使用BlueXP勒索软件保护

BlueXP ransomware protection

NetApp
March 22, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/bluexp-ransomware-protection/rp-use-overview.html on March 22, 2024. Always check docs.netapp.com for the latest.

目录

使用BlueXP勒索软件保护 1
使用BlueXP勒索软件保护 1
使用信息板可一目了然地查看工作负载运行状况 1
保护工作负载免受勒索软件攻击 3
响应检测到的勒索软件警报 10
从勒索软件攻击中恢复(消除意外事件后) 12

使用BlueXP勒索软件保护

使用BlueXP勒索软件保护

使用BlueXP勒索软件保护、您可以查看工作负载运行状况并保护工作负载。

- "在BlueXP勒索软件保护中发现工作负载"。
- "从信息板查看保护和工作负载运行状况"。
  - 查看勒索软件防护建议并采取相应行动。
- "保护工作负载"：
  - 为工作负载分配勒索软件保护策略。
  - 增强应用程序保护、防止未来发生勒索软件攻击。
  - 创建、更改或删除保护策略。
- "响应对潜在勒索软件攻击的检测"。
- "从攻击中恢复" (事故被消除后)。
- "配置保护设置"。

使用信息板可一目了然地查看工作负载运行状况

BlueXP勒索软件保护信息板可提供有关工作负载保护运行状况的概览信息。您可以快速确定存在风险或受保护的工作负载、识别受意外事件影响或处于恢复状态的工作负载、并通过查看受保护或存在风险的存储量来衡量保护程度。

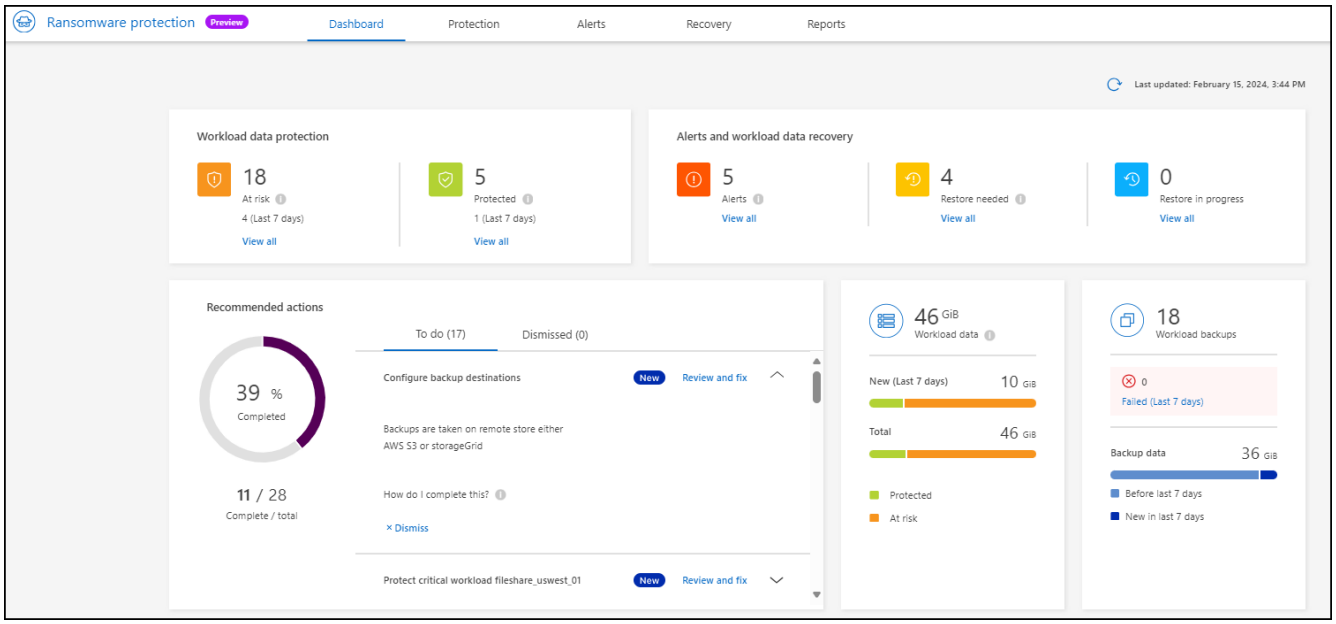
您还可以使用信息板查看保护建议并采取相应措施。

使用信息板查看工作负载运行状况

步骤

1. 从BlueXP左侧导航栏中、选择*保护*>*防软件保护*。

   发现后、信息板将显示工作负载数据保护的运行状况。



2. 在信息板中、您可以在每个窗格中查看和执行以下任一操作：

   - 工作负载数据保护：单击*查看全部*可在保护页面上查看所有存在风险或受保护的工作负载。如果保护级别与保护策略不匹配、则工作负载将面临风险。请参见 "保护工作负载"。
   - 警报和工作负载数据恢复：单击*查看全部*可查看已影响工作负载、在消除意外事件后已做好恢复准备或正在恢复的活动意外事件。请参见 "响应检测到的警报"。

     意外事件可归类为以下状态之一：

     - 受影响(显示在"警报"页面上)
     - 准备恢复(显示在恢复页面上)
     - 恢复(显示在恢复页面上)
     - 恢复失败(显示在恢复页面上)
     - 已恢复(显示在"恢复"页面上)
   - 建议的操作：要提高保护能力，请查看每个建议并单击*Review and fix*。

     请参见 "查看信息板上的保护建议" 或 "保护工作负载"。

     自您上次访问信息板以来添加的任何建议至少24小时内都以"新增"表示。操作按优先级顺序列出、最重要的操作位于顶部。您可以查看每项内容并对其采取行动、也可以将其取消。

   操作总数不包括已取消的操作。

   - 工作负载数据：监控过去7天保护范围的变化。
   - 工作负载备份：监控服务创建的工作负载备份在过去7天内失败或成功完成的更改。

查看信息板上的保护建议

BlueXP勒索软件保护可评估工作负载的保护情况、并建议采取措施来提高保护水平。

您可以查看建议并对其执行操作、从而将建议状态更改为"完成"。或者、如果要稍后再对其执行操作、可以将其取消。取消操作会将建议移动到已取消操作的列表中、您可以稍后查看这些操作。

以下是此服务提供的建议示例。

建议	Description	如何解决
添加勒索软件保护策略	此工作负载当前不受保护。	为工作负载分配策略。 请参见 "保护工作负载免受勒索软件攻击"。
配置备份目标	此工作负载当前没有任何备份目标。	向此工作负载添加备份目标以对其进行保护。 请参见 "配置保护设置"。
加强策略。	某些工作负载可能没有足够的保护。通过策略加强对工作负载的保护。	提高保留率、添加备份、强制执行不可配置的备份、阻止可疑文件扩展名、在二级存储上启用检测等。 请参见 "保护工作负载免受勒索软件攻击"。
保护关键或重要应用程序工作负载免受勒索软件的攻击。	"保护"页面将显示未受保护的关键或重要应用程序工作负载(取决于分配的优先级)。	为这些工作负载分配策略。 请参见 "保护工作负载免受勒索软件攻击"。
保护关键或重要文件共享工作负载免受勒索软件的侵害。	保护页面将显示未受保护的文件共享或数据存储库类型的关键或重要工作负载。	为每个工作负载分配一个策略。 请参见 "保护工作负载免受勒索软件攻击"。
查看新警报	存在新警报。	查看新警报。 请参见 "响应检测到的勒索软件警报"。

步骤

1. 从BlueXP左侧导航栏中、选择*保护*>*防软件保护*。
2. 从“建议的操作”窗格中，选择一个建议，然后选择*Review and fix*。
3. 要在以后取消操作，请选择*Dismiss*。

   此建议将从待办事项列表中清除、并显示在已取消列表中。

   > 您可以稍后将已取消的项目更改为待办事项。当您将项目标记为已完成或将已取消的项目更改为待办事项操作时，总操作数将增加1。

4. 要查看有关如何执行建议的信息，请选择*INFORI*图标。

保护工作负载免受勒索软件攻击

您可以通过使用BlueXP勒索软件保护完成以下操作来保护工作负载免受勒索软件攻击。

- 查看现有工作负载保护。
- 为工作负载分配策略。

    - 增强应用程序保护、防止未来的RW攻击。
    - 更改以前在RW服务中受保护的工作负载的保护。
- 管理策略(仅限您创建的策略)。

在发现期间、BlueXP勒索软件保护会为每个工作负载分配一个优先级。工作负载优先级由以下Snapshot频率决定：

- 严重：每小时创建的Snapshot副本数少于1个(保护计划极具攻击性)
- 重要：每天创建的Snapshot副本少于1个、但每小时创建的Snapshot副本多于1个
- 标准：每天创建1个以上的Snapshot副本

保护状态：工作负载可以显示以下保护状态之一、以指示是否已应用策略：

- 受保护：应用策略。
- 存在风险：未应用任何策略。
- 进行中：正在应用策略、但尚未完成。
- *failed *：已应用策略，但策略不起作用。

保护运行状况：工作负载可以具有以下保护运行状况之一：

- 运行状况良好：工作负载已启用保护、备份和Snapshot副本已完成。
- 进行中：正在进行备份或Snapshot副本。
- 失败：备份或Snapshot副本未成功完成。
- 不适用：工作负载未启用保护或保护不足。

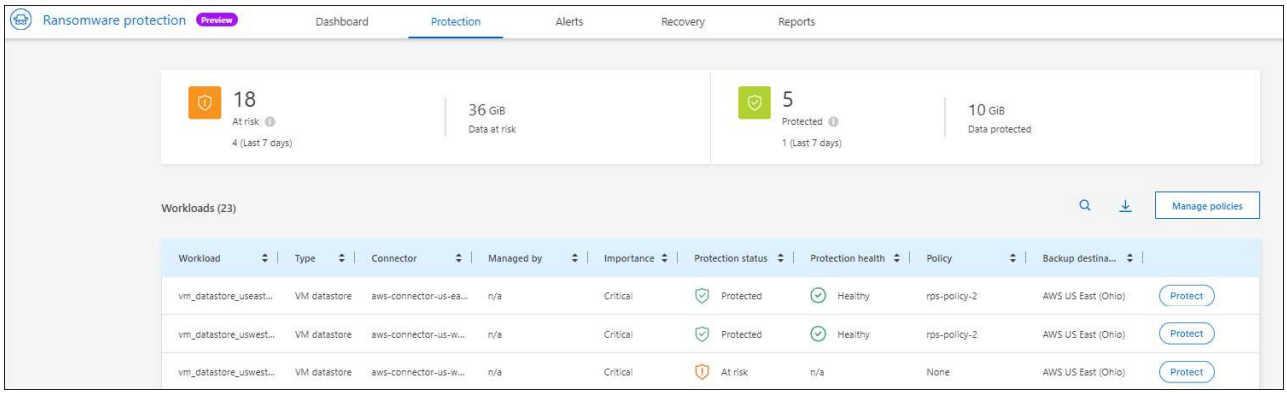
查看工作负载勒索软件保护

保护工作负载的第一步是查看当前工作负载及其保护状态。您可以看到以下类型的工作负载：

- VM工作负载
- 文件共享工作负载

步骤

1. 从BlueXP左侧导航栏中、选择*保护*>*防软件保护*。
2. 执行以下操作之一：
    - 从"DDashboard Data Protection (信息板数据保护)"窗格中、选择*查看全部*。
    - 从菜单中，选择*Protection。



3. 在此页面中、您可以为工作负载分配策略。

为工作负载分配预定义的保护策略

为了帮助保护您的数据、您可以将现有勒索软件保护策略分配给一个或多个工作负载。您还可以为已具有策略的工作负载分配不同的策略。

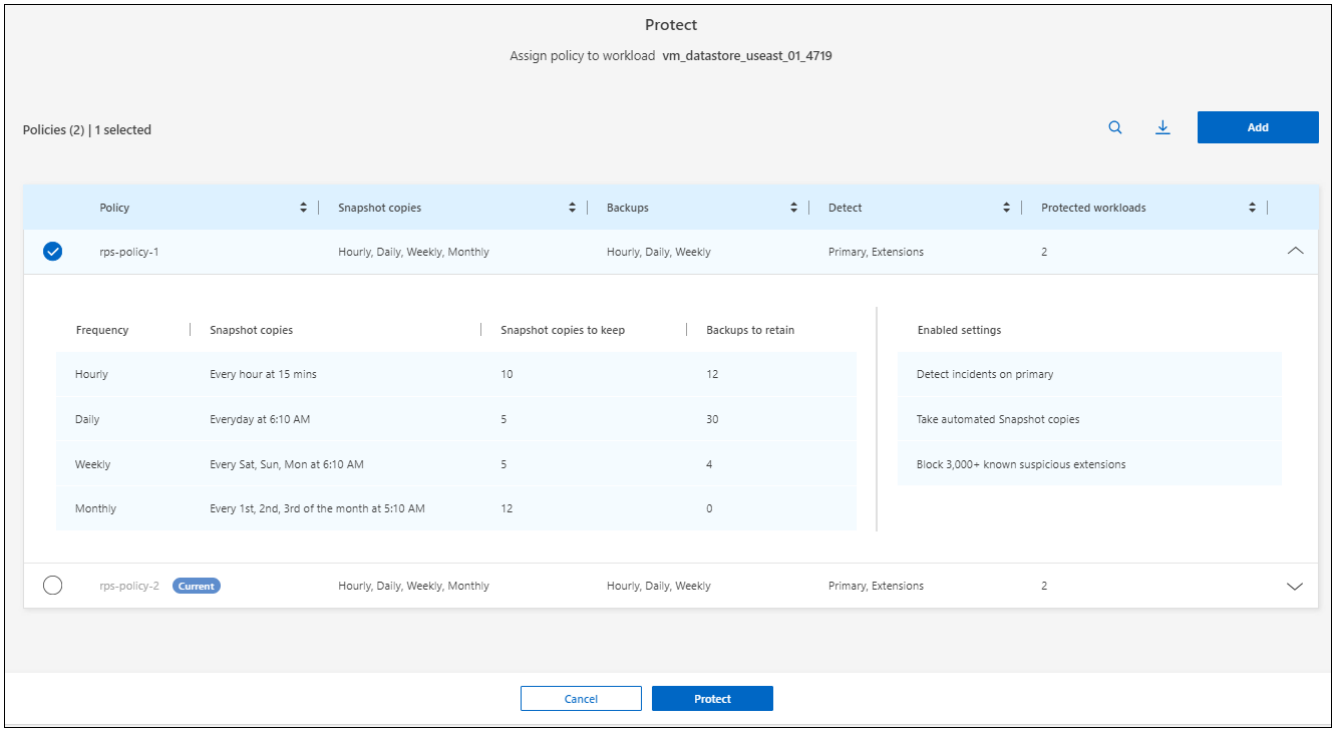
BlueXP勒索软件保护包括以下与工作负载优先级一致的预定义策略：

策略级别	Snapshot	Frequency	保留(天)	Snapshot副本数	Snapshot副本的最大总数
关键工作负载策略	每季度	每15分钟	3.	288	309
	每天	每1天	14	14	309
	每周	每1周	35	5.	309
	每月	每30天	60	2.	309
重要的工作负载策略	每季度	每30分钟	3.	144.	165
	每天	每1天	14	14	165
	每周	每1周	35	5.	165
	每月	每30天	60	2.	165
标准工作负载策略	每季度	每60分钟	3.	72.	93
	每天	每1天	14	14	93
	每周	每1周	35	5.	93
	每月	每30天	60	2.	93

步骤

1. 从BlueXP勒索软件保护中、执行以下操作之一：
   - 从"DDashboard Data Protection (信息板数据保护)"窗格中、选择*查看全部*。
   - 从"Darding Recommendation (信息板建议)"窗格中、选择有关分配策略的建议、然后选择*Review and fix*。
   - 从菜单中，选择*Protection。
2. 在保护页面中，查看工作负载，然后选择工作负载旁边的*protote*。

   此时将显示一个策略列表。



3. 要查看详细信息、请单击策略上的向下箭头。
4. 选择要分配给工作负载的策略。
5. 选择*保护*。
6. 查看"DDashboard Recommended Actions"(信息板建议操作)窗格、该窗格将操作显示为"Completed"(已完成)。

创建保护策略

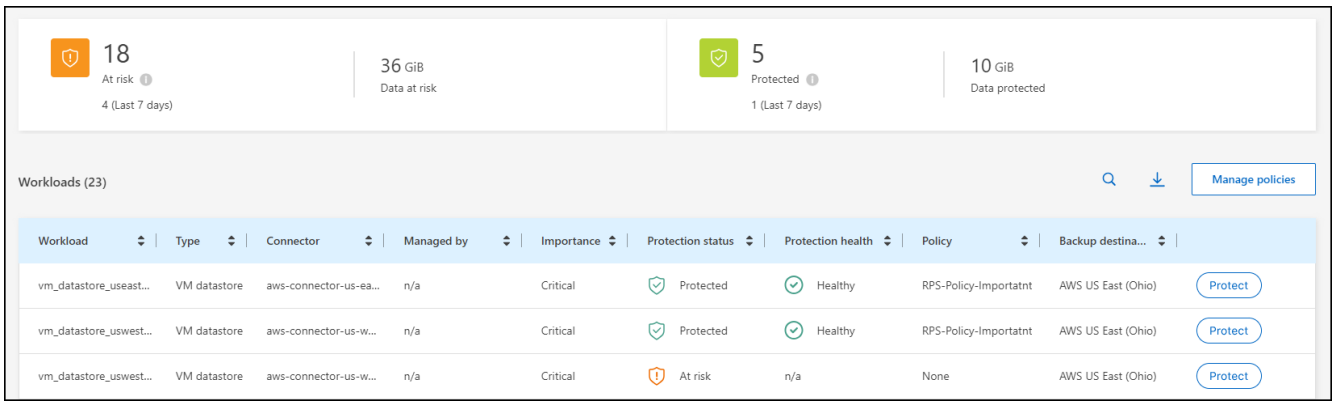
如果现有策略不能满足您的业务需求、您可以创建新的保护策略。您可以从头开始创建自己的策略、也可以使用现有策略并修改其设置。

您可以创建用于管理主存储和二级存储的策略、并按相同或不同方式处理主存储和二级存储。

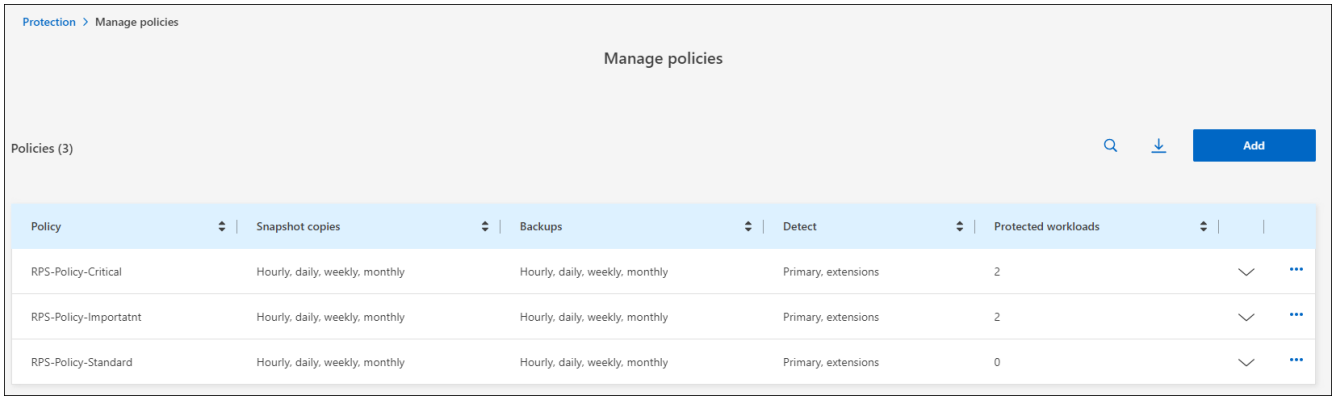
您可以在管理策略时或在将策略分配给工作负载的过程中创建策略。

策略管理期间创建策略的步骤

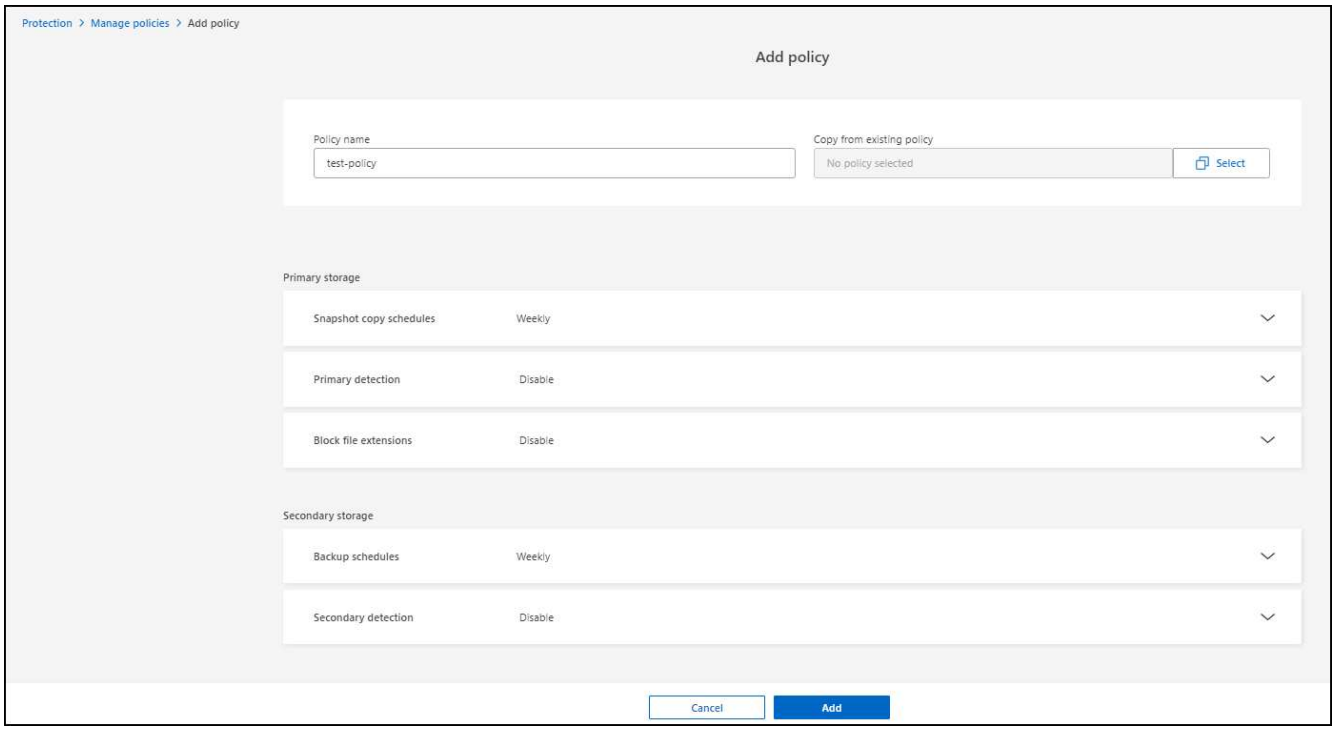
1. 从BlueXP勒索软件保护菜单中、选择*保护*。



2. 在保护页面中，选择*Manage Policies*。



3. 从“管理策略”页面中，选择*Add*。



4. 输入新策略名称或现有策略名称以进行复制。如果输入现有策略名称、请选择要复制的策略。

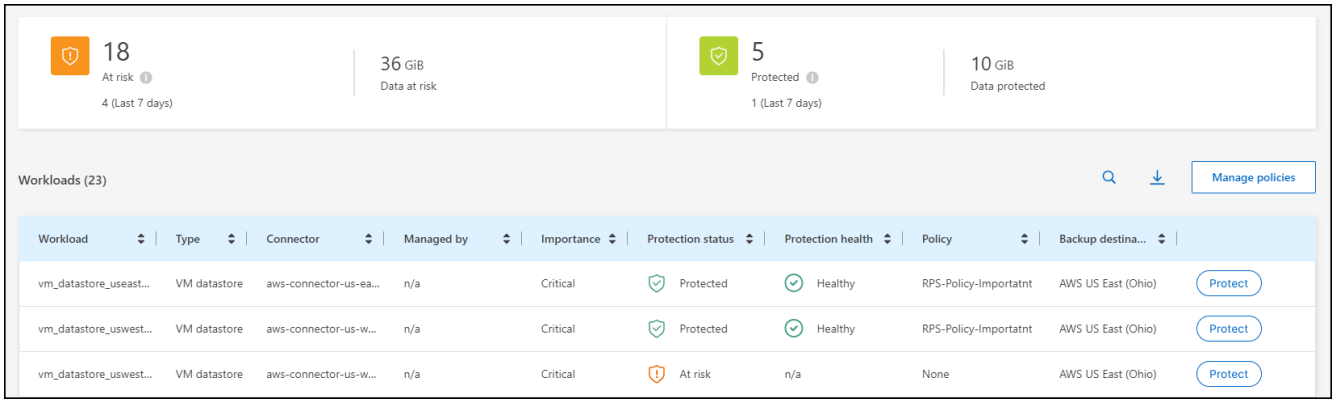
> 如果选择复制和修改现有策略、则必须至少更改一个设置、使其唯一。

5. 对于每个项目、选择向下箭头。
   - 主存储：
     - **Snapshot**副本计划：选择计划选项、要保留的Snapshot副本数、然后选择以启用计划。
     - 主要检测：使服务能够检测主存储上的勒索软件事件。
     - 阻止文件扩展名：启用此选项可使服务阻止已知的可疑文件扩展名。启用主检测后、该服务会自动创建Snapshot副本。
   - 二级存储：
     - 备份计划：为二级存储选择计划选项并启用计划。
     - 二级检测：使服务能够检测二级存储上的勒索软件事件。
     - 锁定备份：选择此选项可防止二级存储上的备份在一段时间内被修改或删除。这也称为_immutable storage_。

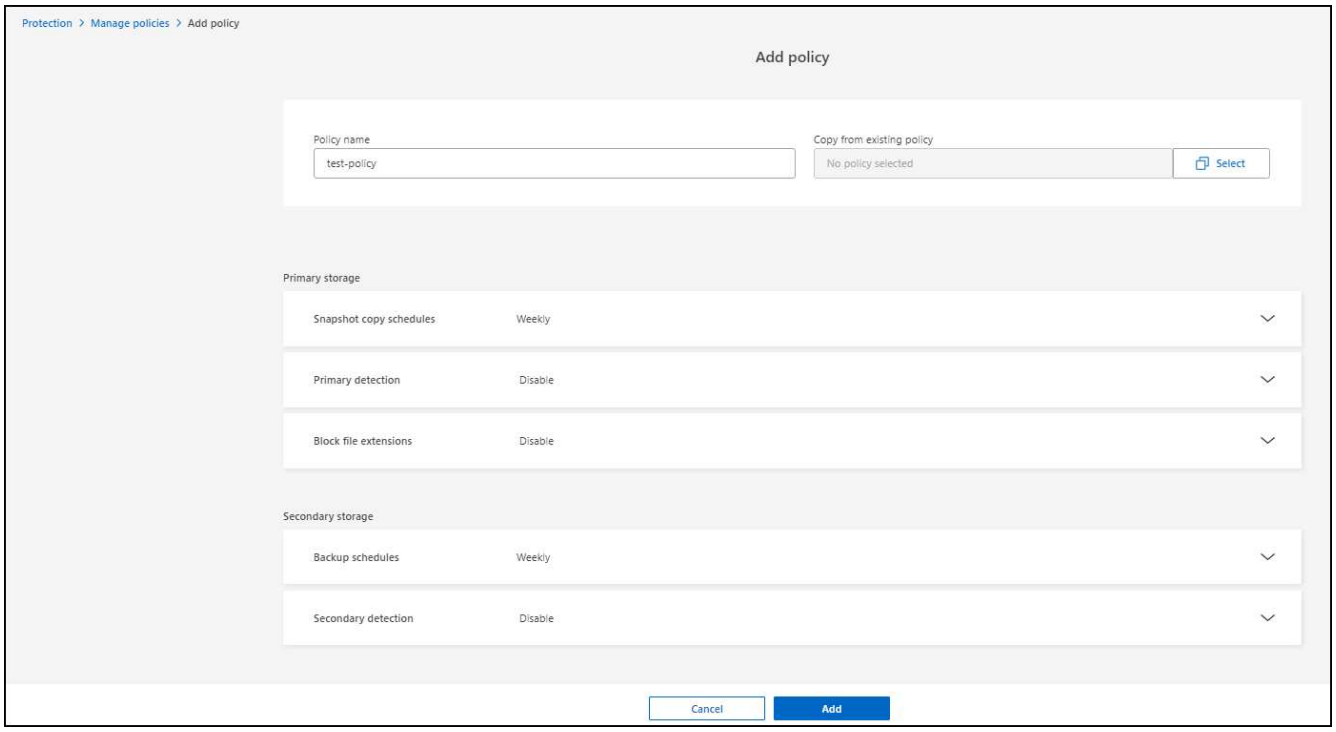
       此选项使用NetApp DataLock技术、该技术可锁定二级存储上的备份。备份文件锁定(并保留)的时间段称为DataLock保留期限。它基于您定义的备份策略计划和保留设置以及14天的缓冲区。任何少于30天的DataLock保留策略将取整为最短30天。
6. 选择 * 添加 * 。

在分配保护策略期间创建策略的步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。



2. 在保护页面中，选择*Protect*。
3. 在保护页面中，选择*Add*。



4. 完成此过程、与从管理策略页面创建策略的过程相同。

分配其他保护策略

您可以为工作负载选择其他保护策略。
您可能希望通过更改保护策略来增强保护、以防止未来发生勒索软件攻击。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。
2. 从保护页面中、选择一个工作负载、然后选择*保护*。
3. 在保护页面中、为此工作负载选择其他策略。
4. 要更改策略的任何详细信息、请选择右侧的向下箭头并更改详细信息。
5. 选择*保存*以完成更改。

编辑现有策略

只有当某个策略未与工作负载关联时、您才能更改此策略的详细信息。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。
2. 在保护页面中，选择*Manage Policies*。
3. 在管理策略页面中，选择要更改的策略的*Actions*选项。
4. 从操作菜单中，选择*Edit policy*。
5. 更改详细信息。
6. 选择*保存*以完成更改。

删除策略

您可以删除当前未与任何工作负载关联的保护策略。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。
2. 在保护页面中，选择*Manage Policies*。
3. 在管理策略页面中，选择要删除的策略的*Actions*选项。
4. 从操作菜单中，选择*Delete policy*。

响应检测到的勒索软件警报

如果BlueXP勒索软件保护检测到可能的攻击、则BlueXP勒索软件保护信息板和右上角的BlueXP通知中会显示一条警报、指示可能发生勒索软件攻击。该服务还会立即开始创建Snapshot副本。此时，您应在BlueXP勒索软件保护*Alerts*选项卡中查看潜在风险。

要开始恢复数据、请将警报标记为已准备好恢复、以便存储管理员可以开始恢复过程。

每个警报可能会在状态不同的不同卷上发生多个意外事件、因此请务必查看所有意外事件。

该服务提供有关导致发出警报的原因的信息、称为_证据_、例如：

- 已创建或更改文件扩展名
- 已创建文件、并且增加了列出的百分比
- 发生文件删除并增加了列出的百分比

警报基于以下类型的行为：

- 潜在攻击：当自主防兰森异常保护检测到新的扩展、且在过去24小时内重复发生20多次时、会发出警报(默认行为)。
- 警告：根据以下行为出现警告：
  - 以前未发现新扩展的检测，同样的行为重复的时间不足以将其声明为攻击。
  - 观察到的熵高。
  - 文件读/写/重命名/删除操作导致活动超出基线时100%激增。

证据基于ONTAP中的"自主防兰软件保护"提供的信息。有关详细信息，请参见 "自主勒索软件保护概述"。

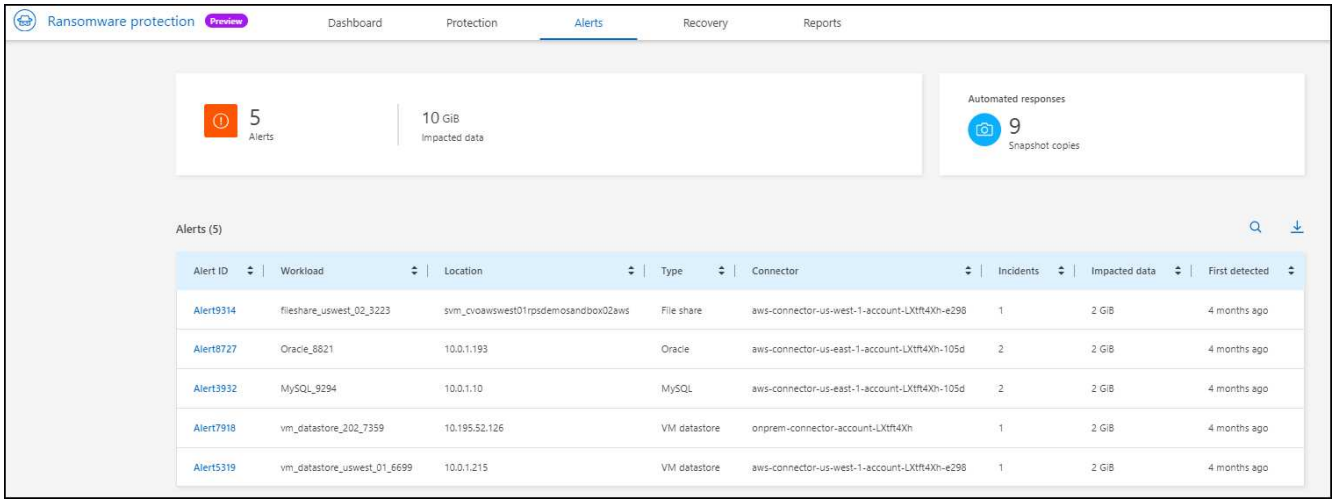
查看警报

您可以从BlueXP勒索软件保护信息板或*警报*选项卡访问警报。

步骤

1. 在BlueXP勒索软件保护信息板中、查看警报窗格。
2. 在其中一个雕像下方选择*查看全部*。

3. 单击某个警报可查看每个卷上每个警报的所有意外事件。
4. 要查看其他警报，请单击左上角的面包屑中的*Alert*。
5. 查看警报页面上的警报。



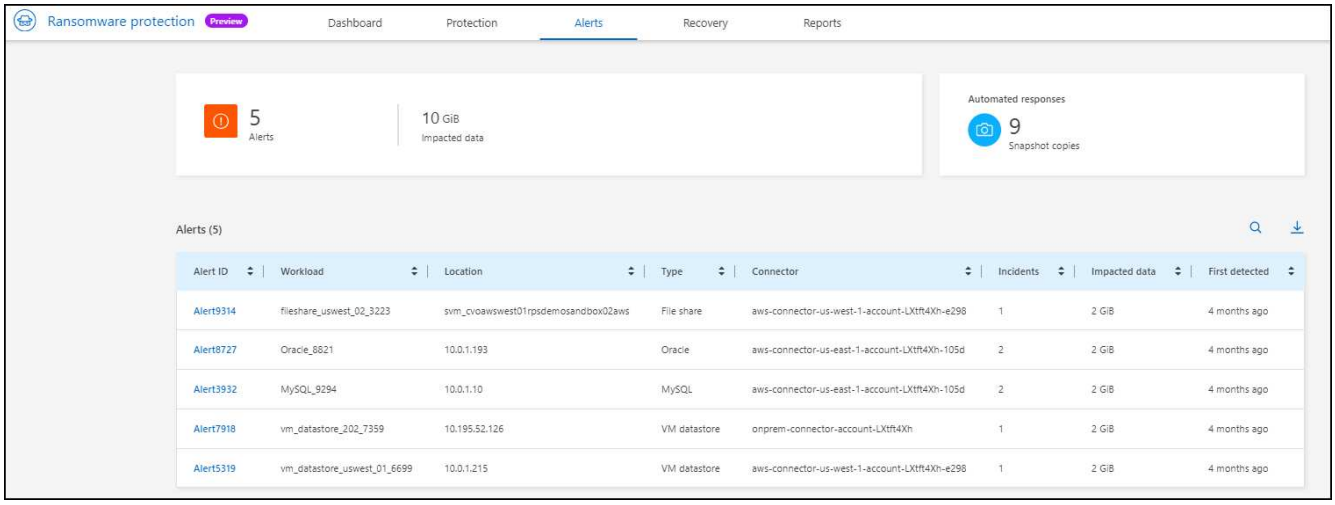
6. 继续 [将勒索软件事件标记为已做好恢复准备(在消除意外事件后)]。

将勒索软件事件标记为已做好恢复准备(在消除意外事件后)

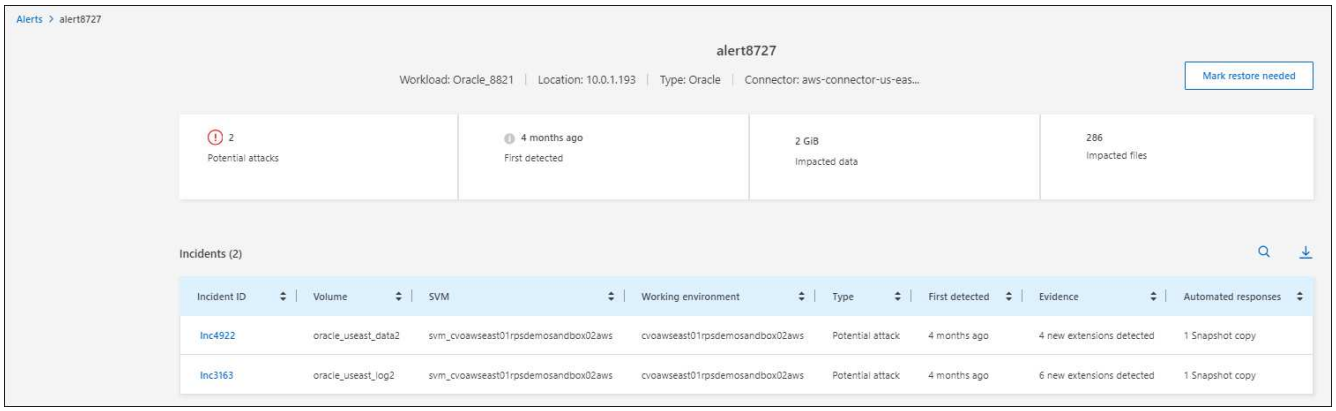
在缓解了攻击并准备好恢复工作负载之后、您应与存储管理团队沟通、指出数据已准备好进行恢复、以便他们可以启动恢复过程。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*警报*。



2. 在警报页面中、选择警报。
3. 查看警报中的意外事件。



4. 如果您确定意外事件已准备好恢复、请选择*标记需要恢复*。
5. 确认操作并选择*Mark restore Need*。
6. 要启动工作负载恢复、请在消息中选择*恢复*工作负载或选择*恢复*选项卡。

结果

将警报标记为恢复后、警报将从"Alerts"(警报)选项卡移至"Recover "(恢复)选项卡。

从勒索软件攻击中恢复(消除意外事件后)

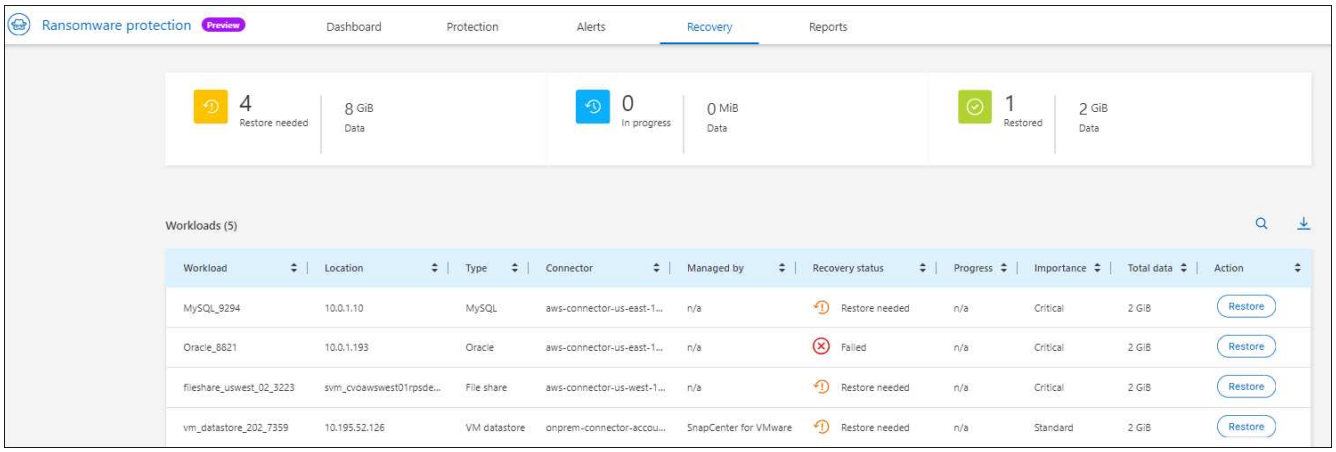
工作负载标记为"准备恢复"后、BlueXP勒索软件保护会建议使用实际恢复点(Recovery Point、RPA)、并编排工作流以实现防崩溃恢复。

查看已准备好还原的工作负载

查看处于"需要还原"恢复状态的工作负载。

步骤

1. 执行以下操作之一：
   - 在信息板中、查看警报窗格中的"需要还原"总计、然后选择*查看全部*。
   - 从菜单中，选择*RecRecovery *。
2. 查看*Recy过程*页面中的工作负载信息。



恢复工作负载

通过使用BlueXP勒索软件保护、存储管理员可以确定如何以最佳方式从建议的还原点或首选还原点恢复工作负载。

安全存储管理员可以在不同级别恢复数据：

- 恢复所有卷
- 在卷级别或文件和文件夹级别恢复应用程序。
- 在卷级别、目录级别或文件/文件夹级别恢复文件共享。
- 从虚拟机级别的数据存储库中恢复。

此过程会根据工作负载类型稍有不同。

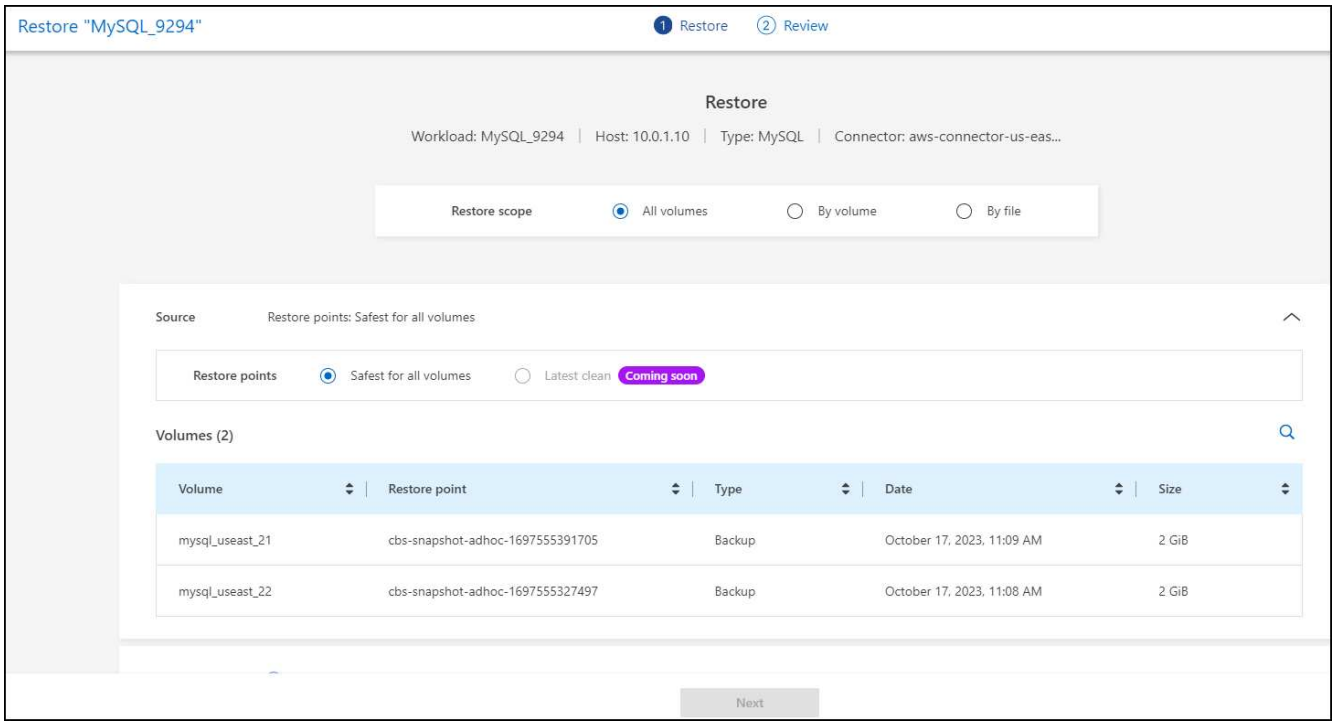
步骤

1. 从BlueXP勒索软件保护菜单中、选择*恢复*。
2. 查看*Recy过程*页面中的工作负载信息。
3. 选择处于"Restore Need"状态的工作负载。
4. 要恢复，请选择*Restore*。
5. 恢复范围：选择要完成的恢复类型：
   - 所有卷
   - 按卷
   - 按文件：您可以指定要还原的文件夹或单个文件。

     您最多可以选择100个文件或一个文件夹。
6. 根据您选择的是应用程序、卷还是文件、继续执行以下过程之一。

还原所有卷

1. 在还原页面的还原范围中、选择*所有卷*。



2. **Source**:选择Source旁边的向下箭头以查看详细信息。
   a. 选择要用于还原数据的还原点。

> BlueXP勒索软件保护会将最佳还原点标识为意外事件发生前的最新备份、并显示"对所有卷最安全"的指示。这意味着、所有卷都将还原到检测到的第一个卷受到首次攻击之前的副本。

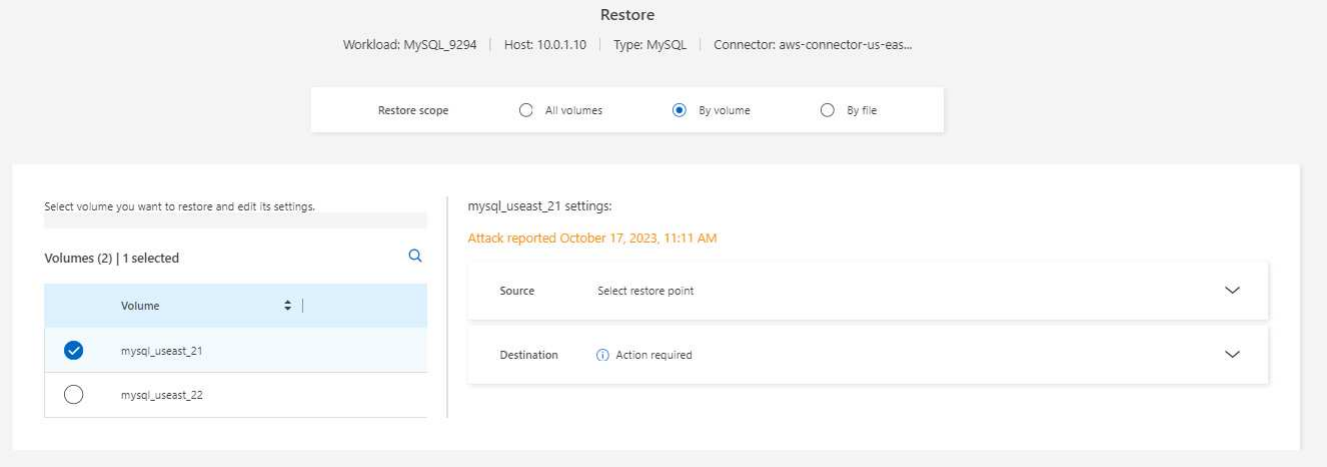
3. 目的地：选择目的地旁边的向下箭头可查看详细信息。
   a. 选择工作环境。
   b. 选择Storage VM。
   c. 选择聚合。
   d. 更改要在所有新卷之前添加的卷前缀。

> 新卷名称显示为前缀+原始卷名称+备份名称+备份日期。

4. 选择 * 保存 * 。
5. 选择 * 下一步 * 。
6. 查看您的选择。
7. 选择 * 还原 * 。
8. 从顶部菜单中选择*恢复*以查看恢复页面上的工作负载、其中操作状态将在各个状态之间移动。

在卷级别还原应用程序工作负载

1. 在"Restore"页面的"Restore scope (还原范围)"中、选择*by volume*。



2. 在卷列表中、选择要还原的卷。
3. **Source**:选择Source旁边的向下箭头以查看详细信息。
   a. 选择要用于还原数据的还原点。

   BlueXP勒索软件保护会将最佳还原点标识为事件发生前的最新备份、并显示"建议"指示。

4. 目的地：选择目的地旁边的向下箭头可查看详细信息。
   a. 选择工作环境。
   b. 选择Storage VM。
   c. 选择聚合。
   d. 查看新卷名称。

   新卷名称显示为原始卷名称+备份名称+备份日期。

5. 选择 * 保存 * 。
6. 选择 * 下一步 * 。
7. 查看您的选择。
8. 选择 * 还原 * 。
9. 从顶部菜单中选择*恢复*以查看恢复页面上的工作负载、其中操作状态将在各个状态之间移动。

在文件级别还原应用程序工作负载

1. 在“还原”页面的“还原范围”中，选择*by file*。
2. 在卷列表中、选择要还原的卷。
3. **Source**:选择Source旁边的向下箭头以查看详细信息。
   a. 选择要用于还原数据的还原点。

   BlueXP勒索软件保护会将最佳还原点标识为事件发生前的最新备份、并显示"建议"指示。

b. 最多选择100个文件或单个文件夹进行还原。

4. 目的地：选择目的地旁边的向下箭头可查看详细信息。
   a. 选择将数据还原到何处：原始源位置或您可以指定的备用位置。

> 虽然原始文件或目录将被还原的数据覆盖、但原始文件和文件夹名称将保持不变、除非您指定新名称。

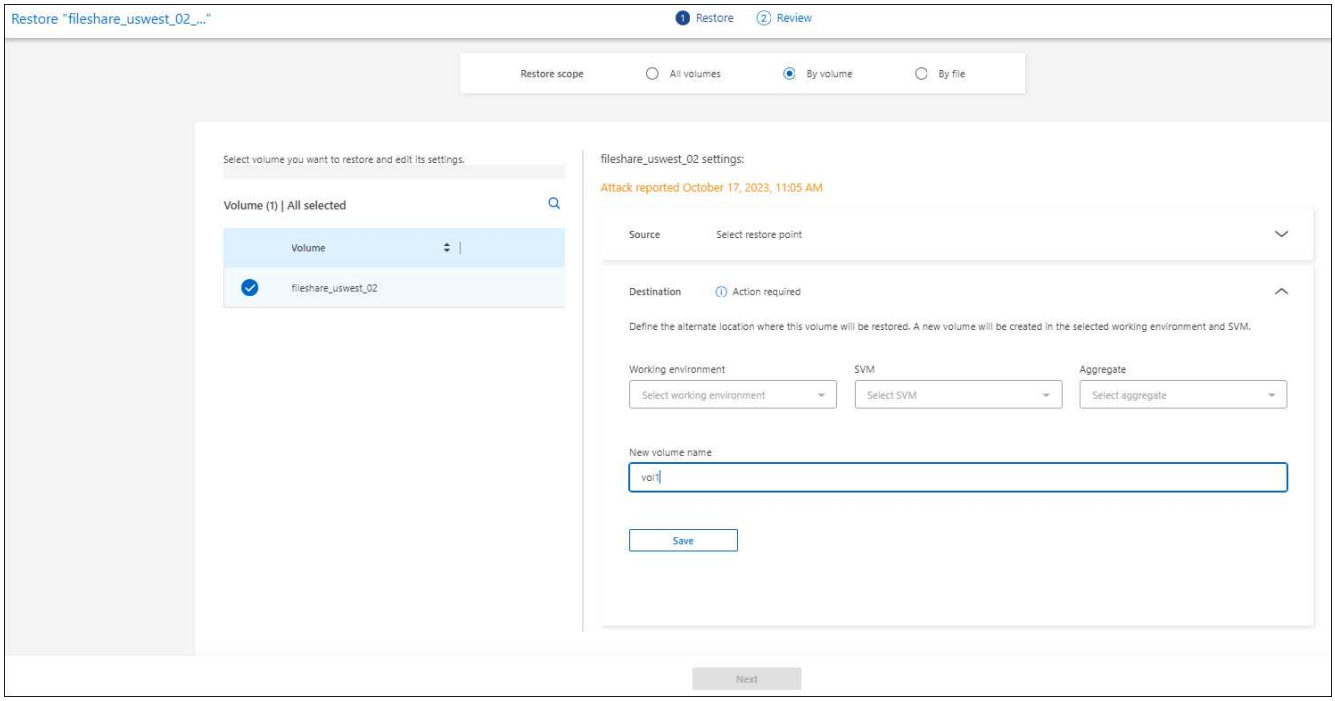
   b. 选择工作环境。
   c. 选择Storage VM。
   d. (可选)输入路径。

> 如果未指定还原路径、则这些文件将还原到顶级目录的新卷。

   e. 选择是希望恢复的文件或目录的名称与当前位置同名还是不同名称。
5. 选择 * 保存 * 。
6. 选择 * 下一步 * 。
7. 查看您的选择。
8. 选择 * 还原 * 。
9. 从顶部菜单中选择*恢复*以查看恢复页面上的工作负载、其中操作状态将在各个状态之间移动。

在卷或文件级别还原文件共享或数据存储库

1. 选择要还原的文件共享或数据存储库后、在还原页面的还原范围中、选择*按卷*或*按文件*。



2. 在卷列表中、选择要还原的卷。

3. **Source**:选择Source旁边的向下箭头以查看详细信息。
   a. 选择要用于还原数据的还原点。

   BlueXP勒索软件保护会将最佳还原点标识为事件发生前的最新备份、并显示"建议"指示。

4. 目的地：选择目的地旁边的向下箭头可查看详细信息。
   a. 选择将数据还原到何处：原始源位置或您可以指定的备用位置。

   虽然原始文件或目录将被还原的数据覆盖、但原始文件和文件夹名称将保持不变、除非您指定新名称。

   b. 选择工作环境。
   c. 选择Storage VM。
   d. (可选)输入路径。

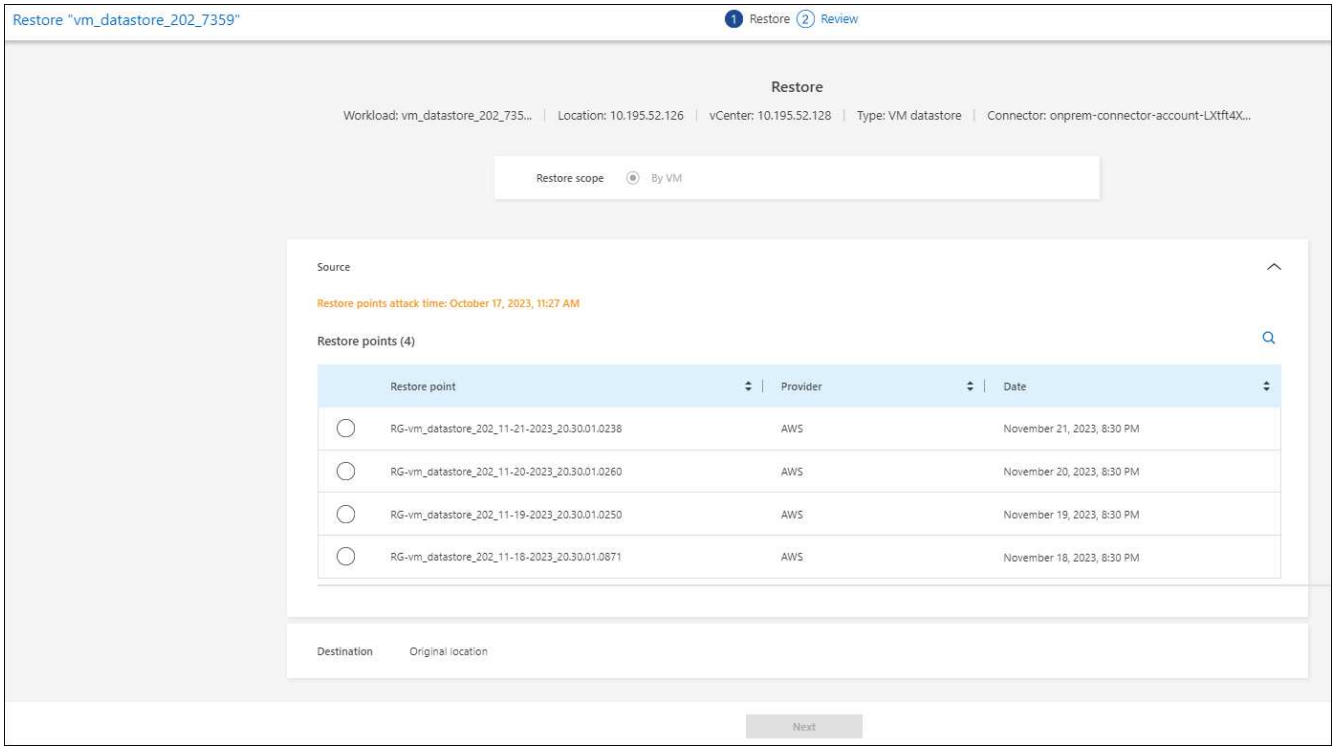
   如果未指定还原路径、则这些文件将还原到顶级目录的新卷。

5. 选择 * 保存 * 。
6. 查看您的选择。
7. 选择 * 还原 * 。
8. 从菜单中选择*恢复*以查看恢复页面上的工作负载、其中操作状态将在各个状态之间移动。

在虚拟机级别还原虚拟机文件共享

在选择要还原的虚拟机后的"RecRecovery (恢复)"页面上、继续执行以下步骤。

1. **Source**:选择Source旁边的向下箭头以查看详细信息。



2. 选择要用于还原数据的还原点。
3. 目的地：原始位置。
4. 选择 * 下一步 * 。
5. 查看您的选择。
6. 选择 * 还原 * 。
7. 从菜单中选择*恢复*以查看恢复页面上的工作负载、其中操作状态将在各个状态之间移动。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。