Citrix NetScaler 시작

Aug 30, 2016

이 라이브러리 섹션은 복잡한 네트워킹 장비를 설치하고 구성하는 시스템 및 네트워크 관리자를 대상으로 하며, 다음 항목을 비롯한 NetScaler의 초기 설정 및 기본 구성에 대해 설명합니다.

NetScaler 이해

Citrix NetScaler 제품은 일종의 응용 프로그램 스위치로서 응용 프로그램별 트래픽 분석을 수행하여 웹 응용 프로그램을 위한 계층 4-계층 7(L4–L7) 네트워크 트래픽을 지능적으로 분산시키고 최적화하며 보안을 유지합니다. 예를 들어, NetScaler는 오랫동안 지속된 TCP 연결 대신 개별 HTTP 요청에 대해 부하 분산 결정을 내리므로 서버 실패나 속도 저하를 좀더 빠르고 클라이언트에 덜 방해가 되도록 관리할 수 있습니다. NetScaler 기능 집합은 스위칭 기능, 보안 및 보호 기능, 서버-팜 최적화 기능 등으로 개략적으로 분류할 수 있습니다.

스위칭 기능

응용 프로그램 서버 앞에 배포할 경우 NetScaler는 클라이언트 요청을 지정하는 방식으로 트래픽을 최적으로 분산시킵니다. 관리자는 HTTP 또는 TCP 요청 본문의 정보 및 URL, 응용 프로그램 데이터 유형 또는 쿠키와 같은 L4-L7 헤더 정보를 기준으로 응용 프로그램 트래픽을 세그먼트화할 수 있습니다. 여러 가지 부하 분산 알고리즘 및 폭넓은 서버 헬스 체크를 통해 클라이언트 요청이 올바른 서버로 지정되도록 함으로써 응용 프로그램 가용성을 높입니다.

보안 및 보호 기능

NetScaler 보안 및 보호 기능은 응용 프로그램 계층 공격으로부터 웹 응용 프로그램을 보호합니다. NetScaler에서는 정당한 클라이언트 요청을 허용하고 악의적인 요청을 차단할 수 있습니다. 서비스 거부(DoS) 공격에 대한 기본 제공 방어 기능을 제공하며, 서버를 무력화할 수 있는 응용 프로그램 트래픽의 과도한 증가를 방지하는 기능을 지원합니다. 사용 가능한 기본 제공 방화벽은 버퍼 오버플로 악용, SQL 삽입 시도, 교차 사이트 스크립팅 공격 등 응용 프로그램 계층 공격으로부터 웹 응용 프로그램을 보호합니다. 또한 방화벽은 회사 기밀 정보 및 민감한 고객 데이터를 보호함으로써 ID 도용 보호 기능을 제공합니다.

최적화 기능

최적화 기능은 SSL(Secure Sockets Layer) 처리, 데이터 압축, 클라이언트 연결 유지, TCP 버퍼링 및 서버에서 정적 및 동적 콘텐츠 캐싱 등의 리소스를 많이 사용하는 작업의 부하를 줄입니다. 그러면 서버 팜에서 서버의 성능이 향상되고 결과적으로 응용 프로그램의 속도가 빨라집니다. NetScaler는 높은 지연 및 정체된 네트워크 링크로 인한 문제를 완화하는 여러 가지 투명한 TCP 최적화를 지원하여 클라이언트나 서버의 구성을 변경하지 않고도 응용 프로그램의 전달 속도를 높일 수 있습니다.

정책 및 식 이해

정책은 NetScaler에서 트래픽 필터링 및 관리에 대한 특정 세부 사항을 정의합니다. 정책은 식 및 작업의 두 부분으로 구성됩니다. 식은 정책이 일치하는 요청 유형을 정의합니다. 작업은 요청이 식과 일치할 경우 NetScaler에서 무엇을 해야 하는지 말해줍니다. 예를 들어, 식은 보안 공격 유형에 대한 특정 URL 패턴과 일치하도록 정의하고, 작업은 연결을 끊거나 재설정하도록 지정할 수 있습니다. 각 정책에는 우선 순위가 있으며, 우선 순위에 따라 정책이 평가되는 순서가 결정됩니다.

NetScaler가 트래픽을 수신하면 적절한 정책 목록에 따라 트래픽의 처리 방법이 결정됩니다. 목록의 각 정책에는 정책과 일치하기 위한 연결 충족 조건을 정의하는 하나 이상의 식이 포함됩니다.

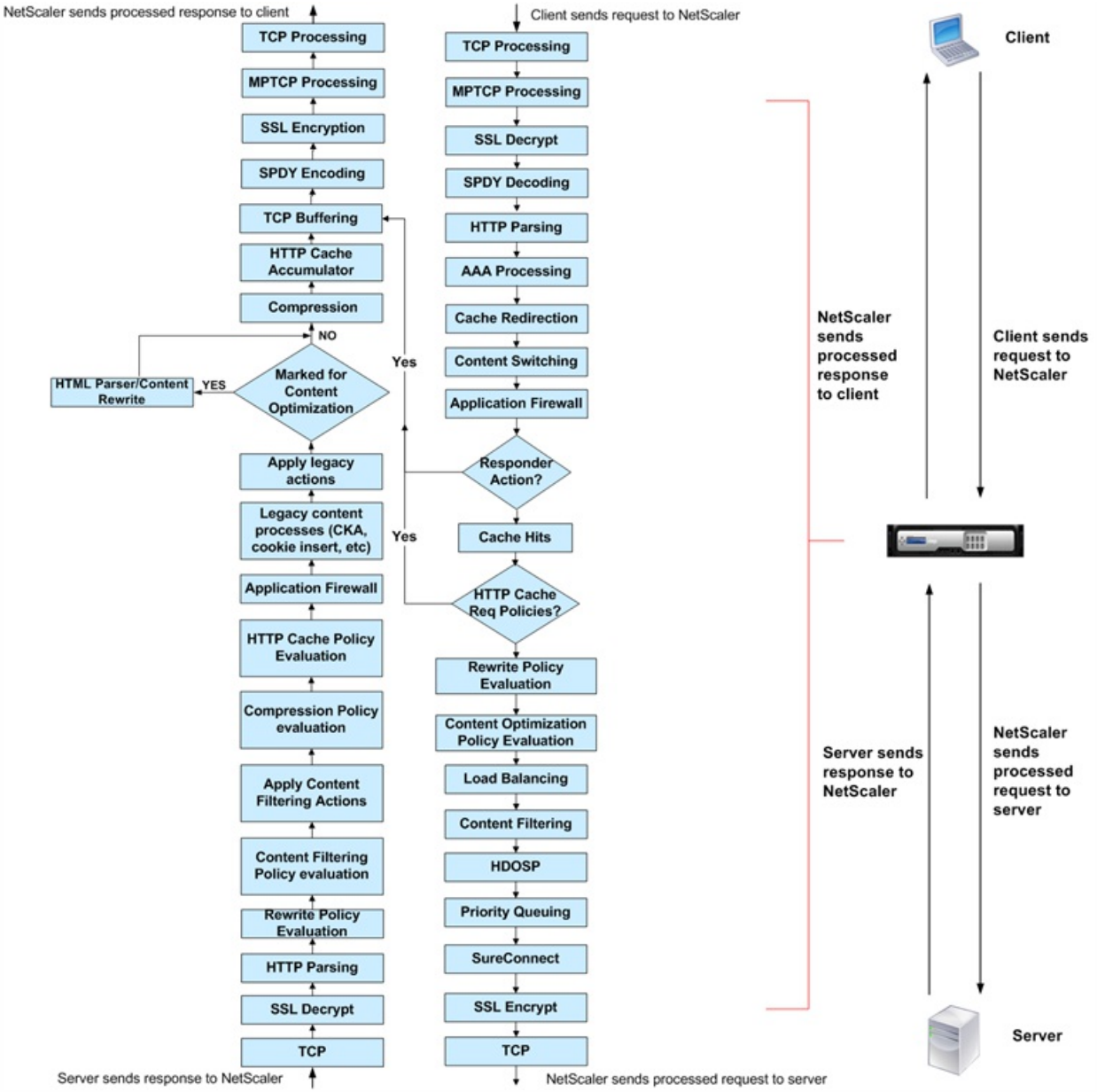
다시 쓰기 정책을 제외한 모든 정책 유형에 대해 NetScaler는 요청이 일치하는 첫 번째 정책만 구현합니다(일치하는 다른 추가 정책은 고려하지 않습니다). 다시 쓰기 정책의 경우 NetScaler는 순서대로 정책을 평가하고 여러 정책이 일치하면 해당하는 순서로 연관된 작업을 수행합니다. 정책 우선 순위에 따라 원하는 결과가 달라질 수 있습니다.

기능 처리 순서

요구 사항에 따라 여러 기능을 구성하도록 선택할 수 있습니다. 예를 들어, 압축 및 SSL 오프로드를 둘 다 구성하도록 선택할 수 있습니다. 이 경우 송신 패킷은 클라이언트로 보내지기 전에 압축된 다음 암호화됩니다.

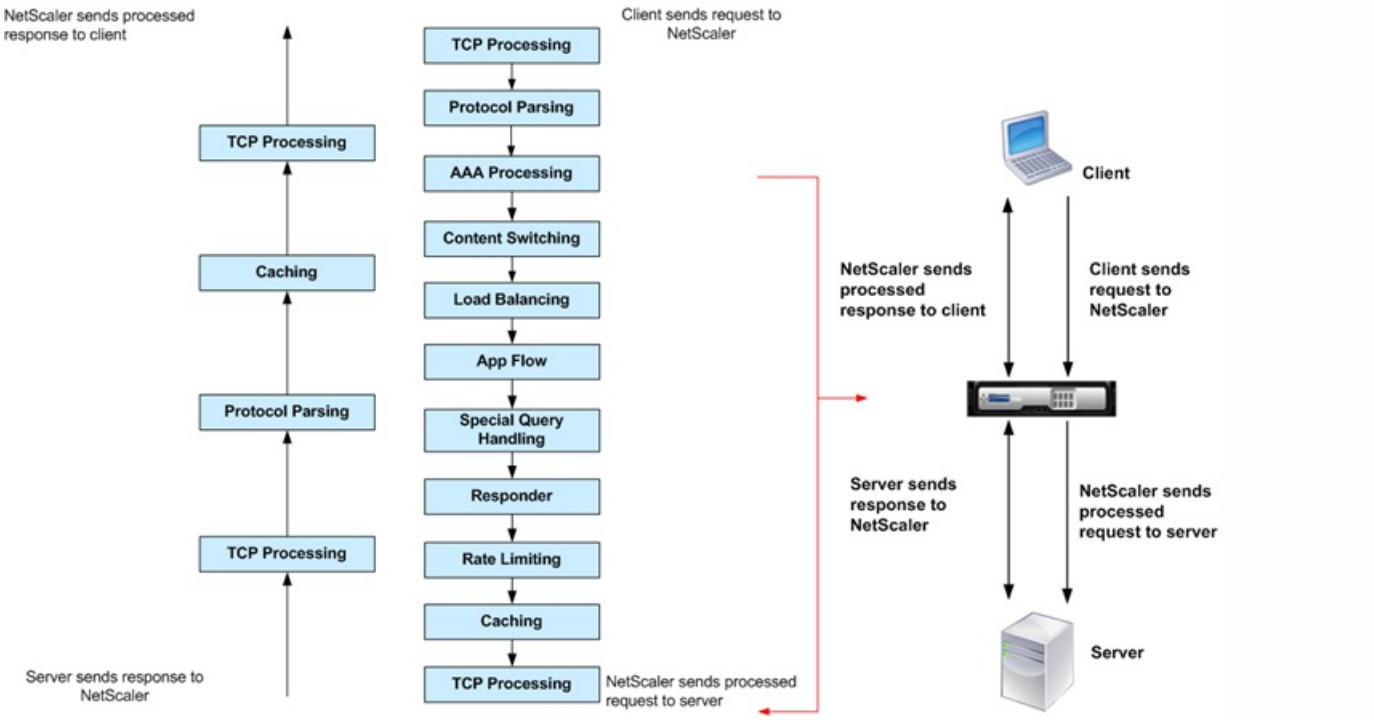
다음 그림에서는 NetScaler의 L7 패킷 흐름을 보여 줍니다.

그림 1. L7 패킷 흐름 다이어그램



다음 그림에서는 NetScaler의 DataStream 패킷 흐름을 보여 줍니다. DataStream은 MySQL 및 MS SQL 데이터베이스에 대해 지원됩니다. DataStream 기능에 대한 자세한 내용은 "DataStream"을 참조하십시오.

그림 2. DataStream 패킷 흐름 다이어그램



NetScaler 장비는 어떤 네트워크에 적합한가?

Aug 30, 2016

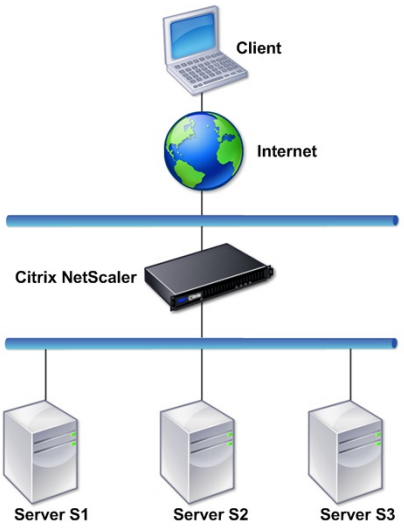
NetScaler 장비는 클라이언트와 서버 사이에 배치되므로 클라이언트 요청과 서버 응답이 NetScaler를 통해 이루어집니다. 일반적인 설치에서 장비에 구성된 가상 서버는 클라이언트가 장비 뒤에 있는 응용 프로그램에 액세스하는 데 사용하는 연결 지점을 제공합니다. 이 경우 장비는 해당 가상 서버와 연관된 공용 IP 주소를 소유하고, 실제 서버는 사설망에서 격리됩니다. 또한 장비를 투명 모드에서 L2 브리지 또는 L3 라우터로 작동하거나 이러한 모드 및 기타 모드의 측면을 조합할 수도 있습니다.

물리적 배포 모드

업데이트 날짜: 2013년 09월 04일

논리적으로 클라이언트와 서버 사이에 있는 NetScaler 장비는 두 가지 물리적 모드인 인라인 모드 및 단일 암 모드 중 하나로 배포할 수 있습니다. 인라인 모드에서는 여러 네트워크 인터페이스가 서로 다른 이더넷 세그먼트에 연결되고 장비는 클라이언트와 서버 사이에 배치됩니다. 장비는 각 클라이언트 네트워크 및 각 서버 네트워크에 대해 별도의 네트워크 인터페이스를 가집니다. 이 구성에서 장비 및 서버는 서로 다른 서브넷에 존재할 수 있습니다. L4-L7 기능을 투명하게 적용하는 장비를 사용하면 서버를 공용 네트워크에 두고 클라이언트가 장비를 통해 서버에 직접 액세스하도록 할 수 있습니다. 일반적으로 가상 서버(나중에 설명)는 실제 서버를 대표하도록 구성됩니다. 다음 그림에서는 일반적인 인라인 배포를 보여 줍니다.

그림 1. 인라인 배포



단일 암 모드에서는 장비의 한 네트워크 인터페이스만 이더넷 세그먼트에 연결됩니다. 이 경우 장비는 네트워크의 클라이언트 쪽 및 서버 쪽을 격리하지 않고, 구성된 가상 서버를 통해 응용 프로그램에 대한 액세스를 제공합니다. 단일 암 모드는 일부 환경에서 NetScaler 설치에 필요한 네트워크 변경 작업을 단순화할 수 있습니다.

인라인(이중 암) 및 단일 암 배포의 예를 보려면 "일반적인 네트워크 토폴로지 이해"를 참조하십시오.

L2 장치로서 Citrix NetScaler

업데이트 날짜: 2013년 09월 04일

L2 장치로 작동하는 NetScaler를 L2 Mode로 작동한다고 말합니다. L2 Mode에서는 다음의 모든 조건이 충족될 경우 NetScaler가 네트워크 인터페이스 간에 패킷을 전달합니다.

- 패킷의 목적지가 다른 장치의 MAC(media access control)주소 입니다.
- 대상 MAC 주소가 다른 네트워크 인터페이스에 있습니다.
- 네트워크 인터페이스가 동일한 가상 LAN(VLAN)의 멤버입니다.

기본적으로 모든 네트워크 인터페이스는 사전 정의된 VLAN, VLAN 1의 멤버입니다. ARP(Address Resolution Protocol) 요청 및 응답은 동일한 VLAN의 멤버인 모든 네트워크 인터페이스에 전달됩니다. 브리징 루프를 피하려면 다른 L2 장치가 NetScaler와 병렬로 작동하는 경우 L2 Mode를 사용하지 말아야 합니다.

L2 모드와 L3 모드가 상호 작용하는 방식에 대한 자세한 내용은 "패킷 전달 모드 구성"을 참조하십시오.

L2 모드 구성에 대한 자세한 내용은 "L2 모드 활성화 및 비활성화"를 참조하십시오.

패킷 전달 장치로서 Citrix NetScaler

업데이트 날짜: 2014년 03월 14일

NetScaler 장비는 패킷 전달 장치로 작동할 수 있으며, 이 작동 모드를 L3 모드라고 합니다. L3 모드를 사용하면 장비에서 장비에 속하지 않은 IP 주소로 향하는 모든 수신된 유니캐스트 패킷을 해당 대상의 경로가 있는 경우 전달합니다. 또한 장비는 VLAN 간에 패킷을 라우팅할 수도 있습니다.

L2 및 L3의 두 가지 작동 모드에서 장비는 일반적으로 다음에 해당하는 패킷을 삭제합니다.

- 멀티캐스트 프레임
- 장비의 MAC 주소를 대상으로 하는 알 수 없는 프로토콜 프레임(비-IP 및 비-ARP)
- 스패닝 트리 프로토콜(BridgeBPDU가 ON이 아닌 경우)

L2 모드와 L3 모드가 상호 작용하는 방식에 대한 자세한 내용은 "패킷 전달 모드 구성"을 참조하십시오.

L3 모드 구성에 대한 자세한 내용은 "L3 모드 활성화 및 비활성화"를 참조하십시오.

NetScaler가 클라이언트 및 서버와 통신하는 방식

Aug 30, 2016

NetScaler 장비는 대개 서버 팜의 앞에 배포되고, 클라이언트 쪽 구성 없이 클라이언트와 서버 사이에서 투명한 TCP 프록시로 동작합니다. 이 기본적인 작동 모드를 요청 교환 기술이라고 하며 NetScaler 기능의 핵심입니다. 요청 교환을 통해 장비는 TCP 연결 멀티플렉스 및 오프로드, 지속 연결 관리, 요청(응용 프로그램 계층) 레벨에서 트래픽 관리 등의 작업을 수행할 수 있습니다. 이 기능은 장비가 요청이 전달되는 TCP 연결에서 HTTP 요청을 구분할 수 있기 때문에 가능합니다.

구성에 따라 장비는 서버에 요청을 전달하기 전에 트래픽을 처리할 수 있습니다. 예를 들어, 클라이언트가 서버의 보안 응용 프로그램에 액세스를 시도할 경우 장비는 서버에 트래픽을 보내기 전에 필요한 SSL 처리를 수행할 수 있습니다.

서버 리소스에 대한 효율적이고 안전한 액세스를 위해 장비는 NetScaler 소유 IP 주소라고 하는 IP 주소 집합을 사용합니다. 네트워크 트래픽을 관리하려면 NetScaler 소유 IP 주소를 사용자 구성의 빌딩 블록이 되는 가상 엔터티에 할당합니다. 예를 들어 부하 분산을 구성하려면 가상 서버를 만들어 클라이언트 요청을 받고 이를 해당 서버의 응용 프로그램을 나타내는 엔터티인 서비스로 배포합니다.

NetScaler 소유 IP 주소 이해

업데이트 날짜: 2014년 03월 12일

프록시로 동작하기 위해 NetScaler 장비는 다양한 IP 주소를 사용합니다. 주요한 NetScaler 소유 IP 주소는 다음과 같습니다.

NSIP(NetScaler IP) 주소

NSIP 주소는 장비 관리, 장비 자체에 대한 일반적인 시스템 액세스 및 고가용성 구성에서 장비 간 통신에 사용되는 IP 주소입니다.

VIP(가상 서버 IP) 주소

VIP 주소는 가상 서버와 연관된 IP 주소입니다. 이 주소는 클라이언트가 연결하는 공용 IP 주소입니다. 폭넓은 범위의 트래픽을 관리하는 장비에는 구성된 많은 VIP가 있을 수 있습니다.

SNIP(서브넷 IP) 주소

SNIP 주소는 연결 관리 및 서버 모니터링에 사용됩니다. 각 서브넷에 SNIP 주소를 여러 개 지정할 수 있습니다. SNIP 주소는 VLAN에 바인딩될 수 있습니다.

IP 집합

IP 집합은 IP 주소의 모음이며 장비에 SNIP로 구성됩니다. IP 집합은 해당 집합에 포함된 IP 주소의 사용법을 확인하는 데 도움이 되는 의미 있는 이름으로 식별됩니다.

넷 프로필

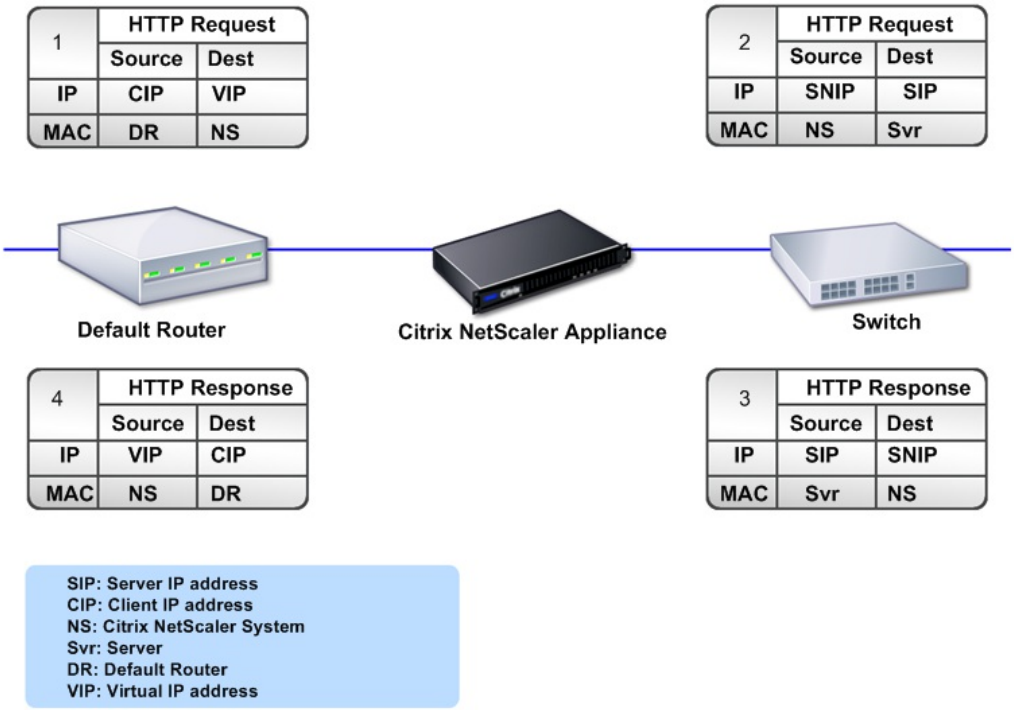
넷 프로필 또는 네트워크 프로필에는 IP 주소나 IP 집합이 포함됩니다. 넷 프로필은 부하 분산 또는 콘텐츠 스위칭 가상 서버, 서비스, 서비스 그룹 또는 모니터에 바인드될 수 있습니다. 물리적 서버 또는 피어와의 통신 중에 장비는 프로필에 지정된 주소를 원본 IP 주소로 사용합니다.

트래픽 흐름 관리 방식

업데이트 날짜: 2014년 03월 12일

NetScaler 장비는 TCP 프록시로 동작하므로 서버에 패킷을 보내기 전에 IP 주소를 변환합니다. 가상 서버를 구성할 경우 클라이언트는 서버에 직접 연결하는 대신 NetScaler의 VIP 주소에 연결합니다. 가상 서버의 설정에 따라 장비는 적당한 서버를 선택하고 클라이언트의 요청을 해당 서버로 보냅니다. 다음 그림에 표시된 것과 같이 장비는 기본적으로 SNIP 주소를 사용하여 서버와의 연결을 설정합니다.

그림 1. 가상 서버 기반 연결



가상 서버가 없을 경우 장비가 요청을 수신하면 투명하게 서버에 요청을 전달합니다. 이 작동을 투명 모드라고 합니다. 투명 모드에서 작동할 때 장비는 수신 클라이언트 요청의 원본 IP 주소를 SNIP 주소로 변환하지만 목적지 IP 주소는 변경하지 않습니다. 이 모드가 작동하려면 L2 또는 L3 모드가 적절히 구성되어야 합니다.

서버에 실제 클라이언트 IP 주소가 필요한 경우에는 클라이언트 IP 주소를 추가 필드로 삽입하여 HTTP 헤더를 수정하도록 구성하거나 서버 연결을 위해 SNIP 주소 대신 클라이언트 IP 주소를 사용하도록 장비를 구성할 수 있습니다.

트래픽 관리 빌딩 블록

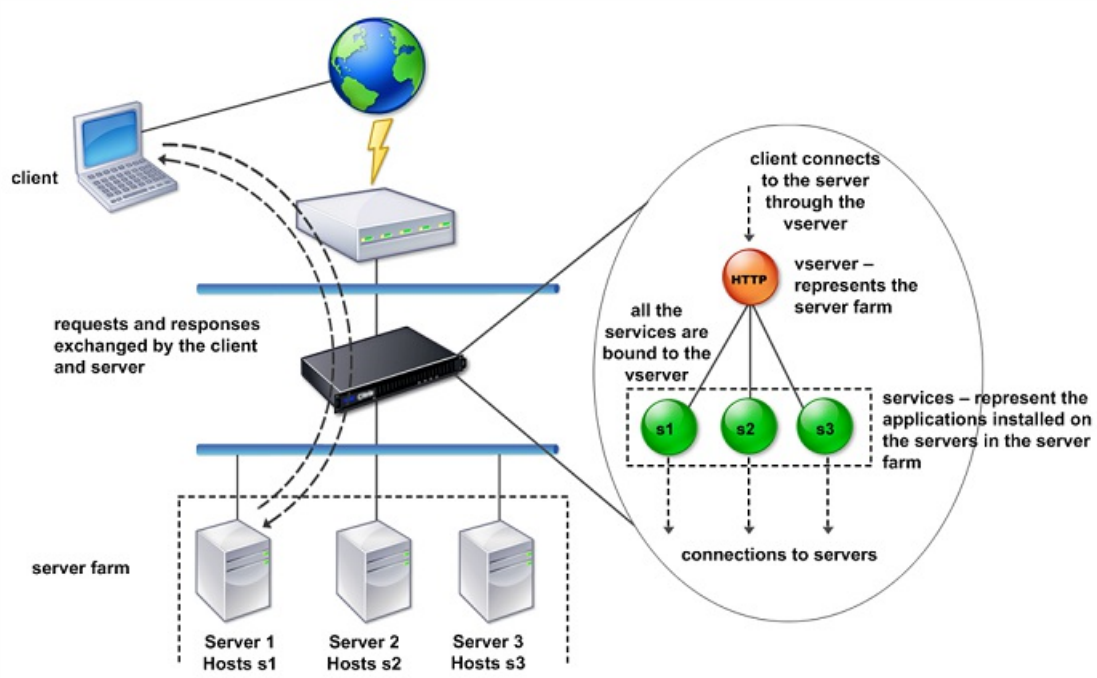
업데이트 날짜: 2013년 06월 24일

NetScaler 장비의 구성은 일반적으로 트래픽 관리를 위한 빌딩 블록으로 사용되는 일련의 가상 엔터티로 이루어집니다. 빌딩 블록 방식은 트래픽 흐름을 구분하는 데 도움이 됩니다. 가상 엔터티는 대개 트래픽 처리를 위한 IP 주소, 포트 및 프로토콜 처리기를 나타내는 추상입니다. 클라이언트는 이러한 가상 엔터티를 통해 응용 프로그램 및 리소스에 액세스합니다. 가장 일반적으로 사용되는 엔터티는 가상 서버 및 서비스입니다. 가상 서버는 서버 팜 또는 원격 네트워크의 서버 그룹을 나타내고, 서비스는 각 서버의 특정 응용 프로그램을 나타냅니다.

대부분의 기능 및 트래픽 설정은 가상 엔터티를 통해 활성화됩니다. 예를 들어, 특정 가상 서버를 통해 서버 팜에 연결된 클라이언트에 모든 서버 응답을 압축하도록 장비를 구성할 수 있습니다. 특정 환경에 대해 장비를 구성하려면 해당하는 기능을 식별한

다음 이러한 기능을 제공하기 위한 가상 엔터티의 올바른 조합을 선택해야 합니다. 대부분의 기능은 서로 연결된 일련의 가상 엔터티를 통해 제공됩니다. 이 경우 가상 엔터티는 제공되는 응용 프로그램의 최종 구조로 만들어지는 블록과 같습니다. 가상 엔터티를 추가, 제거, 수정, 바인딩, 활성화 및 비활성화하여 기능을 구성할 수 있습니다. 다음 그림에서는 이 섹션에서 설명한 개념을 보여 줍니다.

그림 2. 트래픽 관리 빌딩 블록 작동 방식



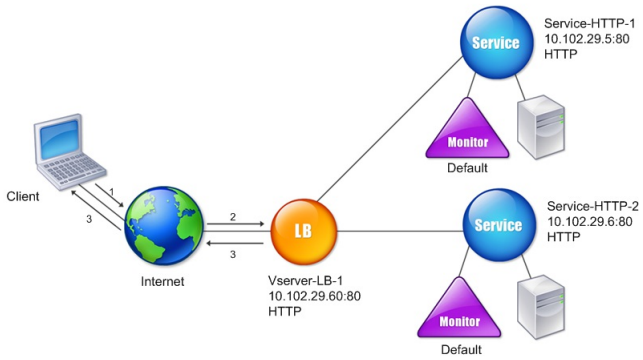
단순한 부하 분산 구성

업데이트 날짜: 2013년 08월 30일

다음 그림에 표시된 예에서 NetScaler 장비는 부하 분산 장치로 작동하도록 구성되었습니다. 이 구성의 경우 부하 분산에 맞게 가상 엔터티를 구성하고 특정 순서로 바인딩해야 합니다. 부하 분산 장치로서 장비는 클라이언트 요청을 여러 서버에 걸쳐 분산시키므로 리소스 활용률을 최적화합니다.

일반적인 부하 분산 구성의 기본적인 빌딩 블록은 서비스 및 부하 분산 가상 서버입니다. 서비스는 서버의 응용 프로그램을 나타냅니다. 가상 서버는 클라이언트가 연결하는 단일 IP 주소를 제공하여 서버를 추상화합니다. 클라이언트 요청이 서버에 보내지도록 하려면 각 서비스를 가상 서버에 바인딩해야 합니다. 즉, 모든 서버에 대해 서비스를 만든 다음 가상 서버에 바인딩해야 합니다. 클라이언트는 VIP 주소를 사용하여 NetScaler 장비에 연결합니다. 장비가 VIP 주소로 보낸 클라이언트 요청을 수신하면 부하 분산 알고리즘에 따라 결정된 서버로 요청을 보냅니다. 부하 분산에서는 모니터라는 가상 엔터티를 사용하여 구성된 특정 서비스(서버와 응용 프로그램)에서 요청 수신 가능 여부를 추적합니다.

그림 3. 가상 서버, 서비스 및 모니터 부하 분산



부하 분산 알고리즘 구성과 함께 부하 분산 구성의 동작 및 성능에 영향을 미치는 여러 가지 매개 변수를 구성할 수 있습니다. 예를 들어, 원본 IP 주소를 기준으로 지속성을 유지하도록 가상 서버를 구성할 수 있습니다. 그러면 장비가 특정 IP 주소에서 전송되는 모든 요청을 동일한 서버로 지정합니다.

가상 서버 이해

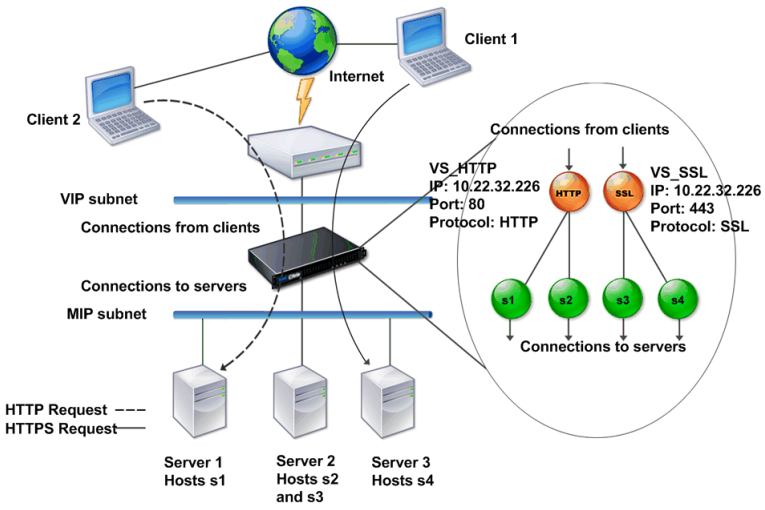
업데이트 날짜: 2013년 09월 06일

가상 서버는 외부 클라이언트가 서버에 호스트된 응용 프로그램에 액세스하는 데 사용할 수 있는 명명된 NetScaler 엔터티입니다. 가상 서버는 영숫자 이름, VIP(가상 IP) 주소, 포트 및 프로토콜로 나타냅니다. 가상 서버의 이름은 로컬에서만 의미를 가지며 가상 서버를 쉽게 식별하기 위해 마련되었습니다. 클라이언트가 서버의 응용 프로그램에 액세스를 시도할 경우 물리적 서버의 IP 주소 대신 VIP에 요청을 보냅니다. 장비가 VIP 주소에서 요청을 수신하면 가상 서버에서의 연결을 종료하고 클라이언트를 대신하여 서버와의 자체 연결을 사용합니다. 가상 서버의 포트와 프로토콜은 가상 서버가 나타내는 응용 프로그램을 결정합니다. 예를 들어, 웹 서버는 포트와 프로토콜이 각각 80 및 HTTP로 설정된 가상 서버 및 서비스로 나타낼 수 있습니다. 여러 가상 서버는 동일한 VIP 주소를 사용할 수 있지만 프로토콜과 포트는 달라야 합니다.

가상 서버는 기능을 제공하기 위한 지점입니다. 압축, 캐싱 및 SSL 오프로드와 같은 대부분의 기능은 일반적으로 가상 서버에서 활성화됩니다. 장비가 VIP 주소에서 요청을 수신하면 요청이 수신된 포트 및 해당 프로토콜을 기준으로 적당한 가상 서버를 선택합니다. 그런 다음 장비는 가상 서버에서 구성된 기능에 따라 적절히 요청을 처리합니다.

대부분의 경우 가상 서버는 서비스와 나란히 작동합니다. 여러 서비스를 하나의 가상 서버에 바인딩할 수 있습니다. 이러한 서비스는 서버 팜의 물리적 서버에서 실행되는 응용 프로그램을 나타냅니다. 장비는 VIP 주소에서 수신된 요청을 처리한 후 가상 서버에서 구성된 부하 분산 알고리즘에 따라 결정된 서버에 요청을 전달합니다. 다음 그림은 이러한 개념을 보여 줍니다.

그림 4. 단일 VIP 주소의 여러 가상 서버



위의 그림은 VIP 주소가 같지만 포트와 프로토콜이 다른 두 가상 서버로 이루어진 구성을 보여 줍니다. 각 가상 서버에는 연결된 두 가지 서비스가 있습니다. 서비스 s1 및 s2는 VS_HTTP에 연결되고 서버 1 및 서버 2의 HTTP 응용 프로그램을 나타냅니다. 서비스 s3 및 s4는 VS_SSL에 연결되고 서버 2 및 서버 3의 SSL 응용 프로그램을 나타냅니다(서버 2는 HTTP 및 SSL 응용 프로그램을 둘 다 제공합니다). 장비가 VIP 주소에서 HTTP 요청을 수신하면 VS_HTTP의 설정에 지정된 대로 요청을 처리하고 서버 1 또는 서버 2에 요청을 보냅니다. 마찬가지로 장비가 VIP 주소에서 HTTPS 요청을 수신하면 VS_SSL의 설정에 지정된 대로 요청을 처리하고 서버 2 또는 서버 3에 요청을 보냅니다.

가상 서버를 항상 특정 IP 주소, 포트 번호 또는 프로토콜로 나타내는 것은 아닙니다. 가상 서버를 와일드카드로 나타낼 수도 있으며, 이 경우 와일드카드 가상 서버라고 합니다. 예를 들어, 특정 포트 번호를 사용하지만 VIP 대신 와일드카드로 가상 서버를 구성할 경우 장비는 해당 프로토콜과 일치하고 미리 정의된 포트를 대상으로 하는 모든 트래픽을 가로채어 처리합니다. VIP 및 포트 번호 대신 와일드카드를 사용하는 가상 서버의 경우 장비는 해당 프로토콜과 일치하는 모든 트래픽을 가로채어 처리합니다.

가상 서버는 다음 범주로 그룹화할 수 있습니다.

부하 분산 가상 서버

요청을 수신하고 적당한 서버로 리디렉션합니다. 적당한 서버를 선택할 때는 사용자가 구성하는 다양한 부하 분산 방법을 기준으로 합니다.

캐시 리디렉션 가상 서버

동적 콘텐츠에 대한 클라이언트 요청을 원본 서버로 리디렉션하고, 정적 콘텐츠에 대한 요청을 캐시 서버로 리디렉션합니다. 캐시 리디렉션 가상 서버는 부하 분산 가상 서버와 함께 작동하기도 합니다.

콘텐츠 스위칭 가상 서버

클라이언트가 요청한 콘텐츠를 기준으로 트래픽을 서버에 지정합니다. 예를 들어, 이미지에 대한 모든 클라이언트 요청을 이미지만 제공하는 서버로 지정하는 콘텐츠 스위칭 가상 서버를 생성할 수 있습니다. 콘텐츠 스위칭 가상 서버는 부하 분산 가상 서버와 함께 작동하기도 합니다.

VPN(가상 사설망) 가상 서버

터널링된 트래픽을 해독하고 인트라넷 응용 프로그램으로 보냅니다.

SSL 가상 서버

SSL 트래픽을 수신하고 암호 해독한 후 적당한 서버로 리디렉션합니다. 적당한 서버 선택 방법은 부하 분산 가상 서버를 선택하는 방법과 유사합니다.

서비스 이해

업데이트 날짜: 2014년 03월 12일

서비스는 서버의 응용 프로그램을 나타냅니다. 서비스는 대개 가상 서버와 함께 사용되지만, 가상 서버가 없을 경우 서비스가 응용 프로그램 특정 트래픽을 관리할 수 있습니다. 예를 들어, NetScaler 장비에서 웹 서버 응용 프로그램을 나타내는 HTTP 서비스를 생성할 수 있습니다. 클라이언트가 웹 서버에 호스트된 웹 사이트에 액세스를 시도할 경우 장비는 HTTP 요청을 가로채고 웹 서버와의 투명한 연결을 생성합니다.

서비스 전용 모드에서 장비는 프록시로 작동합니다. NetScaler는 클라이언트 연결을 종료하고 SNIP 주소를 사용하여 서버 연결을 설정하고 수신 클라이언트 요청의 목적지 IP 주소를 SNIP 주소로 변환합니다. 클라이언트는 서버의 IP 주소로 직접 요청을 보내지만 서버는 이러한 요청을 SNIP 주소에서 오는 것으로 인식합니다. 장비가 IP 주소, 포트 번호 및 시퀀스 번호를 변환합니다.

서비스도 기능을 적용하기 위한 지점입니다. SSL 가속화의 예를 생각해 보겠습니다. 이 기능을 사용하려면 SSL 서비스를 생성하고 SSL 인증서를 서비스에 바인딩해야 합니다. 장비가 HTTPS 요청을 수신하면 트래픽을 해독하고 일반 텍스트로 서버에 보냅니다. 하지만 서비스 전용 모드에서는 제한된 기능 집합만 구성할 수 있습니다.

서비스는 모니터라는 엔터티를 사용하여 응용 프로그램의 상태를 추적합니다. 모든 서비스에는 서비스 유형을 기준으로 하는 연결된 기본 모니터가 있습니다. 모니터에서 구성된 설정에 따라 장비는 정기적으로 응용 프로그램에 점검을 보내 상태를 확인합니다. 점검이 실패하면 장비는 서비스가 중지된 것으로 표시합니다. 이 경우 장비는 클라이언트 요청에 해당하는 오류 메시지로 응답하거나 부하 분산 정책에 따라 요청을 다시 라우팅합니다.

Citrix NetScaler 제품 라인 소개

Sep 13, 2016

Citrix NetScaler 제품 라인은 애플리케이션 수준 보안, 최적화 및 트래픽 관리를 단일 통합 장비로 결합함으로써 인터넷 및 사설망을 통한 애플리케이션 제공을 최적화합니다. NetScaler 장비를 서버실에 설치하고 관리대상 서버에 대한 모든 연결을 NetScaler를 통해 라우팅할 수 있습니다. 그렇게 하면 사용하도록 설정한 NetScaler 기능 및 정책이 들어오거나 나가는 트래픽에 적용됩니다.

NetScaler는 기존 부하 분산 장치, 서버, 캐시 및 방화벽에 대한 보완 장치로 모든 네트워크에 통합할 수 있습니다. 추가적인 클라이언트측 또는 서버측 소프트웨어가 필요하지 않으며, NetScaler 웹 기반 GUI 및 CLI를 사용하여 구성할 수 있습니다.

NetScaler 장비는 다중 코어 프로세서와 같은 사양을 가진 다양한 하드웨어 플랫폼에서 사용할 수 있습니다.

NetScaler 운영 체제는 모든 NetScaler 하드웨어 플랫폼을 위한 기반 운영 체제입니다. NetScaler 운영 체제는 Standard, Enterprise, Platinum 등의 세 가지 에디션에서 사용할 수 있습니다.

Citrix NetScaler 하드웨어 플랫폼

NetScaler 하드웨어는 다중 코어 프로세서와 같은 하드웨어 사양을 가진 다양한 플랫폼에서 사용할 수 있습니다. 모든 하드웨어 플랫폼은 고속 이더넷, 기가비트 이더넷 및 10기가비트 이더넷 인터페이스의 조합을 지원합니다.

NetScaler에는 다음 플랫폼을 사용할 수 있습니다.

- Citrix NetScaler MPX 5500
- Citrix NetScaler MPX 5550/5650
- Citrix NetScaler MPX 7500/9500
- Citrix NetScaler MPX 8200/8400/8600
- Citrix NetScaler MPX 9700/10500/12500/15500
- Citrix NetScaler MPX 11500/13500/14500/16500/18500/20500
- Citrix NetScaler MPX 11515/11520/11530/11540/11542
- Citrix NetScaler MPX 17500/19500/21500
- Citrix NetScaler MPX 17550/19550/20550/21550
- Citrix NetScaler MPX 22040/22060/22080/22100/22120
- Citrix NetScaler MPX 24100/24150
- Citrix NetScaler MPX 25100T/25160T
- T1010
- T1100(Gen1)
- T1100(16)
- T1120
- T1200
- T1300
- T1300-40G

하드웨어 플랫폼 사양에 대한 자세한 내용은 Hardware Platforms(하드웨어 플랫폼)를 참조하십시오.

다음 표는 NetScaler의 여러 에디션 및 사용 가능한 하드웨어 플랫폼을 나열한 것입니다.

표 1. 제품 에디션 및 MPX 하드웨어 플랫폼

하드웨어	MPX 5500	MPX 5550/5650	MPX 7500/9500	MPX 8200/8400/8600	MPX 24100/24150	MPX 25100T/25160T
Platinum Edition	예	예	예	예	예	예

Enterprise Edition	예	예	예	예	예	예
Standard Edition	예	예	예	예	예	예

표 2. 제품 에디션 및 MPX 하드웨어 플랫폼(계속됨)

하드웨어	MPX 9700/10500/12500/15500	MPX 17500/19500/21500	MPX 17550/19550/20550/21550
Platinum Edition	예	예	예
Enterprise Edition	예	예	예
Standard Edition	예	예	예

표 3. 제품 에디션 및 MPX 하드웨어 플랫폼(계속됨)

하드웨어	MPX 22040/22060/22080/22100/22120	MPX 11500/13500/14500/16500/18500/20500	MPX 11515/11520/11530/11540/11542
Platinum Edition	예	예	예
Enterprise Edition	예	예	예
Standard Edition	예	예	예

표 4. 제품 에디션 및 T1 하드웨어 플랫폼

하드웨어	T1010	T1100	T1120	T1200	T1300
Basic Edition	예	예	예	예	예
Advanced Edition	예	예	예	예	예

Citrix NetScaler 에디션

업데이트 날짜: 2013년 09월 04일

NetScaler 운영 체제는 Standard, Enterprise 및 Platinum Edition으로 제공됩니다. Enterprise 및 Standard Edition은 사용할 수 있는 기능이 한정되어 있습니다. 모든 에디션에는 기능 라이센스가 필요합니다.

라이센스를 다운로드하고 설치하는 방법에 대한 지침은 "http://support.citrix.com/article/ctx121062"를 참조하십시오.

Citrix NetScaler 에디션에 대한 설명은 다음과 같습니다.

- *— Citrix NetScaler, Standard Edition*
  . 중소 규모 기업에 종합적인 L4-L7 트래픽 관리를 제공하여 웹 응용 프로그램 가용성을 높일 수 있습니다.
- *— Citrix NetScaler, Enterprise Edition*
  . 웹 응용 프로그램 가속 및 고급 L4-L7 트래픽 관리를 제공하여 기업에서 웹 응용 프로그램 성능 및 가용성을 높이고 데이터 센터 비용을 줄일 수 있습니다.
- *— Citrix NetScaler, Platinum Edition*
  . 데이터 센터 비용을 줄이고, 전체적인 응용 프로그램 성능 파악으로 응용 프로그램 성능을 높이며, 고급 응용 프로그램 보안을 지원하는 웹 응용 프로그램 제공 솔루션을 제공합니다.

다음 표에는 Citrix NetScaler 제품 라인에서 지원되는 기능이 각 에디션별로 요약되어 있습니다.

표 4. Citrix NetScaler 응용 프로그램 제공 제품 라인 기능

주요 기능	Platinum Edition	Enterprise Edition	Standard Edition
응용 프로그램 가용성			
L4 부하 분산	예	예	예
L7 콘텐츠 스위칭	예	예	예
AppExpert 속도 제어	예	예	예
IPv6 지원	예	예	예
GSLB(Global Server Load Balancing)	예	예	선택 사항
동적 라우팅 프로토콜	예	예	아니요
서지 보호	예	예	아니요
우선 순위 대기열	예	예	아니요
응용 프로그램 가속			
클라이언트 및 서버 TCP 최적화	예	예	예
Citrix AppCompress for HTTP	예	예	선택 사항
Citrix AppCache	예	선택 사항	아니요
Citrix Branch Repeater client	예	아니요	아니요
응용 프로그램 보안			

주요 기능	Platinum Edition	Enterprise Edition	Standard Edition
L4 DoS 방어	예	예	예
L7 콘텐츠 필터링	예	예	예
HTTP/URL 다시 쓰기	예	예	예
NetScaler Gateway, EE SSL VPN	예	예	예
L7 DoS 방어	예	예	아니요
AAA 보안	예	예	아니요
XML 보안을 사용한 응용 프로그램 방화벽	예	선택 사항	아니요
단순한 관리 기능			
AppExpert Visual Policy Builder	예	예	예
AppExpert 서비스 콜아웃	예	예	예
AppExpert 템플릿	예	예	예
역할 기반 관리	예	예	예
구성 마법사	예	예	예
Citrix Command Center	예	예	아니요
Citrix EdgeSight for NetScaler	예	선택 사항	아니요
Web 2.0 최적화			
다양한 인터넷 응용 프로그램 지원	예	예	예
고급 서버 오프로드	예	예	아니요
낮은 TCO(총 소유 비용)			
TCP 버퍼링	예	예	예
TCP 멀티플렉싱	예	예	예
SSL 오프로드 및 가속화	예	예	예

주요 기능	Platinum Edition	Enterprise Edition	Standard Edition
캐시 리디렉션	예	예	아니요
Citrix EasyCall	예	아니요	아니요

표 5. Citrix NetScaler T1 제품 라인 기능

주요 기능	Advanced Edition	Basic Edition
응용 프로그램 가용성		
L4 부하 분산	예	예
L7 콘텐츠 스위칭	예	예
AppExpert 속도 제어	예	예
IPv6 지원	예	예
GSLB(Global Server Load Balancing)	예	선택 사항
동적 라우팅 프로토콜	예	예
서지 보호	예	아니요
우선 순위 대기열	예	아니요
응용 프로그램 가속		
클라이언트 및 서버 TCP 최적화	예	예
Citrix AppCompress for HTTP	예	선택 사항
Citrix AppCache	예	아니요
Citrix Branch Repeater client	아니요	아니요
응용 프로그램 보안		
L4 DoS 방어	예	예
L7 콘텐츠 필터링	예	예
HTTP/URL 다시 쓰기	예	예

NetScaler Gateway, EE SSL VPN	아니요	아니요
L7 DoS 방어	예	아니요
AAA 보안	예	아니요
XML 보안을 사용한 응용 프로그램 방화벽	선택 사항	아니요
단순한 관리 기능		
AppExpert Visual Policy Builder	예	예
AppExpert 서비스 콜아웃	예	예
AppExpert 템플릿	예	예
역할 기반 관리	예	예
구성 마법사	예	예
Citrix Command Center	예	아니요
Citrix EdgeSight for NetScaler	선택 사항	아니요
Web 2.0 최적화		
다양한 인터넷 응용 프로그램 지원	예	예
고급 서버 오프로드	예	아니요
낮은 TCO(총 소유 비용)		
TCP 버퍼링	예	예
TCP 멀티플렉싱	예	예
SSL 오프로드 및 가속화	예	예
캐시 리디렉션	예	아니요
Citrix EasyCall	아니요	아니요

참고: 이 정보를 작성할 때 최대한 정확한 정보가 되도록 노력했지만 이 내용은 변경될 수 있습니다. 최신 정보는 Citrix 지원 (http://www.citrix.com)을 참조하십시오.

NetScaler 하드웨어에서 지원되는 릴리스

업데이트 날짜: 2014년 06월 30일

다음 표에는 NetScaler MPX 플랫폼에서 지원되는 릴리스의 초기 NetScaler 빌드가 나와 있습니다.

표 6. NetScaler MPX 모델에서 지원되는 릴리스

하드웨어	소프트웨어 릴리스	소프트웨어 빌드 번호
MPX 5500	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체
MPX 5550/5650	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	71.6.nc 이상
	9.3	59.5.nc 이상
MPX 7500/9500	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체
MPX 8005/8015	11.1	전체

	11.0	전체
	10.5	전체
	10.1	122.17.nc 이상
	9.3	65.8.nc 이상
MPX 8200/8400/8600	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	70.7.nc 이상
	9.3	58.5.nc 이상
MPX 9700/10500/12500	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체
MPX 9700/10500/12500 10G	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체

MPX 15500	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체
MPX 15500 10G	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체
MPX 11500/13500/14500/16500/18500/20500	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	52.3.nc 이상
MPX 11515/11520/11530/11540/11542	11.1	전체
	11.0	전체
	10.5	전체
	10.1	123.11.nc 이상

	9.3	65.8.nc 이상
MPX 15000	11.1	지원되지 않음
	11.0	지원되지 않음
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체
MPX 17000	11.1	지원되지 않음
	11.0	지원되지 않음
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체
MPX 17500/19500/21500	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체
MPX 17550/19550/20550/21550	11.1	전체
	11.0	전체
	10.5	전체
	10.1	전체

	10.0	전체
	9.3	53.5.nc 이상
MPX 22040/22060/22080/22100/22120	11.0	전체
	10.5	51.10.nc 이상
	10.1	123.11.nc 이상
	9.3	65.8.nc 이상
MPX 24100/24150	11.1	전체
	11.0	전체
	10.5	51.10.nc 이상
	10.1	129.11.nc 이상
MPX 25100T/25160T	11.0	전체
	10.5	57.7.nc 이상
	10.1	132.8.nc 이상

표 7. NetScaler T1 모델에서 지원되는 릴리스

하드웨어	소프트웨어 릴리스	소프트웨어 빌드 번호
T1010	11.0	전체
	10.5	전체
	10.1	전체
	10.0	전체
	9.3	전체
T1100	11.0	전체
	10.5	전체

	10.1	전체
	10.0	전체
	9.3	전체
T1120	11.0	전체
	10.5	57.7.nc 이상
T1200	11.0	전체
	10.5	51.10.nc 이상
	10.1	123.11.nc 이상
	9.3	65.8.nc 이상
T1300	11.0	전체
	10.5	57.7.nc 이상
	10.1	132.8.nc 이상

지원되는 브라우저

업데이트 날짜: 2014년 06월 24일

구성 유틸리티 및 대시보드에 액세스하려면 워크스테이션에 지원되는 웹 브라우저와 버전 1.6 이상의 Java 애플릿 플러그인이 설치되어 있어야 합니다.

운영 체제	브라우저	버전
Windows 7	Internet Explorer	8, 9 및 10
	Mozilla Firefox	3.6.25 이상
	Google Chrome	15 이상
Windows 64비트	Internet Explorer	8 및 9
	Google Chrome	15 이상
MAC	Mozilla Firefox	12 이상

운영 체제	브라우저	버전
	Safari	5.1.3
	Google Chrome	15 이상

NetScaler 하드웨어 설치

Aug 30, 2016

NetScaler 장비를 설치하기 전에 먼저 사전 설치 체크리스트를 검토합니다. NetScaler는 일반적으로 랙에 마운트되며 모든 모델은 랙 레일 하드웨어와 함께 제공됩니다. 7000을 제외한 모든 모델은 Small Form Factor Pluggable SFP, XFP 또는 SFP+ 송수신 장치를 지원합니다. 장비를 장착하고 송수신 장치를 설치한 후 NetScaler를 네트워크에 연결합니다. 콘솔 케이블을 사용하여 NetScaler를 개인용 컴퓨터에 연결하면 초기 구성을 수행할 수 있습니다. 그 밖의 모든 연결을 완료한 후 NetScaler를 전원에 연결합니다.

이 문서에는 다음이 포함되어 있습니다.

- 안전, 주의, 경고 및 기타 정보
- 장비 포장 풀기
- 장비 랙 탑재
- 1G SFP 송수신 장치 설치 및 제거
- XFP 및 10G SFP+ 송수신 장치 설치 및 제거
- 케이블 연결

안전, 주의, 경고 및 기타 정보

Aug 30, 2016

안전 수칙

아래 안전 수칙은 제품을 설치하기 전에 반드시 숙지해야 할 주의 및 위험 관련 정보를 제공합니다.

수칙 1

위험: 전원, 전화 및 통신 케이블의 전류는 위험합니다.

전기 충격 위험을 피하려면:

- 뇌우를 동반한 폭풍이 심할 경우 케이블 연결 또는 연결 해제 작업을 수행하거나 이 제품의 설치, 유지 관리, 재구성 등의 작업을 수행하지 마십시오.
- 모든 전원 코드는 배선과 접지가 올바로 수행된 전기 콘센트에 연결하십시오.
- 이 제품에 연결할 모든 장비는 올바로 배선된 콘센트에 연결하십시오.
- 가능한 경우 신호용 케이블을 연결 또는 연결 해제할 때 한 손만 사용하십시오.
- 화재, 홍수, 건물 손상 등의 징후가 있는 경우 장비의 전원을 절대 켜지 마십시오.
- 설치 및 구성 절차에서 달리 지시한 경우를 제외하고 장치 덮개를 열기 전에 연결된 전원 코드, 이동통신 시스템, 네트워크 및 모뎀의 연결을 해제하십시오.
- 이 제품 또는 연결된 장치의 덮개를 설치, 이동 또는 여는 경우 다음 표에 설명된 바와 같이 케이블을 연결 또는 연결 해제하십시오.

연결	연결 해제
1. 이 제품에 연결할 모든 전원 및 장비를 끕니다. 2. 모든 케이블을 장치에 연결합니다. 3. 신호용 케이블을 커넥터에 연결합니다. 4. 전원 코드를 전원에 연결합니다. DC 시스템의 경우 -48VDC 연결의 전극이 RTN은 (+)로, -48VDC는 (-)로 올바른지 확인합니다. 접지의 경우 안전을 위해 구멍이 2개인 러그(Lug)를 사용해야 합니다. 5. 모든 전원을 켭니다.	1. 이 제품에 연결할 모든 전원 및 장비를 끕니다. 2. AC 시스템의 경우 자가 발전형 전원 연결기에서 모든 전원 코드를 뽑거나 AC 전원공급장치에서 전원을 차단합니다. 3. DC 시스템의 경우 차단기 패널에서 DC 전원의 연결을 해제하거나 전원을 끈 후 DC 케이블을 뽑습니다. 4. 커넥터에서 신호용 케이블을 뽑습니다. 5. 장치에서 모든 케이블을 뽑습니다.

수칙 2

주의: CD-ROM, DVD 드라이브, 광섬유 장치, 송신기 등의 레이저 제품을 설치하는 경우 다음을 참고하십시오.

- 덮개를 제거하지 마십시오. 레이저 제품의 덮개를 제거하면 위험한 레이저 방사선에 노출될 수 있습니다. 장치 내에는 서비스 가능한 부품이 없습니다.
- 여기에 지정된 절차가 아닌 다른 방식으로 절차를 수행하거나 조정기 또는 컨트롤을 사용하면 위험한 방사선 노출을 유발할 수 있습니다.

위험: 일부 레이저 제품에는 내장형 Class 3A 또는 Class 3B 레이저 다이오드가 포함되어 있습니다. 다음 사항에 유의하십시오.

- 개봉 시 레이저 방사선에 주의하십시오. 빔을 쳐다보거나 광학 계기를 육안으로 직접 확인하지 말고 빔에 직접적으로 노출되는 것을 피하십시오.

수칙 3

주의:

다음 레이블이 부착된 부품 또는 전원공급장치의 덮개를 절대 제거하지 마십시오.

이 레이블이 부착된 구성 요소 내에는 위험한 수준의 전압, 전류 및 에너지가 흐릅니다. 이러한 구성 요소 내에는 서비스 가능한 부품이 없습니다. 이러한 부품 중 하나에 문제가 있는 것으로 의심되면 서비스 기술자에게 문의하십시오.

수칙 4

주의: 다음 레이블은 뜨거운 표면이 가까이 있다는 것을 나타냅니다.

수칙 5

위험: 분기 회로에 과부하가 걸리면 특정 상황에서 잠재적 화재 및 전기 충격의 위험이 있습니다. 이러한 위험을 피하려면 시스템 요구 사항이 분기 회로 보호 요구 사항을 초과하지 않는지 확인하십시오. 전기 사양은 장치와 함께 제공되는 정보를 참조하십시오.

수칙 6

주의: 이 장비는 DC 공급 회로의 접지된 도체를 장비의 접지 도체에 연결하는 것을 허용하도록 설계되었습니다. 이러한 방식으로 연결하는 경우 다음 모든 조건을 충족해야 합니다.

- 이 장비는 DC 공급 시스템의 접지극 도체에 직접 연결되거나, DC 공급 시스템의 접지극 도체에 연결되는 접지 단자 막대나 버스의 접착 점퍼에 직접 연결되어야 합니다.
- 이 장비는 동일한 DC 공급 회로의 접지된 도체와 접지 도체(및 DC 시스템의 접지 지점) 간을 연결하는 다른 장비와 동일한 인접 영역(예: 인접 캐비닛)에 위치해야 합니다. DC 시스템을 다른 위치에 접지해서는 안 됩니다.
- DC 공급원은 이 장비와 동일한 구역 내에 위치해야 합니다.
- DC 전원과 접지극 도체 연결 지점 간의 접지된 회로 도체에서 장치를 교환하거나 연결을 끊어서는 안 됩니다.

수칙 7

위험: 전원, 전화 및 통신 케이블의 전류는 위험합니다.

전기 충격 위험을 피하려면:

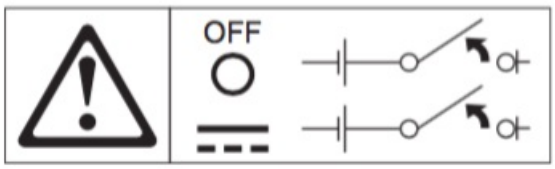
- 뇌우를 동반한 폭풍이 심할 경우 케이블 연결 또는 연결 해제 작업을 수행하거나 이 제품의 설치, 유지 관리, 재구성 등의 작업을 수행하지 마십시오.
- 모든 전원 코드는 배선과 접지가 올바로 수행된 전기 콘센트에 연결하십시오.
- 이 제품에 연결할 모든 장비는 올바로 배선된 콘센트에 연결하십시오.
- 가능한 경우 신호용 케이블을 연결 또는 연결 해제할 때 한 손만 사용하십시오.
- 화재, 홍수, 건물 손상 등의 징후가 있는 경우 장비의 전원을 절대 켜지 마십시오.
- 설치 및 구성 절차에서 달리 지시한 경우를 제외하고 장치 덮개를 열기 전에 연결된 전원 코드, 이동통신 시스템, 네트워크 및 모뎀의 연결을 해제하십시오.
- 이 제품 또는 연결된 장치의 덮개를 설치, 이동 또는 여는 경우 다음 표에 설명된 바와 같이 케이블을 연결 또는 연결 해제하십시오.

연결	연결 해제
1. 이 제품에 연결할 모든 전원 및 장비를 끕니다. 2. 모든 케이블을 장치에 연결합니다. 3. 신호용 케이블을 커넥터에 연결합니다. 4. 전원 코드를 전원에 연결합니다. DC 시스템의 경우 -48VDC 연결의 전극이 RTN은 (+)로, -48VDC는 (-)로 올바른지 확인합니다. 접지의 경우 안전을 위해 구멍이 2개인 러그(Lug)를 사용해야 합니다. 5. 모든 전원을 켭니다.	1. 이 제품에 연결할 모든 전원 및 장비를 끕니다. 2. AC 시스템의 경우 자가 발전형 전원 연결기에서 모든 전원 코드를 뽑거나 AC 전원공급장치에서 전원을 차단합니다. 3. DC 시스템의 경우 차단기 패널에서 DC 전원의 연결을 해제하거나 전원을 끈 후 DC 케이블을 뽑습니다. 4. 커넥터에서 신호용 케이블을 뽑습니다. 5. 장치에서 모든 케이블을 뽑습니다.

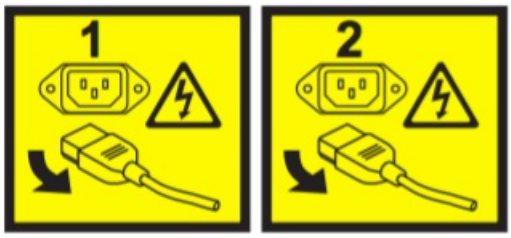
수칙 8

주의: 이 장치는 전원 제어 단추를 제공하지 않습니다. 전원공급장치를 제거하거나 유닛을 꺼도 장치에 공급되는 전류가 차단되지 않습니다. 또한 장치에는 둘 이상의 전원 코드가 있을 수 있습니다. 장치에서 모든 전류를 차단하려면 전원에서 모든 전원 코드를 뽑았는지 확인하십시오.

NetScaler MPX 17500 및 21550(이전의 T1100) DC 전원 옵션:



T1100 AC Power Option:



수칙 9

주의: 전기 충격 위험 또는 에너지 위험을 줄이려면:

- NEC 및 IEC 60950-1 First Edition인 The Standard for Safety of Information Technology Equipment(정보통신기기의 전기 안전에 관한 표준)에 명시된 대로 숙련된 서비스 담당자가 접근이 제한된 위치에서 이 장비를 설치해야 합니다.
- 장비를 올바로 접지된 SELV(안전 초저전압) 전원에 연결하십시오. SELV 전원은 일반/단일 장애 조건으로 인해 전압이 안전 수준(60V 직류)을 초과하는 것을 방지하기 위해 고안된 보조 회로입니다.
- 쉽게 사용할 수 있는 승인된 정격 전원 차단 장치를 현장 배선에 포함하십시오.
- 분리 회로의 과전류 차단을 위해 필요한 회로 차단기 등급은 제품 설명서에서 사양을 참조하십시오.
- 구리선 도체만 사용하십시오. 필요한 배선 규격은 제품 설명서에서 사양을 참조하십시오.
- 배선 단자 너트에 필요한 토크 값은 제품 설명서에서 사양을 참조하십시오.

광섬유 안전 정보

위험: 위험한 방사선

광섬유 제품은 레이저 방사선을 사용하므로 잠재적으로 부상을 일으킬 수 있습니다. 노출된 포트에서 이러한 방사선이 방출될 수 있습니다. 레이저 방사선에 직접 노출되지 않도록 하십시오. 빔을 쳐다보거나 광학 계기를 육안으로 직접 확인하지 마십시오. 광섬유 송수신 장치 모듈의 보호막을 제거하지 마십시오.

주의, 경고 및 기타 정보

주의, 경고, 전원 및 사이트 요구 사항과 관련하여 추가 정보를 확인하려면 사이트 및 랙 준비와 전기 안전 사전 주의 사항을 참조하십시오.

장비 포장 풀기

Aug 30, 2016

케이블, 어댑터 및 레일 키트와 같은 특정 장비의 하드웨어 부속품은 사용자가 주문한 하드웨어 플랫폼에 따라 달라질 수 있습니다. 견고하고 공간이 충분한 탁자 위에서 새 장비가 담긴 상자의 포장을 풀고 내용물을 확인합니다.

다음 목록을 사용하여 상자에 들어 있어야 할 모든 항목을 수령했는지 확인합니다.

- 주문한 장비
- RJ-45 - DB-9 어댑터 1개
- 약 1.8미터 RJ-45/DB-9 케이블 1개

다음 표에는 각 장비 모델에 포함된 전원 케이블의 수가 나와 있습니다.

모델 번호	전원 케이블
• MPX 5500 • MPX 5550/5650, • MPX 7500/9500, • MPX 8005/8015/8200/8400/8600/8800	1
• MPX 15000, • MPX 17000 • MPX 9700/10500/12500/15500 • MPX 11500/13500/14500/16500/18500/20500, MPX 11515/11520/11530/11540/11542 • MPX 14000, MPX 17500/19500/21500 • MPX 25100T/25160T • T1010 • T1100(Gen1) • T1100(16) • T1120 • T1300 • T1300-40G	2
• MPX 22040/22060/22080/22100/22120 • MPX 24100/24150 • T1200	4

참고: 각 케이블에 사용할 수 있는 전원 콘센트가 있는지 확인합니다.
참고: 전원 케이블은 AC 모델에만 사용할 수 있습니다.
참고: 브라질 고객의 경우 전원 케이블이 제공되지 않습니다. **ABNT NBR 14136:2002** 표준에 맞는 케이블을 사용하십시오.

- 4개의 기둥이 달린 표준 레일 키트 1개
  참고: 받은 키트가 랙과 맞지 않는 경우, 적절한 키트를 주문하려면 Citrix 영업 담당자에게 문의하십시오.

새 장비와 함께 상자에 포함된 항목 외에 설치 및 초기 구성 프로세스를 완료하려면 다음 항목이 필요합니다.

- 네트워크에 연결할 각각의 추가 이더넷 포트용 이더넷 케이블
- 네트워크 스위치 또는 허브에서 네트워크에 연결할 각각의 NetScaler 이더넷 포트에 사용할 수 있는 이더넷 포트 1개
  참고: 송수신 장치 모듈은 별도로 판매됩니다. 사용 중인 장비의 송수신 장치 모듈을 주문하려면 Citrix 영업 담당자에게 문의하십시오. Citrix가 제공하는 송수신 장치만 장비에서 지원됩니다.
- 관리 워크스테이션으로 작동할 컴퓨터

장비 랙 탑재

Aug 30, 2016

대부분의 장비는 EIA-310-D 사양을 준수하는 표준 서버 랙에 설치할 수 있습니다. 장비에는 레일이 함께 제공되는데, 이 레일을 먼저 설치한 후 장비를 탑재해야 합니다. 십자 드라이버와 일자 드라이버만 있으면 장비를 설치할 수 있습니다.

주의: 랙에 장비를 하나의 유닛으로 설치할 경우에는 아래쪽에 탑재합니다. 랙에 다른 유닛을 포함하는 경우 가장 무거운 유닛을 아래쪽에 설치합니다. 랙에 고정 장치를 사용할 경우에는 장비를 탑재하기 전에 먼저 고정 장치를 설치합니다.
다음 표에는 여러 가지 하드웨어 플랫폼과 각 플랫폼에 필요한 랙 유닛이 나와 있습니다.
표 1. 각 플랫폼의 높이 요구 사항

플랫폼	랙 유닛 수
MPX 5500	1U
MPX 5550/5650	
MPX 7500/9500	
MPX 8005/8015/8200/8400/8600/8800	
MPX 14000	
T1010	
MPX 15000, MPX 17000	2U
MPX 9700/10500/12500/15500	
MPX 11500/13500/14500/16500/18500/20500	
MPX 11515/11520/11530/11540/11542	
MPX 17500/19500/21500	
MPX 17550/19550/20550/21550	
MPX 22040/22060/22080/22100/22120	
MPX 24100/24150	

MPX 25100T/25160T	
T1100	
T1120	
T1200	
T1300	

각 장비는 왼쪽과 오른쪽에 하나씩 2개의 레일 어셈블리와 레일 연결 나사가 포함된 탑재용 레일 키트와 함께 제공됩니다. 어셈블리는 내부 레일과 랙 레일로 구성됩니다. 제공된 레일 키트는 길이가 28인치입니다(38인치로 확장됨). 23인치(33인치로 확장됨) 레일 키트를 주문하려면 Citrix 영업 담당자에게 문의하십시오.
참고: 사각형 구멍 랙과 원형 구멍 랙 모두에 동일한 레일 키트가 사용됩니다. 나삿니가 있는 원형 구멍 랙과 관련된 자세한 지침은 "랙에 레일 어셈블리 설치"를 참조하십시오.
장비를 탑재하려면 먼저 레일을 설치한 다음 랙에 장비를 설치합니다.

다음 작업을 수행하여 장비를 탑재합니다.
- 내부 레일을 레일 어셈블리에서 제거합니다.
- 내부 레일을 장비에 연결합니다.
- 랙 레일을 랙에 설치합니다.
- 장비를 랙에 설치합니다.

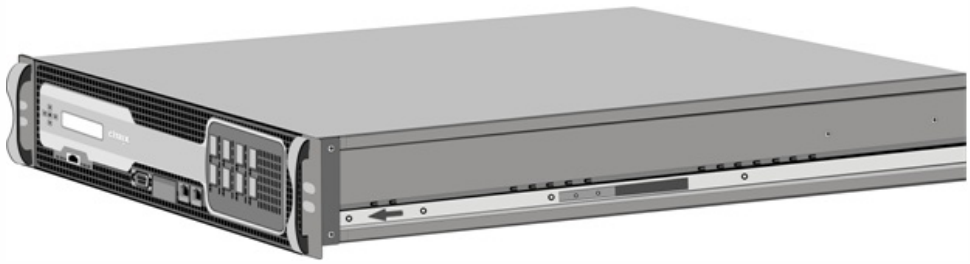
장비에는 랙 레일 하드웨어가 제공됩니다. 이 하드웨어는 양쪽에 하나씩 장비에 연결되는 두 개의 내부 레일과 랙에 연결되는 랙 레일 어셈블리로 구성됩니다. 다음 그림에서는 Citrix NetScaler 장비의 랙 마운팅과 관련된 단계를 보여 줍니다.

내부 레일을 레일 어셈블리에서 제거하려면

1. 레일 어셈블리를 평평한 표면 위에 놓습니다.
2. 내부 레일을 어셈블리 앞쪽으로 밀어 꺼냅니다.
3. 내부 레일이 완전히 레일 어셈블리 밖으로 나올 때까지 걸쇠를 누릅니다.
4. 1-3단계를 반복하여 두 번째 내부 레일을 제거합니다.

내부 레일을 장비에 연결하려면

1. 장비 오른쪽에 있는 핸들 뒤에 오른쪽 내부 레일을 놓습니다.
2. 레일의 구멍을 장비 측 해당 구멍에 맞춥니다.
3. 다음 그림과 같이 제공된 나사로 레일을 장비에 연결합니다. 나사는 1U 장비의 경우 측면당 4개이고 2U 장비의 경우 측면당 5개입니다.
   그림 1. 내부 레일 연결



4. 1-3단계를 반복하여 왼쪽 내부 레일을 장비의 다른 쪽에 설치합니다.

랙 레일을 랙에 설치하려면

1. 나삿니가 있는 원형 구멍 랙의 경우 3단계로 건너뜁니다.
2. 다음 그림과 같이 사각 너트 유지대를 랙의 앞면 기둥과 뒷면 기둥에 설치합니다. 나사를 조이기 전에 사각 너트를 해당 1U 또는 2U 장비의 올바른 구멍에 맞춰야 합니다. 세 개의 구멍은 크기가 고르지 않습니다.

   그림 2. 앞면 랙 기둥에 유지대 설치

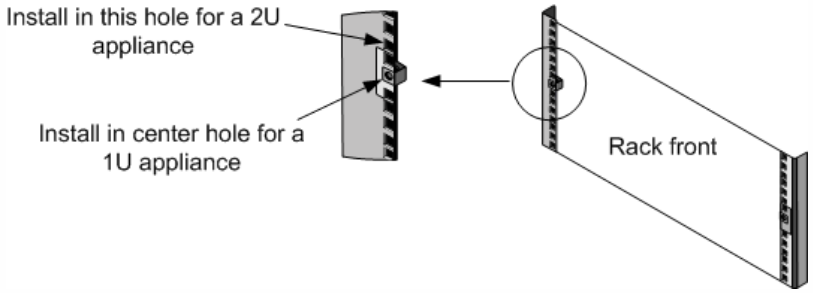
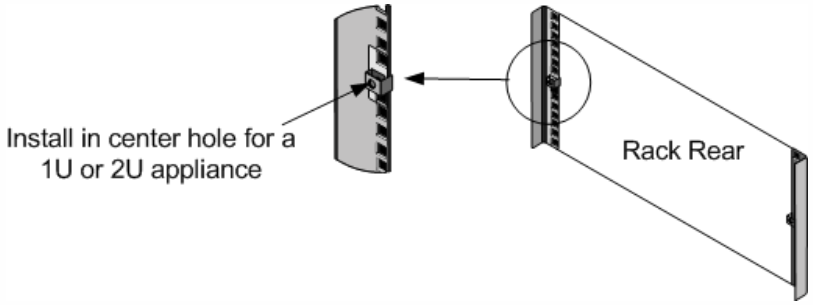
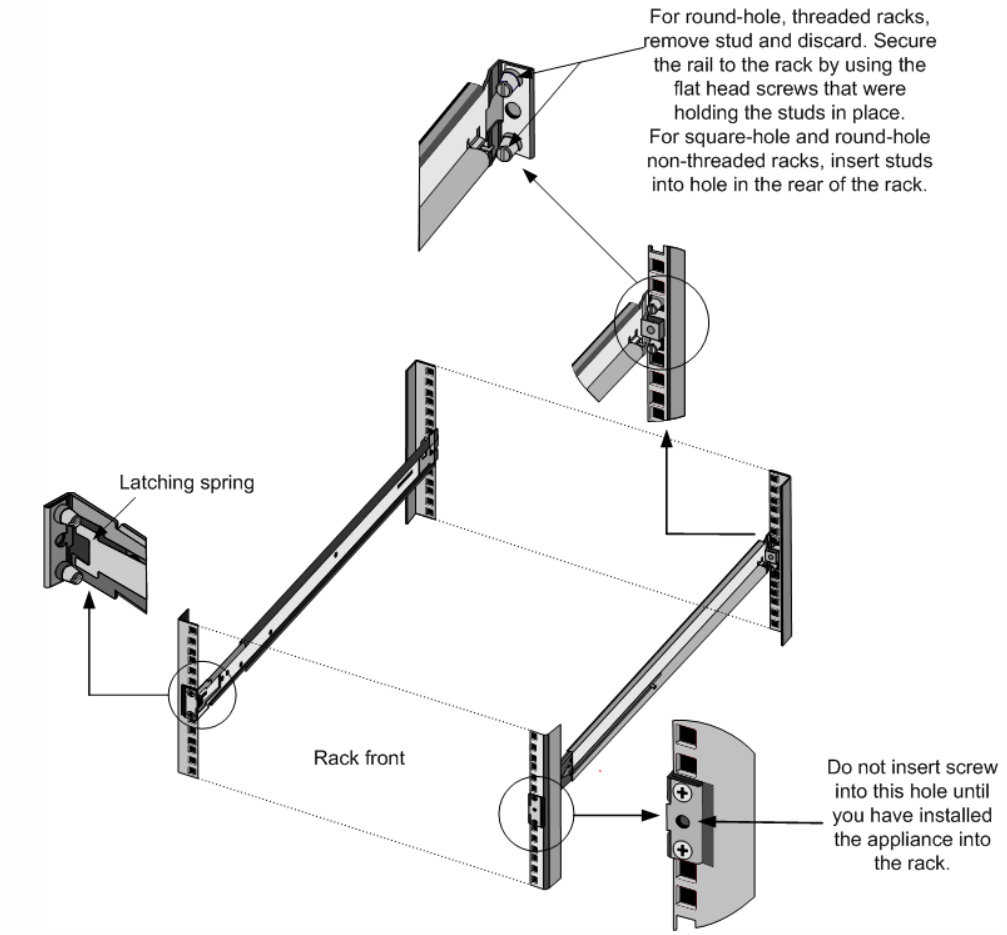


   그림 3. 뒷면 랙 기둥에 유지대 설치



3. 다음 그림과 같이 조정 가능한 레일 어셈블리를 랙에 설치합니다. 나사를 사용해서 후면 레일 플랜지를 랙에 고정합니다. 나사로 레일을 제자리에 고정하면 걸쇠 스프링을 제거할 수도 있습니다.

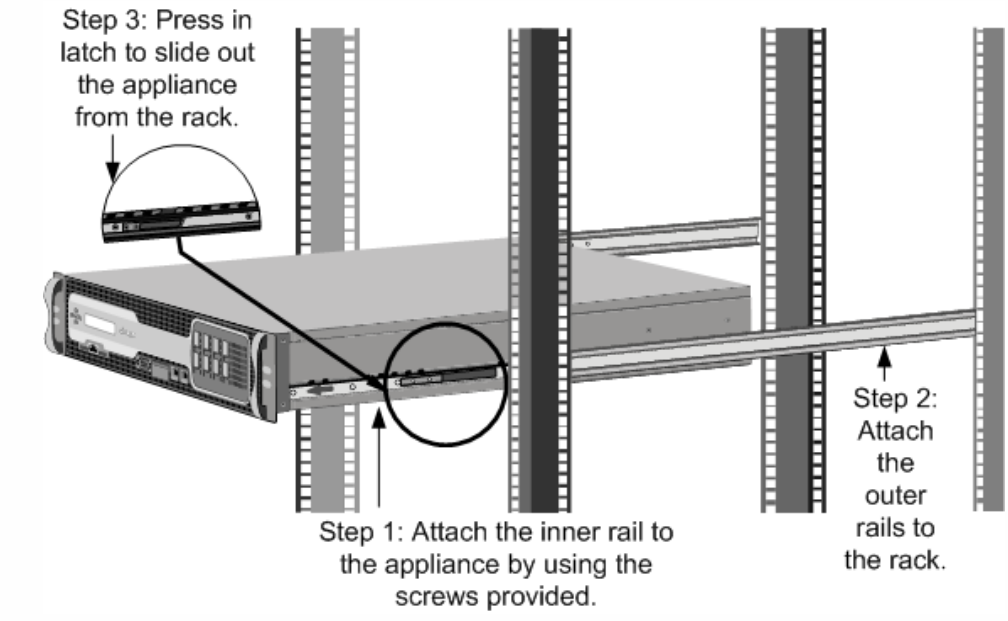
   그림 4. 랙에 레일 어셈블리 설치



장비를 랙에 설치하려면

1. 장비에 연결된 내부 레일을 랙 레일에 맞춥니다.
2. 양쪽에 같은 힘을 가하면서 장비를 랙 레일에 밀어 넣습니다.
3. 장비를 랙에서 완전히 잡아 당기면서 장비가 제자리에 고정되었는지 확인합니다.

그림 5. 장비 랙 탑재



1G SFP 송수신 장치 설치 및 제거

Aug 30, 2016

참고: 이 섹션의 내용은 MPX 8005/8015/8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 11515/11520/11530/11540/11542, MPX 22040/22060/22080/22100/22120, MPX 24100/24150 및 T1010/1200 장비에 적용됩니다.

SFP(Small Form Factor Pluggable)는 초당 최대 1기가비트의 속도로 작동할 수 있는 초소형 송수신 장치로서 구리 유형과 파이버 유형으로 사용할 수 있습니다. 1G SFP 구리 송수신 장치를 삽입하면 1G SFP 포트가 1000BASE-T 포트로 변환됩니다. 1G SFP 파이버 송수신 장치를 삽입하면 1G SFP 포트가 1000BASE-X 포트로 변환됩니다. 1G SFP 송수신 장치가 삽입되는 1G SFP 포트에서는 자동 협상 기능이 기본적으로 사용됩니다. 포트와 네트워크 사이에 링크가 설정되는 즉시 케이블 양쪽 끝의 속도와 모드가 일치하게 됩니다.

참고: 1G SFP 송수신 장치는 e1k 인터페이스를 사용하는 릴리스 9.3 빌드 47.5 이상의 NetScaler 장비에서 운영 중 스왑 가능합니다. 다음 플랫폼은 1G SPF 송수신 장치를 지원합니다.

- MPX 7500/9500
- MPX 8005/8015/8200/8400/8600/8800
- MPX 9700/10500/12500/15500
- MPX 11500/13500/14500/16500/18500/20500
- MPX 11515/11520/11530/11540/11542
- MPX 22040/22060/22080/22100/22120
- MPX 24100/24150
- T1010
- T1200

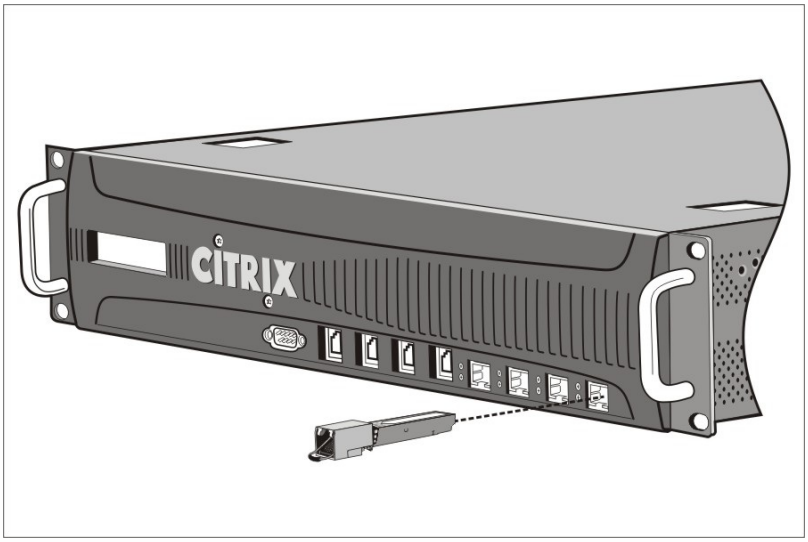
주의: NetScaler장비는 Citrix Systems 이외 공급업체의 1G SFP 송수신 장치를 지원하지 않습니다. NetScaler 장비에 타사 1G SFP 송수신 장치를 설치하려고 하면 보증은 무효가 됩니다.

1G SFP 송수신 장치를 장비의 전면 패널에 있는 1G SFP 포트에 삽입합니다. 송수신 장치를 자주 설치하고 제거하면 제품 수명이 단축됩니다. 1G SFP 송수신 장치 또는 장비가 손상되지 않도록 신중히 제거 절차를 따릅니다.

주의: 케이블이 연결된 상태로 송수신 장치를 설치하지 않도록 합니다. 케이블이 연결된 상태에서는 송수신 장치의 케이블, 커넥터 또는 광 인터페이스가 손상될 수 있습니다.

1G SFP 송수신 장치를 설치하려면

1. 1G SFP 송수신 장치를 상자에서 주의하여 꺼냅니다.
   위험: 광섬유 송수신 장치 또는 케이블을 눈으로 직접 보지 않도록 합니다. 이들 장치에서는 눈을 손상시킬 수 있는 레이저 빔이 나옵니다.
2. 다음 그림과 같이 1G SFP 송수신 장치를 장비의 전면 패널에 있는 1G SFP 송수신 장치 포트 앞쪽에 맞춥니다.
   주의: 다음 그림에서는 실제 장비가 표시되지 않을 수 있습니다.
   그림 1. 1G SFP 송수신 장치 설치



3. 엄지와 검지로 1G SFP 송수신 장치를 잡고 송수신 장치가 제자리에 물리는 소리가 들릴 때까지 1G SFP 송수신 장치 포트에 삽입합니다.
4. 송수신 장치를 잠급니다.
5. LED가 녹색으로 표시되어 두 번 깜박이는지 확인합니다. 이는 송수신 장치가 올바르게 작동하고 있음을 나타냅니다.
6. 파이버 1G SFP 송수신 장치를 사용하는 경우에는 케이블을 삽입할 준비가 되었을 때만 송수신 장치 및 케이블에 부착된 먼지 방지용 캡을 제거합니다.

1G SFP 송수신 장치를 제거하려면

1. 1G SFP 송수신 장치에서 케이블을 분리합니다. 광섬유 케이블을 사용하는 경우에는 케이블을 치워 두기 전에 먼지 방지용 캡을 다시 장착합니다.
   위험: 광섬유 송수신 장치 또는 케이블을 눈으로 직접 보지 않도록 합니다. 이들 장치에서는 눈을 손상시킬 수 있는 레이저 빔이 나옵니다.
2. 1G SFP 송수신 장치의 잠금을 해제합니다.
3. 엄지와 검지로 1G SFP 송수신 장치를 잡고 천천히 포트에서 당겨 꺼냅니다.
4. 파이버 1G SFP 송수신 장치를 제거하는 경우에는 송수신 장치를 치워 두기 전에 먼지 방지용 캡을 다시 장착합니다.
5. 1G SFP 송수신 장치를 원래의 상자나 다른 적절한 용기에 넣습니다.

XFP 및 10G SFP+ 송수신 장치 설치 및 제거

Aug 30, 2016

참고: 이 섹션의 내용은 MPX 8005/8015/8200/8400/8600/8800, MPX 9700/10500/12500/15500, MPX 15000, MPX 17000, MPX 11500/13500/14500/16500/18500/20500, MPX 11515/11520/11530/11540/11542, MPX 14000, MPX 17500/19500/21500, MPX 17550/19550/20550/21550, MPX 22040/22060/22080/22100/22120, MPX 24100/24150, MPX 25100T/25160T 및 T1100(Gen1), T1100(16), T1120, T1300 및 T1300-40G 장비에 적용됩니다.

10기가비트 SFP(XFP 또는 SFP+)는 초당 최대 10기가비트의 속도로 작동할 수 있는 초소형 광 송수신 장치입니다. XFP/10G SFP+ 송수신 장치가 삽입되는 XFP/10G SFP+ 포트에서는 자동 협상 기능이 기본적으로 사용됩니다. 포트와 네트워크 사이에 링크가 설정되는 즉시 케이블 양쪽 끝에서 모드가 일치하게 되며 10G SFP+ 송수신 장치의 경우에는 속도도 자동 협상됩니다.

참고: XFP 송수신 장치는 NetScaler 장비에서 **운영 중 스왑 가능하지 않습니다**. XFP 송수신 장치를 삽입한 후에는 NetScaler 장비를 다시 시작해야 합니다.

하지만 10G SFP+ 송수신 장치는 ixgbe(ix) 인터페이스를 사용하는 릴리스 9.3 빌드 57.5 이상의 NetScaler 장비에서 운영 중 스왑 가능합니다.

다음 플랫폼은 10G SPF+ 송수신 장치를 지원합니다.

- MPX 8005/8015/8200/8400/8600/8800
- MPX 9700/10500/12500/15500 10G 및 10G FIPS
- MPX 11500/13500/14500/16500/18500/20500
- MPX 11515/11520/11530/11540/11542
- MPX 14000
- MPX 17500/19500/21500
- MPX 17550/19550/20550/21550
- MPX 22040/22060/22080/22100/22120
- MPX 24100/24150
- MPX 25100T/25160T
- T1100(Gen1)
- T1100(16)
- T1120
- T1300
- T1300-40G

다음 플랫폼은 XFP 송수신 장치를 지원합니다.

- MPX 15000
- MPX 17000

주의: NetScaler 장비는 Citrix Systems 이외 공급업체가 제공하는 XFP/10G SFP+ 송수신 장치를 지원하지 않습니다. NetScaler 장비에 타사 XFP/10G SFP+ 송수신 장치를 설치하려고 하면 보증은 무효가 됩니다.

XFP/10G SFP+ 송수신 장치를 장비의 전면 패널에 있는 XFP/10G SFP+ 포트에 삽입합니다. 송수신 장치를 자주 설치하고 제거하면 제품 수명이 단축됩니다. 송수신 장치 또는 장비가 손상되지 않도록 신중히 제거 절차를 따릅니다.

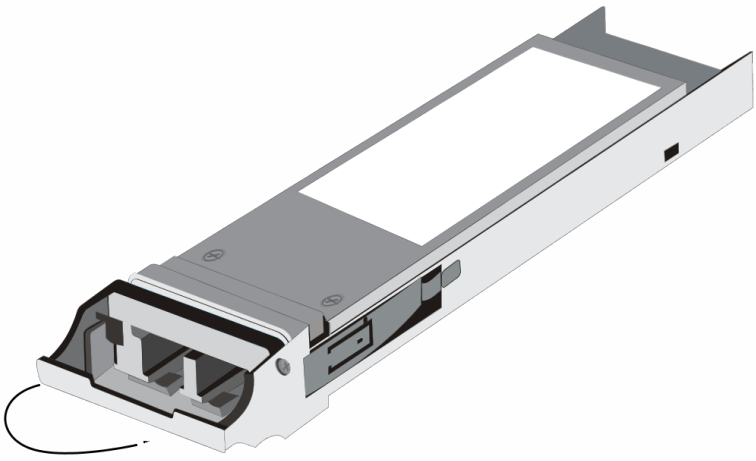
주의: 케이블이 연결된 상태로 송수신 장치를 설치하지 않도록 합니다. 케이블이 연결된 상태에서는 송수신 장치의 케이블, 커넥터 또는 광 인터페이스가 손상될 수 있습니다.

XFP/10G SFP+ 송수신 장치를 설치하려면

1. XFP/10G SFP+ 송수신 장치를 상자에서 주의하여 꺼냅니다.
   위험: 광섬유 송수신 장치 및 케이블을 눈으로 직접 보지 않도록 합니다. 이들 장치에서는 눈을 손상시킬 수 있는 레이저 빔이

나옵니다.

2. XFP/10G SFP+ 송수신 장치를 장비의 전면 패널에 있는 XFP/10G SFP+ 송수신 장치 포트 앞쪽에 맞춥니다.
3. 엄지와 검지로 XFP/10G SFP+ 송수신 장치를 잡고 송수신 장치가 제자리에 맞춰지는 소리가 들릴 때까지 XFP/10G SFP+ 송수신 장치 포트에 삽입합니다.
4. 다음 그림과 같이 잠금 힌지를 아래로 이동합니다.
   그림 1. XFP 송수신 장치 잠금



5. LED가 녹색으로 표시되어 두 번 깜박이는지 확인합니다. 이는 송수신 장치가 올바르게 작동하고 있음을 나타냅니다.
6. 케이블을 삽입할 준비가 되었을 때만 송수신 장치 및 케이블에 부착된 먼지 방지용 캡을 제거합니다.

XFP/10G SFP+ 송수신 장치를 제거하려면

1. XFP/10G SFP+ 송수신 장치에서 케이블을 분리합니다. 케이블을 치워 두기 전에 먼지 방지용 캡을 다시 장착합니다.
   위험: 광섬유 송수신 장치 또는 케이블을 눈으로 직접 보지 않도록 합니다. 이들 장치에서는 눈을 손상시킬 수 있는 레이저 빔이 나옵니다.
2. 잠금 힌지를 위로 이동하여 XFP/10G SFP+ 송수신 장치의 잠금을 해제합니다.
3. 엄지와 검지로 XFP/10G SFP+ 송수신 장치를 잡고 천천히 포트에서 당겨 꺼냅니다.
4. 송수신 장치를 치워 두기 전에 먼지 방지용 캡을 다시 장착합니다.
5. XFP/10G SFP+ 송수신 장치를 원래의 상자나 다른 적절한 용기에 넣습니다.

케이블 연결

Aug 30, 2016

장비가 랙에 안전하게 탑재되면 케이블을 연결할 수 있습니다. 먼저 이더넷 케이블 및 선택 사항인 콘솔 케이블을 연결합니다. 마지막으로 전원 케이블을 연결합니다.

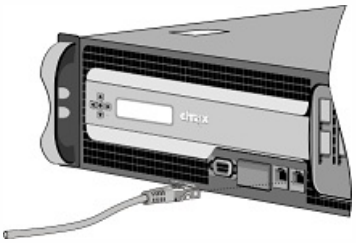
위험: 장비를 설치하거나 복구하기 전에 전원 또는 전선과 접촉할 가능성이 있는 장신구 및 기타 금속 물체를 모두 제거합니다. 작동 중인 전원 또는 전선과 접지 양쪽에 접할 경우 금속 물체가 급속히 뜨거워지고 화재가 발생할 수 있으며, 옷이 타거나 금속 물체가 노출된 터미널에 녹아버릴 수 있습니다.

Connecting the Ethernet Cables

이더넷 케이블은 장비와 네트워크를 연결하는 데 사용됩니다. 필요한 케이블 유형은 네트워크 연결에 사용되는 포트의 유형에 따라 다릅니다. 10/100/1000BASE-T 포트 또는 1G SFP 구리 송수신 장치에는 표준 RJ-45 커넥터가 포함된 범주 5e 또는 범주 6 이더넷 케이블을 사용합니다. 1G SFP 파이버 송수신 장치, 10G SFP+ 또는 XFP 송수신 장치에는 LC 이중 커넥터가 달린 광섬유 케이블을 사용합니다. 광섬유 케이블의 다른 쪽 끝에 있는 커넥터 유형은 연결할 장치의 포트에 따라 다릅니다.

이더넷 케이블을 10/100/1000BASE-T 포트 또는 1G SFP 구리 송수신 장치에 연결하려면

1. 이더넷 케이블의 한쪽 끝에 있는 RJ-45 커넥터를 다음 그림에 나와 있는 것과 같이 장비의 전면 패널에 있는 해당 포트에 삽입합니다.
   그림 1. 이더넷 케이블 삽입



2. 다른 쪽 끝의 RJ-45 커넥터를 라우터나 스위치 같은 대상 장치에 삽입합니다.
3. 연결이 설정되면 LED가 주황색으로 표시되는지 확인합니다.

이더넷 케이블을 1G SFP 파이버, 10G SFP+ 또는 XFP 송수신 장치에 연결하려면

1. 송수신 장치 및 케이블에서 먼지 방지용 뚜껑을 제거합니다.
2. 광섬유 케이블 한쪽 끝의 LC 커넥터를 장비의 전면 패널에 있는 해당 포트에 삽입합니다.
3. 다른 쪽 끝의 커넥터를 라우터나 스위치 같은 대상 장치에 삽입합니다.
4. 연결이 설정되면 LED가 주황색으로 표시되는지 확인합니다.

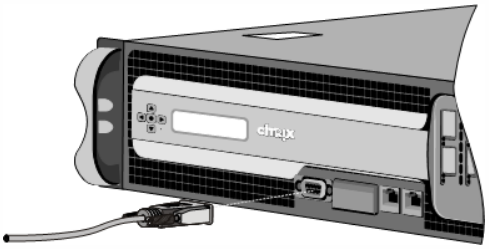
콘솔 케이블 연결

콘솔 케이블을 사용하여 장비를 구성하는 데 사용할 컴퓨터 또는 터미널에 해당 장비를 연결할 수 있습니다. 또는 네트워크에 연결된 컴퓨터를 사용할 수도 있습니다. 콘솔 케이블을 연결하기 전에 VT100 터미널 에뮬레이션, 9600보드, 8 데이터 비트, 1 정지 비트 및 패리티를 지원하고 흐름 제어가 없음으로 설정되도록 컴퓨터를 구성합니다. 그런 다음 콘솔 케이블의 한쪽 끝을 장비의 RS232 직렬 포트에 연결하고 다른 쪽 끝을 컴퓨터 또는 터미널에 연결합니다.

콘솔 케이블을 컴퓨터 또는 터미널에 연결하려면

1. 케이블 끝의 DB-9 커넥터를 다음 그림에 나타낸 것과 같이 장비의 전면 패널에 있는 콘솔 포트에 삽입합니다.

그림 2. 콘솔 케이블 삽입



참고: 케이블을 RJ-45 컨버터와 함께 사용하려면 선택 사항으로 제공된 컨버터를 콘솔 포트에 삽입한 다음 케이블을 컨버터에 연결합니다.

2. 케이블의 다른 쪽 끝에 있는 RJ-45 커넥터를 컴퓨터 또는 터미널의 직렬 포트에 삽입합니다.

Connecting the Power Cable

각 NetScaler 모델에 포함된 케이블 수에 대한 자세한 내용은 "장비 포장 풀기"를 참조하십시오.

두 개의 전원 케이블이 제공되는 모델은 전원 케이블 하나만으로도 작동할 수 있습니다. 하지만 4개의 전원 케이블이 제공되는 모델의 경우 2개의 케이블을 사용해야 제대로 작동합니다. 3핀 플러그는 접지 플러그이므로 별도의 접지 케이블이 필요 없습니다.

장비를 전원에 연결하려면

1. 전원 케이블의 한쪽 끝을 아래 그림과 같이 전원 공급 장치 옆에 있는 장비 후면 패널의 전원 콘센트에 연결합니다.
   그림 3. 전원 케이블 삽입

2. 전원 케이블의 다른 쪽 끝을 표준 110V/220V 전원 콘센트에 연결합니다.
3. 두 번째 전원 공급 장치가 제공되는 경우 1-2단계를 반복하여 두 번째 전원 공급 장치를 연결합니다.
   참고: The MPX 9700/10500/12500/15500, MPX 11500/13500/14500/16500/18500/20500, MPX 11515/11520/11530/11540/11542, MPX 17500/19500/21500, MPX 17550/19550/20550/21550 및 T1100(Gen1)/T1100(16) 장비는 전원 공급 장치 한쪽에 장애가 발생하거나 장비에 전원 케이블을 한 개만 연결할 경우 고음의 경고음을 냅니다. 경보를 끄려면 장비의 후면 패널에 있는 작은 빨간색 단추를 누릅니다.

Citrix NetScaler 액세스

Aug 30, 2016

NetScaler 장비는 CLI(명령줄 인터페이스)와 GUI(그래픽 사용자 인터페이스)를 모두 제공합니다. GUI에는 장비 구성에 사용되는 구성 유틸리티와 대시보드라고 하는 통계 유틸리티가 있습니다. 최초 액세스를 지원하기 위해 모든 장비에는 기본 NSIP(NetScaler IP) 주소인 192.168.100.1과 기본 서브넷 마스크인 255.255.0.0이 제공됩니다. 초기 구성 중에 새 NSIP 및 연관된 서브넷 마스크를 지정할 수 있습니다.

여러 NetScaler 장치를 배포할 때 IP 주소 충돌이 발생하는 경우 다음과 같은 원인을 고려할 수 있습니다.

- 네트워크의 다른 장치에 이미 지정된 IP 주소인 NSIP를 선택하셨습니까?
- 여러 NetScaler 장비에 동일한 NSIP를 할당하셨습니까?
- NSIP는 모든 물리적 포트에서 접근할 수 있습니다. NetScaler의 포트는 스위치 포트가 아닌 호스트 포트입니다.

다음 표에는 사용할 수 있는 액세스 방법이 요약되어 있습니다.

표 1. NetScaler 장비에 액세스하는 방법

액세스 방법	포트	기본 IP 주소 필요? (Y/N)
CLI	콘솔	아니요
CLI 및 GUI	이더넷	예

CLI 사용

업데이트 날짜: 2013년 09월 04일

워크스테이션을 콘솔 포트에 로컬로 연결하거나, 동일한 네트워크의 워크스테이션에서 SSH(Secure Shell)를 통해 원격으로 연결하여 CLI에 액세스할 수 있습니다.

콘솔 포트를 통해 CLI에 로그온

장비에는 컴퓨터 워크스테이션에 연결하는 데 사용되는 콘솔 포트가 있습니다. 장비에 로그온하려면 직렬 크로스오버 케이블과 터미널 에뮬레이션 프로그램이 지원되는 워크스테이션이 있어야 합니다.
콘솔 포트를 통해 CLI에 로그온하려면

1. 에 설명된 대로 워크스테이션의 직렬 포트에 콘솔 포트를 연결합니다.
2. 워크스테이션에서 하이퍼터미널 또는 다른 터미널 에뮬레이션 프로그램을 시작합니다. 로그온 프롬프트가 나타나지 않을 경우 ENTER를 한 번 이상 눌러 표시해야 할 수 있습니다.
3. 관리자 자격 증명을 사용하여 로그온합니다. 명령 프롬프트(>)가 워크스테이션 모니터에 표시됩니다.

SSH를 사용하여 CLI에 로그온

SSH 프로토콜은 동일한 네트워크의 워크스테이션에서 장비에 원격으로 액세스하기 위한 권장 원격 액세스 방법입니다. SSH 버전 1(SSH1) 또는 SSH 버전 2(SSH2)를 사용할 수 있습니다.

작동하는 SSH 클라이언트가 없을 경우 다음 SSH 클라이언트 프로그램을 다운로드하고 설치할 수 있습니다.

- PuTTY
  여러 플랫폼에서 지원되는 공개 소스 소프트웨어입니다. 다운로드 주소:

  "http://www.chiark.greenend.org.uk/~sgtatham/putty/"

- Vandyke Software SecureCRT

Windows 플랫폼에서 지원되는 상용 소프트웨어입니다. 다운로드 주소:

"http://www.vandyke.com/products/securecrt/"

이러한 모든 프로그램은 Citrix NetScaler 팀에서 테스트하여 NetScaler 장비와 함께 정상적으로 작동한다는 것을 확인했습니다. 기타 프로그램도 정상적으로 작동할 수 있지만 테스트되지는 않습니다.

SSH 클라이언트가 제대로 설치되었는지 확인하려면 SSH 연결을 허용하는 네트워크의 장치에 연결해 보십시오.

SSH 클라이언트를 사용하여 NetScaler에 로그온하려면

1. 워크스테이션에서 SSH 클라이언트를 시작합니다.
2. 초기 구성의 경우 기본 NetScaler IP 주소(NSIP)인 192.168.100.1을 사용합니다. 이후에 액세스할 때는 초기 구성 중에 할당한 NSIP를 사용합니다. 프로토콜로 SSH1 또는 SSH2를 선택합니다.
3. 관리자 자격 증명을 사용하여 로그온합니다. 예를 들면 다음과 같습니다.
   login as: nsroot Using keyboard-interactive authentication. Password: Last login: Tue Jun 16 10:37:28 2009 from 10.102.29.9 Done >

GUI 사용

업데이트 날짜: 2014년 06월 30일

중요: NetScaler 구성 유틸리티에 HTTPS가 액세스하려면 인증서 키 쌍이 필요합니다. NetScaler ADC에서 인증서 키 쌍은 자동으로 내부 서비스에 바인딩됩니다. MPX 또는 SDX 장비에서는 기본 키 크기가 1024바이트이고 VPX 인스턴스에서는 기본 키 크기가 512바이트입니다. 그러나 오늘날 대부분의 브라우저는 1024바이트 미만의 키를 받아들이지 않습니다. 따라서 VPX 구성 유틸리티에 대한 HTTPS 액세스는 차단됩니다.
또한 MPX 장비가 시작될 때 해당 장비에 라이센스가 없는 경우 나중에 라이센스를 추가하여 장비를 다시 시작하면 인증서 바인딩이 손실될 수 있습니다.

HTTPS가 구성 유틸리티에 액세스할 수 있도록 하려면 NetScaler ADC에 1024바이트 이상의 인증서 키 쌍을 설치하고 ADC를 시작하기 전에 적절한 라이센스를 설치하는 것이 좋습니다.

GUI에는 구성 유틸리티와 대시보드라는 통계 유틸리티가 있으며, 이 두 유틸리티는 장비의 이더넷 포트에 연결된 워크스테이션을 통해 액세스할 수 있습니다. 컴퓨터에 지원되는 Java 플러그인이 설치되어 있지 않은 경우 NetScaler에 처음으로 로그온하면 유틸리티에서 플러그인을 다운로드하고 설치할지 물어봅니다. 자동 설치에 실패하면 구성 유틸리티나 대시보드에 로그온하기 전에 별도로 플러그인을 설치할 수 있습니다.

GUI를 실행하는 워크스테이션에 대한 시스템 요구 사항은 다음과 같습니다.

- Windows 기반 워크스테이션의 경우 Java 플러그인 제품을 사용하는 브라우저에서 실행되는 애플릿을 위해 Pentium 166MHz 이상의 프로세서 및 최소 48MB의 RAM이 권장됩니다. 플러그인을 설치하려면 40MB의 사용 가능한 디스크 공간이 있어야 합니다.
- Linux 기반 워크스테이션의 경우 Linux 커널 v2.2.12 이상 및 glibc 버전 2.12-11 이상을 실행하는 Pentium 플랫폼이 필요합니다. 최소 32MB의 RAM이 필요하며, 48MB의 RAM이 권장됩니다. 워크스테이션은 로컬 호스트로 설정된 디스플레이와 함께 사용되는 16비트 컬러 모드, KDE 및 KWM 창 관리자를 지원해야 합니다.
- Solaris 기반 워크스테이션의 경우 Solaris 2.6, Solaris 7 또는 Solaris 8을 실행하는 Sun 및 Java 2 Runtime Environment, Standard Edition, 버전 1.6 이상이 필요합니다.

구성 유틸리티 및 대시보드에 액세스하려면 워크스테이션에 지원되는 웹 브라우저 및 버전 1.6 이상의 Java 애플릿 플러그인이 설치되어 있어야 합니다.

지원되는 브라우저는 다음과 같습니다.

운영 체제	브라우저	버전
Windows 7	Internet Explorer	8, 9 및 10
	Mozilla Firefox	3.6.25 이상

운영 체제	브라우저	버전
	Google Chrome	최신
Windows 64비트	Internet Explorer	8 및 9
	Google Chrome	최신
MAC	Mozilla Firefox	12 이상
	Safari	5.1.3
	Google Chrome	최신

구성 유틸리티 사용

구성 유틸리티에 로그온하면 상황에 맞는 도움말이 있는 그래픽 인터페이스를 통해 장비를 구성할 수 있습니다.

컴퓨터에 지원되는 Java 플러그인이 설치되어 있지 않은 경우 장비에 처음으로 로그온하면 구성 유틸리티에서 플러그인을 다운로드하고 설치할지 물어보는 메시지가 표시됩니다.

참고: Java 2 Runtime Environment를 설치하기 전에 현재 Java 릴리스에 필요한 전체 운영 체제 패치를 설치했는지 확인하십시오.

구성 유틸리티에 로그온하려면

1. 웹 브라우저를 열고 HTTP 주소로 NetScaler IP(NSIP)를 입력합니다. 아직 초기 구성을 설정하지 않은 경우에는 기본 NSIP를 입력합니다(http://192.168.100.1). Citrix Logon(Citrix 로그온) 페이지가 나타납니다.
   참고: 고가용성 설정에 두 NetScaler 장비가 있는 경우 보조 NetScaler의 IP 주소를 입력하여 GUI에 액세스하지 않도록 하십시오. 만약 그렇게 로그인하고 GUI를 사용하여 보조 NetScaler를 구성할 경우 구성 변경 사항은 기본 NetScaler에 적용되지 않습니다.
2. User Name(사용자 이름) 텍스트 상자에 다음을 입력합니다.nsroot.
3. Password(암호) 텍스트 상자에 초기 구성 도중 nsroot 계정에 지정한 관리 암호를 입력하고 Login(로그인)을 클릭합니다. Configuration Utility(구성 유틸리티) 페이지가 나타납니다.
   참고: 워크스테이션에 지원되는 버전의 Java Runtime 플러그인이 설치되어 있지 않은 경우 NetScaler에서 Java 플러그인을 다운로드할지 물어봅니다. 다운로드가 완료되면 구성 유틸리티 페이지가 나타납니다.
   온라인 도움말에 액세스해야 하는 경우 상단 오른쪽의 Help 메뉴에서 Help를 선택하십시오.

통계 유틸리티 사용

대시보드 즉, 통계 유틸리티는 NetScaler의 성능을 모니터링할 수 있는 차트 및 테이블을 표시하는 브라우저 기반 응용 프로그램입니다.

대시보드에 로그온하려면

1. 웹 브라우저를 열고 HTTP 주소로 NSIP를 입력합니다(예: http://). Citrix Logon(Citrix 로그온) 페이지가 나타납니다.
2. User Name(사용자 이름) 텍스트 상자에 다음을 입력합니다.nsroot.
3. Password(암호) 텍스트 상자에 초기 구성 중 nsroot 계정에 지정한 관리 암호를 입력합니다.

Java Runtime 플러그인 설치

Java 플러그인의 자동 설치에 실패할 경우 구성 유틸리티에 로그온하기 전에 별도로 플러그인을 설치할 수 있습니다.

참고: Java 2 Runtime Environment를 설치하기 전에 현재 Java 릴리스에 필요한 전체 운영 체제 패치를 설치했는지 확인하십시오.

워크스테이션에 Java Runtime 플러그인을 설치하려면

1. 웹 브라우저에서 장비의 NSIP 및 포트 번호를 입력합니다.http://:80 Java 플러그인 아이콘이 나타납니다.
2. Java 플러그인 아이콘을 클릭하고 화면의 지시에 따라 플러그인 설치 프로그램을 워크스테이션 하드 디스크에 복사합니다. Java 플러그인 설치 아이콘(예: **j2re-1.6.0**)이 컴퓨터의 지정한 위치에 나타납니다.
3. 플러그인 설치 아이콘을 두 번 클릭하고 화면의 지시에 따라 플러그인을 설치합니다.
4. 웹 브라우저로 돌아와서 Java 플러그인 아이콘을 두 번 클릭하여 GUI 로그온 화면을 표시합니다.

처음으로 NetScaler 구성

Aug 30, 2016

초기 구성은 다기능 Citrix NetScaler, 전용 NetScaler Gateway Enterprise Edition 및 전용 Citrix NetScaler Application Firewall 장비에서 동일합니다. 장비의 초기 구성을 위해 다음 인터페이스 중 하나를 사용할 수 있습니다.

- 처음 사용 마법사 - 웹 브라우저를 사용하여 장비에 연결하는 경우, 이전에 지정하지 않았으면 네트워크 구성 및 라이센스 정보를 입력하라는 메시지가 표시됩니다.
- LCD 키패드 - 네트워크 설정을 지정할 수 있습니다. 단, 라이센스를 업로드하려면 다른 인터페이스를 사용해야 합니다.
- 직렬 콘솔 - 직렬 콘솔에 연결한 다음, 명령줄 인터페이스를 사용하여 네트워크 설정을 지정하고 라이센스를 업로드합니다.
- NITRO API - NITRO API 제품군을 사용하여 NetScaler 장비를 구성할 수 있습니다.

초기 구성의 경우 nsroot를 관리 사용자 이름 및 암호로 사용합니다. 이후에 액세스할 때는 초기 구성 중에 할당한 암호를 사용합니다.

두 개의 NetScaler 장비를 고가용성 쌍으로 설치하는 경우 하나를 기본으로 구성하고 나머지 하나를 보조로 구성합니다.

FIPS 장비에 대한 구성 절차는 NetScaler MPX 장비 또는 NetScaler 가상 장비에 대한 구성 절차와 약간 다릅니다.

설치 마법사 처음 사용

NetScaler 장비(또는 NetScaler 가상 장비)를 처음으로 구성하려는 경우 장비와 동일한 네트워크에 구성된 관리 컴퓨터가 필요합니다.

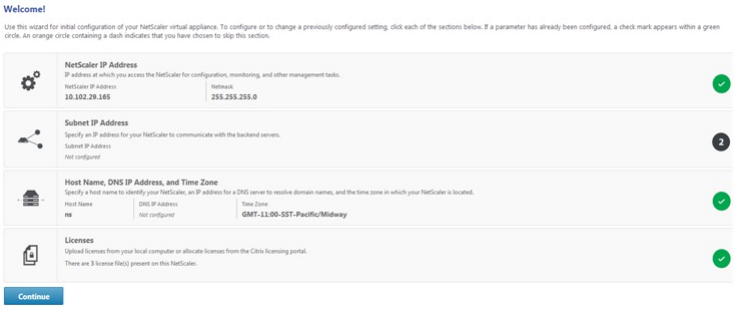
NSIP(NetScaler IP) 주소를 NetScaler 장비의 관리 IP 주소로 할당해야 합니다. 이는 구성, 모니터링 및 기타 관리 작업을 위해 NetScaler에 액세스하는 주소입니다. NetScaler가 백엔드 서버와 통신하려면 SNIP(서브넷 IP) 주소를 할당해야 합니다. NetScaler, 도메인 이름 확인을 위한 DNS 서버의 IP 주소 및 NetScaler가 위치한 표준 시간대를 식별할 수 있도록 호스트 이름을 지정해야 합니다.

다음 조건 중 하나가 충족되면 마법사가 자동으로 나타납니다.

- 장비가 기본 IP 주소(192.168.100.1)로 구성된 경우
- 서브넷 IP 주소가 구성되지 않은 경우
- 라이센스가 장비에 없는 경우

장비를 처음 구성하려면

1. 웹 브라우저에서 다음을 입력합니다. http://192.168.100.1
   참고: NetScaler 소프트웨어는 기본 IP 주소로 미리 구성되었습니다. NSIP 주소가 이미 할당된 경우에는 해당 주소를 웹 브라우저에 입력합니다.
2. User Name(사용자 이름) 및 Password(암호)에서 관리자 자격 증명을 입력합니다. 다음 화면이 나타납니다.



3. 설정을 구성하거나 이전에 구성한 설정을 변경하려면 각 섹션의 내부를 클릭합니다. 완료되면 Continue(계속)를 클릭합니다.
4. 메시지가 표시되면 Reboot(재부팅)를 선택합니다.

LCD 키패드 사용

장비를 처음으로 설치하는 경우 장비의 전면 패널에 있는 LCD 키패드를 사용하여 초기 설정을 구성할 수 있습니다. 키패드는 LCD 표시 모듈과 상호 작용하며, 해당 모듈도 또한 이 장비의 전면 패널에 있습니다.

참고: 새 장비에서 LCD 키패드를 사용한 초기 구성을 기본 구성으로 사용할 수 있습니다. 구성 파일(ns.conf)에는 다음 명령 및 기본값이 포함되어 있습니다.
set ns config -IPAddress 192.168.100.1 -netmask 255.255.0.0

다음 표에는 여러 가지 키 및 그에 대한 설명이 나와 있습니다.

표 1. LCD 키 기능

키	기능
<	커서를 왼쪽으로 한 단계 이동합니다.
>	커서를 오른쪽으로 한 단계 이동합니다.
^	커서 아래의 숫자를 늘립니다.
v	커서 아래의 숫자를 줄입니다.
.	해당 정보를 처리하거나, 변경된 값이 없으면 구성을 종료합니다. 이 키는 Enter 키로도 알려져 있습니다.

LCD 키패드를 사용하여 초기 구성을 수행하려면 "<" 키를 누릅니다.

서브넷 마스크, NetScaler IP(NSIP) 주소 및 게이트웨이를 각각 순서대로 입력하라는 메시지가 표시됩니다. 서브넷 마스크는 NSIP 및 기본 게이트웨이 IP 주소 둘 다와 연결됩니다. NSIP는 NetScaler 장비의 IPv4 주소입니다. 기본 게이트웨이는 라우터에 사용되는 IPv4 주소이며, 이 주소는 NetScaler가 라우팅할 수 없는 외부 IP 트래픽을 처리합니다. NSIP 및 기본 게이트웨이는 동일한 서브넷에 있어야 합니다.

서브넷 마스크에 유효한 값(예: 255.255.255.224)을 입력하면 IP 주소를 입력하라는 메시지가 표시됩니다. 마찬가지로 IP 주소에 유효한 값을 입력하면 게이트웨이 주소를 입력하라는 메시지가 표시됩니다. 잘못된 값을 입력하면 3초 동안 다음과 같은 오류 메시지가 표시된 후 값을 다시 입력하라는 요청이 표시됩니다(여기서, xxx.xxx.xxx.xxx는 입력한 IP 주소임).

Invalid addr! xxx.xxx.xxx.xxx
아무 숫자도 변경하지 않고 Enter(.) 키를 누르면 소프트웨어가 이 키를 사용자 종료 요청으로 해석하고 3초 동안 다음과 같은 메시지가 표시됩니다.

Exiting menu... xxx.xxx.xxx.xxx
올바른 값을 모두 입력한 경우 Enter 키를 누르면 다음과 같은 메시지가 표시됩니다.

Values accepted, Rebooting...
서브넷 마스크, NSIP 및 게이트웨이 값은 구성 파일에 저장됩니다.

참고: HA(고가용성) 쌍 배포에 대한 자세한 내용은 "고가용성"을 참조하십시오.

NetScaler 직렬 콘솔 사용

장비를 처음 설치하는 경우 직렬 콘솔을 사용하여 초기 설정을 구성할 수 있습니다. 직렬 콘솔을 사용하여 시스템 IP 주소 변경, 서브넷 또는 매핑 IP 주소 만들기, 고급 네트워크 설정 구성 및 표준 시간대 변경을 수행할 수 있습니다.

참고: 장비에 직렬 콘솔 포트의 위치를 지정하려면 "Ports(포트)"에서 "RS232 Serial Console Port(RS232 직렬 콘솔 포트)"를 참조하십시오.

직렬 콘솔을 사용하여 초기 설정을 구성하려면

1. 장비에 콘솔 케이블을 연결하십시오. 자세한 내용은 "케이블 연결"에서 "콘솔 케이블 연결"을 참조하십시오.
2. 컴퓨터에서 원하는 vt100 터미널 에뮬레이션 프로그램을 실행하여 장비에 연결한 후 다음 설정을 구성합니다. 9600 보드, 8 데이터 비트, 1 정지 비트, 패리티 및 흐름 제어를 없음으로 설정합니다.
3. Enter 키를 누릅니다. 터미널 화면에 로그온 메시지가 표시됩니다.
   참고: 사용 중인 터미널 프로그램에 따라 Enter 키를 두 번 또는 세 번 눌러야 할 수 있습니다.
4. 관리자 자격 증명으로 장비에 로그온합니다. 영업 담당자 또는 Citrix 고객 서비스 센터에서 관리자 자격 증명을 제공합니다.
5. 프롬프트에서 config ns를 입력하여 NetScaler 구성 스크립트를 실행합니다.
6. 장비의 초기 구성을 완료하려면 지시에 따릅니다.
   참고: 공격자가 장비로 패킷을 보내는 기능을 방해하지 못하게 하려면 조직의 LAN에서 라우팅할 수 없는 IP 주소를 장비 IP 주소로 선택합니다.
   5, 6단계는 다음 NetScaler 명령으로 대신할 수 있습니다. NetScaler 명령 프롬프트에서 다음을 입력합니다.

   set ns config -ipaddress -netmask

   add ns ip -type

   add route

   set system user -password

   save ns config

   reboot

   예제:

   set ns config -ipaddress 10.102.29.60 -netmask 255.255.255.0 add ns ip 10.102.29.61 255.255.255.0 -type snip add route 0.0.0.0 0.0.0.0 10.102.29.1 set system user nsroot -password Enter passwo
   장비의 초기 구성을 마쳤습니다. 장비 구성을 계속하려면 다음 옵션 중 하나를 선택합니다.

   Citrix NetScaler

   장비를 다른 라이센스 기능과 함께 표준 NetScaler로 구성하려는 경우 "Load Balancing(부하 분산)"을 참조하십시오.
   Citrix NetScaler Application Firewall.
   장비를 독립형 응용 프로그램 방화벽으로 구성하려는 경우 "Application Firewall(응용 프로그램 방화벽)"을 참조하십시오.
   NetScaler Gateway.
   장비를 NetScaler Gateway로 구성하려는 경우 "NetScaler Gateway 10.5"를 참조하십시오.

   참고: HA(고가용성) 쌍 배포에 대한 자세한 내용은 "Configuring High Availability(고가용성 구성)"를 참조하십시오.

NITRO API를 사용한 NetScaler 구성

NITRO API를 사용하여 NetScaler 장비를 구성할 수 있습니다. NITRO는 REST(Representational State Transfer) 인터페이스를 통해 기능을 노출합니다. 따라서 NITRO 응용 프로그램은 모든 프로그래밍 언어로 개발할 수 있습니다. 또한 Java나 .NET 또는 Python으로 개발해야 하는 응용 프로그램의 경우 NITRO API는 별도의 SDK(소프트웨어 개발 키트)로 패키지된 관련 라이브러리를 통해 표시됩니다. 자세한 내용은 NITRO API를 참조하십시오.

처음으로 고가용성 쌍 구성

Sep 13, 2016

고가용성 구성으로 두 개의 NetScaler 장비를 배포할 수 있습니다. 이 경우 한 장비는 연결을 적극적으로 허용하고 서버를 관리하며, 다른 장비는 이 장비를 모니터링합니다. 고가용성 구성에서 연결을 적극적으로 허용하고 서버를 관리하는 NetScaler를 주 장치라고 하고, 나머지 장치를 보조 장치라고 합니다. 주 장치에 문제가 발생할 경우 보조 장치가 주 장치가 되어 연결을 유지해 줍니다.

고가용성 쌍에서 각 NetScaler는 하트비트 메시지 또는 상태 확인하라는 정기적인 메시지를 보내 서로 모니터링함으로써 피어 노드의 상태를 확인합니다. 주 장치에 대한 상태 확인에 실패할 경우 보조 장치가 일정 기간 동안 연결을 재시도합니다. 고가용성에 대한 자세한 내용은 "고가용성"을 참조하십시오. 지정된 기간이 끝날 때까지 재시도가 성공하지 못하면 장애 조치(failover) 프로세스에서 보조 장치가 주 장치 대신 실행됩니다. 다음 그림에서는 단일 암 모드의 고가용성 구성과 이중 암 모드의 고가용성 구성을 보여 줍니다.

그림 1. 단일 암 모드의 고가용성

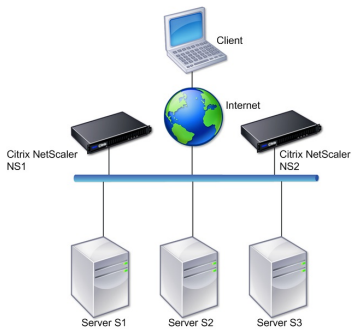


그림 2. 이중 암 모드의 고가용성

One-arm 구성에서는 NS1과 NS2 및 서버 S1, S2, S3가 스위치에 연결됩니다.

Two-arm 구성에서는 NS1과 NS2가 두 스위치에 연결됩니다. 서버 S1, S2, S3은 보조 스위치에 연결됩니다. 클라이언트와 서버 간의 트래픽은 NS1 또는 NS2를 통해 전달됩니다.

고가용성 환경을 설정하려면 NetScaler 하나를 주 장치로, 다른 NetScaler를 보조 장치로 구성해야 합니다. 각 NetScaler에서 다음 작업을 수행하십시오.

- 노드를 추가합니다.
- 사용되지 않는 인터페이스에 대한 고가용성 모니터링을 비활성화합니다.

노드 추가

업데이트 날짜: 2013년 06월 24일

노드는 피어 NetScaler 장비의 논리적 표현입니다. 피어 장치는 ID 및 NSIP로 식별할 수 있습니다. 장비는 이러한 매개 변수를 사용하여 피어와 통신하고 상태를 추적합니다. 노드를 추가하면 기본 장치와 보조 장치는 하트비트 메시지를 비동기적으로 교환합니다. 노드 ID는 64보다 작아야 하는 정수입니다.

명령줄 인터페이스를 사용하여 노드를 추가하려면

명령 프롬프트에서 다음 명령을 입력하여 노드를 추가하고 노드가 추가되었는지 확인합니다.

- add HA node <id> <IPAddress>
- show HA node <id>

예제:

```
add HA node 0 10.102.29.170  Done > show HA node 0 1)  Node ID:  0  IP:  10.102.29.200 (NS200)  Node State: UP  Master State: Primary  SSL Card Status: UP  Hello Interv
```

구성 유틸리티를 사용하여 노드를 추가하려면

1. **System(시스템)** > **High Availability(고가용성)**로 이동합니다.
2. **Nodes(노드)** 탭에서 **Add(추가)**를 클릭합니다.
3. **Create HA Node(HA 노드 만들기)** 페이지의 **Remote Node IP Address(원격 노드 IP 주소)** 텍스트 상자에 원격 노드의 NSIP 주소(예: 10.102.29.170)를 입력합니다.
4. **Configure remote system to participate in High Availability setup(고가용성 설정에 참여하도록 원격 시스템 구성)** 확인란이 선택되었는지 확인합니다. **Remote System Login Credentials(원격 시스템 로그인 자격 증명)** 아래의 텍스트 상자에 원격 노드의 로그인 자격 증명을 입력합니다.
5. **Turn off HA monitor on interfaces/channels that are down(다운된 인터페이스/채널에서 고가용성 모니터 끄기)** 확인란을 선택하여 다운된 인터페이스에서 고가용성 모니터를 비활성화합니다.

추가한 노드가 Nodes(노드) 탭의 노드 목록에 나타나는지 확인합니다.

사용되지 않는 인터페이스에 대한 고가용성 모니터링 비활성화

업데이트 날짜: 2013년 06월 24일

고가용성 모니터는 인터페이스를 모니터링하는 가상 엔터티입니다. 연결되지 않았거나 트래픽에 사용되지 않는 인터페이스에 대한 모니터는 비활성화해야 합니다. DOWN 상태인 인터페이스에서 모니터가 활성화되면 노드가 NOT UP(활성화되지 않음) 상태가 됩니다. 고가용성 구성에서 NOT UP(활성화되지 않음) 상태가 된 주 노드는 고가용성 장애 조치(failover)를 유발할 수 있습니다. 인터페이스는 다음 조건에서 DOWN(비활성화)으로 표시됩니다.

- 인터페이스가 연결되지 않은 상태입니다.
- 인터페이스가 제대로 작동하지 않습니다.
- 인터페이스를 연결하는 케이블이 제대로 작동하지 않습니다.

명령줄 인터페이스를 사용하여 사용되지 않는 인터페이스에 대한 고가용성 모니터를 비활성화하려면

명령 프롬프트에서 다음 명령을 입력하여 사용되지 않는 인터페이스에 대한 고가용성 모니터를 비활성화하고 해당 모니터가 비활성화되었는지 확인합니다.

- set interface -haMonitor OFF
- show interface
  예제:

  > set interface 1/8 -haMonitor OFF Done > show interface 1/8 Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2 flags=0x4000 MTU=1514, native vlan=1, MAC=00:d0:68:15:fd:3d, downti

  사용되지 않는 인터페이스에 대한 고가용성 모니터가 비활성화되면 해당 인터페이스에 대해 show interface 명령을 실행하면 결과에 "HAMON"이 포함되지 않습니다.

구성 유틸리티를 사용하여 사용되지 않는 인터페이스에 대한 고가용성 모니터를 비활성화하려면

1. System(시스템) > Network(네트워크) > Interfaces(인터페이스)로 이동합니다.
2. 모니터를 비활성화해야 하는 인터페이스를 선택합니다.
3. Open(열기)을 클릭합니다. Modify Interface(인터페이스 수정) 대화 상자가 나타납니다.
4. HA Monitoring(고가용성 모니터링)에서 OFF(꺼짐) 옵션을 선택합니다.
5. OK(확인)를 클릭합니다.
6. 인터페이스가 선택되어 있을 때 페이지 아래쪽에 있는 세부 정보에 "HA Monitoring: OFF(고가용성 모니터링: 꺼짐)"가 나타나는지 확인합니다.

처음으로 FIPS 장비 구성

Aug 30, 2016

인증서 키 쌍은 구성 유틸리티에 대한 HTTPS 액세스 및 보안 원격 프로시저 호출에 필요합니다. RPC 노드는 구성 및 세션 정보의 시스템 간 통신에 사용되는 내부 시스템 엔터티입니다. 하나의 RPC 노드는 각 장비에 존재합니다. 이 노드에는 암호가 저장되며 암호는 연결 중인 장비에서 제공하는 암호를 대상으로 확인됩니다. 다른 NetScaler 장비와 통신하려면 각 장비에는 다른 장비에서 인증하는 방법을 포함하여 다른 장비에 대한 정보가 필요합니다. RPC 노드에서는 이 정보를 유지관리하며 이 정보에는 다른 NetScaler 장비의 IP 주소 및 각 장비에 인증하기 위해 사용하는 암호가 포함됩니다.

NetScaler MPX 장비 가상 장비에서 인증서 키 쌍은 자동으로 내부 서비스에 바인딩됩니다. FIPS 장비에서는 인증서 키 쌍을 FIPS 카드의 HSM(하드웨어 보안 모듈)로 가져와야 합니다. 가져오기를 수행하려면 FIPS 카드를 구성하고 인증서 키 쌍을 만들어 내부 서비스에 바인딩해야 합니다.

명령줄 인터페이스를 사용하여 보안 HTTPS를 구성하려면

1. 장비의 FIPS 카드에서 HSM(하드웨어 보안 모듈)을 초기화합니다. HSM 초기화에 대한 자세한 사항은 "Configuring the HSM(HSM 구성)"의 내용을 참조하십시오.
2. 장비가 고가용성 설정의 일부인 경우, SIM을 활성화합니다. 기본 및 보조 장비에서 SIM 활성화에 대한 자세한 내용은 "Configuring FIPS Appliances in a High Availability Setup(고가용성 설정으로 FIPS 장비 구성)"을 참조하십시오.
3. FIPS 키를 장비의 FIPS 카드에 있는 HSM에 가져옵니다. 명령 프롬프트에서 다음을 입력하십시오.
   import ssl fipskey serverkey -key ns-server.key -informPEM
4. 인증서 키 쌍을 추가합니다. 명령 프롬프트에서 다음을 입력하십시오.
   add certkey server -cert ns-server.cert -fipskey serverkey
5. 이전 단계에서 만든 인증서 키를 다음 내부 서비스에 바인딩합니다. 명령 프롬프트에서 다음을 입력하십시오.
   bind ssl servicenshttps-127.0.0.1-443 -certkeyname server

   bind ssl servicenshttps-::11-443 -certkeyname server

구성 유틸리티를 사용하여 보안 HTTPS를 구성하려면

1. 장비의 FIPS 카드에서 HSM(하드웨어 보안 모듈)을 초기화합니다. HSM 초기화에 대한 자세한 사항은 "Configuring the HSM(HSM 구성)"의 내용을 참조하십시오.
2. 장비가 고가용성 설정의 일부인 경우, SIM(보안 정보 시스템)을 활성화합니다. 기본 및 보조 장비에서 SIM 활성화에 대한 자세한 사항은 "Configuring FIPS Appliances in a High Availability Setup(고가용성 설정으로 FIPS 장비 구성)"의 내용을 참조하십시오.
3. FIPS 키를 장비의 FIPS 카드에 있는 HSM에 가져옵니다. FIPS 키 가져오기에 대한 자세한 사항은 "Importing an Existing FIPS Key(기존 FIPS 키 가져오기)"의 내용을 참조하십시오.
4. Traffic Management(트래픽 관리) > SSL > Certificates(인증서)로 이동합니다.
5. 세부 정보 창에서 Install(설치)을 클릭합니다.
6. Install Certificate(인증서 설치) 대화 상자에서 인증서 세부 정보를 입력합니다.
7. Create(만들기)를 클릭한 다음 Close(닫기)를 클릭합니다.
8. Traffic Management(트래픽 관리) > Load Balancing(부하 분산) > Services(서비스)로 이동합니다.
9. 세부 정보 창의 Action(작업) 탭에서 Internal Services(내부 서비스)를 클릭합니다.
10. 목록에서 nshttps-127.0.0.1-443을 선택한 다음 Open(열기)을 클릭합니다.
11. Available(사용 가능) 창의 SSL Settings(SSL 설정) 탭에서, 7단계에서 만든 인증서를 선택하고 Add(추가)를 클릭한 다음 OK(확인)를 클릭합니다.

12. 목록에서 nshttps-::11-443을 선택한 다음 Open(열기)을 클릭합니다.
13. Available(사용 가능) 창의 SSL Settings(SSL 설정) 탭에서, 7단계에서 만든 인증서를 선택하고 Add(추가)를 클릭한 다음 OK(확인)를 클릭합니다.
14. OK(확인)를 클릭합니다.

명령줄 인터페이스를 사용하여 보안 RPC를 구성하려면

1. 장비의 FIPS 카드에서 HSM(하드웨어 보안 모듈)을 초기화합니다. HSM 초기화에 대한 자세한 사항은 "Configuring the HSM(HSM 구성)"의 내용을 참조하십시오.
2. SIM(보안 정보 시스템)을 활성화합니다. 기본 및 보조 장비에서 SIM 활성화에 대한 자세한 사항은 "Configuring FIPS Appliances in a High Availability Setup(고가용성 설정으로 FIPS 장비 구성)"의 내용을 참조하십시오.
3. FIPS 키를 장비의 FIPS 카드에 있는 HSM에 가져옵니다. 명령 프롬프트에서 다음을 입력하십시오.
   import ssl fipskey serverkey -key ns-server.key -informPEM
4. 인증서 키 쌍을 추가합니다. 명령 프롬프트에서 다음을 입력하십시오.
   add certkey server -cert ns-server.cert -fipskey serverkey
5. 인증서 키 쌍을 다음 내부 서비스에 바인딩합니다. 명령 프롬프트에서 다음을 입력하십시오.
   bind ssl servicensrpcs-127.0.0.1-3008 -certkeyname server

   bind ssl servicenskrpcs-127.0.0.1-3009 -certkeyname server

   bind ssl servicensrpcs-::1l-3008 -certkeyname server
6. 보안 RPC 모드를 활성화합니다. 명령 프롬프트에서 다음을 입력하십시오.
   set ns rpcnode -secure예

구성 유틸리티를 사용하여 보안 RPC를 구성하려면

1. 장비의 FIPS 카드에서 HSM(하드웨어 보안 모듈)을 초기화합니다. HSM 초기화에 대한 자세한 사항은 "Configuring the HSM(HSM 구성)"의 내용을 참조하십시오.
2. SIM(보안 정보 시스템)을 활성화합니다. 기본 및 보조 장비에서 SIM 활성화에 대한 자세한 사항은 "Configuring FIPS Appliances in a High Availability Setup(고가용성 설정으로 FIPS 장비 구성)"의 내용을 참조하십시오.
3. FIPS 키를 장비의 FIPS 카드에 있는 HSM에 가져옵니다. FIPS 키 가져오기에 대한 자세한 사항은 "Importing an Existing FIPS Key(기존 FIPS 키 가져오기)"의 내용을 참조하십시오.
4. Traffic Management(트래픽 관리) > SSL > Certificates(인증서)로 이동합니다.
5. 세부 정보 창에서 Install(설치)을 클릭합니다.
6. Install Certificate(인증서 설치) 대화 상자에서 인증서 세부 정보를 입력합니다.
7. Create(만들기)를 클릭한 다음 Close(닫기)를 클릭합니다.
8. Traffic Management(트래픽 관리) > Load Balancing(부하 분산) > Services(서비스)로 이동합니다.
9. 세부 정보 창의 Action(작업) 탭에서 Internal Services(내부 서비스)를 클릭합니다.
10. 목록에서 nsrpcs-127.0.0.1-3008을 선택한 다음 Open(열기)을 클릭합니다.
11. Available(사용 가능) 창의 SSL Settings(SSL 설정) 탭에서, 7단계에서 만든 인증서를 선택하고 Add(추가)를 클릭한 다음 OK(확인)를 클릭합니다.
12. 목록에서 nskrpcs-127.0.0.1-3009를 선택한 다음 Open(열기)을 클릭합니다.
13. Available(사용 가능) 창의 SSL Settings(SSL 설정) 탭에서, 7단계에서 만든 인증서를 선택하고 Add(추가)를 클릭한 다음 OK(확인)를 클릭합니다.
14. 목록에서 nsrpcs-::11-3008을 선택한 다음 Open(열기)을 클릭합니다.
15. Available(사용 가능) 창의 SSL Settings(SSL 설정) 탭에서, 7단계에서 만든 인증서를 선택하고 Add(추가)를 클릭한 다음 OK(확인)를 클릭합니다.

16. OK(확인)를 클릭합니다.
17. System(시스템) > Network(네트워크) > RPC로 이동합니다.
18. 세부 정보 창에서 IP 주소를 선택하고 Open(열기)을 클릭합니다.
19. Configure RPC Node(RPC 노드 구성) 대화 상자에서 Secure(보안)를 선택합니다.
20. OK(확인)를 클릭합니다.

일반적인 네트워크 토폴로지 이해

Aug 30, 2016

"물리적 배포 모드"에 설명된 대로 클라이언트와 서버 간의 인라인 모드나 단일 암 모드로 Citrix NetScaler 장비를 배포할 수 있습니다. 인라인 모드는 가장 일반적인 배포 유형인 이중 암 토폴로지를 사용합니다.

이 문서에는 다음이 포함되어 있습니다.

- 일반적인 Two-Arm 토폴로지 설정
- 일반적인 One-Arm 토폴로지 설정

일반적인 Two-Arm 토폴로지 설정

이중 암 토폴로지에서 한 네트워크 인터페이스는 클라이언트 네트워크에 연결되고 다른 네트워크 인터페이스는 서버 네트워크에 연결되므로 모든 트래픽이 장비를 통과합니다. 이 토폴로지의 경우 하드웨어를 다시 연결해야 할 수 있으므로 잠시 다운 시간이 발생할 수 있습니다. 이중 암 토폴로지는 기본적으로 다중 서브넷으로 공용 서브넷의 장비 및 사설 서브넷의 서버를 사용하는 방법과 투명 모드로 공용 네트워크에서 장비 및 서버를 모두 사용하는 방법으로 구분됩니다.

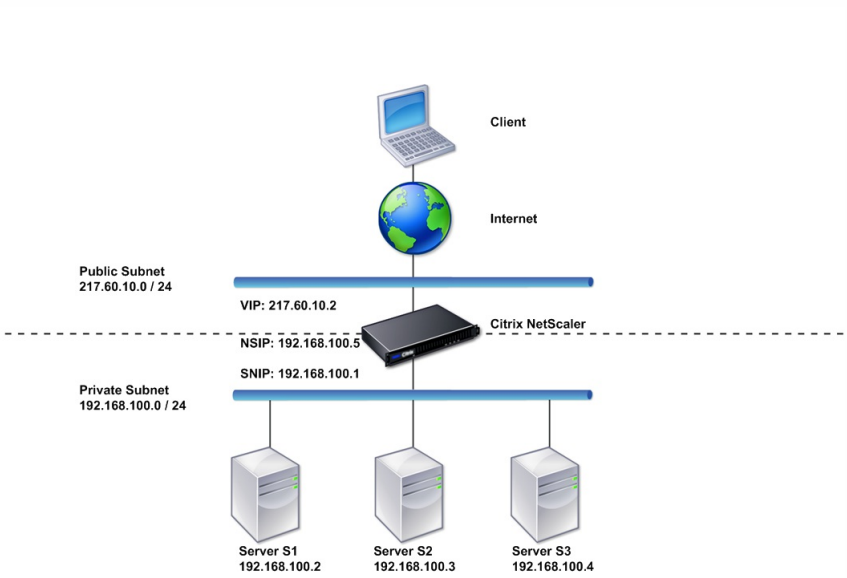
단순한 Two-Arm 다중 서브넷 토폴로지 설정

가장 일반적으로 사용되는 토폴로지 중 하나는 클라이언트와 서버 간의 NetScaler 장비 인라인 모드로, 클라이언트 요청을 처리하도록 가상 서버가 구성되어 있습니다. 이러한 구성은 클라이언트와 서버가 서로 다른 서브넷에 상주할 때 사용됩니다. 대부분의 경우 클라이언트와 서버는 각각 공용 서브넷과 사설 서브넷에 상주합니다.

예를 들어 장비에 HTTP 유형의 가상 서버가 구성되어 있고 서버에서 HTTP 서비스를 실행하고 있는 S1, S2, S3 서버를 관리하기 위해 이중 암 모드로 배포된 장비를 생각해 볼 수 있습니다. 서버는 사설 서브넷에 있으며, SNIP는 장비에서 서버와 통신하도록 구성됩니다. 장비에서 MIP 대신 SNIP를 사용하도록 USNIP(SNIP 사용) 옵션이 활성화되어야 합니다.

다음 그림에 나와 있는 대로 VIP는 공용 서브넷 217.60.10.0에 있고 NSIP, 서버 및 SNIP는 사설 서브넷 192.168.100.0/24에 있습니다.

그림 1. 이중 암 모드, 다중 서브넷에 대한 토폴로지 다이어그램



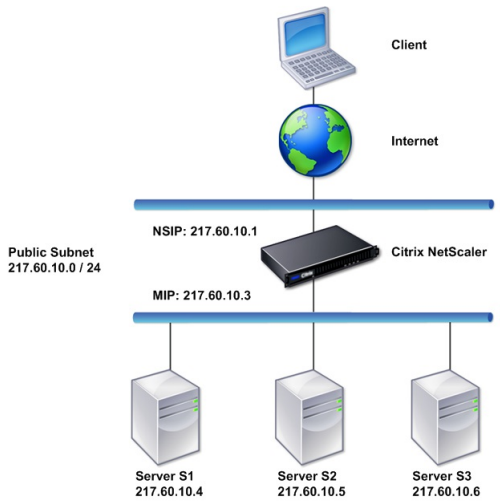
작업 개요: 이중 암 모드, 다중 서브넷에 NetScaler 장비를 배포하려면

1. "Configuring the NetScaler IP Address (NSIP)(NSIP(NetScaler IP 주소) 구성)"에 설명된 대로 NSIP 및 기본 게이트웨이를 구성합니다.
2. "Configuring Subnet IP Addresses(서브넷 IP 주소 구성)"에 설명된 대로 SNIP를 구성합니다.
3. "To enable or disable USNIP mode(USNIP 모드 활성화하거나 비활성화하려면)"에 설명된 대로 USNIP 옵션을 활성화합니다.
4. "Creating a Virtual Server(가상 서버 생성)" 및 "Configuring Services(서비스 구성)"에 설명된 대로 가상 서버 및 서비스를 구성합니다.
5. 네트워크 인터페이스 중 하나를 사설 서브넷에 연결하고, 다른 인터페이스를 공용 서브넷에 연결합니다.

단순한 Two-arm 투명 토폴로지 설정

클라이언트가 가상 서버의 개입 없이 직접 서버에 액세스해야 할 경우 투명 모드를 사용합니다. 서버 IP 주소는 클라이언트에서 액세스할 수 있어야 하므로 공용이어야 합니다. 다음 그림에 나와 있는 예제에서 NetScaler 장비는 클라이언트 및 서버 사이에 위치하므로 트래픽이 장비를 통과해야 합니다. 패킷 브리지를 위해 L2 모드를 활성화해야 합니다. NSIP 및 MIP는 동일한 공용 서브넷 217.60.10.0/24에 있습니다.

그림 2. Two-arm, 투명 모드에 대한 토폴로지 다이어그램



작업 개요: Two-arm 투명 모드로 NetScaler를 배포하려면

1. "Configuring a NetScaler by Using the Command Line Interface(명령줄 인터페이스를 사용하여 NetScaler 구성)"에 설명된 대로 NSIP, MIP 및 기본 게이트웨이를 구성합니다.
2. "L2 모드 활성화 및 비활성화"에 설명된 대로 L2 모드를 활성화합니다.
3. 관리대상 서버의 기본 게이트웨이를 MIP로 구성합니다.
4. 네트워크 인터페이스를 스위치의 해당 포트에 연결합니다.

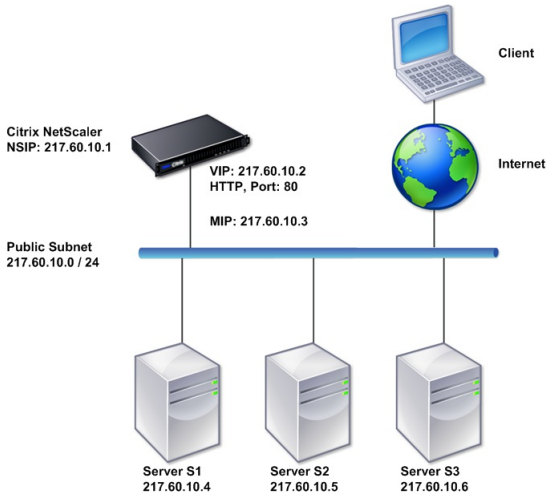
일반적인 One-Arm 토폴로지 설정

One-arm 토폴로지는 기본적으로 One-arm 단일 서브넷 토폴로지 및 One-arm 다중 서브넷 토폴로지로 적용됩니다.

단순한 One-arm 단일 서브넷 토폴로지 설정

클라이언트 및 서버가 동일한 서브넷에 있는 경우 One-arm 단일 서브넷 토폴로지를 사용할 수 있습니다. 예를 들어 S1, S2, S3 서버를 관리하기 위해 단일 암 모드로 배포된 NetScaler를 생각해 볼 수 있습니다. HTTP 유형의 가상 서버는 NetScaler에서 구성되고 HTTP 서비스는 서버에서 실행됩니다. 다음 그림에 표시된 대로 NetScaler IP 주소(NSIP), 매핑 IP 주소(MIP) 및 서버 IP 주소는 동일한 공용 서브넷 217.60.10.0/24에 있습니다.

그림 3. 단일 암 모드, 단일 서브넷에 대한 토폴로지 다이어그램



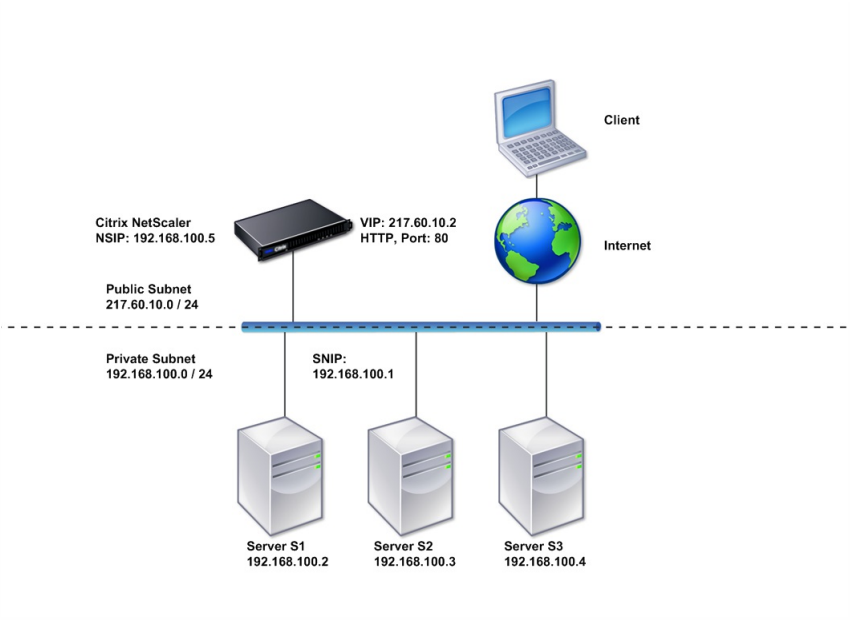
작업 개요: 단일 암 모드, 단일 서브넷에 NetScaler를 배포하려면

1. "Configuring the NetScaler IP Address (NSIP)(NSIP(NetScaler IP 주소) 구성)"에 설명된 대로 NSIP, MIP 및 기본 게이트웨이를 구성합니다.
2. "Creating a Virtual Server(가상 서버 생성)" 및 "Configuring Services(서비스 구성)"에 설명된 대로 가상 서버 및 서비스를 구성합니다.
3. 네트워크 인터페이스 중 하나를 스위치에 연결합니다.

단순한 One-Arm 다중 서브넷 토폴로지 설정

클라이언트와 서버가 서로 다른 서브넷에 있는 경우 One-arm 다중 서브넷 토폴로지를 사용할 수 있습니다. 예를 들어 네트워크의 스위치 SW1에 연결된 서버로 S1, S2, S3 서버를 관리하기 위해 단일 암 모드로 배포된 NetScaler 장비를 생각해 볼 수 있습니다. HTTP 유형의 가상 서버는 장비에서 구성되고 HTTP 서비스는 서버에서 실행됩니다. 이러한 세 서버는 사설 서브넷에 있으므로 서브넷 IP(SNIP) 주소는 이러한 서버와 통신하도록 구성됩니다. 장비가 MIP 대신 SNIP를 사용하도록 USNIP(서브넷 IP 주소 사용) 옵션이 활성화되어야 합니다. 다음 그림과 같이 가상 IP(VIP) 주소는 공용 서브넷 217.60.10.0/24에 있고, NSIP, SNIP 및 서버 IP 주소는 사설 서브넷 192.168.100.0/24에 있습니다.

그림 4. 단일 암 모드, 다중 서브넷에 대한 토폴로지 다이어그램



작업 개요: 단일 암 모드, 다중 서브넷에 NetScaler 장비를 배포하려면

1. "Configuring the NetScaler IP Address (NSIP)(NSIP(NetScaler IP 주소) 구성)"에 설명된 대로 NSIP 및 기본 게이트웨이를 구성합니다.
2. "Configuring Subnet IP Addresses(서브넷 IP 주소 구성)"에 설명된 대로 SNIP를 구성하고 USNIP 옵션을 활성화합니다.
3. "Creating a Virtual Server(가상 서버 생성)" 및 "Configuring Services(서비스 구성)"에 설명된 대로 가상 서버 및 서비스를 구성합니다.
4. 네트워크 인터페이스 중 하나를 스위치에 연결합니다.

시스템 관리 설정 구성

Aug 30, 2016

초기 구성을 완료한 후에는 여러 설정을 구성하여 Citrix NetScaler 장비의 동작을 정의하고 연결 관리 작업을 용이하게 할 수 있습니다. HTTP 요청 및 응답을 처리하기 위한 여러 옵션을 사용할 수 있습니다. 라우팅, 브리징, MAC 기반 전달 모드는 NetScaler로 주소가 지정되지 않은 패킷을 처리하는 데 사용할 수 있습니다. 네트워크 인터페이스의 특성을 정의할 수 있으며 해당 인터페이스를 집적할 수 있습니다. 타이밍 문제를 방지하기 위해 NetScaler 클럭을 NTP(Network Time Protocol) 서버와 동기화할 수 있습니다. NetScaler는 ADNS(Authoritative Domain Name Server)를 포함한 다양한 DNS 모드로 작동할 수 있습니다. 시스템 관리를 위해 SNMP를 설정할 수 있으며 시스템 이벤트의 syslog 로깅을 사용자 정의할 수 있습니다. 배포하기 전에 구성이 완전하고 올바른지 확인해야 합니다.

이 문서에는 다음이 포함되어 있습니다.

- 시스템 설정 구성
- 패킷 전달 모드 구성
- 네트워크 인터페이스 구성
- 시간 동기화 구성
- DNS 구성
- SNMP 구성
- 구성 확인

참고: 위에 나열된 작업 외에 Syslog 로깅을 구성할 수 있습니다. 이에 대한 지침은 “Audit Logging(감사 로깅)”을 참조하십시오.

시스템 설정 구성

Aug 30, 2016

시스템 설정 구성에는 연결 유지 및 서버 오프로드를 활성화하기 위한 HTTP 포트 구성, 각 서버의 최대 연결 수 설정 및 연결당 최대 요청 수 설정과 같은 기본적인 작업이 포함됩니다. 프록시 IP 주소가 적절하지 않은 상황을 위해 클라이언트 IP 주소 삽입 기능을 사용할 수 있으며 HTTP 쿠키 버전을 변경할 수 있습니다.

또한 데이터 연결을 위한 일시적인 포트 대신 제어된 범위의 포트에서 FTP 연결을 열도록 NetScaler 장비를 구성할 수도 있습니다. 방화벽에서 모든 포트를 열면 보안이 취약해지므로 이 경우 보안이 향상됩니다. 범위는 1,024부터 64,000 사이에서 원하는 대로 설정할 수 있습니다.

배포하기 전에 확인 체크리스트를 검토하여 구성을 확인합니다. HTTP 매개 변수 및 FTP 포트 범위를 구성하려면 NetScaler 구성 유틸리티를 사용합니다.

다음 표에 설명된 HTTP 매개 변수의 유형을 수정할 수 있습니다.

표 1. HTTP 매개 변수

매개 변수 유형	지정 대상
HTTP 포트 정보	관리되는 서버가 사용하는 웹 서버 HTTP 포트. 포트를 지정하면 장비가 지정된 포트와 일치하는 목적지 포트가 있는 클라이언트 요청에 대해 요청 교환을 수행합니다. 참고: 수신 클라이언트 요청이 장비에서 구체적으로 구성된 서비스나 가상 서버를 대상으로 하지 않을 경우 요청의 목적지 포트는 전역적으로 구성된 HTTP 포트 중 하나와 일치해야 합니다. 이를 통해 장비는 연결 유지 및 서버 오프로드를 수행할 수 있습니다.
제한	각 관리되는 서버에 대한 최대 연결 수 및 각각의 연결에서 전송되는 최대 요청 수. 예를 들어 Max Connections(최대 연결 수)를 500으로 설정하고 장비가 3개의 서버를 관리하는 중이라면 3개의 서버 각각에 대해 최대 500개의 연결을 열 수 있습니다. 기본적으로 장비는 관리하는 서버에 대해 연결을 무제한으로 생성할 수 있습니다. 연결당 요청 수를 무제한으로 지정하려면 Max Requests(최대 요청 수)를 0으로 설정합니다. 참고: Apache HTTP 서버를 사용하는 경우에는 Max Connections(최대 연결 수)를 Apache httpd.conf 파일의 MaxClients 매개 변수 값과 동일하게 설정해야 합니다. 다른 웹 서버의 경우 이 매개 변수 설정은 선택 사항입니다.
클라이언트 IP 삽입	클라이언트의 IP 주소를 HTTP 요청 헤더에 삽입하는 기능을 설정/해제합니다. 옆에 있는 텍스트 상자에 헤더 필드의 이름을 지정할 수 있습니다. 장비가 관리하는 웹 서버가 매핑 IP 주소 또는 서브넷 IP 주소를 수신하면 해당 서버는 이를 클라이언트의 IP 주소로 식별합니다. 일부 응용 프로그램에서는 로깅 목적으로 또는 웹 서버에서 제공할 콘텐츠를 동적으로 결정하기 위해 클라이언트의 IP 주소가 필요합니다. 클라이언트로부터 장비가 관리하는 하나, 일부 또는 모든 서버로 전송되는 HTTP 헤더 요청에 실제 클라이언트 IP 주소를 삽입할 수 있습니다. 그러면 서버에 대한 약간의 수정 작업을 통해 삽입된 주소에 액세스할 수 있습니다(Apache 모듈, ISAPI 인터페이스 또는 NSAPI 인터페이스 사용).
쿠키 버전	가상 서버에 COOKIEINSERT 지속성이 구성되어 있을 때 사용하는 HTTP 쿠키 버전입니다. 기본값인 버전 0이 인터넷에서 가장 일반적인 유형입니다. 또는 버전 1을 지정할 수도 있습니다.

매개 변수	지정 대상 특정 유형의 요청/응답을 처리하기 위한 옵션이며 HTTP 오류 응답의 로깅을 설정/해제합니다.
서버 헤더 삽입	NetScaler가 생성한 HTTP 응답에 서버 헤더를 삽입합니다.

구성 유틸리티를 사용하여 HTTP 매개 변수를 구성하려면

1. 탐색 창에서 System(시스템)을 확장하고 Settings(설정)를 클릭합니다.
2. 세부 정보 창의 Settings(설정)에서 Change HTTP parameters(HTTP 매개 변수 변경)를 클릭합니다.
3. Configure HTTP parameters(HTTP 매개 변수 구성) 대화 상자에서 위의 표에 나열된 머리글 아래에 나타나는 일부 또는 전체 매개 변수에 대해 값을 지정합니다.
4. OK(확인)를 클릭합니다.

구성 유틸리티를 사용하여 FTP 포트 범위를 설정하려면

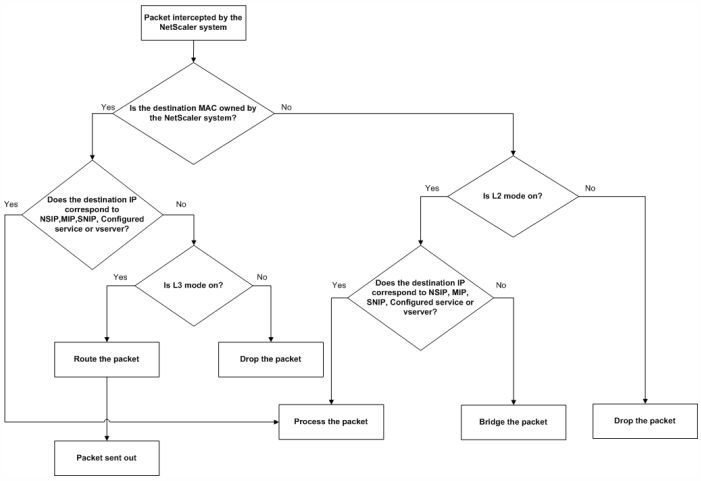
1. 탐색 창에서 System(시스템)을 확장하고 Settings(설정)를 클릭합니다.
2. 세부 정보 창의 Settings(설정)에서 Change global system settings(전역 시스템 설정 변경)를 클릭합니다.
3. FTP Port Range(FTP 포트 범위)의 Start Port(시작 포트) 및 End Port(끝 포트) 텍스트 상자에 지정하려는 범위에서 각각 가장 낮은 포트 번호 및 가장 높은 포트 번호를 입력합니다(예: 5000 및 6000).
4. OK(확인)를 클릭합니다.

패킷 전달 모드 구성

Aug 30, 2016

NetScaler 장비는 장비가 소유한 IP 주소로 향하지 않는 패킷(즉, 해당 IP 주소가 NSIP, MIP, SNIP, 구성된 서비스 또는 구성된 가상 서버가 아닌 경우)을 라우팅하거나 브리징할 수 있습니다. 기본적으로 L3 모드(라우팅)를 사용하고 L2 모드(브리징)를 사용하지 않지만 해당 구성을 변경할 수 있습니다. 다음 순서도에는 장비가 패킷을 평가한 후 이를 처리, 라우팅, 브리징 또는 삭제하는 방법이 나와 있습니다.

그림 1. L2 모드와 L3 모드 간 상호 작용



장비에서는 다음 모드를 사용하여 수신하는 패킷을 전달할 수 있습니다.

- L2 모드
- L3 모드
- MAC 기반 전달 모드

L2 모드 활성화 및 비활성화

업데이트 날짜: 2013년 09월 13일

L2 모드는 L2 전달(브리징) 기능을 제어합니다. 이 모드를 사용하여 NetScaler 장비가 L2 장치로 동작하고 NetScaler 장비를 대상으로 하지 않는 패킷을 브리징하도록 구성할 수 있습니다. 이 모드가 활성화되면 패킷이 장비의 인터페이스에 도달하고 각 인터페이스에는 고유의 MAC 주소가 있기 때문에 패킷은 MAC 주소로 전달되지 않습니다.

L2 모드가 비활성화되면(기본값) 장비는 해당 MAC 주소를 대상으로 하지 않는 패킷을 삭제합니다. 다른 L2 장치가 장비와 병렬로 설치된 경우 브리징(L2) 루프를 막기 위해 L2 모드를 비활성화해야 합니다. 구성 유틸리티 또는 명령줄을 사용하여 L2 모드를 활성화할 수 있습니다.

참고: 장비는 스패닝 트리 프로토콜을 지원하지 않습니다. 루프를 방지하려면 L2 모드를 활성화하는 경우 장비의 두 인터페이스를 동일한 브로드캐스트 도메인에 연결하지 마십시오.

명령줄 인터페이스를 사용하여 L2 모드를 활성화하거나 비활성화하려면

명령 프롬프트에서 다음 명령을 입력하여 L2 모드를 활성화/비활성화하고, L2 모드가 활성화/비활성화되었는지 확인합니다.

- enable ns mode
- disable ns mode
- show ns mode

예제

```
> enable ns mode l2  Done > show ns mode      Mode            Acronym     Status  -------         -------         ------ 1)  Fast Ramp        FR          ON  2)  Layer 2 mode    L2          ON  .
```

구성 유틸리티를 사용하여 L2 모드를 활성화 또는 비활성화하려면

1. 탐색 창에서 System(시스템)을 확장하고 Settings(설정)를 클릭합니다.
2. 세부 정보 창의 Modes and Features(모드 및 기능)에서 Configure modes(모드 구성)를 클릭합니다.
3. L2 모드를 활성화하려면 Configure Modes(모드 구성) 대화 상자에서 Layer 2 Mode(L2 모드) 확인란을 선택합니다. L2 모드를 비활성화하려면 확인란의 선택을 취소합니다.
4. OK(확인)를 클릭합니다. Enable/Disable Mode(s)?(모드를 활성화/비활성화하시겠습니까?) 메시지가 세부 정보 창에 나타납니다.
5. Yes(예)를 클릭합니다.

L3 모드 활성화 및 비활성화

업데이트 날짜: 2013년 09월 13일

L3 모드는 L3 전달 기능을 제어합니다. 이 모드를 사용하여 NetScaler 장비가 라우팅 테이블을 조회하고 NetScaler 장비를 대상으로 하지 않는 패킷을 전달하도록 구성할 수 있습니다. L3 모드가 활성화되면(기본값) 장비는 라우팅 테이블 조회를 수행하고 장비 소유 IP 주소를 대상으로 하지 않는 모든 패킷을 전달합니다. L3 모드를 비활성화할 경우 장비는 이러한 패킷을 삭제합니다.

명령줄 인터페이스를 사용하여 L3 모드를 활성화하거나 비활성화하려면

명령 프롬프트에서 다음 명령을 입력하여 L3 모드를 활성화/비활성화하고, L3 모드가 활성화/비활성화되었는지 확인합니다.

- enable ns mode
- disable ns mode
- show ns mode

예제

```
> enable ns mode l3  Done > show ns mode      Mode                Acronym     Status  -------             -------             ------ 1) Fast Ramp            FR          ON  2) Layer 2 mode         L2
```

구성 유틸리티를 사용하여 L3 모드를 활성화 또는 비활성화하려면

1. 탐색 창에서 System(시스템)을 확장하고 Settings(설정)를 클릭합니다.
2. 세부 정보 창의 Modes and Features(모드 및 기능)에서 Configure modes(모드 구성)를 클릭합니다.
3. L3 모드를 활성화하려면 Configure Modes(모드 구성) 대화 상자에서 Layer 3 Mode(IP Forwarding)(L3 모드(IP 전달)) 확인란을 선택합니다. L3 모드를 비활성화하려면 이 확인란의 선택을 취소합니다.
4. OK(확인)를 클릭합니다. Enable/Disable Mode(s)?(모드를 활성화/비활성화하시겠습니까?) 메시지가 세부 정보 창에 나타납니다.
5. Yes(예)를 클릭합니다.

MAC 기반 전달 모드 활성화 및 비활성화

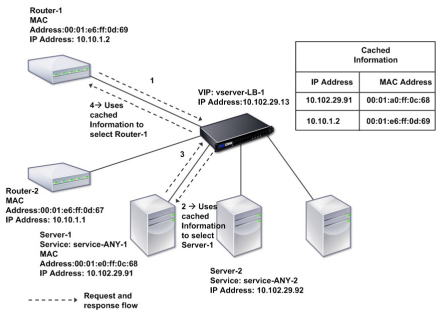
업데이트 날짜: 2013년 09월 13일

NetScaler 장비는 소스의 MAC 주소를 기억하므로 MAC 기반 전달을 사용하면 트래픽을 더욱 효율적으로 처리하고 패킷을 전달할 때 다중 라우팅 또는 ARP 조회를 피할 수 있습니다. 다중 조회를 피하기 위해 장비는 ARP 조회를 수행하는 모든 연결의 소스 MAC 주소를 캐시에 저장하고, 데이터를 동일한 MAC 주소에 반환합니다.

장비는 특정 VPN(가상 사설망)을 통해 흐르는 모든 트래픽이 동일한 VPN 장치를 통과하도록 하므로 MAC 기반 전달은 VPN 장치를 사용하는 경우 유용합니다.

다음 그림에서는 MAC 기반 전달 프로세스를 보여 줍니다.

그림 2. MAC 기반 전달 프로세스



MAC 기반 전달이 활성화되면 장비는 다음의 MAC 주소를 캐시에 저장합니다.

- 인바운드 연결 소스(라우터, 방화벽, VPN 장치 등의 전송 장치)
- 요청 응답 서버

서버가 장비를 통해 응답할 경우 장비는 응답 패킷의 대상 MAC 주소를 캐시에 저장된 주소로 설정하여 트래픽이 대칭으로 흐르도록 하고 응답을 클라이언트에 전달합니다. 이 프로세스는 라우팅 테이블 조회 및 ARP 조회 기능을 우회합니다. 하지만 장비에서 연결을 시작할 때는 조회 기능을 위해 라우팅 및 ARP 테이블을 사용합니다. MAC 기반 전달을 활성화하려면 구성 유틸리티 또는 명령줄을 사용합니다.

일부 배포에서는 수신 및 송신 경로가 서로 다른 라우터를 통해 흘러야 할 수 있습니다. 이러한 상황에서는 MAC 기반 전달이 토폴로지 설계를 무력화합니다. 수신 및 송신 경로가 서로 다른 라우터를 통해 흘러야 하는 GSLB(Global Server Load Balancing) 사이트의 경우, MAC 기반 전달을 비활성화하고 장비의 기본 라우터를 송신 라우터로 사용해야 합니다.

MAC 기반 전달이 비활성화되고 L2 또는 L3 연결이 활성화되면 라우팅 테이블에서 송신 및 수신 연결에 대해 별도의 라우터를 지정할 수 있습니다. MAC 기반 전달을 비활성화하려면 구성 유틸리티 또는 명령줄을 사용합니다.

명령줄 인터페이스를 사용하여 MAC 기반 전달을 활성화하거나 비활성화하려면

명령 프롬프트에서 다음 명령을 입력하여 MAC 기반 전달 모드를 활성화/비활성화하고, 해당 모드가 활성화/비활성화되었는지 확인합니다.

- enable ns mode
- disable ns mode
- show ns mode

예제:

```
> enable ns mode mbf  Done > show ns mode      Mode                Acronym     Status  -------             -------             ------ 1) Fast Ramp            FR          ON  2) Layer 2 mode         L2
```

구성 유틸리티를 사용하여 MAC 기반 전달을 활성화 또는 비활성화하려면

1. 탐색 창에서 System(시스템)을 확장하고 Settings(설정)를 클릭합니다.
2. 세부 정보 창의 Modes and Features(모드 및 기능) 그룹에서 Configure modes(모드 구성)를 클릭합니다.
3. MAC 기반 전달 모드를 활성화하려면 Configure Modes(모드 구성) 대화 상자에서 MAC Based Forwarding(MAC 기반 전달) 확인란을 선택합니다. MAC 기반 전달 모드를 비활성화하려면 확인란의 선택을 취소합니다.
4. OK(확인)를 클릭합니다. Enable/Disable Mode(s)?(모드를 활성화/비활성화하시겠습니까?) 메시지가 세부 정보 창에 나타납니다.
5. Yes(예)를 클릭합니다.

네트워크 인터페이스 구성

Sep 13, 2016

NetScaler 인터페이스는 슬롯/포트 표기법으로 번호가 지정됩니다. 사용자는 개별 인터페이스의 특성을 수정할 수 있을 뿐만 아니라 가상 LAN을 구성하여 특정 호스트 그룹에 대한 트래픽을 제한할 수 있습니다. 또한 링크를 고속 채널로 집적할 수도 있습니다.

Virtual LANs(가상 IP)

NetScaler는 (L2) 포트 및 IEEE802.1Q 태그 가상 LAN(VLAN)을 지원합니다. VLAN 구성은 트래픽을 특정 스테이션 그룹으로 제한해야 할 때 사용됩니다. IEEE 802.1q 태그를 사용하여 네트워크 인터페이스가 여러 VLAN에 속하도록 구성할 수 있습니다.

구성된 VLAN을 IP 서브넷에 바인딩할 수 있습니다. 그러면 NetScaler(서브넷의 호스트에 대한 기본 라우터로 구성된 경우)가 이러한 VLAN 간에 IP 전달을 수행합니다. NetScaler는 다음 유형의 VLAN을 지원합니다.

기본 VLAN

기본적으로 NetScaler의 네트워크 인터페이스는 단일 포트 기반 VLAN에 태그가 지정되지 않은 네트워크 인터페이스로 포함됩니다. 이 기본 VLAN의 VID는 1이며 영구적으로 존재하기에 삭제가 불가능하며 VID를 변경할 수 없습니다.

포트 기반 VLAN

공통의 배타적 L2 브로드캐스트 도메인을 공유하는 네트워크 인터페이스 집합이 포트 기반 VLAN의 멤버십을 정의합니다. 여러 포트 기반 VLAN을 구성할 수 있습니다. 인터페이스를 새 VLAN에 태그가 지정되지 않은 멤버로 추가하면 자동으로 기본 VLAN에서 제거됩니다.

태그가 지정된 VLAN

네트워크 인터페이스는 VLAN의 태그가 지정되거나 태그가 지정되지 않은 멤버가 될 수 있습니다. 각 네트워크 인터페이스는 한 VLAN만의 태그가 지정되지 않은 멤버(고유 VLAN)입니다. 태그가 지정되지 않은 네트워크 인터페이스는 고유 VLAN에 대한 프레임을 태그가 지정되지 않은 프레임으로 전달합니다. 태그된 네트워크 인터페이스는 둘 이상의 VLAN의 일부가 될 수 있습니다. 태그를 구성할 때 링크의 양 끝에 일치하는 VLAN 설정이 있는지 확인하십시오. 구성 유틸리티를 사용하여 VLAN의 태그된 멤버로 바인딩된 포트를 가질 수 있는 태그가 지정된 VLAN(nsvlan)을 정의할 수 있습니다. 이 VLAN을 구성하려면 NetScaler를 재부팅해야 하므로 초기 네트워크 구성 중 완료해야 합니다.

링크 집합 채널

링크 집합은 여러 포트에서 들어오는 데이터를 단일 고속 링크로 결합합니다. 링크 집합 채널을 구성하면 NetScaler와 연결된 다른 장치 간의 통신 채널 용량 및 가용성이 높아집니다. 집적된 링크를 채널이라고도 합니다.

네트워크 인터페이스가 채널에 바인딩되면 채널 매개 변수가 네트워크 인터페이스 매개 변수보다 우선합니다. 네트워크 인터페이스는 하나의 채널에만 바인딩할 수 있습니다. 네트워크 인터페이스를 링크 집합 채널에 바인딩하면 VLAN 구성이 변경됩니다. 즉, 네트워크 인터페이스를 채널에 바인딩하면 해당 인터페이스는 원래 속한 VLAN에서 제거되고 기본 VLAN에 추가됩니다. 하지만 채널을 다시 이전 VLAN이나 새 VLAN에 바인딩할 수 있습니다. 예를 들어, 네트워크 인터페이스 1/2 및 1/3을 ID 2인 VLAN에 바인딩한 다음 링크 집합 채널 LA/1에 바인딩할 경우 네트워크 인터페이스는 기본 VLAN으로 이동하지만 다시 VLAN 2에 바인딩할 수 있습니다.

참고: 또한 LACP(Link Aggregation Control Protocol)를 사용하여 링크 집합을 구성할 수도 있습니다. 자세한 내용은 "Configuring Link Aggregation by Using the Link Aggregation Control Protocol(LACP를 사용하여 링크 집합 구성)"을 참조하십시오.

시간 동기화 구성

Aug 30, 2016

NetScaler 장비가 NTP(Network Time Protocol) 서버의 로컬 시간과 동기화되도록 구성할 수 있습니다. 그러면 NetScaler가 네트워크의 다른 서버와 동일한 날짜 및 시간 설정을 가지게 됩니다. NTP에서는 UDP(User Datagram Protocol) 포트 123을 전송 계층으로 사용합니다. NTP 구성 파일에 NTP 서버를 추가하여 장비가 이러한 서버에서 정기적으로 업데이트를 받도록 해야 합니다.

로컬 NTP 서버가 없는 경우 공식 NTP 사이트(http://www.ntp.org)에서 공개 액세스 NTP 서버 목록을 확인할 수 있습니다.

장비에서 클럭 동기화를 구성하려면

1. 명령줄에 로그온한 다음셸 명령을 사용합니다.
2. 셸 프롬프트에서 /etc 디렉터리의 ntp.conf 파일을 /nsconfig 디렉터리로 복사합니다. 해당 파일이 /nsconfig 디렉터리에 이미 있는 경우 ntp.conf 파일에서 다음 항목을 제거해야 합니다.
   restrict localhost

   restrict 127.0.0.2

   이러한 항목은 장치를 시간 서버로 실행하는 경우에만 필요합니다. 그러나 이 기능은 NetScaler에서 지원되지 않습니다.
3. /nsconfig/ntp.conf를 편집하여 파일의 서버 및 제한 항목 아래에 원하는 NTP 서버에 대한 IP 주소를 입력합니다.
4. /nsconfig 디렉터리에 이름이 rc.netscaler인 파일이 없는 경우 해당 파일을 만듭니다.
5. /nsconfig/rc.netscaler를 편집하여 다음 항목을 추가합니다./usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log &
   이 항목은 ntpd 서비스를 시작하고 ntp.conf 파일을 확인하며 /var/log 디렉터리에 메시지를 로깅합니다.

   참고: NetScaler와 시간 서버 간의 시간 차이가 1000초를 초과할 경우 ntpd 서비스가 종료되고 NetScaler 로그에 메시지가 기록됩니다. 이러한 상황을 방지하려면 강제로 시간을 동기화하는 -g 옵션을 사용하여 ntpd를 시작해야 합니다. 다음 항목을 /nsconfig/rc.netscaler에 추가합니다.
   /usr/sbin/ntpd -g -c /nsconfig/ntp.conf -l /var/log/ntpd.log &

   시간 차이가 클 때 강제로 시간을 동기화하지 않으려는 경우 날짜를 수동으로 설정한 다음 ntpd를 다시 시작하면 됩니다. 셸에서 다음 명령을 실행하여 장비와 시간 서버 간의 시간 차이를 확인할 수 있습니다.

   ntpdate -q
6. 장비를 재부팅하여 시간 동기화를 활성화합니다.
   참고: 장비를 다시 시작하기 전에 시간 동기화를 시작하려면 5단계에서 rc.netscaler 파일에 추가한 다음 명령을 셸 프롬프트에 입력합니다.
   /usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ ntpd.log &

DNS 구성

Aug 30, 2016

NetScaler 장비가 ADNS(Authoritative Domain Name Server), DNS 프록시 서버, 최종 확인 장치 또는 전달 장치로 작동하도록 구성할 수 있습니다. SRV 레코드, AAAA 레코드, A 레코드, MX 레코드, NS 레코드, CNAME 레코드, PTR 레코드, SOA 레코드 등의 DNS 리소스 레코드를 추가할 수 있습니다. 또한 장비는 외부 DNS 서버에 대한 부하를 분산시킬 수 있습니다.

일반적으로 장비를 전달 장치로 구성합니다. 이 구성의 경우 외부 네임 서버를 추가해야 합니다. 외부 서버를 추가한 후에는 구성이 올바른지 확인해야 합니다.

외부 네임 서버를 추가, 제거, 활성화 및 비활성화할 수 있습니다. 해당 IP 주소를 지정하여 네임 서버를 만들거나 기존 가상 서버를 네임 서버로 구성할 수 있습니다.

네임 서버를 추가할 때 IP 주소 또는 가상 IP 주소(VIP)를 지정할 수 있습니다. IP 주소를 사용할 경우 장비는 구성된 네임 서버에 라운드 로빈 방식으로 요청 부하를 분산시킵니다. VIP를 사용할 경우에는 원하는 부하 분산 방식을 지정할 수 있습니다.

명령줄 인터페이스를 사용하여 네임 서버를 추가하려면

명령 프롬프트에서 다음 명령을 입력하여 네임 서버를 추가하고 구성을 확인합니다.

- add dns nameServer
- show dns nameServer

예제:

```
> add dns nameServer 10.102.29.10  Done > show dns nameServer 10.102.29.10 1)      10.102.29.10  -  State: DOWN  Done >
```

구성 유틸리티를 사용하여 네임 서버를 추가하려면

1. Traffic Management(트래픽 관리) > DNS > Name Servers(네임 서버)로 이동합니다.
2. 세부 정보 창에서 Add(추가)를 클릭합니다.
3. Create Name Server(네임 서버 만들기) 대화 상자에서 IP Address(IP 주소)를 선택합니다.
4. IP Address(IP 주소) 텍스트 상자에 네임 서버의 IP 주소를 입력합니다(예:10.102.29.10). 외부 네임 서버를 추가하는 경우 Local(로컬) 확인란의 선택을 취소합니다.
5. Create(만들기)를 클릭한 다음 Close(닫기)를 클릭합니다.
6. 추가한 네임 서버가 Name Servers(네임 서버) 창에 표시되는지 확인합니다.

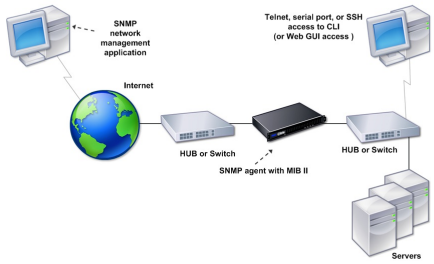
SNMP 구성

Aug 30, 2016

외부 컴퓨터에서 실행되는 SNMP(Simple Network Management Protocol) 네트워크 관리 애플리케이션은 NetScaler의 SNMP 에이전트에 쿼리합니다. 에이전트는 네트워크 관리 애플리케이션에서 요청한 MIB를 검색하고 데이터를 애플리케이션에 보냅니다.

SNMP 모니터링에서는 트랩 메시지 및 경보를 사용합니다. SNMP 트랩 메시지는 에이전트가 비정상 조건을 알리기 위해 생성하는 비동기 이벤트로서 경보로 표시됩니다. 예를 들어 CPU 활용률이 90%를 초과할 때 알림을 받고자 하는 경우 해당 조건에 대한 경보를 설정할 수 있습니다. 다음 그림에서는 SNMP가 활성화되고 구성된 NetScaler 네트워크를 보여 줍니다.

그림 1. NetScaler의 SNMP



NetScaler의 SNMP 에이전트는 SNMP 버전 1(SNMPv1), SNMP 버전 2(SNMPv2) 및 SNMP 버전 3(SNMPv3)을 지원합니다. 에이전트는 이중 언어 모드로 작동하므로 SNMPv2 쿼리(Get-Bulk 등) 및 SNMPv1 쿼리를 처리할 수 있습니다. 또한 SNMP 에이전트는 SNMPv2와 호환되는 트랩을 전송하고, SNMPv2 데이터 유형(counter64 등)을 지원합니다. SNMPv1 매니저(NetScaler에서 SNMP 정보를 요청하는 다른 서버의 프로그램)는 SNMP 쿼리를 처리할 때 NS-MIB-smiv1.mib 파일을 사용합니다. SNMPv2 매니저는 NS-MIB-smiv2.mib 파일을 사용합니다.

NetScaler는 다음의 엔터프라이즈별 MIB를 지원합니다.

표준 MIB-2 그룹의 하위 집합

MIB-2 그룹 SYSTEM, IF, ICMP, UDP 및 SNMP를 제공합니다.

시스템 엔터프라이즈 MIB

시스템별 구성 및 통계를 제공합니다.

SNMP를 구성하려면 SNMP 에이전트를 쿼리할 수 있는 관리자를 지정하고, SNMP 트랩 메시지를 받을 SNMP 트랩 수신기를 추가한 다음 SNMP 경보를 구성합니다.

SNMP 관리자 추가

업데이트 날짜: 2013년 06월 05일

SNMP 버전 1, 2, 3과 호환되는 관리 응용 프로그램을 실행하는 워크스테이션에서 장비에 액세스하도록 구성할 수 있습니다. 이러한 워크스테이션을 SNMP 관리자라고 합니다. 장비에 SNMP 관리자를 지정하지 않을 경우 장비는 네트워크의 모든 IP 주소에 대해 SNMP 쿼리를 허용하고 응답을 보냅니다. 하나 이상의 SNMP 관리자를 구성할 경우 장비는 특정 IP 주소의 SNMP 쿼리만 허용하고 응답을 보냅니다. SNMP 관리자의 IP 주소를 지정할 경우 넷마스크 매개 변수를 사용하여 전체 서브넷에서 액세스를 허용할 수 있습니다. 최대 100개의 SNMP 관리자 또는 네트워크를 추가할 수 있습니다.

명령줄 인터페이스를 사용하여 SNMP 관리자를 구성하려면

명령 프롬프트에서 다음 명령을 입력하여 SNMP 관리자를 추가하고 구성을 확인합니다.

- add snmp manager ... [-netmask]
- show snmp manager

예제:

```
> add snmp manager 10.102.29.5 -netmask 255.255.255.255  Done > show snmp manager 10.102.29.5 1)     10.102.29.5        255.255.255.255  Done >
```

구성 유틸리티를 사용하여 SNMP 관리자를 추가하려면

1. 탐색 창에서 System(시스템), SNMP를 차례로 확장하고 Managers(관리자)를 클릭합니다.
2. 세부 정보 창에서 Add(추가)를 클릭합니다.
3. Add SNMP Manager(SNMP 관리자 추가) 대화 상자에서 IP Address(IP 주소) 텍스트 상자에 관리 응용 프로그램이 실행되는 워크스테이션의 IP 주소를 입력합니다(예:10.102.29.5).
4. Create(만들기)를 클릭한 다음 Close(닫기)를 클릭합니다.
5. 방금 추가한 SNMP 관리자가 창 아래쪽의 Details(세부 정보) 섹션에 표시되는지 확인합니다.

SNMP 트랩 수신기 추가

업데이트 날짜: 2013년 09월 13일

경보를 구성한 후에는 장비에서 트랩 메시지를 보낼 트랩 수신기를 지정해야 합니다. 트랩 수신기의 IP 주소 및 목적지 포트와 같은 매개 변수를 지정하는 것과 별도로 트랩 유형(일반 또는 특정) 및 SNMP 버전을 지정할 수 있습니다.

일반 또는 특정 트랩을 받을 트랩 수신기를 최대 20개 구성할 수 있습니다.

명령줄 인터페이스를 사용하여 SNMP 트랩 수신기를 추가하려면

명령 프롬프트에서 다음 명령을 입력하여 SNMP 트랩을 추가한 다음 제대로 추가되었는지 확인합니다.

- add snmp trap specific
- show snmp trap

예제:

```
> add snmp trap specific 10.102.29.3  Done > show snmp trap Type    DestinationIP   DestinationPort  Version  SourceIP    Min-Severity  Community ----    -------------  ---------------  -------  --------    ---------
```

구성 유틸리티를 사용하여 SNMP 트랩 수신기를 추가하려면

1. 탐색 창에서 System(시스템), SNMP를 차례로 확장하고 Traps(트랩)를 클릭합니다.
2. 세부 정보 창에서 Add(추가)를 클릭합니다.
3. Create SNMP Trap Destination(SNMP 트랩 대상 만들기) 대화 상자에서 Destination IP Address(목적지 IP 주소) 텍스트 상자에 IP 주소를 입력합니다(예:10.102.29.3).
4. Create(만들기)를 클릭한 다음 Close(닫기)를 클릭합니다.
5. 방금 추가한 SNMP 트랩이 창 아래쪽의 Details(세부 정보) 섹션에 표시되는지 확인합니다.

SNMP 경보 구성

업데이트 날짜: 2013년 09월 13일

경보를 구성하여 경보 중 하나에 해당하는 이벤트가 발생할 때 장비가 트랩 메시지를 생성하도록 할 수 있습니다. 경보를 구성하는 작업은 경보를 사용하도록 설정하는 작업과 트랩이 생성되는 심각도 수준을 설정하는 작업으로 구성됩니다. 심각도 수준에는 중요, Major(다소 중요), Minor(사소), 경고, Informational(정보) 등 다섯 가지 수준이 있습니다. 트랩은 경보 심각도가 트랩에 대해 지정된 심각도와 일치할 경우에만 전송됩니다.

일부 경보는 기본적으로 활성화됩니다. SNMP 경보를 비활성화하면 해당하는 이벤트가 발생해도 장비에서 트랩 메시지를 생성하지 않습니다. 예를 들어, Login-Failure SNMP 경보를 비활성화하면 로그인 실패가 발생할 경우 장비에서 트랩 메시지를 생성하지 않습니다.

명령줄 인터페이스를 사용하여 경보를 활성화하거나 비활성화하려면

명령 프롬프트에서 다음 명령을 입력하여 경보를 활성화하거나 비활성화하고 해당 경보가 활성화 또는 비활성화되었는지 확인합니다.

- set snmp alarm [-state ENABLED | DISABLED]
- show snmp alarm

예제:

```
> set snmp alarm LOGIN-FAILURE -state ENABLED  Done > show snmp alarm LOGIN-FAILURE    Alarm          Alarm Threshold  Normal Threshold  Time  State    Severity   Logging  -----          --------
```

명령줄 인터페이스를 사용하여 경보 심각도를 설정하려면

명령 프롬프트에서 다음 명령을 입력하여 경보의 심각도를 설정하고 해당 경보 심각도가 올바르게 설정되었는지 확인합니다.

- set snmp alarm [-severity]
- show snmp alarm

예제:

```
> set snmp alarm LOGIN-FAILURE -severity Major  Done > show snmp alarm LOGIN-FAILURE    Alarm          Alarm Threshold  Normal Threshold  Time  State    Severity   Logging  -----          ----------
```

구성 유틸리티를 사용하여 경보를 구성하려면

1. 탐색 창에서 System(시스템), SNMP를 차례로 확장한 다음 Alarms(경보)를 클릭합니다.
2. 세부 정보 창에서 경보(예: LOGIN-FAILURE)를 선택한 다음 Open(열기)을 클릭합니다.
3. 경보를 사용하려면 Configure SNMP Alarm(SNMP 경보 구성) 대화 상자의 State(상태) 드롭다운 목록에서 Enabled(사용)를 선택합니다. 경보를 사용하지 않으려면 Disabled(사용 안 함)를 선택합니다.
4. Severity(심각도) 드롭다운 목록에서 심각도 옵션(예: Major(다소 중요))을 선택합니다.
5. OK(확인)를 클릭한 다음 Close(닫기)를 클릭합니다.
6. 창 아래쪽의 Details(세부 정보) 섹션에서 구성한 SNMP 경보의 매개 변수가 올바르게 구성되었는지 확인합니다.

구성 확인

Aug 30, 2016

시스템 구성을 완료한 후 다음 체크리스트를 보고 구성을 확인하십시오.

구성 체크리스트

- 실행 중인 빌드:
- 비호환성 문제가 없습니다. (비호환성 문제는 해당 빌드의 릴리스 정보에 나와 있습니다.)
- 포트 설정(속도, 이중, 흐름 컨트롤, 모니터링)이 스위치의 포트와 동일합니다.
- 피크 시간 중 모든 서버측 연결을 지원하도록 매핑 IP 주소가 충분히 구성되었습니다.
  - 구성된 매핑 IP 주소 수: _____
  - 예상되는 동시 서버 연결 수:
    [ ] 62,000 [ ] 124,000 [ ] 기타_____

토폴로지 구성 체크리스트

- 다른 서브넷의 서버 확인을 위한 경로가 사용되었습니다.

  입력된 경로:

  _____

- NetScaler가 공개-사설 토폴로지에 있는 경우 리버스 NAT가 구성되었습니다.
- NetScaler에서 구성된 장애 복구(HA) 설정이 One-arm 또는 Two-arm 구성에서 확인됩니다. 비활성화되어 사용되지 않는 모든 네트워크 인터페이스:

  _____

- NetScaler가 외부 부하 분산 장치 뒤에 배치된 경우 외부 부하 분산 장치의 부하 분산 정책은 "최소 연결"이 아닙니다.
  외부 부하 분산 장치에서 구성된 부하 분산 정책:

  _____

- NetScaler가 방화벽 앞에 배치된 경우 방화벽에 대한 세션 시간 초과가 300초 이상의 값으로 설정되었습니다.
  참고: NetScaler 장비에서 TCP 유휴 연결 시간 초과는 360초입니다. 방화벽의 시간 초과도 300초 이상으로 설정되어 있으면 연결이 일찍 닫히지 않기 때문에 장비에서 TCP 연결 멀티플렉싱을 효과적으로 수행할 수 있습니다.
  세션 시간 초과에 대해 구성된 값: _____

서버 구성 체크리스트

- 모든 서버에서 "연결 유지"가 활성화되었습니다.
  연결 유지 시간 초과에 대해 구성된 값: _____

- 기본 게이트웨이가 올바른 값으로 설정되었습니다. (기본 게이트웨이는 NetScaler 또는 업스트림 라우터여야 합니다.) 기본 게이트웨이:

  _____

- 서버 포트 설정(속도, 이중, 흐름 컨트롤, 모니터링)이 스위치 포트 설정과 동일합니까?

  _____

- Microsoft® Internet Information Server가 사용되는 경우 서버에서 버퍼링이 활성화되었습니다.

- Apache Server가 사용되는 경우 MaxConn(최대 연결 수) 매개변수가 서버 및 NetScaler에서 구성되었습니다.
  설정된 MaxConn(최대 연결 수) 값:

  _____

- Netscape® Enterprise Server™가 사용되는 경우 연결당 최대 요청 수 매개 변수가 NetScaler에서 설정되었습니다. 설정된 연결당 최대 요청 값:

  _____

소프트웨어 기능 구성 체크리스트

- L2 Mode 기능을 비활성화해야 합니까? (다른 2계층 장치가 NetScaler와 병렬로 작동하는 경우 비활성화하십시오.)
  활성화 또는 비활성화해야 하는 이유:

  _____

- MAC 기반 전달 기능을 비활성화해야 합니까? (반환 트래픽에서 사용되는 MAC 주소가 다른 경우 비활성화해야 합니다.)
  활성화 또는 비활성화해야 하는 이유:

  _____

- 호스트 기반 재사용을 비활성화해야 합니까? (서버에 가상 호스팅이 있습니까?)
  활성화 또는 비활성화해야 하는 이유:

  _____

- 과부하 보호 기능의 기본 설정을 변경해야 합니까?
  변경하거나 변경하지 않아야 하는 이유:

  _____

액세스 체크리스트

- 클라이언트측 네트워크에서 시스템 IP에 대해 Ping을 수행할 수 있습니다.
- 서버측 네트워크에서 시스템 IP에 대해 Ping을 수행할 수 있습니다.
- NetScaler를 통해 관리대상 서버에 대해 Ping을 수행할 수 있습니다.
- 관리대상 서버에서 인터넷 호스트에 대해 Ping을 수행할 수 있습니다.
- 브라우저를 통해 관리대상 서버에 액세스할 수 있습니다.
- 브라우저를 사용하여 관리대상 서버에서 인터넷에 액세스할 수 있습니다.
- SSH를 사용하여 시스템에 액세스할 수 있습니다.
- 모든 관리대상 서버에 대한 관리자 액세스가 가능합니다.

참고: Ping 유틸리티를 사용하는 경우 Ping 대상 서버에 ICMP ECHO가 활성화되어 있는지 확인하십시오. 그렇지 않으면 Ping에 실패합니다.

방화벽 체크리스트

다음 방화벽 요구 사항을 충족했습니다.

- UDP 161(SNMP)
- UDP 162(SNMP 트랩)
- TCP/UDP 3010(GUI)
- HTTP 80(GUI)

- TCP 22(SSH)

NetScaler 장비에서 트래픽 부하 분산

Aug 30, 2016

부하 분산 기능은 클라이언트 요청을 여러 서버에 걸쳐 분산시켜 리소스 활용률을 최적화합니다. 제한된 수의 서버가 많은 클라이언트에 서비스를 제공하는 실제 환경에 바탕을 둔 시나리오에서는 서버에 오버로드가 발생하여 서버 팜 성능이 저하될 수 있습니다. Citrix NetScaler 장비는 요청이 수신되면 각 클라이언트 요청을 가장 잘 처리할 수 있는 서버에 전달함으로써 병목 현상을 막을 수 있도록 부하 분산 기준을 사용합니다.

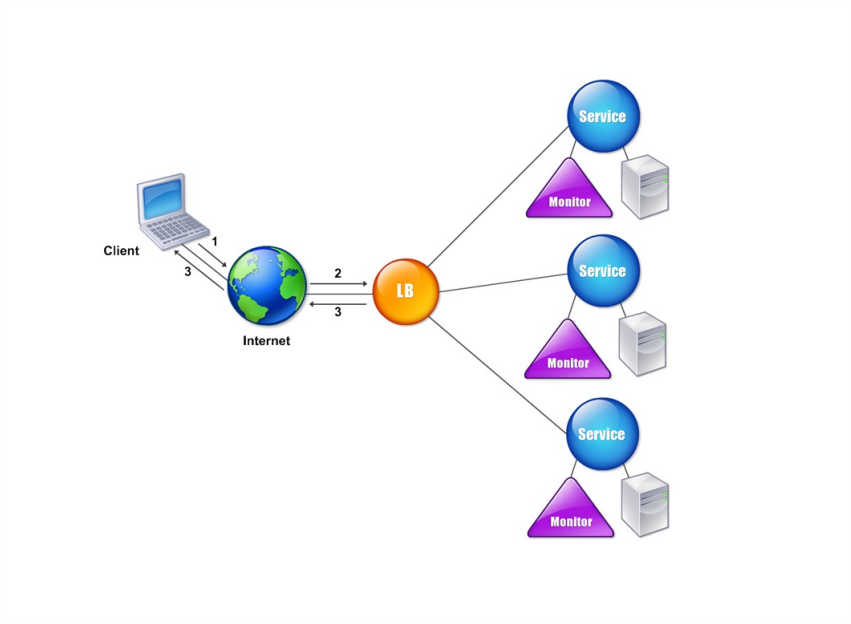
부하 분산을 구성하려면 서버 팜에서 여러 서버를 프록시할 가상 서버를 정의하고 이러한 서버 간에 부하를 분산시킵니다.

클라이언트가 서버 연결을 초기화할 때 가상 서버는 클라이언트 연결을 종료하고 선택된 서버에 대한 연결을 새로 시작하거나 기존 연결을 다시 사용하여 부하 분산을 수행합니다. 부하 분산 기능은 L4(TCP 및 UDP)에서 L7(FTP, HTTP 및 HTTPS)까지 트래픽 관리를 제공합니다.

NetScaler 장비는 부하 분산 방식이라는 여러 가지 알고리즘을 사용하여 서버 간에 부하를 분산시킬 방법을 결정합니다. 기본 부하 분산 방식은 최소 연결 방식입니다.

일반적인 부하 분산 배포는 다음 그림에 설명된 엔터티로 구성됩니다.

그림 1. 부하 분산 아키텍처



엔터티는 다음과 같이 동작합니다.

- **Virtual server(가상 서버)**. IP 주소, 포트 및 프로토콜로 나타내는 엔터티입니다. 가상 서버 IP 주소(VIP)는 대개 공용 IP 주소입니다. 클라이언트는 이 IP 주소에 연결 요청을 보냅니다. 가상 서버는 서버 모음을 나타냅니다.
- **Service(서비스)**. 서버 또는 서버에서 실행되는 응용 프로그램의 논리적 표현입니다. 서버의 IP 주소, 포트 및 프로토콜을 나타냅니다. 서비스는 가상 서버에 바인드됩니다.
- **Server object(서버 개체)**. IP 주소로 나타내는 엔터티입니다. 서버 개체는 서비스를 생성할 때 생성됩니다. 서비스의 IP 주소는 서버 개체의 이름으로 사용됩니다. 서버 개체를 생성한 다음 서버 개체를 사용하여 서비스를 생성할 수도 있습니다.
- **Monitor(모니터)**. 서비스의 상태를 추적하는 엔터티입니다. 장비는 각 서비스에 바인드된 모니터를 사용하여 정기적으로 서버를 점검합니다. 서버가 지정된 응답 시간 초과 이내에 응답하지 않고 지정된 점검 수를 실패할 경우 서비스는 DOWN(작동

중지)으로 표시됩니다. 그러면 장비가 나머지 서비스 간에 부하 분산을 수행합니다.

부하 분산 구성

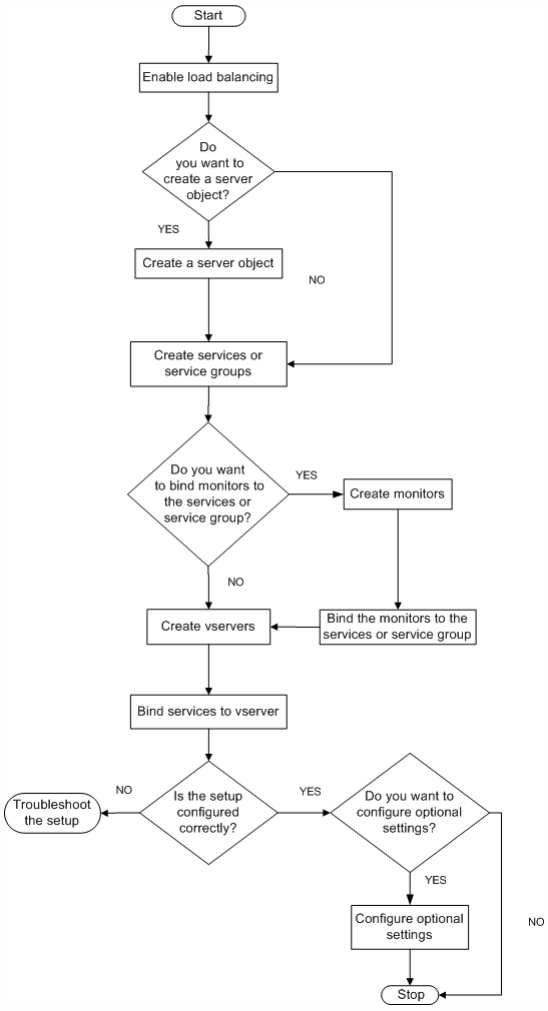
Aug 30, 2016

부하 분산을 구성하려면 먼저 서비스를 생성해야 합니다. 그런 다음 가상 서버를 만들고 서비스를 가상 서버에 바인딩합니다. 기본적으로 NetScaler 장비는 모니터를 각 서비스에 바인딩합니다. 서비스를 바인딩한 후 모든 설정이 올바른지 검토하여 구성을 확인합니다.

참고: 구성을 배포한 후 구성의 엔터티가 작동하는 현황을 보여 주는 통계를 표시할 수 있습니다. 통계 유틸리티를 사용하거나stat lb vserver 명령을 사용합니다.
선택적으로 서비스에 가중치를 할당할 수도 있습니다. 그러면 부하 분산 방식에서 할당된 가중치를 사용하여 서비스를 선택하게 됩니다. 그러나 구성을 처음 시작하는 경우에는 특정 서버와의 연결을 유지해야 하는 세션에 대해 몇몇 기본적인 지속성 설정 및 구성 보호 설정만을 구성하도록 작업을 선택적으로 제한할 수 있습니다.

다음 순서도에는 구성 작업의 순서가 나와 있습니다.

그림 1. 부하 분산 구성을 위한 작업 순서



부하 분산 활성화

업데이트 날짜: 2013년 06월 05일

부하 분산을 구성하려면 먼저 부하 분산 기능을 활성화해야 합니다.

명령줄 인터페이스를 사용하여 부하 분산을 활성화하려면

명령 프롬프트에서 다음 명령을 입력하여 부하 분산을 활성화하고 해당 기능이 활성화되어 있는지 확인합니다.

- enable feature lb
- show feature

예제:

```
> enable feature lb  Done > show feature      Feature              Acronym      Status
-------              -------      ------ 1) Web Logging          WL           OFF  2) Surge Protection    SP           O
```

구성 유틸리티를 사용하여 부하 분산을 활성화하려면

1. 탐색 창에서 System(시스템)을 확장하고 Settings(설정)를 클릭합니다.
2. 세부 정보 창의 Modes and Features(모드 및 기능)에서 Change basic features(기본 기능 변경)를 클릭합니다.
3. Configure Basic Features(기본 기능 구성) 대화 상자에서 Load Balancing(부하 분산) 확인란을 선택하고 OK(확인)를 클릭합니다.
4. Enable/Disable Feature(s)?(기능을 활성화/비활성화하시겠습니까?) 메시지에서 Yes(예)를 클릭합니다.

서비스 및 가상 서버 구성

업데이트 날짜: 2013년 06월 24일

부하를 분산할 서비스를 식별하고 나면 서비스 개체를 만들고 부하 분산 가상 서버를 만든 다음 서비스 개체를 가상 서버에 바인딩하는 방식으로 초기 부하 분산 구성을 구현할 수 있습니다.

명령줄 인터페이스를 사용하여 초기 부하 분산 구성을 구현하려면

명령 프롬프트에서 다음 명령을 입력하여 초기 구성을 구현하고 확인합니다.

- add service
- add lb vserver [ ]
- bind lb vserver
- show service bindings

예제:

```
> add service service-HTTP-1 10.102.29.5 HTTP 80  Done > add lb vserver vserver-LB-1 HTTP 10.102.29.60 80  Done > bind lb vserver vserver-LB-1 service-HTTP-1  Done > show service bindings s
```

구성 유틸리티를 사용하여 초기 부하 분산 구성을 구현하려면

1. Traffic Management(트래픽 관리) > Load Balancing(부하 분산)으로 이동합니다.
2. 세부 정보 창에 있는 Getting Started(시작)에서 Load Balancing wizard(부하 분산 마법사)를 클릭하고 지침에 따라 기본적인 부하 분산 설정을 만듭니다.
3. 탐색 창으로 돌아와서 Load Balancing(부하 분산)을 확장한 다음 Virtual Servers(가상 서버)를 클릭합니다.
4. 구성한 가상 서버를 선택하고 페이지 아래쪽에 표시된 매개 변수가 올바르게 구성되었는지 확인합니다.
5. Open(열기)을 클릭합니다.
6. Services(서비스) 탭에서 각 서비스의 Active(활성) 확인란이 선택되어 있는지 확인하여 가상 서버에 각 서비스가 바인딩되어 있는지 확인합니다.

지속성 설정 선택 및 구성

Aug 30, 2016

해당 가상 서버로 나타낸 서버에서 연결 상태를 유지하려는 경우(전자 상거래에서 사용되는 연결 등) 가상 서버에서 지속성을 구성해야 합니다. 그러면 장비에서 초기 서버 선택에 대해 구성된 부하 분산 방식을 사용하지만, 동일 클라이언트에서 오는 이후의 모든 요청을 해당하는 동일 서버에 전달합니다.

지속성이 구성될 경우 서버가 선택되면 부하 분산 방식을 재정의합니다. 구성된 지속성이 다운된 서비스에 적용될 경우 장비는 부하 분산 방식을 사용하여 새 서비스를 선택하고, 새 서비스가 클라이언트의 이후 요청에 대해 유지됩니다. 선택된 서비스가 서비스 불가 상태일 경우 미해결 요청은 계속해서 서비스하지만 새 요청이나 연결은 받지 않습니다. 시스템 종료 기간이 경과되면 기존 연결은 닫힙니다. 다음 표는 구성 가능한 지속성 유형을 나열한 것입니다.

표 1. 동시 지속 연결 수 제한 사항

지속성 유형	지속 연결
원본 IP, SSL 세션 ID, 규칙, DESTIP, SRCIPDESTIP	250K
CookieInsert, URL Passive, 사용자 지정 서버 ID	메모리 제한. CookieInsert의 경우 타임아웃이 0이면 메모리에서 제한될 때까지 모든 연결이 허용됩니다.

장비의 리소스 부족으로 인해 구성된 지속성을 유지할 수 없는 경우에는 부하 분산 방식으로 서버를 선택하게 됩니다. 지속성은 지속성 유형에 따라 구성된 기간 동안 유지됩니다. 일부 지속성 유형은 특정 가상 서버에만 사용됩니다. 다음 표는 이 관계를 나타냅니다.

표 2. 각 가상 서버 유형에 사용할 수 있는 지속성 유형

지속성 TypeHeader 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge
원본 IP	예	예	예	예	예
CookieInsert	예	예	아니요	아니요	아니요
SSL 세션 ID	아니요	예	아니요	아니요	예
URL Passive	예	예	아니요	아니요	아니요
사용자 정의 서버 ID	예	예	아니요	아니요	아니요
규칙	예	예	아니요	아니요	아니요
SRCIPDESTIP	해당 없음	해당 없음	예	예	해당 없음
DESTIP	해당 없음	해당 없음	예	예	해당 없음

가상 서버 그룹에 대해 지속성을 지정할 수도 있습니다. 그룹에 대해 지속성을 사용하도록 설정하는 경우 그룹의 어떤 가상 서버에서 클라이언트 요청을 수신하든지 클라이언트 요청은 선택된 동일 서버로 지정됩니다. 구성된 지속성 시간이 경과할 경우에는 수신 클라이언트 요청에 대해 그룹의 어떠한 가상 서버도 선택될 수 있습니다.

일반적으로 사용되는 두 가지 지속성 유형은 쿠키를 기준으로 하는 지속성과 URL의 서버 ID를 기준으로 하는 지속성입니다.

쿠키 기준의 지속성 구성

업데이트 날짜: 2013년 08월 23일

쿠키를 기준으로 하는 지속성을 활성화할 경우 NetScaler는 HTTP 쿠키를 HTTP 응답의 Set-Cookie 헤더에 추가합니다. 쿠키에는 HTTP 요청이 보내져야 하는 서비스에 대한 정보가 포함되어 있습니다. 클라이언트는 쿠키를 저장한 다음 이후의 모든 요청에 포함시키고, NetScaler는 이 정보를 사용하여 해당 요청에 대한 서비스를 선택합니다. HTTP 또는 HTTPS 유형의 가상 서버에 대해 이 유형의 지속성을 사용할 수 있습니다.

NetScaler는 = 쿠키를 삽입합니다.

여기서:

- 는 가상 서버 이름에서 파생된 가상 서버 ID입니다.
- 는 서비스 IP 주소의 16진수 값입니다.
- 는 서비스 포트의 16진수 값입니다.

NetScaler는 쿠키를 삽입할 때 ServiceIP 및 ServicePort를 암호화하고, 쿠키를 수신할 때 해독합니다.

참고: 클라이언트에서 HTTP 쿠키를 저장할 수 없는 경우 이후의 요청에는 HTTP 쿠키가 포함되지 않고 지속성이 유지되지 않습니다.
기본적으로 NetScaler에서는 Netscape 사양과 호환되는 HTTP 쿠키 버전 0을 보냅니다. RFC 2109와 호환되는 버전 1을 보낼 수도 있습니다.

HTTP 쿠키를 기준으로 하는 지속성에 대해 시간 초과 값을 구성할 수 있습니다. 다음 사항에 유의하십시오.

- HTTP 쿠키 버전 0이 사용될 경우 NetScaler는 NetScaler의 현재 GMT(Coordinated Universal Time) 시간과 시간 초과 값의 합으로 계산된 쿠키 만료의 절대 GMT(HTTP 쿠키의 만료 특성)를 삽입합니다.
- HTTP 쿠키 버전 1이 사용될 경우 NetScaler는 상대 만료 시간(HTTP 쿠키의 Max-Age 특성)을 삽입합니다. 이 경우 클라이언트 소프트웨어에서 실제 만료 시간을 계산합니다.

참고: 현재 설치된 대부분의 클라이언트 소프트웨어(Microsoft Internet Explorer 및 Netscape 브라우저)는 HTTP 쿠키 버전 0을 인식하지만, 일부 HTTP 프록시는 HTTP 쿠키 버전 1을 인식합니다.
시간 초과 값을 0으로 설정할 경우 NetScaler는 사용된 HTTP 쿠키 버전에 상관 없이 만료 시간을 지정하지 않습니다. 그러면 만료 시간은 클라이언트 소프트웨어에 따라 좌우되고, 이러한 쿠키는 해당 소프

트웨어가 종료될 경우 무효화됩니다. 이 지속성 유형은 시스템 리소스를 소모하지 않습니다. 따라서 무제한의 지속 클라이언트 수를 처리할 수 있습니다.

관리자는 다음 표의 절차에 따라 HTTP 쿠키 버전을 변경할 수 있습니다.

구성 유틸리티를 사용하여 HTTP 쿠키 버전을 변경하려면

1. System(시스템) > Settings(설정)로 이동합니다.
2. 세부 정보 창에서 Change HTTP Parameters(HTTP 매개 변수 변경)를 클릭합니다.
3. Configure HTTP Parameters(HTTP 매개 변수 변경) 대화 상자의 Cookie(쿠키)에서 Version 0(버전 0) 또는 Version 1(버전 1)을 선택합니다.

참고: 매개 변수에 대한 자세한 내용은 "Configuring Persistence Based on Cookies(쿠키 기준의 지속성 구성)"를 참조하십시오.

명령줄 인터페이스를 사용하여 쿠키를 기준으로 지속성을 구성하려면

명령 프롬프트에서 다음 명령을 입력하여 쿠키 기준으로 지속성을 구성한 후 해당 구성을 확인합니다.

- set lb vserver -persistenceTypeCOOKIEINSERT
- show lb vserver

예제:

```
> set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT  Done > show lb vserver vserver-LB-1    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS    .   .   .   Persistence: COOKIEI
```

구성 유틸리티를 사용하여 쿠키를 기준으로 지속성을 구성하려면

1. Traffic Management(트래픽 관리) > Load Balancing(부하 분산) > Virtual Servers(가상 서버)로 이동합니다.
2. 세부 정보 창에서 지속성을 구성할 가상 서버(예: vserver-LB-1)를 선택하고 Open(열기)을 클릭합니다.
3. Configure Virtual Server (Load Balancing)(가상 서버 구성(부하 분산)) 대화 상자의 Method and Persistence(방법 및 지속성) 탭에 있는 Persistence(지속성) 목록에서 COOKIEINSERT를 선택합니다.
4. Time-out (min)(시간 초과(분)) 텍스트 상자에 시간 초과 값을 입력합니다(예:2).
5. OK(확인)를 클릭합니다.
6. 가상 서버를 선택한 다음 창 아래쪽의 Details(세부 정보) 섹션을 보고 지속성을 구성한 가상 서버가 올바르게 구성되었는지 확인합니다.

URL의 서버 ID를 기준으로 하는 지속성 구성

업데이트 날짜: 2013년 08월 23일

NetScaler는 URL의 서버 ID를 기준으로 지속성을 유지할 수 있습니다. URL 수동적 지속성이라는 기술로 NetScaler는 서버 응답에서 서버 ID를 추출하고 클라이언트 요청의 URL 쿼리에 포함시킵니다. 서버 ID는 16진수로 지정된 IP 주소 및 포트입니다. NetScaler는 이후의 클라이언트 요청에서 서버 ID를 추출하고 이 정보를 사용하여 서버를 선택합니다.

URL 수동적 지속성의 경우 클라이언트 요청에서 서버 ID의 위치를 지정하는 페이로드 식 또는 정책 인프라 식을 구성해야 합니다. 식에 대한 자세한 내용은 "Policy Configuration and Reference(정책 구성 및 참조)"를 참조하십시오.

참고: 서버 ID를 클라이언트 요청에서 추출할 수 없는 경우 서버 선택은 부하 분산 방식을 기준으로 합니다.
예: 페이로드 식

sid=를 포함하는 URLQUERY 식은 sid= 토큰이 일치하면 시스템이 클라이언트 요청의 URL 쿼리에서 서버 ID를 추출하도록 구성합니다. 따라서 URL http://www.citrix.com/index.asp?&sid;=c0a864100050의 요청은 IP 주소 10.102.29.10 및 포트 80의 서버로 전달됩니다.

서버 ID를 클라이언트 요청에서 추출할 수 있다면 지속성이 유지되므로 시간 초과 값은 이 유형의 지속성에 영향을 주지 않습니다. 이 지속성 유형은 시스템 리소스를 소모하지 않으므로 무제한의 지속 클라이언트 수를 처리할 수 있습니다.

참고: 매개 변수에 대한 자세한 내용은 "Load Balancing(부하 분산)"을 참조하십시오.

명령줄 인터페이스를 사용하여 URL의 서버 ID를 기준으로 지속성을 구성하려면

명령 프롬프트에서 다음 명령을 입력하여 URL의 서버 ID를 기준으로 지속성을 구성한 후 해당 구성을 확인합니다.

- set lb vserver -persistenceType URLPASSIVE
- show lb vserver

예제:

```
> set lb vserver vserver-LB-1 -persistenceType URLPASSIVE  Done > show lb vserver vserver-LB-1    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS    .   .   .   Persistence: URLPASSI
```

구성 유틸리티를 사용하여 URL의 서버 ID를 기준으로 지속성을 구성하려면

1. Traffic Management(트래픽 관리) > Load Balancing(부하 분산) > Virtual Servers(가상 서버)로 이동합니다.
2. 세부 정보 창에서 지속성을 구성할 가상 서버(예: vserver-LB-1)를 선택하고 Open(열기)을 클릭합니다.
3. Configure Virtual Server (Load Balancing)(가상 서버 구성(부하 분산)) 대화 상자의 Method and Persistence(방법 및 지속성) 탭에 있는 Persistence(지속성) 목록에서 URLPASSIVE를 선택합니다.
4. Time-out (min)(시간 초과(분)) 텍스트 상자에 시간 초과 값을 입력합니다(예:2).
5. Rule(규칙) 텍스트 상자에 올바른 식을 입력합니다. 또는 Rule(규칙) 텍스트 상자 옆에 있는 Configure(구성)를 클릭하고 Create Expression(식 만들기) 대화 상자를 사용하여 식을 만듭니다.
6. OK(확인)를 클릭합니다.
7. 가상 서버를 선택한 다음 창 아래쪽의 Details(세부 정보) 섹션을 보고 지속성을 구성한 가상 서버가 올바르게 구성되었는지 확인합니다.

부하 분산 구성을 보호하기 위한 기능 구성

Aug 30, 2016

가상 서버의 오동작에 대한 알림을 제공하도록 URL 리디렉션을 구성하고, 주 가상 서버를 사용할 수 없게 된 경우에 이를 대신하도록 백업 가상 서버를 구성할 수 있습니다.

URL 리디렉션

업데이트 날짜: 2013년 06월 24일

HTTP 또는 HTTPS 유형의 가상 서버가 다운되거나 비활성화된 경우 장비의 상태와 통신할 수 있도록 리디렉션 URL을 구성할 수 있습니다. 이 URL은 로컬 또는 원격 링크가 될 수 있습니다. 장비는 HTTP 302 리디렉션을 사용합니다.

재지정은 절대 URL 또는 상대 URL이 될 수 있습니다. 구성된 리디렉션 URL에 절대 URL이 포함되어 있는 경우 수신 HTTP 요청에 지정된 URL에 상관 없이 HTTP 리디렉션이 구성된 위치로 보내집니다. 구성된 리디렉션 URL에 도메인 이름(상대 URL)만 포함되어 있는 경우 HTTP 리디렉션은 수신 URL을 리디렉션 URL에서 구성된 도메인에 추가한 후 해당 위치로 보내집니다.

참고: 부하 분산 가상 서버가 백업 가상 서버와 리디렉션 URL로 구성된 경우 백업 가상 서버가 리디렉션 URL보다 우선합니다. 이 경우 리디렉션은 기본 및 백업 가상 서버가 모두 다운되었을 때 사용됩니다.

명령줄 인터페이스를 사용하여 클라이언트 요청을 URL로 리디렉션하도록 가상 서버를 구성하려면

명령 프롬프트에서 다음 명령을 입력하여 클라이언트 요청을 URL로 리디렉션하도록 가상 서버를 구성한 후 해당 구성을 확인합니다.

- set lb vserver -redirectURL
- show lb vserver

예제:

```
> set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance  Done > show lb vserver vserver-LB-1     vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS     State:
```

구성 유틸리티를 사용하여 클라이언트 요청을 URL로 리디렉션하도록 가상 서버를 구성하려면

1. Traffic Management(트래픽 관리) > Load Balancing(부하 분산) > Virtual Servers(가상 서버)로 이동합니다.
2. 세부 정보 창에서 URL 리디렉션을 구성할 가상 서버(예: vserver-LB-1)를 선택하고 Open(열기)을 클릭합니다.
3. Configure Virtual Server (Load Balancing)(가상 서버 구성(부하 분산)) 대화 상자의 Advanced(고급) 탭에 있는 Redirect URL(리디렉션 URL) 텍스트 상자에 URL(예:http://www.newdomain.com/mysite/maintenance)을 입력하고 OK(확인)를 클릭합니다.
4. 서버에 대해 구성한 리디렉션 URL이 창 아래쪽의 Details(세부 정보) 섹션에 표시되는지 확인합니다.

백업 가상 서버 구성

업데이트 날짜: 2013년 06월 24일

주 가상 서버가 다운되거나 사용할 수 없게 된 경우 장비는 연결 또는 클라이언트 요청을 백업 가상 서버로 지정하여 클라이언트 트래픽을 서비스에 전달할 수 있습니다. 또한 장비는 사이트 장애 또는 유지 관리와 관련된 통지 메시지를 클라이언트에 보낼 수도 있습니다. 백업 가상 서버는 프록시이며 클라이언트에 투명하게 작동합니다.

가상 서버를 만들 때 또는 기존 가상 서버의 선택적 매개 변수를 변경할 때 백업 가상 서버를 구성할 수 있습니다. 기존 백업 가상 서버에 대한 백업 가상 서버도 구성하여 중첩된 백업 가상 서버도 만들 수 있습니다. 중첩된 백업 가상 서버의 최대 깊이는 10입니다. 장비는 작동 중인 백업 가상 서버를 검색하고 콘텐츠를 전달할 해당 가상 서버에 액세스합니다.

기본 및 백업 가상 서버가 다운되거나 요청 처리를 위한 임계값에 도달한 경우 사용할 주 가상 서버에 대한 URL 리디렉션을 구성할 수 있습니다.

참고: 백업 가상 서버가 존재하지 않을 경우 가상 서버에 리디렉션 URL이 구성되어 있지 않으면 오류 메시지가 나타납니다. 백업 가상 서버와 리디렉션 URL이 둘 다 구성된 경우에는 백업 가상 서버가 우선합니다.

명령줄 인터페이스를 사용하여 백업 가상 서버를 구성하려면

명령 프롬프트에서 다음 명령을 입력하여 백업 서버를 구성하고 구성을 확인합니다.

- set lb vserver [-backupVserver]
- show lb vserver

예제:

```
> set lb vserver vserver-LB-1 -backupVserver vserver-LB-2  Done > show lb vserver vserver-LB-1     vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS     State: DOWN     Last state change was
```

구성 유틸리티를 사용하여 백업 가상 서버를 설정하려면

1. Traffic Management(트래픽 관리) > Load Balancing(부하 분산) > Virtual Servers(가상 서버)로 이동합니다.
2. 세부 정보 창에서 백업 가상 서버를 구성할 가상 서버(예: vserver-LB-1)를 선택하고 Open(열기)을 클릭합니다.
3. Configure Virtual Server(Load Balancing)(가상 서버 구성(부하 분산)) 대화 상자의 Advanced(고급) 탭에 있는 Backup Virtual Server(백업 가상 서버) 목록에서 백업 가상 서버(예: vserver-LB-2)를 선택한 다음 OK(확인)를 클릭합니다.
4. 구성한 백업 가상 서버가 창 아래쪽의 Details(세부 정보) 섹션에 표시되는지 확인합니다.
   참고: 기본 서버가 다운되었다가 다시 복구되는 경우 주 가상 서버를 명시적으로 다시 설정할 때까지 백업 가상 서버를 기본 서버로 사용하려면 Disable Primary When Down(다운되는 경우 기본 서버 사용 안 함) 확인란을 선택합니다.

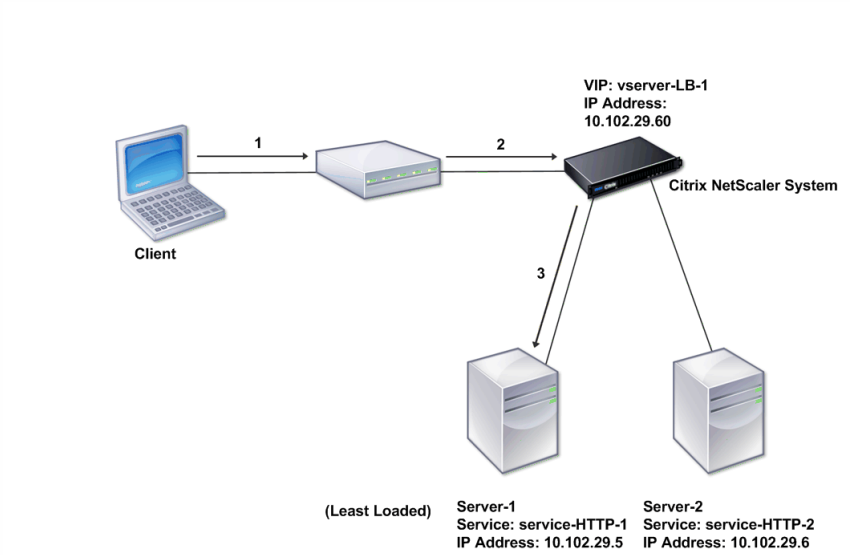
표준 부하 분산 시나리오

Aug 30, 2016

부하 분산 설정에서 NetScaler 장비는 논리적으로 클라이언트와 서버 팜 사이에 위치하여 서버에 대한 트래픽 흐름을 관리합니다.

다음 그림에서는 기본적인 부하 분산 구성 토폴로지를 보여 줍니다.

그림 1. 기본적인 부하 분산 토폴로지



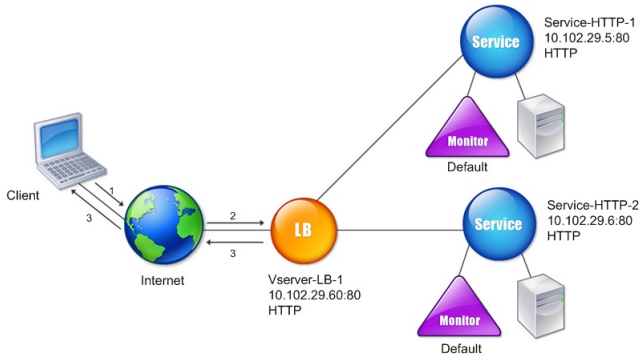
가상 서버는 서비스를 선택하고 클라이언트 요청을 서비스하도록 지정합니다. 위의 그림에서 service-HTTP-1 및 service-HTTP-2 서비스가 만들어지고 이름이 가상 서버-LB-1인 가상 서버에 바인딩되는 시나리오를 살펴봅니다. 가상 서버-LB-1은 클라이언트 요청을 service-HTTP-1 또는 service-HTTP-2에 전달합니다. 시스템은 최소 연결 부하 분산 방식을 사용하여 각 요청에 대한 서비스를 선택합니다. 다음 표에는 시스템에서 구성되어야 하는 기본적인 엔터티의 이름과 값이 나열되어 있습니다.

표 1. LB 구성 매개 변수 값

엔터티 유형	필수 매개 변수 및 샘플 값			
	이름	**IP 주소**	**포트**	**프로토콜**
가상 서버	vserver-LB-1	10.102.29.60	80	HTTP
서비스	service-HTTP-1	10.102.29.5	8083	HTTP
	service-HTTP-2	10.102.29.6	80	HTTP
모니터	기본값	없음	없음	없음

다음 다이어그램은 위의 표에서 설명한 부하 분산 샘플 값 및 필수 매개 변수를 나타낸 것입니다.

그림 2. 부하 분산 엔터티 모델



다음 표에는 명령줄 인터페이스를 사용하여 이러한 부하 분산 설정을 구성하는 데 사용되는 명령이 정리되어 있습니다.

표 2. 초기 구성 작업

작업	명령
부하 분산을 활성화하려면	enable feature lb
service-HTTP-1 이름의 서비스를 생성하려면	add service service-HTTP-1 10.102.29.5 HTTP 80
service-HTTP-2 이름의 서비스를 생성하려면	add service service-HTTP-2 10.102.29.6 HTTP 80
이름이 vserver-LB-1인 가상 서버를 만들려면	add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
service-HTTP-1 이름의 서비스를 vserver-LB-1 이름의 가상 서버에 바인딩하려면	bind lb vserver vserver-LB-1 service-HTTP-1
service-HTTP-2 이름의 서비스를 vserver-LB-1 이름의 가상 서버에 바인딩하려면	bind lb vserver vserver-LB-1 service-HTTP-2

초기 구성 작업에 대한 자세한 내용은 "부하 분산 활성화" 및 "서비스 및 Vserver 구성"을 참조하십시오.

표 3. 확인 작업

작업	명령
vserver-LB-1 이름의 가상 서버 속성을 확인하려면	show lb vserver vserver-LB-1

작업	명령
vserver-LB-1 이름의 가상 서버 통계를 확인하려면	stat lb vserver vserver-LB-1
service-HTTP-1 이름의 서비스 속성을 확인하려면	show service service-HTTP-1
service-HTTP-1 이름의 서비스 통계를 확인하려면	stat service service-HTTP-1
service-HTTP-1 이름의 서비스 바인딩을 확인하려면	show service bindings service-HTTP-1

표 4. 사용자 정의 작업

작업	명령
vserver-LB-1 이름의 가상 서버에 대한 지속성을 구성하려면	set lb vserver vserver-LB-1 -persistenceType SOURCEIP -persistenceMask 255.255.255.255 -timeout 2
vserver-LB-1 이름의 가상 서버에 대한 COOKIEINSERT 지속성을 구성하려면	set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
vserver-LB-1 이름의 가상 서버에 대한 URLPassive 지속성을 구성하려면	set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
vserver-LB-1 이름의 가상 서버에서 클라이언트 요청을 URL에 리디렉션하도록 가상 서버를 구성하려면	set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance
vserver-LB-1 이름의 가상 서버에 백업 가상 서버를 설정하려면	set lb vserver vserver-LB-1 -backupVserver vserver-LB-2

지속성 구성에 대한 자세한 내용은 "지속성 설정 선택 및 구성"을 참조하십시오. 클라이언트 요청을 URL로 리디렉션하도록 가상 서버를 구성하고 백업 가상 서버를 설정하는 방법은 "부하 분산 구성을 보호하기 위한 기능 구성"을 참조하십시오.

압축을 사용하여 부하 분산 트래픽 가속화

Aug 30, 2016

압축은 대역폭 사용량을 최적화할 때 가장 많이 사용되는 방법이며, 대부분의 웹 브라우저에서는 압축된 데이터를 지원합니다. 압축 기능을 활성화하면 NetScaler 장비가 클라이언트의 요청을 가로채 클라이언트에서 압축 콘텐츠를 사용할 수 있는지 확인합니다. 서버에서 HTTP 응답을 수신한 후 장비에서는 콘텐츠를 검사하여 압축 가능 여부를 확인합니다. 콘텐츠가 압축 가능한 경우 장비는 압축하고, 응답 헤더를 수정하여 수행된 압축 유형을 나타내며, 압축된 콘텐츠를 클라이언트에 전달합니다.

NetScaler 압축은 정책 기반 기능입니다. 정책은 요청과 응답을 필터링하여 응답을 압축할지 확인하고, 각 응답에 적용할 압축 유형을 지정합니다. 장비는 텍스트/html, 텍스트/일반, 텍스트/xml, 텍스트/css, 텍스트/rtf, 응용 프로그램/msword, 응용 프로그램/vnd.ms-excel, 응용 프로그램/vnd.ms-powerpoint와 같이 일반적인 MIME 유형을 압축하는 기본 제공 정책을 다양하게 제공합니다. 필요하면 사용자 지정 정책을 만들 수도 있습니다. 장비는 응용 프로그램/8진수 스트림, 이진 파일, 바이트 등의 압축된 MIME 유형과 GIF, JPEG 등의 압축 이미지 형식은 압축하지 않습니다.

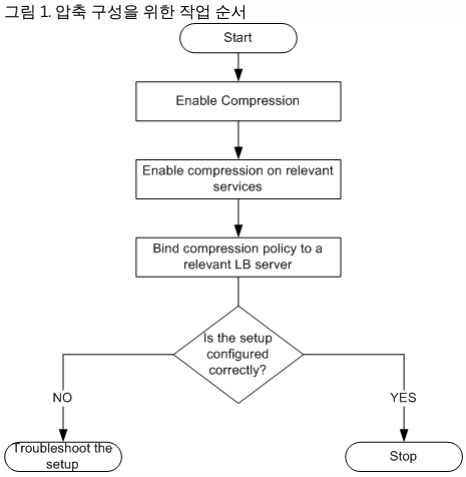
압축을 구성하려면 압축을 전역에서 활성화하는 것은 물론 압축된 응답을 제공해야 하는 각 서비스에 대해서도 압축 기능을 활성화해야 합니다. 부하 분산 또는 콘텐츠 스위칭을 위해 가상 서버를 구성한 경우 가상 서버에 정책을 바인딩해야 합니다. 그렇게 하지 않으면, 장비를 통해 전달되는 모든 트래픽에 정책이 적용됩니다.

압축 구성 작업 순서

업데이트 날짜: 2013년 08월 22일

다음 순서도에서는 부하 분산 설정 시 기본 압축을 구성하기 위한 작업 순서를 보여 줍니다.

그림 1. 압축 구성을 위한 작업 순서



참고: 위 그림의 단계에서는 부하 분산이 이미 구성되어 있는 것으로 가정합니다.

압축 활성화

업데이트 날짜: 2013년 06월 07일

기본적으로 압축은 활성화되지 않습니다. 클라이언트에 보내지는 HTTP 응답을 압축하려면 압축 기능을 활성화해야 합니다.

명령줄 인터페이스를 사용하여 압축을 활성화합니다.

명령 프롬프트에서 다음 명령을 입력하여 압축을 활성화하고 구성을 확인합니다.

- enable ns feature CMP
- show ns feature

예제:

> enable ns feature CMP Done > show ns feature Feature Acronym Status ------- ------- ------ 1) Web Logging WL

구성 유틸리티를 사용하여 압축을 활성화하려면

1. 탐색 창에서 System(시스템)을 확장하고 Settings(설정)를 클릭합니다.
2. 세부 정보 창의 Modes and Features(모드 및 기능)에서 Change basic features(기본 기능 변경)를 클릭합니다.
3. Configure Basic Features(기본 기능 구성) 대화 상자에서 Compression(압축) 확인란을 선택한 다음 OK(확인)를 클릭합니다.
4. Enable/Disable Feature(s)?(기능을 활성화/비활성화하시겠습니까?) 대화 상자에서 Yes(예)를 클릭합니다.

데이터 압축을 위한 서비스 구성

업데이트 날짜: 2013년 08월 22일

전역에서 압축을 활성화하는 것 외에 압축할 파일을 제공하는 각 서비스에 대해서도 압축 기능을 활성화해야 합니다.

명령줄을 사용하여 서비스에 대해 압축을 활성화하려면

명령 프롬프트에서 다음 명령을 입력하여 서비스에 대해 압축을 활성화하고 구성을 확인합니다.

- set service -CMP YES
- show service

예제:

> show service SVC_HTTP1 SVC_HTTP1 (10.102.29.18:80) - HTTP State: UP Last state change was at Tue Jun 16 06:19:14 2009 (+737 ms) Time since last state change: 0 days, 03:03:37.200 Serv

구성 유틸리티를 사용하여 서비스에 대해 압축을 활성화하려면

1. Traffic Management(트래픽 관리) > Load Balancing(부하 분산) > Services(서비스)로 이동합니다.
2. 세부 정보 창에서 압축을 구성하려는 서비스(예: service-HTTP-1)를 선택한 다음 Open(열기)을 클릭합니다.
3. Advanced(고급) 탭의 Settings(설정)에서 Compression(압축) 확인란을 선택한 다음 OK(확인)를 클릭합니다.
4. 서비스를 선택한 경우 HTTP Compression(CMP): ON(HTTP 압축(CMP): 켜짐)이 창의 아래쪽 **Details(세부 정보)** 섹션에 표시되는지 확인하십시오.

가상 서버에 압축 정책 바인딩

업데이트 날짜: 2013년 09월 04일

가상 서버에 정책을 바인딩한 경우 정책은 해당 가상 서버와 연결된 서비스에 의해서만 평가됩니다. Configure Virtual Server (Load Balancing)(가상 서버 구성(부하 분산)) 대화 상자 또는 Compression Policy Manager(압축 정책 관리자) 대화 상자에서 압축 정책을 가상 서버에 바인딩할 수 있습니다. 이 항목에는 Configure Virtual Server (Load Balancing)(가상 서버 구성(부하 분산)) 대화 상자를 사용하여 압축 정책을 부하 분산 가상 서버에 바인딩하는 작업에 대한 지침이 포함되어 있습니다. Compression Policy Manager(압축 정책 관리자) 대화 상자를 사용하여 부하 분산 가상 서버에 압축 정책을 바인딩하는 방법에 대한 자세한 내용은 "Configuring and Binding Policies with the Policy Manager(정책 관리자를 사용하여 정책 구성 및 바인딩)"를 참조하십시오.

명령줄을 사용하여 가상 서버에 압축 정책을 바인딩하거나 바인딩 해제하려면

명령 프롬프트에서 다음 명령을 입력하여 부하 분산 가상 서버에 압축 정책을 바인딩하거나 바인딩 해제하고 구성을 확인합니다.

- (bind | unbind) lb vserver -policyName
- show lb vserver

예제:

```
> bind lb vserver lbvip -policyName ns_cmp_msapp Done > show lb vserver lbvip lbvip (8.7.6.6:80) - HTTP      Type: ADDRESS State: UP Last state change was at Thu May 28 05:37:21 2009 (+685 r
```

구성 유틸리티를 사용하여 압축 정책을 부하 분산 가상 서버에 바인딩하거나 바인딩 해제하려면

1. Traffic Management(트래픽 관리) > Load Balancing(부하 분산) > Virtual Servers(가상 서버)로 이동합니다.
2. 세부 정보 창에서 압축 정책을 바인딩하거나 바인딩 해제할 가상 서버(예: Vserver-LB-1)를 선택한 다음 Open(열기)을 클릭합니다.
3. Configure Virtual Server (Load Balancing)(가상 서버 구성(부하 분산)) 대화 상자의 Policies(정책) 탭에서 Compression(압축)을 클릭합니다.
4. 다음 중 하나를 수행합니다.
   - 압축 정책을 바인딩하려면 Insert Policy(정책 삽입)를 클릭한 다음 가상 서버에 바인딩할 정책을 선택합니다.
   - 압축 정책을 바인딩 해제하려면 가상 서버에서 바인딩 해제할 정책의 이름을 클릭한 다음 Unbind Policy(정책 바인딩 해제)를 클릭합니다.
5. OK(확인)를 클릭합니다.

SSL을 사용하여 부하 분산 트래픽 보안

Aug 30, 2016

Citrix NetScaler SSL 오프로드 기능은 SSL 트랜잭션을 수행하는 웹 사이트의 성능을 투명하게 향상시킵니다. SSL 오프로드는 CPU를 많이 사용하는 SSL 암호화 및 암호 해독 작업의 부하를 로컬 웹 서버에서 장비로 분산시킴으로써 서버에서 SSL 데이터를 처리할 때 발생하는 성능 저하 없이 웹 응용 프로그램을 안전하게 제공합니다. SSL 트래픽이 해독되면 모든 표준 서비스에서 처리할 수 있습니다. SSL 프로토콜은 다양한 유형의 HTTP 및 TCP 데이터와 밀접하게 작동하고 이러한 데이터를 사용하는 트랜잭션을 위한 보안 채널을 제공합니다.

SSL을 구성하려면 먼저 SSL을 활성화해야 합니다. 그런 다음 장비에서 HTTP 또는 TCP 서비스 및 SSL 가상 서버를 구성하고 서비스를 가상 서버에 바인딩합니다. 또한 인증서-키 쌍을 추가하고 SSL 가상 서버에 바인딩해야 합니다. Outlook Web Access 서버를 사용하는 경우에는 SSL 지원을 활성화하기 위한 작업 및 해당 작업을 적용하기 위한 정책을 생성해야 합니다. SSL 가상 서버는 들어오는 암호화된 트래픽을 가로채 협상된 알고리즘을 사용하여 해독합니다. 그런 다음 SSL 가상 서버는 해독된 데이터를 적절한 처리를 위해 장비의 다른 엔터티에 전달합니다.

이 문서에는 다음이 포함되어 있습니다.

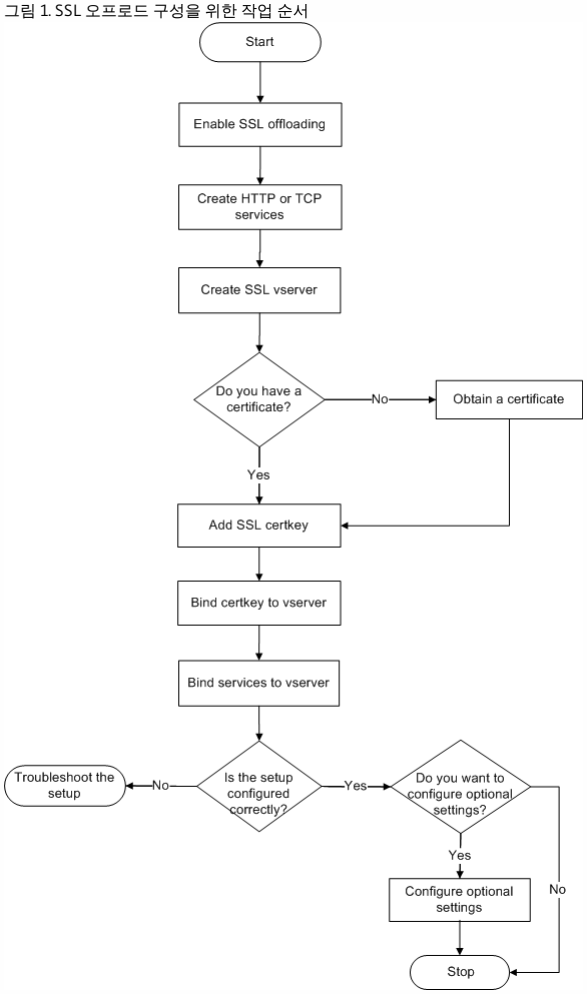
SSL 구성 작업 순서

SSL을 구성하려면 먼저 SSL을 활성화해야 합니다. 그런 다음 NetScaler에서 SSL 가상 서버와 HTTP 또는 TCP 서비스를 만들어야 합니다. 마지막으로 유효한 SSL 인증서와 구성된 서비스를 SSL 가상 서버에 바인드해야 합니다.

SSL 가상 서버는 들어오는 암호화된 트래픽을 가로채 협상된 알고리즘을 사용하여 해독합니다. 그런 다음 SSL 가상 서버는 해독된 데이터를 적절한 처리를 위해 NetScaler의 다른 엔티티에 전달합니다.

다음 순서도는 기본적인 SSL 오프로드 설정을 구성하기 위한 작업 순서를 보여 줍니다.

그림 1. SSL 오프로드 구성을 위한 작업 순서



SSL 오프로드 활성화

SSL 오프로드를 구성하기 전에 SSL 기능을 활성화해야 합니다. SSL 기능을 활성화하지 않고 장비에서 SSL 기반 엔터티를 구성할 수 있지만, SSL을 활성화할 때까지 작동하지 않습니다.

명령줄 인터페이스를 사용하여 SSL을 활성화하려면

명령 프롬프트에서 다음 명령을 입력하여 SSL 오프로드를 활성화하고 구성을 확인합니다.

- enable ns feature SSL
- show ns feature

예제:

```
> enable ns feature ssl  Done  > show ns feature  Feature Acronym Status  ------- ------- ------  1) Web Logging WL ON  2) SurgeProtection SP OFF  3) Load Balancing LB ON . . .  9) SSL Offloading SS
```

구성 유틸리티를 사용하여 SSL을 활성화하려면

1. 탐색 창에서 System(시스템)을 확장하고 Settings(설정)를 클릭합니다.
2. 세부 정보 창의 Modes and Features(모드 및 기능)에서 Change basic features(기본 기능 변경)를 클릭합니다.
3. SSL Offloading(SSL 오프로드) 확인란을 선택하고 OK(확인)를 클릭합니다.
4. Enable/Disable Feature(s)?(기능을 활성화/비활성화하시겠습니까?) 메시지 상자에서 Yes(예)를 클릭합니다.

HTTP 서비스 생성

장비의 서비스는 서버의 응용 프로그램을 나타냅니다. 구성된 서비스는 장비가 네트워크상의 서버에 도달하여 해당 상태를 모니터링할 때까지 비활성화된 상태로 있습니다. 이 항목에서는 HTTP 서비스를 생성하는 방법에 대해 단계별로 설명합니다.

참고: TCP 트래픽의 경우에는 이 항목과 다음 항목에서 설명하는 절차를 수행할 때 HTTP 서비스 대신 TCP 서비스를 생성하십시오.

명령줄 인터페이스를 사용하여 HTTP 서비스를 추가하려면

명령 프롬프트에서 다음 명령을 입력하여 HTTP 서비스를 추가하고 구성을 확인합니다.

- add service (|)
- show service

```
> add service SVC_HTTP1 10.102.29.18 HTTP 80  Done > show service SVC_HTTP1        SVC_HTTP1 (10.102.29.18:80) - HTTP        State: UP        Last state change was at Wed Jul 15 06:13:05 
```

구성 유틸리티를 사용하여 HTTP 서비스를 추가하려면

1. Traffic Management(트래픽 관리) > SSL Offload(SSL 오프로드) > Services(서비스)로 이동합니다.
2. 세부 정보 창에서 Add(추가)를 클릭합니다.
3. Create Service(서비스 만들기) 대화 상자의 Service Name(서비스 이름), Server(서버) 및 Port(포트) 텍스트 상자에 서비스 이름, IP 주소 및 포트를 입력합니다(예:SVC_HTTP1,10.102.29.18및80).
4. Protocol(프로토콜) 목록에서 서비스 유형을 선택합니다(예:HTTP).
5. Create(만들기)를 클릭한 다음 Close(닫기)를 클릭합니다. 구성한 HTTP 서비스가 Services(서비스) 페이지에 나타납니다.
6. 서비스를 선택한 다음 창 아래쪽의 Details(세부 정보) 섹션에서 매개 변수가 올바르게 구성되었는지 확인합니다.

SSL 기반 가상 서버 추가

기본 SSL 오프로드 설정에서 SSL 가상 서버는 암호화된 트래픽을 가로채 해독하고 가상 서버에 바인딩된 서비스에 일반 텍스트 메시지를 보냅니다. CPU를 많이 사용하는 SSL 처리 부하를 장비로 분산시키면 백 엔드 서버에서 더 많은 요청을 처리할 수 있습니다.

명령줄 인터페이스를 사용하여 SSL 기반 가상 서버를 추가하려면

명령 프롬프트에서 다음 명령을 입력하여 SSL 기반 가상 서버를 만들고 구성을 확인합니다.

- add lb vserver [ ]
- show lb vserver

예제:

```
> add lb vserver vserver-SSL-1 SSL 10.102.29.50 443   Done   > show lb vserver vserver-SSL-1   vserver-SSL-1 (10.102.29.50:443) - SSL Type: ADDRESS   State: DOWN[Certkey
```

주의: 보안 연결을 설정하려면 SSL 기반 가상 서버를 활성화하기 전에 먼저 유효한 SSL 인증서를 SSL 기반 가상 서버에 바인딩해야 합니다.

구성 유틸리티를 사용하여 SSL 기반 가상 서버를 추가하려면

1. Traffic Management(트래픽 관리) > SSL Offload(SSL 오프로드) > Virtual Servers(가상 서버)로 이동합니다.
2. 세부 정보 창에서 Add(추가)를 클릭합니다.
3. Create Virtual Server (SSL Offload)(가상 서버 만들기(SSL 오프로드)) 대화 상자에서 Name(이름), IP Address(IP 주소) 및 Port(포트) 텍스트 상자에 가상 서버의 이름, IP 주소 및 포트를 입력합니다(예:Vserver-SSL-1,10.102.29.50및443).
4. Protocol(프로토콜) 목록에서 가상 서버 유형을 선택합니다(예: SSL).
5. Create(만들기)를 클릭한 다음 Close(닫기)를 클릭합니다.
6. 가상 서버를 선택한 다음 창 아래쪽의 Details(세부 정보) 섹션에서 매개 변수가 올바르게 구성되었는지 확인합니다. 인증서-키 쌍 및 서비스가 바인딩되지 않았으므로 가상 서버는 DOWN(비활성화)으로 표시됩니다.

주의: 보안 연결을 설정하려면 SSL 기반 가상 서버를 활성화하기 전에 먼저 유효한 SSL 인증서를 SSL 기반 가상 서버에 바인딩해야 합니다.

SSL 가상 서버에 서비스 바인딩

들어오는 데이터를 해독한 후 SSL 가상 서버는 가상 서버에 바인딩된 서비스에 데이터를 전달합니다.

장비와 서버 간의 데이터 전송은 암호화되거나 일반 텍스트로 전송될 수 있습니다. 장비와 서버 간의 데이터 전송이 암호화될 경우 전체 트랜잭션이 처음부터 끝까지 안전합니다. 종단 간 보안에 대한 자세한 내용은 "SSL Offload and Acceleration(SSL 오프로드 및 가속화)"를 참조하십시오.

명령줄 인터페이스를 사용하여 서비스를 가상 서버에 바인딩하려면

명령 프롬프트에서 다음 명령을 입력하여 서비스를 SSL 가상 서버에 바인딩하고 구성을 확인합니다.

- bind lb vserver
- show lb vserver

예제:

```
> bind lb vserver vserver-SSL-1 SVC_HTTP1   Done   > show lb vserver vserver-SSL-1 vserver-SSL-1 (10.102.29.50:443) - SSL Type:  ADDRESS State: DOWN[Certkey not bound]  Last state ch
```

구성 유틸리티를 사용하여 서비스를 가상 서버에 바인딩하려면

1. Traffic Management(트래픽 관리) > SSL Offload(SSL 오프로드) > Virtual Servers(가상 서버)로 이동합니다.
2. 세부 정보 창에서 가상 서버를 선택하고 Open(열기)을 클릭합니다.
3. Services(서비스) 탭의 Active(활성) 열에서 선택된 가상 서버에 바인딩할 서비스 옆의 확인란을 선택합니다.
4. OK(확인)를 클릭합니다.
5. 창 아래쪽의 Details(세부 정보) 섹션에 있는 Number of Bound Services(바인딩된 서비스 개수) 카운터가 가상 서버에 바인딩된 서비스 개수만큼 증가했는지 확인합니다.

인증서 키 쌍 추가

SSL 인증서는 SSL 키 교환 및 암호화 또는 암호 해독 프로세스의 필수 요소입니다. 인증서는 SSL 핸드셰이크 중에 SSL 서버 ID를 설정하는 데 사용됩니다. NetScaler 장비에 있는 기존의 유효한 SSL 인증서를 사용하거나 고유한 SSL 인증서를 만들 수 있습니다. 장비는 최대 4,096비트의 RSA/DSA 인증서를 지원합니다.

참고: Citrix는 신뢰할 수 있는 인증 기관에서 발급된 유효한 SSL 인증서를 사용할 것을 권장합니다. 유효하지 않은 인증서 및 자체적으로 생성한 인증서는 일부 SSL 클라이언트에서 호환되지 않을 수 있습니다.
인증서는 해당하는 키와 쌍을 이루어야 SSL 처리에 사용될 수 있습니다. 그러면 인증서 키 쌍이 가상 서버에 바인드되고 SSL 처리에 사용됩니다.

명령줄 인터페이스를 사용하여 인증서 키 쌍을 추가하려면

명령 프롬프트에서 다음 명령을 입력하여 인증서 키 쌍을 만들고 구성을 확인합니다.

- add ssl certKey -cert [-key]
- show sslcertkey

예제:

```
> add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-root.key  Done  > show sslcertkey CertKey-SSL-1  Name: CertKey-SSL-1 Status: Valid,  Days to expiration:4811 Version: 3  Serial Num
```

구성 유틸리티를 사용하여 인증서 키 쌍을 추가하려면

1. Traffic Management(트래픽 관리) > SSL > Certificates(인증서)로 이동합니다.
2. 세부 정보 창에서 Add(추가)를 클릭합니다.
3. Install Certificate(인증서 설치) 대화 상자의 Certificate-Key Pair Name(인증서-키 쌍 이름) 텍스트 상자에 추가할 인증서 키 쌍의 이름을 입력합니다(예:Certkey-SSL-1).
4. Details(세부 정보) 아래의 Certificate File Name(인증서 파일 이름)에서 Browse (Appliance)(찾아보기(장비))를 클릭하여 인증서를 찾습니다. 인증서와 키는 모두 장비의 /nsconfig/ssl/ 폴더에 저장되어 있습니다. 로컬 시스템에 있는 인증서를 사용하려면 Local(로컬)을 선택합니다.
5. 사용할 인증서를 선택하고 Select(선택)를 클릭합니다.
6. Private Key File Name(개인 키 파일 이름)에서 Browse (Appliance)(찾아보기(장비))를 클릭하여 개인 키 파일을 찾습니다. 로컬 시스템에 있는 개인 키를 사용하려면 Local(로컬)을 선택합니다.
7. 사용할 키를 선택하고 Select(선택)를 클릭합니다. 인증서 키 쌍에 사용된 키를 암호화하려면 Password(암호) 텍스트 상자에 암호화에 사용할 암호를 입력합니다.
8. Install(설치)을 클릭합니다.
9. 인증서 키 쌍을 두 번 클릭하고 Certificate Details(인증서 세부 정보) 창에서 매개 변수가 올바르게 구성되고 저장되었는지 확인합니다.

가상 서버에 SSL 인증서 키 쌍 바인딩

SSL 인증서와 해당하는 키 쌍을 지정한 후에는 SSL 처리에 사용될 수 있도록 SSL 가상 서버에 인증서 키 쌍을 바인딩해야 합니다. 보안 세션을 사용하려면 클라이언트 컴퓨터와 장비의 SSL 기반 가상 서버 간에 연결을 설정해야 합니다. 그러면 가상 서버에 들어오는 트래픽에 대해 SSL 처리가 수행됩니다. 따라서 장비에서 SSL 가상 서버를 활성화하기 전에 먼저 유효한 SSL 인증서를 SSL 가상 서버에 바인딩해야 합니다.

명령줄 인터페이스를 사용하여 SSL 인증서 키 쌍을 가상 서버에 바인딩하려면

명령 프롬프트에서 다음 명령을 입력하여 SSL 인증서 키 쌍을 가상 서버에 바인딩하고 구성을 확인합니다.

- bind ssl vserver -certkeyName
- show ssl vserver

예제:

```
> bind ssl vserver Vserver-SSL-1 -certkeyName CertKey-SSL-1  Done  > show ssl vserver Vserver-SSL-1  Advanced SSL configuration for VServer Vserver-SSL-1:  DH: DISABLED  Epheme
```

구성 유틸리티를 사용하여 SSL 인증서 키 쌍을 가상 서버에 바인딩하려면

1. Traffic Management(트래픽 관리) > SSL Offload(SSL 오프로드) > Virtual Servers(가상 서버)로 이동합니다.
2. 인증서 키 쌍을 바인딩할 가상 서버(예: Vserver-SSL-1)를 선택하고 Open(열기)을 클릭합니다.
3. Configure Virtual Server (SSL Offload)(가상 서버 구성(SSL 오프로드)) 대화 상자에 있는 SSL Settings(SSL 설정) 탭의 Available(사용 가능)에서 가상 서버에 바인딩할 인증서 키 쌍(예: Certkey-SSL-1)을 선택하고 Add(추가)를 클릭합니다.
4. OK(확인)를 클릭합니다.
5. 선택한 인증서 키 쌍이 Configured(구성됨) 영역에 나타나는지 확인합니다.

Outlook Web Access에 대한 지원 구성

NetScaler 장비에서 OWA(Outlook Web Access) 서버를 사용하는 경우 OWA 서버로 지정된 HTTP 요청에 특수한 헤더 필드 FRONT-END-HTTPS: ON을 삽입하도록 장비를 구성하여 서버에서 http:// 대신 https://로 URL 링크를 생성하도록 해야 합니다.

참고: HTTP 기반 SSL 가상 서버 및 서비스에 대해서만 OWA 지원을 활성화할 수 있습니다. TCP 기반 SSL 가상 서버 및 서비스에 대해서는 적용할 수 없습니다.
OWA 지원을 구성하려면 다음 작업을 수행하십시오.

- OWA 지원을 활성화하기 위한 SSL 작업을 생성합니다.
- SSL 정책을 생성합니다.
- 정책을 SSL 가상 서버에 바인딩합니다.

OWA 지원을 활성화하기 위한 SSL 작업 생성

업데이트 날짜: 2013년 06월 24일

OWA(Outlook Web Access) 지원을 활성화하려면 SSL 작업을 만들어야 합니다. 들어오는 데이터가 정책에 지정된 규칙과 일치하면 SSL 작업이 SSL 정책에 바인드되고 트리거됩니다.

명령줄 인터페이스를 사용하여 OWA 지원을 활성화하기 위한 SSL 작업을 만들려면

명령 프롬프트에서 다음 명령을 입력하여 OWA 지원을 활성화하기 위한 SSL 작업을 만들고 구성을 확인합니다.

- add ssl action -OWASupport ENABLED
- show SSL action
  > add ssl action Action-SSL-OWA -OWASupport enabled Done > show SSL action Action-SSL-OWA Name: Action-SSL-OWA Data Insertion Action: OWA Support: ENABLED Done

구성 유틸리티를 사용하여 OWA 지원을 활성화하기 위한 SSL 작업을 생성하려면

1. Traffic Management(트래픽 관리) > SSL > Policies(정책)로 이동합니다.
2. 세부 정보 창의 Actions(작업) 탭에서 Add(추가)를 클릭합니다.
3. Create SSL Action(SSL 작업 만들기) 대화 상자의 Name(이름) 텍스트 상자에Action-SSL-OWA를 입력합니다.
4. Outlook Web Access에서 Enabled(사용)를 선택합니다.
5. Create(만들기)를 클릭한 다음 Close(닫기)를 클릭합니다.
6. Action-SSL-OWA가 **SSL Actions(SSL 작업)** 페이지에 나타나는지 확인합니다.

SSL 정책 생성

업데이트 날짜: 2013년 09월 04일

정책 인프라를 사용하여 SSL 정책을 생성합니다. 각 SSL 정책에는 바인드된 SSL 작업이 있으며, 작업은 수신 트래픽이 정책에서 구성된 규칙과 일치할 경우 수행됩니다.

명령줄 인터페이스를 사용하여 SSL 정책을 만들려면

명령 프롬프트에서 다음 명령을 입력하여 SSL 정책을 구성하고 구성을 확인합니다.

- add ssl policy -rule -reqAction
- show ssl policy
  예제:

  > add ssl policy Policy-SSL-1 -rule ns_true -reqaction Action-SSL-OWA Done > show ssl policy Policy-SSL-1 Name: Policy-SSL-1 Rule: ns_true Action: Action-SSL-OWA Hits: 0 Policy is

구성 유틸리티를 사용하여 SSL 정책을 생성하려면

1. Traffic Management(트래픽 관리) > SSL > Policies(정책)로 이동합니다.
2. 세부 정보 창에서 Add(추가)를 클릭합니다.
3. Create SSL Policy(SSL 정책 만들기) 대화 상자의 Name(이름) 텍스트 상자에 SSL 정책 이름을 입력합니다(예: Policy-SSL-1).
4. Request Action(요청 작업)에서 이 정책과 연결할 SSL 작업을 선택합니다(예: Action-SSL-OWA). 이 ns_true 일반 식은 성공적인 모든 SSL 핸드셰이크 트래픽에 정책을 적용합니다. 하지만 특정 응답을 필터링해야 하는 경우 상위 레벨의 세부 정보로 정책을 생성할 수 있습니다. 세부적인 정책 식을 구성하는 방법에 대한 자세한 내용은 "정책 및 식 이해"를 참조하십시오.
5. Named Expressions(명명된 식)에서 기본 제공된 일반 식 ns_true 를 선택하고 Add Expression(식 추가)을 클릭합니다. 이제 ns_true 식이 Expression(식) 텍스트 상자에 나타납니다.
6. Create(만들기)를 클릭한 다음 Close(닫기)를 클릭합니다.
7. 정책을 선택한 다음 창 아래쪽의 Details(세부 정보) 섹션에서 정책이 올바르게 구성되었는지 확인합니다.

SSL 정책을 SSL 가상 서버에 바인딩

업데이트 날짜: 2013년 06월 24일

Outlook Web Access에 대한 SSL 정책을 구성한 경우, 들어오는 Outlook 트래픽을 가로채는 가상 서버에 정책을 바인딩합니다. 들어오는 데이터가 SSL 정책에서 구성된 규칙과 일치하면 정책이 트리거되고 연관된 작업이 수행됩니다.

명령줄 인터페이스를 사용하여 SSL 정책을 SSL 가상 서버에 바인딩하려면

명령 프롬프트에서 다음 명령을 입력하여 SSL 정책을 SSL 가상 서버에 바인딩하고 구성을 확인합니다.

- bind ssl vserver -policyName
- show ssl vserver
  예제:

  > bind ssl vserver Vserver-SSL-1 -policyName Policy-SSL-1 Done > show ssl vserver Vserver-SSL-1 Advanced SSL configuration for VServer Vserver-SSL-1: DH: DISABLED Ephem

구성 유틸리티를 사용하여 SSL 정책을 SSL 가상 서버에 바인딩하려면

1. Traffic Management(트래픽 관리) > SSL Offload(SSL 오프로드) > Virtual Servers(가상 서버)로 이동합니다.
2. 세부 정보 창에서 가상 서버(예: Vserver-SSL-1)를 선택하고 Open(열기)을 클릭합니다.
3. Configure Virtual Server (SSL Offload)(가상 서버 구성(SSL 오프로드)) 대화 상자에서 Insert Policy(정책 삽입)를 클릭하고 SSL 가상 서버에 바인딩할 정책을 선택합니다. 경우에 따라 Priority(우선 순위) 필드를 두 번 클릭하고 새 우선 순위 수준을 입력할 수 있습니다.
4. OK(확인)를 클릭합니다.

기능 요약

Aug 30, 2016

Citrix NetScaler 기능은 독립적으로 구성하거나 조합하여 특정 요구 사항을 해결할 수 있습니다. 기능 중 일부는 둘 이상의 범주에 해당되지만, 일반적으로 NetScaler 기능의 대다수는 응용 프로그램 스위칭 및 트래픽 관리 기능, 응용 프로그램 가속화 기능, 응용 프로그램 보안 및 방화벽 기능, 응용 프로그램 가시성 기능으로 분류할 수 있습니다.

기능의 처리 순서를 이해하려면 "기능 처리 순서"를 참조하십시오.

이 문서에는 다음이 포함되어 있습니다.

- 응용 프로그램 스위치 및 트래픽 관리 기능
- 응용 프로그램 가속 기능
- 응용 프로그램 보안 및 방화벽 기능
- 응용 프로그램 가시성 기능
- 클라우드 통합 기능

응용 프로그램 스위치 및 트래픽 관리 기능

Sep 13, 2016

SSL 오프로드

웹 서버의 SSL 암호화 및 암호 해독 부하를 백그라운드에서 오프로드하여 서비스 콘텐츠 요청을 처리하는 서버 리소스의 부하를 줄입니다. SSL은 응용 프로그램의 성능에 많은 부담이 되며 여러 최적화 조치를 비효과적으로 만들 수 있습니다. SSL 오프로드 및 가속화를 통해 Citrix 요청 교환 기술의 모든 장점을 SSL 트래픽에 적용함으로써 최종 사용자의 성능 저하 없이 웹 응용 프로그램의 안전한 전달을 가능하게 합니다.
자세한 내용은 "SSL Offload and Acceleration(SSL 오프로드 및 가속화)"을 참조하십시오.

액세스 제어 목록

수신되는 패킷을 ACL(액세스 제어 목록)과 비교합니다. 패킷이 ACL 규칙과 일치할 경우 규칙에서 지정된 작업이 패킷에 적용됩니다. 그렇지 않을 경우 기본 작업(ALLOW)이 적용되고 패킷은 정상적으로 처리됩니다. 장비에서 수신되는 패킷을 ACL과 비교하려면 ACL을 적용해야 합니다. 모든 ACL은 기본적으로 활성화되지만 NetScaler에서 수신되는 패킷을 비교하려면 ACL을 적용해야 합니다. ACL이 조회 테이블의 일부가 될 필요가 없지만 구성에서 유지해야 하는 경우 ACL을 적용하기 전에 비활성화해야 합니다. NetScaler는 수신되는 패킷을 비활성화된 ACL과 비교하지 않습니다.
자세한 내용은 "Access Control List(액세스 제어 목록)"를 참조하십시오.

부하 분산

부하 분산 결정은 라운드 로빈, 최소 연결, 하중 최저 대역폭, 하중 최저 패킷, 최소 응답 시간 및 URL, 도메인 소스 IP 또는 목적지 IP 주소 해시를 포함하여 다양한 알고리즘을 기준으로 합니다. TCP 및 UDP 프로토콜이 모두 지원되므로 NetScaler에서는 이러한 프로토콜을 기본 전송 수단으로 사용하는 모든 트래픽(예: HTTP, HTTPS, UDP, DNS, NNTP 및 일반적인 방화벽 트래픽)의 부하를 분산시킬 수 있습니다. 또한 NetScaler는 원본 IP, 쿠키, 서버, 그룹 또는 SSL 세션을 기준으로 세션 지속성을 유지할 수 있습니다. 이를 통해 사용자는 사용자 정의 ECV(Extended Content Verification)를 서버, 캐시, 방화벽 및 기타 인프라 장치에 적용하여 이러한 시스템이 정상적으로 작동하고 사용자에게 올바른 콘텐츠를 제공하도록 할 수 있습니다. 또한 Ping, TCP, 또는 HTTP URL을 사용하여 상태 확인을 수행하고, 사용자는 Perl 스크립트를 기반으로 모니터를 생성할 수 있습니다. 확장성이 뛰어난 WAN 최적화를 제공하기 위해 데이터 센터에 배포된 CloudBridge 장비를 NetScaler 장비를 통해 부하 분산시킬 수 있습니다. 동시 세션 수 및 대역폭이 크게 향상될 수 있습니다.
자세한 내용은 "Load Balancing(부하 분산)"을 참조하십시오.

트래픽 도메인

트래픽 도메인은 단일 NetScaler 장비에서 논리적 ADC 파티션을 만드는 방법을 제공합니다. 이를 통해 다양한 응용 프로그램에 대해 네트워크 트래픽을 분할할 수 있습니다. 트래픽 도메인을 사용하여 리소스가 서로 상호 작용하지 않는 다중 분리 환경을 만들 수 있습니다. 특정 트래픽 도메인에 속한 응용 프로그램은 해당 도메인 내에서 엔터티와만 통신하고 트래픽을 처리합니다. 하나의 트래픽 도메인에 속하는 트래픽은 다른 트래픽 도메인의 경계를 통과할 수 없습니다. 따라서 해당 주소가 동일한 도메인 내에서 중복되지 않는 한 장비에서 중복 IP 주소를 사용할 수 있습니다.
자세한 내용은 "트래픽 도메인"을 참조하십시오.

NAT(Network Address Translation)

NAT(Network Address Translation)는 NetScaler 장비를 통과하는 IP 패킷의 소스 및/또는 목적지 IP 주소 및/또는 TCP/UDP 포트 번호의 수정을 포함합니다. 장비에서 NAT를 활성화하면 데이터가 NetScaler를 통과할 때 네트워크의 원본 IP 주소를 수정하여 사설망의 보안을 강화하고 인터넷과 같은 공용 네트워크로부터 보호할 수 있습니다.

NetScaler 장비는 다음 유형의 NAT(Network Address Translation)를 지원합니다.

INAT - INAT(인바운드 NAT)에서 NetScaler 장비에 구성된 IP 주소(보통 공개)는 서버를 대신하여 연결 요청을 수신합니다. 공용 IP 주소에서 장비가 수신한 요청 패킷에 대해, NetScaler는 해당 서버의 사설 IP 주소로 목적지 IP 주소를 대체합니다. 즉, 장비가

클라이언트와 서버 간 프록시 역할을 합니다. INAT 구성에는 NetScaler 장비의 IP 주소와 서버의 IP 주소 간에 일대일 관계를 정의하는 INAT 규칙이 포함됩니다.

RNAT - RNAT(Reverse Network Address Translation)에서 서버에서 초기화된 세션에 대해, NetScaler 장비는 서버가 생성한 패킷의 원본 IP 주소를 장비에 구성된 IP 주소(SNIP 유형)로 대체합니다. 따라서 이 장비는 서버가 생성한 모든 유형의 패킷에 서버의 IP 주소가 노출되는 것을 방지합니다. RNAT 구성에는 조건을 규정하는 RNAT 규칙이 포함됩니다. 장비는 이 조건과 일치하는 패킷에서 RNAT 처리를 수행합니다.

상태 비저장 NAT46 변환 - 상태 비저장 NAT46은 NetScaler 장비의 모든 세션 정보를 유지 관리하지 않고 Pv4 패킷을 IPv6 패킷으로 변환하는 방법 또는 그 반대의 방법으로 IPv4와 IPv6 네트워크 간 통신을 활성화합니다. 상태 비저장 NAT46 구성에는 IPv4-IPv6 INAT 규칙과 NAT46 IPv6 접두사가 포함됩니다.

상태 저장 NAT64 변환 - 상태 저장 NAT64 기능은 NetScaler 장비의 모든 세션 정보를 유지 관리하면서 IPv6 패킷을 IPv4 패킷으로 변환하는 방법 또는 그 반대의 방법으로 IPv4 클라이언트와 IPv6 서버 간 통신을 활성화합니다. 상태 저장 NAT64 구성에는 NAT64 규칙과 NAT64 IPv6 접두사가 포함됩니다.

자세한 내용은 "NAT(Network Address Translation) 구성"을 참조하십시오.

다중 경로 TCP 지원

NetScaler 장비는 MPTCP(다중 경로 TCP)를 지원합니다. MPTCP는 TCP 세션을 유지 관리하는 호스트 간에 이용할 수 있는 다중 경로를 식별하고 사용하는 TCP/IP 프로토콜의 확장입니다. TCP 프로필에서 MPTCP를 활성화하고 가상 서버에 바인딩해야 합니다. MPTCP가 활성화된 경우, 가상 서버는 MPTCP 게이트웨이 기능을 수행하며 클라이언트와의 MPTCP 연결을 해당 서버를 통해 유지 관리되는 TCP 연결로 변환합니다.
자세한 내용은 "MPTCP(Multi-Path TCP)"를 참조하십시오.

콘텐츠 스위칭

구성된 콘텐츠 스위칭 정책에 따라 요청을 보낼 서버가 결정됩니다. 정책 규칙은 IP 주소, URL 및 HTTP 헤더를 기반으로 할 수 있습니다. 이를 통해 사용자, 사용된 에이전트 유형, 사용자 요청한 콘텐츠 등의 사용자 및 장치 특성을 기준으로 스위칭 결정을 내릴 수 있습니다.
자세한 내용은 "Content Switching(콘텐츠 스위칭)"을 참조하십시오.

GSLB(Global Server Load Balancing)

NetScaler의 트래픽 관리 기능을 확장하여 분산된 인터넷 사이트 및 글로벌 엔터프라이즈를 포함시킵니다. 설치가 여러 네트워크 위치 또는 단일 위치의 여러 클러스터에 걸쳐 이루어지든지 상관 없이 NetScaler는 이러한 위치에서 가용성을 유지하고 트래픽을 분산시킵니다. 지능적인 DNS 결정을 통해 사용자가 다운되거나 오버로드 상태의 사이트로 보내지지 않도록 합니다. 근접성 기준 GSLB 방식이 활성화되면 NetScaler는 여러 사이트와 상대적으로 클라이언트의 로컬 DNS 서버(LDNS) 근접성을 기준으로 부하 분산 결정을 내릴 수 있습니다. 근접성 기준 GSLB 방식의 주요 장점은 가장 가까운 사용 가능 사이트를 선택함으로써 응답 시간이 빨라진다는 것입니다.
자세한 내용은 "GSLB(Global Server Load Balancing)"를 참조하십시오.

동적 라우팅

라우터가 인접한 라우터에서 자동으로 토폴로지 정보, 경로 및 IP 주소를 가져올 수 있습니다. 동적 라우팅이 활성화되면 해당하는 라우팅 프로세스는 경로 업데이트를 수신하고 경로를 알려줍니다. 또한 라우팅 프로세스를 수동적 모드로 둘 수도 있습니다. 라우팅 프로토콜을 통해 업스트림 라우터는 동일 비용 다중 경로(Equal Cost Multipath) 기술을 사용하여 두 개의 독립형 NetScaler 장치에서 호스팅되는 동일한 가상 서버로 트래픽 부하를 분산시킬 수 있습니다.
자세한 내용은 "Configuring Dynamic Routes(동적 라우팅 구성)"를 참조하십시오.

링크 부하 분산

다중 WAN 링크의 부하를 분산시키고 링크 장애 조치(failover)를 제공하여 네트워크 성능을 최적화하고 비즈니스 지속성을 유

지합니다. 지능적인 트래픽 제어 및 상태 확인을 적용하여 업스트림 라우터에 걸쳐 트래픽을 효율적으로 분산시킴으로써 네트워크 연결을 거의 항상 사용할 수 있도록 유지합니다. 정책 및 네트워크 조건을 기준으로 송수신 트래픽을 전달할 최적의 WAN 링크를 식별하고, 빠른 장애 감지 및 장애 조치(failover)를 제공하여 WAN 또는 인터넷 링크에서 응용 프로그램을 보호합니다.
자세한 내용은 "Link Load Balancing(링크 부하 분산)"을 참조하십시오.

TCP Optimization(SSL 최적화)

TCP 프로필을 사용하여 TCP 트래픽을 최적화할 수 있습니다. TCP 프로필은 NetScaler 가상 서버가 TCP 트래픽을 처리하는 방식을 정의합니다. 관리자는 기본 제공 TCP 프로필을 사용하거나 사용자 지정 프로필을 구성할 수 있습니다. TCP 프로필을 정의한 다음 단일 가상 서버 또는 다중 가상 서버에 바인딩할 수 있습니다.
TCP 프로필을 통해 활성화할 수 있는 일부 주요 최적화 기능은 다음과 같습니다.

- TCP 연결 유지 - 링크가 끊기는 것을 방지하기 위해 특정 시간 간격으로 피어의 작동 상태를 확인합니다.
- SACK(선택 승인) - 데이터 전송 특히, LFN(long fat network)의 성능을 개선합니다.
- TCP 창 크기 조정 - LFN(long fat network)을 통해 데이터를 효율적으로 전송합니다.

TCP 프로필에 대한 자세한 내용은 "Configuring TCP Profiles(TCP 프로필 구성)"를 참조하십시오.

NetScaler의 Web Interface

응용 프로그램, 콘텐츠 및 데스크톱을 포함하는 XenApp 및 XenDesktop 리소스에 대한 액세스를 제공합니다. 사용자는 표준 웹 브라우저 또는 Citrix XenApp 플러그인을 사용하여 리소스에 액세스할 수 있습니다. Web Interface는 NetScaler 장비의 포트 8080에서 서비스로 실행됩니다. Web Interface 사이트를 만들려면 NetScaler 장비의 Apache Tomcat 웹 서버 버전 6.0.26에서 Java를 실행해야 합니다.
참고: Web Interface는 NetScaler nCore 릴리스에서만 지원됩니다.
자세한 내용은 "Web Interface"를 참조하십시오.

CloudBridge Connector

Citrix OpenCloud 프레임워크의 기반인 Citrix NetScaler CloudBridge Connector 기능은 클라우드 확장 데이터 센터를 구축하는 데 사용되는 도구입니다. OpenCloud Bridge를 사용하면 네트워크를 재구성하지 않고도 클라우드에 있는 하나 이상의 NetScaler 장비 또는 NetScaler 가상 장비를 네트워크에 연결할 수 있습니다. 클라우드 호스팅 응용 프로그램은 하나의 인접한 엔터프라이즈 네트워크에서 실행 중인 것처럼 표시됩니다. OpenCloud Bridge의 주 용도는 회사에서 절감된 비용 및 완화된 응용 프로그램 오류 위험으로 응용 프로그램을 클라우드로 이동할 수 있도록 하는 것입니다. 또한 OpenCloud Bridge는 클라우드 환경에서 네트워크 보안을 강화합니다. OpenCloud Bridge는 클라우드 인스턴스의 NetScaler 장비 또는NetScaler 가상 장비를 LAN의 NetScaler 장비 또는 NetScaler 가상 장비에 연결하는 2계층 네트워크 브리지입니다. 연결은 GRE(Generic Routing Encapsulation) 프로토콜을 사용하는 터널을 통해 실행됩니다. GRE 프로토콜은 다른 프로토콜을 통해 전달할 다양한 네트워크 프로토콜의 패킷을 캡슐화하는 메커니즘을 제공합니다. 그런 다음에는 IPsec(인터넷 프로토콜 보안) 프로토콜 제품군을 사용하여 OpenCloud Bridge의 피어 간 통신에 대한 보안을 유지합니다.
자세한 내용은 "CloudBridge"를 참조하십시오.

DataStream

NetScaler DataStream 기능은 전송되는 SQL 쿼리를 기반으로 요청을 분산시켜 데이터베이스 계층에서 요청 스위칭을 위한 지능형 메커니즘을 제공합니다.

데이터베이스 서버 앞에 배포할 경우 NetScaler는 응용 프로그램 서버 및 웹 서버의 트래픽을 최적으로 분산시킵니다. 관리자는 SQL 쿼리의 정보 및 데이터베이스 이름, 사용자 이름, 문자 세트, 패킷 크기 등을 바탕으로 트래픽을 세그먼트화할 수 있습니다.

사용자는 부하 분산 알고리즘에 따라 요청을 전환하도록 부하 분산을 구성하거나, SQL 쿼리 매개 변수(예: 사용자 이름, 데이터베이스 이름 및 명령 매개 변수)를 기반으로 의사를 결정하도록 콘텐츠 스위칭을 구성하여 스위칭 조건을 세부 지정할 수 있습니다. 또한 데이터베이스 서버 상태를 추적하도록 모니터를 구성할 수 있습니다.

NetScaler 장비의 고급 정책 인프라에는 요청을 평가하고 처리하는 데 사용할 수 있는 식이 포함됩니다. 고급 식은 MySQL 데이

터베이스 서버와 연관된 트래픽을 평가합니다. 고급 정책에서 요청 기반 식(MYSQL.CLIENT 및 MYSQL.REQ로 시작하는 식)을 사용하여 콘텐츠 스위칭 가상 서버 바인딩 지점에서 요청 교환을 결정할 수 있고 응답 기반 식(MYSQL.RES로 시작하는 식)을 사용하여 사용자가 구성한 상태 모니터링에 대한 서버 응답을 평가할 수 있습니다.

참고: DataStream은 MySQL 및 MS SQL 데이터베이스에 대해 지원됩니다.
자세한 내용은 "DataStream"를 참조하십시오.

응용 프로그램 가속 기능

Aug 30, 2016

AppCompress

GZip 압축 프로토콜을 사용하여 HTML 및 텍스트 파일에 대해 투명한 압축 기능을 제공합니다. 일반적인 4:1 압축률은 데이터 센터의 대역폭 요구 사항을 최대 50%까지 낮출 수 있습니다. 또한 사용자의 브라우저에 전달해야 하는 데이터 양을 줄이므로 최종 사용자 응답 시간을 크게 향상시킵니다.
자세한 내용은 "Compression(압축)"을 참조하십시오.

캐시 리디렉션

역방향 프록시, 투명 프록시 또는 정방향 프록시 캐시 팜으로 트래픽 흐름을 관리합니다. 모든 트래픽을 검사하고 캐시에 저장할 수 없는 요청을 식별하여 이러한 요청은 지속 연결을 통해 원본 서버에 직접 보냅니다. 캐시에 저장할 수 없는 요청을 원래 웹 서버에 지능적으로 다시 재지정함으로써 NetScaler 장비는 전체적인 대역폭 소모량 및 이러한 요청에 대한 응답 지연 시간을 줄이면서 캐시 리소스를 확보하고 캐시 적중률을 높입니다.
자세한 내용은 "Cache Redirection(캐시 리디렉션)"을 참조하십시오.

AppCache

정적 콘텐츠와 동적 콘텐츠에 대해 모두 빠른 메모리 내 HTTP/1.1 및 HTTP/1.0 호환 웹 캐싱을 제공하여 웹 콘텐츠 및 응용 프로그램 데이터 전달을 최적화합니다. 이 온보드 캐시는 수신 요청이 보안되거나 데이터가 압축되어 있더라도 수신되는 응용 프로그램 요청 결과를 캐시에 저장한 다음 데이터를 재사용하여 이후의 동일한 정보에 대한 요청을 처리합니다. 온보드 캐시에서 직접 데이터를 서비스함으로써 장비는 정적 및 동적 콘텐츠 요청을 서버에 전달할 필요 없이 페이지 재생성 시간을 단축할 수 있습니다.
자세한 내용은 "Integrated Caching(통합 캐싱)"을 참조하십시오.

TCP 버퍼링

서버의 응답을 버퍼링하여 클라이언트의 속도에 따라 클라이언트에 제공하여 서버의 부하를 신속하게 줄이고 웹 사이트의 성능을 향상시킵니다.
자세한 내용은 "TCP Buffering(TCP 버퍼링)"을 참조하십시오.

응용 프로그램 보안 및 방화벽 기능

Aug 30, 2016

서비스 거부(DoS) 공격 방어

악의적인 분산 서비스 거부(DDoS) 공격 및 기타 유형의 악의적인 공격이 서버에 도달하기 전에 감지하고 막아 네트워크 및 응용 프로그램 성능이 영향을 받지 않도록 합니다. NetScaler 장비는 인증된 클라이언트를 식별하고 우선 순위를 높임으로써 의심되는 클라이언트가 리소스의 상당 부분을 소모하여 사이트를 마비시키지 못하도록 합니다. 장비는 다음과 같은 유형의 악의적인 공격에 대해 응용 프로그램 레벨 보호 기능을 제공합니다.

- SYN 대량 공격
- 파이프라인 공격
- Teardrop 공격
- Land 공격
- Fraggle 공격
- 좀비 연결 공격

장비는 이러한 연결에 대한 서버 리소스 할당을 막아 이러한 유형의 공격에 대해 적극적으로 방어합니다. 그러면 서버는 이러한 이벤트와 연관된 패킷의 대량 유입으로부터 격리됩니다.

또한 장비는 ICMP 비율 제한 및 적극적인 ICMP 패킷 검사를 사용하여 ICMP 기반 공격으로부터 네트워크 리소스를 보호합니다. 추가 보호 수단으로 강력한 IP 리어셈블리를 수행하고, 여러 의심되거나 잘못된 형식의 패킷을 삭제하며, 사이트 트래픽에 ACL을 적용합니다.

자세한 내용은 "HTTP Denial-of-Service Protection(HTTP 서비스 거부 보호)"을 참조하십시오.

콘텐츠 필터링

7계층 레벨에서 웹 사이트에 대한 악의적인 공격으로부터 보호합니다. 장비는 HTTP 헤더를 기준으로 사용자가 구성한 규칙에 따라 각 수신 요청을 검사하고 사용자가 구성한 작업을 수행합니다. 작업에는 연결 재설정, 요청 삭제, 사용자의 브라우저에 오류 메시지 전송 등이 포함될 수 있습니다. 이를 통해 장비는 원치 않는 요청을 걸러내고 서버가 공격에 노출되는 것을 줄일 수 있습니다.
또한 이 기능은 HTTP GET 및 POST 요청을 분석하고 알려진 잘못된 서명을 필터링하여 HTTP 기반 공격으로부터 서버를 보호할 수 있습니다.

자세한 내용은 "Content Filtering(콘텐츠 필터링)"을 참조하십시오.

Responder

고급 필터와 같이 동작하며 장비에서 클라이언트로 전송되는 응답을 생성하는 데 사용할 수 있습니다. 이 기능의 일반적인 용도에는 리디렉션 응답, 사용자 정의 응답 및 재설정 생성이 포함됩니다.
자세한 내용은 "Responder"를 참조하십시오.

다시 쓰기

HTTP 헤더 및 본문 텍스트를 수정합니다. 다시 쓰기 기능을 사용하여 HTTP 헤더를 HTTP 요청 또는 응답에 추가하거나, 개별 HTTP 헤더를 수정하거나, HTTP 헤더를 삭제할 수 있습니다. 또한 요청 및 응답에서 HTTP 본문을 수정할 수도 있습니다.
장비는 요청을 수신하거나 응답을 보낼 때 다시 쓰기 규칙을 확인하고, 해당하는 규칙이 존재하면 웹 서버나 클라이언트 컴퓨터에 전달하기 전에 요청이나 응답에 적용합니다.

자세한 내용은 "Rewrite(다시 쓰기)"를 참조하십시오.

우선 순위 대기열

사용자 요청의 우선 순위를 관리하여 요청량이 급증할 때 가장 중요한 트래픽이 가장 먼저 서비스되도록 합니다. 요청 URL, 쿠키 또는 기타 다양한 요소를 기준으로 우선 순위를 설정할 수 있습니다. 장비는 구성된 우선 순위를 기준으로 3계층 큐에 요청을 두어 과부하나 사이트 공격이 발생하더라도 중요 업무 트랜잭션이 순조롭게 이루어지도록 합니다.
자세한 내용은 "Priority Queuing(우선 순위 대기열)"을 참조하십시오.

서지 보호

서버에 대한 사용자 요청 흐름을 규정하고, 서버의 리소스에 동시에 액세스할 수 있는 사용자 수를 제한하며, 서버가 용량에 도달한 경우 추가 요청을 대기시킵니다. 연결을 설정할 수 있는 비율을 통제함으로써 장비는 대량 요청이 서버로 전달되는 것을 차단하고 사이트 오버로드를 예방합니다.
자세한 내용은 "Surge Protection(서지 보호)"을 참조하십시오.

NetScaler Gateway

NetScaler Gateway는 관리자에게 세부적인 응용 프로그램 수준 정책 및 작업 컨트롤을 제공하여 사용자가 어디서든 작업할 수 있도록 하는 동시에 응용 프로그램과 데이터에 대한 액세스 보안을 유지하는 보안 응용 프로그램 액세스 솔루션입니다. IT 관리자는 Citrix Access Gateway 한 곳에서 회사 내부와 외부에 대해 규정 준수 및 최상위 수준의 정보 보안을 제공할 수 있습니다. 사용자 또한 이 한 곳에서 역할, 장치 및 네트워크에 최적화된 상태로 필요로 하는 기업 응용 프로그램 및 데이터에 액세스할 수 있습니다. 이와 같이 고유한 기능의 결합으로 이동 작업자의 생산성을 극대화할 수 있습니다.

자세한 내용은 "NetScaler Gateway"를 참조하십시오.

응용 프로그램 방화벽

보호된 웹 서버와 해당 웹 서버의 웹 사이트에 연결하는 사용자 간의 트래픽을 필터링하여 사이트 간 스크립팅 공격, 버퍼 오버플로 공격, SQL 삽입 공격, 강제 브라우징 등과 같은 해커 및 맬웨어의 응용 프로그램 악용을 막습니다. 응용 프로그램 방화벽은 모든 트래픽에서 웹 서버 보안에 대한 공격 징후 또는 웹 서버 리소스의 악용 증거를 검사하고 이러한 공격을 막기 위해 적절한 조치를 취합니다.
자세한 내용은 "Application Firewall(응용 프로그램 방화벽)"을 참조하십시오.

응용 프로그램 가시성 기능

Aug 30, 2016

NetScaler Insight Center

NetScaler Insight Center는 웹과 HDX(ICA) 트래픽 전체에서 종단 간 사용자 환경의 가시성을 제공하는 고성능 수집기로, NetScaler ADC 장비가 생성하는 HTTP 및 ICA AppFlow 레코드를 수집하고 계층 3에서 계층 7 통계까지를 다루는 분석 보고서의 데이터를 작성합니다. NetScaler Insight Center는 실시간 데이터의 마지막 5분과 마지막 1시간, 하루, 일주일, 한 달을 기준으로 수집된 기록 데이터에 대해 심층적인 분석을 제공합니다.
HDX(ICA) 분석 대시보드를 활용하면 HDX 사용자, 응용 프로그램, 데스크톱과 게이트웨이 수준 정보에서 드릴다운할 수 있습니다. 마찬가지로, HTTP 분석으로 웹 응용 프로그램, 액세스한 URL, 클라이언트 IP 주소 및 서버 IP 주소, 다른 대시보드를 한 눈에 파악할 수 있습니다. 관리자는 이러한 대시보드에서 사용 사례에 맞게 문제점을 드릴다운하고 식별할 수 있습니다.

EdgeSight for NetScaler

최종 사용자 환경을 기반으로 응용 프로그램 성능 모니터링을 지원합니다. 이 솔루션은 HTML 주입 기능을 활용하여 EdgeSight 서버에서 분석 및 보고서 생성을 위해 사용되는 다양한 시간 값을 얻습니다. EdgeSight for NetScaler는 NetScaler의 성능 이점을 모니터링할 수 있는 방법을 제공하고 네트워크의 잠재적인 병목 지점을 확인합니다.
자세한 내용은 "EdgeSight Monitoring for NetScaler(NetScaler에 대한 EdgeSight 모니터링)"를 참조하십시오.

AppFlow를 사용하여 응용 프로그램 가시성 향상

Citrix NetScaler 장비는 데이터 센터의 모든 응용 프로그램 트래픽에 대한 중앙 제어 지점으로, 응용 프로그램 성능 모니터링, 분석 및 비즈니스 인텔리전스 응용 프로그램에 중요한 흐름 및 사용자 세션 수준 정보를 수집합니다. AppFlow는 RFC 5101에 정의된 IETF(Internet Engineering Task Force) 공개 표준인 IPFIX(Internet Protocol Flow Information eXport) 형식을 사용하여 이 정보를 전송합니다. IPFIX(Cisco NetFlow의 표준화 버전)는 네트워크 흐름 정보를 모니터링하는 데 널리 사용됩니다. AppFlow는 응용 프로그램 수준 정보를 나타내는 새로운 정보 요소를 정의합니다.
AppFlow는 UDP를 전송 프로토콜로 사용하여 *흐름 레코드*라는 수집된 데이터를 하나 이상의 IPv4 수집기에 전송합니다. 이러한 수집기는 흐름 레코드를 집계하여 실시간 또는 보관된 보고서를 생성합니다.

AppFlow는 트랜잭션 수준에서 HTTP, SSL, TCP 및 SSL_TCP 흐름에 대한 가시성을 제공합니다. 사용자는 모니터링할 흐름 유형을 샘플링 및 필터링할 수 있습니다.

응용 프로그램 트래픽을 샘플링 및 필터링하여 모니터링할 흐름 유형을 제한하려면 가상 서버에 AppFlow를 사용하면 됩니다. AppFlow는 가상 서버에 대한 통계도 제공할 수 있습니다.

또한 응용 프로그램 서버를 나타내는 특정 서비스에 AppFlow를 사용하여 해당 응용 프로그램 서버에 대한 트래픽을 모니터링할 수 있습니다.

자세한 내용은 "AppFlow"를 참조하십시오.

Stream Analytics

웹 사이트 또는 응용 프로그램의 성능은 가장 자주 요청되는 콘텐츠의 제공을 얼마나 잘 최적화하는가에 따라 달라집니다. 캐시 및 압축 등의 기술은 서비스를 클라이언트에 신속하게 제공하는 데 유용하지만 가장 자주 요청되는 리소스를 확인하고 해당 리소스를 캐시 또는 압축할 수 있어야 합니다. 웹 사이트 또는 응용 프로그램 트래픽 관련 실시간 통계를 집계하여 가장 자주 사용되는 리소스를 확인할 수 있습니다. 다른 리소스와 비교하여 특정 리소스가 액세스되는 빈도와 이러한 리소스에서 사용되는 대역폭 양 등의 통계는 해당 리소스를 캐시 또는 압축하여 서버 성능과 네트워크 효율성을 향상시킬 수 있는지 여부를 결정하는 데 도움이 됩니다. 또한 응용 프로그램에 대한 응답 시간과 동시 연결 수 같은 통계도 서버 측 리소스를 개선해야 하는지 여부를 판단하는 데 유용합니다.

웹 사이트 또는 응용 프로그램이 자주 변경되지 않으면 통계 데이터를 수집하는 제품을 사용하고 나중에 수동으로 통계를 분석한 후 콘텐츠 제공을 최적화할 수 있습니다. 하지만 수동 최적화를 수행하고 싶지 않거나 웹 사이트 또는 응용 프로그램이 완전히 동적이라면 통계 데이터를 수집할 뿐 아니라 이러한 통계를 기준으로 리소스 제공을 자동으로 최적화할 수 있는 인프라가 필요합니다. NetScaler 장비에서 이 기능은 Stream Analytics 기능을 통해 제공됩니다. 이 기능은 단일 NetScaler 장비에서 작동하며 사용자가 정의한 기준에 따라 실시간 통계를 수집합니다. NetScaler 정책과 함께 사용할 경우 이 기능은 자동 실시간 트래픽 최적화에 필요한 인프라도 제공합니다.

자세한 내용은 "Stream Analytics"를 참조하십시오.

클라우드 통합 기능

Aug 30, 2016

AutoScale

모든 응용 프로그램은 피크와 저점으로 구성된 특정한 사용량 패턴을 지닙니다. 이러한 부하 차이는 사용 사례에 따른 고유한 여러 가지 요인에 의해 결정되므로 특성상 변화가 많으며 예측하기 어렵습니다. 클라우드 사용자는 사용 중인 응용 프로그램군에서 부하를 지속적으로 모니터링하고 이러한 변화가 최종 사용자에게 최소한의 영향만 미칠 수 있도록 확인해야 합니다. 피크 사용량 기간 중에 응용 프로그램군에 오버로드가 걸려 최종 사용자가 상당한 시간을 대기하면 추가적인 응용 프로그램 인스턴스를 배포해야 합니다. 저점 기간 중에는 추가로 배포되었던 응용 프로그램이 충분히 사용되지 않습니다. 따라서 추가 인스턴스를 제거하거나 불필요한 비용 오버헤드를 방지해야 합니다. 대부분의 경우, 이러한 작업을 수동으로 수행해야 합니다.

조직에서 Citrix CloudPlatform을 사용하여 클라우드 환경을 배포하고 관리하는 경우, 사용자는 Citrix NetScaler 장비와 함께 CloudPlatform의 *AutoScale* 기능을 사용하여 응용 프로그램을 필요에 따라 자동으로 크기를 조정할 수 있습니다. AutoScale 기능은 CloudPlatform의 탄력적인 부하 분산 기능의 일부입니다. CloudPlatform 사용자는 AutoScale 기능을 사용하여 응용 프로그램군의 크기를 상향 및 하향 조정하는 자동 크기 조정을 위해 다양한 조건에 대한 임계값을 지정할 수 있습니다. 그런 다음 CloudPlatform은 NetScaler NITRO API를 사용하여 NetScaler 장비를 구성하여 응용 프로그램 VM(가상 컴퓨터)에 대한 트래픽 부하를 분산하고, 응용 프로그램 임계값과 성능을 모니터링하며, 응용 프로그램군에 VM을 추가하거나 반대로 VM을 제거하기 위해 크기 상향 및 크기 하향 조정 조치를 트리거합니다.

NetScaler 관리자는 NetScaler 장비에 AutoScale을 구성하기 위해 어떤 작업도 수행할 필요가 없습니다. 단, 특정한 필수 구성 요소를 인지하고 AutoScale 구성에서 문제가 발생하는 경우 구성 문제를 해결해야 합니다. 구성 문제를 해결하려면 CloudPlatform이 어떻게 작동하며 CloudPlatform이 어떤 구성을 NetScaler 장비에 적용하는지 인지하고 있어야 합니다. 그리고 NetScaler 장비에 발생한 문제를 해결하는 방법에 대한 해결 지식도 있어야 합니다.

AutoScale에 대한 자세한 내용은"AutoScale: Automatic Scaling in the Citrix CloudPlatform Environment(AutoScale: Citrix CloudPlatform 환경에서 자동 크기 조정)"를 참조하십시오.