法よりも、高い弾力性を提供します。

このクラウドプラットフォームアプライアンスは、会社のプロビジョニングシステム（Terraform と Ansible）がリソースレコードを管理する必要があるクラウドゾーンのプライマリとしても構成されています。Terraform と Ansible をグリッドに統合するために、Terraform には Infoblox Terraform Provider が、Ansible には Ansible Automation 向けの Infoblox NIOS Collection が使用されます。

Infoblox の Cloud Network Automation（CNA）は、仮想プライベートクラウド／仮想ネットワーク、サブネット、仮想マシンなどの使用中のクラウドリソースを可視化し、クラウドネットワーク環境の全体像を把握できます。さらに、CNA は仮想検出プロセスによって発見された新しいリソースに対して、DNS レコードを自動で作成することができます。

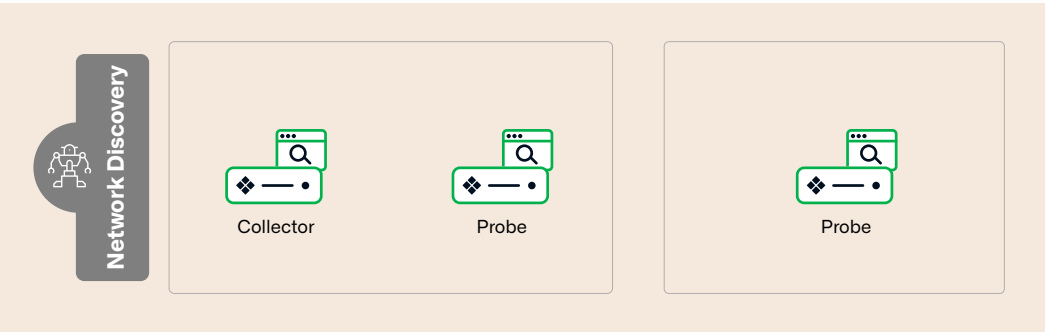
同社が Amazon Route 53 や Azure DNS などのクラウド固有の DNS サービスを利用している場合、それらは同期を通じてグリッドと統合できます。これにより、グリッドのインターフェースと API を通じて、すべての DNS データを一元的に可視化・管理できます。

レポート



グリッドのレポート機能を支えるため、同社は本社に 2 台、指定された災害復旧拠点に 2 台、計 4 台のレポートサーバーを使用しています。4 台のサーバーを使用することは必須ではありませんが、冗長性とパフォーマンスの両面で利点があります。本社側のレポートサーバーが 1 台、あるいは両方故障したとしても、レポートデータが失われることはありません。レポートデータは引き続きインデックス化され、レポートの生成やデータに対する検索も継続して行うことが可能です。4 台のレポートサーバーがある場合、最適な配置は GM 側に 2 台、災害時に昇格させる GMC 側に 2 台設置する構成です。

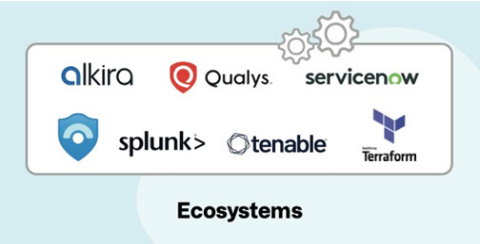
ネットワーク検出



ネットワークディスカバリーは、IPアドレス管理ソリューションの重要なコンポーネントです。ディスカバリーにより、DDIデータベースがネットワークの理想化された状態ではなく、実際の状態を反映していることが保証されます。仮想ディスカバリー機能は、企業のオンプレミス仮想環境およびクラウド環境でのディスカバリーを提供しますが、企業のエンタープライズネットワークにもディスカバリーが必要です。

ネットワーク検出をサポートするアプライアンスは複数あり、本社に 2 台、各大規模拠点に 1 台ずつ配備されています。本社のアプライアンスのうち 1 台は「コンソリデーター」として指定されており、各プローブから検出されたすべてのデータを収集・統合し、GM に複製して DDI データベースに登録します。他のアプライアンスはプローブとして機能し、ネットワーク上のデバイスを検出するために必要なクエリ送信、プロービング、ポーリングを実行します。

外部システムおよびエコシステムの統合



同社では、SIEM システム、チケット発行システム（ServiceNow を使用）に加え、従業員が DDI データベースに対する簡単な変更をリクエストできるセルフサービスポータルなど、さまざまな用途にクラウドベースおよび社内システムの両方を利用しています。グリッド内のアプライアンスは、ログ出力を SIEM に直接送信します。pDNS データなどの DNS ログは Infoblox Data

Connector に送信されます。これは、DNS サーバー側の負荷を軽減するほか、外部システムにデータを送信する前にフィルタリング処理を行うことができるためです（たとえば、内部クエリだけの記録を避けたい場合などに有効です）。

ServiceNow はグリッドと連携して、ユーザーが DDI データベースへの変更（例：IP アドレスの予約、追加、削除）をリクエストできるようにします。また、グリッドはデバイスの参加や離脱、セキュリティ問題の検出時に ServiceNow に通知を送信し、システムにアラートを提供します。

Infobloxは、脅威の早期可視化、信頼性のあるIPアドレス、およびコンテキストに基づくネットワークデータを既存のツールと共有することで、サイロを解消し、ITセキュリティスタック全体を強化し、ROIと運用効率を向上させます。Infobloxエコシステムは、幅広いセキュリティ、ネットワーキング、クラウドツールとシームレスに統合し、オンプレミス、ハイブリッド、マルチクラウド環境全体で脅威検出を強化し、ワークフローを自動化し、対応能力を向上させます。

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：20250221v2