BUKU PUTIH

Mengapa Infoblox untuk DDI

Saatnya Bermigrasi dari BIND dan Microsoft

Daftar Isi

Di banyak organisasi, layanan inti yang memungkinkan konektivitas dan akses ke internet yang andal didasarkan pada produk gratis dan tampaknya gratis. Sementara harga mungkin menarik, produk-produk ini sering membawa serta biaya tersembunyi dari keterbatasan fungsional dan inefisiensi administrasi. Ketika merencanakan pertumbuhan dan perubahan, yang tak terhindarkan dalam jaringan saat ini, penting untuk mempertimbangkan keterbatasan alami “gratis” serta bagaimana layanan inti dapat meningkatkan jaringan ke tingkat berikutnya.

DNS, DHCP dan IPAM: Sejarah Singkat

Pada awal kemunculannya, DNS merupakan metode yang praktis untuk mengakses situs web dan aplikasi, dan DHCP hampir tidak pernah terdengar. Mereka biasanya dikelola oleh siapa pun yang memahaminya dan mengandalkan sistem “gratis” seperti BIND / DHCPD dan Microsoft DNS / DHCP. Terkadang spreadsheet adalah dasar untuk mempertahankan layanan protokol penting (mis. DNS & DHCP). Sistem ini sering kali berkembang dengan kumpulan alat “Do-It-Yourself” yang dikelola oleh tim kecil yang terdiri dari para ahli. Hal ini menghambat keputusan operasional dan perencanaan ketika para ahli tersebut pindah ke peran lain atau ke organisasi lain.

Manajemen Alamat IP (IPAM) adalah peningkatan kemudian, kadang-kadang terputus dari orang-orang yang mengelola DNS dan DHCP. Tim yang mengalokasikan sumber daya dan mendefinisikan jaringan bukanlah orang-orang yang mengelola dan mendefinisikan nama dan alamat.

Dampak bisnis atau keandalan sistem ini sering diabaikan dalam strategi TI secara keseluruhan dan jarang ada aturan yang konsisten tentang kelompok mana (Operasi, Sistem, atau Jaringan) yang bertanggung jawab atas pemeliharaannya. Baru belakangan ini konsep gabungan DNS, DHCP dan IPAM (“DDI”) diadopsi.

DDI dalam Jaringan Modern

Dengan pertumbuhan dan ketergantungan yang luar biasa pada jaringan dan mobilitas selama 20 tahun terakhir, serta ledakan penggunaan perangkat seluler, DNS sekarang diharapkan menjadi layanan “nada sambung” yang hanya berfungsi, setiap saat.

Kebutuhan penting untuk akses ke autentikasi, database, dan sumber daya back-end lainnya, IPv6, IoT, dan hampir semua hal lainnya kini menempatkan DDI sebagai inti jaringan. Hal ini menambah persyaratan tambahan untuk keandalan, integrasi dan akuntabilitas yang ekstrem. Ini tidak pernah sepenuhnya direnungkan sebagai bagian dari model desain asli.

Meskipun solusi gratis atau sumber terbuka dapat menyediakan layanan yang diperlukan, namun solusi ini bisa jadi sangat intensif dalam hal pemeliharaan dan kurang tangguh untuk dianggap sebagai “kelas perusahaan” dalam jaringan modern saat ini.

Bisnis juga berpindah ke lingkungan yang lebih otomatis, terutama di cloud dan ruang virtual. Namun, solusi yang sudah ada ini memerlukan lebih banyak lagi penyesuaian jika ingin beradaptasi dengan tingkat otomatisasi yang diharapkan. Ketika IPv6 menjadi lebih umum, kesulitan ini akan semakin meningkat karena masa-masa pembacaan alamat IP melalui telepon sudah lama berlalu. Untuk mengelola lingkungan yang semakin kompleks ini dengan baik, solusi DDI yang mendukung, terukur, dan dikelola secara terpusat adalah suatu keharusan.

Sederhananya, jika layanan DDI mati, atau perubahan membutuhkan waktu terlalu lama untuk diimplementasikan, fungsi bisnis akan terkena dampak negatif, dan pada akhirnya hal ini menyebabkan hilangnya produktivitas dan keuntungan.

Prioritas Tingkat C

Laporan KPMG baru-baru ini mencantumkan lima prioritas strategis eksekutif bagi para CIO:

- Kecepatan yang lebih tinggi ke pasar
- Digitalisasi bisnis
- Menjadi lebih berbasis data
- Membangun kepercayaan publik
- Menerapkan teknologi disruptif

Di bidang DDI, hal ini dapat dikembangkan menjadi inisiatif seperti “Mengamankan bisnis,” “Meningkatkan kecepatan bisnis” atau “Melindungi reputasi perusahaan.”

Dan ketika mendesain ulang infrastruktur DDI untuk menangani inisiatif seperti ini, tidak perlu banyak usaha untuk menghubungkan titik-titik dan melihat keterbatasan solusi tradisional vs solusi modern yang terintegrasi.

Bisnis hanya bisa aman jika Anda melindungi dan memitigasi semua vektor serangan yang mungkin terjadi terhadap data Anda secara memadai, dan DNS sekarang menjadi saluran utama untuk 78% serangan lapisan aplikasi (DDoS) dan 91% distribusi malware, perintah & kontrol dan eksfiltrasi data.

Reputasi perusahaan dan perkembangan yang ditunjukkan menuju bisnis yang lebih berbasis data hanya akan tercapai jika inti jaringan menggunakan sistem yang menangani kepatuhan dan perlindungan infrastruktur, mitigasi malware, dan model operasi dan penahanan ancaman terpusat.

Dan kecepatan bisnis hanya akan berjalan jika DDI diotomatisasi ke titik di mana ia dapat mendukung pertumbuhan yang cepat dan bervariasi yang dituntut oleh infrastruktur berbasis cloud.

Jalan untuk mewujudkan janji pusat data generasi berikutnya bisa jadi sulit. Infrastruktur DNS tradisional dan pengelolaan alamat IP dalam spreadsheet tidak dapat memberikan efisiensi, visibilitas, atau otomatisasi untuk penyediaan beban kerja - membuat TI harus melakukan proses manual dan memakan waktu untuk menyediakan layanan jaringan inti. Transformasi pusat data yang sesungguhnya lebih dari sekadar otomatisasi penyimpanan dan komputasi, organisasi juga membutuhkan otomatisasi jaringan untuk mewujudkan pusat data yang gesit, dikelola secara terpusat, dan berskala tinggi.

Anda perlu mengetahui di mana semua perangkat Anda berada, apa yang perangkat lakukan, dengan siapa perangkat berbicara, bagaimana perangkat berubah dari waktu ke waktu, dan ke mana harus memfokuskan upaya Anda dengan sumber daya terbatas yang Anda miliki.

Sistem yang Ideal

DDI di lingkungan saat ini harus memenuhi sejumlah kriteria penting:

- Waktu kerja yang andal
- Kemudahan perubahan
- Visibilitas Endpoint dan topologi secara real time
- Integrasi ke sistem otomatis
- Redundansi dan atau waktu pemulihan yang cepat

Dengan demikian, sistem yang ideal harus dikelola secara terpusat, membutuhkan sumber daya minimal untuk pemeliharaan, mudah digunakan dan ditingkatkan. Ini juga harus stabil, aman dan mendukung berbagai kebutuhan yang berbeda. Ini bisa berupa administrator tingkat tinggi, dukungan situs/desktop, tugas otomatisasi, perencanaan jaringan, dan forensik keamanan.

Untuk perencanaan dan forensik, “sumber kebenaran tunggal” adalah kuncinya. Sebuah sistem yang menawarkan satu tempat untuk mencari informasi perangkat atau jaringan apa pun, dan bukan mencari beberapa sistem yang mungkin saling bertentangan atau tidak sinkron.

Hal ini mencakup pola pertumbuhan historis, visibilitas ke dalam tren penggunaan DNS &, riwayat sewa DHCP, dan riwayat perangkat. Semua ini adalah kunci untuk dapat merespons insiden keamanan dengan cepat, memecahkan masalah jaringan, dan perencanaan kapasitas secara umum.

Solusi yang ideal juga dapat berinteraksi dengan sistem lain sebagai bagian dari ekosistem yang lebih besar dan secara dinamis berkomunikasi satu sama lain untuk bertukar informasi. Otomatisasi sekarang menjadi suatu keharusan.

Contohnya antara lain:

- Kueri untuk catatan DNS yang telah ditandai sebagai berpotensi berbahaya, DNS dapat "menangkap" ini melalui Zona Kebijakan Respon. Kecocokan ini kemudian dapat dikomunikasikan ke pemindai perangkat, untuk secara otomatis memindai sistem yang dimaksud untuk kemungkinan masalah dan memberi peringatan seperlunya, dan mengkarantina sistem tersebut.
- Log sewa DHCP dapat dikirim ke sistem pencatatan pihak ketiga untuk melacak tren penggunaan dan korelasi peristiwa
- Sistem otomatis untuk penetapan IP dan reklamasi untuk VM yang baru dibuat dapat mempersingkat waktu penyediaan dari jam atau hari menjadi menit.
- Sistem keamanan titik akhir yang menandai titik akhir yang berbahaya dapat secara otomatis memasukkan informasi ini ke dalam kebijakan keamanan untuk mencegah klien menghubungi titik akhir tersebut.

Tentu saja, ini hanyalah beberapa dari banyak contoh di mana interaksi otomatis antar sistem dapat menghasilkan kemudahan perubahan, visibilitas titik akhir dan topologi secara real time, dan integrasi ke sistem otomatis.

Keunggulan Infoblox

Sistem Lama Tidak Akan Dapat Ditingkatkan

Meskipun BIND menjadi standar industri sehubungan dengan DNS dan Internet, namun membutuhkan tingkat pengetahuan dan keterampilan yang tinggi untuk mengimplementasikan dan mengoperasikannya dengan benar. Ada beberapa langkah manual yang terlibat untuk melakukan tugas-tugas sederhana dengan benar (misalnya, nomor seri zona harus ditambah ketika catatan ditambahkan/dimodifikasi/dihapus). Ketika menerapkan konfigurasi dan fitur yang lebih rumit seperti DNSSEC, ada jebakan yang bisa mengakibatkan kinerja yang tidak terduga dan kemungkinan pemadaman DNS secara total.

Selain itu, meskipun BIND mendukung DNS, ia tidak menyediakan pelaporan terintegrasi untuk memungkinkan pemantauan dan manajemen kinerja, dan tidak menyediakan integrasi dengan manajemen alamat IP, yang mengarah pada ketidaksesuaian antara catatan DNS asli dan apa yang mungkin muncul di IPAM. BIND tidak pernah dikembangkan dengan mempertimbangkan otomatisasi, sehingga tidak mengandung API yang kuat untuk otomatisasi sederhana perubahan catatan DNS, sesuatu yang disediakan oleh sistem DDI yang terfokus.

Mengintegrasikan IPAM dengan DNS

Mengintegrasikan IPAM dengan DNS sangat penting untuk menjaga agar kedua sistem tetap akurat dan tersinkronisasi. Ketika perangkat baru digunakan di jaringan, pemberian alamat IP akan dilakukan terlebih dahulu, yang biasanya diikuti dengan permintaan untuk menambahkan host ke DNS. Dengan mengintegrasikan DNS dan IPAM, proses ini menjadi satu langkah - catatan DNS dibuat pada saat yang sama dengan penetapan IP. Hal ini tidak hanya meningkatkan efisiensi, tetapi juga mengurangi kemungkinan kesalahan karena data tidak ditranskripsi atau diteruskan. Seiring dengan terus berkembangnya IPv6, kebutuhan akan IPAM yang terintegrasi dengan DNS semakin meningkat.

Untuk lebih meningkatkan akurasi DNS dan IPAM, komponen penemuan dapat ditambahkan. Memiliki komponen penemuan yang terintegrasi ke dalam IPAM mengubahnya dari sistem yang hampir sepenuhnya bergantung pada tindakan manusia menjadi "IPAM Otoritatif" yang memberikan administrator jaringan dan operator keamanan pandangan real-time tentang apa yang ada di jaringan setiap saat. Ketika dikombinasikan dengan solusi pelaporan, riwayat alamat IP dapat dilacak dari waktu ke waktu, yang dapat menjadi penting untuk menganalisis peristiwa keamanan dengan benar.

Dengan menggunakan Infoblox DDI, Anda memiliki sistem layanan DNS modern yang mengatasi banyak masalah ini dengan cara-cara berikut:

- Mengonsolidasikan DNS, DHCP, manajemen alamat IP, dan layanan jaringan inti lainnya ke dalam satu platform, yang dikelola dari konsol umum
- Mengatur fungsi DDI secara terpusat di berbagai infrastruktur dengan kemampuan terintegrasi untuk lingkungan cloud hybrid dan cloud publik serta cloud virtual dan privat
- Akses kemampuan Pelaporan & Analisis yang kaya dan terintegrasi untuk perencanaan kapasitas, manajemen aset, kontrol kepatuhan, dan audit
- Tingkatkan efisiensi dan otomatisasi TI dengan mengintegrasikan secara mulus dengan sistem TI lainnya melalui RESTful API, bersama dengan Infoblox Grid

Infoblox untuk DNS vs Microsoft DNS

Ketika harus memilih solusi DNS untuk digunakan dengan Microsoft Active Directory, banyak administrator hanya memilih “apa yang ada di dalam kotak dengan Windows Server.” Namun, ada alasan untuk menggunakan DNS non-Microsoft.

- **Keamanan**: Organisasi menuntut solusi terbaik untuk letak DNS eksternal mereka yang terekspos pada serangan Internet. Tersedia solusi DNS pihak ketiga yang dirancang dan dibangun dari awal dengan mempertimbangkan keamanan. Struktur DNS internal organisasi juga terbuka terhadap ancaman berbahaya, malware, phishing, dan eksfiltrasi data.
- **Visibilitas dan Tampilan tunggal**: Sebagian besar organisasi memiliki perpaduan teknologi yang heterogen. Visibilitas yang akurat dan satu atap sangat penting untuk kepatuhan dan kontrol yang efisien.
- **Efisiensi Operasional**: Mengoptimalkan OpEx dengan memanfaatkan otomatisasi dan alur kerja vs manajemen spreadsheet manual.
- **Layanan Cerdas**: Kontrol lalu lintas berbasis DNS yang terintegrasi, penyeimbangan beban jaringan, dan pemantauan layanan menambah nilai yang besar bagi organisasi. Kesenjangan dalam Microsoft IPAM menciptakan ketidakkonsistenan antara kondisi topologi jaringan saat ini dan informasi yang terkandung dalam Microsoft Active Directory (AD). Hal ini dapat menyebabkan terhentinya layanan dasar seperti otentikasi pengguna dan ketersediaan file.

Infoblox IPAM juga dapat berintegrasi secara mulus dengan Situs dan Layanan AD Microsoft dan menutup celah ini untuk AD dan administrator jaringan. Lebih jauh lagi, Infoblox menjangkau hutan Microsoft dan membawa seluruh lingkungan Microsoft ke dalam GUI yang dikelola secara terpusat, menawarkan visibilitas, efisiensi operasional, dan waktu aktif layanan yang belum pernah ada sebelumnya.

Untuk informasi lebih lanjut, lihat "Microsoft vs Non-Microsoft DNS: Facts vs Fiction," yang ditulis oleh Jeremy Moskowitz, Group Policy MVP.

Integrasi Infoblox dengan Produk dan Ekosistem Lain

Infoblox juga menyediakan integrasi tanpa batas dengan teknologi keamanan dan manajemen terkemuka. Kami mengaktifkan otomatisasi cerdas melalui API terbuka dan mendukung beban kerja di lingkungan cloud dan lokal. Penawaran kami terdiri dari keamanan yang sadar konteks dengan intelijen ancaman tingkat lanjut dan integrasi ekosistem.

Sebagai bagian dari ekosistem keamanan yang lebih besar, Infoblox juga mendukung API REST dan PERL, seperti serta API Outbound berbasis peristiwa, yang dapat berinteraksi dengan sistem lain dalam infrastruktur keamanan untuk menambahkan jaringan untuk pemindaian saat ditambahkan ke IPAM, memicu pemindaian perangkat dan/atau karantina jika perangkat akhir mengirimkan kueri yang cocok dengan aturan RPZ (termasuk Threat Insight), dll. Selain itu, Infoblox juga memiliki integrasi dengan Cisco ISE, McAfee, dan lebih dari 20 lainnya, dan jumlahnya terus bertambah.

Kesimpulan

Apa yang Harus Anda Lakukan

Sistem "gratis", seperti BIND/DHCPD, Microsoft DNS/DHCP dan spreadsheet tidak cukup untuk memenuhi kebutuhan jaringan modern. Luangkan waktu untuk memeriksa kelemahan dalam inti Anda dan kembangkan rencana yang akan memigrasikan Anda ke sistem IPAM yang terintegrasi.

Identifikasi alur kerja dan proses IPAM yang ada dan lihat di mana Anda dapat melakukan perbaikan dalam:

- Waktu kerja yang andal
- Kemudahan perubahan
- Visibilitas Endpoint dan topologi secara real time
- Integrasi ke sistem otomatis
- Redundansi dan atau waktu pemulihan yang cepat

Infoblox juga memiliki rekam jejak yang telah terbukti, sebagai pemimpin pasar dengan lebih dari 50% pangsa pasar, dan lebih dari 8.000 pelanggan, dan kami memiliki sejumlah sumber daya untuk membantu Anda dalam keputusan ini: https://www.infoblox.com/resources/?category=Whitepaprs

Langkah Selanjutnya

Hubungi Tim Penjualan Infoblox Anda untuk mendiskusikan arsitektur penerapan yang disarankan.

Kantor Pusat Perusahaan
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com