efficient iP®

White Paper

Hybrid Cloud DNS: Best Practices for Business Continuity

With Gartner predicting that 90% of enterprises will adopt hybrid infrastructure management capabilities by 2020, it is common knowledge that hybrid cloud adoption is exploding. This growth includes increased use of the internet to deliver applications, sites and services to employees, partners and customers. As DNS is a foundation for application routing, it makes sense therefore for DNS to be extended to public and private cloud environments.

efficient iP®

White Paper

Outline:

Single points of failure will make your business inaccessible

DNS-based attacks - the fastest growing security threat vector

Where are my IP resources ?

Best practices for DNS in cloud architectures

Keeping your business always-on

DNS delivers a critical network service that allows users to reach online business applications, ensuring accessibility of the services you offer. For hybrid cloud environments, deploying DNS servers only in-house brings limitations regarding internet visibility of your business. Conversely, relying solely on DNS servers hosted in public cloud can have significant negative impact on resiliency, consistency control and security of DNS resources. As for all business-critical applications, the optimum solution is therefore undoubtedly to move to a mix of in-house and public cloud DNS - a hybrid cloud DNS solution. However, to ensure service availability, performance, security and efficient management of resources across the hybrid landscape, best practices such as those listed below will need to be incorporated.

Single points of failure will make your business inaccessible

When it comes to DNS in cloud environments, internet visibility is essential for ensuring availability of your website and business-critical services at all times. First and foremost, single points of failure (SPoF) must therefore be avoided. Putting all your eggs in one basket - relying only on having on-premise DNS or only a single public cloud DNS provider for internet visibility - is a risky business. How can you ensure 100% availability for accessing all your services (intranet, supplier portal etc.) or website if your public cloud hosted DNS server a) goes down or b) suffers a cyber attack?

Losing access to DNS services could significantly impact a business's profitability. Imagine the case of an automobile vendor whose business portal is accessed by suppliers as well as customers. If the company relied only on a public DNS server for access to their portal, and the DNS server went down just for an hour or so, all users would lose visibility to the site. As the cost of downtime can be as much as $100,000 per minute (Ponemon Institute study), the results to the company's bottom line and brand image would be catastrophic.

DNS-based attacks - the fastest growing security threat vector

Because of the fundamental role they play in IT infrastructure, public DNS servers are constantly exposed to internet-based attacks and therefore must be secure at all times. This threat is enhanced by the proliferation of non-secure IoT devices that can be easily compromised by hackers and used for large volumetric attacks. The consequences can be dire, as was the case when cloud DNS provider Dyn was attacked and went down in 2016. Businesses affected included some of the largest and most sophisticated organizations on the planet. As they solely relied on Dyn for DNS services, they had no chance of keeping their websites visible and accessible.

Even the largest cloud provider, AWS, is unable to guarantee 100% availability under DDoS attacks, so retaining your local DNS-based service in conjunction with deploying hosted cloud DNS allows you to stay online even if your cloud provider is attacked. Conversely, by having a cloud DNS as an alternative to your own local service, you're covered if your local server is overwhelmed by a direct attack.

Where are my IP resources ?

Those businesses who have already made or are considering the move to hybrid cloud DNS often ask questions around efficiency of operational management. How can I overcome the complexity of managing both internal & public DNS? Amazon Route 53 DNS service offers limited, user-unfriendly support beyond pure AWS environments, which means enterprises cannot create a single, unified DNS-DHCP-IPAM (DDI) solution to serve their entire enterprise with Route 53 alone. Route 53 focuses on only AWS environments, which limits connectivity, visibility, and security when used for non-AWS cloud platforms.

Having a lack of visibility - without a consistent DNS and IPAM solution across the hybrid cloud landscape - means that the IT manager is forced to use several tools to access DNS and IP address data. This leads to inconsistencies in the DNS and IP address space across the enterprise and longer troubleshooting times, as well as making network planning more difficult.

Best practices for DNS in cloud architectures

Hybrid clouds are here to stay for many years, so it is imperative to implement best practices in order to ensure their availability, performance, ease-of-management and security.

Recommendations include:

1. Ensure business accessibility - eliminate single points of failure by implementing a hybrid cloud DNS architecture - a mix of in-house and hosted cloud DNS - to guarantee 100% availability for both public and private services.

One key part of the DNS specification is that it is a distributed system that lets you use multiple servers to host your DNS zones - servers that can all be accessed simultaneously. A hybrid scenario commonly used is to extend public DNS services to Amazon Web Services (AWS) Route 53 global network - a highly available and scalable cloud-based DNS service designed to give businesses an extremely reliable and cost effective way to route end users to Internet applications.

A modern DDI Solution permits dynamic set up and management of the DNS services provided in the Cloud, ensuring correct synchronization of your global DNS infrastructure and proper integration with the embedded IPAM.

2. Maximize customer experience & meet SLAs - provide multiple points of presence and synchronise DNS database across them to reduce latency.

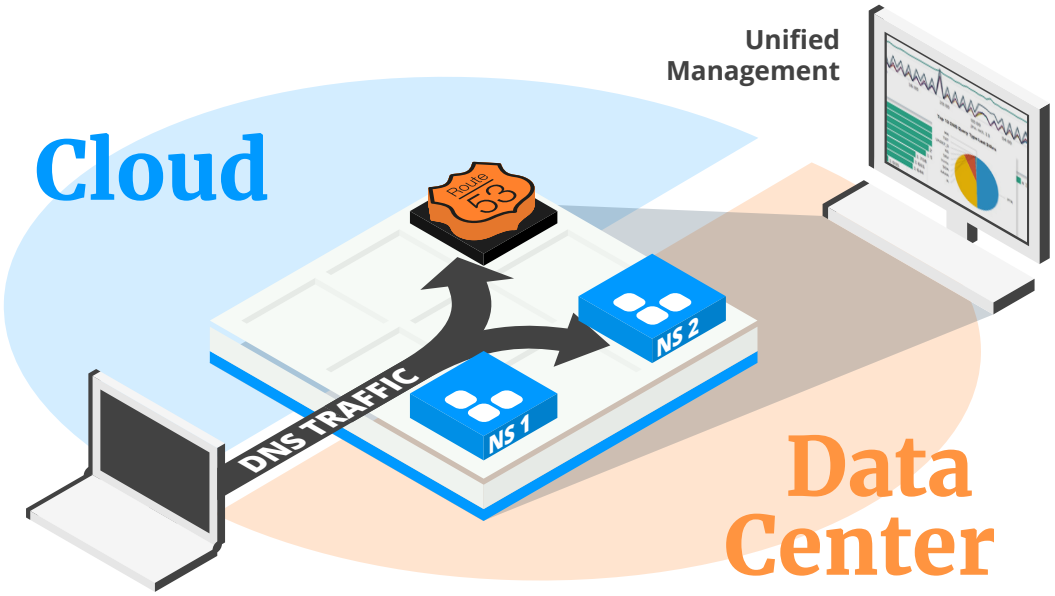
Having multiple points of access (AWS offers more than 52 access points distributed across the world), SLA and customer experience is greatly improved by routing end users to the AWS region that provides the lowest possible latency. Without multiple access spots, if you are a customer in Tokyo and your sole DNS server is located in New York, you most likely will experience some delay sending information back and forth for DNS resolution. By duplicating DNS records across multiple points of presence via Anycast functionality, allowing you to access a DNS server much closer to you, this latency is significantly reduced.

3. Simplify management & provide instant-start services - use an integrated DDI solution to provide a centralized, global view, with consistent, automated configuration.

Once the move to hybrid cloud DNS has been made, it is imperative to keep your DNS servers in sync by simplifying operational management across the internal and public DNS landscape. Fortunately, advanced DDI's are able to integrate with the Route 53 DNS service to provide a centralized console to manage combinations of on-premise, AWS public cloud and private cloud deployments.

The benefits this brings include:

- Complete visibility - from a single pane-of-glass interface, central management of domain name service in the cloud and in-house multi-vendor DNS servers.
- Consistent resource data - DNS records across multiple platforms are integrated within a single platform to improve manageability and consistency. Automation reduces time and cost of configuration modifications and eliminates errors.
- Fast time to market - in a few easy steps, your DNS services are distributed across a series of worldwide locations.



Unified Management for Hybrid Cloud DNS Architecture

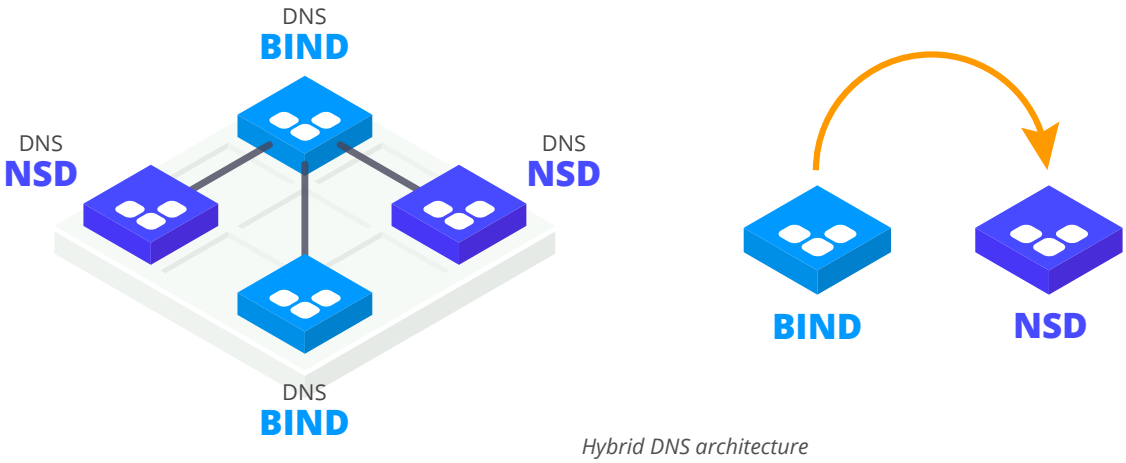
Adding 1-click reversibility provides an easy way to revert from a cloud-based deployment back to full on-premise deployment. This makes hybrid cloud deployment very flexible - you can test a cloud infrastructure and revert back to in-house, in one quick step.

4. Enhance security - leverage innovative in-house DNS Security solutions to protect against all attacks including zero-day, DDoS and data theft. Combined with DNS firewalls, these solutions will help contain the spread of malware.

Hybrid architectures are certainly a secure approach to stand against zero-day attacks - it is unlikely to find the same weakness at the same time in software maintained by different editors. This means only one subset of a platform can be impacted at a time, ensuring availability and integrity of the DNS service.

For in-house DNS recursive functionality, protection against zero-day attacks can be further augmented by implementing innovative DNS Security features such as having multiple DNS engines in one single appliance, allowing customers to switch in real-time from one engine to another during an attack or when maintenance is needed to apply security patches to the primary DNS engine.

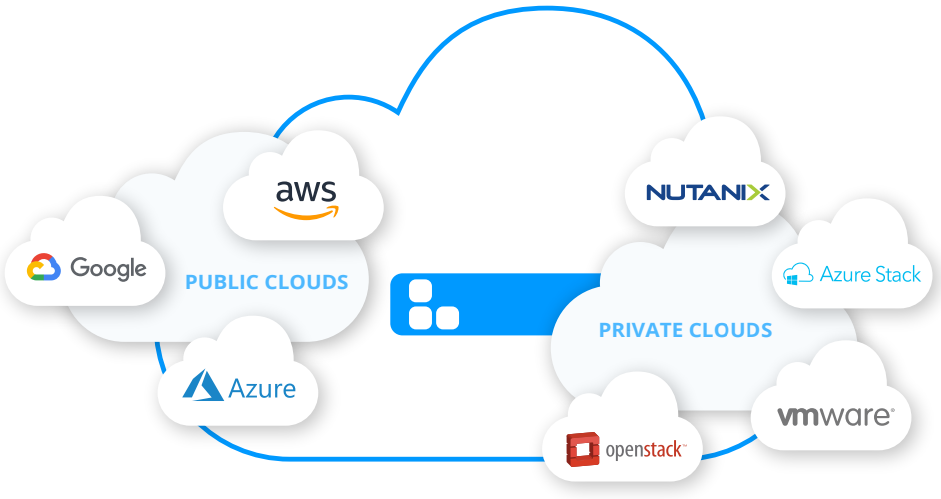
Furthermore, by using hybrid DNS architectures where two active DNS technologies can be mixed on the same cluster, your users will continue using an unaffected server in the event of a DoS attack exploiting a vulnerability. This ensures continued access to your servers, while at the same time preventing the automatic retries designed to multiply the effects of the initial attack.



Hybrid DNS architecture

Additional protection for the local DNS infrastructure against DDoS is also recommended, in particular by utilizing high-performance DNS engines - the most advanced ones can absorb up to 17 million DNS queries per second. These engines will thwart the attack and leave your business unaffected, consequently avoiding costly impacts due to inaccessibility to your applications or website. Lastly, in order to avoid hefty GDPR penalties, organizations need to prove they have made suitable efforts to protect sensitive employee and customer data. Innovative solutions involving real-time analytics, such as DNS Transaction Inspection (DTI), can considerably help to detect data exfiltration attempts.

5. Future-proof your business - select DDI solutions which are "cloud-agnostic", with multi-vendor support for virtualization and orchestration in order to be ready to support public clouds beyond AWS. The DDI solution should be highly scalable (able to manage millions of IP addresses), support multi-tenancy and offer a complete global view of IP resources across your entire hybrid landscape.



Multi-cloud DDI solution

Keeping your business always-on

It is industry best practice to not rely on a single technology in order to avoid any single point of failure, so why not apply this best practice to DNS architecture when EfficientIP offers you such an easy solution for this. In addition, incorporating an advanced DDI solution with automation and orchestration functionality will provide unified, flexible, effortless management resulting in consistent, accurate provisioning, as well as global visibility of IP resources across the hybrid landscape. Lastly, leveraging innovative in-house DNS security functionality will make sure your network is well protected against all attack types and that sensitive data is secure.

Adhering to the above DNS best practices for hybrid cloud infrastructures is sure to help guarantee access to your network applications and other indispensable services, such as email, e-commerce or supplier portal. This should go a long way towards ensuring your business is “always-on”.

efficient iP®

REV: C-1711

As one of the world’s fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752