LÖSUNGSHINWEIS

NAHTLOSE KONTROLLE UND SICHERHEIT FÜR HYBRIDE CLOUD-BEREITSTELLUNGEN MIT AMAZON ROUTE 53 UND INFOBLOX

ZUSAMMENFASSUNG

Der DNS-Dienst Amazon Route 53 bietet über reine Amazon Web Services (AWS)-Umgebungen hinaus eingeschränkte Unterstützung.

Diese Einschränkungen bedeuten, dass Unternehmen keine einzige, einheitliche DNS-, DHCP- und IP-Adressmanagement-Lösung (DDI) erstellen können, um ihr gesamtes Unternehmen, einschließlich ihrer Campusnetzwerke und hybriden Clouds, nur mit Route 53 zu bedienen. Route 53 konzentriert sich nur auf virtuelle private Clouds (VPCs) von AWS, was bei Verwendung für Nicht-AWS-Cloud-Plattformen die Konnektivität, Sichtbarkeit und Sicherheit einschränkt.

Infoblox integriert seine branchenführende DDI-Plattform mit AWS und Amazon Route 53 DNS und bietet eine einheitliche, kommerzielle Enterprise- und Service-Provider-Lösung für AWS- und Hybrid-Cloud-Bereitstellungen. Die Infoblox-Integration mit Amazon Route 53 überbrückt die Kluft zwischen Unternehmens-IT und Cloud-Teams. Sie reduziert die Komplexität und hilft, optimale Sicherheit zu erreichen, indem sie eine einzige Steuerungsebene bereitstellt, um On-Premises-, Private-Cloud- und AWS-Public-Cloud-Bereitstellungen zu verwalten, während sie die Sicherheit dieser Bereitstellungen verbessert. Diese Lösung erfüllt die Anforderungen aktueller und zukünftiger Infoblox-Kunden, die zu AWS expandieren und Amazon Route 53 für DNS nutzen.

MANGELNDE TRANSPARENZ, AUTOMATISIERUNG UND KONSISTENZ KÖNNEN AMAZON ROUTE 53-BEREITSTELLUNGEN BEEINTRÄCHTIGEN

Amazon Route 53 bietet private DNS-Funktionalität innerhalb von AWS VPCs. Ein Unternehmen, das eine hybride Cloud nutzt, steht jedoch auch bei der Nutzung von Amazon Route 53 vor operativen Herausforderungen:

- **Eingeschränktes DNS:** Die DNS-Auflösung oder die Antworten auf Anfragen sind innerhalb ihres AWS-Netzwerks isoliert, was zu Problemen führt, wenn Kommunikation außerhalb einer bestimmten AWS Private Hosted Zone erforderlich ist. Um dieses Problem zu umgehen, richten IT-Teams häufig mehrere BIND-Server ein, um den DNS-Verkehr außerhalb der isolierten AWS-Zonen zu leiten. Dieser Ansatz erhöht die Komplexität und es mangelt an Konsistenz über verschiedene DNS-Bereitstellungen hinweg.
- **Kein IPAM:** AWS hat keine Lösung für das IP-Adressmanagement (IPAM) und bietet oft nur eine eingeschränkte Sichtbarkeit von virtuellen Instanzen, was sich negativ auf das tägliche Management auswirkt und zusätzlichen Zeitaufwand für Audits und Compliance-Zwecke erfordert.

ENTWICKLUNG EINER EINHEITLICHEN DNS- UND IPAM-LÖSUNG MIT AMAZON ROUTE 53

Infoblox DDI for AWS lässt sich in den Amazon Route 53 DNS-Service integrieren und bietet eine zentralisierte Konsole für AWS- und Hybrid-Cloud-Bereitstellungen für Transparenz, konsistente Verwaltung und Sicherheit. Ohne auf die Private Hosted Zones von Amazon Route 53 beschränkt zu sein, ermöglicht die Infoblox- und Amazon Route 53-Lösung zuverlässige Hybrid-Cloud-Bereitstellungen, die über AWS hinausgehen.

- **Mangelnde Sichtbarkeit in der hybriden Cloud:** Ohne eine einheitliche DNS- und IPAM-Lösung in der gesamten Hybrid-Cloud muss die Unternehmens-IT mehrere Tools verwenden, um auf DNS- und IP-Adressdaten zuzugreifen. Dieser Mangel an Sichtbarkeit führt zu längeren Fehlerbehebungszeiten, verringert die Fähigkeit zur Netzwerkplanung und erhöht die Sicherheitsrisiken. Er erhöht auch Inkonsistenzen bei der unternehmensweiten Verwaltung des DNS- und IP-Adressraums.
- **Eingeschränkte DNS-Sicherheit:** Route 53 bietet eingeschränkte DNS-Sicherheit und erweiterte Bedrohungserkennungsfunktionen für AWS- und Hybrid-Cloud-Bereitstellungen. Datenexfiltration durch DNS-Tunneling und Malware, die DNS nutzen, sind häufige Bedrohungen, die IT-Netzwerke lahmlegen können.

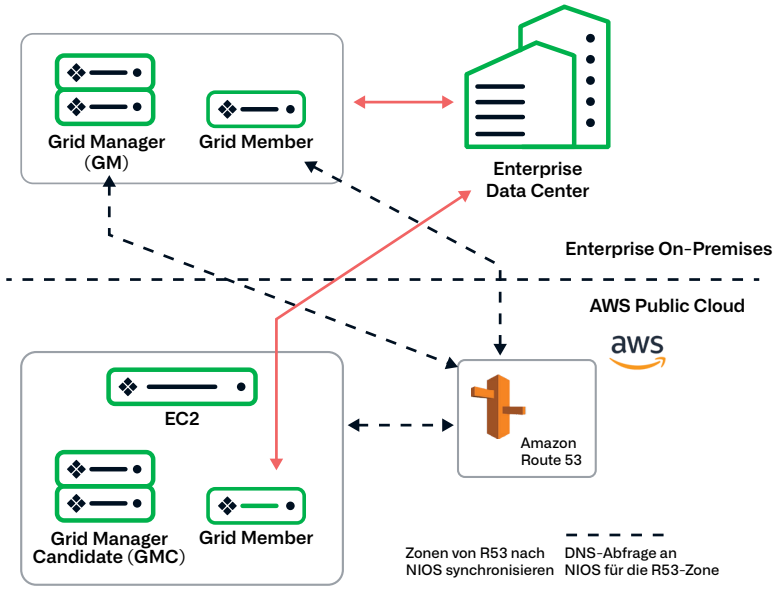


Abbildung 1: Einheitliches Management über eine hybride Cloud hinweg

Bessere kontextuelle Transparenz in AWS- und Hybrid-Deployments

Kontextuelle Netzwerktransparenz ist in den heutigen hybriden Multi-Cloud-Umgebungen entscheidend. Da sich Route 53 ausschließlich auf virtuelle AWS-Ressourcen konzentriert, ist die Sichtbarkeit nur auf diese Public-Cloud-Instanzen beschränkt. Die Infoblox- und AWS-Lösung bietet automatisierte Erkennung, verbesserte Sichtbarkeit und Nachverfolgung von VPCs und EC2-Instanzen auf einer einzigen Plattform, was die Einbindung öffentlicher Cloud-Assets in die gemeinsame DNS- und IP-Adressverwaltung erleichtert. Infoblox vereinfacht das Erstellen und Aufräumen von Datensätzen, nachdem Instanzen gelöscht wurden. Es erkennt und schließt Netzwerkressourcen ein oder aus, indem es Selective Classless Inter-Domain Routing (CIDR oder private IP) vDiscovery verwendet, um eine effiziente Verteilung von IP-Adressen in AWS sicherzustellen.

Für Teams, die mehrere Konten in Amazon Route 53 verwalten und synchronisieren müssen, spart Infoblox erheblich Zeit und AWS-Nutzungsgebühren, indem es die Bereitstellung von vNIOS-Mitgliedern in jedem Konto eliminiert und alle von Route 53 gehosteten Zonen mit dem Grid synchronisiert. vDiscovery reduziert mehrere Erkennungsaufgaben zu einem einzigen Erkennungsauftrag über mehrere AWS-Regionen und -Konten hinweg. Es behält auch Kontofilter bei, um die Auswahl der Region und die Migration bestehender vDiscovery-Aufträge ohne Datenverlust zu ermöglichen, was das Benutzererlebnis, die Effizienz der Arbeitslast und die Kontrolle durch den Administrator verbessert.

Für Kunden auf Bundes- und anderer Regierungsebene ermöglicht Infoblox mehr Transparenz und Kontrolle durch Bereitstellung von Route 53-Synchronisierungsunterstützung und vDiscovery für mehrere AWS GovCloud-Regionen und -Konten. Diese Funktion bietet hochverfügbares und skalierbares DNS und verbindet Benutzeranfragen mit AWS-Internetanwendungen sowie maßgeschneiderten Routing-Richtlinien zur Reduzierung der Latenz.

IT-Teams können den Zeitaufwand für die Prüfung von DNS- und IP-Adressinformationen erheblich minimieren, indem sie eine einheitliche Ansicht der AWS- und Nicht-AWS-Parameter innerhalb einer einzigen Steuerungsebene für Compliance-, Betriebs- und Managementberichte erhalten.

Hohe Verfügbarkeit, Betriebszeit und Resilienz

NIOS ermöglicht es Kunden, die Cloud-Platform-Appliances (CP) ausführen, zwei NIOS-Appliances für hohe Verfügbarkeit (HA) und Betriebszeit zu konfigurieren. HA misst, wie zuverlässig Benutzer auf das System zugreifen können und ob das System durch geplante Wartungsarbeiten oder ungeplante Ausfallzeiten beeinträchtigt wird. Die Betriebszeit gibt die Zeit an, während der ein System betriebsbereit ist. Mit NIOS können Administratoren von beidem profitieren und Single Points of Failure in Azure und anderen Public-Cloud-Umgebungen vermeiden, insbesondere bei unternehmenskritischen Anwendungen und Workloads.

Stärkere DNS-Sicherheit und Kontrolle

In den letzten Jahren haben DDoS-Angriffe (Distributed Denial of Service) auf den Internetdienstanbieter Dyn und andere Organisationen die Notwendigkeit eines Schutzes vor DNS-basierten Bedrohungen verdeutlicht, um kostspielige Geschäftsunterbrechungen, Umsatzeinbußen und Schäden am Markenruf zu minimieren. NIOS fügt Virtual Advanced DNS Protection (vADP) für AWS-Public-Cloud hinzu, um die unterschiedlichsten DNS-Angriffe zu erkennen und abzuwehren, darunter volumetrische Angriffe, NXDOMAIN-Fehler, DNS-Hijacking und andere Exploits. Mit vADP können Administratoren Angriffe schnell erkennen, die DNS-Integrität aufrechterhalten, die Betriebszeit verbessern und den externen DNS-Schutz von lokalen On-Premises-Instanzen auf Public-Cloud-Umgebungen ausweiten.

Um die Systemsicherheit weiter zu stärken, ermöglicht Infoblox die Synchronisierung von vNIOS mit Amazon Route 53 Multi-Account-Subset-Listen, um die Sicherheitslage zu verbessern und die Kontrolle zu erhöhen. Administratoren können die Route 53-Erkennung und -Synchronisierung von einer einzelnen NIOS-Instanz auf eine Liste mehrerer Konten in AWS erweitern. Administratoren können zwischen 1) NIOS, das eine automatische Kontoerkennung bietet, oder 2) der Angabe einer Liste von Konten wählen, die in Route 53-Umgebungen erkannt und synchronisiert werden sollen. Diese Funktion stärkt die Sicherheit, indem sie 1) verhindert, dass untergeordnete Konten auf das Root-Konto zugreifen, 2) den Zugriff von Stellvertretungsadministratoren blockiert, 3) die Entdeckung aller Konten der Organisationseinheit (OU) verhindert und 4) die Berechtigung „Assume-Role“ verwendet. Diese DNS-Sicherheitsvorkehrungen stärken kritische Netzwerkdienste gegen Angriffe und gewährleisten, dass Anwendungen verfügbar und leistungsfähig bleiben, sodass sich Unternehmen auf die Kundenbetreuung und die Führung ihres Geschäfts konzentrieren können.

Pflegen Sie eine konsistente DDI-Plattform für die Hybrid-Cloud

Viele Organisationen implementieren eine hybride Umgebung, die lokale, virtuelle private, hybride und öffentliche Multi-Cloud-Infrastrukturen, einschließlich AWS, kombiniert. Anstelle von manuellen, veralteten Tabellenkalkulationen oder der Komplexität unterschiedlicher Lösungen reduziert Infoblox die Notwendigkeit, allgemeine DNS-Server einzurichten, und ermöglicht die Kommunikation zwischen lokalen Systemen und AWS, indem es DNS-Einträge über mehrere Plattformen hinweg in einer einzigen Steuerungsebene integriert, um Konsistenz und Verwaltbarkeit zu verbessern.

Infoblox unterstützt auch EC2 R6-Instanztypen, wodurch die Leistung verbessert und die Gesamtbetriebskosten gesenkt werden. Infoblox ermöglicht eine direkte Verbindung zu AWS Nitro Systems und der EC2 Serial Console für eine schnellere Fehlerbehebung, mit verbesserter Benutzererfahrung und Kontrolle. vNIOS verbessert die Cloud-Sicherheit und Kontrolle weiter, indem es die Verschlüsselung von Elastic Block Store (EBS) für ruhende Daten, Daten während der Übertragung und alle Volume-Backups ermöglicht.

Flexible Deployment-Optionen

Infoblox DDI für AWS ist eng mit branchenführenden lokalen, virtuellen und physischen Appliances integriert. Die umfassende DDI-Plattform unterstützt die öffentliche AWS-Cloud, private Cloud-Umgebungen (z. B. einschließlich VMware, OpenStack, Microsoft und andere) sowie traditionelle Netzwerke – oder eine beliebige Kombination in einer hybriden Bereitstellung. Die einheitliche Lösung gewährleistet maximale Flexibilität, Skalierbarkeit und Serviceverfügbarkeit.

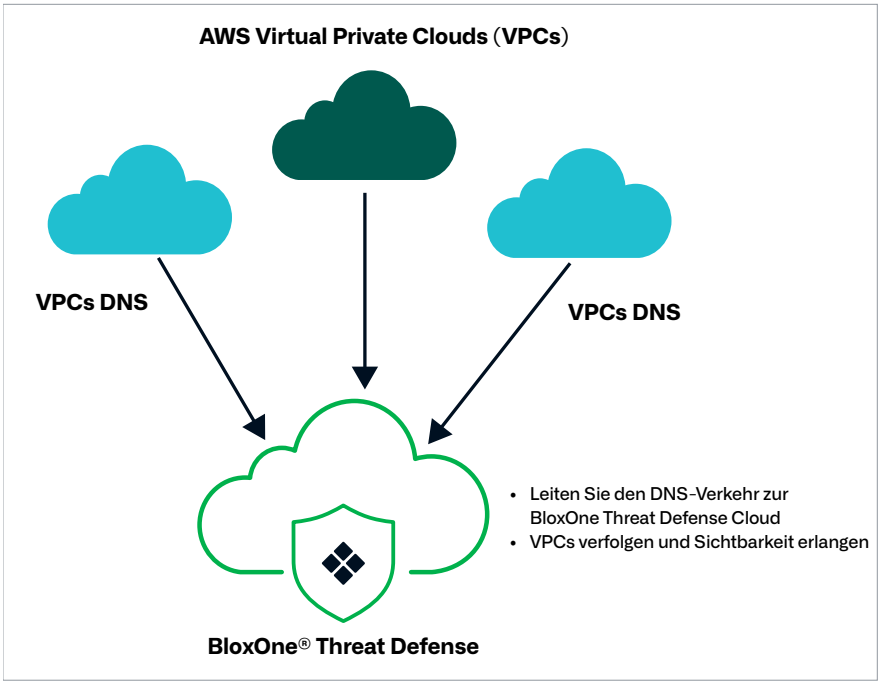
Infoblox bietet eine breite Palette von Bereitstellungsoptionen durch sichere, speziell entwickelte physische und Software-Appliances für kleine Außen- und Zweigstellen, mittelgroße Organisationen und große Unternehmen und Dienstleistungsanbieter mit Rechenzentren und verteilten Standorten. Die physische und Software-Appliance-Plattform Trinzic X6 bietet eine bis zu 50 % bessere DNS- und DHCP-Leistung im Vergleich zu Vorgängermodellen. Sie enthält außerdem kostensparende Lizenzen für die Cloud Platform API-Automatisierung, DNS-Firewall und DNS Traffic Control für globalen Server-Lastausgleich. Ganz gleich, welche Anforderungen Ihr Unternehmen hat: Infoblox bietet Lösungen für kommerzielle Anwender, große Unternehmen und Dienstleistungsanbieter, die eine konsistente kritische Netzwerkerfahrung ermöglichen, zugleich aber auch die Zuverlässigkeit und Flexibilität bieten, die erforderlich ist, damit Sie Ihre Umgebung entsprechend den Anforderungen Ihres Unternehmens skalieren können.

Infoblox ermöglicht die Cloud-Migration, indem es Administratoren die Bereitstellung von Network Insight Discovery- sowie Reporting- und Analytics-Appliances in öffentlichen AWS-Clouds ermöglicht. Network Insight bietet integrierte Layer-2- und Layer-3-Erkennung, IPAM-Synchronisierung mit Geräten, Endhosts und Netzwerkports, Switch-Port-Management sowie Lebenszyklus- und Compliance-Benachrichtigung. Darüber hinaus bietet die auf Splunk, dem Marktführer im Bereich der Datensuche, basierende Infoblox Reporting and Analytics-Lösung Überwachungs-, Visualisierungs- und SIEM-Funktionen. Die Platzierung von lösungsoptimierenden Appliances in AWS unterstützt Cloud-First-Initiativen, vereinfacht die Migration physischer Rechenzentren in die Cloud, reduziert die Ressourcen physischer Rechenzentren und bietet sowohl an Einzel- als auch an mehreren Standorten Einblick in DDI-Metadaten für historische Audits/Compliance, Echtzeit-Warnungen, Netzwerkleistung und Kapazitätsplanung. Auf diese Weise erhalten Unternehmen vollständige On-Demand-Transparenz, vereinfachen die Compliance-Berichterstattung und ermöglichen detaillierte Audits von DNS- und IP-Adressinformationen für AWS-Ressourcen in Netzwerken und geografischen Regionen.

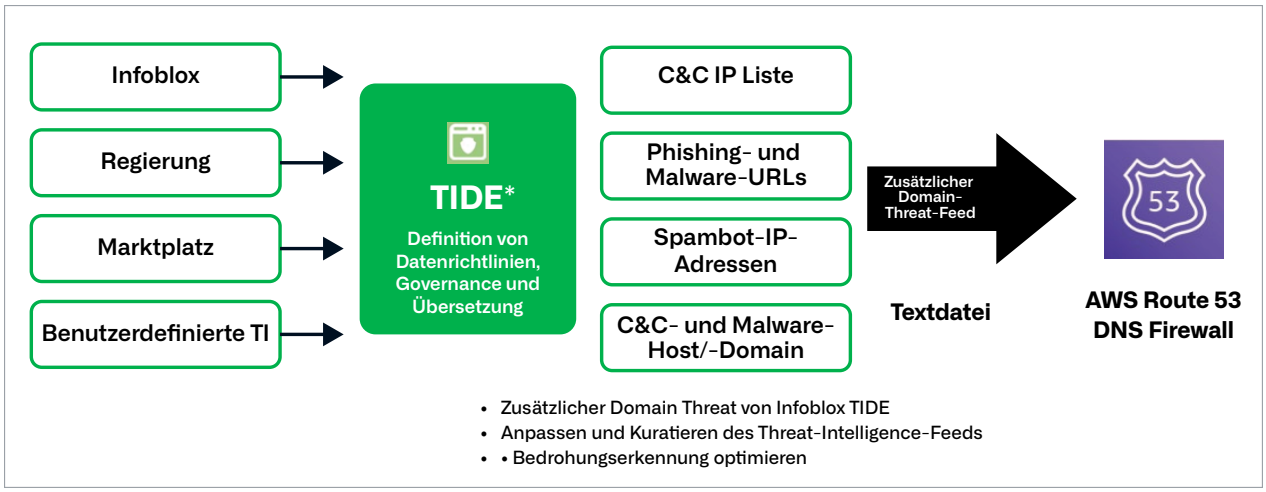
Erweitern Sie die DNS-Layer-Sicherheit und Bedrohungserkennung auf AWS

Benutzer können auch Infoblox DNS Security, IPAM (IP Address Management) und kuratierte Threat Intelligence nutzen, um Einblick in AWS-VPCs zu erhalten und die Bedrohungserkennung für die Amazon Route 53 DNS-Firewall zu optimieren. Durch die Implementierung der BloxOne® Threat Defense von Infoblox als Teil einer umfassenden Strategie wird das Risiko fortgeschrittener Angriffe und Exploits sowie der DNS-Datenexfiltration erheblich reduziert.

Durch umfangreiche Integrationen in das Ökosystem können Sie die Reaktion auf erkannte Ereignisse automatisieren und den Netzwerkkontext nutzen, um die Reaktion zu priorisieren. Benutzer können Bedrohungen in AWS-VPCs effektiv verwalten und minimieren, indem sie den VPC-DNS-Verkehr an die BloxOne Threat Defense Cloud weiterleiten, Cloud-Instanzen verfolgen, sich einen Überblick über diese verschaffen und das Risiko von Cyberbedrohungen verringern.



Darüber hinaus können Organisationen die Infoblox TIDE (Threat Intel Data Exchange-Plattform) nutzen, um Indikatoren für eine Gefährdung (IOCs) sowohl an das Infoblox AWS DNS-Gerät als auch an die Amazon Route 53 DNS-Firewall zu übermitteln, was konsistente Sicherheit für alle Umgebungen bietet und die Genauigkeit mit ihrer Auswahl an Threat-Intelligence-Feeds basierend auf ihrem spezifischen Bedarf erhöht. Der Zugriff auf Dutzende zusätzlicher Bedrohungsfeeds von Infoblox TIDE ergänzt die von der Route 53 DNS Firewall bereitgestellten Feeds. Die Fähigkeit, aktuelle Bedrohungen mithilfe eines angepassten „Super-Feeds“ zu erkennen und zu blockieren, verbessert den Sicherheitsstack an, um die Abwehr-, Untersuchungs- und Reaktionsfähigkeiten zu verbessern.



ZUSAMMENFASSUNG

Der isolierte Fokus von Amazon Route 53 auf AWS führt zu Lücken im Management und bei den Kernnetzwerkdiensten bei der Verwaltung von lokalen und hybriden Multi-Cloud-Infrastrukturen – einschließlich mangelnder Transparenz, Inkonsistenz und Sicherheit über alle Plattformen hinweg. Infoblox DDI für AWS schließt diese Lücken, indem es die branchenführende DDI-Plattform nutzt und die Komplexität mit einer einzigen Konsole zur Verwaltung von On-Premises-, AWS Public Cloud- und kritischen DNS-Komponenten reduziert. BloxOne Threat Defense bietet grundlegende DNS-Sicherheit zum Schutz hybrider Umgebungen durch Bedrohungserkennung, Reaktion und Ökosystemintegrationen zur Optimierung der Sicherheitsleistung.

KONTAKT AUFNEHMEN

Für weitere Informationen oder Antworten zu Infoblox DNS und IPAM sowie anderen Netzwerkdiensten für Amazon Web Services (AWS) wenden Sie sich an Ihr Infoblox-Kundenbetreuungsteam, sehen Sie sich unsere kritischen Netzwerkintegrationen an oder kontaktieren Sie uns unter Infoblox.com.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1 408 986 4000
www.infoblox.com

Version: 20240529v2