방화벽 제어

StorageGRID software

NetApp
July 23, 2026

목차

방화벽 제어

외부 방화벽에서 **StorageGRID** 액세스 제어

외부 방화벽에서 특정 포트를 열거나 닫을 수 있습니다.

StorageGRID 관리 노드의 사용자 인터페이스 및 API에 대한 액세스는 외부 방화벽에서 특정 포트를 열거나 닫아 제어할 수 있습니다. 예를 들어, 시스템 액세스를 제어하는 다른 방법 외에도 방화벽에서 테넌트가 Grid Manager에 연결하지 못하도록 차단할 수 있습니다.

StorageGRID 내부 방화벽을 구성하려면 "내부 방화벽 구성"을 참조하십시오.

포트	설명	포트가 열려 있다면...
443	관리자 노드의 기본 HTTPS 포트	웹 브라우저와 관리 API 클라이언트는 그리드 관리자, 그리드 관리 API, 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다. 참고: 포트 443은 일부 내부 트래픽에도 사용됩니다.
8443	관리 노드의 그리드 관리자 포트 제한	• 웹 브라우저와 관리 API 클라이언트는 HTTPS를 사용하여 그리드 관리자 및 그리드 관리 API에 액세스할 수 있습니다. • 웹 브라우저와 관리 API 클라이언트는 테넌트 관리자 또는 테넌트 관리 API에 접근할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.
9443	관리 노드의 테넌트 관리자 포트 제한	• 웹 브라우저와 관리 API 클라이언트는 HTTPS를 사용하여 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다. • 웹 브라우저와 관리 API 클라이언트는 Grid Manager 또는 Grid Management API에 액세스할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.

제한된 Grid Manager 또는 Tenant Manager 포트에서는 싱글 사인온(SSO)을 사용할 수 없습니다. 사용자가 싱글 사인온으로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다.

관련 정보

- "Grid Manager에 로그인합니다"
- "테넌트 계정 생성"
- "외부 통신"

StorageGRID에서 내부 방화벽 제어 관리

StorageGRID는 각 노드에 내부 방화벽을 포함하여 노드에 대한 네트워크 액세스를 제어함으로써 그리드의 보안을 강화합니다. 방화벽을 사용하여 특정 그리드 배포에 필요한 포트를 제외한 모든 포트에 대한 네트워크 액세스를 차단할 수 있습니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에 적용됩니다.

방화벽 제어 페이지의 세 가지 탭을 사용하여 그리드에 필요한 액세스 권한을 사용자 지정합니다.

- **Privileged address list**: 이 탭을 사용하여 닫힌 포트에 대한 특정 액세스를 허용할 수 있습니다. 외부 액세스 관리 탭에서 닫힌 포트에 액세스할 수 있도록 IP 주소 또는 서브넷(CIDR 표기법)을 추가할 수 있습니다.
- 외부 액세스 관리: 이 탭을 사용하여 기본적으로 열려 있는 포트를 닫거나 이전에 닫았던 포트를 다시 열 수 있습니다.
- 신뢰할 수 없는 클라이언트 네트워크: 이 탭을 사용하여 노드가 클라이언트 네트워크에서 들어오는 트래픽을 신뢰할지 여부를 지정합니다.

  이 탭의 설정은 '외부 액세스 관리' 탭의 설정을 재정의합니다.

  - 신뢰할 수 없는 클라이언트 네트워크를 가진 노드는 해당 노드에 구성된 로드 밸런싱 엔드포인트 포트(전역, 노드 인터페이스 및 노드 유형 바인딩 엔드포인트)에 대한 연결만 허용합니다.
  - 로드 밸런서 엔드포인트 포트는 외부 네트워크 관리 탭의 설정과 관계없이 신뢰할 수 없는 클라이언트 네트워크에서 _유일하게 열려 있는 포트_입니다.
  - 신뢰할 수 있는 경우, 외부 액세스 관리 탭에서 열린 모든 포트와 클라이언트 네트워크에서 열린 모든 로드 밸런서 엔드포인트에 액세스할 수 있습니다.

> ⓘ 한 탭에서 설정한 내용이 다른 탭에서 변경한 액세스 권한에 영향을 줄 수 있습니다. 네트워크가 예상대로 작동하는지 확인하려면 모든 탭의 설정을 확인하십시오.

내부 방화벽 제어를 구성하려면 "방화벽 제어 구성"을 참조하십시오.

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 "외부 방화벽에서 액세스 제어"을 참조하십시오.

특권 주소 목록 및 외부 액세스 관리 탭

'특권 주소 목록' 탭에서는 닫혀 있는 그리드 포트에 대한 액세스 권한이 부여된 하나 이상의 IP 주소를 등록할 수 있습니다. '외부 액세스 관리' 탭에서는 선택한 외부 포트 또는 모든 열린 외부 포트(외부 포트는 기본적으로 그리드에 속하지 않은 노드에서 액세스할 수 있는 포트)에 대한 외부 액세스를 차단할 수 있습니다. 이 두 탭은 그리드에 허용해야 하는 정확한 네트워크 액세스를 사용자 지정하기 위해 함께 사용할 수 있습니다.

> ⓘ 권한 있는 IP 주소는 기본적으로 내부 그리드 포트에 대한 액세스 권한이 없습니다.

예시 **1:** 유지 관리 작업을 위해 점프 호스트 사용

보안이 강화된 호스트인 점프 호스트를 네트워크 관리에 사용하려는 경우를 가정해 보겠습니다. 다음과 같은 일반적인 단계를 따를 수 있습니다.

1. 권한 있는 주소 목록 탭을 사용하여 점프 호스트의 IP 주소를 추가하십시오.

2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단할 수 있습니다.

> 포트 443 및 8443을 차단하기 전에 우선 순위 IP 주소를 추가하십시오. 현재 차단된 포트에 연결된 모든 사용자(본인 포함)는 IP 주소가 우선 순위 주소 목록에 추가되지 않으면 Grid Manager에 액세스할 수 없게 됩니다.

구성을 저장하면 그리드의 관리 노드에 있는 모든 외부 포트가 점프 호스트를 제외한 모든 호스트에 대해 차단됩니다. 그러면 점프 호스트를 사용하여 그리드에서 유지 관리 작업을 더욱 안전하게 수행할 수 있습니다.

예시 **2:** 민감한 포트 잠금

민감한 포트와 해당 포트에서 실행되는 서비스를 차단하고 싶다고 가정해 보겠습니다. 다음과 같은 일반적인 단계를 따를 수 있습니다.

1. '권한 있는 주소 목록' 탭을 사용하여 서비스에 액세스해야 하는 호스트에만 액세스 권한을 부여하십시오.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단할 수 있습니다.

> Grid Manager 및 Tenant Manager에 액세스하는 데 할당된 포트(기본 설정 포트는 443 및 8443)에 대한 액세스를 차단하기 전에 권한 있는 IP 주소를 추가하십시오. 차단된 포트에 현재 연결된 모든 사용자(본인 포함)는 IP 주소가 권한 있는 주소 목록에 추가되지 않으면 Grid Manager에 액세스할 수 없게 됩니다.

구성을 저장하면 해당 포트와 해당 포트의 서비스는 권한 있는 주소 목록에 있는 호스트에서만 사용할 수 있습니다. 다른 모든 호스트는 요청이 어떤 인터페이스를 통해 들어오든 관계없이 해당 서비스에 액세스할 수 없습니다.

예시 **3:** 사용하지 않는 서비스에 대한 액세스 비활성화

네트워크 수준에서 사용하지 않을 일부 서비스를 비활성화할 수 있습니다. 예를 들어 HTTP S3 클라이언트 트래픽을 차단하려면 외부 액세스 관리 탭에서 토글을 사용하여 18084번 포트를 차단하면 됩니다.

신뢰할 수 없는 클라이언트 네트워크 탭

클라이언트 네트워크를 사용하는 경우, 명시적으로 구성된 엔드포인트에서만 인바운드 클라이언트 트래픽을 허용함으로써 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다.

기본적으로 각 그리드 노드의 클라이언트 네트워크는 신뢰할 수 있는 상태입니다. 즉, 기본적으로 StorageGRID는 모든 "사용 가능한 외부 포트"에서 각 그리드 노드에 대한 인바운드 연결을 신뢰합니다.

StorageGRID 시스템에 대한 악의적인 공격 위협을 줄이려면 각 노드의 클라이언트 네트워크를 _신뢰할 수 없음_으로 지정하십시오. 노드의 클라이언트 네트워크가 신뢰할 수 없는 경우 해당 노드는 로드 밸런서 엔드포인트로 명시적으로 구성된 포트에서만 수신 연결을 허용합니다. "로드 밸런서 엔드포인트 구성" 및 "방화벽 제어 구성"을 참조하십시오.

예시 **1:** 게이트웨이 노드는 **HTTPS S3** 요청만 허용합니다

게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 설정하려면 다음과 같은 일반적인 단계를 수행합니다.

1. 해당 "로드 밸런서 엔드포인트" 페이지에서 포트 443을 통해 HTTPS를 사용하는 S3용 로드 밸런서 엔드포인트를 구성하십시오.
2. 방화벽 제어 페이지에서 Untrusted를 선택하여 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없는 것으로

지정합니다.

구성을 저장하면 게이트웨이 노드의 클라이언트 네트워크로 들어오는 모든 인바운드 트래픽은 차단되지만, 포트 443의 HTTPS S3 요청과 ICMP 에코(핑) 요청은 예외적으로 허용됩니다.

예시 **2:** 스토리지 노드가 **S3** 플랫폼 서비스 요청을 보냅니다

스토리지 노드에서 S3 플랫폼 서비스로의 아웃바운드 트래픽은 허용하되, 클라이언트 네트워크에서 해당 스토리지 노드로의 인바운드 연결은 차단하고 싶다고 가정해 보겠습니다. 이 경우 일반적으로 다음과 같은 단계를 수행합니다.

- 방화벽 제어 페이지의 '신뢰할 수 없는 클라이언트 네트워크' 탭에서 스토리지 노드의 클라이언트 네트워크가 신뢰할 수 없음을 지정합니다.

구성을 저장하면 스토리지 노드는 클라이언트 네트워크에서 들어오는 트래픽을 더 이상 수락하지 않지만, 구성된 플랫폼 서비스 대상으로 나가는 요청은 계속 허용합니다.

예제 **3: Grid Manager**에 대한 액세스를 서브넷으로 제한하기

특정 서브넷에서만 Grid Manager에 대한 액세스를 허용하려고 한다고 가정합니다. 다음 단계를 수행합니다.

1. 관리 노드의 클라이언트 네트워크를 서브넷에 연결하십시오.
2. 신뢰할 수 없는 클라이언트 네트워크 탭을 사용하여 클라이언트 네트워크를 신뢰할 수 없는 네트워크로 구성하십시오.
3. 관리 인터페이스 로드 밸런서 엔드포인트를 생성할 때 포트를 입력하고 해당 포트에서 액세스할 관리 인터페이스를 선택하십시오.
4. 신뢰할 수 없는 클라이언트 네트워크에 대해 *예*를 선택하십시오.
5. '외부 액세스 관리' 탭을 사용하여 모든 외부 포트를 차단할 수 있습니다(해당 서브넷 외부 호스트에 대해 특권 IP 주소를 설정했는지 여부와 관계없음).

구성을 저장하면 지정한 서브넷에 있는 호스트만 Grid Manager에 액세스할 수 있습니다. 다른 모든 호스트는 차단됩니다.

StorageGRID 내부 방화벽을 구성합니다

StorageGRID 방화벽을 구성하여 StorageGRID 노드의 특정 포트에 대한 네트워크 액세스를 제어할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 귀하는 "방화벽 제어 관리" 및 "네트워킹 가이드라인"에 있는 정보를 검토하셨습니다.
- 관리 노드 또는 게이트웨이 노드가 명시적으로 구성된 엔드포인트에서만 수신 트래픽을 허용하도록 하려면 로드 밸런싱 엔드포인트를 정의해야 합니다.

> 클라이언트 네트워크 구성을 변경할 때, 로드 밸런서 엔드포인트가 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

이 작업 정보

StorageGRID는 각 노드에 내부 방화벽을 포함하고 있어 그리드 노드의 일부 포트를 열거나 닫을 수 있습니다. 방화벽 제어 탭을 사용하여 그리드 네트워크, 관리 네트워크 및 클라이언트 네트워크에서 기본적으로 열려 있는 포트를 열거나 닫을 수 있습니다. 또한 닫혀 있는 그리드 포트에 액세스할 수 있는 권한 있는 IP 주소 목록을 생성할 수도 있습니다. 클라이언트 네트워크를 사용하는 경우 노드가 클라이언트 네트워크에서 들어오는 트래픽을 신뢰할지 여부를 지정하고 클라이언트 네트워크의 특정 포트에 대한 액세스를 구성할 수 있습니다.

그리드 외부의 IP 주소에 대해 반드시 필요한 포트만 열도록 포트 수를 제한하면 그리드 보안이 강화됩니다. 방화벽 제어 탭 세 곳 각각의 설정을 사용하여 필요한 포트만 열리도록 할 수 있습니다.

방화벽 제어 사용에 대한 자세한 내용(예제 포함)은 "방화벽 제어 관리"을 참조하십시오.

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 "외부 방화벽에서 액세스 제어"을 참조하십시오.

액세스 방화벽 제어

단계

1. * 구성 * > * 보안 * > * 방화벽 제어 * 를 선택합니다.

   이 페이지의 세 탭에 대한 설명은 "방화벽 제어 관리"에 있습니다.

2. 방화벽 설정을 구성하려면 아무 탭이나 선택하십시오.

   이 탭들은 어떤 순서로든 사용할 수 있습니다. 한 탭에서 설정한 구성은 다른 탭에서 수행할 수 있는 작업에 영향을 미치지 않습니다. 그러나 한 탭에서 구성을 변경하면 다른 탭에 구성된 포트의 동작이 변경될 수 있습니다.

권한 있는 주소 목록

권한 있는 주소 목록 탭을 사용하여 기본적으로 닫혀 있거나 외부 액세스 관리 탭의 설정에 따라 닫혀 있는 포트에 호스트가 액세스할 수 있도록 허용할 수 있습니다.

특권 IP 주소 및 서브넷은 기본적으로 내부 그리드 액세스가 허용되지 않습니다. 또한, 특권 주소 목록 탭에서 열린 로드 밸런서 엔드포인트 및 추가 포트는 외부 액세스 관리 탭에서 차단된 경우에도 액세스할 수 있습니다.

'권한 있는 주소 목록' 탭의 설정은 '신뢰할 수 없는 클라이언트 네트워크' 탭의 설정을 재정의할 수 없습니다.

단계

1. Privileged address list 탭에서 닫힌 포트에 대한 액세스 권한을 부여할 주소 또는 IP 서브넷을 입력합니다.
2. 선택적으로 *다른 IP 주소 또는 CIDR 표기법의 서브넷 추가*를 선택하여 권한 있는 클라이언트를 추가할 수 있습니다.

   권한 목록에는 가능한 한 적은 주소만 추가하십시오.

3. 선택적으로 *특권 있는 IP 주소가 StorageGRID 내부 포트에 액세스하도록 허용*을 선택할 수 있습니다. 을 참조하십시오."StorageGRID 내부 포트"

이 옵션을 선택하면 내부 서비스에 대한 일부 보호 기능이 제거됩니다. 가능하면 이 옵션을 비활성화하십시오.

4. *저장*을 선택하세요.

외부 액세스 관리

'외부 액세스 관리' 탭에서 포트를 닫으면, 해당 IP 주소를 권한 있는 주소 목록에 추가하지 않는 한 그리드 IP 주소가 아닌 다른 IP 주소로는 해당 포트에 액세스할 수 없습니다. 기본적으로 열려 있는 포트만 닫을 수 있으며, 닫아 놓은 포트만 열 수 있습니다.

'외부 액세스 관리' 탭의 설정은 '신뢰할 수 없는 클라이언트 네트워크' 탭의 설정을 재정의할 수 없습니다. 예를 들어, 노드가 신뢰할 수 없는 것으로 설정된 경우, '외부 액세스 관리' 탭에서 SSH/22 포트가 열려 있더라도 클라이언트 네트워크에서는 해당 포트가 차단됩니다. '신뢰할 수 없는 클라이언트 네트워크' 탭의 설정은 클라이언트 네트워크에서 닫힌 포트(예: 443, 8443, 9443)를 재정의합니다.

단계

1. *외부 액세스 관리*를 선택합니다. 해당 탭에는 그리드에 있는 모든 노드의 외부 포트(기본적으로 그리드에 속하지 않은 노드에서 액세스할 수 있는 포트) 목록이 표 형식으로 표시됩니다.
2. 다음 옵션을 사용하여 열고 닫을 포트를 구성하십시오.
   - 각 포트 옆에 있는 토글을 사용하여 선택한 포트를 열거나 닫습니다.
   - 표에 나열된 모든 포트를 열려면 *표시된 모든 포트 열기*를 선택하십시오.
   - 표에 나열된 모든 포트를 닫으려면 *표시된 모든 포트 닫기*를 선택하십시오.

Grid Manager 포트 443 또는 8443을 닫으면, 귀하를 포함하여 차단된 포트에 현재 연결된 모든 사용자는 IP 주소가 권한 있는 주소 목록에 추가되지 않은 한 Grid Manager에 대한 액세스 권한을 잃게 됩니다.

표 오른쪽의 스크롤 막대를 사용하여 사용 가능한 모든 포트를 확인하십시오. 검색 필드에 포트 번호를 입력하여 외부 포트 설정을 찾을 수 있습니다. 포트 번호를 부분적으로 입력할 수도 있습니다. 예를 들어 *2*를 입력하면 이름에 "2"가 포함된 모든 포트가 표시됩니다.

3. *저장*을 선택합니다

신뢰할 수 없는 클라이언트 네트워크

노드의 클라이언트 네트워크가 신뢰할 수 없는 경우, 해당 노드는 로드 밸런싱 엔드포인트로 구성된 포트와 이 탭에서 선택적으로 추가한 포트에서만 수신 트래픽을 허용합니다. 또한 이 탭을 사용하여 확장에 추가된 새 노드의 기본 설정을 지정할 수 있습니다.

로드 밸런싱 엔드포인트가 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

신뢰할 수 없는 클라이언트 네트워크 탭에서 변경한 구성 내용은 외부 액세스 관리 탭의 설정을 재정의합니다.

단계

1. *신뢰할 수 없는 클라이언트 네트워크*를 선택하십시오.

2. '새 노드 기본값 설정' 섹션에서 확장 절차에서 새 노드가 그리드에 추가될 때 기본 설정이 무엇이어야 하는지 지정합니다.

   - 신뢰됨(기본값): 확장에 노드가 추가되면 해당 클라이언트 네트워크가 신뢰됩니다.
   - 신뢰할 수 없음: 확장에서 노드가 추가되면 해당 노드의 클라이언트 네트워크는 신뢰할 수 없는 것으로 간주됩니다.

     필요에 따라 이 탭으로 돌아와 특정 새 노드의 설정을 변경할 수 있습니다.

     이 설정은 StorageGRID 시스템의 기존 노드에 영향을 미치지 않습니다.

3. 다음 옵션을 사용하여 명시적으로 구성된 로드 밸런서 엔드포인트 또는 추가로 선택한 포트에서만 클라이언트 연결을 허용해야 하는 노드를 선택하십시오.

   - 표에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가하려면 *표시된 노드에 대해 신뢰하지 않음*을 선택하십시오.
   - 표에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에서 제거하려면 *표시된 노드에 대한 신뢰*를 선택하십시오.
   - 각 노드 옆에 있는 토글을 사용하여 선택한 노드에 대해 클라이언트 네트워크를 신뢰할 수 있음 또는 신뢰할 수 없음으로 설정하십시오.

     예를 들어, *표시된 노드에 대해 신뢰하지 않음*을 선택하여 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가한 다음, 개별 노드 옆에 있는 토글 버튼을 사용하여 해당 노드만 신뢰할 수 있는 클라이언트 네트워크 목록에 추가할 수 있습니다.

     표 오른쪽의 스크롤 막대를 사용하여 사용 가능한 모든 노드를 확인했는지 확인하십시오. 검색 필드를 사용하여 노드 이름을 입력하면 해당 노드의 설정을 찾을 수 있습니다. 부분적으로 이름을 입력할 수도 있습니다. 예를 들어 *GW*를 입력하면 이름에 "GW"가 포함된 모든 노드가 표시됩니다.

4. *저장*을 선택하세요.

   새 방화벽 설정은 즉시 적용되고 효력이 발생합니다. 로드 밸런서 엔드포인트가 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.