백서

왜 DDI용 Infoblox인가?

이제 *BIND* 및 *Microsoft*에서 마이그레이션할 때입니다.

목차

많은 조직에서 인터넷에 안정적으로 연결하여 액세스하는 데 이용하는 핵심 서비스는 무료 또는 무료인 것처럼 보이는 제품을 기반으로 합니다. 가격은 매력적일 수 있지만 이러한 제품에는 낮은 안정성, 보안 취약성 그리고 관리 비효율성이라는 숨겨진 비용이 따르는 경우가 많습니다. 오늘날 네트워크에 필연적인 성장과 변화를 계획할 때는 '무료'라는 태생적 한계와 핵심 서비스를 통해 네트워크를 한 단계 업그레이드할 수 있는 방법을 고려하는 것이 중요합니다.

DNS, DHCP 및 IPAM: 짧은 역사

DNS는 처음 등장했을 때 웹사이트와 애플리케이션에 액세스할 수 있는 편리한 방법이었고 DHCP는 거의 알려진 바가 없었습니다. 일반적으로 이런 서비스를 이해하는 사람에 의해 관리되었으며 BIND/DHCPD 및 Microsoft DNS/DHCP와 같은 "무료" 시스템에 의존했습니다. 때로는 스프레드시트가 필수 프로토콜 서비스(예: DNS 및 DHCP)를 유지하기 위한 기반이 되기도 했습니다. 이러한 시스템은 소규모 전문가 팀이 유지 관리하는 'Do-It-Yourself' 도구 모음으로 발전하는 경우가 많았습니다. 이로 인해 해당 전문가가 다른 역할이나 다른 조직으로 이동할 때 운영 및 계획 결정에 차질을 빚었습니다.

IP 주소 관리(IPAM)는 더디게 개선되어, DNS 및 DHCP를 관리하는 사람들로부터 외면을 당하기도 했습니다. 리소스를 할당하고 네트워크를 정의하는 팀은 이름과 주소를 관리하고 정의하는 사람들이 아니었습니다.

이러한 시스템의 비즈니스 영향이나 안정성은 전체 IT 전략 내에서 무시되는 경우가 많았고, 유지 관리를 담당하는 그룹(운영, 시스템 또는 네트워킹)에 대한 일관된 규칙이 거의 없었습니다. DNS, DHCP 및 IPAM('DDI')의 결합 개념이 채택된 것은 최근의 일입니다.

최신 네트워크의 DDI

지난 20년간 네트워크와 모빌리티에 대한 놀라운 성장과 의존도, 그리고 모바일 디바이스 사용의 폭발적인 증가로 인해 이제 DNS는 장소나 디바이스에 구애받지 않고 누구나 쉽게 이용할 수 있는 '보편적'인 서비스입니다.

인증, 데이터베이스, 기타 백엔드 리소스와 같이 핵심적인 요소들과 IPv6, IoT 및 거의 모든 분야에 필수적으로 액세스해야 함에 따라 DDI는 네트워크의 핵심으로 자리 잡았습니다. 이에 따라 최상의 신뢰성, 통합 및 책임을 위한 추가적인 요건이 뒤따릅니다. 이러한 기능은 초기 설계 모델에서 완벽하게 고려되지는 않았습니다.

무료 또는 오픈 소스 솔루션은 필요한 서비스를 제공할 수 있지만, 유지 관리가 많이 필요하고 오늘날의 최신 네트워크에서 '엔터프라이즈급'으로 간주하기에는 견고성이 부족할 수 있습니다.

게다가 기업들은 특히 클라우드와 가상 공간에서 보다 자동화된 환경으로 전환하는 추세입니다. 그러나 이러한 기존 솔루션은 예상되는 자동화 수준에 적응하려면 훨씬 더 많은 필요맞춤화가합니다. IPv6가 널리 보급됨에 따라 전화로 IP 주소를 읽어내는 시대는 이미 오래 전의 일이기 때문에 이러한 어려움은 더욱 커질 것입니다. 점점 더 복잡해지는 환경을 적절하게 관리하려면 지원 가능하고 확장 가능하며 중앙에서 관리되는 DDI 솔루션이 필수입니다.

간단히 말해, DDI 서비스가 중단되거나 변경 사항을 구현하는 데 시간이 너무 오래 걸리면 비즈니스 기능에 부정적인 영향을 미치고 궁극적으로 생산성과 수익 손실로 이어집니다.

최고 경영진의 우선순위

최근 KPMG 보고서는 CIO를 위한 5가지 경영진 전략 우선순위를 다음과 같이 보여주고 있습니다:

- 시장 출시 속도 향상
- 비즈니스의 디지털화
- 데이터 중심으로 변모
- 대중의 신뢰 구축
- 파괴적 기술 구현

DDI 분야에서 이는 '비즈니스 보안', '비즈니스 속도 향상' 또는 '회사의 명성 보호'와 같은 이니셔티브로 전개될 수 있습니다.

그리고 이러한 이니셔티브를 해결하기 위해 DDI 인프라를 재설계할 때 상황을 이해하고 기존 솔루션의 한계와 최신 통합 솔루션과의 차이점을 파악하는 데 많은 노력이 필요하지 않습니다.

데이터에 대한 모든 가능한 공격 경로를 적절히 보호하고 완화해야만 비즈니스의 보안을 유지할 수 있으며, 현재 DNS는 애플리케이션 계층 공격(DDoS)의 78%, 멀웨어 배포, 명령과 제어 및 데이터 유출의 91%를 차지하는 주요 채널로 사용되고 있습니다.

네트워크의 핵심이 인프라 규정 준수 및 보호, 멀웨어 완화, 중앙 집중식 위협 억제 및 운영 모델을 다루는 시스템을 사용해야만 기업의 명성을 얻고 데이터 중심 비즈니스로의 진전을 보여줄 수 있습니다.

또한 클라우드 기반 인프라가 요구하는 빠르고 가변적인 성장을 지원할 수 있을 정도로 DDI가 자동화되어야만 비즈니스의 속도를 유지할 수 있습니다.

차세대 데이터 센터의 가능성을 실현하는 길은 어려울 수 있습니다. 기존의 DNS 인프라와 스프레드시트에서 IP 주소를 관리하는 것은 워크로드 프로비저닝을 위한 효율성, 가시성 또는 자동화를 제공할 수 없기 때문에 IT 부서는 핵심 네트워크 서비스를 프로비저닝하기 위해 시간이 많이 걸리는 수동적인 프로세스를 수행해야 합니다. 진정한 데이터 센터 혁신은 스토리지 및 컴퓨팅 자동화 그 이상이며, 조직에서는 민첩하며 중앙 관리식의 확장성이 뛰어난 데이터 센터를 실현하기 위해 네트워크를 자동화해야 합니다.

모든 디바이스가 어디에 있고, 무엇을 하고, 누구와 대화하고 있는지 , 시간이 지남에 따라 어떻게 변하는지, 제한된 리소스로 어디에 노력을 집중해야 하는지 알아야 합니다.

이상적인 시스템

오늘날의 환경에서 DDI는 다음과 같은 여러 가지 중요한 기준을 충족해야 합니다.

- 안정적인 가동 시간
- 손쉬운 변경
- 실시간 엔드포인트 및 토폴로지 가시성
- 자동화 시스템에 통합
- 중복성 및/또는 신속한 복구 시간

따라서 이상적인 시스템은 중앙에서 관리되고, 유지 관리에 최소한의 리소스가 필요하며, 배포와 확장이 쉬워야 합니다. 또한 안정적이고 안전해야 하며 다양한 요구 사항을 지원해야 합니다. 여기에는 고위 관리자, 사이트/데스크탑 지원, 자동화 작업, 네트워크 계획, 보안 포렌식 등이 포함될 수 있습니다.

계획 및 포렌식에서는 '단일 정보 소스'가 핵심입니다. 충돌하거나 동기화되지 않을 가능성이 있는 여러 시스템에서 검색하는 대신 모든 디바이스 또는 네트워크 정보를 한 곳에서 제공하는 시스템은 필수입니다.

이는 서비스 이용 패턴, DNS 사용 및 추세에 대한 가시성, DHCP 임대 내역, 디바이스 내역까지 확장 적용됩니다. 이 모든 것이 보안 사고에 신속하게 대응하고, 네트워크 문제를 해결하며, 일반적인 용량 계획을 수립하는 데 핵심적인 역할을 합니다.

이상적인 솔루션은 더 큰 에코시스템의 일부로서 다른 시스템과 상호 작용하고 서로 동적으로 소통하여 정보를 교환할 수 있어야 합니다. 이제 자동화는 필수입니다.

예를 들면 다음과 같습니다:

- 잠재적으로 악의적인 것으로 판명된 DNS 레코드에 대한 쿼리에서 DNS는 응답 정책 영역을 통해 이를 '포착'할 수 있습니다. 그러면 이 일치 항목이 디바이스 스캐너에 전달되어 해당 시스템을 자동으로 스캔하여 가능한 문제를 찾아내고 필요에 따라 경고를 보내고 이 시스템을 격리할 수 있습니다.
- DHCP 임대 로그를 타사 로깅 시스템으로 전송하여 사용 추세 및 이벤트 상관관계를 추적할 수 있습니다.
- 새로 생성된 VM의 IP 할당 및 회수를 위한 자동화된 시스템을 사용하면 프로비저닝 시간을 몇 시간 또는 며칠에서 몇 분으로 단축할 수 있습니다.
- 악의적인 엔드포인트를 탐지하는 엔드포인트 보안 시스템은 이 정보를 보안 정책에 자동으로 푸시하여 클라이언트가 해당 엔드포인트에 접촉하지 못하도록 할 수 있습니다

물론 이는 시스템 간의 자동화된 상호작용을 통해 변경의 용이성, 실시간 엔드포인트 및 토폴로지 가시성, 자동화된 시스템으로의 통합 등 수많은 사례 중 일부에 불과합니다.

Infoblox의 장점

확장되지 않는 레거시 시스템

BIND는 DNS 및 Internet과 관련하여 업계 표준이 되었지만 올바르게 구현하고 운영하려면 높은 수준의 지식과 기술이 필요합니다. 간단한 작업을 올바르게 수행하기 위해 여러 단계의 수동 작업이 필요합니다. DNSSEC와 같은 더 복잡한 구성과 기능을 구현할 때 예측할 수 없는 성능을 초래하고 DNS 전체가 중단될 수도 있는 위험이 있습니다.

또한 BIND는 DNS를 지원하지만 성능 모니터링 및 관리를 위한 통합 보고 기능을 제공하지 않으며, IP 주소 관리와 통합되지 않아 기본 DNS 레코드와 IPAM에 표시되는 레코드 간에 불일치가 발생할 수 있습니다. BIND는 자동화를 염두에 두고 개발되지 않았기 때문에 집중적인 DDI 시스템이 제공하는 DNS 레코드 변경을 간단하게 자동화할 수 있는 강력한 API가 포함되어 있지 않습니다.

IPAM과 DNS 통합

IPAM과 DNS의 통합은 두 시스템을 정확하고 동기화된 상태로 유지하는 데 반드시 필요합니다. 새 디바이스가 네트워크에 배포되면 IP 주소 할당이 먼저 이루어지며, 일반적으로 호스트를 DNS에 추가하라는 요청이 바로 이어집니다. DNS와 IPAM을 통합하면 이 프로세스가 한 번에 이루어집니다. 즉, IP 할당과 동시에 DNS 레코드가 생성됩니다. 이는 효율성을 향상시킬 뿐만 아니라 데이터가 기록되거나 전달되지 않기 때문에 오류 가능성을 줄여줍니다. IPv6의 확산이 계속되면서 DNS와 IPAM 통합의 필요성도 증가하고 있습니다.

DNS 및 IPAM의 정확성을 더욱 향상시키기 위해 검색 구성 요소를 추가할 수 있습니다. 검색 구성 요소를 IPAM에 통합하면 거의 전적으로 사람의 작업에 의존하는 시스템에서 네트워크 관리자와 보안 운영자가 언제든지 네트워크에 무엇이 있는지 실시간으로 파악할 수 있는 '권한 있는 IPAM'으로 개선할 수 있습니다. 보고 솔루션과 함께 사용하면 IP 주소의 이력을 시간에 따라 추적할 수 있으므로 보안 이벤트를 올바르게 분석하는 데 매우 유용합니다.

Infoblox DDI를 사용하면 다음과 같은 방법으로 이러한 많은 문제를 해결하는 최신 DNS 서비스 시스템을 갖출 수 있습니다.

- DNS, DHCP, IP 주소 관리 및 기타 핵심 네트워크 서비스를 단일 플랫폼으로 통합하여 공통 콘솔에서 관리하세요.
- 하이브리드 및 퍼블릭 클라우드와 가상 및 프라이빗 클라우드 환경을 위한 통합 기능을 통해 다양한 인프라 전반에 걸쳐 DDI 기능을 중앙에서 오케스트레이션하세요.
- 자원의 계획, 자산 관리, 규정 준수 제어 및 감사를 위한 풍부한 통합 보고 및 분석 기능을 활용하세요.
- Infoblox Grid와 함께 RESTful API를 통해 다른 IT 시스템과 원활하게 통합하여 IT 효율성 및 자동화를 향상시키세요.

DNS용 Infoblox와 Microsoft DNS 비교

대부분의 관리자들은 Microsoft Active Directory와 함께 사용할 DNS 솔루션을 선택할 때 'Windows Server에 포함된 항목'을 선택하기만 하면 됩니다. 그러나 타사 DNS를 사용해야 하는 이유가 있습니다.

- **보안**: 조직에는 Internet 공격에 노출된 외부 DNS를 위한 최상의 솔루션이 필요합니다. 처음부터 보안을 염두에 두고 설계 및 구축된 서드파티 DNS 솔루션이 하나의 대안입니다. 조직의 내부 DNS 구조는 악의적인 위협, 멀웨어, 피싱 및 데이터 유출에 똑같이 노출되어 있습니다.
- **가시성 및 단일 뷰**: 대부분의 조직에서는 이기종 기술을 혼용하고 있습니다. 효율적인 규정 준수 및 제어를 위해서는 정확한 종합적인 가시성이 필수적입니다.
- **운영 효율성**: 자동화 및 워크플로우를 활용하여 수동 스프레드시트 관리 대비 운영 효율성을 최적화합니다.
- **지능형 서비스**: 통합 DNS 기반 트래픽 제어, 네트워크 부하 분산 및 서비스 모니터링은 조직에 큰 가치를 더합니다. Microsoft IPAM에 공백이 생기면 네트워크 토폴로지의 현재 상태와 Microsoft AD(Active Directory)에 포함된 정보 간에 불일치가 발생합니다. 이로 인해 사용자 인증 및 파일 가용성과 같은 기본 서비스가 완전히 중단될 수 있습니다.

Infoblox IPAM은 Microsoft AD 사이트 및 서비스와 원활하게 통합되어 AD 및 네트워크 관리자를 위해 이러한 간극을 메워줍니다. 또한 Infoblox는 Microsoft 포리스트에 걸쳐 전체 Microsoft 환경을 중앙에서 관리되는 GUI로 통합하여 전례 없는 가시성, 운영 효율성 및 서비스 가동 시간을 제공합니다.

자세한 내용은 그룹 정책 MVP인 Jeremy Moskowitz가 작성한 'Microsoft와 타사 DNS: 사실과 허구'를 참조하십시오.

다른 제품 및 에코시스템과 Infoblox 통합

Infoblox는 업계를 주도하는 보안 및 관리 기술과 원활하게 통합할 수 있도록 합니다. 오픈 API를 통해 지능형 자동화를 지원하고 클라우드와 온프레미스 환경 모두에서 워크로드를 지원합니다. 당사의 제품은 고급 위협 인텔리전스와 에코시스템이 통합된 상황 인식 보안 기능을 갖추고 있습니다.

더 큰 보안 에코시스템의 일부로서 Infoblox는 REST 및 PERL API를 지원하며 IPAM이 탐지해서 추가된 네트워크를 자동으로 다른 보안 시스템과 상호 작용하거나, RPZ(위협 인사이트)에 트리거된 모든 조직의 위협 디바이스를 자동으로 격리 혹은 스캐닝하도록 트리거할 수 있는 이벤트 기반의 아웃바운드 API도 지원합니다. 또한 Infoblox는 Cisco ISE, McAfee 및 20개 이상의 다른 솔루션과도 통합되어 있으며 그 수는 계속 증가하고 있습니다.

결론

권고 사항

BIND/DHCPD, Microsoft DNS/DHCP 및 스프레드시트와 같은 '무료' 시스템은 최신 네트워크의 요구 사항을 적절히 해결하지 못합니다. 시간을 내어 핵심 시스템의 약점을 파악하고 통합 IPAM 시스템으로 마이그레이션할 계획을 세우십시오.

기존 워크플로와 IPAM 프로세스를 식별하고 다음에서 개선할 수 있는 부분을 살펴보십시오.

- 안정적인 가동 시간
- 손쉬운 변경
- 실시간 엔드포인트 및 토폴로지 가시성
- 자동화된 시스템과의 통합
- 중복성 및/또는 신속한 복구 시간

시장 점유율 50% 이상과 12,000개 이상의 고객사를 보유한 Infoblox는 시장 리더로서 검증된 실적을 갖추고 있으며, 귀사의 결정에 도움이 되는 다양한 리소스를 제공하고 있습니다.
https://www.infoblox.com/resources/?category=Whitepaprs

다음 단계

Infoblox 영업 팀에 문의하여 최적의 아키텍처에 대해 상담 받으세요.