



StorageGRID를 클라우드 계층으로 연결 StorageGRID

NetApp
April 10, 2024

This PDF was generated from <https://docs.netapp.com/ko-kr/storagegrid-116/fabricpool/information-needed-to-attach-storagegrid-as-cloud-tier.html> on April 10, 2024. Always check docs.netapp.com for the latest.

목차

StorageGRID를 클라우드 계층으로 연결	1
StorageGRID를 클라우드 계층으로 연결하는 데 필요한 정보	1
로드 밸런싱에 대한 모범 사례	2
고가용성 그룹에 대한 Best Practice	4
StorageGRID IP 주소에 대해 DNS 서버를 구성합니다	5
FabricPool에 대한 고가용성(HA) 그룹을 생성합니다	5
FabricPool용 로드 밸런서 끝점을 만듭니다	6
FabricPool에 대한 테넌트 계정을 생성합니다	8
S3 버킷을 생성하고 액세스 키를 얻습니다	9

StorageGRID를 클라우드 계층으로 연결

StorageGRID를 클라우드 계층으로 연결하는 데 필요한 정보

StorageGRID를 FabricPool의 클라우드 계층으로 연결하려면 먼저 StorageGRID에서 몇 가지 구성 단계를 수행하고 특정 값을 얻어야 합니다.

이 작업에 대해

다음 표에는 StorageGRID를 FabricPool의 클라우드 계층으로 연결할 때 ONTAP에 제공해야 하는 정보가 나와 있습니다. 이 섹션의 항목에서는 StorageGRID 그리드 관리자 및 테넌트 관리자를 사용하여 필요한 정보를 얻는 방법을 설명합니다.



나열된 정확한 필드 이름과 ONTAP에 필요한 값을 입력하는 프로세스는 ONTAP CLI(스토리지 애그리게이트 오브젝트 저장소 구성 생성) 또는 ONTAP System Manager(* 스토리지 * > * 애그리게이트 및 디스크 * > * 클라우드 계층 *)를 사용하는지 여부에 따라 달라집니다.

자세한 내용은 다음을 참조하십시오.

- ["TR-4598: ONTAP 9.9.1의 FabricPool 모범 사례"](#)
- ["ONTAP 9 설명서"](#)

ONTAP 필드	설명
오브젝트 저장소 이름	고유하고 설명이 포함된 이름입니다. 예를 들어, 'storageGRID_Cloud_Tier'와 같습니다.
공급자 유형입니다	StorageGRID(ONTAP System Manager) 또는 SGWS(ONTAP CLI).
포트	FabricPool가 StorageGRID에 연결할 때 사용할 포트입니다. StorageGRID 로드 밸런서 끝점을 정의할 때 사용할 포트 번호를 결정합니다. FabricPool용 로드 밸런서 끝점을 만듭니다
서버 이름입니다	StorageGRID 로드 밸런서 끝점의 FQDN(정규화된 도메인 이름)입니다. 예를 들어, '3.storagegrid.company.com'. 다음 사항에 유의하십시오. <ul style="list-style-type: none">• 여기에서 지정하는 도메인 이름은 StorageGRID 로드 밸런서 끝점에 대해 업로드하는 CA 인증서의 도메인 이름과 일치해야 합니다.• 이 도메인 이름의 DNS 레코드는 StorageGRID에 연결하는 데 사용할 각 IP 주소에 매핑되어야 합니다. StorageGRID IP 주소에 대해 DNS 서버를 구성합니다

ONTAP 필드	설명
컨테이너 이름입니다	<p>이 ONTAP 클러스터에 사용할 StorageGRID 버킷의 이름입니다. 예를 들어, '배합통'을 예로 들 수 있습니다. 이 버킷을 테넌트 관리자에서 생성하거나 ONTAP 9.10 System Manager부터 FabricPool 설정 마법사를 사용하여 버킷을 생성할 수 있습니다.</p> <p>다음 사항에 유의하십시오.</p> <ul style="list-style-type: none"> • 구성을 생성한 후에는 버킷 이름을 변경할 수 없습니다. • 버킷은 버전 관리를 활성화할 수 없습니다. • 데이터를 StorageGRID에 계층화할 각 ONTAP 클러스터에 다른 버킷을 사용해야 합니다. <p>S3 버킷을 생성하고 액세스 키를 얻습니다</p>
액세스 키 및 비밀번호	<p>StorageGRID 테넌트 계정의 액세스 키 및 암호 액세스 키입니다.</p> <p>이러한 값은 테넌트 관리자에서 생성합니다.</p> <p>S3 버킷을 생성하고 액세스 키를 얻습니다</p>
SSL	<p>활성화해야 합니다.</p>
오브젝트 저장소 인증서	<p>StorageGRID 로드 밸런서 끝점을 만들 때 업로드한 CA 인증서입니다.</p> <ul style="list-style-type: none"> • 참고: * 중간 CA가 StorageGRID 인증서를 발급한 경우 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우 루트 CA 인증서를 제공해야 합니다. <p>FabricPool용 로드 밸런서 끝점을 만듭니다</p>

작업을 마친 후

필요한 StorageGRID 정보를 얻은 후 ONTAP로 이동하여 StorageGRID를 클라우드 계층으로 추가하고, 클라우드 계층을 Aggregate로 추가한 다음 볼륨 계층화 정책을 설정할 수 있습니다.

로드 밸런싱에 대한 모범 사례

StorageGRID를 FabricPool 클라우드 계층으로 연결하기 전에 StorageGRID 그리드 관리자를 사용하여 하나 이상의 로드 밸런서 끝점을 구성해야 합니다.

로드 밸런싱이란 무엇입니까?

데이터가 FabricPool에서 StorageGRID 시스템으로 계층화되면 StorageGRID는 로드 밸런서를 사용하여 수집 및 검색 워크로드를 관리합니다. 로드 밸런싱은 여러 스토리지 노드에 FabricPool 워크로드를 분산하여 속도와 연결 용량을 극대화합니다.

StorageGRID 로드 밸런서 서비스는 모든 관리 노드 및 모든 게이트웨이 노드에 설치되며 계층 7 로드 밸런싱을

제공합니다. 클라이언트 요청에 대한 TLS(Transport Layer Security) 종료를 수행하고 요청을 검사하며 스토리지 노드에 대한 새로운 보안 연결을 설정합니다.

각 노드의 로드 밸런서 서비스는 클라이언트 트래픽을 스토리지 노드로 전달할 때 독립적으로 작동합니다. 로드 밸런서 서비스는 가중 프로세스를 통해 더 많은 요청을 CPU 가용성이 높은 스토리지 노드로 라우팅합니다.

StorageGRID 로드 밸런서 서비스가 권장되는 로드 밸런싱 메커니즘이지만 타사 로드 밸런서를 대신 통합할 수도 있습니다. 자세한 내용은 NetApp 어카운트 담당자에게 문의하거나 ["TR-4626: StorageGRID 타사 및 글로벌 로드 밸런서"](#)를 참조하십시오.



게이트웨이 노드의 별도의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않으며 FabricPool에서 더 이상 사용하지 않는 것이 좋습니다.

StorageGRID 로드 밸런싱에 대한 Best Practice

일반적으로 StorageGRID 시스템의 각 사이트에는 부하 분산 서비스가 있는 두 개 이상의 노드가 포함되어야 합니다. 예를 들어 사이트에는 두 개의 게이트웨이 노드 또는 관리 노드와 게이트웨이 노드가 모두 포함될 수 있습니다. SG100 또는 SG1000 서비스 어플라이언스, 베어 메탈 노드 또는 가상 머신(VM) 기반 노드를 사용 중이든, 각 로드 밸런싱 노드에 적절한 네트워킹, 하드웨어 또는 가상화 인프라가 있는지 확인하십시오.

게이트웨이 노드 및 관리 노드가 수신 및 발신 FabricPool 요청에 사용할 포트를 정의하려면 StorageGRID 로드 밸런서 끝점을 구성해야 합니다.

로드 밸런서 끝점 인증서에 대한 Best Practice

FabricPool과 함께 사용할 로드 밸런서 끝점을 만들 때는 HTTPS를 프로토콜로 사용해야 합니다. TLS 암호화 없이 StorageGRID와 통신하는 것은 지원되지만 권장되지 않습니다.

그런 다음 공개적으로 신뢰할 수 있는 인증서나 개인 인증 기관(CA)에서 서명한 인증서를 업로드하거나 자체 서명된 인증서를 생성할 수 있습니다. 이 인증서를 통해 ONTAP는 StorageGRID를 사용하여 인증할 수 있습니다.

가장 좋은 방법은 CA 서버 인증서를 사용하여 연결을 보호하는 것입니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다.

로드 밸런서 끝점에서 사용할 CA 인증서를 요청할 때는 인증서의 도메인 이름이 해당 로드 밸런서 끝점에 대해 ONTAP에 입력한 서버 이름과 일치하는지 확인합니다. 가능한 경우 와일드카드(*)를 사용하여 가상 호스트 스타일 URL을 허용합니다. 예를 들면 다음과 같습니다.

```
*.s3.storagegrid.company.com
```

StorageGRID를 FabricPool 클라우드 계층으로 추가하는 경우 루트 및 하위 CA(인증 기관) 인증서뿐만 아니라 ONTAP 클러스터에 동일한 인증서를 설치해야 합니다.



StorageGRID는 여러 가지 목적으로 서버 인증서를 사용합니다. 로드 밸런서 서비스에 연결하는 경우 S3 및 Swift API 인증서를 선택적으로 사용할 수 있습니다.

로드 밸런싱 끝점의 서버 인증서에 대한 자세한 내용은 다음을 참조하십시오.

- [로드 밸런서 엔드포인트를 구성합니다](#)

고가용성 그룹에 대한 Best Practice

StorageGRID를 FabricPool 클라우드 계층으로 연결하기 전에 StorageGRID 그리드 관리자를 사용하여 고가용성(HA) 그룹을 구성해야 합니다.

고가용성(HA) 그룹이란 무엇입니까?

로드 밸런서 서비스를 항상 사용하여 FabricPool 데이터를 관리할 수 있도록 여러 관리 및 게이트웨이 노드의 네트워크 인터페이스를 고가용성(HA) 그룹이라고 하는 단일 엔터티로 그룹화할 수 있습니다. HA 그룹의 액티브 노드에 장애가 발생할 경우 그룹의 다른 노드가 워크로드를 계속 관리할 수 있습니다.

각 HA 그룹은 연결된 노드의 공유 서비스에 대한 고가용성 액세스를 제공합니다. 예를 들어, 게이트웨이 노드에만 있거나 관리 노드와 게이트웨이 노드 모두에 있는 인터페이스로 구성된 HA 그룹은 공유 로드 밸런서 서비스에 대한 고가용성 액세스를 제공합니다.

HA 그룹을 생성하려면 다음 일반 단계를 수행합니다.

1. 하나 이상의 관리 노드 또는 게이트웨이 노드에 대한 네트워크 인터페이스를 선택합니다. 그리드 네트워크 인터페이스(eth0), 클라이언트 네트워크 인터페이스(eth2) 또는 VLAN 인터페이스를 선택할 수 있습니다.



VLAN 인터페이스를 사용하여 FabricPool 트래픽을 분리하려는 경우 네트워크 관리자는 먼저 트렁크 인터페이스와 해당 VLAN을 구성해야 합니다. 각 VLAN은 숫자 ID 또는 태그로 식별됩니다. 예를 들어 네트워크에서 FabricPool 트래픽에 VLAN 100을 사용할 수 있습니다.

2. 그룹에 하나 이상의 가상 IP(VIP) 주소를 할당합니다. FabricPool과 같은 클라이언트 응용 프로그램은 이러한 VIP 주소를 사용하여 StorageGRID에 연결할 수 있습니다.
3. 기본 인터페이스로 사용할 인터페이스를 지정하고 백업 인터페이스의 우선 순위를 결정합니다. Primary 인터페이스는 장애가 발생하지 않는 한 Active 인터페이스입니다.

HA 그룹에 둘 이상의 인터페이스가 포함되어 있고 기본 인터페이스에 장애가 발생하면 VIP 주소가 우선 순위 순서대로 첫 번째 백업 인터페이스로 이동합니다. 이 인터페이스에 장애가 발생하면 VIP 주소가 다음 백업 인터페이스로 이동합니다. 이 장애 조치 프로세스는 일반적으로 몇 초 밖에 걸리지 않으며 클라이언트 응용 프로그램에 거의 영향을 주지 않고 정상적인 재시도 동작에 의존하여 작업을 계속할 수 있을 정도로 빠릅니다.

장애가 해결되고 더 높은 우선 순위 인터페이스를 다시 사용할 수 있게 되면 VIP 주소가 사용 가능한 가장 높은 우선 순위 인터페이스로 자동 이동됩니다.

고가용성(HA) 그룹에 대한 모범 사례

FabricPool용 StorageGRID HA 그룹을 생성하는 모범 사례는 다음과 같이 워크로드에 따라 다릅니다.

- 운영 워크로드 데이터에 FabricPool을 사용할 계획이라면 데이터 검색이 중단되지 않도록 최소 2개의 로드 밸런싱 노드를 포함하는 HA 그룹을 생성해야 합니다.
- FabricPool 스냅샷 전용 볼륨 계층화 정책 또는 비 운영 로컬 성능 계층(예: 재해 복구 위치 또는 NetApp SnapMirror® 대상)을 사용하려는 경우 하나의 노드만 사용하여 HA 그룹을 구성할 수 있습니다.

다음 지침은 Active-Backup HA에 대한 HA 그룹 설정(한 노드는 활성 상태이고 한 노드는 백업)에 대해 설명합니다.

그러나 DNS 라운드 로빈 또는 Active-Active HA를 사용하는 것이 좋습니다. 이러한 기타 HA 구성의 이점에 대한 자세한 내용은 [를 참조하십시오 HA 그룹에 대한 구성 옵션](#).

StorageGRID IP 주소에 대해 DNS 서버를 구성합니다

고가용성 그룹 및 로드 밸런서 끝점을 구성한 후에는 ONTAP 시스템의 DNS(도메인 이름 시스템)에 StorageGRID 서버 이름(정규화된 도메인 이름)을 FabricPool가 연결에 사용할 IP 주소에 연결하는 레코드가 포함되어 있는지 확인해야 합니다.

DNS 레코드에 입력하는 IP 주소는 로드 밸런싱 노드의 HA 그룹을 사용하는지 여부에 따라 달라집니다.

- HA 그룹을 구성한 경우 FabricPool는 해당 HA 그룹의 가상 IP 주소에 연결됩니다.
- HA 그룹을 사용하지 않는 경우 FabricPool는 게이트웨이 노드 또는 관리 노드의 IP 주소를 사용하여 StorageGRID 로드 밸런서 서비스에 연결할 수 있습니다.

또한 DNS 레코드가 와일드카드 이름을 포함하여 필요한 모든 끝점 도메인 이름을 참조하는지 확인해야 합니다.

FabricPool에 대한 고가용성(HA) 그룹을 생성합니다

FabricPool와 함께 사용하도록 StorageGRID를 구성할 때 HA(고가용성) 그룹을 하나 이상 선택적으로 생성할 수 있습니다. HA 그룹은 관리 노드, 게이트웨이 노드 또는 둘 다에서 하나 이상의 네트워크 인터페이스로 구성됩니다.

필요한 것

- [를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저](#).
- 루트 액세스 권한이 있습니다.
- VLAN을 사용하려는 경우 VLAN 인터페이스를 만들었습니다. [을 참조하십시오 VLAN 인터페이스를 구성합니다](#).

이 작업에 대해

각 HA 그룹은 가상 IP 주소(VIP)를 사용하여 연결된 노드의 공유 서비스에 대한 고가용성 액세스를 제공합니다.

이 작업에 대한 자세한 내용은 [을 참조하십시오 고가용성 그룹을 관리합니다](#).

단계

1. 구성 > * 네트워크 > * 고가용성 그룹 * 을 선택합니다.
2. Create * 를 선택합니다.
3. 고유한 이름과 설명을 입력합니다(선택 사항).
4. 이 HA 그룹에 추가할 인터페이스를 하나 이상 선택하십시오.

열 머리글을 사용하여 행을 정렬하거나 검색어를 입력하여 인터페이스를 보다 빠르게 찾을 수 있습니다.

5. 이 HA 그룹에 대한 기본 인터페이스 및 백업 인터페이스를 확인합니다.

행을 끌어 놓아서 * Priority order * 열의 값을 변경합니다.

목록의 첫 번째 인터페이스는 기본 인터페이스입니다. Primary 인터페이스는 장애가 발생하지 않는 한 Active

인터페이스입니다.

HA 그룹에 둘 이상의 인터페이스가 포함되어 있고 활성 인터페이스에 장애가 발생하면 VIP 주소가 우선 순위 순서대로 첫 번째 백업 인터페이스로 이동합니다. 이 인터페이스에 장애가 발생하면 VIP 주소가 다음 백업 인터페이스로 이동합니다. 장애가 해결되면 VIP 주소가 사용 가능한 우선 순위가 가장 높은 인터페이스로 다시 이동됩니다.

6. CIDR 표기법 —로 VIP 서브넷을 지정합니다. IPv4 주소 뒤에 슬래시와 서브넷 길이(0-32)를 입력합니다.

네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. 예를 들어, '192.16.0.0/22'가 있습니다.

7. 선택적으로, StorageGRID 액세스에 사용되는 ONTAP IP 주소가 StorageGRID VIP 주소와 동일한 서브넷에 없는 경우 StorageGRID VIP 로컬 게이트웨이 IP 주소를 입력합니다. 로컬 게이트웨이 IP 주소는 VIP 서브넷 내에 있어야 합니다.
8. HA 그룹에 대한 가상 IP 주소를 하나 이상 입력합니다. 최대 10개의 IP 주소를 추가할 수 있습니다. 모든 VIP는 VIP 서브넷 내에 있어야 합니다.

IPv4 주소를 하나 이상 입력해야 합니다. 선택적으로 추가 IPv4 및 IPv6 주소를 지정할 수 있습니다.

9. Create HA group * 을 선택한 다음 * Finish * 를 선택합니다.

FabricPool용 로드 밸런서 끝점을 만듭니다

FabricPool과 함께 사용하도록 StorageGRID를 구성할 때는 로드 밸런서 끝점을 구성하고 로드 밸런서 끝점 인증서를 업로드해야 합니다. 이 인증서는 ONTAP과 StorageGRID 간의 연결을 보호하는 데 사용됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 [지원되는 웹 브라우저](#).
- 루트 액세스 권한이 있습니다.
- 다음 파일이 있습니다.
 - 서버 인증서: 사용자 지정 서버 인증서 파일입니다.
 - 서버 인증서 개인 키: 사용자 지정 서버 인증서 개인 키 파일입니다.
 - CA 번들: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

이 작업에 대해

이 작업에 대한 자세한 내용은 을 참조하십시오 [로드 밸런서 엔드포인트를 구성합니다](#).

단계

1. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다.
2. Create * 를 선택합니다.

×

Create a load balancer endpoint

1 Enter endpoint details

2 Select binding mode

3 Attach certificate

Endpoint details

Name ?

Port ?

Enter an unused port or accept the suggested port.

10443

Client type ?

Select the type of client application that will use this endpoint.

☒ S3
☐ Swift

Network protocol ?

Select the network protocol clients will use with this endpoint. If you select HTTPS, attach the security certificate before saving the endpoint.

☐ HTTPS (recommended)
☒ HTTP

Cancel

Continue

3. 끝점 세부 정보를 입력합니다.

필드에 입력합니다	설명
이름	끝점에 대한 설명 이름입니다
포트	<p>로드 밸런싱에 사용할 StorageGRID 포트입니다. 이 필드의 기본값은 10443이지만 사용하지 않는 외부 포트는 입력할 수 있습니다. 80 또는 443을 입력하면 엔드포인트는 게이트웨이 노드에서만 구성됩니다. 이러한 포트는 관리 노드에 예약되기 때문입니다.</p> <ul style="list-style-type: none"> 참고: * 다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. 를 참조하십시오 네트워크 포트 참조. <p>StorageGRID를 FabricPool 클라우드 계층으로 연결할 때 ONTAP에 동일한 포트 번호를 제공해야 합니다.</p>
클라이언트 유형입니다	S3 * 를 선택합니다.

필드에 입력합니다	설명
네트워크 프로토콜	<p>HTTPS * 를 선택합니다.</p> <p>• 참고 *: * HTTP * 사용은 지원되지만 권장되지 않습니다.</p>

4. Continue * 를 선택합니다.

5. 바인딩 모드를 지정합니다.

글로벌 * 설정(권장)을 사용하거나 이 끝점의 접근성을 다음 중 하나로 제한합니다.

- 특정 노드의 특정 네트워크 인터페이스
- 특정 HA(고가용성) 가상 IP 주소(VIP) 워크로드를 훨씬 더 높은 수준으로 격리해야 하는 경우에만 이 옵션을 사용하십시오.

6. Continue * 를 선택합니다.

7. 인증서 업로드 * (권장)를 선택한 다음 서버 인증서, 인증서 개인 키 및 선택적 CA 번들로 이동합니다.

8. Create * 를 선택합니다.



끝점 인증서 변경 내용을 모든 노드에 적용하는 데 최대 15분이 걸릴 수 있습니다.

FabricPool에 대한 테넌트 계정을 생성합니다

FabricPool용 그리드 관리자에서 테넌트 계정을 만들어야 합니다.

필요한 것

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

이 작업에 대해

테넌트 계정을 사용하면 클라이언트 애플리케이션이 StorageGRID에 객체를 저장하고 검색할 수 있습니다. 각 테넌트 계정에는 고유한 계정 ID, 인증된 그룹 및 사용자, 버킷 및 객체가 있습니다.

여러 ONTAP 클러스터에 동일한 테넌트 계정을 사용할 수 있습니다. 또는 필요에 따라 각 ONTAP 클러스터에 대한 전용 테넌트 계정을 생성할 수 있습니다.



이 지침에서는 Grid Manager에 대해 SSO(Single Sign-On)를 구성했다고 가정합니다. SSO가 활성화되지 않은 경우 를 사용합니다 [테넌트 계정을 생성하기 위한 지침입니다](#) 대신

단계

1. Tenants * 를 선택합니다.
2. Create * 를 선택합니다.
3. 표시 이름과 설명을 입력합니다.
4. S3 * 를 선택합니다.

5. 스토리지 할당량 * 필드는 비워 둡니다.
6. 플랫폼 서비스 사용을 활성화하려면 * 플랫폼 서비스 허용 * 을 선택합니다.

플랫폼 서비스가 설정된 경우 테넌트는 외부 서비스에 액세스하는 CloudMirror 복제와 같은 기능을 사용할 수 있습니다.

7. 자체 ID 소스 사용 * 을 선택하지 마십시오.
8. S3 선택 허용 * 을 선택하지 마십시오.
9. 테넌트에 대한 초기 루트 액세스 권한을 가지려면 그리드 관리자에서 기존 통합 그룹을 선택합니다.
10. 테넌트 생성 * 을 선택합니다.

S3 버킷을 생성하고 액세스 키를 얻습니다

FabricPool 워크로드에 StorageGRID를 사용하기 전에 FabricPool 데이터용 S3 버킷을 생성해야 합니다. 또한 FabricPool에 사용할 테넌트 계정에 대한 액세스 키와 비밀 액세스 키를 얻어야 합니다.

필요한 것

- FabricPool 사용을 위해 테넌트 계정을 만들었습니다.

이 작업에 대해

다음 지침은 StorageGRID 테넌트 관리자를 사용하여 버킷을 생성하고 액세스 키를 얻는 방법을 설명합니다. 테넌트 관리 API 또는 StorageGRID S3 REST API를 사용하여 이러한 작업을 수행할 수도 있습니다. 또는 ONTAP 9.10을 사용하는 경우 대신 FabricPool 설정 마법사를 사용하여 버킷을 생성할 수 있습니다.

자세한 내용:

- [테넌트 계정을 사용합니다](#)
- [S3을 사용합니다](#)

단계

1. 테넌트 관리자에 로그인합니다.

다음 중 하나를 수행할 수 있습니다.

- Grid Manager의 Tenant Accounts 페이지에서 테넌트의 * Sign In * 링크를 선택하고 자격 증명을 입력합니다.
- 웹 브라우저에 테넌트 계정의 URL을 입력하고 자격 증명을 입력합니다.

2. FabricPool 데이터용 S3 버킷을 생성합니다.

사용하려는 각 ONTAP 클러스터에 대해 고유한 버킷을 생성해야 합니다.

- a. 스토리지(S3) * > * 버킷 * 을 선택합니다.
- b. Create bucket * 을 선택합니다.
- c. FabricPool과 함께 사용할 StorageGRID 버킷의 이름을 입력합니다. 예를 들어, '배합통'을 예로 들 수 있습니다.



버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

버킷 이름은 다음 규칙을 준수해야 합니다.

- 각 StorageGRID 시스템에서 고유해야 합니다(테넌트 계정에서만 고유한 것은 아님).
- DNS를 준수해야 합니다.
- 3자 이상 63자 이하여야 합니다.
- 인접한 레이블이 마침표로 구분된 하나 이상의 레이블일 수 있습니다. 각 레이블은 소문자 또는 숫자로 시작하고 끝나야 하며 소문자, 숫자 및 하이픈만 사용할 수 있습니다.
- 텍스트 형식의 IP 주소처럼 보이지 않아야 합니다.
- 가상 호스팅 스타일 요청에서 기간을 사용하지 않아야 합니다. 마침표는 서버 와일드카드 인증서 확인에 문제를 일으킬 수 있습니다.

d. 이 버킷의 영역을 선택합니다.

기본적으로 모든 버킷은 us-east-1 영역에 생성됩니다.

Create bucket

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

fabricpool-bucket

Region ?

us-east-1

Cancel

Create bucket

e. Create bucket * 을 선택합니다.



FabricPool 버킷의 경우 권장되는 버킷 정합성 수준은 새 버킷의 기본 설정인 * 읽기 후 새 쓰기 * 입니다. 사용 가능 * 또는 기타 정합성 보장 레벨을 사용하기 위해 FabricPool 버킷을 편집하지 마십시오.

3. 액세스 키와 비밀 액세스 키를 생성합니다.

- 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.
- Create key * 를 선택합니다.

- c. Create access key * 를 선택합니다.
- d. 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 복사하거나 * Download.csv * 를 선택하여 액세스 키 ID와 비밀 액세스 키가 포함된 스프레드시트 파일을 저장합니다.

StorageGRID를 FabricPool 클라우드 계층으로 구성할 때 ONTAP에 이러한 값을 입력합니다.



나중에 새 액세스 키와 비밀 액세스 키를 생성하는 경우 ONTAP가 중단 없이 StorageGRID에 데이터를 저장하고 검색할 수 있도록 ONTAP에서 해당 값을 즉시 업데이트해야 합니다.

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.