



랜섬웨어 보호 문서

Ransomware Protection

NetApp
June 13, 2022

목차

랜섬웨어 보호 문서	1
랜섬웨어 차단 기능	2
2022년 6월 12일	2
2022년 5월 11일	2
2022년 3월 15일	2
2022년 2월 9일	3
시작하십시오	4
랜섬웨어 차단 에 대해 알아보십시오	4
랜섬웨어 차단 기능을 사용하십시오	6
데이터 원본에 대한 사이버 보안 권장 사항 관리	6
지식 및 지원	15
지원을 위해 등록하십시오	15
도움을 받으십시오	16
법적 고지	18
저작권	18
상표	18
특허	18
개인 정보 보호 정책	18
오픈 소스	18

랜섬웨어 보호 문서

랜섬웨어 차단기 새로운 기능

랜섬웨어 차단기 새로운 기능에 대해 알아보십시오.

2022년 6월 12일

이제 **ONTAP** 스토리지 **VM**에 대한 **NAS** 파일 시스템 감사 상태가 추적됩니다

작업 환경의 스토리지 VM 중 40% 미만에서 파일 시스템 감사가 활성화된 경우 **Cyber Resilience Map**에 경고가 추가됩니다. SMB 및 NFS 이벤트를 추적 및 로깅하지 않는 SVM의 정확한 수를 **ONTAP** 환경의 **패널**에서 감사 로그에 확인할 수 있습니다. 그런 다음 SVM에 대한 감사를 사용할지 여부를 결정할 수 있습니다.

이제 온박스 **Anti-Ransomware**가 볼륨에 대해 활성화되지 않은 경우 경고가 표시됩니다

이 정보는 이전에 **ONTAP Environments** **패널**의 온프레미스 **ONTAP** 시스템에 대해 보고되었습니다. 그러나 이제 온박스 **Anti-Ransomware** 기능이 볼륨의 40% 미만으로 켜지면 **Cyber Resilience Map**에서 경고가 보고되므로 대시보드에서 이 정보를 볼 수 있습니다.

이제 **ONTAP** 시스템용 **FSX**가 추적되어 볼륨 스냅샷을 활성화할 수 있습니다

ONTAP 환경의 **장** **패널**은 이제 **ONTAP** 시스템용 **FSx**의 볼륨에 대한 스냅샷 복사본의 상태를 제공합니다. 볼륨의 40% 미만이 스냅샷으로 보호되는 경우 **Cyber Resilience Map**에서도 경고가 표시됩니다.

2022년 5월 11일

ONTAP 환경의 보안 강화를 추적하는 새 **패널**.

ONTAP 환경의 새로운 **패널**은(는)에 따라 배포가 얼마나 안전한지 추적하는 **ONTAP** 시스템의 특정 설정 상태를 제공합니다. "**ONTAP 시스템에 대한 NetApp 보안 강화 가이드**를 참조하십시오"로 이동합니다. "**ONTAP의 랜섬웨어 방지 기능**" 비정상적인 활동을 사전에 감지하여 경고합니다.

권장사항을 검토한 후 잠재적 문제를 어떤 방식으로 해결할 것인지 결정할 수 있습니다. 다음 단계에 따라 클러스터의 설정을 변경하거나, 변경 사항을 다른 시간으로 연기하거나, 제안을 무시할 수 있습니다. "**자세한 내용을 보려면 여기를 클릭하십시오**".

클라우드 백업을 사용하여 다양한 범주의 데이터를 보호하는 방법을 보여주는 새로운 **패널**입니다.

이 새로운 **Backup Status** **패널**에서는 랜섬웨어 공격으로 인해 복구해야 할 경우 가장 중요한 데이터 범주가 얼마나 포괄적으로 백업되는지 보여 줍니다. 이 데이터는 환경에서 Cloud Backup에 의해 백업된 특정 범주의 항목 수를 시각적으로 나타냅니다. "**자세한 내용을 보려면 여기를 클릭하십시오**".

2022년 3월 15일

비즈니스 **Critical Data**의 사용 권한 상태를 추적할 수 있는 새 **패널**입니다

새로운 **PANEL_Business Critical data permissions analysis**는 비즈니스에 중요한 데이터의 사용 권한 상태를

표시합니다. 이를 통해 비즈니스 크리티컬 데이터를 얼마나 잘 보호하고 있는지 빠르게 평가할 수 있습니다. ["자세한 내용을 보려면 여기를 클릭하십시오"](#).

이제 사용 권한 열기 영역에 **OneDrive** 및 **SharePoint** 계정이 포함됩니다

이제 랜섬웨어 보호 대시보드의 개방형 권한 영역에 OneDrive 계정 및 SharePoint 계정에서 스캔되는 파일에 대한 사용 권한이 포함됩니다.

2022년 2월 9일

새로운 랜섬웨어 보호 서비스

새로운 랜섬웨어 보호 서비스를 통해 사이버 보안에 대한 관련 정보를 확인하고 데이터가 사이버 공격에 얼마나 복원되는지 평가할 수 있습니다. 또한 알림 목록과 데이터 보안 개선을 위한 해결 방법도 제공합니다.

["이 새로운 서비스에 대해 자세히 알아보십시오"](#).

시작하십시오

랜섬웨어 차단 에 대해 알아보십시오

랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. 랜섬웨어 보호 서비스를 통해 사이버 보안에 대한 관련 정보를 보고 사이버 공격에 대한 조직의 복원력을 평가할 수 있습니다. 또한 알림 목록과 데이터 보안 개선을 위한 해결 방법도 제공합니다.

"랜섬웨어 차단 의 사용 사례에 대해 알아보십시오".



랜섬웨어 보호 서비스는 현재 베타 버전입니다.

피처

랜섬웨어 차단 기능은 단일 가시성 및 제어 지점을 제공하여 다양한 작업 환경과 인프라 계층에서 데이터 보안을 관리 및 세분화하여 위협이 발생했을 때 보다 효과적으로 대응할 수 있도록 지원합니다. 현재 사이버 스토리지 보호 작업에 도움이 되는 여러 기능을 제공하고 있습니다. 향후 추가 기능이 추가될 예정입니다. 현재 기능은 다음과 같은 경우에 식별합니다.

- 작업 환경의 볼륨은 정기적인 Snapshot 복사본을 만들어 보호되지 않습니다.
- 를 사용하여 클라우드에 백업을 생성하면 작업 환경의 볼륨이 보호되지 않습니다 "[클라우드 백업](#)".
- 작업 환경 및 데이터 소스의 데이터는 를 사용하여 스캔되지 않습니다 "[클라우드 데이터 감지](#)" 규정 준수 및 개인 정보 보호에 대한 우려 사항을 파악하고 최적화 기회를 찾습니다.

이 기능은 랜섬웨어 보호 관점에서도 중요합니다. 중요한(비즈니스에 중요한) 데이터의 위치를 더 잘 이해하여 보호에 집중할 수 있기 때문입니다.

- 랜섬웨어 공격으로 인해 복구해야 할 경우 가장 중요한 범주의 데이터가 백업되지 않습니다.
- 작업 환경 또는 데이터 소스에서 암호화된 파일의 비율이 비정상적으로 증가했습니다.

이는 네트워크에서 랜섬웨어 공격이 시작했다는 것을 나타내는 지표가 될 수 있습니다.

- 파일에서 중요한 데이터가 검색되고 작업 환경 또는 데이터 소스에서 액세스 권한 수준이 너무 높습니다.
- 사용자가 Active Directory 도메인 관리자 그룹에 추가되었습니다.
- 클러스터의 ONTAP 소프트웨어 버전은 오래되었으며 최상의 보호 및 보안 기능을 제공하도록 업데이트해야 합니다.
- ONTAP 시스템에서 NAS 파일 시스템 감사가 설정되지 않았습니다.

CIFS 감사를 설정하면 시스템 관리자가 폴더 권한 변경, 파일 읽기 또는 쓰기 실패, 파일 생성, 수정 또는 삭제 시기 등의 정보를 추적하는 감사 이벤트가 생성됩니다.

- 온박스 안티 랜섬웨어 기능은 ONTAP 시스템에서 지원되지 않습니다.

ONTAP의 랜섬웨어 방지 기능은 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하여 경고합니다.

"랜섬웨어 보호 대시보드에서 이러한 잠재적인 문제를 확인하는 방법을 알아보십시오."

Cloud Volumes ONTAP 시스템을 사용할 경우 작업 환경에서 직접 배포할 수 있는 몇 가지 추가적인 랜섬웨어 보호 기능이 있습니다. ["랜섬웨어에 대한 보호를 강화하는 방법을 알아보십시오"](#).

지원되는 작업 환경 및 데이터 소스

"클라우드 데이터 감지" 랜섬웨어 보호 서비스를 이용하려면 사전 요구사항이 있어야 합니다. Data Sense를 설치 및 활성화한 후 랜섬웨어 Protection을 사용하여 다음 유형의 작업 환경 및 데이터 소스에 대한 사이버 공격에 데이터가 얼마나 복원되는지 확인할 수 있습니다.

- 작업 환경: *
 - Cloud Volumes ONTAP(AWS, Azure 또는 GCP에 구축)
 - 온프레미스 ONTAP 클러스터
 - Azure NetApp Files
 - ONTAP용 Amazon FSx
 - Amazon S3
- 데이터 소스: *
 - 비 NetApp 파일 공유
 - 오브젝트 스토리지(S3 프로토콜 사용)
 - 데이터베이스(Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA, SQL Server)
 - OneDrive 계정
 - SharePoint 계정
 - Google Drive 계정

또한 랜섬웨어 차단 기능은 글로벌 Active Directory 구성이 있는 경우 모니터링하기도 합니다 ["클라우드 데이터 센스에서 구성했습니다"](#).

랜섬웨어 차단의 작동 방식

고수준에서 랜섬웨어 차단은 다음과 같이 작동합니다.

1. 랜섬웨어 방지 기능은 스토리지 시스템, Cloud Data Sense, Cloud Backup 및 기타 Cloud Manager 리소스에서 정보를 수집하여 랜섬웨어 보호 대시보드를 채웁니다.
2. 랜섬웨어 보호 대시보드를 사용하여 시스템의 보호 기능을 대략적으로 파악할 수 있습니다.
3. 제공된 보고 툴을 사용하여 사이버 스토리지 보호 노력을 지원할 수 있습니다.

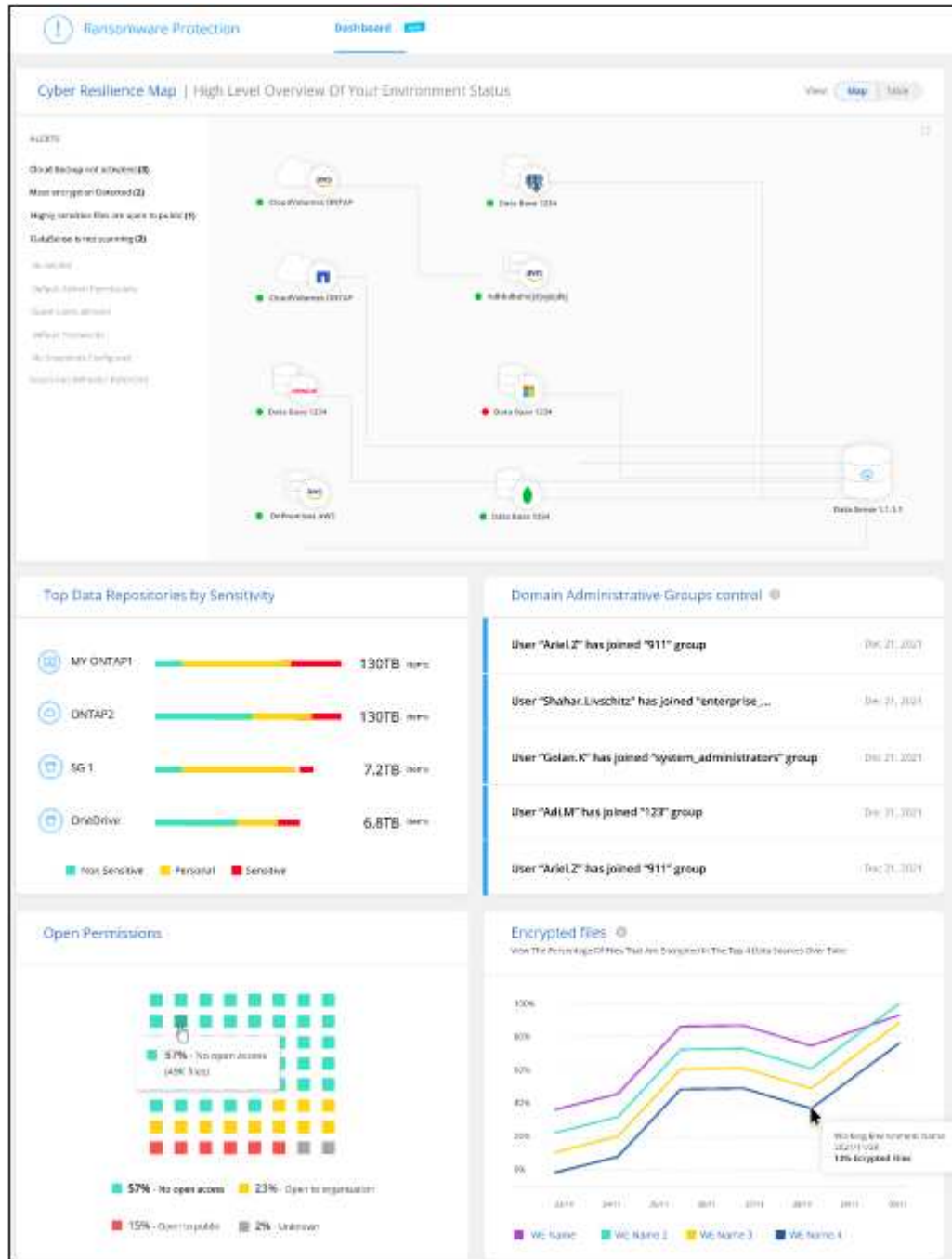
비용

Beta 기간 중에는 랜섬웨어 보호 서비스에 별도의 비용이 들지 않습니다.

랜섬웨어 차단 기능을 사용하십시오

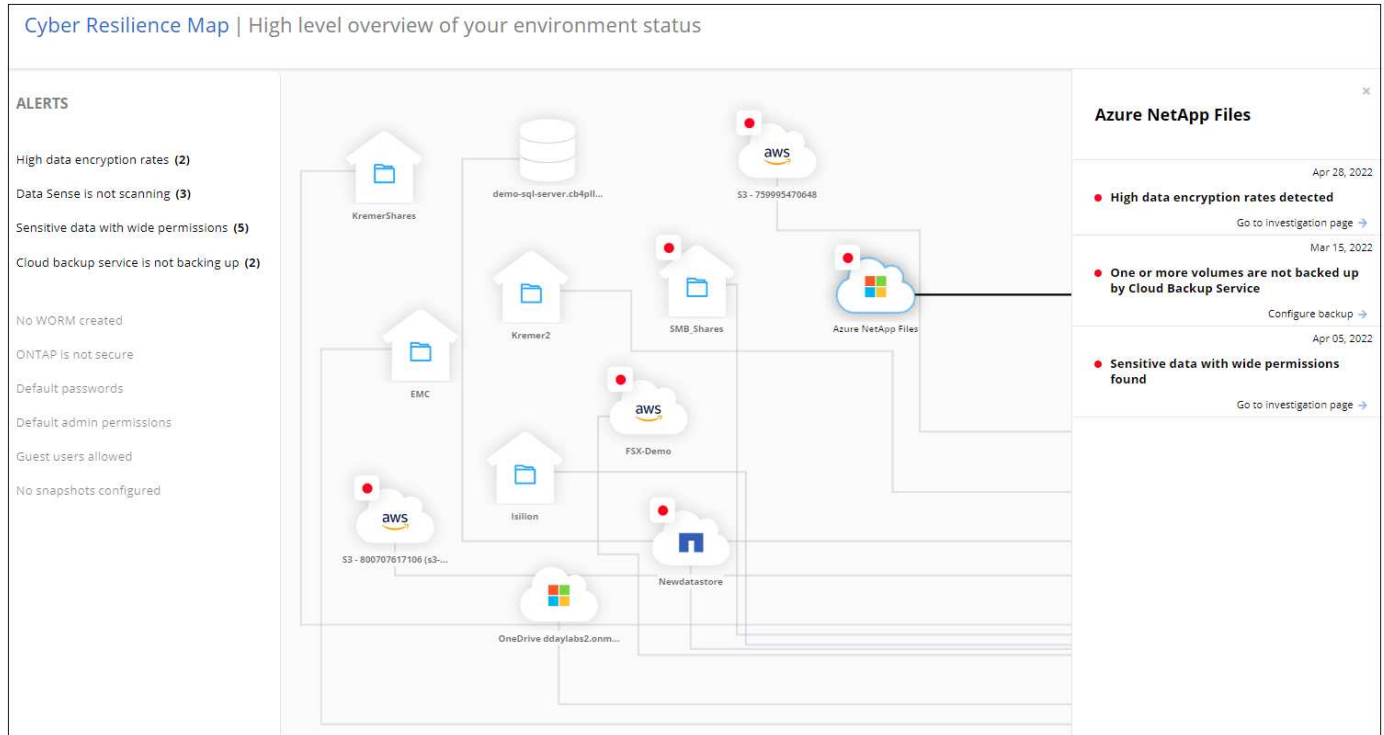
데이터 원본에 대한 사이버 보안 권장 사항 관리

Cloud Manager 랜섬웨어 보호 대시보드를 사용하여 모든 작업 환경 및 데이터 소스의 사이버 탄력성에 대한 개요를 볼 수 있습니다. 각 영역을 드릴다운하여 자세한 내용과 가능한 해결 방법을 찾을 수 있습니다.



사이버 복원력 맵

Cyber Resilience Map은 대시보드의 주요 영역입니다. 이를 통해 모든 작업 환경과 데이터 소스를 시각적으로 확인하고 관련 사이버 복원력 정보를 볼 수 있습니다.



이 맵은 다음 세 부분으로 구성됩니다.

왼쪽 패널

모든 데이터 소스에서 서비스가 모니터링 중인 알림 목록을 표시합니다. 또한 사용자 환경에서 활성화된 각 특정 경고의 수도 표시됩니다. 많은 유형의 경고가 있는 경우 이러한 경고를 먼저 해결하기 위한 좋은 이유가 될 수 있습니다.

가운데 패널

모든 데이터 소스, 서비스 및 Active Directory를 그래픽 형식으로 표시합니다. 건강한 환경에는 녹색 표시기가 있고 경고가 있는 환경에는 빨간색 표시기가 있습니다.

오른쪽 패널

빨간색 표시기가 있는 데이터 원본을 클릭하면 이 패널에 해당 데이터 원본에 대한 경고가 표시되고 경고 해결을 위한 권장 사항이 제공됩니다. 가장 최근 경고가 먼저 나열되도록 경고가 정렬됩니다. 많은 권장 사항으로 인해 문제를 해결할 수 있는 다른 Cloud Manager 서비스로 안내됩니다.

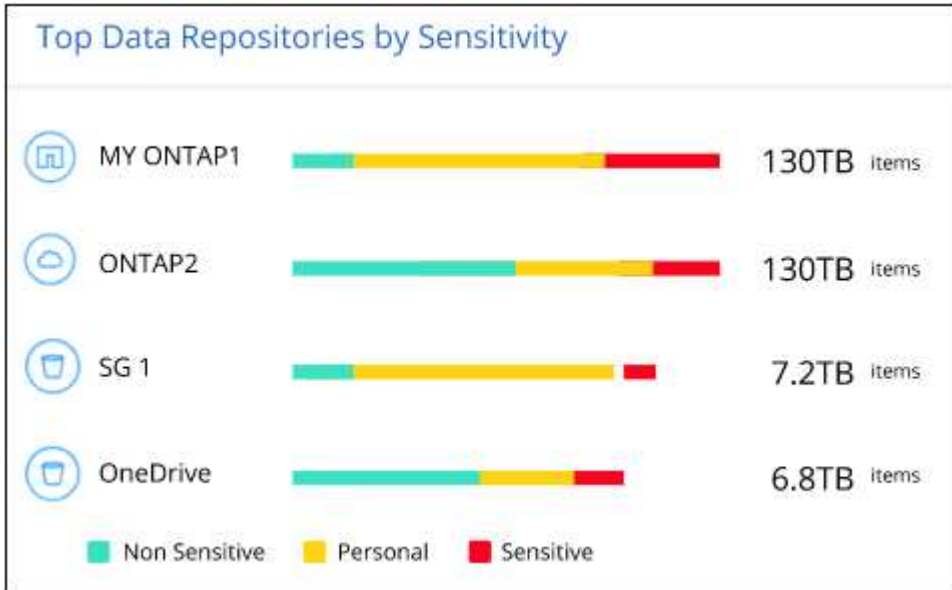
현재 추적된 알림 및 권장 해결 방법은 다음과 같습니다.

경고	설명	해결
높은 데이터 암호화 속도가 감지되었습니다	데이터 소스에서 암호화된 파일 또는 손상된 파일의 비율이 비정상적으로 증가했습니다. 즉, 지난 7일 동안 암호화된 파일의 비율이 20% 이상 증가했습니다. 예를 들어 파일의 50%가 암호화되면 이 숫자가 60%로 증가하게 됩니다.	링크를 클릭하여 을 시작합니다 "데이터 감지 조사 페이지" . 여기서 Specific_Working Environment_and_Category(암호화 및 손상) _의 필터를 선택하여 모든 암호화 및 손상된 파일의 목록을 볼 수 있습니다.
광범위한 권한이 있는 중요한 데이터가 발견되었습니다	파일에서 중요한 데이터가 검색되고 데이터 소스에서 액세스 권한 수준이 너무 높습니다.	링크를 클릭하여 을 시작합니다 "데이터 감지 조사 페이지" . 여기에서 특정_작업 환경_,민감도 수준(민감한 개인) 및 _열기 권한 _에 대한 필터를 선택하여 이 문제가 있는 파일 목록을 볼 수 있습니다.
Cloud Backup을 사용하여 하나 이상의 볼륨이 백업되지 않습니다	작업 환경의 일부 볼륨이 을(를) 사용하여 보호되고 있지 않습니다 "클라우드 백업" .	링크를 클릭하여 Cloud Backup을 시작한 다음 작업 환경에서 백업하지 않는 볼륨을 식별하고 해당 볼륨에 대해 백업을 설정할 것인지 결정할 수 있습니다.
데이터 소스에 있는 하나 이상의 저장소(볼륨, 버킷 등)가 데이터 센스에 의해 스캔되지 않습니다	데이터 원본의 일부 데이터가 을(를) 사용하여 스캔되지 않습니다 "클라우드 데이터 감지" 규정 준수 및 개인 정보 보호 문제를 식별하고 최적화 기회를 찾습니다.	링크를 클릭하여 데이터 센스를 시작하고 스캔하지 않는 항목에 대한 스캐닝 및 매핑을 활성화합니다.
온박스 앤티 랜섬웨어는 일부 볼륨에 대해 활성화되지 않습니다	온프레미스 ONTAP 시스템의 일부 볼륨에 이 없습니다 "NetApp의 랜섬웨어 방지 기능" 활성화됨.	링크를 클릭하면 로 리디렉션됩니다 ONTAP 환경 패널을 강화합니다 문제가 있는 작업 환경으로 이동합니다. 문제 해결 방법을 확인할 수 있습니다.
ONTAP 버전이 업데이트되지 않았습니다	클러스터에 설치된 ONTAP 소프트웨어 버전이 의 권장 사항을 따르지 않습니다 "ONTAP 시스템에 대한 NetApp 보안 강화 가이드를 참조하십시오" .	링크를 클릭하면 로 리디렉션됩니다 ONTAP 환경 패널을 강화합니다 문제가 있는 작업 환경으로 이동합니다. 문제 해결 방법을 확인할 수 있습니다.
일부 볼륨에 대해 스냅샷이 구성되지 않았습니다	작업 환경의 일부 볼륨은 볼륨 스냅샷을 생성하여 보호되지 않습니다.	링크를 클릭하면 로 리디렉션됩니다 ONTAP 환경 패널을 강화합니다 문제가 있는 작업 환경으로 이동합니다. 문제 해결 방법을 확인할 수 있습니다.
모든 SVM에 대해 파일 운영 감사가 활성화되어 있지 않습니다	작업 환경의 일부 스토리지 VM에는 파일 시스템 감사가 설정되어 있지 않습니다. 파일의 사용자 작업을 추적할 수 있도록 하는 것이 좋습니다.	링크를 클릭하면 로 리디렉션됩니다 ONTAP 환경 패널을 강화합니다 문제가 있는 작업 환경으로 이동합니다. SVM에서 NAS 감사를 활성화해야 하는지 여부를 조사할 수 있습니다.

데이터 민감도에 따른 상위 데이터 저장소

Sensitivity Level을 통한 상위 데이터 리포지토리 _ 패널에는 가장 중요한 항목이 포함된 상위 4개의 데이터 저장소 (작업 환경 및 데이터 소스)가 나열됩니다. 각 작업 환경의 막대 차트는 다음과 같이 구분됩니다.

- 중요하지 않은 데이터입니다
- 개인 데이터
- 민감한 개인 데이터



각 섹션 위로 마우스를 가져가면 각 범주의 총 항목 수를 볼 수 있습니다.

각 영역을 클릭하면 데이터 감지 조사 페이지에서 필터링된 결과를 볼 수 있으므로 더 자세히 조사할 수 있습니다.

도메인 관리자 그룹 제어

도메인 관리자 그룹 제어 패널에는 도메인 관리자 그룹에 추가된 최신 사용자가 표시되어 모든 사용자가 해당 그룹에서 허용되는지 확인할 수 있습니다. 이(가) 있어야 합니다 "[글로벌 Active Directory 통합](#)" 클라우드 데이터 센스로 들어가 이 패널이 활성화되도록 합니다.

Domain Administrative Groups control ⓘ	
User "Ariel.Z" has joined "911" group	Dec 21, 2021
User "Shahar.Livschitz" has joined "enterprise_..."	Dec 21, 2021
User "Golan.K" has joined "system_administrators" group	Dec 21, 2021
User "Adi.M" has joined "123" group	Dec 21, 2021

기본 관리 그룹에는 "관리자", "도메인 관리자", "엔터프라이즈 관리자", "엔터프라이즈 키 관리자" 및 "키 관리자"가 포함됩니다.

열려 있는 권한 유형에 따라 데이터가 나열됩니다

Open Permissions_패널은 스캔되는 모든 파일에 대해 존재하는 각 권한 유형의 백분율을 표시합니다. 차트는 데이터 센스에서 제공되며 다음과 같은 유형의 권한을 보여 줍니다.

- 개방 액세스 없음
- 조직에 열기
- 공개
- 알 수 없는 액세스

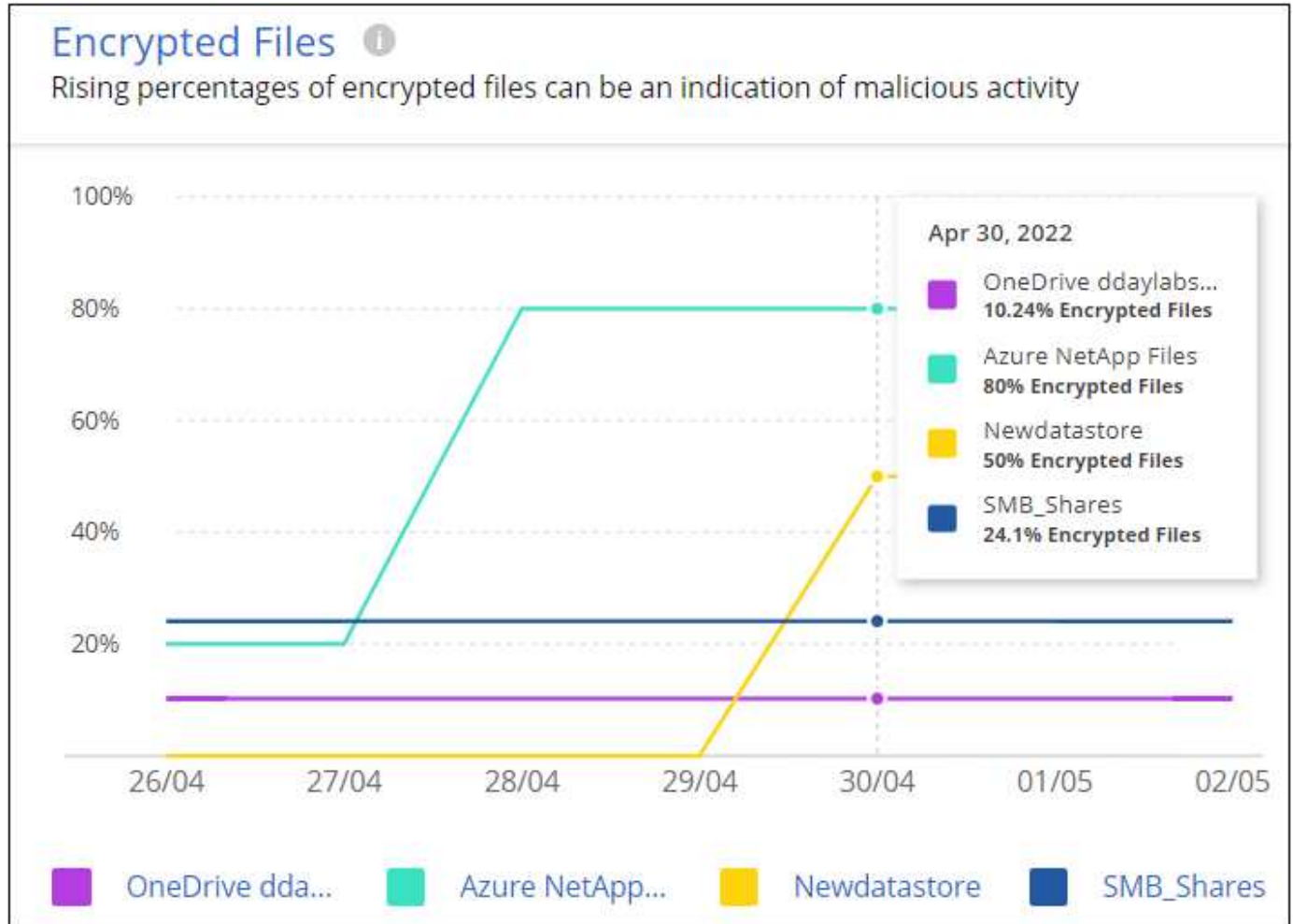


각 섹션 위로 마우스를 가져가면 각 범주의 파일 백분율 및 총 개수를 볼 수 있습니다.

각 영역을 클릭하면 데이터 감지 조사 페이지에서 필터링된 결과를 볼 수 있으므로 더 자세히 조사할 수 있습니다.

암호화된 파일에 의해 데이터가 나열됩니다

Encrypted Files 패널은 시간이 지남에 따라 암호화되는 파일의 비율이 가장 높은 상위 4개의 데이터 소스를 표시합니다. 일반적으로 암호로 보호된 항목입니다. 이를 위해 지난 7일 동안의 암호화 속도를 비교하여 어떤 데이터 소스가 20% 이상 증가하는지 확인합니다. 이 용량이 증가하면 랜섬웨어가 이미 시스템을 공격하게 됩니다.



데이터 소스 중 하나에 대한 행을 클릭하여 데이터 감지 조사 페이지에서 필터링된 결과를 보고 더 자세히 조사할 수 있습니다.




































ONTAP 시스템 강화 상태

ONTAP 환경 _패널 은(는) 에 따라 배포가 얼마나 안전한지 추적하는 ONTAP 시스템의 특정 설정 상태를 제공합니다. "ONTAP 시스템에 대한 NetApp 보안 강화 가이드 를 참조하십시오" 로 이동합니다. "ONTAP의 랜섬웨어 방지 기능" 비정상적인 활동을 사전에 감지하여 경고합니다.

권장사항을 검토한 후 잠재적 문제를 어떤 방식으로 해결할 것인지 결정할 수 있습니다. 다음 단계에 따라 클러스터의 설정을 변경하거나, 변경 사항을 다른 시간으로 연기하거나, 제안을 무시할 수 있습니다.

이 패널은 현재 NetApp ONTAP 시스템용 온프레미스 ONTAP, Cloud Volumes ONTAP 및 Amazon FSx를 지원합니다.

Harden your ONTAP environments

Working Environment	ONTAP Anti Ransomware ⓘ	NAS Auditing ⓘ	ONTAP Version ⓘ	Snapshots ⓘ	
MY ONTAP1					  
ONTAP2					  
AccOI_ONTAP					  
CVO828					  
FSx					  

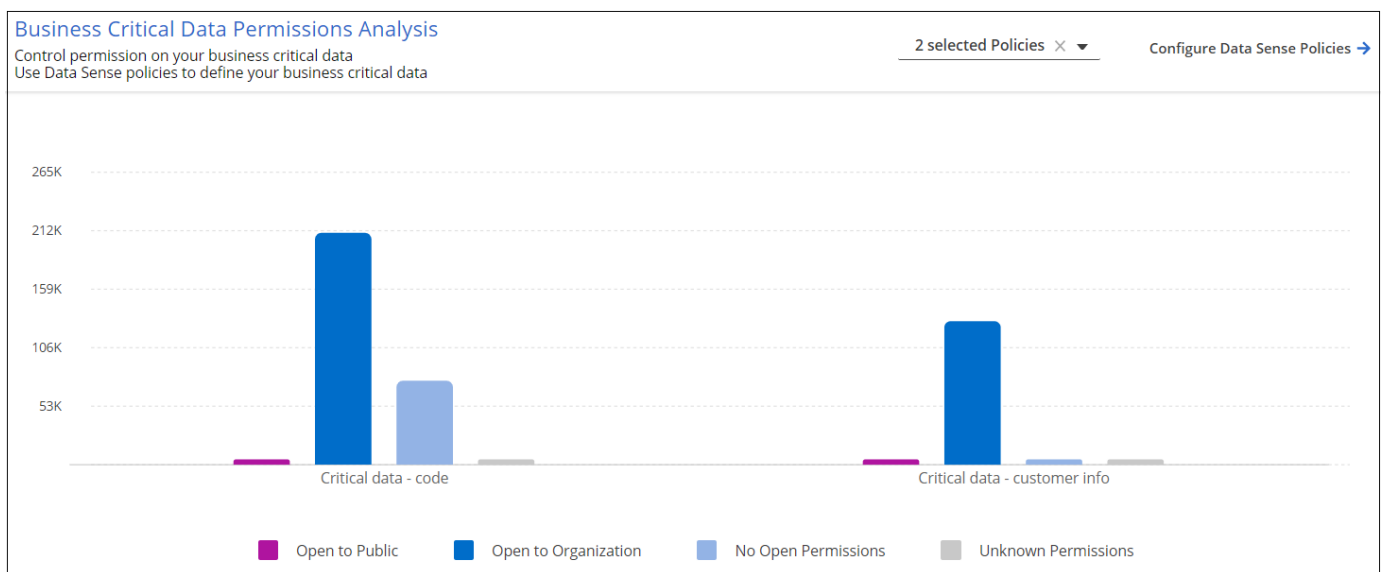
추적 중인 설정은 다음과 같습니다.

강화 목표	설명	해결
ONTAP의 랜섬웨어 방지 기술	온박스 안티 랜섬웨어가 활성화된 볼륨의 비율입니다. 사내 ONTAP 시스템에만 적용됩니다. 녹색 상태 아이콘은 볼륨의 85% 이상이 활성화되어 있음을 나타냅니다. 노란색은 40-85%가 활성화되었음을 나타냅니다. 빨간색은 40% 미만임을 나타냅니다.	"볼륨에서 안티 랜섬웨어를 활성화하는 방법을 확인하십시오" System Manager 사용:
NAS 감사	파일 시스템 감사가 설정된 스토리지 VM의 수입입니다. 녹색 상태 아이콘은 SVM의 85% 이상이 NAS 파일 시스템 감사를 설정했음을 나타냅니다. 노란색은 40-85%가 활성화되었음을 나타냅니다. 빨간색은 40% 미만임을 나타냅니다.	"SVM에서 NAS 감사를 사용하는 방법을 알아보십시오" CLI 사용
ONTAP 버전	클러스터에 설치된 ONTAP 소프트웨어의 버전입니다. 녹색 상태 아이콘은 버전이 현재 버전임을 나타냅니다. 노란색 아이콘은 클러스터가 1개 또는 2개의 패치 버전이나 온프레미스 시스템의 경우 1개의 부 버전 뒤이거나 Cloud Volumes ONTAP의 경우 1개의 주 버전 뒤임을 나타냅니다. 빨간색 아이콘은 클러스터가 3개의 패치 버전 또는 2개의 부 버전 또는 온프레미스 시스템의 경우 1개의 주 버전 또는 Cloud Volumes ONTAP의 경우 2개의 주 버전 뒤임을 나타냅니다.	"사내 클러스터를 업그레이드하는 가장 좋은 방법을 확인하십시오" 또는 "Cloud Volumes ONTAP 시스템".

강화 목표	설명	해결
스냅샷 수	데이터 볼륨에 대해 활성화된 스냅샷 기능과 스냅샷 복사본이 있는 볼륨의 비율은 얼마입니까? 녹색 상태 아이콘은 볼륨의 85% 이상이 스냅샷을 활성화했음을 나타냅니다. 노란색은 40-85%가 활성화되었음을 나타냅니다. 빨간색은 40% 미만임을 나타냅니다.	"온프레미스 클러스터에서 볼륨 스냅샷을 활성화하는 방법을 알아보십시오", 또는 "Cloud Volumes ONTAP 시스템에", 또는 "ONTAP 시스템용 FSx에서".

중요한 비즈니스 데이터에 대한 사용 권한의 상태입니다

비즈니스 크리티컬 데이터 권한 분석 패널은 비즈니스에 중요한 데이터의 사용 권한 상태를 표시합니다. 이를 통해 비즈니스 크리티컬 데이터를 얼마나 잘 보호하고 있는지 빠르게 평가할 수 있습니다.



처음에 이 패널은 선택한 기본 정책을 기반으로 데이터를 표시합니다. 하지만 가장 중요한 비즈니스 데이터를 보기 위해 만든 가장 중요한 데이터 감지 정책 2개를 선택할 수 있습니다. 자세한 내용은 ["데이터 센스를 사용하여 정책을 만드십시오"](#).

그래프에는 정책의 기준을 충족하는 모든 데이터에 대한 사용 권한 분석이 표시됩니다. 다음과 같은 항목 수가 나열됩니다.

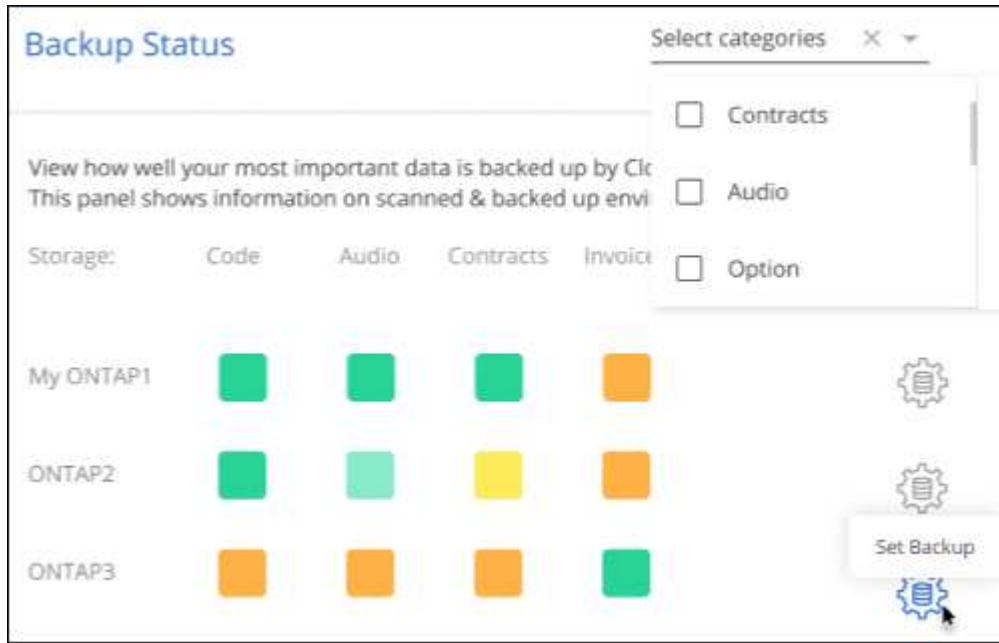
- 공개 권한으로 열기 – Data Sense에서 공개라고 여기는 항목입니다
- 조직 권한에 대한 공개 – Data Sense가 조직에 개방적이라고 여기는 항목입니다
- 열린 권한 없음 – Data Sense에서 열린 권한이 없는 것으로 간주하는 항목입니다
- 알 수 없는 권한 – Data Sense에서 알 수 없는 사용 권한으로 간주하는 항목입니다

차트의 각 막대 위로 마우스를 가져가면 각 범주의 결과 수를 볼 수 있습니다. 막대를 클릭하면 열려 있는 권한이 있는 항목과 파일 권한을 조정해야 하는지 여부를 자세히 조사할 수 있도록 데이터 감지 조사 페이지가 표시됩니다.

중요한 비즈니스 데이터의 백업 상태입니다

Backup Status_panel은 Cloud Backup을 사용하여 서로 다른 범주의 데이터를 보호하는 방법을 보여줍니다. 랜섬웨어 공격으로 인해 복구해야 할 경우에 대비하여 가장 중요한 범주의 데이터가 포괄적으로 백업되는 방식을 식별합니다. 이 데이터는 작업 환경에서 특정 범주의 항목 수를 시각적으로 나타낸 것입니다.

Cloud Backup_and_scanned를 사용하여 이미 백업되고 있는 온프레미스 ONTAP 및 Cloud Volumes ONTAP 작업 환경만 클라우드 데이터 센스를 사용하여 표시됩니다.



처음에 이 패널은 선택한 기본 범주를 기반으로 데이터를 표시합니다. 그러나 추적할 데이터 범주를 선택할 수 있습니다. 예를 들어 코드 파일, 계약 등을 선택할 수 있습니다. 의 전체 목록을 참조하십시오 "범주" 클라우드 데이터 센스를 통해 작업 환경을 구축할 수 있습니다. 그런 다음 최대 4개의 범주를 선택합니다.

데이터가 채워진 후 차트의 각 사각형 위로 마우스를 가져가면 작업 환경의 같은 범주에 있는 모든 파일에서 백업된 파일 수가 표시됩니다. 녹색 사각형은 파일 중 85% 이상이 백업되고 있음을 의미합니다. 노란색 정사각형은 파일 중 40%~85%가 백업되고 있음을 의미합니다. 빨간색 사각형은 40% 이하의 파일이 백업되고 있음을 의미합니다.

행 끝에 있는 Cloud Backup 버튼을 클릭하여 Cloud Backup 인터페이스로 이동하여 각 작업 환경에서 더 많은 볼륨에 대한 백업을 활성화할 수 있습니다.

지식 및 지원

지원을 위해 등록하십시오

NetApp 기술 지원으로 지원 케이스를 생성하기 전에 NetApp Support 사이트 계정을 Cloud Manager에 추가한 다음 지원을 위해 등록해야 합니다.

NSS 계정을 추가합니다

지원 대시보드를 이용하면 모든 NetApp Support 사이트 계정을 단일 위치에서 추가 및 관리할 수 있습니다.

단계

1. 아직 NetApp Support 사이트 계정이 없는 경우 **"1인 등록"**.
2. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 * 지원 * 을 선택합니다.



3. NSS 관리 > NSS 계정 추가 * 를 클릭합니다.
4. 메시지가 표시되면 * 계속 * 을 클릭하여 Microsoft 로그인 페이지로 리디렉션됩니다.

NetApp은 Microsoft Azure Active Directory를 지원 및 라이선싱과 관련된 인증 서비스의 ID 공급자로 사용합니다.

5. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

이 작업을 수행하면 Cloud Manager에서 NSS 계정을 사용할 수 있습니다.

참고 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님).

계정을 등록하여 지원을 받을 수 있습니다

지원 등록은 지원 대시보드의 Cloud Manager에서 가능합니다.

단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 * 지원 * 을 선택합니다.



2. Resources * 탭에서 * Register for Support * 를 클릭합니다.
3. 등록할 NSS 자격 증명을 선택한 다음 * 등록 * 을 클릭합니다.

도움을 받으십시오

NetApp은 다양한 방법으로 Cloud Manager 및 클라우드 서비스를 지원합니다. 기술 자료(KB) 기사 및 커뮤니티 포럼과 같은 광범위한 무료 셀프 지원 옵션이 24x7 제공됩니다. 지원 등록에는 웹 티켓팅을 통한 원격 기술 지원이 포함됩니다.

자체 지원

이 옵션은 하루 24시간, 주 7일 동안 무료로 사용할 수 있습니다.

- "기술 자료"

Cloud Manager 기술 자료를 검색하여 문제를 해결할 수 있는 유용한 문서를 찾습니다.

- "커뮤니티"

Cloud Manager 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새 토론을 만들어보십시오.

- 문서화

현재 보고 있는 Cloud Manager 문서입니다.

- <mailto:ng-cloudmanager-feedback@netapp.com> [피드백 이메일]

저희는 귀하의 의견을 소중하게 생각합니다. 클라우드 관리자 개선에 도움이 되는 피드백을 제출해 주십시오.

NetApp 지원

위의 자체 지원 옵션 외에도 NetApp 지원 엔지니어와 협력하여 지원을 활성화한 이후의 모든 문제를 해결할 수 있습니다.

단계

1. Cloud Manager에서 * 도움말 > 지원 * 을 클릭합니다.
2. 기술 지원 아래에서 사용 가능한 옵션 중 하나를 선택합니다.
 - a. NetApp 기술 지원을 위한 전화 번호를 찾으려면 * 문의하다
 - b. 문제 열기 * 를 클릭하고 옵션 중 하나를 선택한 다음 * 보내기 * 를 클릭합니다.

NetApp 담당자가 귀하의 케이스를 검토하고 곧 다시 귀하에 연락을 드릴 것입니다.

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

<http://www.netapp.com/us/legal/copyright.aspx>

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

<https://www.netapp.com/us/media/patents-page.pdf>

개인 정보 보호 정책

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이선스에 대한 정보를 제공합니다.

- ["Cloud Manager 3.9에 대한 고지 사항"](#)

저작권 정보

Copyright © 2022 NetApp, Inc. All rights reserved. 미국에서 인쇄된 본 문서의 어떤 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 그래픽, 전자적 또는 기계적 수단(사진 복사, 레코딩 등)으로도 저작권 소유자의 사전 서면 승인 없이 전자 검색 시스템에 저장 또는 저장.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지 사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 "있는 그대로" 제공되며 상품성 및 특정 목적에 대한 적합성에 대한 명시적 또는 묵시적 보증을 포함하여 이에 제한되지 않고, 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 또는 파생적 손해(소계 물품 또는 서비스의 조달, 사용 손실, 데이터 또는 수익 손실, 계약, 엄격한 책임 또는 불법 행위(과실 또는 그렇지 않은 경우)에 관계없이 어떠한 책임도 지지 않으며, 이는 이러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구입의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허 또는 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 미국 출원 중인 특허로 보호됩니다.

권리 제한 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.277-7103(1988년 10월) 및 FAR 52-227-19(1987년 6월)의 기술 데이터 및 컴퓨터 소프트웨어의 권리(Rights in Technical Data and Computer Software) 조항의 하위 조항 (c)(1)(ii)에 설명된 제한사항이 적용됩니다.

상표 정보

NETAPP, NETAPP 로고 및 에 나열된 마크는 NetApp에 있습니다 <http://www.netapp.com/TM> 는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.