



ANF 및 JetStream을 사용한 재해 복구 NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

목차

ANF 및 JetStream을 사용한 재해 복구	1
온프레미스 데이터 센터에 JetStream DR 설치	2
실행 명령을 사용하여 Azure VMware Solution 프라이빗 클라우드에 AVS용 JetStream DR 설치	6
장애 조치/장애 복구 수행	9
랜섬웨어 복구	12

ANF 및 JetStream을 사용한 재해 복구

클라우드 재해 복구를 수행하는 것은 사이트 중단 및 데이터 손상 사고(예: 랜섬웨어)로부터 작업 부하를 보호하는 탄력적이고 비용 효율적인 방법입니다. VMware VAIO 프레임워크를 사용하면 온프레미스 VMware 워크로드를 Azure Blob 스토리지에 복제하고 복구할 수 있어 데이터 손실이 최소화되거나 거의 없고 RTO가 거의 0에 가깝습니다.

JetStream DR을 사용하면 온프레미스에서 AVS로 복제된 워크로드를 원활하게 복구하고 특히 Azure NetApp Files로 복구할 수 있습니다. DR 사이트에서 최소한의 리소스와 비용 효율적인 클라우드 스토리지를 사용하여 비용 효율적인 재해 복구를 가능하게 합니다. JetStream DR은 Azure Blob Storage를 통해 ANF 데이터 저장소로의 복구를 자동화합니다. JetStream DR은 네트워크 매핑에 따라 독립적인 VM 또는 관련 VM 그룹을 복구 사이트 인프라로 복구하고 랜섬웨어 보호를 위한 지정 시점 복구를 제공합니다.

이 문서는 JetStream DR의 작동 원리와 주요 구성 요소에 대한 이해를 제공합니다.

솔루션 배포 개요

1. 온프레미스 데이터 센터에 JetStream DR 소프트웨어를 설치합니다.
 - a. Azure Marketplace(ZIP)에서 JetStream DR 소프트웨어 번들을 다운로드하고 지정된 클러스터에 JetStream DR MSA(OVA)를 배포합니다.
 - b. I/O 필터 패키지로 클러스터를 구성합니다(JetStream VIB 설치).
 - c. DR AVS 클러스터와 동일한 지역에 Azure Blob(Azure Storage 계정)을 프로비저닝합니다.
 - d. DRVA 어플라이언스를 배포하고 복제 로그 볼륨(기존 데이터 저장소 또는 공유 iSCSI 스토리지의 VMDK)을 할당합니다.
 - e. 보호된 도메인(관련 VM 그룹)을 만들고 DRVA와 Azure Blob Storage/ANF를 할당합니다.
 - f. 보호를 시작합니다.
2. Azure VMware Solution 프라이빗 클라우드에 JetStream DR 소프트웨어를 설치합니다.
 - a. 실행 명령을 사용하여 JetStream DR을 설치하고 구성합니다.
 - b. 동일한 Azure Blob 컨테이너를 추가하고 도메인 검색 옵션을 사용하여 도메인을 검색합니다.
 - c. 필요한 DRVA 어플라이언스를 배포합니다.
 - d. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
 - e. 보호된 도메인을 가져오고 RocVA(복구 VA)를 구성하여 VM 배치에 ANF 데이터 저장소를 사용합니다.
 - f. 적절한 장애 조치(failover) 옵션을 선택하고 RTO가 거의 0에 가까운 도메인이나 VM에 대해 지속적인 복원을 시작합니다.
3. 재해 발생 시 지정된 AVS DR 사이트의 Azure NetApp Files 데이터 저장소로 장애 조치를 트리거합니다.
4. 보호 사이트가 복구된 후 보호 사이트로 장애 복구를 호출합니다. 시작하기 전에 이 문서에 표시된 대로 전제 조건이 충족되었는지 확인하십시오. ["링크"](#) 또한 JetStream 소프트웨어에서 제공하는 대역폭 테스트 도구(BWT)를 실행하여 JetStream DR 소프트웨어와 함께 사용할 때 Azure Blob 저장소의 잠재적 성능과 복제 대역폭을 평가합니다. 연결성을 포함한 전제 조건이 갖춰진 후 AVS용 JetStream DR을 설정하고 구축하세요. ["Azure 마켓플레이스"](#). 소프트웨어 번들을 다운로드한 후 위에 설명된 설치 과정을 진행하세요.

많은 수의 VM(예: 100개 이상)에 대한 보호를 계획하고 시작할 때 JetStream DR Automation Toolkit의 용량 계획

도구(CPT)를 사용하세요. 보호할 VM 목록과 RTO 및 복구 그룹 기본 설정을 제공한 다음 CPT를 실행합니다.

CPT는 다음과 같은 기능을 수행합니다.

- RTO에 따라 VM을 보호 도메인으로 결합합니다.
- DRVA의 최적 수와 리소스를 정의합니다.
- 필요한 복제 대역폭을 추정합니다.
- 복제 로그 볼륨 특성(용량, 대역폭 등)을 식별합니다.
- 필요한 객체 스토리지 용량을 추정하는 등의 작업입니다.

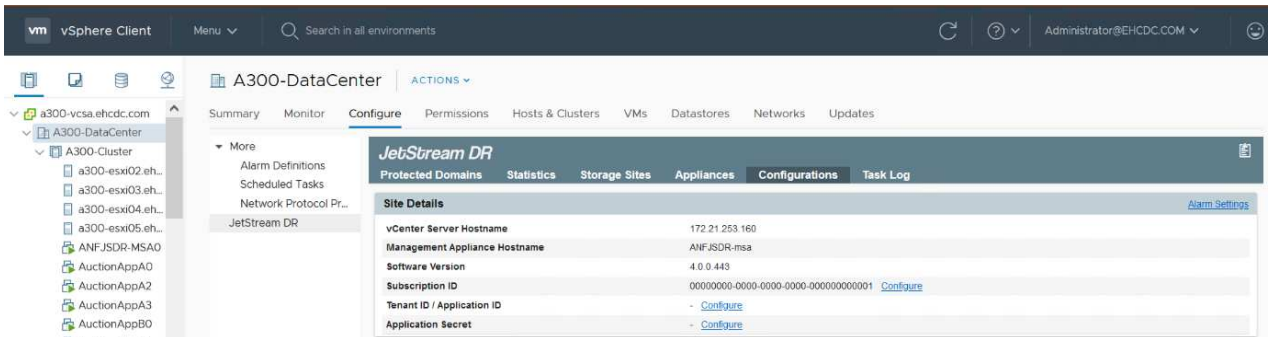


규정된 도메인의 수와 내용은 평균 IOPS, 총 용량, 우선순위(장애 조치 순서를 정의함), RTO 등 다양한 VM 특성에 따라 달라집니다.

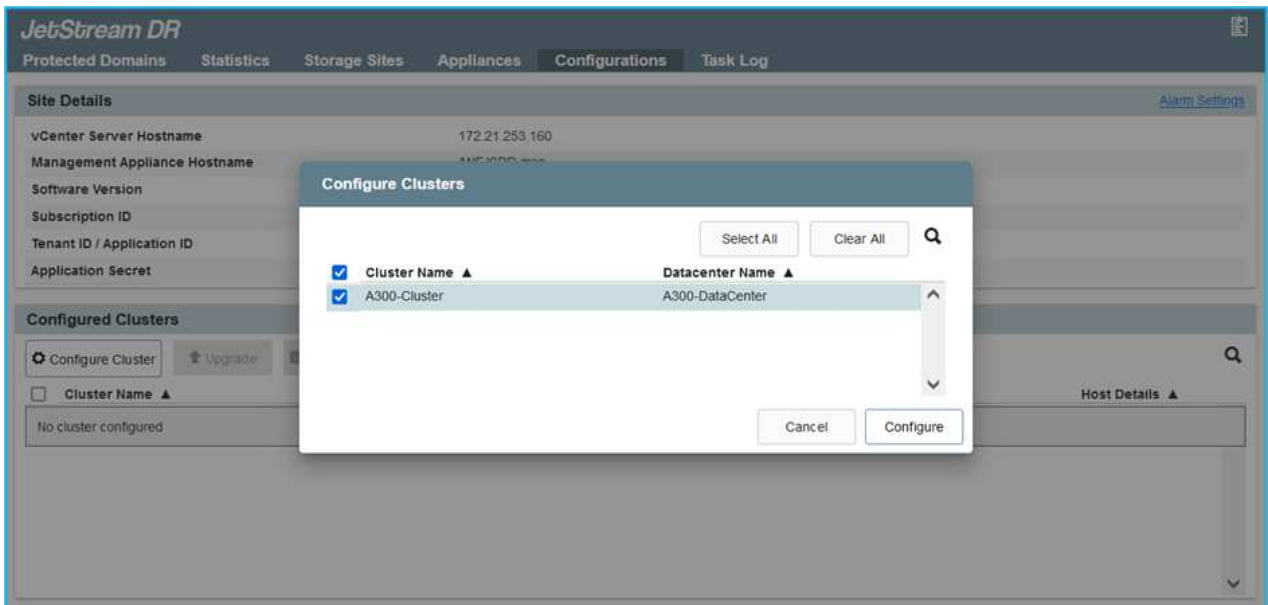
온프레미스 데이터 센터에 **JetStream DR** 설치

JetStream DR 소프트웨어는 JetStream DR 관리 서버 가상 어플라이언스(MSA), DR 가상 어플라이언스(DRVA), 호스트 구성 요소(I/O 필터 패키지)의 세 가지 주요 구성 요소로 구성됩니다. MSA는 컴퓨팅 클러스터에 호스트 구성 요소를 설치하고 구성한 다음 JetStream DR 소프트웨어를 관리하는 데 사용됩니다. 다음 목록은 설치 과정에 대한 간략한 설명을 제공합니다.

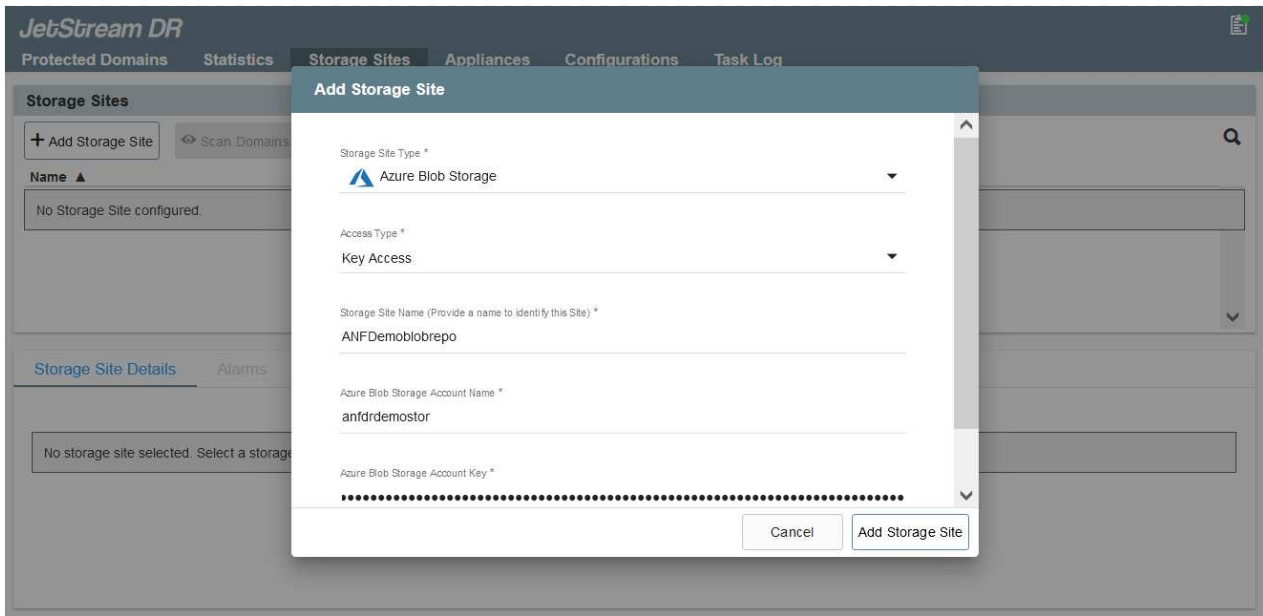
1. 필수 조건을 확인하세요.
2. 리소스 및 구성 권장 사항을 알아보려면 용량 계획 도구를 실행합니다(선택 사항이지만 개념 증명 시험에 권장됨).
3. 지정된 클러스터의 vSphere 호스트에 JetStream DR MSA를 배포합니다.
4. 브라우저에서 DNS 이름을 사용하여 MSA를 시작합니다.
5. MSA에 vCenter 서버를 등록합니다. 설치를 수행하려면 다음의 자세한 단계를 완료하세요.
6. JetStream DR MSA가 배포되고 vCenter Server가 등록된 후 vSphere Web Client를 사용하여 JetStream DR 플러그인에 액세스합니다. 데이터 센터 > 구성 > JetStream DR로 이동하여 이 작업을 수행할 수 있습니다.



7. JetStream DR 인터페이스에서 적절한 클러스터를 선택하세요.



8. I/O 필터 패키지로 클러스터를 구성합니다.



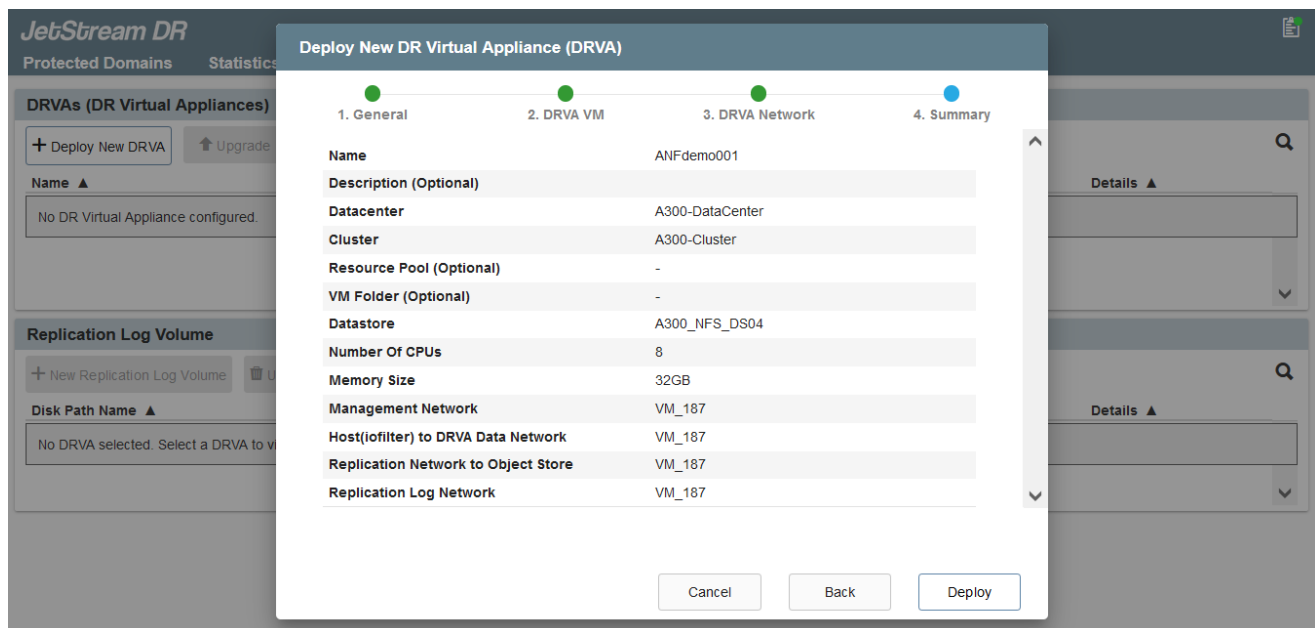
9. 복구 사이트에 Azure Blob Storage를 추가합니다.

10. 어플라이언스 탭에서 DRVA(DR Virtual Appliance)를 배포합니다.



DRVA는 CPT에서 자동으로 생성할 수 있지만 POC 시험의 경우 DR 주기를 수동으로 구성하고 실행하는 것이 좋습니다(보호 시작 > 장애 조치 > 장애 복구).

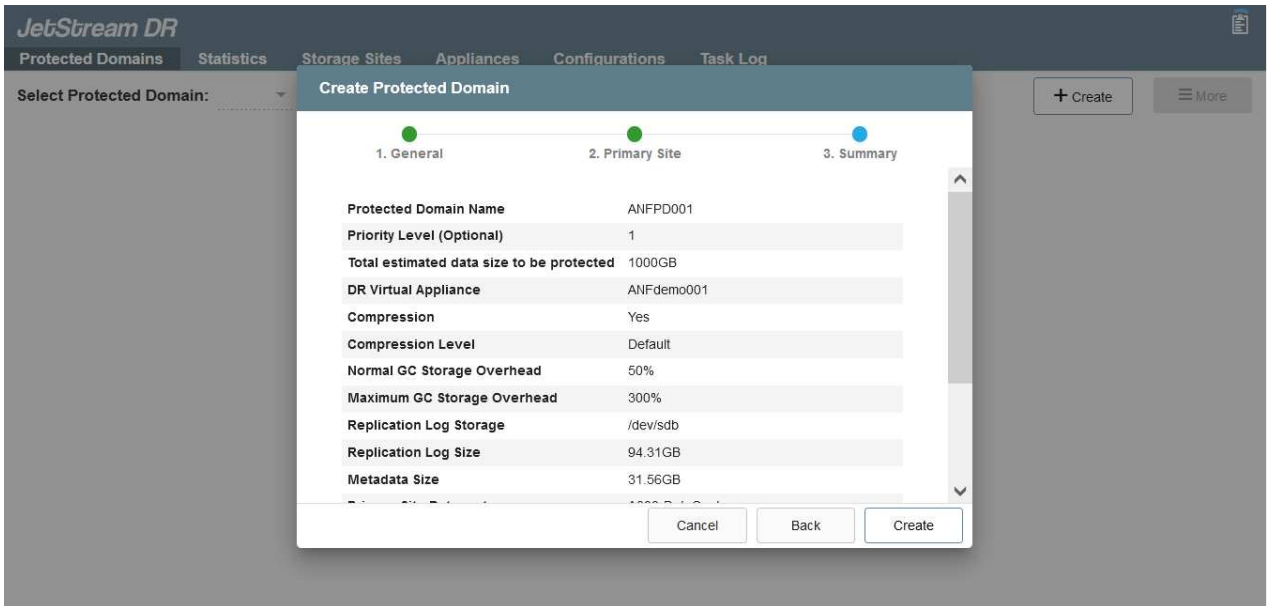
JetStream DRVA는 데이터 복제 프로세스의 주요 기능을 용이하게 하는 가상 어플라이언스입니다. 보호된 클러스터에는 최소한 하나의 DRVA가 포함되어야 하며, 일반적으로 호스트당 하나의 DRVA가 구성됩니다. 각 DRVA는 여러 개의 보호된 도메인을 관리할 수 있습니다.



이 예에서는 80개의 가상 머신에 대해 4개의 DRVA가 생성되었습니다.

1. 사용 가능한 데이터 저장소나 독립적인 공유 iSCSI 스토리지 풀에서 VMDK를 사용하여 각 DRVA에 대한 복제 로그 볼륨을 생성합니다.

2. 보호된 도메인 탭에서 Azure Blob Storage 사이트, DRVA 인스턴스 및 복제 로그에 대한 정보를 사용하여 필요한 수의 보호된 도메인을 만듭니다. 보호된 도메인은 클러스터 내에서 함께 보호되고 장애 조치/장애 복구 작업에 대한 우선 순위가 지정된 특정 VM 또는 VM 세트를 정의합니다.



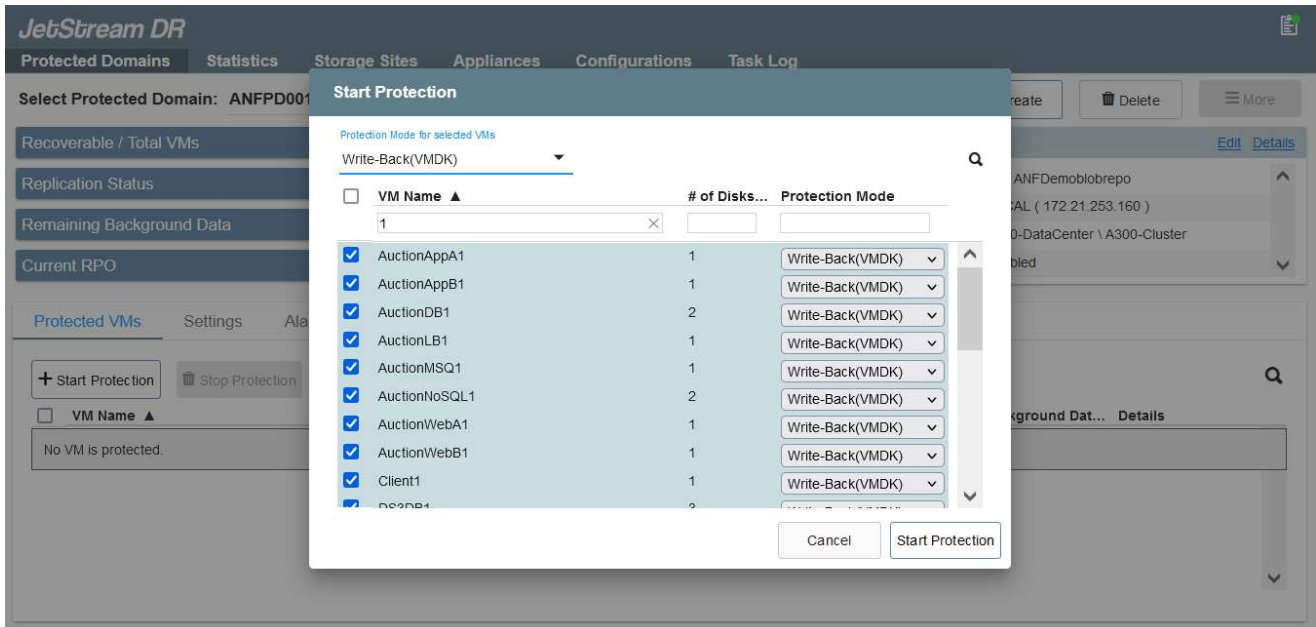
3. 보호하려는 VM을 선택하고 보호된 도메인의 VM 보호를 시작합니다. 이렇게 하면 지정된 Blob Store에 데이터 복제가 시작됩니다.



보호된 도메인의 모든 VM에 동일한 보호 모드가 사용되는지 확인합니다.



Write-Back(VMDK) 모드는 더 높은 성능을 제공할 수 있습니다.



복제 로그 볼륨이 고성능 스토리지에 배치되었는지 확인하세요.



장애 조치 실행 설명서를 구성하여 VM을 그룹화(복구 그룹이라고 함), 부팅 순서 순서를 설정하고 IP 구성과 함께 CPU/메모리 설정을 수정할 수 있습니다.

실행 명령을 사용하여 Azure VMware Solution 프라이빗 클라우드에 AVS용 JetStream DR 설치

복구 사이트(AVS)의 모범 사례는 미리 3노드 파일럿 라이트 클러스터를 만드는 것입니다. 이를 통해 다음 항목을 포함하여 복구 사이트 인프라를 미리 구성할 수 있습니다.

- 목적지 네트워킹 세그먼트, 방화벽, DHCP 및 DNS와 같은 서비스 등.
- AVS용 JetStream DR 설치
- ANF 볼륨을 데이터 저장소로 구성하고 JetStream DR은 미션 크리티컬 도메인에 대해 거의 0에 가까운 RTO 모드를 지원합니다. 이러한 도메인의 경우 대상 저장소가 미리 설치되어야 합니다. 이 경우에는 ANF가 권장되는 저장 유형입니다.



세그먼트 생성을 포함한 네트워크 구성은 온프레미스 요구 사항에 맞게 AVS 클러스터에서 구성되어야 합니다.

SLA 및 RTO 요구 사항에 따라 지속적인 장애 조치 또는 일반(표준) 장애 조치 모드를 사용할 수 있습니다. RTO가 거의 0에 가까운 경우, 회복 부위에서 지속적인 수분 보충을 시작해야 합니다.

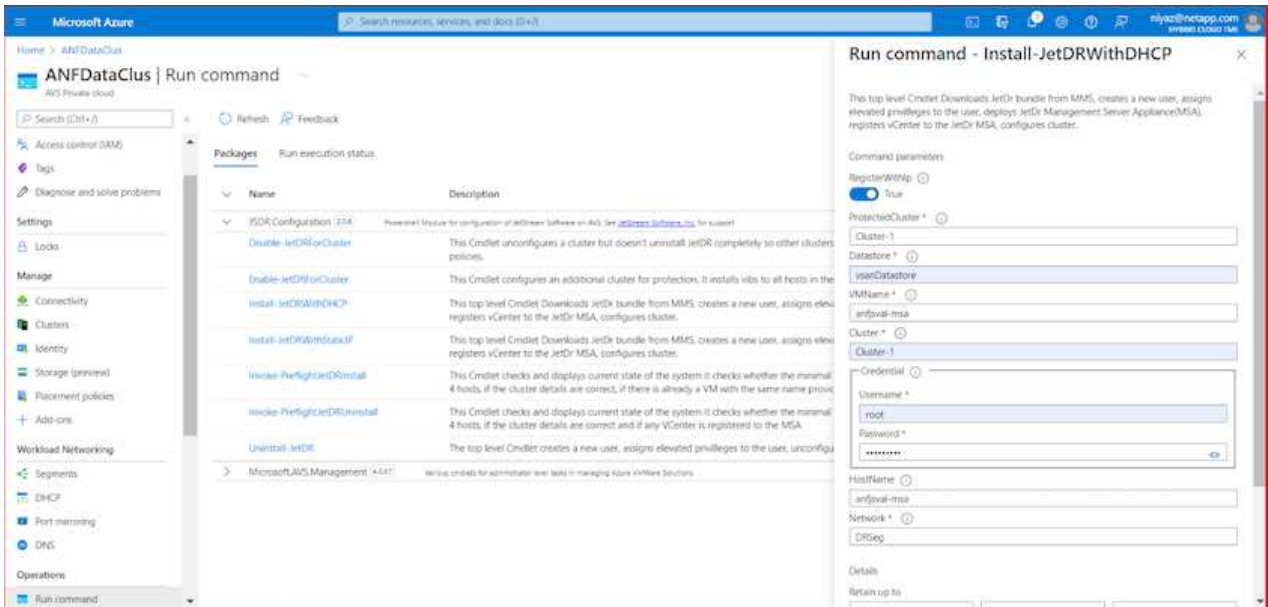
Azure VMware Solution 프라이빗 클라우드에 AVS용 JetStream DR을 설치하려면 다음 단계를 완료하세요.

1. Azure Portal에서 Azure VMware 솔루션으로 이동하여 프라이빗 클라우드를 선택하고 명령 실행 > 패키지 > JSDR.Configuration을 선택합니다.



Azure VMware Solution의 기본 CloudAdmin 사용자에게는 AVS용 JetStream DR을 설치할 수 있는 권한이 없습니다. Azure VMware Solution을 사용하면 JetStream DR에 대한 Azure VMware Solution 실행 명령을 호출하여 JetStream DR을 간단하고 자동으로 설치할 수 있습니다.

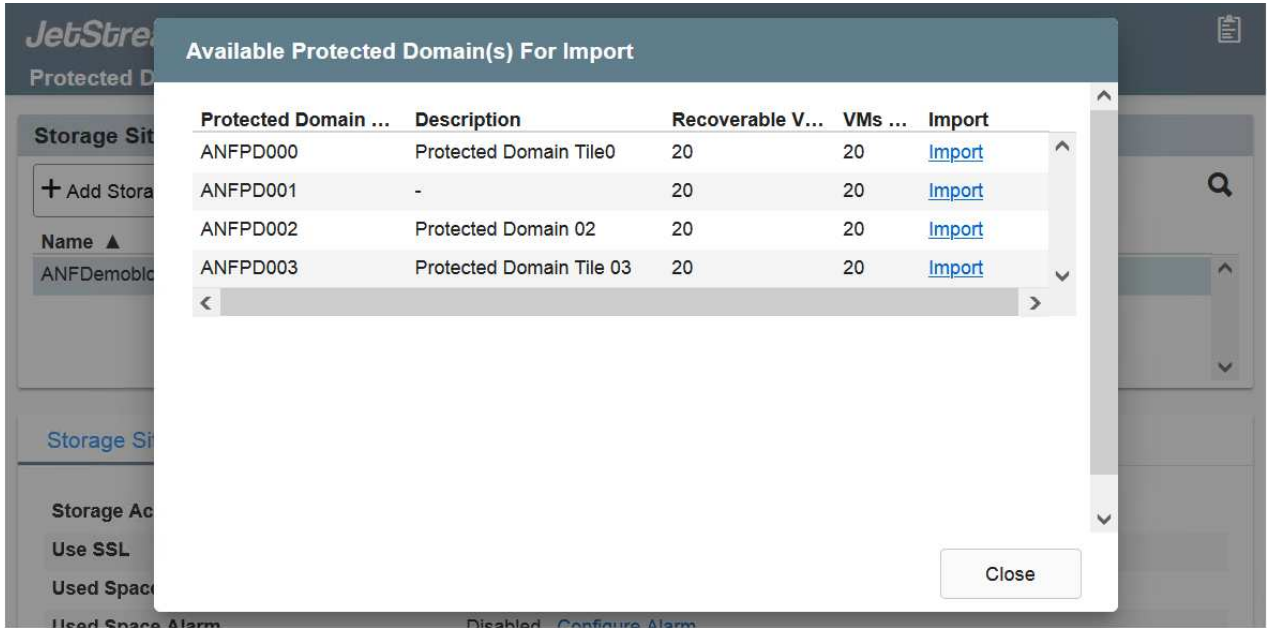
다음 스크린샷은 DHCP 기반 IP 주소를 사용하여 설치하는 방법을 보여줍니다.



2. AVS용 JetStream DR 설치가 완료되면 브라우저를 새로 고칩니다. JetStream DR UI에 액세스하려면 SDDC 데이터센터 > 구성 > JetStream DR로 이동하세요.



3. JetStream DR 인터페이스에서 온-프레미스 클러스터를 스토리지 사이트로 보호하는 데 사용된 Azure Blob Storage 계정을 추가한 다음 도메인 검사 옵션을 실행합니다.

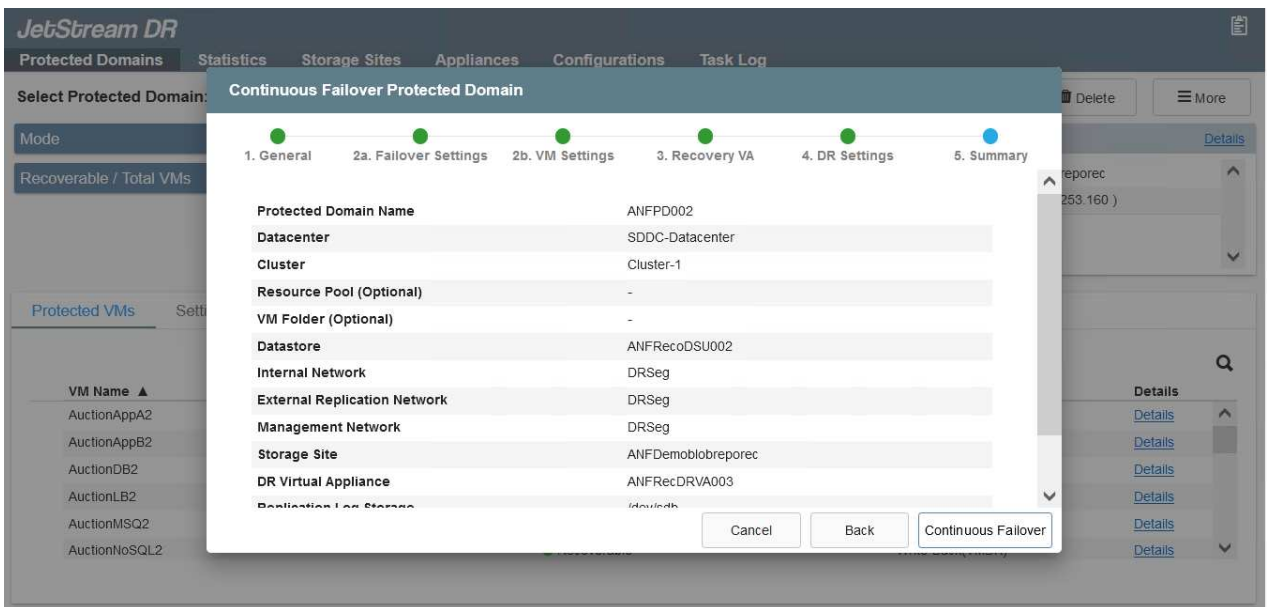


4. 보호된 도메인을 가져온 후 DRVA 어플라이언스를 배포합니다. 이 예에서는 JetStream DR UI를 사용하여 복구 사이트에서 수동으로 지속적인 수분 공급이 시작됩니다.



이러한 단계는 CPT에서 만든 계획을 사용하여 자동화할 수도 있습니다.

5. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
6. 보호된 도메인을 가져오고 VM 배치를 위해 ANF 데이터 저장소를 사용하도록 복구 VA를 구성합니다.



선택한 세그먼트에서 DHCP가 활성화되어 있고 충분한 IP를 사용할 수 있는지 확인하세요. 도메인이 복구되는 동안 동적 IP가 일시적으로 사용됩니다. 복구 중인 각 VM(지속적인 재수화 포함)에는 개별 동적 IP가 필요합니다. 복구가 완료되면 IP가 해제되어 재사용될 수 있습니다.

7. 적절한 장애 조치 옵션(지속적인 장애 조치 또는 장애 조치)을 선택합니다. 이 예에서는 연속 재수화(연속 장애 조치)가 선택되었습니다.

The screenshot shows the JetStream DR web interface. At the top, there's a navigation bar with tabs: Protected Domains, Statistics, Storage Sites, Appliances, Configurations, and Task Log. Below the navigation bar, there's a section for 'Select Protected Domain: ANFPD000' with a 'View all' link and buttons for '+ Create', 'Delete', and 'More'. A 'Configurations' dropdown menu is open, showing options: 'Restore', 'Failover', 'Continuous Failover', and 'Test Failover'. Below this, there's a table for 'Protected VMs' with columns: VM Name, Protection Status, Protection Mode, and Details. The table lists two VMs: AuctionAppA0 and AuctionAppB0, both with a 'Recoverable' status and 'Write-Back(VMDK)' protection mode.

VM Name ▲	Protection Status ▲	Protection Mode ▲	Details
AuctionAppA0	✓ Recoverable	Write-Back(VMDK)	Details
AuctionAppB0	✓ Recoverable	Write-Back(VMDK)	Details

장애 조치/장애 복구 수행

장애 조치(Failover)/장애 복구(Failback)를 수행하는 방법

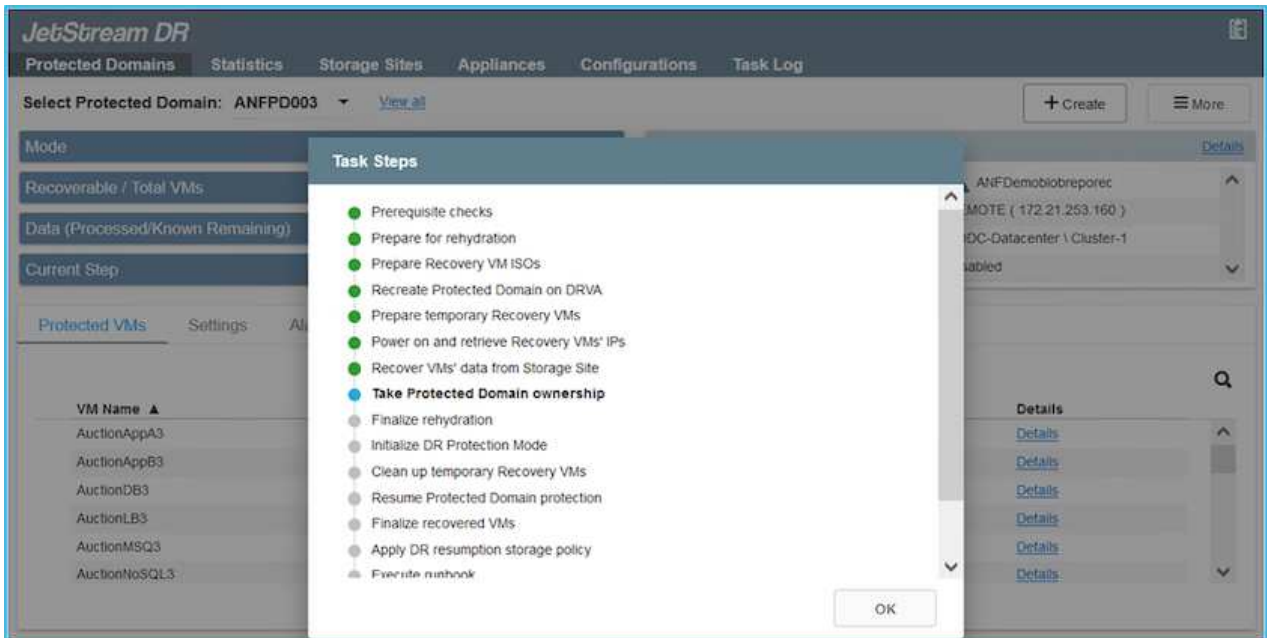
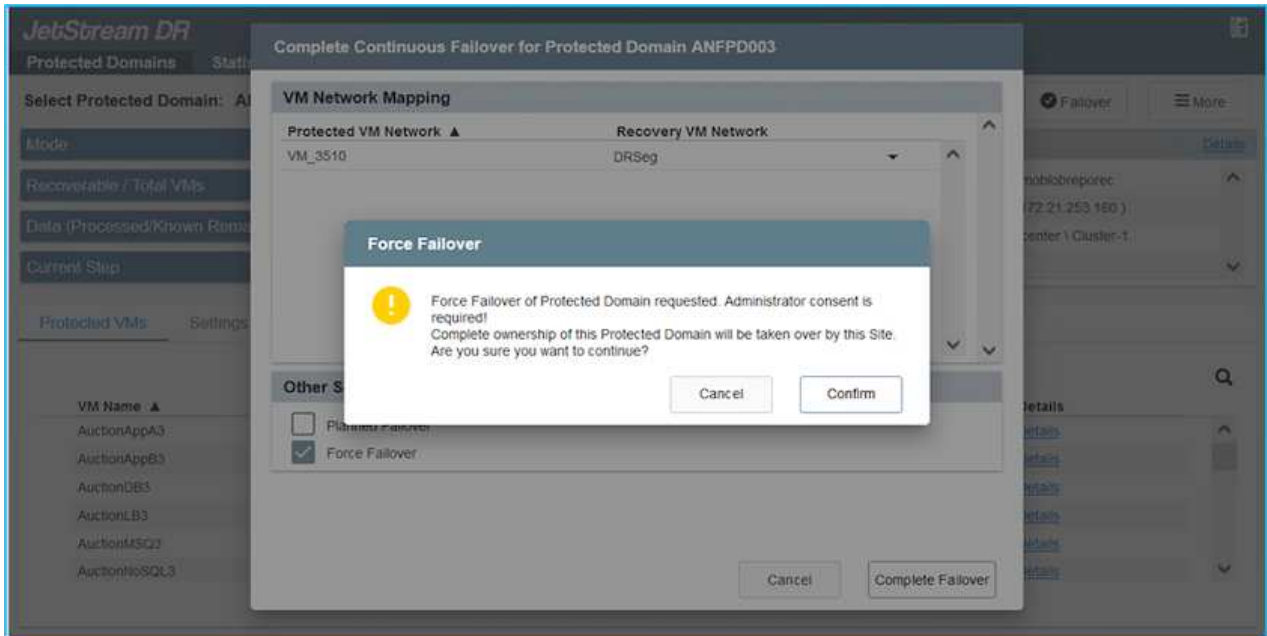
1. 온프레미스 환경의 보호된 클러스터에서 재해(부분적 또는 전체적 장애)가 발생한 후 장애 조치를 트리거합니다.



CPT는 Azure Blob Storage에서 AVS 클러스터 복구 사이트로 VM을 복구하는 장애 조치 계획을 실행하는 데 사용할 수 있습니다.

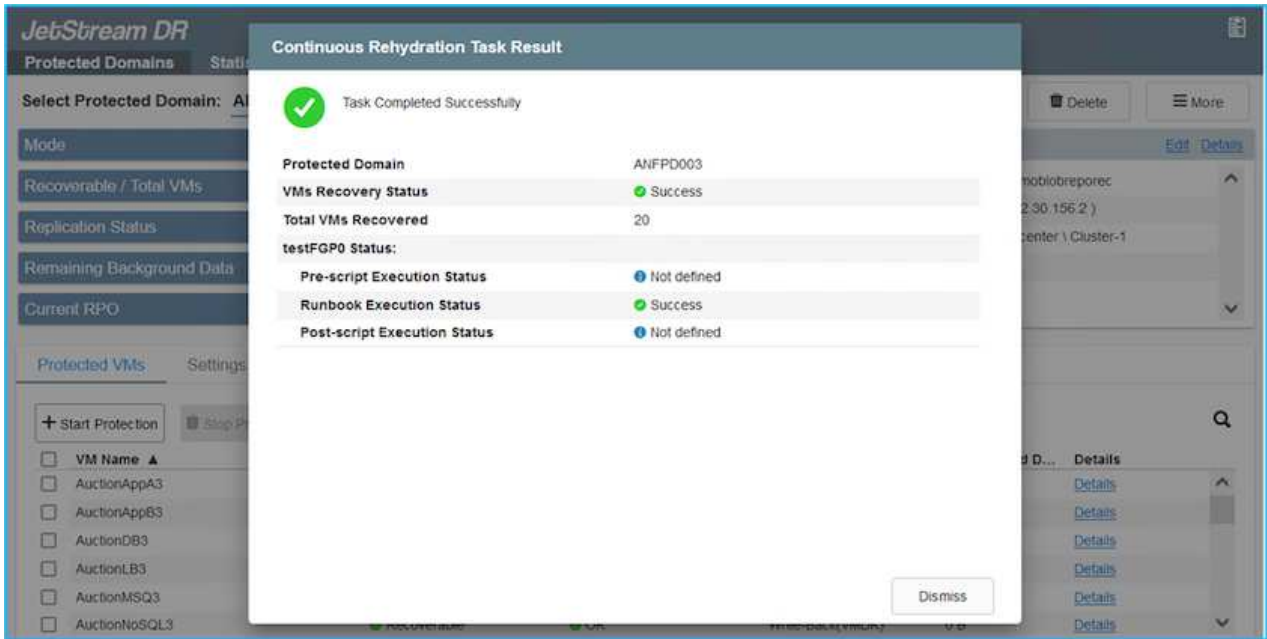


(지속적인 재수화 또는 표준 재수화의) 장애 조치(failover) 후 보호된 VM이 AVS에서 시작되면 보호가 자동으로 재개되고 JetStream DR은 Azure Blob Storage의 적절한/원래 컨테이너로 데이터를 계속 복제합니다.



작업 표시줄에는 장애 조치 활동의 진행 상황이 표시됩니다.

- 작업이 완료되면 복구된 VM에 액세스하여 정상적으로 업무를 계속 진행합니다.



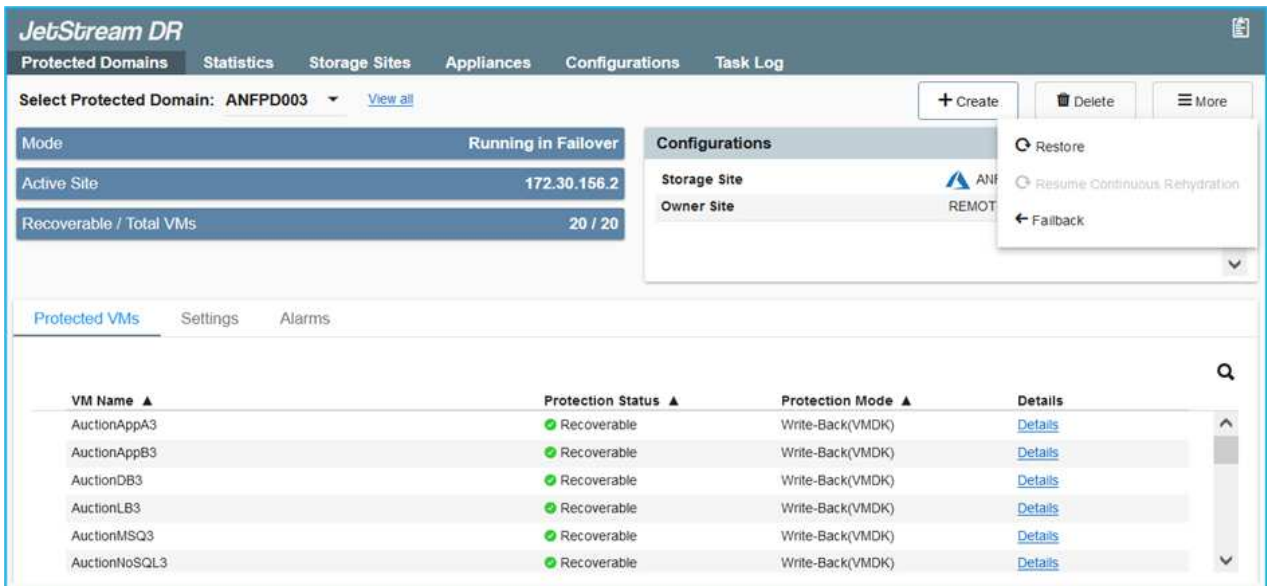
기본 사이트가 다시 가동되면 장애 복구를 수행할 수 있습니다. VM 보호가 재개되었으며 데이터 일관성을 확인해야 합니다.

- 온프레미스 환경을 복원합니다. 재해 사고의 유형에 따라 보호된 클러스터의 구성을 복원하거나 검증해야 할 수도 있습니다. 필요한 경우 JetStream DR 소프트웨어를 다시 설치해야 할 수도 있습니다.



참고사항: recovery_utility_prepare_failback Automation Toolkit에서 제공하는 스크립트를 사용하면 원래 보호된 사이트에서 오래된 VM, 도메인 정보 등을 정리하는 데 도움이 될 수 있습니다.

- 복원된 온프레미스 환경에 액세스하고 Jetstream DR UI로 이동하여 적절한 보호 도메인을 선택합니다. 보호된 사이트가 장애 복구 준비가 되면 UI에서 장애 복구 옵션을 선택합니다.





CPT에서 생성된 장애 복구 계획은 VM과 해당 데이터를 개체 저장소에서 원래 VMware 환경으로 반환하는 데에도 사용할 수 있습니다.



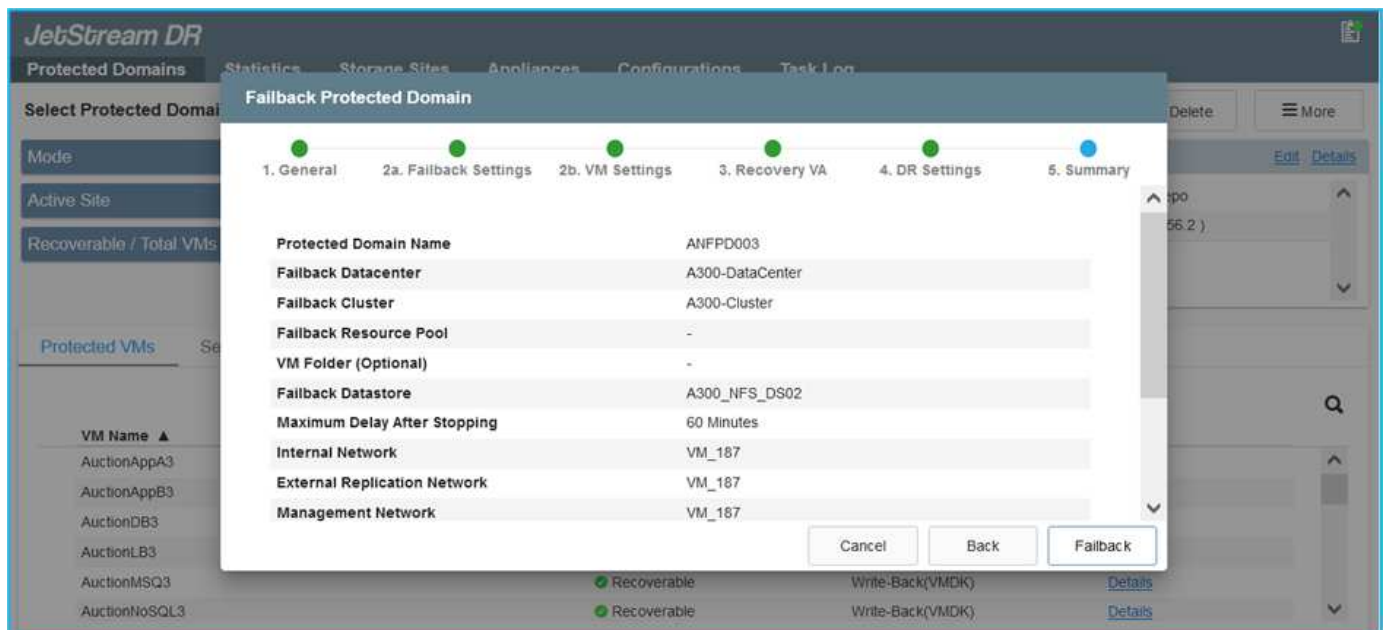
복구 사이트에서 VM을 일시 중지한 후 보호 사이트에서 다시 시작한 후의 최대 지연 시간을 지정합니다. 이 시간에는 장애 조치 VM을 중지한 후 복제를 완료하는 시간, 복구 사이트를 정리하는 시간, 보호된 사이트에서 VM을 다시 만드는 시간이 포함됩니다. NetApp 권장하는 값은 10분입니다.

장애 복구 프로세스를 완료한 후 VM 보호 및 데이터 일관성이 재개되었는지 확인합니다.

랜섬웨어 복구

랜섬웨어로부터 복구하는 것은 힘든 일일 수 있습니다. 특히, IT 조직에서는 안전한 복귀 지점을 결정하기 어려울 수 있으며, 일단 결정된 후에는 복구된 워크로드가 재발하는 공격(잠복 맬웨어 또는 취약한 애플리케이션을 통한 공격)으로부터 안전하게 보호되는지 확인하는 방법도 어려울 수 있습니다.

AVS용 JetStream DR과 Azure NetApp Files 데이터 저장소를 함께 사용하면 조직이 사용 가능한 시점으로부터 복구할 수 있으므로 필요한 경우 작업 부하를 기능적이고 격리된 네트워크로 복구할 수 있어 이러한 문제를 해결할 수 있습니다. 복구를 통해 애플리케이션은 남북 트래픽에 노출되지 않은 상태에서도 서로 작동하고 통신할 수 있으므로 보안 팀은 법의학 조사 및 기타 필요한 수정 작업을 안전하게 수행할 수 있습니다.



저작권 정보

Copyright © 2025 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.