Infoblox
NEXT LEVEL NETWORKING

DDI에는 왜 인포블록스인가

이제 BIND 및 Microsoft에서 전환할 때

많은 기업들이 안정적인 인터넷 연결 및 접속을 위해 사용하고 있는 핵심 서비스는 무료 제품이거나 무료로 보이는 제품에 기반하고 있다. 가격이 매력적일 수 있으나, 이러한 제품들은 흔히 기능이 제한적이고 비효율적인 관리로 인해 숨겨진 비용을 내포하고 있다. 오늘날 네트워크에서 불가피한 확장 및 변경을 계획하고 있다면, 이러한 "무료 제품"의 태생적 제한사항을 필수적으로 고려해야 하며, 핵심 네트워크 서비스의 업그레이드를 통해 네트워크가 어떻게 개선될 수 있을지 또한 생각해야 한다.

DNS, DHCP 및 IPAM: 짧은 역사

초기에 DNS는 웹사이트 및 애플리케이션에 접근하기 위한 편리한 방법이었으며, DHCP는 사실상 매우 생소한 개념이었다. 보통 누구든지 이 개념들을 이해한 사람들이 관리했으며, BIND/DHCPD 및 Microsoft DNS/DHCP와 같은 "무료" 시스템에 의존했다. 때로는 필수 프로토콜 서비스(DNS 및 DHCP 등)가 스프레드시트를 기반으로 유지 및 관리되기도 했다. 이러한 시스템들은 대개 소규모 전문가 팀에 의해 유지 및 관리되는 "직접 만들어진(DIY)" 도구들을 통해 진화해 왔다. 따라서, 이러한 전문가들이 다른 직책 혹은 다른 회사로 옮기게 되면 운영 및 계획에 있어 의사결정이 어려워졌다.

IP 주소 관리(IP Address management, IPAM)는 이후 개선된 개념으로, 때로는 DNS 및 DHCP를 관리하던 이들과 분리되기도 했다. 자원 분배 및 네트워크 정의를 담당하던 팀이 네트워크 이름과 주소를 관리하고 정의하던 이들과 달랐던 것이다.

이러한 시스템들의 안정성이나 사업에 미치는 영향은 전체 IT 전략상 무시되기 쉬웠으며 (운영, 시스템, 네트워크 담당 중) 누가 유지관리 책임을 지는지에 대해 일관된 규칙을 찾기 어려웠다. "DDI", 즉 통합된 DNS, DHCP 및 IPAM의 개념이 채택된 것은 최근의 일이다.

현대화된 네트워크상의 DDI

지난 20년간 네트워크 및 이동성은 놀랍게 성장했으며 그에 대한 의존도 또한 높아졌다. 모바일 기기의 활용 역시 폭발적으로 늘어남에 따라 이제 DNS는 상시 작동하는 "신호음"과 같은 서비스로 생각된다.

인증, 데이터베이스, 기타 백엔드 자원, IPv6, 사물인터넷, 그 밖의 거의 모든 것에 대한 접근의 필요성이 중요해지면서 이제 네트워크의 중심에 DDI가 있게 되었다. 이로 인해 극도의 안정성, 통합성 및 책임성이라는 추가적인 요구사항이 생긴다. 이들은 기존에 설계된 모델의 일부로서 충분히 고려되지 않은 개념들이다.

무료 솔루션 및 오픈소스 솔루션이 필요한 서비스를 제공할 수는 있지만, 유지관리가 어렵고 견고성이 떨어지므로 오늘날의 현대화된 네트워크 환경에서 "기업 수준"에 부합한다고 판단하기는 어려울 수 있다.

기업들은 또한 보다 자동화된 환경을 향해 움직이고 있으며, 특히 클라우드 및 가상 공간에 대해 그렇다. 그러나 앞서 언급된 기존 솔루션들은 기대되는 자동화 수준에 맞추기 위해서는 훨씬 더 많은 조정이 필요하다. IPv6가 점점 보편화되어 더 이상 유선상으로 IP주소를 불러주는 경우가 없어짐에 따라 이러한 어려움은 더욱 심화될 것이다. 이처럼 점점 더 복잡해지는 환경을 제대로 관리하기 위해서는 지원이 가능하고 확장 가능한 중앙 관리 DDI 솔루션이 필수적이다.

간단히 설명하자면, DDI 서비스가 다운되거나 변동을 이행하는 데 너무 오랜 시간이 소요되면 사업 기능에 부정적인 영향을 미치며, 이는 궁극적으로 생산성 및 수익성의 손실로 이어진다.

C-수준 우선순위

최근 KPMG 보고서는 다음 5가지의 CIO를 위한 전략 우선순위를 제시하였다.

- 보다 빠른 마케팅 속도
- 사업의 디지털화
- 데이터 중심
- 공공 신뢰 구축
- 혁신 기술의 도입

DDI 분야에서는 이러한 우선순위들이 “사업 보안 강화”, “사업 속도 개선” 혹은 “회사 평판 보호”와 같은 추진목표로 발전할 수 있다.

따라서 이러한 추진목표를 달성하기 위해 DDI 인프라를 재설계하는 경우 각 요소를 연결하여 생각함으로써 현대화된 통합 솔루션 대비 기존 솔루션의 한계를 인식하는 것은 어려운 일이 아니다.

침입 가능성이 있는 모든 경로를 차단 및 보호하여 데이터를 보호해야만 사업이 안전하게 유지될 수 있다. 오늘날 DNS는 디도스(DDoS) 공격의 78%를 차지하는 주요 경로이며, 악성 소프트웨어 배포, C&C, 데이터 반출의 91%가 DNS 상에서 이루어진다.

기업의 좋은 평판과 데이터 중심 사업을 향해 나아가고 있음을 보여주기 위해서는 네트워크의 중심에서 인프라 합치와 보안 문제를 해결해주는 시스템을 이용해야 한다. 해당 시스템은 또한 악성 소프트웨어를 차단하고 중앙에서 위협 봉쇄 및 운영 모델을 제공해야 한다.

사업의 진행속도 역시 DDI가 자동화되어 클라우드 기반의 인프라가 요구하는 빠르고 역동적인 성장을 지원할 수 있어야만 유지가 가능하다.

차세대 데이터센터라는 약속을 실현하는 길은 험난할 수도 있다. 전통적 DNS 인프라나 IP주소를 스프레드시트로 관리하는 것으로는 효율성, 가시성 및 워크로드 프로비저닝의 자동화를 확보할 수 없다. IT 담당자들이 핵심 네트워크 서비스 프로비저닝을 위해 많은 시간이 소요되는 수작업을 계속해야 하기 때문이다. 진정한 데이터 센터로의 변화는 저장 공간이나 컴퓨터를 자동화하는 과정 이상을 요구한다. 기업들은 네트워크를 함께 자동화하여 중앙에서 관리되며 기민하고 확장성이 높은 데이터 센터를 실현해야 한다.

모든 기기가 어디에 있는지, 무엇을 하고 있는지, 누구와 이야기하고 있는지, 시간이 지남에 따라 어떻게 변화하는지, 주어진 한정된 자원으로 어디에 노력을 집중해야 하는지 이해할 수 있어야 한다.

이상적인 시스템

오늘날 네트워크 환경의 DDI는 다음과 같은 여러 중요한 기준에 부합해야 한다.

- 안정적인 가동시간
- 변경의 용이함
- 실시간 엔드포인트 및 토폴로지 가시성
- 자동화 시스템과의 통합
- 중복성, 혹은 빠른 복구 시간

따라서 이상적인 시스템은 중앙에서 관리되고, 유지에 있어 최소한의 자원만을 필요로 하며, 배치 및 확장이 용이해야 한다. 안정성과 보안성을 갖추고, 다양하고 상이한 요구사항을 지원해야 한다. 이는 수준 높은 관리자, 사이트 및 데스크탑 지원, 자동화 과제, 네트워크 계획 및 보안 조사 등이 될 수 있다.

계획과 조사에 있어서는 “단일 검색 소스”가 중요하다. 여러 곳에서 검색을 해야 하거나 서로 충돌하거나 동기화되지 않은 시스템들을 검색해야 하는 시스템이 아닌, 한 곳에서 검색을 통해 모든 기기 또는 네트워크 정보를 찾아낼 수 있는 시스템이 필수적이다.

이는 이전의 발달 패턴에도 확장 적용되며 DNS 사용 및 경향에 대한 가시성, DHCP 대여 기록 및 기기 기록을 확인함에 있어서도 동일하게 적용된다. 이러한 모든 요소들은 보안 사고에 신속하게 대응하고 네트워크 문제를 해결하며 일반적 용량 계획에 있어 핵심적인 요소들이다.

이상적인 솔루션은 또한 더 큰 에코시스템의 일부로서 다른 시스템과 상호작용할 수 있어야 하며, 서로 정보 교환을 위해 역동적으로 통신할 수 있어야 한다. 오늘날 자동화는 필수 조건이다.

여기에는 다음과 같은 사례가 포함된다.

- 악성일 가능성이 있는 것으로 식별된 DNS 기록에 대한 질의를 DNS가 대응정책영역을 통해 “포착”할 수 있다. 이렇게 포착된 정보는 이후 기기 스캐너로 전송되어 해당 시스템의 문제가 될 수 있는 부분을 자동으로 스캔한다. 필요 시 경고 후, 해당 시스템을 격리한다.
- DHCP 대여 기록을 타사 기록 시스템에 전송하여 사용 추세와 사건 연관성을 추적할 수 있다.
- IP 할당을 위한 자동화 시스템 및 신규 생성된 VM의 자동 교정을 통해 프로비저닝에 소요되는 시간을 몇 시간 또는 몇 일에서 몇 분으로 줄여준다.
- 엔드포인트 보안 시스템이 악성 엔드포인트를 식별하면 자동으로 해당 정보를 보안 정책으로 가져가 클라이언트가 해당 엔드포인트에 접촉하는 것을 방지한다.

이러한 사례들은 시스템간 자동화된 상호작용이 변화 용이성, 실시간 엔드포인트 및 토폴로지 가시성, 자동화 시스템 통합으로 이어질 수 있다는 사실을 보여주는 다양한 사례들 중 일부에 불과하다.

인포블록스의 장점

확장 불가능한 기존 시스템

BIND가 DNS와 인터넷에 관련해 업계 기준이 되었지만, BIND는 제대로 실행 및 운영하려면 높은 수준의 지식과 기술을 필요로 한다. 단순한 작업도 제대로 수행하려면 여러 수작업이 수반된다(일례로 기록이 추가/변경/삭제된 경우 한 영역의 일련번호가 일정하게 증가되어야 함). DNSSEC와 같이 보다 복잡한 설정 및 기능을 실행할 때는 예상치 못한 결과 혹은 때로는 완전한 DNS 정지에 이를 수 있는 위험요소들이 존재한다.

나아가, BIND가 DNS를 지원하긴 하지만 시스템 성능을 감시 및 관리하기 위한 통합 보고기능을 제공하지 않으며, IP 주소 관리 시스템과도 통합성을 제공하지 않는다. 이는 DNS 기록 원본과 IPAM상 나타나는 기록 사이에 차이점을 야기할 수 있다. BIND는 자동화를 염두에 두고 개발된 시스템이 아니기 때문에 DNS 기록 변경을 단순 자동화하기 위해 충분한 API를 갖고 있지 못하다. 집중된 DDI 시스템은 이러한 부분을 제공한다.

IPAM과 DNS의 통합

IPAM과 DNS를 통합하는 것은 두 시스템을 정확하고 동기화된 상태로 유지하는 데에 있어 필수적이다. 새로운 기기가 네트워크상에 나타나면 IP 주소가 먼저 할당되고 이후 바로 해당 호스트를 DNS에 추가하라는 요청이 이어지게 된다. DNS를 IPAM과 통합하게 되면 이러한 절차가 한 번에 처리되며 IP 주소가 할당됨과 동시에 DNS 기록이 생성된다. 이러한 절차는 효율성을 제고할 뿐만 아니라 오류의 가능성 또한 줄여준다. 데이터가 필사되거나 중계될 필요가 없기 때문이다. IPv6 보급이 지속됨에 따라 IPAM과 DNS의 통합에 대한 필요성은 계속 증가한다.

DNS 및 IPAM의 정확도를 더욱 제고하기 위해 발견 요소를 추가할 수 있다. IPAM로 발견 요소를 통합시키면 인간의 행동에 거의 전적으로 의존하던 시스템이 “권한 있는 IPAM” 시스템으로 바뀌며 네트워크 관리자 및 보안 담당자가 특정 시점에 네트워크상에 어떤 요소들이 있는지 실시간으로 확인할 수 있다. 보고 솔루션과 통합 시, IP주소 기록을 시간 경과에 따라 추적 가능하며, 이는 보안 이벤트들을 제대로 분석하는 데 매우 중요할 수 있다.

인포블록스 DDI 활용 시 이러한 문제들을 다음과 같이 해결하는 현대화된 DNS 서비스를 제공받는다.

- DNS, DHCP, IP 주소 관리, 기타 핵심 네트워크 서비스들을 하나의 플랫폼에 통합하여 공용 콘솔에서 관리 가능
- DDI 기능을 다양한 인프라에 걸쳐 통합된 기능을 통해 중앙에서 조정하여 하이브리드 및 공공 클라우드, 그리고 가상 및 개인 클라우드 환경 활용을 지원
- 풍부한 통합 보고 및 분석 기능을 활용하여 용량 계획, 자산 관리, 이행 통제 및 감사를 수행
- RESTful API 및 인포블록스 Grid를 함께 활용하여 기타 IT시스템과 매끄럽게 통합하여 IT 효율성 및 자동화 제고

인포블록스 DNS vs Microsoft DNS

Microsoft 액티브 디렉터리와 함께 사용할 DNS 솔루션 선택 시 많은 관리자들은 단순히 “윈도우 서버에 같이 들어 있는 것”을 선택한다. 그러나 Microsoft DNS가 아닌 솔루션을 사용해야 하는 이유가 있다.

- 보안: 기업들은 외부 DNS가 인터넷 공격에 노출되어 있기 때문에 최고의 솔루션을 요구한다. 설계 초기부터 보안을 염두에 두고 설계 및 제작된 제3자 DNS 솔루션들이 있다. 기업의 내부 DNS 구조 역시 악성 위협, 악성 소프트웨어, 피싱 및 데이터 반출에 동일하게 노출되어 있다.
- 가시성 및 단일화된 시야: 대부분의 기업들은 이질적인 여러 기술을 함께 사용하고 있다. 정확하고 단일화된 가시성은 효율적인 규정 준수 및 제어에 필수적인 요소이다.
- 운영 효율: 자동화 및 워크플로를 활용하여 운영비용 최적화 vs 수작업으로 스프레드시트 관리
- 스마트 서비스: DNS 기반 통합 트래픽 통제, 네트워크 하중 조정 및 서비스 모니터링 기능은 기업의 가치에 크게 기여한다. Microsoft IPAM 내에 존재하는 공백 지점들은 현 상태의 네트워크 토폴로지와 Microsoft 액티브 디렉터리에 들어 있는 정보 간의 모순을 야기한다. 이는 사용자 승인 및 파일 가용성 등 기본적인 서비스의 전면 중단으로까지 이어질 수 있다.

인포블록스 IPAM은 또한 Microsoft 액티브 디렉터리 사이트 및 서비스와 매끄럽게 통합되어 액티브 디렉터리 및 네트워크 관리자 양쪽의 관점에서 공백 지점을 채워준다. 나아가 인포블록스는 Microsoft 포레스트를 활용하여 전체 Microsoft 환경을 중앙 관리되는 GUI로 불러온다. 이를 통해 독보적인 가시성, 운영 효율, 서비스 가동 시간을 제공한다.

더 자세한 정보는 “Microsoft DNS vs Microsoft 이외의 DNS: 사실과 허구(Microsoft vs Non-Microsoft DNS: Facts vs Fiction)” 참조. 그룹 정책 MVP 제레미 모스코비츠(Jeremy Moskowitz) 저.

인포블록스와 타사 제품의 통합 및 에코시스템

인포블록스는 또한 업계를 선도하는 보안 및 관리 기술과도 매끄러운 통합을 제공한다. 공개된 API를 통해 스마트 자동화가 가능하며 클라우드 및 온프레미스 환경에서 워크로드를 지원한다. 인포블록스는 첨단 위협 정보와 에코시스템 통합을 갖춘 컨텍스트 인식형 보안을 제안한다.

보다 큰 보안 에코시스템의 일부로서 인포블록스는 REST 및 PERL API를 지원하며, 이벤트 기반의 아웃바운드 API 또한 지원한다. 이를 통해 보안 인프라 내의 다른 시스템들과 상호작용하여 IPAM에 추가되는 네트워크를 스캔 목록에 추가하고 단말기가 대응정책영역의 규칙(위협 인사이트 포함)에 상응하는 질의를 전송하는 경우 기기 스캔 혹은 격리를 시행할 수 있다. 또한 인포블록스는 Cisco ISE, McAfee를 비롯한 기타 20여개 플랫폼과 통합되어 있으며, 이 숫자는 늘어나고 있다.

결론

무엇을 해야 하는가

BIND/DHCPD, Microsoft DNS/DHCP, 스프레드시트와 같은 “무료” 시스템들은 현대화된 네트워크의 요구사항을 충분히 해결하지 못한다. 시간을 들여 기존 핵심 서비스의 취약점을 살펴보고, 통합된 IPAM 시스템으로 전환할 계획을 수립해야 한다.

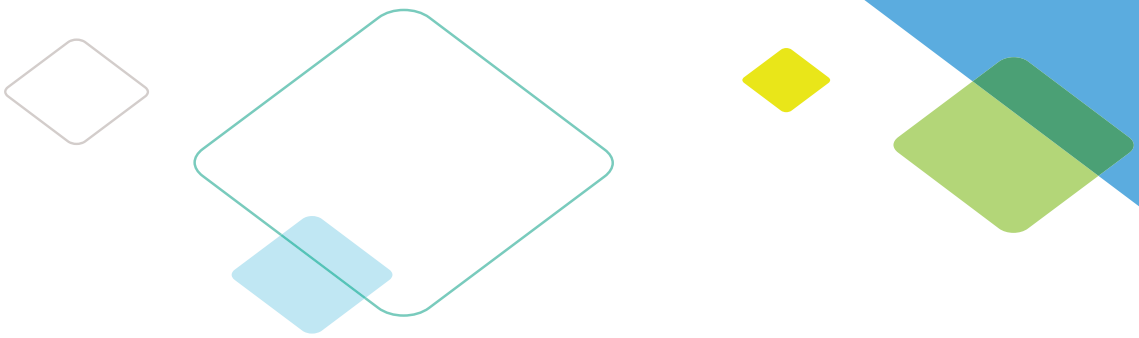
기존 워크플로 및 IPAM 절차들을 확인하여 다음의 분야에서 개선될 부분이 있는지 살펴본다.

- 안정적인 가동시간
- 변경의 용이함
- 실시간 엔드포인트 및 토폴로지 가시성
- 자동화 시스템과의 통합
- 중복성, 혹은 빠른 복구 시간

인포블록스는 50% 이상의 시장 점유율로 시장을 선도하고 있으며, 8,000여개 업체의 고객을 확보하는 등 입증된 실적을 갖고 있다. 또한 결정을 돕기 위한 많은 자원을 갖추고 있다.
https://www.infoblox.com/resources/?category=Whitepapers

다음 단계

인포블록스 세일즈팀에 연락하여 배치 구조에 대한 제안사항을 상담하십시오.



Infoblox
NEXT LEVEL NETWORKING

인포블록스는 보안 클라우드 관리 네트워크 서비스를 통해 더 높은 수준의 DDI로 이행하는 방법을 선도하고 있다. 인포블록스는 온프레미스, 클라우드 및 하이브리드 네트워크에 더 높은 수준의 보안, 신뢰성, 자동화를 제공하여 고객에게 네트워크 관리를 위한 단일 창으로 이동하는 경로를 안내한다. 인포블록스는 Fortune 지 선정 500대 기업 중 350개 기업을 비롯해 8,000명의 고객을 보유하여 50%의 시장 점유율을 차지하고 있는 널리 인정 받는 선두 기업이다.

본사 | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (미국 및 캐나다 수신자부담) | info@infoblox.com | www.infoblox.com