



BlueXP 랜섬웨어 보호 기능을 사용하십시오 BlueXP ransomware protection

NetApp
March 22, 2024

목차

BlueXP 랜섬웨어 보호 기능을 사용하십시오	1
BlueXP 랜섬웨어 보호 기능을 사용하십시오	1
대시보드를 사용하여 작업 부하 상태를 한눈에 확인합니다	1
랜섬웨어 공격으로부터 워크로드를 보호합니다	4
감지된 랜섬웨어 경고에 대응합니다	10
랜섬웨어 공격에서 복구(사고가 무력화된 후)	12

BlueXP 랜섬웨어 보호 기능을 사용하십시오

BlueXP 랜섬웨어 보호 기능을 사용하십시오

BlueXP 랜섬웨어 보호를 사용하여 워크로드 상태를 확인하고 워크로드를 보호할 수 있습니다.

- "BlueXP 랜섬웨어 방어에서 워크로드를 찾아보십시오".
- "대시보드에서 보호 및 워크로드 상태를 확인합니다".
 - 랜섬웨어 차단 권장 사항을 검토하고 조치를 취하십시오.
- "워크로드 보호":
 - 워크로드에 랜섬웨어 보호 정책을 할당합니다.
 - 애플리케이션 보호를 높여 미래의 랜섬웨어 공격을 방지합니다.
 - 보호 정책을 생성, 변경 또는 삭제합니다.
- "잠재적인 랜섬웨어 공격 탐지에 대응".
- "공격에서 복구하십시오" (인시던트가 종결화된 후)
- "보호 설정을 구성합니다".

대시보드를 사용하여 작업 부하 상태를 한눈에 확인합니다

BlueXP 랜섬웨어 방어 대시보드에서는 워크로드의 보호 상태에 대한 간략한 정보를 제공합니다. 따라서 위험에 노출되거나 보호되는 워크로드를 신속하게 확인하고, 사고 또는 복구 작업의 영향을 받는 워크로드를 식별하고, 보호되는 스토리지의 양을 확인하여 보호 범위를 측정할 수 있습니다.

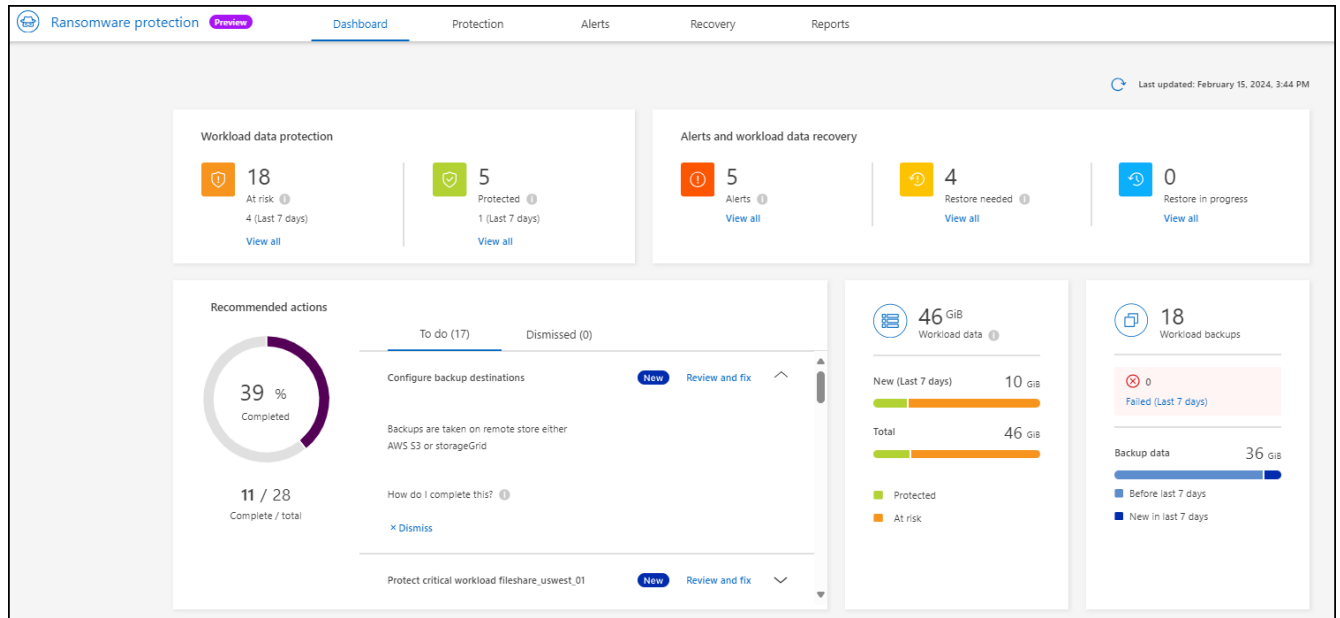
대시보드를 사용하여 보호 권장 사항을 검토하고 조치를 취할 수도 있습니다.

대시보드를 사용하여 워크로드 상태를 검토합니다

단계

1. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.

검색이 완료되면 대시보드에 워크로드 데이터 보호의 상태가 표시됩니다.



2. 대시보드에서 각 창에서 다음 중 하나를 보고 수행할 수 있습니다.

- * Workload data protection *: * View All * 을 클릭하면 보호 페이지에서 위험하거나 보호되는 모든 워크로드를 볼 수 있습니다. 보호 수준이 보호 정책과 일치하지 않을 경우 워크로드가 위험에 노출됩니다. 을 참조하십시오 ["워크로드 보호"](#).
- * 경고 및 워크로드 데이터 복구 *: 워크로드에 영향을 미치는 활성 인시던트를 보거나 인시던트가 무효화되거나 복구 중인 후 복구할 준비가 된 인시던트를 보려면 * 모두 보기 * 를 클릭합니다. 을 참조하십시오 ["감지된 경고에 응답합니다"](#).

인시던트는 다음 상태 중 하나로 분류됩니다.

- 영향 받음(경고 페이지에 표시됨)
- 복구 준비(복구 페이지에 표시)
- 복구 중(복구 페이지에 표시)
- 복구 실패(복구 페이지에 표시)
- 복구됨(복구 페이지에 표시)
- * 권장 조치 *: 보호 수준을 높이려면 각 권장 사항을 검토하고 * 검토 및 수정 * 을 클릭하십시오.

을 참조하십시오 ["대시보드에서 보호 권장 사항을 검토합니다"](#) 또는 ["워크로드 보호"](#).

마지막으로 대시보드를 방문한 이후에 추가된 모든 권장 사항은 최소 24시간 동안 "신규"로 표시됩니다. 작업은 우선 순위에 따라 나열되고 가장 중요한 작업은 맨 위에 표시됩니다. 각 항목을 검토하고 조치를 취하거나 해제할 수 있습니다.

총 작업 수는 해제된 작업을 포함하지 않습니다.

- * 워크로드 데이터 *: 지난 7일 동안 보호 범위의 변경 사항을 모니터링합니다.
- * Workload Backups *: 지난 7일 동안 실패했거나 성공적으로 완료된 서비스에 의해 생성된 워크로드 백업의 변경 사항을 모니터링합니다.

대시보드에서 보호 권장 사항을 검토합니다

BlueXP 랜섬웨어 보호는 워크로드의 보호를 평가하고 이 보호 기능을 개선하기 위한 조치를 권장합니다.

권장 사항을 검토하고 조치를 취하면 권장 상태가 완료로 변경됩니다. 또는 나중에 조치를 취하려는 경우 해당 조치를 해제할 수 있습니다. 작업을 취소하면 나중에 검토할 수 있도록 추천 내용이 무시된 작업 목록으로 이동합니다.

다음은 서비스가 제공하는 권장 사항의 샘플입니다.

권장 사항	설명	해결 방법
랜섬웨어 차단 정책을 추가하십시오	워크로드가 현재 보호되지 않습니다.	워크로드에 정책을 할당합니다. 을 참조하십시오 " 랜섬웨어 공격으로부터 워크로드를 보호합니다 ".
백업 대상을 구성합니다	현재 워크로드에 백업 대상이 없습니다.	이 워크로드를 보호하려면 백업 대상을 추가하십시오. 을 참조하십시오 " 보호 설정을 구성합니다 ".
정책을 더 강력하게 만듭니다.	일부 워크로드는 보호 기능이 충분하지 않을 수 있습니다. 정책으로 워크로드 보호 강화	보존 증가, 백업 추가, 변경 불가능한 백업 적용, 의심스러운 파일 확장자 차단, 보조 스토리지에서 감지 기능 활성화 등의 작업을 수행할 수 있습니다. 을 참조하십시오 " 랜섬웨어 공격으로부터 워크로드를 보호합니다 ".
랜섬웨어로부터 중요 또는 중요 애플리케이션 워크로드를 보호합니다.	보호 페이지에는 보호되지 않는 중요 또는 중요(할당된 우선 순위 수준 기준) 애플리케이션 워크로드가 표시됩니다.	이러한 워크로드에 정책을 할당합니다. 을 참조하십시오 " 랜섬웨어 공격으로부터 워크로드를 보호합니다 ".
랜섬웨어로부터 중요 또는 중요 파일 공유 워크로드를 보호합니다.	보호 페이지에는 보호되지 않는 파일 공유 또는 데이터 저장소 유형의 중요 워크로드 또는 중요 워크로드가 표시됩니다.	각 워크로드에 정책을 할당합니다. 을 참조하십시오 " 랜섬웨어 공격으로부터 워크로드를 보호합니다 ".
새 경고를 검토합니다	새 알림이 있습니다.	새 경고를 검토합니다. 을 참조하십시오 " 감지된 랜섬웨어 경고에 대응합니다 ".

단계

1. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.
2. 권장 작업 창에서 권장 사항을 선택하고 * 검토 및 수정 * 을 선택합니다.
3. 나중에 작업을 취소하려면 * 해제 * 를 선택합니다.

권장 사항이 To Do(작업) 목록에서 지워지고 해제된 목록에 나타납니다.



나중에 해제된 항목을 할 일 항목으로 변경할 수 있습니다. 항목을 완료로 표시하거나 해제된 항목을 할 일 작업으로 변경하면 총 작업이 1씩 증가합니다.

4. 권장 사항에 대한 조치 방법에 대한 정보를 검토하려면 * 정보 * 아이콘을 선택합니다.

랜섬웨어 공격으로부터 워크로드를 보호합니다

BlueXP 랜섬웨어 보호를 사용하여 다음 작업을 완료하여 랜섬웨어 공격으로부터 워크로드를 보호할 수 있습니다.

- 기존 워크로드 보호 보기
- 워크로드에 정책을 할당합니다.
 - 향후 RW 공격을 예방하기 위해 애플리케이션 보호 강화
 - 이전에 RW 서비스에서 보호되었던 작업 부하에 대한 보호를 변경합니다.
- 정책을 관리합니다(사용자가 만든 정책만 해당).

BlueXP 랜섬웨어 방어는 검색 중에 각 워크로드에 우선순위를 할당합니다. 워크로드 우선 순위는 다음과 같은 스냅샷 주파수에 의해 결정됩니다.

- * 중요 *: 시간당 1개 미만의 스냅샷 복사본 생성(매우 공격적인 보호 일정)
- * 중요 *: 매일 1회 미만으로 스냅샷 복사본을 생성합니다
- * 표준 *: 매일 1개 이상의 스냅샷 복사본이 생성됩니다
- 보호 상태 *: 워크로드는 다음 보호 상태 중 하나를 표시하여 정책이 적용되었는지 여부를 나타낼 수 있습니다.
- * Protected *: 정책이 적용됩니다.
- * 위험 *: 정책이 적용되지 않습니다.
- * 진행 중 *: 정책이 적용되지만 아직 완료되지 않았습니다.
- * 실패 *: 정책이 적용되었지만 작동하지 않습니다.
- 보호 상태 *: 워크로드는 다음 보호 상태 중 하나일 수 있습니다.
- * 정상 *: 워크로드에 보호가 설정되어 있으며 백업 및 스냅샷 복사본이 완료되었습니다.
- * in progress *: 백업 또는 스냅샷 복사본이 진행 중입니다.
- * 실패 *: 백업 또는 스냅샷 복사본이 성공적으로 완료되지 않았습니다.
- * N/A *: 워크로드에 보호가 활성화되지 않았거나 충분하지 않습니다.

워크로드 랜섬웨어 방어 보기

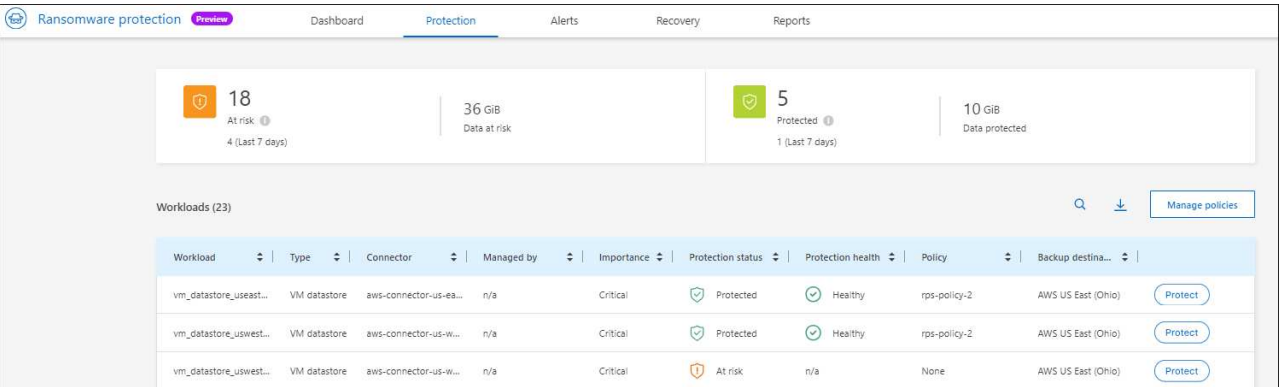
워크로드를 보호하는 첫 번째 단계 중 하나는 현재 워크로드와 해당 워크로드의 보호 상태를 확인하는 것입니다. 다음과 같은 워크로드 유형을 볼 수 있습니다.

- VM 워크로드
- 파일 공유 워크로드

단계

1. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.
2. 다음 중 하나를 수행합니다.

- 대시보드 데이터 보호 창에서 * 모두 보기 * 를 선택합니다.
- 메뉴에서 * 보호 * 를 선택합니다.



3. 이 페이지에서 워크로드에 정책을 할당할 수 있습니다.

워크로드에 사전 정의된 보호 정책을 할당합니다

데이터를 보호하기 위해 하나 이상의 워크로드에 기존 랜섬웨어 방지 정책을 할당할 수 있습니다. 이미 정책이 있는 워크로드에 다른 정책을 할당할 수도 있습니다.

BlueXP 랜섬웨어 보호에는 워크로드 우선순위에 따라 다음과 같은 사전 정의된 정책이 포함됩니다.

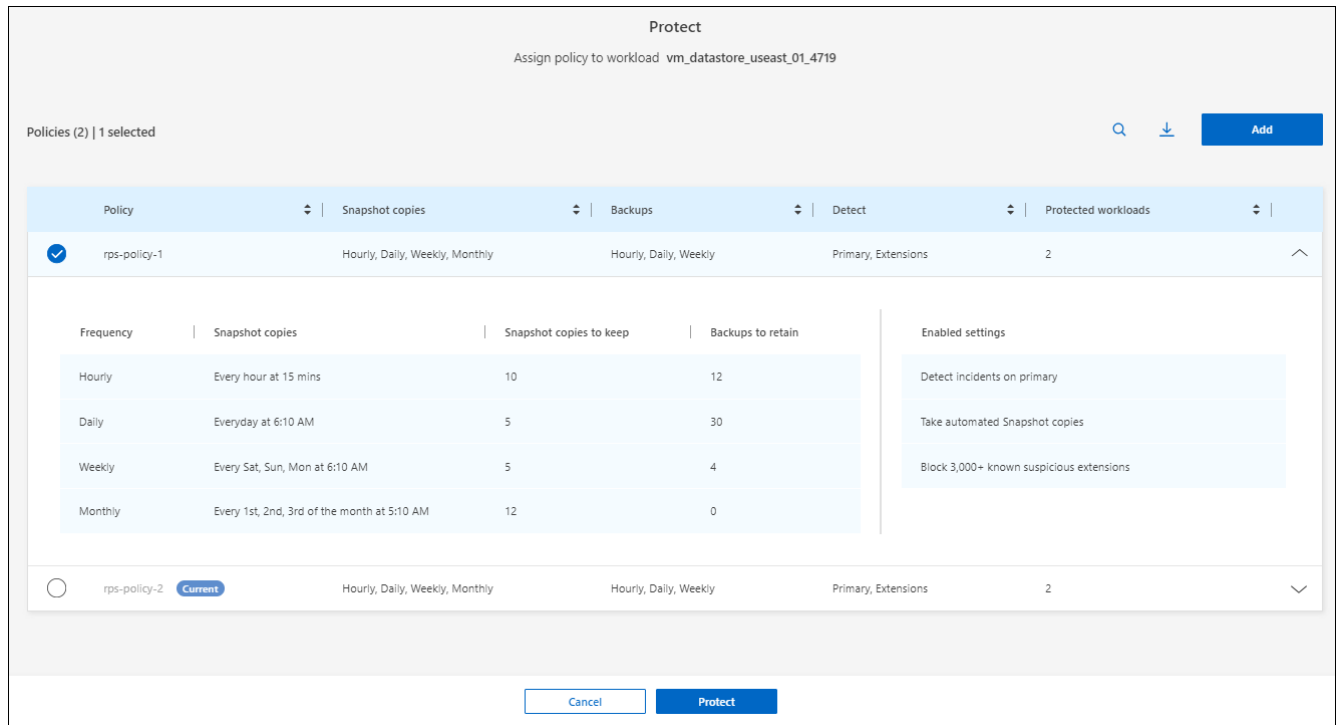
정책 레벨	스냅샷	주파수	보존(일)	스냅샷 복사본 수	총 최대 스냅샷 복사본 수
* 중요 워크로드 정책 *	매시간 분기	15분마다	3	288	309
	매일	1일마다	14	14	309
	매주	1주마다	35	5	309
	매월	30일마다	60	2	309
* 중요 워크로드 정책 *	매시간 분기	30분마다	3	144	165
	매일	1일마다	14	14	165
	매주	1주마다	35	5	165
	매월	30일마다	60	2	165

정책 레벨	스냅샷	주파수	보존(일)	스냅샷 복사본 수	총 최대 스냅샷 복사본 수
* 표준 워크로드 정책 *	매시간 분기	60분마다	3	72	93
	매일	1일마다	14	14	93
	매주	1주마다	35	5	93
	매월	30일마다	60	2	93

단계

1. BlueXP 랜섬웨어 방어에서 다음 중 하나를 수행하십시오.
 - 대시보드 데이터 보호 창에서 * 모두 보기 * 를 선택합니다.
 - 대시보드 추천 창에서 정책 할당에 대한 권장 사항을 선택하고 * 검토 및 수정 * 을 선택합니다.
 - 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지에서 워크로드를 검토하고 워크로드 옆에 있는 * 보호 * 를 선택합니다.

정책 목록이 나타납니다.



3. 자세한 내용을 보려면 정책의 아래쪽 화살표를 클릭하십시오.
4. 워크로드에 할당할 정책을 선택합니다.
5. protect * 를 선택합니다.
6. 작업이 "완료됨"으로 표시된 대시보드 권장 작업 창을 검토합니다.

보호 정책을 생성합니다

기존 정책이 비즈니스 요구 사항을 충족하지 못하는 경우 새 보호 정책을 만들 수 있습니다. 새로 만들거나 기존 정책을 사용하고 설정을 수정할 수 있습니다.

운영 및 2차 스토리지를 통제하고 운영 및 2차 스토리지를 동일하거나 다르게 처리하는 정책을 생성할 수 있습니다.

정책을 관리할 때나 워크로드에 정책을 할당하는 동안 정책을 생성할 수 있습니다.

정책을 관리하는 동안 정책을 생성하는 단계입니다

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.

18

At risk ⓘ

4 (Last 7 days)

36 GiB

Data at risk

5

Protected ⓘ

1 (Last 7 days)

10 GiB

Data protected

Workloads (23)

🔍

⬇

Manage policies

Workload	Type	Connector	Managed by	Importance	Protection status	Protection health	Policy	Backup destina...
vm_datastore_useast...	VM datastore	aws-connector-us-ea...	n/a	Critical	<div>🛡️ Protected</div>	<div>🟢 Healthy</div>	RPS-Policy-Importatnt	AWS US East (Ohio) <div>Protect</div>
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	<div>🛡️ Protected</div>	<div>🟢 Healthy</div>	RPS-Policy-Importatnt	AWS US East (Ohio) <div>Protect</div>
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	<div>🔴 At risk</div>	<div>n/a</div>	None	AWS US East (Ohio) <div>Protect</div>

2. 보호 페이지에서 * 정책 관리 * 를 선택합니다.

Protection > Manage policies						
Manage policies						
Policies (3) 🔍 ⬇ Add						
Policy	Snapshot copies	Backups	Detect	Protected workloads		
RPS-Policy-Critical	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2	⌵	⋮
RPS-Policy-Importatnt	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2	⌵	⋮
RPS-Policy-Standard	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	0	⌵	⋮

3. 정책 관리 페이지에서 * 추가 * 를 선택합니다.

Protection > Manage policies > Add policy

Add policy

Policy name

Copy from existing policy

Primary storage

Snapshot copy schedules

Weekly

▼

Primary detection

Disable

▼

Block file extensions

Disable

▼

Secondary storage

Backup schedules

Weekly

▼

Secondary detection

Disable

▼

4. 새 정책 이름을 입력하거나 기존 정책 이름을 입력하여 복사합니다. 기존 정책 이름을 입력한 경우 복사할 정책을 선택합니다.



기존 정책을 복사하고 수정하도록 선택한 경우 하나 이상의 설정을 고유하게 변경해야 합니다.

5. 각 항목에 대해 아래쪽 화살표를 선택합니다.

◦ * 운영 스토리지 *:

- * Snapshot copy schedules *: 일정 옵션, 유지할 스냅샷 복사본 수를 선택하고 일정 활성화를 선택합니다.
- * 기본 감지 *: 운영 스토리지에서 랜섬웨어 사고를 감지할 수 있도록 서비스를 지원합니다.
- * 파일 확장자 차단 *: 서비스에서 알려진 의심스러운 파일 확장자를 차단하려면 이 기능을 활성화하십시오. 이 서비스는 기본 감지가 활성화될 때 자동화된 스냅샷 복사본을 생성합니다.

◦ * 보조 스토리지 *:

- * 백업 스케줄 *: 보조 스토리지에 대한 스케줄 옵션을 선택하고 스케줄을 활성화합니다.
- * 2차 감지 *: 2차 스토리지에서 랜섬웨어 사고를 감지할 수 있도록 서비스를 지원합니다.
- * 백업 잠금 *: 보조 스토리지의 백업이 특정 기간 동안 수정되거나 삭제되지 않도록 하려면 이 옵션을 선택합니다. 이를 `_immutable storage_`라고도 합니다.

이 옵션은 보조 스토리지의 백업을 잠그는 NetApp DataLock 기술을 사용합니다. 백업 파일이 잠기고 유지되는 기간을 DataLock 보존 기간이라고 합니다. 이는 정의한 백업 정책 일정 및 보존 설정과 14일 버퍼를 기반으로 합니다. 30일 미만의 모든 DataLock 보존 정책은 최소 30일로 반올림됩니다.

6. 추가 * 를 선택합니다.

보호 정책을 할당하는 동안 정책을 생성하는 단계입니다

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.

18

At risk

4 (Last 7 days)

36 GiB

Data at risk

5

Protected

1 (Last 7 days)

10 GiB

Data protected

Workloads (23)

Manage policies

Workload	Type	Connector	Managed by	Importance	Protection status	Protection health	Policy	Backup destina...
vm_datastore_useast...	VM datastore	aws-connector-us-ea...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)

2. 보호 페이지에서 * 보호 * 를 선택합니다.
3. 보호 페이지에서 * 추가 * 를 선택합니다.

Protection > Manage policies > Add policy

Add policy

Policy name

test-policy

Copy from existing policy

No policy selected

Select

Primary storage

Snapshot copy schedules

Weekly

Primary detection

Disable

Block file extensions

Disable

Secondary storage

Backup schedules

Weekly

Secondary detection

Disable

Cancel

Add

4. 정책 관리 페이지에서 정책을 만드는 것과 같은 프로세스를 완료합니다.

다른 보호 정책을 할당합니다

워크로드에 따라 다른 보호 정책을 선택할 수 있습니다.
보호 정책을 변경하여 미래의 랜섬웨어 공격을 방지하도록 보호 수준을 높일 수도 있습니다.

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지에서 워크로드를 선택하고 * 보호 * 를 선택합니다.
3. 보호 페이지에서 워크로드에 대한 다른 정책을 선택합니다.
4. 정책에 대한 세부 정보를 변경하려면 오른쪽의 아래쪽 화살표를 선택하고 세부 정보를 변경합니다.
5. 변경을 완료하려면 * 저장 * 을 선택합니다.

기존 정책을 편집합니다

정책이 워크로드와 연결되어 있지 않은 경우에만 정책의 세부 정보를 변경할 수 있습니다.

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지에서 * 정책 관리 * 를 선택합니다.
3. 정책 관리 페이지에서 변경하려는 정책에 대한 * 작업 * 옵션을 선택합니다.
4. 작업 메뉴에서 * 정책 편집 * 을 선택합니다.
5. 세부 정보를 변경합니다.
6. 변경을 완료하려면 * 저장 * 을 선택합니다.

정책을 삭제합니다

현재 워크로드와 연결되어 있지 않은 보호 정책을 삭제할 수 있습니다.

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지에서 * 정책 관리 * 를 선택합니다.
3. 정책 관리 페이지에서 삭제할 정책에 대한 * 작업 * 옵션을 선택합니다.
4. 작업 메뉴에서 * 정책 삭제 * 를 선택합니다.

감지된 랜섬웨어 경고에 대응합니다

BlueXP 랜섬웨어 방어가 잠재적 공격을 감지하면 BlueXP 랜섬웨어 방어 대시보드와 오른쪽 상단의 BlueXP 알림에 경고가 표시되어 잠재적 랜섬웨어 공격을 나타냅니다. 또한 스냅샷 복사본 만들기가 즉시 시작됩니다. 이제 BlueXP 랜섬웨어 방어 * 경고 * 탭에서 잠재적 위험을 고려해야 합니다.

데이터 복구를 시작하려면 스토리지 관리자가 복구 프로세스를 시작할 수 있도록 경고를 복구 준비 상태로 표시합니다.

각 경고에는 서로 다른 상태의 다른 볼륨에 여러 인시던트가 있을 수 있으므로 모든 인시던트를 확인해야 합니다.

이 서비스는 다음과 같이 알림을 발생시킨 원인에 대한 _evidence_ 라는 정보를 제공합니다.

- 파일 확장명이 만들어지거나 변경되었습니다
- 파일 생성이 완료되었고 목록에 표시된 비율만큼 증가했습니다
- 파일 삭제가 발생했고 나열된 비율만큼 증가했습니다

알림은 다음 유형의 동작을 기반으로 합니다.

- * 잠재적 공격 *: Autonomous Ransomware Protection이 새로운 연장을 감지하고 최근 24시간 동안 20회 이상 반복할 때 경고가 발생합니다(기본 동작).
- * 경고 *: 다음 동작에 따라 경고가 발생합니다.

- 새 확장의 감지는 이전에 식별되지 않았으며 동일한 동작이 이를 공격으로 선언할 수 있는 충분한 시간을 반복하지 않습니다.
- 높은 엔트로피가 관찰됩니다.
- 파일 읽기/쓰기/이름 바꾸기/삭제 작업에서 기준선을 넘어서는 100% 활동이 급증했습니다.

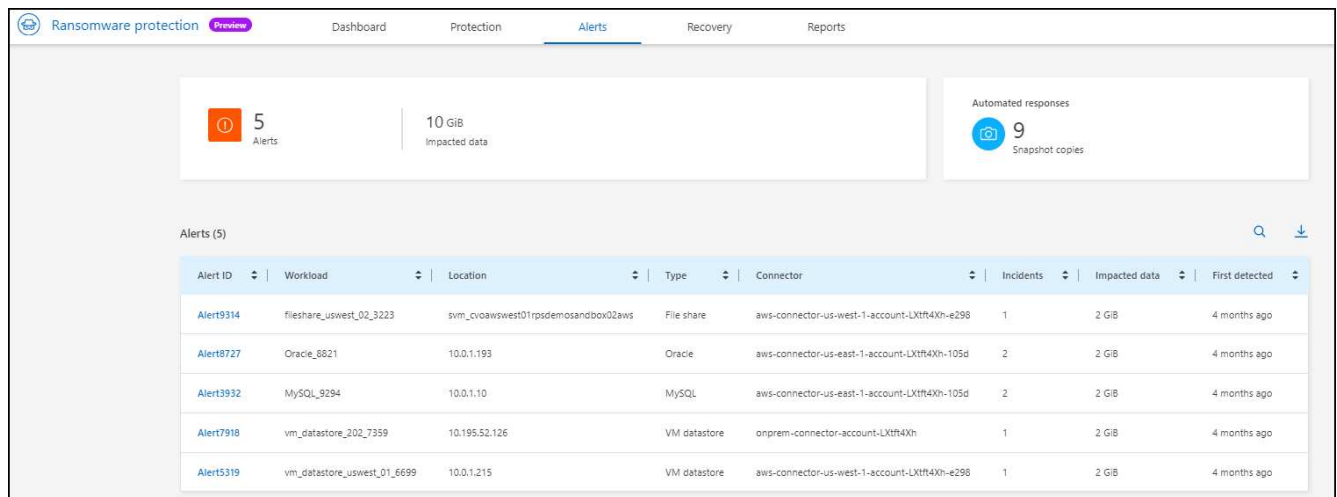
증거는 ONTAP의 자율적 랜섬웨어 방어에 대한 정보를 기반으로 합니다. 자세한 내용은 ["자율 랜섬웨어 보호 개요"](#)를 참조하십시오.

알림을 봅니다

BlueXP 랜섬웨어 보호 대시보드 또는 * Alerts * 탭에서 알림에 액세스할 수 있습니다.

단계

1. BlueXP 랜섬웨어 방어 대시보드에서 Alerts 창을 검토합니다.
2. 조각상 중 하나에서 * 모두 보기 * 를 선택합니다.
3. 각 경고에 대한 각 볼륨의 모든 인시던트를 검토하려면 경고를 클릭합니다.
4. 추가 경고를 검토하려면 왼쪽 상단의 이동 경로에서 * Alert * 를 클릭합니다.
5. 경고 페이지에서 경고를 검토합니다.



Alert ID	Workload	Location	Type	Connector	Incidents	Impacted data	First detected
Alert9314	fileshare_uswest_02_3223	svm_cvoawswest01rpsdemosandbox02aws	File share	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago
Alert8727	Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert3932	MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert7918	vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-account-LXtf4Xh	1	2 GiB	4 months ago
Alert5319	vm_datastore_uswest_01_6699	10.0.1.215	VM datastore	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago

6. 를 계속 진행합니다 [랜섬웨어 인시던트를 복구 준비 상태로 표시\(인시던트가 해소된 후\)](#).

랜섬웨어 인시던트를 복구 준비 상태로 표시(인시던트가 해소된 후)

공격을 완화하고 워크로드를 복구할 준비가 된 후에는 스토리지 관리 팀과 데이터를 복구할 수 있도록 준비해 두었다가 복구 프로세스를 시작할 수 있도록 해야 합니다.

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * Alerts * 를 선택합니다.

Alerts (5)

Alert ID	Workload	Location	Type	Connector	Incidents	Impacted data	First detected
Alert9314	fileshare_uswest_02_3223	svm_cvoawswest01rpsdemosandbox02aws	File share	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago
Alert8727	Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert3932	MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert7918	vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-account-LXtf4Xh	1	2 GiB	4 months ago
Alert5319	vm_datastore_uswest_01_6699	10.0.1.215	VM datastore	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago

- Alerts 페이지에서 알람을 선택합니다.
- 알림에서 인시던트를 검토합니다.

alert8727

Workload: Oracle_8821 | Location: 10.0.1.193 | Type: Oracle | Connector: aws-connector-us-east-1-account-LXtf4Xh-105d

2 Potential attacks | 4 months ago First detected | 2 GiB Impacted data | 286 Impacted files

Incidents (2)

Incident ID	Volume	SVM	Working environment	Type	First detected	Evidence	Automated responses
Inc4922	oracle_ustest_data2	svm_cvoawseast01rpsdemosandbox02aws	cvoawseast01rpsdemosandbox02aws	Potential attack	4 months ago	4 new extensions detected	1 Snapshot copy
Inc3163	oracle_ustest_log2	svm_cvoawseast01rpsdemosandbox02aws	cvoawseast01rpsdemosandbox02aws	Potential attack	4 months ago	6 new extensions detected	1 Snapshot copy

- 인시던트를 복구할 준비가 되었다고 판단되면 * 복원 필요 표시 * 를 선택합니다.
- 작업을 확인하고 * 복원 필요 표시 * 를 선택합니다.
- 워크로드 복구를 시작하려면 메시지에서 * 복구 * 워크로드를 선택하거나 * 복구 * 탭을 선택합니다.

결과

경고가 복구용으로 표시된 후 경고 탭에서 복구 탭으로 이동합니다.

랜섬웨어 공격에서 복구(사고가 무력화된 후)

워크로드가 "Ready for Recovery"로 표시된 후 BlueXP 랜섬웨어 방어는 RPA(Recovery Point Actual)를 권장하고 충돌 방지 복구를 위한 워크플로우를 조정합니다.

복원할 준비가 된 워크로드를 봅니다

"복구 필요" 복구 상태에 있는 워크로드를 검토합니다.

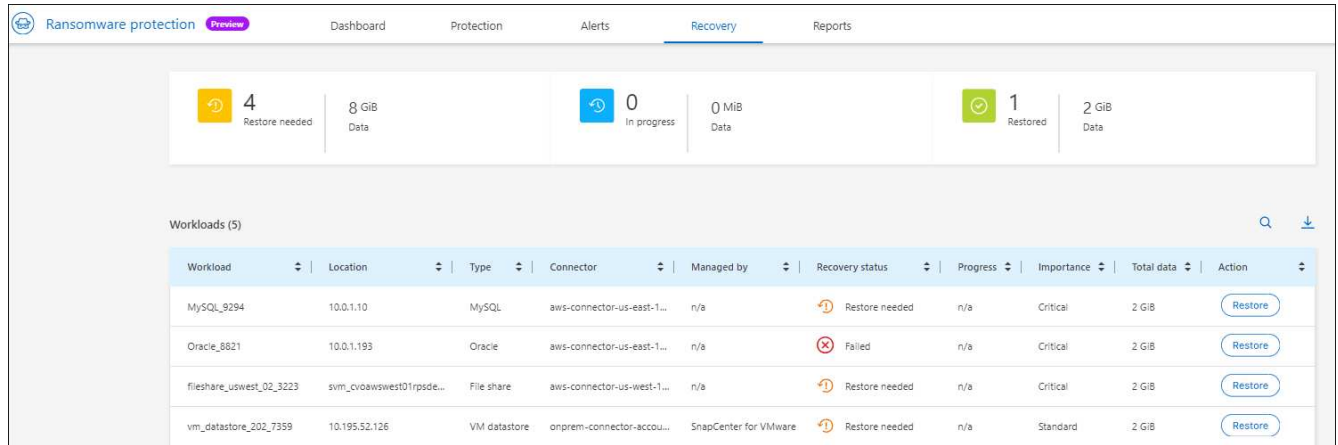
단계

- 다음 중 하나를 수행합니다.

◦ 대시보드의 Alerts 창에서 "Restore needed" 합계를 검토하고 * View All * 을 선택합니다.

◦ 메뉴에서 * 복구 * 를 선택합니다.

2. 복구 * 페이지에서 워크로드 정보를 검토합니다.



The screenshot shows the 'Recovery' tab in the Ransomware protection interface. At the top, there are three summary cards: '4 Restore needed' (8 GiB Data), '0 In progress' (0 MiB Data), and '1 Restored' (2 GiB Data). Below these is a 'Workloads (5)' section with a table listing various workloads and their recovery status.

Workload	Location	Type	Connector	Managed by	Recovery status	Progress	Importance	Total data	Action
MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1...	n/a	Restore needed	n/a	Critical	2 GiB	Restore
Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1...	n/a	Failed	n/a	Critical	2 GiB	Restore
fileshare_uswest_02_3223	svm_cvoawswe01rpsde...	File share	aws-connector-us-west-1...	n/a	Restore needed	n/a	Critical	2 GiB	Restore
vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-accou...	SnapCenter for VMware	Restore needed	n/a	Standard	2 GiB	Restore

워크로드를 복구합니다

스토리지 관리자는 BlueXP 랜섬웨어 보호를 사용하여 권장 복원 지점 또는 원하는 복원 지점에서 워크로드를 복구할 최적의 방법을 결정할 수 있습니다.

보안 스토리지 관리자는 다양한 수준에서 데이터를 복구할 수 있습니다.

- 모든 볼륨을 복구합니다
- 볼륨 레벨 또는 파일 및 폴더 레벨에서 애플리케이션을 복구합니다.
- 볼륨 레벨, 디렉토리 또는 파일/폴더 레벨에서 파일 공유를 복구합니다.
- VM 레벨의 데이터 저장소에서 복구합니다.

워크로드 유형에 따라 프로세스가 약간 다릅니다.

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 복구 * 를 선택합니다.
2. 복구 * 페이지에서 워크로드 정보를 검토합니다.
3. "복원 필요" 상태의 워크로드를 선택합니다.
4. 복원하려면 * Restore * 를 선택합니다.
5. * 복원 범위 * : 완료하려는 복원 유형을 선택하십시오.
 - 모든 볼륨
 - 볼륨 기준
 - 파일별: 복원할 폴더 또는 단일 파일을 지정할 수 있습니다.



최대 100개의 파일 또는 단일 폴더를 선택할 수 있습니다.

6. 응용 프로그램, 볼륨 또는 파일 선택 여부에 따라 다음 절차 중 하나를 계속합니다.

모든 볼륨을 복원합니다

1. 복원 페이지의 복원 범위에서 * 모든 볼륨 * 을 선택합니다.

Restore "MySQL_9294"

1 Restore 2 Review

Restore

Workload: MySQL_9294 | Host: 10.0.1.10 | Type: MySQL | Connector: aws-connector-us-eas...

Restore scope

☒ All volumes ☐ By volume ☐ By file

Source Restore points: Safest for all volumes

Restore points

☒ Safest for all volumes ☐ Latest clean Coming soon

Volumes (2)

Volume	Restore point	Type	Date	Size
mysql_useast_21	cbs-snapshot-adhoc-1697555391705	Backup	October 17, 2023, 11:09 AM	2 GiB
mysql_useast_22	cbs-snapshot-adhoc-1697555327497	Backup	October 17, 2023, 11:08 AM	2 GiB

Next

2. * 소스 *: 자세한 내용을 보려면 소스 옆에 있는 아래쪽 화살표를 선택하십시오.

- a. 데이터를 복원하는 데 사용할 복원 지점을 선택합니다.



BlueXP 랜섬웨어 방어 기능은 사고 발생 직전에 가장 적합한 복원 지점을 최신 백업으로 식별하고 "모든 볼륨에 가장 안전함" 표시를 보여줍니다. 즉, 처음 검색된 볼륨에 대한 첫 번째 공격 이전에 모든 볼륨이 복제본으로 복원됩니다.

3. * 대상 *: 세부 정보를 보려면 대상 옆에 있는 아래쪽 화살표를 선택하십시오.

- a. 작업 환경을 선택합니다.
- b. 스토리지 VM을 선택합니다.
- c. 애그리게이트를 선택합니다.
- d. 모든 새 볼륨의 앞에 붙일 볼륨 접두사를 변경합니다.



새 볼륨 이름은 접두사 + 원래 볼륨 이름 + 백업 이름 + 백업 날짜로 나타납니다.

4. 저장 * 을 선택합니다.
5. 다음 * 을 선택합니다.
6. 선택 사항을 검토합니다.
7. Restore * 를 선택합니다.
8. 상단 메뉴에서 * 복구 * 를 선택하여 작업 상태가 이동하는 복구 페이지에서 작업량을 검토합니다.

볼륨 레벨에서 애플리케이션 워크로드 복원

1. 복원 페이지의 복원 범위에서 * By volume * 을 선택합니다.

Restore

Workload: MySQL_9294 | Host: 10.0.1.10 | Type: MySQL | Connector: aws-connector-us-eas...

Restore scope: ☐ All volumes ☒ By volume ☐ By file

Select volume you want to restore and edit its settings.

Volumes (2) | 1 selected

Volume
<input checked="" type="radio"/> mysql_useast_21
<input type="radio"/> mysql_useast_22

mysql_useast_21 settings:

Attack reported October 17, 2023, 11:11 AM

Source: Select restore point

Destination: Action required

2. 볼륨 목록에서 복원할 볼륨을 선택합니다.
3. * 소스 *: 자세한 내용을 보려면 소스 옆에 있는 아래쪽 화살표를 선택하십시오.
 - a. 데이터를 복원하는 데 사용할 복원 지점을 선택합니다.



BlueXP 랜섬웨어 방어 기능은 사고 발생 전에 가장 적합한 복원 지점을 최신 백업으로 식별하고 "권장" 표시를 보여줍니다.

4. * 대상 *: 세부 정보를 보려면 대상 옆에 있는 아래쪽 화살표를 선택하십시오.
 - a. 작업 환경을 선택합니다.
 - b. 스토리지 VM을 선택합니다.
 - c. 애그리게이트를 선택합니다.
 - d. 새 볼륨 이름을 검토합니다.



새 볼륨 이름이 원래 볼륨 이름 + 백업 이름 + 백업 날짜로 나타납니다.

5. 저장 * 을 선택합니다.
6. 다음 * 을 선택합니다.
7. 선택 사항을 검토합니다.
8. Restore * 를 선택합니다.
9. 상단 메뉴에서 * 복구 * 를 선택하여 작업 상태가 이동하는 복구 페이지에서 작업량을 검토합니다.

파일 레벨에서 애플리케이션 워크로드 복구

1. 복원 페이지의 복원 범위에서 * By file * 을 선택합니다.
2. 볼륨 목록에서 복원할 볼륨을 선택합니다.
3. * 소스 *: 자세한 내용을 보려면 소스 옆에 있는 아래쪽 화살표를 선택하십시오.

- a. 데이터를 복원하는 데 사용할 복원 지점을 선택합니다.



BlueXP 랜섬웨어 방어 기능은 사고 발생 전에 가장 적합한 복원 지점을 최신 백업으로 식별하고 "권장" 표시를 보여줍니다.

- b. 복원할 파일 최대 100개 또는 폴더 하나를 선택합니다.

- 4. * 대상 *: 세부 정보를 보려면 대상 옆에 있는 아래쪽 화살표를 선택하십시오.

- a. 데이터를 복원할 위치(원래 원본 위치 또는 지정할 수 있는 대체 위치)를 선택합니다.



원래 파일 또는 디렉토리는 복원된 데이터로 덮어 쓰지만 새 이름을 지정하지 않으면 원래 파일과 폴더 이름은 그대로 유지됩니다.

- b. 작업 환경을 선택합니다.
- c. 스토리지 VM을 선택합니다.
- d. 필요한 경우 경로를 입력합니다.



복구 경로를 지정하지 않으면 파일이 최상위 디렉토리의 새 볼륨으로 복원됩니다.

- e. 복원된 파일 또는 디렉토리의 이름을 현재 위치와 같게 할지 다른 이름으로 지정할지 선택합니다.

- 5. 저장 * 을 선택합니다.
- 6. 다음 * 을 선택합니다.
- 7. 선택 사항을 검토합니다.
- 8. Restore * 를 선택합니다.
- 9. 상단 메뉴에서 * 복구 * 를 선택하여 작업 상태가 이동하는 복구 페이지에서 작업량을 검토합니다.

볼륨 또는 파일 레벨에서 파일 공유 또는 데이터 저장소를 복구합니다

- 1. 복원할 파일 공유 또는 데이터 저장소를 선택한 후 복원 페이지의 복원 범위에서 * By volume * 또는 * by file * 을 선택합니다.

2. 볼륨 목록에서 복원할 볼륨을 선택합니다.
3. * 소스 *: 자세한 내용을 보려면 소스 옆에 있는 아래쪽 화살표를 선택하십시오.
 - a. 데이터를 복원하는 데 사용할 복원 지점을 선택합니다.



BlueXP 랜섬웨어 방어 기능은 사고 발생 전에 가장 적합한 복원 지점을 최신 백업으로 식별하고 "권장" 표시를 보여줍니다.

4. * 대상 *: 세부 정보를 보려면 대상 옆에 있는 아래쪽 화살표를 선택하십시오.
 - a. 데이터를 복원할 위치(원래 원본 위치 또는 지정할 수 있는 대체 위치)를 선택합니다.



원래 파일 또는 디렉토리는 복원된 데이터로 덮어 쓰지만 새 이름을 지정하지 않으면 원래 파일과 폴더 이름은 그대로 유지됩니다.

- b. 작업 환경을 선택합니다.
- c. 스토리지 VM을 선택합니다.
- d. 필요한 경우 경로를 입력합니다.



복구 경로를 지정하지 않으면 파일이 최상위 디렉토리의 새 볼륨으로 복원됩니다.

5. 저장 * 을 선택합니다.
6. 선택 사항을 검토합니다.
7. Restore * 를 선택합니다.
8. 메뉴에서 * 복구 * 를 선택하여 작업 상태가 이동하는 복구 페이지에서 작업량을 검토합니다.

VM 레벨에서 VM 파일 공유를 복원합니다

복구할 VM을 선택한 후 복구 페이지에서 다음 단계를 계속합니다.

1. * 소스 *: 자세한 내용을 보려면 소스 옆에 있는 아래쪽 화살표를 선택하십시오.

Restore "vm_datastore_202_7359"

1 Restore 2 Review

Restore

Workload: vm_datastore_202_735... | Location: 10.195.52.126 | vCenter: 10.195.52.128 | Type: VM datastore | Connector: onprem-connector-account-LXtft4X...

Restore scope: ☒ By VM

Source

Restore points attack time: October 17, 2023, 11:27 AM

Restore points (4)

Restore point	Provider	Date
<input type="radio"/> RG-vm_datastore_202_11-21-2023_20.30.01.0238	AWS	November 21, 2023, 8:30 PM
<input type="radio"/> RG-vm_datastore_202_11-20-2023_20.30.01.0260	AWS	November 20, 2023, 8:30 PM
<input type="radio"/> RG-vm_datastore_202_11-19-2023_20.30.01.0250	AWS	November 19, 2023, 8:30 PM
<input type="radio"/> RG-vm_datastore_202_11-18-2023_20.30.01.0871	AWS	November 18, 2023, 8:30 PM

Destination: Original location

Next

2. 데이터를 복원하는 데 사용할 복원 지점을 선택합니다.
3. * 대상 *: 원래 위치로.
4. 다음 * 을 선택합니다.
5. 선택 사항을 검토합니다.
6. Restore * 를 선택합니다.
7. 메뉴에서 * 복구 * 를 선택하여 작업 상태가 이동하는 복구 페이지에서 작업량을 검토합니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

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

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

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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