



신뢰할 수 없는 클라이언트 네트워크를 관리합니다

StorageGRID

NetApp
September 04, 2024

목차

- 신뢰할 수 없는 클라이언트 네트워크를 관리합니다..... 1
 - 신뢰할 수 없는 클라이언트 네트워크 관리: 개요..... 1
 - 노드의 클라이언트 네트워크를 신뢰할 수 없습니다..... 1

신뢰할 수 없는 클라이언트 네트워크를 관리합니다

신뢰할 수 없는 클라이언트 네트워크 관리: 개요

클라이언트 네트워크를 사용하는 경우 명시적으로 구성된 끝점에서만 인바운드 클라이언트 트래픽을 허용하여 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다.

기본적으로 각 그리드 노드의 클라이언트 네트워크는 `_trusted_` 입니다. 즉, 기본적으로 StorageGRID는 사용 가능한 모든 외부 포트의 각 그리드 노드에 대한 인바운드 연결을 신뢰합니다(의 외부 통신에 대한 정보 참조) [네트워킹 지침](#)을 클릭합니다.

각 노드의 클라이언트 네트워크가 `_untrusted_`로 지정함으로써 StorageGRID 시스템에 대한 악의적인 공격의 위협을 줄일 수 있습니다. 노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 인바운드 연결만 허용합니다. 을 참조하십시오 [로드 밸런서 엔드포인트를 구성합니다](#).

예 1: 게이트웨이 노드는 HTTPS S3 요청만 허용합니다

게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 한다고 가정합니다. 다음과 같은 일반 단계를 수행합니다.

1. 로드 밸런서 엔드포인트 페이지에서 포트 443에서 HTTPS를 통해 S3에 대한 로드 밸런서 끝점을 구성합니다.
2. 신뢰할 수 없는 클라이언트 네트워크 페이지에서 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없도록 지정합니다.

구성을 저장한 후 게이트웨이 노드의 클라이언트 네트워크의 모든 인바운드 트래픽은 포트 443 및 ICMP 에코(ping) 요청의 HTTPS S3 요청을 제외하고 삭제됩니다.

예 2: 스토리지 노드가 S3 플랫폼 서비스 요청을 전송합니다

스토리지 노드에서 아웃바운드 S3 플랫폼 서비스 트래픽을 활성화하되 클라이언트 네트워크의 해당 스토리지 노드에 대한 인바운드 연결을 차단하려는 경우를 가정해 봅니다. 이 일반 단계를 수행합니다.

- 신뢰할 수 없는 클라이언트 네트워크 페이지에서 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 나타냅니다.

구성을 저장한 후 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 Amazon Web Services에 대한 아웃바운드 요청은 계속 허용합니다.

노드의 클라이언트 네트워크를 신뢰할 수 없습니다

클라이언트 네트워크를 사용하는 경우 각 노드의 클라이언트 네트워크를 신뢰할 수 있는지 신뢰할 수 없는지 여부를 지정할 수 있습니다. 또한 확장에 추가된 새 노드의 기본 설정을 지정할 수도 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 [지원되는 웹 브라우저](#).
- 루트 액세스 권한이 있습니다.

- 관리자 노드 또는 게이트웨이 노드가 명시적으로 구성된 끝점에서만 인바운드 트래픽을 수락하도록 하려면 로드 밸런서 끝점을 정의해야 합니다.



로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 신뢰할 수 없는 클라이언트 네트워크 * 를 선택합니다.

신뢰할 수 없는 클라이언트 네트워크 페이지에는 StorageGRID 시스템의 모든 노드가 나열됩니다. 노드의 클라이언트 네트워크를 신뢰할 수 있어야 하는 경우 사용할 수 없는 이유 열에 항목이 포함됩니다.

Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network ☒ Trusted
Default ☐ Untrusted

Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	
Client Network untrusted on 0 nodes.		

Save

2. 새 노드 기본값 설정 * 섹션에서 확장 절차에서 그리드에 새 노드를 추가할 때 기본 설정을 지정합니다.

- * 신뢰 *: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 있습니다.
- * 신뢰할 수 없음 *: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 없습니다. 필요에 따라 이 페이지로 돌아가 특정 새 노드의 설정을 변경할 수 있습니다.



이 설정은 StorageGRID 시스템의 기존 노드에는 영향을 주지 않습니다.

3. 신뢰할 수 없는 클라이언트 네트워크 노드 선택 * 섹션에서 명시적으로 구성된 로드 밸런서 끝점에서만 클라이언트 연결을 허용할 노드를 선택합니다.

제목에서 확인란을 선택하거나 선택 취소하여 모든 노드를 선택하거나 선택 취소할 수 있습니다.

4. 저장 * 을 선택합니다.

새 방화벽 규칙이 즉시 추가되고 적용됩니다. 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.