



F5XC の導入で変わるDNS運用 : DR対策と負荷軽減の実例

F5ネットワークスジャパン合同会社

Solutions Architect

Akira Suzuki

July 2024

F5 Distributed Cloud (F5XC)の構成コンポーネント



Volterra
分散クラウド基盤
=
+
既存技術を統合

F5XCは、SaaS基盤を
利用したソリューション

f5 BIG-IP

N NGINX
Part of F5

F5は、“BIGIP” だけじゃないんです！

F5グローバルネットワーク

Webアプリケーションへの攻撃を最寄りのF5データセンターで防御

- 約30拠点のデータセンター
- 数十Tbps以上の帯域
- 世界中のISPとピアリング
- 自動拡張型デザイン



各PoP配下でDNSサービスを提供

DNSサービスのオンプレの課題や DR (Disaster Recovery)の重要性

DNSのDR(Disaster Recovery)の重要性

- DNSサービスの重要性を考えると、インターネットの今回を支える技術であるため、サービス停止を極力抑える必要がある。

1. インターネットアクセスの可用性

→DNSは、ユーザーがドメイン名を入力するとIPアドレスに変換する役割を担っており、この変換が機能しないと、ユーザーはウェブサイトにはアクセスできなくなります。DNSの障害はインターネット全体のアクセスを妨げるため、可用性を確保することが重要です。

2. ビジネスの継続性

→企業のウェブサイトやオンラインサービスが利用できなくなると、売上の損失や顧客の信頼を失う可能性があり、DNSのDR計画により、障害発生時にも迅速に対応し、サービスを復旧させることができます。特にeコマースサイトやオンラインバンキングなどのクリティカルなサービスにとってはDRの重要となります。

3. セキュリティ

→DNS障害は、DDoS攻撃などのサイバー攻撃の一環として発生することがあります。DR計画は、こうした攻撃に対する耐性を高め、迅速な復旧を可能にすることで、セキュリティを強化できます。

4. 顧客満足度の維持

→DNS障害はユーザーエクスペリエンスに直接影響します。迅速な復旧とサービスの継続性を確保することで、顧客満足度を維持することができます。特に、顧客がサービスの停止によって不便を感じることをないようにするために、DRは重要です。

オンプレDNSの課題

・DNS運用をオンプレで実施されている方が多いと思いますが、その点の課題でどう言ったものがあるのでしょうか？

1. 可用性と冗長性の確保

→オンプレでDNSを運用する場合、ハードウェアやネットワークの障害が直接的に影響を与えます。
サーバーがダウンすると、DNS解決が行えなくなり、ウェブサイトやサービスが利用できなくなるリスクがある。

2. スケーラビリティ

→オンプレのDNSサーバーは、トラフィックの急激な増加に対してスケーリングが難しい場合があります。
特にDDoS攻撃などに対しては、サーバーのリソースが限られているため、対応が困難です。

3. 管理とメンテナンスの負担

→オンプレDNSは、自社でのハードウェア管理やソフトウェアの更新、セキュリティパッチの適用が必要です。
これらの作業は時間とリソースを消費し、専門知識も求められます。

4. セキュリティリスク

→オンプレDNSサーバーは、外部からの攻撃（例えばDDoS攻撃やキャッシュポイズニング）に対して脆弱です。
これにより、DNSサービスが停止したり、ユーザーが偽のサイトに誘導されるリスクがある。

5. コスト

→オンプレDNS運用は、初期導入コストやハードウェアの更新、保守費用がかかります。また、必要なスタッフの人件費も考慮する必要があります。

いま説明した課題を解決するには・・・

- ・今、説明した課題を解決するために・・・一案として、



SaaSを利用したDNSサービスを利用してみることを考えてみるのもありではないでしょうか？

1. 高可用性と冗長性

→SaaSベースのDNSサービスは、複数の地理的に分散したデータセンターを持っており、冗長性と高可用性を提供します。これにより、DNSサービスの中断リスクが大幅に減少します。

2. スケーラビリティ

→SaaSベースのDNSサービスは、自動的にスケーリングされ、トラフィックの急増にも対応できます。これにより、オンプレミスのDNSサーバーで発生するリソース不足の問題を回避可能です。

3. セキュリティ

→DDoS攻撃やキャッシュポイズニングなどのサイバー攻撃に対する高度なセキュリティ対策を提供します。例えば、DNSSECのサポートやトラフィックの監視・フィルタリングを行うことで、セキュリティを強化可能です。

4. 運用と管理の簡素化

→SaaSベースのDNSサービスを利用することで、ハードウェアの管理やソフトウェアの更新、セキュリティパッチの適用など運用負担が軽減されます。プロバイダーがこれらの管理を代行するため、IT部門は他の重要な業務に集中できます。

具体的な事例紹介

ミライコミュニケーション様の事例紹介



CUSTOMER STORY
株式会社ミライコミュニケーションネットワーク

大規模な攻撃を契機に、DDoS対策の導入を検討。
HiddenプライマリDNSなど機能性、導入時の柔軟性を評価し、
F5のクラウドサービスを導入

Products

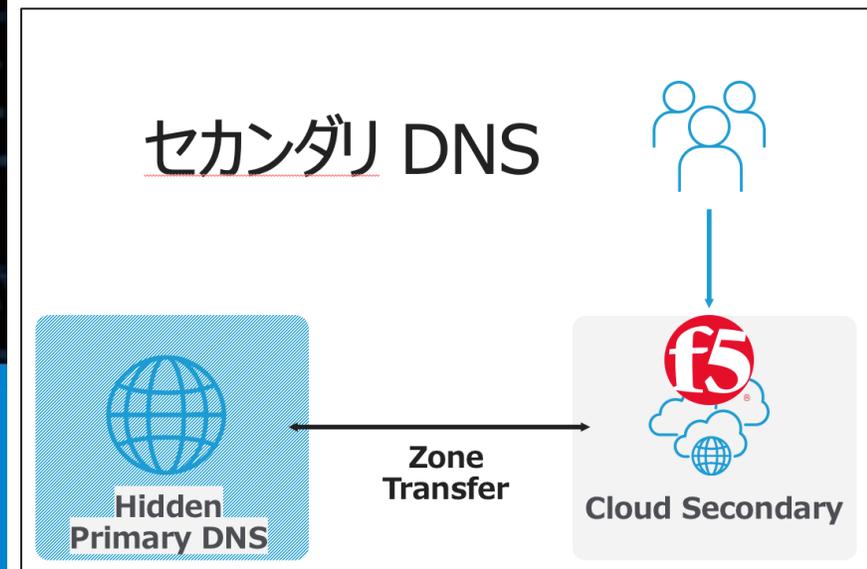
- ・ Distributed Cloud DNS

Challenges

- ・ DNSサーバへのDDoS攻撃に対処
- ・ クラウド型サービスの迅速な導入
- ・ 自治体の入札に対応可能な予算管理

Benefits

- ・ 既存のDNSサーバ活用により、迅速な導入が可能
- ・ クラウド上のセカンダリDNSがすべてのクエリに対応
- ・ バージョンアップ作業など、運用負荷軽減



F5XCで何が課題でどう解決できるか・・・

- ・ 2023年12月にDNSへのDDoS攻撃があり、名前解決が困難な状態を経験した

→ DNSへのDDoS対策サービスの導入が必要だと判断

- ・ プライマリ・セカンダリDNSの選択の柔軟性

→ 他社サービスの場合、プライマリ、セカンダリの利用を契約時に確定する必要があった。
運用時でもF5XCは自由に選択可能。

- ・ コストについて

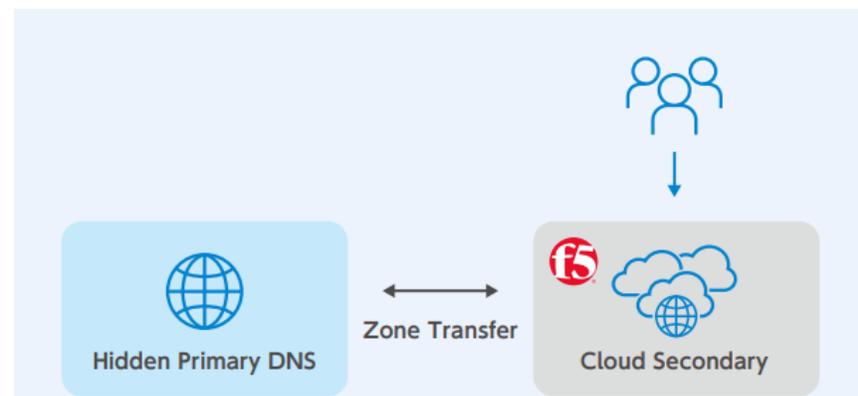
→ 他社はクエリ課金でコスト変動するなど

F5XCはその点、Zone数を基準にした課金方式で、契約期間中の追加課金がないというメリットがあります。

- ・ 現状の構成を生かした構成

→ 既存のプライマリDNSサーバをそのまま利用でき、変更作業などの手順、運用形態の変更の必要がない点。セカンダリDNSをSaaSにすることで、DR的に利用方法が可能。

F5XC自身、多機能を持ち合わせており、DNSに特化したサービスから将来的にサービスの拡張性の可能性。



F5 Distributed Cloud DNSは、Primary/Secondary DNSの設置が可能です。既存のPrimary DNSはそのまま設定専用として利用し、F5のクラウド上にSecondary DNSを置いてDNSクエリを処理することで、DDoS攻撃からの防御や、地理的に分散されたクラウドネットワークによるレスポンス改善を実現します。

動作デモ (Primary DNS設定)

F5XC Primary DNS設定デモ

The screenshot displays the F5 Distributed Cloud Console interface. The main content area features a "Welcome to the F5 Distributed Cloud Console" message and a "Common services" section. The "DNS Management" service is highlighted, with a description: "Configure and manage primary or secondary DNS service". To the right, a terminal window shows the command `a.suzuki@GHL4TLDP25 ~ % dig f5jp-test.net NS` being executed against a background image of rolling hills.

f5jp-handson Distributed Cloud Console Home

Search

Support

Welcome to the F5 Distributed Cloud Console

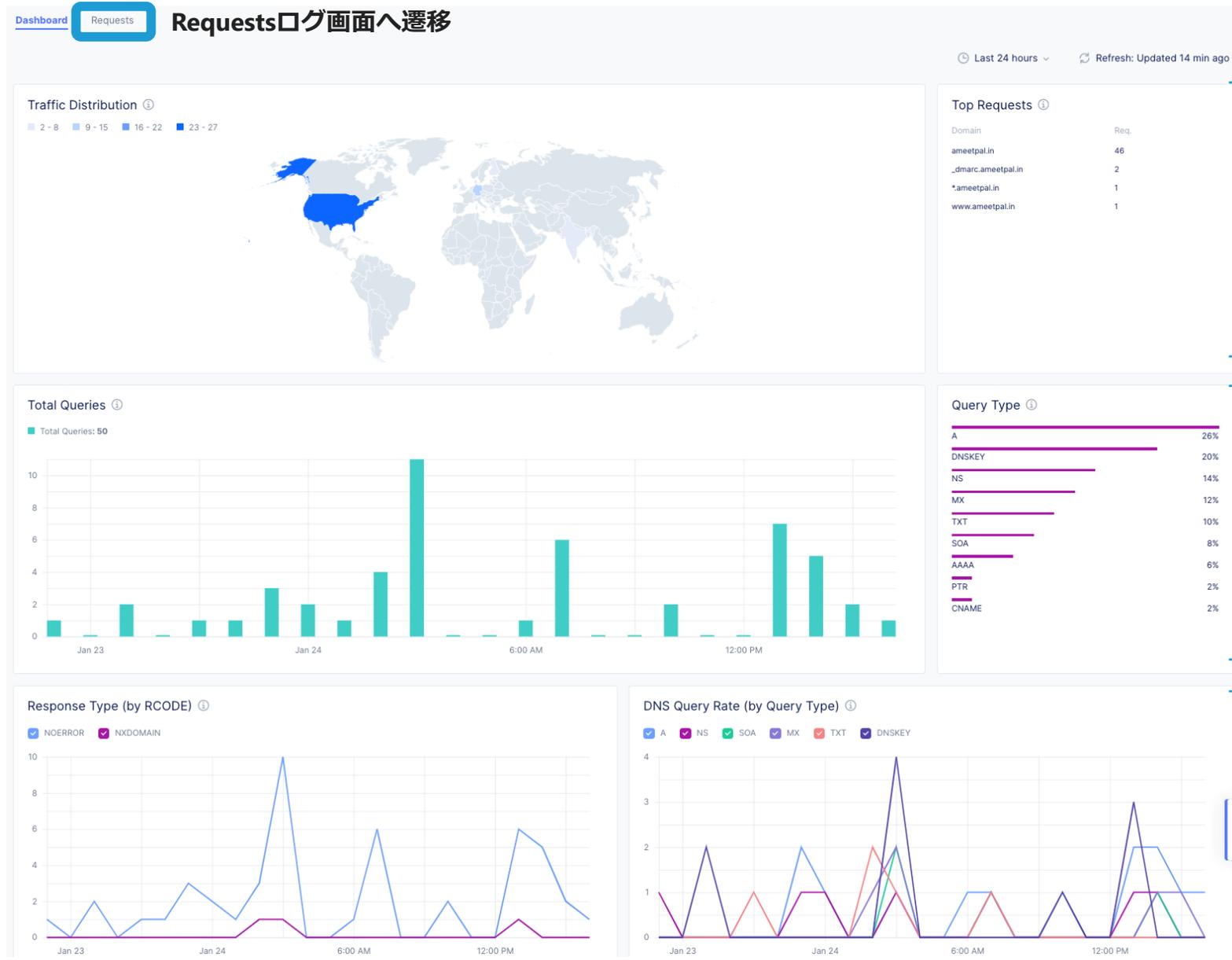
F5 Distributed Cloud Console delivers a set of networking, security, and app management services that can be used to solve various use-cases.

Common services [View Catalog](#)

- Web App & API Protection**
Create a load balancer and configure WAF, Bot, and API security services for your apps
- Multi-Cloud Network Connect**
Networking & security across clouds, edge and on-premises
- Multi-Cloud App Connect**
Connect apps across clouds, edge and on-premises using Load Balancers
- Distributed Apps**
Deploy apps in our global PoPs (REs) or your cloud/edge sites
- DNS Management**
Configure and manage primary or secondary DNS service
- Bot Defense**
Deploy bot mitigation for F5 BIG-IP and other 3rd party services
- Data Intelligence** New
Advance Your Security Intelligence and Fraud Defenses
- Client-Side Defense** Preview
Monitor and mitigate fraudulent app requests at the client devices

[Help](#)

Performanceダッシュボード



国別送信元分布

リクエスト数多い
ドメイン名リスト

時系列での
クエリの
ヒストグラム

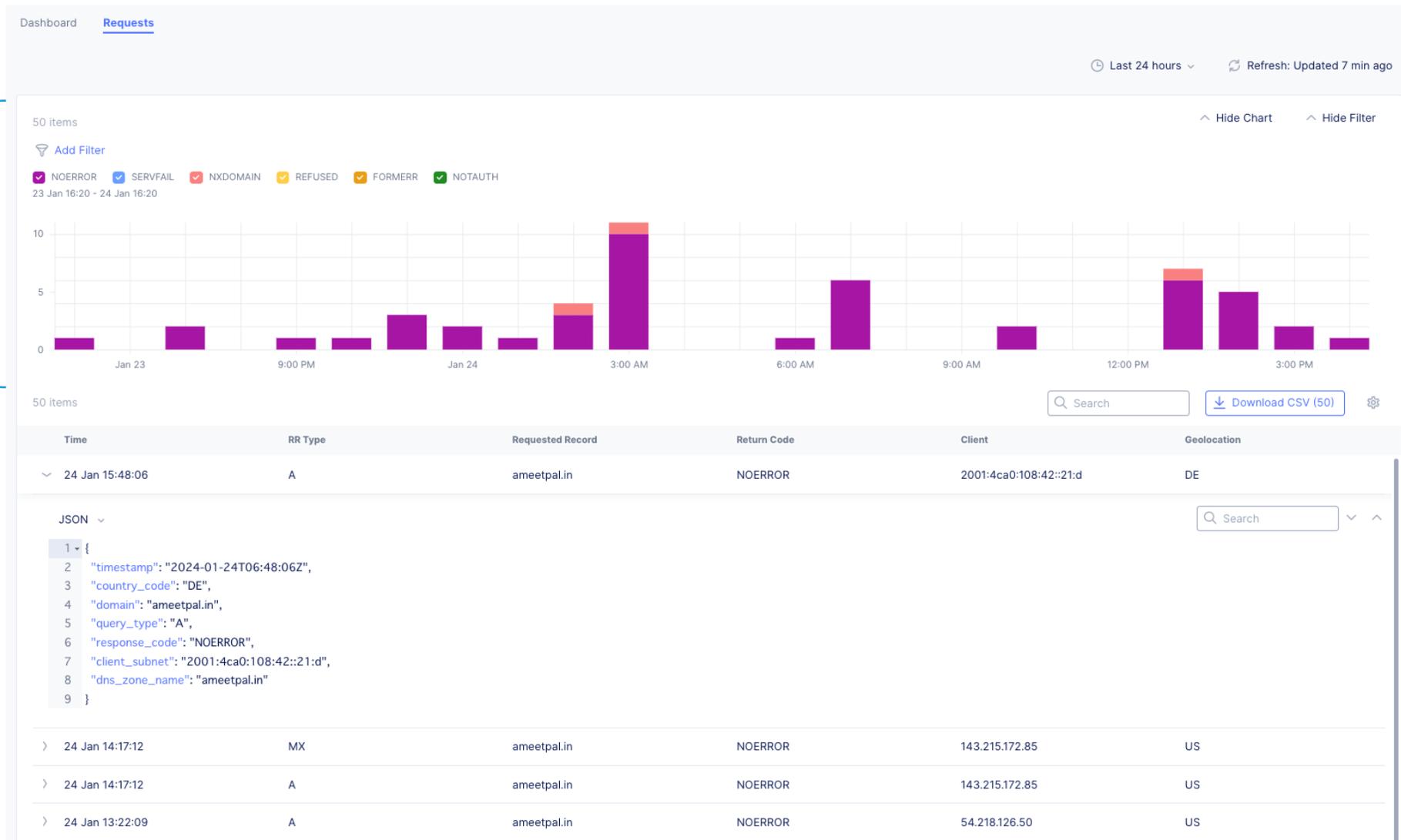
クエリタイプ別の
占める割合

時系列での
応答タイプ
数量

時系列での
クエリタイプ別
リクエスト数

Requests ログ画面

時系列での
リクエスト
統計



個別
クエリログ

