클라우드 타겟을 통한 백업 보호

ONTAP 9

NetApp
April 24, 2024

목차

클라우드 타겟을 통한 백업 보호

클라우드 타겟 관계에 대한 요구사항

소스 및 타겟 환경이 S3 SnapMirror 클라우드 백업 보호에 대한 클라우드 타겟 요구사항을 충족하는지 확인합니다.

데이터 버킷에 액세스하려면 오브젝트 저장소 공급자의 유효한 계정 자격 증명이 있어야 합니다.

클러스터가 클라우드 오브젝트 저장소에 연결하려면 먼저 클러스터에서 인터클러스터 네트워크 인터페이스 및 IPspace를 구성해야 합니다. 각 노드에서 Enter 클러스터 네트워크 인터페이스를 생성하여 로컬 스토리지에서 클라우드 오브젝트 저장소로 데이터를 원활하게 전송해야 합니다.

StorageGRID 대상의 경우 다음 정보를 알아야 합니다.

- FQDN(정규화된 도메인 이름) 또는 IP 주소로 표시되는 서버 이름입니다
- 버킷 이름. 버킷이 이미 있어야 합니다
- 액세스 키
- 비밀 키

또한 StorageGRID 서버 인증서에 서명하는 데 사용되는 CA 인증서는 '보안 인증서 설치 명령'을 사용하여 ONTAP S3 클러스터의 관리 스토리지 VM에 설치해야 합니다. 자세한 내용은 을 참조하십시오 "CA 인증서를 설치하는 중입니다" StorageGRID를 사용하는 경우

AWS S3 타겟의 경우 다음 정보를 알아야 합니다.

- FQDN(정규화된 도메인 이름) 또는 IP 주소로 표시되는 서버 이름입니다
- 버킷 이름. 버킷이 이미 있어야 합니다
- 액세스 키
- 비밀 키

ONTAP 클러스터의 관리 스토리지 VM에 대한 DNS 서버는 FQDN(사용된 경우)을 IP 주소로 확인할 수 있어야 합니다.

새 버킷에 대한 백업 관계 생성(클라우드 타겟)

새 S3 버킷을 생성할 때 StorageGRID 시스템 또는 Amazon S3 구축 등 오브젝트 저장소 공급자의 S3 SnapMirror 타겟 버킷에 즉시 백업할 수 있습니다.

시작하기 전에

- 객체 저장소 공급자에 대한 유효한 계정 자격 증명 및 구성 정보가 있습니다.
- 소스 시스템에 인터클러스터 네트워크 인터페이스 및 IPspace가 구성되었습니다.
- • 소스 스토리지 VM의 DNS 구성은 타겟의 FQDN을 확인할 수 있어야 합니다.

시스템 관리자

1. 스토리지 VM을 편집하여 사용자를 추가하고 사용자를 그룹에 추가합니다.
   a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭하고 을 클릭합니다 S3 * 아래.

      을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.

2. 소스 시스템에 Cloud Object Store 추가:
   a. 보호 > 개요 * 를 클릭한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.
   b. 추가 * 를 클릭한 다음 * Amazon S3 * 또는 * StorageGRID * 를 선택합니다.
   c. 다음 값을 입력합니다.
      - 클라우드 오브젝트 저장소 이름
      - URL 스타일(경로 또는 가상 호스팅)
      - 스토리지 VM(S3에 대해 활성화됨)
      - 개체 저장소 서버 이름(FQDN)
      - 오브젝트 저장소 인증서
      - 액세스 키
      - 비밀 키
      - 컨테이너(버킷) 이름입니다
3. S3 SnapMirror 정책이 없는 경우 기본 정책을 사용하지 않으려면 다음과 같이 하십시오.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 을 클릭합니다 → 보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
      - 정책 이름과 설명을 입력합니다.
      - 정책 범위, 클러스터 또는 SVM을 선택합니다
      - S3 SnapMirror 관계에 대해 * Continuous * 를 선택합니다.
      - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. SnapMirror 보호를 통해 버킷 생성:
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력한 다음 * 추가 옵션 * 을 클릭합니다.
   c. 사용 권한 * 에서 * 추가 * 를 클릭합니다. 사용 권한 확인은 선택 사항이지만 사용하는 것이 좋습니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * 조치 * - 다음 값이 표시되는지 확인합니다.

```
`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetO
bjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
```

- * 리소스 * - 기본값(_(버켓 이름, 버켓 이름/ *) 또는 필요한 기타 값을 사용합니다.

  을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.

d. 보호 * 에서 * SnapMirror(ONTAP 또는 클라우드) * 를 선택하고 * 클라우드 스토리지 * 를 선택한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.

Save * 를 클릭하면 소스 스토리지 VM에 새 버킷이 생성되고 클라우드 오브젝트 저장소에 백업됩니다.

CLI를 참조하십시오

1. 이 SVM에서 처음으로 S3 SnapMirror 관계를 구축할 경우, 소스 및 타겟 SVM 모두에 루트 사용자 키가 있는지 확인하고 그렇지 않을 경우 다시 생성하십시오. 'vserver object-store-server user show' + 루트 사용자에 대한 액세스 키가 있는지 확인하십시오. 그렇지 않으면 다음을 입력합니다. 'vserver object-store-server user reenate-keys-vserver svm_name-user_root_'+키가 이미 있으면 키를 다시 생성하지 마십시오.
2. 소스 SVM에서 버킷을 생성합니다. 'vserver object-store-server bucket create-vserver_svm_name_-bucket_bucket_name_[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'
3. 기본 버킷 정책에 액세스 규칙을 추가합니다. 'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_store_resources_[-sid_text_][-index_integer_integer

   예

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. S3 SnapMirror 정책이 없는 경우 기본 정책('스냅샷 미러 정책 생성 - vserver svm_name - policy policy_name - type continuous[-RPO_integer_][-throttle_throttle_type_][-comment_text_][*additional_options*]')를 사용하지 않으려는 경우 S3 SnapMirror 정책을 생성합니다

   매개 변수: * "type continuous" - S3 SnapMirror 관계에 대한 유일한 정책 유형(필수) * '-RPO' – 복구 시점 목표의 시간(초 단위)을 지정합니다(선택 사항). * '-throttle' – 처리량/대역폭의 상한값을 킬로바이트/초 단위로 지정합니다(선택 사항).

   예

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

5. 타겟이 StorageGRID 시스템인 경우 소스 클러스터의 관리 SVM에 StorageGRID CA 서버 인증서를 설치합니다. '보안 인증서 설치 유형 server-ca-vserver_src_admin_svm_-cert-name_storage_grid_server_certificate_'

   자세한 내용은 보안 인증서 설치 man 페이지를 참조하십시오.

6. S3 SnapMirror 대상 오브젝트 저장소 정의:'sapmirror object-store config create-vserver_svm_name_-object-store-name_target_store_name_-usage data-provider-type{AWS_S3|SGWs}-server_target_FQDN_-container-name_remote_bucket_name_-is-ssl-enabled true-port_port_port_key_password_access-access

   매개 변수: * '-object-store-name' - 로컬 ONTAP 시스템에 있는 오브젝트 저장소 타겟의 이름입니다. 이 워크플로에는 '-usage' – 'data'를 사용합니다. ' *'-provider-type' –'AWS_S3','sgws'(StorageGRID) 대상이 지원됩니다. * '-server' – 대상 서버의 FQDN 또는 IP 주소입니다. * '-is-ssl-enabled' – SSL 활성화는 선택 사항이지만 권장됩니다. + 자세한 내용은 '스냅샷 객체 저장 구성 생성' man 페이지를 참조하십시오.

   예

   ```
   src_cluster::> snapmirror object-store config create -vserver vs0
   -object-store-name sgws-store -usage data -provider-type SGWS
   -server sgws.example.com -container-name target-test-bucket -is-ssl
   -enabled true -port 443 -access-key abc123 -secret-password xyz890
   ```

7. S3 SnapMirror 관계 생성: 'sapmirror create-source-path_svm_name_:/bucket/*bucket_name* -destination-path_object_store_name_:/objstore-policy_policy_name_'

   매개 변수:
   * `-destination-path` - 이전 단계에서 만든 개체 저장소 이름과 고정 값입니다 `objstore`.
   를 누릅니다
   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

   예

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/test-
   bucket -destination-path sgws-store:/objstore -policy test-policy
   ```

8. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

기존 버킷(클라우드 타겟)에 대한 백업 관계 생성

ONTAP 9.10.1 이전 릴리즈에서 S3 구성을 업그레이드한 경우와 같이 언제든지 기존 S3 버킷 백업을 시작할 수 있습니다.

시작하기 전에

- 객체 저장소 공급자에 대한 유효한 계정 자격 증명 및 구성 정보가 있습니다.
- 소스 시스템에 인터클러스터 네트워크 인터페이스 및 IPspace가 구성되었습니다.
- 소스 스토리지 VM의 DNS 구성은 타겟의 FQDN을 확인할 수 있어야 합니다.

시스템 관리자

1. 사용자 및 그룹이 올바르게 정의되었는지 확인합니다. * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭합니다 S3 아래.

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.

2. S3 SnapMirror 정책이 없는 경우 기본 정책을 사용하지 않으려면 다음과 같이 하십시오.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 을 클릭합니다 → 보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
   c. 정책 이름과 설명을 입력합니다.
   d. 정책 범위, 클러스터 또는 SVM을 선택합니다
   e. S3 SnapMirror 관계에 대해 * Continuous * 를 선택합니다.
   f. 스로틀 * 및 * 복구 지점 목표 값 * 을 입력합니다.
3. 소스 시스템에 Cloud Object Store 추가:
   a. 보호 > 개요 * 를 클릭한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.
   b. 추가 * 를 클릭한 다음, StorageGRID Webscale * 용 * Amazon S3 * 또는 * 기타 * 를 선택합니다.
   c. 다음 값을 입력합니다.
      - 클라우드 오브젝트 저장소 이름
      - URL 스타일(경로 또는 가상 호스팅)
      - 스토리지 VM(S3에 대해 활성화됨)
      - 개체 저장소 서버 이름(FQDN)
      - 오브젝트 저장소 인증서
      - 액세스 키
      - 비밀 키
      - 컨테이너(버킷) 이름입니다
4. 기존 버킷의 버킷 접근 정책이 여전히 요구 사항을 충족하는지 확인합니다.
   a. 스토리지 * > * 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 사용 권한 * 탭에서 을 클릭합니다 * 편집 * 을 선택한 다음 * 권한 * 에서 * 추가 * 를 클릭합니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * Actions * - GetObject, PutObject, DeleteObject, ListBucket, GetBuckketAcl, GetObjectAcl, ListBuckketMultipartUploads, ListMultiPartUploadParts 등의 값이 표시되는지 확인합니다
      - * 리소스 * - 기본값((버켓 이름, 버켓 이름/ *) 또는 필요한 기타 값을 사용합니다.

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.
5. S3 SnapMirror를 사용하여 버킷 백업:

a. 스토리지 * > * 버킷 * 을 클릭한 다음 백업할 버킷을 선택합니다.

b. 보호 * 를 클릭하고 * 대상 * 에서 * 클라우드 스토리지 * 를 선택한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.

Save * 를 클릭하면 기존 버킷이 클라우드 오브젝트 저장소로 백업됩니다.

CLI를 참조하십시오

1. 기본 버킷 정책의 액세스 규칙이 올바른지 확인합니다. 'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_store_resources_[-sid_text_integer']

   예

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. S3 SnapMirror 정책이 없는 경우 기본 정책('스냅샷 미러 정책 생성 - vserver svm_name - policy policy_name - type continuous[-RPO_integer_][-throttle_throttle_type_][-comment_text_][*additional_options*]')를 사용하지 않으려는 경우 S3 SnapMirror 정책을 생성합니다

   매개 변수: * "type continuous" - S3 SnapMirror 관계에 대한 유일한 정책 유형(필수) * '-RPO' – 복구 시점 목표의 시간(초 단위)을 지정합니다(선택 사항). * '-throttle' – 처리량/대역폭의 상한값을 킬로바이트/초 단위로 지정합니다(선택 사항).

   예

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. 타겟이 StorageGRID 시스템인 경우 소스 클러스터의 관리 SVM에 StorageGRID CA 인증서를 설치합니다. '보안 인증서 설치 유형 server-ca-vserver_src_admin_svm_-cert-name_storage_grid_server_certificate_'

   자세한 내용은 보안 인증서 설치 man 페이지를 참조하십시오.

4. S3 SnapMirror 대상 오브젝트 저장소 정의:'sapmirror object-store config create-vserver_svm_name_-object-store-name_target_store_name_-usage data-provider-type{AWS_S3|SGWs}-server_target_FQDN_-container-name_remote_bucket_name_-is-ssl-enabled true-port_port_port_key_password_access-access

   매개 변수: * '-object-store-name' - 로컬 ONTAP 시스템에 있는 오브젝트 저장소 타겟의 이름입니다. 이 워크플로에는 '-usage' – 'data'를 사용합니다. ' *'-provider-type' –'AWS_S3','sgws'(StorageGRID) 대상이 지원됩니다. * '-server' – 대상 서버의 FQDN 또는 IP 주소입니다. * '-is-ssl-enabled' – SSL 활성화는 선택 사항이지만 권장됩니다. + 자세한 내용은 '스냅샷 객체 저장 구성 생성' man 페이지를 참조하십시오.

예

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. S3 SnapMirror 관계 생성: 'sapmirror create-source-path_svm_name_:/bucket/*bucket_name* -destination-path_object_store_name_:/objstore-policy_policy_name_'

   매개 변수:
   * `-destination-path` - 이전 단계에서 만든 개체 저장소 이름과 고정 값입니다 `objstore`.
   를 누릅니다
   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

클라우드 대상에서 버킷 복원

소스 버킷의 데이터가 손실되거나 손상된 경우 대상 버킷에서 복구하여 데이터를 다시 채울 수 있습니다.

이 작업에 대해

대상 버킷을 기존 버킷 또는 새 버킷으로 복원할 수 있습니다. 복구 작업의 타겟 버킷은 대상 버킷의 논리적 사용 공간보다 커야 합니다.

기존 버킷을 사용하는 경우 복원 작업을 시작할 때 비어 있어야 합니다. 복구는 시간 내에 버킷을 "롤백"하지 않고 빈 버킷을 이전 컨텐츠로 채웁니다.

시스템 관리자

백업 데이터 복원:

1. 보호 > 관계 * 를 클릭한 다음 * S3 SnapMirror * 를 선택합니다.
2. 을 클릭합니다 ⋮ 그런 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 * 기존 버킷 * (기본값) 또는 * 새 버킷 * 을 선택합니다.
   - 기존 버킷 * (기본값)으로 복원하려면 다음 작업을 완료하십시오.
     - 기존 버킷을 검색할 클러스터와 스토리지 VM을 선택합니다.
     - 기존 버킷을 선택합니다.
     - destination_s3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
   - 새 버킷 * 으로 복원하려면 다음 값을 입력합니다.
     - 새로운 버킷을 호스팅할 클러스터 및 스토리지 VM
     - 새로운 버킷의 이름, 용량 및 성능 서비스 수준. 을 참조하십시오 "스토리지 서비스 레벨" 를 참조하십시오.
     - 대상 S3 서버 CA 인증서의 내용.
4. 대상 * 에서 _source_S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
5. 보호 > 관계 * 를 클릭하여 복구 진행률을 모니터링합니다.

CLI 절차

1. 복원할 새 대상 버킷을 생성합니다. 자세한 내용은 을 참조하십시오 "버킷에 대한 백업 관계 생성(클라우드 타겟)".
2. 대상 버킷에 대한 복구 작업을 시작합니다.
   `snapmirror restore -source-path object_store_name:/objstore -destination -path svm_name:/bucket/bucket_name`

   예

   다음 예에서는 대상 버킷을 기존 버킷으로 복원합니다.
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```