INFOBLOX® REFERENZARCHITEKTUR UND BEST PRACTICES FÜR NIOS DDI

EIN PRAKTISCHER BLICK AUF DIE IMPLEMENTIERUNG VON DNS- UND DHCP-DIENSTEN MIT INFOBLOX NIOS DDI- UND INFOBLOX THREAT DEFENSE™-PRODUKTEN AUF EINEM NETZWERK FÜR MEHR EINFACHHEIT, SICHERHEIT UND SKALIERBARKEIT.

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG 3

DAS UNTERNEHMEN 5

EIN WICHTIGER HINWEIS ZUR DIMENSIONIERUNG 5

STEUERUNGSEBENE 6

EXTERNER AUTORITATIVER DNS 7

LOKALE WEITERLEITUNG..... 8

INTERNER DNS..... 8

DHCP 9

REMOTE-BÜROS 9

CLOUD 10

REPORTING..... 11

NETZWERKERKENNUNG 11

INTEGRATIONEN VON EXTERNEN SYSTEMEN UND ÖKOSYSTEMEN 11

ZUSAMMENFASSUNG

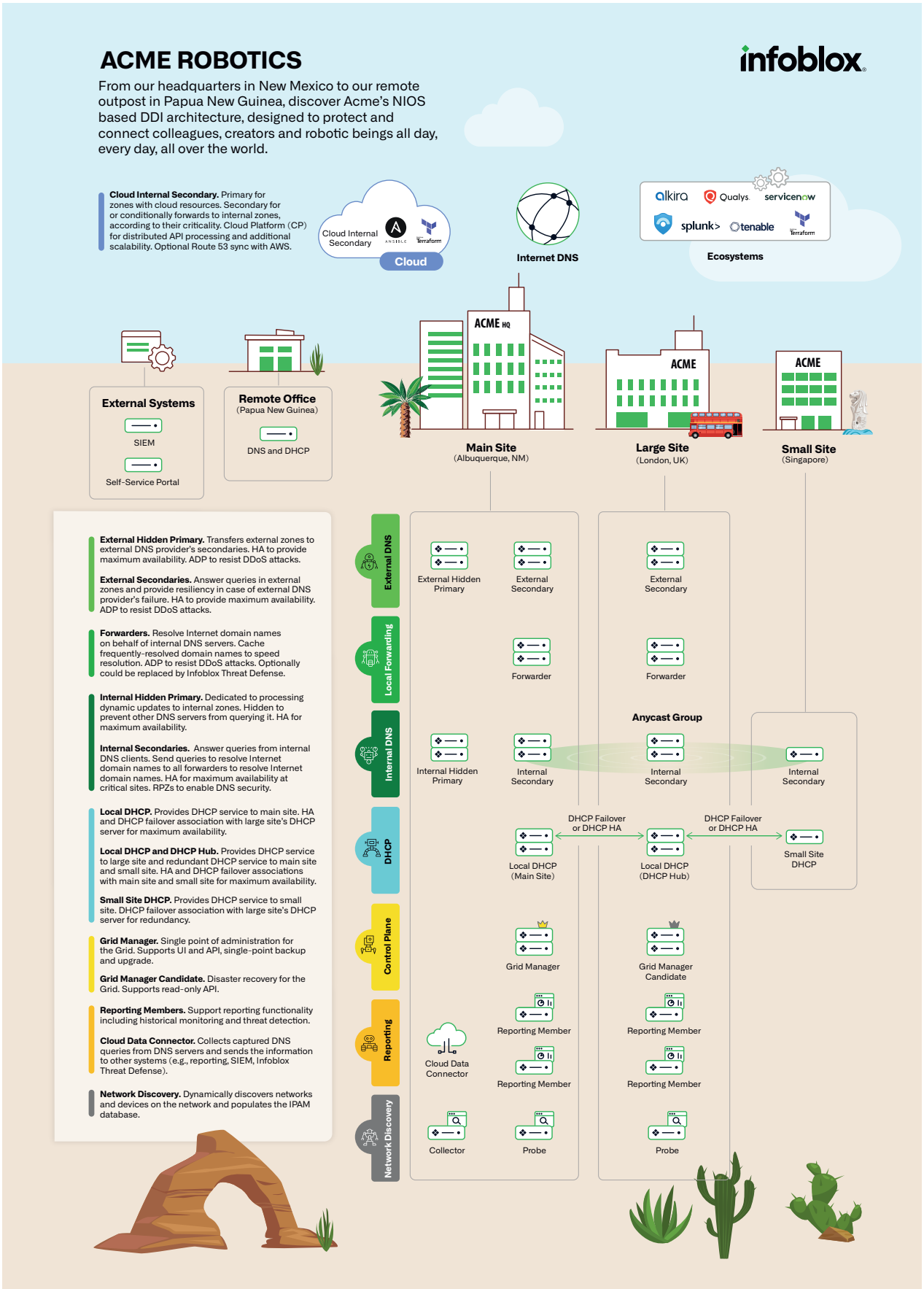
Dieser Leitfaden, der auf Basis von Whitepapern von Cricket Liu und dem Infoblox® Architecture Review Board (ARB) entwickelt wurde, hebt die gemeinsamen Anstrengungen unseres internen Gremiums hervor, das für die Überprüfung aller nicht-trivialen Designs der Solutions Architects von Infoblox verantwortlich ist. Neben dem ARB tragen auch verschiedene technische Experten bei Infoblox ihr spezielles Fachwissen bei, um sicherzustellen, dass unsere Lösungen robust, innovativ und mit den Best Practices der Branche abgestimmt sind.

NIOS-Geräte sind ein ideales Mittel zur Bereitstellung von Domain Name System (DNS)- und Dynamic Host Configuration Protocol (DHCP)-Diensten und präsentierten später eine Architektur zur effizienten, zuverlässigen und sicheren Unterstützung dieser Dienste und Sicherheitsdienste. Dieser Leitfaden erweitert diese White Papers, um mehrere neue Entwicklungen in der Welt der Informationstechnologie zu umfassen:

- Die Verwendung von DNS als kritisches Sicherheitstool
- Den Aufstieg von Public Clouds und Cloud-Computing
- Die zunehmende Bedeutung der Self-Service-IT, gefördert durch Dienste wie ServiceNow
- Die Ausweitung der Unternehmensnetzwerke auf mehr kleine Außenstellen
- Die Notwendigkeit der Integration mit SIEM-Systemen (Security Information and Event Management) und anderen Sicherheitstechnologien

Um zu demonstrieren, wie diese neuen Entwicklungen unterstützt werden können, werden wir eine Fallstudie eines Unternehmens und seines Unternehmensnetzwerks präsentieren und eine DDI-Architektur (DNS, DHCP und IP-Adressverwaltung) entwickeln, um die Anforderungen basierend auf den Best Practices für die Branche zu erfüllen. Das Design wird die Anforderungen des Unternehmens hinsichtlich Verfügbarkeit, Leistung, Sicherheit und Disaster Recovery, Unterstützung für cloudbasiertes Computing und Anwendungen sowie der Integration mit internen und cloudbasierten Systemen berücksichtigen.

Denken Sie beim Lesen dieses Dokuments an Ihre eigene DDI-Infrastruktur. Bietet sie dasselbe Maß an Resilienz, Leistung und Sicherheit? Gibt es Aspekte dieses Designs, die Sie für Ihren eigenen Gebrauch anpassen könnten?


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
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

DAS UNTERNEHMEN

Vor Kurzem wurden wir gebeten, eine neue DNS-Architektur für das multinationale Unternehmen ACME Robotics zu entwerfen. ACME ist ein bekannter Anbieter von Robotikgeräten für eine Vielzahl von Funktionen. ACME Robotics produziert, vermarktet und vertreibt Produkte und verfügt über eine Vertriebs- und Supportorganisation.

Der Markt des Unternehmens erstreckt sich über die ganze Welt, konzentriert sich jedoch insbesondere auf den amerikanischen Südwesten.

Dieses Unternehmen hat vier Klassen von Standorten, die mit seinem Unternehmensnetzwerk verbunden sind:

1. Der Hauptsitz von ACME in Albuquerque, New Mexico, umfasst die größte Anzahl von Benutzern (etwa 2.000). Der Hauptsitz beherbergt auch das primäre Rechenzentrum des Unternehmens.
2. Ein großer Standort im englischen London umfasst ungefähr 500 lokale Benutzer.
3. Kleine Standorte, darunter auch Singapur, unterstützen normalerweise nicht mehr als 100 Benutzer. Kleine Standorte sind in geografische Regionen unterteilt, die jeweils von einem Regionalbüro betreut werden. Jeder kleine Standort ist über eine Verbindung zum zuständigen Regionalbüro mit dem Unternehmensnetzwerk verbunden.
4. Remote-Standorte unterstützen in der Regel weniger als 24 Benutzer. Remote-Standorte sind über eine VPN- oder SD-WAN-Verbindung mit dem Internet und dem Unternehmensnetzwerk verbunden.

Das Unternehmen hat eine bedeutende Online-Präsenz, die es zur Vermarktung seiner Produkte nutzt. Um dies zu unterstützen, werden zwei Public Clouds genutzt: AWS und Azure. In jeder Cloud laufen mehrere Anwendungen, und einige erfordern den Zugriff auf interne Ressourcen. Die Bereitstellung in der Cloud wird je nach Anwendung durch Terraform oder Ansible automatisiert.

Das Unternehmen verwendet ServiceNow, um den Mitarbeitern zu ermöglichen, IT-Änderungen anzufordern, einschließlich Änderungen an DNS und DHCP. Es betreibt ein internes SIEM und ist aufgrund der Branche, in der es tätig ist, verpflichtet, passive DNS-Daten (pDNS) zu erfassen und zu archivieren.

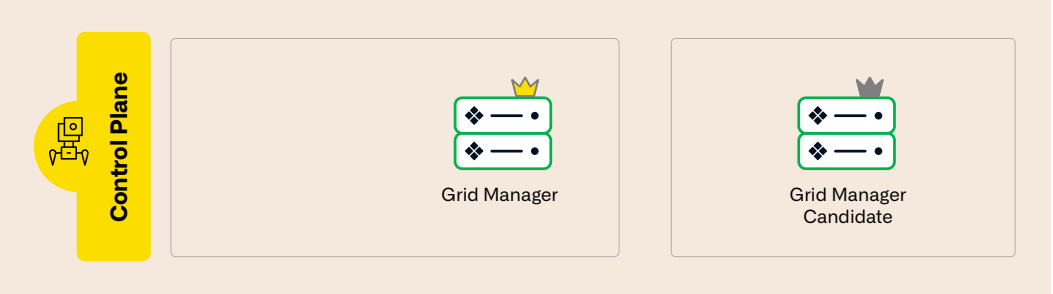
Die IT-Support-Mitarbeiter des Unternehmens sind auf den Hauptsitz und große Standorte verteilt. Jedes Regionalbüro verfügt über einen IT-Mitarbeiter, der hauptsächlich für den lokalen Support für Desktops und Laptops zuständig ist und den Mitarbeitern am Hauptsitz als dortige „Augen und Hände“ dient.

Das Unternehmen erlaubt seinen Mitarbeitern, ihre eigenen Geräte mit zur Arbeit zu bringen, isoliert diese jedoch auf Gastnetzwerken. Die durchschnittliche Anzahl der Geräte pro Mitarbeiter und die von ihnen erzeugte Transaktionslast sind in das Design eingeflossen.

EIN WICHTIGER HINWEIS ZUR DIMENSIONIERUNG

Ein wichtiger Aspekt von Architekturen, den wir in diesem Entwurf bzw. diesem Dokument nicht behandeln, ist die Größenbestimmung. Um sicherzustellen, dass die DNS- und DHCP-Server genügend Leistung erbringen, um die Last des Unternehmens zu bewältigen, müsste das Unternehmen die DNS- und DHCP-Transaktionsraten für jeden einzelnen Server im Design messen oder zumindest schätzen und Appliances spezifizieren, die diese Last bewältigen können. Darüber hinaus müsste das Unternehmen einen angemessenen „Spielraum“ einplanen: zusätzliche Serverkapazität, um unvorhergesehene Lastspitzen (z. B. aufgrund eines Stromausfalls und der anschließenden Wiederherstellung der Stromversorgung an einem Standort) abzudecken. Schließlich müsste das Unternehmen das Wachstum im Laufe der Zeit schätzen und planen: Wenn das Unternehmen plant, massiv Personal einzustellen, andere Unternehmen zu übernehmen oder mit einem anderen Unternehmen zu fusionieren, kann dies erhebliche Auswirkungen auf die DNS- und DHCP-Last haben.

STEUERUNGSEBENE



Beginnen wir mit der DDI-Kontrollebene, die in diesem Entwurf aus einem Grid Manager (GM) am Hauptsitz in Albuquerque und einem Grid Manager Candidate (GMC) am großen Standort in London besteht.

In einem Infoblox NIOS Grid unterstützt der GM die webbasierte Benutzeroberfläche, die von Administratoren genutzt wird, und die Programmierschnittstelle, die von Entwicklern zur Automatisierung von DDI-Aufgaben genutzt wird.[1] Der GM verwaltet auch die Kommunikation und Synchronisation mit allen Infoblox-Mitgliedern[2] im Grid; diese Appliances unterstützen DNS, DHCP und andere Dienste. Angesichts seiner kritischen Rolle sollte der GM immer als VRRP-HA-Appliance-Paar (Virtual Router Redundancy Protocol; hohe Verfügbarkeit) am selben physischen Standort bereitgestellt werden. Der GM kann auch zur Aktualisierung und Wartung von ADP-Regeln (Advanced DNS Protection) und Threat Insight-Modulen verwendet werden.

Der GMC ist eine Nachbildung des GM und wird in Echtzeit mit dem GM synchronisiert. Sollten beide Appliances, die die Rolle des GM unterstützen, ausfallen, kann ein Administrator dem GMC mit einem einfachen Befehl die Rolle des GM zuweisen. Der neu ernannte GM wird die anderen Appliances im Grid informieren und die Aufgaben des ehemaligen GM übernehmen. Wie beim GM sollte der GMC immer als VRRP-HA-Paar von Appliances am selben physischen Standort bereitgestellt werden.

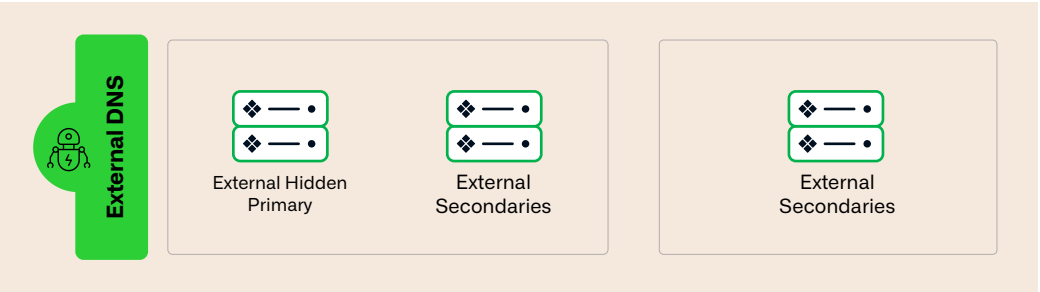
Infoblox Grids unterstützen die Benennung vieler GMCs, aber dieses Unternehmen hat London als seinen Disaster-Recovery-Standort identifiziert und wird daher nur dort einen GMC hosten.

Wir haben erwähnt, dass wir die Dimensionierung in diesem Dokument nicht behandeln werden. Ein Hinweis zur Dimensionierung von GMCs ist jedoch angebracht: GMCs unterstützen die (sehr praktische) Fähigkeit, schreibgeschützte Programmierschnittstellen-Aufrufe zu verarbeiten, was beispielsweise für die Integration mit ServiceNow, das ACME verwendet, nützlich sein kann. Berücksichtigen Sie bei der Dimensionierung von GMCs sowohl die Belastung des GM **als auch** die Belastung des GMC durch alle schreibgeschützten Programmierschnittstellen-Aufrufe, die er verarbeitet. Im Katastrophenfall muss der GMC, wenn er zum GM hochgestuft wird, die aggregierte Last des GM und seiner früheren Rolle als GMC bewältigen können. Alternativ können Sie einen oder mehrere GMCs hinzufügen und diese für die Verarbeitung schreibgeschützter Programmierschnittstellen-Aufrufe reservieren.

1 Mit bestimmten Ausnahmen: Siehe den Abschnitt „Cloud“ für Einzelheiten.

2 Beachten Sie, dass wir den Begriff „Appliance“ verwenden, um sowohl physische als auch virtuelle Appliances zu bezeichnen. Letztere laufen auf fast jeder Virtualisierungsplattform und in Public Clouds.

EXTERNER AUTORITATIVER DNS



Die externen autoritativen DNS-Server führen das Advertising der Zonen des Unternehmens im Internet durch und ermöglichen es Kunden und Partnern im Internet, E-Mails an die Adressen des Unternehmens zu senden, die Website des Unternehmens zu besuchen, auf dem Internet zugewandte Anwendungen zuzugreifen und vieles mehr. Ihre Rolle ist entscheidend, denn ihre Verfügbarkeit wirkt sich direkt auf den Umsatz, die Kundenzufriedenheit und den Ruf des Unternehmens aus.

Die externe autoritative DNS-Infrastruktur besteht aus drei Nameservern: einem versteckten primären Nameserver am Hauptsitz in Albuquerque und jeweils einem sekundären Nameserver am Hauptsitz und am großen Standort in London. Jeder Nameserver ist ein VRRP-HA-Paar von Appliances. Dadurch können die Administratoren die DNS-Server aktualisieren, ohne dass es zu Ausfallzeiten kommt, was notwendig sein könnte, wenn beispielsweise ein Bug oder eine Sicherheitslücke in BIND gefunden wurde, oder wenn größere Appliances notwendig werden, wenn das Unternehmen wächst.

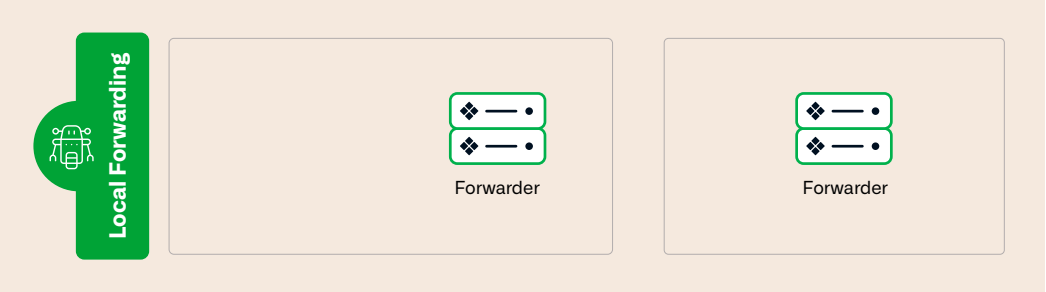
Die **erweiterte** externe autoritative DNS-Infrastruktur umfasst auch die DNS-Server, die von einem internetbasierten DNS-Hosting-Anbieter betrieben werden. DNS-Hosting-Anbieter wie Cloudflare und Neustar's UltraDNS stellen zahlreiche DNS-Server im gesamten Internet bereit – eine weit verteilte DNS-Infrastruktur, die für das Unternehmen schwierig zu verwalten und kostspielig zu betreiben wäre. Allerdings kommt es auch bei DNS-Hosting-Anbietern manchmal zu Ausfällen,[3] also kann der Betrieb von zwei sekundären DNS-Servern im unternehmenseigenen Netzwerk und an anderen Präsenzpunkten eine günstige und effektive Versicherung sein. Offensichtlich hängt dies von der erwarteten Abfragelast ab. Wenn eine größere Anzahl von sekundären Nameservern in Betracht gezogen wird, kann sich die Verwendung von Anycast als besonders nützlich erweisen.

Ein versteckter primärer DNS-Server verfügt über eine autoritative Kopie der externen Zonen, beantwortet aber keine Anfragen von DNS-Servern im Internet. Stattdessen überträgt dieser DNS-Server diese Zonen an den DNS-Hosting-Anbieter.

Als zusätzlichen Schutz vor den Gefahren der direkten Kommunikation mit dem Internet verwenden die externen autoritativen DNS-Server ADP, das eine Reihe von Angriffen auf DNS-Server erkennt, entschärft und meldet.

3 Siehe den DDoS-Angriff auf Dyn im Oktober 2016, https://de.wikipedia.org/wiki/DDoS-Angriffe_auf_Dyn.

LOKALE WEITERLEITUNG

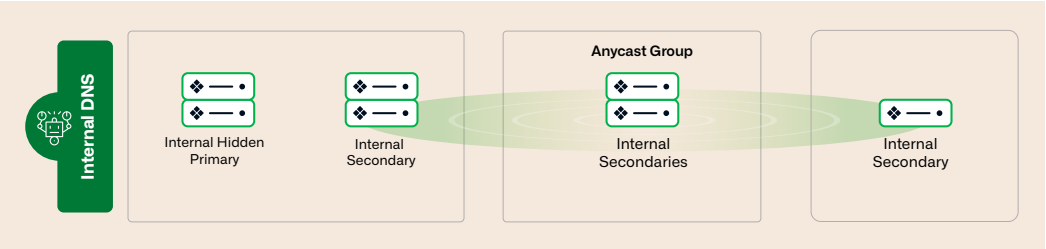


Die lokalen Forwarder, manchmal auch als Caching-Forwarder bezeichnet, sind interne DNS-Server, die dafür vorgesehen sind, Internet-Domainnamen im Auftrag interner DNS-Server aufzulösen, indem sie DNS-Server im Internet abfragen. Indem das Unternehmen nur einer kleinen Anzahl interner DNS-Server erlaubt, direkt mit DNS-Servern im Internet zu kommunizieren, verringert es seine Anfälligkeit für bestimmte Arten potenzieller Schwachstellen, wie etwa Pufferüberläufe, die durch die Rückgabe schlecht formatierter Antworten ausgelöst werden.

Das Unternehmen verfügt über zwei Forwarder, einen am Hauptsitz und einen am großen Standort, der für Disaster Recovery vorgesehen ist. Beide sind VRRP-HA-Paare. Trotz seiner Bestimmung als Disaster-Recovery-Gerät wird der Forwarder am großen Standort auch dann verwendet, wenn der Forwarder am Hauptsitz verfügbar ist, was nicht nur Redundanz, sondern auch zusätzlichen Durchsatz bietet. Interne DNS-Server wählen den zu verwendenden Forwarder anhand der Paketumlaufzeit für an diesen Forwarder gesendete Abfragen aus und treffen ihre Auswahl nach dem Zufallsprinzip, wenn die Paketumlaufzeit ungefähr gleich ist. Daher verwenden diese internen DNS-Server abhängig von ihrer Reaktionsfähigkeit beide Forwarder. Dadurch wird die Last zwischen ihnen besser ausgeglichen.

Als zusätzlichen Schutz vor den Gefahren der direkten Kommunikation mit dem Internet verwenden die Forwarder ADP, das eine Reihe von Angriffen auf DNS-Server und den von bestimmten bekannten DNS-Tunneling-Tools generierten Datenverkehr mit hohem Volumen erkennt und stoppt. Für DNS-Tunneling mit geringem Volumen (niedrig und langsam) kann Threat Insight auf diesen Nameservern bereitgestellt werden. Die Threat Insight-Funktion ist auch über das Infoblox-Portal und den Infoblox DNS Forwarding Proxy (DFP) verfügbar. Bei einer NIOS-Bereitstellung verwendet Threat Insight zur Durchsetzung
Response Policy Zones (RPZ).

INTERNER DNS



Da DNS ein so kritischer Netzwerkdienst ist, benötigen alle internen Standorte des Unternehmens einen lokalen DNS-Server. Der Hauptsitz hat zwei davon, beides HA-Paare, da einer als versteckter primärer Server für interne Zonen dient. Ein versteckter primärer Server ist ein Server, der für das Verarbeiten dynamischer Aktualisierungen der von ihm verwalteten Zonen vorgesehen ist, anstatt Anfragen von Clients zu beantworten. Der andere Server bearbeitet Client-Anfragen und ist ein sekundärer Server für interne Zonen; um andere Domainnamen aufzulösen, fragt er einen der Forwarder ab.

Die großen Standorte des Unternehmens verfügen ebenfalls über HA-Paare, die als sekundäre DNS-Server fungieren. Kleine Standorte haben einzelne (d. h. keine HA-)Appliances. Um zusätzliche Redundanz des DNS-Dienstes bereitzustellen, sind alle DNS-Server in der Zentrale,

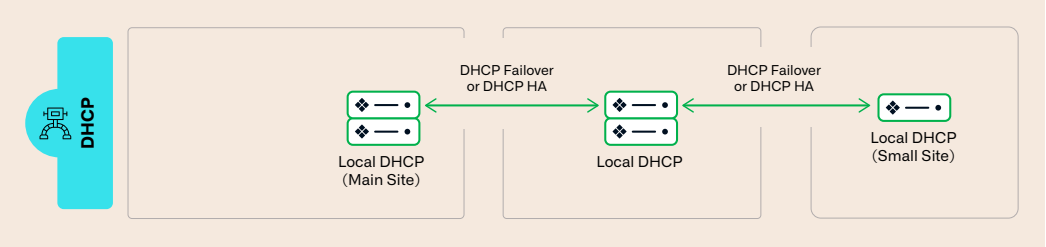
an großen und kleinen Standorten Teil einer von zwei Anycast-Gruppen. DNS-Server in Gruppe A haben eine virtuelle IP-Adresse, die mit ihrem DNS-Dienst verknüpft ist; Server in Gruppe B haben eine andere virtuelle IP-Adresse. Interne Geräte[4] haben ihre DNS-Stub-Resolver so konfiguriert, dass sie erst eine virtuelle IP-Adresse und dann die andere abfragen. Dies garantiert nahezu, dass interne Geräte ihre erste Anfrage an einen responsiven DNS-Server senden.

Alle internen rekursiven DNS-Server sind mit RPZ „verkabelt". RPZ werden von internetbasierten RPZ-Anbietern, einschließlich Infoblox, übertragen und enthalten Echtzeit-Feeds mit Bedrohungsdaten, darunter Domainnamen, die bekanntermaßen böswillig verwendet werden, und IP-Adressen von bekannten böswilligen autoritativen Nameservern im Internet. Diese RPZ verhindern die Auflösung bösartiger Domainnamen durch DNS-Clients und lokalisieren schnell die Geräte, die versuchen, sie aufzulösen, sodass das IT-Sicherheitsteam des Unternehmens infizierte Geräte rasch identifizieren und unter Quarantäne stellen kann. Eine dieser RPZ kann von Threat Insight gespeist werden, wenn es DNS-Tunnel erkennt.

Das Unternehmen verfügt auch über geografisch basierte Anwendungen innerhalb der Organisation, die jeder im Unternehmensnetzwerk nutzen kann. Darüber hinaus besteht der Wunsch nach Lastausgleich und Redundanz. Infoblox DNS Traffic Control (DTC) ist eine Load-Balancing-Lösung, die die Anwendungsreaktionszeiten und -leistung optimiert, indem sie den DNS-Verkehr basierend auf dem Standort des Clients, der Server-Verfügbarkeit und der Netzwerktopologie intelligent leitet. DTC ist auf den internen autoritativen DNS-Servern konfiguriert.

Wir werden DNS für Außenstellen in einem separaten Abschnitt mit dem Titel „Außenstellen" behandeln.

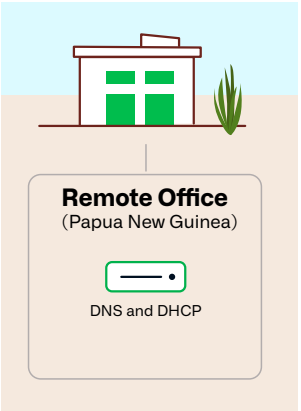
DHCP



Wie DNS ist DHCP ein kritischer Netzwerkdienst, daher benötigen alle internen Standorte des Unternehmens einen lokalen DHCP-Server. Ähnlich wie DNS wird DHCP von HA-Paaren am Hauptsitz und an großen Standorten sowie von einzelnen Appliances an kleinen Standorten unterstützt. Um jedoch zusätzliche Redundanz bereitzustellen, werden die DHCP-Server in DHCP-Failover-Zuordnungen konfiguriert: Jeder DHCP-Server hat einen Peer-DHCP-Server, mit dem er Informationen über DHCP-Lease-Pools austauscht, und beide können Leases aus diesen Lease-Pools an Clients vergeben. Auf diese Weise verfügen selbst Standorte mit nur einer Appliance über einen redundanten DHCP-Dienst. Diese DHCP-Server verwenden DDNS (Dynamic Domain Name System), um DNS-Einträge auf dem versteckten primären Server für interne Zonen zu aktualisieren.

REMOTE-BÜROS

Die Außenstellen des Unternehmens sind per Definition klein und bieten jeweils nur einer bescheidenen Anzahl von Mitarbeitern Platz. Es gibt jedoch eine ganze Reihe von Außenstellen, deren Konnektivität mit dem Internet und dem übrigen Unternehmensnetzwerk nach wie vor wichtig ist. Die meisten Außenstellen verfügen über einen High-Speed-Internetzugang, jedoch keine dedizierte Verbindung zum Unternehmensnetzwerk. Stattdessen können sie den Datenverkehr für DNS- und DHCP-Dienste über ein VPN an das Unternehmensnetzwerk leiten. In diesem Fall verwendet das Unternehmen Infoblox Universal DDI™, die cloudverwaltete



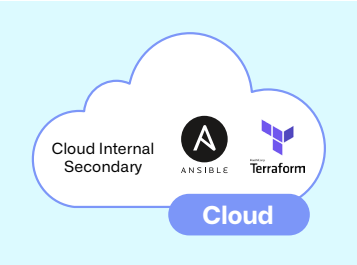
4 Ausgenommen sind jene in Außenstellen: Informationen zu deren Konfiguration finden Sie im Abschnitt „Außenstellen".

DDI-Lösung von Infoblox, um diesen Büros DNS und DHCP bereitzustellen. Jede cloudverwaltete Appliance, NIOS-X, stellt DNS und DHCP für die Außenstelle bereit. Die DNS-Server der Außenstellen sind nicht Teil der Anycast-Infrastruktur des Unternehmens; Clients in den Außenstellen fragen zuerst den lokalen DNS-Server ab und greifen dann auf die IP-Adressen der beiden Anycast-Gruppen zurück.

Um redundantes DHCP bereitzustellen, befindet sich der DHCP-Server jeder Außenstelle in einer erweiterten Aktiv-Passiv-Beziehung mit dem DHCP-Server einer nahegelegenen Außenstelle. Dies ermöglicht es beiden Servern, DHCP für Clients in beiden Außenstellen bereitzustellen, wodurch auch für Außenstellen redundante DHCP-Dienste bereitgestellt werden können.

Eine Alternative für Standorte, die vollständig auf das Internet für ihren Betrieb angewiesen sind, ist NIOS-X as a Service, die cloudbasierte Lösung von Infoblox, die DDI-Dienste als Managed Service bereitstellt. Es bietet Skalierbarkeit, Flexibilität und verbesserte Sicherheit, indem diese kritischen Netzwerkdienste in der Cloud gehostet werden, wodurch die Notwendigkeit für lokale Hardware entfällt. NIOS-X as a Service lässt sich nahtlos in andere Infoblox-Lösungen integrieren und bietet einen einheitlichen und vereinfachten Ansatz für das Netzwerkmanagement und die Sicherheit, wodurch ein zuverlässiger und effizienter Netzwerkbetrieb gewährleistet wird.

CLOUD



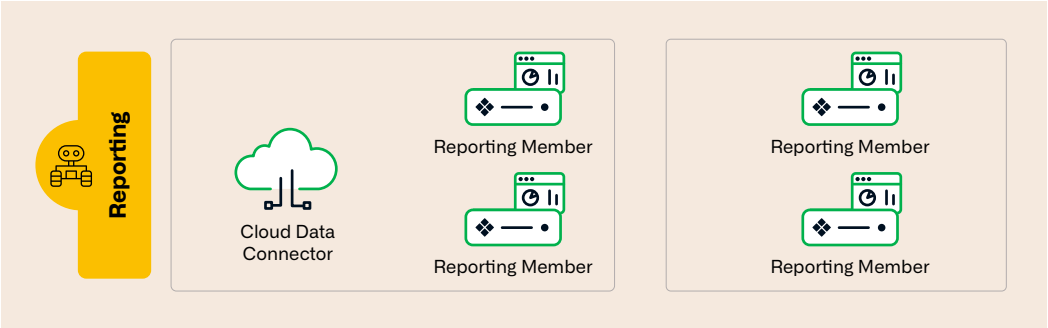
Das Unternehmen nutzt mehrere Public Clouds, um sowohl interne als auch dem Internet zugewandte Anwendungen zu unterstützen. Jede Cloud hostet eine oder mehrere virtuelle Cloud-Plattform-Appliances, die als sekundäre Appliances für interne Zonen konfiguriert sind, in denen Cloud-Anwendungen und Workloads Domainnamen auflösen müssen. Dies bietet eine bessere Ausfallsicherheit als die Verwendung der bedingten Weiterleitung, um für die Auflösung interner Domainnamen Anfragen an interne DNS-Server zu leiten.

Die Cloud-Plattform-Appliance ist auch als primär für die Cloud-Zonen konfiguriert, in denen die Bereitstellungssysteme des Unternehmens, Terraform und Ansible, Ressourceneinträge verwalten müssen. Um Terraform und Ansible mit dem Grid zu integrieren, verwendet Terraform den Infoblox Terraform Provider, während Ansible die Infoblox NIOS Collection für Ansible Automation verwendet.

Die Cloud Network Automation (CNA) von Infoblox bietet auch Einblick in die Cloud-Netzwerkumgebung und zeigt die verwendeten Cloud-Ressourcen wie Virtual Private Clouds/virtuelle Netzwerke, Subnetze und virtuelle Maschinen an. Darüber hinaus kann CNA automatisch DNS-Einträge für neue Elemente erstellen, die durch den virtuellen Erkennungsprozess erkannt werden.

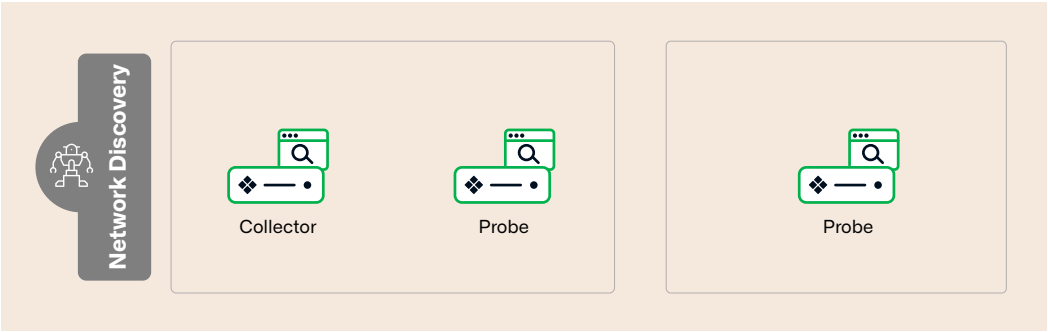
Wenn das Unternehmen Cloud-spezifische DNS-Dienste wie Amazon Route 53 oder Azure DNS verwendet, können diese Dienste mithilfe der Synchronisierung in das Grid integriert werden. Dadurch bleibt die zentrale Sichtbarkeit und Kontrolle für alle DNS-Daten über die Grid-Schnittstelle und API erhalten.

REPORTING



Zur Unterstützung der Berichtsfunktionen des Grids verwendet das Unternehmen vier Berichtsserver – zwei am Hauptsitz und zwei am für Disaster Recovery vorgesehenen Standort. Die Verwendung von vier Servern ist zwar nicht unbedingt erforderlich, bietet jedoch sowohl Redundanz als auch zusätzliche Leistung: Einer oder beide Berichtsserver am Hauptsitz können ausfallen, ohne dass Berichtsdaten verloren gehen. Die Berichtsdaten werden weiterhin indiziert, Berichte können weiterhin erstellt und Suchen nach Berichtsdaten durchgeführt werden. Bei vier Berichtsservern wäre die optimale Platzierung folgendermaßen: zwei beim GM und zwei beim GMC, die während eines Disaster-Recovery-Ereignisses hochgestuft würden.

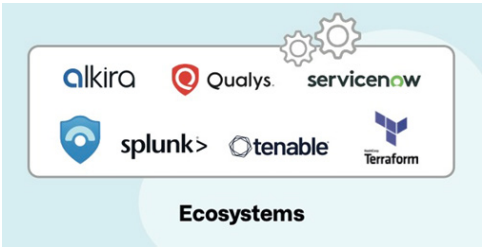
NETZWERKERKENNUNG



Netzwerkerkennung ist eine kritische Komponente einer IP-Adressverwaltungslösung: Die Erkennung stellt sicher, dass die DDI-Datenbank den tatsächlichen Zustand des Netzwerks widerspiegelt und nicht etwa eine idealisierte Version davon. Die virtuelle Erkennungsfunktion bietet Erkennung in den lokalen virtuellen und Cloud-Umgebungen des Unternehmens, aber auch die Erkennung des Unternehmensnetzwerks ist erforderlich.

Mehrere Appliances unterstützen die Netzwerkerkennung: zwei am Hauptsitz und eine an jedem großen Standort. Eine der Appliances am Hauptsitz wird als Konsolidierer festgelegt: Sie empfängt alle von den verschiedenen Sonden erkannten Daten, konsolidiert sie und repliziert sie an den GM, um sie in die DDI-Datenbank aufzunehmen. Die anderen Appliances sind Sonden, die die Abfragen, Sondierungen und Pollings durchführen, die zur Erkennung von Geräten im Netzwerk erforderlich sind.

INTEGRATIONEN VON EXTERNEN SYSTEMEN UND ÖKOSYSTEMEN



Das Unternehmen verwendet sowohl cloudbasierte als auch interne Systeme für eine Vielzahl von Funktionen, darunter ihr SIEM-System, ihr Ticketsystem (wir möchten an dieser Stelle daran erinnern, dass ServiceNow verwendet wird) und ein Self-Service-Portal, das es seinen Mitarbeitern zur Verfügung stellt, damit sie einfache Änderungen an der DDI-Datenbank

anfordern können. Appliances im Grid senden die protokollierten Ausgaben direkt an das SIEM. DNS-Protokolle, wie etwa pDNS-Daten, werden an den Infoblox Data Connector gesendet, da dieser die Last reduziert, die den DNS-Servern beim Senden der Daten entsteht, und die Daten filtern kann, bevor sie an externe Systeme gesendet werden (um beispielsweise die Protokollierung rein interner Abfragen zu vermeiden, falls dies gewünscht ist).

Durch die Integration mit dem Grid ermöglicht ServiceNow den Benutzern, Änderungen an der DDI-Datenbank anzufordern und beispielsweise IP-Adressen zu reservieren, hinzuzufügen oder zu löschen. Das Grid kann auch Benachrichtigungen an ServiceNow senden, die das System alarmieren, wenn Geräte dem Netzwerk beitreten oder es verlassen und wenn Sicherheitsprobleme erkannt werden.

Durch die gemeinsame Nutzung von Bedrohungsfrüherkennung, autoritativen IP-Adressen und kontextbezogenen Netzwerkdaten mit bestehenden Tools bricht Infoblox Silos auf und stärkt den gesamten IT-Security-Stack, was einen besseren ROI und betriebliche Effizienz gewährleistet. Das Infoblox-Ökosystem lässt sich nahtlos in eine breite Palette von Sicherheits-, Netzwerk- und Cloud-Tools integrieren, um die Erkennung von Bedrohungen zu verbessern, Workflows zu automatisieren und die Reaktionsfähigkeit in lokalen, Hybrid- und Multi-Cloud-Umgebungen zu erhöhen.

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: 20250221v2