LÖSUNGSHINWEIS

DER AUFBAU EINER AGILEN UND AUSFALLSICHEREN NETZWERKINFRASTRUKTUR

Unternehmen modernisieren ihre Netzwerke, um den Herausforderungen der ständig wachsenden Regulierungslandschaft und den sich stets weiterentwickelnden Bedrohungen zu begegnen. Viele Unternehmen verlassen sich für ihre kritischen Betriebsprozesse auf Microsoft-Umgebungen, aber mit begrenzten Möglichkeiten ist es schwierig, Netzwerksicherheit und die Verfügbarkeit von Anwendungen zu gewährleisten. Häufige Ausfälle und Verstöße aufgrund von Systembeschränkungen innerhalb der Microsoft-Infrastruktur unterstreichen den Bedarf an speziell entwickelten DNS-Lösungen für kritische Netzwerke.

DIE MODERNISIERUNG KRITISCHER NETZWERKE

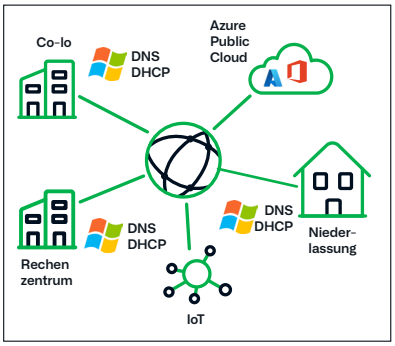
Eine Netzwerkinfrastruktur umfasst zahlreiche Komponenten – Firewalls, Router, Switches, WLAN-Geräte, Domain Name Server, DHCP-Server und mehr. Die meisten kritischen Infrastrukturelemente erhalten bereits Upgrades auf moderne Hardware- oder Softwareversionen. Aber was ist mit Domain Name Servern und DHCP-Servern? Sind Ihre zentralen Netzwerkdienste immer noch nicht modernisiert? Veraltete Netzwerkdienste, Freeware wie Microsoft oder Do-it-yourself-Lösungen (DIY) sind unzusammenhängend, langsam und anfällig für Sicherheitsrisiken, was zu massiven Ausfällen führen kann.

EIN KOSTENLOSER ANSATZ KANN TEUER WERDEN

Die typische kritische Netzwerkinfrastruktur ist über Rechenzentren, zahlreiche Niederlassungen, Multi-Cloud-Umgebungen und Co-Location-Servicecenter verteilt. Es ist schwierig, diese Art von vielfältiger Infrastruktur mit kostengünstigen Tools zu verwalten, da diese zu Systemeinschränkungen, fragmentierter Sichtbarkeit und Ineffizienzen führen. Auch wenn die anfänglichen Investitionskosten geringer erscheinen, wiegen die Betriebskosten, die Ihnen mit der Microsoft-Infrastruktur oder anderen kostenlosen Tools entstehen würden, den „Kostenlos“-Aspekt auf. Diese Tools erhöhen das Fehler- und Ausfallrisiko aufgrund manueller Konfigurationen und Workarounds.

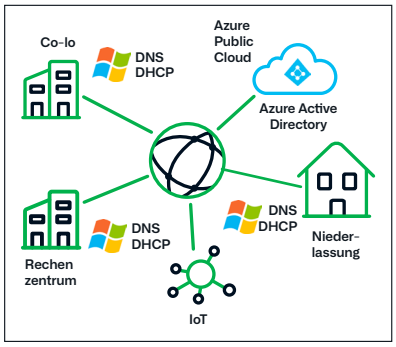
- **Skalierungsbeschränkungen:** Es gibt keinen zentralen Verwaltungspunkt und bei Wachstum ist aufgrund von Systembeschränkungen keine Skalierung möglich. Die Microsoft-Verwaltungskonsole kann bei über 8–10 Servern pro Profil nicht skaliert werden.
- **Keine zentrale Ansicht:** Protokollkonsolidierung (Audit und Service) erfordert Skripting, und ohne DNS- und DHCP-Integration ist IPAM nicht autoritativ.
- **Mangel an erweiterten Funktionen:** Es sind kein DNS Anycast und keine Rekursion pro Serverkonfiguration erforderlich, was die Konfigurationszeit erhöht.
- **Pro Server-Konfiguration:** Die Zonenverwaltung von Mitgliedsservern ist in der Azure-Integration nicht verfügbar und Sie müssen den Cache für neue Updates oder zur Fehlerbehebung leeren.
- **Auswirkungen auf die Leistung:** Verzögerungen bei der DNS-Replikation und das Einschalten der Debug-Protokollierung beeinträchtigen die Leistung.

> Geschätzte jährliche Kosten von 3.300 USD pro Server – das sind über **$1.3M** pro Jahr
>
> - Network Architect, Multinational Oil and Gas Company.



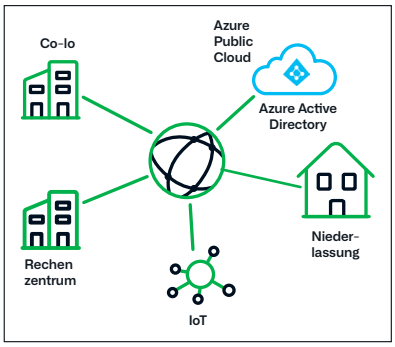
Microsoft AD Enterprise umfasst Skalierbarkeitsbeschränkungen, einen Mangel an erweiterten Funktionen und Sicherheitslücken.

Abbildung 1: Microsoft AD Enterprise



Azure AD Enterprise bietet lediglich fragmentierte Transparenz, begrenzte Sicherheit und keine zentrale Verwaltung.

Abbildung 2: Azure AD Enterprise



Infoblox DDI Enterprise bietet einen vollen Funktionsumfang mit Transparenz, Automatisierung und Kontrolle sowie Skalierbarkeit, Sicherheit und Resilienz.

Abbildung 3: Infoblox DDI Enterprise

DIE INFOBLOX-LÖSUNG FÜR ECHTE AUSFALLSICHERHEIT UND AGILITÄT

OPTIMIEREN SIE GESCHÄFTSKRITISCHE ABLÄUFE

Nutzen Sie die speziell entwickelte DDI-Lösung (DNS, DHCP und IPAM) von Infoblox und profitieren Sie von vollständiger zentralisierter Transparenz, Automatisierung und Kontrolle für Ihre kritischen Netzwerke.

Mit Infoblox profitieren Sie von zahlreichen Vorteilen:

- Keine Ausfallzeiten durch Patches, Upgrades oder Fehlkonfigurationen
- Keine regelmäßigen Tests, wodurch menschliches Versagen ausgeschlossen und das Risiko von Ausfällen erheblich reduziert wird
- Shift-Left-Sicherheit bietet robusten Schutz auf DNS-Ebene und erkennt Cyberangriffe frühzeitig
- DNS-Datenexfiltration und weitere Schwachstellen wie Domain-Generierungsalgorithmen und Lookalike-Domains werden blockiert

Laut einer ROI-basierten Kundenstudie eines unabhängigen Marktforschungsunternehmens umfassen die jährlichen Einsparungen mit Infoblox unter anderem:

> „Die Lösung von Infoblox hat uns im Vergleich zu unserer Microsoft-Bereitstellung Einsparungen in Höhe von **40%** beschert."
>
> Netzwerkarchitekt, multinationales Öl- und Gasunternehmen.

69% geringerer Zeitaufwand für typische DNS/DHCP-Konfigurationsänderungen	**70%** geringerer Zeitaufwand für die Fehlerbehebung bei DNS/DHCP-Ausfällen	Eine um **90%** verkürzte Erfassungszeit für Netzwerkgerätedaten	**98%** weniger Aufwand beim Onboarding und die fortlaufende Schulung des Netzwerkteams

ZUSAMMENFASSUNG

DDI ist von grundlegender Bedeutung für jedes Unternehmen, das für seine Geschäftstätigkeit auf ein Netzwerk angewiesen ist. Während die Microsoft-Infrastruktur aufgrund ihrer Kosteneffizienz eine attraktive Option für die Verwaltung von DDI-Diensten zu sein scheint, kann sie für Unternehmen, die für ihre kritischen Vorgänge auf diese Dienste angewiesen sind, ein riskantes Unterfangen darstellen. Infoblox hingegen bietet Ihnen eine robuste, zuverlässige und speziell entwickelte DDI-Lösung.

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.

Hauptsitz der Gesellschaft
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20230803v1