보안 설정을 구성합니다

StorageGRID 11.7

NetApp
April 12, 2024

목차

보안 설정을 구성합니다

TLS 및 SSH 정책을 관리합니다

TLS 및 SSH 정책은 클라이언트 응용 프로그램과 보안 TLS 연결을 설정하고 내부 StorageGRID 서비스에 대한 보안 SSH 연결을 설정하는 데 사용되는 프로토콜과 암호를 결정합니다.

보안 정책은 TLS 및 SSH가 이동 중인 데이터를 암호화하는 방법을 제어합니다. 일반적으로 시스템이 일반 조건 호환이거나 다른 암호를 사용해야 하는 경우가 아니면 최신 호환성(기본값) 정책을 사용합니다.

이러한 정책에서 암호를 사용하도록 일부 StorageGRID 서비스가 업데이트되지 않았습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 을(를) 보유하고 있습니다 "루트 액세스 권한".

보안 정책을 선택합니다

단계

1. 구성 * > * 보안 * > * 보안 설정 * 을 선택합니다.

   TLS 및 SSH 정책 * 탭에는 사용 가능한 정책이 표시됩니다. 현재 활성 정책은 정책 타일에 녹색 확인 표시로 표시됩니다.

2. 타일을 검토하여 사용 가능한 정책에 대해 알아봅니다.

정책	설명
최신 호환성(기본값)	강력한 암호화가 필요하거나 특별한 요구 사항이 없는 경우 기본 정책을 사용합니다. 이 정책은 대부분의 TLS 및 SSH 클라이언트와 호환됩니다.
레거시 호환성	이전 클라이언트에 대한 추가 호환성 옵션이 필요한 경우 이 정책을 사용합니다. 이 정책의 추가 옵션을 사용하면 최신 호환성 정책보다 보안이 덜 강화될 수 있습니다.
일반 조건	일반 조건 인증이 필요한 경우 이 정책을 사용합니다.

정책	설명
FIPS 엄격한	일반 조건 인증이 필요하고 밸런서 엔드포인트, 테넌트 관리자 및 그리드 관리자를 로드하기 위해 외부 클라이언트 연결에 NetApp 암호화 보안 모듈 3.0.0을 사용해야 하는 경우 이 정책을 사용합니다. 이 정책을 사용하면 성능이 저하될 수 있습니다.
맞춤형	자신의 암호를 적용해야 하는 경우 사용자 지정 정책을 만듭니다.

3. 각 정책의 암호화, 프로토콜 및 알고리즘에 대한 세부 정보를 보려면 * 상세 정보 보기 * 를 선택합니다.
4. 현재 정책을 변경하려면 * 정책 사용 * 을 선택합니다.

   정책 타일에서 * 현재 정책 * 옆에 녹색 확인 표시가 나타납니다.

사용자 지정 보안 정책을 만듭니다

사용자 고유의 암호를 적용해야 하는 경우 사용자 지정 정책을 만들 수 있습니다.

단계

1. 만들려는 사용자 지정 정책과 가장 유사한 정책 타일에서 * 세부 정보 보기 * 를 선택합니다.
2. 클립보드로 복사 * 를 선택한 다음 * 취소 * 를 선택합니다.

3. 사용자 정의 정책 * 타일에서 * 구성 및 사용 * 을 선택합니다.
4. 복사한 JSON을 붙여 넣고 필요한 내용을 변경합니다.
5. Use policy * 를 선택합니다.

   사용자 지정 정책 타일의 * 현재 정책 * 옆에 녹색 확인 표시가 나타납니다.

6. 필요에 따라 * 구성 편집 * 을 선택하여 새 사용자 지정 정책을 더 많이 변경합니다.

일시적으로 기본 보안 정책으로 돌아갑니다

사용자 지정 보안 정책을 구성한 경우 구성된 TLS 정책이 과 호환되지 않는 경우 Grid Manager에 로그인하지 못할 수 있습니다 "구성된 서버 인증서입니다".

일시적으로 기본 보안 정책으로 되돌릴 수 있습니다.

단계

1. 관리자 노드에 로그인:
   a. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
   b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
   c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
   d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

      루트로 로그인하면 프롬프트가 에서 변경됩니다 `$` 를 선택합니다 `#`.

2. 다음 명령을 실행합니다.

   ```
   restore-default-cipher-configurations
   ```

3. 웹 브라우저에서 동일한 관리 노드의 그리드 관리자에 액세스합니다.
4. 의 단계를 따릅니다 보안 정책을 선택합니다 정책을 다시 구성합니다.

네트워크 및 개체 보안을 구성합니다

네트워크 및 개체 보안을 구성하여 저장된 개체를 암호화하고, 특정 S3 및 Swift 요청을 방지하거나, 스토리지 노드에 대한 클라이언트 연결이 HTTPS 대신 HTTP를 사용하도록 허용할 수 있습니다.

저장된 오브젝트 암호화

저장된 오브젝트 암호화를 통해 S3를 통해 수집된 모든 오브젝트 데이터를 암호화할 수 있습니다. 기본적으로 저장된 개체는 암호화되지 않지만 AES - 128 또는 AES - 256 암호화 알고리즘을 사용하여 개체를 암호화하도록 선택할 수 있습니다. 이 설정을 활성화하면 새로 수집된 모든 객체가 암호화되지만 기존 저장된 객체는 변경되지 않습니다. 암호화를 사용하지 않도록 설정하면 현재 암호화된 개체는 암호화된 상태로 유지되지만 새로 수집된 개체는 암호화되지 않습니다.

저장된 오브젝트 암호화 설정은 버킷 레벨 또는 오브젝트 레벨 암호화로 암호화되지 않은 S3 오브젝트에만 적용됩니다.

StorageGRID 암호화 방법에 대한 자세한 내용은 를 참조하십시오 "StorageGRID 암호화 방법을 검토합니다".

클라이언트 수정을 방지합니다

클라이언트 수정 방지 는 시스템 전체 설정입니다. 클라이언트 수정 방지 * 옵션을 선택하면 다음 요청이 거부됩니다.

S3 REST API

- 버킷 요청을 삭제합니다
- 기존 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 수정하는 요청

Swift REST API

- 컨테이너 요청을 삭제합니다
- 기존 객체 수정 요청. 예를 들어, 덮어쓰기, 삭제, 메타데이터 업데이트 등의 작업이 거부됩니다.

스토리지 노드 연결에 대해 **HTTP**를 설정합니다

기본적으로 클라이언트 애플리케이션은 스토리지 노드에 대한 직접 연결에 HTTPS 네트워크 프로토콜을 사용합니다. 비프로덕션 그리드를 테스트할 때와 같이 이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다.

S3 및 Swift 클라이언트가 스토리지 노드에 직접 HTTP 연결을 해야 하는 경우에만 스토리지 노드 연결에 HTTP를 사용합니다. HTTPS 연결만 사용하는 클라이언트 또는 로드 밸런서 서비스에 연결된 클라이언트(에서 할 수 있기 때문에)에는 이 옵션을 사용할 필요가 없습니다 "각 로드 밸런서 엔드포인트를 구성합니다" HTTP 또는 HTTPS 사용).

을 참조하십시오 "요약: 클라이언트 연결을 위한 IP 주소 및 포트" HTTP 또는 HTTPS를 사용하여 스토리지 노드에 연결할 때 사용하는 S3 및 Swift 포트에 대해 알아봅니다.

옵션을 선택합니다

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 루트 액세스 권한이 있습니다.

단계

1. 구성 * > * 보안 * > * 보안 설정 * 을 선택합니다.
2. Network and objects * 탭을 선택합니다.
3. 저장된 개체 암호화의 경우 저장된 개체를 암호화하지 않으려면 * 없음 * (기본값) 설정을 사용하거나 * AES-128 * 또는 * AES-256 * 을 선택하여 저장된 개체를 암호화합니다.
4. S3 및 Swift 클라이언트가 특정 요청을 하지 못하게 하려면 * 클라이언트 수정 방지 * 를 선택합니다(선택 사항).

   이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐싱됩니다.

5. 클라이언트가 스토리지 노드에 직접 접속하고 HTTP 연결을 사용하려는 경우 선택적으로 * 스토리지 노드 연결에 HTTP 사용 * 을 선택합니다.

   요청이 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

6. 저장 * 을 선택합니다.

브라우저 비활성 시간 초과 변경

특정 시간 이상 사용하지 않는 경우 Grid Manager 및 Tenant Manager 사용자가 로그아웃되는지 여부를 제어할 수 있습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 루트 액세스 권한이 있습니다.

이 작업에 대해

브라우저 비활성 시간 초과 기본값은 15분입니다. 사용자의 브라우저가 이 시간 동안 활성화되어 있지 않으면 사용자가 로그아웃됩니다.

필요에 따라 * 다음 이후 비활성 사용자 로그아웃 * 옵션을 설정하여 제한 시간을 늘리거나 줄일 수 있습니다.

브라우저 비활성 시간 초과는 다음과 같은 방법으로 제어됩니다.

- 시스템 보안을 위해 포함되어 있는 별도의 구성 불가능한 StorageGRID 타이머입니다. 기본적으로 각 사용자의 인증 토큰은 사용자가 로그인 한 후 16시간 후에 만료됩니다. 사용자의 인증이 만료되면 브라우저 비활성 시간 초과가 비활성화되거나 브라우저 시간 초과 값에 도달하지 않은 경우에도 해당 사용자는 자동으로 로그아웃됩니다. 토큰을 갱신하려면 사용자가 다시 로그인해야 합니다.
- StorageGRID에 대해 SSO(Single Sign-On)가 활성화된 경우 ID 공급자에 대한 시간 제한 설정입니다.

  SSO가 활성화되어 있고 사용자의 브라우저가 시간 초과되면 사용자는 SSO 자격 증명을 다시 입력하여 StorageGRID에 다시 액세스해야 합니다. 을 참조하십시오 "Single Sign-On 구성".

단계

1. 구성 * > * 보안 * > * 보안 설정 * 을 선택합니다.
2. Browser inactivity timeout *(브라우저 비활성 시간 초과 *) 탭을 선택합니다.
3. 다음 이후 * 사용자 로그아웃 * 필드에서 브라우저 시간 제한 기간을 60초에서 7일 사이로 지정합니다.

   브라우저 제한 시간을 초, 분, 시간 또는 일 단위로 지정할 수 있습니다.

4. 저장 * 을 선택합니다. 브라우저가 지정된 시간 동안 비활성 상태인 경우 사용자는 Grid Manager 또는 Tenant Manager에서 로그아웃됩니다.

   새 설정은 현재 로그인한 사용자에게는 영향을 주지 않습니다. 사용자는 다시 로그인하거나 브라우저를 새로 고쳐야 새 시간 초과 설정을 적용할 수 있습니다.