

vSphere Data Protection 관리 가이드

vSphere Data Protection 6.1

본 문서는 새 버전으로 바뀔 때까지 명시된 각 제품 버전과 모든 후속 버전을 지원합니다. 본 문서의 최신 버전을 확인하려면 다음 사이트를 참조하십시오.

<http://www.vmware.com/kr/support/pubs>

EN-001795-00

vmware[®]

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<http://www.vmware.com/kr/support/>

VMware 웹 사이트에서 최신 제품 정보를 확인할 수 있습니다.

본 문서에 대한 의견은 다음 e-메일로 보내주시기 바랍니다.

docfeedback@vmware.com

Copyright © 2007–2015 VMware, Inc. All rights reserved. 본 제품은 미국 및 국제 저작권법 및 지적재산권법에 따라 보호됩니다. VMware 제품에는 <http://www.vmware.com/go/patents>에 명시된 하나 이상의 특허가 적용됩니다.

VMware는 미국 및/또는 기타 국가에서 VMware, Inc.의 등록 상표 또는 상표입니다. 본 문서에 언급된 기타 모든 명칭과 표시는 해당 소유권자의 상표일 수 있습니다.

VMware, Inc.

서울특별시 강남구 영동대로 517 아셈타워 30층

전화: (02)6001-3890

팩스: (02)6001-3899

웹 사이트: <http://www.vmware.com/kr>

목차

- 1 vSphere Data Protection 이해 13
 - vSphere Data Protection 소개 14
 - VDP의 이점 14
 - VDP 기능 15
 - 이미지 레벨 백업 및 복구 16
 - 단일 VMDK 백업 및 복구 16
 - 게스트 레벨 백업 및 복구 16
 - 복제 17
 - 파일 레벨 복구 17
 - 사용자 환경 개선 프로그램 17
 - VDP 아키텍처 17

- 2 VDP 설치 및 구성 21
 - vSphere Data Protection 용량 요구 사항 22
 - 소프트웨어 요구 사항 22
 - 하드웨어 버전 및 마이그레이션 22
 - vSphere 호스트 및 vSphere Flash 읽기 캐시 호환성 및 성능 22
 - 지원되지 않는 디스크 유형 22
 - 지원되지 않는 가상 볼륨 22
 - 시스템 요구 사항 23
 - VDP 시스템 요구 사항 23
 - IPv6 요구 사항 23
 - 설치 전 구성 23
 - DNS 구성 23
 - NTP 구성 24
 - vCenter 호스트 및 클러스터 보기 24
 - 사용자 계정 구성 24
 - VDP Best Practice 26
 - 일반적인 Best Practice 26
 - 구축 Best Practice 26
 - 핫 애드(HotAdd) Best Practice 27
 - 초기 VDP 구축 시의 스토리지 용량 27
 - 사이징 27
 - VDP 용량 모니터링 28
 - VDP 설치 29
 - OVF 템플릿 배포 29
 - 초기 구성 30

- 3 VDP 어플라이언스 마이그레이션 33
 - VDP 어플라이언스 5.8.x 이상에서 6.1로 마이그레이션 34

- 4 VDP 어플라이언스의 설치 후 구성 35
 - VDP-Configure 유틸리티 정보 36
 - 상태 보기 36
 - 서비스 시작 및 중지 37
 - VDP 로그 또는 진단 정보 수집 38
 - 구성 설정 수정 40

- 네트워크 설정 40
- vCenter Server 등록 40
- 어플라이언스 롤백 41
- 긴급 복구 42
 - 자동 호스트 감지 44
 - 복구 시점 새로 고침 44
 - vCenter에 호스트 다시 연결 44
- 5 VDP와 vCenter 간의 통신 보안 45**
 - VDP 인증서 교체 46
 - 보안 통신을 위한 VDP 서버 인증 47
 - vCenter Server로 VDP 어플라이언스 통신 보안 48
 - vCenter Server와의 프록시 통신 보안 49
- 6 VDP 구성 51**
 - 로그인 보안 52
 - 사용자 환경 개선 프로그램 구성 52
 - 구성 및 모니터링 53
 - 백업 어플라이언스 구성 보기 53
 - 백업 기간 편집 55
 - e-메일 알림 및 보고서 구성 55
 - 사용자 인터페이스 로그 보기 57
 - 무결성 검사 실행 57
 - VDP 작업 모니터링 58
 - 최근 작업 보기 58
 - 경보 보기 59
 - 이벤트 콘솔 보기 60
 - 용량 사용 문제를 표시하는 지속적인 팝업 메시지 60
 - VDP 종료 및 시작 절차 60
- 7 프록시 61**
 - 프록시 개요 62
 - 외부 프록시 구축 전 고려 사항 62
 - 외부 프록시 구축 62
 - 구축할 프록시 수 및 프록시당 프록시 처리량 62
 - 프록시 처리량 관리 63
 - 외부 프록시 지원 64
 - 외부 프록시 추가 65
 - 내부 프록시 비활성화 66
 - (선택 사항) 프록시 인증서 인증 구성 66
 - 외부 프록시 상태 모니터링 67
 - 상태 기준 67
 - 외부 프록시 로그 67
- 8 스토리지 관리 69**
 - 새 스토리지 생성 70
 - 최소 스토리지 성능 71
 - 기존 VDP 디스크 연결 72
 - 스토리지 분리 및 다시 연결 73
 - 스토리지 구성 보기 74
 - 검색 테스트 활성화 75
 - 검색 테스트를 활성화하도록 구성 파일 변경 75

9 Data Domain 통합 77

- VDP와 Data Domain 시스템 통합 78
- 아키텍처 개요 78
- VDP 클라이언트 지원 79
- Best Practice 79
 - Data Domain 제한 사항 79
 - 백업 80
 - 복구 80
 - 보안 - 암호화 80
 - 데이터 마이그레이션 80
- 통합 전 요구 사항 80
 - 네트워크 처리량 81
 - 네트워크 구성 81
 - NTP 구성 81
 - 라이선스 등록 81
 - 포트 사용 및 방화벽 요구 사항 82
 - 용량 82
 - Data Domain 시스템 스트림 82
 - Data Domain과 함께 사용되는 기존 백업 제품 82
- VDP 통합을 위한 Data Domain 시스템 준비 83
- Data Domain 시스템 추가 84
- Data Domain 시스템 편집 85
- VDP 어플라이언스에서 Data Domain 시스템 삭제 85
- VDP 및 Data Domain에서 백업 87
 - VDP 및 Data Domain에서 백업이 작동하는 방식 87
 - 백업 데이터가 저장되는 위치 87
 - VDP 어플라이언스가 백업 데이터를 관리하는 방법 88
 - 지원되는 백업 유형 88
 - 백업 취소 및 삭제 88
 - 백업에 대한 Data Domain 타겟 선택 88
- 복제 제어 89
 - 복제 데이터 흐름 89
 - 복제 스케줄 89
 - 복제 구성 89
 - VDP를 사용한 복제 모니터링 89
- 서버 유지 보수 작업 모니터링 90
- Data Domain 시스템에서 Avamar 체크포인트 백업 복구 90
 - 복구 작업을 위한 조건 90
 - 체크포인트 복구 수행 90
- VDP 어플라이언스에서 Data Domain 모니터링 92
 - vSphere Web Client를 사용하여 모니터링 92
 - VDP 구성 유틸리티를 사용하여 모니터링 93
- 전체 Data Domain 시스템에서 스토리지 재확보 93
- 일반적인 문제 및 해결책 95
 - Data Domain 시스템이 오프라인 상태인 경우 백업 실패 95
 - Data Domain 시스템 삭제 후 롤백 95

10 VDP 디스크 확장 97

- 사전 요구 사항 98
- VMFS 힙 크기 권장 사항 98
- 디스크 확장 수행 99
 - 스토리지 구성 보기 100
- 성능 분석 101
 - 성능 분석 테스트 실행 101
- Essentials Plus를 사용한 디스크 확장 101

- 11 VDP 사용 103**
 - VDP 액세스 104
 - CLI를 사용하여 VDP 어플라이언스 액세스 104
 - 유용한 명령 104
 - VDP 사용자 인터페이스 이해 105
 - VDP 어플라이언스 전환 106
 - VDP 사용자 인터페이스 106
 - 보고서 탭에서 정보 보기 106
 - 새로 고침 106
 - 작업 실패 탭 106
 - 작업 세부 정보 탭 107
 - 보호되지 않는 클라이언트 탭 108

- 12 백업 관리 109**
 - 백업 작업 110
 - 가상 머신 선택 110
 - 사용 중단된 가상 머신 확인 110
 - 백업 스케줄 지정 111
 - 보존 정책 설정 111
 - 전체 이미지 백업 작업 생성 112
 - 개별 디스크에 대한 백업 작업 생성 113
 - 지원되지 않는 디스크 유형 113
 - 제한 사항 114
 - 개별 디스크의 마이그레이션 114
 - 상태 및 백업 작업 세부 정보 보기 115
 - 백업 작업 편집 115
 - 백업 작업 클론 생성 115
 - 백업 작업 삭제 115
 - 백업 작업 활성화 또는 비활성화 115
 - 기존 백업 작업 즉시 실행 115
 - 백업 잠금 및 잠금 해제 116
 - VDP에서 Avamar로 백업 작업 마이그레이션 117
 - Guidelines 117
 - 권장 사항 117
 - 사전 요구 사항 117
 - 절차 117
 - 문제 해결 118

- 13 자동 백업 검증 119**
 - 자동 백업 검증 정보 120
 - 제한 사항 120
 - Best Practice 120
 - 새 백업 검증 작업 생성 121
 - 백업 검증 작업 편집 123
 - 백업 검증 작업 클론 생성 123
 - 백업 검증 작업 실행 123
 - 백업 검증 모니터링 124
 - 백업 검증 작업 활성화 및 비활성화 124
 - 백업 검증 작업 삭제 124

- 14 복구 관리 125**
 - 복구 작업 126
 - 제한 사항 126
 - 복구할 백업 선택 126

- 백업 목록 필터링 127
- 스냅샷이 존재할 때 복구 127
- 이미지 백업을 원래 위치로 복구 127
- 이미지 백업을 새 위치로 복구 129
 - 새 위치로 복구 실행 전 vMotion 기능 해제 130
- 개별 SCSI 디스크로 백업 복구 130
- 복구 탭에서 백업 삭제 131
- 복구 탭에서 선택한 모든 백업 지우기 131

15 복제 133

- 복제 작업 134
 - 복제 호환성 134
 - 복제 및 Data Domain 136
 - 복제에 대한 Best Practice 136
 - 제한 사항 136
 - 복제 작업에 대한 백업 유형 정의 136
- 복제 작업 생성 137
- 대상 관리 140
- 복제 작업 편집 141
- 복제 작업 클론 생성 141
- 복제 작업 삭제 141
- 복제 작업 활성화 또는 비활성화 141
- 상태 및 복제 작업 세부 정보 보기 141
- 기존 복제 작업 즉시 실행 141
- 소스로 다시 복제 142
 - 복구된 백업의 노드 구조 142
 - 다시 복제된 백업의 노드 구조 142
 - 복제 대상 142
- 복제 복구 호환성 143
- 복제 복구 활성화 또는 비활성화 143
- 복제 복구 143
- 멀티 테넌시 144

16 파일 레벨 복구 사용 147

- VDP Restore Client 소개 148
 - LVM 및 EXT 지원 148
 - 파일 레벨 복구 제한 사항 148
 - 지원되지 않는 VMDK 구성 149
 - 지원되지 않는 Windows 구성 149
- Restore Client에 로그인 149
 - 기본 로그인 149
 - 고급 로그인 150
- 백업 마운트 151
- 백업 필터링 151
- 마운트된 백업 탐색 151
- 파일 레벨 복구 수행 151
 - 기본 로그인 모드에서 Restore Client 사용 151
 - 고급 로그인 모드에서 Restore Client 사용 152
- 복구 모니터링 153

17 VDP 애플리케이션 지원 155

- VDP 애플리케이션 지원 156
 - 애플리케이션 에이전트 설치 156
 - Microsoft Windows에서 사용자 계정 컨트롤 설정 확인 156

UAC가 활성화된 경우 VDP 클라이언트 설치	156
Microsoft SQL Server 백업 및 복구	157
Microsoft SQL Server 옵션	157
하드웨어 요구 사항	157
Microsoft SQL Server 지원	157
VDP for SQL Server Client 설치	158
페일오버 클러스터에서 클러스터 클라이언트 구성	159
AlwaysOn 가용성 그룹에 대한 클러스터 클라이언트 구성	160
Microsoft SQL Server 백업 작업 생성	162
Microsoft SQL Server의 백업 복구	164
클라이언트 작업 모니터링	165
VDP Plug-in for SQL Server 제거	165
Microsoft Exchange Server 백업 및 복구	165
Microsoft Exchange Server 옵션	166
Microsoft Exchange Server 지원	166
Microsoft .NET Framework 4 요구 사항	166
하드웨어 요구 사항	166
지원되지 않는 Microsoft Exchange Server	167
VDP for Exchange Server Client 설치	167
DAG 또는 클러스터 환경에서 설치	167
Exchange DAG 클라이언트 구성	168
VMware Exchange Backup User Configuration Tool 사용	170
VDP 백업 서비스 수동 구성	171
Microsoft Exchange Server 백업 작업 생성	171
Microsoft Exchange Server의 백업 복구	173
DAG 또는 클러스터에서 복제 일시 중단	174
클라이언트 작업 모니터링	174
Exchange Server 플러그인 제거	174
Microsoft Exchange Server에 대한 세밀한 레벨의 복구	175
Microsoft SharePoint Server 백업 및 복구	178
하드웨어 요구 사항	178
지원되는 Microsoft SharePoint Server	178
VDP for SharePoint Server Client 설치	179
Microsoft SharePoint Server 백업 작업 생성	180
Microsoft SharePoint Server의 백업 복구	181
클라이언트 작업 모니터링	181
VDP Plug-in for SharePoint Server 제거	181
18 VDP 재해 복구	183
기본 재해 복구	184
184	
A VDP 포트 사용	185
B 필요한 최소 vCenter 사용자 계정 권한	189
C VDP 문제 해결	193
VDP 어플라이언스 설치 문제 해결	194
설치 관리자 패키지 문제 해결	194
VDP 관리 문제 해결	194
VDP 백업 문제 해결	195
VDP 백업 성능 문제 해결	197
VDP 복구 문제 해결	197
VDP 복제 문제 해결	199
VDP 무결성 검사 문제 해결	199

자동 백업 검증 문제 해결 199

Restore Client(파일 레벨 복구) 문제 해결 200

VDP 라이선스 등록 문제 해결 202

VDP 어플라이언스 문제 해결 202

VDP Microsoft Exchange Server 문제 해결 203

VDP Microsoft SQL Server 문제 해결 204

VDP Microsoft SharePoint Server 문제 해결 205

스토리지 용량 문제 해결 205

- VDP 로컬 스토리지 용량 모니터링 205
- Data Domain 스토리지 용량 모니터링 205
- 용량 문제 모니터링 206
- 스토리지 공간을 비우는 일반적인 단계 206

VDP 기술 자료 문서 액세스 207

색인 209

본 가이드 정보

*vSphere Data Protection 관리 가이드*에서는 중소, 성장, 중견 기업 환경을 위한 설치 및 백업 관리 정보에 대해 설명합니다. 본 가이드에서는 문제 해결 시나리오 및 권장 해결 방법도 다룹니다.

대상

본 가이드는 VDP(vSphere® Data Protection)를 사용하여 백업 솔루션을 제공하려는 사용자를 대상으로 합니다. 본 가이드에 수록된 정보는 가상 머신 기술 및 데이터 센터 운영에 익숙한 Windows 또는 Linux 시스템 관리자를 대상으로 합니다.

입력 표기법

VMware는 본 문서에서 다음과 같은 입력 표기법을 사용합니다.

굵은 글꼴	인터페이스 요소의 이름(예: 창, 대화상자, 버튼, 필드, 탭, 키, 메뉴 경로 등 특히 사용자가 선택하거나 클릭할 수 있는 요소의 이름)에 사용
<i>기울임꼴</i>	본문 중 참조되는 문서의 전체 제목에 사용
Monospace	용도 <ul style="list-style-type: none">■ 시스템 출력(예: 오류 메시지, 스크립트)■ 시스템 코드■ 경로 이름, 파일 이름, 프롬프트 및 구문■ 명령 및 옵션
<i>Monospace</i> <i>기울임꼴</i>	변수에 사용
Monospace 굵은 글꼴	사용자 입력에 사용
[]	선택적 값은 대괄호로 표시합니다.
	세로줄은 대체 선택 항목. 즉 또는을 의미합니다.
{ }	중괄호는 사용자가 지정해야 하는 내용(예: x, y 또는 z)을 의미합니다.
...	줄임표는 예에서 생략된 중요하지 않은 정보를 나타냅니다.

VMware Technical Publications 용어집

VMware Technical Publications에서는 사용자에게 생소할 수 있는 용어에 대한 정의를 제공합니다. VMware 기술 문서에서 사용된 용어에 대한 정의는 <http://www.vmware.com/kr/support/pubs>를 참조하십시오.

문서에 대한 의견

VMware는 문서 개선에 도움이 되는 제안 사항을 언제든지 환영합니다. 의견이 있으시면 docfeedback@vmware.com으로 보내주시기 바랍니다.

기술 지원 및 교육 리소스

다음 섹션에서는 이용할 수 있는 기술 지원 리소스에 대해 설명합니다. 다른 VMware 가이드의 최신 버전을 확인하려면 <http://www.vmware.com/kr/support/pubs>를 참조하십시오.

온라인 지원

온라인 지원을 사용하여 기술 지원 요청서를 제출하고 제품 및 계약 정보를 확인하고 제품을 등록하려면 http://www.vmware.com/support/phone_support.html을 참조하십시오.

지원 오퍼링

VMware 지원 오퍼링을 통해 비즈니스 요구 사항을 충족하는 방법에 대해 살펴보려면 <http://www.vmware.com/kr/support/services>를 참조하십시오.

VMware 전문 서비스

VMware Education Services 교육 과정은 현장 참조 톨로 사용하도록 고안된 광범위한 실습, 사례 연구 예제 및 교육 자료를 제공합니다. 교육 과정은 현장, 강의실 및 온라인으로 이용할 수 있습니다. 현장 파일럿 프로그램 및 구현을 위한 Best Practice를 위해 VMware Consulting Services는 가상화 환경을 평가, 계획, 구축 및 관리하는데 도움이 되는 오퍼링을 제공합니다. 교육 강의, 인증 프로그램 및 컨설팅 서비스에 대한 정보 확인하려면 <http://www.vmware.com/kr/services>를 참조하십시오.

vSphere Data Protection 이해

이 장에서 다루는 내용은 다음과 같습니다.

- “vSphere Data Protection 소개”(14페이지)
- “VDP의 이점”(14페이지)
- “VDP 기능”(15페이지)
- “복제”(17페이지)
- “파일 레벨 복구”(17페이지)
- “사용자 환경 개선 프로그램”(17페이지)
- “VDP 아키텍처”(17페이지)

vSphere Data Protection 소개

VDP(vSphere Data Protection)는 EMC 솔루션을 기반으로 하며 간단하게 구축할 수 있는 디스크 기반의 강력한 백업 및 복구 솔루션입니다. VDP는 VMware vCenter Server와 완벽하게 통합되어 백업 작업을 중앙에서 효율적으로 관리할 수 있을 뿐만 아니라 중복 제거된 대상 스토리지 위치에 백업을 저장할 수도 있습니다.

VMware vSphere Web Client 인터페이스는 가상 머신의 백업 및 복구를 선택, 예약, 구성 및 관리하는 데 사용됩니다.

백업하는 동안 VDP는 가상 머신의 일시 중지 스냅샷을 생성합니다. 중복 제거는 모든 백업 작업과 함께 자동으로 수행됩니다.

다음은 본 문서에서 백업 및 복구와 관련하여 사용되는 용어입니다.

- **데이터 저장소(datastore)**는 데이터 센터에서 기본이 되는 물리적 스토리지 리소스 조합에 대한 가상 표현으로, 가상 머신 파일에 대한 스토리지 위치(예: 물리적 디스크, RAID 또는 SAN)입니다.
- **CBT(Changed Block Tracking)**는 시간 경과에 따라 변경되는 가상 머신의 스토리지 블록을 계속 추적하는 VMkernel 기능입니다. VMkernel은 가상 머신의 블록 변경을 계속 추적함으로써 VMware의 vStorage API를 활용하기 위해 개발된 애플리케이션의 백업 프로세스를 개선합니다.
- **FLR(File Level Recovery)**를 사용하면 보호된 가상 머신의 로컬 관리자가 로컬 머신에 대한 백업을 찾아 마운트할 수 있습니다. 그런 다음 관리자는 마운트된 백업에서 개별 파일을 복구할 수 있습니다. FLR은 VDP Restore Client를 사용하여 수행됩니다.
- **VMware VADP(vStorage APIs for Data Protection)**를 사용하면 각 가상 머신 내부에서 백업 작업을 실행하는 데 따른 중단이나 오버헤드 없이도 백업 소프트웨어에서 중앙 집중식으로 가상 머신 백업을 수행할 수 있습니다.
- **VMDK(Virtual Machine Disk)**는 게스트 운영 체제에 물리적 디스크 드라이브로 표시되는 파일 또는 파일 집합입니다. 이러한 파일은 호스트 머신 또는 원격 파일 시스템에 있을 수 있습니다.
- **VDP 어플라이언스**는 VDP를 위해 특별히 구축된 가상 어플라이언스입니다.

VDP의 이점

VDP(vSphere Data Protection)의 이점은 다음과 같습니다.

- 전원이 꺼져 있거나 vSphere 호스트 간에 마이그레이션하는 경우에도 모든 가상 머신에 대해 빠르고 효율적인 데이터 보호 기능을 제공합니다.
- 전체 백업에서 특히 많은 가변 길이 중복 제거 기술을 사용하여 백업 데이터에 의해 소비되는 디스크 공간을 대폭 줄여줍니다.
- CBT(Changed Block Tracking) 및 VMware 가상 머신 스냅샷을 사용하여 가상 머신의 백업 비용을 줄여주고 백업 기간을 최소화합니다.
- 각 가상 머신에 타사 에이전트를 설치할 필요 없이 손쉽게 백업을 수행합니다.
- 웹 포털에서 관리할 수 있는 vSphere 내의 통합 구성 요소로 간단하고 직관적인 설치 방식을 사용합니다.
- vSphere Web Client에 통합된 VDP 구성에 바로 액세스합니다.
- 체크포인트 및 롤백 방식을 사용하여 백업을 보호합니다.
- 웹 기반 인터페이스에서 최종 사용자가 시작한 파일 레벨 복구를 사용하여 Windows 및 Linux 파일을 간단하게 복구합니다.
- vCenter Server를 사용할 수 없거나 사용자가 vSphere Web Client를 사용하여 VDP UI에 액세스할 수 없는 경우에 긴급 복구를 통해 가상 머신을 복구할 수 있도록 지원합니다.
- 복제를 통해 대상 타겟에 있는 백업 복제본을 사용할 수 있으므로 소스 VDP 어플라이언스에 장애가 발생하는 경우 데이터 손실을 방지할 수 있습니다.
- 중복 제거 저장소의 이점

기업의 데이터는 상당히 중복되어 있습니다. 즉, 시스템 내 또는 여러 시스템에서 동일한 파일이 존재합니다(예: 여러 수신자에게 전송된 운영 체제 파일 또는 문서). 편집된 파일도 이전 버전과 상당히 중복됩니다. 기존의 백업 방법은 모든 중복 데이터를 계속해서 저장하기 때문에 이 문제가 가중됩니다. 그러나 vSphere Data Protection은 특허 받은 중복 제거 기술을 사용하여 파일 및 하위 파일 데이터 세그먼트 레벨에서 중복을 제거합니다.

- 가변 길이 데이터 세그먼트와 고정 길이 데이터 세그먼트 비교

세그먼트(또는 하위 파일) 레벨에서 중복 데이터를 제거하는 핵심 요소는 세그먼트 크기를 확인하는 방법입니다. 고정 블록 또는 고정 길이 세그먼트는 일반적으로 스냅샷과 일부 중복 제거 기술에서 사용됩니다. 그러나 데이터 세트의 작은 변경(예: 파일 맨 앞에 데이터 삽입)으로도 데이터 세트의 전체 고정 길이 세그먼트가 변경될 수 있습니다. 이는 데이터 세트가 아주 조금만 변경된 경우에도 마찬가지입니다. vSphere Data Protection은 지능적인 가변 길이 방법을 사용하여 세그먼트 크기를 결정합니다. 즉, 데이터를 검사하여 논리적 경계 지점을 결정함으로써 효율성을 향상시켰습니다.

- 논리적 세그먼트 결정

VDP는 모든 시스템에서 최적의 효율성을 도출하기 위해 고안된, 특허 받은 세그먼트 크기 결정 방법을 사용합니다. VDP의 알고리즘은 컨텍스트에 따라 달라지는 세그먼트 경계를 결정하기 위해 데이터 세트의 바이너리 구조를 분석합니다. 가변 길이 세그먼트의 크기는 평균 24KB이고 이는 다시 평균 12KB로 추가 압축됩니다. VDP는 VMDK 파일 내의 바이너리 구조를 분석하여 모든 파일 유형 및 크기에 적용하고 데이터의 중복을 제거합니다.

VDP 기능

vSphere Data Protection 버전 6.0 제품부터는 이전에 VDP Advanced에 포함되었던 모든 기능이 포함되어 있습니다. VDP 기능은 vSphere Essential+의 일부로 포함되어 있으므로 특정 라이선스 키가 필요하지 않습니다. VDP 기능은 다음 표에 정리되어 있습니다.

표 1-1. VDP 기능

기능	VDP
VDP 어플라이언스당 지원되는 가상 머신	최대 400개
vCenter당 지원되는 어플라이언스 수	최대 20개
사용 가능한 스토리지 크기	0.5TB, 1TB, 2TB, 4TB, 8TB
이미지 레벨 백업 지원	있음
개별 디스크 백업 지원	있음
이미지 레벨 복구 작업 지원	있음
이미지 레벨 복제 작업 지원	있음
호스트에 직접 복구 지원	있음
분리/재마운트 가능한 데이터 파티션 지원	있음
FLR(File Level Recovery) 지원	예, 외부 프록시를 사용하여 LVM 및 EXT4 지원
Microsoft Exchange Server, SQL Server 및 SharePoint Server에 대한 게스트 레벨 백업 및 복구 지원	있음
애플리케이션 레벨 복제 지원	있음
Data Domain 시스템으로 백업 지원	있음
Microsoft Server에서 세밀한 레벨의 복구 기능	있음
ABV(Automatic Backup Verification) 지원	있음
외부 프록시 지원	예, 최대 개수인 8개의 외부 프록시가 구축된 경우 최대 24개의 동시 가상 머신 지원
사용자 환경 개선 프로그램에 대한 지원	있음

이미지 레벨 백업 및 복구

vSphere Data Protection은 가상 머신의 백업 처리 오버헤드를 VDP 어플라이언스로 분산시키기 위한 vSphere 내의 기능인 vStorage API for Data Protection과 통합되는 이미지 레벨 백업을 생성합니다. VDP 어플라이언스는 vCenter Server와 통신하여 가상 머신의 .vmdk 파일의 스냅샷을 생성합니다. 중복 제거는 특허 받은 가변 길이 중복 제거 기술을 사용하여 어플라이언스 내에서 진행됩니다.

규모가 크며 지속적으로 확장되고 있는 여러 VMware 환경을 지원하기 위해 각 VDP 어플라이언스는 내부 프록시를 사용하는 경우 최대 8개의 가상 머신을 동시에 백업할 수 있고, 최대 개수인 8개의 외부 프록시가 VDP 어플라이언스와 함께 구축된 경우 최대 24개의 가상 머신을 백업할 수 있습니다.

이미지 레벨 백업의 효율성을 높이기 위해 VDP는 CBT(Changed Block Tracking) 기능을 활용합니다. 이 기능은 주어진 가상 머신 이미지에 대한 백업 시간을 크게 줄이고 특정 백업 기간 내에 많은 가상 머신을 처리할 수 있도록 지원합니다.

복구하는 동안 CBT를 활용하면 VDP는 가상 머신을 원래 위치에 보다 빠르고 효율적으로 복구할 수 있습니다. 복구 프로세스 중에 VDP는 CBT를 사용하여 마지막 백업 이후 변경된 블록을 확인합니다. CBT를 사용하면 복구 작업 동안 vSphere 환경 내에서 데이터 전송이 줄어들고, 더욱 중요한 것은 복구 시간이 단축됩니다.

또한 VDP는 두 복구 방법(전체 이미지 복구 또는 CBT를 활용한 복구) 간 워크로드를 자동으로 평가하여 복구 시간이 가장 빠른 방법을 수행합니다. 이는 복구 대상 가상 머신에서 마지막 백업이 수행된 후 변경률이 매우 높거나 CBT 분석 작업의 오버헤드가 전체 이미지를 직접 복구하는 작업보다 더 높은 시나리오에서 유용합니다. VDP는 환경에서 가상 머신 이미지 복구 시간이 가장 빠른 방법을 결정합니다.

VDP는 내장 Platform Service Controller를 사용한 VCSA(vCenter Server Appliance)의 백업을 지원합니다.

외부 Platform Services Controller를 사용하여 vCenter Server 및 VCSA의 백업을 수행하려면 <http://kb.vmware.com/kb/2110294>에 나온 단계를 수행합니다.

단일 VMDK 백업 및 복구

전체 이미지 백업 작업에는 전체 VM(Virtual Machine)에 있는 모든 디스크가 하나의 이미지 백업으로 포함되어 있습니다. 개별 디스크 백업 작업에서는 필요한 디스크만 선택할 수 있습니다. 스냅샷 제한으로 인해 지원되지 않는 디스크 유형이 있는 VM의 이미지 레벨 백업에는 지원되지 않는 디스크 유형이 포함되지 않습니다.

VM을 복구할 때 VDP 어플라이언스는 VM 구성 파일(.vmx)을 복구하므로 원래 VM의 모든 VMDK가 생성됩니다. 원래 VMDK가 백업되지 않은 경우 복구 프로세스는 VMDK를 임시 VMDK로 생성합니다. 이 경우 VM의 기능이 완전하게 작동하지 않을 수 있습니다. 하지만 보호된 VMDK는 복구 시 액세스할 수 있습니다.

개별 디스크를 백업하는 방법에 대한 지침은 **“개별 디스크에 대한 백업 작업 생성”**(113페이지) 섹션을 참조하십시오.

게스트 레벨 백업 및 복구

VDP는 Microsoft SQL Server, Exchange Server 및 SharePoint Server에 대한 게스트 레벨 백업을 지원합니다. 게스트 레벨 백업을 사용하는 클라이언트 에이전트(VMware VDP for SQL Server Client, VMware VDP for Exchange Server Client 또는 VMware VDP for SharePoint Server Client)는 일반적으로 백업 에이전트가 물리적인 서버에 설치되는 방식과 동일하게 SQL Server, Exchange Server 또는 SharePoint Server에 설치됩니다.

VMware 게스트 레벨 백업의 이점은 다음과 같습니다.

- 가상 머신 내부의 Microsoft SQL Server, Microsoft Exchange Server 또는 SharePoint Server에 대한 추가적인 애플리케이션 지원 제공
- Microsoft SQL Server, Microsoft Exchange Server 또는 SharePoint Server 전체 또는 선택된 데이터베이스에 대한 백업 및 복구 지원
- 물리적 머신과 가상 머신에 동일한 백업 방식 제공

게스트 레벨 백업 및 복구에 대한 자세한 내용은 **“VDP 애플리케이션 지원”**(155페이지) 섹션을 참조하십시오.

복제

복제를 사용하면 소스 VDP 어플라이언스에서 장애가 발생한 경우에 대상 타겟에 있는 백업 복제본을 사용할 수 있으므로 데이터 손실을 방지할 수 있습니다.

복제 작업은 복제할 백업과 백업을 복제할 시간 및 위치를 결정합니다. 복구 시점이 없는 클라이언트에 대한 예약 복제 작업 또는 임시 복제 작업의 경우 클라이언트는 대상 서버에서만 복제됩니다. VDP6.0 이상으로 생성된 백업은 다른 VDP 어플라이언스, EMC Avamar 서버 또는 Data Domain 시스템에 복제될 수 있습니다. 타겟 VDP 어플라이언스가 5.8 이하인 경우 타겟은 VDP Advanced 또는 Replication Target Identity여야 합니다.

복제에 대한 자세한 내용은 15장, “복제,”(133페이지)를 참조하십시오.

파일 레벨 복구

FLR(File Level Recovery)을 사용하면 보호된 가상 머신의 로컬 관리자가 로컬 머신에 대한 백업을 찾아 마운트할 수 있습니다. 그런 다음 관리자는 마운트된 백업에서 개별 파일을 복구할 수 있습니다. FLR은 VDP Restore Client를 사용하여 수행됩니다.

FLR에 대한 자세한 내용은 16장, “파일 레벨 복구 사용,”(147페이지) 섹션을 참조하십시오.

사용자 환경 개선 프로그램

사용자 환경 개선 프로그램은 VDP 환경에 대한 암호화된 구성 및 사용 정보를 분석하기 위해 VMware 서버로 보낼 수 있게 해 주는 옵션입니다. 사용자 환경 개선 프로그램의 목적은 VDP에서 VDP 제품의 품질, 신뢰성 및 기능을 개선할 수 있도록 하는 것입니다. 사용자 환경 개선 프로그램은 기본적으로 활성화되어 있지 않습니다. 설치 중 VDP Configure 유틸리티의 제품 개선 페이지에서 사용자 환경 개선 프로그램을 활성화할 수 있습니다. 또한 VDP 설치 후에는 설치 후 UI에서 언제든지 이 옵션을 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 “사용자 환경 개선 프로그램 구성”(52페이지) 섹션을 참조하십시오.

VDP 아키텍처

VDP는 vSphere에서 지원하는 스토리지에 구축할 수 있습니다. 지원되는 스토리지는 VMFS, NFS 및 VSAN 데이터 저장소가 포함됩니다. VDP 관리는 vSphere Web Client를 사용하여 수행합니다.

백업 데이터는 중복 제거되고 VDP 가상 어플라이언스 또는 지원되는 Data Domain 어플라이언스를 구성하는 .vmdk 파일에 저장됩니다.

다음 그림에는 VDP의 일반 아키텍처가 나와 있습니다.

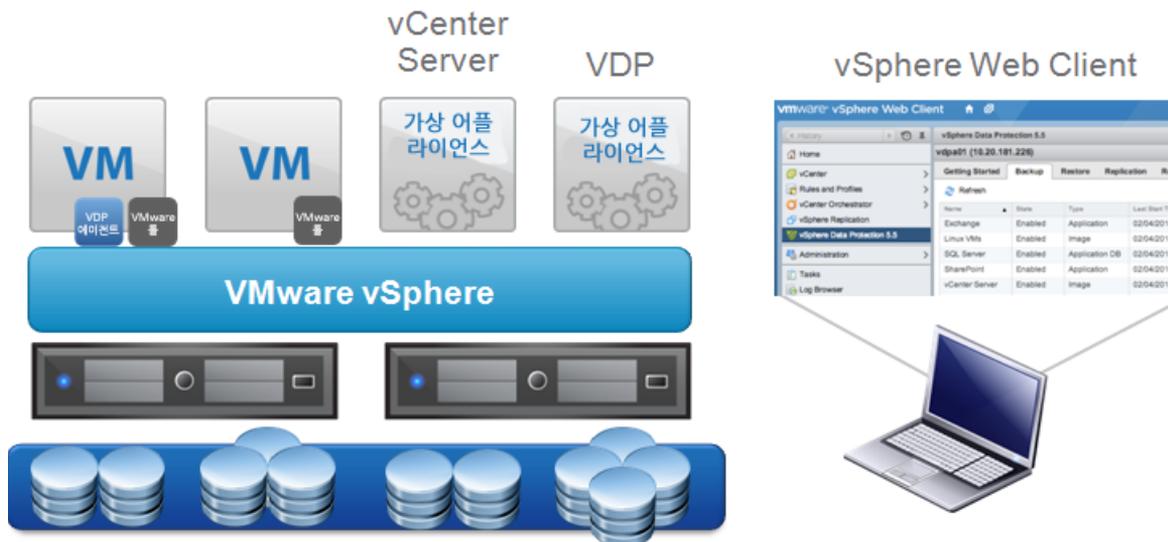


그림 1-1. VDP 일반 아키텍처

VDP 일반 아키텍처는 다음 구성 요소로 이루어집니다.

- vCenter Server 5.5 이상
- vSphere 호스트 버전 5.1 이상에 설치된 VDP 가상 어플라이언스
- vSphere Web Client
- 애플리케이션 백업 에이전트

다음 그림에는 VDP의 세부 아키텍처가 나와 있습니다.

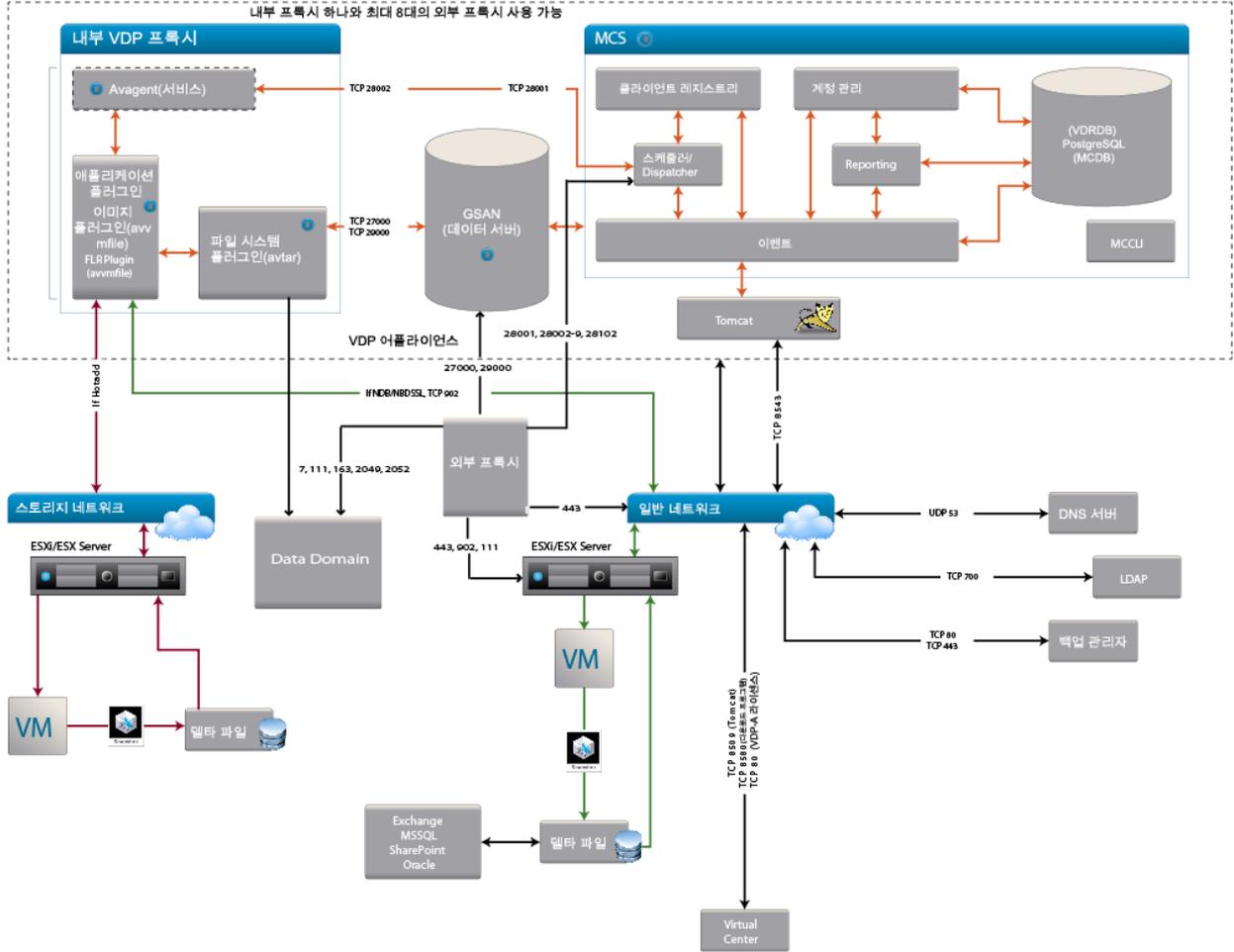


그림 1-2. VDP 세부 아키텍처

VDP의 세부 아키텍처는 다음과 같은 중요 구성 요소로 구성되어 있습니다.

- **MCS:** MCS(Management Console Server)는 VDP 서버에 대해 중앙 집중식 관리(스케줄링, 모니터링, 관리)를 제공하며 관리자가 사용하는 서버 측 프로세스를 실행합니다. 이러한 프로세스에는 모든 Java 프로세스와 postgres(SQL) 프로세스가 포함됩니다.

이 구성 요소에 해당하는 로그 파일은 `/usr/local/avamar/var/mc/server_log/mcserver.log`입니다.

- **AvAgent:** VDP 어플라이언스의 각 프록시 내에서 서비스로 실행됩니다. 이 구성 요소는 MCS와의 통신을 설정하고 유지 관리합니다. AvAgent는 들어오는 작업 지시를 위해 15초마다 한 번씩 MCS 서버를 폴링합니다. AvAgent는 백업 또는 복구와 같은 작업 지시에 대한 응답으로 AvVcbImage를 생성하며, 이에 따라 AvTar이 호출됩니다.

이 구성 요소에 해당하는 로그 파일은 `/usr/local/avamarclient/var-proxy-N/avagent.log`입니다.

- **AvVcbImage:** vSphere VMFS(Virtual Machine File System)에서 파일 및 디렉토리의 탐색, 백업 및 복구를 실행할 수 있게 합니다.

이 구성 요소에 해당하는 로그 파일은

`/usr/local/avamarclient/var-proxy-N/<Jobname>-<EPOCH>-vmimagew.log`입니다.

- **AvTar:** 백업 및 복구를 위한 주 프로세스입니다. AvTar은 GSAN과 통신합니다.

이 구성 요소에 해당하는 로그 파일은

`/usr/local/avamarclient/var-proxy-N/<Jobname>-<EPOCH>-vmimagew_avtar.log`입니다.

- **GSAN:** GSAN(Global Storage Area Network)은 VDP 어플라이언스의 구성 요소이며, 데이터 서버나 스토리지 서버로 불리기도 합니다.

이 구성 요소에 해당하는 로그 파일은 `/data01/cur/gsan.log`입니다.

VDP 설치 및 구성

이 장에서 다루는 내용은 다음과 같습니다.

- [“vSphere Data Protection 용량 요구 사항”](#)(22페이지)
- [“소프트웨어 요구 사항”](#)(22페이지)
- [“시스템 요구 사항”](#)(23페이지)
- [“설치 전 구성”](#)(23페이지)
- [“VDP Best Practice”](#)(26페이지)
- [“VDP 설치”](#)(29페이지)
- [“초기 구성”](#)(30페이지)

vSphere Data Protection 용량 요구 사항

VDP(vSphere Data Protection) 용량 요구 사항은 다음을 비롯한 여러 요소에 따라 달라집니다.

- 보호된 가상 머신의 수
- 각 보호된 가상 머신에 포함된 데이터의 양
- 백업되는 데이터의 유형(예: OS 파일, 문서 및 데이터베이스)
- 백업 데이터 보존 기간(일일, 주간, 월간 또는 연간)
- 데이터 변경률

참고 가상 머신의 크기, 데이터 유형 및 데이터 변경률이 평균적이고 보존 정책이 30일이라고 가정하면 1TB의 VDP 백업 데이터 용량으로 약 25대의 가상 머신을 지원할 수 있습니다.

소프트웨어 요구 사항

VDP 6.1에는 다음 소프트웨어가 필요합니다.

- vCenter Server 5.5 이상

VDP 6.1에서는 Linux 기반 vCenter Server 가상 어플라이언스와 Windows 기반 vCenter Server를 지원합니다.

- vSphere Web Client

다음 링크에서는 현재 vSphere 웹 브라우저 지원에 대한 정보를 제공합니다.

<https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.install.doc%2FGUID-F6D456D7-C559-439D-8F34-4FCF533B7B42.html&resultof=%22web%22%20%22client%22>

웹 브라우저에 Adobe Flash Player 11.3 이상이 활성화되어 있어야 vSphere Web Client 및 VDP 기능에 액세스할 수 있습니다.

- vSphere 호스트 5.0 이상

하드웨어 버전 및 마이그레이션

가상 머신의 하드웨어 버전은 최신 버전의 vSphere 호스트에 구성된 가상 머신을 이전 버전으로 마이그레이션할 수 없도록 제한합니다. VDP 어플라이언스를 5.1 이하 버전의 vSphere 호스트로 마이그레이션하면 작동하지 않습니다.

vSphere 호스트 및 vSphere Flash 읽기 캐시 호환성 및 성능

VDP 어플라이언스는 하드웨어 버전 7의 가상 머신으로 구축되므로 이전 vSphere 4.x 호스트와 호환됩니다. vSphere Flash Read Cache 지원 디스크는 vSphere 5.x 이상 호스트에서만 사용할 수 있으므로 가상 머신의 하드웨어 버전은 10 이상이어야 합니다. 결과적으로 VDP 어플라이언스를 사용하여 vSphere Flash 읽기 캐시 지원 디스크의 이미지 레벨 백업을 수행하려고 시도할 경우 현재 구성에서는 어플라이언스가 핫 애드(HotAdd) 대신 NBD(Network Block Device) 프로토콜을 전송 모드로 사용하므로 성능에 부정적인 영향을 미칩니다.

지원되지 않는 디스크 유형

- 백업을 계획할 때 VDP에서 디스크를 지원하는지 확인해야 합니다. 현재 VDP는 다음 가상 하드웨어 디스크 유형을 지원하지 않습니다.
 - 독립형
 - RDM 독립형 - 가상 호환 모드
 - RDM 물리적 호환 모드

지원되지 않는 가상 볼륨

VDP 어플라이언스 버전 6.1은 가상 볼륨(VVOL)에 있는 가상 머신의 백업 및 복구를 지원하지 않습니다.

시스템 요구 사항

다음 섹션에는 VDP의 시스템 요구 사항이 나와 있습니다.

VDP 시스템 요구 사항

VDP는 다음 구성으로 사용할 수 있습니다.

- 0.5TB
- 1TB
- 2TB
- 4TB
- 6TB
- 8TB

중요 VDP를 구축한 후 크기를 늘릴 수 있습니다.

VDP의 최소 시스템 요구 사항은 다음과 같습니다.

표 2-2. VDP의 최소 시스템 요구 사항

	0.5TB	1TB	2TB	4TB	6TB	8TB
프로세서	최소 2GHz 프 로세서 4개					
메모리	4GB	4GB	4GB	8GB	10GB	12GB
디스크 공간	873GB	1,600GB	3TB	6TB	9TB	12TB

IPv6 요구 사항

IPv6 환경에서 VDP가 사용하는 DNS 서버의 호스트 이름에는 AAAA 레코드만 포함되어야 합니다. DNS 서버에는 호스트 이름이 동일한 A 및 AAAA 레코드가 모두 포함되지 않아야 합니다.

설치 전 구성

VDP를 설치하기 전에 다음의 설치 전 단계를 완료하십시오.

- [“DNS 구성”](#)(23페이지)
- [“NTP 구성”](#)(24페이지)
- [“사용자 계정 구성”](#)(24페이지)
- [“VDP Best Practice”](#)(26페이지)

DNS 구성

DNS 서버는 VDP 및 vCenter에서 경방향 및 역방향 조회를 모두 지원해야 합니다.

VDP를 구축하기 전에 IP_address_VDP_Appliance 및 FQDN(Fully Qualified Domain Name)에 대해 DNS 서버에 항목을 추가해야 합니다. 또한 VMware 프록시 노드(포트 53)에서 TCP 프로토콜과 UDP 프로토콜 모두를 통해 DNS와 통신할 수 있어야 합니다. DNS를 제대로 설정하지 못할 경우 런타임 또는 구성 문제가 많이 발생할 수 있습니다.

DNS가 제대로 구성되어 있는지 확인하려면 vCenter Server에서 명령 프롬프트를 사용하여 다음 명령을 실행하십시오.

- `nslookup <FQDN_of_VDP>`

이 `nslookup` 명령은 VDP 어플라이언스의 FQDN을 반환합니다.

- `nslookup <FQDN_of_vCenter>`

이 `nslookup` 명령은 vCenter Server의 FQDN을 반환합니다.

`nslookup` 명령에서 적절한 정보를 반환하는 경우 명령 프롬프트를 닫습니다. `nslookup` 명령에서 찾는 정보를 반환하지 않는 경우에는 vCenter에서 `/etc/hosts` 파일에 VDP 이름과 주소를 수동으로 추가할 수 있습니다.

NTP 구성

VDP는 VMware 툴을 활용하여 NTP를 통해 시간을 동기화합니다. 모든 vSphere 호스트와 vCenter Server에서 NTP가 제대로 구성되어 있어야 합니다. VDP 어플라이언스는 vSphere를 통해 올바른 시간을 얻으므로 NTP로 구성하면 안 됩니다.

주의 VDP 어플라이언스에서 직접 NTP를 구성하는 경우 시간 동기화 오류가 발생할 수 있습니다.

NTP 구성에 대한 자세한 내용은 ESXi 및 vCenter Server 설명서를 참조하십시오.

vCenter 호스트 및 클러스터 보기

VDP 어플라이언스는 호스트 및 클러스터 보기에서 생성된 폴더 및 리소스 보기를 사용할 수 있습니다. vSphere Web Client의 호스트 및 클러스터 보기에서 다음 작업을 수행할 수 있습니다.

- 사용자 계정 구성
- 스냅샷 생성
- ISO 이미지 마운트
- 스냅샷 제거
- 스냅샷으로 되돌리기
- 디스크 확장
- VDP 어플라이언스 시스템 설정 구성
- vCenter 인벤토리에서 VDP 어플라이언스 제거

호스트 및 클러스터 보기 액세스

- 1 웹 브라우저에서 다음 주소로 vSphere Web Client에 액세스합니다.

`https://<IP_address_vCenter_Server>:9443/vsphere-client/`

- 2 관리자 권한으로 로그인합니다.
- 3 **vCenter** > 호스트 및 클러스터를 선택합니다.

사용자 계정 구성

vCenter 사용자 계정을 VDP에 사용하거나 SSO admin 사용자를 VDP에 사용하려면 먼저 이러한 사용자를 vCenter 루트 노드에 관리자로 추가해야 합니다. 그룹 역할에서 권한을 상속받은 사용자는 유효하지 않습니다.

참고 보안 수준이 높은 환경에서는 VDP 어플라이언스를 구성 및 관리하는 데 필요한 vCenter 사용자 계정 권한을 제한할 수 있습니다. 계정 권한 범주는 “필요한 최소 vCenter 사용자 계정 권한”(189페이지) 섹션에 나와 있습니다.

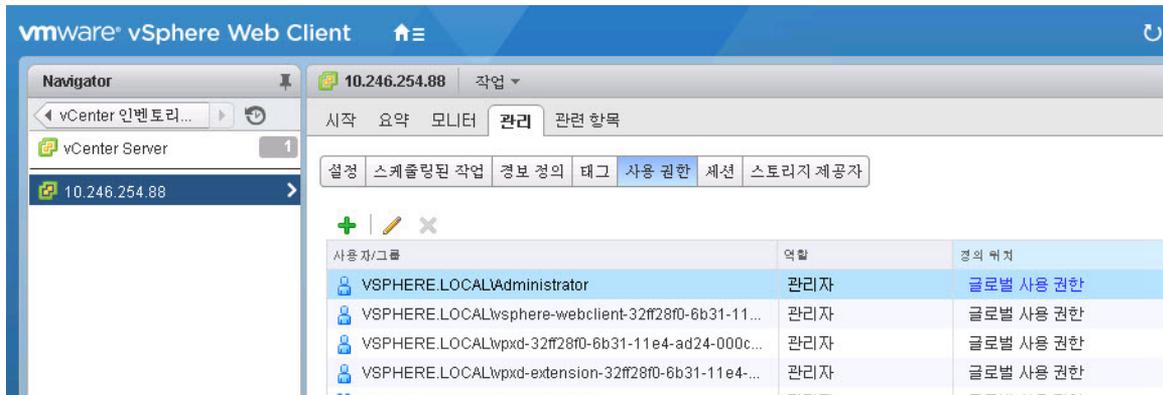
vSphere Web Client에서 다음 단계에 따라 VDP 사용자 또는 SSO admin 사용자를 구성하십시오.

- 1 웹 브라우저에서 다음 주소로 vSphere Web Client에 액세스합니다.

https://<IP_address_vCenter_Server>:9443/vsphere-client/

- 2 관리자 권한으로 로그인합니다.
- 3 **vCenter > 호스트 및 클러스터**를 선택합니다.
- 4 페이지 왼쪽에서 vCenter Server를 클릭합니다.

중요 트리 구조의 루트 수준에서 vCenter를 선택해야 합니다(**호스트 및 클러스터** 아래 표시됨). vCenter VM을 선택하면 구성이 실패합니다.



- 5 관리 탭을 클릭한 다음 **사용 권한**을 선택합니다.
- 6 **사용 권한 추가(+)** 아이콘을 클릭합니다.
- 7 **추가**를 클릭합니다.
- 8 도메인 드롭다운 목록에서 도메인, 서버 또는 VSPHERE.LOCAL을 선택합니다.
참고: vCenter 5.1 이전 버전의 경우 기본 도메인은 SYSTEM-DOMAIN입니다.
- 9 VDP를 관리하거나 SSO admin 사용자 역할을 할 사용자를 선택한 다음 **추가**를 클릭합니다.
- 10 **확인**을 클릭합니다.
- 11 **할당된 역할** 목록에서 **관리자**를 선택합니다.
- 12 **하위 객체에 전파** 상자가 선택되어 있는지 확인합니다.
- 13 **확인**을 클릭합니다.

사용자가 관리자 아래에 나열되는지 확인하려면 **홈 > 관리 > 역할 관리자**로 이동하여 **관리자** 역할을 클릭합니다. 방금 추가한 사용자가 해당 역할의 오른쪽에 나열되어야 합니다.

중요 VDP Configure 유틸리티를 사용하는 VDP 백업 사용자가 도메인 계정에 속한 경우 VDP-configure에서 "SYSTEM-DOMAIN\admin" 형식을 사용하십시오. 사용자 이름을 "admin@SYSTEM-DOMAIN" 형식으로 입력한 경우 백업 관련 작업이 최근에 실행 중인 작업에 표시되지 않을 수 있습니다.

중요 도메인 계정 암호에는 공백을 포함할 수 없습니다.

VDP Best Practice

VDP(vSphere Data Protection) 어플라이언스를 구축, 사용 및 모니터링할 때 다음 Best Practice를 따라야 합니다.

일반적인 Best Practice

- 블록 크기 제한을 피하기 위해 VDP 어플라이언스를 공유된 VMFS5 이상에 구축하십시오.
- CBT(Changed Block Tracking)를 지원하려면 모든 가상 머신에서 하드웨어 버전 7 이상을 실행하고 있어야 합니다.
- VDP가 백업할 각 가상 머신에 VMware Tools를 설치하십시오. VMware 툴은 백업을 진행하기 전에 게스트 운영 체제에서 특정 프로세스를 중지시키는 추가적인 백업 기능을 제공합니다. VMware 툴은 파일 레벨 복구를 사용하는 일부 기능을 위해서도 필요합니다.
- VDP 어플라이언스 및 vCenter의 네트워크를 구성할 경우 NAT 또는 기타 구성 방법(방화벽, IDS 또는 TSNR)을 사용하여 네트워크 주소 정보를 수정하지 마십시오. 이러한 지원되지 않는 방법을 가상 네트워크의 일부로 구축하면 일부 VDP 기능이 설계대로 작동하지 않을 수 있습니다.

구축 Best Practice

VDP 어플라이언스를 구축할 때는 항상 다음 사항을 Best Practice로 고려하십시오.

- 어플라이언스를 구축하기 전에 VDP 어플라이언스에 대한 DNS 레코드를 생성합니다. DNS에서 정방향 및 역방향 조회가 모두 설정되어 있는지 확인합니다.
- VDP를 구축할 때 마지막 단계 중 하나는 스토리지 성능 분석을 실행하는 옵션입니다. VDP가 실행되고 있는 스토리지가 성능 요구 사항을 충족하거나 초과하는지 확인하려면 이 분석을 실행합니다. 분석을 완료하는 데는 30분에서 몇 시간까지 소요될 수 있습니다.
- 보호된 가상 머신이 상주할 위치가 아닌 별도의 데이터 저장소에 VDP 어플라이언스를 배치합니다.
- 백업 작업을 예약할 때 시작 시간에 시차를 두는 것을 고려합니다.
- 데이터베이스나 Exchange Server와 같이 변경률이 높은 애플리케이션을 백업할 때는 비정형 데이터가 있는 다른 VM의 이미지 레벨 백업과 인터리빙(최적화)합니다.

데이터베이스는 정형 데이터에 속하고 이미지 레벨 백업은 비정형 데이터에 속합니다. 데이터베이스는 고유한 데이터를 생성하는 경우가 많아 중복 제거 비율이 낮지만 이미지 레벨 백업은 중복 제거 비율이 높습니다. 두 애플리케이션 백업 간에서 이미지 레벨 백업을 인터리빙하면 중복 제거 엔진의 부하가 감소하여 백업 성능이 향상됩니다.

참고 일반적으로, 스냅샷 처리 시간이 오래 걸려 성능에 영향을 미칠 수 있으므로 변경률이 높은 애플리케이션 또는 VM는 이미지 레벨 백업을 수행하지 마십시오.

- 실행 중일 수 있는 다른 프로세스를 고려합니다. 백업 작업이 실행 중일 때 복제 또는 자동 백업 검증을 예약하지 마십시오. 가능하면 이러한 작업이 백업 작업이 완료된 후 유지 보수 시간이 시작되기 전에 실행되도록 예약합니다.
- 내부 프록시가 활성화되어 있어야 하며 긴급 복구 작업을 수행할 때 자동으로 활성화됩니다.

핫 애드(HotAdd) Best Practice

백업 및 복구 속도는 높이고 네트워크 라우팅, 방화벽 및 SSL 인증서 문제에 대한 노출은 줄이기 위해 핫 애드(HotAdd) 전송 방식이 권장됩니다. 핫 애드(HotAdd) 대신 NBD(Network Block Device) 전송 방식이 사용되는 경우 백업 성능이 저하됩니다.

핫 애드(HotAdd)로 마운트될 디스크에 대해 다음 필수 요구 사항을 충족해야 합니다.

- vSphere Host 버전 5.0을 사용하는 경우에는 호스트에 핫 애드(HotAdd)에 대한 라이선스가 있어야 합니다. vSphere Host 5.1 이상 버전에는 이 기능이 기본적으로 포함됩니다.
- 백업할 가상 디스크가 포함된 스토리지에 대한 경로가 있는 vSphere 호스트에 VDP 어플라이언스를 구축해야 합니다.
- 핫 애드(HotAdd)는 IDE로 구성된 가상 디스크에는 사용되지 않습니다. 네트워크를 통한 입출력은 성능에 부정적인 영향을 미칩니다. 대신 SCSI 가상 디스크를 사용하십시오.
- VDP가 상주하는 VMFS 볼륨의 총 용량은 백업할 최대 가상 디스크의 크기와 동일해야 합니다. 사용 가능한 용량은 이 크기보다 적을 수 있습니다.
- VDP가 상주하는 VMFS 볼륨의 블록 크기는 백업할 최대 가상 디스크의 크기보다 크거나 같아야 합니다.
- 백업할 가상 머신에는 독립적인 가상 하드 디스크가 없어야 합니다.
- 백업할 가상 머신은 VDP 어플라이언스와 동일한 데이터 센터(vCenter Server 컨테이너 개체)에 있어야 합니다. 핫 애드(HotAdd) 전송은 데이터 센터 경계를 교차할 수 없습니다.
- vCenter Server의 VMDK 및 가상 머신은 백업할 가상 머신과 관련된 것과 이름이 동일해야 합니다.
- vSphere Flash 읽기 캐시(vFlash)를 사용하는 가상 머신에서는 핫 애드(HotAdd)가 작동하지 않습니다.

핫 애드(HotAdd) Best Practice에 대한 자세한 내용은 다음 기술 자료 문서를 참조하십시오.

<http://kb.vmware.com/kb/2048138>

초기 VDP 구축 시의 스토리지 용량

새로운 VDP(vSphere Data Protection) 어플라이언스가 구축되면 일반적으로 해당 어플라이언스가 처음 몇 주 동안 빠르게 채워집니다. 이는 백업되는 거의 모든 클라이언트가 고유한 데이터를 포함하기 때문입니다. 다른 유사한 클라이언트가 백업되거나 동일한 클라이언트가 한 번 이상 백업되는 경우에는 VDP 중복 제거 기능이 가장 효과적입니다.

따라서 초기 백업 후 후속 백업에서 어플라이언스에 백업되는 고유한 데이터는 더 줄어듭니다. 초기 백업이 완료되고 최대 보존 기간이 지나면 시스템이 해제되는 만큼의 새로운 데이터를 매일 저장할 수 있을지 관찰 및 측정할 수 있습니다. 이를 용량 활용도의 안정 상태에 도달했다고 합니다. 안정 상태의 이상적인 용량은 80%입니다.

사이징

vSphere Data Protection 사이징은 다음을 기준으로 필요한 vSphere Data Protection 어플라이언스의 크기와 수를 결정하는 데 도움이 됩니다.

- VM 수 및 유형(VM이 파일 시스템 또는 데이터베이스 데이터를 포함하는가?)
- 데이터 양
- 보존 기간(매일, 매주, 매월, 매년)
- 일반적인 변경률

다음 표에는 vSphere Data Protection 사이징 권장 사항에 대한 예가 나와 있습니다.

표 2-3. vSphere Data Protection 사이징 권장 사항의 예

VM 수	클라이언트당 데이터 스토리지	보존 기간 : daily	보존 기간 : 주별	보존 기간 : monthly	보존 기간 : yearly	권장 사항
25	20	30	0	0	0	1-0.5TB
25	20	30	4	12	7	1-2TB
25	40	30	4	12	7	2-2TB
50	20	30	0	0	0	1-1TB
50	20	30	4	12	7	2-2TB
50	40	30	4	12	7	3-2TB
100	20	30	0	0	0	1-2TB
100	20	30	4	12	7	3-2TB
100	40	30	4	12	7	6-2TB

위의 권장 사항(지침으로만 참조)은 다음과 같은 가정을 기반으로 합니다.

- VM은 주로 파일 시스템 데이터를 포함합니다. VM이 데이터베이스 데이터를 포함하는 있는 경우 중복 제거 비율이 낮아집니다.
- 파일 시스템 데이터에 대한 초기 중복 제거 비율은 70%입니다.
- 파일 시스템 데이터에 대한 일일 중복 제거 비율은 99.7%입니다.
- 연간 증가율은 5%입니다.

중요 구축할 어플라이언스의 크기를 확실히 알 수 없는 경우 더 큰 vSphere Data Protection 데이터 저장소를 사용하는 것이 좋습니다. 애플리케이션을 구축하고 난 후에는 데이터 저장소의 크기를 변경할 수 없습니다.

VDP 용량 모니터링

VDP 용량은 사전 예방적으로 모니터링해야 합니다. **VDP 보고서** 탭의 사용된 용량에서 VDP 용량을 확인할 수 있습니다(안정 상태를 결정하는 데 사용됨). 자세한 내용은 **“보고서 탭에서 정보 보기”**(106페이지) 섹션을 참조하십시오.

표 2-4에서는 주요 용량 임계값에 대한 VDP 동작에 대해 설명합니다.

표 2-4. 용량 임계값

임계값	값	동작
용량 경고	80%	VDP에서 경고 이벤트를 실행합니다.
용량 오류	95%	용량이 95% 이상 차 있으면 백업 작업을 위한 작업이 vCenter에서 생성되지 않습니다.
상태 점검 한도	95%	기존 백업을 완료할 수 있지만 새 백업 작업은 일시 중단됩니다. VDP에서 경고 이벤트를 실행합니다.
서버 읽기 전용 한도	100%	VDP는 어플라이언스 상태를 관리자로 변경함으로써 읽기 전용 모드로 전환되며 새 데이터를 허용하지 않습니다.

용량이 80%를 초과하면 다음의 용량 관리 지침을 사용하십시오.

- 새 가상 머신을 백업 클라이언트로 추가하는 것을 중단
- 불필요한 복구 시점 제거
- 이제는 필요 없게 된 작업 삭제
- 보존 정책을 재평가하여 보존 정책을 줄일 수 있는지 확인
- VDP 어플라이언스 추가 고려 및 여러 개의 어플라이언스 간 백업 작업의 균형 유지

VDP 설치

VDP(vSphere Data Protection) 설치하는 두 단계를 통해 완료됩니다.

- “OVF 템플릿 배포”(29페이지)
- “초기 구성”(30페이지)

OVF 템플릿 배포

사전 요구 사항

- vSphere 호스트 5.0 이상
- vCenter Server 5.5 이상
- vSphere Web Client에서 vCenter Server에 로그인하여 OVF 템플릿을 구축합니다. vSphere Web Client에 연결할 수 없으면 vSphere Web Client 서비스가 시작되었는지 확인합니다.
- VDP 어플라이언스는 포트 902를 사용하여 vSphere 호스트에 연결합니다. VDP 어플라이언스와 vSphere 호스트 사이에 방화벽이 있는 경우 포트 902를 열어야 합니다. 포트 사용에 대한 자세한 내용은 [A장, “VDP 포트 사용,”](#)(185페이지) 섹션을 참조하십시오.
- VMware Client Integration Plug-in을 브라우저에서 설치해야 합니다. 설치되어 있지 않은 경우 다음 절차 중에 설치할 수 있습니다.

절차

- 1 웹 브라우저에서 다음 주소로 vSphere Web Client에 액세스합니다.
https://<IP_address_vCenter_Server>:9443/vsphere-client/
- 2 관리자 권한으로 로그인합니다.
- 3 **vCenter > 데이터 센터**를 선택합니다.
- 4 **객체 탭에서 작업 > OVF 템플릿 배포**를 클릭합니다.
- 5 메시지가 표시되면 VMware Client Integration Plug-in을 허용 및 설치합니다.
- 6 VDP 어플라이언스가 있는 소스를 선택합니다. 기본적으로 파일 이름 대화상자는 OVF 패키지(*.ovf)로 설정되어 있습니다. 파일 이름의 오른쪽 드롭다운 상자에서 **OVA 패키지(*.ova)**를 선택합니다.
- 7 VDP 어플라이언스 .ova 파일의 위치로 이동합니다. 데이터 저장소에 맞는 적절한 파일을 선택했는지 확인합니다. **열기**를 클릭합니다.
- 8 VDP 어플라이언스 .ova 파일을 선택한 후 **다음**을 클릭합니다.
- 9 템플릿 세부 정보를 검토하고 **다음**을 클릭합니다.
- 10 EULA 동의 화면에서 라이선스 계약을 읽고 **동의를** 클릭한 후 **다음**을 클릭합니다.
- 11 이름 및 폴더 선택 화면에서 VDP 어플라이언스 이름을 입력합니다. 이름을 입력할 때 FQDN(Fully Qualified Domain Name)을 사용하십시오. VDP 구성이 vCenter 인벤토리에서 어플라이언스를 찾을 때 이 이름을 사용합니다. 설치 후에는 VDP 어플라이언스 이름을 변경하지 마십시오.
- 12 VDP 어플라이언스를 배포할 폴더 또는 데이터 센터를 클릭한 후 **다음**을 클릭합니다.
- 13 리소스 선택 화면에서 VDP 어플라이언스에 대한 호스트를 선택하고 **다음**을 클릭합니다.
- 14 스토리지 선택 화면에서 가상 디스크 형식을 선택하고 VDP 어플라이언스에 대한 스토리지 위치를 선택합니다. **다음**을 클릭합니다.
- 15 네트워크 설정 화면에서 VDP 어플라이언스에 대한 대상 네트워크를 선택하고 **다음**을 클릭합니다.
- 16 템플릿 사용자 지정 화면에서 **기본 게이트웨이 DNS, 네트워크 1 IP 주소 및 네트워크 1 넷마스크**를 지정합니다. IP 주소가 올바르게 DNS 서버의 항목과 일치하는지 확인합니다. 이 대화상자에서 잘못된 IP 주소를 설정하면 .ova를 다시 배포해야 합니다. **다음**을 클릭합니다.

참고 VDP 어플라이언스는 DHCP를 지원하지 않습니다. 정적 IP 주소가 필요합니다.

17 완료 준비 화면에서 모든 구축 옵션이 올바르게 확인합니다. **구축 후 전원 켜기** 옵션을 선택하고 **마침**을 클릭합니다.

vCenter는 VDP 어플라이언스를 구축하고 설치 모드로 부팅합니다. **최근 작업**을 모니터링하여 구축이 완료되는 시점을 확인할 수 있습니다.

초기 구성

사전 요구 사항

- VDP .ovf 템플릿이 성공적으로 구축되었는지 확인하십시오. 자세한 내용은 **“OVF 템플릿 배포”**(29페이지) 섹션을 참조하십시오.
- 사용자가 vSphere Web Client를 통해 vCenter Server에 로그인한 상태여야 합니다.
- 데이터 저장소에 가용 디스크 공간이 충분해야 합니다. 초기 어플라이언스 구성 중에 선택 사항인 성능 분석 테스트를 실행하는 경우 데이터 저장소당 각 디스크에 41GB가 필요합니다(예를 들면 동일한 데이터 저장소에 디스크가 3개 있는 경우 가용 공간 123GB가 필요함). 사용 가능한 공간이 부족한 경우 테스트에서는 읽기, 쓰기 및 검색(선택 사항) 테스트 모두에 대해 0 값을 보고하고 최종 상태를 공간 부족으로 표시합니다.

절차

1 웹 브라우저에서 다음 주소로 vSphere Web Client에 액세스합니다.

https://<IP_address_vCenter_Server>:9443/vsphere-client/

2 관리자 권한으로 로그인합니다.

3 **vCenter 홈 > vCenter > VM 및 템플릿**을 선택합니다. vCenter 트리를 확장하고 VDP 어플라이언스를 선택합니다.

4 VDP 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **콘솔 열기**를 선택하여 VDP 어플라이언스로 콘솔 세션을 엽니다.

5 설치 파일이 로드되면 VDP 메뉴에 대한 시작 페이지가 나타납니다. 웹 브라우저를 열고 다음을 입력합니다.

https://<IP_address_VDP_appliance>:8543/vdp-configure/

VDP 로그인 페이지가 표시됩니다.

6 **사용자** 필드에 **root**를 입력하고 **암호** 필드에 **changeme**를 입력한 다음 **로그인**을 클릭합니다.

VDP 시작 페이지가 나타납니다.

7 다음을 클릭합니다.

네트워크 설정 대화상자가 기본적으로 나타납니다.

8 VDP 어플라이언스에 대한 다음 네트워크 및 서버 정보를 지정하거나 확인합니다. 값이 올바르게 채워졌는지 확인합니다. 값이 올바르게 않으면 설치가 실패합니다.

a IPv4 또는 IPv6 정적 주소

b 넷마스크

c 게이트웨이

d 기본 DNS

e 보조 DNS

f 호스트 이름

g 도메인

- 9 다음을 클릭합니다.
시간대 대화상자가 나타납니다.
- 10 VDP 어플라이언스에 적합한 시간대를 선택하고 다음을 클릭합니다.
VDP 자격 증명 대화상자가 나타납니다.
- 11 암호 필드에 다음 기준에 따라 VDP 어플라이언스 암호를 입력한 다음 **암호 확인** 필드에 암호를 다시 입력하여 암호를 확인합니다. 이 암호는 범용 구성 암호입니다.
4가지 문자 클래스는 다음과 같습니다.
- 대문자 A-Z
 - 소문자 a-z
 - 숫자 0-9
 - 특수 문자(예: ~!@#,.)
- 다음 기준에 따라 암호를 생성합니다.
- 4가지 문자 클래스를 모두 사용하는 경우 암호는 6자 이상이어야 합니다.
 - 3가지 문자 클래스를 사용하는 경우 암호는 7자 이상이어야 합니다.
 - 1~2가지 문자 클래스를 사용하는 경우 암호는 8자 이상이어야 합니다.
- 12 다음을 클릭합니다.
vCenter 등록 페이지가 나타납니다.

vCenter 등록
vCenter 서버의 호스트 이름 또는 IP 주소를 지정하십시오. 또한 vCenter 서버에 객체를 등록할 수 있는 권한이 있는 사용자의 사용자 이름과 암호를 제공하십시오.

vCenter 사용자 이름:

vCenter 암호:

vCenter FQDN 또는 IP:

vCenter HTTP 포트:

vCenter HTTPS 포트:

vCenter 인증서를 검증합니다.

인증서 업로드:

SSO 인증을 위해 vCenter 사용

13 다음 필드에 정보를 입력합니다.

- vCenter 사용자 이름

사용자가 도메인 계정에 속한 경우 "SYSTEM-DOMAIN\admin" 형식으로 이름을 입력합니다.

주의 SSO admin 사용자가 <username@vsphere.local> 형식의 vCenter 사용자 이름으로 지정된 경우 VDP 운영 관련 작업은 vSphere Web Client의 vCenter Recent Tasks 창에 나타나지 않습니다. 작업이 Recent Tasks 창에 나타나게 하려면 SSO admin 사용자를 <vsphere.local\username> 형식으로 지정합니다.

- vCenter 암호

- vCenter FQDN 또는 IP

- vCenter HTTP 포트

기본 포트는 80입니다. 기본 포트 이외의 포트를 사용하려면 **/etc/firewall.base**에서 포트를 열고 **avfirewall** 서비스를 다시 시작해야 합니다.

다른 모든 통신에 사용되는 HTTPS 포트 대신 HTTP 포트를 통해 vCenter에 연결해야 하는 경우 HTTP 포트에 대해 사용자 지정 값을 지정합니다.

- vCenter HTTPS 포트

기본 포트는 443입니다. 기본 포트 이외의 포트를 사용하려면 **/etc/firewall.base**에서 포트를 열고 **avfirewall** 서비스를 다시 시작해야 합니다.

이 필드가 비활성화된 경우 SSO 인증에 대해 **SSO 인증을 위해 vCenter 사용** 확인란을 선택합니다.

참고 vCenter의 vCenter 서버 어플라이언스에 SSO가 포함된 경우 **SSO 인증을 위해 vCenter 사용** 확인란을 활성화된 상태로 두십시오. 확인란을 선택 취소하여 이 선택을 비활성화하는 경우 SSO 서버 FQDN 또는 IP 주소와 SSO 포트 필드를 입력해야 합니다.

- 연결 테스트를 클릭합니다.

연결 성공 메시지가 나타납니다. 이 메시지가 나타나지 않으면 설정 문제를 해결하고 성공 메시지가 나타날 때까지 이 단계를 반복합니다.

vCenter 등록 페이지에 다음과 같은 메시지가 표시될 경우 **"사용자 계정 구성"**(24페이지)에 설명된 단계를 수행합니다.

지정된 사용자가 vDP 전용 사용자가 아니거나 vDP를 관리할 vCenter 권한이 부족합니다. 사용자 역할을 업데이트하고 다시 시도하십시오.

14 다음을 클릭하여 스토리지 유형 선택 과정을 안내하는 **스토리지 생성** 페이지로 진행합니다. 스토리지 구성 정보와 초기 구성 마법사를 완료하는 데 필요한 최종 단계는 **"새 스토리지 생성"**(70페이지) 섹션을 참조하십시오.

VDP 어플라이언스 마이그레이션

이 장은 다음과 같은 항목으로 구성되어 있습니다.

- [“VDP 어플라이언스 5.8.x 이상에서 6.1로 마이그레이션”](#)(34페이지)

VDP 어플라이언스 5.8.x 이상에서 6.1로 마이그레이션

VDP 6.1은 이전 버전에서의 업그레이드를 지원하지 않습니다. 하지만 모든 작업, 유지 보수 기간 및 데이터를 VDP 5.8.x 이상 어플라이언스에서 VDP 6.1 어플라이언스로 마이그레이션할 수 있습니다.

- 1 VDP 초기 구성 마법사를 시작합니다.
- 2 시작 페이지부터 vCenter 등록 페이지까지 필요한 필드를 지정합니다.
- 3 스토리지 생성 페이지에서 다음을 수행합니다.
 - a VDP 마이그레이션을 선택합니다.
 - b 다음 필드에 정보를 지정합니다.
 - IP 주소 : VDP 5.8.x 이상 어플라이언스의 IP 주소를 입력합니다 .
 - 암호 : VDP 5.8.x 이상 어플라이언스의 암호를 입력합니다 .
 - c 인증 검증을 클릭합니다.
인증이 성공하는지 확인하십시오.
 - d Next를 클릭합니다.
 - e 경고 메시지 상자에 VDP를 마이그레이션하면 소스 VDP <xx.xx.xx.xx>이(가) 종료됩니다. 계속하시겠습니까?라는 메시지가 나타나면 예를 클릭합니다.
 - f Next를 클릭합니다.
- 4 VDP 마이그레이션 페이지에서 다음을 수행합니다.
 - a 진행 상황과 로그 메시지가 올바르게 나타나는지 확인하십시오.
 - b Next를 클릭합니다.
- 5 디바이스 할당 페이지에서 다음을 수행합니다.
 - a 찾아보기 버튼을 클릭하여 ESX 데이터 저장소를 찾은 다음 순서에 관계 없이 마이그레이션할 VDP의 데이터 디스크를 선택합니다.
 - b 디스크 검증이 성공하는지 확인하십시오.
 - c Next를 클릭합니다.
- 6 CPU 및 메모리 페이지부터 완료 페이지까지 필요한 필드를 지정합니다.

VDP 어플라이언스의 설치 후 구성

이 장에서 다루는 내용은 다음과 같습니다.

- [“VDP-Configure 유틸리티 정보”](#)(36페이지)
- [“상태 보기”](#)(36페이지)
- [“서비스 시작 및 중지”](#)(37페이지)
- [“VDP 로그 또는 진단 정보 수집”](#)(38페이지)
- [“구성 설정 수정”](#)(40페이지)
- [“어플라이언스 롤백”](#)(41페이지)
- [“긴급 복구”](#)(42페이지)

VDP-Configure 유틸리티 정보

VDP(vSphere Data Protection) 설치 중에 VDP Configure 유틸리티는 "설치" 모드로 실행됩니다. 이 모드에서는 초기 네트워킹 설정, 시간대, VDP 어플라이언스 암호 및 vCenter 자격 증명을 입력할 수 있습니다. 또한 설치 모드에서 스토리지를 생성하거나 연결하고 경우에 따라 성능 평가 툴을 실행할 수 있습니다. 초기 설치 후 VDP Configure 유틸리티는 "유지 보수" 모드로 실행되고 다른 사용자 인터페이스가 표시됩니다.

VDP Configure 유틸리티에 액세스하려면 웹 브라우저를 열고 다음을 입력하십시오.

https://<IP_address_VDP_Appliance>:8543/vdp-configure/

VDP 어플라이언스 사용자 이름과 암호를 사용하십시오. VDP 구성 유틸리티에 로그인할 때 시스템 상태 점검 스크립트가 실행됩니다. VDP 구성 유틸리티 탭에서 구성 작업을 수행하기 위해서는 시스템 상태 점검이 완료 될 때까지 기다려야 합니다.

참고 어플라이언스를 구성한 후 선택적으로 VDP 구성 유틸리티에서 성능 분석 테스트를 실행할 수 있습니다. 테스트를 실행하려면 데이터 저장소당 각 디스크에 41GB가 필요합니다. 이 공간을 사용할 수 없으면 유틸리티에서는 공간이 부족하다고 보고하고 성능 분석 테스트가 실행되지 않습니다.

다음 구성 작업을 수행하려면 구성 인터페이스를 사용하십시오.

- **"스토리지 관리"**(69페이지): 스토리지 구성을 확인하고 Data Domain 시스템을 추가 및 편집하고 VDP 어플라이언스에서 디스크 스토리지를 추가 또는 확장할 수 있습니다.
- **"상태 보기"**(36페이지): VDP 어플라이언스에서 현재 실행 중이거나 중지된 서비스를 확인할 수 있습니다.
- **"서비스 시작 및 중지"**(37페이지): VDP 어플라이언스에서 선택한 서비스를 시작 및 중지할 수 있습니다.
- **"VDP 로그 또는 진단 정보 수집"**(38페이지): VDP 어플라이언스에서 문제 해결 목적으로 현재 로그를 다운로드할 수 있습니다.
- **"구성 설정 수정"**(40페이지): 네트워크 설정을 보거나 변경하고, vCenter 등록을 구성하고, 시스템 설정(시간대 정보 및 VDP 자격 증명)을 보거나 편집하고, 외부 프록시 및 내부 프록시 구성 옵션을 통해 프록시 처리량을 관리할 수 있습니다.
- **"어플라이언스 롤백"**(41페이지): VDP 어플라이언스를 이전에 확인된 유효한 상태로 복구할 수 있습니다.
- **"긴급 복구"**(42페이지): VDP 어플라이언스를 실행하는 호스트에 바로 가상 머신을 복구할 수 있습니다. 이 긴급 복구 절차는 vCenter를 사용할 수 없을 때 사용하기 위한 용도입니다.
- **"프록시 처리량 관리"**(63페이지): 외부 및 내부 프록시를 관리할 수 있습니다. 최대 8개의 외부 프록시 가상 머신을 구축할 수 있습니다. 8개의 외부 프록시를 구축하면 핫애드(Hot-Add) 기능을 사용하여 백업 처리량을 개선하고 더 많은 동시 백업 및 복구 작업을 실행할 수 있습니다.

상태 보기

구성 탭에 VDP에서 필요로 하는 모든 서비스와 각 서비스의 현재 상태가 나열됩니다. 표 4-5에서는 VDP에 사용되는 서비스에 대해 설명합니다.

표 4-5. VDP 어플라이언스에서 실행 중인 서비스에 대한 설명

서비스	설명
핵심 서비스	VDP 어플라이언스 백업 엔진을 구성하는 서비스입니다. 이 서비스가 비활성화되면 예약 또는 "필요 시" 백업 작업이 실행되지 않고 복구 작업을 시작할 수 없습니다.
관리 서비스	관리 서비스의 중지는 기술 지원부의 지시에 따라 수행해야 합니다.
파일 레벨 복구 서비스	파일 레벨 복구 작업의 관리를 지원하는 서비스입니다.
백업 복구 서비스	백업 복구를 지원하는 서비스입니다.
유지 보수 서비스	백업 보존 기간이 만료되었는지 여부를 평가하는 등 유지 보수 작업을 수행하는 서비스입니다. 유지 보수 서비스는 VDP 어플라이언스가 구축된 후 첫 24-48시간은 비활성 상태입니다. 이로 인해 초기 백업에 대한 백업 기간이 더 길어집니다.
백업 스케줄러	백업 스케줄러는 예약된 백업 작업을 시작하는 서비스입니다. 백업 스케줄러가 중지된 경우 예약 백업이 실행되지 않습니다. 필요 시 백업은 여전히 시작될 수 있습니다.

참고 실행이 중지된 서비스가 하나라도 있으면 vCenter Server에서 알림이 트리거됩니다. 중지된 서비스가 다시 시작되면 경보는 제거됩니다. 경보가 트리거되거나 제거되기 전에 최대 10분 정도 지연될 수 있습니다.

이 서비스를 위해 표시되는 상태는 다음 중 하나일 수 있습니다.

- 시작 중
- 시작 실패
- 실행 중
- 중지 중
- 중지 실패
- 중지됨
- 로드 중-가져오기 상태
- 복구 불가능(핵심 서비스만 해당)
- 복구 중(관리 서비스만 해당)
- 복구 실패(관리 서비스만 해당)

새로 고침 아이콘을 클릭하면 상태 표시가 업데이트됩니다.

서비스 시작 및 중지

상태 화면에서 **시작**을 클릭하여 중지된 서비스를 재시작할 수 있고 **중지**를 클릭하여 실행 중인 서비스를 중지할 수 있습니다. 그러나 일반적으로 실행 중인 서비스의 중지는 기술 지원부의 지시에 따라 수행해야 합니다.

서비스가 중지된 경우 **시작**을 클릭하여 재시작을 시도할 수 있습니다. 그러나 일부 경우 서비스가 제대로 작동하려면 추가 문제 해결 단계가 필요합니다.

모든 서비스가 중지되면 다음 순서로 서비스를 시작합니다.

- 1 핵심 서비스
- 2 관리 서비스
- 3 백업 스케줄러
- 4 유지 보수 서비스
- 5 파일 레벨 복구 서비스
- 6 백업 복구 서비스

VDP 로그 또는 진단 정보 수집

로그 수집기 탭에서는 VDP 로그 파일을 개별적으로나 전체적으로 다운로드할 수 있습니다. 로그 수집기 탭에는 로그 파일이 4개의 섹션으로 그룹화되어 있습니다. 표 4-6에서는 각 그룹의 로그 파일에 대해 설명합니다.

표 4-6. 로그 수집기 탭에서 사용할 수 있는 로그 파일

Group	로그 파일
모든 VDP 어플라이언스 로그	VDP 어플라이언스와 관련된 로그 파일
클라이언트 로그	Microsoft 애플리케이션과 관련된 로그 파일
구성	프록시, 구성 검사기, 에이전트 등의 VDP 구성 파일. 이러한 구성 파일은 /space/vdp/config에 있습니다.
외부 프록시 로그	외부 프록시 가상 머신의 로그 파일 이러한 로그 파일은 외부 프록시가 하나 이상 구축된 경우에만 표시됩니다.

참고 모든 로그는 /space/vdp/logs에 위치합니다.

모든 VDP 어플라이언스 로그 그룹은 다음 하위 그룹으로 구분되므로 특정 로그 파일만 다운로드할 수 있습니다.

표 4-7. 모든 VDP 어플라이언스 로그 그룹에서 사용할 수 있는 로그 파일

Group	로그 파일
핵심 VDP 서비스	GSAN, VDP, AVI, 시스템 및 DPN과 관련된 로그 파일
관리 서비스	MC 서버와 관련된 로그 파일
파일 시스템 서비스	HFScheck와 관련된 로그 파일
파일 레벨 복구 서비스	FLR과 관련된 로그 파일
복제	복제 및 복제 복구와 관련된 로그 파일
이미지 백업 및 복구	백업 및 복구와 관련된 로그 파일

절차

- 1 웹 브라우저를 열고 다음을 입력합니다.

https://<IP_address_VDP_Appliance>:8543/vdp-configure/

- 2 VDP 사용자 이름과 암호를 사용해서 로그인합니다.

- 3 로그 수집기 탭에서 하나 이상의 옵션을 선택하고 다운로드를 클릭하여 로그 파일을 다운로드합니다.

- **모든 VDP 어플라이언스 로그:** 이 옵션을 선택하고 다운로드를 클릭하여 모든 로그 파일을 VDP 서비스에서 .zip 파일로 다운로드합니다.

다운로드 위치 선택 대화상자가 나타납니다. 기본 로그 번들 이름은 LogBundle.zip입니다.

해당 파일을 고유한 이름으로 바꾸십시오. 로그 번들은 주로 VDP 어플라이언스 로그를 지원 담당자에게 보내기 위해 사용됩니다.

- 다음 목록에서 특정 제목 아래의 모든 로그를 다운로드하려면 해당 제목 옆의 확인란을 선택하고 다운로드를 클릭합니다.
- 여러 제목 아래에 나열된 로그 파일을 다운로드하려면 하나 이상의 로그 파일 옆에 있는 확인란을 선택하고 다운로드를 클릭합니다.
- **클라이언트 로그:** 클라이언트 장애 로그를 모두 포함하는 취합된 텍스트 파일을 다운로드하려면 이 옵션을 선택하고 다운로드를 클릭합니다.
- **구성:** VDP 구성 파일 정보만 다운로드하려면 이 옵션을 선택하고 다운로드를 클릭합니다.

다음 표에는 영역별 문제를 해결하기 위해 다운로드해야 하는 로그 파일에 대한 정보가 정리되어 있습니다.

표 4-8. 영역별 문제를 해결하기 위해 다운로드해야 하는 로그 파일

문제 해결 영역	로그 그룹	어플라이언스의 위치	다운로드할 관련 로그 파일
업그레이드	핵심 VDP 서비스 -> AVI	/space/vdp/logs/avi_logs/server_log/	avinstaller.log.0
이미지 백업 또는 복구	이미지 백업 및 복구 및 외부 프록시 로그 (외부 프록시를 사용하는 경우)	<ul style="list-style-type: none"> ■ /space/vdp/logs/image_proxy/avamarclient/ ■ /usr/local/avamarclient/var(외부 프록시의 경우) 	<ul style="list-style-type: none"> ■ *.log 파일(avtar 로그라고도 함, 백업에 대한 정보 포함) ■ *.alg 파일(작업 지시 정보 포함)
복제	복제	/space/vdp/logs/replicate/client/	<ul style="list-style-type: none"> ■ *Replicate-avrepscript.log ■ *Replicate.log ■ *Replicate.alg
파일 레벨 복구	파일 레벨 복구 서비스	<ul style="list-style-type: none"> ■ /usr/local/avamarclient/bin/logs ■ /space/vdp/logs/flr_proxy/ ■ /space/vdp/logs/vdp_logs/flr/server_logs/ 	<ul style="list-style-type: none"> ■ flr-server.log ■ *.log ■ flr_debug.txt ■ flr_msg.txt ■ flr_out.txt
VDP 플러그인	핵심 VDP 서비스 -> VDP	/space/vdp/logs/vdp_logs/vdr/server_logs/	vdr_server.log
VDP 구성 유틸리티	핵심 VDP 서비스 -> VDP	/space/vdp/logs/vdp_logs/vdr/server_logs/	vdr-configure.log
무결성 검사	파일 시스템 서비스 -> HFSCheck	/space/vdp/logs/hfsccheck/	*.log

다음 표에는 Microsoft 애플리케이션의 백업 및 복구 문제를 해결하기 위해 수집해야 하는 로그에 대한 정보가 정리되어 있습니다.

표 4-9. 영역별 문제를 해결하기 위해 다운로드해야 하는 로그 파일

Plug-in	로그 파일 위치	취합할 관련 로그 파일
SQL VDP 플러그인	<ul style="list-style-type: none"> ■ 독립 실행형 SQL: C:\Program Files\avp\var ■ SQL 페일오버 클러스터: 클러스터 구성 시 WCCW(Windows Cluster Configuration Wizard)를 사용하여 지정된 공유 드라이브의 var 폴더 ■ SQL AlwaysOn 클러스터: 클러스터 구성 시 WCCW를 사용하여 지정된 var 폴더 클러스터 구성 시 공유 드라이브가 지정된 경우 공유 드라이브에 모든 노드의 로그 파일이 포함됩니다. 클러스터 구성 시 로컬 폴더가 지정된 경우 각 클러스터 노드에 로그 파일이 포함됩니다. 	<ul style="list-style-type: none"> ■ SQL VSS 플러그인의 로그 ■ Avtar 로그 ■ Avagent 로그 ■ 클라이언트의 Windows 애플리케이션 및 시스템 이벤트 뷰어 로그
SharePoint VDP 플러그인	C:\Program Files\avp\var	<ul style="list-style-type: none"> ■ SharePoint VSS 플러그인의 로그 ■ Avtar 로그 ■ Avagent 로그 ■ 클라이언트의 Windows 애플리케이션 및 시스템 이벤트 뷰어 로그

표 4-9. 영역별 문제를 해결하기 위해 다운로드해야 하는 로그 파일

Plug-in	로그 파일 위치	취합할 관련 로그 파일
참고		
<ul style="list-style-type: none"> SharePoint 통합 팜에서 모든 SQL 백엔드를 포함한 모든 SharePoint Server 노드의 로그를 취합해야 합니다. SharePoint Server가 SQL 페일오버 또는 AlwaysOn 클러스터 또는 둘 모두에 연결된 경우 클러스터 구성 시 WCCW를 사용하여 지정된 공유 var 폴더에도 로그 집합이 생성됩니다. 		
Exchange VDP 플러그인	<ul style="list-style-type: none"> 각 VDP 클라이언트: C:\Program Files\avp\var Exchange DAG용 Windows Cluster Configuration Wizard에서 지정된 공유 var 폴더 	<ul style="list-style-type: none"> Exchange 플러그인의 로그 Avtar 로그 Avagent 로그 클라이언트의 Windows 애플리케이션 및 시스템 이벤트 뷰어 로그

구성 설정 수정

설치 후 VDP Configure 유틸리티에 액세스하면 VDP Configure 유틸리티가 유지 보수 모드로 실행됩니다. 유지 보수 모드에서 **구성** 탭을 클릭하면 모든 설정을 지정하거나 설치할 때 입력한 설정을 수정할 수 있습니다. 네트워크 설정 및 시스템 설정을 구성하고 vCenter를 등록할 수 있습니다.

네트워크 설정

구성 탭에서 다음 네트워크 설정을 구성할 수 있습니다.

참고 네트워크 설정을 변경하는 경우 변경 후 바로 무결성 검사를 수동으로 실행합니다. 무결성 검사를 실행하지 못하면 이전 체크포인트로 롤백할 때 VDP 연결 오류가 발생할 수 있습니다. 지침은 **“무결성 검사 실행”**(57페이지) 섹션을 참조하십시오.

- **IPv4 또는 IPv6 정적 주소:** 인터페이스의 인터넷 프로토콜 v4 또는 v6 설정입니다.
- **넷마스크/접두사:** IPv4 또는 IPv6 정적 주소의 네트워크 마스크 또는 접두사입니다.
- **게이트웨이:** IPv4 또는 IPv6 정적 주소의 게이트웨이 주소입니다.
- **운영 DNS:** DNS 확인에 사용되는 운영 도메인 이름 시스템입니다.
- **보조 DNS:** DNS 확인에 사용되는 보조 도메인 이름 시스템입니다.
- **Hostname:** 네트워크에서 컴퓨터를 식별하는 데 사용되는 고유한 이름입니다(예: vdp-primary).
- **도메인:** 웹 사이트를 식별할 수 있는 고유한 이름입니다(예: emc.com). **도메인을 도메인 이름**이라고도 합니다.

vCenter Server 등록

주의 vCenter Server 호스트 이름, vCenter Server 암호, vCenter Server FQDN 또는 IP 주소, vCenter Server 포트 번호 등을 변경하면 VDP 어플라이언스와 연결된 백업 작업, 복제 작업 및 백업 검증 작업이 모두 손실됩니다. 기존 복구 시점은 그대로 유지되지만, 백업 작업과 복제 작업은 재생성해야 합니다.

vCenter Server 등록을 재구성하는 프로세스를 실행하려면 먼저 다음 조건을 모두 충족해야 합니다.

- 다른 재구성 프로세스(예: 암호 또는 네트워크 재구성)가 실행 중이지 않아야 합니다.
- 백업, 복제 또는 복구 작업이 실행 중이지 않아야 합니다.
- 무결성 검사가 실행 중이지 않아야 합니다.
- 모든 서비스가 VDP 어플라이언스에서 실행 중이어야 합니다.

vCenter 등록 자격 증명을 변경하는 경우 변경 후 바로 무결성 검사를 수동으로 실행하십시오. 무결성 검사를 실행하지 못하면 이전 체크포인트로 롤백할 때 VDP 연결 오류가 발생할 수 있습니다. 지침은 **“무결성 검사 실행”**(57페이지) 섹션을 참조하십시오.

어플라이언스 롤백

VDP 어플라이언스가 적합성이 맞지 않거나 불안정한 상태가 될 수 있습니다. 일부 경우 VDP Configure 유틸리티는 적합성이 맞지 않거나 불안정한 상태를 감지하여 로그인 즉시 다음과 유사한 메시지를 표시합니다.

VDP 어플라이언스가 완전하게 종료되지 않은 것으로 보입니다. 데이터 보호 기능을 복구하려면 체크포인트 롤백을 수행해야 할 수 있습니다. 이 프로세스는 '롤백' 탭에서 시작할 수 있습니다.

주의 기본적으로 VDP는 2개의 시스템 체크포인트를 유지합니다. 체크포인트로 롤백하는 경우 체크포인트 이후에 수행된 모든 백업 및 구성 변경 내용은 롤백 완료 후 손실됩니다.

첫 번째 체크포인트는 VDP 설치 시 생성됩니다. 후속 체크포인트는 유지 보수 서비스에 의해 생성됩니다. 이 서비스는 VDP 운영 후 첫 24~48시간 동안 비활성화됩니다. 이 기간 동안 롤백하는 경우 VDP 어플라이언스는 기본 구성으로 설정되고 모든 백업 구성 또는 백업은 유실됩니다.

참고 VMware VDP for Exchange Server Client 또는 VMware VDP for SQL Server Client가 체크포인트와 롤백 사이에 설치된 경우 해당 클라이언트는 다시 설치해야 합니다.

다음 절차에 따라 VDP 어플라이언스를 롤백하십시오.

주의 가장 최근에 검증된 체크포인트로만 롤백하십시오.

사전 요구 사항

VDP 어플라이언스가 설치되어 있어야 하고 VDP 어플라이언스 암호가 필요합니다.

절차

1 웹 브라우저를 열고 다음을 입력합니다.

`https://<IP_address_VDP_Appliance>:8543/vdp-configure/`

2 VDP 사용자 이름과 암호를 사용해서 로그인합니다.

3 **롤백** 탭을 클릭합니다.

4 잠금 아이콘을 클릭하여 VDP 롤백을 활성화합니다.

5 VDP 어플라이언스 암호를 입력하고 **확인**을 클릭합니다.

잠금 아이콘이 잠금 해제된 아이콘으로 바뀝니다.

6 롤백하려는 체크포인트를 클릭합니다.

7 **선택한 체크포인트로 VDP 롤백 수행**을 클릭합니다.

VDP 어플라이언스 롤백의 결과에 대해 설명하는 경고 메시지가 표시됩니다.

8 **예**를 클릭합니다.

롤백이 시작되었음을 알리는 정보 메시지가 표시됩니다.

9 **확인**을 클릭합니다.

VDP 어플라이언스가 롤백을 시도하고 상태 정보를 표시합니다. 또한 롤백의 성공 또는 실패를 알리는 정보 메시지도 표시합니다.

10 **확인**을 클릭합니다.

VDP 어플라이언스가 성공적으로 롤백하지 못한 경우 고객 서비스에 문의하십시오.

긴급 복구

VDP의 여러 핵심 작업은 vCenter Server에 종속됩니다. vCenter Server를 사용할 수 없거나 사용자가 vSphere Web Client를 사용하여 VDP UI에 액세스할 수 없는 경우 직접 연결식 호스트 긴급 복구를 통해 가상 머신을 복구할 수 있습니다.

긴급 복구 작업은 VDP 어플라이언스를 실행하는 VDP 호스트에 직접 가상 머신을 복구합니다. 긴급 복구 탭에는 VDP 어플라이언스에 의해 백업된 가상 머신 목록이 표시됩니다. 이러한 가상 머신은 VDP 어플라이언스가 실행되고 있는 호스트에 새 가상 머신으로 복구할 수 있습니다.

Best Practice 및 권장 사항

긴급 복구 작업을 수행하기 전에 다음 요구 사항을 충족해야 합니다.

- 복구되는 가상 머신에는 VDP 어플라이언스가 실행되고 있는 호스트에서 지원하는 가상 하드웨어 버전이 있어야 합니다.
- 타겟 데이터 저장소에 가용 공간이 충분하여 전체 가상 머신을 수용할 수 있어야 합니다.
- 가상 머신이 복구되는 타겟 VMFS 데이터 저장소에서 VMDK 파일 크기를 지원해야 합니다.
- VDP 어플라이언스가 실행 중인 호스트에서 복구되는 가상 머신에 대한 네트워크 연결을 제공해야 합니다.
- VDP 어플라이언스가 실행되는 호스트에는 관리자 권한이 있는 로컬 계정이 하나 이상 있어야 합니다.

제한 사항 및 지원되지 않는 기능

- 긴급 복구 작업이 수행되는 vSphere 호스트는 vCenter 인벤토리에 속할 수 없습니다. 현재 vCenter Server에서 관리되는 vSphere 호스트는 vCenter Server와의 연결을 임시로 끊어야 긴급 복구를 수행할 수 있습니다. vCenter Server와의 연결을 끊으려면 vSphere Web Client 대신 vSphere 호스트에 직접 연결된 vSphere Client를 사용합니다.
- 긴급 복구를 사용하면 인벤토리에서 호스트 레벨의 루트에만 복구할 수 있습니다.
- 긴급 복구를 사용하려면 VDP에서 사용하는 DNS 서버가 사용 가능해야 하고 타겟 vSphere 호스트 이름을 완전히 확인할 수 있어야 합니다.
- 긴급 복구는 전원이 꺼진 상태에서 가상 머신을 복구합니다. 호스트에 수동으로 로그인하고 복구된 가상 머신의 전원을 켜야 합니다.
- 긴급 복구는 가상 머신을 새 가상 머신으로 복구합니다. 가상 머신에 제공된 이름은 이미 존재하는 가상 머신의 이름과 중복되지 않아야 합니다.
- 긴급 복구는 MSapp 클라이언트를 나열하지 않습니다.
- 긴급 복구 작업을 수행할 때 내부 프록시가 자동으로 활성화됩니다. 내부 및 외부 프록시가 모두 활성화되는 경우에는 VDP Configure 유틸리티에서 내부 프록시를 비활성화해야 긴급 복구가 성공적으로 완료됩니다.

절차

- 1 아직 수행하지 않은 경우, 호스트의 vSphere 클라이언트에 로그인하고 호스트 관리의 **요약** 탭에서 다음 단계를 수행합니다.
 - a **vCenter에서 호스트 연결 해제**를 클릭합니다.
 - b vCenter에서 호스트를 제거하려면 메시지가 표시되었을 때 **예**를 클릭합니다.
- 2 VDP Configure 유틸리티에 로그인합니다.
https://<IP_address_VDP_Appliance>:8543/vdp-configure/
- 3 **긴급 복구** 탭을 클릭합니다.

VDP로 보호되는 가상 머신이 긴급 복구 대화상자에 나열됩니다. 여기서 가상 머신에 대한 다음 세부 정보를 확인할 수 있습니다.

- **이름:** VDP 어플라이언스로 보호되는 가상 머신의 이름입니다. 펼치기 화살표를 클릭하여 선택한 가상 머신의 마지막 복구 날짜와 시간을 확인할 수 있습니다.
 - **마지막으로 알려진 경로:** vCenter 인벤토리 목록에서 마지막으로 알려진 가상 머신의 위치입니다. 이 위치는 가상 머신이 이동하는 경우 업데이트됩니다.
 - **복구 실행 세부 정보:**
 - **Client Name:** 복구되는 가상 머신의 이름입니다.
 - **상태:** 복구의 통과 또는 실패 상태입니다.
 - **시작 시간:** 복구를 시작한 시간입니다.
 - **완료 시간:** 복구를 완료한 시간입니다.
 - **전송된 바이트:** 복구 중에 전송된 바이트 수입니다.
- 4 복구 시점으로 사용할 가상 머신을 선택하고 **복구**를 클릭합니다.
VDP 자격 증명 대화상자가 나타납니다.
- 5 호스트 자격 증명 대화상자에 유효한 호스트 자격 증명을 입력합니다.
- **ESXi 호스트 이름 또는 IP:** vSphere 호스트 이름 또는 vSphere 호스트 IP 주소를 입력합니다.
 - **포트 - 443:** 기본적으로 채워져 있습니다.
 - **Username:** vSphere 호스트 사용자 이름을 입력합니다. 권장되는 호스트 사용자 이름은 "root"입니다. 다른 호스트 사용자 이름의 경우, 사용자 계정에 가상 머신 생성 권한이 있어야 합니다.
 - **암호:** vSphere 호스트 암호를 입력합니다. 잘못된 호스트 자격 증명을 입력한 경우 오류 메시지가 표시되고 호스트에 연결할 수 없습니다.
- 참고** 선택한 가상 머신과 vCenter의 연결이 성공적으로 끊어지지 않은 경우 오류 메시지가 나타나고 계속 진행할 수 없습니다.
- 6 **확인**을 클릭합니다.
백업 복구 화면에서 새 이름과 대상으로 복구가 시작됩니다.
- 7 백업 복구 대화상자에는 다음 정보가 표시됩니다.
- **클라이언트 이름:** 가상 머신이 복구되는 클라이언트의 이름입니다.
 - **백업:** 백업의 날짜 및 타임 스탬프입니다.
 - **새 이름:** 새 이름을 입력해야 하는 필드입니다. 이미 존재하는 가상 머신의 이름을 중복해서 사용할 수 없습니다.
 - **대상:** vSphere 호스트 이름입니다.
 - **데이터 저장소:** 대상 타겟으로 사용할 수 있는 데이터 저장소의 드롭다운 목록입니다.
- 8 **새 이름** 필드에 새 이름을 입력합니다. 이름은 고유해야 하며 최대 255자까지 지정할 수 있습니다. 이름에 ~ !@ \$ ^ % { } [] | , ` ; # \ / : * ? < > ' " & 같은 문자는 사용할 수 없습니다. 또한 â, é, ì, ù, ñ 같은 분음 문자도 사용할 수 없습니다.
- 9 백업할 대상 타겟으로 데이터 저장소를 선택합니다.

주의 데이터 저장소 용량 크기가 나열됩니다. 복구를 수행할 수 있을 정도로 디스크 공간이 충분한 데이터 저장소를 선택해야 합니다. 공간이 부족할 경우 복구에 실패합니다.

10 **복구**를 클릭합니다.

11 최근 작업 대화상자에서 진행률을 확인하여 복구가 성공적으로 제출되었는지 확인합니다.

참고 복구된 가상 머신은 인벤토리에서 vSphere 호스트 레벨에 나열됩니다. 특정 인벤토리 경로로의 복구는 지원되지 않습니다.

자동 호스트 감지

vSphere Data Protection 5.5 및 이전 버전의 경우 사용자가 긴급 복구를 수행하려면 먼저 vSphere 호스트 값을 식별하여, 연결을 끊고, 해당 값을 채워 넣어야 합니다. vSphere Data Protection 5.8 이상 버전에서는 어플라이언스에서 현재 등록된 호스트를 자동으로 감지하고 호스트 자격 증명 대화상자에 호스트 이름 또는 IP 값을 미리 채워 넣습니다. 따라서 클러스터에 호스트가 매우 많은 상황에서 현재 상주하는 호스트를 식별하여 vCenter와의 연결을 끊어야 하는 사용자들의 부담을 덜어 줍니다.

드물지만 다음과 같은 경우에는 어플라이언스가 등록되어 있으며 최근 업데이트된 호스트를 감지하지 못하고 이전 값을 표시합니다.

- vCenter를 사용할 수 없고 VDP 어플라이언스가 HA 지원 클러스터링에 따라 다른 호스트로 마이그레이션된 후에는 어플라이언스가 등록되었던 이전 호스트가 표시됩니다.
- 어플라이언스가 다른 호스트로 마이그레이션된 후에 곧 vCenter를 사용할 수 없게 된 경우. 이 경우 어플라이언스에서 vCenter의 이벤트를 처리 및 업데이트하는 데 일정 시간이 소요되므로 새 호스트를 감지할 수 없습니다.

이러한 두 경우 모두 사용자가 어플라이언스가 등록된 호스트를 직접 확인해야 합니다.

복구 시점 새로 고침

- 1 VDP-Configure URL에 로그인합니다.
`https://<IP_Address_VDP_Appliance>:8543/vdp-configure/`
- 2 긴급 복구 탭을 클릭합니다.
- 3 새로 고침을 클릭합니다.
로드 표시줄이 복구 시점을 새로 고칩니다.

vCenter에 호스트 다시 연결

- 1 vCenter를 복구합니다. 지침은 “복구 작업”(126페이지) 섹션을 참조하십시오.

참고 복구된 vCenter는 기본적으로 전원이 꺼져 있습니다.

- 2 vCenter 복구가 완료되면 vCenter의 전원을 켭니다.
- 3 vCenter URL에 로그인하여 모든 서비스가 실행 중인지 확인합니다.

`https://<IP_address_vCenter>:5480`

Windows 기반 vCenter의 경우 vCenter Server를 실행하는 서버에 관리자로 로그인하고 모든 Windows 서비스가 실행 중인지 확인합니다.

- 4 vSphere 클라이언트를 통해 복구된 vCenter에 로그인합니다.

`https://<IP_address_vCenter>:9443/vsphere-client/`

- 5 vSphere 클라이언트에서 vSphere 호스트를 새로 복구된 vCenter에 추가합니다.

참고 vCenter가 복구된 후, vCenter 서비스가 시작되는 동안 약 20분의 지연이 발생할 수 있습니다. 이 지연 시간 동안에는 백업 또는 복구 작업을 성공적으로 수행할 수 없습니다. 지연이 발생하는 경우 백업 또는 복구를 나중에 시도하십시오.

VDP 와 vCenter 간의 통신 보안

이 장에서 다루는 내용은 다음과 같습니다.

- “VDP 인증서 교체”(46페이지)
- “보안 통신을 위한 VDP 서버 인증”(47페이지)
- “vCenter Server로 VDP 어플라이언스 통신 보안”(48페이지)
- “vCenter Server와의 프록시 통신 보안”(49페이지)

VDP 인증서 교체

포트 8543의 VDP 인증서를 새 자체 서명된 인증서나 CA 서명된 인증서로 교체할 수 있습니다.

다음 단계에 따라 VDP 인증서를 교체하십시오.

- 1 다음 명령을 실행하여 서비스를 중지합니다.

```
root@vdp#: emwebapp.sh --stop
```

- 2 다음 명령을 실행하여 **tomcat** 별칭을 삭제합니다.

```
root@vdp#: /usr/java/latest/bin/keytool -delete -alias tomcat
```

- 3 다음 명령을 실행하여 SSL 인증서를 생성합니다.

```
root@vdp#: /usr/java/latest/bin/keytool -genkeypair -v -alias tomcat -keyalg
RSA -sigalg SHA256withRSA -keystore /root/.keystore -storepass changeit
-keypass changeit -validity 3650 -dname "CN=vdp.vmware, OU=VDP, O=OrgName,
L=PUNE, S=MH, C=IN"
```

- 4 자체 서명된 인증서를 사용하려면 6단계로 이동합니다.

- 5 CA 서명된 인증서를 사용하려면 다음과 같이 합니다.

- a 다음 명령을 실행하여 CSR(Certificate Signing Request)을 생성합니다.

```
root@vdp#: /usr/java/latest/bin/keytool -certreq -keyalg RSA -alias tomcat
-file csrFileName.csr
```

- b CSR 콘텐츠를 사용하여 CA 서명된 인증서를 **.p7b** 형식으로 가져오고 인증서를 저장합니다.

- c 다음 명령을 실행하여 .p7b 체인 인증서 파일을 가져옵니다.

```
root@vdp#: /usr/java/latest/bin/keytool -import -alias tomcat -keystore
/root/.keystore -file /<Path_to_the_Certificate>/<chainCertFileName.p7b>
```

- 6 다음 명령을 실행하여 **tomcat** 별칭이 있는 인증서 항목이 키 저장소에 존재하는지 확인합니다.

```
root@vdp#: /usr/java/latest/bin/keytool -list -v -keystore /root/.keystore
-storepass changeit -keypass changeit
```

- 7 인증서 항목이 키 저장소에 존재하면 **addFingerprint.sh** 스크립트를 실행합니다.

```
root@vdp#: ./usr/local/avamar/bin/addFingerprint.sh
```

- 8 다음 명령을 실행하여 서비스를 시작합니다.

```
root@vdp#: emwebapp.sh --start
```

보안 통신을 위한 VDP 서버 인증

VDP 서버와 통신하는 동안 MITM(Man-in-the-Middle) 공격을 방지하고 인증서가 제공하는 보안을 최대한 활용하기 위해 VDP는 콘솔에 지문을 제공합니다. 다음 그림에 샘플 지문이 나와 있습니다.

```

*****
Welcome to the vSphere Data Protection 6.1 appliance. Version: 6.1.0.108

Quickstart Guide: (How to get VDP running quickly)

1 - Open a browser to: https://[redacted]8543/vdp-configure
2 - Review the Network Settings
3 - Enter the Time Zone
4 - Enter the VDP credentials
5 - Enter the vCenter Registration information
6 - Click Test Connection
7 - Click Finish

*****
SSL thumbprint for UDP server:
SHA256 Fingerprint=4C:4A:41:89:A0:44:4A:2C:90:B1:3B:8D:E7:EA:35:80:15:AD:27:34:4
2:8B:9D:79:45:26:CC:E5:BE:14:6A:87
SHA1 Fingerprint=60:A8:6D:DB:9A:C7:6A:66:70:E5:97:D7:BE:EA:A8:28:4C:1F:4C:C7

*Login
Set Timezone (Current:IST)

Use Arrow Keys to navigate
and <ENTER> to select your choice.

```

<https://<vdp-ip>:8543/vdp-configure> URL을 사용하여 VDP 서버에 액세스할 때 SSL 인증서가 같은 VDP 서버에서 가져온 것인지 그리고 유효한지를 확인하십시오. SSL 인증서가 유효한지를 확인하려면 콘솔에 있는 지문과 SSL 핸드셰이크 중에 브라우저가 받은 SSL 인증서가 일치하는지 여부를 확인하십시오. VDP에는 기본 SSL 인증서가 있습니다.

기본 인증서를 변경하려면 keytool에 있는 새 인증서를 키 저장소에 **privatekeyentry**로 가져오십시오.

새 인증서를 가져온 후에 VDP 콘솔에서 업데이트된 지문을 확인하려면 다음 단계를 수행하십시오.

- 1 다음 명령을 실행하여 서비스를 중지합니다.
emwebapp.sh --stop
- 2 addFingerprint.sh 스크립트를 실행합니다.
./usr/local/avamar/bin/addFingerprint.sh
- 3 다음 명령을 실행하여 서비스를 시작합니다.
emwebapp.sh -start
- 4 VDP 어플라이언스를 다시 시작합니다.

vCenter Server로 VDP 어플라이언스 통신 보안

VDP 어플라이언스는 여러 가지 목적을 위해 SSL 인증서 확인을 거치거나 확인 없이도 vCenter 서버에 HTTPS 연결을 설정할 수 있습니다. SSL 인증서를 확인하지 못하면 vCenter Server와 VDP 어플라이언스가 MITM(Man-in-the-Middle) 공격을 받기 쉽습니다. VDP는 이제 vCenter 서버에 등록하는 중에 vCenter 서버 인증서를 업로드하거나 VDP 인증서 저장소에서 인증서를 서명하는 것을 지원합니다. 이후 인증서는 vCenter 서버와의 테스트 연결을 비롯한 모든 후속 HTTPS 연결에서 vCenter 서버를 인증하고 신뢰함으로써 VDP 어플라이언스를 보호하는 데 사용됩니다.

사전 요구 사항

다음 URL을 사용하여 vCenter 인증서를 **.p7b**, **.cer** 또는 **.crt** 형식으로 다운로드합니다.

https://<vCenter_IP_address>/sdk

절차

■ 초기 구성의 경우:

- a 다음 URL을 사용하여 초기 구성 마법사를 엽니다.

https:<IP_address_VDP_appliance>:8543/vdp-configure/

- b **vCenter** 등록 페이지에서 다음을 수행합니다.

- i 로그인 자격 증명, 호스트 이름 또는 IP 주소, 포트 번호 같은 vCenter 정보를 해당 필드에 지정합니다.

- ii **vCenter** 인증서 확인을 선택합니다.

VDP 어플리케이션 통신을 vCenter로 보안하지 않으려면 **vCenter** 인증서 확인을 선택 취소합니다. 이 옵션을 선택 취소하면 vCenter 인증서를 확인하지 않습니다.

- iii **업로드**를 클릭하고 다운로드한 vCenter 인증서를 선택합니다.

- iv **연결 테스트**를 클릭합니다.

vCenter 인증서가 유효하면 vCenter와 연결됩니다. 아니면 연결이 실패합니다.

■ vCenter를 다시 등록하는 경우:

- a 다음 URL을 사용하여 VDP 구성 유틸리티에 로그인합니다.

https:<IP_address_VDP_appliance>:8543/vdp-configure/

- b 구성 탭에서 설정 아이콘을 클릭하고 **vCenter** 등록을 선택합니다.

vCenter 등록 마법사가 나타납니다.

- c **vCenter** 등록 페이지에서 **내용을 확인했습니다. vCenter를 다시 구성하겠습니다.**를 선택하고 다음을 클릭합니다.

- d **vCenter** 구성 페이지에서 다음을 수행합니다.

- i 로그인 자격 증명, 호스트 이름 또는 IP 주소, 포트 번호 같은 vCenter 정보를 해당 필드에 지정합니다.

- ii **vCenter** 인증서 확인을 선택합니다.

- iii **업로드**를 클릭하고 다운로드한 vCenter 인증서를 선택합니다.

- iv 다음을 클릭합니다.

- e **완료 준비** 페이지에서 정보를 검토하고 **마침**을 클릭합니다.

vCenter 인증서 및 기타 정보가 유효하면 vCenter와 연결됩니다. 아니면 재등록이 실패합니다.

vCenter Server와의 프록시 통신 보안

기본적으로 VDP 서버 관리 서비스 및 프록시는 vCenter Server에 연결할 때 SSL 인증서를 검증하지 않습니다. 이로 인해 vCenter Server가 MITM(Man-in-the-Middle) 악용에 취약해질 수 있으므로, vCenter Server에 대한 무단 액세스가 발생할 수 있습니다. 각 프록시가 vCenter Server에 연결할 때 SSL 인증서 인증을 사용하도록 구성하면 이 취약성이 해소됩니다.

사전 요구 사항

vCenter Server에 CA(Certificate Authority)에서 서명한 SSL 인증서가 설치되어 있는지 확인합니다.

<http://kb.vmware.com/kb/2034833>에서 CA 서명된 SSL 인증서를 생성하고 vCenter Server에 설치하는 방법과 vSphere 5.1 또는 5.5 환경에 CS 서명된 인증서를 구축하는 방법에 대한 정보를 제공합니다.

<http://kb.vmware.com/kb/2111219>에서는 vSphere 6.0 환경에서 기본 인증서를 CA 서명된 SSL 인증서로 교체하는 방법에 대한 정보를 제공합니다.

절차

- 1 명령 셸을 열고 프록시에 root로 로그인합니다.
- 2 vCenter Server 인증서를 프록시의 `/usr/local/avamarclient/bin`에 복사합니다.

■ Linux vCenter인 경우:

- vCenter 5.x:
 - 서버 인증서: `/etc/vmware-vpx/ssl/ruicert.crt`
 - 루트 인증서: `/etc/vmware-vpx/ssl/ruica-cert.pem`
- vCenter 6.0:
 - 서버 인증서: `/etc/vmware-vpx/ssl/ruicert.crt`
 - 루트 인증서: `/var/lib/vmware/vmca/root.cer`

SCP를 통해 vCenter의 해당 인증서를 프록시의 `/usr/local/avamarclient/bin`에 복사합니다.

자체 서명된 인증서의 경우 서버 인증서만 사용합니다.

CA 서명된 인증서의 경우 다음 명령을 실행하여 체인 인증서를 생성합니다.

```
cat ruicert root.cer > chain_cert.pem
```

■ Windows vCenter의 경우:

- vCenter 5.x:
 - 서버 인증서: `C:\ProgramData\VMware\VMware VirtualCenter\SSL\ruicert.crt`
 - 루트 인증서: `C:\ProgramData\VMware\VMware VirtualCenter\SSL\cacert.pem`
- vCenter 6.0:
 - 서버 인증서:
 - `C:\ProgramData\VMware\vCenterServer\cfg\vmware-vpx\ssl\ruicert.crt`
 - 루트 인증서: `C:\ProgramData\VMware\vCenterServer\data\vmca\root.cer`

SCP를 통해 vCenter의 해당 인증서를 프록시의 `/usr/local/avamarclient/bin`에 복사합니다.

자체 서명된 인증서의 경우 서버 인증서만 사용합니다.

CA 서명된 인증서의 경우 다음 명령을 실행하여 체인 인증서를 생성합니다.

```
cat ruicert root.cer > chain_cert.pem
```

참고 체인 SSL 인증서가 vCenter에 사용되는 경우 체인의 모든 인증서가 포함된 **chain.pem** 파일을 프록시의 `/usr/local/avamarclient/bin`으로 복사합니다.

- 3 다음을 입력하여 인증서에 대한 운영 체제 권한을 적절히 설정합니다.

```
chmod 600 /usr/local/avamarclient/bin/<certificate_file>
```

여기서 *certificate_file*은 서버 인증서 또는 체인 인증서입니다.

- 4 UNIX 텍스트 편집기에서 `/usr/local/avamarclient/var/avvcbimageAll.cmd`를 엽니다.

- 5 파일 끝에 다음 내용을 추가합니다.

```
--ssl_server_authentication_file=/usr/local/avamarclient/bin/<certificate_file>
```

여기서 *certificate_file*은 서버 인증서 또는 체인 인증서입니다.

참고 체인 vCenter SSL 인증서의 경우 **chain.pem**을 사용합니다.

- 6 변경 내용을 저장하고 `avvcbimageAll.cmd`를 닫습니다.

- 7 UNIX 텍스트 편집기에서 `/usr/local/avamarclient/var/avvmwfileAll.cmd`를 엽니다.

- 8 파일 끝에 다음 내용을 추가합니다.

```
--ssl_server_authentication_file=/usr/local/avamarclient/bin/<certificate_file>
```

여기서 *certificate_file*은 서버 인증서 또는 체인 인증서입니다.

참고 체인 vCenter SSL 인증서의 경우 **chain.pem**을 사용합니다.

- 9 변경 내용을 저장하고 `avvmwfileAll.cmd`를 닫습니다.

- 10 UNIX 텍스트 편집기에서 `/etc/vmware/config`를 엽니다.

- 11 파일 끝에 다음 내용을 추가합니다.

```
vix.enableSslCertificateCheck = "true"
```

```
vix.sslCertificateFile = "/usr/local/avamarclient/bin/<certificate_file>"
```

여기서 *certificate_file*은 서버 인증서 또는 체인 인증서입니다.

- 12 변경 내용을 저장하고 `/etc/vmware/config`를 닫습니다.

- 13 UNIX 텍스트 편집기에서 `/usr/local/avamarclient/var/vddkconfig.ini`를 엽니다.

- 14 **vixDiskLib.linuxSSL.verifyCertificates**의 값을 0에서 1로 변경합니다.

- 15 변경 내용을 저장하고 `vddkconfig.ini`를 닫습니다.

- 16 프록시에서 백업 또는 복구 작업이 실행 중이지 않은지 확인합니다.

- 17 다음 명령을 실행하여 `avagent` 및 `vmwareflr` 서비스를 다시 시작합니다.

```
service avagent-vmware restart
```

```
service vmwareflr restart
```

결과

프록시는 vCenter Server에 연결할 때 SSL 인증서를 사용 및 검증합니다.

vCenter 환경에 구축하는 각 프록시에 대해 이 절차를 반복합니다.

VDP 구성

이 장에서 다루는 내용은 다음과 같습니다.

- [“로그인 보안”](#)(52페이지)
- [“사용자 환경 개선 프로그램 구성”](#)(52페이지)
- [“구성 및 모니터링”](#)(53페이지)
- [“VDP 작업 모니터링”](#)(58페이지)
- [“VDP 종료 및 시작 절차”](#)(60페이지)

로그인 보안

VDP configuration 유틸리티의 보안 향상을 위해 사용자 로그인 시도가 다섯 번 실패하면 VDP configuration 유틸리티가 5분 동안 잠깁니다. 이 시간 동안에는 로그인을 시도할 수 없습니다. 이미 로그인되어 있는 기존 세션은 영향을 받지 않습니다.

잠긴 경우:

- 로그인을 시도하는 동안 VDP 구성 유틸리티에 사용자에게 대한 안내 메시지가 표시됩니다.
- 잠금에 대한 vCenter 이벤트가 생성됩니다.
- `vdp-configure.log`에 잠금을 초래한 로그인 시도 실패 시간, 해당 사용자, 소스 주소 및 요청 헤더가 캡처됩니다.

`vdp-configure.log` 파일을 확인하려면 터미널 또는 콘솔 관리자와 기본 암호를 사용하여 VDP 어플라이언스에 로그인합니다.

사용자 환경 개선 프로그램 구성

사용자 환경 개선 프로그램은 VDP 환경에 대한 암호화된 구성 및 사용 정보를 분석하기 위해 VMware 서버로 보낼 수 있게 해 주는 옵션입니다.

참고 사용자 환경 개선 프로그램(PhoneHome)은 IPv6 전용 vSphere Data Protection 환경에서는 지원되지 않습니다.

VDP는 VMware로 다음 유형의 데이터를 보냅니다.

- VDP 및 vSphere의 버전 정보
- VDP 표준 시간대 및 가동 시간
- 보호되는 VM 및 보호되지 않는 VM 수
- 구성된 용량
- Data Domain 사용 여부(예/아니오)
- 용량 사용률
- 구성되고 등록된 내부 및 외부 프록시 수
- 사용자가 구성한 프록시당 작업 지시 수
- 유지 보수 및 관리 상태
- 유효한 최신 체크포인트 날짜
- 사용 중인 에이전트(SQL Server, Exchange, Exchange GLR/DAG 및 SharePoint)
- 마지막 무결성 체크포인트 상태
- VDP 상태
- 타임 스탬프와 오류 코드를 포함한 작업 실패에 대한 세부 정보
- 각 오류 코드별 실패한 작업 수

VDP 설치 중 VDP Configuration 유틸리티의 제품 개선 페이지에서 사용자 환경 개선 프로그램을 활성화할 수 있습니다. 제품 개선 페이지에는 **사용자 환경 개선 프로그램 사용** 확인란이 있습니다. 기본적으로 이 확인란은 선택되어 있지 않습니다.

설치 후 언제든지 웹 브라우저에서 VDP Configure 유틸리티에 액세스하여 사용자 환경 개선 프로그램을 사용하거나 사용하지 않도록 설정할 수 있습니다.

사전 요구 사항

방화벽으로 보호되는 네트워크에서 사용자 환경 개선 프로그램이 VMware 서버로 데이터를 업로드할 때 연결 문제가 발생하지 않도록 네트워크를 수정해야 하는 경우가 있습니다. 사용자 환경 개선 프로그램이 VMware 서버로 데이터를 업로드하는 데 방화벽이 방해가 되지 않도록 하려면 다음 VMware 서버에 대한 네트워크를 여십시오.

- <https://vcsa.vmware.com:443>
- <https://phtransfer.vmware.com:443>

절차

- 1 웹 브라우저를 열고 다음을 입력합니다.
`https://<IP_address_VDP_appliance>:8543/vdp-configure/`
- 2 VDP 사용자 이름과 암호를 사용해서 로그인합니다.
- 3 구성 탭에서  아이콘을 클릭하고 **제품 개선**을 선택합니다.
제품 개선 페이지가 나타납니다.
- 4 **사용자 환경 개선 프로그램 사용** 확인란을 선택하거나 선택 취소하여 사용자 환경 개선 프로그램을 사용하거나 사용하지 않도록 설정합니다.

구성 및 모니터링

vSphere Web Client에서 어플라이언스 및 스토리지 관련 정보 외에 백업 기간 구성 세부 정보를 확인 및 수정할 수 있습니다. 예약된 일정에 따라 e-메일 보고서를 보내도록 VDP 어플라이언스를 구성할 수도 있습니다.

백업 어플라이언스 구성 보기

백업 어플라이언스 정보는 백업 어플라이언스 세부 정보, 스토리지 요약 정보 및 백업 기간 구성에 대한 정보를 제공합니다. 백업 어플라이언스 정보에는 다음이 포함됩니다.

- 표시 이름
- 제품 이름
- IP 주소
- 주 버전(VDP 버전 번호)
- 부 버전(기술 지원부에서 사용함)
- 상태
- 호스트
- vCenter Server
- VDP 백업 사용자
- VDP 어플라이언스 시간
- 시간대

이러한 옵션은 VDP 어플라이언스 설치 중 구성되며 VDP Configure 유틸리티를 통해 편집할 수 있습니다. [“VDP 어플라이언스의 설치 후 구성”](#)(35페이지)에서 자세한 내용을 확인하십시오.

VDP 어플라이언스 스토리지 요약에는 다음이 포함됩니다.

- **용량:** VDP 어플라이언스의 총 용량입니다.
- **가용 공간:** 백업에 사용할 수 있는 공간의 크기입니다.
- **중복 제거된 크기:** 중복이 제거된 형식으로 백업이 차지하는 디스크 공간입니다.
- **중복 제거되지 않은 크기:** 중복이 제거되지 않은 원래 형식으로 전환될 경우 백업이 차지하는 디스크 공간입니다.

참고 페이지에서 데이터를 새로 고치려면 **스토리지 요약** 옆에 있는 새로 고침 아이콘을 클릭합니다.

왼쪽에는 VDP 용량 확인을 위한 색상 컨테이너가 표시됩니다.

- 사용된 스토리지 용량이 80% 미만이면 컨테이너가 녹색입니다.
- 사용된 스토리지 용량이 80%에서 90% 사이이면 컨테이너가 노란색입니다. 다음과 같은 메시지가 나타납니다.

VDP 스토리지가 거의 가득 찼습니다.

- 사용된 스토리지 용량이 95%에서 100% 사이이면 컨테이너가 빨간색입니다. 다음과 같은 메시지가 나타납니다.

VDP 스토리지가 거의 가득 찼습니다.

- 사용된 스토리지 용량이 100%이면 컨테이너가 빨간색입니다. 다음과 같은 메시지가 나타납니다.

VDP 스토리지가 가득 찼습니다.

참고 Data Domain 시스템이 VDP 구성에 추가되어 있으면 Data Domain 스토리지 요약 정보도 나타납니다.

그림 6-3에는 백업 기간 구성이 표시되어 있습니다.

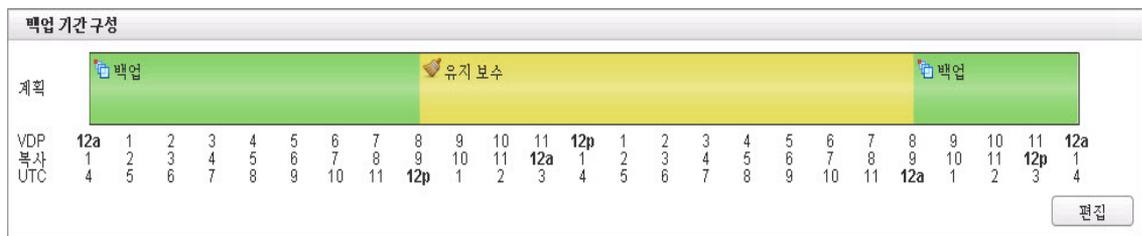


그림 6-3. 백업 기간 구성

하루 24시간은 다음 두 개의 운영 기간으로 나뉩니다.

- **백업 윈도우:** 하루 중 정상적인 예약 백업을 수행하기 위해 예약된 시간입니다.
- **유지 보수 윈도우:** 하루 중 무결성 검사와 같은 일상적인 VDP 유지 보수 작업을 수행하기 위해 예약된 시간입니다. VDP가 유지 보수 모드에 있는 동안에는 백업을 예약하거나 "지금 백업" 작업을 수행하지 마십시오. 백업 작업은 실행되지만 VDP의 유지 보수 작업에 필요한 리소스가 백업 작업에 소모됩니다.

유지 보수 기간이 시작되었을 때 실행 중이거나 유지 보수 기간 동안 실행된 작업은 계속 실행됩니다.

참고 블랙아웃 기간이 제거되었으므로 무결성 검사 및 가비지 수집과 같은 작업이 유지 보수 기간 동안 중단 없이 실행됩니다.

백업 기간 편집

백업 요청을 처리할 수 있는 기간을 변경할 수 있습니다.

사전 요구 사항

- VDP가 설치 및 구성되어 있어야 합니다.
- vSphere Web Client에 로그인하고 VDP 어플라이언스에 연결합니다.

절차

- 1 VDP 어플라이언스에 접속합니다. 자세한 내용은 “VDP 액세스”(104페이지)을 참조하십시오.
- 2 VDP UI에서 구성 탭을 선택합니다(기본적으로 백업 어플라이언스 보기가 표시됨).
- 3 백업 어플라이언스 보기의 오른쪽 하단에서 편집 버튼을 클릭합니다.

그림 6-4에 나온 것처럼 백업 시작 시간 옵션과 기간 옵션이 표시됩니다.

백업 기간구성

계획: 백업 유지 보수 백업

VDP 복사	12a	1	2	3	4	5	6	7	8	9	10	11	12a	1	2	3	4	5	6	7	8	9	10	11	12a	1
UTC	4	5	6	7	8	9	10	11	12p	1	2	3	4	5	6	7	8	9	10	11	12a	1	2	3	4	5

백업 시작 시간: 오후 8:00

백업 기간: 12 시간

저장 취소

그림 6-4. 편집 모드의 백업 기간 구성

- 4 드롭다운 화살표를 사용하여 백업 기간의 시작 시간을 선택합니다.
 - 5 백업 기간을 입력합니다. 최소 백업 기간은 4시간이고 최대 백업 기간은 16시간입니다.
 - 6 **저장**을 클릭합니다.
- 설정이 성공적으로 저장되었음을 알리는 대화상자가 나타납니다.
- 7 **확인**을 클릭합니다.

VDP가 백업 기간 구성을 변경합니다.

e-메일 알림 및 보고서 구성

SMTP e-메일 보고서를 지정된 수신자에게 전송하도록 VDP를 구성할 수 있습니다. e-메일 보고서를 설정한 경우 다음과 같은 정보가 포함된 e-메일 메시지가 전송됩니다.

- 주의가 필요한 항목
- VDP 어플라이언스 상태
- 백업 작업 요약
- 가상 머신 요약
- 복제 요약
- 보호되지 않는 가상 머신

참고 VDP e-메일 알림 및 보고서는 참조(CC), 숨은 참조(BCC) 및 SSL 인증서를 지원하지 않습니다.

사전 요구 사항

- VDP가 설치 및 구성되어 있어야 합니다.
- vSphere Web Client에 로그인하고 VDP 어플라이언스에 연결합니다.
- e-메일 알림 및 보고서에 대한 e-메일 계정이 있어야 합니다.

절차

- 1 VDP 어플라이언스에 접속합니다. 자세한 내용은 **"VDP 액세스"**(104페이지)을 참조하십시오.
- 2 VDP 사용자 인터페이스에서 **구성** 탭을 선택합니다.
- 3 **e-메일**을 선택하고 **편집**을 클릭합니다.
- 4 다음 필드에 정보를 지정합니다.
 - **e-메일 보고서 활성화:** e-메일 보고서를 활성화하려면 이 옵션을 선택합니다.
 - **보내는 메일 서버:** e-메일을 보낼 때 사용할 SMTP 서버 이름을 입력합니다. 이 이름은 IP 주소, 호스트 이름 또는 정규화된 도메인 이름으로 입력할 수 있습니다. VDP 어플라이언스에서 입력된 이름을 확인할 수 있어야 합니다.

비인증 e-메일 서버에 대한 기본 포트는 25이고, 인증 e-메일 서버에 대한 기본 포트는 587입니다. 서버 이름에 콜론(:)과 포트 번호를 추가하여 다른 포트를 지정할 수 있습니다. 예를 들어, "emailserver" 서버에서 포트 8025를 사용하도록 지정하려면 emailserver:8025를 입력하십시오.
 - (옵션) **서버 연결 시 로그인 필요:** SMTP 서버에서 인증을 요구할 경우 이 옵션을 선택합니다.
 - **Username:** 인증할 사용자 이름을 입력합니다.
 - **암호:** 사용자 이름과 연결된 암호를 입력합니다.

VDP는 암호를 검증하지 않습니다. 사용자가 입력한 암호는 e-메일 서버로 직접 전달됩니다.
 - **보낸 사람 주소:** e-메일 보고서를 보내는 발신 e-메일 주소를 입력합니다. 이 주소는 하나만 입력할 수 있습니다.
 - **받는 사람 주소:** e-메일 주소를 심표로 구분하여 최대 10개까지 입력합니다.
 - **전송 시간:** 드롭다운 목록에서 VDP가 보고서를 e-메일로 전송할 시간을 선택합니다.
 - **전송 일:** 보고서를 전송할 요일을 선택합니다.
 - **보고서 로캘:** e-메일 보고서에 사용할 국가를 선택합니다.
 - **CSV 첨부 파일 사용:** CSV 형식의 첨부 파일로 e-메일 보고서를 받으려면 이 옵션을 선택합니다.
 - **VDP 경고 e-메일 알림 설정:** VDP 경고 e-메일 알림을 사용하려면 이 옵션을 선택합니다. 이 옵션을 선택할 경우, VDP 알림이 트리거되거나 계시된 이벤트가 VDP 알림 상태를 노란색에서 빨간색으로 변경할 때 VDP가 e-메일 알림을 전송합니다.
- 5 **저장** 버튼을 클릭합니다.
- 6 e-메일 구성을 테스트하려면 **테스트 e-메일 보내기**를 클릭하십시오.

사용자 인터페이스 로그 보기

구성 탭에서 로그를 클릭하면 VDP에 대한 사용자 인터페이스 로그가 표시됩니다. 이는 사용자 인터페이스로 시작된 활동을 세부적으로 기술하며 몇 가지 주요 상태 항목을 식별하는 개괄적인 로그입니다.

화면에 표시된 세부 정보를 브라우저가 실행 중인 시스템에 파일로 저장하려면 **보기 내보내기**를 클릭합니다.

자세한 로그는 VDP 구성 유틸리티를 사용하여 다운로드할 수 있습니다. 지침은 [“VDP 로그 또는 진단 정보 수집”](#)(38페이지) 섹션을 참조하십시오.

무결성 검사 실행

무결성 검사는 중복 제거 저장소에서 데이터 무결성을 확인 및 유지 관리합니다. 무결성 검사의 결과는 체크포인트입니다. 기본적으로 VDP에서는 유지 보수 기간 동안 무결성 검사를 매일 실행합니다. 또한 무결성 검사를 수동으로 시작할 수도 있습니다.

주의 VDP 어플라이언스에 마지막으로 유효한 무결성 검사가 실패했거나 기간이 지났다는 알림이 표시될 경우 수동 무결성 검사를 실행하십시오. 무결성 검사 기간이 지났는데도 VDP 어플라이언스에서 계속 백업하도록 허용하는 경우 마지막으로 검증된 체크포인트로의 롤백이 필요하면 잠재적인 백업 데이터 손실 위험이 있습니다.

VDP Configure 유틸리티의 **롤백** 탭을 통해 VDP 체크포인트의 모든 목록을 볼 수 있습니다. 자세한 내용은 [“어플라이언스 롤백”](#)(41페이지) 섹션을 참조하십시오.

사전 요구 사항

- VDP가 설치 및 구성되어 있어야 합니다.
- vSphere Web Client에 로그인하고 VDP 어플라이언스에 연결합니다.

절차

- 1 VDP 어플라이언스에 접속합니다. 자세한 내용은 [“VDP 액세스”](#)(104페이지)을 참조하십시오.
- 2 VDP UI의 구성 탭에서  아이콘을 클릭하고 **무결성 검사 실행**을 선택합니다.
수동 무결성 검사를 수행할지 여부를 확인하는 화면이 나타납니다.
- 3 **예**를 클릭합니다.
무결성 검사가 시작되었음을 알리는 메시지가 나타납니다.
- 4 **확인**을 클릭합니다.
VDP가 무결성 검사를 시작합니다.
- 5 최근 작업을 통해 무결성 검사 진행률을 모니터링합니다.

참고 VDP 무결성 검사가 실행 중일 때 유지 보수 서비스가 중지됩니다. 이로 인해 일시적인 VDP 오류가 발생할 수 있습니다. 무결성 검사가 완료될 때까지 기다리면 유지 보수 서비스가 자동으로 재시작되고 VDP 오류 메시지가 해결됩니다.

VDP 작업 모니터링

다음 방법 중 하나를 사용하여 VDP 어플라이언스의 작업을 모니터링할 수 있습니다.

- [“최근 작업 보기”](#)(58페이지) 참조).
- [“경보 보기”](#)(59페이지)
- [“이벤트 콘솔 보기”](#)(60페이지)

VDP에 의해 생성된 작업, 이벤트 및 경보는 "VDP:"가 앞에 붙습니다. 그러나 VDP 프로세스의 일부로 발생하는 일부 작업 및 이벤트는 vCenter Server에 의해 수행되므로 이 접두사로 시작되지 않습니다.

예를 들어, VDP가 실행 중인 가상 머신에 대해 예약된 백업 작업을 실행할 경우 다음과 같은 작업 항목이 생성됩니다.

- 1 가상 머신 스냅샷 생성(백업할 가상 머신에서 vCenter 작동)
- 2 VDP: 예약된 백업 작업(VDP가 백업 작업 시작)
- 3 가상 머신 재구성(VDP 어플라이언스가 가상 센터에서 서비스 요청)
- 4 스냅샷 제거(백업을 완료한 가상 머신에서 가상 센터 작동)

VDP에 의해 생성된 작업 또는 이벤트만 작업 또는 이벤트 콘솔에 표시하려면 "VDP:"를 **필터 필드**에 입력하십시오.

최근 작업 보기

VDP는 다음 작업을 수행할 때 최근 작업 창에 작업 항목을 생성합니다.

- 백업
- 자동 백업 검증
- 복구
- 복제
- 복제 복구
- VDP-Configuration
- 무결성 검사

최근 작업 창에서 작업 항목을 클릭하면 화면 하단에 있는 창에 작업 세부 정보가 표시됩니다. 작업 세부 정보는 **최근 작업** 아래 **실행 중** 탭의 가상 머신 아이콘 옆에 있는 링크를 클릭하여 표시할 수도 있습니다.

또한 **실행 중** 작업 창에서도 취소 작업 아이콘을 클릭하여 작업을 취소할 수 있습니다.

경보 보기

표 6-10에는 VDP(vSphere Data Protection) 어플라이언스가 트리거할 수 있는 알림이 나와 있습니다.

표 6-10. vSphere Data Protection 경보

경보 이름	경보 설명
VDP: [001] VDP 어플라이언스에 대한 가장 최근의 체크포인트가 기간이 지났습니다.	VDP 사용자 인터페이스의 구성 탭에서 모든 작업 아이콘을 클릭한 다음 "무결성 검사 실행"을 선택합니다.
VDP: [002] VDP 어플라이언스가 거의 꽉 찼습니다.	VDP 어플라이언스에 추가 백업 공간이 거의 없습니다. 불필요하거나 오래된 백업을 수동으로 삭제하는 방법과 백업 작업의 보존 정책을 변경해 백업 보존 기간을 줄이는 방법으로 어플라이언스의 공간을 확보할 수 있습니다.
VDP: [003] VDP 어플라이언스가 꽉 찼습니다.	VDP 스토리지가 가득 찼습니다. 추가 공간이 확보될 때까지 어플라이언스는 읽기 전용 모드로 실행됩니다. 불필요하거나 오래된 백업을 삭제하는 방법으로 공간을 확보할 수 있습니다.
VDP: [004] VDP 어플라이언스 데이터 저장소가 최대 용량에 근접하고 있습니다.	VDP 어플라이언스가 디스크를 프로비저닝한 데이터 저장소가 최대 용량에 근접하고 있습니다. 데이터 저장소의 최대 용량에 도달하면 VDP 어플라이언스가 일시 중단됩니다. 데이터 저장소에 추가 공간이 확보될 때까지 어플라이언스를 재개할 수 없습니다.
VDP: [005] 핵심 서비스가 실행되고 있지 않습니다.	VDP Configure 유틸리티를 사용하여 핵심 서비스를 시작합니다.
VDP: [006] 관리 서비스가 실행되고 있지 않습니다.	VDP Configure 유틸리티를 사용하여 관리 서비스를 시작합니다.
VDP: [007] 파일 시스템 서비스가 실행되고 있지 않습니다(VDP 버전 5.5 이하에서 지원됨).	VDP Configure 유틸리티를 사용하여 파일 시스템 서비스를 시작합니다. 참고: 이 경보는 VDP 버전 5.8 이상에서는 지원되지 않습니다.
VDP: [008] 파일 레벨 복구 서비스가 실행되고 있지 않습니다.	VDP Configure 유틸리티를 사용하여 파일 레벨 복구 서비스를 시작하십시오.
VDP: [009] 유지 보수 서비스가 실행되고 있지 않습니다.	VDP Configure 유틸리티를 사용하여 유지 보수 서비스를 시작하십시오.
VDP: [010] 백업 스케줄러가 실행되고 있지 않습니다.	VDP Configure 유틸리티를 사용하여 백업 스케줄러를 시작하십시오.
VDP: [013] 보호된 가상 머신 제한이 초과되었습니다.	지원되는 보호된 가상 머신 수를 초과했습니다.
VDP: [014] 백업 복구 서비스가 실행되고 있지 않습니다.	VDP Configure 유틸리티를 사용하여 백업 복구 서비스를 시작하십시오.
VDP: [015] 복제 서비스가 실행되고 있지 않습니다.	VDP Configure 유틸리티를 사용하여 복제 서비스를 시작합니다.
VDP:[016] Data Domain 스토리지가 거의 가득 찼습니다.	Data Domain 스토리지가 거의 가득 찼습니다. 불필요하거나 오래된 백업을 수동으로 삭제하는 방법과 백업 작업의 보존 정책을 변경해 백업 보존 기간을 줄이는 방법으로 Data Domain 스토리지의 공간을 확보할 수 있습니다.
VDP:[017] Data Domain 스토리지가 가득 찼습니다.	Data Domain 스토리지가 가득 찼습니다. 불필요하거나 오래된 백업을 수동으로 삭제하는 방법으로 공간을 확보할 수 있습니다.

이벤트 콘솔 보기

VDP는 다음 이벤트 유형을 생성할 수 있습니다. 정보, 오류, 경고. 다음은 이벤트 유형에 대한 예입니다.

- **Info:** “VDP: 중요한 가상 머신 백업 작업이 생성되었습니다.”
- **경고:** “VDP: Host123 클라이언트를 중요한 가상 머신 백업 작업에 추가할 수 없습니다...”
- **오류:** “VDP: 어플라이언스가 모든 권한에서 읽기 전용으로 변경되었습니다.”

VDP는 어플라이언스에서 발생한 모든 변경 사항에 대해 이벤트를 생성합니다. 일반적으로 어플라이언스의 기능이 저하되는 상태 변경은 오류 레이블이 표시되고 기능이 향상되는 상태 변경은 정보 레이블이 표시됩니다. 예를 들어, 무결성 검사를 시작할 때 VDP는 무결성 검사를 수행하기 전에 어플라이언스가 읽기 전용으로 설정되기 때문에 오류 레이블이 표시된 이벤트를 생성합니다. 무결성 검사 후 VDP는 어플라이언스가 읽기 전용에서 모든 권한으로 변경되기 때문에 정보 레이블이 표시된 이벤트를 생성합니다.

이벤트 항목을 클릭하면 관련 이벤트 **표시** 링크를 비롯하여 해당 이벤트에 대한 세부 정보가 표시됩니다.

용량 사용 문제를 표시하는 지속적인 팝업 메시지

VDP 어플라이언스 스토리지 또는 Data Domain 스토리지 사용량이 심각한 수준에 이르면 관련 메시지가 포함된 알림 표시줄이 vSphere Web Client에 표시됩니다. 이 메시지의 텍스트와 아이콘은 스토리지 사용량에 따라 달라집니다. 동일한 텍스트와 아이콘이 **구성 탭의 스토리지 요약** 섹션에 표시됩니다.

알림 표시줄 아래에 있는 숨김/표시 컨트롤을 사용하여 알림 표시줄을 숨기거나 표시할 수 있습니다. 알림 표시줄의 숨김과 표시는 페이드 및 크기 재조정 효과를 사용하여 애니메이션됩니다.

높은 심각도 메시지를 나타내는 아이콘이 숨김/표시 컨트롤 왼쪽에 표시됩니다. 알림 표시줄을 숨긴 경우 용량 알림을 확인하도록 높은 심각도 메시지 아이콘이 나타납니다.

또한 알림 표시줄 오른쪽에는 **구성 - 백업 어플라이언스** 링크가 포함되어 있습니다. 링크를 클릭하면 **구성 탭의 백업 어플라이언스** 창이 표시되고 알림 표시줄의 링크가 숨겨집니다.

스토리지 사용량이 심각한 수준이 아닌 경우 알림 표시줄과 숨김/표시 컨트롤이 레이아웃에 표시되거나 포함되지 않습니다.

웹 브라우저 창의 크기를 재조정하는 경우 알림 표시줄이 내용에 맞춰 확대/축소됩니다. 표시줄에 맞추기 위해 텍스트가 잘릴 경우 메시지에 툴 설명이 표시됩니다.

VDP 종료 및 시작 절차

VDP 어플라이언스를 종료해야 하는 경우 vCenter Server Web Client에서 **게스트 운영 체제 종료** 작업을 사용합니다. 이 작업을 사용하면 어플라이언스의 완전한 종료가 수행됩니다. **게스트 운영 체제 종료** 작업 없이 어플라이언스의 전원을 끈 경우 손상이 발생할 수 있습니다. VDP 어플라이언스를 종료하고 재시작하는 데는 30분 정도 소요될 수 있습니다. 가상 머신 콘솔을 사용하여 상태를 모니터링할 수 있습니다. 어플라이언스가 종료된 후에는 vCenter Server Web Client에서 **전원 켜기** 작업을 사용하여 재시작할 수 있습니다.

어플라이언스가 제대로 종료되지 않은 경우 재시작할 때 마지막으로 검증된 체크포인트로 롤백을 수행합니다. 즉, 체크포인트와 예기치 않은 종료 사이에 발생한 백업 작업 또는 백업에 대한 변경 사항은 유실됩니다. 이는 예상된 동작이며, 예기치 않은 종료에도 시스템이 손상되지 않도록 보장합니다. 자세한 내용은 **“어플라이언스 롤백”**(41페이지) 섹션을 참조하십시오.

VDP 어플라이언스는 유지 보수 작업을 지원하고 복구 작업에 사용할 수 있도록 24x7 상시 실행되도록 설계되었습니다. 특별한 이유가 없으면 VDP 어플라이언스를 종료하지 마십시오.

참고 vCenter Server 패치 또는 업그레이드 전에 VDP 종료 절차를 따르십시오.

프록시

이 장에서 다루는 내용은 다음과 같습니다.

- “프록시 개요”(62페이지)
- “프록시 처리량 관리”(63페이지)
- “외부 프록시 지원”(64페이지)
- “(선택 사항) 프록시 인증서 인증 구성”(66페이지)
- “외부 프록시 상태 모니터링”(67페이지)

프록시 개요

이 장에서는 VDP 어플라이언스의 내부 및 외부 프록시 사용에 대해 설명합니다.

초기 구축 후 VDP 어플라이언스에는 내부 프록시만 구성되어 있습니다. VDP 어플라이언스가 완전히 구축된 후 사용자는 VDP 구성 UI에서 외부 프록시를 최대 8개까지 구축할 수 있습니다. VDP 어플라이언스용 외부 프록시를 구성하는 경우 프로세스 중에 내부 프록시가 자동으로 비활성화됩니다.

외부 프록시 구축 전 고려 사항

VDP 어플라이언스에서 사용할 프록시를 하나 이상 구축할 때는 다음 사항을 고려하십시오.

- VDP 어플라이언스는 데이터 저장소에 액세스하지 못하므로, 핫 애드(HotAdd) 전송 방식이 사용되지 않습니다. 백업의 관점에서 VMware 핫 애드 Best Practice를 정의하려면 다음 VMware 기술 자료 문서를 참조하십시오.
<http://kb.vmware.com/kb/1008072>
- 더 많은 백업을 동시에 수행해야 하고 vSphere 호스트의 리소스나 데이터 저장소 성능에 의해 제약을 받지 않아야 합니다. 최대 24개의 동시 백업 작업이 지원됩니다.
- LVM(Logical Volume Manager) 또는 EXT4 기반 파일 시스템에서 FLR(File Level Recovery)을 수행하려면 외부 프록시가 필요합니다.

외부 프록시 구축

백업 프로세스 중에 핫 애드(HotAdd)를 활용하려면 프록시 어플라이언스가 타겟 가상 머신이 있는 데이터 저장소에 직접 액세스할 수 있어야 합니다. 백업 에이전트 어플라이언스는 연결된 vSphere 호스트의 데이터 저장소 액세스 권한을 활용합니다. 외부 프록시를 구축할 때는 어플라이언스가 vSphere 호스트를 통해 원하는 데이터 저장소에 액세스할 수 있는지 확인하십시오.

프록시 어플라이언스가 타겟 가상 머신이 있는 데이터 저장소에 액세스할 수 없는 경우 HotAdd 대신 NBDtransport 메시지가 호출되며, 이로 인해 백업 속도가 크게 감소할 수 있습니다.

구축할 프록시 수 및 프록시당 프록시 처리량

구축할 프록시 수 및 프록시당 프록시 처리량 구성을 고려할 때는 다음을 Best Practice로 고려하십시오.

단일 프록시를 사용할 경우

- 외부 프록시에서 메모리 및 CPU에 대해 기본 구성을 사용하여 구축된 경우 백업을 실행할 때 최적의 프록시 처리량은 6개입니다. 프록시당 프록시 처리량을 늘려 6개가 넘으면 성능이 저하됩니다.
- 외부 프록시에서 CPU를 늘릴 경우 단일 외부 프록시에서 메모리를 늘릴 때보다 성능이 나아집니다.
- 외부 프록시 구성을 8개 CPU로 수정하는 경우 프록시당 8개의 프록시 처리량을 실행하면 최적입니다. 레벨 0 및 레벨 1 백업의 경우에도 마찬가지입니다. 이 구성을 사용하면 네트워크 대역폭이 제한 요소가 됩니다.

레벨 0 백업에 여러 외부 프록시를 사용할 경우

- 구축되는 프록시 수를 최대화하면 최상의 성능을 얻지 못할 수 있습니다.
- 프록시 수를 늘리면 프록시당 최적 프록시 처리량이 줄어들 수 있습니다. 예를 들어 외부 프록시 2개가 실행 중이면 프록시당 프록시 처리량을 6개 실행 중일 때 결과가 가장 좋을 수 있습니다. 외부 프록시 4개가 실행 중이면 프록시당 프록시 처리량을 4개 실행 중일 때 결과가 가장 좋을 수 있습니다. 이 결과는 vSphere 호스트당 프록시 수에 의해 제약받을 수 있습니다.
- 설정된 수의 백업을 수행할 때는 프록시 수 대신 프록시당 프록시 처리량을 늘리는 편이 낫습니다.

레벨 1 백업에 여러 외부 프록시를 사용할 경우

가상 머신에 대한 증분(레벨 1) 백업을 실행 중인 경우 프록시 수를 늘리는 것을 고려하십시오. 프록시당 4개의 프록시 처리량을 실행하면 프록시 수를 줄이고 프록시당 8개의 프록시 처리량을 실행할 때보다 성능이 낮습니다.

VDP 어플라이언스에서 실행되는 백업 볼륨 늘리기

백업이 실행된 후 계속 실행 중일 때 VDP 어플라이언스에서 특정 시간 동안 수행하는 백업의 볼륨을 늘려야 하는 경우가 있습니다. 지정된 시간에 수행되는 백업량을 늘리는 경우 다음 Best Practice를 고려하십시오.

- vSphere 서버 리소스가 제약 조건으로 작용하는 경우 프록시당 프록시 처리량을 더 많이 실행하고 프록시 수를 줄입니다.
- vSphere 서버 리소스의 제약을 받지 않는 경우 프록시 수를 늘리고 프록시당 프록시 처리량을 4개로 유지합니다.
- 원하는 백업을 처리하는 데 6-8개의 외부 프록시가 필요한 경우 프록시당 프록시 처리량을 늘리고 구축되는 외부 프록시 수를 제한합니다.

VDP 어플라이언스에서 실행되는 동시 백업 줄이기

VDP 어플라이언스에서 백업의 실행이 시작된 후에 VDP 어플라이언스에서 실행 중인 동시 백업 수를 줄여 데이터 저장소와 관련 스토리지의 로드를 제한해야 하는 경우가 있습니다. VDP 어플라이언스에서 실행 중인 동시 백업 수량을 줄일 때는 다음 Best Practice를 고려하십시오.

- 쓰기 성능이 더 빠른 데이터 저장소에 VDP 어플라이언스를 배치합니다. 데이터 저장소로 NFS보다는 iSCSI를 선택합니다.
- 백업 동안 보호된 가상 머신이 있는 데이터 저장소의 로드가 높은 경우 프록시 수 및 프록시당 프록시 처리량을 4개 이하로 줄입니다. 그러면 백업을 수행할 때 검색 및 읽기 작업량이 감소합니다.

프록시 처리량 관리

프록시 처리량 관리 마법사에서는 인프라를 기준으로 동시 백업 및 복구 작업 수를 구성할 수 있습니다. 프록시 처리량 관리 마법사를 사용하여 내부 및 외부 프록시 모두에 대한 값을 설정할 수 있습니다. VDP 어플라이언스에서는 최대 8개의 외부 프록시를 지원하며 최대 동시 백업 작업 수는 24개입니다.

자세한 내용은 “[구축할 프록시 수 및 프록시당 프록시 처리량](#)”(62페이지) 섹션을 참조하십시오.

주의 동시 백업 및 복구를 위해 선택한 클라이언트 수는 글로벌하게 적용되는 설정입니다. 이 설정은 내부 및 외부 프록시 설정 모두에 적용됩니다.

절차

- 1 웹 브라우저를 열고 다음을 입력합니다.
`https://<IP_address_VDP_Appliance>:8543/vdp-configure/`
- 2 VDP 사용자 이름과 암호를 사용해서 로그인합니다.
- 3 구성 탭을 클릭합니다.
- 4 **작업** 목록에서 **프록시 처리량 관리**를 선택합니다.
프록시 관리 페이지가 나타납니다.
- 5 동시에 실행할 백업 및 복구 클라이언트의 수를 1~8 범위 내에서 선택합니다.
- 6 다음을 클릭합니다.
완료 준비 페이지가 나타납니다.
- 7 **마침**을 클릭하여 변경 내용을 적용합니다.

외부 프록시 지원

VDP Advanced 어플라이언스 버전 5.5.6 이하는 내부 프록시로만 구성되므로, 프록시 서비스가 VDP 어플라이언스 내부에서 실행되고 어플라이언스의 작업 요청을 관리하도록 등록됩니다. VDP 6.0 어플라이언스에 대해 외부 프록시를 구성할 수 있습니다.

참고 외부 프록시가 포함된 VDP 어플라이언스는 EXT4 파일 시스템을 사용하는 가상 머신에서 FLR(File Level Recovery)을 지원합니다.

외부 프록시 구축을 위한 Best Practice

참고 외부 프록시를 사용하도록 어플라이언스를 구성할 경우 내부 프록시는 자동으로 비활성화됩니다.

일반적으로 핫 애드(HotAdd) 전송을 사용하면 NBD(Network Block Device) 전송을 사용하여 네트워크를 통해 백업 및 복구할 때보다 빠릅니다.

외부 프록시 Best Practice

■ 분리된 프록시 정리

VDP 어플라이언스에 등록되었지만 vCenter 인벤토리에 더 이상 존재하지 않는 외부 프록시를 분리된 프록시라고 합니다. 프록시 가상 머신이 vCenter 인벤토리에 남아 있고 프록시에 대해 "VM이 삭제되었거나 현재 vCenter에서 관리되고 있지 않습니다."라는 경고가 표시되는 경우 VDP 구성 유틸리티를 통해 프록시 가상 머신을 다시 시작할 수 있습니다. 문제가 지속되는 경우 잘못된 네트워크 구성으로 인해 호스트 이름을 확인할 수 없는 문제가 나타날 수 있습니다. 이 문제를 해결하려면 분리된 프록시를 삭제하고 새 프록시를 재구축하십시오.

■ vCenter에서 프록시의 ESXi 호스트 제거

외부 프록시의 ESXi 호스트가 vCenter에서 제거된 경우 VDP 어플라이언스는 프록시를 분리된 프록시로 간주하고 VDP 구성 유틸리티에서 이 프록시를 선택하면 "VM이 삭제되었거나 현재 vCenter에서 관리되고 있지 않습니다."라는 경고가 표시됩니다. ESXi 호스트를 vCenter에 추가하지 않을 경우 VDP 구성 유틸리티에서 분리된 프록시 항목을 삭제하십시오.

■ vCenter 전환

프록시의 ESXi 호스트가 VDP의 ESXi 호스트와 함께 새 vCenter로 이동되지 않은 경우 해당 프록시는 VDP 구성 유틸리티에서 분리된 프록시로 나타납니다. 프록시의 호스트를 새 vCenter로 이동하거나 VDP의 호스트를 다시 원래 vCenter로 이동할 계획이 아닌 경우 VDP 구성 유틸리티에서 분리된 프록시를 삭제하십시오.

■ VDP 롤백

VDP 어플라이언스를 이전 체크포인트로 롤백한 경우 체크포인트를 생성한 후 추가하거나 삭제한 외부 프록시는 VDP 구성 유틸리티에서 분리된 프록시로 나타납니다. 추가된 외부 프록시의 경우 VDP 구성 유틸리티를 통해 다시 시작하여 재등록하거나 재구축할 수 있습니다. 삭제된 프록시의 경우에는 VDP 구성 유틸리티에서 분리된 프록시 항목을 삭제하십시오.

■ 처음부터 VDP 재구축 및 롤백

VDP 어플라이언스에 문제가 발생하여 처음부터 재구축해야 하는 경우와 어플라이언스가 Data Domain의 체크포인트로 롤백된 경우에는 VDP 구성 유틸리티를 사용하여 어플라이언스의 암호를 즉시 변경하십시오. 체크포인트 생성 이전에 구축된 외부 프록시는 분리된 프록시로 표시됩니다. 이러한 분리된 프록시는 VDP 구성 유틸리티에서 삭제하십시오. 재구축된 VDP 어플라이언스에서 체크포인트 롤백 이전에 구축된 외부 프록시는 "외부 프록시로 인증하지 못했습니다."라는 경고와 함께 나타납니다. VDP 어플라이언스의 암호를 변경한 후에는 프록시의 암호를 업데이트하십시오.

■ 테이프에서 VDP 재해 복구

재해 발생 후 테이프에서 VDP 어플라이언스를 복구한 경우 VDP 구성 유틸리티에서 분리된 외부 프록시를 삭제하고 새 프록시를 구축하십시오.

■ 암호 업데이트

VDP 구성 유틸리티를 통해 VDP 어플라이언스의 암호를 변경하는 경우 VDP 어플라이언스는 등록된 모든 외부 프록시에서 암호를 업데이트합니다. 프록시의 암호가 업데이트되지 않은 경우 프록시를 선택할 때 "외부 프록시로 인증하지 못했습니다."라는 경고가 표시됩니다. VDP 구성 유틸리티를 통해 프록시의 암호를 수동으로 업데이트할 수 있습니다.

■ 프록시 재시작

기존에 등록된 외부 프록시가 VDP 구성 유틸리티에서 등록되지 않은 것으로 표시되는 경우 프록시를 다시 시작합니다. 그러면 프록시의 전원 주기가 진행되고 프록시가 VDP 어플라이언스에 다시 등록됩니다.

■ 긴급 복구

외부 프록시로 긴급 복구 작업을 수행하는 경우 내부 프록시가 자동으로 활성화됩니다. 긴급 복구 작업이 완료되고 모든 ESXi 호스트가 vCenter에 다시 연결되면 내부 프록시를 삭제하거나 외부 프록시를 모두 삭제할 수 있습니다. 긴급하지 않은 복구 작업에 대해 내부 프록시와 외부 프록시를 모두 활성화하지 마십시오.

제한 사항

- 외부 VDP 프록시는 vSphere 호스트 5.1 이상에서만 지원됩니다.
- VDP 어플라이언스당 외부 프록시는 8개로 제한됩니다.
- 최대 동시 백업 작업 수는 24개입니다.
- EXT4 파일 시스템을 사용하는 가상 머신에서 FLR(File Level Recovery)을 수행하려면 외부 프록시를 사용해야 합니다.

외부 프록시 추가

프록시 추가 마법사를 사용하면 최대 8개의 외부 프록시를 추가 및 구축하고 VDP 구성 유틸리티에서 VDP 어플라이언스에 등록할 수 있습니다.

절차

- 1 웹 브라우저를 열고 다음을 입력합니다.
https://<IP_address_VDP_Appliance>:8543/vdp-configure/
- 2 VDP 사용자 이름과 암호를 사용해서 로그인합니다.
- 3 구성 탭을 클릭합니다.
- 4 작업 목록에서 **프록시 추가**를 선택합니다.
 프록시 추가 페이지가 나타납니다.
- 5 호스트 및 스토리지 페이지에서 다음 자격 증명을 지정한 후 다음을 클릭합니다.
 - **호스트**: 목록에서 대상 호스트를 선택합니다.
 - **Storage**: 목록에서 대상 스토리지 디바이스를 선택합니다.
 - **네트워크 연결**: 목록에서 가상 머신의 네트워크 연결을 선택합니다.
- 6 네트워크 페이지에서 다음 네트워크 설정을 지정한 후 다음을 클릭합니다.
 - **IPv4 정적 주소**: 인터페이스의 인터넷 프로토콜 v4 또는 v6 설정입니다.
 - **넷마스크**: IPv4 또는 IPv6 정적 주소의 네트워크 마스크입니다.
 - **게이트웨이**: IPv4 또는 IPv6 정적 주소의 게이트웨이 주소입니다.
 - **운영 DNS**: DNS 확인에 사용되는 운영 도메인 이름 시스템입니다.
 - **보조 DNS**: DNS 확인에 사용되는 보조 도메인 이름 시스템입니다.
- 7 완료 준비 페이지에서 구축 설정을 검토합니다.

참고 완료 준비 페이지에서 외부 프록시 가상 머신의 이름을 변경할 수 있습니다.

8 **마침**을 클릭하여 프록시를 구축합니다.

5단계에서 선택한 데이터 저장소에 프록시가 구축되는지 확인합니다. 성공적으로 구축된 후 프록시가 VMware vSphere DRS(Distributed Resource Scheduler™) 클러스터에 구축되면 클러스터는 Storage VMotion을 사용하여 프록시를 이동할 수 있습니다. 다른 스토리지로 마이그레이션하는 동안 프록시에서 실행 중인 작업은 손상될 위험이 있습니다. DRS 클러스터에 있는 프록시의 경우 핫 애드(HotAdd) 기능이 작동하지 않습니다. 따라서 프록시의 DRS를 수동으로 해제해야 합니다. 내부 프록시를 사용 중인 경우 이 시나리오가 VDP 어플라이언스에도 적용됩니다.

프록시의 DRS를 수동으로 해제하려면 다음 단계를 따르십시오.

- 1 이 프록시를 호스팅하는 클러스터에 대해 **DRS** 탭을 선택합니다.
- 2 가상 머신 옵션을 클릭합니다.
- 3 **자동화** 수준 아래에서 프록시 가상 머신을 찾아 **비활성화**로 변경합니다.

내부 프록시 비활성화

사용자가 외부 프록시 백업 중 체크포인트로 롤백 작업을 수행하는 경우 롤백이 완료되면 VDP 구성 유틸리티에 내부 프록시가 표시될 때 내부 프록시를 비활성화하라는 경고 메시지가 함께 표시됩니다.

절차

- 1 VDP 구성 유틸리티의 **프록시** 목록에서 내부 프록시를 선택합니다.
- 2 프록시 작업 아이콘에서 **프록시 관리**를 선택합니다.
내부 프록시 관리 마법사가 표시됩니다.
- 3 **내부 프록시 비활성화** 확인란을 활성화하고 **다음**을 클릭합니다.
- 4 마법사의 완료 준비 페이지에서 **마침**을 클릭하여 변경 사항을 적용합니다.

(선택 사항) 프록시 인증서 인증 구성

기본적으로 프록시는 vCenter Server에 연결할 때 SSL 인증서를 검증하지 않습니다. 이로 인해 vCenter Server가 MITM(Man-in-the-Middle) 악용에 취약해질 수 있으므로, vCenter Server에 대한 무단 액세스가 발생할 수 있습니다. 각 프록시가 vCenter Server에 연결할 때 SSL 인증서 인증을 사용하도록 구성하면 이 취약성이 해소됩니다. 자세한 내용은 [5장, “VDP와 vCenter 간의 통신 보안”\(45페이지\)](#)에 나와 있습니다.

외부 프록시 상태 모니터링

상태 기준

외부 프록시에 대해 보고되는 상태는 다음과 같은 기준에 기반합니다.

- 디스크 사용량
 - 경고: 70% 용량보다 큰 파일 시스템
 - 중요 경고: 90% 용량보다 큰 파일 시스템
- CPU 로드
 - 경고: 15분 로드 평균이 1.5보다 큼
 - 중요 경고: 15분 로드 평균이 5.0보다 큼
- 메모리 사용량
 - 경고: 사용량이 85%보다 큼
 - 중요 경고: 사용량이 95%보다 큼

외부 프록시 로그

외부 프록시 로그는 외부 프록시가 하나 이상 구성된 경우에만 표시됩니다. 이 로그 번들을 다운로드하면 .zip 파일이 브라우저로 스트리밍됩니다. 이 .zip 파일에는 외부 프록시 로그가 모두 포함되어 있습니다. 내부 프록시는 이 로그 번들에서 제외됩니다.

로그 다운로드에 대한 자세한 내용은 [“VDP 로그 또는 진단 정보 수집”](#)(38페이지) 섹션을 참조하십시오.

스토리지 관리

이 장에서 다루는 내용은 다음과 같습니다.

- [“새 스토리지 생성”](#)(70페이지)
- [“기존 VDP 디스크 연결”](#)(72페이지)
- [“스토리지 분리 및 다시 연결”](#)(73페이지)
- [“스토리지 구성 보기”](#)(74페이지)

새 스토리지 생성

초기 구성 마법사는 스토리지 유형 선택, VDP 스토리지 디스크에 디바이스 할당 등을 안내하고 성능 평가 툴을 실행할 수 있는 옵션을 제공합니다.

제한 사항

새 스토리지를 생성 중인 동안에는 어플라이언스를 새 호스트 또는 새 데이터 저장소로 마이그레이션할 수 없습니다.

사전 요구 사항

- VDP 어플라이언스가 구축되어 있어야 하고 초기 구성 마법사의 스토리지 생성 페이지에 로그인해야 합니다.
- OVA 구축 후 VDP 어플라이언스에서 vSphere HA를 즉시 비활성화합니다. VDP 어플라이언스에서 스토리지 생성을 포함한 초기 구성을 수행한 후에 어플라이언스의 vSphere HA를 활성화할 수 있습니다.

절차

- 1 초기 구성 마법사의 스토리지 생성 페이지에서 새 스토리지 생성을 선택합니다. 스토리지를 생성하면 선택한 데이터 저장소에 새 스토리지 노드가 생성됩니다.
- 2 다음 용량 옵션 중 하나를 선택하고 다음을 클릭합니다.

- 0.5
- 1
- 2
- 4
- 6
- 8

디바이스 할당 페이지가 나타납니다. 새 스토리지를 생성하는 경우, 필요한 디스크 수를 알 수 있습니다.

- 3 프로비저닝 드롭다운 목록에서 프로비저닝 유형을 선택합니다.
 - **일반 Lazy-Zeroed**(권장되는 기본 프로비저닝 유형): 일반 Lazy-Zeroed 프로비저닝은 기본적으로 일반 형식으로 가상 디스크를 생성합니다. 가상 디스크가 생성되면 가상 디스크에 필요한 용량이 할당됩니다. 생성 중에 물리적 디바이스에 남아 있는 데이터는 지워지지 않지만 나중에 가상 머신에서 처음 쓰기 작업을 할 때 필요 시 모두 삭제됩니다.
 - **일반 Eager-Zeroed**: 일반 Eager-Zeroed 프로비저닝은 데이터 보안이 우려될 때 사용되는 일반 가상 디스크 유형을 생성합니다. 가상 디스크가 생성되면 가상 디스크에 필요한 용량이 할당됩니다. 이전 데이터가 있는 데이터 저장소에서 일반 Eager-Zeroed 프로비저닝을 사용해 가상 디스크를 생성한 경우 이전 데이터는 지워지고 복구할 수 없습니다. 다른 유형의 디스크를 생성하는 것보다 이 형식의 디스크를 생성하는 데 시간이 더 걸릴 수 있습니다.
 - **가상**: 씬 디스크의 경우 사용자가 디스크 크기로 입력한 값을 기준으로 디스크가 필요로 하는 만큼 데이터 저장소 공간을 프로비저닝합니다. 씬 디스크는 적은 용량으로 시작해서 초기 작업에 필요한 만큼만 데이터 저장소 공간을 사용합니다.
- 4 디스크를 데이터 저장소에 모두 할당했다면 다음을 클릭합니다.

완료 준비 페이지에서 스토리지 구성에 대한 성능 분석을 실행하고 다음을 클릭하여 변경 사항을 적용할 수 있습니다. 성능 분석 테스트를 건너뛸 수도 있지만 실행하는 것이 좋습니다.

- 5 다음을 클릭하면 스토리지 구성이 시작되고 실행을 취소할 수 없다는 경고 메시지가 표시됩니다. 계속하려면 **예**를 클릭합니다.

가능한 결과는 통과, 실패, 조건부 통과입니다. 조건부 통과는 검색 테스트(기본적으로 제외됨)를 선택한 경우만 해당됩니다. 모든 테스트가 성공하면 결과는 통과입니다. 쓰기 또는 읽기 테스트가 성공적이지 않으면 결과는 실패입니다. 검색 테스트를 선택한 경우 쓰기 및 읽기 테스트가 성공적이지만 검색 테스트가 실패하면 결과는 조건부 통과입니다.

- a 테스트를 실행하려면 **스토리지 구성에 대해 성능 분석 실행 확인란**을 선택하여 스토리지 구성이 최소 성능 기대치를 충족하는지 확인합니다. **표 8-11**에는 최소 성능 기대치가 나와 있습니다.

이 테스트에서는 디스크에 대해 쓰기, 읽기 및 검색 성능 테스트를 수행합니다. 스토리지 구성에 따라 성능 분석을 완료하는 데 30분에서 몇 시간까지 소요될 수 있습니다.

- b 테스트가 성공적으로 실행된 후 어플라이언스를 자동으로 재시작하려면 **성공한 경우 어플라이언스 재시작**을 선택하고 다음을 클릭하여 테스트를 시작합니다.

성능 분석 테스트는 서버에서 시작되고 테스트가 실행되는 동안 브라우저를 닫을 수 있습니다.

- 테스트가 성공하면 구성이 완료되었다는 메시지가 나타나고 서버에서 어플라이언스를 자동으로 재시작합니다.
- 테스트가 조건부로 통과 또는 실패한 경우에는 성능 분석 결과가 나타나지만 서버에서 어플라이언스를 자동으로 재시작하지 않습니다. 테스트 결과를 보려면 VDP-Configure에 다시 로그인하여 클라이언트를 수동으로 재시작해야 합니다.

참고 59초 내에 **재시작**을 클릭하지 않으면 어플라이언스가 자동으로 재시작되고 서비스를 시작합니다. VDP 어플라이언스가 재시작되면 일련의 자동 구성 단계가 수행됩니다. 이 단계를 완료하는 데에는 30-45분 정도 소요될 수 있습니다.

다음과 같은 경우에는 어플라이언스가 자동으로 재시작됩니다.

- VDP 구성 마법사가 끝날 때 성능 분석을 수행하도록 선택하는 경우
- VDP 구성 마법사에서 테스트 성공 후 VDP 어플라이언스를 재시작하는 확인란을 선택한 경우
- 테스트 성공 후

최소 스토리지 성능

VDP 어플라이언스를 구성할 때 성능 테스트는 구축된 어플라이언스의 크기에 따라 다양한 결과를 냅니다.

표 8-11에는 VDP 어플라이언스 크기별로 읽기, 쓰기 및 검색 성능에 대한 최소 기대치가 나와 있습니다.

표 8-11. 스토리지 성능에 대한 최소 기대치

VDP 어플라이언스 크기 (TB)	디스크 크기	읽기 최소값	쓰기 최소값	검색 최소값
단일 데이터 저장소	256GB	10MB/s	20MB/s	106Seeks/s
0.5	256GB	60MB/s	30MB/s	400Seeks/s
1.0	512GB	60MB/s	30MB/s	400Seeks/s
2.0	1024GB	60MB/s	30MB/s	400Seeks/s
4.0	1024GB	80MB/s	40MB/s	400Seeks/s
6.0	1024GB	80MB/s	40MB/s	400Seeks/s
8.0	1024GB	150MB/s	120MB/s	400Seeks/s

기존 VDP 디스크 연결

초기 구성 마법사의 스토리지 생성 페이지에는 **기존 VDP 디스크 연결** 옵션이 있습니다. 이 옵션을 사용하면 데이터 저장소를 찾고 이전에 사용된 VDP 디스크를 선택한 다음 선택한 디스크를 새 VDP 어플라이언스에 자동으로 연결할 수 있습니다. 이러한 디스크는 새 VDP 어플라이언스에 자동으로 추가됩니다.

주의 이 절차의 단계를 수행하지 않은 채 사용된 VDP 디스크를 새 VDP 어플라이언스에 수동으로 연결하려고 시도하지 마십시오. 사용된 VDP 디스크를 가져오는 경우에는 복구 지점만 가져오고 백업 작업과 구성 정보(예: e-메일 보고서)는 가져오지 않습니다. 작업을 다시 생성해야 합니다. 가져온 복구 지점은 **/REPLICATE/VDP_IMPORTS** 도메인에 있습니다. vSphere 웹 클라이언트의 **/REPLICATE/VDP_IMPORTS** 도메인에서 실제 복구 지점을 볼 수 있습니다. VDP가 불안정하거나 잘못된 스토리지 구성을 감지하는 경우 작업이 실패합니다.

기존 스토리지를 연결하면 새 스토리지를 생성할 때 필요한 용량 옵션을 선택할 필요가 없습니다.

이전에 사용된 VDP 디스크가 새 VDP 어플라이언스에 연결되면 다음 변경 사항이 발생합니다.

- 이전에 사용된 VDP와 관련된 모든 백업 작업이 삭제되므로 재생성해야 합니다.
- 이전에 사용된 VDP와 관련된 모든 복제 작업이 삭제되므로 재생성해야 합니다.
- 이전에 사용된 VDP와 관련된 복구 시점은 그대로 유지됩니다. 복구 시점은 원래 VM 이름에 임의 문자로 된 문자열이 추가된 형태로 나타납니다.
- 백업 복구 마법사의 복구 옵션 설정 페이지에서 이전에 사용된 VDP 디스크와 관련된 복구 시점에 대해 **원래 위치로 복구** 옵션이 비활성화됩니다.
- e-메일 보고 기능을 재구성해야 합니다.

사전 요구 사항

- 기존 스토리지를 연결하기 전에 **“VDP 설치 및 구성”(21페이지)**의 설명에 따라 VDP 어플라이언스를 설치 및 구성해야 합니다.
- VDP 어플라이언스에 연결하고자 하는 VDP 스토리지는 모두 백업해야 합니다.

절차

- 1 초기 구성 마법사의 스토리지 생성 페이지에서 **기존 VDP 디스크 연결**을 선택하고 다음을 클릭합니다.

디바이스 할당 대화상자가 나타납니다.

- 2 첫 번째 줄임표 버튼을 클릭합니다.

a 연결할 첫 번째 vmdk 파일을 찾습니다.

b 해당 vmdk 파일을 강조 표시하고 **선택**을 클릭합니다.

참고 이전에 사용된 VDP 어플라이언스의 데이터 디스크만 연결하도록 선택할 수 있습니다. OS 부트 파티션은 선택할 수 없습니다. 200GB의 기본 디스크 파티션(OS 부트 파티션)을 선택할 경우 오류 메시지가 나타납니다.

vmdk 파일을 원하는 순서로 연결할 수 있습니다. 첫 번째 vmdk 파일을 선택하면 시스템은 디스크를 분석하고 선택할 추가 디스크 수를 정의합니다.

참고 연결 프로세스가 진행되는 동안 언제든지 **재설정** 버튼을 클릭하여 디바이스 할당 대화상자를 원래 상태로 재설정할 수 있습니다.

- 3 정의할 다음 디스크에 해당하는 줄임표 버튼을 클릭합니다.

a 연결할 다음 vmdk 파일을 찾습니다.

b 해당 vmdk 파일을 강조 표시하고 **선택**을 클릭합니다.

각 디스크는 추가되기 전에 일치하는 디스크로 검증됩니다. 검증에 실패하면 오류 메시지가 나타납니다. 오류 메시지를 확인하려면 빨간색으로 강조 표시된 디스크 위에 마우스를 가져가십시오.

- 4 나머지 모든 디스크에 대해 **3단계**를 반복합니다.

- 5 모든 디스크가 할당된 후 **다음**을 클릭하여 전체 디스크를 검증합니다.

완료 준비 페이지가 나타납니다.

- 6 **Next**를 클릭합니다.

시스템에

다음 프로세스는 스토리지 구성을 시작합니다. 이 작업은 취소할 수 없습니다. 계속하시겠습니까? 라는 메시지가 표시됩니다.

- 7 **예**를 클릭합니다.

시스템에는 이전에 사용된 VDP 어플라이언스와 관련된 루트 암호를 제공하라는 메시지가 표시됩니다.

- 8 **암호 및 암호 확인** 입력란에 이전에 사용된 VDP 어플라이언스의 루트 암호를 입력한 다음 **확인**을 클릭합니다.

- 9 변경 사항을 적용하고 재부팅하려면 **마침**을 클릭합니다.

참고 스토리지 구성이 성공한 경우 시스템이 자동으로 재부팅되고 서비스를 시작합니다. VDP 어플라이언스가 재부팅되면 일련의 자동 구성 단계가 수행됩니다. 이 단계를 완료하는 데에는 30-45분 정도 소요될 수 있습니다.

구성이 완료되면 무결성 검사가 시작됩니다.

스토리지 분리 및 다시 연결

다음 절차에서는 VDP 어플라이언스의 기본 디스크 파티션(OS 부트 파티션)이 손상되거나 손실되어 VDP 어플라이언스를 복구할 수 없는 경우 수행해야 하는 단계에 대해 설명합니다.

사전 요구 사항

- vmdk 파일이 분리되었다가 다시 연결되는 VDP 어플라이언스에 하나 이상의 검증된 체크포인트가 있어야 합니다.
- 새로운 VDP 어플라이언스는 이전 VMDK 디스크 데이터와 호환되도록 구축해야 합니다. 즉, VDP 어플라이언스는 디스크 데이터와 같은 버전이거나 최신 버전이어야 합니다.
- 이전 VDP 어플라이언스의 vmdk 파일은 새로 구축한 VDP 어플라이언스에서 액세스할 수 있는 데이터 저장소에 있어야 합니다.

참고 다시 연결하는 동안 이전 VDP 어플라이언스의 루트 암호를 입력하라는 메시지가 표시됩니다.

Best Practice

- VDP 어플라이언스에 다시 연결하기 전에 모든 vmdk 파일의 백업 복사본을 만드십시오.
- 가능한 경우 **게스트 운영 체제 종료** 작업을 사용하여 VDP 어플라이언스를 종료한 후 VDP 어플라이언스에서 vmdk 파일을 분리합니다. 그렇지 않은 경우 마지막 방법으로 가상 머신의 전원을 끕니다.
- VDP 어플라이언스에서 vmdk 파일을 분리하기 전에 vmdk 파일의 전체 경로와 이름을 메모해 둡니다. 이 정보는 새로 구축된 VDP 어플라이언스에 디스크를 다시 연결할 때 필요합니다.

절차

- 1 vSphere Client에서 VDP 어플라이언스로 이동한 후 가상 머신에서 **게스트 운영 체제 종료** 작업을 수행합니다.

참고 **게스트 운영 체제 종료** 작업이 회색으로 표시된 경우 **vCenter > 호스트 및 클러스터**로 이동하여 VDP 어플라이언스를 마우스 오른쪽 버튼으로 클릭한 후 **VM 전원 끄기**를 선택합니다.

- 2 VDP 어플라이언스에서 vmdk 파일을 분리합니다.
 - a vSphere Web Client에서 하드웨어 설정을 편집할 권한이 있는 사용자로 로그인합니다.
 - b **vCenter > Hosts and Clusters**로 이동합니다.
 - c 왼쪽 트리에서 VDP 어플라이언스가 나타날 때까지 펼치기 화살표를 클릭합니다.

- d VDP 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
가상 머신 속성이 나타납니다. **하드웨어** 탭이 기본적으로 선택되어 있습니다.
하드 디스크 1은 항상 기본 200GB OS 부트 파티션입니다. VDP 어플라이언스에서 하드 디스크 1을 제거하지 마십시오.
 - e 목록에서 하드 디스크 2를 클릭합니다.
 - f **Disk File** 필드에서 vmdk 파일의 전체 경로와 이름을 메모해 둡니다. 이 정보는 디스크를 다시 연결할 때 필요합니다.
 - g **Remove**를 클릭합니다.
 - h 제거 옵션에서 **Remove from virtual machine**을 선택합니다.
 - i 목록에 있는 모든 하드 디스크(2부터 x 까지)에 대해 제거 옵션을 반복합니다.
 - j 2부터 x 까지 하드 디스크를 제거한 후 **OK**를 클릭합니다.
- 3 초기 구성 마법사의 스토리지 생성 페이지에서 **기존 VDP 디스크 연결**을 선택하고 **"기존 VDP 디스크 연결"**(72페이지)에 나와 있는 단계를 수행합니다.

스토리지 구성 보기

스토리지 탭에서는 스토리지 요약, 용량 활용도 정보 및 성능 분석 세부 정보가 제공됩니다.

용량 활용도 버튼을 누르면 데이터 저장소의 상태 정보를 제공하는 페이지가 표시됩니다.

- 데이터 저장소 아이콘 옆의 가로 막대 그래프는 데이터 저장소가 얼마나 가득 찼는지를 백분율로 보여 줍니다.
- 원형 차트는 데이터 저장소의 공간을 분류하여 보여 줍니다. 주황색은 데이터 저장소에서 사용된 공간의 용량을 나타냅니다. 녹색은 데이터 저장소의 가용 공간 용량을 나타냅니다. 파란색은 데이터 저장소에 구축된 가상 머신에서 실행되는 다른 애플리케이션이 사용하는 데이터 저장소 공간을 나타냅니다.
- 원형 차트 옆의 표에는 각 데이터 파티션 이름, 크기, 프로비저닝 유형 및 vmdk 파일 이름이 나열됩니다. 다음 예에서는 데이터 01이라는 데이터 파티션에 대한 정보를 보여 줍니다.

데이터 01	256GiB	씬(Thin)	sample-vdp-241168_6..0.0.117_1.vmdk
--------	--------	---------	-------------------------------------

이 예에서 256GiB는 사용할 수 있는 최대 크기를 나타냅니다.

성능 분석 버튼을 누르면 성능 분석 테스트의 통계가 포함된 표가 표시됩니다.

열	설명
데이터 저장소	데이터 저장소의 이름입니다.
완료 날짜	테스트가 완료된 날짜입니다.
결과	테스트 결과 다음 중 하나가 표시될 수 있습니다. <ul style="list-style-type: none"> ■ 실행 안 함 ■ 통과 ■ Failed <p>쓰기 또는 읽기 테스트가 성공적이지 않으면 결과는 "실패"입니다.</p> <ul style="list-style-type: none"> ■ 조건부 통과 <p>쓰기 및 읽기 테스트가 성공적이지만 검색 테스트(선택 사항)가 실패하면 결과는 "조건부 통과"입니다.</p>
읽기(MiB/s)	읽기 테스트에 대한 초당 용량(MB)입니다.
쓰기(MiB/s)	쓰기 테스트에 대한 초당 용량(MB)입니다.
검색(Seeks/s)	검색 테스트에 대한 초당 용량(MB)입니다.

사전 요구 사항

VDP 스토리지 디스크가 사용 가능한 데이터 저장소 위치에 배포되어야 하고, 디스크가 검증되어야 하며, 시스템이 재부팅되어, 시스템 서비스가 작동 중이어야 합니다.

절차

- 1 VDP-Configure URL에 로그인합니다.

https://<IP_address_VDP_appliance>:8543/vdp-configure/

- 2 스토리지 탭을 클릭합니다.

사용 가능한 데이터 저장소와 사용 가능한 총 스토리지 용량 및 각 데이터 저장소에 사용할 수 있는 스토리지 용량이 표시된 스토리지 요약 정보가 표시됩니다.

참고 페이지에서 데이터를 새로 고치려면 **스토리지 요약** 옆에 있는 새로 고침 아이콘을 클릭합니다.

- 3 데이터 저장소에 대한 상태 정보를 보려면 **용량 활용도**를 클릭합니다. 이 페이지는 기본값입니다.

- 4 성능 테스트를 실행하려면 **성능 분석**을 클릭하고 표에서 데이터 저장소를 선택한 다음 **실행**을 클릭합니다.

성능 분석 테스트에서는 데이터 저장소에 256GB vmdk를 생성하고 읽기, 쓰기 및 검색을 실행하여 데이터 저장소 성능을 확인합니다.

검색 테스트 활성화

검색 테스트는 원하는 스토리지의 검색 성능을 파악하도록 설계되었습니다. 이는 기본 스토리지가 싼 프로비저닝되지 않은 경우에 유용합니다. 대부분의 현장 구축에서는 싼 프로비저닝된 볼륨을 사용하므로 검색 테스트 결과는 혼란을 줄 수 있습니다. 검색 테스트는 가상화 환경에는 적합하지 않습니다. 따라서 이 테스트는 DAT Test Suite의 일부로 실행되는 기본 테스트에서 제외됩니다. 관리자가 코드를 구성 파일에 포함하는 경우 코드가 여전히 존재하며 검색 테스트가 수행될 수 있습니다.

검색 테스트를 실행하고자 하는 경우 먼저 아래 지침을 따라 구성 파일을 변경해야 합니다. 그런 다음 검색 테스트가 포함된 성능 분석 툴을 실행할 수 있습니다.

검색 테스트를 활성화하도록 구성 파일 변경

- 1 PuTTY를 사용하여 VDP 어플라이언스에 대한 SSH 세션을 시작합니다.
- 2 `/usr/local/vdr/etc/benchmark-settings.xml` 파일을 엽니다. 쓰기 권한이 필요합니다.
- 3 옵션 아래에서 `<runSeekTest>false</runSeekTest>`를 `<runSeekTest>true</runSeekTest>`로 변경합니다.
- 4 파일을 저장하고 PuTTY를 종료합니다.
- 5 성능 분석 제품군을 실행합니다.

Data Domain 통합

이 장에서 다루는 내용은 다음과 같습니다.

- “VDP와 Data Domain 시스템 통합”(78페이지)
- “아키텍처 개요”(78페이지)
- “VDP 클라이언트 지원”(79페이지)
- “Best Practice”(79페이지)
- “통합 전 요구 사항”(80페이지)
- “VDP 통합을 위한 Data Domain 시스템 준비”(83페이지)
- “Data Domain 시스템 추가”(84페이지)
- “Data Domain 시스템 편집”(85페이지)
- “VDP 어플라이언스에서 Data Domain 시스템 삭제”(85페이지)
- “VDP 및 Data Domain에서 백업”(87페이지)
- “복제 제어”(89페이지)
- “서버 유지 보수 작업 모니터링”(90페이지)
- “Data Domain 시스템에서 Avamar 체크포인트 백업 복구”(90페이지)
- “VDP 어플라이언스에서 Data Domain 모니터링”(92페이지)
- “전체 Data Domain 시스템에서 스토리지 재확보”(93페이지)
- “일반적인 문제 및 해결책”(95페이지)

VDP와 Data Domain 시스템 통합

VDP와 Data Domain 시스템을 통합하면 다음이 지원됩니다.

- 물리적 Data Domain 시스템을 VDP 백업의 백업 타겟으로 사용
- 백업 데이터의 타겟 대상을 백업 작업 생성 중에 설정할 수 있음
- 사용자가 백업 대상(VDP 또는 Data Domain)에 따른 영향 없이 작업을 수행할 수 있음

아키텍처 개요

Data Domain 시스템은 DD OS 소프트웨어를 통해 데이터 중복 제거를 수행합니다. Data Domain 시스템에 대한 VDP 소스 기반의 데이터 중복 제거는 DD Boost 라이브러리를 사용하여 수행됩니다.

VDP에서는 API 기반 통합을 통해 DD Boost 라이브러리를 사용하여 Data Domain 파일 시스템에 포함된 디렉토리, 파일 및 기타 항목을 액세스하고 조작합니다. VDP는 DD Boost API를 통해 Data Domain 시스템의 일부 속성과 기능을 볼 수 있습니다. 이를 통해 VDP에서는 Data Domain 시스템에 저장된 백업 이미지를 제어할 수 있습니다. 또한 유지 보수 작업을 관리하고 원격 Data Domain 시스템으로의 복제를 제어할 수도 있습니다.

DD Boost는 Data Domain 시스템 추가 중에 VDP 어플라이언스에 자동으로 설치됩니다.

그림 9-5에서는 VDP와 Data Domain이 통합된 솔루션의 아키텍처를 개략적으로 보여 줍니다. VDP와 Data Domain을 통합할 경우 특정 백업 정책이 VDP 어플라이언스를 타겟으로 하는지 또는 Data Domain 시스템을 타겟으로 하는지를 지정할 수 있습니다.

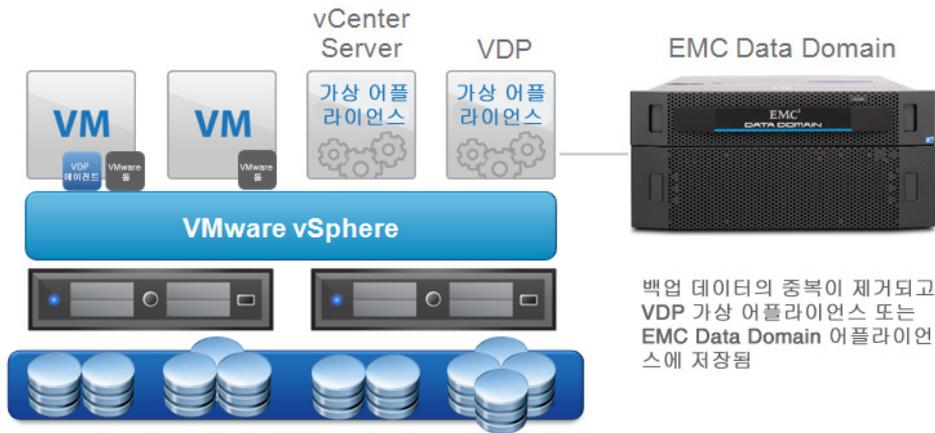


그림 9-5. VDP 및 Data Domain 솔루션

VDP 어플라이언스를 백업 스토리지의 타겟으로 선택한 경우 VDP 어플라이언스는 중복 제거 세그먼트 처리를 수행합니다.

Data Domain 시스템을 백업 타겟으로 선택하면 백업 데이터가 Data Domain 시스템으로 전송됩니다. 생성되는 관련 메타데이터는 VDP 어플라이언스에 동시에 전송되어 저장됩니다. VDP 어플라이언스는 이 메타데이터를 사용하여 Data Domain 시스템에서 복구 작업을 수행합니다.

VDP 클라이언트 지원

VDP 및 Data Domain 시스템 통합에서는 다음과 같은 플러그인을 지원합니다.

- VDP Plug-in for Exchange Server VSS
- VDP Plug-in for SharePoint Server VSS
- VDP Plug-in for SQL Server

Best Practice

Data Domain 시스템이 연결된 VDP의 제한 사항은 무엇입니까?

VDP 어플라이언스에서 TB 용량당 최대 25개의 가상 머신을 보호하는 것이 좋습니다. 이 숫자는 가상 머신의 크기, 일반적인 변경률 및 각 가상 머신의 데이터 양에 따라 달라질 수 있습니다. 이를 고려하면 Data Domain 시스템에 데이터를 백업하는 VDP 어플라이언스당 최대 200개의 가상 머신을 보호할 수 있습니다.

백업 데이터는 Data Domain 시스템에 저장되고 백업 작업 메타데이터만 VDP 어플라이언스에 저장되므로, 표준 Data Domain 시스템의 경우 0.5TB VDP 어플라이언스를 구축하고 64TB Data Domain 시스템의 경우 1TB VDP 어플라이언스를 구축하십시오.

다음 목록에는 Data Domain 시스템당 권장되는 VDP 어플라이언스 수가 나와 있습니다.

- DD160 및 DD620당 VDP 1개
- DD2200당 VDP 1개
- DD2500 및 DD4xxx당 VDP 2개
- DD7200 및 DD990당 VDP 3개

백업을 모두 Data Domain으로 이동하려는 경우 어느 정도 크기의 VDP 어플라이언스가 필요합니까?

Data Domain 시스템이 VDP 어플라이언스에 스토리지 디바이스로 연결된 경우 VDP 어플라이언스는 Data Domain 시스템을 대상으로 사용하여 백업에 대한 메타데이터만 저장합니다. 확인된 바에 따르면 백업 데이터를 모두 Data Domain 시스템으로 보내는 경우 16TB Data Domain 시스템에 0.5TB의 VDP 어플라이언스만 있으면 됩니다. 백업을 VDP 어플라이언스로 보내는 경우에는 VDP 어플라이언스에 저장할 데이터를 기준으로 VDP 어플라이언스 크기를 적절히 늘려야 합니다. 64TB 이상의 Data Domain 시스템에서는 백업 데이터에 사용될 것으로 예상되는 Data Domain 시스템 스토리지 64TB당 1TB의 VDP 어플라이언스를 구축할 수 있습니다.

VM에 이미지, 그림 및 PDF 파일이 많습니다. VDP 어플라이언스 또는 Data Domain 시스템 중에 어떤 것을 이러한 백업의 대상으로 설정해야 합니까?

이미지, 그림 및 PDF 파일에 대한 중복 제거 성능은 Data Domain 시스템이 표준 VDP 어플라이언스보다 우수합니다.

Data Domain 제한 사항

다음은 VDP 어플라이언스와 함께 Data Domain 시스템을 사용할 경우에 대해 정의된 현재의 제한 사항입니다.

- VDP 어플라이언스에 Data Domain 시스템을 연결한 경우, Data Domain 시스템이 연결된 VDP 어플라이언스의 VMDK에 대해 VDP 어플라이언스의 "기존 스토리지 가져오기" 기능을 사용할 수 없습니다.
- VDP 어플라이언스에는 한 번에 하나의 Data Domain 시스템만 연결할 수 있습니다.
- VDP Configuration UI에서 Data Domain 시스템을 삭제할 수 없습니다. Data Domain 시스템을 삭제하려면 "VDP 어플라이언스에서 Data Domain 시스템 삭제"(85페이지)에 정의된 수동 단계를 사용하십시오.
- Data Domain과 VDP의 연결이 끊어진 경우 VDP 어플라이언스가 Data Domain 시스템을 모니터링하지 않습니다. 어플라이언스 간의 연결이 끊어졌음을 나타낼 수 있는 동작으로는 무결성 검사, hfscheck, 백업 실패 등이 있습니다.

- Data Domain 시스템과 VDP 어플라이언스 간의 연결이 끊어진 경우 Data Domain 시스템 또는 VDP 어플라이언스를 업그레이드할 수 없습니다.

백업

백업 중에 VDP 어플라이언스는 백업 대상에 대한 백업 요청을 생성합니다. Data Domain 시스템을 대상으로 사용하는 옵션이 백업 요청에 포함되어 있으면 백업 데이터가 Data Domain 시스템에 저장됩니다. 메타데이터는 VDP 어플라이언스에 저장됩니다.

복구

데이터 복구 프로세스는 백업 관리자에게 드러나지 않게 처리됩니다. 백업 관리자는 현재 VDP 구축 환경에서 기본적으로 사용되는 것과 동일한 VDP 복구 프로세스를 사용합니다.

보안 - 암호화

Data Domain 시스템이 연결된 VDP 어플라이언스를 사용할 경우 두 가지 백업 데이터 스트림이 있을 수 있습니다. 백업 데이터가 VDP 어플라이언스에 기록되는 경우 백업 데이터는 전송 중 항상 압축되고 암호화됩니다. 백업 데이터가 Data Domain 시스템으로 라우팅되는 경우에는 네트워크를 통해 Data Domain 시스템으로 전송될 때 ddboost 유틸리티를 사용하여 백업 데이터를 암호화합니다.

데이터 마이그레이션

VDP 어플라이언스에서 직접 Data Domain 시스템으로 백업 데이터를 마이그레이션할 수 없습니다.

VM 또는 어플라이언스를 백업하기 위한 백업 타겟으로 VDP 어플라이언스 대신 Data Domain 시스템을 사용하려면 백업 작업을 편집하여 대상을 Data Domain 시스템으로 정의한 다음 Data Domain 시스템으로 백업을 수행합니다. 백업 타겟을 Data Domain 시스템으로 변경하면 그 다음 백업은 전체 백업으로 실행됩니다.

Data Domain 시스템으로 백업한 후에는 VDP 어플라이언스에서 이전 백업을 삭제할 수 있습니다. 백업을 수동으로 삭제하는 방법에 대한 자세한 내용은 [“백업 작업 삭제”](#)(115페이지) 섹션을 참조하십시오. 백업을 수동으로 삭제하지 않는 경우에는 별도의 작업 없이 만료됩니다.

통합 전 요구 사항

Data Domain 시스템과 VDP 어플라이언스를 통합하기 전에 다음 항목을 검토하십시오.

- [“네트워크 처리량”](#)(81페이지)
- [“네트워크 구성”](#)(81페이지)
- [“NTP 구성”](#)(81페이지)
- [“라이선스 등록”](#)(81페이지)
- [“포트 사용 및 방화벽 요구 사항”](#)(82페이지)
- [“용량”](#)(82페이지)
- [“Data Domain 시스템 스트림”](#)(82페이지)
- [“Data Domain과 함께 사용되는 기존 백업 제품”](#)(82페이지)

참고 이 섹션에서는 VDP 어플라이언스와 Data Domain 시스템이 이미 설치 및 구성되어 있다고 가정합니다.

네트워크 처리량

VDP에서는 VDP 어플라이언스와 Data Domain 시스템이 WAN(Wide Area Network)을 통해 연결할 수 있습니다. 이 구성을 사용하려면 먼저 Data Domain 시스템의 방화벽 포트 요구 사항을 확인하십시오. 자세한 내용은 “VDP 포트 사용”(185페이지)을 참조하십시오.

WAN을 통해 VDP 어플라이언스 복제를 사용하여 소스 VDP 어플라이언스 및 Data Domain 시스템에서 타겟 VDP 어플라이언스로 데이터를 복제할 수 있습니다(Data Domain 시스템이 연결된 경우).

Data Domain 시스템과 VDP 어플라이언스를 통합하기 전에, 사용할 수 있는 네트워크 대역폭이 충분한지 확인하십시오. Data Domain 시스템에서 사용할 수 있는 최대 처리량을 구현하려면(복구, 제로 레벨 백업 및 제로 레벨 백업 후의 후속 증분 백업의 경우) 네트워크 인프라스트럭처에서 Data Domain 시스템의 최대 처리량에 필요한 대역폭보다 많은 대역폭을 제공해야 합니다. 네트워크 처리량을 확인하려면 Data Domain 시스템에서 다음과 같이 `system show performance` 명령을 입력합니다.

```
system show performance [{hr | min | sec} [{hr | min | sec}]]
```

예를 들면 다음과 같습니다.

```
system show performance 24 hr 10 min
```

이 명령은 최근 24시간 동안의 시스템 성능을 10분 간격으로 표시합니다. 최소 간격은 1분입니다.

네트워크 구성

다음과 같은 네트워크 구성을 설정(또는 확인)하십시오.

- Data Domain 시스템에 FQDN(Fully Qualified Domain Name)을 할당합니다.
- Data Domain 시스템을 등록할 때는 IP 주소가 아니라 FQDN을 사용합니다. IP 주소를 사용하면 최적화된 데이터 중복 제거 트래픽을 등록된 인터페이스를 통해 배타적으로 라우팅하는 기능이 제한될 수 있습니다.
- Data Domain 시스템의 DNS가 올바르게 구성되어 있는지 확인합니다.
- 다음 시스템 간에 정방향 및 역방향 DNS 조회 기능이 작동하는지 확인합니다.
 - VDP 어플라이언스
 - Data Domain 시스템
 - 백업 및 복구 클라이언트
 - vCenter Server
 - vSphere 호스트
- 호스트 파일을 사용하여 라우팅이 불가능한 IP 주소로 연결되는 호스트 이름을 확인합니다.
- 대체 또는 로컬 IP 인터페이스에 연결된 보조 호스트 이름을 생성하지 마십시오.

NTP 구성

VDP 어플라이언스, vCenter Server, vSphere 호스트 및 Data Domain 시스템이 동일한 NTP(Network Time Protocol) 서버를 사용하도록 구성하십시오.

라이선스 등록

운영 환경이 아래 표 9-12의 라이선스 요구 사항을 충족하는지 확인하십시오.

표 9-12. 라이선스 요구 사항

제품	라이선스 요구 사항
VDP 어플라이언스	VDP 어플라이언스를 사용하려면 유효한 vSphere 호스트 라이선스(최소 Essentials Plus)가 필요합니다.
Data Domain 시스템	Data Domain 시스템에 DD Boost 라이선스가 설치되어 있어야 합니다.

포트 사용 및 방화벽 요구 사항

VDP 어플라이언스와 Data Domain 시스템 간의 통신을 가능하게 하려면 “VDP 포트 사용”(185페이지)에 나온 포트 사용 및 방화벽 요구 사항을 검토하고 구현하십시오.

용량

Data Domain 시스템 및 VDP 어플라이언스에 저장할 데이터 양을 계산할 때 백업 스토리지 요구 사항을 세심하게 평가하십시오. 다른 모든 서버에서 Data Domain 시스템으로 전송되는 데이터를 사용한 예상치를 포함하십시오.

Data Domain 시스템이 최대 스토리지 용량에 도달한 경우 용량이 추가되거나 이전 백업이 삭제 또는 만료되기 전에는 더 이상 Data Domain 시스템에 백업되지 않습니다.

“VDP 어플라이언스에서 Data Domain 모니터링”(92페이지)에 용량 모니터링 방법이 자세히 나와 있습니다.

Data Domain 시스템 스트림

각 Data Domain 시스템에는 성능 저하 없이 동시에 유지할 수 있는 최대 연결 및 데이터 스트림 수에 대한 유동적 제한이 있습니다. 스트림 수는 Data Domain 시스템 모델에 따라 달라집니다. 예를 들어 DD990은 540개의 백업 스트림을 지원할 수 있지만 DD620은 20개의 백업 스트림을 지원합니다.

최대 스트림 값 변경

기본적으로 VDP 어플라이언스는 최대 스트림 값으로 16을 사용하도록 구성됩니다.

VDP 어플라이언스에서 Data Domain 시스템과 관련된 스트림 수를 수정해야 하는 경우 다음 단계를 수행하십시오. 이러한 단계에 따라 변경한 사항은 이후에 Data Domain 시스템을 편집하거나 VDP 어플라이언스에 추가할 때만 적용됩니다.

- 1 VDP 어플라이언스의 명령줄로 이동하고(어플라이언스의 터미널 또는 SSH/Putty 사용) 다음 명령을 입력합니다.

```
cd /usr/local/vdr/etc/
```

- 2 텍스트 편집기를 사용하여 `vdp-options.properties` 파일을 편집합니다.

- 3 `com.vmware.vdp.option.datadomain.maxstreamsoverride=num` 필드를 삽입합니다. 여기서 `num`은 Data Domain 시스템의 최대 스트림 수입니다.

- 4 수정된 파일을 저장합니다.

- 5 Data Domain 시스템을 추가 또는 편집합니다. 5분 동안 적절한 프로세스가 실행될 수 있게 합니다.

이제 `ddrmaint read-ddr-info` 파일에 사용자가 구성한 "max-streams" 속성이 포함되어야 합니다.

Data Domain과 함께 사용되는 기존 백업 제품

Data Domain 시스템에서 다른 타사 백업 및 아카이빙 소프트웨어를 사용할 수 있습니다. VDP 어플라이언스에서는 Data Domain 시스템을 독점 소유한다고 가정하지 않습니다. 다른 소프트웨어 제품과 시스템을 공유하는 경우 적절한 사이징 계산이 필요합니다. VDP 어플라이언스는 기본적으로 제공되는 Data Domain 시스템 스냅샷 및 복제 기능을 사용하지 않습니다.

복제는 DD Boost SDK 라이브러리를 통해 복사와 클론 생성 방법을 사용하여 수행됩니다. 하지만 다른 타사 제품은 기본적으로 제공되는 Data Domain 시스템 스냅샷 및 복제 기능을 사용할 수 있습니다. 이 경우 전체 Data Domain 시스템의 스냅샷이나 전체 Data Domain 시스템의 복제에 VDP 어플라이언스 데이터가 포함됩니다.

VDP 통합을 위한 Data Domain 시스템 준비

VDP와 Data Domain 시스템의 통합을 지원하려면 운영 환경에서 표 9-13에 나열된 Data Domain 시스템 요구 사항을 충족하는지 확인하십시오.

표 9-13. Data Domain 시스템 요구 사항

Data Domain 기능 또는 사양	VDP 어플라이언스와 함께 사용하기 위한 요구 사항
DD OS(Data Domain Operating System)	VDP 통합에는 DD OS 5.4.0.8 또는 DD OS 5.5.x 이상이 필요합니다.
DD Boost	VDP 통합에는 DD Boost 2.6.x가 필요합니다. DD Boost 소프트웨어를 사용하면 Data Domain 시스템에서 테이프를 에뮬레이트하지 않아도 백업 서버가 스토리지 시스템과 통신할 수 있습니다. DD Boost에는 백업 서버에서 실행되는 구성 요소와 Data Domain 시스템에서 실행되는 구성 요소가 있습니다. 백업 서버에서 실행되는 구성 요소(DD Boost 라이브러리)는 VDP 어플라이언스에 통합됩니다. DD Boost 소프트웨어는 선택적으로 사용할 수 있는 제품으로, Data Domain 시스템에 사용하려면 별도의 라이선스가 필요합니다.
Data Domain 디바이스 유형	VDP 어플라이언스는 지원되는 DD OS 버전을 실행하는 모든 Data Domain 시스템을 지원합니다.
DD Boost 사용자 계정	DD Boost 라이브러리는 Data Domain 시스템에 생성된 고유한 로그인 계정 이름을 사용합니다. 이 계정 이름을 DD Boost 계정이라고 합니다. 각 Data Domain 시스템당 하나의 DD Boost 계정만 생성할 수 있습니다. 이 계정의 이름을 바꾸거나 암호를 변경한 경우 Data Domain 구성 옵션을 편집하여 VDP 어플라이언스에서 변경 사항을 즉시 업데이트해야 합니다. DD Boost 계정 정보를 업데이트하지 않으면 무결성 검사 오류가 발생하거나 백업/복구 문제가 발생할 수 있습니다. DD Boost 계정에는 관리자 권한이 있어야 합니다.

Data Domain 시스템을 VDP Configuration에 추가하려면 먼저 DD Boost를 활성화하고 백업, 복구 및 복제(적용 가능한 경우)를 위해 Data Domain 시스템에 액세스할 때 사용할 VDP 어플라이언스용 DD Boost 사용자 계정을 생성하여 Data Domain 시스템을 준비해야 합니다.

Data Domain 시스템을 준비하려면

- 1 CLI에 관리 사용자로 로그인하고 다음 명령을 입력하여 Data Domain 시스템에서 DD Boost를 비활성화합니다.

```
ddboost disable
```

- 2 DD Boost 계정 및 암호를 생성합니다.

- a 다음 명령을 입력하여 관리자 권한이 있는 DD Boost 계정을 생성합니다.

```
user add USER role admin
```

여기서 USER는 새 계정의 사용자 이름입니다.

- b 다음 명령을 입력하여 새 계정을 DD Boost 사용자로 설정합니다.

```
ddboost set user-name USER
```

여기서 USER는 계정의 사용자 이름입니다.

- 3 다음 명령을 입력해 DD Boost를 활성화하여 변경 내용을 적용합니다.

```
ddboost enable
```

중요 DD Boost 계정 이름 또는 암호를 변경한 경우 VDP 구성 유틸리티에서 Data Domain 시스템 구성을 편집해야 합니다. 그렇지 않으면 모든 백업, 복구 및 유지 보수 작업이 실패합니다.

Data Domain 시스템 추가

Data Domain 시스템은 DD OS 소프트웨어를 통해 데이터 중복 제거를 수행합니다. Data Domain 시스템을 백업 타겟으로 선택하면 백업 데이터가 Data Domain 시스템으로 전송됩니다. Data Domain 시스템은 하나만 구성할 수 있습니다.

절차

- 1 다음 URL을 사용하여 VDP 구성 유틸리티에 로그인합니다.

https:<IP_address_VDP_appliance>:8543/vdp-configure/

- 2 스토리지 탭을 클릭합니다.

스토리지 요약 정보에 Data Domain 시스템 및 각 데이터 저장소에 대한 총 가용 스토리지 및 가용 용량에 대한 통계가 표시됩니다.

- 3 작업 목록에서 **Data Domain 추가**를 선택합니다.

호스트 구성 대화상자가 표시됩니다.

- 4 Data Domain 시스템 정보를 지정합니다.

- a **Data Domain FQDN 또는 IP** 상자에 추가할 Data Domain 시스템의 FQDN 또는 IP 주소를 입력합니다.

참고 대체 또는 로컬 IP 인터페이스와 연결된 IP 주소 또는 보조 호스트 이름은 사용하지 마십시오. 이 경우 최적화된 중복 제거 트래픽을 라우팅하는 VDP 어플라이언스의 기능이 제한될 수 있습니다.

- b **DDBoost 사용자 이름** 상자에 백업, 복구 및 복제용 Data Domain 시스템에 액세스하기 위해 사용할 VDP에 대한 DD Boost 계정 이름을 입력합니다.
- c **암호** 상자에 VDP에서 백업, 복구 및 복제를 위해 Data Domain 시스템에 액세스할 때 사용할 계정의 암호를 입력합니다.
- d **암호 확인** 상자에 암호를 한 번 더 입력하여 확인합니다.
- e **체크포인트 복제 활성화 확인란**을 클릭하여 체크포인트 백업 지원을 설정합니다. 이 경우 VDP 체크포인트를 Data Domain 시스템(DD OS 5.3 이상 사용)에 저장할 수 있습니다. 나중에 재해 복구가 필요한 경우 이러한 체크포인트가 사용됩니다.

- 5 SNMP를 구성하려면 다음을 클릭합니다.

SNMP 대화상자가 표시됩니다. VDP와 Data Domain 시스템의 통합에 맞게 구성할 수 있는 SNMP 옵션에는 다음이 포함됩니다.

- **Getter/Setter 포트 번호** 입력란에는 SNMP 객체를 수신하고 설정할 Data Domain 시스템의 포트가 나와 있습니다. 기본값은 161입니다.
- **SNMP 커뮤니티 문자열** 입력란에는 Data Domain 시스템에 대한 읽기 전용 액세스를 위해 VDP에서 사용하는 커뮤니티 문자열이 나와 있습니다.
- **트랩 포트 번호** 입력란에는 트랩 포트가 나와 있습니다. 기본값은 163입니다.

- 6 다음을 클릭합니다.

완료 준비 대화상자가 나타납니다.

- 7 **추가**를 클릭하여 Data Domain 구성을 저장합니다.

Data Domain 추가 작업이 성공하면 다음 UI 변경 사항이 발생합니다.

- 시스템에서 새 체크포인트를 생성하는데, 이는 약 10분 정도 소요됩니다.
- Data Domain 정보는 VDP 어플라이언스의 다음 위치에 나타납니다.
 - **백업 탭**: 새 백업 작업 생성 마법사에서 스토리지 타겟으로 Data Domain 시스템을 사용할 수 있습니다.
 - **복구 탭**: 백업 복구 마법사의 이름 옆에 Data Domain이 표시됩니다.

- **보고서 탭:** Data Domain 시스템에 대한 백업 상태 보고서를 제공합니다.
- **스토리지 요약:** Data Domain에 대한 총 가용 스토리지 및 가용 용량에 대한 통계가 표시됩니다. 자세한 내용은 [“스토리지 구성 보기”](#)(74페이지) 섹션을 참조하십시오.
- **e-메일 보고:** Data Domain 구성에 대한 요약이 표시됩니다.

참고 Data Domain 시스템을 VDP 구성에 추가하면 VDP 어플라이언스에서 Data Domain 시스템에 VDP 어플라이언스에 대한 MTree를 만듭니다. MTree는 DD Boost 경로 내에 만들어진 디렉토리를 참조합니다. Data Domain 시스템은 최대 100개의 MTree를 지원합니다. 이 제한에 도달하면 VDP 구성에 Data Domain 시스템을 추가할 수 없습니다.

Data Domain 시스템 편집

- 1 다음 URL을 사용하여 VDP 구성 유틸리티에 로그인합니다.

`https:<IP_address_VDP_appliance>:8543/vdp-configure/`

- 2 **스토리지 탭**을 클릭합니다.

스토리지 요약 정보에 Data Domain 및 각 데이터 저장소에 대한 총 가용 스토리지 및 가용 용량에 대한 통계가 표시됩니다.

- 3 **작업 목록**에서 **Data Domain 편집**을 선택합니다.

호스트 구성 대화상자가 표시됩니다.

- 4 Data Domain 시스템에 대한 설정을 필요에 따라 편집합니다. [“Data Domain 시스템 추가”](#)(84페이지)에 대화상자의 각 설정에 대한 세부 정보가 나와 있습니다.

- 5 다음을 클릭합니다.

- 6 편집이 완료되면 **마침**을 클릭합니다.

참고 Data Domain 시스템 호스트 이름, DD Boost 사용자 이름 또는 DD Boost 암호를 편집한 경우 시스템에서 자동으로 새 체크포인트를 생성하는데, 이는 약 10분 정도 소요됩니다. 체크포인트에 대한 내용은 [“어플라이언스 롤백”](#)(41페이지)에 나와 있습니다.

참고 기간이 지난 Data Domain 시스템 이름 또는 DD Boost 정보를 사용하여 체크포인트로 롤백하는 경우 롤백이 실패합니다.

VDP 어플라이언스에서 Data Domain 시스템 삭제

VDP 어플라이언스에서 Data Domain 시스템을 삭제하기 전에 다음 사항에 유의하십시오.

- vSphere Web Client에서 VDP 플러그인을 사용하여 Data Domain에 저장된 모든 복구 시점을 삭제해야 합니다.
- Data Domain 시스템에 백업 작업이 있으면 안 됩니다. Data Domain 시스템이 대상으로 구성된 위치에 백업 작업이 존재하는 경우 백업 작업을 편집하여 새 대상을 설정하거나 해당 백업 작업을 삭제해야 합니다.
- Best Practice로, 복구 시점을 검사하고 백업 작업을 검증한 후 VDP 어플라이언스의 **구성 탭**에서 무결성 검사를 실행합니다.
- 명령줄 인터페이스를 사용하여 VDP에서 Data Domain을 제거하십시오. 아래에서 자세한 지침을 참조하십시오.
- Data Domain 시스템을 삭제한 후에는 VDP 사용자 인터페이스에서 무결성 검사를 또 한번 실행하여 Data Domain 시스템이 잘못되었는지 확인하십시오.

참고 VMware 기술 자료 문서 2063806에 Data Domain 시스템 삭제에 대한 정보가 나와 있습니다. 이 문서는 내부 문서입니다. 기술 지원부에 문의하십시오.

절차

- 1 Data Domain 시스템을 삭제하기 전에 Data Domain 시스템에 저장된 복구 시점을 모두 삭제합니다. vSphere Web Client를 사용하여 복구 시점을 삭제합니다.
 - a VDP 플러그인의 복구 탭으로 이동합니다.
 - b 탐색 모음에서 수동 복구 탭을 선택합니다.
 - c Data Domain 시스템에 백업한 클라이언트의 경우 Data Domain 서버에 저장되었다고 위치가 표시된 복구 시점을 모두 제거합니다.
- 2 Data Domain 시스템을 대상으로 사용하는 백업 작업이 없는지 확인합니다. Data Domain 시스템이 대상으로 설정된 백업 작업이 존재하는 경우 백업 작업을 편집하여 새 대상을 설정하거나 백업 작업을 삭제해야 합니다.
- 3 Best Practice로, 복구 시점을 검사하고 백업 작업을 검증한 후 VDP 플러그인의 구성 탭에서 무결성 검사를 실행합니다.
- 4 무결성 검사와 무결성 검사에 대한 검증이 완료되면 VDP 어플라이언스에서 Data Domain 시스템을 제거할 수 있습니다. 명령줄을 사용합니다.
 - a VDP 어플라이언스로 SSH 또는 Putty를 수행합니다.
 - b `status.dpn` 명령을 실행하고 `Last checkpoint` 및 `Last hfscheck`가 완료되었는지 확인합니다. 그렇지 않은 경우 완료되었다고 표시될 때까지 이 단계를 반복합니다.
 - c `mccli server show-prop` 명령을 실행합니다. 이 명령은 다음 출력과 유사한 결과를 표시합니다.

Attribute	Value
State	Full Access
Active sessions	0
Total capacity	575.9 GB
Capacity used	0 bytes
Server utilization	0.0%
Bytes protected	0 bytes
Bytes protected quota	Not configured
License expiration	Never
Time since Server initialization	1 days 20h:58m
Last checkpoint	2014-10-10 09:03:48 MDT
Last validated checkpoint	2014-10-09 09:02:16 MDT
System Name	gs-pod187.test.domain
System ID	1381255529@00:50:56:86:46:10
HFSAddr	gs-pod187.test.domain
HFSPort	27000

System ID에는 숫자 다음에 @ 기호, 그리고 그 다음에는 VDP 어플라이언스의 MAC 주소가 포함됩니다. @ 기호 앞의 숫자를 확인하십시오. Data Domain 시스템에서는 이 숫자를 DPN ID로 참조합니다.

- 5 다음 명령을 실행합니다.

```
ddrmaint has-backups -dpnid=num -ddr-server=DDRSERVER | grep 'hasbackups'
```

여기서 `num`은 **c 단계**에서 확인한 DPN ID이고, `DDRSERVER`는 DDR 서버의 호스트 이름 또는 IP 주소입니다. `grep` 명령의 작은따옴표와 단어 `hasbackups` 사이에 공백이 있다는 점에 유의하십시오.

이 명령은 다음 결과 중 하나를 표시합니다.

```
hasbackups="true"
```

또는

```
hasbackups="false"
```

- 6 반환된 정보가 `hasbackups='true'` 인 경우 **1 단계**와 **2 단계**를 반복해야 합니다. **1 단계**와 **2 단계**를 반복 (또는 해당 단계가 완료되었는지 확인)한 후 **5 단계**를 반복합니다.

- 7 **5 단계**에서 여전히 'hasbackups=true'가 표시되면 **a 단계**를 계속합니다. 그렇지 않으면 **11 단계**를 실행해야 합니다.
- VDP UI를 사용하여 Data Domain 시스템에서 백업 제거를 시도했는데도 Data Domain 시스템에서 계속 백업 데이터가 있다고 표시되는 경우 Data Domain 데이터 파티션을 Linux VM에 마운트하여 데이터 디렉토리를 정리해야 합니다. Linux VM을 사용할 수 없는 경우 다음 단계에 VDP 어플라이언스를 사용할 수 있습니다.
- 기본적으로 Data Domain 시스템의 백업에 대한 데이터는 모두 단일 LSU(Logical Storage Unit)에 저장됩니다. VDP의 LSU는 이름이 Avamar-<DPNID>이고 /data/coll 아래에 있습니다.
- Data Domain 운영 체제 인터페이스에서 파일 시스템에 액세스할 수 없는 경우에는 LSU에 대한 원격 액세스 권한을 부여해야 합니다. 이렇게 하려면 다음 단계에 따라 Data Domain 시스템에 원격으로 액세스해야 합니다.
- a Data Domain 시스템으로 Putty 또는 SSH 수행
 - b `nfs add /data/coll <IP of Linux VM>` 명령을 실행합니다.
이 명령은 NFS export for "/data/coll" added라는 결과를 반환해야 합니다.
예상한 결과가 반환되지 않는 경우 `nfs help`를 입력하여 명령의 man 페이지를 표시합니다. 예상한 결과가 반환되는 경우에는 SSH 또는 Putty 세션을 종료합니다.
 - c **b 단계**에서 사용된 Linux VM에 루트 사용자로 Putty 또는 SSH합니다.
 - d `mkdir /mnt/DataDomain01` 명령을 실행합니다.
 - e `mount <IP of DD>:/data/coll /mnt/DataDomain01` 명령을 실행합니다.
 - f `ls -ltr /mnt/DataDomain01/avamar-<DPNID>` 명령을 실행합니다. 여기서 DPNID는 **c 단계**에서 확인한 값입니다. 출력에는 VDP 백업이 저장된 하위 디렉토리가 표시되어야 합니다.
 - g `rm -rf /mnt/DataDomain01/avamar-<DPNID>/*` 명령을 실행합니다. 여기서 DPNID는 **c 단계**에서 확인한 값입니다. 이 명령을 실행하면 VDP 백업에서 모든 데이터가 제거됩니다.
- 8 **f 단계**를 반복하여 데이터가 모두 제거되었는지 확인합니다.
- 9 Linux 가상 머신을 종료합니다.
- 10 VDP 어플라이언스로 Putty 또는 SSH를 수행합니다.
- 11 `mccli dd delete --name=<DD IP or hostname> --force=true` 명령을 실행합니다.
- 12 Data Domain 시스템을 삭제한 후 VDP UI에서 무결성 검사를 다시 실행합니다. Data Domain 정보가 있는 이전 체크포인트는 이제 유효하지 않습니다.

VDP 및 Data Domain에서 백업

다음 항목에서는 VDP 및 Data Domain 시스템 백업에 대해 설명합니다.

- VDP 및 Data Domain 시스템에서 백업이 작동하는 방식
- 백업에 대한 Data Domain 타겟 선택

VDP 및 Data Domain에서 백업이 작동하는 방식

백업 중에 VDP 어플라이언스는 vCenter Server에 백업 요청을 보냅니다. Data Domain 시스템을 타겟으로 사용하는 옵션이 백업 요청에 포함되어 있으면 백업 데이터는 Data Domain 시스템에 저장되고 메타데이터는 VDP 어플라이언스에 저장됩니다.

다음 항목에서는 VDP 및 Data Domain에서 백업이 작동하는 방식을 자세히 설명합니다.

백업 데이터가 저장되는 위치

백업에 대한 모든 데이터는 단일 Data Domain 시스템에서 단일 전용 MTree 아래에 저장됩니다.

VDP 어플라이언스가 백업 데이터를 관리하는 방법

백업 중에 VDP 어플라이언스는 백업에 대한 메타데이터를 클라이언트에서 VDP 데이터 파티션으로 보냅니다. 이 프로세스를 통해 VDP 어플라이언스는 데이터가 Data Domain 시스템에 저장되어 있더라도 백업을 관리할 수 있습니다.

VDP 어플라이언스는 Data Domain 시스템에 파일의 원래 경로와 파일 이름을 저장하지 않습니다. 대신 VDP 어플라이언스는 Data Domain 시스템에서 고유한 파일 이름을 사용합니다.

지원되는 백업 유형

동일한 대상(VDP 어플라이언스 또는 Data Domain 시스템)의 클라이언트에 대해 모든 백업 유형(전체, 차등, 증분)을 저장하십시오. 백업 유형을 여러 대상에 분산시키면 안 됩니다. 예를 들어 클라이언트의 초기 전체 백업은 VDP 어플라이언스에 저장하고 후속 차등 백업은 Data Domain 시스템에 저장하는 방식은 사용하지 마십시오.

백업 취소 및 삭제

진행 중인 백업을 취소하는 경우 VDP 어플라이언스는 Data Domain 시스템에 기록된 백업 데이터를 VDP 어플라이언스 가비지 수집 프로세스의 다음 주기 동안 삭제합니다.

VDP에서 백업을 삭제하는 경우에는 VDP 가비지 수집 프로세스의 다음 주기 동안 Data Domain 시스템에서 백업이 삭제됩니다.

“[백업 작업 삭제](#)”(115페이지)에는 백업을 취소하거나 삭제하는 방법에 대한 지침이 나와 있습니다.

백업에 대한 Data Domain 타겟 선택

VDP 어플라이언스와 Data Domain 시스템이 통합된 후에는 [그림 9-6](#)에 나온 대로 새 백업 작업 생성 워크플로우에서 Data Domain 스토리지를 "대상"으로 사용하는 옵션이 VDP 어플라이언스에 대한 백업 타겟에 제공됩니다.

새 백업 작업 생성

<ul style="list-style-type: none"> ✓ 1 작업 유형 ✓ 2 데이터 유형 ✓ 3 백업 소스 <li style="background-color: #005596; color: white; padding: 2px 5px;">4 대상 5 스케줄 6 보존 정책 7 작업 이름 8 완료 준비 	<p>대상</p> <p>이 작업에 대한 백업이 상주하게 될 위치를 선택하십시오.</p> <hr/> <p><input checked="" type="radio"/> VDP 어플라이언스 스토리지 사용 어플라이언스로 정의된 스토리지에 백업을 저장합니다.</p> <p><input type="radio"/> Data Domain 스토리지 사용 ⓘ Data Domain 스토리지에 백업을 저장합니다. 10.246.253.135</p>
---	--

그림 9-6. 새 백업 작업 생성 마법사 - 대상 페이지

백업 작업 편집 마법사를 사용하여 백업 작업의 대상을 변경할 수 있습니다. 백업 작업을 편집하는 방법에 대한 자세한 내용은 “[백업 작업 편집](#)”(115페이지) 섹션을 참조하십시오.

참고 백업 작업의 대상을 수정하면 다음에 수행되는 백업은 전체 백업이 됩니다. 새 대상에는 이전의 전체 백업 데이터가 저장되지 않습니다.

복제 제어

Data Domain 시스템이 연결된 VDP 어플라이언스에서 백업 데이터를 복제하는 경우 Data Domain 시스템 간에 복제가 수행됩니다. 그러나 복제 작업은 VDP 사용자 인터페이스를 사용하여 구성합니다.

VDP 어플라이언스에서 복제를 구성하고 모니터링합니다. 또한 DD Boost 작업을 확인하여 Data Domain 시스템을 통해 복제 작업을 모니터링할 수도 있습니다. 이 작업을 모니터링하는 방법에 대한 지침은 *Data Domain 운영 체제 관리 가이드*를 참조하십시오.

VDP 어플라이언스에서 백업된 데이터의 복제를 Data Domain 복제 기능을 사용하여 시작하지 마십시오. Data Domain 복제를 사용하는 경우 VDP 어플라이언스에 저장된 메타데이터가 복제되지 않았으므로 복제된 데이터에서 관련 VDP 어플라이언스를 참조하지 않습니다.

복제 데이터 흐름

VDP는 데이터를 Data Domain 시스템 간에 직접 복제합니다. 복제 프로세스에서는 복제할 각 백업을 검토하며, 백업 데이터를 Data Domain 시스템에 저장하기로 결정한 경우에는 DD Boost를 통해 소스 Data Domain 시스템에서 타겟 Data Domain 시스템으로 데이터를 복제하는 요청을 실행합니다. 이 경우 Data Domain 시스템에서 데이터의 복제를 담당합니다. 복제되는 각 백업에 대해 이에 대한 분석이 수행됩니다.

복제 스케줄

Data Domain 시스템에서 VDP 데이터 복제는 VDP 복제 스케줄에 따라 수행됩니다. VDP 어플라이언스의 데이터 복제와 별도로 Data Domain 시스템의 데이터 복제를 예약해서는 안 됩니다.

복제 구성

Data Domain 시스템을 VDP의 백업 타겟으로 사용하는 경우 복제를 구성하려면 vSphere Web Client에서 VDP 플러그인을 사용합니다.

VDP 복제 구성에 대한 자세한 내용은 [“복제”](#)(133페이지) 섹션을 참조하십시오.

참고 복제할 때 소스가 Data Domain 시스템이 연결된 VDP 어플라이언스인 경우 타겟(Avamar 서버이든 VDP 어플라이언스이든)에도 Data Domain 시스템이 연결되어 있어야 합니다.

VDP를 사용한 복제 모니터링

VDP 어플라이언스를 사용하여 Data Domain 시스템과 관련된 복제 작업을 비롯한 복제 작업을 모니터링하려면 다음 단계를 수행하십시오.

- 1 vSphere Web Client에서 vSphere Data Protection 플러그인에 로그인합니다.
- 2 **복제** 탭을 클릭합니다.
 - **복제** 탭에는 모든 복제 작업, 마지막 실행 시간 및 예약된 다음 실행 시간이 표시됩니다.
 - 복제 작업을 선택하면 복제 작업 세부 정보 프레임에 포함된 대상 서버와 클라이언트가 표시됩니다.
 - 복제 열을 선택하면 **보고서** 탭에 복제 작업과 보호되는 각 클라이언트의 마지막 복제 실행 시간이 표시됩니다.

서버 유지 보수 작업 모니터링

VDP 어플라이언스에서는 Data Domain 시스템의 백업 데이터에 대해 VDP 무결성 검사, 체크포인트, 롤백, 가비지 수집 및 보안 백업 삭제를 비롯한 시스템 유지 보수 작업을 수행합니다.

ddrmaint 유틸리티는 Data Domain 시스템에서 VDP 어플라이언스에 대해 필요한 작업을 모두 구현합니다. ddrmaint 유틸리티는 VDP 어플라이언스에서 수행되는 모든 유지 보수 작업을 ddrmaint.log 파일에 기록합니다. 이 로그 파일은 /usr/local/avamar/var/ddrmaintlogs 디렉토리에서 찾을 수 있습니다.

ddrmaint.log 파일의 크기가 25MB에 도달하면 기존 로그 버전이 순환됩니다. 기존 ddrmaint.log 파일의 이름이 ddrmaint.log.1로 변경되고 새 ddrmaint.log 파일이 생성됩니다. ddrmaint.log.X의 기존 복제본도 로그 카운터가 1씩 증가합니다(예: ddrmaint.log.1은 ddrmaint.log.2로 마이그레이션됨).

Data Domain 시스템에서 Avamar 체크포인트 백업 복구

Data Domain 시스템에서 VDP 체크포인트 백업을 생성한 경우 원래 VDP 어플라이언스 실패 시 체크포인트를 새 VDP 어플라이언스로 복구할 수 있습니다.

복구 작업을 위한 조건

“[체크포인트 복구 수행](#)”(90페이지) 섹션의 절차에서는 다음과 같은 조건에 해당되는 경우에 체크포인트 복구를 수행하는 방법을 설명합니다.

- Data Domain 시스템 타겟에 VDP 어플라이언스에 대한 유효한 체크포인트가 있습니다.
- 실패한 VDP 어플라이언스가 교체되었습니다.
- 교체용 VDP 어플라이언스가 백업 데이터 또는 메타데이터가 없는 새 어플라이언스입니다.
- 교체용 VDP 어플라이언스의 크기가 원래 VDP 어플라이언스보다 크거나 같습니다.
- 교체용 VDP 어플라이언스에 원래 VDP 어플라이언스와 동일한 수의 데이터 파티션이 있어야 합니다.
- 교체용 VDP 어플라이언스에 원래 VDP 어플라이언스와 동일한 호스트 이름과 IP 주소가 있어야 합니다.

체크포인트 복구 수행

Data Domain 시스템에서 새 VDP 어플라이언스로 체크포인트를 복구하려면 다음과 같이 하십시오.

- 1 VDP 어플라이언스에 루트로 로그인하고 CLI 프롬프트에서 다음 명령을 입력하여 복구할 수 있는 체크포인트를 쿼리합니다.

```
ddrmaint cp-backup-list --full --ddr-server=Data_Domain_system --ddr-user=DD_Boost_user_name
--ddr-password=DD_Boost_user_password
```

여기서:

- *Data_Domain_system*은 VDP 어플라이언스 체크포인트 백업이 있는 Data Domain 시스템입니다.
- *DD_Boost_user_name*은 VDP 및 Data Domain 시스템 통합에 사용된 DD Boost 사용자 계정입니다.
- *DD_Boost_user_password*는 VDP 및 Data Domain 시스템 통합에 사용된 DD Boost 사용자 계정 암호입니다.

다음 예와 비슷한 내용이 출력됩니다.

```
===== Checkpoint =====
VDP Advanced Name: a4dpe223d
VDP Advanced MTree/LSU: avamar-1346892530
Data Domain 시스템 이름 : griffin-dd10.asl.lab.emc.com
VDP Advanced Client Path: /MC_SYSTEM/avamar-1346892530
VDP Advanced Client ID: 8b75468f70dc8ff0fa2e5118cec8ecddf7fcece
Checkpoint Name: cp.20140919184604
Checkpoint Backup Date: 2014-09-19 11:51:12
Data Partitions: 6
Attached Data Domain systems: griffin-dd10.asl.lab.emc.com
```

- 2 Data Domain 시스템에 저장된 체크포인트에서 VDP 어플라이언스에 저장된 백업을 `cprestore` 명령을 사용하여 복구합니다(기본 백업 타겟 Data Domain 시스템의 자격 증명과 Data Domain 서버 이름 필요). `cprestore` 명령은 복구 작업에 사용됩니다. `cprestore` 명령은 다음 작업을 수행합니다.

- Data Domain 시스템에 NFS 내보내기를 생성합니다.
- Data Domain NFS 내보내기를 VDP 어플라이언스에 마운트합니다.
- VDP 어플라이언스에 있는 필요한 백업 파일을 Data Domain 시스템의 백업 체크포인트로부터 각 데이터 파티션의 해당하는 VDP 어플라이언스 체크포인트 디렉토리로 복사합니다.
- NFS 마운트 및 내보내기를 취소합니다.

Data Domain 시스템의 백업을 복구하려면 VDP 어플라이언스에서 다음 명령을 입력하십시오.

```
/usr/local/avamar/bin/cprestore --hfscreatetime=VDP_ID --ddr-server=Data_Domain_system
--ddr-user=DD_Boost_user_name --cptag=Checkpoint_name
```

여기서:

- `VDP_ID`는 1 단계의 출력에서 확인됩니다. VDP 어플라이언스의 `MTree/LSU:avamar-1346892530` 필드에서 `VDP_ID`는 1346892530입니다.
 - `Data_Domain_system`은 VDP 어플라이언스 체크포인트 백업이 있는 Data Domain 시스템입니다. 이전 체크포인트 출력 예에서 이 값은 `griffin-dd10.as1.lab.emc.com`입니다.
 - `DD_Boost_user_name`은 VDP 및 Data Domain 시스템 통합에 사용된 DD Boost 사용자 계정입니다. 이전 체크포인트 출력 예에서 이 값은 `VDP`입니다.
 - `Checkpoint_name`은 체크포인트의 이름입니다. 이전 체크포인트 출력 예에서 이 값은 `cp.20140919184604`입니다.
- 3 다음 명령을 입력하여 VDP 어플라이언스를 중지합니다.
- dpnctl stop**
- "Do you wish to shut down the local instance of EMS?"라는 확인 메시지가 나타납니다. **Y**를 입력합니다.
- 4 롤백을 시작하려면 다음 명령을 입력합니다.
- dpnctl start --force_rollback**
- 어플라이언스가 종료되었다는 메시지가 나타납니다. 선택 목록도 나타납니다.
- 5 옵션 3, "롤백할 특정 체크포인트 선택"을 선택합니다.
- 롤백이 완료될 때까지 기다립니다. VDP 어플라이언스에 있는 데이터 양에 따라 롤백에 최대 1시간까지 걸릴 수 있습니다. 롤백이 완료되면 명령 프롬프트가 반환됩니다.
- 6 롤백 중 생성된 사용자 정의 임시 파일을 열고 롤백이 오류 없이 완료되었는지 확인합니다.
- 7 내부 프록시가 활성화되어 있는 경우 VDP 구성 유틸리티를 사용하여 먼저 내부 프록시를 비활성화한 후에 다시 활성화하십시오.
- 8 분리된 프록시 즉, 오래된 VDP 어플라이언스에 구축된 외부 프록시가 있는 경우 VDP 구성 유틸리티를 사용하여 다음 단계를 수행합니다.
- a 분리된 프록시를 삭제합니다.
 - b VDP 어플라이언스의 암호를 변경합니다.
 - c 외부 프록시를 추가합니다.
- 9 VDP 어플라이언스에서 새 체크포인트를 생성합니다.
- a VDP 구성 탭에서 무결성 검사 실행을 선택하여 새 체크포인트를 생성합니다.
 - b 체크포인트가 시작되었으면 확인을 클릭합니다.

VDP 어플라이언스에서 Data Domain 모니터링

VDP 어플라이언스에 연결된 Data Domain 시스템의 용량에 대한 개괄적인 정보를 검토하려면 vSphere Web Client나 VDP 구성 유틸리티를 사용합니다.

- vSphere Web Client에서 VDP 플러그인을 열고 구성 탭으로 이동하여 Data Domain 시스템에 대한 용량 요약 을 봅니다.
- VDP 구성 유틸리티에서 스토리지 탭을 열고 Data Domain 시스템에 대한 스토리지 요약 정보를 봅니다.

참고 페이지에서 데이터를 새로 고치려면 스토리지 요약 옆에 있는 새로 고침 아이콘을 클릭합니다.

Data Domain 시스템이 용량 한도에 도달하면 “전체 Data Domain 시스템에서 스토리지 재확보”(93페이지) 섹션의 지침에 따라 디바이스에서 공간을 재확보할 수 있습니다.

표 9-14. Data Domain의 용량 임계값

임계값	값	동작
용량 경고	80%	VDP에서 경고 이벤트를 실행합니다.
용량 오류	95%	용량이 95% 이상 차 있으면 백업 작업을 위한 작업이 vCenter에서 생성되지 않습니다.
상태 점검 한도	95%	기존 백업을 완료할 수 있지만 새 백업 작업은 일시 중단됩니다. VDP에서 Data Domain에 대한 오류 이벤트가 발생합니다.

참고 Data Domain 시스템이 99% 용량에 도달하면 유지 보수 작업이 실패합니다. Best Practice 권장 사항은 Data Domain 용량 사용량을 80%로 제한하는 것입니다.

vSphere Web Client를 사용하여 모니터링

- 1 vSphere Web Client에서 VDP 플러그인을 엽니다.
- 2 구성 탭의 스토리지 요약 섹션에 다음 정보가 표시됩니다.
 - Data Domain 시스템 FQDN 또는 IP 주소
 - Data Domain 시스템의 용량
 - Data Domain 시스템에서 사용 가능한 공간
 - Data Domain 시스템에서 사용된 용량
- 3 왼쪽에는 Data Domain 용량 확인을 위한 색상 컨테이너가 표시됩니다.
 - 사용된 스토리지 용량이 80% 미만이면 컨테이너가 녹색입니다.
 - 사용된 스토리지 용량이 80%에서 90% 사이이면 컨테이너가 노란색입니다. 다음과 같은 메시지가 나타납니다.
Data Domain 스토리지가 거의 가득 찼습니다.
 - 사용된 스토리지 용량이 95%에서 100% 사이이면 컨테이너가 빨간색입니다. 다음과 같은 메시지가 나타납니다.
Data Domain 스토리지가 거의 가득 찼습니다.
 - 사용된 스토리지 용량이 100%이면 컨테이너가 빨간색입니다. 다음과 같은 메시지가 나타납니다.
Data Domain 스토리지가 가득 찼습니다.

VDP 구성 유틸리티를 사용하여 모니터링

- 1 다음 URL을 사용하여 VDP 구성 유틸리티에 로그인합니다.

https://<IP_address_VDP_appliance>:8543/vdp-configure/

- 2 스토리지 탭의 스토리지 요약 섹션에 다음 정보가 표시됩니다.

- DD 호스트 이름 또는 IP 주소
- 총 가용 용량
- 현재 사용 가능한 용량
- 사용한 용량(비율)

참고 페이지에서 데이터를 새로 고치려면 **스토리지 요약** 옆에 있는 새로 고침 아이콘을 클릭합니다.

- 3 왼쪽에는 Data Domain 용량 확인을 위한 색상 컨테이너가 표시됩니다.

- 사용된 스토리지 용량이 80% 미만이면 컨테이너가 녹색입니다.
- 사용된 스토리지 용량이 80%에서 90% 사이이면 컨테이너가 노란색입니다. 다음과 같은 메시지가 나타납니다.
Data Domain 스토리지가 거의 가득 찹니다.
- 사용된 스토리지 용량이 95%에서 100% 사이이면 컨테이너가 빨간색입니다. 다음과 같은 메시지가 나타납니다.
Data Domain 스토리지가 거의 가득 찹니다.
- 사용된 스토리지 용량이 100%이면 컨테이너가 빨간색입니다. 다음과 같은 메시지가 나타납니다.
Data Domain 스토리지가 가득 찹니다.

전체 Data Domain 시스템에서 스토리지 재확보

Data Domain 시스템에서 스토리지 공간을 모두 사용하는 경우 다음 문제가 발생할 수 있습니다.

- 백업이 성공하지 못하며, 시작되지 않을 수 있습니다.
- Data Domain 시스템에서 정보를 변경하는 작업(예: 가비지 수집 중 체크포인트, 활성 백업 및 만료된 백업 삭제)이 실패합니다. 이러한 작업에는 전체 Data Domain 시스템에서 허용되지 않는 디렉토리 이름 바꾸기가 수반되기 때문에 실패할 수 있습니다.

전체 Data Domain 시스템에서 사용된 스토리지를 재확보하려면 다음 단계를 수행하십시오.

- 1 스토리지를 사용 중인 데이터의 소스를 확인합니다. 데이터의 소스가 특정 클라이언트, 특정 VDP 어플라이언스와 연관된 클라이언트 그룹 또는 Data Domain 시스템에 데이터를 저장하는 다른 백업 제품일 수 있습니다.
- 2 진행 중인 백업을 모두 취소합니다. 이 작업은 VDP 어플라이언스의 명령줄에서 수행해야 합니다.
 - a VDP 어플라이언스에 대한 SSH 또는 Putty 세션을 열고 다음 명령을 실행합니다.


```
su - admin
ssh-agent bash
ssh-add .ssh/dpnid
```
 - b `mccli activity show` 명령을 실행합니다.
이 명령은 다음 샘플 출력과 유사한 결과를 반환합니다.

```
admin@gs-pod192:~/>: mccli activity show
0,23000,CLI command completed successfully.
```

ID	Status	Error Code	Start Time	Elapsed	End Time	Type	Progress	Bytes	New Bytes	Client
9138660744236309	Running		0 2013-12-09 09:44 MST	00h:27m:25s	2013-12-10 09:44 MST	On-Demand Backup			54.3 GB	4.2% Win2008R2-GSClone /10.7.242.175/VirtualMachines

```

9138660744234709 Completed 0 2013-12-09 09:44 MST 00h:02m:51s 2013-12-09 09:47 MST On-Demand Backup 40.0 GB
<0.05% GermanExchange /10.7.242.175/VirtualMachines
9138660718256909 Completed 0 2013-12-09 09:39 MST 00h:01m:06s 2013-12-09 09:40 MST On-Demand Backup 40.0 GB
<0.05% GermanExchange /10.7.242.175/VirtualMachines
9138660744235609 Completed 0 2013-12-09 09:44 MST 00h:20m:37s 2013-12-09 10:04 MST On-Demand Backup 40.0 GB
2.6% ActiveDirectory /10.7.242.175/VirtualMachines \

```

실행 중인 백업을 취소하는 명령을 실행하려면 아래의 'AppliancePassword' 값으로 입력하는 어플라이언스 암호를 알아야 합니다. 실행 중인 작업의 ID도 기록해 두어야 합니다.

c `mccli activity cancel --mcsuserid=MCUser --mcpasswd=AppliancePassword --id=XXXXX` 명령을 입력합니다. 여기서 `AppliancePassword`는 어플라이언스 암호이고 `XXXXX`는 실행 중인 작업 중 취소할 작업의 ID입니다. 이 명령은 다음 출력과 유사한 결과를 반환합니다.

```

admin@gs-pod192:~>: mccli activity cancel --mcsuserid=MCUser --mcpasswd=Test12345 --id=9138660744236309
0,22205,Backup cancelled via console
Attribut 값
-----
activity-id9138660744236309

```

- 3 실행 중 상태의 모든 작업에 대해 **c 단계**를 반복합니다.
- 4 백업 및 복구를 일시 중단합니다. VDP 어플라이언스에서 이 작업을 수행하려면 명령줄에서 프록시를 비활성화합니다. 이 명령을 실행하기 전에 수행해야 하는 중요한 백업 또는 복구가 없는지 최종 사용자와 함께 확인합니다.
 - a VDP 어플라이언스에 대한 SSH 또는 Putty 세션을 엽니다.
 - b `service avagent-vmware stop` 명령을 실행합니다.
- 5 VDP 어플라이언스에서 서버 유지 보수 작업을 일시 중단합니다.
 - a 다음 URL을 사용하여 VDP 구성 유틸리티에 로그인합니다.
`https://<IP_address_VDP_appliance>:8543/vdp-configure`
 - b 유지 보수 서비스가 **실행 중**으로 표시되는 경우 **중지** 버튼을 클릭합니다
- 6 Data Domain 시스템에서 VDP 어플라이언스의 기존 STAGING, DELETED 또는 cur/DELETED 디렉토리를 수동으로 삭제합니다.
- 7 Data Domain Enterprise Manager를 사용하여 Data Domain 파일 시스템 정리 작업을 시작합니다.
이 프로세스에서는 VDP 어플라이언스 서비스 유지 보수 작업이 성공적으로 완료되는 데 필요한 공간을 충분히 확보합니다.
- 8 VDP 어플라이언스에서 서버 유지 보수 작업을 재시작합니다.
 - a 다음 URL을 사용하여 VDP 구성 유틸리티에 로그인합니다.
`https://<IP_address_VDP_appliance>:8543/vdp-configure`
 - b 유지 보수 서비스가 **중지됨**으로 표시되는 경우 **시작** 버튼을 클릭합니다
- 9 백업 및 복구를 실행할 수 있도록 VDP 어플라이언스에서 프록시를 재시작합니다.
 - a VDP 어플라이언스에 대한 SSH 또는 Putty 세션을 엽니다.
 - b `service avagent-vmware start` 명령을 실행합니다.

일반적인 문제 및 해결책

이 섹션에는 VDP Appliance 백업을 Data Domain 시스템에 저장할 때 발생하는 일반적인 문제와 해결책이 나와 있습니다.

Data Domain 시스템이 오프라인 상태인 경우 백업 실패

백업이 시작될 때 Data Domain 시스템이 오프라인 상태인 경우 5분 이상 지난 후에 백업이 실패할 수 있습니다. 이 실패는 거의 모든 DD Boost 작업에 대해 최소 제한 시간이 5분이기 때문에 발생합니다.

백업 실패 문제를 해결하려면 Data Domain 시스템을 온라인 상태로 설정한 다음 백업을 다시 시도하십시오.

Data Domain 시스템 삭제 후 롤백

“VDP 어플라이언스에서 Data Domain 시스템 삭제”(85페이지)에 대한 절차를 수행한 후 체크포인트로 롤백하는 경우 VDP 어플라이언스에서 Data Domain 시스템이 제거된 상태로 롤백됩니다.

VDP 어플라이언스에 Data Domain 시스템을 다시 추가하려면 VDP Configuration UI를 사용하십시오. 자세한 내용은 “Data Domain 시스템 추가”(84페이지) 섹션을 참조하십시오.

Data Domain 도메인 시스템 삭제 이전의 체크포인트로 롤백하는 경우에는 Data Domain 시스템이 계속 연결되고 제대로 구성된 상태를 유지합니다. Data Domain 시스템을 제거하려면 “VDP 어플라이언스에서 Data Domain 시스템 삭제”(85페이지) 절차를 따르십시오.

애플리케이션 롤백으로 이러한 상태와 다른 상태가 되는 경우에는 지원 서비스에 문의하여 적절한 해결책을 정의하는 것이 좋습니다.

VDP 디스크 확장

이 장에서 다루는 내용은 다음과 같습니다.

- [“사전 요구 사항”\(98페이지\)](#)
- [“VMFS 힙 크기 권장 사항”\(98페이지\)](#)
- [“디스크 확장 수행”\(99페이지\)](#)
- [“성능 분석”\(101페이지\)](#)
- [“Essentials Plus를 사용한 디스크 확장”\(101페이지\)](#)

사전 요구 사항

디스크 확장 전에 구성이 다음 요구 사항을 충족하는지 확인하십시오. 이러한 요구 사항을 충족하지 않으면 VDP가 손상되어 클론이나 VDP 백업에서 복구해야 할 수 있습니다.

- 새 구성에 필요한 최소 CPU 및 메모리 요구 사항이 충족되었는지 확인합니다.
 - VDP 용량 옵션(2TB, 4TB, 6TB 및 8TB)에 대한 최소 가상 CPU 수는 4개입니다.
 - 가상 머신당 최소 메모리 양은 용량에 따라 달라집니다.

용량 크기	필요 메모리
2TB	6GB
4TB	8GB
6TB	10GB
8TB	12GB

- CPU 및 메모리 핫 애드(Hot-Add)가 모두 활성화되었는지 확인합니다. 업그레이드된 어플라이언스의 경우 기본적으로 CPU 및 메모리 핫 애드(Hot-Add) 옵션이 비활성화됩니다.

참고

- Essentials Plus 라이선스가 있는 경우 필요한 메모리를 핫 플래깅할 수 없습니다. VDP에 할당된 메모리를 수동으로 늘려야 합니다. 자세한 내용은 [“Essentials Plus를 사용한 디스크 확장”](#)(101페이지) 섹션을 참조하십시오.
- 확장에 필요한 가용 디스크 공간이 있는지 확인합니다. **스토리지** 탭에서 디스크 공간을 확인할 수 있습니다. [“스토리지 구성 보기”](#)(74페이지) 섹션을 참조하십시오.
- 디스크 확장은 백업 기간 중에 백업 작업이나 복구, 무결성 검사 등의 다른 VDP 작업이 실행 중이지 않을 때 수행하십시오. 디스크 확장을 시도하기 전에 모든 VDP 서비스가 실행 중인 상태인지 확인하십시오. 자세한 내용은 [“서비스 시작 및 중지”](#)(37페이지) 섹션을 참조하십시오.
- vCenter에 관리 권한이 있는지 확인합니다. vCenter에 대한 관리 권한이 있는지 확인하려면 [“사용자 계정 구성”](#)(24페이지) 섹션을 참조하십시오.
- VMFS 힙 크기가 vSphere 호스트와 연결된 가상 디스크 공간의 크기에 맞는 올바른 값으로 설정되었는지 확인합니다. 자세한 내용은 [“VMFS 힙 크기 권장 사항”](#)(98페이지) 섹션을 참조하십시오.
- 클론 생성 작업 전에 어플라이언스의 MAC 주소를 적어 두십시오. 나중에 스토리지에서 장애가 발생한 경우에 이 MAC 주소가 사용됩니다.
- 디스크 확장 전에 VDP 어플라이언스의 클론이나 백업을 만들고 유효한지 확인합니다.

VMFS 힙 크기 권장 사항

VMFS 힙 크기에 따라 각 vSphere 호스트에서 지원하는 가상 디스크 공간의 크기가 결정됩니다. 가상 디스크 공간이 구성된 VMFS 힙 크기를 초과할 경우, 다음과 같은 현상이 발생할 수 있습니다.

- 가상 머신이 오작동합니다.
- 메모리를 할당할 수 없음 오류 메시지가 나타납니다.
- 가상 머신이 작동을 중단하거나 시작되지 않습니다.

디스크 확장 전에 VMFS 힙 크기가 새 가상 디스크 용량에 맞게 제대로 구성되었는지 확인합니다. VMFS 힙 크기를 늘리면 vSphere 호스트 커널에 할당되는 메모리 용량이 증가하며, 변경 내용을 적용하려면 시스템을 재부팅해야 합니다.

표 10-15에는 동일한 설정을 사용하는 VMFS3과 VMFS5가 정의되어 있습니다.

표 10-15. VMFS 힙 크기 설정

버전/빌드	기본 힙 양	호스트당 기본적으로 허용되는 열린 VMDK 스토리지		최대 힙 양	최대 힙 값	호스트당 최대 열린 VMDK 스토리지
		최소 힙 양	최대 힙 양			
vSphere Host 5.0 업데이트 2(914586) 이하	80MB	8TB	해당 없음	256MB	255	25TB
vSphere Host 5.0 패치 5(1024429) 이상	256MB	60TB	256MB	640MB	255	60TB
vSphere Host 5.1 패치 1(914609) 이하	80MB	8TB	해당 없음	256MB	255	25TB
vSphere Host 5.1 업데이트 1(1065491) 이상	256MB	60TB	256MB	640MB	255	60TB

참고 vSphere 5.5 이상에는 한층 개선된 힙 제거 프로세스가 포함되어 있으므로, 메모리를 많이 소모하는 큰 힙이 더 이상 필요하지 않습니다. vSphere 5.5 이상은 256MB의 최대 힙 크기를 지원하고 호스트가 64TB VMFS의 모든 주소 공간에 액세스할 수 있도록 지원합니다.

VMware 기술 자료 문서 1004424에 VMFS 힙 크기 설정을 변경하기 위한 단계가 나와 있습니다.

디스크 확장 수행

VDP에서는 **스토리지 확장** 마법사를 사용하여 데이터 저장소 용량을 확장할 수 있습니다. 디스크 확장 기능을 이용하면 VDP 스토리지를 1TB, 2TB, 4TB, 6TB 또는 8TB로 확장할 수 있습니다.

참고 프로비저닝 유형을 씬 프로비저닝에서 일반(thick) 프로비저닝으로 변경할 수 없습니다. 디스크는 초기 구성 동안 할당된 프로비저닝 유형을 상속합니다.

일반 Eager-Zeroed 유형의 VMDK를 확장하는 경우 일반 Lazy-Zeroed 부분만 확장됩니다.

VMware 기술 자료 문서 1035823에 VMDK의 크기를 늘리고 VMDK를 일반 Eager-Zeroed로 만드는 단계가 나와 있습니다.

사전 요구 사항

초기 구성 시 VDP 스토리지 디스크를 검증해야 합니다.

절차

1 다음 URL을 사용하여 VDP 구성 유틸리티에 로그인합니다.

`https://<IP_address_VDP_appliance>:8543/vdp-configure/`

2 **스토리지** 탭을 클릭합니다.

스토리지 요약 섹션에는 사용 가능한 총 스토리지 용량 및 각 데이터 저장소에 사용할 수 있는 스토리지 용량과 함께 사용 가능한 데이터 저장소가 표시됩니다.

참고 페이지에서 데이터를 새로 고치려면 **스토리지 요약** 옆에 있는 새로 고침 아이콘을 클릭합니다.

3 **작업** 목록에서 **스토리지 확장**을 선택합니다.

스토리지 확장 마법사가 나타나고 현재 용량이 표시됩니다.

4 디스크 크기를 확장 중인지 또는 디스크 수를 늘리는 것인지 결정합니다.

참고 2TB까지 확장하는 동안 디스크 수는 3개로 유지되지만 기존 디스크의 크기는 증가합니다. 디스크가 확장되면 각 데이터 저장소에 대해 디스크 수를 선택하는 제어 기능은 비활성화됩니다.

- a 디스크 크기를 확장하려면 목록에서 새 용량을 선택합니다. VDP 스토리지를 1TB, 2TB, 4TB, 6TB 또는 8TB로 확장할 수 있습니다.
- b 디스크를 추가하려면 사용 가능한 총 스토리지 디스크 수가 할당될 때까지 디스크 열에서 디스크 수를 늘립니다. 모든 디스크를 단일 데이터 저장소에 할당할 수도 있고 디스크를 여러 데이터 저장소에 배포할 수도 있습니다.

5 다음을 클릭합니다.

디바이스 할당 대화상자에 할당에 사용할 수 있는 것으로 알려진 데이터 저장소와 할당할 디스크 수가 표시됩니다.

성능 분석이 실패했거나, 실행된 적이 없거나, 선택한 데이터 저장소 중 하나 이상에서 기간이 지난 것으로 시스템에서 확인한 경우 경고 메시지가 나타납니다. 선택한 데이터 저장소에서 성능 분석을 실행할지 여부에 따라 다음 중 하나를 수행하십시오.

- 예를 클릭하면 마법사를 중단하고 선택한 데이터 저장소에서 성능 분석을 실행합니다. 성능 분석 톨을 실행하려면 **"성능 분석"**(101페이지) 섹션을 참조하십시오.
- **아니요**를 클릭하면 디스크 확장을 계속합니다.

6 다음을 클릭하면 스토리지 확장 마법사의 다음 패널로 이동합니다.

현재 구성에 필요한 최소 CPU 및 메모리 요구 사항이 CPU 및 메모리 대화상자에 표시됩니다.

7 각 가상 머신에 대한 가상 CPU 수를 선택합니다.

VDP 가상 머신에 허용되는 최대 가상 CPU 수는 8개입니다.

8 VDP 가상 머신에 할당할 메모리 양을 선택합니다.

- 가상 머신당 최소 메모리 양은 용량에 따라 달라집니다.
 - 2TB 용량 - 6GB 메모리
 - 4TB 용량 - 8GB 메모리
 - 6TB 용량 - 10GB 메모리
 - 8TB 용량 - 12GB 메모리
- VDP 가상 머신에 허용되는 최대 메모리 양은 64GB입니다.

9 완료 준비 대화상자에서 **마침**을 클릭하여 변경 사항을 적용합니다.

참고 스토리지 구성이 완료되면 시스템이 자동으로 체크포인트를 생성하고 무결성 검사를 수행합니다.

스토리지 구성 보기

스토리지 확장이 완료된 후 **스토리지 탭의 스토리지 요약** 섹션을 사용하여 각 데이터 저장소에 사용 가능한 총 가용 스토리지 및 스토리지 용량을 검증할 수 있습니다.

알려진 제한 사항

디스크 확장 후에 바로 로드 밸런싱이 발생하고 결과에 나타나는 사용된 용량은 잘못된 값을 표시합니다. 그러나 다음 유지 보수 기간이 완료되면 값이 올바르게 표시됩니다.

절차

1 다음 URL을 사용하여 VDP 구성 유틸리티에 로그인합니다.

https://<IP_address_VDP_appliance>:8580/vdp-configure

2 스토리지 탭을 클릭합니다.

스토리지 요약 섹션에 각 데이터 저장소에 대한 총 가용 스토리지 및 스토리지 용량이 표시됩니다.

참고 페이지에서 데이터를 새로 고치려면 **스토리지 요약** 옆에 있는 새로 고침 아이콘을 클릭합니다.

성능 분석

성능 분석 테스트에서는 쓰기, 읽기 및 검색 성능 테스트를 수행합니다. 초기 구성 중에 성능 분석 테스트를 통해 구성된 VDP 디스크의 읽기, 쓰기 및 검색 기능이 평가됩니다. 초기 구성 후에는 데이터 저장소에 256GB의 임시 디스크를 생성하는 방법으로 데이터 저장소의 성능을 측정하는 테스트가 실행됩니다.

가능한 테스트 결과는 다음과 같습니다.

- 알 수 없음
- 실패
- 통과

성능 분석 테스트 실행

- 1 다음 URL을 사용하여 VDP 구성 유틸리티에 로그인합니다.

`https://<IP_address_VDP_appliance>:8543/vdp-configure`

- 2 스토리지 탭에서 **성능 분석**을 클릭합니다.

성능 분석 테스트에서는 선택한 데이터 저장소에 임시 디스크를 생성하고 해당 디스크에서 테스트를 실행합니다. 성능 분석이 완료되면 임시 디스크는 자동으로 제거됩니다.

- 3 성능 분석 테스트를 실행할 데이터 저장소를 선택합니다.
- 4 성능 분석을 시작하려면 **실행**을 클릭합니다.

참고 언제든지 **취소**를 클릭하여 성능 분석 테스트를 중지할 수 있습니다.

Essentials Plus를 사용한 디스크 확장

Essentials Plus 라이선스가 있는 경우 메모리 핫 애드(Hot-Add)를 활성화할 수 없습니다. 타겟 용량에 필요한 대로 VDP에 할당된 메모리를 수동으로 조정해야 합니다.

참고 이 제한 사항은 vSphere 5.x 호스트에 적용됩니다. 표 10-16에 나열된 메모리 요구 사항에 따라 vSphere 호스트에 필요한 최소 메모리를 수동으로 설정해야 합니다.

VDP의 용량 크기에 따른 메모리 요구 사항은 다음과 같습니다.

표 10-16. 가상 하드웨어에 대한 메모리 요구 사항

용량 크기	필요 메모리
2TB	6GB
4TB	8GB
6TB	10GB
8TB	12GB

절차

Essentials Plus 라이선스를 사용하여 디스크 확장을 수행하려면 다음 단계를 완료하십시오.

- 1 웹 브라우저에서 다음 주소로 vSphere Web Client에 액세스합니다.

`https://<IP_address_vCenter_Server>:9443/vsphere-client/`

- 2 확장하기 전에 가상 머신에서 **게스트 운영 체제 종료** 작업을 사용하여 VDP 어플라이언스를 종료합니다.

이 작업을 사용하면 VDP 어플라이언스의 완전한 종료가 수행됩니다. **게스트 운영 체제 종료** 작업 없이 어플라이언스의 전원을 끈 경우 손상이 발생할 수 있습니다. VDP 어플라이언스를 종료하고 재시작하는 데는 30분 정도 소요될 수 있습니다. 가상 머신 콘솔을 통해 상태를 모니터링할 수 있습니다.

- 3 표 10-16에 나와 있는 요구 사항을 참조하여 VDP 어플라이언스에 할당된 메모리를 늘립니다.

- a 웹 브라우저에서 다음 주소로 vSphere Web Client에 액세스합니다.
https://<IP_address_vCenter_Server>:9443/vsphere-client/
 - b vSphere Web Client에 하드웨어 설정을 편집할 권한이 있는 사용자로 로그인합니다.
 - c **vCenter > 호스트 및 클러스터**를 클릭합니다.
 - d 왼쪽 트리에서 VDP 어플라이언스가 나타날 때까지 펼치기 화살표를 클릭합니다.
 - e VDP 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
 - f **가상 하드웨어** 탭을 클릭합니다.
 - g **메모리** 필드에 값을 입력하여 메모리 용량을 늘립니다.
 - h **확인**을 클릭합니다.
- 4 VDP 어플라이언스를 다시 시작하려면 VDP 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **전원 켜기**를 선택합니다.

VDP 사용

이 장에서 다루는 내용은 다음과 같습니다.

- [“VDP 액세스”\(104페이지\)](#)
- [“CLI를 사용하여 VDP 어플라이언스 액세스”\(104페이지\)](#)
- [“VDP 사용자 인터페이스 이해”\(105페이지\)](#)
- [“VDP 어플라이언스 전환”\(106페이지\)](#)
- [“VDP 사용자 인터페이스”\(106페이지\)](#)
- [“보고서 탭에서 정보 보기”\(106페이지\)](#)

VDP 액세스

vSphere Web Client를 사용하여 VDP를 액세스하고 관리합니다.

참고 vCenter Server 없이 VDP를 사용할 수 없습니다. 링크 모드에서 VDP 어플라이언스는 연결된 vCenter Server와만 작동합니다. VDP 어플라이언스가 vSphere Web Client에 나타나지 않을 경우, 링크 모드에서 해당 vCenter를 제거하십시오.

사전 요구 사항

VDP를 사용하기 전에 [“VDP 설치 및 구성”\(21페이지\)](#)의 설명에 따라 VDP를 설치 및 구성해야 합니다.

절차

- 1 웹 브라우저에서 다음 주소로 vSphere Web Client에 액세스합니다.
`https://<IP_address_vCenter_Server>:9443/vsphere-client/`
- 2 자격 증명 페이지에 vCenter 관리 사용자 이름과 암호를 입력하고 **로그인**을 클릭합니다. 지정한 사용자 계정에 관리자 권한이 있어야 합니다.
- 3 vSphere Web Client에서 **VDP**를 선택합니다.
- 4 **VDP 시작** 페이지에서 VDP 어플라이언스를 선택하고 연결을 클릭합니다.

CLI를 사용하여 VDP 어플라이언스 액세스

현재는 사용자가 vSphere Client 콘솔, SSH 또는 Putty 세션을 사용하여 VDP 어플라이언스 명령줄에 액세스할 수 있습니다. VDP 5.8 이상 릴리즈에서는 SSH 또는 Putty를 사용하여 루트 사용자로 VDP 어플라이언스에 로그인하는 기능이 제거되었습니다.

SSH 또는 Putty를 사용하여 어플라이언스에 액세스하려면 admin 사용자로 로그인해야 합니다.

VDP 5.8 이상 릴리즈에서는 admin 사용자의 기본 암호도 변경되었습니다. 이 암호는 사용자가 VDP 구성 UI에서 어플라이언스 구성을 완료하기 전에 VDP 어플라이언스에 로그인한 경우에만 적용됩니다. 이때 사용되는 admin 암호는 88RttoTriz!!입니다.

어플라이언스 구성이 완료되면 새로 구성된 어플라이언스 암호를 사용하여 admin 사용자로 명령줄에 액세스할 수 있습니다.

유용한 명령

다음 표에는 몇 가지 유용한 명령이 정리되어 있습니다.

표 11-17. 유용한 VDP 명령

명령	설명
status.dpn	VDP 상태를 표시합니다.
dpnctl status	VDP 서비스 상태를 표시합니다.
emwebapp.sh -- test	VDP Enterprise Manager 웹 애플리케이션 상태를 테스트합니다.
capacity.sh	지난 30일 간의 백업 작업에서 공간 사용량을 분석하여 새 데이터의 크기와 가비지 수집이 복구한 공간을 표시합니다.
cplist	체크포인트 상태를 표시합니다.
mccli server show-prop	vSphere 웹 클라이언트에 나타나는 것과 동일한 VDP 어플라이언스 속성을 표시합니다.
mccli activity show	백업 작업 정보를 표시합니다. 각 작업은 단일 가상 머신의 백업 작업입니다.
mccli dd show-prop	Data Domain 시스템 속성을 표시합니다.
mccli client show --domain=/vCenter FQDN 또는 IP/VirtualMachines --recursive=true	보호된 가상 머신을 나열합니다.

표 11-17. 유용한 VDP 명령

명령	설명
mccli backup show --name=/ vCenter FQDN 또는 IP/VirtualMachines/Virtual Machine name --recursive=true	가상 머신 백업을 나열합니다.
mccli -help	사용 가능한 명령 옵션을 나열합니다.

VDP 사용자 인터페이스 이해

vSphere Data Protection용 vSphere Web Client를 사용하여 VDP를 구성 및 관리합니다.

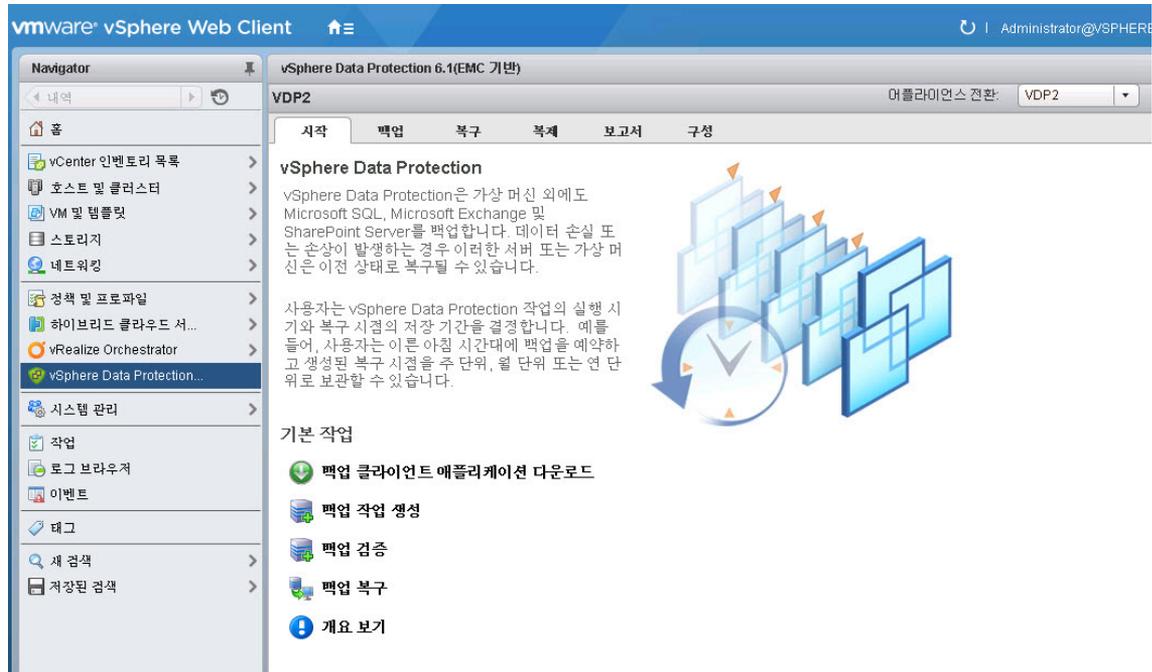


그림 11-7. vSphere Data Protection 사용자 인터페이스

vSphere Data Protection 사용자 인터페이스는 다음 6개의 탭으로 구성됩니다.

- **시작:** VDP 기능에 대한 개요와 백업 클라이언트 애플리케이션 다운로드, 백업 작업 생성, 백업 검증, 백업 복구 및 개요 보기로 바로 연결되는 링크를 제공합니다.
- **백업:** 예약된 백업 작업 목록과 각 백업 작업에 대한 세부 정보를 제공합니다. 이 페이지에서 백업 작업을 생성하고 편집할 수도 있습니다. 또한 이 페이지는 백업 작업을 즉시 실행할 수 있는 기능도 제공합니다. 자세한 내용은 [“보고서 탭에서 정보 보기”](#)(106페이지)에 나와 있습니다.
- **복구:** 복구할 수 있는 성공적인 백업 목록을 제공합니다. 자세한 내용은 [“복구 작업”](#)(126페이지)에 나와 있습니다.
- **복제:** 복제할 수 있는 성공적인 백업 목록을 제공합니다. 자세한 내용은 [“복제 작업”](#)(134페이지)에 나와 있습니다.
- **보고서:** vCenter Server의 가상 머신에 대한 백업 상태 보고서를 제공합니다. 자세한 내용은 [“보고서 탭에서 정보 보기”](#)(106페이지)에 나와 있습니다.
- **Configuration:** VDP가 구성된 방식에 대한 정보를 표시하고 이 중 일부 설정을 편집할 수 있습니다. 자세한 내용은 [“VDP 구성”](#)(51페이지)에 나와 있습니다.

VDP 어플라이언스 전환

각 vCenter Server는 VDP 어플라이언스를 최대 20개까지 지원합니다. **어플라이언스 전환** 옵션의 오른쪽에 있는 드롭다운 목록에서 어플라이언스를 선택하여 어플라이언스를 전환할 수 있습니다.

참고 드롭다운 목록에서 VDP 어플라이언스는 사전순으로 정렬되므로 화면에 표시되는 목록의 첫 번째 항목이 현재 어플라이언스와 일치하지 않을 수 있습니다. VDP 화면 왼쪽에 표시되는 어플라이언스 이름이 현재 어플라이언스이고 드롭다운 목록의 어플라이언스 이름은 사용 가능한 어플라이언스 목록의 첫 번째입니다.

VDP 사용자 인터페이스

VDP 사용자 인터페이스에는 다음과 같은 기능이 포함되어 있습니다.

- Microsoft Exchange Server, SQL Server 및 SharePoint Server에 대한 게스트 레벨 백업
- 디스크 확장 및 추가(디스크 확장)
- Data Domain 시스템으로 백업
- GLR(Granular Level Recovery)
- 자동 백업 검증

이러한 옵션에 대한 설명은 “**VDP 애플리케이션 지원**”(156페이지)에 나와 있습니다. 여기에는 애플리케이션 레벨 백업 및 복구를 수행하는 방법도 자세히 설명되어 있습니다.

보고서 탭에서 정보 보기

보고서 탭에는 다음 정보가 표시됩니다.

어플라이언스 상태 정보

- **어플라이언스 상태:** VDP 어플라이언스의 상태입니다.
- **무결성 검사 상태:** 무결성 검사를 시작하려면 녹색 오른쪽 화살표를 클릭합니다. 상태 값은 정상 또는 기간 지남입니다.
 - 정상은 무결성 검사가 지난 2일 동안 성공적으로 완료되었음을 나타내고,
 - 기간 지남은 무결성 검사가 지난 2일 동안 실행되지 않았거나 성공적으로 완료되지 않았음을 나타냅니다.
- **사용된 용량:** 총 VDP 용량 중 백업에 사용된 용량의 비율입니다.
- **사용된 DDR 용량:** 총 용량 중 Data Domain 시스템에서 사용된 용량의 비율입니다(해당되는 경우).
- **최근에 실패한 백업:** 가장 최근에 완료된 백업 작업에서 백업하지 못한 가상 머신의 수입입니다.
- **최근에 실패한 백업 검증:** 최근에 실패한 백업 검증 작업의 수입입니다.
- **최근에 실패한 복제:** 최근에 실패한 복제 작업의 수입입니다.
- **보호된 총 VM:** VDP 어플라이언스에서 보호되는 가상 머신의 총 수입입니다.

참고 VDP 어플라이언스는 400개의 가상 머신을 지원합니다. 최대 가상 머신 수를 초과하는 경우 경보가 생성되고 로그 탭에 오류 메시지가 표시됩니다.

새로 고침

보고서 탭의 데이터를 업데이트하려면 언제든지 **새로 고침** 버튼을 클릭합니다.

작업 실패 탭

작업 실패 탭에는 지난 72시간 내에 실패한 작업에 대한 세부 정보가 표시됩니다.

실패 시간: 작업이 실패한 날짜 및 시간입니다.

이는 작업이 실패한 이유입니다.

클라이언트/소스 이름: vCenter와 연결된 클라이언트입니다.

작업 이름: 실패한 작업의 이름입니다.

작업 유형: 실패한 작업의 유형(예: 예약 백업 또는 필요 시 백업)입니다.

다음 실행 시간: 작업이 다음에 실행되도록 예약된 날짜 및 시간입니다.

로그 보기: 클라이언트 로그 세부 정보를 볼 수 있는 작업 실패 클라이언트 로그 대화상자를 시작하려면 클릭합니다. 클라이언트 로그 대화상자에서 로그 파일이 제공되지 않는 경우 다음 세 가지 로그 메시지 중 하나가 나타날 수 있습니다.

- 로그 파일을 검색하지 못했습니다. 이 메시지는 다음과 같은 경우에 나타날 수 있습니다.
 - 관리 서비스가 최근에 재시작되었습니다.
 - 정기 로그 유지 보수로 인해 이전 로그 파일이 제거되었습니다.
 - 로그가 비어 있거나 존재하지 않을 수 있습니다.
 - 오류가 발생했을 수 있습니다.
- 로그를 검색하지 못했습니다. 로그는 일반적으로 작업이 완료되고 72시간 후에 제거됩니다.
- 검색된 로그 파일이 비어 있습니다.

참고 일부 복제 소스 및 복제 대상 로깅은 **작업 실패** 탭을 통해 제공되지 않습니다. 그러나 VDP 구성 유틸리티에서 일반 로그 번들을 사용하여 복제 로그를 검색할 수 있습니다. 자세한 내용은 [“VDP 로그 또는 진단 정보 수집”](#)(38페이지) 섹션을 참조하십시오.

작업 아이콘

작업 실패 탭의 오른쪽에 있는 작업 아이콘 목록에서 다음 작업을 수행할 수 있습니다.

- **작업 재실행:** 실패한 작업을 강조 표시하고 클릭하여 실패한 작업을 재실행합니다. 복구 실패에 대해서는 작업 재실행 기능을 사용할 수 없습니다.

참고 실패한 클라이언트에 대해서만 백업을 실행하려면 **백업** 탭의 **지금 백업** 아래에서 **기간이 지난 소스만 백업**을 선택하십시오.

- **CSV로 내보내기:** 현재 테이블을 심표로 구분된 값(CSV) 파일로 내보내려면 클릭합니다.
- **모든 열 표시:** 열 이름의 X를 클릭하여 열을 하나 이상 숨긴 다음 **모든 열 표시**를 클릭하여 UI에서 숨겨진 열을 표시합니다.

필터

다음 기준 중 하나를 선택하여 작업 실패 세부 정보를 필터링 및 사용자 지정할 수 있습니다. 지난 72시간 내에 발생한 작업 실패에 대한 정보가 나타납니다.

- **모두 표시:** 가상 머신에 대한 작업 실패 정보를 모두 표시합니다. **모두 표시**가 기본값입니다.
- **오류:** 오류 메시지를 기준으로 작업 실패 정보를 필터링합니다.
- **작업:** 선택한 작업에 대한 작업 실패 정보를 필터링합니다.
- **고객:** 지정된 클라이언트에 대한 작업 실패 정보를 필터링합니다.

작업 세부 정보 탭

작업 세부 정보 탭에서는 작업 유형(백업, 복제 또는 백업 검증)을 선택하고 선택한 작업에 대한 세부 정보를 표시할 수 있습니다. 백업이 기본 작업 유형입니다.

작업 세부 정보는 다음 세 가지 섹션으로 나뉩니다.

- **클라이언트 정보**

- **Client Name:** vCenter와 연결된 클라이언트입니다. 복제 도메인의 일반 가상 머신 클라이언트 및 사용 중단된 가상 머신 클라이언트에는 해시된 마스크 값이 복제된 이름, 복구된 이름 및 가져온 이름에 추가되어 표시됩니다.
- **유형:** 유형을 이미지, MS SQL Server, MS SharePoint Server 또는 MS Exchange Server로 표시합니다. 애플리케이션(MS SQL Server, MS SharePoint Server 또는 MS Exchange Server)은 VDP 어플라이언스에서만 지원됩니다.
- **작업:** 작업 이름입니다. 가상 머신이 두 개의 다른 작업에 있는 경우 여러 작업 이름이 나타납니다.
- **마지막 실행**
 - **작업 이름:** 작업의 이름입니다.
 - **완료:** 작업이 완료된 날짜 및 시간입니다.
 - **결과:** 작업이 성공했는지, 실패했는지, 성공했으나 예외가 발생했는지 또는 취소되었는지를 나타냅니다.
작업이 성공했으나 예외가 발생한 경우 **로그 보기** 링크를 클릭하여 로그에서 예외에 대한 정보를 검토합니다.
- **다음 실행**
 - **작업 이름:** 다음에 예약된 작업 이름이 나타납니다. 가상 머신이 일정이 다른 두 개의 다른 작업에 있는 경우 다음 예약된 작업 이름이 나타납니다.
 - **예약:** 작업이 다음에 실행되도록 예약된 날짜 및 시간입니다.

작업 아이콘

작업 세부 정보 탭의 오른쪽에 있는 작업 아이콘 목록에서 다음 작업을 수행할 수 있습니다.

- **CSV로 내보내기:** 현재 테이블을 심표로 구분된 값(CSV) 파일로 내보내려면 클릭합니다.
- **모든 열 표시:** 열 이름의 X를 클릭하여 열을 하나 이상 숨긴 다음 **모든 열 표시**를 클릭하여 UI에서 숨겨진 열을 표시합니다.

필터

다음 기준 중 하나를 선택하여 작업 세부 정보를 필터링 및 사용자 지정할 수 있습니다. 지난 72시간 내에 발생한 작업 실패에 대한 정보가 나타납니다.

- **모두 표시:** 가상 머신에 대한 작업 세부 정보를 모두 표시합니다. **모두 표시**가 기본값입니다.
- **고객:** 클라이언트를 기준으로 작업 실패 정보를 필터링합니다.
- **마지막 실행:** 마지막으로 실행된 작업에 대한 작업 세부 정보를 필터링합니다.
- **다음 실행:** 다음 예약된 작업에 대한 작업 세부 정보를 필터링합니다.

보호되지 않는 클라이언트 탭

- **Client Name:** 보호되지 않는 클라이언트의 이름입니다.
- **IP 주소:** 보호되지 않는 클라이언트의 IP 주소 또는 호스트 이름입니다.
- **VM 경로:** 가상 머신이 있는 위치의 경로입니다.

작업 아이콘

보호되지 않는 클라이언트 탭의 오른쪽에 있는 작업 아이콘 목록에서 다음 작업을 수행할 수 있습니다.

- **CSV로 내보내기:** 현재 테이블을 심표로 구분된 값(CSV) 파일로 내보내려면 클릭합니다.

백업 관리

이 장에서 다루는 내용은 다음과 같습니다.

- “백업 작업”(110페이지)
- “가상 머신 선택”(110페이지)
- “백업 스케줄 지정”(111페이지)
- “보존 정책 설정”(111페이지)
- “전체 이미지 백업 작업 생성”(112페이지)
- “개별 디스크에 대한 백업 작업 생성”(113페이지)
- “상태 및 백업 작업 세부 정보 보기”(115페이지)
- “백업 작업 편집”(115페이지)
- “백업 작업 클론 생성”(115페이지)
- “백업 잠금 및 잠금 해제”(116페이지)
- “VDP에서 Avamar로 백업 작업 마이그레이션”(117페이지)

백업 작업

백업 작업은 백업 스케줄 및 특정 보존 정책과 관련된 하나 이상의 가상 머신으로 구성됩니다. 백업 작업은 백업 탭에서 새 백업 작업 생성 마법사를 사용하여 생성 및 편집할 수 있습니다.

제한 사항

- VDP는 다음과 같은 특수 가상 머신을 백업하지 않습니다.
 - VDP 어플라이언스
 - VSA(vSphere Storage Appliance)
 - VDR(VMware Data Recovery) 어플라이언스
 - 템플릿
 - 보조 내결함성 노드
 - 프록시
 - AVE(Avamar Virtual Edition) 서버

마법사에서 이러한 VM을 선택할 수 있습니다. **마침**을 클릭하여 마법사를 완료하면 이러한 특수 가상 머신이 작업에 추가되지 않았다는 경고가 표시됩니다.

- 이름에 특수 문자가 포함된 가상 머신은 백업 작업에 추가할 수 없습니다. 이름에 ~!@\$%^&(){}[]|,;#\/*?<>"'& 같은 문자는 사용할 수 없습니다. 또한 â, é, ì, ü, ñ 같은 분음 문자도 사용할 수 없습니다.
- 버스 공유가 구성된 가상 머신에서 스냅샷을 사용하여 백업을 수행하는 것은 지원되지 않습니다. SCSI 버스 공유가 필요한 경우 다음 기술 자료 문서를 참조하십시오. <http://kb.vmware.com/kb/1006392>

사전 요구 사항

- VDP가 vCenter Server에 설치 및 구성되어 있어야 합니다.
- vSphere Web Client에 로그인하고 VDP 어플라이언스에 연결합니다.

가상 머신 선택

데이터 센터에 있는 모든 가상 머신과 같이 가상 머신 모음을 지정하거나 개별 가상 머신을 선택할 수 있습니다. 전체 리소스 풀, 호스트, 데이터 센터 또는 폴더가 선택된 경우 해당 컨테이너에 추가된 새로운 모든 가상 머신은 후속 백업에 포함됩니다. 단일 가상 머신이 선택된 경우 이후 가상 머신에 추가된 모든 디스크는 백업에 포함됩니다. 가상 머신이 선택된 컨테이너에서 원래 선택되지 않은 다른 컨테이너로 이동된 경우 해당 가상 머신은 더 이상 백업에 포함되지 않습니다.

백업할 가상 머신을 수동으로 선택할 수 있습니다. 이렇게 하면 이동한 가상 머신도 백업이 보장됩니다.

사용 중단된 가상 머신 확인

다음과 같은 상황에서는 가상 머신 클라이언트가 사용 중단되어 백업, 복구 또는 복제 작업에 사용할 수 없게 됩니다.

- **호스트:** 인벤토리에서 제거됨(클러스터, 호스트 폴더, 데이터 센터, 데이터 센터 폴더 등 호스트의 상위 컨테이너가 제거된 경우에도 발생)
- **가상 머신:** 디스크에서 삭제됨
- **가상 머신:** 인벤토리에서 제거됨

다음과 같은 상황에서는 가상 머신 클라이언트가 사용 중단되지 않고 하위 가상 머신에 인벤토리에 그대로 남게 됩니다.

- **리소스 풀:** 인벤토리에서 제거됨
- **vApp:** 인벤토리에서 제거됨
- **호스트:** 연결되지 않음

- 호스트: 유지 보수 모드 진입
- 호스트: 종료

백업 스케줄 지정

새 백업 작업 생성 마법사의 스케줄 페이지에서(아래 절차의 [7단계](#)) 백업 작업 시 가상 머신을 백업하는 간격을 지정할 수 있습니다. 백업은 백업 기간 시작 시점에 가능한 한 근접하여 발생합니다. 사용 가능한 간격은 일 단위, 주 단위 또는 월 단위입니다.

보존 정책 설정

VDP 어플라이언스에 대한 보존 정책은 백업 작업별로 따로 설정합니다. 백업 작업에서 생성되는 각 복구 시점에서는 생성될 당시의 보존 정책을 유지합니다. 백업 작업의 보존 정책을 수정하는 경우 새 정책은 새로 생성되는 복구 시점에만 영향을 줍니다. 이전에 생성된 복구 시점은 이전 보존 정책을 유지합니다.

백업 작업 생성 마법사의 보존 정책 페이지([8단계](#))에서 백업 보존 기간을 지정합니다.

처음 세 개 옵션인 **영구, 기간, 만료일**은 그룹에 있는 모든 가상 머신의 모든 백업에 동일하게 적용됩니다. 네 번째 옵션인 **다음 스케줄** 또는 사용자 지정 보존 스케줄은 내부적으로 매일, 매주, 매월 또는 매년 태그가 지정된 백업에만 적용됩니다.

참고 다음 스케줄 기본값은 60일입니다. **사용자 지정 보존** 기본값은 안 함입니다.

하루 중 첫 번째 백업은 매일 태그를 받습니다. 이 백업이 해당 주, 월 및 연도의 첫 번째 백업이기도 한 경우 이 백업은 매주, 매월 및 매년 태그도 받습니다. **다음 스케줄** 또는 사용자 지정 보존 스케줄 옵션으로 지정된 시간 간격은 내부 태그가 지정된 백업에만 적용됩니다. [표 12-18](#)에서는 보존 정책 옵션에 대해 설명합니다.

표 12-18. 보존 정책 옵션

옵션	설명
영구	백업 작업이 만료되지 않도록 설정합니다. 이 옵션으로 생성된 가상 머신 백업은 삭제되지 않습니다.
기간	백업 작업의 기간을 일, 주, 월 또는 년 단위로 설정합니다. 이 옵션으로 생성된 가상 머신 백업은 생성 날짜로부터 지정된 시점까지 저장됩니다. 예를 들어 백업 작업에 대해 보존 정책을 30일로 설정하면 실행되는 각 작업의 만료 날짜는 앞으로 30일 후가 됩니다.
만료일	특정 만료 날짜를 설정합니다. 이 옵션으로 생성된 가상 머신 백업은 만료일 필드에 지정된 날짜에 삭제됩니다.
이 스케줄 또는 사용자 지정 보존 스케줄	매일, 매주, 매월 또는 매년의 내부 태그가 지정된 백업에 대한 보존 간격을 설정합니다. 백업에는 이러한 내부 태그가 여러 개 있을 수 있습니다. 그 중 시간 간격이 가장 긴 태그가 우선적으로 고려됩니다. 예를 들어, 매주 태그가 지정된 백업을 8주 동안 보존하도록 설정하고 매월 태그가 지정된 백업을 한 달 동안 보존하도록 설정할 경우, 매주 및 매월 태그가 모두 있는 백업은 8주 동안 보존됩니다.

전체 이미지 백업 작업 생성

사전 요구 사항

- VDP가 vCenter Server에 설치 및 구성되어 있어야 합니다.
- VDP에서 지원하는 디스크여야 합니다. VDP는 다음 가상 하드웨어 디스크 유형을 지원하지 않습니다.
 - 독립형
 - RDM 독립형 - 가상 호환 모드
 - RDM 물리적 호환 모드

절차

1 웹 브라우저에서 VDP에 액세스합니다.

2 **백업** 탭을 클릭합니다.

백업 탭에는 생성된 백업 작업 목록이 표시됩니다. 목록의 각 열에 대해서는 다음 표에서 설명합니다.

표 12-19. 백업 탭의 열 설명

열	설명
이름	백업 작업의 이름입니다.
상태	백업 작업의 활성화 또는 비활성화 여부를 나타냅니다. 비활성화된 백업 작업은 실행되지 않습니다.
유형	애플리케이션 또는 이미지 같은 백업 유형입니다.
마지막 시작 시간	백업 작업이 시작된 마지막 시간입니다.
기간	해당 작업이 마지막 실행되었을 때 완료하는 데 소요된 시간입니다.
다음 실행 시간	백업 작업이 다시 실행되도록 예약된 시간입니다.
성공 수	백업 작업이 마지막으로 실행되었을 때 성공적으로 백업된 가상 머신의 수입니다. 이 수치는 각 백업 작업 후에 업데이트됩니다.
실패 수	백업 작업이 마지막으로 실행되었을 때 성공적으로 백업되지 않은 가상 머신의 수입니다. 이 수치는 각 백업 작업 후에 업데이트됩니다.

3 **백업 작업 조치** 메뉴에서 **새로 만들기**를 선택하여 새 백업 작업 생성 마법사를 실행합니다.

시작 탭에서 새 백업 작업 생성 마법사를 실행할 수도 있습니다. 이를 수행하려면 기본 작업 아래의 **백업 작업 생성**을 클릭합니다.

4 **작업 유형** 페이지에서 **게스트 이미지**를 선택한 후 **다음**을 클릭합니다.

애플리케이션 옵션을 사용하면 Microsoft Exchange Server, Microsoft SQL Server 및 Microsoft SharePoint Server에 대한 백업 작업을 생성할 수 있습니다. 자세한 내용은 **"VDP 애플리케이션 지원"**(155페이지)에 나와 있습니다.

5 **데이터 유형** 페이지에서 **다음**을 클릭합니다.

참고 중단 장애 시에는 애플리케이션 정합성이 보장되는 백업이 진행되지 않기 때문에 **비중단 장애로 파일백업** 옵션을 선택 취소하지 마십시오.

6 **백업 소스** 페이지에서 **펼치기 화살표**를 클릭하여 가상 머신을 연속적으로 표시합니다. 백업 작업에 추가할 항목 옆의 확인란을 선택한 후 **다음**을 클릭합니다.

참고 Data Domain 시스템이 백업 타겟으로 구성된 경우 타겟 대상을 구성하는 데 추가적인 단계가 있습니다. **로컬 스토리지** 또는 **Data Domain 스토리지**를 선택합니다.

7 **스케줄** 페이지에서 백업 작업의 스케줄을 선택하고 **다음**을 클릭합니다.

- 8 **보존 정책** 페이지에서 보존 기간을 선택하고 다음을 클릭합니다. 선택할 수 있는 보존 기간은 아래에 설명되어 있습니다.
- **영구:** 이 백업 작업에서 가상 머신에 대한 모든 백업은 절대 만료되지 않습니다.
 - **기간:** 이 옵션으로 생성된 가상 머신 백업은 생성 날짜로부터 지정된 간격이 경과된 후에 만료됩니다. 간격은 일, 주, 월 또는 년으로 지정할 수 있습니다.
 - **만료일:** 이 백업 작업에서 가상 머신에 대한 모든 백업이 지정된 날짜에 만료됩니다.
 - **다음 스케줄:** 내부 태그가 할당된 백업에 대한 보존 간격을 지정합니다. 예약된 일별 백업을 정기적으로 수행할 때 일부 백업에는 다음과 같은 보존 유형 중 하나가 자동으로 할당됩니다.
 - **매일:** 매일 성공적인 첫 번째 예약 백업
 - **주 단위:** 매주 성공적인 첫 번째 예약 백업
 - **월 단위:** 매월 성공적인 첫 번째 예약 백업
 - **연 단위:** 매년 성공적인 첫 번째 예약 백업
- 필요 시 백업 작업에 대한 **다음 스케줄** 기본값은 60일입니다.
- 보존 유형을 할당하기 위해 하루는 00:00:01 GMT에 시작되고, 각 주는 일요일에 시작되고, 각 월은 해당 월의 첫 번째 날짜에 시작되고, 각 연도는 1월 1일에 시작됩니다.
- 백업에 하나 이상의 내부 태그가 지정된 경우 간격이 더 긴 태그가 우선합니다. 예를 들어, 매주 태그가 지정된 백업을 8주 동안 보존하도록 설정하고 매월 태그가 지정된 백업을 한 달 동안 보존하도록 설정할 경우, 매주 및 매월 태그가 모두 지정된 백업은 8주 동안 보존됩니다.
- 주의** 백업 만료 후 새로운 유지 보수 기간이 시작되면 VDP 어플라이언스는 백업 데이터에 대한 참조를 제거하므로 이후 만료된 백업을 복구할 수 없습니다. VDP 어플라이언스는 다른 복구 시점에서 백업 데이터를 사용하고 있는지 여부를 확인합니다. 데이터가 사용되고 있지 않다고 시스템에서 확인한 경우 데이터가 제거되고 디스크 용량이 확보됩니다.
- 9 **이름** 페이지에서 백업 작업 이름을 입력하고 다음을 클릭합니다.
- 백업 작업 이름은 고유해야 하며 최대 255자까지 지정할 수 있습니다. 백업 작업 이름에 ~!@\$%^&()*[]|,;#/:*?<>"'& 같은 문자는 사용할 수 없습니다. 또한 â, é, ì, ù, ñ 같은 분음 문자도 사용할 수 없습니다.
- 10 **완료 준비** 페이지에서 백업 작업에 대한 요약 정보를 검토하고 **마침**을 클릭합니다.
- 정보 대화상자에서 백업 작업이 성공적으로 생성되었는지 확인합니다. 백업 작업은 몇 분 정도 소요될 수 있습니다.
- 11 **확인**을 클릭합니다.
- 이제 새로 생성된 백업 작업이 **백업** 탭에 나열됩니다.

개별 디스크에 대한 백업 작업 생성

전체 이미지 백업 작업에서는 전체 가상 머신에 있는 모든 디스크가 하나의 이미지 백업으로 취합됩니다. 개별 디스크 백업 작업에서는 필요한 디스크만 선택할 수 있습니다. 이 기능을 사용하면 운영 체제나 보존 정책 같은 특정 구성 조건에 따라 필터링할 수 있습니다.

지원되지 않는 디스크 유형

개별 디스크 백업을 계획할 때 VDP에서 디스크를 지원하는지 확인해야 합니다. 현재 VDP는 다음 가상 하드웨어 디스크 유형을 지원하지 않습니다.

- 독립형
- RDM 독립형 - 가상 호환 모드
- RDM 물리적 호환 모드
- 버스 공유가 지원되는 SCSI 컨트롤러에 부착된 가상 디스크

참고 가상 머신에 지원되지 않는 VMDK가 포함된 경우 이 VMDK는 회색으로 표시되고 확인란을 사용할 수 없습니다.

지원되지 않는 디스크 유형의 백업에 대한 자세한 내용은 “[단일 VMDK 백업 및 복구](#)”(16페이지) 섹션을 참조하십시오.

제한 사항

여러 VMDK가 포함된 가상 머신에서 단일 VMDK의 백업을 수행하려면 해당 가상 머신에 있는 모든 VMDK의 스냅샷을 저장할 수 있는 충분한 공간이 데이터 저장소에 있어야 합니다. 백업 작업의 목적이 단일 VMDK를 백업하는 것이라도 백업 프로세스에서는 가상 머신에 있는 모든 VMDK의 스냅샷을 생성합니다.

사전 요구 사항

VDP 어플라이언스가 vCenter Server에 설치 및 구성되어 있어야 합니다.

절차

1 웹 브라우저에서 VDP에 액세스합니다.

2 **백업** 탭을 클릭하고 **백업 작업 조치**에서 **새로 만들기**를 클릭하여 새 백업 작업 생성 마법사를 시작합니다.

참고 시작 탭에서 새 백업 작업 생성 마법사를 시작할 수도 있습니다. 이를 수행하려면 기본 작업 아래의 **백업 작업 생성**을 클릭합니다.

3 개별 가상 머신 디스크를 백업하려면 데이터 유형으로 **개별 디스크**를 선택한 후 **다음**을 클릭합니다.

가상 머신 페이지에 인벤토리 트리가 표시됩니다. 이 트리에는 vCenter Server에 있는 모든 객체 및 가상 머신이 포함됩니다.

펼치기 화살표를 클릭하면 트리의 콘텐츠가 연속적으로 표시됩니다. 백업 작업에 추가할 항목 옆의 확인란을 선택한 후 **다음**을 클릭합니다.

4 스케줄 페이지에서 작업에 대한 스케줄을 선택하고 **다음**을 클릭합니다.

5 보존 정책 페이지에서 기본 보존 정책을 적용하거나 대체 보존 정책을 지정하고 **다음**을 클릭합니다.

6 이름 페이지에서 백업 작업 이름을 입력하고 **다음**을 클릭합니다.

백업 작업 이름은 고유해야 하며 최대 255자까지 지정할 수 있습니다. 백업 작업 이름에 ~!@\$%^&(){}|[]\;#\/:.*?<>"'& 같은 문자는 사용할 수 없습니다. 또한 â, é, ì, ù, ñ 같은 분음 문자도 사용할 수 없습니다.

7 완료 준비 페이지에서 백업 작업에 대한 요약 정보를 검토한 후 **마침**을 클릭합니다.

정보 대화상자에서 백업 작업이 성공적으로 생성되었는지 확인합니다. 백업 작업은 몇 분 정도 소요될 수 있습니다.

8 **확인**을 클릭합니다.

이제 새로 생성된 백업 작업이 **백업** 탭에 나열됩니다.

개별 디스크의 마이그레이션

SVMotion™(VMware Storage VMotion)은 가동 중지 또는 서비스 중단 없이 VMDK 파일을 라이브 마이그레이션하기 위한 직관적 인터페이스를 제공하는 VMware vSphere의 구성 요소입니다. 다음 VMware vSphere 설명서 센터 웹 사이트에서 vMotion 및 SVMotion을 이용한 마이그레이션에 관한 정보를 찾을 수 있습니다.

<http://pubs.vmware.com/vsphere-51/index.jsp>

가상 머신을 한 데이터 저장소에서 다른 데이터 저장소로 마이그레이션할 때 두 가지 옵션이 제공됩니다.

- 전체 가상 머신을 한 번에 다른 데이터 저장소로 마이그레이션합니다.
- 개별 디스크를 다른 데이터 저장소로 마이그레이션하고, 단일 가상 머신용 디스크는 다른 데이터 저장소에 상주할 수 있습니다.

전체 가상 머신이 마이그레이션되면 VDP 어플라이언스는 보호된 VMDK의 새 위치로 백업 작업을 업데이트합니다.

VDP 6.0 이상 릴리즈부터 개별 디스크(vmdk 파일)를 한 데이터 저장소에서 다른 데이터 저장소로 마이그레이션할 경우 VDP가 데이터 저장소의 변경을 인식하고 다음 백업 중 vmdk를 적절히 백업합니다.

상태 및 백업 작업 세부 정보 보기

백업 탭에는 VDP로 생성된 백업 작업 목록이 표시됩니다. 백업 작업을 클릭하면 **백업 작업 세부 정보** 창에서 다음과 같은 작업 세부 정보를 확인할 수 있습니다.

- **이름:** 백업 작업의 이름입니다.
- **상태:** 백업 작업의 활성화 또는 비활성화 여부를 나타냅니다.
- **소스:** 백업 작업에 포함된 가상 머신 목록입니다.
- **기간 지남:** 작업이 마지막으로 실행되었을 때 백업하지 못한 모든 가상 머신 목록입니다.

백업 작업 편집

백업 작업을 생성한 후에는 해당 백업 작업을 강조 표시하고 **백업 작업 조치 > 편집**을 선택하여 해당 작업을 편집할 수 있습니다.

백업 작업 클론 생성

백업 작업을 생성한 후에는 해당 작업을 템플릿으로 사용해 해당 백업 작업을 강조 표시하고 **백업 작업 조치 > 클론**을 선택하여 다른 작업을 생성할 수 있습니다.

클론 작업을 수행하면 백업 작업 클론 생성 마법사가 시작되고 마법사의 첫 번째 세 페이지에 원래 작업의 정보(가상 머신, 스케줄, 보존 정책)가 자동으로 입력됩니다. 클론으로 생성된 작업은 고유한 이름을 필요로 합니다. 이미지 백업을 개별 디스크 백업으로 변경할 수 없고 개별 디스크 백업도 이미지 백업으로 변경할 수 없으므로, 데이터 유형을 제외하고 원래 작업에서 복제된 설정은 모두 수정할 수 있습니다.

참고 전체 이미지 백업 및 개별 디스크 백업의 클론을 생성할 수 있습니다.

백업 작업 삭제

백업 작업을 강조 표시하고 **백업 작업 조치 > 삭제**를 선택하여 해당 작업을 삭제할 수 있습니다.

참고 백업 탭에서 삭제를 사용하면 해당 작업만 삭제됩니다. 해당 작업에 따라 이전에 생성한 모든 백업 데이터는 관련 보존 정책에 따라 VDP에 의해 보존됩니다. 백업을 삭제하려면 **복구** 탭에서 삭제를 사용하십시오.

백업 작업 활성화 또는 비활성화

이후 백업 작업의 실행을 일시적으로 중지하려는 경우 백업 작업을 비활성화할 수 있습니다. 비활성화된 백업 작업을 편집 및 삭제할 수 있습니다. VDP는 비활성화된 작업이 활성화될 때까지 해당 작업을 실행하지 않습니다.

백업 작업을 강조 표시하고 **백업 작업 조치 > 활성화/비활성화**를 선택하여 백업 작업을 활성화 또는 비활성화할 수 있습니다.

기존 백업 작업 즉시 실행

다음 방법 중 하나를 사용하여 백업 작업을 즉시 실행할 수 있습니다.

- 보호된 가상 머신을 백업하도록 선택
- 기존 백업 작업을 실행하도록 선택

보호된 가상 머신 즉시 백업

- 1 다음 옵션 중 하나를 사용하여 즉시 백업하려는 보호된 가상 머신을 선택합니다.
 - 인벤토리 트리에서 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 모든 VDP 작업 > 지금 백업. 을 선택합니다. 가상 머신이 백업 작업에 속해 있어야 이 선택 항목이 나타납니다.
 - 인벤토리 트리에서 가상 머신을 클릭한 다음 **작업** 버튼을 클릭합니다. 모든 VDP 작업 > 지금 백업을 선택합니다. 가상 머신이 백업 작업에 속해 있어야 이 선택 항목이 나타납니다.
 - **보고서** 탭에서 가상 머신을 클릭하고 작업 아이콘을 클릭한 다음 **지금 백업**을 선택합니다. 지금 백업 대화상자가 나타납니다.
- 2 VDP 어플라이언스 및 백업 작업을 선택한 다음 **확인**을 클릭합니다. 백업 작업이 시작되었음을 알리는 정보 대화상자가 나타납니다.
- 3 **확인**을 클릭합니다. VDP가 백업 작업을 시작합니다.

백업 작업 즉시 실행

- 1 VDP 사용자 인터페이스의 **백업** 탭에서 즉시 실행할 작업을 클릭합니다.

백업 탭에서 Ctrl 또는 Shift 키를 누른 채 클릭하여 여러 개의 작업을 선택할 수 있습니다. 특정 백업 작업을 여러 개 선택하려면 Ctrl 키를 누른 채 클릭합니다. 일정 범위의 백업 작업을 선택하려면 Shift 키를 누른 채 클릭합니다.
- 2 **지금 백업**을 클릭합니다.

다음 옵션을 선택할 수 있는 드롭다운 선택 화면이 나타납니다.

 - **모든 소스 백업**: 백업 작업 시 모든 가상 머신을 백업합니다.
 - **기간이 지난 소스만 백업**: 백업 작업이 마지막으로 실행되었을 때 성공적으로 백업되지 않은 가상 머신만 백업합니다.
- 3 즉시 백업할 소스를 클릭합니다.
- 4 백업이 요청되었다는 메시지가 나타나면 **확인**을 클릭합니다.

VDP가 백업 작업을 시작합니다.

VDP가 백업 기간 또는 유지 보수 기간 시간대에 있는 경우 **지금 백업**을 사용하여 백업 작업을 즉시 시작할 수 있습니다.

백업 잠금 및 잠금 해제

유지 보수 기간 동안 VDP는 어플라이언스의 모든 백업을 점검하고 백업 보존 기간의 만료 여부를 평가합니다. 백업이 만료된 경우 VDP는 어플라이언스에서 만료된 백업을 제거합니다. 그러나 VDP가 백업을 삭제하지 못하도록 하려면 해당 백업을 잠그면 됩니다. VDP는 해당 백업의 잠금이 해제될 때까지 그 백업에 대한 보존 기간을 평가하지 않습니다.

참고 VDP 데이터베이스에 있는 데이터는 잠금 상태가 됩니다. 디스크를 가져오면 VDP 데이터베이스가 지워집니다 ("[기존 VDP 디스크 연결](#)"(72페이지) 참조). 디스크를 가져오면 잠금 설정된 백업에 대한 원래 만료 날짜가 "안 함"으로 재할당되므로 이 디스크를 잠금 해제할 수 없습니다.

참고 개별 디스크 백업은 잠글 수 없습니다. 전체 이미지 백업만 잠글 수 있습니다.

사전 요구 사항

- VDP가 vCenter Server에 설치 및 구성되어 있어야 합니다.
- vSphere Web Client에 로그인하고 VDP 어플라이언스에 연결합니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다.
- 2 VDP 사용자 인터페이스의 **복구** 탭에서 테이블에 표시된 백업과 연결된 펼치기 화살표를 클릭하여 잠글 백업을 찾습니다.
- 3 잠글 백업 옆의 확인란을 선택합니다.
- 4 **잠금/잠금 해제** 아이콘을 클릭합니다.
백업을 잠그면 백업 아이콘()에 잠금 아이콘이 겹쳐 표시됩니다. 이제 백업이 잠겼습니다.
- 5 백업을 잠금 해제하려면 **잠금/잠금 해제** 아이콘을 다시 클릭합니다.
잠금 표시가 지워지면 VDP가 다음 유지 보수 기간 동안 백업의 보존 날짜를 평가합니다.

VDP에서 Avamar로 백업 작업 마이그레이션

VDP 6.1을 사용하면 백업 작업과 백업 검증 작업을 Avamar로 마이그레이션할 수 있습니다. 이 마이그레이션을 통해 백업 그룹과 가상 머신 백업 검증 그룹을 타겟 Avamar 서버에서 인식하고 완전히 실행할 수 있습니다.

마이그레이션이 완료된 후:

- 데이터 세트, 보존, 스케줄 등과 같은 새로운 그룹/클라이언트 레코드 및 관련 레코드가 타겟 Avamar 서버에 있게 됩니다.
- Avamar는 마이그레이션 전에 VDP에서와 동일한 정책을 사용하여 동일한 가상 머신 클라이언트를 보호할 수 있습니다.

Guidelines

- VDP 마이그레이션은 일회성 프로세스입니다. 마이그레이션이 일단 실행된 후에는 VDP에서 추가 마이그레이션이 불가능해집니다.
- 마이그레이션 프로세스를 통해 백업 작업과 백업 검증 작업의 세부 정보만 마이그레이션됩니다.
- 애플리케이션 백업 작업 시 VDP 서버가 아닌 Avamar 서버에서 애플리케이션 클라이언트를 재등록해야 새로 마이그레이션된 작업이 적절히 실행됩니다.

권장 사항

마이그레이션을 수행하기 전에 기존의 모든 백업을 타겟 Avamar 서버로 복제합니다.

사전 요구 사항

- 소스 vCenter 클라이언트를 타겟 Avamar 서버에 사전에 등록해야 합니다. 그렇지 않으면 마이그레이션을 수행할 수 없으며, 소스 vCenter를 타겟 Avamar 서버에서 새 VMware vCenter 클라이언트로 수동으로 추가해야 합니다.
- 소스 vCenter와 함께 작동하도록 타겟에서 VMware Image Proxy를 사전에 구축 및 구성해야 합니다.

절차

- 1 웹 브라우저를 열고 주소 표시줄에 다음 URL을 입력합니다.
https://<IP_address_of_VDP_Appliance>:8543/vdp-configure/
- 2 적절한 VDP 사용자 이름과 암호를 해당 필드에 입력합니다.
- 3 **Avamar 마이그레이션** 탭에서 해당 정보를 검토합니다.
정보에 마이그레이션 기록이 있으면 VDP가 이미 마이그레이션된 것이며 다시 마이그레이션될 수 없습니다.
- 4 **마이그레이션**을 클릭합니다.

마이그레이션 마법사가 나타납니다.

- 5 **백업 작업 마이그레이션** 페이지에서 다음을 수행합니다.
 - a 작업 마이그레이션과 관련된 정보를 꼼꼼히 검토하고 장애를 방지하기 위해 필요한 작업을 수행합니다.
 - b 적절한 옵션을 선택하여 마이그레이션을 활성화합니다.
 - c 다음을 클릭합니다.
 - 6 **대상 선택** 페이지에서 다음을 수행합니다.
 - a 대상 Avamar 서버 위치와 서버 자격 증명을 적절한 필드에 입력합니다.
 - b **인증 검증**을 클릭하여 VDP와 대상 Avamar 서버 간의 연결을 테스트합니다.
 - c 다음을 클릭합니다.
 - 7 **작업 선택** 페이지에서 다음을 수행합니다.
 - a **백업 작업 및 백업 검증 작업** 탭의 테이블에서 마이그레이션할 작업을 선택합니다.
모든 작업이 기본적으로 선택됩니다. 테이블 헤더의 확인란을 선택하거나 선택 취소하여 모든 작업을 선택하거나 선택 취소할 수 있습니다.
 - b 다음을 클릭합니다.
 - 8 **검증** 페이지에서 검증 결과를 검토하고 다음을 클릭합니다.
 - 9 **완료 준비** 페이지에서 선택한 작업에 대한 요약 정보를 검토하고 **마이그레이션**을 클릭합니다.
- 마이그레이션이 완료된 후 다음 상태를 확인합니다.

- VDP가 비활성화되어 있고 **Avamar 마이그레이션** 탭에 마이그레이션 기록이 표시됩니다.
- 비활성화된 상태에서는 다음 VDP 기능만 활성화됩니다.
 - 전체 이미지 복구
 - 디스크 복구
 - 파일 레벨 복구
 - 긴급 복구
- vSphere Web Client 및 VDP 구성 클라이언트에 알림 메시지가 표시됩니다.
- 기존 백업의 보존이 동일하게 유지됩니다.

다음 추가 단계를 수행할 수 있습니다.

- 비활성화된 기능을 재활성화하려면 **활성화**를 클릭합니다.
- 대상 Avamar 서버에 등록되지 않은 클라이언트가 포함된 애플리케이션 백업 작업이 있을 경우 이러한 클라이언트를 대상 Avamar 서버에 등록해야 새로 마이그레이션된 작업이 적절히 실행됩니다. 클라이언트를 등록하려면 **마이그레이션** 마법사를 닫기 전에 **사용자 개입** 대화상자에서 정보를 검토해야 합니다. **사용자 개입** 대화상자에는 클라이언트와 클라이언트를 등록할 도메인 목록이 포함되어 있습니다. 이 목록을 확인하려면 **대상 클라이언트**를 클릭합니다.

문제 해결

- 마이그레이션이 완료된 후 실패한 작업의 목록을 확인하고, 마이그레이션을 다시 시도하거나 종료할 수 있습니다.
- **추가 정보...** 링크를 클릭하여 실패한 작업에 대한 추가 정보를 확인합니다.
- 자세한 내용은 **avamar-migration.log** 파일을 참조하십시오.

자동 백업 검증

이 장에서 다루는 내용은 다음과 같습니다.

- “자동 백업 검증 정보”(120페이지)
- “새 백업 검증 작업 생성”(121페이지)
- “백업 검증 작업 편집”(123페이지)
- “백업 검증 작업 클론 생성”(123페이지)
- “백업 검증 작업 실행”(123페이지)
- “백업 검증 모니터링”(124페이지)
- “백업 검증 작업 활성화 및 비활성화”(124페이지)
- “백업 검증 작업 삭제”(124페이지)

자동 백업 검증 정보

자동 백업 검증, 즉 ABV(Automatic Backup Verification)는 예약된 일정에 따라 또는 필요 시에 백업을 검증하여 복구 시점의 무결성을 보장하는 방법입니다. ABV에는 다음과 같은 특성이 있습니다.

- 백업은 다음과 같은 이름 규칙을 사용하여 임시 가상 머신에 복구됩니다.
`VDP_VERIFICATION_<vm-name> -<unique number>`
- ABV 작업 중에는 항상 NIC가 비활성화되기 때문에 백업은 네트워크 충돌 없이 복구됩니다. NIC가 비활성화된 상태이므로, Ping 테스트를 수행할 수 없습니다.
- 백업 검증 작업이 완료된 후 임시 가상 머신(검증 중인 가상 머신이라고도 함)은 인벤토리에서 제거 및 삭제됩니다.
- 모든 VM에 대해 마지막으로 성공한 전체 이미지 백업만 검증됩니다. 최근 작업 창과 이벤트 로그에서는 어떤 백업이 검증되었는지 보고합니다.

제한 사항

- 다음 구성에 대해서는 백업 검증이 지원되지 않습니다.
 - 단일 VMDK 백업
 - RDM 디스크의 이미지 백업(물리적 모드). RDM 가상 종속 디스크는 지원됩니다.
 - Microsoft 애플리케이션(Exchange Server, SharePoint Server 및 SQL Server)의 애플리케이션 데이터베이스 백업은 지원되지 않습니다.
 - 복제된 백업
 - 가져온 디스크에서 생성한 백업
- 대상 호스트의 경로를 변경한 경우 검증이 실패합니다. 호스트를 새 위치로 이동한 경우 검증 작업을 편집하고 대상 호스트를 다시 선택해야 합니다.
- 마찬가지로 데이터 저장소 이름을 변경한 경우 검증 작업을 편집하여 동일하거나 다른 데이터 저장소를 다시 선택해야 작업을 다시 실행할 수 있습니다.
- 일부 경우 VDP가 vCenter 인벤토리에서 검증 중인 VM을 자동으로 삭제하지 못합니다. 이 경우 검증 중인 VM을 수동으로 삭제해야 합니다.
- 4.0 이전 버전의 vSphere 호스트는 임시 가상 머신을 복구할 대상 호스트로 사용할 수 없습니다.

Best Practice

시간 및 리소스 충돌

백업 검증 기능을 사용할 때 시간 및 리소스 충돌을 방지하기 위한 조치를 취할 수 있습니다.

- 1 VDP를 처음 설치할 때 초기 전체 백업을 실행합니다.
- 2 초기 백업이 실행된 후 첫 번째 증분 백업을 실행합니다.
- 3 백업 실행 소요 시간을 결정하고 증분 백업이 완료된 후 실행할 백업 검증 작업을 예약합니다.

대상 선택

대상을 선택할 때는 다음 권장 사항을 고려하십시오.

- 여러 개의 검증 작업이 동시에 실행될 경우 로드 밸런스하십시오. 작업을 동시에 실행할 경우 작업 수를 5개로 제한하십시오.
- 임시 가상 머신이 복구될 호스트와 데이터 저장소에 충분한 가용 공간이 있어야 합니다.

일반

- 가상 머신 백업 시점에 VMware Tools가 해당 가상 머신에 설치되어 있는지 확인하십시오.

- 하트비트 시간 초과 간격을 환경에 따라 최적의 값으로 설정하십시오. 참고로, 일부 가상 머신은 VMware Tools 하트비트 송수신 시간이 다른 가상 머신보다 더 오래 걸릴 수 있습니다.
- 대상 호스트 및 데이터 저장소의 가용성을 주기적으로 확인하십시오. 작업을 편집하고 필요한 경우 대상을 재구성하십시오. 대상 호스트 또는 데이터 저장소를 사용할 수 없는 경우 작업을 편집하여 새 대상을 선택하십시오.
- 고급 검증 옵션으로 검증 스크립트를 선택하기 전에 게스트 운영 체제에서 스크립트를 수동으로 실행하여 성공적으로 실행되는지 확인하십시오.

새 백업 검증 작업 생성

백업 검증 작업은 필요 시 또는 스케줄의 일부로 실행됩니다. 백업 탭의 백업 검증 섹션을 사용하여 백업 검증 작업을 생성하고 관리할 수 있습니다.

사전 요구 사항

- 백업 작업 또는 복구 시점이 있어야 가상 머신의 검증 작업을 생성할 수 있습니다. 백업 작업 및 복구 유형은 전체 이미지여야 합니다.
- 백업 시 가상 머신에 VMware Tools가 설치되어 있어야 합니다. 검증 중인 VM에서 VMware Tools를 찾을 수 없는 경우 하트비트 검증이 실패합니다.
- 선택한 데이터 저장소에는 사용 가능한 공간이 충분해야 합니다.
- 검증 스크립트를 사용하려는 경우 네트워크의 다른 VM과의 연결에 따라 검증 스크립트가 달라지면 안 됩니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다.
- 2 백업 탭을 클릭합니다.
- 3 백업 탭에서 백업 검증을 클릭합니다.
- 4 백업 검증 작업 조치 메뉴에서 새로 만들기를 선택합니다.
새 백업 검증 작업 생성 마법사가 가상 머신 페이지에 열립니다.
- 5 가상 머신 페이지에서 검증 작업을 생성하려는 가상 머신을 선택한 후 다음을 클릭합니다.
 - 검증별로 가상 머신을 하나씩만 선택할 수 있습니다. 항목을 여러 개 선택하는 것은 지원되지 않습니다.
 - 가상 머신은 전체 이미지 백업 작업에 포함되어야 합니다. 또는 복구 시점을 포함해도 됩니다.
 - 필요한 경우 가상 머신의 이름을 기준으로 필터링할 수 있습니다.
 - 가상 머신 백업에 VMware Tools가 있어야 하며, 그렇지 않으면 검증 작업이 실패합니다.
- 6 검증 옵션 페이지에서 옵션을 선택합니다.
 - **하트비트 검증:** 이 옵션이 스크립트 검증 선택 여부와 관계없이 백업 검증을 위한 기본 옵션입니다. 하트비트 검증에서는 가상 머신의 전원이 켜진 후 특정 시간 내에 VMware Tools 하트비트가 수신되었는지 여부를 점검합니다. VMware Tools 하트비트가 수신된 경우 게스트 운영 체제가 성공적으로 부팅되어 안정적인 상태에 있음을 나타냅니다.

참고 게스트 운영 체제 하트비트는 검증에 대한 기본 옵션입니다.

- **스크립트 검증:** 이 옵션은 고급 검증 옵션입니다. 가상 머신에 대해 게스트 운영 체제에서 실행되는 애플리케이션 및 서비스의 상태를 검증하려면 스크립트 검증을 사용합니다. 스크립트는 사전 정의되어야 하며 게스트 운영 체제에 미리 존재해야 합니다. 네트워크의 다른 가상 머신과의 연결에 따라 검증 스크립트가 달라지면 안 됩니다.

게스트 운영 체제에서 스크립트를 실행하기로 선택한 경우 다음 정보를 지정합니다.

- **Username:** 게스트 운영 체제에 로그인할 때 사용되는 사용자 ID를 입력합니다.

- **암호:** 게스트 운영 체제에 로그인할 때 사용되는 암호를 입력합니다.
- **암호 확인:** 암호를 다시 입력하십시오.
- **게스트에 대한 검증 스크립트:** 게스트 운영 체제의 스크립트 위치에 대한 전체 경로를 입력합니다. 스크립트 구성에 대한 자세한 내용은 “[검증 스크립트 구성](#)”(122페이지) 섹션을 참조하십시오.

7 다음을 클릭합니다.

8 대상 페이지에서 대상을 선택합니다.

- **대상 경로:** 검증 중인 가상 머신과 대상 호스트가 호환되어야 하며, 대상 호스트에 검증 중인 가상 머신을 복구할 리소스가 충분해야 합니다. 검증하기 위해 백업을 임시로 복구할 대상으로 독립 실행형 호스트나 클러스터 내 호스트를 선택해야 합니다. 리소스 풀 및 vApp은 유효한 대상으로 사용할 수 없습니다. 4.0 이전 버전의 vSphere 호스트는 지원되지 않습니다.
- **데이터 저장소:** 선택한 호스트에 따라 데이터 저장소 목록이 표시됩니다. 검증 중인 가상 머신을 복구할 데이터 저장소를 하나만 선택해야 합니다. 선택한 데이터 저장소에 충분한 공간이 있는지 확인하십시오.

9 다음을 클릭합니다.

10 스케줄 페이지에서 실행할 백업 검증 작업의 스케줄을 선택합니다. 이 페이지에서 선택한 설정에 따라 검증 작업의 실행 빈도와 일시가 결정됩니다.

- a **백업 검증 스케줄:** 간격을 매일, 매주 또는 매월로 지정합니다.
- b **서버에서 시작 시간:** 예약한 날에 백업 검증을 수행할 시간을 지정합니다.

11 다음을 클릭합니다.

12 작업 이름 페이지에서 검증 작업을 식별할 고유한 이름을 입력한 후 다음을 클릭합니다.

검증 작업 이름은 모든 영문자와 숫자를 포함할 수 있습니다. 특수 문자는 공백, 밑줄, 하이픈 및 마침표만 허용됩니다.

13 완료 준비 페이지에서 생성할 백업 검증 작업의 요약 검토합니다. 필요한 경우 뒤로를 클릭하여 해당 페이지로 돌아가서 작업 구성을 변경할 수 있습니다. 작업을 저장할 준비가 되면 **마침**을 클릭합니다.

참고 또한 복구 탭의 백업 검증 섹션에서 백업 검증 작업에 대한 요약 검토할 수 있습니다.

14 백업 검증 작업이 성공적으로 생성되었다는 메시지가 나타나면 **확인**을 클릭합니다.

검증 스크립트 구성

검증 스크립트를 사용하려는 경우 지원되는 스크립트 형식은 .bat, .cmd, .sh 및 .exe입니다. 유효한 스크립트 파일은 File Manager나 탐색기 보기에서 파일을 두 번 클릭하여 실행할 수 있습니다. 스크립트가 지원되지 않는 형식인 경우에는 지원되는 형식 내에 스크립트 실행을 포함해야 합니다.

예를 들어 .ps 형식은 지원되지 않으므로 Windows Power Shell(.ps1) 스크립트는 VDP를 사용하여 직접 호출하거나 실행할 수 없습니다. 그러나 지원되는 형식(예: .bat)을 통해 .ps 스크립트를 호출한 다음 게스트 OS에서 스크립트 위치의 전체 경로를 지정할 수 있습니다. 스크립트를 실행하기 전에 실행 정책을 **제한 없음**으로 설정해야 합니다.

스크립트는 0 또는 0이 아닌 정수를 반환해야 합니다. 0이 반환된 경우 스크립트 검증이 성공한 것입니다. 0이 아닌 정수가 반환된 경우 스크립트 검증이 실패한 것입니다.

백업 검증 작업 편집

백업 검증 작업을 생성한 후 필요에 따라 편집할 수 있습니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다.
- 2 **백업** 탭을 클릭합니다.
- 3 **백업** 탭에서 **백업 검증**을 클릭합니다.
- 4 편집할 백업 검증 작업을 선택한 다음 **백업 검증 작업 조치** 메뉴에서 **편집**을 선택합니다.
백업 검증 작업 편집: *job_name* 마법사가 가상 머신 페이지에 열립니다.
- 5 마법사를 진행하는 동안 필요한 경우 변경합니다.
- 6 변경 사항을 완료하면 **마침**을 클릭합니다.
- 7 백업 검증 작업이 성공적으로 저장되었다는 메시지가 나타나면 **확인**을 클릭합니다.

백업 검증 작업 클론 생성

검증 작업을 강조 표시하고 **백업 검증 작업 조치** > **클론**을 선택하면 해당 검증 작업을 템플릿으로 사용해 다른 작업을 생성할 수 있습니다.

클론 작업을 수행하면 백업 검증 작업 클론 생성 마법사가 시작되고 마법사의 첫 번째 세 페이지에 원래 작업의 정보(가상 머신, 스케줄, 보존 정책)가 자동으로 입력됩니다. 클론으로 생성된 작업은 고유한 이름을 필요로 합니다.

백업 검증 작업 실행

백업 검증 작업을 생성하고 난 후에는 필요 시 검증을 실행하거나 스케줄에 따라 백업 검증 작업이 시작될 때까지 기다려 검증을 호출할 수 있습니다. 완전한 백업 검증 주기는 다음과 같습니다.

- **복구**: 선택한 가상 머신에 대한 최신 백업이 임시 가상 머신으로 복구됩니다. 임시 가상 머신은 백업 검증 후 삭제됩니다.
- **전원 켜기**: 임시 가상 머신이 복구된 후에는 전원이 켜지기 전에 NIC를 비활성화하도록 구성됩니다.
- **부팅 OS**: 가상 머신의 전원이 켜진 후 게스트 운영 체제가 완전히 부팅될 때까지 기다립니다.
- **하트비트 검증**: 게스트 OS가 부팅된 후에 어플라이언스는 복구된 가상 머신에서 VMware Tools 하트비트를 수신 대기합니다. 어떤 이유로든 하트비트가 수신되지 않은 경우 검증 작업은 실패하고 백업은 양호한 상태에 있지 않게 됩니다.
- **검증 스크립트**: 스크립트는 고급 레벨의 검증(검증 스크립트)을 선택한 경우에만 실행됩니다. 이 기능은 사용자가 정의 및 지정한 맞춤형 스크립트를 실행하여 게스트 운영 체제에서 실행 중인 애플리케이션의 상태를 검증합니다.
- **전원 끄기**: 스크립트 검증이 완료된 후에는 가상 머신의 전원이 꺼집니다.
- **가상 머신 삭제**: 이 마지막 단계에서는 복구된 가상 머신이 삭제되고 vCenter에서(최근 작업 창 및 이벤트 로그에서) 검증 결과를 보고합니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다.
- 2 **백업** 탭을 클릭합니다.
- 3 **백업** 탭에서 **백업 검증**을 클릭합니다.
- 4 실행할 백업 검증 작업을 선택한 다음 **지금 검증**을 클릭합니다.
- 5 백업 검증 요청이 성공적으로 실행되었다는 메시지가 나타나면 **확인**을 클릭합니다.

백업 검증 모니터링

모든 가상 머신에 대해 마지막으로 성공한 백업만 검증됩니다. 아래 방법 중 하나를 사용하여 검증 작업 결과를 확인할 수 있습니다.

- vCenter 작업/이벤트
- 보고서 탭. 자세한 내용은 “[보고서 탭에서 정보 보기](#)”(106페이지) 섹션을 참조하십시오.
- e-메일 보고서 자세한 내용은 “[e-메일 알림 및 보고서 구성](#)”(55페이지) 섹션을 참조하십시오.
- 클라이언트 로그. <https://<IP address or hostname of VDP>:8543/vdp-configure>에서 클라이언트 로그를 다운로드할 수 있습니다.

백업 검증 작업 활성화 및 비활성화

백업 검증 작업을 생성한 후 필요에 따라 활성화 및 비활성화할 수 있습니다. 백업 검증 작업을 비활성화하면 활성화할 때까지 다시 실행되지 않습니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다. 지침은 “[백업 작업](#)”(110페이지) 섹션을 참조하십시오.
- 2 **백업** 탭을 클릭합니다.
- 3 **백업** 탭에서 **백업 검증**을 클릭합니다.
- 4 활성화 또는 비활성화할 백업 검증 작업을 선택하고 **백업 검증 작업 조치** 메뉴에서 **활성화/비활성화**를 선택합니다.
- 5 백업 검증 작업이 성공적으로 활성화 또는 비활성화되었다는 메시지가 나타나면 **확인**을 클릭합니다.

백업 검증 작업 삭제

더 이상 필요하지 않은 백업 검증 작업은 삭제할 수 있습니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다. 지침은 “[백업 작업](#)”(110페이지) 섹션을 참조하십시오.
- 2 **백업** 탭을 클릭합니다.
- 3 **백업** 탭에서 **백업 검증**을 클릭합니다.
- 4 삭제할 백업 검증 작업을 선택하고 **백업 검증 작업 조치** 메뉴에서 **삭제**를 선택합니다.
- 5 선택한 작업을 삭제할지 확인하는 메시지가 나타나면 **예**를 클릭합니다.
- 6 백업 검증 작업이 성공적으로 삭제되었다는 메시지가 나타나면 **확인**을 클릭합니다.

복구 관리

이 장에서 다루는 내용은 다음과 같습니다.

- “복구 작업”(126페이지)
- “복구할 백업 선택”(126페이지)
- “백업 목록 필터링”(127페이지)
- “스냅샷이 존재할 때 복구”(127페이지)
- “이미지 백업을 원래 위치로 복구”(127페이지)
- “이미지 백업을 새 위치로 복구”(129페이지)
- “개별 SCSI 디스크로 백업 복구”(130페이지)
- “복구 탭에서 백업 삭제”(131페이지)
- “복구 탭에서 선택한 모든 백업 지우기”(131페이지)

복구 작업

가상 머신을 백업한 후 백업을 원래 위치나 대체 위치로 복구할 수 있습니다.

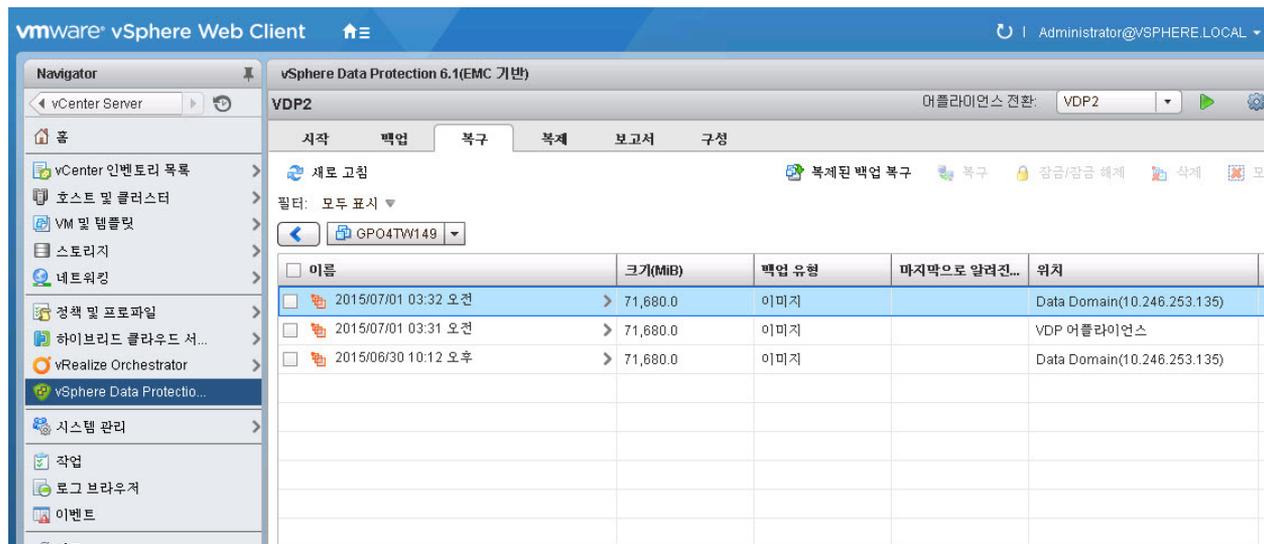
복구 작업은 **복구** 탭에서 수행됩니다. **복구** 탭에는 VDP 어플라이언스에 의해 백업된 가상 머신 목록이 표시됩니다. 백업 목록을 탐색하여 특정 백업을 선택 및 복구할 수 있습니다. 이 목록에는 장애 발생 시 경합성이 보장되는 백업과 애플리케이션 경합성이 보장되는 백업에 대한 아이콘이 표시됩니다.

아이콘 관련 정보는 페이지의 왼쪽 아래에 있는 범례를 참조하십시오. 복구할 백업을 선택하기 전에 장애 발생 시 경합성이 보장되는 백업과 해당 백업의 만료 날짜를 확인하십시오.

참고 애플리케이션 경합성이 보장되는 백업의 삭제는 Windows 클라이언트에만 적용됩니다. Linux 클라이언트에서는 애플리케이션 경합성이 보장되는 백업이 **경합성 수준이 올바르지 않음** 아이콘과 함께 나타납니다.

복구 탭에 표시되는 정보는 시간이 지나면서 오래된 정보가 됩니다. 복구할 수 있는 백업에 대한 최신 정보를 확인하려면 **새로 고침**을 클릭하십시오.

다음 그림에는 **복구** 탭이 나와 있습니다.



제한 사항

- 복구 마법사에서는 동일한 MSApp 클라이언트에 대해 여러 복구 시점을 선택할 수 없습니다. 동일한 클라이언트의 복구 시점은 한 번에 하나만 선택할 수 있습니다.
- 타겟 가상 머신에 SCSI 버스 공유가 구성된 경우 해당 가상 머신으로의 복구는 지원되지 않습니다.

복구할 백업 선택

백업은 다음 옵션을 통해 복구할 수 있습니다.

- VDP UI의 시작 탭에서 **백업 복구**를 클릭합니다.
- 복구 탭에서 복구 시점을 선택하고 **복구**를 클릭합니다.
- vCenter 인벤토리 목록에서 보호된 가상 머신을 마우스 오른쪽 버튼으로 클릭한 다음 모든 **VDP 작업 > 복구 테스트**를 선택합니다. 백업 선택 페이지에 백업 목록이 표시됩니다.

백업 목록 필터링

복구할 수 있는 백업 목록은 다음과 같은 방법으로 드롭다운 화살표를 사용하여 필터링할 수 있습니다.

- **백업 날짜:** "다음 날짜 이전", "다음 날짜 이후", "다음 날짜" 또는 "다음 날짜 이외" 기준으로 필터링
- **클라이언트 이름:** "포함", "포함하지 않음", "같음" 또는 "같지 않음" 기준으로 필터링
- **위치:** 백업 위치를 기준으로 필터링

새로 고침 버튼을 클릭하거나 필터 드롭다운 메뉴에서 모두 표시를 선택하여 필터를 지우십시오.

백업 선택 페이지에서 복구할 가상 머신을 선택할 수 있습니다.

스냅샷이 존재할 때 복구

이전 버전의 VDP에서는 가상 머신에 스냅샷이 포함되어 있는 경우에도 원래 가상 머신으로 복구를 수행할 수 있었습니다. VDP 버전 5.5 이상에서는 가상 머신에 스냅샷이 있으면 복구를 수행할 수 없습니다.

주의 복구를 수행하기 전에 가상 머신에서 존재할 수 있는 스냅샷을 모두 제거하십시오. 타겟 가상 머신에 스냅샷이 포함되어 있으면 복구 작업이 실패합니다.

스냅샷을 올바르게 사용하는 방법에 관해서는 다음 기술 자료 문서를 참조하십시오.

- <http://kb.vmware.com/kb/1025279>
- <https://community.emc.com/thread/145249?start=0&start=0>

이미지 백업을 원래 위치로 복구

백업 복구 마법사를 사용하여 수동으로 백업을 복구할 수 있습니다.

전체 가상 머신이 아니라 개별 디스크를 복구하도록 선택한 경우 원래 위치에 복구할 수 없는 세 가지 시나리오가 있습니다.

- 원본 디스크가 독립 - 영구(Independent - Persistent)로 표시되어 있습니다.
- 원본 디스크가 타겟 가상 머신에서 제거되었습니다.
- 원본 디스크가 타겟 가상 머신에서 삭제되었습니다.

참고 서로 다른 두 가지 타임 스탬프에서 동일한 디스크를 복구하는 작업은 허용되지 않습니다. 서로 다른 두 가지 타임 스탬프로 백업된 디스크의 복구를 시도하는 경우 중복된 하드 디스크 제거 옵션이 제공됩니다. 중복된 하드 디스크가 제거될 때까지 복구는 진행되지 않습니다.

사전 요구 사항

- VDP가 vCenter Server에 설치 및 구성되어 있어야 합니다.
- vSphere Web Client에 로그인하고 VDP 어플라이언스에 연결합니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다.
- 2 복구 탭을 클릭합니다.
- 3 필요한 경우 검색 범위를 좁혀서 백업을 필터링합니다.
- 4 이름 열에 나열된 가상 머신을 선택합니다. 가상 머신을 클릭하면 수행된 백업 목록으로 확장됩니다. 하나 이상의 백업을 선택하거나 하나의 백업을 클릭하고 복구할 디스크를 찾을 수 있습니다.

참고 초기 구성 중 상이한 VDP 어플라이언스에서 스토리지를 가져온 경우 클라이언트(가상 머신) 이름은 복구 탭의 **VDP_IMPORT** 도메인에서 임의 문자로 이루어진 문자열을 추가하여 변경됩니다.

- 5 하나 이상의 항목을 복구하도록 선택하려면 각 항목 옆에 있는 확인란을 선택합니다.
- 6 복구를 클릭하여 백업 복구 마법사를 시작합니다.

- 7 **백업 선택** 페이지에서 다음을 수행합니다.
 - a 선택한 백업 목록에서 장애 발생 시 정합성이 보장되는 백업을 확인합니다. 장애 발생 시 정합성이 보장되는 백업을 복구하지 않으려면 해당 백업을 제거합니다.
 - b 다음을 클릭합니다.
- 8 **복구 옵션 설정** 페이지에서 다음을 수행합니다.
 - a **원래 위치로 복구** 옵션이 선택된 상태로 둡니다. 원래 위치에 vmdk 파일이 있는 경우 해당 파일을 덮어씁니다.

참고 원래 가상 머신의 가상 디스크가 제거되었거나 삭제된 경우에는 원래 위치로 복구 옵션을 사용할 수 없습니다. VMDK는 새 위치에 복구해야 합니다.

- b 가상 머신을 해당 구성과 함께 복구하려면 **가상 머신 및 구성 복구**를 선택합니다.
 - c 다음을 클릭합니다.
- 9 **완료 준비** 페이지에서 다음을 수행합니다.
 - a 복구 요청에 대한 요약을 검토합니다.
요약에는 다음 정보가 표시됩니다.
 - 교체 또는 원래 위치로 복구할 가상 머신의 수 그리고 생성하거나 새 위치로 복구할 머신의 수
 - 복구를 위해 선택한 백업 목록에 장애 발생 시 정합성이 보장되는 백업이 포함된 경우 복구를 계속 진행할지 여부를 선택하는 확인란

장애 발생 시 정합성이 보장되는 복구를 진행하도록 선택하면, 경우에 따라 복구가 실패합니다.

복구 설정을 변경하려는 경우 마법사 페이지에서 **뒤로** 버튼을 클릭하거나 마법사 화면 왼쪽에서 해당 번호의 단계 제목을 클릭하여 해당 페이지로 돌아갑니다.
 - b **마침**을 클릭하여 복구 작업을 시작합니다.
복구가 시작되었다는 메시지가 표시됩니다.
 - c **확인**을 클릭합니다.
- 10 **최근 작업** 창에서 복구의 진행률을 모니터링합니다.

참고 복구 프로세스 동안 **NIC 다시 연결**을 선택한 경우 새로 생성된 가상 머신에 대한 네트워크 구성을 확인합니다. 새 가상 머신 NIC는 원래 가상 머신과 동일한 IP 주소를 사용할 수 있지만, 이로 인해 충돌이 발생할 수 있습니다.

이미지 백업을 새 위치로 복구

백업 복구 마법사를 사용하여 수동으로 백업을 복구할 수 있습니다. 백업 복구 마법사의 복구 옵션 설정 페이지에서 이미지 백업을 복구할 위치를 지정할 수 있습니다.

사전 요구 사항

- VDP가 vCenter Server에 설치 및 구성되어 있어야 합니다.
- vSphere Web Client에 로그인하고 VDP 어플라이언스에 연결합니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다.
- 2 **복구** 탭을 클릭합니다.
- 3 필요한 경우 검색 범위를 좁혀서 백업을 필터링합니다.
- 4 이름 열에 나열된 가상 머신을 선택합니다. 클라이언트(가상 머신)를 클릭하면 수행된 백업의 목록으로 확장됩니다. 하나 이상의 백업을 선택하거나 하나의 백업을 클릭하고 복구할 디스크 또는 애플리케이션을 찾을 때까지 드릴다운할 수 있습니다.

참고 이름 열에 나타나는 클라이언트 이름은 초기 구성 중 상이한 VDP 어플라이언스에서 스토리지를 가져온 경우 임의 문자로 이루어진 문자열을 추가하여 변경됩니다.

- 5 하나 이상의 항목을 복구하도록 선택하려면 각 항목 옆에 있는 확인란을 선택합니다.
- 6 **복구**를 클릭하여 백업 복구 마법사를 시작합니다.
- 7 **백업 선택** 페이지에서 복구할 백업을 클릭하고 **다음**을 클릭합니다.
- 8 **복구 옵션 설정** 페이지에서 다음을 수행합니다.
 - a **원래 위치로 복구** 확인란의 선택을 취소하고 새 위치로 복구할 각 백업에 대한 복구 옵션을 설정합니다.
 - b 다음 필드에 정보를 지정합니다.
 - **새 가상 머신 이름:** 복구된 가상 머신의 새 이름을 입력합니다.
 - **대상:** 선택을 클릭하고 새 대상을 선택합니다.
 - **데이터 저장소:** 가상 머신이 복구될 데이터 저장소를 선택합니다.
 - c **다음**을 클릭합니다.
- 9 **완료 준비** 페이지에서 다음을 수행합니다.
 - a 복구 요청에 대한 요약 검토합니다.

이 요약 정보에서 교체 또는 원래 위치로 복구할 가상 머신의 수, 그리고 생성 또는 새 위치로 복구할 가상 머신의 수를 확인할 수 있습니다.

복구 요청에 대한 설정을 변경하려는 경우 **뒤로** 버튼을 클릭하여 해당 화면으로 돌아가거나 마법사 화면 왼쪽에서 해당 번호의 단계 제목을 클릭하십시오.
 - b **마침**을 클릭하여 복구 작업을 시작합니다.

복구가 시작되었다는 메시지가 표시됩니다.
 - c **확인**을 클릭합니다.
- 10 **최근 작업** 창에서 복구의 진행률을 모니터링합니다.

참고 복구 프로세스 동안 **NIC 다시 연결**을 선택한 경우 새로 생성된 가상 머신에 대한 네트워크 구성을 확인합니다. 새 가상 머신 NIC는 원래 가상 머신과 동일한 IP 주소를 사용할 수 있지만, 이로 인해 충돌이 발생할 수 있습니다.

새 위치로 복구 실행 전 vMotion 기능 해제

vSphere vMotion 기능을 사용하면 실행 중인 가상 머신을 한 물리적 서버에서 다른 물리적 서버로 라이브 마이그레이션할 수 있습니다. 백업 또는 복구를 수행하는 동안 VDP 어플라이언스에서 vMotion 작업이 실행되지 않는지 확인합니다. 자세한 내용은 “백업 작업이 활성화된 경우에는 Storage vMotion 작업이 허용되지 않습니다.”(196페이지)을 참조하십시오.

백업 윈도우 중에 그리고 새 위치로 복구를 수행하기 전에 VM과 데이터 저장소 레벨에서 vMotion 기능을 비활성화합니다.

- 1 웹 브라우저에서 다음 주소로 vSphere Web Client에 액세스합니다.
https://<IP_address_vCenter_Server>:9443/vsphere-client/
- 2 **vCenter > 호스트 및 클러스터**를 선택합니다.
- 3 **DRS** 탭에서 왼쪽 메뉴에 나열된 모든 DRS 클러스터에 대해 **수동**을 선택합니다.
- 4 **인벤토리 > 데이터 저장소**를 선택합니다.
- 5 가상 머신, 프록시 및 VDP가 상주하는 각 데이터 저장소에 대해 다음을 수행합니다.
 - a 데이터 저장소를 선택합니다.
 - b **Edit Settings**를 선택합니다.
 - c 왼쪽 메뉴의 **일반** 아래에서 **SDRS 자동화**를 클릭합니다.
 - d 오른쪽 창에서 **자동화 기능 제공 안 함(수동)**을 선택합니다.
 - e **가상 머신 설정**을 선택합니다.
 - f 모든 가상 머신에 대해 SDRS 자동화가 **해제됨** 또는 **수동**으로 표시되는지 확인합니다.

개별 SCSI 디스크로 백업 복구

백업 복구 마법사를 사용하여 개별 SCSI 디스크로 백업을 복구할 수 있습니다. 백업 복구 마법사의 복구 옵션 설정 페이지에서 개별 SCSI 디스크를 복구할 위치를 지정할 수 있습니다.

참고 SCSI ID는 서로 다른 VM의 여러 복구 요청을 지원하지 않습니다. 여러 복구 작업을 시작할 수는 있지만 첫 번째 복구만 성공합니다. 원래 또는 기존 가상 머신에서 여러 개의 디스크를 새 디스크로 복구하는 경우 복구할 모든 디스크는 동일한 백업 및 동일한 가상 머신에서 온 디스크여야 합니다.

사전 요구 사항

- VDP가 vCenter Server에 설치 및 구성되어 있어야 합니다.
- vSphere Web Client에 로그인하고 VDP 어플라이언스에 연결합니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다.
- 2 **복구** 탭을 클릭합니다.
- 3 필요한 경우 검색 범위를 좁혀서 백업을 필터링합니다.
- 4 이름 열에 나열된 가상 머신을 선택합니다. 클라이언트(가상 머신)를 클릭하면 수행된 백업의 목록으로 확장됩니다. 하나 이상의 백업을 선택하거나 하나의 백업을 클릭하고 복구할 디스크 또는 애플리케이션을 찾을 때까지 드릴다운할 수 있습니다.

참고 이름 열에 나타나는 클라이언트 이름은 초기 구성 중 상이한 VDP 어플라이언스에서 스토리지를 가져온 경우 임의 문자로 이루어진 문자열을 추가하여 변경됩니다.

- 5 하나 이상의 항목을 복구하도록 선택하려면 각 항목 옆에 있는 확인란을 선택합니다.
- 6 **복구**를 클릭하여 백업 복구 마법사를 시작합니다.
- 7 **백업 선택** 페이지에서 복구할 백업을 클릭하고 다음을 클릭합니다.

- 8 복구 옵션 설정 페이지에서 원래 위치로 복구 확인란의 선택을 취소하고 새 위치로 복구할 각 백업에 대한 복구 옵션을 설정합니다.
 - a 다음 정보를 지정합니다.
 - 대상: 새 대상을 선택하려면 선택을 클릭합니다. 백업이 복구될 새 위치 대상 컨테이너(vApp, 리소스 풀, 호스트 또는 데이터 센터)를 선택하거나 기존 가상 머신의 원래 위치인 기본 대상을 적용할 수 있습니다.
 - 새 가상 머신 이름: 새 가상 머신 이름 필드는 기존 가상 머신 이름으로 자동 입력됩니다. 컨테이너로 복구하는 경우 이 필드를 수정하여 가상 머신에 새 이름을 지정할 수 있습니다. 기존 가상 머신으로 복구하는 경우 이름을 수정할 수 없습니다.
 - 데이터 저장소: 첫 번째 디스크가 현재 상주하는 데이터 저장소를 나열합니다. 디스크를 기존 가상 머신으로 복구하는 경우 이 필드를 편집할 수 없습니다. 디스크를 새 컨테이너로 복구하는 경우 가상 머신이 복구될 데이터 저장소를 선택하십시오.
 - 디스크 ID: 복구 타겟으로 사용 가능한 SCSI 디스크 ID 슬롯을 나열합니다. 목록에는 현재 가상 머신에 연결된 SCSI 컨트롤러의 빈 SCSI 슬롯만 표시됩니다. 목록에서 복구 타겟으로 SCSI 가상 디스크 슬롯을 선택하십시오.

IDE로 구성된 가상 디스크로는 복구할 수 없습니다. SCSI 가상 디스크만 지원됩니다. SCSI 컨트롤러에서는 최대 15개의 디스크가 허용됩니다. 슬롯 7은 예약되어 있으며 사용할 수 없습니다.

참고 백업 복구 마법사에서는 사용 가능한 SCSI 슬롯이 부족해도 새 컨트롤러를 자동으로 추가하지 않습니다. 디스크 복구를 시작하기 전에 새 SCSI 컨트롤러를 추가해야 합니다.

 - b 다음을 클릭합니다.
- 9 완료 준비 페이지에서 다음을 수행합니다.
 - a 복구 요청에 대한 요약 검토합니다.

이 요약 정보에서 교체 또는 원래 위치로 복구할 가상 머신의 수, 그리고 생성 또는 새 위치로 복구할 가상 머신의 수를 확인할 수 있습니다.

복구 요청에 대한 설정을 변경하려는 경우 뒤로 버튼을 클릭하여 해당 화면으로 돌아가거나 마법사 화면 왼쪽에서 해당 번호의 단계 제목을 클릭하십시오.
 - b 마침을 클릭하여 복구 작업을 시작합니다.

복구가 시작되었다는 메시지가 표시됩니다.
 - c 확인을 클릭합니다.
- 10 최근 작업 창에서 복구의 진행률을 모니터링합니다.

복구 탭에서 백업 삭제

VDP가 백업 작업에 설정된 보존 정책에 따라 백업을 삭제합니다. 그러나 복구 탭에서 삭제할 백업 작업을 선택하고 삭제 아이콘을 클릭하여 백업 작업을 수동으로 삭제할 수 있습니다.

복구 탭에서 선택한 모든 백업 지우기

- 1 수동 복구 탭의 백업 목록에서 지울 백업을 선택한 다음 모든 선택 항목 지우기를 클릭합니다.
- 2 새로 고침 버튼을 클릭하여 복구 탭의 데이터를 업데이트합니다.

이 장에서 다루는 내용은 다음과 같습니다.

- “복제 작업”(134페이지)
- “복제 작업 생성”(137페이지)
- “대상 관리”(140페이지)
- “복제 작업 편집”(141페이지)
- “복제 작업 클론 생성”(141페이지)
- “복제 작업 삭제”(141페이지)
- “복제 작업 활성화 또는 비활성화”(141페이지)
- “상태 및 복제 작업 세부 정보 보기”(141페이지)
- “기존 복제 작업 즉시 실행”(141페이지)
- “소스로 다시 복제”(142페이지)
- “복제 복구 호환성”(143페이지)
- “복제 복구 활성화 또는 비활성화”(143페이지)
- “복제 복구”(143페이지)
- “멀티 테넌시”(144페이지)

복제 작업

복제를 사용하면 소스 VDP 어플라이언스에서 장애가 발생한 경우에 대상 타겟에 있는 백업 복제본을 사용할 수 있으므로 데이터 손실을 방지할 수 있습니다. 복제 작업은 복제할 백업과 백업을 복제할 시간 및 위치를 결정합니다. 복구 시점이 없는 클라이언트에 대한 예약 복제 작업 또는 임시 복제 작업의 경우 클라이언트는 대상 서버에서만 복제될 수 있습니다. VDP 어플라이언스로 생성된 백업은 다른 VDP 어플라이언스, Avamar 서버 또는 Data Domain 시스템에 복제될 수 있습니다.

복제 호환성

표 15-20 및 표 15-21에는 백업을 생성하는 데 사용된 VDP 제품에 따라 복제할 수 있는 백업과 복제할 수 없는 백업이 정리되어 있습니다.

이러한 표에서는 다음과 같은 약어가 사용됩니다.

- **VDP-A:** VDP Advanced 어플라이언스
- **RTI:** 복제 타겟 ID

중요 VDP Advanced는 VDP 5.8 이하에 적용됩니다. RTI는 VDP 5.8에만 적용됩니다.

- **DD:** Data Domain 시스템
- **N:** 아니요. 타겟이 지원되지 않음
- **Y:** 예. 타겟이 지원됨
- **(R):** 권장
- **(NR):** 권장하지 않음
- **(HP):** 해시된 암호

표 15-20. 복제 소스 매트릭스 - 1부

다음 제품을 사용하여 생성된 백업...	복제 가능한 타겟															
	VDP 5.5.1.x	VDP 5.5.1.x	VDP 5.5.5.x	VDP-A 5.5.5.x	VDP-A 5.5.5.x + DD	VDP 5.5.6.x	VDP-A 5.5.6.x	VDP-A 5.5.6.x + DD	VDP 5.8.x	VDP-A 5.8.x	VDP-A 5.8.x + DD	VDP 6.0.x	VDP 6.0.x + DD	VDP 6.1.x	VDP 6.1.x + DD	
VDP 5.5.1.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
VDP 5.5.1.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
VDP 5.5.5.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
VDP-A 5.5.5.x	N	N	N	Y (R)	Y (R)	N	Y	Y	N	Y(H P)	Y(H P)	Y(H P)	Y (HP)	Y (HP)	Y (HP)	
VDP-A 5.5.5.x + DD	N	N	N	N	Y (R)	N	N	Y	N	N	Y(H P)	N	Y (HP)	N	Y (HP)	
VDP 5.5.6.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
VDP-A 5.5.6.x	N	N	N	Y	Y	N	Y	Y	N	Y(H P)	Y (HP)	Y (HP)	Y (HP)	Y (HP)	Y (HP)	
VDP-A 5.5.6.x + DD	N	N	N	N	Y	N	N	Y	N	N	Y(H P)	N	Y(H P)	N	Y (HP)	
VDP 5.8.x	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
VDP-A 5.8.x	N	N	N	Y	Y	N	Y	Y	N	Y(R)	Y	Y(R)	Y	Y(R)	Y	
VDP-A 5.8.x + DD	N	N	N	N	Y	N	N	Y	N	N	Y(R)	N	Y(R)	N	Y(R)	
RTI 5.8.x	N	N	N	Y	Y	N	Y	Y	N	Y(R)	Y	Y(R)	Y	Y(R)	Y	
RTI 5.8.x + DD	N	N	N	N	Y	N	N	Y	N	N	Y(R)	N	Y(R)	N	Y(R)	
VDP 6.0.x	N	N	N	Y	Y (R)	N	Y	Y (R)	N	Y	Y (R)	Y	Y (R)	Y	Y (R)	

표 15-20. 복제 소스 매트릭스 - 1부 (계속)

다음 제품을 사용하여 생성된 백업...	복제 가능한 타겟														
	VDP 5.5.1.x	VDP 5.5.1.x	VDP 5.5.5.x	VDP-A 5.5.5.x	VDP-A 5.5.5.x + DD	VDP 5.5.6.x	VDP-A 5.5.6.x	VDP-A 5.5.6.x + DD	VDP 5.8.x	VDP-A 5.8.x	VDP-A 5.8.x + DD	VDP 6.0.x	VDP 6.0.x + DD	VDP 6.1.x	VDP 6.1.x + DD
VDP 6.0.x + DD	N	N	N	N	Y	N	N	Y	N	N	Y	N	Y	N	Y
VDP 6.1.x	N	N	N	Y	Y (R)	N	Y	Y (R)	N	Y	Y (R)	Y	Y (R)	Y	Y (R)
VDP 6.1.x + DD	N	N	N	N	Y	N	N	Y	N	N	Y	N	Y	N	Y

표 15-21. 복제 소스 매트릭스 - 2부

다음 제품을 사용하여 생성된 백업...	복제 가능한 타겟										
	RTI 5.8.x	RTI 5.8.x + DD	VDP 6.0.x	VDP 6.0.x + DD	Avamar SP1 6.1.1.87	Avamar SP2 6.1.2.47	Avamar 7.0.0.427	Avamar 7.0.1.56	Avamar 7.1.x.x	Avamar 7.1.x.x + DD	
VDP 5.5.1.x	N	N	N	N	N	N	N	N	N	N	
VDP 5.5.1.x	N	N	N	N	Y	Y	Y	Y	Y	Y	
VDP 5.5.5.x	N	N	N	N	Y	Y	Y	Y (R)	Y	Y	
VDP-A 5.5.5.x	Y (HP)	Y	Y	N	Y	Y	Y (R)	Y (R)	Y	Y	
VDP-A 5.5.5.x + DD	N	Y (HP)	N	Y (HP)	Y (NR)	Y (NR)	Y (NR)	Y (NR)	Y	Y	
VDP 5.5.6.x	N	N	N	N	Y	Y	Y (R)	Y	Y	Y	
VDP-A 5.5.6.x	Y (HP)	Y (HP)	Y (HP)	N	Y	Y	Y (R)	Y (R)	Y	Y	
VDP-A 5.5.6.x + DD	N	Y (HP)	N	Y (HP)	Y (NR)	Y (NR)	Y (NR)	Y (NR)	Y	Y	
VDP 5.8.x	N	N	N	N	Y	Y	Y	Y	Y (R)	Y	
VDP-A 5.8.x	Y (R)	Y	Y (HP)	N	Y	Y	Y	Y	Y (R)	Y	
VDP-A 5.8.x + DD	N	Y (R)	N	Y (HP)	Y (NR)	Y (NR)	Y (NR)	Y	Y	Y	
RTI 5.8.x	Y (R)	Y	Y (HP)	N	Y	Y	Y	Y	Y (R)	Y	
RTI 5.8.x + DD	N	Y (R)	N	Y (HP)	Y (NR)	Y (NR)	Y (NR)	Y (NR)	Y (NR)	Y (R)	
VDP 6.0.x	Y	Y (R)	Y (HP)	Y (R)	Y (HP)	Y (HP)	Y (HP)	Y (HP)	Y (HP)	N	
VDP 6.0.x + DD	N	Y	N	Y (HP)	N	N	N	N	N	Y (HP)	
VDP 6.1.x	Y	Y (R)	Y (HP)	Y (R)	Y (HP)	Y (HP)	Y (HP)	Y (HP)	Y (HP)	N	
VDP 6.1.x + DD	N	Y	N	Y (HP)	N	N	N	N	N	Y (HP)	

복제 및 Data Domain

소스 VDP 어플라이언스에 백업 타겟으로 Data Domain 시스템이 있는 경우 복제 대상 VDP 어플라이언스에도 Data Domain 시스템이 있어야 합니다. 이와 유사하게 VDP에서 Avamar 서버로 복제하는 경우 Avamar 서버에 Data Domain 시스템이 있어야 합니다.

참고 DD Boost 2.6과 Data Domain 5.4.1.1 이상, 5.5.x 및 5.6이 지원됩니다.

Data Domain과 Avamar 백업 타겟이 단일 복제 작업으로 결합된 경우 복제 작업은 실패합니다. 모든 Data Domain 클라이언트 또는 모든 Avamar 클라이언트를 백업 타겟으로 구성해야 합니다.

복제에 대한 Best Practice

- 완료된 클라이언트 백업만 복제되기 때문에 백업 작업이 적은 시간에 실행되도록 복제를 예약해야 합니다. 이렇게 하면 각 복제 세션이 진행되는 동안 가장 많은 수의 클라이언트 백업이 복제됩니다.
- 복제 타겟 서버에서 root 계정에 대한 사용자 ID 또는 암호를 변경하는 경우 소스 서버에서 대상 사용자 ID 및 암호를 새 암호로 업데이트해야 합니다.
- 복제 대상 관리를 사용하면 동일한 복제 대상 서버와 연결된 하나 이상의 복제 작업에 대한 정보를 업데이트할 수 있습니다.
- 동적 또는 비정적 데이터의 복제는 지원되지 않으므로 백업 작업이 적은 시간에 복제를 실행해야 합니다.
- 여러 백업 및/또는 복구 작업이 동시에 실행 중인 경우 여러 클라이언트의 복제 및/또는 복구를 동시에 실행할 수 없습니다.
- 버전이 서로 다른 서버 간의 복제가 지원되지만 대상 서버의 VDP 버전이 소스 서버의 VDP 버전과 같거나 그 이상인지 확인하십시오.
- 복제 작업 정책을 생성할 때, 예약된 각 복제 작업 중에 모든 클라이언트가 성공적으로 복제되도록 복제 그룹의 크기를 최적화하십시오. 그룹 크기가 매우 큰 경우 복제를 완료하는 데 더 많은 시간이 걸립니다. 따라서 그룹을 크기가 더 작으며 독립적으로 예약할 수 있는 두 개의 그룹으로 분할합니다.
- 단일 작업에 속하는 여러 복제 작업이 서로 다른 VM에서 실행될 경우 병렬로 실행되지 않습니다. 이 동작을 변경하려면 `/usr/local/vdr/etc/vdp-options.properties` 파일에 `com.vmware.vdp.option.replicate.maxstreams` 속성을 추가합니다.

예를 들어 `com.vmware.vdp.option.replicate.maxstreams=8` 속성을 추가합니다.

제한 사항

- 복제 작업이 시작되면 소스 서버에 상주하는 무활동의 정적 데이터만 처리할 수 있습니다. 따라서 소스 서버에 데이터를 기록하고 있는데 아직 완전히 완료되지 않은 작업(예: 처리 중인 백업 작업)은 복제 작업에 속하지 않게 됩니다. 그러나 해당 데이터는 다음 복제 작업 중에 복제됩니다.
- 소스 VDP 어플라이언스에서 복제된 클라이언트의 백업 수가 증가하면 각 클라이언트를 찾는 데 필요한 시간이 증가합니다.
- 복제된 백업 유형을 선택하는 방법으로만 가져온 백업을 복제할 수 있습니다.

가져온 백업의 경우, 가져오기 프로세스를 통해 클라이언트와 계정이 현재 계정 경로에서 `/REPLICATE/VDP_IMPORTS/`로 이동됩니다. 이 수준의 도메인 이름에는 타임 스탬프가 포함되며, 이름 끝에 타임 스탬프가 추가됩니다. 또한 가져오기 프로세스를 통해 모든 작업이 삭제됩니다. 이러한 백업을 복제하려면 해당 유형의 복제된 백업을 선택한 후에 가져온 백업을 선택해야 합니다.

복제 작업에 대한 백업 유형 정의

백업을 생성할 때 보존 정책 및 백업 스케줄을 지정합니다. 복제 작업에 사용할 백업 유형을 정의할 때 다음 요소를 고려하십시오.

- 보존 정책. 자세한 내용은 “[보존 정책 설정](#)”(111페이지) 섹션을 참조하십시오.
- 필요 시 또는 예약 백업 유형:

- 모든 백업 작업이 **지금 백업** 옵션을 사용하여 실행되는 경우 이는 필요 시 백업으로 간주되고 백업 유형과 관련이 없습니다. 이 백업을 복제하려면 **사용자 시작** 백업 유형을 선택해야 합니다(새 복제 작업 생성 마법사의 **6단계**).
- 백업을 예약하려면 예약 옵션을 지정해야 합니다(새 복제 작업 생성 마법사의 **10단계**).

복제 작업 생성

새 복제 작업 생성 마법사를 사용하여 복제 작업을 생성할 수 있습니다.

참고 다른 소스 서버에서 이미 복제된 복구 시점 또는 클라이언트를 새 복제 작업 생성 마법사에서 사용할 수 있습니다.

사전 요구 사항

- VDP가 vCenter Server에 설치 및 구성되어 있어야 합니다.
- vSphere Web Client에 로그인하고 VDP 어플라이언스에 연결합니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다. 지침은 **“VDP 액세스”**(104페이지) 섹션을 참조하십시오.
- 2 **복제** 탭을 클릭합니다.

복제 탭에는 생성된 복제 작업 목록이 표시됩니다. 다음 표에는 열과 해당 설명이 나와 있습니다.

표 15-22. 복제 탭의 열에 대한 설명

열	설명
이름	복제 작업의 이름입니다.
상태	복제 작업의 상태입니다.
대상	클라이언트 백업이 복제되는 위치입니다.
마지막 실행 시간	복제 작업이 실행된 마지막 시간입니다.
기간	작업이 마지막으로 실행되었을 때 복제 완료에 소요된 시간입니다.
다음 실행 시간	복제 작업이 다시 실행되도록 예약된 시간입니다.
클라이언트 수	작업에서 백업이 보호되고 복제되는 클라이언트의 수입니다. 이 값은 사용자가 편집 기능을 사용하여 복제 작업에 클라이언트를 추가하거나 제거할 때만 변경됩니다.

- 3 **복제 작업 조치** 메뉴에서 **새로 만들기**를 선택하여 새 복제 작업 생성 마법사를 시작합니다.
- 4 유형 선택 페이지에서 게스트 이미지(로컬 백업)을 복제할지 아니면 복제된 백업을 복제할지 선택한 후 다음을 클릭합니다.

유형 선택 페이지가 나타납니다. 이 페이지에서는 선택한 복제 유형에 따라 적절한 클라이언트가 나타납니다.

유형이 복제된 백업인 경우 다음과 같습니다.

- VDP 어플라이언스에는 복제된 백업 및 복구된 백업 클라이언트가 다른 타겟 서버로 복제하는 옵션으로 표시됩니다.
- 클라이언트 테이블에는 마지막으로 알려진 경로가 아니라 소스 경로 열의 소스 경로가 표시됩니다.

참고 게스트 이미지와 애플리케이션 백업 옵션을 모두 사용할 수 있습니다.

- 5 클라이언트 선택 페이지에서 다음 작업 중 하나를 수행합니다.
 - 모든 클라이언트 백업을 복제하려면 **모든 클라이언트**를 클릭한 후 다음을 클릭합니다.

- 특정 클라이언트의 백업만 복제하려면 **개별 클라이언트 선택**을 클릭한 다음 **유형** 목록에서 유형을 선택합니다. 옵션으로는 이미지, MS SQL Server, MS Exchange Server 및 MS SharePoint Server가 있습니다.

참고 일반 가상 머신 백업과 사용 중단된 가상 머신 백업 모두 복제할 수 있습니다. 사용 중단된 가상 머신이 일반 가상 머신으로 다시 추가된 경우 해당 가상 머신이 동일한 이름으로 두 번 표시됩니다. 사용 중단된 가상 머신 이름에는 접미사가 추가됩니다. 클라이언트를 선택할 때는 접미사가 없는 일반 가상 머신을 선택하십시오.

개별 클라이언트 선택을 선택하면 하나 이상의 클라이언트를 선택할 수 있습니다. 원하는 경우 선택하기 전에 클라이언트를 필터링할 수 있습니다. 클라이언트를 필터링하려면 다음과 같이 하십시오.

- a **필터** 옆의 **모두 표시**를 클릭하고 **클라이언트**를 선택합니다.

클라이언트 이름으로 필터링하려면 **이름**을 선택합니다. vCenter 클라이언트에 대한 다음 정보가 나타납니다.

- **Name:** "같음", "같지 않음", "포함" 또는 "포함하지 않음" 필터를 사용하여 클라이언트 이름을 쿼리합니다.
- **상태:** 값은 "전원 켜짐", "전원 꺼짐", "일시 중단됨", "활성화됨" 또는 "활성화 안 됨"입니다.
- **클라이언트 유형:** 클라이언트의 유형입니다.

- b 다음을 클릭합니다.

백업 선택 항목 페이지가 나타납니다. 이 페이지에서 작업이 실행될 때 복제되는 백업의 수를 제한할 수 있습니다. 백업 옵션을 선택하지 않을 경우 선택한 가상 머신에 대한 모든 백업이 복제됩니다.

- 6 **새 복제 작업 생성** 마법사의 **백업 선택 항목** 페이지에서 다음을 수행합니다.

- a **백업 유형**을 선택합니다.

매일: 일별 백업만 복제됩니다.

주 단위: 주별 백업만 한 번 복제됩니다.

월 단위: 월별 백업만 복제됩니다.

연 단위: 연간 백업만 복제됩니다.

사용자 시작: 사용자가 시작한 백업만 복제됩니다.

참고 사용자가 시작한 백업에는 고급 보존 옵션이 유지되지 않습니다. 이러한 백업은 별도의 백업 유형으로 플래그를 지정해야 합니다.

- b **클라이언트당 복제할 최대 백업 수**를 지정합니다.

제한 없음: 이 옵션을 선택하면 **백업 유형** 기준을 충족하는, 클라이언트에 대한 기존의 모든 백업이 복제됩니다. 백업 개수는 무제한입니다.

백업 개수: 이 옵션을 선택하면 복제할 백업이 날짜순으로 지정됩니다. 필요 시 백업이든 예약 백업이든 상관 없이 가장 최근의 백업이 선택됩니다. 최대 백업 개수는 999입니다.

- c **날짜 제한**을 지정합니다.

없음: 백업 유형 및 클라이언트당 복제할 최대 백업 수 기준을 충족하는 모든 백업이 복제됩니다. 다른 제한은 없습니다.

Last: 숫자와 시간 단위를 선택합니다. 이 옵션은 지정된 일수, 주수, 월수 또는 연수 동안 생성된 백업만 포함시켜 백업 선택을 제한합니다.

범위 기준: 시작 날짜 및 시간을 선택하고 종료 날짜 및 시간을 선택합니다. 특정 날짜부터, 특정 날짜까지 또는 두 날짜 중간을 지정할 수 있습니다.

- d 다음을 클릭합니다.

Destination 페이지가 나타납니다. 이 페이지에서 클라이언트 백업이 복제되는 대상에 대한 연결 정보를 지정합니다.

Avamar Server를 복제 대상으로 사용할 수 있습니다. 이를 수행하려면 Avamar Server의 IP 주소, 포트, 로그인 자격 증명을 대상 페이지에 입력합니다.

참고 가상 머신 클라이언트의 이름을 변경한 경우 VDP는 새 복제 작업 생성 마법사의 이름 열에 이름이 변경된 클라이언트를 표시합니다. 이름이 변경된 가상 머신 클라이언트의 복제를 수행할 때 대상이 Avamar 서버 또는 AVE(Avamar Virtual Edition)인 경우 변경된 이름은 Avamar에 반영되지 않습니다. Avamar 서버는 이름이 변경되기 전에 등록된 이전 이름을 표시합니다. 이는 알려진 문제입니다.

7 새 복제 작업 생성 마법사의 **대상** 페이지에서 다음 정보를 지정합니다.

참고 대상은 모두 백업 데이터가 복제되는 VDP 어플라이언스 또는 Avamar 서버를 나타냅니다.

- **호스트 이름 또는 IP:** 대상의 호스트 이름 또는 IP 주소입니다.
- **Port:** VDP가 대상과 통신하는 포트 번호입니다. 기본값은 SSL 암호화 복제에 대한 표준 포트인 29000입니다.
- **Username:** 대상에 로그인하는 데 사용되는 사용자 이름입니다.
- **암호:** 대상에 로그인하는 데 사용되는 암호입니다.
- **경로:** 멀티 테넌시 구성에 사용되는 도메인을 식별하는 고유한 이름입니다. 멀티 테넌시 구성에 대한 자세한 내용은 “[멀티 테넌시](#)”(144페이지)를 참조하십시오.

복제 및 복제된 백업 복구 작업의 경우 사용자 이름으로 **repluser**를 사용합니다. **repluser** 사용자 이름의 자격 증명은 루트 사용자와 동기화된 상태로 유지됩니다.

8 **인증 검증**을 클릭하여 VDP와 대상 간의 연결을 테스트합니다.

9 **다음**을 클릭합니다.

Schedule 페이지가 나타납니다. 이 페이지에서 백업 복제 빈도와 복제 발생 일시를 지정합니다.

10 새 복제 작업 생성 마법사의 **스케줄** 페이지에서 다음을 수행합니다.

a 스케줄 옵션 중 하나를 선택합니다.

- **매일:** 매일 백업을 복제하려면 이 옵션을 선택합니다.
- **매주 다음 요일에 수행:** 매주 지정된 요일에 백업을 복제하려면 이 옵션을 선택하고 요일을 선택합니다.
- **매월 ... 일자에 수행:** 매월 지정된 날짜에 백업을 복제하려면 이 옵션을 선택하고 날짜를 선택합니다.

b **서버에서 시작 시간**을 선택하여 예정된 날에 복제가 발생하는 시간을 지정합니다.

Best Practice: 완료된 클라이언트 백업만 복제되기 때문에 백업 작업이 적은 시간에 실행되도록 복제를 예약해야 합니다. 이렇게 하면 각 복제 세션이 진행되는 동안 가장 많은 수의 클라이언트 백업이 복제됩니다.

c **다음**을 클릭합니다.

보존 페이지가 나타납니다. 이 페이지에서 복제된 백업이 대상 머신에서 완료되는 시점을 지정합니다.

11 새 복제 작업 생성 마법사의 **보존** 페이지에서 다음을 수행합니다.

a 각 백업의 현재 만료 날짜를 사용하려면 **각 백업에 대해 현재 만료 유지**를 선택합니다.

b 백업 유형을 기준으로 만료 날짜를 지정하려면 **백업 유형별로 만료 시점 설정**을 선택하고 각 유형에 대해 일, 주, 월 또는 연 수를 선택합니다.

c 복제 작업을 영구적으로 보관하려면 **영구 보관**을 선택합니다.

d **다음**을 클릭합니다.

이름 페이지가 나타납니다. 이 페이지에서 복제 작업의 이름을 지정합니다.

- 12 새 복제 작업 생성 마법사의 **이름** 페이지에서 다음을 수행합니다.
 - a 복제 작업의 이름을 입력합니다.
복제 작업 이름은 고유해야 하며 최대 255자까지 지정할 수 있습니다. 작업 이름에 ~!@\$%^&(){}|!.,;#\/:*?<>"'& 같은 문자는 사용할 수 없습니다. 또한 â, é, ì, ù, ñ 같은 분음 문자도 사용할 수 없습니다.
 - b 다음을 클릭합니다.
완료 준비 페이지가 나타납니다. 이 페이지에서 작업을 저장하기 전에 생성한 복제 작업에 대한 요약 검토할 수 있습니다.
- 13 새 복제 작업 생성 마법사의 **완료 준비** 페이지에서 다음을 수행합니다.
 - a 정보를 검토합니다.
 - b **마침**을 클릭하여 작업을 생성합니다.

대상 관리

복제 탭에서 기존 복제 작업을 선택한 다음 3단계 대상 관리 마법사를 사용하여 모든 작업에 대한 대상 연결 정보를 변경할 수 있습니다.

Best Practice

복제 작업과 다양한 대상 서버의 조합을 선택하는 것이 아니라 동일한 특정 복제 대상 서버와 연결된 복제 작업을 모두 업데이트해야 합니다.

절차

- 1 웹 브라우저에서 VDP에 액세스합니다. 지침은 **“VDP 액세스”**(104페이지) 섹션을 참조하십시오.
- 2 **복제** 탭을 클릭합니다.
복제 탭에는 생성된 복제 작업 목록이 표시됩니다.
- 3 복제 작업을 강조 표시하고 **복제 작업 조치 > 대상 관리**를 선택합니다.
대상 관리 마법사가 나타납니다.
- 4 복제 작업 페이지에서 연결된 대상을 업데이트할 복제 작업을 클릭하고 **다음**을 클릭합니다. 여러 작업을 선택할 수 있습니다.
- 5 대상 관리 마법사의 **대상** 페이지에서 다음 정보를 지정합니다.

참고 대상은 모두 백업 데이터가 복제되는 VDP 어플라이언스 또는 Avamar 서버를 나타냅니다.

- **호스트 이름 또는 IP:** 대상의 호스트 이름 또는 IP 주소입니다.
- **Port:** VDP가 대상과 통신하는 포트 번호입니다. 허용 가능한 유일한 포트는 SSL 암호화 복제에 대한 표준 포트인 29000입니다.
- **Username:** 대상에 로그인하는 데 사용되는 사용자 이름입니다.
- **암호:** 대상에 로그인하는 데 사용되는 암호입니다.
- **경로:** 도메인을 식별하는 고유한 이름입니다. 이 필드는 멀티 테넌시 구성에 사용됩니다. 멀티 테넌시 구성에 대한 자세한 내용은 **“멀티 테넌시”**(144페이지)를 참조하십시오.

복제 및 복제된 백업 복구 작업의 경우 사용자 이름으로 **repluser**를 사용합니다. **repluser** 사용자 이름의 자격 증명은 루트 사용자와 동기화된 상태로 유지됩니다.

- 6 **인증 검증**을 클릭하여 VDP와 대상 간의 연결을 테스트합니다.
- 7 **다음**을 클릭합니다.
- 8 완료 준비 페이지에서 선택한 복제 작업에 할당될 대상을 검토합니다. **마침**을 클릭하여 복제 작업을 업데이트하거나 **뒤로**를 클릭하여 변경합니다.

복제 작업 편집

복제 작업을 강조 표시하고 **복제 작업 조치 > 편집**을 선택하여 복제 작업을 편집할 수 있습니다.

복제 작업 클론 생성

복제 작업을 템플릿으로 사용해 다른 작업을 생성할 수 있습니다. 복제 작업을 강조 표시하고 **복제 작업 조치 > 클론**을 선택합니다.

클론 작업을 수행하면 복제 작업 클론 생성 마법사가 시작되고 원래 작업의 정보가 자동으로 입력됩니다. 클론으로 생성된 작업은 고유한 이름을 필요로 합니다. 원래 작업에서 복제된 설정은 모두 수정할 수 있습니다.

복제 작업 삭제

복제 작업을 강조 표시하고 **복제 작업 조치 > 삭제**를 선택하여 복제 작업을 삭제할 수 있습니다.

참고 여러 복제 작업을 선택하여 삭제할 수 있습니다. 복제 작업을 삭제하면 특정 복제 대상과 연결된 복제 작업 수가 감소합니다. 복제 작업을 삭제하여 복제 대상에 연결된 복제 작업이 없어진 경우 삭제 요청의 일환으로 복제 대상을 제거하는 옵션이 제공됩니다.

복제 작업 활성화 또는 비활성화

이후 복제 작업의 실행을 일시적으로 중지하려는 경우 복제 작업을 비활성화할 수 있습니다. 비활성화된 복제 작업을 편집 및 삭제할 수 있습니다. VDP는 비활성화된 작업이 활성화될 때까지 해당 작업을 실행하지 않습니다.

복제 작업을 강조 표시하고 **복제 작업 조치 > 활성화/비활성화**를 선택하여 복제 작업을 활성화하거나 비활성화할 수 있습니다.

상태 및 복제 작업 세부 정보 보기

복제 탭에는 VDP로 생성된 복제 작업 목록이 표시됩니다. 작업을 클릭하면 다음과 같은 복제 작업 세부 정보를 확인할 수 있습니다. 복제 작업 세부 정보 창에 다음과 같은 세부 정보가 표시됩니다.

- **Name:** 복제 작업의 이름입니다.
- **상태:** 복제 작업의 상태입니다.
- **대상:** 작업에 지정된 백업이 복제된 위치입니다.
- **클라이언트:** 작업에 의해 백업이 복제된 클라이언트의 목록입니다.
- **마지막 실행 시간:** 복제 작업이 실행된 마지막 시간입니다.
- **기간:** 작업이 마지막으로 실행되었을 때 복제 완료에 소요된 시간입니다.
- **다음 실행 시간:** 작업이 다음에 실행되도록 예약된 날짜 및 시간입니다.

기존 복제 작업 즉시 실행

작업을 강조 표시하고 **지금 복제**를 클릭하여 복제 작업을 즉시 실행할 수 있습니다.

소스로 다시 복제

VDP 어플라이언스 간에 백업 데이터를 복제하도록 복제 작업을 설정할 수 있습니다.

복구된 백업의 노드 구조

처음에 소스 서버를 사용하여 유효한 복구 작업이 시작되면 /REPLICATE 링크 아래에 소스 서버 노드가 생성됩니다. 모든 복구된 백업은 소스 VDP 어플라이언스의 **복구** 탭에서 해당 /REPLICATE 링크 아래에 표시됩니다.

소스 VDP 어플라이언스에서 복제 타겟 서버로 성공적으로 복제되면 복제 소스 서버에서 타겟 서버에 있는 복제된 백업을 복구할 때 소스 서버의 FQDN(Fully Qualified Domain Name)이 **복구** 탭의 /REPLICATE 링크 아래에 표시됩니다. 복구된 백업에는 이 백업이 복구된 타겟 서버 FQDN이 표시되지 않습니다.

다시 복제된 백업의 노드 구조

사용자가 복제된 백업을 복제하는 경우에는 복제 소스 노드가 복제 타겟 서버의 /REPLICATE 링크 아래에 표시되지 않습니다.

복제된 백업이 성공적으로 복제되면 이후 타겟 서버의 **복구** 탭에 상위 소스 서버(가상 머신이 원래 백업된 소스 서버) 정보가 /REPLICATE 링크 아래에 표시됩니다.

복제된 백업이 서버 B에서 서버 C(서버 A를 사용하여 가상 머신이 원래 백업된 서버)로 성공적으로 복제되면 서버 C의 VDP 어플라이언스에 있는 **복구** 탭의 /REPLICATE 링크에 실제 복제 소스 서버 B에 대한 정보가 표시되지 않고 서버 A에 대한 정보가 표시됩니다.

복제 대상

다음은 복제 대상이 필요한 경우의 예입니다.

- 로컬 VDP 어플라이언스에 있는 백업을 원격 복제 타겟에 복제한 후 로컬 어플라이언스에서 백업을 제거하거나 삭제하는 경우. **소스로 다시 복제** 기능을 사용하면 원격 대상에 있는 백업을 검색하고 로컬 어플라이언스로 다시 복사하여 특정 백업을 복구할 수 있습니다. 로컬 어플라이언스에서 백업을 다시 복구한 후에는 일반 프로세스에 따라 복구할 수 있습니다.
- 손상된 VDP를 교체하기 위해 새 VDP 어플라이언스를 설치해야 하는 경우. 기존에 복제 대상에 복제한 특정 백업을 복구해야 합니다. **소스로 다시 복제** 기능을 사용하면 복제 대상에 연결하고, 이 대상에서 백업을 검색하고, 검색한 백업을 로컬 어플라이언스로 다시 복사하여 특정 백업을 복구할 수 있습니다. 새 VDP 어플라이언스에서 백업을 다시 복구한 후에는 일반 프로세스에 따라 복구할 수 있습니다.

참고 Avamar 서버에서는 복구 마법사를 사용할 수 없습니다. Avamar 서버에는 소스로 다시 복제할 수 있는 옵션이 없습니다.

복제 복구 호환성

표 15-23에는 지원되는 복제 복구 타겟 및 복제 복구 소스 서버가 나와 있습니다.

표 15-23. 복제 복구 호환성 매트릭스

복제 복구 타겟 (다음에서 복구)	복제 복구 소스(다음으로 복구)				
	VDP 5.8	VDP Advanced 5.8	VDP Advanced 5.8 타겟 ID	VDP 6.0	VDP 6.1
VDP 5.8.0.x	없음	없음	없음	있음	있음
VDP Advanced 5.8.0.x	없음	있음	있음	있음	있음
VDP Replication Target Identity 5.8.0.x	없음	있음	있음	있음	있음
VDP 5.5.1.356	없음	없음	없음	없음	없음
VDP 5.5.5.180	없음	없음	없음	없음	없음
VDP Advanced 5.5.5.180	없음	있음	있음	있음	있음
VDP 5.5.6.56	없음	없음	없음	없음	없음
VDP Advanced 5.5.6.56	없음	있음	있음	있음	있음
Avamar Server 7.0.x	있음	있음	있음	있음	있음
AVE(Avamar Virtual Edition) 6.0.x	있음	있음	있음	있음	있음
Avamar Server/AVE 7.1.x	있음	있음	있음	있음	있음
AVE 7.2.x	있음	있음	있음	있음	있음
VDP 6.0	No	있음	있음	있음	있음
VDP 6.1	No	있음	있음	있음	있음

중요 VDP Advanced는 버전 5.8 이하에 적용됩니다. RTI(Replication Target Identity)는 VDP 5.8에만 적용됩니다.

복제 복구 활성화 또는 비활성화

VDP 버전 5.5 이상의 경우 VDP 어플라이언스에서 Avamar 스토리지 서버 또는 Data Domain 시스템과 같은 복제 타겟 대상으로 복제할 때 포트 29000이 사용됩니다.

복제 복구 기능을 활성화하려면 복제 소스 서버에서 포트 29000이 열려 있어야 합니다. 포트 29000을 열면 복제된 백업이 복제 타겟 대상으로 복제될 수 있습니다. 포트 29000이 닫혀 있으면 복제 복구가 비활성화되며 대상을 유효한 복제 복구 타겟으로 검증할 수 없습니다.

기본적으로 VDP 어플라이언스에서는 포트 29000이 열려 있습니다. 포트 29000을 열고 닫는 방법에 대한 절차는 표준 Linux 서버 설명서를 참조하십시오.

복제 복구

새로 설치한 VDP에서는 새 복제 작업 생성 마법사를 사용하여 대상(백업이 복제된 컴퓨터)을 지정할 수 있습니다. 대상을 추가한 후에는 복제된 백업을 복구할 수 있습니다.

참고 복제 복구에 대한 현재 구축에서는 로컬 VDP 어플라이언스에서 가상 머신 클라이언트의 이름이 변경되는 경우 해당 이름 변경 사항이 복제 타겟으로 사용되는 원격 VDP Advanced 어플라이언스의 백업으로 전파되지 않습니다. 새 가상 머신 이름은 로컬 복구 지점에는 반영되지만 대상에는 반영되지 않습니다.

복제 타겟 선택 옵션은 vCenter Server가 변경된 후 비활성화되며 vCenter Server 변경 이후 새 복제 작업을 생성할 때까지 활성화되지 않습니다.

- 1 웹 브라우저에서 VDP에 액세스합니다. 지침은 “VDP 액세스”(104페이지) 섹션을 참조하십시오.
- 2 복구 탭을 클릭합니다.
- 3 복구 탭에서 복제된 백업 복구를 클릭합니다.
복구 마법사가 나타납니다.



- 4 대상 페이지에서 다음 옵션 중 하나를 선택합니다.
 - 기존 복제 작업에서 사용할 대상 선택
 - 새 원격 대상 지정
- 5 인증 검증을 클릭합니다.
- 6 클라이언트 및 백업 페이지에서 이 어플라이언스로 복구할 원격 클라이언트 및 백업을 선택합니다. 화살표를 클릭하여 클라이언트를 확장하고 해당 백업을 확인할 수 있습니다.
- 7 완료 준비 페이지에서 복구할 항목을 검토합니다.
- 8 마침을 클릭하여 복구 요청을 시작하거나, 변경이 필요한 경우 뒤로를 클릭하여 이전 화면으로 돌아갑니다.

멀티 테넌시

VDP에는 멀티 테넌시 지원이 포함되어, 여러 고객이나 조직이 단일 VDP 어플라이언스에서 별도의 계정을 가질 수 있습니다. 각 고객 또는 조직은 VDP 어플라이언스에 복제할 수 있을 뿐 아니라 복제 복구 기능을 사용하여 복제된 데이터에 액세스할 수도 있습니다. 특정 고객 또는 조직의 복제된 데이터는 해당 고객 또는 조직의 계정 자격 증명을 사용해야만 액세스할 수 있습니다. root 및 repluser와 같이 모든 권한이 있는 기본 자격 증명을 사용하면 복제된 모든 데이터에 액세스할 수 있습니다. 이러한 자격 증명은 개별 고객 또는 조직과 공유하면 안 됩니다. 특정 계정의 복제된 데이터는 다른 모든 계정의 복제된 데이터와 분리됩니다.

VDP, VDP 복제 타겟(VDP 5.8에서만 사용 가능), Avamar(버전 7.1 이상 권장) 및 Avamar Virtual Edition(버전 7.1 이상 권장)이 멀티 테넌시가 지원되는 타겟입니다.

모든 VDP 어플라이언스에서 제공되는 create_av_domain.rb 스크립트를 사용하여 멀티 테넌시 계정을 생성할 수 있습니다. create_av_domain.rb 스크립트는 다음과 같은 매개 변수를 정의합니다.

사용 방법: create_av_domain.rb

```

-c, --company=<Company-Name>      (필수 사항)
-d, --department=<Department-Name> (선택 사항)
-u, --username=<User-Name>        (필수 사항)
-p, --password=<User-Password>    (필수 사항)
-h, --help

```

company 값에는 고객의 회사 또는 조직 이름을 포함해야 합니다. 선택 사항인 department 값에는 동일한 company 값을 공유하는 여러 계정을 설정할 수 있지만 각 계정의 department 값은 고유해야 합니다. company 와 department 값이 결합되어 계정을 구성합니다. 각 계정에는 복제된 데이터를 보관할 수 있는 분리된 버킷이 있습니다. 사용자 이름 및 암호 매개 변수는 계정의 액세스 자격 증명을 정의합니다. 단일 계정의 액세스 증명 집합을 여러 개 생성할 때는 company 및 department에 동일한 값을 사용하되 username과 password에는 다른 값을 사용하여 create_av_domain.rb 스크립트를 여러 번 실행할 수 있습니다.

다음 단계에 따라 create_av_domain.rb 스크립트를 실행하십시오.

- 1 복제 타겟 서버에 admin 사용자로 로그인(ssh)합니다.
- 2 다음 명령을 실행하고 루트 암호를 제공합니다.

```
su - root
```

- 3 경로를 다음 디렉토리로 변경합니다.

```
cd /usr/local/vdr/configure/bin
```

- 4 다음 명령을 실행하고 생성하는 계정에 적합한 값을 지정합니다.

```
./create_av_domain.rb --company=<Company-Name> --department=<Department-Name> --username=<User-Name>
--password=<User-Password>
```

예:

```
./create_av_domain.rb --company=Acme --department=Marketing --username=fred --password=topsecret
```

계정을 생성한 후 VDP 어플라이언스에서 복제 대상을 정의할 때 계정 정보를 입력합니다. 복제 대상 페이지에는 원격 대상의 호스트 이름 또는 IP, 사용자 자격 증명(사용자 이름 및 암호) 및 경로 값이 필요합니다. 경로 값은 create_av_domain.rb 스크립트를 사용하여 계정을 설정할 때 제공한 company 및 department 값으로 구성되는 계정 식별자입니다. 슬래시 하나로 company 및 department 값을 구분합니다. 위 예에서 경로 값은 **Acme/Marketing**입니다.

파일 레벨 복구 사용

이 장에서 다루는 내용은 다음과 같습니다.

- [“VDP Restore Client 소개”](#)(148페이지)
- [“Restore Client에 로그인”](#)(149페이지)
- [“백업 마운트”](#)(151페이지)
- [“백업 필터링”](#)(151페이지)
- [“마운트된 백업 탐색”](#)(151페이지)
- [“파일 레벨 복구 수행”](#)(151페이지)
- [“복구 모니터링”](#)(153페이지)

VDP Restore Client 소개

VDP는 전체 가상 머신의 백업을 생성합니다. 이러한 백업은 vSphere Web Client를 통해 VDP UI를 사용하여 온전히 그대로 복구할 수 있습니다. 그러나 이러한 가상 머신에서 특정 파일만 복구하려는 경우 웹 브라우저를 통해 액세스하는 VDP Restore Client를 사용하십시오. 이를 FLR(File Level Restore)이라고 합니다.

Restore Client를 사용하면 특정 가상 머신 백업을 파일 시스템으로 마운트한 다음, 이 파일 시스템을 검색하여 복구하려는 파일을 찾을 수 있습니다.

Restore Client 서비스는 VDP에서 백업을 관리하는 가상 머신의 경우에만 사용할 수 있습니다. 이를 위해 vCenter 콘솔 또는 다른 원격 연결을 통해 VDP에서 백업한 가상 머신 중 하나에 로그인해야 합니다.

참고 이전에 사용된 VDP 디스크로부터 가져온 복구 시점에서 FLR을 수행하려면 새 VDP를 사용하여 VM의 백업을 하나 이상 생성합니다.

주의 vSphere 6.0에서 지원되는 웹 브라우저는 “[소프트웨어 요구 사항](#)”(22페이지) 섹션을 참조하십시오. Internet Explorer 10은 지원되지 않으며 Restore Client와 함께 사용 시 안정적이지 않습니다.

LVM 및 EXT 지원

LVM(Logical Volume Manager) 및 확장 파일 시스템에서 관리되는 논리적 볼륨을 고려할 때는 다음에 유의하십시오.

- 한 개의 물리적 볼륨(.vmdk)은 정확하게 한 개의 논리적 볼륨에 매핑되어야 합니다.
- Ext2 및 Ext3 형식(MBR(Master Boot Record)이 있는 기본 파티션 및 MBR이 없는 독립형 파티션)만 지원됩니다.
- LVM 및 ext4는 외부 프록시를 사용하는 경우에만 지원됩니다.

파일 레벨 복구 제한 사항

FLR의 제한 사항은 다음과 같습니다.

- 타겟 가상 머신에 VMware Tools가 설치되어 있어야 합니다. 최상의 결과를 얻으려면 모든 가상 머신에서 사용 가능한 최신 버전의 VMware Tools가 실행되고 있는지 확인하십시오. 오래된 버전에서는 파일 레벨 복원 작업 중에 찾아보기 작업을 수행하는 동안 오류가 발생할 수 있습니다.
 - 심볼 링크는 찾거나 복원할 수 없습니다.
 - 백업 내 포함된 특정 디렉토리 또는 복구 대상을 검색할 때 총 5,000개의 파일 또는 폴더로 제한됩니다.
 - 즉, 동일한 복구 작업에서 5,000개 이상의 폴더나 파일을 복구할 수 없습니다.
 - 파티션이 생성되면 하위 인덱스를 먼저 채워야 합니다. 단일 파티션을 생성하여 파티션 인덱스 2, 3 또는 4에 지정할 수 없습니다. 단일 파티션은 파티션 인덱스 1에 지정해야 합니다.
 - VM이 NAT(Network Address Translation) 뒤에 있는 경우 FLR이 작동하지 않습니다.
 - 네트워크 어플라이언스가 NAT를 사용하고 모든 VDP 트래픽을 프록시 또는 방화벽을 통해 전송하는 경우 VDP에서 클라이언트를 찾을 수 없다는 오류 메시지가 FLR에 표시됩니다.
 - 이전 버전의 VMware 툴을 사용하는 경우 FLR이 실패합니다. 타겟 가상 머신에 최신 버전의 VMware 툴을 설치해야 합니다.
 - ACL은 복구할 수 없습니다.
 - 가상 머신이 백업으로부터 복구된 경우에는 가상 머신에서 Restore Client에 로그인할 수 없습니다. 복구된 가상 머신의 UUID(Universal Unique Identifier)가 다르기 때문에 인증이 실패합니다.
- 해결 방법:** 새 가상 머신을 백업하고 **고급 로그인** 모드를 사용하여 Restore Client에 로그인하십시오. 자세한 내용은 “[고급 로그인](#)”(150페이지)을 참조하십시오.
- Novell NSS 볼륨에서는 FLR이 작동하지 않습니다.

지원되지 않는 VMDK 구성

FLR은 다음 가상 디스크 구성을 지원하지 않습니다.

- 포맷되지 않은 디스크
- 동적 디스크(Windows)
- GPT(GUID Partition Table) 디스크
- 확장 파티션(유형: 05h, 0Fh, 85h, C5h, D5h)
- 둘 이상의 파티션이 있는 가상 디스크
- 단일 파티션에 매핑된 2개 이상의 가상 디스크
- 암호화된 폴더 또는 파일
- 파일 또는 폴더를 원래 가상 머신에 복구할 경우 SCSI 디스크만 지원됩니다.
- 0바이트 파일
- 압축된 파티션

참고 경우에 따라(대개 확장된 파티션의 경우), 전체 백업 이미지를 임시 가상 머신에 복구한 후 필요한 폴더 또는 파일을 선택적으로 복제할 수 있습니다.

지원되지 않는 Windows 구성

FLR은 다음 Windows 8 및 Windows Server 2012 구성을 지원하지 않습니다.

- 중복 제거된 NTFS(New Technology File System)
- ReFS(Resilient File System)
- EFI(Extensible Firmware Interface) 부트로더

Restore Client에 로그인

Restore Client는 기본 또는 고급 모드에서만 작동합니다. Windows 백업 파일은 Windows 시스템에만 복구할 수 있고 Linux 백업 파일은 Linux 시스템에만 복구할 수 있습니다.

참고 Windows 7 가상 머신에서 Restore Client에 로그인하려고 시도할 경우 FLR에 대한 최소 제한 설정에 UAC(User Access Control) 설정을 지정해야 작동할 수 있습니다.

기본 로그인

기본 로그인을 사용하여 VDP를 통해 백업한 가상 머신에서 Restore Client로 연결합니다. 로그인한 가상 머신의 로컬 관리자 자격 증명을 사용하여 복구 클라이언트에 로그인합니다(그림 16-8 참조).

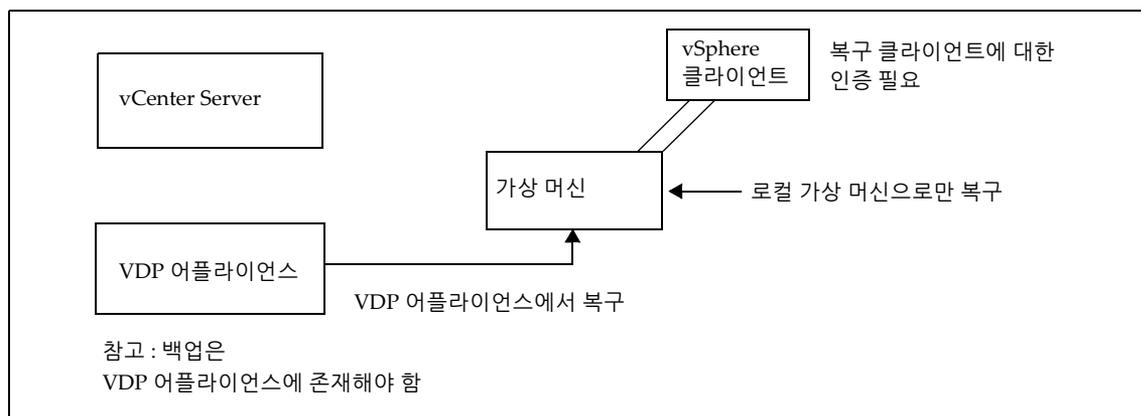


그림 16-8. FLR 기본 로그인

로그인 지침은 “[기본 로그인 모드에서 Restore Client 사용](#)”(151페이지) 섹션을 참조하십시오.

기본 로그인을 사용하여 Restore Client는 해당 로컬 가상 머신에 대한 백업만 표시합니다. 예를 들어, "WS44"라는 이름의 Windows 호스트에서 기본 모드로 Restore Client에 로그인한 경우 "WS44"의 백업만 마운트하고 찾을 수 있습니다.

고급 로그인

고급 로그인을 사용하여 VDP를 통해 백업한 가상 머신에서 Restore Client로 연결합니다. 로그인한 가상 머신의 로컬 관리자 자격 증명뿐만 아니라 VDP 어플라이언스를 vCenter Server에 등록하는 데 사용한 관리자 자격 증명을 사용하여 Restore Client에 로그인합니다(그림 16-9 참조).

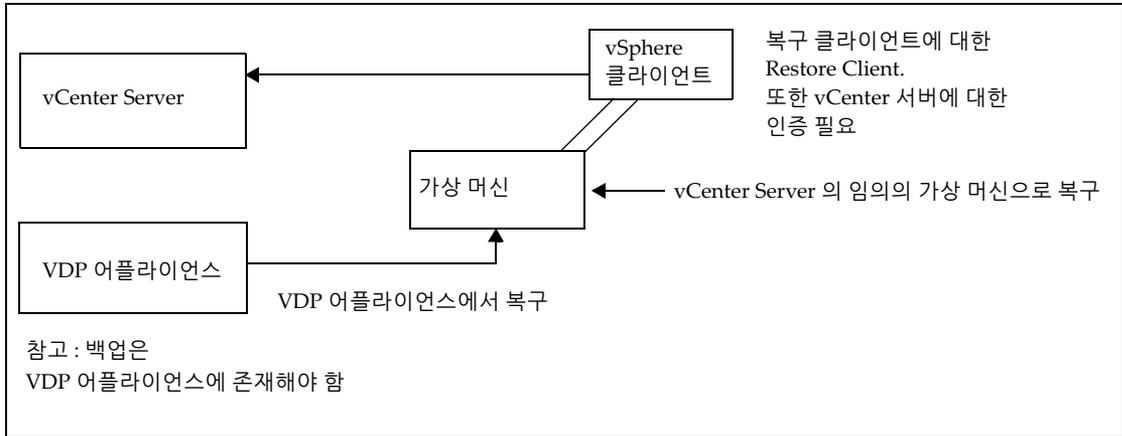


그림 16-9. FLR 고급 로그인

로그인 지침은 “[고급 로그인 모드에서 Restore Client 사용](#)”(152페이지) 섹션을 참조하십시오.

Restore Client에 연결한 후 VDP에서 백업한 모든 가상 머신의 파일을 마운트하고 찾거나 복구할 수 있습니다. 모든 복구 파일은 사용자가 현재 로그인한 가상 머신으로 복구됩니다.

FLR 고급 로그인에는 VDP 어플라이언스를 설치할 때 지정한 것과 동일한 vCenter 사용자 자격 증명을 사용해야 합니다. 자세한 내용은 “[VDP 설치](#)”(29페이지) 섹션을 참조하십시오.

백업 마운트

로그인하면 마운트된 백업 관리 대화상자가 나타나고, 기본적으로 마운트할 수 있는 모든 백업이 표시됩니다. 이 대화상자의 형식은 로그인 방법에 따라 달라집니다.

- 기본 로그인을 사용하는 경우 로그인한 클라이언트에서 마운트할 수 있는 모든 백업이 대화상자에 나열됩니다.
- 고급 로그인을 사용하는 경우 VDP에 백업된 모든 클라이언트가 대화상자에 나열됩니다. 각 클라이언트 아래에는 마운트할 수 있는 모든 백업 목록이 표시됩니다.

참고 대화상자 오른쪽 하단에 있는 **마운트**, **마운트 해제** 또는 **모두 마운트 해제** 버튼을 사용하여 최대 254개의 vmdk 파일 이미지를 마운트할 수 있습니다.

백업 필터링

마운트된 백업 관리 대화상자에는 모든 백업을 표시하거나 백업 목록을 필터링하는 옵션이 있습니다. 목록은 다음 방법으로 필터링할 수 있습니다.

- **모든 복구 시점** - 모든 백업이 표시됩니다.
- **복구 시점 날짜** - 특정 기간의 백업만 표시됩니다.
- **VM 이름** - 필터 필드에서 입력한 텍스트가 표시 이름에 포함되어 있는 호스트의 백업만 표시됩니다. 로그인한 가상 머신에 속하는 백업만 표시되므로 이 옵션은 기본 로그인에서는 사용할 수 없습니다.

마운트된 백업 탐색

백업이 마운트된 후 Restore Client 사용자 인터페이스의 왼쪽에 표시된 트리를 사용하여 백업 콘텐츠를 탐색할 수 있습니다. 트리의 모양은 기본 로그인을 사용할 때와 고급 로그인을 사용할 때 각각 다릅니다.

파일 레벨 복구 수행

Restore Client의 기본 화면에서 왼쪽 열의 파일 시스템 트리를 탐색한 다음, 트리에서 디렉토리를 클릭하거나 오른쪽 열에서 파일 또는 디렉토리를 클릭하여 특정 파일을 복구할 수 있습니다.

기본 로그인 모드에서 Restore Client 사용

Windows 또는 Linux 가상 머신에서 기본 로그인 모드로 Restore Client를 사용하면 전체 가상 머신을 복구할 필요 없이 해당 머신에 대한 복구 시점에서 개별 파일에 액세스할 수 있습니다.

사전 요구 사항

- VDP(vSphere Data Protection)가 vCenter Server에 설치 및 구성되어 있는지 확인합니다.
- 기본 로그인의 경우 VDP에서 백업한 가상 머신에서만 Restore Client에 로그인할 수 있습니다.
- 백업에서 파일 레벨 복구를 수행하려면 가상 머신에 VMware Tools를 설치해야 합니다. VMware Tools를 지원하는 운영 체제의 목록은 VMware 웹 사이트를 참조하십시오.

절차

- 1 원격 데스크톱 또는 vSphere Web Client에서 VDP를 통해 백업한 로컬 호스트에 액세스합니다.
- 2 다음을 통해 VDP Restore Client에 액세스합니다.
`https://<IP_address_of_VDP_appliance>:8543/flr`
- 3 **로컬 자격 증명** 아래 **자격 증명** 페이지에서 로컬 호스트에 대한 **사용자 이름** 및 **암호**를 지정하고 **로그인**을 클릭합니다.
마운트된 백업 관리 대화상자가 나타나고, 액세스하고 있는 클라이언트의 모든 복구 시점이 나열됩니다.
- 4 복구할 마운트 시점을 선택하고 **마운트**를 클릭합니다. 
마운트가 완료되면 드라이브 아이콘이 녹색 네트워크 드라이브  로 나타납니다.
- 5 **닫기**를 클릭합니다.
- 6 **마운트된 백업** 창에서 복구할 폴더 및 파일을 탐색하여 선택합니다.
- 7 **선택한 파일 복구**를 클릭합니다.
- 8 **대상 선택** 대화상자에서 복구할 드라이브 및 대상 폴더를 탐색하여 선택합니다.
- 9 **복구**를 클릭합니다.
복구 시작 확인 대화상자가 나타납니다.
- 10 **예**를 클릭합니다.
성공적으로 시작되었음을 알리는 대화상자가 나타납니다.
- 11 **확인**을 클릭합니다.
- 12 **복구 모니터링** 탭에서 복구 상태를 검토하여 복구가 성공했는지 확인합니다.

고급 로그인 모드에서 Restore Client 사용

Windows 또는 Linux 가상 머신에서 고급 로그인 모드로 Restore Client를 사용하면 vCenter Server에서 파일 레벨 복구를 수행할 복구 시점이 포함된 가상 머신에 액세스할 수 있습니다.

사전 요구 사항

- VDP가 vCenter Server에 설치 및 구성되어 있는지 확인합니다.
- FLR 고급 로그인에는 VDP 어플라이언스를 설치할 때 지정한 것과 동일한 vCenter 사용자 자격 증명을 사용해야 합니다. 자세한 내용은 **"VDP 설치"**(29페이지) 섹션을 참조하십시오.
- 백업에서 파일 레벨 복구를 수행하려면 가상 머신에 VMware Tools를 설치해야 합니다. VMware Tools를 지원하는 운영 체제의 목록은 VMware 웹 사이트를 참조하십시오.

절차

- 1 원격 데스크톱을 사용하여 원격으로 로그인하거나 vSphere Web Client를 사용하여 가상 머신에 액세스합니다.
- 2 다음을 통해 VDP Restore Client에 액세스합니다.
`https://<IP_address_of_VDP_appliance>:8543/flr`
- 3 **로컬 자격 증명** 아래 **자격 증명** 페이지에서 로컬 호스트에 대한 **사용자 이름** 및 **암호**를 지정합니다. **vCenter 자격 증명** 필드에서 vCenter 관리자의 **사용자 이름** 및 **암호**를 지정하고 **로그인**을 클릭합니다.
마운트된 백업 관리 대화상자가 나타납니다. 여기에는 VDP에 백업되는 동일한 유형의 모든 클라이언트에 대한 모든 복구 시점이 나열됩니다.

- 4 복구할 마운트 시점을 선택하고 **마운트**를 클릭합니다. 
- 마운트가 완료되면 드라이브 아이콘이 녹색 네트워크 드라이브  로 표시됩니다.
- 5 **닫기**를 클릭합니다.
- 6 **마운트된 백업** 창에서 복구할 가상 머신, 폴더 및 파일을 탐색하여 선택합니다.
- 7 **선택한 파일 복구**를 클릭합니다.
- 8 **대상 선택** 대화상자에서 복구할 드라이브 및 대상 폴더를 탐색하여 선택합니다.
- 9 **복구**를 클릭합니다.
복구 시작 확인 대화상자가 나타납니다.
- 10 **예**를 클릭합니다.
성공적으로 시작되었음을 알리는 대화상자가 나타납니다.
- 11 **확인**을 클릭합니다.
- 12 **복구 모니터링** 탭에서 복구 상태를 검토하여 복구가 성공했는지 확인합니다.

복구 모니터링

Restore Client의 현재 및 이전 작업을 모니터링하려면 **복구 모니터링** 버튼을 클릭하십시오. 복구 모니터링 화면에는 현재 진행 중인 복구 작업과 최근에 완료된 복구 작업에 대한 정보가 표시됩니다.

열 제목을 클릭하여 표에 있는 열을 정렬할 수 있습니다. 표 제목을 클릭하면 정렬 순서가 뒤바뀌고, 위로 또는 아래로 화살표를 클릭하면 정렬 순서가 오름차순 또는 내림차순으로 바뀝니다.

기본적으로 **복구 모니터링**에는 진행 중이거나 현재 세션에서 완료된 모든 작업이 표시됩니다. 이전 세션에서 완료되거나 실패한 작업을 보려면 **완료된 작업 표시**를 선택합니다. 이전에 완료된 작업과 실패한 작업이 현재 실행 중인 작업 및 보류 중인 작업과 함께 표시됩니다.

VDP 애플리케이션 지원

이 장에서 다루는 내용은 다음과 같습니다.

- [“VDP 애플리케이션 지원”\(156페이지\)](#)
- [“Microsoft SQL Server 백업 및 복구”\(157페이지\)](#)
- [“Microsoft Exchange Server 백업 및 복구”\(165페이지\)](#)
- [“Microsoft SharePoint Server 백업 및 복구”\(178페이지\)](#)

VDP 애플리케이션 지원

VDP는 Microsoft Exchange Server, SQL Server 및 SharePoint Server에 대한 세밀한 게스트 레벨의 백업과 복구를 지원합니다. 게스트 레벨 백업을 지원하기 위해 VDP 클라이언트가 Exchange Server, SharePoint Server 및 SQL Server에 설치됩니다.

애플리케이션 에이전트 설치

애플리케이션 에이전트를 설치하려면 다음과 같은 애플리케이션별 지침을 참조하십시오.

- “VDP for SQL Server Client 설치”(158페이지)
- “VDP for Exchange Server Client 설치”(167페이지)
- “VDP for SharePoint Server Client 설치”(179페이지)

Microsoft Windows에서 사용자 계정 컨트롤 설정 확인

UAC(User Account Control) 기능은 애플리케이션 소프트웨어를 표준 사용자 권한으로 제한합니다. 소프트웨어 설치와 같은 일부 작업을 수행하려면 관리자 권한을 제공해야 합니다. UAC는 기본적으로 활성화되어 있습니다.

UAC가 활성화된 컴퓨터에서 관리자 권한 없이 VDP 클라이언트 또는 플러그인 설치 관리자를 시작하면 소프트웨어가 올바르게 설치되지 않습니다. UAC를 비활성화하거나 무시할 수 있습니다. 이 장의 설치 절차에서는 UAC를 무시하는 한 가지 방법을 설명합니다. 다른 방법과 추가 정보는 Microsoft 설명서를 참조하십시오.

UAC가 활성화된 경우 VDP 클라이언트 설치

UAC가 활성화된 상태에서 VDP 클라이언트를 설치하려고 하면 다음과 같은 오류 메시지가 나타납니다.

VMware VDP for <Microsoft Application> Server 를 설치할 수 없습니다 . 관리자로 로그인했고 설치 사전 요구 사항이 모두 충족되었는지 확인하십시오 .

이 문제를 해결하려면 다음 단계를 수행하여 관리자 권한으로 설치 관리자를 실행해야 합니다.

- 1 Windows에서 명령 프롬프트 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 2 명령 프롬프트 창에서 다음 경로를 입력하여 작업 디렉토리를 설치 패키지가 있는 위치로 변경합니다.

```
cd install_path
```

여기서 *install_path*는 설치 패키지가 포함된 임시 폴더의 전체 경로입니다.

- 3 적절한 명령을 입력하여 설치 관리자를 시작합니다.

```
msiexec /i VMwareVDPExchange-windows-x86_64-<version>.msi
msiexec /i VMwareVDP Moss-windows-x86_64-<version>.msi
msiexec /i VMwareVDPSQL-windows-x86_64-<version>.msi
msiexec /i VMwareVDPSQL-windows-x86_32-<version>.msi
```

여기서 *version*은 VDP 클라이언트 버전입니다.

Microsoft SQL Server 백업 및 복구

VDP는 Microsoft SQL Server에 대한 향상된 백업 및 복구 옵션을 지원합니다.

이 섹션에서는 다음 내용을 다룹니다.

- [“Microsoft SQL Server 지원”\(157페이지\)](#)
- [“VDP for SQL Server Client 설치”\(158페이지\)](#)
- [“Microsoft SQL Server 백업 작업 생성”\(162페이지\)](#)
- [“Microsoft SQL Server의 백업 복구”\(164페이지\)](#)

Microsoft SQL Server 옵션

Microsoft SQL Server에 대해 지원되는 옵션은 다음과 같습니다.

- 선택된 SQL Server 백업
- 전체 데이터베이스 인스턴스를 백업하도록 선택
- 개별 데이터베이스를 백업하도록 선택
- 전체, 차등 또는 증분 백업 지원
- 전체 백업 후 증분 백업을 사용하도록 지원
- 멀티 스트리밍 백업 지원(최대 6개 스트림)
- 단순 모드 데이터베이스 백업 지원(증분 건너뛴)
- 원래 위치 또는 대체 위치로 복구
- 지정된 경로를 사용하여 원래 인스턴스에서 데이터베이스 복구
- 지정된 경로를 사용하여 다른 인스턴스로 데이터베이스 복구

하드웨어 요구 사항

[표 17-24](#)에는 Microsoft SQL Server에 대한 하드웨어 요구 사항이 나와 있습니다.

표 17-24. Microsoft SQL Server에 대한 하드웨어 요구 사항

요구 사항	최소
메모리(RAM)	512MB(2GB 권장)
하드 드라이브 공간	소프트웨어 설치를 위한 1GB의 영구 하드 드라이브 공간 Microsoft SQL Server 소프트웨어에는 물리적 RAM 64MB당 12MB의 영구 하드 드라이브 공간도 추가적으로 필요합니다. 이 공간은 로컬 캐시 파일을 위해 필요합니다.

Microsoft SQL Server 지원

VDP는 다음 버전의 SQL Server를 지원합니다.

- 다음 SQL 버전의 SQL Server 페일오버 클러스터
 - SQL Server 2014
 - SQL Server 2012
 - SQL Server 2008, 2008 R2
 - SQL Server 2005
- 다음 SQL 버전의 SQL AlwaysOn 클러스터
 - SQL Server 2014
 - SQL Server 2012

- SQL Server 2014
 - Windows Server 2014에서 실행되는 SQL Server 2012(x86/x64)
 - Windows Server 2008 SP2 이상에서 실행되는 SQL Server 2014(x86/x64)
 - Windows Server 2008 R2 SP1 이상에서 실행되는 SQL Server 2014(x86/x64)
- Windows Server 2012에서 실행되는 SQL Server 2012(x86/x64)
- Windows Server 2008 SP2 이상에서 실행되는 SQL Server 2012(x86)
- Windows Server 2008 R2 SP1 이상에서 실행되는 SQL Server 2012(x64)
- 다음 운영 체제에서 실행되는 SQL Server 2008 R2 이상:
 - Windows Server 2008 이상(x86/x64)
 - Windows Server 2008 R2(x64)
 - Windows Server 2012
- 다음 운영 체제에서 실행되는 SQL Server 2008 SP1
 - Windows Server 2008 SP1 이상(x86/x64)
 - Windows Server 2008 R2(x64)
 - Windows Server 2012
- 다음 운영 체제에서 실행되는 SQL Server 2005 SP3:
 - Windows Server 2008 SP1 이상(x86/x64)
 - Windows Server 2008 R2(x64)
- Windows Server 2008(X86/x64)에서 실행되는 SQL Server 2005 SP2

VDP for SQL Server Client 설치

게스트 레벨 백업을 지원하려면 각 SQL Server에 백업과 복구를 지원하기 위한 VDP for SQL Server Client가 설치되어 있어야 합니다.

클러스터에 VDP for SQL Server Client를 설치하려면 각 노드에 VDP for SQL Server Client를 설치하고 노드를 모두 등록한 다음 VDP 클러스터 클라이언트를 구성하십시오. 클러스터에 VDP for SQL Server Client를 설치하려면 다음 단계를 수행하십시오.

- 1 클러스터의 각 노드에서 동일한 폴더에 VDP for SQL Server Client를 설치합니다.

설치 프로세스가 소프트웨어를 설치한 다음 클러스터의 각 노드를 VDP 어플라이언스에 등록하고 활성화합니다.

- 2 VMware VDP Windows Cluster Configuration Wizard를 사용하여 VDP 어플라이언스를 구성합니다.

사전 요구 사항

- VDP를 사용하기 전에 **“VDP 설치 및 구성”**(21페이지)의 설명에 따라 VDP 어플라이언스를 설치 및 구성해야 하며 SQL Server에 대한 관리 권한이 있어야 합니다.
- 다음 소프트웨어가 SQL Server에 설치되어 있어야 합니다.
 - .NET 4.0
 - SQL Server 설치 구성 요소
 - 클라이언트 도구 SDK

절차

- 1 각 SQL Server 클라이언트에서 vSphere Web Client에 액세스합니다.
https://<IP_address_vCenter_Server>:9443/vsphere-client/
 - 2 자격 증명 페이지에 vCenter 관리 사용자 이름과 암호를 입력하고 **로그인**을 클릭합니다.
 - 3 vSphere Web Client에서 **VDP**를 선택합니다.
 - 4 VDP 시작 페이지에서 VDP 어플라이언스를 선택하고 **연결**을 클릭합니다.
 - 5 **구성** 탭을 클릭합니다.
 - 6 **클라이언트 다운로드**에서 **Microsoft SQL Server 32비트** 또는 **Microsoft SQL Server 64비트**를 클릭합니다(SQL Server 클라이언트의 버전에 따라).
 - 7 사용 중인 브라우저에 따라 .msi 파일을 저장하거나 실행할 수 있습니다. .msi 파일을 실행하면 VMware VDP for SQL Server 설치 마법사가 시작됩니다. **다음**을 클릭합니다.
 - 8 최종 사용자 사용권 계약 페이지에서 라이선스를 읽고 동의하는 경우 **동의함**과 **다음**을 차례로 클릭합니다.
 - 9 어플라이언스 등록 정보 페이지에 SQL Server를 백업할 VDP 어플라이언스의 이름을 입력하고 **다음**을 클릭합니다.
 - 10 VMware VDP for SQL Server 설치 준비 페이지에서 **설치**를 클릭합니다.
 - 11 VMware VDP for SQL Server 설치 마법사 완료 페이지에서 **마침**을 클릭합니다.
- 추가 SQL Server에 대해 이 절차를 반복합니다.

페일오버 클러스터에서 클러스터 클라이언트 구성

페일오버 클러스터의 VDP 클러스터 클라이언트를 사용하면 클러스터의 공유 스토리지에 있는 SQL Server 데이터를 백업 및 복구할 수 있습니다. 이때 백업 또는 복구 시 어떤 노드에서 데이터를 관리하는 중인지는 상관 없습니다. VMware VDP Windows Cluster Configuration Wizard는 페일오버 클러스터에서 SQL Server 플러그인 클러스터 클라이언트를 구성하는 단계를 제공합니다.

절차

- 1 클러스터의 활성 노드에 도메인 관리자로 로그인합니다. 이 계정은 각 클러스터 노드에서 로컬 Administrators 그룹의 구성원이기도 해야 합니다.
- 2 다음과 같이 VMware VDP Windows Cluster Configuration Wizard를 시작합니다.
 - Windows Server 2012에서 시작 화면을 열고 **VMware VDP Windows Cluster Configuration Wizard**를 선택합니다.
 - Windows Server 2008에서 시작 메뉴를 열고 **프로그램 파일 > VMware VDP > VMware VDP Windows Cluster Configuration Wizard**를 선택합니다.
- 3 **시작** 페이지에서 **다음**을 클릭합니다.
- 4 **플러그인** 페이지에서 **SQL**을 선택하고 **다음**을 클릭합니다.
클러스터 노드 페이지가 나타나고 노드의 목록과 상태가 표시됩니다.
- 5 **클러스터 노드** 페이지에서 환경이 다음 요구 사항을 충족하는지 확인하고 **다음**을 클릭합니다.
 - 각 SQL Server 노드가 작동 상태여야 합니다.
 - 각 노드의 Windows 클라이언트 소프트웨어 설치 상태가 설치됨이어야 합니다.
 - 각 노드의 SQL Server 플러그인 설치 상태가 설치됨이어야 합니다.
- 6 **작업** 페이지에서 **모든 노드에 대해 새 클러스터 클라이언트 구성**을 선택하고 **다음**을 클릭합니다.
- 7 **사전 요구 사항** 페이지에서 환경이 사전 요구 사항을 모두 충족하는지 확인합니다.
사전 요구 사항 옆의 선택 표시는 환경이 사전 요구 사항을 충족한다는 것을 나타냅니다.

환경이 사전 요구 사항을 하나라도 충족하지 않는 경우 마법사를 종료하고 문제를 해결한 다음 마법사를 다시 시작합니다.

- 8 환경에서 사용하는 IP 버전을 선택하고 다음을 클릭합니다.
- 9 **SQL 설정** 페이지에서 다음을 수행합니다.
 - a 목록에서 클러스터 클라이언트의 클러스터 그룹, 서비스 또는 역할을 선택합니다.
 - Windows Server 2012에서는 **클러스터 클라이언트의 클러스터 역할** 목록에서 클러스터 클라이언트의 클러스터 역할을 선택합니다.
 - Windows Server 2008에서는 **클러스터 클라이언트의 클러스터 서비스** 목록에서 클러스터 클라이언트의 클러스터 서비스를 선택합니다.
 - b **클러스터 클라이언트에 대한 공유 볼륨** 목록에서 클러스터 클라이언트의 공유 볼륨을 선택합니다.
 - c 다음을 클릭합니다.
- 10 **서버 설정** 페이지에서 다음과 같이 VDP 어플라이언스에 대한 설정을 지정합니다.
 - a **이름** 상자에 VDP 어플라이언스의 DNS 이름을 입력하거나 **IPv4/IPv6 주소** 상자에 IP 주소를 입력합니다.
 - b **포트 번호** 상자에 VDP 클라이언트/서버 통신에 사용되는 데이터 포트를 입력합니다.

참고 VDP 클라이언트가 VDP 어플라이언스와 통신하는 데 사용하는 기본 포트는 포트 28001입니다.

 - c **클러스터 클라이언트의 var 디렉토리** 상자에 폴더 또는 볼륨의 이름을 입력하거나 **찾아보기**를 클릭하여 폴더 또는 볼륨을 선택합니다.

이 폴더 또는 볼륨에는 클러스터 클라이언트 구성 및 로그 파일이 저장됩니다. 클러스터의 모든 노드에는 이 폴더 또는 볼륨에 대한 쓰기 권한이 있어야 합니다.

참고 네트워크의 원격 경로 이름 대신 클러스터가 소유한 볼륨을 선택하십시오.

 - d 다음을 클릭합니다.
- 11 **요약** 페이지에서 구성 설정을 검토하고 **구성**을 클릭합니다.

Progress 페이지에 구성 상태가 표시됩니다.
- 12 **결과** 페이지에서 정보를 검토하고 **닫기**를 클릭합니다.

AlwaysOn 가용성 그룹에 대한 클러스터 클라이언트 구성

AlwaysOn 가용성 그룹에 대한 VDP 클러스터 클라이언트를 사용하면 가용성 그룹의 SQL Server 데이터베이스를 백업 및 복구할 수 있습니다. VMware VDP Windows Cluster Configuration Wizard는 AlwaysOn 가용성 그룹에서 SQL Server 플러그인에 대한 VDP 클러스터 클라이언트를 구성하는 단계를 제공합니다.

절차

- 1 클러스터 노드에 도메인 관리자로 로그인합니다. 이 계정은 각 클러스터 노드에서 로컬 Administrators 그룹의 구성원이기도 해야 합니다.
- 2 다음과 같이 VMware VDP Windows Cluster Configuration Wizard를 시작합니다.
 - Windows Server 2012에서 **시작** 화면을 열고 **VMware VDP Windows Cluster Configuration Wizard**를 선택합니다.
 - Windows Server 2008에서 **시작** 메뉴를 열고 **프로그램 파일 > VMware VDP > VMware VDP Windows Cluster Configuration Wizard**를 선택합니다.
- 3 **시작** 페이지에서 다음을 클릭합니다.
- 4 **플러그인** 페이지에서 **SQL AlwaysOn**을 선택하고 다음을 클릭합니다.

- 5 클러스터 노드 페이지에서 다음을 수행합니다.
 - a 환경이 다음 요구 사항을 충족하는지 확인합니다.
 - 각 SQL Server 노드가 작동 상태여야 합니다.
 - 각 노드의 Windows 클라이언트 소프트웨어 설치 상태가 설치됨이어야 합니다.
 - 각 노드의 SQL Server 플러그인 설치 상태가 설치됨이어야 합니다.
 - b 다음을 클릭합니다.
- 6 작업 페이지에서 모든 노드에 대해 새 클러스터 클라이언트 구성을 선택하고 다음을 클릭합니다.
- 7 사전 요구 사항 페이지에서 환경이 사전 요구 사항을 모두 충족하는지 확인합니다.

사전 요구 사항 옆의 선택 표시는 환경이 사전 요구 사항을 충족한다는 것을 나타냅니다.

환경이 사전 요구 사항을 충족하지 않는 경우 마법사를 종료하고 문제를 해결한 다음 마법사를 다시 시작합니다.
- 8 환경에서 사용하는 IP 버전을 선택하고 다음을 클릭합니다.
- 9 SQL AlwaysOn 설정 페이지에서 다음을 수행합니다.
 - a 목록에서 클러스터 클라이언트의 클러스터 그룹, 서비스 또는 역할을 선택합니다.
 - Windows Server 2012에서는 클러스터 클라이언트의 클러스터 역할 목록에서 클러스터 클라이언트의 클러스터 역할을 선택합니다.
 - Windows Server 2008에서는 클러스터 클라이언트의 클러스터 서비스 목록에서 클러스터 클라이언트의 클러스터 서비스를 선택합니다.

클러스터 클라이언트의 이름이 클러스터 클라이언트 이름 필드에 표시됩니다.

참고 각 가용성 그룹의 가용성 그룹 Listener를 구성해야 합니다. Listener가 없는 가용성 그룹에 대해서는 클러스터 클라이언트를 구성하지 마십시오.

 - b 다음을 클릭합니다.
- 10 서버 설정 페이지에서 다음과 같이 VDP 어플라이언스에 대한 설정을 지정합니다.
 - a 이름 상자에 VDP 어플라이언스의 DNS 이름을 입력하거나 IPv4/IPv6 주소 상자에 IP 주소를 입력합니다.
 - b 포트 번호 상자에 VDP 클라이언트/서버 통신에 사용되는 데이터 포트를 입력합니다.

참고 VDP 어플라이언스가 통신하는 데 사용하는 기본 포트는 포트 28001입니다.

 - c 클러스터 클라이언트의 var 디렉토리 상자에 폴더 또는 볼륨의 이름을 입력하거나 찾아보기를 클릭하여 폴더 또는 볼륨을 선택합니다.

이 폴더 또는 볼륨에는 클러스터 클라이언트 구성 및 로그 파일이 저장됩니다. 클러스터의 모든 노드에는 이 폴더 또는 볼륨에 대한 쓰기 권한이 있어야 합니다.

참고 네트워크의 원격 경로 이름 대신 클러스터가 소유한 볼륨을 선택하십시오.

 - d 다음을 클릭합니다.
- 11 요약 페이지에서 구성 설정을 검토하고 구성을 클릭합니다.

Progress 페이지에 구성 상태가 표시됩니다.
- 12 결과 페이지에서 정보를 검토하고 닫기를 클릭합니다.

Microsoft SQL Server 백업 작업 생성

백업에 사용할 수 있는 각 SQL Server에 VMware VDP for SQL Server Client를 설치해야 합니다. 클라이언트 설치에 대한 자세한 내용은 “VDP for SQL Server Client 설치”(158페이지) 섹션을 참조하십시오.

- 1 vSphere Web Client에서 **백업** 탭을 선택합니다.
- 2 **백업** 탭에서 **백업 작업 조치**를 클릭하고 **새로 만들기**를 선택하여 **새 백업 작업 생성** 마법사를 시작합니다.
마법사의 작업 유형 페이지에서 **애플리케이션**을 선택합니다. 이 옵션을 사용하면 전체 서버 또는 선택한 데이터베이스를 백업할 수 있습니다.

애플리케이션 백업

작업 유형 페이지에서 **애플리케이션**을 선택하면 애플리케이션 서버를 백업할지 또는 개별 데이터베이스를 백업할지 선택할 수 있습니다.

- 1 **새 백업 작업 생성** 마법사의 **작업 유형** 페이지에서 **애플리케이션**을 선택하고 **다음**을 클릭합니다.
- 2 **데이터 유형** 페이지에서 다음 옵션 중 하나를 선택하고 **다음**을 클릭합니다.
 - **전체 서버**: 이 옵션을 사용하면 전체 애플리케이션 서버를 백업할 수 있습니다.
 - **선택된 데이터베이스**: 이 옵션을 사용하면 개별 애플리케이션 서버 데이터베이스를 백업할 수 있습니다.
- 3 **백업 소스** 페이지에서 다음 백업 소스 중 하나 옆의 화살표를 클릭하여 목록을 확장합니다.
 - **Microsoft SQL Server SQL Server** 백업의 경우 선택합니다.
 - **Microsoft SQL 페일오버 클러스터**: SQL 페일오버 클러스터 백업의 경우 선택합니다.
 - **Microsoft SQL AlwaysOn 클러스터 SQL AlwaysOn 가용성 그룹** 백업의 경우 선택합니다.
- 4 다음 단계 중 하나를 수행합니다.
 - 전체 서버를 백업하기로 선택한 경우 백업할 SQL Server 옆의 확인란을 선택하고 **다음**을 클릭합니다.
참고 Best Practice는 백업 작업당 SQL Server를 하나씩만 선택하는 것입니다.
 - 선택한 데이터베이스를 백업하는 경우 SQL Server 옆의 화살표를 클릭하고 계속 드릴다운하여 백업할 데이터베이스 또는 스토리지 그룹을 선택한 후 **다음**을 클릭합니다.
- 5 **백업 옵션** 페이지에서 백업 유형(**전체**, **차등**, **증분**)을 선택합니다. 구성할 수 있는 옵션은 선택한 유형에 따라 달라집니다.
 - **전체**: **전체** 옵션은 모든 객체, 시스템 테이블 및 데이터를 포함해 전체 데이터베이스를 백업합니다. 전체 백업에 대한 옵션은 다음과 같습니다.
 - **전체 백업 후 증분 강제 백업**: 이 확인란을 선택하거나 선택을 취소하여 전체 백업 사이에 발생하는 트랜잭션을 포함한 증분 백업이 수행되도록 할지 여부를 지정할 수 있습니다. 이 기능을 사용하면 전체 백업 사이의 한 시점에서의 시점 복구가 생성됩니다.
단순 복구 모델을 사용하는 데이터베이스에서는 트랜잭션 로그 백업을 지원하지 않으므로 이 옵션을 사용하지 마십시오. 여기에는 마스터 데이터베이스와 msdb 데이터베이스와 같은 시스템 데이터베이스가 포함됩니다.
단순 복구 모델 데이터베이스에는 **단순 복구 모델 데이터베이스에 적용** 옵션을 사용합니다.
 - **멀티 스트림 백업 활성화**: 데이터베이스당 하나의 스트림을 사용하여 여러 데이터베이스를 동시에 백업하거나 여러 병렬 스트림을 사용하여 단일 데이터베이스를 백업할 수 있습니다. 여러 병렬 스트림을 사용하여 단일 데이터베이스를 백업하도록 선택하는 경우, 백업 시 사용될 각 스트림의 최소 크기를 지정할 수 있습니다.
최소 스트림 크기를 결정한 후에는 다음 등식을 사용하여 데이터베이스를 백업하는 데 사용되는 스트림 수를 계산할 수 있습니다.
데이터베이스 크기/최소 스트림 크기 = 스트림 수

예를 들어, 데이터베이스가 1,280MB이고 최소 스트림 크기를 기본 설정인 256MB로 설정할 경우, 이 데이터베이스의 전체 백업을 수행하는 데 사용되는 스트림 수는 다음 등식과 같이 5개입니다.

$$1,280\text{MB}/256 = 5$$

트랜잭션 로그 및 차등 백업의 경우, 전체 데이터베이스 크기가 아니라 백업할 데이터의 크기가 스트림 수를 계산하는 데 사용됩니다. 데이터베이스 크기가 최소 스트림 크기보다 작은 경우, VDP는 단일 스트림을 사용하여 데이터베이스를 백업합니다.

최소 스트림 크기에 기초하여 데이터베이스의 스트림 수를 계산한 결과, 이 수가 백업용으로 구성된 최대 스트림 수를 초과할 경우, 해당 데이터베이스의 백업에는 최대 스트림 수만 사용됩니다.

- **단순 복구 모델 데이터베이스에 적용:** 이 옵션은 VDP가 트랜잭션 로그 백업을 지원하지 않는 단순 복구 모델을 사용하는 데이터베이스의 증가분(트랜잭션 로그) 백업을 처리하는 방법을 지정합니다.

오류 시 증분 건너뛰기(기본 설정): 서로 다른 복구 모델을 사용하는 데이터베이스를 백업하도록 선택할 경우, 단순 복구 모델을 사용하는 데이터베이스는 백업에 포함되지 않습니다. 백업은 완료되지만 예외가 발생하고 오류 메시지가 로그에 기록됩니다. 단순 복구 모델을 사용하는 데이터베이스만 백업하도록 선택한 경우에는 백업이 실패합니다.

경고 시 증분 건너뛰기: 서로 다른 복구 모델을 사용하는 데이터베이스를 백업하도록 선택할 경우, 단순 복구 모델을 사용하는 데이터베이스는 백업에 포함되지 않습니다. 백업이 성공적으로 완료되고, 단순 복구 모델을 사용하는 각 데이터베이스별로 로그에 경고가 기록됩니다. 단순 복구 모델을 사용하는 데이터베이스만 백업하도록 선택한 경우에는 백업이 실패합니다.

증분에서 전체로 상향: 단순 복구 모델을 사용하는 데이터베이스에 대해서는 트랜잭션 로그 백업 대신 전체 백업이 자동으로 발생합니다.

- **데이터베이스 로그 잘라내기:** 이 옵션은 데이터베이스 트랜잭션 로그 잘라내기 동작이 제어되는 방법을 지정합니다. 다음과 같은 잘라내기 옵션이 있습니다.

증분 백업에만 적용(기본 설정): 백업 유형이 증분(트랜잭션 로그)으로 설정된 경우 데이터베이스 트랜잭션 로그가 잘립니다. 백업 유형이 전체 또는 차등인 경우에는 로그 잘라내기가 발생하지 않습니다.

모든 백업 유형에 적용: 백업 유형과 관계없이 데이터베이스 트랜잭션 로그가 잘립니다. 이 설정은 로그 백업 체인을 끊으므로 백업 유형이 전체로 설정된 경우가 아니면 사용해서는 안 됩니다.

Never: 어떤 상황에서도 데이터베이스 트랜잭션 로그가 잘리지 않습니다.

- **인증 방식:** 인증 방식은 SQL Server에 연결할 때 NT 인증을 사용할지 또는 SQL Server 인증을 사용할지를 지정합니다. SQL Server 인증을 선택한 경우 SQL Server 로그인 이름과 암호를 지정하십시오.
- **백업에 대한 가용성 그룹 복제본:** 다음 4가지 옵션이 있습니다.

1차 목표: 이 옵션을 선택하면 선택한 Always On 가용성 그룹의 운영 복제본에서 백업이 실행됩니다.

보조 우선: 이 옵션을 선택하면 선택한 Always On 가용성 그룹의 보조 복제본에서 백업이 실행됩니다. 보조 복제본을 사용할 수 없는 경우 운영 복제본에서 백업이 실행됩니다.

보조만: 이 옵션을 선택하면 선택한 Always On 가용성 그룹의 보조 복제본에서 백업이 실행됩니다. 보조 복제본을 사용할 수 없는 경우 백업이 중단되고 해당 오류 메시지가 로그 파일에 기록됩니다.

SQL Server 정의: 이 옵션을 선택하면 SQL Server 구성에 따라 운영 또는 보조 복제본에서 백업이 실행됩니다. Automated_Backup_Preference를 none으로 설정하는 경우 운영 복제본에서 백업이 실행됩니다.

- **차등 또는 증분:** 차등 옵션은 마지막 전체 백업 이후 변경된 모든 데이터를 백업합니다. 증분 옵션은 트랜잭션 로그만 백업합니다. 전체 백업과 다른 유일한 구성 옵션은 증분 백업이 아니라 전체 백업을 강제 적용할 수 있다는 것입니다.

- **전체 강제 백업:** 이 확인란을 선택하거나 선택을 취소하여 VDP가 로그 간격을 감지하거나 이전 전체 백업이 없는 경우 트랜잭션 로그(증분) 또는 차등 백업을 적용할 수 있는 전체 백업을 수행할지 여부를 결정합니다. 이 옵션은 필요 시 전체 백업의 수행을 효과적으로 자동화합니다.
 차등 또는 증분을 선택할 경우 이 옵션이 선택된 상태로 두어야 합니다(기본 설정). 그렇지 않으면 VDP에 기존의 전체 백업이 존재하지 않는 경우 데이터를 복구하지 못할 수 있습니다.
- 6 다음을 클릭합니다.
 - 7 스케줄 페이지에서 백업 작업에 대한 백업 스케줄과 시작 시간을 선택하고 다음을 클릭합니다.
 스케줄을 구성하는 방법에 대한 자세한 내용은 “백업 스케줄 지정”(111페이지) 섹션을 참조하십시오.
 - 8 보존 정책 페이지에서 백업 유지 기간에 대한 옵션을 선택하고 다음을 클릭합니다.
 보존 정책을 구성하는 방법에 대한 자세한 내용은 “보존 정책 설정”(111페이지) 섹션을 참조하십시오.
 - 9 이름 페이지에서 백업 작업 이름을 입력하고 다음을 클릭합니다.
 - 10 완료 준비 페이지에서 백업 작업에 대한 요약 정보를 검토하고 마침을 클릭합니다.
 - 11 백업 작업이 성공적으로 생성되었다는 메시지가 나타나면 확인을 클릭합니다.

Microsoft SQL Server의 백업 복구

백업을 Microsoft SQL Server에서 실행했으면 이러한 백업을 원래 위치나 대체 위치로 복구할 수 있습니다.

절차

- 1 vSphere Web Client에서 복구 탭을 선택합니다.
- 2 복구할 백업을 선택합니다. SQL Server는 여러 개를 선택할 수 있지만 복구 시점은 각 SQL Server별로 하나만 선택할 수 있습니다.
- 3 복구를 클릭합니다.
- 4 백업 선택 페이지에서 복구할 백업 작업을 선택하고 다음을 클릭합니다.
- 5 복구 옵션 선택 페이지에서 다음을 수행합니다.
 - a 다음 단계 중 하나를 수행합니다.
 - 백업을 원래 위치로 복구하려면 원래 위치로 복구 옵션을 선택된 상태(기본 설정)로 둡니다.
 - 백업을 대체 위치로 복구하려면 원래 위치로 복구 옵션을 지우고 다음을 수행합니다.
 - i 선택을 클릭하여 대상 위치를 선택합니다.
 - ii **SQL 인스턴스** 입력란에 SQL 인스턴스 이름을 입력합니다. "로컬"을 사용하는 경우 괄호 안에 입력해야 합니다.
 - iii **위치 경로** 입력란에 데이터베이스 파일을 복구할 기존의 전체 Windows 경로를 입력합니다.
 위치 경로가 존재하지 않을 경우 해당 경로가 생성되지 않으므로 복구가 실패합니다.
 - iv **로그 파일 경로** 입력란에 로그 파일을 복구할 기존의 전체 Windows 경로를 입력합니다.
 - b 고급 옵션을 지정하려면 고급 옵션 옆의 화살표를 클릭하여 목록을 확장합니다. 옵션은 다음과 같습니다.
 - **SQL REPLACE 사용:** 이 옵션은 동일한 이름을 가진 데이터베이스나 파일이 이미 존재하는 경우에도 SQL Server가 필요한 데이터베이스와 관련 파일을 생성하도록 지정합니다.
 이 옵션은 사용자가 실수로 다른 데이터베이스나 파일을 덮어쓰는 것을 방지하기 위한 SQL Server 안전 검사보다 우선 적용됩니다. 이 안전 검사는 Microsoft Transact-SQL 참조 설명서 RESTORE 명령 섹션에 설명되어 있습니다.

- **운영 복제본에서만 복구:** `--recover-primary-only` 플래그를 설정하여 보조 복제본의 자동 복구를 비활성화하고 운영 복제본에서만 복구를 수행합니다. 기본적으로 이 확인란이 활성화된 상태이므로 운영 복제본에서만 복구가 수행됩니다. 이 옵션은 AlwaysOn 가용성 그룹에 있는 데이터베이스에 대해서만 활성화됩니다.

참고 운영 복제본에서만 데이터베이스를 복구한 후에 보조 복제본의 해당 데이터베이스는 복구 중 상태가 됩니다.

- **Tail 로그 백업:** 복구 프로세스에서 Tail 로그 백업을 수행하려면 해당 데이터베이스가 온라인 상태이고 전체 또는 대량 로그되는 복구 모델을 사용해야 합니다. 시스템 데이터베이스(예: 마스터 및 msdb 데이터베이스)는 단순 복구 모델을 사용하므로 이러한 데이터베이스에 대해서는 Tail 로그 백업을 수행할 수 없습니다.

다른 SQL Server 인스턴스로 리디렉션 복구를 수행할 경우에는 Tail 로그 백업을 선택하지 마십시오.

- **시스템 데이터베이스 복구:** 시스템 데이터베이스만 복구해야 하는 경우는 드물지만, 하나 이상의 시스템 데이터베이스가 손상된 경우에는 이러한 복구가 필요할 수 있습니다.

대개 사용자 데이터베이스를 복구하는 동시에 시스템 데이터베이스를 복구해야 하는 경우가 더 많습니다. 시스템 데이터베이스와 사용자 데이터베이스를 모두 복구하도록 선택하면 시스템 데이터베이스가 먼저 복구됩니다.

시스템 데이터베이스를 복구하면 VDP Microsoft SQL Server Client가 SQL Server 서비스 관리에 사용되는 데이터베이스를 자동으로 올바른 순서(마스터, msdb, 모델 순)로 복구합니다.

- **인증 방식:** 인증 방식은 SQL Server에 연결할 때 NT 인증을 사용할지 또는 SQL Server 인증을 사용할지를 지정합니다. SQL Server 인증을 선택한 경우 SQL Server 로그인 이름과 암호를 지정하십시오.
- **복구 작업:** SQL AlwaysOn 클러스터 환경에서 복구를 수행하는 경우 복구 또는 복구 안 함 중에서 적절한 값을 선택합니다.

c 다음을 클릭합니다.

- 6 **완료 준비** 페이지에서 복구 요청을 검토하고 **마침**을 클릭합니다.
- 7 복구가 시작되었다는 메시지가 표시되면 **확인**을 클릭합니다.
- 8 **최근 작업** 창에서 복구 진행률을 모니터링합니다.

클라이언트 작업 모니터링

클라이언트 로그를 수집하고 분석하여 모든 클라이언트 작업에 대한 작업 및 이벤트를 모니터링할 수 있습니다. 클라이언트 로그는 Microsoft 애플리케이션(MSApp) 관련 로그입니다. 취합된 클라이언트 로그에는, 통과되었지만 예외가 발생했거나 실패한 복제, 백업, 복구 또는 ABV(Automatic Backup Verification) 작업이 모두 포함됩니다. 자세한 내용은 **“VDP 로그 또는 진단 정보 수집”**(38페이지) 섹션을 참조하십시오.

VDP Plug-in for SQL Server 제거

VDP Plug-in for SQL Server를 제거하려면

- Windows Server 2012 또는 Windows Server 2008에서는 **프로그램 및 기능**을 사용합니다.
- Windows Server 2003에서는 **프로그램 추가/제거**를 사용합니다.

Microsoft Exchange Server 백업 및 복구

이 섹션에서는 다음 내용을 다룹니다.

- **“Microsoft Exchange Server 지원”**(166페이지)
- **“VDP for Exchange Server Client 설치”**(167페이지)
- **“VMware Exchange Backup User Configuration Tool 사용”**(170페이지)

- “VDP 백업 서비스 수동 구성”(171페이지)
- “Microsoft Exchange Server 백업 작업 생성”(171페이지)
- “Microsoft Exchange Server의 백업 복구”(173페이지)
- “Microsoft Exchange Server에 대한 세밀한 레벨의 복구”(175페이지)
- “Exchange Server 플러그인 제거”(174페이지)

Microsoft Exchange Server 옵션

VDP는 Microsoft Exchange Server에 대한 향상된 백업 및 복구 옵션을 지원합니다.

- 선택된 Exchange Server 백업
- 선택된 개별 Exchange 데이터베이스 또는 스토리지 그룹 백업
- 증분 백업을 수행할 수 있는 기능
- 멀티 스트리밍 백업 지원(최대 10개 스트림)
- 순환 로깅 지원(상향, 순환, 건너뛰기)
- Exchange를 원래 위치나 대체 위치로 복구할 수 있는 기능
- 복구 중에 로그가 재생되지 않도록 하는 옵션
- RSG(Recovery Storage Group)/RDB(Recovery Database)
- 세밀한 레벨의 복구

Microsoft Exchange Server 지원

표 17-25에는 VDP Plug-in for Microsoft Exchange를 지원하는 Microsoft Exchange Server 버전 및 운영 체제가 나와 있습니다.

표 17-25. 지원되는 Microsoft Exchange Server 버전 및 운영 체제

Exchange Server 버전	운영 체제
<ul style="list-style-type: none"> ■ Exchange Server 2013 ■ Exchange Server 2013 DAG(Database Availability Group) 	<ul style="list-style-type: none"> ■ Windows Server 2012(x64) ■ Windows Server 2012 R2(x64) ■ Windows Server 2008 R2(x64)
<ul style="list-style-type: none"> ■ Exchange Server 2010 SP3 ■ Exchange Server 2010 DAG(Database Availability Group) 	<ul style="list-style-type: none"> ■ Windows Server 2012(x64) ■ Windows Server 2008 R2(x64) ■ Windows Server 2008 SP2(x64)
<ul style="list-style-type: none"> ■ Exchange Server 2007 SP3 	<ul style="list-style-type: none"> ■ Windows Server 2008 R2(x64) ■ Windows Server 2008 SP2(x64)

Microsoft .NET Framework 4 요구 사항

Exchange Server VSS 플러그인을 사용하려면 Exchange Server 포리스트의 각 서버에 Microsoft .NET Framework 4를 설치해야 합니다. Microsoft 다운로드 센터에서 "Microsoft .NET Framework 4"를 검색하여 다운로드와 추가 정보를 찾으십시오.

하드웨어 요구 사항

표 17-26에는 VDP Plug-in for Microsoft Exchange Server에 대한 하드웨어 요구 사항이 정리되어 있습니다.

표 17-26. Microsoft Exchange Server에 대한 하드웨어 요구 사항

요구 사항	최소
메모리(RAM)	64MB
하드 드라이브 공간	소프트웨어를 설치하려면 최소 100MB의 영구 하드 드라이브 공간이 필요합니다(1GB 권장). 로컬 캐시 파일에는 물리적 RAM 64MB당 12MB의 영구 하드 드라이브 공간이 추가적으로 필요합니다.

지원되지 않는 Microsoft Exchange Server

Microsoft Exchange Server 2007 클러스터(SCC, CCR, SCR)는 VDP Plug-in for Microsoft Exchange Server에서 지원되지 않습니다.

VDP for Exchange Server Client 설치

게스트 레벨 백업을 지원하려면 각 Exchange Server에 백업과 복구를 지원하기 위한 VMware VDP(vSphere Data Protection) for Exchange Server Client가 설치되어 있어야 합니다.

사전 요구 사항

VDP를 사용하기 전에 “[VDP 설치 및 구성](#)”(21페이지)의 설명에 따라 VDP 어플라이언스를 설치 및 구성해야 하며 Exchange Server에 대한 관리 권한이 있어야 합니다.

절차

- 1 각 Exchange Server 클라이언트에서 vSphere Web Client에 액세스합니다.
`https://<IP_address_vCenter_Server>:9443/vsphere-client/`
- 2 자격 증명 페이지에 vCenter 관리 사용자 이름과 암호를 입력하고 **로그인**을 클릭합니다.
- 3 vSphere Web Client에서 **VDP**를 선택합니다.
- 4 VDP 시작 페이지에서 VDP 어플라이언스를 선택하고 **연결**을 클릭합니다.
- 5 **구성** 탭을 클릭합니다.
- 6 **클라이언트 다운로드**에서 **Microsoft Exchange Server 64비트**를 클릭합니다.
- 7 사용 중인 브라우저에 따라 .msi 파일을 저장하거나 실행할 수 있습니다. .msi 파일을 실행하면 VMware VDP for Exchange Server 설치 마법사가 시작됩니다. **다음**을 클릭합니다.
- 8 **최종 사용자 사용권 계약** 페이지에서 라이선스를 읽고 동의하는 경우 **동의함**과 **다음**을 차례로 클릭합니다.
- 9 **어플라이언스 등록 정보** 페이지에서 Exchange Server를 백업할 VDP 어플라이언스의 정규화된 도메인 이름 또는 IP 주소를 입력하고 **다음**을 클릭합니다.
- 10 (선택 사항) 세밀한 레벨의 복구에 서버를 사용할 계획이면 **Exchange Server GLR** 플러그인을 설치하는 옵션을 선택합니다.

참고 Exchange Server GLR 옵션을 선택한 경우 Microsoft Exchange Server를 재부팅해야 합니다.

- 11 **VMware VDP for Exchange Server 설치 준비** 페이지에서 **설치**를 클릭합니다.
- 12 **VMware VDP for Exchange Server 설치 마법사 완료** 페이지에서 **마침**을 클릭합니다.

VDP Exchange Backup User Configuration Tool 확인란을 선택한 경우 “[VMware Exchange Backup User Configuration Tool 사용](#)”(170페이지) 섹션으로 진행합니다.

VDP Exchange Backup Configuration Tool 확인란을 선택하지 않은 경우에는 “[VDP 백업 서비스 수동 구성](#)”(171페이지) 섹션으로 진행합니다.

추가 Exchange Server에 대해 이 절차를 반복합니다.

DAG 또는 클러스터 환경에서 설치

절차

- 1 Exchange for VDP는 단일 독립 실행형 설치 관리자로 구성됩니다. 각 Exchange 서버에서 메일박스 서버 역할을 사용하여 VDP for Exchange Client 플러그인을 설치합니다.

세밀한 레벨의 복구에 서버를 사용하려면 Exchange GLR 플러그인과 Exchange VSS 플러그인을 모두 설치하는 옵션을 선택합니다. DAG 환경에서는 GLR용 서버를 하나 이상 구성해야 합니다.

참고 Exchange GLR 플러그인을 설치한 후 Exchange 서버를 다시 시작해야 합니다.

- 2 각 Exchange 서버를 VDP 어플라이언스에 클라이언트로 등록합니다.
- 3 VmwareVDPBackupUser 계정을 생성 및 구성합니다.
- 4 VMware VDP Windows Cluster Configuration Wizard를 사용하여 Exchange DAG 클라이언트 또는 VDP 클러스터 클라이언트를 구성합니다.

Exchange DAG 클라이언트 구성

Exchange DAG 클라이언트를 구성하면 Exchange Server 2013 또는 2010 DAG에서 데이터베이스의 페더레이션 백업을 수행할 수 있습니다.

사전 요구 사항

Exchange DAG 클라이언트를 구성하기 전에 DAG 클러스터 환경이 다음 사전 요구 사항을 충족하는지 확인하십시오.

- VDP Windows 클라이언트가 설치되어 있어야 합니다.
- VDP Backup Plug-in for Exchange DAG가 설치되어 있어야 합니다.
- 노드에 DAG 클라이언트가 이미 구성된 경우 DAG 그룹이 있어야 합니다.
- 새 VDP Exchange DAG 클라이언트에 할당할 수 있는 사용되지 않은 정적 IP 주소가 있어야 합니다.
- 모든 클러스터 노드의 컴퓨터 계정이 SMB 공유에 대해 모든 권한을 가지고 있어야 합니다.
- Exchange DAG 페더레이션 백업에서 var 디렉토리로 사용할 네트워크 공유를 생성해야 합니다.

절차

- 1 DAG에서 VmwareVDPBackupUser 계정을 사용하여 Exchange 서버에 로그인합니다.
- 2 다음과 같이 VMware VDP Windows Cluster Configuration Wizard를 시작합니다.
 - Windows Server 2012에서 시작 화면을 열고 **VMware VDP Windows Cluster Configuration Wizard**를 선택합니다.
 - Windows Server 2008에서 시작 메뉴를 열고 **프로그램 파일 > VMware VDP > VMware VDP Windows Cluster Configuration Wizard**를 선택합니다.
- 3 시작 페이지에서 다음을 클릭합니다.
- 4 플러그인 페이지에서 **Exchange DAG**를 선택하고 다음을 클릭합니다.
- 5 DAG 노드 페이지에서 다음을 수행합니다.
 - a 환경이 다음 요구 사항을 충족하는지 확인합니다.
 - 각 Exchange 서버가 **작동** 상태여야 합니다.
 - 각 서버의 Windows 클라이언트 소프트웨어 설치 상태가 설치됨입니다.
 - 각 서버의 Exchange VSS 플러그인 설치 상태가 설치됨입니다.
 - b 다음을 클릭합니다.
- 6 작업 페이지에서 **모든 노드에 대해 새 DAG 클라이언트 구성**을 선택하고 다음을 클릭합니다.
- 7 **사전 요구 사항** 페이지에서 다음을 수행합니다.
 - a 환경이 모든 사전 요구 사항을 충족하는지 확인합니다.

사전 요구 사항 옆의 선택 표시는 환경이 사전 요구 사항을 충족한다는 것을 나타냅니다.

환경이 사전 요구 사항을 충족하지 않는 경우 마법사를 종료하고 문제를 해결한 다음 마법사를 다시 시작합니다.
 - b 환경에서 사용하는 인터넷 프로토콜 버전(IPv4 또는 IPv6)을 선택합니다.
 - c 다음을 클릭합니다.

- 8 **DAG 클라이언트 설정** 페이지에서 DAG 클라이언트에 대한 클러스터 그룹의 클라이언트 설정을 지정합니다.
 - a 네트워크 목록에서 네트워크를 선택합니다.
 - b **Exchange DAG 클라이언트 IPv4/IPv6 주소** 상자에 DAG 클라이언트 클러스터 그룹의 IP 주소를 입력합니다. 고유하고 사용되지 않은 IP 주소를 지정해야 합니다. DAG의 IP 주소를 사용하지 마십시오.
 - c **Exchange DAG 클라이언트 IP 서브넷 마스크** 입력란에 DAG 클라이언트 클러스터 그룹의 네트워크 마스크를 입력합니다.
 - d 다음을 클릭합니다.
- 9 사용자 설정 페이지에서 다음을 수행합니다.
 - a 다음 로그인 계정 중 하나를 선택합니다.
 - 로컬 시스템 계정
 - 이 계정 및 VmwareVDPBackupUser 계정의 계정 이름과 암호를 지정합니다.
 - b 다음을 클릭합니다.
- 10 **서버 설정** 페이지에서 다음과 같이 VDP 어플라이언스에 대한 설정을 지정합니다.
 - a 이름 상자에 VDP 어플라이언스의 DNS 이름을 입력하거나 **IPv4/IPv6 주소** 상자에 IP 주소를 입력합니다.
 - b **DAG 클라이언트의 VDP 클라이언트 도메인** 상자에 Exchange DAG 클라이언트의 VDP 도메인 이름을 입력합니다.
 - c **포트 번호** 상자에 VDP 클라이언트/서버 통신에 사용되는 데이터 포트를 입력합니다.
 - d **클러스터 클라이언트의 var 디렉토리** 상자에 클러스터 클라이언트 var 폴더의 경로를 입력하거나 **찾아보기**를 클릭하여 위치를 선택합니다.

var 폴더는 Exchange DAG 클라이언트 구성 및 로그 파일을 저장합니다. VmwareVDPBackupUser 계정 및 클러스터의 모든 노드는 이 위치에 대한 쓰기 권한이 있어야 합니다.

참고 DAG의 각 서버가 액세스할 수 있는 볼륨을 선택합니다.

 - e 다음을 클릭합니다.
- 11 **요약** 페이지에서 마법사에서 지정한 설정을 검토하고 **구성**을 클릭합니다.

Progress 페이지에 구성 상태가 표시됩니다.
- 12 **결과** 페이지에서 정보를 검토하고 **닫기**를 클릭합니다.

VMware Exchange Backup User Configuration Tool 사용

VMware VDP for Exchange Server Client 설치 중에 **Exchange Backup User Configuration 유틸리티** 시작 확인란을 선택한 경우에는 설치가 완료된 후 VDP Exchange Backup User Configuration Tool이 자동으로 시작됩니다.

VMwareVDPBackupUser 계정

VDP Microsoft Exchange Server Client에는 Exchange Server에 대한 직접 액세스가 필요합니다. VDP에 적절한 도메인과 관리자 레벨 권한을 부여하려면 VMwareVDPBackupUser라는 특수 사용자 계정이 필요합니다. 이 사용자 계정은 VDP Microsoft Exchange Server Client 설치 후 기본적으로 실행되는 VDP Exchange Backup User Configuration Tool을 통해 설정됩니다.

참고 VDP Backup Agent 서비스는 더 이상 이 계정으로 실행할 필요가 없고 사용자가 **Backup Agent** 구성 확인란을 선택할 필요도 없습니다. VDP Backup Agent를 로컬 시스템 계정으로 실행하도록 구성한 경우 사용자가 백업 작업을 생성하거나 백업 및 복구 작업을 수행할 때 자격 증명을 입력해야 합니다.

VMwareVDPBackupUser는 다음과 같이 구성됩니다.

- 이 사용자 계정이 추가되어 적절한 Active Directory, Exchange 및 그룹 계정에 대해 활성화됩니다. 이 사용자 계정은 다음 그룹에 추가됩니다.
 - 백업 운영자
 - 도메인 사용자
 - 도메인 관리자(Exchange Server 2007용)
 - Exchange Server
 - Exchange Server 2010 및 2013용 Exchange 조직 관리(Microsoft Exchange 보안 그룹 내)
 - Exchange Server 2007의 경우 Exchange 조직 관리자
- 이 사용자 계정에 대한 메일박스가 생성, 활성화 및 테스트됩니다.
- Exchange 도메인에서 사용자 계정이 설정 및 활성화된 후 VDP Microsoft Exchange Server Client를 실행하는 각 Exchange Server에서 설정 및 활성화됩니다. VMwareVDPBackupUser 계정을 사용하려면 VDP 백업 서비스가 구성되어 있어야 합니다.

사전 요구 사항

- VDP를 사용하기 전에 “**VDP 설치 및 구성**”(21페이지)의 설명에 따라 VDP를 설치 및 구성해야 합니다.
- VMware VDP for Exchange Server Client 설치 중에 **Exchange Backup User Configuration 유틸리티** 시작 확인란을 선택해야 합니다. 사용자가 설치 시에 이 확인란을 선택하지 않은 경우 다음 위치에서 VMware Exchange Backup User Configuration Tool을 수동으로 시작할 수 있습니다.

```
x:\program files\avp\bin\vmbackupusercfg.exe
```

- .NET 4.0이 Exchange Server에 설치되어 있어야 합니다.

절차

- 1 VMware Exchange Backup User Configuration Tool에서 구성할 사용자의 상태에 따라 **새 사용자** 또는 **기존 사용자**를 선택합니다.
- 2 **사용자 이름** 필드에 VMwareVDPBackupUser 계정의 사용자 이름을 입력합니다. 필요한 경우 VMwareVDPBackupUser의 기본 이름을 사용할 수 있습니다.
- 3 **암호** 필드에 계정 암호를 입력합니다.
- 4 **암호 확인** 필드에 암호를 다시 입력합니다.
- 5 **Exchange Server** 필드에서 VDP Microsoft Exchange Server Client가 설치된 Exchange Server의 이름을 선택합니다.
- 6 **스토리지 그룹** 필드(Exchange Server 2007의 경우에만 활성화)에서 스토리지 그룹 이름을 선택합니다.

- 7 **메일박스 저장소** 필드에서 VMwareVDPBackupUser 계정의 메일박스 데이터베이스를 선택합니다.
- 8 **점검**을 클릭하여 새 사용자 설정을 테스트합니다. 사용자가 Active Directory에 없는 경우 점검이 실패합니다.
- 9 **서비스 구성**을 클릭합니다.
- 10 통과했거나 성공적이었던 테스트 집합이 메시지 로그에 나열됩니다. 모든 점검 테스트가 통과된 경우 **닫기**를 클릭합니다.

VDP 백업 서비스 수동 구성

이미 VDP Exchange Backup User Configuration Tool을 실행했으면 VMwareVDPBackupUser 계정이 생성되어 있습니다. VDP 백업 서비스를 실행하기 위해 다음 단계를 사용하여 VMwareVDPBackupUser 계정을 수동으로 구성합니다.

- VDP를 사용하기 전에 **“VDP 설치 및 구성”**(21페이지)의 설명에 따라 VDP를 설치 및 구성해야 합니다.
- Exchange Backup User Configuration 유틸리티 시작을 통해 VMwareVDPBackupUser 계정이 생성되었습니다.

절차

- 1 VMwareVDPBackupUser 또는 관리 권한을 가진 다른 사용자로 Exchange Server에 로그인합니다.
- 2 **시작 > 프로그램 > 관리 도구 > 서비스**를 선택하여 서비스 애플리케이션을 시작합니다.
- 3 서비스 창에서 서비스 목록에 있는 **Backup Agent**를 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
- 4 Backup Agent 속성 대화상자에서 **로그온** 탭을 클릭합니다.
- 5 **이 계정** 버튼을 선택하고 VDP Exchange Backup User Configuration Tool에서 생성된 사용자 이름(기본적으로 VMwareVDPBackupUser)을 지정합니다.
- 6 **암호 및 암호 확인** 필드에 VMwareVDPBackupUser 계정 암호를 입력한 다음 **확인**을 클릭합니다.
- 7 서비스 목록에서 Backup Agent 서비스를 마우스 오른쪽 버튼으로 클릭하고 **다시 시작**을 선택합니다.

참고 GLR이 설치된 경우 "VMware VDP Exchange GLR Service"에 대해서도 이 절차를 반복해야 합니다.

Microsoft Exchange Server 백업 작업 생성

Microsoft Exchange Server Client를 백업에 사용하려면 VMware VDP Microsoft Exchange Server Client가 설치되어 있어야 합니다. 클라이언트 설치에 대한 자세한 내용은 **“VDP for Exchange Server Client 설치”**(167페이지) 섹션을 참조하십시오.

- 1 vSphere Web Client에서 **백업** 탭을 선택합니다.
- 2 **백업** 탭에서 **백업 작업 조치**를 클릭하고 **새로 만들기**를 선택하여 **새 백업 작업 생성** 마법사를 시작합니다.
- 3 마법사의 작업 유형 페이지에서 **애플리케이션**을 선택합니다. 이 옵션을 사용하면 전체 서버 또는 선택한 데이터베이스를 백업할 수 있습니다.

선택한 작업 유형에 따라 여기에서 선택할 수 있는 옵션이 결정됩니다. 선택 항목에 따라 아래 해당 섹션의 지침을 따릅니다.

애플리케이션 백업

작업 유형 페이지에서 **애플리케이션**을 선택하면 애플리케이션 서버를 백업할지 또는 개별 데이터베이스를 백업할지 선택할 수 있습니다.

- 1 새 백업 작업 생성 마법사의 **작업 유형** 페이지에서 **애플리케이션**을 선택하고 **다음**을 클릭합니다.
- 2 **데이터 유형** 페이지에서 다음 옵션 중 하나를 선택하고 **다음**을 클릭합니다.
 - **전체 서버**: 이 옵션을 사용하면 전체 애플리케이션 서버를 백업할 수 있습니다.

- **선택된 데이터베이스:** 이 옵션을 사용하면 개별 애플리케이션 서버 데이터베이스를 백업할 수 있습니다.
- 3 **백업 소스** 페이지에서 **Microsoft Exchange Server** 옆의 화살표를 클릭하여 목록을 확장합니다.
 - 4 다음 중 하나를 수행합니다.

참고 Best Practice는 백업 작업당 Exchange Server를 하나만 선택하는 것입니다.

 - 전체 서버를 백업하기로 선택한 경우 백업할 Exchange Server 옆의 확인란을 선택한 후 다음을 클릭합니다.
 - 선택한 데이터베이스를 백업하기로 선택한 경우 Exchange Server 옆의 화살표를 클릭하고 계속 드릴 다운하여 백업할 데이터베이스 또는 스토리지 그룹을 선택한 후 다음을 클릭합니다. 클라이언트가 로컬 시스템 계정으로 실행 중인 경우 사용자가 Exchange 관리자 자격 증명을 제공해야 Exchange 서버로 드릴다운할 수 있습니다.

참고 백업 타겟이 Exchange 2007 Server인 경우 개별 데이터베이스를 선택할 수 없고 대신 스토리지 그룹을 선택해야 합니다.
 - 5 **백업 옵션** 페이지에서 다음을 수행합니다.
 - a 전체 또는 **중분** 백업 유형을 선택합니다. 전체 백업이 존재하지 않을 경우 중분 백업이 전체 백업으로 자동으로 상향됩니다.

참고 클라이언트가 로컬 시스템 계정으로 실행 중인 경우 사용자는 Exchange 관리자 자격 증명을 제공해야 합니다. 로컬 시스템 계정으로 실행 중이지 않은 경우에는 자격 증명 없이도 실행됩니다.

중분을 선택한 경우 순환 로깅 옵션을 지정할 수 있습니다. 순환 로깅을 사용하면 시스템에 상주하는 트랜잭션 로그 수를 줄일 수 있습니다. 전체가 아니라 일부 스토리지 그룹 또는 데이터베이스에 대해서만 순환 로깅이 활성화되어 있는 혼합 환경에서는 이러한 설정 중 하나를 선택하여 VDP가 증가분 백업을 처리하는 방법을 지정할 수 있습니다.

 - **Promote**(기본 설정): 이 옵션은 saveset에 순환 로깅이 활성화된 데이터베이스가 있으면 중분 백업을 전체 백업으로 상향시킵니다. 순환 로깅 활성화 여부와 관계없이 모든 데이터베이스가 백업됩니다. 하나 이상의 데이터베이스에 순환 로깅이 활성화되어 있으면 saveset의 모든 데이터베이스에서 중분 백업이 전체 백업으로 상향됩니다.
 - **Circular:** 이 옵션은 순환 로깅이 활성화된 모든 데이터베이스의 모든 중분 백업을 전체 백업으로 상향시키고 순환 로깅이 활성화되지 않은 데이터베이스는 건너뛵니다.
 - **Skip:** 이 옵션은 순환 로깅이 비활성화된 모든 데이터베이스의 중분 백업을 수행하고 순환 로깅이 활성화된 모든 데이터베이스는 건너뛵니다.
 - b (DAG 클러스터에만 해당) **기본 서버 순서** 목록 상자에서 Exchange 데이터베이스 백업에 사용할 서버의 우선 순위를 지정합니다. FQDN이 아니라 서버 이름을 지정하십시오. 항목이 여러이면 심표로 구분합니다. 목록을 지정하지 않는 경우 Exchange VSS 플러그인은 DAG의 모든 서버를 목록에 사전순으로 추가합니다.
 - c (DAG 클러스터에만 해당) 백업할 데이터베이스 유형을 선택합니다.
 - 정상적인 패시브 복사본이 있는 경우 각 데이터베이스의 패시브 복사본을 백업하려면 **패시브** 옵션을 선택합니다. 정상적인 패시브 복사본이 없는 경우 VDP 어플라이언스는 액티브 복사본을 백업합니다.
 - 각 데이터베이스 액티브 복사본만 백업하려면 **액티브**만 선택합니다.
 - 각 데이터베이스 패시브 복사본만 백업하려면 **패시브**만 선택합니다. 정상적인 패시브 복사본이 없는 경우에는 백업에 데이터베이스가 포함되지 않습니다.
 - 6 여러 프로세서를 사용하는 백업 작업의 병렬 처리를 허용하려면 **멀티 스트림 백업 활성화** 옵션을 선택합니다. 슬라이더 막대를 사용하여 사용할 스트림 수를 선택합니다.

최대 10개의 스트림을 사용할 수 있습니다. 각 스트림에는 별도의 프로세서 코어가 필요합니다. 이 기능을 통해 멀티 프로세서를 활용하여 백업 성능을 높일 수 있습니다.
 - 7 다음을 클릭합니다.

- 8 스케줄 페이지에서 백업 작업에 대한 백업 스케줄과 시작 시간을 선택한 후 다음을 클릭합니다.
스케줄을 구성하는 방법에 대한 자세한 내용은 “백업 스케줄 지정”(111페이지) 섹션을 참조하십시오.
- 9 보존 정책 페이지에서 백업 유지 기간에 대한 옵션을 선택한 후 다음을 클릭합니다.
보존 정책을 구성하는 방법에 대한 자세한 내용은 “보존 정책 설정”(111페이지) 섹션을 참조하십시오.
- 10 이름 페이지에서 백업 작업 이름을 입력한 후 다음을 클릭합니다.
- 11 완료 준비 페이지에서 백업 작업에 대한 요약 정보를 검토한 후 마침을 클릭합니다.
- 12 백업 작업이 성공적으로 생성되었다는 메시지가 나타나면 확인을 클릭합니다.

Microsoft Exchange Server의 백업 복구

Microsoft Exchange Server에서 백업을 실행한 후 이러한 백업을 원래 위치나 대체 위치로 복구할 수 있습니다.

주의 타겟 Microsoft Exchange Server에는 백업이 수행된 Microsoft Exchange Server와 동일한 Exchange 버전 및 서비스 팩이 있어야 합니다. 그렇지 않을 경우 복구가 실패합니다.

절차

- 1 vSphere Web Client에서 복구 탭을 선택합니다.
- 2 복구할 백업이 속한 클라이언트를 클릭합니다.
- 3 복구할 백업을 클릭합니다.
- 4 백업의 전체 콘텐츠를 복구하려면 **Exchange 정보 저장소 확인란**을 선택합니다.
- 5 모든 타겟을 선택한 후 복구 버튼을 클릭합니다.

참고 클라이언트가 로컬 시스템 계정으로 실행 중인 경우 사용자는 Exchange 관리자 자격 증명을 제공해야 합니다. 로컬 시스템 계정으로 실행 중이지 않은 경우에는 자격 증명 필요하지 않습니다.

- 6 복구 옵션 선택 페이지에서는 원래 위치로 복구 옵션이 기본 설정이며 수정할 수 없습니다.
- 7 (선택 사항) GLR의 경우 복구 옵션 선택 페이지에서 다음을 수행합니다.
 - **Restore to Original Location:** RDB를 생성할 다른 클라이언트를 선택하거나 다른 메일박스로 복구하려는 경우 이 확인란의 선택을 취소합니다.
 - **대상 클라이언트:** 백업에서 RDB가 생성되고 마운트될 Exchange Server입니다. 이 클라이언트는 VDP Exchange GLR 플러그인이 설치된 Exchange Server여야 합니다.
 - **대상 메일박스:** 선택한 메일박스를 복구할 메일박스의 e-메일 주소로 설정합니다.
- 8 고급 옵션을 지정하려면 고급 옵션 옆의 화살표를 클릭하여 목록을 확장합니다.
다음 옵션을 지정합니다.

- **Allow database overwrite:** 복구 작업에 포함된 것과 이름이 같은 기존 데이터베이스를 덮어씹습니다. 이 옵션을 선택하면 Exchange Server 내부의 "파일 복구 허용" 플래그가 수정됩니다.
- **Restore into RSG/RDB:** RSG(Restore Storage Group)는 Exchange Server 2007에서 사용되고 RDB(Recovery Database)는 Exchange Server 2010 및 Exchange Server 2013에서 사용됩니다. RSG/RDB는 운영 데이터베이스 대신 RSG/RDB로 복구하는 데 사용됩니다. **RSG/RDB로 복구**를 선택한 경우 다음 옵션을 구성할 수 있습니다.
 - **Overwrite existing RSG/RDB:** 기존 RSG/RDB를 덮어씹습니다. 이 옵션은 주의해서 사용하십시오.
 - **RSG/RDB name:** 복구에 사용되는 RSG/RDB 이름입니다. 지정된 이름의 RSG/RDB가 아직 존재하지 않으면 새로 생성됩니다. 지정된 이름의 RSG/RDB가 이미 존재하는 경우에는 **기존 RSG/RDB 덮어쓰기** 옵션을 사용하여 덮어씹습니다.
 - **RSG/RDB database path:** RSG/RDB 데이터베이스 파일이 복구될 경로입니다(예: C:\myrdb). 이 필드는 선택적 필드입니다. 이 필드가 비어 있으면 기본 위치가 사용됩니다.

- **RSG/RDB log path:** RSG/RDB 로그 파일이 복구될 경로입니다(예: C:\myrdb). 이 필드는 선택적 필드입니다. 이 필드가 비어 있으면 기본 위치가 사용됩니다.
 - **트랜잭션 로그 재생 안 함** 확인란을 선택하거나 선택 취소하여 트랜잭션 로그를 복구하지만 재생하지 않을지 여부를 선택합니다. 이 옵션을 선택하면 데이터베이스를 마운트하기 전에 추가 트랜잭션 로그를 수동으로 복사할 수 있습니다.
 - 복구 중에 로그 파일에서 충돌이 발생하는 경우 **로그 경로 이동** 입력란을 사용하여 복구 전에 기존 로그 파일을 이동할 위치를 지정합니다. 로그 파일 경로를 지정하지 않았는데 트랜잭션 로그에 차이가 있는 경우 복구 프로세스에서 현재 트랜잭션 로그가 자동으로 logs_time_date라는 하위 폴더로 이동합니다. 시간 및 날짜 값은 복구 시간 및 날짜입니다. 이 하위 폴더는 데이터베이스 또는 스토리지 그룹의 트랜잭션 로그 폴더에 있습니다. 이러한 로그를 사용하여 필요한 경우 복구 작업을 분석하거나 오류가 발생했던 지점까지 해당 로그를 적용할 수 있습니다.
 - Exchange DAG 클러스터 구성의 복구 옵션에 대해서는 **“DAG 또는 클러스터에서 복제 일시 중단”**(174 페이지) 섹션을 참조하십시오.
- 9 **완료 준비** 페이지에서 복구 요청을 검토하고 **마침**을 클릭합니다.
 - 10 복구가 시작되었다는 메시지가 표시되면 **확인**을 클릭합니다.
 - 11 **최근 작업** 창에서 복구 진행률을 모니터링합니다.

DAG 또는 클러스터에서 복제 일시 중단

복구 중에 **복제 자동화 일시 중단** 확인란을 선택하는 경우 VDP 어플라이언스는 복구 중에 액티브 데이터베이스 또는 스토리지 그룹에서 패시브 데이터베이스 또는 스토리지 그룹으로의 복제를 자동으로 일시 중단합니다.

또한 복구 수행 전에 Exchange 관리 셸을 사용하여 패시브 데이터베이스 또는 스토리지 그룹으로의 복제를 수동으로 일시 중단할 수도 있습니다.

절차

Exchange Server 2013 또는 2010에서 DAG의 서버에서 Exchange 관리 셸에 다음 명령을 입력하여 복구 전 패시브 데이터베이스 또는 스토리지 그룹으로의 복제를 수동으로 일시 중단합니다.

```
suspend-MailboxDatabaseCopy -Identity database\I
```

여기서 *database*는 데이터베이스의 이름이고 *server*는 패시브 복제본이 있는 DAG 서버의 이름입니다.

클라이언트 작업 모니터링

클라이언트 로그를 수집하고 분석하여 모든 클라이언트 작업에 대한 작업 및 이벤트를 모니터링할 수 있습니다. 클라이언트 로그는 Microsoft 애플리케이션(MSApp) 관련 로그입니다. 취합된 클라이언트 로그에는, 통과되었지만 예외가 발생했거나 실패한 복제, 백업, 복구 또는 ABV(Automatic Backup Verification) 작업이 모두 포함됩니다. 자세한 내용은 **“VDP 로그 또는 진단 정보 수집”**(38페이지) 섹션을 참조하십시오.

Exchange Server 플러그인 제거

Exchange Server 플러그인을 제거하려면 **프로그램 및 기능**을 사용하십시오.

Exchange Server GLR 플러그인은 Exchange Server 플러그인을 제거하면 자동으로 제거됩니다. Exchange Server GLR 플러그인을 제거한 후 컴퓨터를 다시 시작해야 합니다.

Microsoft Exchange Server에 대한 세밀한 레벨의 복구

VDP Plug-in for Exchange GLR(Granular Level Restore)은 타겟 서버에 임시 가상 드라이브를 마운트하고 하나의 Exchange Server 데이터베이스 또는 스토리지 그룹을 백업에서 가상 드라이브의 RDB(Recovery Database) 또는 RSG(Recovery Storage Group)로 복구합니다.

다음을 참조하십시오.

- VDP의 GLR은 메일박스 레벨에서만 복구를 지원합니다. 개별 항목 레벨에서는 GLR이 지원되지 않습니다.
- 백업은 VMware VDP Exchange Server 플러그인을 사용한 전체 백업이어야 합니다.
- 공용 폴더 데이터베이스를 포함하는 백업에 대해 GLR 작업을 수행할 수 있지만, GLR을 사용하여 공용 폴더 데이터베이스 자체에서 찾거나 복구할 수는 없습니다.

GLR 시스템 요구 사항

VDP Plug-in for Exchange Server GLR을 사용한 GLR 프로세스를 수행하려면 백업 및 복구에 필요한 기본 요구 사항에 컴퓨터 하드웨어 및 리소스 요구 사항이 추가됩니다. 표 17-27에는 VDP Plug-in for Exchange Server GLR에 대한 시스템 요구 사항이 정리되어 있습니다.

표 17-27. GLR 시스템 요구 사항

요구 사항	최소
메모리(RAM)	VDP Plug-in for Exchange Server GLR에는 추가 메모리(RAM)가 필요합니다. 최소 RAM 요구 사항은 1GB입니다. 필요한 추가 메모리 또는 총 메모리는 기존 메모리와 현재 시스템 성능에 따라 달라집니다. <ul style="list-style-type: none"> ■ VDP Plug-in for Exchange Server VSS의 일반 작업을 수행하는 리소스가 이미 제한적이고 속도가 느린 경우 VDP Plug-in for Exchange Server GLR 작업을 지원하려면 상당히 많은 메모리를 추가해야 합니다. ■ VDP Plug-in for Exchange Server VSS의 일반 작업을 수행하는 성능이 현재 적정한 경우 VDP Plug-in for Exchange Server GLR 작업을 지원하는 데 추가 메모리가 필요하지 않을 수 있습니다.
하드 드라이브 공간	Exchange Server 데이터베이스 및 로그 파일에 대한 쓰기를 보존하는 디스크 스테이징 영역을 제공하려면 추가 디스크 공간이 필요합니다.

참고 또한 Microsoft 웹 사이트에서 최신 MAPI 클라이언트 라이브러리 및 CDO 1.2.1을 다운로드하고 라이브러리와 CDO를 Exchange Server GLR 플러그인이 있는 각 Exchange Server에 설치해야 합니다. 최신 버전이 없으면 일부 기능이 작동하지 않을 수 있습니다.

멀티 스트리밍 요구 사항

멀티 스트리밍을 사용할 경우 VDP Plug-in for Exchange Server VSS의 기본 요구 사항에 컴퓨터 하드웨어 및 리소스 요구 사항이 추가됩니다. 이와 더불어, 멀티 스트리밍을 위한 여러 구성 권장 사항이 있습니다.

표 17-28에는 멀티 스트리밍을 위한 하드웨어 및 소프트웨어 권장 사항이 나와 있습니다.

표 17-28. 멀티 스트리밍 요구 사항

하드웨어 및 소프트웨어	권장 사항
CPU	스트림당 하나 이상의 프로세서 코어
메모리(RAM)	48GB 이상
하드 디스크	운영 체제/Exchange Server 설치용 디스크 드라이브 1개 각 Exchange Server 데이터베이스용 디스크 드라이브 또는 RAID 드라이브 그룹 1~2개 속도가 7200RPM 이상인 디스크 드라이브
네트워크 어댑터	1GB
운영 체제	Windows Server 2008 SP2 이상

멀티 스트리밍 Exchange Server 구성 요구 사항

VDP는 멀티 스트리밍을 사용한 백업 중에 상당히 많은 CPU를 사용합니다. 활성 Exchange Server에서의 이러한 추가적인 CPU 사용은 성능에 영향을 주고 최종 사용자에게도 영향을 줍니다.

Exchange Server 환경이 다음과 같은 멀티 스트리밍 요구 사항을 충족하는지 확인하십시오.

- 각 데이터베이스를 별도의 물리적 디스크에 배치합니다. 가능한 경우 각 데이터베이스에서 하나의 디스크에 데이터베이스 파일을 배치하고 또 다른 별도의 디스크에 트랜잭션 로그를 배치합니다.
- 각 데이터베이스 또는 스토리지 그룹의 크기가 거의 동일한 경우에 최상의 결과가 나옵니다.

백업에 대해 멀티 스트리밍 옵션을 지정하는 경우 백업 세트의 각 디스크에 대해 최대 하나의 백업 스트림을 지정하십시오. 예를 들면 다음과 같습니다.

- 각 데이터베이스가 고유한 디스크에 있는 데이터베이스 두 개를 백업하는 경우 최대 스트림 수로 2를 지정합니다.
- 두 개의 디스크에 각 데이터베이스와 로그가 있는 데이터베이스 두 개를 백업하는 경우(총 네 개의 디스크) 최대 스트림 수로 4를 지정합니다.

VSS 요구 사항

VDP Plug-in for Exchange Server VSS는 Microsoft VSS(Volume Shadow Copy Service) 기술을 사용하여 백업을 수행합니다. VSS는 시스템의 애플리케이션이 볼륨에 데이터를 쓰는 동안에도 계속 볼륨을 백업할 수 있게 해주는 프레임워크입니다.

지원되는 VSS Provider 및 Writer

Exchange Server VSS 플러그인은 Microsoft 소프트웨어 새도우 복제본 공급자 및 다음과 같은 VSS Writer를 사용합니다.

- Microsoft Exchange Server Store VSS Writer
- Microsoft Exchange Server Replication VSS Writer

Exchange Server VSS 플러그인은 하드웨어 공급자를 지원하지 않습니다.

VSS 스냅샷 볼륨 요구 사항

Microsoft VSS 프레임워크는 VSS 스냅샷 하나당 64개의 볼륨을 지원합니다. 따라서 데이터 세트를 생성하거나 필요 시 백업을 수행할 때 포함하는 볼륨이 64개를 초과하면 안 됩니다. 스냅샷에서 볼륨을 64개 이상 포함하는 경우 백업이 실패하고 이벤트 로그에 다음과 같은 오류가 표시됩니다.

VSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHED.

또한 VSS 프레임워크는 새도우 복제본의 수를 볼륨당 64개로 제한합니다. 볼륨의 새도우 복제본 수가 64개를 초과하는 경우에는 백업이 실패하고 이벤트 로그에 다음과 같은 오류가 표시됩니다.

VSS_E_MAXIMUM_NUMBER_OF_SNAPSHOTS_REACHED.

GLR을 수행하기 전에 GLR 로그 파일 활성화

GLR 로그 파일을 사용하여 세밀한 레벨의 복구를 추적 및 디버깅할 수 있습니다. 다음 단계를 수행하여 GLR 로그 파일을 활성화하십시오.

- 1 텍스트 편집기를 사용하여 C:\Program Files\avp\var 폴더에 명령 파일을 생성합니다. 여기서 C:\Program Files\avp는 설치 폴더입니다.
- 2 명령 파일을 저장하고 닫습니다.

표 17-29에는 GLR을 추적 및 디버깅할 수 있게 해 주는 VDP 로그 파일이 나와 있습니다.

표 17-29. VDP 로그 파일

로그 파일	내용	디버깅 활성화 플래그	플래그에 대한 명령 파일
Axionfs.log	AvFS 파일 시스템 호출에 대한 추적 및 디버깅 정보	--debug x19=327680	axionfs.cmd
avmapi.log	MAPI 호출에 대한 추적 및 디버깅 정보	--debug	avmapi.cmd

표 17-29. VDP 로그 파일

avexglr_plugin.log	RDB 및 RSG 생성, 마운트, 찾아보기 및 복구에 대한 추적 및 디버깅 정보	--debug	avexchglr.cmd
Aveexchglrsvc.log	RDB 및 RSG 생성, 마운트, 찾아보기 및 복구에 대한 추적 및 디버깅 정보	--debug	aveexchglrsvc.cmd
ps_exec.log	Exchange Server 클라이언트의 PowerShell 명령 실행에 대한 추적 및 디버깅 정보	--debug	ps_exec.cmd

Exchange Server 데이터베이스 백업

Exchange Server 데이터베이스를 백업하는 지침은 [“애플리케이션 백업”](#)(162페이지) 섹션을 참조하십시오.

개별 메일박스 복구

참고 세밀한 레벨의 복구를 수행하기 전에 타겟 Exchange Server(2010 또는 2013)에서 모든 RDB를 수동으로 삭제해야 합니다. GLR 프로세스는 타겟 Exchange Server 2007 서버에서 RSG를 자동으로 삭제합니다.

개별 메일박스를 백업한 후 데이터베이스에서 개별 메일박스를 찾아서 추출하여 복구할 수 있습니다. 선택한 항목은 VDP 어플라이언스에서 원래 메일박스의 복구된 항목 폴더로 복구됩니다. 그런 다음 유지할 항목을 찾아 선택할 수 있습니다. 세밀한 레벨에서 백업을 복구하는 방법에 대한 지침은 [“Microsoft Exchange Server의 백업 복구”](#)(173페이지) 섹션을 참조하십시오.

복구가 완료된 후에는 가상 드라이브가 자동으로 마운트 해제되고 GLR의 타겟 서버에서 RDB 또는 RSG가 삭제됩니다. Exchange Server 2007은 자동으로 삭제됩니다. Exchange Servers 2010 및 2013의 경우에는 GLR을 수행하기 전에 자동으로 삭제해야 합니다.

절차

- 1 vSphere Web Client에서 **복구** 탭을 선택합니다.
 - 2 복구할 백업을 선택하고 **복구** 아이콘을 클릭하여 백업 복구 마법사를 시작합니다.
백업 선택 페이지가 나타납니다.
 - 3 복구할 백업이 속한 클라이언트를 클릭합니다.
 - 4 복구할 백업을 클릭합니다.
 - 5 계층의 임의의 레벨에서 복구하도록 선택합니다. 복구 타겟이 메일박스 레벨에 있으면 복구는 GLR로 간주됩니다.
 - Microsoft Exchange Server 2007의 경우 백업 계층은 다음과 같습니다.
Exchange Server 이름 -> 백업 날짜 -> Exchange 정보 저장소 -> 스토리지 그룹 -> 데이터베이스 -> 사서함.
 - Microsoft Exchange Server 2010 또는 2013의 경우 백업 계층은 다음과 같습니다.
Exchange Server 이름 -> 백업 날짜 -> Exchange 정보 저장소 -> 데이터베이스 -> 사서함.
 - 6 모든 타겟을 선택했다면 **복구** 버튼을 클릭합니다.
- 참고** 클라이언트가 로컬 시스템 계정으로 실행 중인 경우 사용자는 Exchange 관리자 자격 증명을 제공해야 합니다. 클라이언트가 로컬 시스템 계정으로 실행 중이지 않은 경우에는 자격 증명 필요하지 않습니다.
- 7 완료 준비 페이지에서 복구 요청을 검토한 다음 **마침**을 클릭합니다.
 - 8 복구가 성공적으로 시작되었음을 알리는 메시지가 표시되면 **확인**을 클릭합니다.
 - 9 최종 작업 창에서 복구 진행률을 모니터링합니다.

Microsoft SharePoint Server 백업 및 복구

VDP는 Microsoft SharePoint Server의 백업 및 복구를 지원합니다. 현재 판별로 하나의 SharePoint Server 시스템만 지원됩니다.

참고 SharePoint Server 구성 또는 관리자의 데이터베이스만 복구하면 SharePoint Server 애플리케이션이 손상될 수 있습니다. 따라서 콘텐츠 데이터베이스만 복구하는 경우 외에는 전체 백업을 복구해야 합니다.

하드웨어 요구 사항

표 17-30에는 Microsoft SharePoint Server에 대한 하드웨어 요구 사항이 나와 있습니다.

표 17-30. Microsoft SharePoint Server에 대한 하드웨어 요구 사항

요구 사항	최소
메모리(RAM)	2GB
파일 시스템	NTFS

지원되는 Microsoft SharePoint Server

VDP는 다음 버전의 Microsoft SharePoint Server를 지원합니다.

- SharePoint Server 2007 SP2 이상
 - Windows Server 2008 R2
 - Windows Server 2008
- SharePoint Server 2010, 2010 SP1
 - Windows Server 2008 SP2
 - Windows Server 2008 R2
- SharePoint Server 2013
 - Windows Server 2012
 - Windows Server 2008 R2 SP1 이상
- SharePoint Server 2013 SP1:
 - Windows Server 2012 R2

VDP for SharePoint Server Client 설치

팜의 각 SharePoint Server에 VDP 클라이언트 플러그인을 설치합니다. SharePoint 팜은 SharePoint Server의 모음으로, 상호 연동되어 단일 사이트를 지원하는 일련의 기본적인 SharePoint Server 서비스를 제공합니다.

다음 그림은 소규모, 중간 규모 및 대규모 팜에 대한 SharePoint 토폴로지를 보여 줍니다.

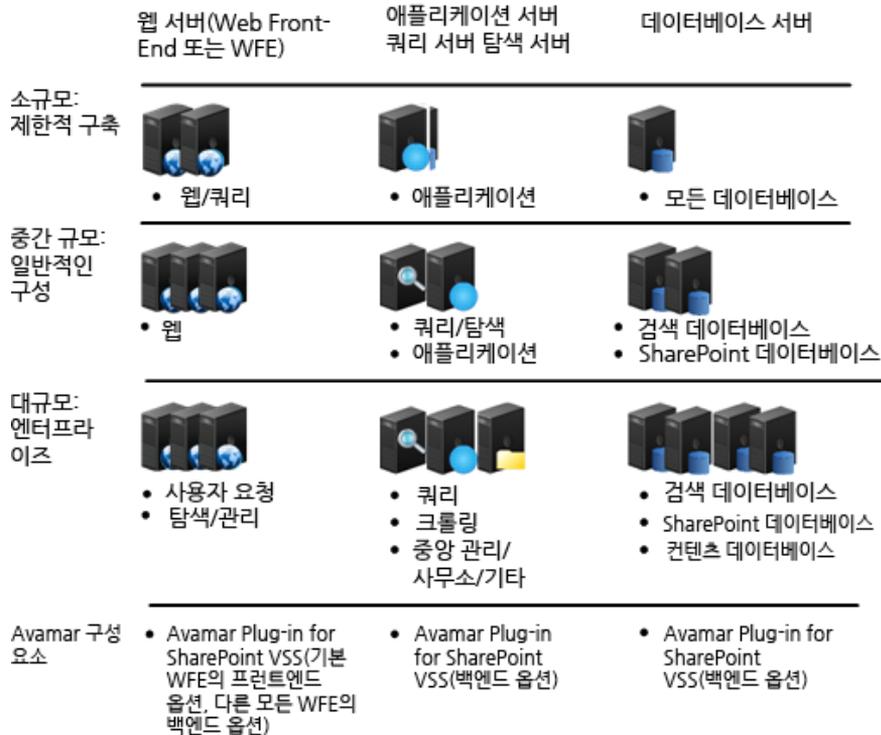


그림 17-10. SharePoint 토폴로지

제한 사항

SharePoint VSS Writer는 SharePoint Server 팜 관리자 계정으로 실행해야 합니다.

사전 요구 사항

- VDP 어플라이언스가 “VDP 설치 및 구성”(21페이지)의 설명에 따라 설치 및 구성되어 있어야 합니다.
- 각 SharePoint Server에 대한 로컬 관리자 권한이 있어야 합니다.

절차

- 1 각 SharePoint Server 클라이언트에서 vSphere Web Client에 액세스합니다.
https://<IP_address_vCenter_Server>:9443/vsphere-client/
- 2 자격 증명 페이지에 vCenter 관리 사용자 이름과 암호를 입력하고 로그인을 클릭합니다.
- 3 vSphere Web Client에서 **VDP**를 선택합니다.
- 4 **VDP 시작** 페이지에서 VDP 어플라이언스를 선택하고 연결을 클릭합니다.
- 5 구성 탭을 클릭합니다.
- 6 클라이언트 다운로드에서 **Microsoft SharePoint Server 64비트**를 클릭합니다. 사용 중인 브라우저에 따라 .msi 파일을 저장하거나 실행할 수 있습니다.
VMware VDP for SharePoint Server 설치 마법사가 시작됩니다.
- 7 다음을 클릭합니다.

- 8 **최종 사용자 사용권 계약** 페이지에서 라이선스를 읽고 동의하는 경우 **동의함**과 **다음**을 차례로 클릭합니다.
 - 9 **어플라이언스 등록 정보** 페이지에서 SharePoint Server를 백업할 VDP 어플라이언스의 이름 또는 IP 주소를 입력하고 **다음**을 클릭합니다.
 - 10 **VMware VDP for SharePoint Server 설치 준비** 페이지에서 **설치**를 클릭합니다.
 - 11 설치 중에, 설치하는 서버가 운영 백업 서버(프런트엔드)인지 SharePoint Server 팜의 다른 구성원 서버(백엔드)인지 선택합니다.
- 참고** 프런트엔드 서버는 하나의 팜 서버에만 설치할 수 있으며 웹 프런트엔드 또는 애플리케이션 서버여야 합니다.
- 12 **VMware VDP for SharePoint Server 설치 마법사 완료** 페이지에서 **마침**을 클릭합니다.

Microsoft SharePoint Server 백업 작업 생성

VDP for SharePoint Server Client를 설치한 후 SharePoint 가상 머신 클라이언트를 백업에 사용할 수 있습니다.

- 1 vSphere Web Client에서 **백업** 탭을 클릭합니다.
- 2 **백업** 탭에서 **백업 작업 조치**를 클릭한 다음 **새로 만들기**를 선택하여 **새 백업 작업 생성** 마법사를 시작합니다.
- 3 마법사의 **작업 유형** 페이지에서 **애플리케이션**을 선택합니다. 이 옵션은 가상 머신에서 실행 중인 SharePoint Server 애플리케이션을 백업합니다.
- 4 **다음**을 클릭하여 아래 지침을 따릅니다.

애플리케이션 백업

전체 SharePoint Server 애플리케이션 서버만 백업할 수 있습니다. 개별 데이터베이스 백업은 현재 릴리즈에서 지원되지 않습니다.

- 1 **데이터 유형** 페이지에서 **전체 서버**를 선택하고 **다음**을 클릭합니다.
- 2 **백업 소스** 페이지에서 **다음**을 수행합니다.
 - a **Microsoft SharePoint Server** 옆의 화살표를 클릭하여 목록을 확장합니다.
 - b 백업할 SharePoint Server 옆의 확인란을 선택합니다.
 - c **다음**을 클릭합니다.
- 3 **백업 옵션** 페이지에서 필요한 경우 아래로 스크롤하여 **프런트엔드로 설치한 SharePoint Server**를 찾습니다.
 - a **팜 관리자 자격 증명** 섹션에서 관리자 **로그인 ID** 및 **로그인 암호**를 입력합니다
 - b 백업하는 동안 다중 스레드의 실행을 허용하려면 **멀티 스트림 백업 활성화** 옵션을 선택합니다. 슬라이더 막대로 사용할 스트림 수를 선택한 다음 **그룹화 기준** 메뉴에서 **데이터베이스** 또는 **볼륨**을 선택합니다.
 - c **다음**을 클릭합니다.
- 4 **스케줄** 페이지에서 백업 작업에 대한 백업 스케줄과 시작 시간을 선택한 후 **다음**을 클릭합니다.
- 5 **보존 정책** 페이지에서 백업 보존 기간에 대한 옵션을 선택한 후 **다음**을 클릭합니다.
- 6 **이름** 페이지에서 백업 작업 이름을 입력한 후 **다음**을 클릭합니다.
- 7 **완료 준비** 페이지에서 선택 항목을 확인합니다.

설정이 맞으면 **마침**을 클릭합니다. 설정이 정확하지 않으면 **뒤로** 버튼을 클릭하여 마법사의 해당 페이지로 돌아갑니다.

Microsoft SharePoint Server의 백업 복구

SharePoint Server에서 백업을 실행한 후 이러한 백업을 원래 위치나 대체 위치로 복구할 수 있습니다.

- 1 vSphere Web Client에서 **복구** 탭을 클릭합니다.
- 2 복구할 백업을 선택하고 **복구** 아이콘을 클릭합니다.
- 3 **백업 선택** 페이지에서 복구할 백업 작업을 선택합니다. SharePoint Server는 여러 개를 선택할 수 있지만 복구 시점은 각 서버별로 하나만 선택할 수 있습니다. 복구에 사용할 백업 작업을 선택(또는 확인)하고 다음을 클릭합니다.
- 4 **복구 옵션 선택** 페이지에서 다음을 수행합니다.
 - a 다음 단계 중 하나를 수행합니다.
 - 백업을 원래 위치로 복구하려면 **원래 위치로 복구** 옵션을 선택된 상태(기본 설정)로 둡니다.
 - 백업을 대체 위치로 복구하려면 **원래 위치로 복구** 옵션을 지웁니다. **선택**을 클릭하여 대상을 선택하고 백업을 복구할 대상 위치에 대한 전체 Windows 경로를 입력합니다.
 - b 고급 옵션을 지정하려면 **고급 옵션** 옆의 화살표를 클릭하여 목록을 확장합니다.
 - **로그인 ID**: SharePoint Server 관리자의 로그인 ID를 입력합니다. 형식은 **DOMAIN\user**입니다.
 - **로그인 암호**: 대상 클라이언트에 로그인할 때 사용되는 팜 관리자의 암호를 입력합니다.
 - **애플리케이션 풀**(선택 사항): SharePoint Server 2013의 경우 검색 서비스 애플리케이션을 복구할 기존 애플리케이션 풀의 이름을 입력합니다.
 - **암호화 방식**: 목록에서 암호화 방식을 선택합니다.
 - **고급 옵션**(지원 전용): 이 확인란에는 아무것도 입력하지 마십시오. EMC 지원 전용입니다.
 - c 다음을 클릭합니다.
- 5 **완료 준비** 페이지에서 선택 항목을 확인합니다. 모두 정확하면 **마침**을 클릭합니다. 설정이 정확하지 않으면 뒤로 버튼을 클릭하여 올바른 구성을 생성합니다.
- 6 복구가 시작되었다는 메시지가 표시되면 **확인**을 클릭합니다.
- 7 **최근 작업** 창에서 복구 진행률을 모니터링합니다.

클라이언트 작업 모니터링

클라이언트 로그를 수집하고 분석하여 모든 클라이언트 작업에 대한 작업 및 이벤트를 모니터링할 수 있습니다. 클라이언트 로그는 Microsoft 애플리케이션(MSApp) 관련 로그입니다. 취합된 클라이언트 로그에는, 통과되었지만 예외가 발생했거나 실패한 복제, 백업, 복구 또는 ABV(Automatic Backup Verification) 작업이 모두 포함됩니다. 자세한 내용은 [“VDP 로그 또는 진단 정보 수집”](#)(38페이지) 섹션을 참조하십시오.

VDP Plug-in for SharePoint Server 제거

Windows Server 2008 또는 Windows Server 2012 설치 시스템에서 VDP Plug-in for SharePoint Server를 제거하려면 **프로그램 및 기능**을 사용하십시오.

VDP 재해 복구

이 장에서 다루는 내용은 다음과 같습니다.

- “[기본 재해 복구](#)”(184페이지)

기본 재해 복구

재해가 발생할 경우 다른 방법을 사용하여 데이터 또는 VDP 어플라이언스를 복구할 수 있습니다.

- VDP 체크포인트 사용

VDP는 백업을 저장 및 관리할 수 있는 강력한 기능을 제공합니다. 장애 발생 시 가장 먼저 알려진 검증된 체크포인트로 롤백을 수행해야 합니다(“[어플라이언스 롤백](#)”(41페이지) 참조).

- Data Domain 체크포인트 복제 사용

환경에서 Data domain 통합을 사용하는 경우 체크포인트 복제 기능을 사용하여 장애가 발생한 VDP 어플라이언스를 복구할 수 있습니다. 체크포인트 복제 기능은 Data Domain에서 VDP 체크포인트의 백업을 생성합니다. 이러한 체크포인트를 사용하여 장애 발생 시 VDP 어플라이언스를 복구할 수 있습니다. 자세한 내용은 “[Data Domain 시스템에서 Avamar 체크포인트 백업 복구](#)”(90페이지)을 참조하십시오.

- VDP 스토리지 분리 및 다시 연결

어플라이언스 OS 디스크에 장애 또는 손상이 발생할 경우 새 VDP를 구축하고 장애가 발생한 VDP의 데이터 디스크를 다시 연결할 수 있습니다. 자세한 내용은 “[스토리지 분리 및 다시 연결](#)”(73페이지)을 참조하십시오.

- 복제 사용

VDP의 복제 기능을 사용하여 재해 발생 시 데이터를 복구할 수 있습니다. 백업을 원격 VDP 어플라이언스로 복제할 수 있습니다. 이렇게 하면 운영 VDP 어플라이언스에 재해가 발생할 경우 보조 VDP 어플라이언스에서 데이터를 복구할 수 있습니다. 자세한 내용은 “[복제](#)”(133페이지)을 참조하십시오.

VDP 포트 사용

표 A-31에는 VDP에서 사용하는 포트가 정리되어 있습니다.

표 A-31. VDP 포트 사용

제품	포트	프로토콜	소스	대상	용도
VDP	7	TCP	VDP	Data Domain 시스템	ECHO 서비스 Data Domain 시스템을 등록하는 데 필요
VDP	21	TCP	VDP	FTP 서버	FTP
VDP	22	TCP	사용자	VDP	디버깅을 위한 SSH(Secure Shell) 액세스
VDP	23	TCP	VDP	내부	내부
VDP	25	TCP	VDP	EMC 고객 지원 본부	SFTP
VDP	53	TCP/UDP	VDP	iDNS 서버	이름 확인에 필요
VDP	67	UDP	DHCP 서버	VDP	DHCP
VDP	68	UDP	VDP	DHCP 서버	DHCP
VDP	69	TCP	내부 스위치	VDP	TFTP
VDP	80	TCP	VDP	vCenter	http(라이선스 등록용)
VDP	88	TCP/UDP	VDP	KDC(Key Distribution Center)	SMTP
VDP	111	TCP/UDP	VDP	vSphere 호스트	RPC 포트 매퍼 기능에 대한 액세스 Data Domain 시스템에 백업이 저장된 경우 필요
VDP	123	TCP/UDP	NTP 시간 서버	VDP	NTP
VDP	161	TCP	Data Domain 시스템	VDP	Data Domain 시스템의 SNMP 객체용 Getter/Setter 포트 Data Domain 시스템에 Avamar 클라이언트 백업을 저장하는 데 필요
VDP	162	TCP/UDP	VDP	SNMP 에이전트	SNMP 트랩
VDP	163	TCP	VDP	Data Domain의 SNMP 서비스	MC SNMP Manager
VDP	389	TCP/UDP	VDP	LDAP	LDAP
VDP	443	TCP	VDP	vCenter 또는 SSO	https
VDP	464	TCP/UDP	VDP	vCenter	Kerberos
VDP	514	UDP	유틸리티 노드 또는 단일 노드 서버	VDP	syslog

표 A-31. VDP 포트 사용

제품	포트	프로토콜	소스	대상	용도
VDP	700	TCP	VDP LDAP	Active Directory	Loginmgr 툴
VDP	703	TCP	Avamar 서버 노드	VDP	AKM 서비스
VDP	902	TCP	VDP	VMware ESX 서버 프록시	VMware ESX 서버 프록시 서비스
VDP	2049	TCP/UDP	VDP	Data Domain 시스템의 NFS 데몬	Data Domain 시스템의 NFS 데몬
VDP	2052	TCP/UDP	VDP	Data Domain 시스템의 NFS 마운트 프로세스	Data Domain 시스템의 NFS 마운트 프로세스
VDP	2888	TCP	Avamar Extended Retention 미디어 액세스 노드	VDP	AVDTO Avamar Extended Retention을 지원하는 데 필요
VDP	3008	TCP	VDP	Data Domain 시스템의 액티브 아카이브 서비스	Data Domain 시스템의 액티브 아카이브 서비스
VDP	5480	TCP	VDP	외부 프록시	외부 프록시
VDP	5489	TCP	VDP	Avamar 프록시	프록시 서비스
VDP	5555	TCP	<ul style="list-style-type: none"> ■ Avamar Client Manager를 실행하는 유틸리티 노드 ■ PostgreSQL 관리자 클라이언트 컴퓨터 	VDP	PostgreSQL 관리자 서버
VDP	5568	TCP	Avamar Extended Retention 미디어 액세스 노드	VDP	PostgreSQL
VDP	5671	TCP	<ul style="list-style-type: none"> ■ 로컬 호스트 ■ 기타 Avamar 유틸리티 노드 ■ Avamar Extended Retention 컴퓨터 ■ EMC Backup and Recovery Manager 컴퓨터 	VDP	RabbitMQ
VDP	6667	TCP	Avamar Extended Retention 미디어 액세스 노드	VDP	아카이브 서비스 이벤트
VDP	7000	TCP	Avamar Extended Retention 미디어 액세스 노드	VDP	Apache Tomcat
VDP	7443	TCP	Avamar Extended Retention 미디어 액세스 노드	VDP	Apache Tomcat
VDP	7444	TCP	VDP	VMware vCenter	VMware vCenter 통신 포트
VDP	7778	TCP	Avamar Administrator 관리 콘솔	VDP	RMI

표 A-31. VDP 포트 사용

제품	포트	프로토콜	소스	대상	용도
VDP	7779	TCP	Avamar Administrator 관리 콘솔	VDP	RMI
VDP	7780	TCP	Avamar Administrator 관리 콘솔	VDP	RMI
VDP	7781	TCP	Avamar Administrator 관리 콘솔	VDP	RMI
VDP	7937 - 9936	TCP/UDP	VDP	NetWorker Server	NetWorker 서비스
VDP	8080	TCP	VDP	NetWorker Server	NetWorker 서버용 통신 포트
VDP	8105	TCP	클라이언트 컴퓨터	VDP	Apache Tomcat
VDP	8109	TCP	클라이언트 컴퓨터	VDP	Apache Tomcat
VDP	8181	TCP	클라이언트 컴퓨터	VDP	HTTP
VDP	8444	TCP	웹 브라우저 클라이언트	VDP	HTTPS
VDP	8505	TCP	유틸리티 노드 또는 단일 노드 서버	VDP	Apache Tomcat
VDP	8509	TCP	유틸리티 노드 또는 단일 노드 서버	VDP	Apache Tomcat AJP 커넥터
VDP	8543	TCP	vSphere Web Client	VDP	Tomcat용 리디렉션
VDP	8580	TCP	vCenter	VDP	VDP Downloader
VDP	9443	TCP	vCenter	VDP	VDP 웹 서비스
VDP	19000	TCP/UDP	Avamar 서버 노드	VDP	GSAN
VDP	19500	TCP/UDP	Avamar 서버 노드	VDP	GSAN
VDP	20000	TCP/UDP	Avamar 서버 노드	VDP	GSAN
VDP	20500	TCP/UDP	Avamar 서버 노드	VDP	GSAN
VDP	25000	TCP/UDP	Avamar 서버 노드	VDP	GSAN
VDP	25500	TCP/UDP	Avamar 서버 노드	VDP	GSAN
VDP	26000	TCP/UDP	Avamar 서버 노드	VDP	GSAN
VDP	26500	TCP/UDP	Avamar 서버 노드	VDP	GSAN
VDP	27000	TCP	VDP	vCenter	라이선스 통신
참고: VDP에서는 라이선스용으로 포트 27000을 열어 두어야 합니다. vCenter 통신에는 포트 27000이 필요하지 않습니다.					
VDP	27500	TCP	Avamar 서버 노드 또는 Replicator 소스 노드	VDP	Avamar 서버
VDP	28001	TCP	클라이언트 컴퓨터, VMWare 프록시	VDP	Avamar server CLI, MCS
VDP	28002~28011	TCP	Avamar Extended Retention 미디어 액세스 노드	VDP	Avamar Extended Retention 지원
VDP	28009	TCP	VMware 프록시	VDP	avagent
VDP	29000	TCP	클라이언트 컴퓨터	VDP	Avamar 서버 SSL
VDP	30001	TCP	클라이언트 컴퓨터 VMWare 프록시	VDP	MCS

표 A-31. VDP 포트 사용

제품	포트	프로토콜	소스	대상	용도
VDP	30002	TCP	VDP	클라이언트 컴퓨터	클라이언트 또는 avagent 연결에 필요
VDP	30003	TCP	클라이언트 컴퓨터	VDP	MCS
VDP	30102~30109	TCP	VMware 프록시	VDP	avagent
VDP	61617	TCP	Avamar Extended Retention 미디어 액세스 노드	VDP	Apache ActiveMQ SSL
VDP	61619	TCP	VDP	EMC Backup and Recovery Manager를 실행하는 클라이언트	EMC Backup and Recovery Manager와의 통신을 허용하는데 필요

필요한 최소 vCenter 사용자 계정 권한

vSphere Web Client를 사용하여 VDP 사용자 또는 SSO admin 사용자를 구성하려면 “사용자 계정 구성”(24페이지) 섹션을 참조하십시오. 보안 수준이 높은 환경에서는 VDP 어플라이언스를 구성 및 관리하는 데 필요한 vCenter 사용자 계정 권한을 다음 범주로 제한할 수 있습니다.

경보

- 생성
- 수정

데이터 저장소

- 공간 할당
- 데이터 저장소 찾아보기
- 데이터 저장소 구성(VSAN 지원용)
- 하위 레벨(low level) 파일 작업
- 데이터 저장소 이동
- 데이터 저장소 제거
- 파일 제거
- 데이터 저장소 이름 변경

확장

- 확장 등록
- 확장 업데이트

폴더

- 폴더 생성

글로벌

- 작업 취소
- 방법 비활성화
- 방법 활성화
- 라이선스
- 이벤트 기록
- 사용자 지정 특성 관리
- 설정

네트워크

- 네트워크 할당
- 구성

리소스

- 리소스 풀에 가상 머신 할당

세션

- 세션 검증

작업

- 작업 생성
- 작업 업데이트

가상 머신 > 구성

- 기존 디스크 추가
- 새 디스크 추가
- 디바이스 추가 또는 제거
- Advanced
- CPU 수 변경
- 리소스 변경
- 디스크 변경 추적
- 디스크 리스(Disk Lease)
- 가상 디스크 확장
- 호스트 USB 디바이스
- 메모리
- 디바이스 설정 수정
- 원시 디바이스
- 경로에서 다시 로드
- 디스크 제거
- 이름 변경
- 게스트 정보 재설정
- 주석 설정
- 설정
- 스왑 파일 교체
- 가상 머신 호환성 업그레이드

가상 머신 > 게스트 작업

- 게스트 작업 수정
- 게스트 작업 프로그램 실행
- 게스트 작업 쿼리

가상 머신 > 상호 작용

- 콘솔 상호 작용
- 디바이스 연결
- VIX API에서 게스트 운영 체제 관리
- 전원 끄기
- 전원 켜기
- 재설정
- VMware Tools 설치

가상 머신 > 인벤토리

- 새로 생성
- 등록
- 제거
- 등록 취소

가상 머신 > 프로비저닝

- 디스크 액세스 허용
- 읽기 전용 디스크 액세스 허용
- 가상 머신 다운로드 허용
- 템플릿으로 표시

가상 머신 > 스냅샷 관리

- 스냅샷 생성
- 스냅샷 제거
- 스냅샷으로 되돌리기

vApp

- 내보내기
- 가져오기
- vApp 애플리케이션 구성

VDP 문제 해결

이 장에서는 다음과 같은 문제 해결 항목을 다룹니다.

- [“VDP 어플라이언스 설치 문제 해결”](#)(194페이지)
- [“VDP 관리 문제 해결”](#)(194페이지)
- [“VDP 라이선스 등록 문제 해결”](#)(202페이지)
- [“VDP 백업 문제 해결”](#)(195페이지)
- [“VDP 복구 문제 해결”](#)(197페이지)
- [“VDP 복제 문제 해결”](#)(199페이지)
- [“VDP 무결성 검사 문제 해결”](#)(199페이지)
- [“자동 백업 검증 문제 해결”](#)(199페이지)
- [“Restore Client\(파일 레벨 복구\) 문제 해결”](#)(200페이지)
- [“VDP 어플라이언스 문제 해결”](#)(202페이지)
- [“VDP Microsoft Exchange Server 문제 해결”](#)(203페이지)
- [“VDP Microsoft SQL Server 문제 해결”](#)(204페이지)
- [“VDP Microsoft SharePoint Server 문제 해결”](#)(205페이지)
- [“스토리지 용량 문제 해결”](#)(205페이지)
- [“VDP 기술 자료 문서 액세스”](#)(207페이지)

VDP 어플라이언스 설치 문제 해결

VDP(vSphere Data Protection) 어플라이언스 설치 문제가 있는 경우 다음과 같이 하십시오.

- 모든 소프트웨어가 최소 소프트웨어 요구 사항을 충족하는지 확인합니다. 자세한 내용은 “[소프트웨어 요구 사항](#)”(22페이지) 섹션을 참조하십시오.
- 하드웨어가 최소 하드웨어 요구 사항을 충족하는지 확인합니다. 자세한 내용은 “[시스템 요구 사항](#)”(23페이지) 섹션을 참조하십시오.
- DNS가 VDP 어플라이언스에 맞게 제대로 구성되어 있는지 확인합니다. 자세한 내용은 “[설치 전 구성](#)”(23페이지) 섹션을 참조하십시오.

설치 관리자 패키지 문제 해결

문제 해결에 사용할 수 있는 업그레이드 관련 로그를 찾으려면 로그 번들에서 avinstaller.log.0 파일을 참조하십시오.

VDP 관리 문제 해결

다음 문제 해결 항목에서는 VDP 관리와 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

VDP 어플라이언스가 응답하지 않습니다. 요청을 다시 시도하십시오.

이전에 VDP에 연결할 수 있었는데 이 메시지가 나타나는 경우 다음을 점검하십시오.

- vCenter Server에 대해 VDP를 검증하는 데 사용하는 사용자 이름 또는 암호가 변경되지 않았는지 확인합니다. 하나의 사용자 계정과 암호만 VDP 검증용으로 사용됩니다. 이 정보는 VDP-Configure 유틸리티를 통해 구성됩니다. 자세한 내용은 “[vCenter Server 등록](#)”(40페이지) 섹션을 참조하십시오.
- 초기 VDP 설치 후 IP 및 DNS 구성에 대한 네트워크 설정이 변경되지 않았는지 확인합니다. 자세한 내용은 “[DNS 구성](#)”(23페이지) 섹션을 참조하십시오.

VDP 플러그인이 응답하지 않음

vCenter UI의 VDP 플러그인에 **VDP 플러그인이 응답하지 않습니다.**라는 메시지가 표시될 경우 그 이유는 대부분 하나 이상의 VDP 어플라이언스 서비스 또는 전체 VDP 어플라이언스가 중단되었기 때문입니다.

다음 단계를 수행하여 이 문제를 해결합니다.

- 1 다음 명령을 실행하여 원격 머신에서 VDP 어플라이언스에 대해 ping을 수행합니다.

```
ping <VDP_appliance_IP_address>
```

출력에 아무런 메시지도 표시되지 않을 경우 VDP 어플라이언스가 중단되었거나 연결 불가능한 상태입니다. 이 경우 VDP 어플라이언스를 관리하는 vCenter Server에 로그인하여 VDP 어플라이언스를 시작하거나, 네트워크 문제를 해결합니다.

- 2 다음 URL을 사용하여 VDP 구성 유틸리티를 엽니다.

```
https://<VDP_appliance_IP_address>:8543/vdp-configure/
```

이 페이지가 올바르게 표시되지 않을 경우 tomcat 애플리케이션 서버가 중지된 것입니다. ssh 클라이언트(putty)를 사용하여 VDP 어플라이언스에 로그인하고 다음 명령을 실행하여 tomcat 서비스를 재시작합니다.

```
emwebapp.sh -restart
```

VDP 백업 문제 해결

다음 문제 해결 항목에서는 백업과 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

백업 작업 데이터를 로드하는 중

이 메시지는 단일 백업 작업에 대해 많은 수의 VM(최대 100개)이 선택된 경우 오랫동안(최대 5분) 나타날 수 있습니다. 또한 이 메시지는 대규모 작업의 잠금/잠금 해제, 새로 고침, 삭제 등의 작업에도 해당될 수 있습니다. 이는 대규모 작업이 선택된 경우 예상되는 동작입니다. 작업이 완료되면 이 메시지는 사라지는데, 이는 최대 5분 정도 소요될 수 있습니다.

{backupjob name} 백업 작업을 생성하는 동안 {client name} 클라이언트를 VDP 어플라이언스에 추가할 수 없음

이 오류는 vApp 컨테이너 또는 vSphere 호스트에 중복된 호스트 이름이 있는 경우에 발생할 수 있습니다. 이 경우 하나의 백업 작업만 추가됩니다. 모든 중복된 클라이언트 이름을 해결하십시오.

다음 항목을 찾을 수 없어 {client name} 클라이언트를 선택하지 못함

이 오류는 백업 작업을 편집하는 동안 백업 대상 VM을 찾을 수 없는 경우 발생할 수 있습니다. 이는 알려진 문제입니다.

단일 vmdk를 다른 데이터 저장소로 마이그레이션하는 경우 VMDK 백업 작업이 실패하고 아무 메시지도 표시되지 않음

개별 VMDK를 한 데이터 저장소에서 다른 데이터 저장소로 마이그레이션하는 동안 VDP는 마이그레이션된 디스크가 포함된 모든 백업 작업을 업데이트합니다. 경우에 따라 VDP는 백업 작업에서 참조하는 디스크가 마이그레이션된 위치를 정확히 파악할 수 없습니다. 이 경우 백업 작업이 업데이트되지 않습니다. 예를 들어 새 데이터 저장소의 디스크 폴더 이름이 원래 데이터 저장소의 폴더와 다르면 이 문제가 발생할 수 있습니다. VDP는 VMDK가 마이그레이션된 위치를 파악할 수 없는 경우 백업 작업이 더 이상 정확하지 않을 수 있다는 vCenter 알림을 전송합니다.

VDP 어플라이언스가 종료되거나 VMDK 마이그레이션 중 emwebapp.sh 서비스가 중지될 경우 VDP가 마이그레이션을 감지할 수 없습니다. 백업 작업은 업데이트되지 않습니다. 백업 작업이 동기화되지 않으면 vCenter에 알림이 전송되지 않습니다. 백업 작업이 VMDK 위치와 동기화되지 않으면 백업 작업이 계속 성공적으로 완료되지만 마이그레이션된 디스크를 더 이상 백업하지 않습니다.

이 문제를 해결하려면 백업 작업을 업데이트합니다. 그런 다음 VDP vCenter 플러그인을 사용하여 마이그레이션된 VMDK를 백업 작업에 다시 추가합니다.

VDP에 데이터 저장소 용량이 충분하지 않은 경우 백업이 실패합니다.

데이터 저장소 용량이 충분하지 않은 경우 예약된 백업이 92% 완료된 상태에서 실패할 수 있습니다. VDP 데이터 저장소가 썸 프로비저닝으로 구성되고 최대 용량에 도달하지 않은 경우 스토리지 리소스를 추가하십시오.

VM에 VMware 내결함성이 활성화된 경우 백업이 실패함

VM에 내결함성이 활성화된 경우 백업이 실패합니다. 이는 예상된 동작입니다. VDP는 내결함성이 활성화된 VM 백업을 지원하지 않습니다.

VM이 다른 클러스터 그룹의 내외부로 이동하는 경우 관련 백업 소스가 유실될 수 있습니다

호스트가 클러스터로 이동될 때 리소스 풀 및 vApp을 보존하는 옵션이 사용된 경우 컨테이너는 복제되지 않고 재생성됩니다. 결과적으로 이름은 같아도 더 이상 동일한 컨테이너는 아닙니다. 호스트가 클러스터 내외부로 이동한 후 컨테이너를 보호하는 모든 백업 작업을 검증하거나 재생성하십시오.

여기치 않은 종료 후 최근의 백업 작업 및 백업이 유실됩니다

언제든지 여기치 않은 종료가 발생하면 VDP 어플라이언스는 마지막으로 검증된 체크포인트로 롤백을 사용합니다. 이는 예상된 동작입니다. 자세한 내용은 “[어플라이언스 롤백](#)”(41페이지) 섹션을 참조하십시오.

백업 작업이 활성화된 경우에는 Storage vMotion 작업이 허용되지 않습니다.

vSphere vMotion은 물리적 서버 간에 실행 중인 가상 머신의 라이브 마이그레이션을 지원하는 기능입니다. 백업 작업이 활성화된 상태에서는 VDP 어플라이언스에서 vMotion 작업을 실행할 수 없습니다. 이는 예상된 동작입니다. vMotion 작업을 수행하기 전에 모든 백업 작업을 완료해야 합니다.

백업이 수행되는 동안 자동화된 vMotion 또는 Storage VMotion이 시작되면 경우에 따라 일부 백업이 실패하거나 스냅샷 삭제가 실패합니다. 이러한 경우 다음 단계를 수행하십시오.

- 1 마이그레이션이 완료될 때까지 기다립니다.
- 2 **백업 > 백업 작업 이름 > 지금 백업**을 사용하여 장애가 발생한 VM의 백업을 수행합니다.

참고 보고서 > 작업 실패 > 작업 재실행을 사용하여 백업을 수행하지 마십시오.

가상 머신, 데이터 저장소, 폴더 또는 데이터 센터 이름에 특정 문자가 사용된 경우 백업이 실패합니다

가상 머신 이름, 데이터 저장소, 폴더 또는 데이터 센터 이름에 특수 문자가 사용된 경우 .vmx 파일이 백업에 포함되지 않습니다. 다음은 .vmx 파일 백업을 차단하는 특수 문자 목록입니다(문자 형식 또는 이스케이프 시퀀스 형식).

- & %26
- + %2B
- / %2F
- = %3D
- ? %3F
- % %25
- \ %5C
- ~ %7E
-] %5D

작업 아이콘을 통해 재실행 옵션을 선택하면 실패한 클라이언트 백업만이 아니라 모든 클라이언트에 대해 백업이 실행됩니다.

백업 작업에서 한 클라이언트 백업이 실패할 경우 **보고서** 탭에서 작업 아이콘을 통해 **작업 재실행** 옵션을 사용하여 실패한 백업을 재실행하면 백업 작업에 포함된 모든 클라이언트에 대한 백업이 실행됩니다.

실패한 클라이언트에 대해서만 백업을 실행하려면 **백업** 탭의 **지금 백업** 아래에서 **기간이 지난 소스만 백업**을 선택하십시오.

지금 백업 작업 시작 오류

용량이 95% 넘게 사용된 VDP 어플라이언스 스토리지 또는 Data Domain 스토리지에 **지금 백업** 작업을 수행할 경우 백업이 불가능하다는 오류 메시지가 vSphere Web Client에 표시됩니다.

VDP 백업 성능 문제 해결

다음 문제 해결 항목에서는 백업 성능과 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

백업 데이터 세트가 저장되어 있는 디스크 하위 시스템의 성능 확인

[https://VDP appliance IP/hostname:8543/vdp-configure](https://VDP_appliance_IP/hostname:8543/vdp-configure) 페이지에 있는 성능 분석 툴을 실행하여 VDP 백업이 저장되어 있는 데이터 저장소가 VDP에 권장되는 최소 읽기/쓰기 값을 충족하는지 확인합니다. 다음 표에는 VDP에 필요한 최소 읽기/쓰기 값이 정리되어 있습니다.

표 C-32. VDP의 최소 읽기/쓰기 값

VDP 어플라이언스 크기	디스크 크기	최소 읽기 값	최소 쓰기 값
0.5TB	256GB	60MB/s	30MB/s
1.0TB	512GB	60MB/s	30MB/s
2.0TB	1024GB	60MB/s	30MB/s
4.0TB	1024GB	80MB/s	40MB/s
6.0TB	1024GB	80MB/s	40MB/s
8.0TB	1024GB	150MB/s	120MB/s

백업에서 NBD 전송 모드가 아닌 핫 애드(HotAdd) 전송 모드를 사용하는지 확인

핫 애드(HotAdd) 전송 방식을 사용하면 백업 및 복구 속도는 높이고 네트워크 라우팅, 방화벽 및 SSL 인증서 문제에 대한 노출을 줄일 수 있습니다. 핫 애드(HotAdd) 전송 방식 대신 NBD(Network Block Device) 전송 방식을 사용하는 경우 백업 성능이 저하됩니다.

NBD 전송 모드를 사용하는 경우 네트워크 병목 현상 확인

핫 애드(Hotadd) 전송 모드를 사용할 수 없는 경우 사용 중인 환경에 네트워크 문제가 없으며 ESXi Server 네트워크 구성에 백업 성능을 저하시킬 수 있는 다른 문제가 없는지 확인해야 합니다.

VDP 복구 문제 해결

다음 문제 해결 항목에서는 복원과 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

복구 탭에 "백업을 로드하는 중" 메시지가 표시되고 로드 속도가 느려집니다

각 백업을 복원 탭에서 로드하는 데 일반적으로 VM 백업당 2초가 소요됩니다. 이는 예상된 동작입니다.

복구 탭의 로드 또는 새로 고침 속도가 느려짐

많은 수의 VM이 있는 경우 복구 탭의 로드 또는 새로 고침 속도가 느려질 수 있습니다. 100개의 VM을 대상으로 테스트 시 최대 4시간 30분이 소요될 수 있습니다.

백업된 가상 머신이 DVS에 연결되고 다른 ESX로 복구될 경우 VM의 전원 켜기가 실패함

복구 후 가상 머신의 전원을 켜면 vCenter에 다음과 같은 PowerOnFailure 오류가 반환됩니다.

```
DRS cannot find a host to power on or migrate the virtual machine. Network interface 'Network adapter 1' uses network '77 d3 02 50 5f 76 ca d7-db f9 42 6c 0f 6f 87 1f', which is not accessible.
```

이 오류 메시지는 가상 머신을 복구하는 환경에 가상 머신 백업 시 있었던 네트워크 연결이 없는 경우에 발생합니다. 예를 들어 분산형 vSwitch에 연결된 가상 머신을 백업한 후에 DRS(Distributed Resource Scheduler) 클러스터의 일부인 ESX 호스트로 가상 머신을 복구할 경우 vSwitch가 DRS 클러스터에 없기 때문에 가상 머신의 전원 켜기가 실패합니다.

이 문제를 해결하려면 가상 머신 설정을 편집하고 네트워크 어댑터에 대한 네트워크 연결을 설정합니다. 그런 다음 가상 머신의 전원을 켭니다.

디스크 레벨 복구는 타겟 데이터 저장소를 지정할 수 있는 옵션을 제공하지 않습니다.

새 위치로 디스크 레벨 복구는 가상 머신의 각 디스크에 대해 타겟 데이터 저장소를 지정할 수 있는 옵션을 제공하지 않습니다. 현재, VDP는 백업 중에 건너뛴 디스크를 포함하여 가상 머신의 모든 디스크를 지정된 타겟 데이터 저장소로 복구합니다.

이 문제를 해결하려면 사용 가능한 공간이 충분하여 백업 중에 건너뛴 디스크를 포함하여 가상 머신의 모든 디스크를 수용할 수 있는 타겟 데이터 저장소를 지정합니다.

원래 위치로 복구할 때 삭제된 디스크를 건너뛴다.

타겟 가상 머신에 백업된 원래 가상 머신과 동일한 디스크 사용 공간이 더 이상 없는 경우(디스크가 가상 머신에서 제거되거나 삭제된 경우), 복구 창에서 복구 시점 타임 스탬프를 선택한 후 "원래 위치로 복구" 작업을 수행하면 가상 머신의 누락된 디스크를 복구하지 못합니다.

해결책은 누락된 디스크를 가상 머신에 수동으로 추가한 후 디스크를 원래 위치에 복구하는 것입니다. 디스크의 크기가 가상 머신이 백업될 때의 크기와 같아야 합니다.

이 해결책이 실패할 경우 디스크를 새 위치에 복구하여 새 가상 머신을 생성합니다. 복구 작업이 완료되면 복구된 디스크를 새 가상 머신에서 분리하고 필요한 가상 머신에 연결합니다.

디스크를 기존 가상 머신으로 복구할 때 이름 충돌 발생

디스크를 기존 가상 머신으로 복제할 때 이름 충돌 때문에 실패합니다. 새 디스크가 복구되는 데이터 저장소와 동일한 저장소에 기존 .vmdk 디스크가 있는 경우 충돌이 발생합니다.

이 문제를 해결하려면 이름 충돌을 일으키는 기존 디스크를 제거하거나 이름을 바꾸십시오.

'긴급 복구' 복구 시점에 대해 타임 스탬프 세부 정보가 표시되지 않음

VDP Configure 유틸리티의 긴급 복구 탭에서 복구 시점을 탐색할 때 사용자에게 복구 시점에 대한 타임 스탬프 세부 정보가 표시되지 않을 수 있습니다. 이 문제는 시간대가 UTC로 정의된 경우에 발생합니다.

다음 단계에 따라 UTC 시간대를 변경하십시오.

- 1 VDP 구성 유틸리티를 엽니다.
- 2 구성 탭에서 시간대 변경을 선택합니다.
- 3 UTC 시간대 외의 시간대를 선택하고 **저장**을 클릭합니다.
- 4 **변경 내용 적용**을 클릭합니다.
- 5 웹 서비스가 다시 시작된 후 VDP 구성 유틸리티에 로그인하고 타임 스탬프를 확인합니다.

VDP 복제 문제 해결

다음 문제 해결 항목에서는 복제와 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

마지막으로 성공한 복제 정보와 마지막으로 실패한 복제 정보는 e-메일 보고서에 포함되지 않습니다.

복제 작업이 완료된 후에 생성된 예약 e-메일 보고서 및 임시 e-메일 보고서는 복제 작업 요약에 마지막으로 성공한 복제 작업과 마지막으로 실패한 복제 작업에 대한 정보를 포함하지 않습니다.

VDP에서는 성공한 복제 작업과 실패한 복제 작업에 대한 정보를 얻을 수 없습니다.

복제 작업 실패 오류

대상 서버가 정상 또는 모든 권한 상태에 있는 경우 VDP 어플라이언스는 대상 서버의 상태를 올바르게 보고합니다. 대상 서버가 관리, 읽기 전용 또는 동기화 상태에 있는 경우 VDP 어플라이언스는 복제 작업이 실패할 때 기타 오류를 보고합니다.

대상 서버의 사용 용량이 95%가 넘고 **지금 복제** 작업을 시작할 수 없는 경우 용량 문제에 대한 경고 메시지가 표시됩니다. 마찬가지로 스토리지 용량이 95% 넘게 사용되는 경우에도 복제된 백업을 VDP 어플라이언스 또는 Data Domain 스토리지로 복구할 수 없습니다. 용량 문제에 대한 경고 메시지가 표시됩니다.

실행 오류를 정확하게 보고하지 않을 경우 사용자는 대상 서버의 상태를 확인할 수 없습니다.

복제 작업 진행률이 무한정으로 미완료 상태에서 벗어나지 못합니다.

VDP 작업 창에는 복제 작업에 대해 "기타 오류"가 표시되고 서버에서 복제를 위한 세션을 시작하지 못합니다. 이 오류의 가능한 원인 중 하나는 타겟 서버에 대한 핵심 관리 서비스의 실행 중단입니다.

관리 서비스를 확인하고 실행 중이 아닌 경우 핵심 서비스를 재시작한 후 복제 작업을 다시 시도하십시오.

단일 작업 내에서 각기 다른 가상 머신에 대해 생성된 여러 복제 작업이 병렬로 실행되지 않고 연속적으로 실행됨

여러 가상 머신에 대한 복제 작업은 병렬로 처리해야 합니다. 순차 동작은 동일한 클라이언트에 다른 복제 작업이 이미 실행 중인 경우에만 발생합니다. 이 경우 클라이언트 복제 작업은 이미 실행 중인 복제 작업이 완료될 때까지 대기합니다.

이 문제를 해결하려면 `/usr/local/vdr/etc/vdp-options.properties` 파일에 `com.vmware.vdp.option.replicate.maxstreams` 속성을 추가해야 합니다. 기본값은 1입니다. 속성을 추가하거나 편집할 때 기본 설정을 변경하는 경우 어플라이언스에서는 새 값을 복제 작업에 대한 최대 동시 프로세스 수로 설정합니다.

VDP 무결성 검사 문제 해결

무결성 검사를 시작한 후 "VDP: 무결성 검사" 작업이 최근 작업 아래 **실행 중** 작업 탭에 표시되기 전에 몇 초간 지연될 수 있습니다. 이와 유사하게 무결성 검사를 취소할 때 작업이 실제로 취소되기 전에 몇 초간 지연될 수 있습니다.

일부 경우(예: 무결성 검사 진행률이 90% 이상인 경우) 무결성 검사가 취소되기 전에 실제로 완료된 것일 수 있습니다. 무결성 검사가 성공적으로 완료된 경우에도 작업 콘솔에 무결성 검사가 취소되었다는 오류가 계속 표시될 수 있습니다.

무결성 검사를 시작하기 전에 어플라이언스의 무결성 검사 상태(보고서 탭에 표시됨)가 "기간 지남"인 것을 알고 있었다면 작업을 취소한 즉시 상태를 관찰하여 취소 작업의 성공 여부를 확인할 수 있습니다. 무결성 검사 상태가 "정상"인 경우 검사가 성공적으로 완료된 것이고, 상태가 "기간 지남"인 경우 검사가 취소된 것입니다.

자동 백업 검증 문제 해결

다음 문제 해결 항목에서는 자동 백업 검증과 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

데이터 저장소 이름을 변경한 후 자동 백업 검증 작업이 실패합니다.

이 오류는 대상 데이터 저장소 이름을 변경하거나 VDP 외부로 이동한 경우 발생할 수 있습니다.

작업을 편집하고 이름이 변경된 또는 이동된 대상 데이터 저장소를 새 대상으로 선택하십시오. 지침은 ["백업 검증 작업 편집"](#)(123페이지) 섹션을 참조하십시오.

하나 이상의 ABV 작업이 실패하고 "가상 머신을 생성하지 못했습니다."라는 오류가 표시되며 vCenter 인벤토리에 분리된 상태의 가상 머신이 남아 있습니다.

ABV에서 가상 머신 생성에 사용한 버전과 호환되지 않는 이전 버전을 사용하는 호스트에 있는 복구된 가상 머신에 대한 검증을 트리거했습니다. 이로 인해 가상 머신이 분리된 상태로 남게 되는데, 이것은 이와 같은 상황에서 관리자가 복구 관련 문제를 제대로 해결하는 데 필요한 계획된 동작입니다.

vCenter 또는 데이터 저장소 인벤토리에 남은 임시 가상 머신을 수동으로 삭제하거나 등록 취소하십시오.

ABV 작업을 취소하면 VDP_VERIFICATION_XXXX 가상 머신이 대상 호스트에 남습니다.

ABV 작업 취소 후 대상 호스트에 남겨진 VDP_VERIFICATION_* 가상 머신을 찾고 수동으로 제거하여 이 문제를 해결할 수 있습니다.

데이터 저장소에서 사용 가능한 공간이 부족하여 요청된 작업을 수행할 수 없음

ABV 작업 또는 예약된 작업이 실패하고, 때론 실제 데이터 손실이 발생하거나, 공간 부족으로 데이터 저장소 작업을 완료하지 못했다는 오류 메시지가 로그에 포함됩니다.

데이터 저장소에서 공간을 확보하고 실패한 ABV 작업을 다시 시도하십시오. 데이터 저장소의 공간 관리를 지속적으로 규칙적으로 수행하여 공간이 부족하지 않도록 하고, 특히 데이터 저장소 공간 사용에 영향을 주는 예약된 작업 전에는 주의를 기울이십시오.

Restore Client(파일 레벨 복구) 문제 해결

다음 문제 해결 항목에서는 Restore Client와 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

로그인 실패, vCenter에서 10.100.1.10의 가상 머신을 찾을 수 없음

이 오류는 VDP에 의해 백업되지 않은 호스트에서 Restore Client에 연결하려고 시도하는 경우 발생할 수 있습니다.

VDP에 의해 백업된 가상 머신에 로그인한 다음 Restore Client에 연결하십시오.

로그인 실패, vCenter에서 가상 머신을 찾을 수 없음

파일 레벨 복구를 수행한 후 소스 가상 머신에 로그인하면 로그인이 실패하고 다음 오류가 나타납니다.

로그인하지 못했습니다. vCenter에서 가상 머신을 찾을 수 없습니다.

NIC가 연결되지 않은 상태에서 VM 이미지를 새 가상 머신에 복구하는 경우에 이 오류가 발생할 수 있습니다. 이 경우 FLR은 복구가 완료된 후 짧은 시간 동안 소스 가상 머신에 로그인할 수 없습니다. 이 문제를 해결하려면 복구가 완료된 후 몇 분 정도 기다렸다가 소스 가상 머신에 로그인하십시오.

복구 작업이 오류 코드 1007과 함께 실패

복구 작업이 실패하고 오류 코드 1007 "작업 실패 - 클라이언트 오류"가 표시될 경우 읽기 전용 대상(예: CD 드라이브) 또는 미디어가 로드되지 않은 이동식 미디어 디바이스(예: 디스크 드라이브)를 선택했기 때문일 수 있습니다.

새로운 대상을 사용하여 다시 복구를 시도하거나 대상 디바이스가 쓰기 가능한지 확인하십시오.

파일 레벨 복구 마운트 과정에서 VMDK 파일에 여러 파티션이 포함되어 있는 경우 마지막 파티션만 표시됨

Restore Client는 확장된 볼륨을 지원하지 않습니다. 이는 예상된 동작입니다. 이미지 레벨 복구를 수행하고 필요한 파일을 수동으로 복제하십시오.

파일 레벨 복구 마운트 과정에서 지원되지 않은 파티션을 마운트하지 못함

다음 디스크 형식은 Restore Client에서 지원하지 않으므로 이는 Restore Client 마운트가 실패할 경우 예상되는 동작입니다.

- 포맷되지 않은 디스크
- 확장 파티션(유형: 05h, 0Fh, 85h, C5h, D5h)
- 동적 디스크(Windows)/멀티 드라이브 파티션(2개 이상의 가상 디스크로 구성된 파티션)
- 중복 제거된 NTFS
- ReFS(Resilient File System)
- EFI 부트로더
- 암호화된 파티션
- 압축된 파티션

이미지 레벨 복구를 수행하고 필요한 파일을 수동으로 복제하십시오.

심볼 링크가 복구 클라이언트에 표시되지 않음

복구 클라이언트는 심볼 링크 탐색을 지원하지 않습니다.

가상 머신을 가져온 후, 가져오기 전에 백업한 가상 머신에 대한 FLR 로그인이 실패함

이전에 사용된 VDP 디스크로부터 가져온 복구 시점에서 FLR을 수행하려면 새 VDP를 사용하여 VM의 백업을 하나 이상 생성합니다.

중첩된 컨테이너 제한 사항

다른 컨테이너를 포함하는 VMware 컨테이너(즉, 중첩된 컨테이너 구조. 예: vApp-1에 여러 가상 머신이 포함되고, vApp-1 내에 vApp-2라는 컨테이너가 중첩되어 있고, vApp-2에도 여러 가상 머신이 포함됨)를 복구하는 경우 VDP 어플라이언스는 계층의 최상위만 복구합니다. 이 제한 사항에 대한 두 가지 임시적인 해결책은 다음과 같습니다.

- 컨테이너 구조를 단층화합니다.
- 두 v-App(vApp-1 및 vApp-2)을 별도로 백업할 수 있는 별도의 컨테이너 항목으로 추가합니다. 복구할 때는 vApp-1을 먼저 복구한 다음 vApp-2를 vApp-1에 복구합니다.

VDP 라이선스 등록 문제 해결

다음 문제 해결 항목에서는 라이선스 등록과 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

호스트에 라이선스가 등록된 경우에도 라이선스 위반 이벤트가 발생함

클러스터의 호스트에 라이선스를 등록하는 경우 클러스터의 모든 호스트에 라이선스를 등록해야 합니다. 그렇지 않으면 모든 호스트가 라이선스 계약을 위반한 것으로 간주됩니다. 클러스터의 특성으로 인해 어느 시점에서든 특정 가상 머신이 어떤 호스트에 속하는지 알 수가 없습니다. 따라서 전체 클러스터에 유효한 라이선스가 등록되어야 합니다. 라이선스 키를 적절히 할당하는 것은 관리자의 책임입니다.

평가판 라이선스가 만료되고 시스템 기능이 저하됨(사용할 수 없음)

설계상, VDP 어플라이언스는 라이선스 요구 사항이 충족되지 않을 때마다 핵심 서비스를 종료합니다. 이와 같은 현상은 평가판 라이선스가 만료되면 발생할 수 있습니다.

미션 크리티컬 데이터에는 평가판 라이선스를 사용하지 마십시오. 평가판 라이선스는 VDP Advanced 어플라이언스를 시범적으로 사용해 보는 기회로 삼고, 해당 어플라이언스는 써보고 버리는 물건 정도로 생각해야 합니다.

그러나 이후 영구적인(비평가판) vSphere Data Protection 라이선스 키를 구입하는 경우 해당 어플라이언스를 복구하기 위한 방법이 있습니다. 시스템에서 핵심 서비스를 강제로 비활성화하는 1시간 간격으로 다음 단계를 수행해야 합니다.

- 1 VDP Configuration 유틸리티를 사용하여 모든 서비스를 수동으로 재시작합니다.
- 2 vSphere Web Client에서 VDP 어플라이언스에 액세스합니다.
 - a 구성 탭의 라이선스 할당 포틀릿으로 이동합니다.
 - b 영구적인 새 라이선스 키를 시스템에 추가합니다.

그러면 어플라이언스의 상태가 영구적으로 업그레이드되고 해당 서비스가 작동 상태를 유지하게 됩니다.

참고 이 방식으로 복구해야 할 평가판 어플라이언스가 여러 개 있는 경우 각 어플라이언스에 대해 위 절차를 반복해야 합니다. 업데이트를 적용하려면 영구 라이선스 키를 제거한 다음 다시 추가하면 됩니다.

또는 라이선스 키를 한 번 설치하고 라이선스 감사가 실행될 때까지 24시간 동안 기다릴 수 있습니다. 라이선스 감사 프로세스는 영구 라이선스 키의 존재를 감지하고 해당 어플라이언스를 평가판 라이선스 키로부터 업그레이드합니다. VDP Configuration 유틸리티를 사용하여 모든 서비스를 수동으로 재시작해야 합니다.

VDP 어플라이언스 문제 해결

다음 문제 해결 항목에서는 VDP 어플라이언스와 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

VMware VDP for Exchange Server Client 또는 VMware VDP for SQL Server Client가 VDP 어플라이언스에 더 이상 등록되어 있지 않음

VDP 어플라이언스 이름이 변경되었거나 해당 클라이언트가 설치되었는데 새 체크포인트가 생성되지 않고 롤백이 발생한 경우에 이 문제가 발생할 수 있습니다. 이 문제를 해결하려면 모든 VDP SQL Server 및 Exchange Server Client를 다시 설치하십시오.

백업 작업에 SQL Server 또는 Exchange Server가 둘 이상 포함되고 이들 서버에 동일한 데이터베이스 경로가 있는데 한 서버 인스턴스의 데이터베이스는 선택하고 동일한 경로의 다른 인스턴스는 선택하지 않은 경우, 동일한 경로의 두 번째 인스턴스도 백업됨

이 문제를 해결하려면 백업 작업당 하나의 Exchange Server 또는 SQL Server만 포함하거나 모든 데이터베이스 경로가 고유하도록 합니다.

하나 이상의 클라이언트를 복구할 수 없음. 클라이언트가 비활성 상태이며 복구를 수행할 수 있는 상응하는 클라이언트가 없음.

이 문제는 사용자가 복구 시점을 선택하지 않고 복구 마법사를 호출하려고 시도하거나 등록 취소된 클라이언트에 복구 시점이 있는 경우에 발생할 수 있습니다. 두 경우 모두 운영 환경에 비활성 상태의 클라이언트가 있고 상응하는 타겟 클라이언트가 없는 경우 복구를 수행할 수 없습니다.

VDP 어플라이언스 게스트 운영 체제(Linux)가 읽기 전용이 됨

다음 증상이 모두 나타나는 경우 Linux 게스트 운영 체제가 읽기 전용이 됩니다.

- 1 다음 메시지에 나온 대로 서비스 상태를 확인하거나 접근할 수 없습니다.

```
root@dummysxxx:/usr/local/#: dpnctl status
/bin/chown: changing ownership of `/usr/local/avamar/var/log': Read-only file system
dpnctl: ERROR: running as user "root" - problem opening log file "/usr/local/avamar/var/log/dpnctl.log" (-rw-rw-r--) -
dpnctl: ERROR: traceback on exit:
dpnctl_util: pen_log_file (/usr/local/avamar/bin/dpnctl line YYY)
```

- 2 VDP-Configure UI에 로그인할 수 없습니다.
- 3 vCenter Server 웹 클라이언트 내에서 VDP 플러그인에 연결할 수 없습니다.

다음 VMware 기술 자료 문서에 읽기 전용이 될 수 있는 파일 시스템에 대한 자세한 정보가 나와 있습니다.
<http://kb.vmware.com/kb/51306>

기술 지원에 문의하기 전에 어플라이언스를 다시 시작하십시오. 그러면 문제가 해결될 수 있습니다.

VDP Microsoft Exchange Server 문제 해결

다음 문제 해결 항목에서는 Exchange Server와 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

마운트되지 않은 또는 오프라인 데이터베이스를 건너뛰십시오

백업 수행 시 데이터베이스가 마운트되지 않았거나 오프라인인 경우 백업이 해당 데이터베이스를 건너뛰니다. 일반적으로, 마운트되지 않은 데이터베이스는 운영 중이 아니므로 이런 상황은 문제가 안 됩니다.

드라이브 문자 및 볼륨이 혼합된 경우 백업이 실패할 수 있습니다

볼륨 G:\ 및 C:\MOUNTPOINT와 같이 다른 경로를 통해 동일한 데이터베이스 파일을 가리키도록 Exchange Server를 구성한 경우 백업이 실패할 수 있습니다.

이 백업 오류를 피하려면 동일한 경로를 사용하여 데이터베이스를 가리키도록 Exchange Server 데이터베이스를 구성하십시오. 예를 들어, 드라이브 G:\ 또는 C:\mountpoint와 같은 위치에 DB1, DB2, DB3이라는 3개의 데이터베이스가 있는 경우 다음 경로 예 중 하나(둘 다는 아님)를 사용하십시오.

- G:\DB1, G:\DB2, G:\DB3
- C:\mountpoint\DB1, C:\mountpoint\DB2, C:\mountpoint\DB3

RDB 복구가 실패하거나 사용할 수 없는 RDB가 생성되는 경우

VDP에서는 Microsoft가 Exchange Server 2013에서 RDB가 안정화되도록 권장하는 시간 동안 대기한 후에 복구를 시작합니다. 이 안정화가 대기 시간을 초과하면 복구가 실패하거나 사용할 수 없는 RDB가 생성됩니다. 이 경우 RDB 안정화를 위한 대기 시간을 늘릴 수 있습니다.

RDB 안정화 대기 시간을 늘리려면

- 1 텍스트 편집기를 사용하여 C:\Program Files\avp\var 폴더에 avexchglr.cmd 파일을 생성합니다. 여기서 C:\Program Files\avp는 설치 폴더입니다.
- 2 명령 파일에 다음 텍스트를 입력합니다.

```
--rdb_stabilize_wait=n
```

여기서 n은 초 단위의 대기 시간입니다. 기본값은 60초입니다.

3 저장한 다음 파일을 닫습니다.

복구 요구 사항이 충족되지 않습니다

Exchange Server 데이터베이스를 복구할 때 대상 Exchange Server의 버전과 서비스 팩은 백업이 수행된 Exchange Server와 동일해야 합니다.

대상 및 소스 서버에 있는 Exchange Server 버전이 일치하지 않는 경우 복구가 실패합니다.

간격이 감지된 경우 로그 파일이 이동됩니다

정상 복구 동안 트랜잭션 로그 간격이 감지된 경우 기존 로그 파일은 logs_TIME_DATE라는 폴더로 이동됩니다. 이때 TIME과 DATE는 복구 시간과 날짜를 나타냅니다. 폴더는 Exchange Server 2007 스토리지 그룹 또는 Exchange Server 2010 데이터베이스의 트랜잭션 로그 파일 경로의 하위 폴더로 생성됩니다. 이러한 로그를 사용하여 필요한 경우 복구 작업을 분석하거나 오류가 발생했던 지점까지 해당 로그를 적용할 수 있습니다.

복구 후 Exchange Server 2007 데이터베이스가 마운트됩니다

복구 시작 전에 VDP는 스토리지 그룹에서 복구하도록 선택하지 않은 데이터베이스도 포함하여 모든 데이터베이스를 마운트 해제합니다. 복구가 완료되면 VDP는 스토리지 그룹에서 이전에 마운트되지 않았던 데이터베이스도 포함하여 모든 기존 데이터베이스를 마운트하려고 시도합니다. VDP는 Active Directory에 있어도 디스크에는 없는 데이터베이스의 마운트를 시도하지 않습니다.

오래된 백업에서 선택한 데이터베이스 복구는 실패할 수 있습니다

새 백업이 있는데 오래된 백업에서 선택된 데이터베이스를 복구하려고 하면 복구가 실패할 수 있습니다. 이 문제가 발생하면 로그 폴더 경로에 생성된 restore.env 파일을 해당 경로의 모든 로그 파일과 함께 삭제한 다음 복구를 다시 실행하십시오. 또한 하나 이상의 데이터베이스를 마운트한 경우 이벤트 뷰어를 통해 이벤트 로그를 확인하십시오.

VDP Microsoft SQL Server 문제 해결

다음 문제 해결 항목에서는 SQL Server와 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

SQL Server 2012에서 일부 데이터베이스가 보이지 않음

SQL Server 관리자 그룹에 Windows 시스템 서비스 계정을 추가하면 이 문제를 해결할 수 있습니다.

- 1 SQL Server Management Studio에서 해당 인스턴스에 대한 보안 노트와 로그인 노트를 차례로 확장합니다.
- 2 NT AUTHORITY\SYSTEM 계정을 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.
로그인 속성 대화상자가 나타납니다.
- 3 목록에서 서버 역할 페이지를 선택하고 sysadmin 사용자 옆에 있는 확인란을 선택합니다.
- 4 확인을 클릭합니다.

데이터베이스가 현재 복구 중인 경우 데이터베이스 백업이 실패할 수 있습니다

Microsoft SQL Server는 데이터베이스가 복구 상태에 있는 경우 백업을 지원하지 않습니다.

Tail 로그 백업 옵션이 선택된 SQL 복구가 실패함

이 문제는 마지막 복구가 마지막 전체 백업 이후에 수행된 경우 발생할 수 있습니다. 복구 전에 데이터베이스에 대해 전체 백업을 수행하십시오.

복구 옵션 Tail 로그 백업이 활성화되어 있고 데이터베이스가 존재하지 않거나 오프라인인 경우 복구가 실패할 수 있습니다. 이 경우 Tail 로그 백업 옵션을 비활성화하십시오.

VDP Microsoft SharePoint Server 문제 해결

다음 문제 해결 항목에서는 SharePoint Server와 관련한 몇 가지 일반적인 문제를 식별하여 해결하는 방법을 설명합니다.

일부 데이터베이스를 복구하지 못했는데도 SharePoint 리디렉션 복구 작업 상태가 성공으로 표시됩니다.

서버 이름 대신 IP 주소를 사용할 경우 리디렉션 복구를 실행할 때 일부 SharePoint 팜 백업이 실패하지만 UI에서는 성공으로 표시합니다.

SharePoint 팜의 일부 또는 전부에 대한 리디렉션 복구의 별칭을 생성할 때는 IP 주소가 아니라 서버 이름을 사용하십시오.

스토리지 용량 문제 해결

VDP 어플라이언스 및 Data Domain 시스템에 저장할 데이터 양을 계산할 때 백업 스토리지 요구 사항을 세심하게 평가하십시오. 다른 서버가 VDP 어플라이언스 및 Data Domain 시스템에 전송하는 데이터를 사용한 예상치를 포함하십시오. 예를 들어 다른 VDP 어플라이언스의 복제 작업을 기준으로 삼거나 같은 Data Domain 시스템을 다른 VDP 어플라이언스와 공유하는 등의 방법이 있습니다.

새로운 VDP 어플라이언스를 구축할 때는 처음 몇 주 동안 스토리지가 빠른 속도로 채워집니다. 백업하는 모든 클라이언트에 고유한 데이터가 포함되어 있기 때문입니다. 다른 유사한 클라이언트가 백업되거나 동일한 클라이언트가 한 번 이상 백업되는 경우에는 VDP 중복 제거 기능이 더 효과적입니다.

따라서 초기 백업 후 후속 백업에서 VDP 어플라이언스에 백업되는 고유한 데이터는 더 줄어듭니다. 초기 백업이 완료되면(즉, 로컬 백업 및 다른 서버로부터의 백업이 보존 기간을 초과함) 시스템이 매일 해제되는 양만큼의 데이터를 새로 저장할 수 있습니다. 이 프로세스를 용량 활용도의 안정 상태에 도달하는 것이라고 합니다. 안정 상태의 이상적인 용량은 80%입니다.

VDP 로컬 스토리지 용량 모니터링

다음 방법을 사용하여 VDP 스토리지 용량을 사전 예방적으로 모니터링해야 합니다.

- vSphere 웹 클라이언트를 사용합니다.
자세한 내용은 [“백업 어플라이언스 구성 보기”](#)(53페이지) 섹션을 참조하십시오.
[“보고서 탭에서 정보 보기”](#)(106페이지)에 설명된 단계를 수행하여 용량을 볼 수도 있습니다.
- VDP 구성 유틸리티를 사용합니다.
자세한 내용은 [“스토리지 구성 보기”](#)(74페이지) 섹션을 참조하십시오.
- e-메일 알림 및 보고서를 구성하고 모니터링합니다.
자세한 내용은 [“e-메일 알림 및 보고서 구성”](#)(55페이지) 섹션을 참조하십시오.

Data Domain 스토리지 용량 모니터링

다음 방법을 사용하여 Data Domain 시스템의 스토리지 용량을 모니터링할 수 있습니다.

- vSphere 웹 클라이언트를 사용합니다.
자세한 내용은 [“vSphere Web Client를 사용하여 모니터링”](#)(92페이지) 섹션을 참조하십시오.
- VDP 구성 유틸리티를 사용합니다.
자세한 내용은 [“VDP 구성 유틸리티를 사용하여 모니터링”](#)(93페이지) 섹션을 참조하십시오.
- e-메일 알림 및 보고서를 구성하고 모니터링합니다.
자세한 내용은 [“e-메일 알림 및 보고서 구성”](#)(55페이지) 섹션을 참조하십시오.

용량 문제 모니터링

용량 문제는 VDP 어플라이언스나 Data Domain 시스템 또는 이 둘 모두의 스토리지가 거의 가득 찼을 때 시작됩니다. 다음 방법을 사용하여 용량 문제를 모니터링할 수 있습니다.

- 용량 문제 경보는 vCenter에서 트리거됩니다. vSphere 클라이언트나 vSphere 웹 클라이언트에서 경보를 볼 수 있습니다.
- VDP 경보가 트리거될 때 e-메일을 받도록 VDP 경보 e-메일 알림을 설정할 수 있습니다. 자세한 내용은 “[e-메일 알림 및 보고서 구성](#)”(55페이지) 섹션을 참조하십시오. VDP 경보에는 용량 문제 경보도 포함되어 있습니다.

용량 문제가 미치는 영향

VDP 어플라이언스나 Data Domain 시스템 또는 이 둘 모두의 스토리지 용량이 80%를 초과하는 경우:

- *VDP/Data Domain* 스토리지가 거의 가득 찼습니다라는 노란색 경보가 트리거됩니다.
- 경고 메시지는 알림 표시줄 그리고 vSphere 웹 클라이언트의 **스토리지 요약** 섹션과 VDP 구성 유틸리티에 나타납니다.

VDP 어플라이언스나 Data Domain 시스템 또는 이 둘 모두의 스토리지 용량이 95%를 초과하는 경우:

- *VDP/Data Domain* 스토리지가 거의 가득 찼습니다라는 빨간색 경보가 트리거됩니다.
- 오류 메시지는 알림 표시줄 그리고 vSphere 웹 클라이언트의 **스토리지 요약** 섹션과 VDP 구성 유틸리티에 나타납니다.
- VDP 어플라이언스 및 Data Domain 시스템에서 지금 백업 작업과 복제된 백업 복구를 수행할 수 없습니다.

VDP 어플라이언스나 Data Domain 시스템 또는 이 둘 모두의 스토리지 용량이 100%에 도달하는 경우:

- *VDP/Data Domain* 스토리지가 가득 찼습니다라는 빨간색 경보가 트리거됩니다.
- 오류 메시지는 알림 표시줄 그리고 vSphere 웹 클라이언트의 **스토리지 요약** 섹션과 VDP 구성 유틸리티에 나타납니다.
- VDP 어플라이언스 및 Data Domain 시스템의 현재 백업이 실패합니다.
- VDP 어플라이언스 및 Data Domain 시스템에서 새 백업을 수행할 수 없습니다.
- VDP 어플라이언스 및 Data Domain 시스템으로의 데이터 복제가 실패합니다.
- Data Domain 시스템에서 정보를 변경하는 작업이 실패합니다. 이러한 작업에는 가비지 수집 중 체크포인트, 활성 백업 및 만료된 백업 삭제가 포함됩니다. 이들 작업은 전체 Data Domain 시스템에서 허용되지 않는 디렉토리 이름 바꾸기가 수반되기 때문에 실패할 수 있습니다.
- VDP 어플라이언스가 관리자 상태로 있습니다.

스토리지 공간을 비우는 일반적인 단계

최대 용량에 도달하는 것을 방지하기 위해 다음 단계를 수행하여 스토리지 공간을 비워야 합니다. 스토리지 용량이 80%를 초과하면 다음 단계를 수행하십시오.

- 가상 머신을 백업 클라이언트로 추가하지 않습니다.
- 불필요한 복구 시점 제거
- 원치 않는 작업을 삭제합니다.
- 보존 정책을 재평가하여 보존 정책을 줄입니다.
- VDP 어플라이언스를 추가하고 여러 어플라이언스 간 백업 작업의 균형을 맞춥니다.
- Data Domain 시스템을 VDP 어플라이언스에 추가하지 않은 경우에는 추가하고 VDP 어플라이언스와 Data Domain 시스템 간 백업 작업의 균형을 맞춥니다.
- 로컬 VDP 스토리지 디스크를 확장합니다. 자세한 내용은 “[VDP 디스크 확장](#)”(97페이지) 섹션을 참조하십시오.

- Data Domain 시스템이 용량 한도에 도달하면 “[전체 Data Domain 시스템에서 스토리지 재확보](#)”(93페이지)에 설명된 공간 재확보 단계를 수행하십시오.

VDP 기술 자료 문서 액세스

추가 문제 해결 정보는 다음 사이트에서 VDP 기술 자료 문서를 통해 확인할 수 있습니다.

<http://www.vmware.com/selfservice/microsites/microsite.do>

Products > VMware vSphere Data Protection 범주 > Troubleshooting을 선택하십시오.

색인

A

Adobe Flash Player **22**

B

Best Practice

Data Domain **79**

general **26**

VDP 어플라이언스 구축 **26**

긴급 복구 **42**

백업 **63**

복제 **136, 140**

자동 백업 검증 **120**

지원되는 디스크 유형 **22, 113**

초기 VDP 구축 시의 스토리지 용량 **27**

프록시 **64**

프록시 구축 **62**

핫 애드(HotAdd) **27, 62, 64**

C

CA(인증 기관) **49**

CBT(Changed Block Tracking) **14, 16, 26**

CPU 로드 **67**

D

Data Domain

Best Practice **79**

VDP 구성에 시스템 추가 **84**

VDP 어플라이언스에서 모니터링 **92**

VDP 어플라이언스에서 삭제 **85**

VDP 통신에 대한 포트 사용 요구 사항 **82**

VDP 통합에서 클라이언트 지원 **79**

VDP 통합을 위한 시스템 준비 **83**

VDP 환경의 제한 사항 **79**

VDP를 사용한 백업 **87**

구성 **78**

백업에 대한 타겟 선택 **88**

서버 유지 보수 작업 모니터링 **90**

아키텍처 개요 **78**

용량 모니터링 **92**

일반적인 문제 및 해결책 **95**

전체 시스템에서 스토리지 재확보 **93**

최대 스트림 값 변경 **82**

통합 전 요구 사항 **80**

Data Domain 스토리지 구성 **78**

DNS 구성

설정 **23**

확인 **23**

DRS(Distributed Resource Scheduler) **66**

dvSwitch(distributed vSwitch) 문제 해결 **197**

E

Essential Plus 라이선스 **98**

e-메일 보고서 **53, 55**

F

FLR(File Level Recovery)

개요 **14, 148**

요구 사항 **62**

이점 **17**

제한 사항 **65, 148**

지원 **64**

지원되지 않는 VMDK 구성 **149**

G

GLR(Granular Level Restore)

Microsoft Exchange 2007 서버 **177**

Microsoft Exchange 2010 또는 2013 서버 **177**

로그 파일 **176**

문제 해결 **176**

L

LVM(Logical Volume Manager) **62, 148**

M

Master Boot Record **148**

Microsoft Exchange

RDB 대기 시간 증가 **203**

UAC가 활성화된 경우 클라이언트 설치 **156**

구성 톨 사용 **170**

백업 복구 **173**

백업 서비스 수동 구성 **171**

백업 작업 생성 **171**

서버 옵션 **166**

애플리케이션 백업 **171**

클라이언트 설치 **167**

Microsoft SharePoint

백업 복구 **181**

백업 작업 생성 **180**

서버 백업 및 복구 **178**

Microsoft SQL

백업 및 복구 **157**

백업 복구 **164**

백업 작업 생성 **162**

- 서버 옵션 **157**
- 서버 지원 **157**
- 애플리케이션 백업 **162**
- 클라이언트 설치 **158**
- MITM(Man-in-the-Middle) 공격 **49**
- N**
- NAT(Network Address Translation) **148**
- NBD(Network Block Device) **22, 27, 64**
- NTFS **149, 178, 201**
- O**
- OVF 템플릿 파일 **30**
- OVF 템플릿 파일, 구축 **29**
- R**
- RTI(Replication Target Identity) **134, 143**
- S**
- SSL 인증서 **49**
- SSO 관리자 **25**
- storage
 - summary **54**
- SVMotion
 - VMDK 파일의 라이브 마이그레이션에 사용됨 **114**
- V**
- vCenter
 - 사용자 계정 권한 **189**
- vCenter Server
 - VDP 어플라이언스 전환 **106**
 - 버전 요구 사항 **22**
 - 지원되는 버전 **29**
 - 호스트 이름, 암호 등 변경 **40**
- VCSA(vCenter Server Appliance) **16**
- VDP 디스크
 - 연결 **72**
- VDP 라이선스 등록, 문제 해결 **202**
- VDP 어플라이언스 시작 **60**
- VDP 어플라이언스 종료 **60**
- VDP, 지원되지 않는 디스크 유형 **22, 113**
- VDP(vSphere Data Protection) 설치
 - 소프트웨어 요구 사항 **22**
- VDP(vSphere Data Protection) 어플라이언스
 - shutdown **60**
 - startup **60**
 - vCenter Server에서 전환 **106**
 - 구축 시의 Best Practice **26**
 - 설명 **14**
 - 손상 **73**
 - 어플라이언스 롤백 **41**
- VDP-Configure 유틸리티 **36**
- VMDK(Virtual Machine Disk) **14**
- VMFS 힙 크기 **98**
- vMotion
 - 새 위치로 복구 실행 전 기능 해제 **130**
- VMware VADP(vStorage APIs for Data Protection) **14**
- VMware 툴 **24, 120**
- vSphere Data Protection(VDP)
 - Setup **30**
 - vSphere Web Client를 사용하여 액세스 **104**
 - 구성 변경 **40**
 - 기술 자료 문서 액세스 **207**
 - 로그 수집 중 **38**
 - 명령줄에서 액세스 **104**
 - 사용자 인터페이스 **106**
 - 사이징 **22**
 - 서비스 상태 보기 **36**
 - 서비스 시작 및 중지 **37**
 - 소프트웨어 요구 사항 **22**
 - 용량 필요 **27**
 - 작업 모니터링 **58**
 - 지원되는 구성 **23**
- vSphere Flash 읽기 캐시 및 ESXi 호환성 **22**
- vSphere Flash 읽기 캐시와 ESXi의 호환성 **22**
- vSphere HA **70**
- vSphere Web Client **105**
 - Adobe Flash Player 요구 사항 **22**
 - 지원되는 웹 브라우저 **22**
- vSphere 호스트, 지원되는 버전 **22**
- 가**
- 가변 길이 데이터 세그먼트 **15**
- 가상 볼륨(VVOL) **22**
- 개별 디스크
 - 마이그레이션 시 영향 **114**
 - 백업 작업 생성 **16, 113**
- 개별 디스크 백업
 - 절차 **114**
 - 지원되는 디스크 유형 **113**
- 경보, 보기 **59**
- 고정 길이 데이터 세그먼트 **15**
- 기술 자료, 문서 액세스 **207**
- 기술 지원 리소스 **12**
- 긴급 복구
 - Best Practice **42**
 - performing **42**
 - 복구 시점 문제 해결 **198**
 - 자동 호스트 감지 **44**
 - 제한 사항 **42**
 - 지원되지 않는 기능 **42**
- 나**
- 내부 프록시, 비활성화 **66**

네트워크 설정, 구성 **40**

노드 구조, 복제 **142**

다

데이터 보호

CBT(Changed Block Tracking) 사용 **14**

FLR(File Level Recovery) 사용 **14, 148**

VMDK(Virtual Machine Disk) 사용 **14**

VMware VADP(vStorage APIs for Data Protection) 사용 **14**

데이터 저장소 사용 **14**

동시 백업 **63**

디스크 사용량 **67**

디스크 확장

Essentials Plus 사용 **101**

디스크 확장 및 추가 **99**

요구 사항 **98**

제한 사항 **100**

디스크, VDP 지원 유형 **22, 113**

라

라이센스

Essential Plus **98**

평가판 라이선스 만료 문제 해결 **202**

라이센스 감사 **202**

라이센스 키(license key)

영구 **202**

요구 사항 **15**

로그

번들 **38, 194**

보기 **57**

수집 **38**

프록시 **67**

로그 번들, 파일 이름 **38, 194**

로그 수집 **38**

로그 수집 중 **38**

마

마운트 제한 사항 **151**

멀티 테넌시, 지원 **144**

메모리 사용량 **67**

모니터링

Data Domain 용량 **92**

Data Domain 유지 보수 작업 **90**

VDP 어플라이언스에서 Data Domain 모니터링 **92**

VDP 작업 **58**

백업 검증 작업 **124**

용량 **28**

무결성 검사, 실행 **57**

문제 해결

ABV(Automatic Backup Verification) **200**

Microsoft Exchange RDB 대기 시간 **203**

VDP Exchange 백업 **203**

VDP SQL 백업 **204**

VDP SQL 복구 **204**

VDP 어플라이언스가 응답하지 않습니다. **194**

VM에 VMware 내결함성이 활성화된 경우 백업이 실패함 **195**

vSphere Data Protection Exchange 복구 **204**

vSphere Data Protection 무결성 검사 **199**

vSphere Data Protection에 데이터 저장소 용량이 충분하지 않은 경우 백업이 실패합니다 **195**

게스트 운영 체제(Linux)가 읽기 전용이 됨 **203**

관련 백업 소스가 유실될 수 있음 **195**

단일 vmdk를 다른 데이터 저장소로 마이그레이션하는 경우 VMDK 백업 작업이 자동으로 실패합니다. **195**

디스크를 기존 가상 머신으로 복구할 때 이름 충돌 **198**

라이센스 위반 이벤트 **202**

백업 로드 속도가 느려짐 **197**

백업 작업 데이터 로드 **195**

복구 작업 실패 **200**

복제 작업 **199**

복제 작업 실패 오류 **199**

분산형 vSwitch에 연결된 경우 가상 머신 전원 켜기가 실패합니다. **197**

세밀한 레벨의 복구 **176**

예기치 않은 종료 후 최근 백업이 유실됨 **195**

클라이언트를 추가할 수 없음 **195**

특수 문자가 사용된 경우 백업이 실패함 **196**

파일 레벨 복구 **200, 201**

항목을 찾을 수 없음 **195**

바

백업

검증 **124**

동시 백업 수 줄이기 **63**

마운트 **151**

실행 개수 늘리기 **63**

필터링 **151**

확인 **124**

백업 검증 작업

모니터링 **124**

사용 안 함 **124**

삭제 **124**

생성 **121, 124**

실행 **123**

제한 사항 **120**

클론 생성 **123**

편집 **123**

백업 기간, 편집 **55**

백업 마운트 **151**

백업 및 복구

Changed Block Tracking 사용 **14**

- VMDK(Virtual Machine Disk) 사용 **14**
- VMware VADP(vStorage APIs for Data Protection) 사용 **14**
- 데이터 저장소 사용 **14**
- 파일 레벨 복구 사용 **14, 148**
- 백업 복구
 - SCSI 디스크 ID로 **128, 129, 131**
 - 새 위치로 **128, 129, 131**
 - 수동 **127, 129, 130**
 - 스냅샷이 존재하는 경우 **127**
 - 원래 위치로 **128, 129, 131**
 - 호스트에 직접 **42**
- 백업 스케줄 **136**
- 백업 작업
 - VDP에서 Avamar로 마이그레이션 **117**
 - 개별 디스크 **112, 113**
 - 전체 이미지 **112**
- 백업 필터링 **151**
- 보고서 탭
 - Data Domain 상태 보기 **84**
 - 정보 보기 **106**
- 보기
 - 경보 **59**
 - 스토리지 요약 **74, 100**
 - 이벤트 콘솔 **60**
 - 작업 **58**
- 보안
 - CA(인증 기관) **49**
 - MITM(Man-in-the-Middle) 공격 **49**
 - SSL 인증서 **49**
 - 로그인 시도 **52**
- 보존 정책 **113, 136**
- 복구
 - 이동식 미디어 **200**
 - 읽기 전용 미디어 **200**
- 복구 시점, 새로 고침 **44**
- 복제
 - Best Practice **136, 140**
 - Data Domain 백업 타겟 **136**
 - 기존 작업 즉시 실행 **141**
 - 노드 구조 **142**
 - 대상 **142**
 - 대상 관리 **140**
 - 복구 **143**
 - 복제할 백업 선택 **137**
 - 소스로 복구 **142**
 - 작업 삭제 **141**
 - 작업 상태 및 세부 정보 보기 **141**
 - 작업 생성 **137**
 - 작업 예약 및 관리 **17, 134**
 - 작업 클론 생성 **141**
 - 작업 편집 **141**
 - 작업 활성화 또는 비활성화 **141**
- 제한 사항 **136**
- 사
 - 사용자 환경 개선 프로그램 **17, 52**
 - 새 위치로 복구
 - 실행 전 vMotion 기능 해제 **130**
 - 서비스
 - 관리 서비스 **36**
 - 백업 스케줄러 **36**
 - 상태 정의 **37**
 - 시작 및 중지 **37**
 - 유지 보수 서비스 **36**
 - 파일 레벨 복구 서비스 **36**
 - 파일 시스템 서비스 **36**
 - 핵심 서비스 **36**
 - 설치 요구 사항 **22**
 - 성능 분석
 - 실행 **101**
 - 테스트 결과 **101**
 - 소프트웨어 요구 사항 **22**
 - 스토리지
 - 기존 VDP 디스크 연결 **72**
 - 기존 스토리지 가져오기 **70**
 - 분리 **73**
 - 생성 **70**
 - 요약 보기 **74**
 - 스토리지 요약, 보기 **100**
 - 시간 동기화 오류 **24**
- 아
 - 안정 상태의 용량 **27**
 - 어플라이언스
 - 롤백 **41**
 - 어플라이언스 롤백 **41**
 - 업그레이드
 - 하드웨어 버전 **22**
 - 완료된 작업 표시 **153**
 - 용량
 - utilization **74**
 - VDP, 초기 구축 **27**
 - 모니터링 **28**
 - 백업에 충분하지 않음 **195**
 - 안정적인 상태 **27**
 - 요구 사항 **22**
 - 이미지 레벨 백업 **16**
 - 이벤트 콘솔, 보기 **60**
- 자
 - 자동 백업 검증
 - Best Practice **120**
 - 문제 해결 **200**
 - 설명 **120**
 - 자동 백업 검증. *참고 항목*

백업 검증 작업

- 작업 세부 정보 탭 **107**
- 작업 실패 탭 **106**
- 작업, 보기 **58**
- 중복 제거, 이점 **15**
- 지원되는 디스크 유형 **22, 113**

파

- 포트 29000 **143**
- 프로비저닝 유형 **70**
- 프록시
 - Best Practice **64**
 - 관리 **63**
 - 구축 **62**
 - 내부, 비활성화 **66**
 - 상태 **67**
 - 외부 지원 **64**
 - 추가 **65**
- 프록시 로그 **67**
- 플랫폼 제품 지원 **16**

하

- 하드웨어 버전
 - 마이그레이션 중 **22**
 - 업그레이드 **22**
- 핫 애드(HotAdd) **22, 27, 62, 64, 66, 148**
- 호스트에 직접 복구 **42**
- 호환성 매트릭스
 - 복제 복구 **143**
 - 복제 소스 **134**