vSphere Data Protection 관리 가이드

vSphere Data Protection 5.1

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/support/pubs.

KO-000846-00

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

VMware, Inc.
서울특별시 강남구 삼성동 159-1
아셈 타워 30 층 (우)135-798
www.vmware.com/kr

목차

1 vSphere Data Protection 이해 7
- vSphere Data Protection 소개 8
- 이미지 레벨 백업 및 복구 8
- 파일 레벨 복구 9
- 중복 제거 저장소의 이점 9
  - 가변 길이 데이터 세그먼트와 고정 길이 데이터 세그먼트 비교 9
  - 논리적 세그먼트 결정 9
- vSphere Data Protection 아키텍처 10

2 vSphere Data Protection 설치 및 구성 11
- vSphere Data Protection 사이징 12
- 소프트웨어 요구 사항 12
- 시스템 요구 사항 13
- vSphere Data Protection 사양 13
- 설치 전 구성 13
  - DNS 구성 13
  - NTP 구성 14
  - 사용자 계정 구성 14
  - OVF 템플릿 배포 14
  - 사전 요구 사항 14
  - 절차 15
- vSphere Data Protection 설치 및 구성 15
  - 사전 요구 사항 15
  - 절차 15
- 설치 후 구성 17
  - 상태 탭 17
  - 구성 탭 18
  - 롤백 탭 18
  - 업그레이드 탭 19
  - VDP-configure 사용 19
- vSphere Data Protection 어플라이언스 업그레이드 19
  - vSphere Data Protection 어플라이언스 스냅샷 생성 20
  - 업그레이드 설치 20
  - 스냅샷 제거 21

3 vSphere Data Protection 사용 23
- vSphere Data Protection 사용자 인터페이스 이해 24
  - 시작 탭 24
  - 백업 탭 25
  - 복구 탭 26
  - 보고서 탭 26
  - 구성 탭 26
- vSphere Data Protection 액세스 26
- vSphere Data Protection 어플라이언스 전환 27

백업 작업 생성 27
가상 머신 27
스케줄 27
보존 정책 27
완료 준비 28
백업 작업 마법사 사용 28
지금 백업 28
가상 머신 복구 29
백업 선택 29
복구 옵션 설정 29
백업에서 가상 머신 복구 29
복구 작업 진행률 보기 30
백업 작업 잠금 30
보고서 보기 30
보고서 탭의 필터링 30
구성 관리 31
백업 어플라이언스 세부 정보 확인 및 편집 31
백업 기간 구성 31
유지 보수 기간 설정 변경 33
수동으로 무결성 검사 실행 33
e- 메일 알림 구성 33
체크포인트 및 롤백 사용 34
파일 레벨 복구 사용 35
파일 레벨 복구 지원 구성 : 35
파일 레벨 복구 제한 사항 36
로그인 옵션 36
기본 로그인 모드에서 복구 클라이언트 사용 37
고급 로그인 모드에서 복구 클라이언트 사용 37
vSphere Data Protection 종료 및 시작 절차 38

4 vSphere Data Protection 용량 관리 39
씬 (thin) 또는 일반 (thick) 프로비저닝 디스크 선택이 미치는 영향 40
사전 요구 사항 40
절차 40
초기 vSphere Data Protection 구축에 스토리지 용량이 미치는 영향 40
vSphere Data Protection 용량 모니터링 40
vSphere Data Protection 용량 임계값 41
용량 관리 41

5 vSphere Data Protection 문제 해결 43
vSphere Data Protection 어플라이언스 설치 44
vSphere Data Protection 백업 44
vSphere Data Protection 복구 45
파일 레벨 복구 45
vSphere Data Protection 보고 46

6 vSphere Data Protection 포트 사용 47

7 vSphere Data Protection 재해 복구 49

색인 51

본 가이드 정보

vSphere Data Protection 관리 가이드에는 중소, 성장, 중견 기업 환경을 위한 설치 및 백업 관리 정보가 수록되어 있습니다.

대상

본 가이드는 vSphere Data Protection을 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.

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/support/pubs를 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/support/pubs를 참조하십시오.

온라인 지원

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

지원 오퍼링

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

VMware Professional Services

VMware Education Services 교육 과정은 현장 참조 툴로 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 관리하는 데 도움이 되는 오퍼링을 제공합니다. 교육 강의, 인증 프로그램 및 컨설팅 서비스에 대한 정보 확인하려면 http://www.vmware.com/kr/services를 참조하십시오.

1 vSphere Data Protection 이해

vSphere Data Protection(VDP)은 간단하게 구축할 수 있는 디스크 기반의 강력한 백업 및 복구 솔루션입니다. vSphere Data Protection은 VMware vCenter Server와 완벽하게 통합되어 백업 작업을 중앙에서 효율적으로 관리할 수 있을 뿐만 아니라 중복 제거된 대상 스토리지에 백업을 저장할 수도 있습니다.

vSphere Data Protection의 이점은 다음과 같습니다.

- 전원이 꺼져 있거나 물리적 호스트 간에 이동하는 경우에도 모든 가상 머신에 대해 빠르고 효율적인 데이터 보호 기능을 제공합니다.
- 전체 백업에서 지능적인 중복 제거 기술을 사용하여 백업 데이터에 의해 소비되는 디스크 공간을 대폭 줄여 줍니다.
- 변경 블록 추적 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.
- 표준 vSphere Web Client에 통합된 vSphere Data Protection 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.

이 장에서 다루는 내용은 다음과 같습니다.

- "vSphere Data Protection 소개", 8페이지
- "이미지 레벨 백업 및 복구", 8페이지
- "파일 레벨 복구", 9페이지
- "중복 제거 저장소의 이점", 9페이지
- "vSphere Data Protection 아키텍처", 10페이지

vSphere Data Protection 소개

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

백업하는 동안 vSphere Data Protection은 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: 변경 블록 추적)**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.
- **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 VM 백업을 수행할 수 있습니다.
- **VMDK(Virtual Machine Disk: 가상 머신 디스크)**는 게스트 운영 체제에 물리적 디스크 드라이브로 표시되는 파일 또는 파일 집합입니다. 이러한 파일은 호스트 머신 또는 원격 파일 시스템에 있을 수 있습니다.
- **vSphere Data Protection 어플라이언스**는 vSphere 데이터 보호를 위해 특별히 구축된 가상 어플라이언스입니다.

이미지 레벨 백업 및 복구

vSphere Data Protection은 VM의 백업 처리 오버헤드를 vSphere Data Protection 어플라이언스로 분산시키기 위한 vSphere 내의 기능인 VADP(vStorage API for Data Protection)와 통합되는 이미지 레벨 백업을 생성합니다. 어플라이언스는 vCenter Server와 통신하여 VM의 VMDK 스냅샷을 생성합니다. 중복 제거는 특허 받은 가변 길이 중복 제거 기술을 사용하여 어플라이언스 내에서 진행됩니다.

대규모로 지속적으로 확장되는 다수의 VMware 환경을 지원하기 위해 각 vSphere Data Protection 어플라이언스는 8개의 가상 머신에 동시에 백업하여 데이터 보호 워크로드 용량을 향상시킬 수 있습니다.

이미지 레벨 백업의 효율성을 높이기 위해 vSphere Data Protection은 VADP의 CBT(Changed Block Tracking) 기능을 활용합니다. CBT는 vSphere Data Protection에서 마지막 백업 이후 변경된 디스크 블록만 백업하는 VMware 기능입니다. 이 기능을 사용하면 해당 VM 이미지의 백업 시간이 대폭 줄어들고 많은 수의 VM을 특정 백업 기간 내에 처리할 수 있게 됩니다.

복구하는 동안 CBT를 활용하면 vSphere Data Protection은 VM을 원래 위치에 보다 빠르고 효율적으로 복구할 수 있습니다. 복구 프로세스가 진행되는 동안 vSphere Data Protection은 VADP에 쿼리하여 마지막 백업 후 변경된 블록을 확인한 다음, 복구하는 동안 해당 블록만 복구 또는 교체합니다. 이렇게 하면 복구 작업 동안 vSphere 환경 내에서 데이터 전송이 줄어들고, 더욱 중요한 것은 RTO(Recovery Time Objective: 복구 시간 목표)가 단축됩니다.

또한 vSphere Data Protection은 두 복구 방법(전체 이미지 복구 또는 CBT를 활용한 복구) 간 워크로드를 자동으로 평가하여 복구 시간이 가장 빠른 방법을 수행합니다. 이는 복구 대상 VM에서 마지막 백업이 수행된 후 변경률이 매우 높거나 CBT 분석 작업의 오버헤드가 전체 이미지를 직접 복구하는 작업보다 더 높은 시나리오에서 유용합니다. vSphere Data Protection은 특정 시나리오 또는 환경에서 VM 이미지 복구 시간이 가장 빠른 구축 방법을 지능적으로 결정합니다.

VMware 이미지 백업의 이점은 다음과 같습니다.

- 게스트 운영 체제에 상관 없이 VM에 대한 전체 이미지 백업을 제공합니다.
- 유효한 라이센스가 있어 사용할 수 있는 경우 효율적인 전송 방법인 SCSI 핫애드(hotadd)를 활용하므로 네트워크에서 전체 VMDK 이미지를 복제하지 않아도 됩니다.
- 이미지 레벨 백업에서 파일 레벨 복구를 제공합니다.
- vSphere Data Protection 어플라이언스에서 보호하는 모든 .vmdk 파일에서 중복 제거를 수행합니다.

- 백업 및 복구 시간을 단축하기 위해 변경 블록 추적을 사용합니다.
- 중복을 제거하고 데이터를 압축하여 네트워크 트래픽을 최소화합니다.
- 각 VM에서 백업 에이전트를 관리할 필요가 없습니다.
- 처리량을 높이기 위해 동시 백업 및 복구를 지원합니다.

중요 VM 이미지 백업에 대한 Best Practice는 각 가상 머신에 VMware 툴을 설치하는 것입니다. VMware 툴은 백업을 진행하기 전에 게스트 운영 체제에서 특정 프로세스를 중지시키는 추가적인 백업 기능을 제공합니다.

파일 레벨 복구

FLR(File Level Recovery: 파일 레벨 복구)을 사용하면 보호된 VM의 로컬 관리자가 로컬 머신에 대한 백업을 찾아 마운트할 수 있습니다. 그런 다음 관리자는 마운트된 백업에서 개별 파일을 복구할 수 있습니다. 파일 레벨 복구는 vSphere Data Protection Restore Client를 사용하여 수행됩니다.

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 비효율성을 없앴습니다.

논리적 세그먼트 결정

vSphere Data Protection은 모든 시스템에서 최적의 효율성을 도출하기 위해 고안된 특허 받은 세그먼트 크기 결정 방법을 사용합니다. vSphere Data Protection 알고리즘은 데이터 세트의 바이너리 구조(데이터 세트를 구성하는 모든 0과 1)를 분석하여 컨텍스트에 종속되는 세그먼트 경계를 확인합니다. 가변 길이 세그먼트의 크기는 평균 24KB이고 이는 다시 12KB로 압축됩니다.

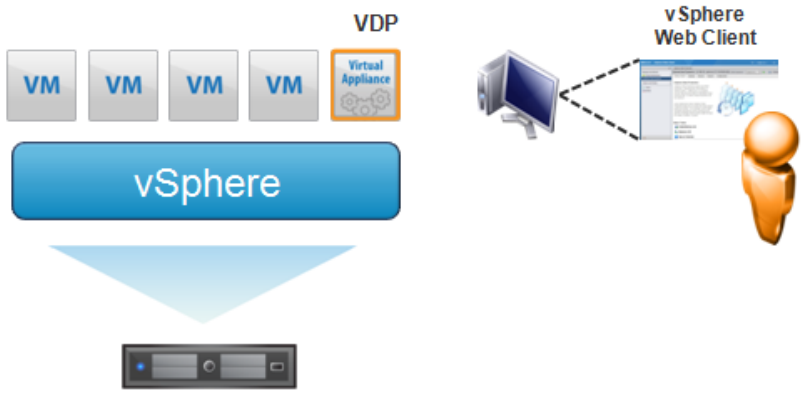
vSphere Data Protection은 VMDK 파일 내의 바이너리 구조를 분석하여 모든 파일 유형 및 크기에 적용하고 지능적으로 데이터의 중복을 제거합니다.

vSphere Data Protection 아키텍처

vSphere Data Protection(VDP)은 vSphere Web Client 및 vSphere Data Protection 어플라이언스를 사용하여 중복이 제거된 스토리지에 백업을 저장합니다.

vSphere Data Protection은 서로 다른 시스템에서 실행되는 구성 요소 집합으로 구성됩니다(아래 다이어그램 참조).

- vSphere 5.1
- vSphere Data Protection 어플라이언스(ESX/ESXi 4.x 또는 5.x에 설치됨)
- vSphere Web Client



vSphere Data Protection 설치 및 구성 2

이 장에서 다루는 내용은 다음과 같습니다.

- "vSphere Data Protection 사이징", 12페이지
- "소프트웨어 요구 사항", 12페이지
- "시스템 요구 사항", 13페이지
- "설치 전 구성", 13페이지
- "OVF 템플릿 배포", 14페이지
- "vSphere Data Protection 설치 및 구성", 15페이지
- "설치 후 구성", 17페이지

vSphere Data Protection 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(일일, 주간, 월간, 연간)
- 일반적인 변경률

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

표 2-1. vSphere Data Protection 사이징 권장 사항의 예

VM 수	클라이언트 당 데이터 스토리지	보존 기간: 일일	보존 기간: 주간	보존 기간: 월간	보존 기간: 연간	권장 사항
25	20GB	30	0	0	0	1 - 0.5TB VDP
25	20GB	30	4	12	7	1 - 2TB VDP
25	40GB	30	4	12	7	2 - 2TB VDP
50	20GB	30	0	0	0	1 - 1TB VDP
50	20GB	30	4	12	7	2 - 2TB VDP
50	40GB	30	4	12	7	3 - 2TB VDP
100	20GB	30	0	0	0	1 - 2TB VDP
100	20GB	30	4	12	7	3 - 2TB VDP
100	40GB	30	4	12	7	6 - 2TB VDP

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. 어플라이언스를 구축하고 난 후에는 데이터 저장소의 크기를 변경할 수 없습니다.

소프트웨어 요구 사항

vSphere Data Protection 5.1에는 다음 소프트웨어가 필요합니다.

- VMware vCenter Server
  - vCenter Server Linux 또는 Windows: 버전 5.1
  - vSphere Web Client는 Microsoft Internet Explorer 7 및 8(현재 IE 8에서 vSphere Web Client를 실행하는 데는 알려진 문제가 있음) 또는 Mozilla Firefox 3.6 이상에서 지원됩니다.
  - 웹 브라우저에 Adobe Flash Player 11.3 이상이 활성화되어 있어야 vSphere Web Client 또는 vSphere Data Protection 기능에 액세스할 수 있습니다.

- VMware ESX/ESXi(다음 버전이 지원됨)
  - 4.0, 4.0i, 4.1i, 5.0i, 5.1
- 어플라이언스 버전:
  - vSphere Data Protection: 5.1

시스템 요구 사항

vSphere Data Protection 어플라이언스는 다음 세 가지 옵션으로 제공됩니다.

- 0.5TB VDP
- 1TB VDP
- 2TB VDP

중요 vSphere Data Protection을 구축하고 난 후에는 크기를 변경할 수 없습니다.

각 vSphere Data Protection 옵션에 대한 시스템 요구 사항은 다음 표에 명시되어 있습니다.

	0.5TB VDP	1TB VDP	2TB VDP
vSphere Data Protection 전용 프로세서	최소 4개의 2GHz 프로세서를 vSphere Data Protection에 상시 사용 가능	최소 4개의 2GHz 프로세서를 vSphere Data Protection에 상시 사용 가능	최소 4개의 2GHz 프로세서를 vSphere Data Protection에 상시 사용 가능
vSphere Data Protection 전용 물리적 메모리	4GB	4GB	4GB
디스크 공간	850GB	1,600GB	3,100GB
네트워크 연결	1GbE 연결	1GbE 연결	1GbE 연결

vSphere Data Protection 사양

vSphere Data Protection은 다음 사양을 지원합니다.

- 각 vSphere Data Protection 어플라이언스는 최대 100개의 VM에 대한 백업을 지원합니다.
- 각 vCenter Server는 최대 10개의 vSphere Data Protection 어플라이언스를 지원할 수 있습니다.
- 0.5TB, 1TB 또는 2TB의 중복 제거 스토리지를 지원합니다.

설치 전 구성

vSphere Data Protection을 설치하기 전에 DNS 및 NTP를 구성해야 합니다.

DNS 구성

vSphere Data Protection을 구축하기 전에 어플라이언스 IP 주소 및 FQDN에 대해 DNS 서버에 항목을 추가해야 합니다. 이 DNS 서버는 정방향 및 역방향 조회를 지원해야 합니다.

중요 DNS를 제대로 설정하지 못할 경우 런타임 또는 구성 문제가 많이 발생할 수 있습니다.

DNS가 제대로 구성되었는지 확인하려면 다음과 같이 하십시오.

1 명령 프롬프트를 열고 다음 명령을 입력합니다.

nslookup <*VDP IP 주소*> <*DNS IP 주소*>

nslookup 명령은 vSphere Data Protection 어플라이언스의 FQDN을 반환합니다.

2 다음 명령을 입력합니다.

nslookup <*VDP의 FQDN*> <*DNS IP 주소*>

nslookup 명령은 vSphere Data Protection 어플라이언스의 IP 주소를 반환합니다.

3 nslookup 명령이 적절한 정보를 반환한 경우 명령 프롬프트를 닫고, 그렇지 않은 경우 vSphere Data Protection을 설치하기 전에 DNS 구성을 해결하십시오.

NTP 구성

vSphere Data Protection은 NTP(Network Time Protocol)를 사용합니다. vSphere Data Protection을 설치하기 전에 vSphere Data Protection이 설치될 vCenter Server 및 ESXi 호스트에 NTP를 구성해야 합니다.

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

사용자 계정 구성

vCenter 사용자 계정을 vSphere Data Protection에 사용하거나 SSO admin 사용자를 vSphere Data Protection에 사용하려면 먼저 이러한 계정을 vCenter 루트 노드에 관리자로 특별히 추가해야 합니다. vSphere Client에서 다음 단계에 따라 vSphere Data Protection 사용자 또는 SSO admin 사용자를 구성하십시오.

1 vSphere Web Client에 로그인하고 **vCenter** > **Hosts and Clusters**를 선택합니다.

2 왼쪽 창에서 vCenter Server를 클릭합니다.

3 **Manage** 탭을 클릭한 다음 **Permissions** 하위 탭을 클릭합니다.

4 **Add permission** 아이콘을 클릭합니다.

5 **Add**를 클릭합니다.

6 Domain 드롭다운에서 도메인, 서버 또는 SYSTEM-DOMAIN을 선택합니다.

7 vSphere Data Protection을 관리하거나 SSO admin 사용자 역할을 할 사용자를 선택한 다음 **Add**를 클릭합니다.

8 **OK**를 클릭합니다.

9 Assigned Role 드롭다운에서 Administrator를 선택합니다.

10 Propagate to child objects 상자가 선택되어 있는지 확인합니다.

11 **OK**를 클릭합니다.

사용자가 Administrators 아래에 나열되는지 확인하려면 **Home** > **Administration** > **Role Manager**로 이동하여 **Administrator** 역할을 클릭합니다. 방금 추가한 사용자가 해당 역할의 오른쪽에 나열되어야 합니다.

중요 VDP-configure UI를 사용하는 vSphere Data Protection 백업 사용자가 도메인 계정에 속해 있는 경우 VDP-configure에서 "SYSTEM-DOMAIN\admin" 형식으로 사용되어야 합니다. 사용자 이름을 "admin@SYSTEM-DOMAIN" 형식으로 입력한 경우 백업 관련 작업이 최근에 실행 중인 작업에 표시되지 않을 수 있습니다.

OVF 템플릿 배포

사전 요구 사항

- vSphere Data Protection 어플라이언스는 ESXi 4.0, 4.1, 5.0 또는 5.1 호스트에 설치됩니다.
- vCenter 5.1이 필요합니다. vSphere Web Client에서 vCenter에 로그인하여 OVF 템플릿을 배포합니다.
- 포트 902를 사용하여 vSphere Data Protection 어플라이언스를 ESXi에 연결합니다. 어플라이언스와 ESXi 사이에 방화벽이 있는 경우 포트 902를 열어야 합니다.
- VMware Client Integration Plug-in 5.1.0을 브라우저에서 설치해야 합니다.

절차

1 vSphere Web Client에 로그인하고 **vCenter > Datacenters**를 선택합니다.

2 Objects 탭에서 **Actions > Deploy OVF Template**을 클릭합니다.

3 vSphere Data Protection 어플라이언스가 있는 소스를 선택합니다.

4 기본적으로 소스 선택 대화상자는 OVF Packages로 설정됩니다. 이를 **OVA Packages**로 변경합니다.

5 어플라이언스를 선택하고 **Open**을 클릭합니다.

6 어플라이언스 .ova 파일이 선택되면 **Next**를 클릭합니다.

7 템플릿 세부 정보를 검토하고 **Next**를 클릭합니다.

8 Accept EULAs 화면에서 라이센스 계약을 읽고 **Accept**를 클릭한 후 **Next**를 클릭합니다.

9 Select name and folder 화면에서 어플라이언스 이름을 입력하고 구축할 폴더 또는 데이터 센터를 클릭한 후 **Next**를 클릭합니다.

10 어플라이언스에 대한 호스트를 선택하고 **Next**를 클릭합니다.

11 가상 디스크 형식(자세한 내용은 "씬(thin) 또는 일반(thick) 프로비저닝 디스크 선택이 미치는 영향", 40페이지 참조)과 어플라이언스에 대한 스토리지 위치를 선택합니다. **Next**를 클릭합니다.

12 어플라이언스에 대한 Destination Network를 선택하고 **Next**를 클릭합니다.

13 Customize template에서 **Default Gateway, DNS, Network 1 IP Address, Network 1 Netmask**를 지정합니다. IP 주소가 올바른지 확인합니다. 이 대화상자에서 잘못된 IP 주소를 설정하면 .ova를 다시 배포해야 합니다. **Next**를 클릭합니다.

참고 vSphere Data Protection 어플라이언스는 DHCP를 지원하지 않습니다. 어플라이언스는 정적 IP 주소가 필요합니다.

14 Ready to complete 화면에서 모든 구축 옵션이 올바른지 확인한 다음 **Finish**를 클릭합니다.

vCenter가 vSphere Data Protection 어플라이언스를 구축합니다. **Recent Tasks**를 모니터링하여 구축이 완료되는 시점을 확인합니다.

vSphere Data Protection 설치 및 구성

사전 요구 사항

vSphere Data Protection .ovf 템플릿("OVF 템플릿 배포", 14페이지 참조)이 성공적으로 배포되어야 하고, 사용자는 vSphere Web Client에서 vCenter Server에 로그인해야 합니다.

절차

1 **vCenter Home > vCenter > VMs and Templates**를 선택합니다. vCenter 트리를 확장하고 vSphere Data Protection 어플라이언스를 선택합니다. 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Power On**을 선택합니다.

2 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Open Console**을 선택합니다.

3 설치 파일이 로드되면 vSphere Data Protection 메뉴에 대한 시작 화면이 나타납니다. 웹 브라우저를 열고 다음을 입력합니다.

https://<*VDP 어플라이언스의 IP 주소*>:8543/vdp-configure/

4 VMware 로그인 화면에서 다음을 입력합니다.

a 사용자: **root**

b 암호: **changeme**

c **로그인**을 클릭합니다.

5 시작 화면이 나타납니다. **다음**을 클릭합니다.

6 네트워크 설정 대화상자가 나타납니다. 다음을 지정 또는 확인합니다.

a IPv4 정적 주소

b 넷마스크

c 게이트웨이

d 기본 DNS

e 보조 DNS

f 호스트 이름

g 도메인

7 **다음**을 클릭합니다.

8 시간대 대화상자가 나타납니다. 해당 시간대를 선택한 후 **다음**을 클릭합니다.

9 vSphere Data Protection 자격 증명 대화상자가 나타납니다. vSphere Data Protection 자격 증명을 어플라이언스 암호에 입력합니다. 이는 범용 구성 암호입니다. 다음을 포함하는 암호를 지정합니다.

- 9자
- 대문자 1개 이상
- 소문자 1개 이상
- 숫자 1개 이상
- 특수 문자는 포함할 수 없음

10 **다음**을 클릭합니다.

11 vCenter 등록 대화상자가 나타납니다. 다음을 지정합니다.

a vCenter 사용자 이름(사용자가 도메인 계정에 속하는 경우 "SYSTEM-DOMAIN\admin" 형식으로 입력해야 합니다.)

b vCenter 암호

c vCenter 호스트 이름(IP 주소 또는 FQDN)

d vCenter 포트

e SSO 호스트 이름(IP 주소 또는 FQDN)

f SSO 포트

12 **연결 테스트**를 클릭합니다.

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

"지정된 사용자가 VDP 전용 사용자가 아니거나 VDP를 관리할 vCenter 권한이 부족합니다. 사용자 역할을 업데이트하고 다시 시도하십시오"라는 메시지가 나타나면 "사용자 계정 구성", 14페이지으로 이동하여 사용자 역할 업데이트 방법에 대한 지침을 참조하십시오.

13 **확인**을 클릭합니다.

14 **다음**을 클릭합니다.

15 완료 준비 페이지가 나타납니다. **마침**을 클릭합니다.

16 구성이 완료되었다는 메시지가 나타납니다. **확인**을 클릭합니다.

이제 vSphere Data Protection 어플라이언스 구성이 완료되었지만 vSphere Web Client로 돌아가서 어플라이언스를 재부팅해야 합니다. vSphere Web Client에서 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Restart Guest OS**를 선택합니다. Confirm Restart 메시지에서 **Yes**를 클릭합니다. 재부팅하는 데 최대 30분 정도 걸릴 수 있습니다.

설치 후 구성

vSphere Data Protection을 설치하는 동안 구성 유틸리티를 처음 실행하면 "설치" 모드에서 실행됩니다. 이 모드에서는 초기 네트워킹 설정, 시간대, 어플라이언스 암호 및 vCenter 자격 증명을 입력할 수 있습니다. 초기 설치 후 VDP-configure 유틸리티가 "유지 보수" 모드에서 실행되고 다른 사용자 인터페이스가 표시됩니다.

VDP-configure에 액세스하려면 웹 브라우저를 열고 다음을 입력하십시오.

https://*<VDP 어플라이언스의 IP 주소>*:8543/vdp-configure/

유지 보수 인터페이스의 용도는 다음과 같습니다.

- 상태 보기 - 어플라이언스에서 현재 실행 중인 또는 현재 중지된 서비스를 확인할 수 있습니다.
- 서비스 시작 및 중지 - 어플라이언스에서 선택한 서비스를 시작 및 중지할 수 있습니다.
- 로그 수집 중 - 어플라이언스에서 현재 로그를 다운로드할 수 있습니다.
- vSphere Data Protection 구성 확인 또는 변경 - 네트워크 설정 확인 또는 변경, vCenter 등록 구성, 시스템 설정(시간대 정보 및 vSphere Data Protection 자격 증명) 확인 또는 편집 등을 수행할 수 있습니다.
- 어플라이언스 롤백 - 어플라이언스를 이전에 알려진 유효한 상태로 복구할 수 있습니다. ("체크포인트 및 롤백 사용", 34페이지 참조)
- 업그레이드 - vSphere Data Protection 어플라이언스에서 ISO 이미지를 업그레이드할 수 있습니다.

상태 탭

상태 탭은 vSphere Data Protection 서비스를 보거나, 중지하거나 시작하는 데 사용합니다.

상태 옵션 관리

상태 탭의 왼쪽 화면에는 vSphere Data Protection 어플라이언스에서 실행되는 주요 서비스의 상태가 표시됩니다. 다음 서비스의 상태가 표시됩니다.

표 2-2. vSphere Data Protection 어플라이언스에서 실행 중인 서비스에 대한 설명

서비스	설명
핵심 서비스	어플라이언스 백업 엔진을 구성하는 서비스입니다. 이 서비스가 비활성화되면 예약된 또는 "요청 시" 백업 작업이 실행되지 않고 복구 작업을 시작할 수 없습니다.
관리 서비스	관리 서비스는 기술 지원 서비스의 지시에 따라서만 중지해야 합니다.
파일 시스템 서비스	파일 레벨 복구 작업을 위해 백업을 마운트할 수 있는 서비스입니다.
파일 레벨 복구 서비스	파일 레벨 복구 작업의 관리를 지원하는 서비스입니다.
유지 보수 서비스	백업 보존 기간이 만료되었는지 여부를 평가하는 등 유지 보수 작업을 수행하는 서비스입니다. vSphere Data Protection 어플라이언스가 운영되는 처음 24-48시간 동안 유지 보수 서비스는 비활성화됩니다. 따라서 초기 백업을 완료하기 위해 추가 시간이 할당됩니다.
백업 스케줄러	백업 스케줄러는 예약된 백업 작업을 시작하는 서비스입니다. 이 서비스가 중지되면 예약된 백업은 실행되지 않지만 "요청 시" 백업은 시작할 수 있습니다.

이 서비스를 위해 표시되는 상태는 다음과 같습니다.

- 시작 중
- 시작 실패
- 실행 중
- 중지 중
- 중지 실패
- 중지됨
- 로드 중(가져오는 중)

- 복구 불가능(핵심 서비스만 해당)
- 복구 중(관리 서비스만 해당)
- 복구 실패(관리 서비스만 해당)

서비스 시작 및 중지

상태 화면에서 **시작**을 클릭하여 중지된 서비스를 시작하거나 **중지**를 클릭하여 실행 중인 서비스를 중지할 수 있습니다. 그러나 일반적으로 실행 중인 서비스를 중지할 때는 기술 지원 서비스의 지시에 따라야 합니다.

서비스가 중지되면 **시작**을 클릭하여 재시작하도록 시도할 수 있지만 일부 경우 서비스를 제대로 작동하기 위해서는 추가 문제 해결 단계가 필요합니다.

로그 파일 수집

로그 파일 번들을 사용하면 vSphere Data Protection 어플라이언스의 로그를 지원 담당자에게 쉽게 전송할 수 있습니다. **로그 수집**을 클릭하면 vSphere Data Protection 서비스에서 모든 로그를 "로그 번들"로 다운로드할 수 있습니다. 표시된 "다른 이름으로 저장" 대화상자를 사용하여 웹 브라우저가 실행 중인 컴퓨터의 파일 시스템에 로그 번들을 다운로드할 수 있습니다. 로그 번들의 이름은 LogBundle.zip입니다.

구성 탭

구성 탭은 vSphere Data Protection 구성을 보거나 편집하는 데 사용합니다.

다음과 같은 vSphere Data Protection 구성을 보거나 편집할 수 있습니다.

- 네트워크 설정
  - IP 주소
  - 넷마스크
  - 게이트웨이
  - 기본 DNS
  - 보조 DNS
  - 호스트 이름
  - 도메인
- vCenter 등록
  - vCenter 사용자 이름
  - vCenter 암호
  - vCenter 호스트 이름
  - vCenter 포트
  - SSO 호스트 이름
  - SSO 포트
- 시스템 설정
  - 시간대
  - VDP 자격 증명(VDP 암호 변경)

롤백 탭

롤백 탭은 vSphere Data Protection 데이터가 손상된 경우에 알려진 체크포인트로 롤백하는 데 사용합니다.

참고 롤백 사용에 대해서는 "체크포인트 및 롤백 사용", 34페이지에서 다룹니다.

업그레이드 탭

업그레이드 탭은 vSphere Data Protection 어플라이언스에서 ISO 이미지를 업데이트하는 데 사용합니다.

참고 업그레이드 수행에 대해서는 "VDP-configure 사용", 19페이지에서 다룹니다.

VDP-configure 사용

VDP-configure는 설치 후 구성에 사용합니다.

사전 요구 사항

vSphere Data Protection 어플라이언스를 설치 및 구성하고 vSphere Data Protection 관리 계정으로 로그인해야 합니다.

절차

1 웹 브라우저를 열고 다음을 입력합니다.

https://*<VDP 어플라이언스의 IP 주소>*:8543/vdp-configure/

2 VMware 로그인 화면에서 다음을 입력합니다.

a 사용자: **root**

b 암호: ***VDP 암호***

c **로그인**을 클릭합니다.

3 (선택 사항) vSphere Data Protection 서비스를 보려면 **상태** 탭을 클릭합니다. vSphere Data Protection 서비스를 중지 또는 시작하려면 관련 중지 또는 시작 버튼을 클릭합니다.

4 (VMware 지원 서비스에서 요청하는 경우 선택 사항) 지원 로그 파일을 생성하려면 **상태** 탭을 클릭한 다음 **로그 수집** 버튼을 클릭합니다. 로그 번들 파일을 저장하고 VMware 지원 서비스의 지침에 따라 파일을 제출합니다.

5 (선택 사항) vSphere Data Protection 구성을 보거나 편집하려면 **상태** 탭을 클릭합니다.

- 네트워크 설정에 대해 구성을 보거나 편집합니다. 구성을 변경한 경우 **저장** 버튼을 클릭합니다.
- vCenter 등록에서 설정을 편집할 수 있습니다. 설정을 편집하려면 잠금 아이콘을 클릭합니다. vCenter 등록 설정을 변경하는 경우 현재 백업 작업 설정이 유실되므로 백업 작업을 재구성해야 합니다. 변경한 경우 **저장** 버튼을 클릭합니다.
- 시스템 설정에서 시간대를 보거나 편집할 수 있습니다. 시간대를 변경한 경우 **저장** 버튼을 클릭합니다. **VDP 암호 변경** 버튼을 클릭하여 vSphere Data Protection 암호를 변경할 수 있습니다.

vSphere Data Protection 어플라이언스 업그레이드

업그레이드 프로세스는 다음과 같은 일반적인 단계로 구성됩니다.

1 vSphere Data Protection 어플라이언스 스냅샷 생성

2 업그레이드 설치

3 스냅샷 제거

참고 어플라이언스를 업그레이드한 후 vSphere Web Client에 처음으로 로그인할 때 vSphere Web Client에 vSphere Data Protection이 표시되지 않을 것입니다. 그러면 vSphere Web Client에서 로그아웃했다가 다시 로그인해야 합니다. 이후 로그인에서는 vSphere Data Protection이 표시될 것입니다.

사전 요구 사항

소프트웨어 업그레이드를 수행하려면 ISO 업그레이드 이미지를 다운로드하고 모든 vSphere Data Protection 서비스를 실행해야 합니다.

vSphere Data Protection 어플라이언스 스냅샷 생성

설치 시 vSphere Data Protection 어플라이언스에서 사용하는 가상 디스크는 "Independent - Persistent"로 설정됩니다. 그러나 스냅샷을 생성하려면 디스크를 일시적으로 "Dependent"로 변경해야 합니다.

vSphere Data Protection 어플라이언스 스냅샷을 생성하려면 다음과 같이 하십시오.

1 vSphere Web Client를 사용하여 vCenter Server에 하드웨어 설정을 편집하고 스냅샷을 생성할 권한이 있는 사용자로 로그인합니다.

2 **Hosts and Clusters**를 클릭합니다.

3 왼쪽 트리에서 vSphere Data Protection 어플라이언스가 표시될 때까지 펼치기 화살표를 클릭합니다.

4 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Shut Down Guest OS**를 선택합니다.

5 **Yes**를 클릭합니다. vSphere Data Protection 어플라이언스가 종료될 때까지 기다립니다. 이 작업은 몇 분 정도 소요될 수 있습니다.

6 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings**를 선택합니다.

7 하드 디스크 2부터 시작하여 펼치기 화살표를 클릭합니다.

8 가상 하드웨어 표의 디스크 모드 행에서 **Dependent**를 클릭합니다.

9 하드 디스크 3에서 계속하여 나머지 모든 디스크가 종속 모드로 설정될 때까지 8단계를 반복합니다.

10 **OK**를 클릭합니다.

11 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **All vCenter Actions > Snapshot> Take Snapshot**을 선택합니다.

12 스냅샷의 이름을 입력합니다. 설명(선택 사항)을 입력합니다. **OK**를 클릭합니다.

13 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Power On**을 선택합니다.

업그레이드 설치

1 vSphere Web Client를 사용하여 vCenter Server에 관리자로 로그인합니다.

2 **Hosts and Clusters**를 클릭합니다.

3 왼쪽 트리에서 vSphere Data Protection 어플라이언스가 표시될 때까지 펼치기 화살표를 클릭합니다.

4 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings**를 선택합니다.

5 Virtual Hardware 탭에서 CD/DVD 드라이브를 확장합니다. 드롭다운 메뉴에서 **Datastore ISO File**을 선택합니다.

6 Select File에서 ISO 이미지로 이동하여 선택합니다. **OK**를 클릭합니다.

7 데이터 저장소 ISO의 오른쪽에서 **Connected** 상자를 선택합니다. **OK**를 클릭합니다. ISO 파일의 크기에 따라 마운트하는 데 최대 5분 정도 걸릴 수 있습니다.

8 웹 브라우저를 열고 다음을 입력합니다.

https://<*VDP 어플라이언스의 IP 주소*>:8543/vdp-configure/

9 VMware 로그인 화면에서 다음을 입력합니다.

a 사용자: **root**

b 암호: ***VDP 암호***

c **로그인**을 클릭합니다.

10 **업그레이드** 탭을 클릭합니다. ISO 이미지를 사용할 수 있고 상태가 준비 상태인지 확인합니다. 그렇지 않은 경우 ISO 이미지가 계속 로드 중일 수 있습니다.

참고 ISO 이미지가 나타나지 않으면 VDP-configure에서 로그아웃한 후 다시 로그인합니다.

11 **VDP 업그레이드**를 클릭합니다. 업그레이드 설치가 시작됩니다. 업그레이드의 설치 부분은 시간이 오래 걸릴 수 있지만 상태 표시줄에 설치 진행 상태가 표시됩니다.

12 업그레이드가 성공적으로 설치되면 **확인**을 클릭합니다. vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Shut Down Guest OS**를 선택합니다.

스냅샷 제거

업그레이드가 성공적으로 완료된 후 스냅샷을 제거하는 것이 좋습니다.

스냅샷을 제거하려면 다음과 같이 하십시오.

1 vSphere Web Client를 사용하여 vCenter Server에 하드웨어 설정 편집 및 스냅샷 제거 권한이 있는 사용자로 로그인합니다.

2 **Hosts and Clusters**를 클릭합니다.

3 왼쪽 트리에서 vSphere Data Protection 어플라이언스가 표시될 때까지 펼치기 화살표를 클릭합니다.

4 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **All vCenter Actions > Snapshot > Snapshot Manager**를 선택합니다.

5 vSphere Data Protection 어플라이언스에 대해 생성한 스냅샷을 클릭합니다.

6 **Delete**를 클릭한 다음 **Yes**를 클릭합니다.

7 **Close**를 클릭합니다.

8 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings**를 선택합니다.

9 하드 디스크 2부터 시작하여 펼치기 화살표를 클릭합니다.

10 Virtual Hardware 표의 디스크 모드 행에서 **Independent - Persistent**를 클릭합니다.

11 하드 디스크 3에서 계속하여 나머지 모든 디스크가 Independent - Persistent 모드로 설정될 때까지 10단계를 반복합니다.

12 ISO 이미지의 마운트를 해제합니다. Virtual Hardware 탭에서 CD/DVD 드라이브를 확장합니다. 드롭다운 메뉴에서 Client Device를 선택합니다. **OK**를 클릭합니다.

13 **OK**를 클릭합니다.

14 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Power On**을 선택합니다.

15 재부팅이 완료되면 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings**를 선택합니다.

vSphere Data Protection 어플라이언스 업그레이드 프로세스가 완료되었습니다.

vSphere Data Protection 사용 3

vSphere Data Protection(VDP)을 설치 및 구성한 후 vSphere Data Protection용 vSphere Web Client를 통해 관리할 수 있습니다.

이 장에서 다루는 내용은 다음과 같습니다.

- "vSphere Data Protection 사용자 인터페이스 이해", 24페이지
- "vSphere Data Protection 액세스", 26페이지
- "vSphere Data Protection 어플라이언스 전환", 27페이지
- "백업 작업 생성", 27페이지
- "가상 머신 복구", 29페이지
- "보고서 보기", 30페이지
- "구성 관리", 31페이지
- "체크포인트 및 롤백 사용", 34페이지
- "파일 레벨 복구 사용", 35페이지
- "vSphere Data Protection 종료 및 시작 절차", 38페이지

vSphere Data Protection 사용자 인터페이스 이해

vSphere Data Protection용 vSphere Web Client는 vSphere Data Protection을 구성 및 관리하는 데 사용할 수 있는 새로운 사용자 인터페이스 요소를 제공합니다.

vSphere Data Protection 사용자 인터페이스는 다음 5개의 탭으로 구성됩니다.

- **시작** - vSphere Data Protection 기능에 대한 개요와 백업 작업 생성 마법사 및 복구 마법사로 바로 연결되는 링크를 제공합니다.
- **백업** - 예약된 백업 작업 목록과 각 백업 작업에 대한 세부 정보를 제공합니다. 이 페이지에서 백업 작업을 생성 및 편집할 수도 있습니다. 또한 이 페이지는 백업 작업을 즉시 실행할 수 있는 기능도 제공합니다.
- **복구** - 복구할 수 있는 성공적인 백업 목록을 제공합니다.
- **보고서** - vCenter의 가상 머신에 대한 백업 상태 보고서를 제공합니다.
- **구성** - vSphere Data Protection 구성 방식에 대한 정보를 표시하고 일부 설정을 편집할 수 있습니다.

각 탭은 다음 섹션에서 자세히 설명합니다.

시작 탭

시작 탭에서는 vSphere Data Protection에 대한 소개 정보와 일반적인 구성 작업을 시작하는 방법을 제공합니다.

표 3-1. 시작 탭

아이콘	이름	설명
	백업 작업 생성	백업 작업 마법사를 실행합니다. 자세한 내용은 "백업 작업 마법사 사용", 28페이지를 참조하십시오.
	가상 머신 복구	가상 머신 복구 마법사를 실행합니다. 자세한 내용은 "백업에서 가상 머신 복구", 29페이지를 참조하십시오.
	개요 보기	현재 보기를 보고서 탭으로 전환하여 기존 작업의 상태를 검토할 수 있는 화면을 제공합니다. 자세한 내용은 "보고서 보기", 30페이지를 참조하십시오.

백업 탭

백업 탭에는 기존 백업 작업과 그 상태에 대한 정보가 표시됩니다. 또한 임시 백업 작업을 생성, 편집, 삭제, 활성화/비활성화 및 실행하는 방법도 제공합니다.

표 3-2. 백업 탭 아이콘

아이콘	이름	설명
	새로 만들기	백업 작업 마법사를 실행합니다. 자세한 내용은 "백업 작업 마법사 사용", 28페이지 섹션을 참조하십시오.
	편집	백업 작업 마법사를 실행하여 기존 작업을 편집합니다.
	삭제	선택한 백업 작업을 삭제합니다.
	활성화/비활성화	백업 작업을 활성화 또는 비활성화 상태로 구성합니다.
	지금 백업	임시 백업을 실행합니다.

백업 탭에는 생성된 백업 작업 목록이 표시됩니다. 백업 작업은 표 형태로 나열되며 다음 정보가 포함됩니다.

표 3-3. 백업 작업 열 설명

열	설명
이름	백업 작업의 이름
상태	활성화됨 또는 비활성화됨입니다. 비활성화된 백업 작업은 실행되지 않습니다.
마지막 시작 시간	작업이 시작된 마지막 시간입니다.
기간	작업의 마지막 실행 시 소요된 시간입니다.
다음 실행 시간	작업이 다시 실행되도록 예약된 시간입니다.
성공 수	백업 작업이 마지막으로 실행되었을 때 성공적으로 백업된 VM의 수입니다.
실패 수	백업 작업이 마지막으로 실행되었을 때 성공적으로 백업되지 않은 VM의 수입니다.

복구 탭

복구 탭에는 vSphere Data Protection 어플라이언스로 백업된 VM 목록이 표시됩니다. 백업 목록을 이동하여 특정 백업을 선택 및 복구할 수 있습니다. 시간이 지나면서 복구 탭에는 오래된 정보가 표시될 수 있습니다. 복구할 수 있는 백업에 대한 최신 정보를 확인하려면 **새로 고침**을 클릭하십시오.

복구 탭에서는 다음 아이콘이 사용됩니다.

표 3-4. 복구 탭 아이콘

아이콘	이름	설명
	복구	백업에서 가상 머신 복구를 실행합니다. 이는 가상 머신을 선택한 복구 시점에 저장된 상태로 복구하는 방법을 구성합니다. 자세한 내용은 "백업에서 가상 머신 복구", 29페이지 섹션을 참조하십시오. 기본적으로 vSphere Data Protection은 백업 작업에 명시된 보존 정책에 따라 기존 복구 시점의 저장 및 삭제를 관리합니다.
	잠금/잠금 해제	잠금은 백업 작업의 만료 시점을 "종료 날짜 없음"으로 변경합니다.
	삭제	선택한 복구 시점이 삭제되도록 지정합니다.
	모든 선택 항목 지우기	복구 탭에서 모든 선택 항목을 지웁니다.

보고서 탭

보고서 탭은 vSphere Data Protection 어플라이언스와 가상 센터의 VM에 대한 개요 정보를 제공합니다.

구성 탭

구성 탭에서는 vSphere Data Protection 어플라이언스에 대한 유지 보수 작업을 관리할 수 있습니다.
이 탭에서는 다음 세 가지 작업을 수행할 수 있습니다.

- 백업 기간 보기 또는 편집("백업 기간 구성", 31페이지 참조)
- 무결성 검사 실행("수동으로 무결성 검사 실행", 33페이지 참조)
- e-메일 구성("e-메일 알림 구성", 33페이지 참조)

vSphere Data Protection 액세스

vSphere Data Protection은 vSphere Web Client를 통해 액세스합니다.

참고 vSphere Data Protection은 vSphere Web Client를 통해서만 관리합니다. vSphere Client는 vSphere Data Protection 관리를 지원하지 않습니다.

사전 요구 사항

vSphere Data Protection을 사용하려면 먼저 "vSphere Data Protection 설치 및 구성", 11페이지 섹션을 참조하여 vSphere Data Protection 어플라이언스를 설치 및 구성해야 합니다.

절차

1 웹 브라우저에서 vSphere Web Client에 액세스합니다.

https://*<vCenter Server의 IP 주소>*:9443/vsphere-client/

2 자격 증명 페이지에 vCenter 사용자 이름과 암호를 입력하고 **Login**을 클릭합니다.

vSphere Data Protection은 이 정보를 사용해 vCenter에 연결하여 백업을 수행하므로 지정된 사용자 계정에 관리 권한이 있어야 합니다.

3 vSphere Web Client에서 **vSphere Data Protection**을 선택합니다.

4 vSphere Data Protection 시작 페이지에서 vSphere Data Protection 어플라이언스를 선택하고 **연결**을 클릭합니다.

vSphere Data Protection 어플라이언스 전환

각 vCenter Server는 최대 10개의 vSphere Data Protection 어플라이언스를 지원합니다. 어플라이언스 전환 레이블의 오른쪽에 있는 드롭다운 목록에서 어플라이언스를 선택하여 어플라이언스를 전환할 수 있습니다.

참고 vSphere Data Protection 어플라이언스는 드롭다운 목록에 사전순으로 정렬되므로 화면에 표시되는 목록의 첫 번째 항목이 현재 어플라이언스와 일치하지 않을 수 있습니다. vSphere Data Protection 화면의 왼쪽에 있는 어플라이언스 이름은 현재 어플라이언스이고, 드롭다운 목록에 있는 어플라이언스 이름은 사용 가능한 어플라이언스 목록의 첫 번째 어플라이언스입니다.

백업 작업 생성

백업할 가상 머신, 백업 발생 빈도, 백업을 저장할 보존 기간 등이 포함된 백업 작업을 생성할 수 있습니다. vSphere Data Protection은 백업 기간을 사용하여 새로운 백업 및 보존 정책을 생성하거나 기존의 특정 백업을 제거합니다.

가상 머신

데이터 센터에 있는 모든 VM과 같이 VM 모음을 지정하거나 개별 VM을 선택할 수 있습니다. 전체 리소스 풀, 호스트, 데이터 센터 또는 폴더가 선택된 경우 해당 컨테이너에 있는 새로운 모든 VM은 후속 백업에 포함됩니다. VM이 선택된 경우 VM에 추가된 모든 디스크는 백업에 포함됩니다. VM이 선택된 컨테이너에서 선택되지 않은 다른 컨테이너로 이동된 경우 해당 VM은 더 이상 백업에 포함되지 않습니다.

백업할 VM을 수동으로 선택할 수 있습니다. 이렇게 하면 이동한 VM도 백업이 보장됩니다.

참고 vSphere Data Protection을 사용하여 vSphere Data Protection 어플라이언스를 백업하는 작업은 지원되지 않습니다.

스케줄

백업 스케줄은 선택 항목의 백업 빈도를 결정합니다. 백업은 백업 기간 시작 시점에 가능한 한 근접하여 발생합니다. 백업이 매일, 매주 또는 특정 날짜에 실행되도록 예약할 수 있습니다.

보존 정책

백업 보존 정책을 사용하여 시스템에 백업을 보존하는 기간을 지정할 수 있습니다.

보존 정책은 발생하는 각 백업에 할당됩니다. 백업 보존 기간이 만료되면 백업이 삭제됩니다.

표 3-5에서는 백업의 보존 정책에 대해 설명합니다.

표 3-5. 보존 정책 설정

보존 설정	설명
영구	백업을 영구 보존할 수 있습니다. 이 설정은 이 보존 정책이 할당된 모든 백업이 시스템 수명 동안 보존되도록 하는 데 유용합니다.
기간 (보존 기간)	고정 보존 기간을 백업이 수행된 후 며칠, 몇 주, 몇 개월 또는 몇 년으로 정의할 수 있습니다. 예를 들어, 백업이 6개월 후에 만료되도록 지정할 수 있습니다.
만료일 (종료일)	특정 날짜를 만료 날짜로 지정할 수 있습니다. 예를 들어, 백업이 2013년 12월 31일에 만료되도록 지정할 수 있습니다.
기간 (다음 스케줄)	고정 보존 기간을 며칠, 몇 주, 몇 개월 또는 몇 년으로 정의할 수 있습니다. 예를 들어, 백업이 30일, 52주, 12개월, 2년 동안 유지되도록 지정할 수 있습니다.

완료 준비

백업 작업에 대한 설정을 검토합니다. 이 페이지에서는 다음과 같은 정보를 제공합니다.

- 백업 작업의 이름
- 이 작업으로 백업할 가상 머신
- 가상 머신 백업 스케줄
- 백업에 선택된 보존 정책

백업 작업 마법사 사용

백업 작업 마법사를 사용하면 백업할 가상 머신과 백업 발생 시기를 지정할 수 있습니다.

절차

1. vSphere Web Client에서 **vSphere Data Protection**을 선택합니다.
2. vSphere Data Protection 시작 페이지에서 vSphere Data Protection 어플라이언스를 선택하고 **연결**을 클릭합니다.
3. **백업** 탭을 클릭하고 **새로 만들기**를 클릭하여 백업 작업 마법사를 실행합니다.
4. 가상 머신 페이지에서 개별 가상 머신 또는 백업할 가상 머신이 포함된 컨테이너를 선택하고 **다음**을 클릭합니다.
5. 스케줄 페이지에서 작업에 대한 백업 스케줄을 선택하고 **다음**을 클릭합니다.
6. 보존 정책 페이지에서 기본 보존 정책을 적용하거나 대체 보존 정책을 지정하고 **다음**을 클릭합니다.
7. 이름 페이지에서 백업 작업 이름을 입력하고 **다음**을 클릭합니다.
8. 완료 준비 페이지에서 백업 작업에 대한 요약 정보를 검토하고 **마침**을 클릭합니다.
9. 정보 대화상자에서 백업 작업이 성공적으로 생성되었는지 확인합니다. **확인**을 클릭합니다.

지금 백업

백업 작업이 생성되면 지금 백업 아이콘을 사용하여 백업 작업을 수동으로 시작할 수 있습니다.

사전 요구 사항

지금 백업 옵션을 사용하려면 먼저 vSphere Data Protection을 설치 및 구성하고 백업 작업이 하나 이상 있어야 합니다.

절차

1 vSphere Web Client에서 **vSphere Data Protection**을 선택합니다.

2 vSphere Data Protection 시작 페이지에서 vSphere Data Protection 어플라이언스를 선택하고 **연결**을 클릭합니다.

3 **백업** 탭을 클릭하고 백업 작업을 선택합니다. **지금 백업**을 클릭하고 모든 소스 백업 또는 기간이 경과된 소스만 백업을 선택합니다.

- 모든 소스 백업은 모든 작업이 백업되도록 지정합니다.
- 기간이 경과된 소스만 백업은 마지막 백업 시도에서 실패한 백업 작업을 지정합니다.

가상 머신 복구

가상 머신 복구 마법사를 사용하면 복구할 가상 머신, 복구 방법 및 복구 위치를 지정할 수 있습니다.

주의 복구하는 VM에 스냅샷이 포함되어 있는 경우 복구가 실패합니다. 따라서 복구 프로세스를 시작하기 전에 VM에서 스냅샷을 제거하십시오.

백업 선택

백업 선택은 복구할 가상 머신을 지정합니다. 복구는 백업 작업 생성과 유사하므로 가상 머신의 컨테이너 또는 특정 가상 머신을 지정할 수 있습니다. 가상 머신을 다른 위치로 복구할 수도 있습니다.

복구 옵션 설정

복구 옵션 설정은 백업이 복구되는 위치를 지정합니다.

다음과 같이 지정할 수 있습니다.

- 백업을 원래 위치에 복구
- 백업을 다른 위치에 복구
  - 새 이름
  - 대상
  - 데이터 저장소 위치

가상 머신의 클론을 생성하려면 복구하는 가상 머신의 이름을 변경하십시오.

완료 준비

복구 작업에 대한 설정을 검토합니다. 요약에는 복구할 VM 수, 생성할 VM 수 등과 같은 정보가 포함됩니다.

백업에서 가상 머신 복구

가상 머신 복구 마법사를 사용하여 가상 머신을 이전 백업 상태로 복구합니다.

사전 요구 사항

가상 머신을 복구하려면 먼저 vSphere Data Protection을 구성하고 복구할 백업이 하나 이상 있어야 합니다.

절차

1 vSphere Web Client에서 **vSphere Data Protection**을 선택합니다.

2 vSphere Data Protection 시작 페이지에서 vSphere Data Protection 어플라이언스를 선택하고 **연결**을 클릭합니다.

3 **복구** 탭을 클릭하고 **복구** 버튼을 클릭합니다.

4 가상 머신 복구 마법사가 나타납니다.

5 백업 선택 페이지에서 가상 머신을 복구할 소스를 지정하고 **다음**을 클릭합니다.

6 VM에 하나 이상의 백업 시점이 있는 경우 복구 대상이 아닌 모든 시점의 선택을 취소합니다. 백업 시점은 하나만 선택해야 합니다.

7 복구 설정 페이지에서 클라이언트 복구 시점 및 백업 복구 시점이 올바른지 확인합니다. 원래 위치로 복구를 선택할 수도 있고 원래 위치로 복구 확인란 선택을 취소하고 다른 대상 및 데이터 저장소를 지정하여 다른 위치로 복구할 수도 있습니다. **다음**을 클릭합니다.

8 완료 준비 페이지에서 구성을 검토하고 **마침**을 클릭합니다.

가상 머신이 마법사에 지정된 대로 복구됩니다.

복구 작업 진행률 보기

복구 작업이 시작되면 최근 작업 창에서 현재 복구 프로세스를 확인할 수 있습니다.

백업 작업 잠금

잠금 아이콘은 백업 작업 만료 시점을 "종료 날짜 없음"으로 변경하는 데 사용합니다. 이렇게 하면 백업 작업을 수동으로 만료할 수 없고 만료 날짜가 지나도 자동으로 삭제되지도 않습니다. 그러나 잠금 옵션을 사용해도 백업 작업이 삭제되는 것을 막을 수는 없습니다. 즉, 관리자가 잠금 설정된 작업을 수동으로 삭제할 수 있기 때문입니다. 백업 작업을 잠그려면 복구 탭에서 백업 작업을 선택하고 잠금 아이콘을 클릭하십시오. 잠긴 백업 작업에는 백업 작업 이름의 왼쪽에 노란색 자물쇠가 표시됩니다.

보고서 보기

보고서 탭에는 다음에 대한 현재 상태가 표시됩니다.

- 어플라이언스 상태
- 사용한 용량
- 무결성 검사 상태
- 최근에 성공한 백업
- 최근에 실패한 백업

보고서 탭의 필터링

기본적으로 보고서 탭에는 vCenter Server와 관련된 모든 가상 머신이 표시됩니다. 보고서 탭의 필터 옵션은 다음을 기준으로 필터링합니다.

- 모두 표시
- 가상 머신
  - 이름
  - 상태
  - 마지막으로 성공한 백업
- 마지막 백업 작업
  - 이름
  - 상태
  - 날짜

구성 관리

구성 탭은 구성 정보를 확인하고 수정하는 데 사용합니다. 이 섹션에서는 다음 내용을 다룹니다.

- "백업 어플라이언스 세부 정보 확인 및 편집", 31페이지
- "백업 기간 구성", 31페이지
- "유지 보수 기간 설정 변경", 33페이지
- "수동으로 무결성 검사 실행", 33페이지
- "e-메일 알림 구성", 33페이지

구성 탭을 통해 백업 어플라이언스 세부 정보, 스토리지 개요 및 백업 기간 구성을 볼 수 있습니다.

백업 어플라이언스 세부 정보 확인 및 편집

백업 어플라이언스 세부 정보에는 다음 정보가 포함됩니다.

- IP 주소
- VDP 어플라이언스 버전
- 상태
- vCenter Server
- 현재 사용자
- 현지 시간
- 시간대
- 가용 공간
- 중복 제거된 크기
- 중복 제거되지 않은 크기

참고 스토리지 용량의 단위는 GiB(GB와는 다름)로 이는 1024MB를 말합니다.

백업 기간 구성

하루 24시간은 3개의 운영 기간(백업, 블랙아웃 및 유지 보수)으로 나뉩니다. 이러한 기간 동안 다양한 시스템 작업이 수행됩니다.

백업 기간

백업 기간은 하루 중 정상적인 예약된 백업을 수행하도록 할당된 시간입니다.

- 운영에 미치는 영향 - 기본적으로 백업 기간에는 유지 보수 작업이 수행되지 않습니다.
- 기본 설정 - 기본 백업 기간은 로컬 서버 시간으로 오후 8시에 시작되어 다음 날 아침 8시까지 12시간 동안 중단 없이 계속됩니다.
- 사용자 지정 - 특정 사이트 요구 사항에 맞게 백업 기간 시작 시간 및 기간을 지정할 수 있습니다.

vSphere Data Protection은 백업 기간 동안 하루에 한 번 각 가상 머신을 백업하려고 시도합니다. 백업은 백업 기간 시작과 동시에 시작되며 최대 8개의 백업 작업을 한 번에 실행할 수 있습니다.

참고 여러 vSphere Data Protection 어플라이언스가 동일한 가상 머신을 백업하는 경우 백업 기간을 조정하여 다른 어플라이언스의 백업 작업이 서로 겹치지 않도록 해야 합니다. 백업 작업이 겹치는 경우 백업이 실패합니다.

블랙아웃 기간

블랙아웃 기간은 하루 중 서버에 대한 무제한 액세스를 요구하는 가비지 수집과 같은 서버 유지 보수 작업을 수행하도록 할당된 시간입니다. 가비지 수집은 시스템에 저장된 모든 백업에서 더 이상 참조되지 않는 데이터의 고립된 청크를 삭제합니다.

- 운영에 미치는 영향 - 블랙아웃 기간에는 백업 또는 관리 작업이 허용되지 않습니다. 그러나 복구는 수행할 수 있습니다.
- 기본 설정 - 기본 블랙아웃 기간은 로컬 서버 시간으로 오전 8시에 시작되어 당일 오전 11시까지 3시간 동안 중단 없이 계속됩니다.
- 사용자 지정 - 특정 사이트 요구 사항에 맞게 블랙아웃 기간을 지정할 수 있습니다.

블랙아웃 기간을 변경하면 유지 보수 기간에도 영향을 줍니다. 예를 들어, 블랙아웃 기간을 3시간에서 2시간으로 변경하면 유지 보수 기간이 1시간 일찍 시간되어 1시간 늘어납니다. 그러나 백업 기간은 영향을 받지 않습니다.

유지 보수 기간

유지 보수 기간은 하루 중 무결성 검사 검증과 같은 일상적인 서버 유지 보수 작업을 수행하도록 할당된 시간입니다.

- 운영에 미치는 영향 - 짧은 기간 동안 백업 또는 관리 작업이 허용되지 않을 수 있습니다.

  유지 보수 기간 동안 백업을 시작할 수는 있지만, 그럴 경우 백업 및 유지 보수 작업에 영향을 줍니다. 이와 같은 이유로 유지 보수 기간 동안에는 모든 백업 또는 관리 작업을 최소화하십시오. 그러나 복구는 수행할 수 있습니다.

  무결성 검사 및 백업이 겹칠 수 있지만, 그럴 경우 입출력 리소스 경합이 발생하여 두 작업 모두 완료 시간이 길어지고 실패할 수도 있습니다.
- 기본 설정 - 기본 유지 보수 기간은 로컬 서버 시간으로 오전 11시에 시작되어 당일 오후 8시까지 9시간 동안 중단 없이 계속됩니다.
- 사용자 지정 - 유지 보수 기간은 직접 사용자 지정할 수는 없지만 시작 시간과 기간은 백업 및 블랙아웃 기간 설정에서 파생됩니다.

유지 보수 기간은 블랙아웃 기간 직후에 시작되며 백업 기간 시작 시간 전까지 계속됩니다.

무결성 검사

이 작업은 중복 제거 저장소의 데이터 무결성을 검증 및 유지하기 위해 수행합니다. vSphere Data Protection은 유지 보수 기간 동안 증가분 또는 전체 무결성 검사를 완료하도록 설계되었습니다. 증가분 무결성 검사는 가장 최근에 수행된 전체 또는 증가분 무결성 검사 이후 중복 제거 저장소에 추가된 체크포인트의 무결성을 검증합니다. 또한 vSphere Data Protection은 하루에 한 번 모든 체크포인트에 대한 무결성 검사를 수행하도록 설계되었습니다. 자세한 내용은 "체크포인트 및 롤백 사용", 34페이지 섹션을 참조하십시오.

유지 보수 기간을 사용할 때는 무결성 검사가 컴퓨팅 리소스를 소비하지 않도록 해야 합니다. 그렇지 않으면 진행 중인 백업 작업에 방해가 될 수 있습니다. 결과적으로 유지 보수 기간과 백업 기간은 서로 겹치지 않아야 합니다. 유지 보수는 정해진 기간 내에 완료되지 않을 경우 중지됩니다. 유지 보수가 중지되더라도 대상은 백업 및 복구와 같은 다른 작업에 대해 잠기지 않습니다. 다음 번에 대상 유지 보수 기간이 시작되면 중단된 부분부터 작업이 계속됩니다. 유지 보수 기간 구성에 대한 자세한 내용은 "유지 보수 기간 설정 변경", 33페이지 섹션을 참조하십시오.

또한 무결성 검사는 수동으로 시작할 수도 있습니다. 무결성 검사가 수동으로 시작되면 항상 전체 대상에 대한 전체 무결성 검사를 수행하고 유지 보수 기간을 사용하지 않습니다. 일반적으로 무결성 검사가 진행 중이어도 중복 제거 저장소에서의 백업 및 복구 작업이 허용됩니다. 복구 시점을 삭제하도록 수동으로 표시한 경우 무결성 검사가 진행되는 동안 백업은 허용되지 않지만 복구 작업은 허용됩니다. 무결성 검사가 진행되는 동안 중복 제거 저장소에서 손상된 복구 시점이 발견된 경우 손상된 복구 시점을 삭제하도록 표시한 후 수동 무결성 검사를 실행해야 합니다. 수동으로 실행한 무결성 검사가 진행되는 동안에는 백업 및 복구가 허용되지 않습니다. 무결성 검사를 수동으로 시작하는 방법에 대한 자세한 내용은 "수동으로 무결성 검사 실행", 33페이지 섹션을 참조하십시오.

vSphere Data Protection은 무결성 검사의 진행률에 대한 정보를 저장합니다. 결과적으로 vSphere Data Protection 어플라이언스가 무결성 검사를 중지하면 검사가 중지된 시점부터 프로세스를 재시작할 수 있습니다. 따라서 무결성 검사가 완료된 작업은 유실되지 않습니다. 어플라이언스는 유지 보수 기간이 지나면 무결성 검사를 중지합니다. 진행률을 추적하면 무결성 검사를 완료하는 데 도움이 됩니다. 사용자가 개입하여 수동으로 중지한 무결성 검사는 진행률 정보를 저장하지 않으므로, 그러한 중지 후 무결성 검사는 처음부터 다시 시작됩니다.

유지 보수 기간 설정 변경

구성 탭을 통해 유지 보수 기간 설정을 변경합니다.

사전 요구 사항

유지 보수 기간 설정을 변경하려면 먼저 vSphere Data Protection을 설치 및 구성해야 합니다.

절차

1 vSphere Web Client에서 **vSphere Data Protection**을 선택합니다.

2 vSphere Data Protection 시작 페이지에서 vSphere Data Protection 어플라이언스를 선택하고 **연결**을 클릭합니다.

3 **구성** 탭을 클릭합니다.

4 백업 기간 구성에서 **편집**을 클릭합니다.

5 백업 시작 시간, 백업 기간 및 블랙아웃 기간을 선택하고 **저장**을 클릭합니다.

수동으로 무결성 검사 실행

무결성 검사는 구성 탭에서 수동으로 실행할 수 있습니다.

사전 요구 사항

무결성 검사를 실행하려면 먼저 vSphere Data Protection을 구성해야 합니다.

절차

1 vSphere Web Client에서 **vSphere Data Protection**을 선택합니다.

2 vSphere Data Protection 시작 페이지에서 vSphere Data Protection 어플라이언스를 선택하고 **연결**을 클릭합니다.

3 **구성** 탭을 클릭합니다.

4 백업 기간 구성에서 설정 아이콘(구성 탭 오른쪽 상단)을 클릭하고 **무결성 검사 실행**을 클릭합니다.

5 확인 대화상자가 나타납니다. **예**를 클릭합니다.

e-메일 알림 구성

e-메일 알림이 활성화된 경우 다음 정보가 포함된 e-메일이 전송됩니다.

- VDP 어플라이언스 상태
- 백업 작업 요약
- 가상 머신 요약

사전 요구 사항

e-메일 보고서를 구성하려면 e-메일 계정이 있어야 합니다.

절차

1 vSphere Web Client에서 **vSphere Data Protection**을 선택합니다.

2 vSphere Data Protection 시작 페이지에서 vSphere Data Protection 어플라이언스를 선택하고 **연결**을 클릭합니다.

3 **구성** 탭을 클릭합니다.

4 **e-메일** 버튼을 클릭합니다.

5 화면 오른쪽 하단에 있는 **편집** 버튼을 클릭합니다.

6 다음을 지정합니다.

   a **e-메일 보고서 활성화**를 선택합니다.

   b **보내는 메일 서버**를 지정합니다.

   c (선택 사항) **서버 연결 시 로그인 필요**를 선택합니다. 이 옵션이 선택된 경우 관련 **사용자 이름** 및 **암호**를 지정합니다.

   d **보낸 사람 주소**를 지정합니다.

   e **받는 사람 주소**를 지정합니다.

   f **전송 일**을 지정합니다.

   g **보고서 로캘**을 선택합니다.

7 **저장** 버튼을 클릭합니다.

체크포인트 및 롤백 사용

체크포인트는 재해 복구를 지원할 명확한 목적으로 수행되는 시스템 전반에 걸친 백업입니다. 체크포인트는 "유지 보수 기간", 32페이지에서 설명하는 것처럼 유지 보수 기간 동안 하루에 한 번 예약 및 생성됩니다. vSphere Data Protection은 두 개의 체크포인트를 저장합니다(검증된 것과 검증되지 않은 것). 롤백은 검증된 체크포인트에 저장된 데이터를 사용하여 vSphere Data Protection 어플라이언스를 알려진 정상적인 상태로 복구하는 과정입니다. 기본적으로 유지 보수 서비스는 vSphere Data Protection 어플라이언스가 구축된 후 24-48시간 동안 비활성화됩니다. 따라서 초기 백업을 지원하기 위해 백업 기간이 길어질 수 있습니다.

예기치 않은 종료가 발생한 경우 어플라이언스는 재시작될 때 마지막으로 검증된 체크포인트로 롤백을 수행합니다. 이는 예상된 동작이며, 어플라이언스 손상을 방지하기 위해 사용됩니다.

어플라이언스가 구축될 때 임시 체크포인트가 생성됩니다. 이 체크포인트에는 설치 시점의 어플라이언스 설정이 포함됩니다. 어플라이언스가 구축된 후 처음 24-48시간 동안 예기치 않은 종료가 발생하면 어플라이언스는 임시 체크포인트로 롤백을 수행합니다. 임시 체크포인트 생성과 예기치 않은 종료 사이에 생성된 백업 작업 또는 백업은 유실됩니다. 이 기간 동안 체크포인트를 생성하려면 무결성 검사를 수동으로 실행하십시오. 자세한 내용은 "수동으로 무결성 검사 실행", 33페이지 섹션을 참조하십시오.

참고 롤백을 사용할 경우 선택한 체크포인트 이후에 발생한 모든 백업은 유실됩니다.

사전 요구 사항

롤백을 실행하려면 먼저 vSphere Data Protection을 설치 및 구성하고 체크포인트를 생성 및 검증해야 합니다.

주의 가장 최근에 검증된 체크포인트로만 롤백을 수행하는 것이 좋습니다.

절차

1 웹 브라우저를 열고 다음을 입력합니다.

http://<*VDP 어플라이언스의 IP 주소*>:8543/vdp-configure/

2 VMware 로그인 화면에서 다음을 입력합니다.

a 사용자: **root**

b 암호: ***VDP 암호***

c **로그인**을 클릭합니다.

3 롤백 **탭**을 클릭합니다.

4 **VDP 롤백을 활성화하도록 잠금 해제**를 클릭합니다.

5 경고 대화상자에 선택한 체크포인트 이후에 발생한 모든 백업은 유실된다는 경고가 표시됩니다. 허용 가능한 경우 vSphere Data Protection 어플라이언스 암호를 입력하고 **확인**을 클릭합니다.

6 검증된 체크포인트(valid=true)를 선택하고 **선택한 체크포인트로 VDP 롤백 수행**을 클릭합니다.

파일 레벨 복구 사용

vSphere Data Protection은 전체 가상 머신에 대한 백업을 생성합니다. 이러한 백업은 vSphere Data Protection용 vSphere Web Client를 사용하여 완전히 복구할 수 있습니다. 그러나 가상 머신의 특정 파일만 복구하려는 경우 vSphere Data Protection Restore Client를 사용하십시오.

복구 클라이언트를 사용하면 특정 가상 머신 백업을 파일 시스템으로 마운트한 다음, 이 파일 시스템을 검색하여 복구하려는 파일을 찾을 수 있습니다.

복구 클라이언트는 다음 두 가지 모드 중 하나의 모드로 작동합니다.

- 기본 - 로그인한 머신에서 생성한 백업만 마운트할 수 있고 복구한 파일은 모두 이 클라이언트로 복구됩니다.

  예를 들어, 이름이 "WS44"인 Windows 호스트에서 기본 모드로 복구 클라이언트에 로그인하면 "WS44"의 백업만 마운트하고 찾을 수 있습니다.

- 고급 - vSphere Data Protection에 포함된 모든 백업을 마운트하고 찾을 수 있습니다.

지정된 시간에 최대 8개의 백업을 마운트할 수 있습니다.

참고 파일 레벨 복구를 사용하여 파일을 복구하려면 복구 클라이언트에 연결할 가상 머신에 VMware 툴이 설치되어 있어야 합니다. VMware 툴이 설치되어 있는 가상 머신은 복구 클라이언트를 사용하여 VMware 툴이 설치되어 있지 않는 머신의 백업에서 파일을 복구할 수 있습니다. 그러나 VMware 툴이 없는 가상 머신은 복구 클라이언트를 사용해도 파일을 성공적으로 복구할 수 없습니다.

참고 복구 클라이언트는 VMware vSphere vMotion 또는 VMware vSphere Storage vMotion 사용을 지원하지 않습니다.

파일 레벨 복구 지원 구성:

파일 레벨 복구는 다음 파일 시스템의 백업에서 수행될 수 있습니다.

- NTFS(MBR 사용 기본 파티션)
- ext2(MBR 사용 기본 파티션)
- ext3(MBR 사용 기본 파티션)
- ext2 사용 LVM(MBR 사용 기본 파티션 및 독립 실행형 [MBR 없음] LVM(ext2 사용))
- ext3 사용 LVM(MBR 사용 기본 파티션 및 독립 실행형 [MBR 없음] LVM(ext3 사용))

파일 레벨 복구 제한 사항

파일 레벨 복구는 다음 가상 디스크 구성을 지원하지 않습니다.

- 포맷되지 않은 디스크
- 동적 디스크(Windows) / 멀티 드라이브 파티션(즉, 2개 이상의 가상 디스크로 구성된 파티션)
- GPT(GUID Partition Table) 디스크
- ext4 파일 시스템
- FAT16 파일 시스템
- FAT32 파일 시스템
- 확장 파티션
- 암호화된 파티션
- 압축된 파티션

파일 레벨 복구에는 또한 다음과 같은 제한 사항이 있습니다.

- 심볼 링크(Symbolic link)는 복구 또는 검색할 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.

다음 제한 사항은 LVM(Logical Volume Manager)에서 관리하는 논리적 볼륨에 적용됩니다.

- 한 개의 물리적 볼륨(.vmdk)은 정확하게 한 개의 논리적 볼륨에 매핑되어야 합니다.
- ext2와 ext3 형식만 지원됩니다.

로그인 옵션

다음 두 가지 방법 중 하나를 사용하여 vSphere Data Protection Restore Client에 로그인할 수 있습니다.

파일 레벨 복구 서비스는 백업을 vSphere Data Protection에서 관리하는 가상 머신에 대해서만 사용할 수 있습니다. 즉, vCenter 콘솔 또는 일부 다른 원격 연결을 통해 vSphere Data Protection에서 백업한 가상 머신 중 하나에 로그인해야 복구 클라이언트에 로그인할 수 있습니다.

기본 로그인

기본 로그인을 사용하여 연결하려면 먼저 vSphere Data Protection에서 백업한 가상 머신에서 복구 클라이언트에 연결해야 합니다. 로그인한 가상 머신의 로컬 관리자 자격 증명을 사용하여 복구 클라이언트에 로그인합니다. 복구 클라이언트는 로그인한 가상 머신에 대한 백업만 표시하고, 복구된 모든 파일은 현재 로그인한 가상 머신에 복구됩니다.

고급 로그인

고급 로그인을 사용하여 연결하려면 vSphere Data Protection에서 백업한 가상 머신에서 복구 클라이언트에 연결해야 합니다. 로그인한 가상 머신의 로컬 관리자 자격 증명 및 vCenter Server에 대한 관리자 자격 증명을 사용하여 복구 클라이언트에 로그인합니다 . 복구 클라이언트에 연결한 후 vSphere Data Protection에서 백업한 모든 가상 머신의 파일을 마운트하고 찾거나 복구할 수 있습니다. 복구된 모든 파일은 현재 로그인한 가상 머신에 복구됩니다.

기본 로그인 모드에서 복구 클라이언트 사용

Windows 또는 Linux 가상 머신에서 기본 로그인 모드로 복구 클라이언트를 사용하면 전체 가상 머신을 복구할 필요 없이 해당 머신에 대한 복구 시점에서 개별 파일에 액세스할 수 있습니다.

사전 요구 사항

vSphere Data Protection 백업을 수행하려면 먼저 VM에 VMware 툴이 설치되어 있어야 합니다. VMware 툴을 지원하는 운영 체제 목록은 VMware 웹 사이트를 참조하십시오.

복구 클라이언트에서 지원하는 디스크 유형은 다음과 같습니다.

- Windows(기본 디스크, 비확장): NTFS
- Linux (기본 디스크, 비확장): LVM, ext2, ext3

절차

1 원격 데스크톱 또는 vSphere Web Client를 사용하여 vSphere Data Protection을 통해 백업한 로컬 호스트에 액세스합니다.

2 다음을 통해 vSphere Data Protection Restore Client에 액세스합니다.

https://<*VDP 어플라이언스의 IP 주소*>:8543/flr

3 로컬 자격 증명 아래 자격 증명 페이지에서 로컬 호스트에 대한 **사용자 이름** 및 **암호**를 지정하고 **로그인**을 클릭합니다.

4 마운트된 백업 관리 대화상자가 나타납니다. 여기에는 액세스하는 클라이언트에 대한 모든 복구 시점이 나열됩니다. 복구할 마운트 시점을 선택하고 **마운트**를 클릭합니다.

5 마운트가 완료되면 드라이브 아이콘이 녹색 네트워크 드라이브로 나타납니다.

6 **닫기**를 클릭합니다.

7 마운트된 백업 창에서 복구할 폴더 및 파일을 탐색하여 선택합니다.

8 **선택한 파일 복구...**를 클릭합니다.

9 대상 선택 대화상자에서 복구할 드라이브 및 대상 폴더를 탐색하여 선택합니다.

10 **복구**를 클릭합니다.

11 복구 시작 확인 대화상자가 나타나면 **예**를 클릭합니다.

12 성공적으로 시작되었음을 알리는 대화상자가 나타나면 **확인**을 클릭합니다.

13 **복구 모니터링** 탭을 클릭하여 복구 상태를 확인합니다.

14 작업이 완료된 상태인지 확인합니다.

고급 로그인 모드에서 복구 클라이언트 사용

Windows 또는 Linux 가상 머신에서 고급 로그인 모드로 복구 클라이언트를 사용하면 vCenter Server에서 파일 레벨 복구를 수행할 복구 시점이 포함된 가상 머신에 액세스할 수 있습니다.

사전 요구 사항

백업을 수행하려면 먼저 VM에 VMware 툴이 설치되어 있어야 합니다. VMware 툴을 지원하는 운영 체제 목록은 VMware 웹 사이트를 참조하십시오.

복구 클라이언트에서 지원하는 디스크 유형은 다음과 같습니다.

- Windows(기본 디스크, 비확장): NTFS
- Linux (기본 디스크, 비확장): LVM, ext2, ext3

절차

1 원격 데스크톱 또는 vSphere Web Client를 사용하여 가상 머신에 액세스합니다.

2 다음을 통해 vSphere Data Protection Restore Client에 액세스합니다.

https://*<VDP 어플라이언스의 IP 주소>*:8543/flr

3 로컬 자격 증명 아래 자격 증명 페이지에서 로컬 호스트에 대한 **사용자 이름** 및 **암호**를 지정합니다. vCenter 자격 증명에서 vCenter 관리자의 **사용자 이름** 및 **암호**를 지정하고 **로그인**을 클릭합니다.

4 마운트된 백업 관리 대화상자가 나타납니다. 여기에는 액세스하는 클라이언트에 대한 모든 복구 시점이 나열됩니다. 복구할 마운트 시점을 선택하고 **마운트**를 클릭합니다.

5 마운트가 완료되면 드라이브 아이콘이 녹색 네트워크 드라이브로 나타납니다.

6 **닫기**를 클릭합니다.

7 마운트된 백업 창에서 복구할 가상 머신, 폴더 및 파일을 탐색하여 선택합니다.

8 **선택한 파일 복구...**를 클릭합니다.

9 대상 선택 대화상자에서 복구할 드라이브 및 대상 폴더를 탐색하여 선택합니다.

10 **복구**를 클릭합니다.

11 복구 시작 확인 대화상자가 나타나면 **예**를 클릭합니다.

12 성공적으로 시작되었음을 알리는 대화상자가 나타나면 **확인**을 클릭합니다.

복구가 완료되면 **복구 모니터링** 탭을 클릭하여 복구 상태를 확인할 수 있습니다.

vSphere Data Protection 종료 및 시작 절차

vSphere Data Protection 어플라이언스를 종료해야 하는 경우 **Shut Down Guest OS** 작업을 사용합니다. 이 작업을 사용하면 어플라이언스의 완전한 종료가 수행됩니다. 게스트 운영 체제 종료 작업 없이 어플라이언스의 전원을 끈 경우 손상이 발생할 수 있습니다. 어플라이언스가 종료된 후 **Power On** 작업을 통해 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 "체크포인트 및 롤백 사용", 34페이지 섹션을 참조하십시오.

중요 vSphere Data Protection 어플라이언스는 유지 보수 작업을 지원하고 복구 작업에 사용할 수 있도록 24x7 상시 실행되도록 설계되었습니다. 따라서 종료해야 할 특별한 이유가 없는 한 종료하지 않아야 합니다.

vSphere Data Protection 용량 관리

4

이 장에서는 vSphere Data Protection 용량 관리에 중점을 두며 다루는 내용은 다음과 같습니다.

- "씬(thin) 또는 일반(thick) 프로비저닝 디스크 선택이 미치는 영향", 40페이지
- "초기 vSphere Data Protection 구축에 스토리지 용량이 미치는 영향", 40페이지
- "vSphere Data Protection 용량 모니터링", 40페이지
- "vSphere Data Protection 용량 임계값", 41페이지
- "용량 관리", 41페이지

씬(thin) 또는 일반(thick) 프로비저닝 디스크 선택이 미치는 영향

vSphere Data Protection 데이터 저장소에 대한 씬(thin) 또는 일반(thick) 디스크 파티셔닝 선택에는 장점과 단점이 있습니다.

씬 프로비저닝은 가상화 기술을 사용하여 물리적으로 사용 가능한 것보다 더 많은 디스크 리소스가 사용 가능한 것으로 표시되도록 합니다. 이 기능은 관리자가 디스크 공간을 활발하게 모니터링하고 씬 디스크가 증가할 때 물리적 디스크 공간을 추가로 할당할 수 있는 경우 유용합니다. 그러나 관리가 이루어지지 않고 vSphere Data Protection 데이터 저장소가 공간을 할당할 수 없는 씬 프로비저닝 디스크에 있는 경우 vSphere Data Protection 어플라이언스에 장애가 발생합니다. 이때 검증된 체크포인트로 롤백을 수행할 수 있습니다(자세한 내용은 "체크포인트 및 롤백 사용", 34페이지 참조). 체크포인트 이후 발생한 백업은 모두 유실됩니다.

일반(thick) 프로비저닝은 디스크가 생성되면 모든 필요한 스토리지를 할당합니다. vSphere Data Protection 데이터 저장소에 대한 Best Practice는 신속한 구축이 가능하도록 vSphere Data Protection 어플라이언스를 구축할 때 씬 프로비저닝 디스크를 생성하고, 구축 후 디스크를 씬 프로비저닝에서 일반(thick) 프로비저닝으로 변환하는 것입니다.

다음은 씬 프로비저닝을 일반(thick) 프로비저닝으로 변환하는 절차입니다. 이 절차를 수행하기 위해서는 vSphere Data Protection 어플라이언스를 종료해야 하고 완료하는 데는 몇 시간이 소요될 수 있습니다.

사전 요구 사항

vSphere Data Protection 어플라이언스는 씬 프로비저닝을 사용하여 설치해야 합니다. 디스크를 일반(thick) 프로비저닝으로 늘릴 수 있는 충분한 디스크 공간이 있어야 합니다.

절차

1. vSphere Client에서 vSphere Data Protection 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **Shut Down Guest OS**를 선택합니다.
2. 어플라이언스를 강조 표시하고 **Summary** 탭을 선택합니다. **Storage** 섹션에서 데이터 저장소를 마우스 오른쪽 버튼으로 클릭하고 **Browse Datastore...**를 선택합니다.
3. 데이터 저장소 브라우저 화면에서 어플라이언스를 선택하고 관련 데이터 저장소를 확장합니다.
4. .vmdk 파일을 마우스 오른쪽 버튼으로 클릭하고 **Inflate**를 선택합니다.
5. 각 .vmdk 파일에 이 단계를 반복합니다.
   - 0.5TB VDP의 경우 3개의 .vmdk 파일이 있습니다.
   - 1TB VDP의 경우 7개의 .vmdk 파일이 있습니다.
   - 2TB VDP의 경우 13개의 .vmdk 파일이 있습니다.

초기 vSphere Data Protection 구축에 스토리지 용량이 미치는 영향

새로운 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 경우 vSphere Data Protection 중복 제거 기능이 가장 잘 활용됩니다.

따라서 초기 백업 후 후속 백업에서 어플라이언스에 백업되는 고유한 데이터는 더 줄어듭니다. 초기 백업이 완료되고 최대 보존 기간이 지나면 시스템이 유지 보수 기간 동안 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.

vSphere Data Protection 용량 모니터링

vSphere Data Protection 용량은 사전 예방적으로 모니터링해야 합니다. vSphere Data Protection 보고서 탭의 사용한 용량에서 vSphere Data Protection 용량을 확인할 수 있습니다.

vSphere Data Protection 용량 임계값

다음 표에서는 주요 용량 임계값에 대한 vSphere Data Protection 동작에 대해 설명합니다.

표 4-1. vSphere Data Protection 용량 임계값

임계값	값	동작
용량 경고	80%	vSphere Data Protection에서 경고 이벤트를 실행합니다.
상태 점검 한도	95%	기존 백업을 완료할 수 있지만 새 백업 작업은 일시 중단됩니다. vSphere Data Protection에서 경고 이벤트를 실행합니다.
서버 읽기 전용 한도	100%	vSphere Data Protection이 읽기 전용 모드로 전환되고 새로운 데이터가 허용되지 않습니다.

용량 관리

용량이 80%를 초과하면 다음의 용량 관리 지침을 사용해야 합니다.

- 새로운 VM을 백업 클라이언트로 추가하는 것을 중단
- 불필요한 백업 작업 삭제
- 보존 정책을 재평가하여 보존 정책을 줄일 수 있는지 확인
- vSphere Data Protection 어플라이언스 추가 고려 및 여러 개의 어플라이언스 간 백업 작업의 균형 유지

vSphere Data Protection 문제 해결

5

이 장에서는 다음과 같은 문제 해결 항목을 다룹니다.

- "vSphere Data Protection 어플라이언스 설치", 44페이지
- "vSphere Data Protection 백업", 44페이지
- "vSphere Data Protection 복구", 45페이지
- "파일 레벨 복구", 45페이지
- "vSphere Data Protection 보고", 46페이지

vSphere Data Protection 어플라이언스 설치

vSphere Data Protection 어플라이언스 설치 문제가 있는 경우 다음과 같이 하십시오.

- 모든 소프트웨어가 최소 소프트웨어 요구 사항("소프트웨어 요구 사항", 12페이지 참조)을 충족하는지 확인합니다.
- 하드웨어가 최소 하드웨어 요구 사항("시스템 요구 사항", 13페이지 참조)을 충족하는지 확인합니다.
- DNS가 vSphere Data Protection 어플라이언스에 맞게 제대로 구성되어 있는지 확인합니다 ("설치 전 구성", 13페이지 참조).

vSphere Data Protection 백업

다음은 vSphere Data Protection 백업에 대해 알려진 문제입니다.

"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 문제는 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 없습니다."

이 오류는 vApp 컨테이너 또는 ESX/ESXi 호스트에 중복된 호스트 이름이 있는 경우 발생할 수 있습니다. 이 경우 하나의 백업 작업만 추가됩니다. 모든 중복된 클라이언트 이름을 해결하십시오.

"다음 항목을 찾을 수 없어 선택하지 못했습니다."

이 오류는 백업 작업을 편집하는 동안 백업 대상 VM을 찾을 수 없는 경우 발생할 수 있습니다. 이는 알려진 문제입니다.

Windows 2008 R2 VM의 경우 "disk.EnableUUID"가 "true"로 구성되어 있으면 백업에 실패할 수 있습니다.

Windows 2008 R2 백업은 VM의 *disk.EnableUUID*가 *true*로 설정되어 있으면 실패할 수 있습니다. 이 문제를 해결하려면 vmx 구성 매개 변수 *disk.EnableUUID*를 *false*로 수동으로 업데이트할 수 있습니다.

vSphere Web Client를 사용하여 *disk.EnableUUID*를 *false*로 구성하려면 다음과 같이 하십시오.

1 해당 VM을 마우스 오른쪽 버튼으로 클릭하고 **Shut Down Guest OS**를 선택하여 VM을 종료합니다.

2 VM을 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings**를 선택합니다.

3 **VM Options**를 클릭합니다.

4 **Advanced** 섹션을 확장하고 **Edit Configuration**을 클릭합니다.

5 *disk.EnableUUID*라는 이름을 찾아 값을 *false*로 설정합니다.

6 **OK**를 클릭합니다.

7 **OK**를 클릭합니다.

8 해당 VM을 마우스 오른쪽 버튼으로 클릭하고 **Power On**을 클릭합니다.

구성 매개 변수를 업데이트한 후에는 Windows 2008 R2 VM의 백업이 성공할 것입니다.

vSphere Data Protection 데이터 저장소 용량이 충분하지 않은 경우 백업이 실패합니다.

vSphere Data Protection 데이터 저장소 용량이 충분하지 않은 경우 예약된 백업이 92% 완료된 상태에서 실패할 수 있습니다. vSphere Data Protection 데이터 저장소가 씬 프로비저닝으로 구성되고 최대 용량에 도달하지 않은 경우 스토리지 리소스를 추가하십시오. vSphere Data Protection 데이터 저장소가 일반(thick) 프로비저닝으로 구성되고 용량에 도달한 경우 "vSphere Data Protection 용량 관리", 39페이지 섹션을 참조하십시오.

VM에 VMware 내결함성이 활성화된 경우 백업이 실패합니다.

VM에 내결함성이 활성화된 경우 백업이 실패합니다. 이는 예상된 동작이며, vSphere Data Protection은 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.

예기치 않은 종료 후 최근의 백업 작업 및 백업이 유실됩니다.

언제든지 예기치 않은 종료가 발생하면 vSphere Data Protection 어플라이언스는 마지막으로 검증된 체크포인트로 롤백을 사용합니다. 이는 예상된 동작입니다. 자세한 내용은 "체크포인트 및 롤백 사용", 34페이지를 참조하십시오.

vSphere Data Protection 복구

다음은 vSphere Data Protection 복구에 대해 알려진 문제입니다.

복구 탭에 "백업을 로드하는 중" 메시지가 표시되고 로드 속도가 느려집니다.

각 백업을 복구 탭에서 로드하는 데 일반적으로 VM 백업당 2초가 소요됩니다. 이는 예상된 동작입니다.

VM에 관련 스냅샷이 있는 경우 원래 위치로 복구가 실패합니다.

VM에 관련 스냅샷이 있는 경우 원래 위치로 복구할 수 없습니다. 이는 예상된 동작이며, vSphere Data Protection는 원래 위치에 대한 스냅샷이 있는 VM에 대해서는 복구를 지원하지 않습니다. VM을 대체 위치로 복구하거나 원래 위치로 복구하기 전에 스냅샷을 삭제하십시오.

파일 레벨 복구

다음은 vSphere Data Protection Restore Client의 파일 레벨 복구 기능에 대해 알려진 문제입니다.

파일 레벨 복구 마운트 동안 VMDK 파일에 여러 파티션이 포함되어 있는 경우 마지막 파티션만 표시됩니다.

복구 클라이언트는 확장된 볼륨을 지원하지 않습니다. 이는 예상된 동작입니다. 이미지 레벨 복구를 수행하고 필요한 파일을 수동으로 복제하십시오.

파일 레벨 복구 마운트 동안 지원되지 않은 파티션을 마운트하지 못했습니다

다음 디스크 형식은 복구 클라이언트에서 지원하지 않으므로 이는 복구 클라이언트 마운트가 실패할 경우 예상되는 동작됩니다.

- 포맷되지 않은 디스크
- FAT32
- 확장 파티션
- 동적 디스크
- GPT 디스크
- Ext4 fs
- 암호화된 파티션
- 압축된 파티션

이미지 레벨 복구를 수행하고 필요한 파일을 수동으로 복제하십시오.

심볼 링크가 복구 클라이언트에 표시되지 않습니다.

복구 클라이언트는 심볼 링크 탐색을 지원하지 않습니다.

vSphere Data Protection 보고

다음은 vSphere Data Protection 보고에 대해 알려진 문제입니다.

복구 탭의 로드 또는 새로 고침 속도가 느려집니다.

많은 수의 VM이 있는 경우 복구 탭의 로드 또는 새로 고침 속도가 느려질 수 있습니다. 100개의 VM을 대상으로 테스트 시 최대 4시간 30분이 소요되었습니다.

vSphere Data Protection 포트 사용

6

vSphere Data Protection은 다음 표에 나열된 포트를 사용합니다.

표 6-1. vSphere Data Protection 포트 사용

포트	프로토콜	관련 서비스
22	TCP	ssh
80	TCP	http
111	TCP	rpcbind
443	TCP	https
700	TCP	Loginmgr 툴
5555	TCP	Postgres
5558	TCP	Postgres
7778	TCP	VDP RMI
7779	TCP	VDP RMI
8509	TCP	Tomcat AJP 커넥터
8543	TCP	Tomcat용 리디렉션
8580	TCP	VDP Downloader
9443	TCP	VDP 웹 서비스
25000	TCP/UDP	VDP 내부 통신
26000	TCP/UDP	VDP 내부 통신
27000	TCP	VDP 클라이언트 서버 통신
28001	TCP	VDP 내부 프록시
28002	TCP	VDP 내부 프록시
28003	TCP	VDP 내부 프록시
28004	TCP	VDP 내부 프록시
28005	TCP	VDP 내부 프록시
28006	TCP	VDP 내부 프록시
28007	TCP	VDP 내부 프록시
28008	TCP	VDP 내부 프록시
28009	TCP	VDP 내부 프록시
29000	TCP	VDP 내부 클라이언트 보안 통신
34250	TCP	ssl/soap gSoap(로컬 호스트)
53	UDP	DNS

표 6-1. vSphere Data Protection 포트 사용

포트	프로토콜	관련 서비스
111	UDP	RPC
941	UDP	RPC

7 vSphere Data Protection 재해 복구

vSphere Data Protection은 백업을 저장 및 관리할 수 있는 강력한 기능을 제공합니다. 장애 발생 시 가장 먼저 알려진 검증된 체크포인트로 롤백을 수행해야 합니다("체크포인트 및 롤백 사용", 34페이지 참조). vSphere Data Protection 어플라이언스 장애를 복구하려면 다음 절차에 따라 어플라이언스 백업 및 관련된 모든 vSphere Data Protection 백업을 생성하여 재해 복구 시 사용해야 합니다.

다음은 vSphere Data Protection 재해 복구 지침입니다.

1 vSphere Data Protection 어플라이언스를 종료하기 전에 실행 중인 백업 또는 유지 보수 작업이 없는지 확인합니다. 사용된 백업 방법과 소요 시간에 따라 예약된 작업이 없는 시간에 vSphere Data Protection 백업을 예약합니다. 예를 들어, 백업 기간이 8시간이고 백업 완료에 1시간이 소요되는 경우 유지 보수 작업 예약 전에 추가 7시간이 더 있는 것입니다. 이는 어플라이언스를 종료 및 백업하는 데 이상적인 시간입니다. 자세한 내용은 "백업 기간 구성", 31페이지 섹션을 참조하십시오.

2 vSphere Client에서 해당 플라이언스로 이동합니다. VM에서 게스트 운영 체제 종료를 수행합니다. 전원 끄기를 사용하지 마십시오. 전원 끄기 작업은 물리적 서버에서 플러그를 분리하는 것과 동일하며 완전히 종료되지 않을 수 있습니다. 자세한 내용은 "vSphere Data Protection 종료 및 시작 절차", 38페이지 섹션을 참조하십시오.

3 어플라이언스가 종료된 것으로 확인되면 선호하는 보호 방법을 사용하여 계속 진행합니다.

4 vSphere Data Protection 백업이 완료되고 vSphere Data Protection에 대해 수행되는 백업/스냅샷/복제 작업이 없는지 확인합니다.

5 vSphere Client에서 어플라이언스에 대한 전원 켜기를 수행합니다.

색인

C

CBT(Changed Block Tracking) **8**

D

DNS 구성 **13**

E

e- 메일 알림 **33**

F

FLR 고급 로그인 **36**
FLR 기본 로그인 **36**
FLR(파일 레벨 복구) **9**

O

OVF 템플릿 파일 **14**

V

vCenter 등록 **18**
VDP-configure 유틸리티 **17**
VMDK(가상 머신 디스크) **8**
VMware VADP(vStorage APIs for Data Protection) **8**
vSphere Data Protection 구성 **18**
vSphere Data Protection 사양 **13**
vSphere Data Protection 사이징 **12**
vSphere Data Protection 설치 **15**
vSphere Data Protection 스토리지 용량 **40**
vSphere Data Protection 시스템 설정 **18**
vSphere Data Protection 씬 (thin) 프로비저닝 디스크 **40**
vSphere Data Protection 아키텍처 **10**
vSphere Data Protection 암호 **18**
vSphere Data Protection 어플라이언스 **10**
vSphere Data Protection 어플라이언스 세부 정보 **31**
vSphere Data Protection 어플라이언스 정의 **8**
vSphere Data Protection 어플라이언스 종료 및 시작 **38**
vSphere Data Protection 일반 (thick) 프로비저닝 디스크 **40**
vSphere Data Protection 재해 복구 **49**

ㄱ

가변 길이 데이터 세그먼트 **9**
고정 길이 데이터 세그먼트 **9**
구성 탭 **31**
기술 지원 리소스 **5**
기업의 **9**

ㄷ

데이터 저장소 **8**

ㄹ

롤백 **34**

ㅁ

무결성 검사 **32**

ㅂ

백업 기간 **31**
백업 스케줄 **27**
백업 작업 **27**
백업 작업 마법사 **28**
백업 작업 잠금 **30**
백업 탭 **25**
보고서 탭 **30**
보존 정책 **27**
복구 마법사 **29**
복구 클라이언트 **35**
블랙아웃 기간 **32**

ㅅ

스냅샷
- 되돌리기 **21**
- 생성 **20**
- 제거 **21**

스냅샷으로 되돌리기 **21**
시스템 요구 사항 **13**
시작 탭 **24**

ㅇ

안정 상태의 용량 **40**
어플라이언스 스냅샷 생성 **20**
유지 보수 기간 **32**
이미지 레벨 백업 **8**

ㅈ

중복 제거 저장소 **9**
지금 백업 **28**

ㅊ

체크포인트 **34**

ㅍ

파일 레벨 복구 **35**
플랫폼 제품 지원 **8**
필터 옵션 **30**