LÖSUNGSHINWEIS

TRINZIC X6 LÖST HERAUSFORDERUNGEN IN DEN BEREICHEN AUTOMATISIERUNG, SICHERHEIT UND BETRIEBSZEIT IN HYBRIDEN MULTI-CLOUD-NETZWERKEN

NIOS 9.0.1

Die Vorteile der Cloud-Vernetzung veranlassen Unternehmen aus nahezu allen Marktsektoren, Datenplattformen und Anwendungen von veralteten und physischen Rechenzentren in hybride Multi-Cloud-Umgebungen zu migrieren.

Anwendungsverfügbarkeit, Ausfallsicherheit, Disaster Recovery, Workflow-Automatisierung, Skalierbarkeit, Agilität und potenzielle IT-Kostenvorteile sind einige der überzeugenden, wenn nicht gar dringenden Gründe, die Unternehmensinfrastruktur zu modernisieren. Auf dem Weg zur hybriden Multi-Cloud-Migration stoßen Organisationen jedoch auf zahlreiche Herausforderungen, die die Modernisierung des Arbeitsplatzes und die Erreichung von Cloud-Vorteilen verzögern oder sogar zum Stillstand bringen können. Als führendes Unternehmen im Bereich einheitlicher Netzwerk- und Sicherheitsdienste hat Infoblox diese Herausforderungen vorausgesehen und mit führenden globalen Unternehmen zusammengearbeitet, um Lösungen zu entwickeln, die die wichtigsten Hindernisse bei der Cloud-Migration vereinfachen und beseitigen. Mit NIOS 9.0.1 und Trinzic X6, der speziell entwickelten physischen und Software-Appliance-Plattform von Infoblox, unterstützt Infoblox Unternehmen dabei, häufige Fallstricke zu vermeiden, Cloud-Vorteile schneller zu realisieren und bessere, robustere Lösungen zu implementieren, um eine schnellere Wertschöpfung zu erzielen.

UNTERNEHMERISCHE HERAUSFORDERUNGEN

Mit NIOS 9.0.1 löst Infoblox einige der häufigsten geschäftlichen Herausforderungen und ermöglicht die Modernisierung des Arbeitsplatzes, indem es drei kostensparende „sitewide“-Lizenzen (bisher separat erhältlich) als Teil der Trinzic X6-Plattform einbezieht: Cloud Platform (CP) API-Automatisierung, DNS-Firewall (DFW) und DNS Traffic Control (DTC) globales Server-Load-Balancing. Diese Lösungen adressieren Geschäftsprobleme wie die Skalierung der Workload-Automatisierung und Überlebensfähigkeit über Silos und Multi-Cloud-Umgebungen hinweg, den Schutz Ihres Unternehmens am Rand durch die Verwendung von Response Policy Zones (RPZs) zum Abfangen und Blockieren der DNS-Auflösung von bösartigen Netzwerk-IPs oder -Domänen, und die Verbesserung der Anwendungsverfügbarkeit und des Benutzererlebnisses durch die Reduzierung von Latenzen und die Ermöglichung von Disaster Recovery. Diese Solution Note untersucht jede dieser Funktionen und Fähigkeiten einzeln, einschließlich der wichtigsten Anwendungsfälle, der Funktionsweise der Lösung und ihrer potenziellen Vorteile für hybride Multi-Cloud-Umgebungen.

Trinzic X6 löst dringende Herausforderungen bei der Cloud-Modernisierung, indem es „standortweite“ Lizenzen für Cloud Platform (CP) API Automation, DNS Firewall (DFW) und DNS Traffic Control (DTC) Global Server Load Balancing beinhaltet.

CLOUD PLATFORM (CP) API-AUTOMATISIERUNG

ANWENDUNGSFÄLLE

- Skalierung der Programmierschnittstelle DDI-Automatisierung
- Vermeiden Sie das Backhauling von API-Aufrufen
- Erweitern Sie DDI auf Multi-Cloud-Umgebungen
- Vereinfachen Sie die Zugriffskontrolle für Netzwerk- und Cloud-Teams
- Reduzieren Sie die Komplexität der Netzwerkoperationen
- Kosten sparen und einen starken ROI erzielen

VORTEILE

- **Verteilte API-Verarbeitung:** Die CP-Lizenz skaliert die DDI-Leistung und verteilt die Programmierschnittstellen-Lasten lokal.
- **Delegierte Administration und Mandantenfähigkeit:** Administratoren können DDI-Objekte für die programmgesteuerte

CLOUD PLATFORM (CP) API-AUTOMATISIERUNG

SKALIERUNG UND AUTOMATISIERUNG DER DDI-INFRASTRUKTUR FÜR CLOUD-UMGEBUNGEN

Wenn Unternehmen Cloud-Bereitstellungen einführen, werden Orchestrierungs- und Automatisierungsfunktionen entscheidend. Die Infoblox CP API-Lizenz verbessert die Skalierbarkeit und Belastbarkeit von Rechenzentrumsbereitstellungen, indem sie die API-Verarbeitung verteilt und API-Aufrufe sowie DNS/DHCP-Protokolldienste lokal in jedem Rechenzentrum oder jeder Cloud-Umgebung hält. Diese Art der Lokalisierung ermöglicht es Unternehmen, ihre kritischen Netzwerkdienste mit einer Architektur zu skalieren, die die Anforderungen der heutigen verteilten Cloud-Bereitstellungen optimiert und zukünftige Bereitstellungstopologien ermöglicht.

WARUM ÄNDERN: MODERNISIERUNG DER DNS- UND IPAM-INFRASTRUKTUR

Die Automatisierung und Verteilung kritischer DDI-Netzwerkdienste (DNS, DHCP und IPAM) sind für moderne, dynamische Infrastrukturen unerlässlich. Anwendungen können vor Ort in privaten Clouds, außerhalb des Unternehmens in öffentlichen Clouds oder in einer hybriden Umgebung bereitgestellt werden, indem einfach die Konfigurationen in der Cloud-Management- oder Orchestrierungsplattform geändert werden. Ebenso können Anwendungen verschoben werden, um die Infrastruktur-as-a-Service (IaaS)-Ressourcen besser zu nutzen. Daher ist es entscheidend, dass DDI flexibel, automatisiert und über diese Umgebungen verteilt ist.

Als Teil des Bereitstellungsworkflows ist eine Integration zwischen den Server-/Cloud-Teams erforderlich, um die Rechen-, Speicher- und Netzwerkanforderungen für jede Virtuelle Maschine (VM) bereitzustellen:

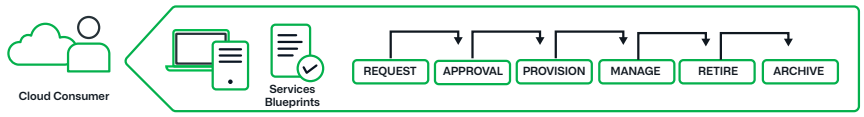

Abbildung 1: Die Erstellung von virtuellen Maschinen (VMs) überschneidet sich mit den Server-/Cloud- und Netzwerk-Teams, um VMs bereitzustellen, zu verwalten und stillzulegen.

WARUM JETZT: AUTOMATISIEREN UND SKALIEREN SIE DDI IN UNTERNEHMENSQUALITÄT FÜR HYBRIDE MULTI-CLOUD-NETZWERKE

Die Lizenz für die CP-Programmierschnittstelle meistert die Herausforderung verteilter DDI-Dienste, indem sie DNS- und DHCP-Protokolle mit Programmierschnittstellen-Verwaltung von DDI-Datensätzen in einer einzigen Trinzic X6-Plattform bereitstellt, die direkt in das Infoblox Grid integriert ist. Wenn virtuelle Maschinen bereitgestellt werden, weist die CP-Lizenz IP-Adressen zu und erstellt automatisch DNS-Einträge für jede virtuelle Maschine, wodurch Engpässe vermieden werden, die durch die manuelle Bereitstellung von IP-Adressen und einzelnen DNS-Einträgen entstehen. Die CP-Lizenz ermöglicht außerdem die Überlebensfähigkeit von Programmierschnittstellen, die verteilte Programmierschnittstellen-Verarbeitung und die Delegierung von Autoritäten.

Infoblox integriert sich mit führenden Cloud-Management-Plattformen über RESTful-APIs, um die Agilität zu verbessern, indem es IP-Adressverwaltung und automatisierte DNS-Bereitstellung für Workloads bereitstellt. Cloud-Orchestrierungsplattformen verwenden Programmierschnittstellen-Aufrufe, um Netzwerkdienste für die Automatisierung von DNS und IP-Adressen bereitzustellen. Die Bearbeitung dieser Programmierschnittstellen-Aufrufe wird für die Bereitstellung von virtuellen Maschinen entscheidend und erfordert eine skalierbare, resiliente Lösung ohne Single Point of Failure.

Verwaltung durch bestimmte Cloud- oder Automatisierungsprojekte delegieren. Sie können die Objekte auch nach Mandanten segmentieren und verwalten, während sie gleichzeitig eine zentrale Übersicht beibehalten.

- **Verbesserte Überlebensfähigkeit:** Da die Programmierschnittstelle-Automatisierung auf lokaler Appliance-Ebene erfolgt, kann die Erstellung von Cloud- und Virtualisierungsumgebungen auch dann fortgesetzt werden, wenn die Verbindung zum Grid Manager verloren geht.
- **Vollständige Integration mit Infoblox DDI:** Die CP-Funktionalität arbeitet mit herkömmlichen DDI-Geräten in einem Infoblox-Grid und unterstützt die interne DNS-Sicherheit von Infoblox.
- **Direkte Integration mit führenden Plattformen:** Infoblox bietet vorgefertigte Integrationen mit VMware vRA/vRO, AWS EC2, GCP, Azure, OpenStack und anderen Plattformen, die für eine schnelle Bereitstellung und einen schnellen Nutzen optimiert sind.

Zentralisierte Sichtbarkeit und Verwaltung für Hybrid-Cloud-Bereitstellungen

Die Datensynchronisierungs- und verteilten Datenbankfunktionen des Infoblox Grid erleichtern die zentrale Verwaltung aller DDI-Daten, während sie die Unterstützung der DNS- und DHCP-Protokolle verteilen. Die CP-Lizenz geht mit diesem Konzept noch einen Schritt weiter, indem sie Programmierschnittstellen-Updates für dieselben Infoblox-Mitglieder ermöglicht, die DNS/DHCP bereitstellen. Das Infoblox Grid führt eine bidirektionale Synchronisation aller Daten innerhalb des Grids nahezu in Echtzeit durch und bietet die einzigartige Möglichkeit, Aktualisierungen kritischer DDI-Datensätze über den Grid Manager und/oder über Mitglieder von Trinzic X6 CP vorzunehmen. Diese Funktion bietet Unternehmen dieselben Vorteile einer verteilten, hochverfügbaren Programmierschnittstellen-Verarbeitung, wie sie bei der Bereitstellung von DNS-/DHCP-Protokollen aus ihrem Infoblox Grid erhalten würden.

Verbesserte Programmierschnittstellen-Verwaltung mit Cloud-Management-Plattformen

Ohne die CP-Lizenz werden Programmierschnittstellen-Aufrufe im Rahmen der Bereitstellung der Infoblox Cloud Network Automation an den Infoblox Grid Manager gesendet. Dieser Ansatz funktioniert gut, wenn die Kommunikation mit dem Grid Manager verfügbar ist. Sollte jedoch die Netzwerkkonnektivität zwischen der Cloud-Verwaltungsplattform/dem Orchestrator und dem primären Rechenzentrum, das den Grid Manager hostet, unterbrochen werden, wird die Verwaltung von DNS und IP-Adressen beeinträchtigt, und das Risiko eines Dienstausfalls steigt.

Die Infoblox CP-Lizenz bedient DNS und DHCP genauso wie herkömmliche Grid-Mitglieder, ist aber auch in der Lage, IPAM-Datensätze zu synchronisieren und zu verwalten. Diese Funktionen stellen sicher, dass alle Programmierschnittstellen-Aufrufe im selben Rechenzentrum oder in derselben Cloud-Umgebung bleiben, während DNS-/DHCP-Änderungen in Echtzeit erfolgen. Dadurch werden Verfügbarkeits- und Latenzprobleme beseitigt, selbst wenn die Verbindung zum Grid Manager verloren geht. Wenn die Verbindung wiederhergestellt wird, werden die Daten zwischen dem Grid Manager und den Mitgliedern der Cloud-Plattform automatisch synchronisiert. Dieser Synchronisierungsschritt stellt die lokale Überlebensfähigkeit sicher, während er gleichzeitig eine zentralisierte Sichtbarkeit und Verwaltung bietet. In skalierten Cloud-Umgebungen, in denen virtuelle Maschinen über mehrere Standorte verteilt sind, verbessert die lokale Programmierschnittstellen-Funktion die Gesamtzuverlässigkeit des Systems und vermeidet Latenzzeiten bei Programmierschnittstellen-Aufrufen, die über ein Wide Area Network gesendet werden müssen.

Verteiltes DDI-Management und Unterstützung für Multi-Tenancy

Die Infoblox CP-Lizenz unterstützt ein Delegationsmodell, das es Organisationen ermöglicht, DDI zu segmentieren, um die Verwaltung von Datensätzen für Zonen, Unterzonen, Netzwerke/Subnetze oder Bereiche an bestimmte Organisationen oder Projekte innerhalb einer Organisation zu delegieren. Bei Verwendung mit Infoblox Cloud Network Automation ermöglicht die CP-Lizenz Netzwerkadministratoren, die Verwaltung von DDI-Datensätzen, die spezifisch für OpenStack- oder VMware vRA-Mandanten oder AWS EC2 VPCs sind, zu delegieren und zu isolieren, was die Verwaltung von Multi-Tenant-Umgebungen erleichtert.

Zusätzliche CP-Lizenzen können bei Bedarf bereitgestellt werden, um die Protokoll- und Programmierschnittstellen-Kapazität zu erhöhen oder um kritische Netzwerkdienste für neue Cloud-Umgebungen bereitzustellen, sobald diese eingerichtet werden. Diese Funktion verbessert die Gesamtzeit bis zur Bereitstellung und bietet gleichzeitig zusätzliche Skalierbarkeit und Resilienz für Cloud-Implementierungen. Die CP-Fähigkeit ist entscheidend für die Bereitstellung der dynamischen und skalierbaren DDI-Dienste, die hybride Multi-Cloud-Implementierungen benötigen.

WARUM INFOBLOX: SKALIERUNG ZUVERLÄSSIGER DDI-AUTOMATISIERUNG, LEISTUNG UND AUSFALLSICHERHEIT FÜR DAS MULTI-CLOUD-UNTERNEHMEN

Die CP-Lizenz von Infoblox optimiert DDI auf Unternehmensniveau für eine zuverlässige und skalierbare Leistung und Überlebensfähigkeit der Cloud-Netzwerkautomatisierung. Sie bietet vollständige Sichtbarkeit der physischen und virtuellen Ressourcen mit einem einzigen Steuerungsebenen-Management. Sie nutzt auch robuste Programmierschnittstellen-Integrationen mit AWS, Azure, GCP, OpenStack, VMware und anderen Plattformen, um die Automatisierung im gesamten hybriden Multi-Cloud-Unternehmen zu skalieren.

DNS-FIREWALL (DFW)

DNS-SCHUTZ BIS AN DIE UNTERNEHMENSGRENZEN

Die Infoblox DNS-Firewall ist ein Domain Name System (DNS)-Dienst, der Response Policy Zones (RPZs) mit einem Threat Intelligence-Dienst (Malware-Feed) nutzt, um DNS zu schützen, indem er Malware erkennt, eindämmt und kontrolliert. Diese Art von Malware nutzt DNS zur Kommunikation mit Command and Control (C&C)-Servern und Botnetzen für Eindringversuche, Datenexfiltration oder andere bösartige Aktivitäten. RPZs bieten eine Möglichkeit, die Reputation der von Clients abgefragten Server und Dienste zu verstehen und Richtlinien und Maßnahmen festzulegen, um zu verhindern, dass Netzwerkbenutzer und -systeme eine Verbindung zu bekannten bösartigen Internetstandorten herstellen. Durch die Einbeziehung der DFW-Lizenz in NIOS für physische und Software-Appliances unterstützt Infoblox Sie dabei, Ihr gesamtes Unternehmen an lokalen Standorten, in Rechenzentren und über die Cloud bis zum Netzwerkrand zu schützen.

WARUM WECHSELN: DIE DNS-INFRASTRUKTUR STEHT UNTER BESCHUSS.

Angriffe auf die DNS-Infrastruktur bleiben eine der Hauptursachen für die Tausenden von Datenschutzverletzungen, die täglich in allen Branchen weltweit auftreten. DNS wird durch eine breite Palette volumetrischer DNS-, DDoS- oder DNS-Amplifikations-/Reflexionsangriffe und Exploits angegriffen, wie etwa DNS-Cache-Poisoning, Spoofing und Session-Hijacking, die den Betrieb der heutigen Next Generation Firewalls (NGFWs) umgehen oder sogar stören. Die meisten NGFWS sind nicht in der Lage, diese Bedrohungen zu erkennen oder zu bewältigen, da sie den Datenverkehr über Port 53 zulassen, das Protokoll, über das DNS-Abfragen und -Antworten gesendet werden.

WARUM JETZT: VERHINDERN SIE DATENEXFILTRATION UND DIE VERBINDUNG ZU BÖSARTIGEN ORTEN

DNS wird zunehmend als Pfad für Datenexfiltration verwendet, indem das IP-Protokoll durch Port 53 getunnelt wird, entweder unwissentlich durch unentdeckte, mit Malware infizierte Geräte oder absichtlich durch böswillige Akteure. Erschwerend kommt hinzu, dass die meiste Malware erst mehr als 200 Tage nach der Infektion entdeckt wird, wodurch Unternehmen dem Verlust von sensiblen Kundendaten, Finanzdaten, geistigem Eigentum und anderen kritischen Informationen ausgesetzt sind.

WARUM INFOBLOX: VEREINHEITLICHUNG VON NETZWERK- UND SICHERHEITSLÖSUNGEN FÜR UNÜBERTROFFENE LEISTUNG UND SCHUTZ.

Infoblox DFW ist die führende DNS-basierte Netzwerksicherheitslösung. Mit DFW vereinheitlicht Infoblox Netzwerk und Sicherheit, indem es Datenexfiltration-Malware über lokale Bereitstellungen bis an den Rand des Cloud-Netzwerks eindämmt und kontrolliert. DFW arbeitet durch die Integration von DNS-RPZs, der optionalen BloxOne Threat Defense von Infoblox, Threat Insight oder forensischen IoC-Feeds (Indicators of Compromise) von Drittanbietern, um Malware zu erkennen, zu blockieren und umzuleiten. Infoblox kombiniert DFW mit IPAM-Netzwerkdaten im Grid, um infizierte Geräte zur Remediation zu isolieren. Durch den Einsatz von DHCP-Fingerprinting und Identity Mapping können Administratoren den Benutzernamen erfassen, der mit einem infizierten Gerät verknüpft ist, und die Auswirkungen von Bedrohungen früh in der Cyber-Kill-Chain reduzieren. Darüber hinaus ermöglicht DFW die DNS-Umleitung, sodass Administratoren Domänen blockieren oder an einen „Walled Garden“ oder andere bestimmte Standorte weiterleiten können. DFW kann außerdem als Auslöser für Integrationen von Sicherheitsökosystemen für Kunden mit der Ecosystem-Lizenz verwendet werden. DFW lässt sich auch in Infoblox Reporting and Analytics integrieren, um zusammenfassende

DNS-FIREWALL (DFW)

ANWENDUNGSFÄLLE

- Bringen Sie die IOC-Erkennung an den Netzwerkrand (on-prem oder in der Cloud)
- Aktivieren Sie DFW auf der Hardware- oder Software-Appliance.
- Bedrohungsschutz mit Infoblox und/oder Feeds von Drittanbietern ermöglichen
- Stellen Sie den DNS-Malware-Schutz sicher
- Verbessern Sie den bestehenden Sicherheitsstack

VORTEILE

- **Malware erkennen, eindämmen und kontrollieren:** Kombinieren Sie Netzwerk- und Sicherheitstools und -daten, um infizierte oder bösartige Kommunikation frühzeitig zu erkennen und zu kontrollieren.
- **Reduzieren Sie die Auswirkungen von DNS-Bedrohungen für Unternehmen:** Kombinieren Sie RPZs mit optionalen Threat Intelligence-Feeds, um das Unternehmen von lokalen bis hin zu Cloud-Bereitstellungen zu schützen.
- **Verbessern Sie die Sichtbarkeit, Automatisierung und Kontrolle:** Ermöglichen Sie Administratoren, umfangreiche Kontextdaten einzusehen, die Reaktion auf Bedrohungen zu automatisieren, Sicherheitsbedrohungen umzuleiten und zu beheben.
- **Aktivieren Sie Integrationen des Sicherheitsökosystems:** Verbessern Sie das Bedrohungsbewusstsein, die Sichtbarkeit, den Austausch und die Reaktion durch umfangreiche Integrationen im Ökosystem.

Berichte und umfassende Kontextdaten bereitzustellen, darunter die häufigsten RPZ-Treffer, die häufigsten bösartigen Hostnamen, die häufigsten bösartigen Benutzer und viele andere Sicherheitsmetriken. Schließlich bietet DFW eine zuverlässige Grundlage für den Schutz vor DNS-Malware und verbessert die Wirkung und den ROI des bestehenden Sicherheits-Stacks des Kunden.

Wie funktioniert es?

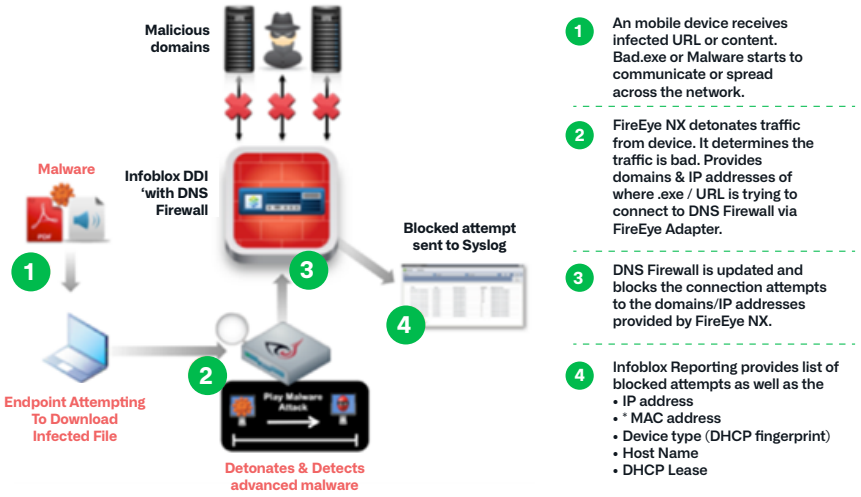

Abbildung 2: Wie die DNS-Firewall funktioniert, um böswillige Verbindungsversuche zu blockieren.

DNS TRAFFIC CONTROL (DTC)

VERBESSERUNG DES TRAFFIC-MANAGEMENTS, DER ANWENDUNGSVERFÜGBARKEIT UND DER BENUTZERERFAHRUNG.

Die Infoblox DTC-Lizenz ist eine integrierte Global Server Load Balancing (GSLB)-Lösung, die das Management des Netzwerkverkehrs, zuverlässige Anwendungsverfügbarkeit, Service-Ausfallsicherheit und Disaster Recovery für lokale und hybride Multi-Cloud-Netzwerke bietet. DTC integriert autoritative IPAM-Daten mit DNS- und GSLB-Server-Gesundheitsmetriken, Geo-IP und erweiterbaren Attributen (EAs oder Benutzer-Metatags), um den Benutzerverkehr intelligent auf optimale Server für maximale Betriebszeit und Benutzererfahrung zu lenken.

WARUM WECHSELN: DIE GLOBALE MODERNISIERUNG VERÄNDERT DIE NETZWERKLANDSCHAFT

Die regionale und globale Arbeitsplatzmodernisierung verändert das On-Premises- und hybride Multi-Cloud-Unternehmen. Direkter Zugriff auf Cloud-Anwendungen von überall hat die Erwartungen an ein schnelles, effizientes und stets verfügbares Kundenerlebnis erhöht. SD-WAN ermöglicht lokalen Niederlassungen direkten Internetzugang. 5G-Funktionen entwickeln sich und das IoT erhöht die Anforderungen an die Konnektivität von Netzwerkressourcen. Diese Herausforderungen werden noch größer, wenn Unternehmen neue Plattformen und Technologien einführen. Die Benutzer erwarten Echtzeit-Performance, insbesondere von E-Commerce- und internen Portalen. Die Verwaltung von Legacy- und modernen Anwendungen wird immer komplexer, insbesondere bei Fusionen und Übernahmen. Die Datenschutzbestimmungen werden verschärft und Verstöße werden streng geahndet. Veränderte Trends bei mobilen und Remote-Mitarbeitern und -Niederlassungen, Globalisierung, Konsolidierung von Rechenzentren, anhaltende Ressourcenbeschränkungen und zunehmende DNS-, Malware- und Stealth-Angriffe belasten die Teams, die mit der verantwortungsvollen und nachhaltigen Verwaltung des Netzwerk-Traffics, der Betriebszeit und der Geschäftskontinuität beauftragt sind, noch stärker.

- **Integration von Berichterstattung und Analytik:** Erhalten Sie auf Abruf zusammenfassende, forensische und visualisierte Berichte über umfangreiche Netzwerkdaten.
- Verbessern Sie den bestehenden Sicherheits-Stack: Steigern Sie die Wirkung, den Wert und den ROI der vorhandenen Sicherheitstools und Integrationen.

DNS TRAFFIC CONTROL (DTC)

ANWENDUNGSFÄLLE

- Kosteneffizientes globales Verkehrsmanagement in internen und externen On-Premise- und Hybrid-Clouds
- Betriebszeit für On-Premise- und SaaS-Anwendungen basierend auf Subnetz, GeoIP und erweiterbaren Attributen
- Disaster Recovery (DR) für Ausfallsicherheit nach katastrophalen Störungen
- Domänenzonenkonsolidierung und Replikation von Servern und Ressourcen
- Programmierschnittstellen-basierte Anwendungsskalierung über private, hybride und Multi-Clouds
- Standortbezogene Sensibilisierung für MS AD-Clients
- Vollständig integrierte Berichterstattung und Analysen

VORTEILE

- **Integriertes DNS/Global Server Load Balancing (GSLB):** Integriert autorisierendes IP-Adressmanagement (IPAM) mit DNS und GSLB, um eine hochverfügbare Intranet- und Internet-App-Verfügbarkeit und -Leistung von fünf Neunen zu gewährleisten, ohne von einer separaten DNS-Plattform abhängig zu sein.
- **Intelligentes globales Traffic-Management:** Verwendet DNS-basierte GSLB, um

WARUM JETZT: KOSTENGÜNSTIGE, ZUVERLÄSSIGE GLOBALE VERFÜGBARKEIT UND GESCHÄFTSKONTINUITÄT

Der DTC von Infoblox bietet eine kostengünstige Lösung im Vergleich zu anderen konkurrierenden Application Delivery Controllern (ADCs), um die sich ändernden Herausforderungen des globalen Verkehrsmanagements zu bewältigen. DTC sorgt für hohe Benutzerzufriedenheit durch zuverlässige Anwendungsverfügbarkeit, Leistung und nahtloses Failover. Es nutzt eine benutzerfreundliche Oberfläche und robuste Programmierschnittstellen, um Netzwerkverkehrslasten über geodiverse, lokale und hybride Multi-Cloud-Umgebungen für E-Commerce, kundenorientierte Portale, das Web und interne geschäftskritische Anwendungen zu verteilen. Es bietet auch Geschäftskontinuität und Disaster Recovery im Falle eines katastrophalen Ereignisses, um den normalen Betrieb wiederherzustellen.

WARUM INFOBLOX: VEREINHEITLICHUNG VON NETZWERK- UND SICHERHEITSLÖSUNGEN FÜR UNÜBERTROFFENE LEISTUNG UND SCHUTZ.

DTC von Infoblox integriert autoritative IPAM-Daten mit DNS und GSLB, um den Benutzer-Traffic intelligent auf optimale Server zu leiten. Im Gegensatz zu konkurrierenden ADCs handelt es sich um eine vollständig integrierte DNS-Lösung, daher ist sie schneller und zuverlässiger als das Anfügen von Layer-2- und Layer-3-Protokollen. Es bietet mehrere Lastausgleichsalgorithmen und flexible, automatisierte Zustandsüberprüfungen, um die Serververfügbarkeit sicherzustellen. DTC ist skalierbar, um den sich ändernden Datenverkehrsvolumina und den Geschäftsanforderungen gerecht zu werden. Für optimale Sichtbarkeit verwendet DTC eine einfache Benutzeroberfläche und einen Visualizer, der Load Balanced Domain Names (LBDNs), Pool- und Serverbeziehungen sowie -attribute anzeigt. Außerdem ermöglicht es im Gegensatz zu anderen ADCs Echtzeit-Tests von LBDNs, Pools und Servern vor der Inbetriebnahme, um die Einsatzbereitschaft sicherzustellen. DTC kann GeoIP- und EA-Daten (benutzerdefinierte Metatags) verwenden, um den Traffic in regionsspezifische Zonen zur Einhaltung von Vorschriften und zum Schutz der Privatsphäre sowie zur Optimierung von Anwendungen zu steuern. Ein integriertes, auf Splunk basierendes Reporting- und Analysetool, das vorgefertigte und anpassbare DTC-Dashboards, Berichte, Suchfunktionen, Warnmeldungen und eine automatische Berichtsverteilung bietet, ist separat erhältlich. Schließlich integriert sich DTC in die Infoblox-Erkennungsquellen, um die Topologien basierend auf IP-Subnetz-, GeoIP- und EA-Daten automatisch zu aktualisieren. Mit Programmierschnittstellen können Sie schnell neue Serverinstanzen hinzufügen, neue Apps bereitstellen, mit anderen Systemen integrieren und Routineaufgaben automatisieren. Da DTC direkt in das Grid integriert ist, besteht keine Notwendigkeit, die Softwarebereitstellungen, -konfigurationen und -updates einer separaten Plattform zu verwalten.

den Benutzerdatenverkehr auf intelligente Weise an den optimalen Server weiterzuleiten, basierend auf dem Standort von Client und Server, dem Serverzustand und der Serververfügbarkeit.

- **DTC Visualizer:** Zeigt lastverteilte Domainnamen (LBDNs), Pool- und Serverbeziehungen und Attribute über eine einzige GUI-Visualisierung an.
- **Pre-Production-Tests:** Ermöglicht das schnelle Testen neuer und aktualisierter LBDNs, Pools und Server in Echtzeit, um die Produktionsbereitschaft vor der Liveschaltung sicherzustellen.
- **Compliance:** Ermöglicht die Verwendung von GeoIP- und EA-Daten (Extensible Attribute), um den Datenverkehr auf regionsspezifische Zonen für LBDNs und Pools zu beschränken und so die Einhaltung von Datenschutzbestimmungen zu unterstützen.
- **Integrierte Berichterstattung und Analyse:** Bereitstellung von Splunk-basierten, vorgefertigten und anpassbaren Dashboards, Berichten, Suchfunktionen, Warnmeldungen und automatisierter Berichtsverteilung für mehr Transparenz und Kontrolle.
- **API-Automatisierung:** Fügen Sie neue Serverinstanzen hinzu, stellen Sie schnell neue Apps bereit, integrieren Sie sie in andere Systeme und automatisieren Sie routinemäßige GSLB-Verwaltungsaufgaben. Sparen Sie Zeit und Geld mit dieser benutzerfreundlichen, gut dokumentierten API, die die Funktionalität der Web-GUI widerspiegelt.

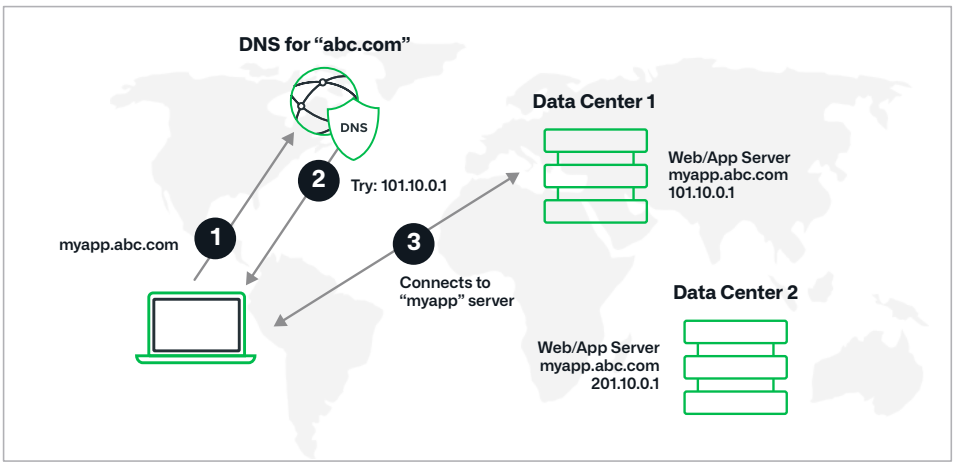

Abbildung 3: DTC-Bereitstellung, die 1) Bereitstellung der App, 2) DNS-Verbindung des Unternehmens und 3) Bereitstellung des myapp-Servers in verteilten Rechenzentren zeigt.

ZUSAMMENFASSUNG UND NÄCHSTE SCHRITTE

Mit NIOS 9.0.1 und der Trinzic X6-Plattform bietet Infoblox einen Mehrwert, indem es die Herausforderungen der Cloud-Modernisierung löst und „standortweite“ Lizenzen, die zuvor separat verkauft wurden, für Cloud Platform (CP) DNS-Firewall (DFW) und DNS Traffic Control (DTC) Global Server Load Balancing einschließt. Diese Lösungen adressieren häufig auftretende Geschäftsprobleme wie die Skalierung der Workload-Automatisierung und die Überlebensfähigkeit über Silos und Multi-Cloud-Umgebungen hinweg; den Schutz Ihres Unternehmens bis an den Rand durch die Verwendung von Response Policy Zones (RPZs) zum Abfangen und Blockieren von DNS-Auflösungen von bösartigen Netzwerk-IPs oder Domänen; sowie die Verbesserung des Datenverkehrsmanagements, der Anwendungsbetriebszeit und der Benutzerfreundlichkeit. Um mehr zu erfahren oder eine Testversion zu starten, wenden Sie sich an Ihr Account Team bei Infoblox.com/de.

KONTAKT AUFNEHMEN

Weitere technische Informationen finden Sie in den NIOS 9.0.1 Hinweisen zur Veröffentlichung (verfügbar bei GA, 21.08.2023) im Infoblox Support Portal unter https://support.infoblox.com.

Um spezifische Antworten zur NIOS- oder Trinzic X6-Plattform von Infoblox oder zum umfangreichen Angebot an hybriden Multi-Cloud-Integrationen zur Modernisierung der Arbeitsumgebung zu erhalten, wenden Sie sich an Ihr Infoblox-Account-Team oder kontaktieren Sie uns unter Infoblox.com/de.

infoblox.

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/de

Version: 20230731v1