BlueXP勒索软件保护文档

BlueXP ransomware protection

NetApp
March 22, 2024

目录

BlueXP勒索软件保护文档

发行说明：BlueXP勒索软件保护的新增功能预览版

了解BlueXP勒索软件保护预览版中的新增功能。

2024年3月5日

此预览版BlueXP勒索软件保护包括以下更新：

- 保护策略管理：除了使用预定义策略之外，您现在还可以创建、更改和删除策略。 "了解有关管理策略的更多信息"。
- 二级存储上的不可更改性**(DataLock)**：现在、您可以在对象存储中使用NetApp DataLock技术使备份在二级存储上不可更改。 "了解有关创建保护策略的更多信息"。
- 自动备份到**AWS**：除了使用NetApp StorageGRID之外、您现在还可以选择StorageGRID作为备份目标。 "了解有关配置备份目标的更多信息"。
- 用于调查潜在攻击的其他功能：您现在可以查看更多取证详细信息来调查检测到的潜在攻击。 "详细了解如何响应检测到的勒索软件警报"。
- 恢复过程。恢复过程得到了改进。现在、您可以在一个工作流中逐个卷、恢复工作负载的所有卷、甚至恢复卷中的几个文件。 "详细了解如何从勒索软件攻击中恢复(在消除意外事件后)"。

"了解BlueXP勒索软件保护"。

2023年10月6日

BlueXP勒索软件保护服务是一种SaaS解决方案、用于保护数据、检测潜在攻击以及从勒索软件攻击中恢复数据。

对于预览版、该服务可保护各个BlueXP帐户之间基于应用程序的Oracle、MySQL、VM数据存储库和内部NAS存储上的文件共享以及AWS上的Cloud Volumes ONTAP (使用NFS协议)工作负载、并将数据备份到Amazon Web Services云存储。

BlueXP勒索软件保护服务可充分利用多种NetApp技术、以便您的数据安全管理员或安全运营工程师可以实现以下目标：

- 一目了然地查看所有工作负载上的勒索软件保护。
- 深入了解勒索软件保护建议
- 根据BlueXP勒索软件保护建议改善保护状况。
- 分配勒索软件保护策略、以保护您的首要工作负载和高风险数据免受勒索软件攻击。
- 监控工作负载的运行状况、防止勒索软件攻击发现数据异常。
- 快速评估勒索软件事件对工作负载的影响。
- 通过还原数据并确保存储的数据不会再次感染、从勒索软件事件中智能恢复。

"了解BlueXP勒索软件保护"。

入门

了解BlueXP勒索软件保护预览版

勒索软件攻击可能会阻止对系统和数据的访问、攻击者可能会索要赎金以换取数据释放或解密。据IDC调查、勒索软件受害者遭受多次勒索软件攻击的情况并不少见。攻击可能会中断一天到几周的数据访问。

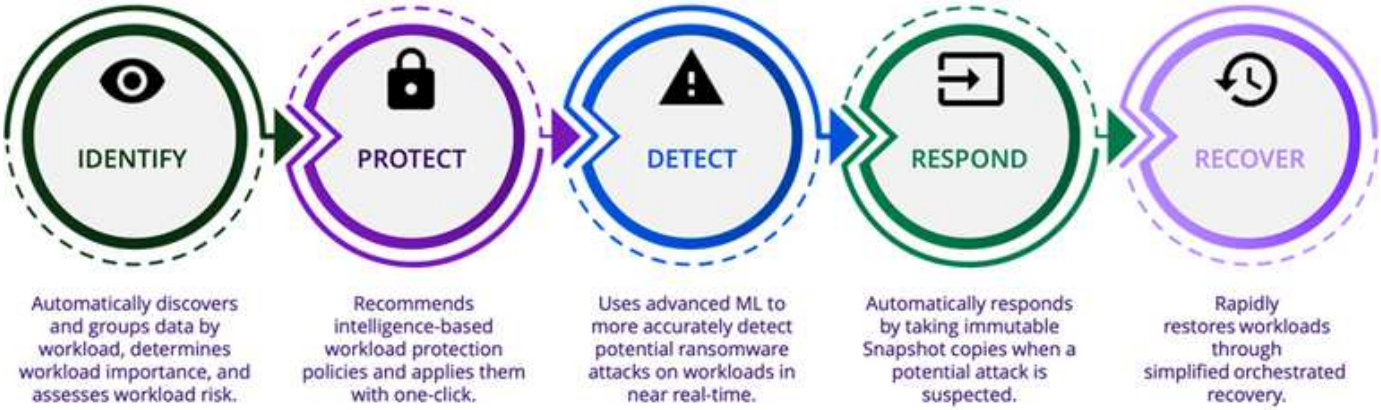
BlueXP勒索软件保护是一种用于勒索软件保护、检测和恢复的业务流程服务。对于预览版、该服务可保护Oracle、MySQL、VM数据存储库、 在内部NAS存储以及Amazon Web Services中的Cloud Volumes ONTAP (使用NFS协议)上跨BlueXP帐户共享文件、并将数据备份到Amazon Web Services云存储或NetApp StorageGRID。

> 本文档以技术预览形式提供。 对于此预览版产品、NetApp保留在正式发布之前修改产品详细信息、内容和时间表的权利。

BlueXP勒索软件保护功能的用途

BlueXP勒索软件保护服务可充分利用多种NetApp技术、以便存储管理员、数据安全管理员或安全运营工程师可以实现以下目标：

- *识别*在BlueXP中采用NFS工作环境的NetApp内部NAS中、跨BlueXP帐户、工作空间和BlueXP连接器的所有基于应用程序的工作负载、文件共享工作负载或由VMware管理的工作负载。然后、该服务会对数据优先级进行分类、并为您提供有关改进勒索软件保护的建议。
- *通过在数据上启用备份和Snapshot副本来保护*工作负载。
- *检测*可能是勒索软件攻击的异常。
- 通过自动启动**NetApp ONTAP Snapshot**副本对潜在的勒索软件攻击做出响应。
- *恢复*您的工作负载、通过编排多种NetApp技术帮助加快工作负载正常运行时间。您可以选择恢复卷、文件夹或特定文件。该服务可提供有关最佳选项的建议。



使用BlueXP勒索软件保护的优势

BlueXP勒索软件保护具有以下优势：

- 发现工作负载和数据集、根据使用情况索引分析优先级并对其相对重要性进行排名。
- 评估您的勒索软件保护态势、并将其显示在易于理解的信息板中。
- 根据发现和保护状况分析、提供有关后续步骤的建议。
- 通过一键访问应用AI/ML驱动的数据保护建议。
- 保护MySQL、Oracle、VMware数据存储库和文件共享等顶级基于应用程序的工作负载中的数据。
- 使用AI技术实时检测对主存储上数据的勒索软件攻击。
- 通过创建Snapshot副本并启动异常活动警报、针对检测到的潜在攻击启动自动操作。
- 应用精选恢复以满足RPO策略要求。BlueXP勒索软件保护可使用多种NetApp恢复服务编排从勒索软件事件中恢复的过程、包括BlueXP备份和恢复(原Cloud Backup)。

成本

NetApp不会因使用BlueXP勒索软件保护预览版而向您收费。

许可

BlueXP勒索软件保护预览版本身不需要任何特殊许可。 所有预览许可证均为评估许可证。

> 对于预览版、NetApp可帮助您设置评估版和任何所需的许可证。

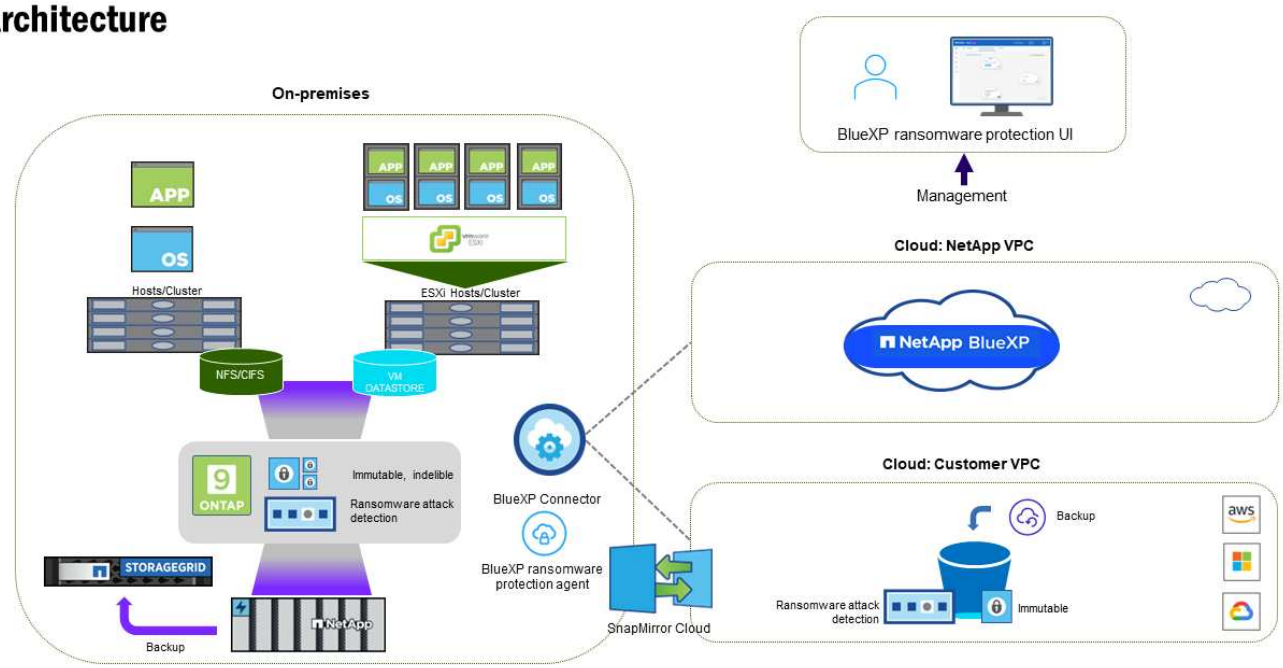
BlueXP勒索软件保护预览版需要以下许可证：

- ONTAP
- NetApp自主防网络软件保护技术。请参见 "自主勒索软件保护概述" 了解详细信息。
- BlueXP备份和恢复服务

BlueXP勒索软件保护的工作原理

总体而言、BlueXP勒索软件保护的工作原理是这样的。

Architecture



功能	Description
识别	• 查找连接到BlueXP的所有客户内部NAS (NFS挂载)数据。 • 识别ONTAP服务API中的客户数据、并将其与工作负载关联起来。了解更多信息 "ONTAP" 和 "SnapCenter 软件"。 • 发现每个卷的NetApp Snapshot副本和备份策略的当前保护级别以及任何机载检测功能。然后、该服务会使用BlueXP备份和恢复、BlueXP数字顾问以及ONTAP服务和NetApp技术(例如、自动防软件保护、FPolicy、备份策略和Snapshot策略)将此保护状态与工作负载关联起来。 了解更多信息 "自主勒索软件保护" 和 "BlueXP备份和恢复"， "BlueXP数字顾问"，和 "ONTAP FPolicy"。 • 根据自动发现的保护级别为每个工作负载分配业务优先级、并根据工作负载的业务优先级为其建议保护策略。 • 勒索软件保护还会了解策略关联、并为类似的工作负载推荐自定义策略。
保护	• 主动监控工作负载、并通过将策略应用于每个已识别的工作负载来编排BlueXP备份和恢复以及ONTAP API的使用。
检测	• 使用集成的机器学习(ML)模型检测潜在的攻击、该模型可检测潜在的异常加密和活动。 • 提供双层检测、从检测主存储中的潜在勒索软件攻击开始、并通过创建额外的自动Snapshot副本创建最近的数据还原点来响应异常活动。通过该服务、您可以更深入地挖掘、更精确地识别潜在攻击、而不会影响主工作负载的性能。 • 使用ONTAP、自动防软件保护和FPolicy技术确定攻击关联工作负载的特定可疑文件并映射到相关工作负载。

功能	Description
响应	• 显示相关数据、例如文件活动、用户活动和熵、以帮助您完成有关攻击的取证审查。 • 使用NetApp技术和产品(例如ONTAP、自动防兰软件保护和FPolicy)启动快速Snapshot副本。
恢复	• 使用BlueXP备份和恢复、ONTAP、自主防兰软件保护和FPolicy技术和服务确定最佳Snapshot或备份并建议最佳实际恢复点(RPA)。 • 协调工作负载(包括VM、文件共享和数据库)的恢复、确保应用程序一致性。

支持的备份目标、工作环境和数据源

使用BlueXP勒索软件保护预览查看数据在以下类型的备份目标、工作环境和数据源遭受网络攻击时的恢复能力：

支持的备份目标

- Amazon Web Services (AWS) S3
- NetApp StorageGRID

支持的工作环境

- 内部ONTAP NAS (使用NFS协议)
- ONTAP Select
- AWS中的Cloud Volumes ONTAP (使用NFS协议)

数据源

对于预览版、此服务可保护以下基于应用程序的工作负载：

- NetApp文件共享
- VMware 数据存储库
- 数据库(对于预览版本、Oracle和MySQL)

可能有助于您进行勒索软件保护的术语

了解一些与勒索软件保护相关的术语可能会让您受益匪浅。

- 保护：BlueXP勒索软件保护中的保护意味着确保使用保护策略定期向不同的安全域进行Snapshot和不可更改的备份。
- 工作负载：BlueXP勒索软件保护预览版中的工作负载可以包括MySQL或Oracle数据库、VMware数据存储库或文件共享。

BlueXP勒索软件保护前提条件

通过验证您的操作环境、登录、网络访问和Web浏览器是否已准备就绪、开始实施BlueXP

勒索软件保护。

要使用BlueXP勒索软件保护预览版、您需要满足以下前提条件：

- NetApp StorageGRID或AWS S3中用于备份目标和访问权限集的帐户

  请参见 "AWS权限列表" 了解详细信息。

- ONTAP 9.11.1及更高版本
  - 集群管理员ONTAP权限
  - NetApp自主勒索软件保护的许可证、由BlueXP勒索软件保护使用、在内部ONTAP实例上启用、具体取决于您使用的ONTAP版本。请参见 "自主勒索软件保护概述"。

    有关更多许可详细信息、请参见 "了解BlueXP勒索软件保护"。

- 在BlueXP中：
  - 必须在BlueXP中为每个虚拟私有云(Virtual Private Cloud、VPC)或内部区域设置一个BlueXP Connector。请参见 "BlueXP文档以配置连接器"。

    > 如果您有多个BlueXP连接器、该服务将扫描除当前显示在BlueXP UI中的连接器之外的所有连接器上的数据。

  - 在工作环境中启用了备份的BlueXP备份和恢复服务
  - 采用NetApp NAS内部存储的BlueXP工作环境
  - 至少有一个活动连接器连接到内部ONTAP集群的BlueXP帐户。所有源环境和工作环境都必须位于同一个BlueXP帐户中。
  - 具有用于发现资源的帐户管理员权限的BlueXP用户帐户
  - "标准BlueXP要求"

BlueXP勒索软件保护快速入门

下面概述了开始使用BlueXP勒索软件保护所需的步骤。每个步骤中的链接将转到一个页面，其中提供了更多详细信息。

1 查看前提条件

"确保您的环境满足这些要求"。

2 设置勒索软件保护服务

- "准备NetApp StorageGRID或Amazon Web Services作为备份目标"。
- "在BlueXP中配置连接器"。
- "配置备份目标"。
- "在BlueXP中发现工作负载"。

3 下一步是什么?

设置服务后、接下来可以执行以下操作。

- "在信息板上查看工作负载保护运行状况"。
- "保护工作负载"。
- "响应对潜在勒索软件攻击的检测"。
- "从攻击中恢复(在消除意外事件后)"。

设置BlueXP勒索软件保护

要使用BlueXP勒索软件保护、请执行几个步骤进行设置。

开始之前、请查看 "前提条件" 以确保您的环境已准备就绪。

准备备份目标

准备以下备份目标之一:

- NetApp StorageGRID
- Amazon Web Services

在备份目标本身中配置选项后、您可以稍后在BlueXP勒索软件保护服务中将其配置为备份目标。

准备**StorageGRID**以成为备份目标

如果要使用StorageGRID作为备份目标、请参见 "StorageGRID 文档" 有关StorageGRID的详细信息、请参见。

准备**AWS**以成为备份目标

- 在AWS中设置帐户。
- 配置 "AWS权限" 在AWS中。

有关在BlueXP中管理AWS存储的详细信息、请参见 "管理Amazon S3存储分段"。

设置**BlueXP**

下一步是设置BlueXP和BlueXP勒索软件保护服务。

请查看 "标准BlueXP要求"。

在**BlueXP**中创建连接器

您应联系NetApp销售代表试用此服务。然后、当您使用BlueXP Connector时、它将包括勒索软件保护服务的相应功能。

要在使用此服务之前在BlueXP中创建Connector、请参阅所述的BlueXP文档 "如何创建BlueXP Connector"。

> 如果您有多个BlueXP连接器、该服务将扫描除当前显示在BlueXP UI中的连接器之外的所有连接器上的数据。此服务将发现与此帐户关联的所有工作空间和所有连接器。

访问**BlueXP**勒索软件保护

您可以使用NetApp BlueXP登录到BlueXP勒索软件保护服务。从BlueXP左侧导航栏中、选择*保护*>*防软件保护*。

有关详细信息，请参见 "访问BlueXP勒索软件保护"。

在**BlueXP**勒索软件保护中配置备份目标

使用BlueXP勒索软件保护备份目标选项配置备份目标。有关详细信息，请参见 "配置设置选项"。

访问**BlueXP**勒索软件保护

您可以使用NetApp BlueXP登录到BlueXP勒索软件保护服务。

要登录到BlueXP、您可以使用NetApp 支持站点 凭据、也可以使用电子邮件和密码注册NetApp云登录。 "了解有关登录的更多信息"。

步骤

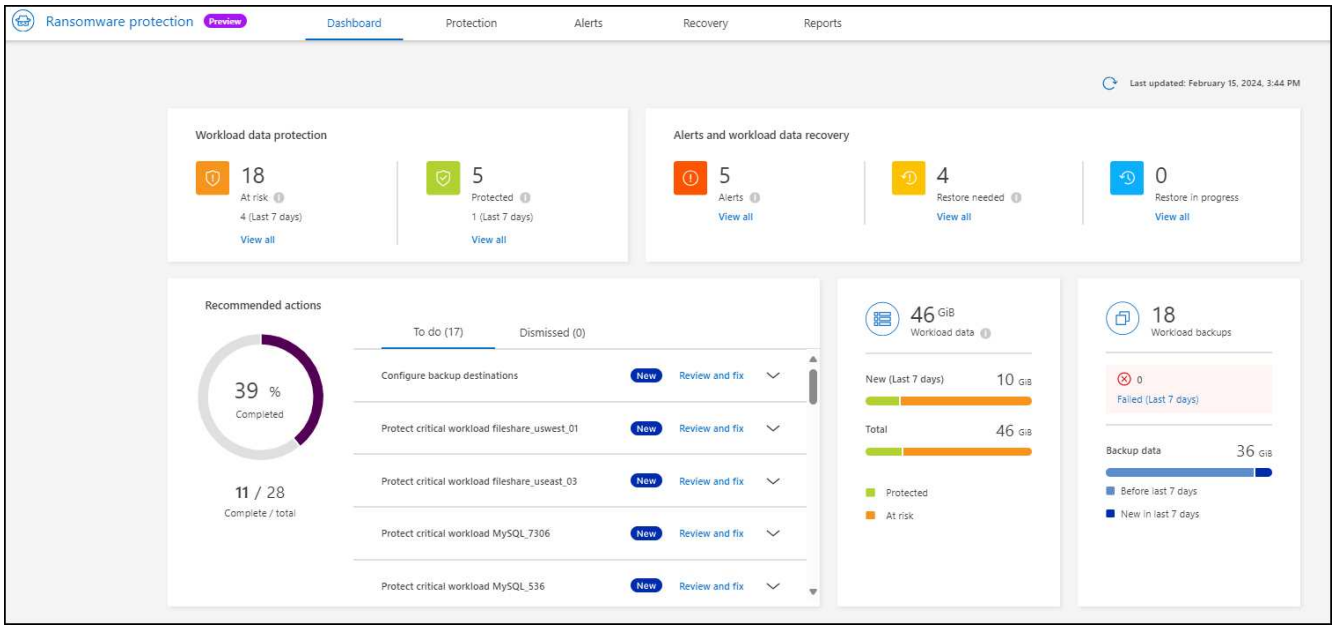
1. 打开Web浏览器并转到 "BlueXP控制台"。

   此时将显示NetApp BlueXP登录页面。

2. 登录到BlueXP。
3. 从BlueXP左侧导航栏中、选择*保护*>*防软件保护*。

   如果这是您首次登录此服务、则会显示登录页面。

   否则、将显示BlueXP勒索软件保护信息板。



4. 开始使用此服务。
   - 如果您没有BlueXP连接器或它不是此预览版的连接器、您可能需要联系NetApp支持部门或按照消息注册此预览版。
   - 如果您是BlueXP的新用户且尚未使用任何Connector、则在选择"防软件保护"时、将显示一条有关注册的消息。请继续并提交表单。NetApp将就您的评估请求与您联系。
   - 如果您是具有现有Connector的BlueXP用户、则在选择"防软件保护"时、将显示有关注册的消息。
   - 如果您已经参与了预览，则在选择“防系统保护”时，您可以继续使用该服务。如果尚未选择*发现工作负载*选项，则应选择此选项。

在BlueXP勒索软件保护中发现工作负载

要使用BlueXP勒索软件保护、该服务需要首先发现数据。在发现期间、BlueXP勒索软件保护功能会分析帐户中所有BlueXP连接器和工作空间中工作环境中的所有卷和文件。

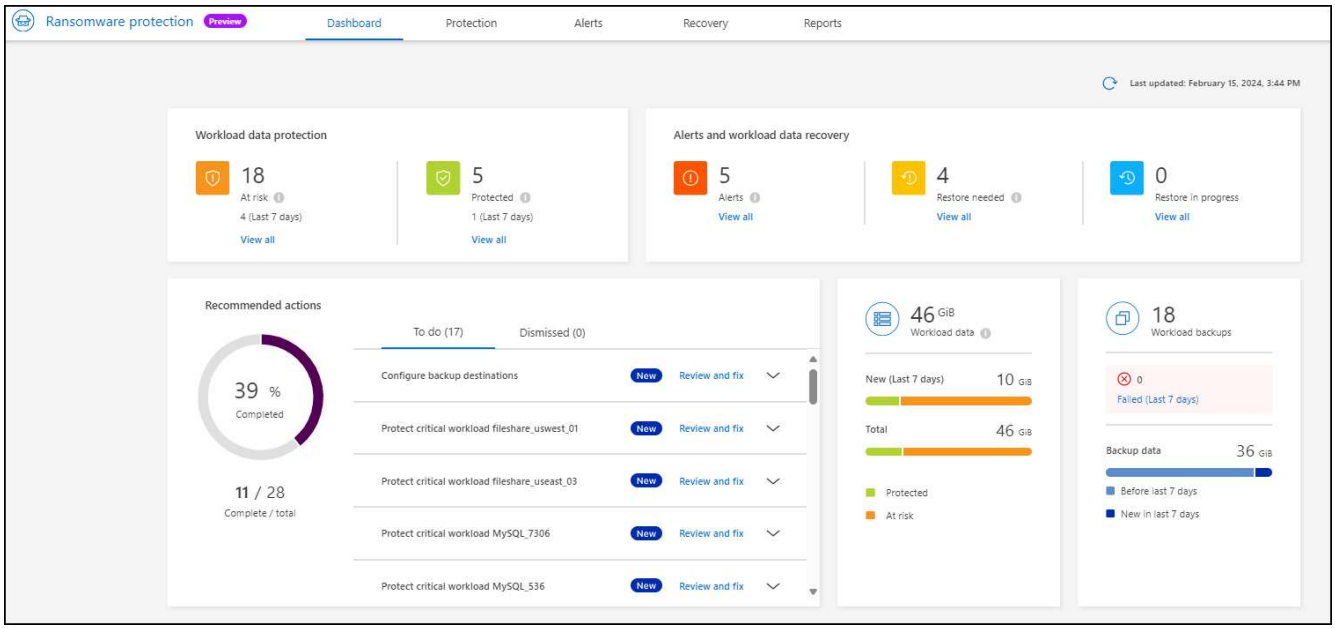
> 对于预览版、BlueXP勒索软件保护可评估MySQL应用程序、Oracle应用程序、VMware数据存储库和文件共享。

该服务会评估现有保护级别、包括当前备份保护、Snapshot副本和NetApp自动防软件保护选项。然后、该服务会根据评估结果建议如何改进勒索软件保护。

步骤

1. 从BlueXP左侧导航栏中、选择*保护*>*防软件保护*。
2. 从初始登录页面中选择*发现工作负载*。

   此服务会发现工作负载数据、并在信息板中显示数据保护的运行状况。



配置BlueXP勒索软件保护设置

您可以通过查看信息板上的建议来配置备份目标。

添加备份目标

BlueXP勒索软件保护可以识别尚未进行任何备份的工作负载以及尚未分配任何备份目标的工作负载。

要保护这些工作负载、您应添加一个备份目标。您可以选择以下备份目标之一：

- NetApp StorageGRID
- Amazon Web Services （AWS）

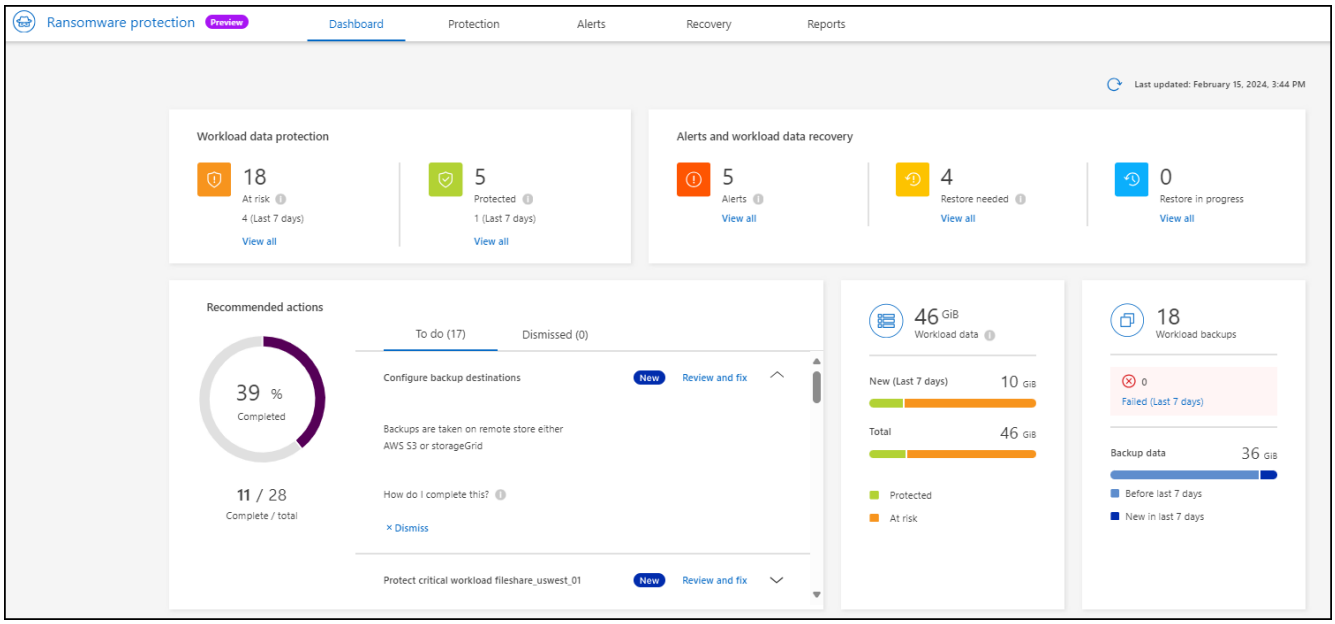
您可以根据信息板中的建议操作添加备份目标。

从信息板的建议操作访问备份目标选项

信息板提供了许多建议。其中一个建议可能是配置备份目标。

步骤

1. 从BlueXP左侧导航栏中、选择*保护*>*防软件保护*。
2. 查看信息板的"建议操作"窗格。

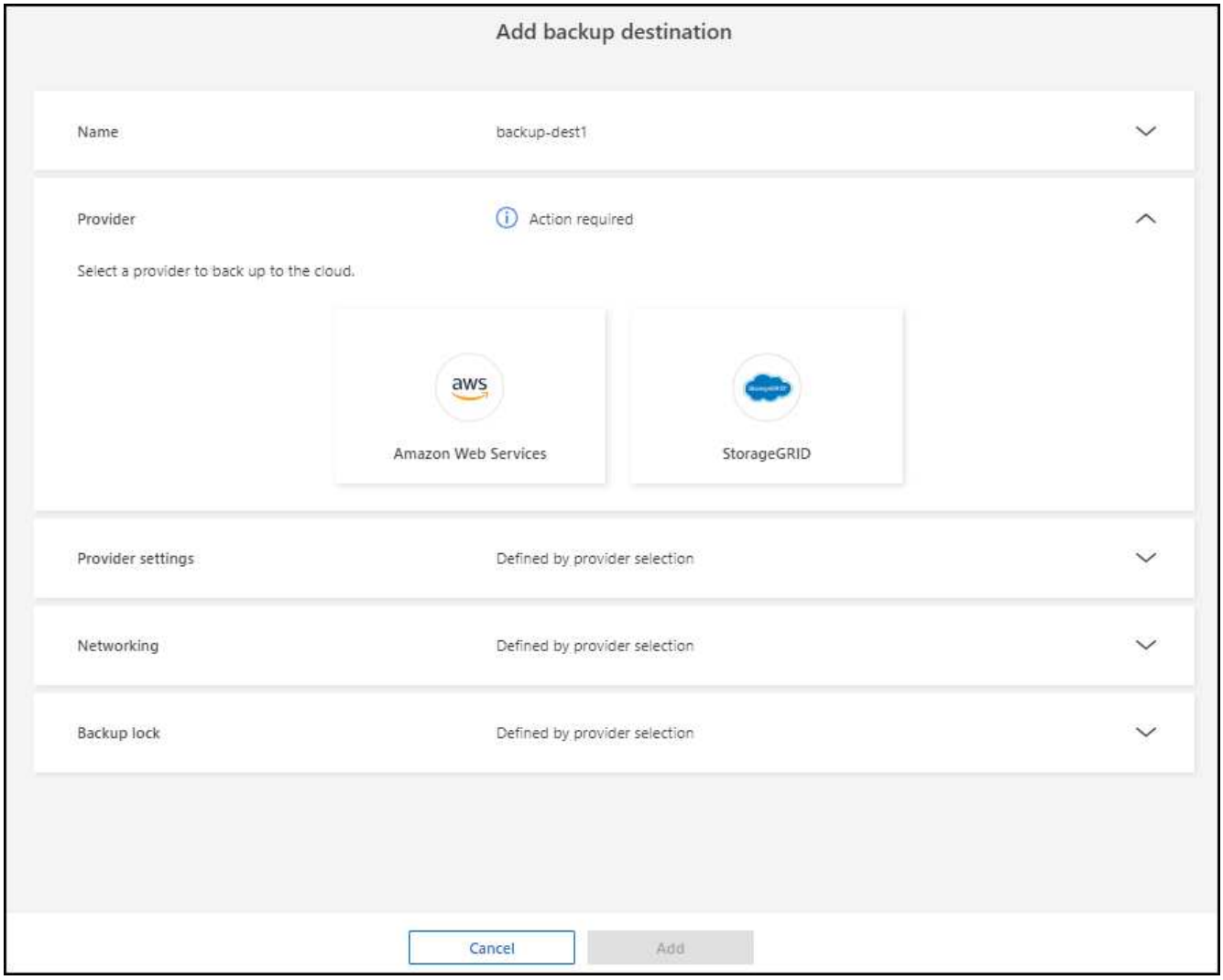


3. 从信息板中，选择*Review and fix*以获取“配置备份目标”的建议。
4. 根据备份提供程序继续执行说明。

将StorageGRID添加为备份目标

要将NetApp StorageGRID设置为备份目标、请输入以下信息。

1. 在*设置>备份目的地*页面中，选择*添加*。
2. 输入备份目标的名称。



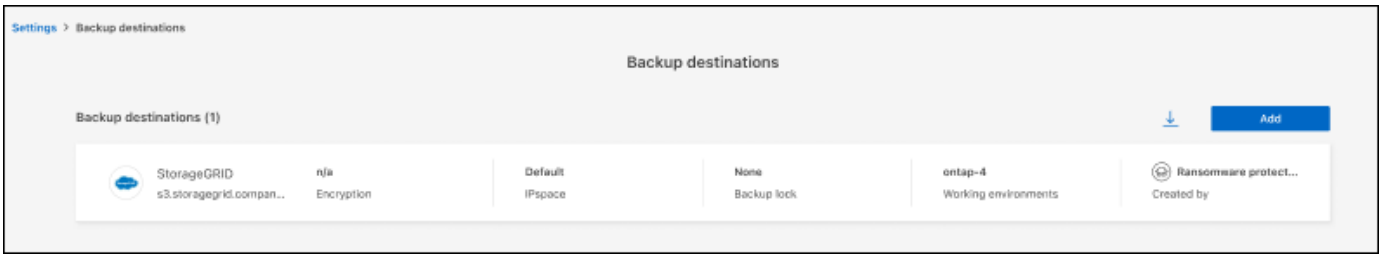
3. 选择* StorageGRID *。
4. 选择每个设置旁边的向下箭头、然后输入或选择值：
   - 提供者设置：
     - 创建新存储分段或自带存储分段来存储备份。
     - StorageGRID网关节点完全限定域名、端口、StorageGRID访问密钥和机密密钥凭据。
   - 联网：选择IP空间。
     - IP空间是要备份的卷所在的集群。此 IP 空间的集群间 LIF 必须具有出站 Internet 访问权限。
   - **Backup lock**:选择您希望服务保护备份不被修改或删除。此选项使用NetApp数据锁技术。每个备份都将在保留期限内锁定、或者至少锁定30天、再加上长达14天的缓冲期。

     如果您现在配置备份锁定设置、则在配置备份目标后、您将无法稍后更改该设置。

     - 合规模式：用户在保留期间无法覆盖或删除受保护的备份文件。
5. 选择 * 添加 * 。

结果

新备份目标将添加到备份目标列表中。

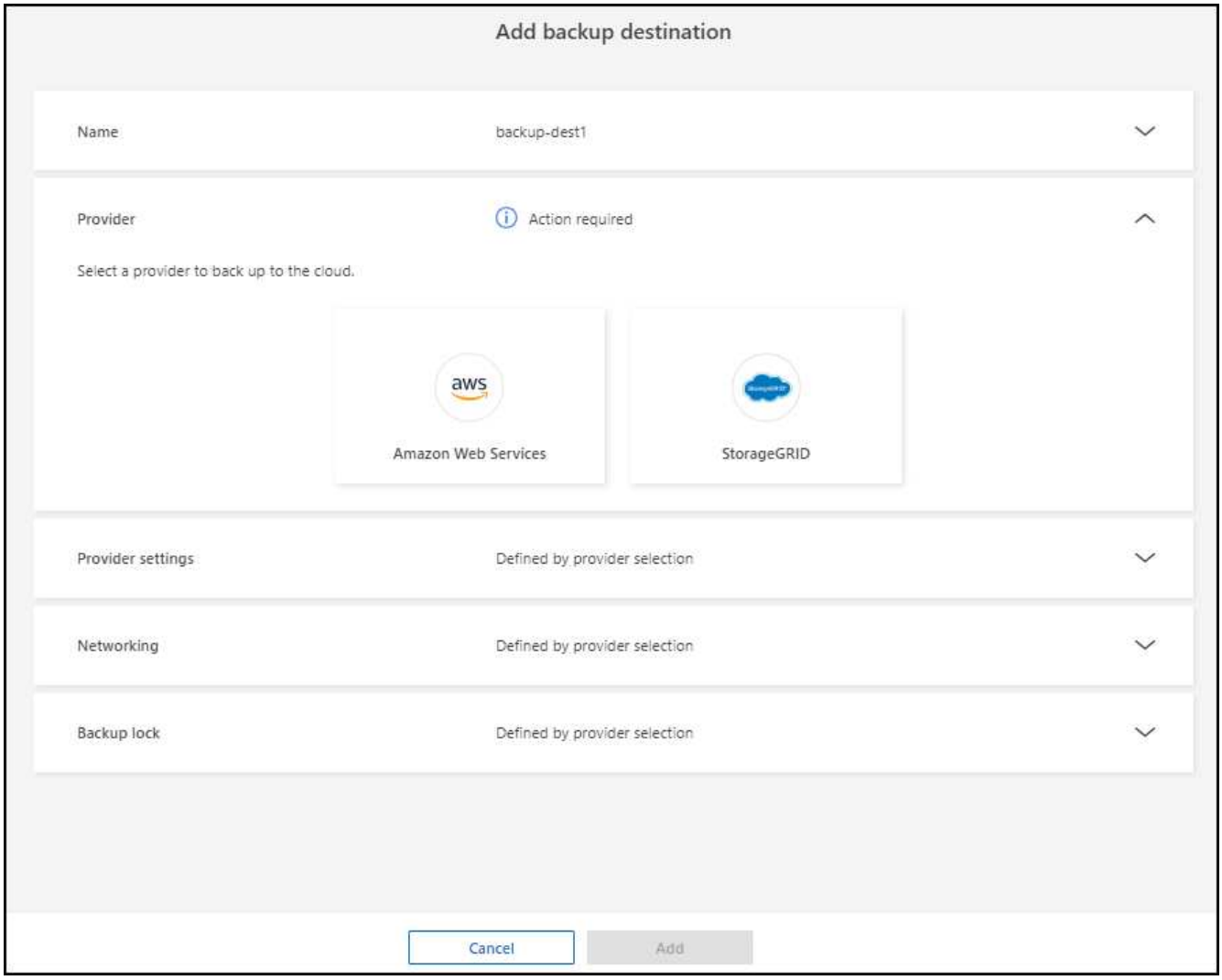


将Amazon Web Services添加为备份目标

要将AWS设置为备份目标、请输入以下信息。

有关在BlueXP中管理AWS存储的详细信息、请参见 "管理Amazon S3存储分段"。

1. 在*设置>备份目的地*页面中，选择*添加*。
2. 输入备份目标的名称。



3. 选择* Amazon Web Services*。
4. 选择每个设置旁边的向下箭头、然后输入或选择值：

- 提供者设置：
  - 创建新存储分段、如果BlueXP中已存在现有存储分段、则选择现有存储分段、或者自带存储分段来存储备份。
  - AWS帐户、区域、AWS凭据的访问密钥和机密密钥

    "如果要自带存储分段、请参见添加S3存储分段"。

- 加密：如果要创建新的S3存储分段，请输入提供程序提供给您的加密密钥信息。如果您选择了现有存储分段、则加密信息已可用。

  默认情况下、存储分段中的数据使用AWS管理的密钥进行加密。您可以继续使用AWS管理的密钥、也可以使用自己的密钥管理数据加密。

- 联网：选择IP空间以及是否使用专用端点。
  - IP空间是要备份的卷所在的集群。此 IP 空间的集群间 LIF 必须具有出站 Internet 访问权限。
  - (可选)选择是否使用先前配置的AWS专用端点(PrivateLink)。

    如果要使用AWS PrivateLink、请参见 "适用于Amazon S3的AWS PrivateLink"。

- **Backup lock**:选择您希望服务保护备份不被修改或删除。此选项使用NetApp数据锁技术。每个备份都将在保留期限内锁定、或者至少锁定30天、再加上长达14天的缓冲期。

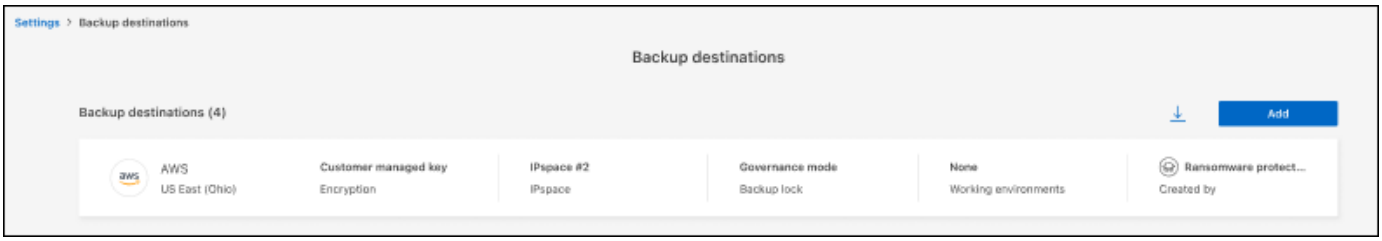
  ! 如果您现在配置备份锁定设置、则在配置备份目标后、您将无法稍后更改该设置。

  - 监管模式：特定用户(具有S3：BypassGovernance保留 权限)可以在保留期间覆盖或删除受保护的文件。
  - 合规模式：用户在保留期间无法覆盖或删除受保护的备份文件。

5. 选择 * 添加 * 。

结果

新备份目标将添加到备份目标列表中。



BlueXP勒索软件保护的常见问题

如果您只是想快速了解问题解答，此常见问题解答会很有帮助。

访问

什么是**BlueXP**勒索软件保护**URL**?
对于URL、在浏览器中输入： "https://console.bluexp.netapp.com/" 以访问BlueXP控制台。

要使用**BlueXP**勒索软件防护、您是否需要许可证？
不需要NetApp许可证文件(NLF)。BlueXP勒索软件保护预览版本身不需要任何特殊许可。 所有预览许可证均为评估许可证。

此服务的预览版本需要BlueXP备份和恢复服务许可证。

> 对于预览版、NetApp可帮助您设置评估版和任何所需的许可证。

如何启用**BlueXP**勒索软件保护？
BlueXP勒索软件保护不需要任何支持。BlueXP左侧导航栏会自动启用勒索软件保护选项。

要获得预览版、您需要注册或联系NetApp销售代表试用此服务。然后、当您使用BlueXP Connector时、它将包括适用于此服务的功能。

- BlueXP勒索软件保护是否可在标准模式、受限模式和专用模式下使用？**
  目前、BlueXP勒索软件保护仅在标准模式下可用。敬请关注更多信息。

有关所有BlueXP服务中这些模式的说明、请参阅 "BlueXP部署模式"。

如何处理访问权限？
只有帐户管理员才能启动服务并发现工作负载(因为这涉及到承诺使用资源)。后续交互可由任何角色完成。

哪种设备分辨率是最佳的？
BlueXP勒索软件保护的建议设备分辨率为1、1080或更高。

我应该使用哪种浏览器？
任何现代浏览器都能正常工作。

与其他服务的交互

BlueXP勒索软件保护是否了解**NetApp ONTAP**中的保护设置？
是的、BlueXP勒索软件保护功能可发现ONTAP中设置的Snapshot计划。

如果您使用**BlueXP**勒索软件保护设置策略，您将来是否只需要对此服务进行更改？
我们建议您通过BlueXP勒索软件保护服务更改策略。

工作负载

工作负载由什么组成？
工作负载包括单个应用程序实例使用的所有卷。例如、部署在ora3.host.com上的Oracle数据库实例的数据和日志可以分别使用vol1和vol2。这些卷共同构成该Oracle数据库实例的特定实例的工作负载。

BlueXP勒索软件保护如何划分工作负载数据的优先级？
预览版的数据优先级由创建的Snapshot副本和计划的备份决定。

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

已添加新卷，但尚未显示
如果向环境添加了新卷、请重新启动发现并应用保护策略来保护此新卷。

信息板未显示我的所有工作负载。可能会出什么问题?
目前仅支持NFS卷。系统会筛选出iSCSI卷、CIFS卷和其他不受支持的配置、这些配置不会显示在信息板上。

保护策略

- BlueXP勒索软件策略是否与其他类型的工作负载策略共存？*
  目前、BlueXP备份和恢复(Cloud Backup)支持每个卷一个备份策略。因此、BlueXP备份和恢复以及BlueXP勒索软件保护共享备份策略。

Snapshot副本不受限制、可以与每个服务分开添加。

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。

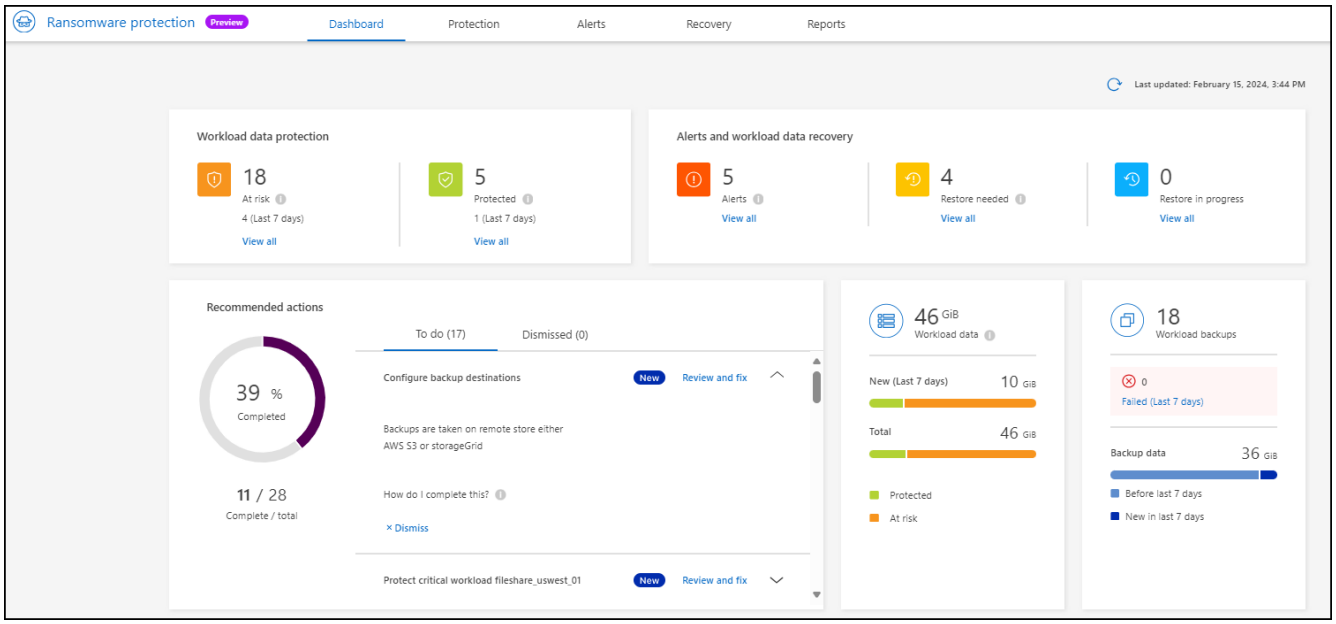
您还可以使用信息板查看保护建议并采取相应措施。

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。

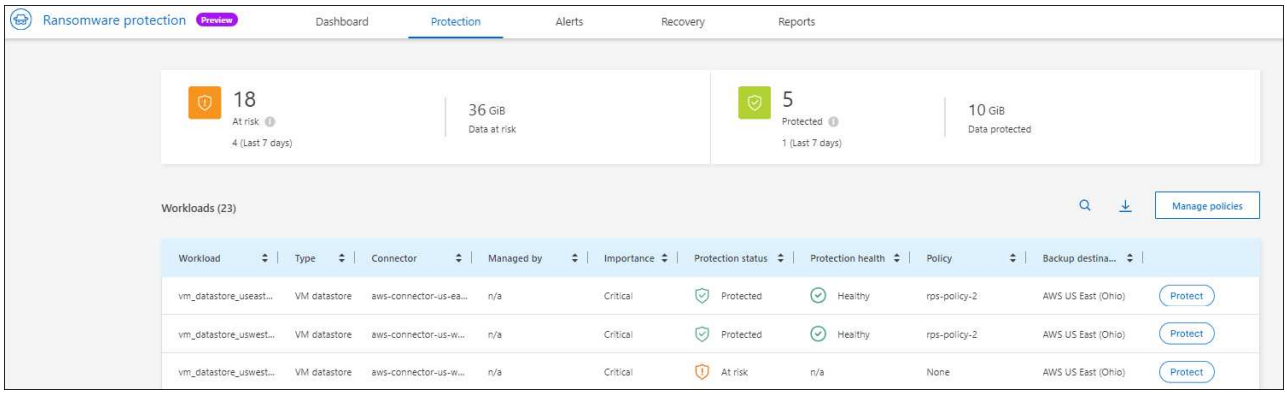
查看工作负载勒索软件保护

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。

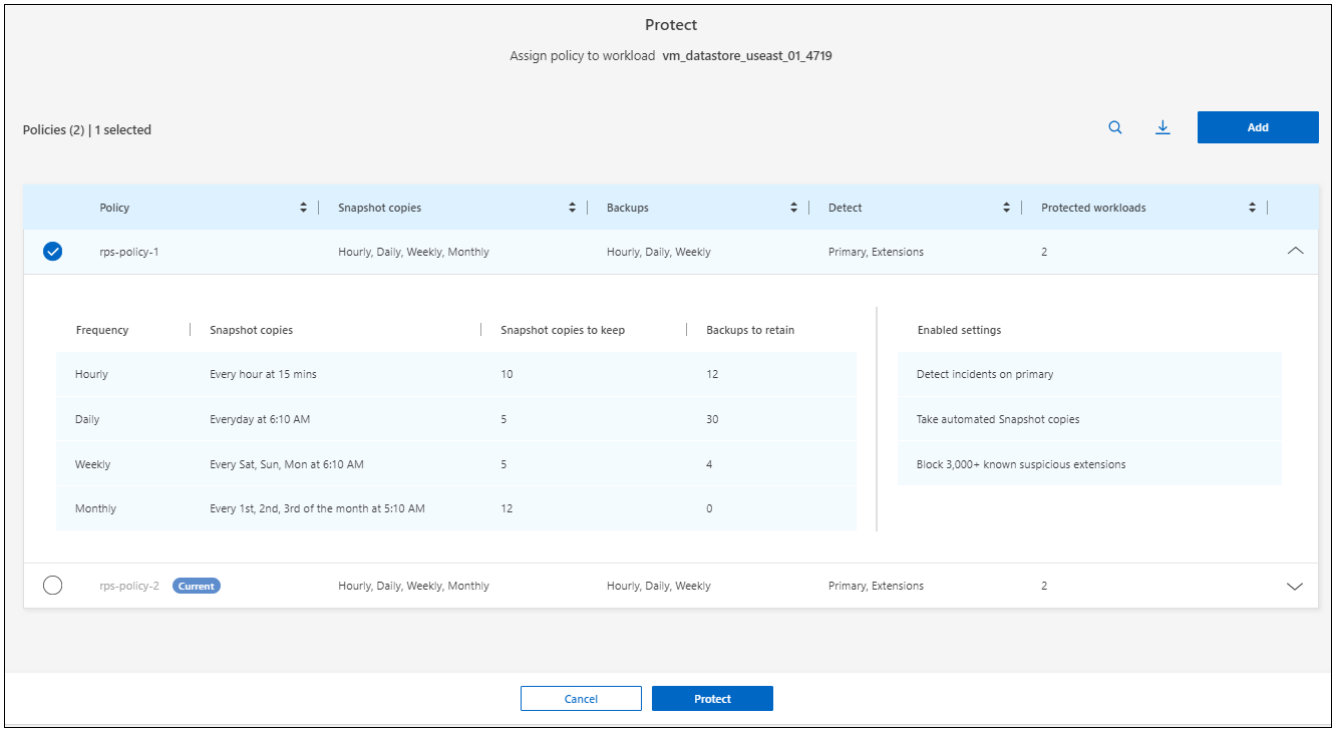
BlueXP勒索软件保护包括以下与工作负载优先级一致的预定义策略：

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

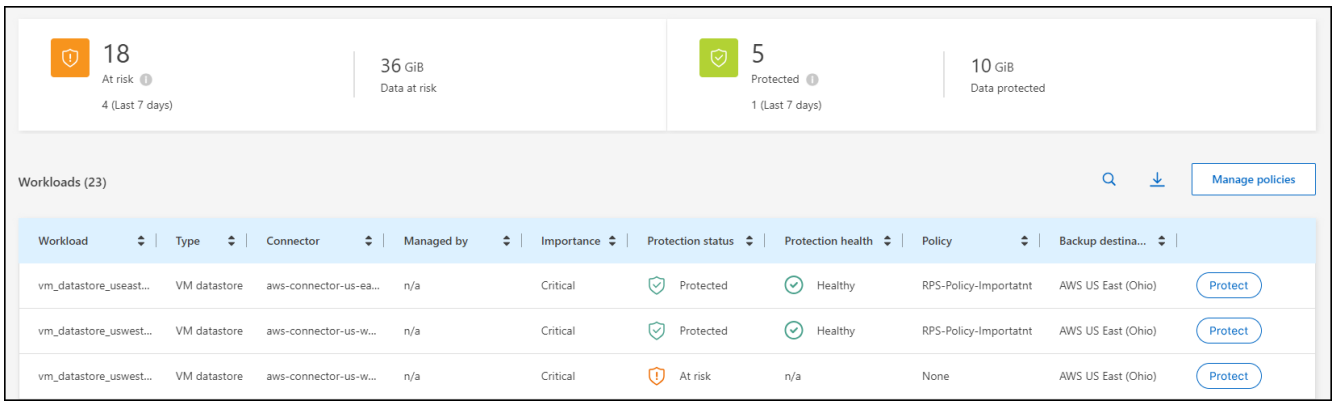
如果现有策略不能满足您的业务需求、您可以创建新的保护策略。您可以从头开始创建自己的策略、也可以使用现有策略并修改其设置。

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。

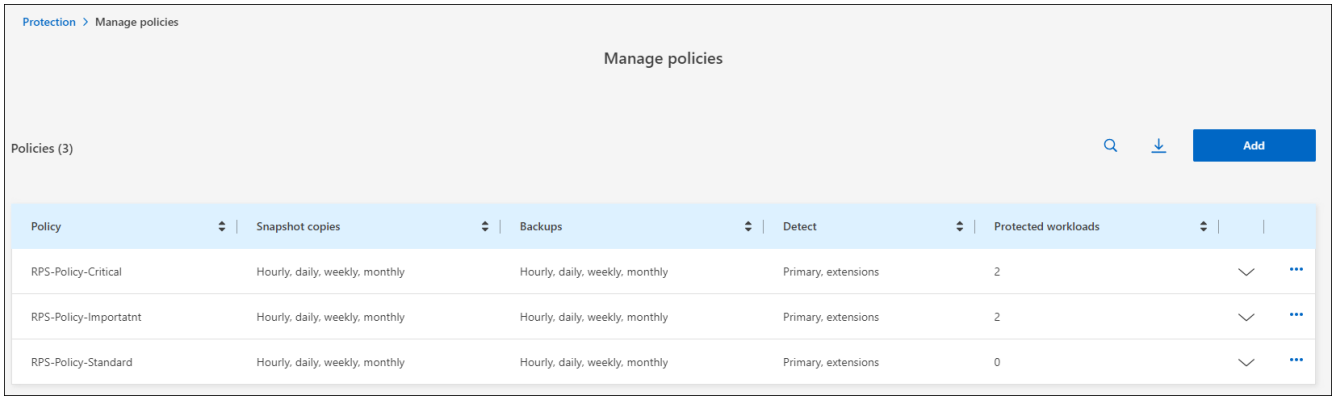
您可以在管理策略时或在将策略分配给工作负载的过程中创建策略。

策略管理期间创建策略的步骤

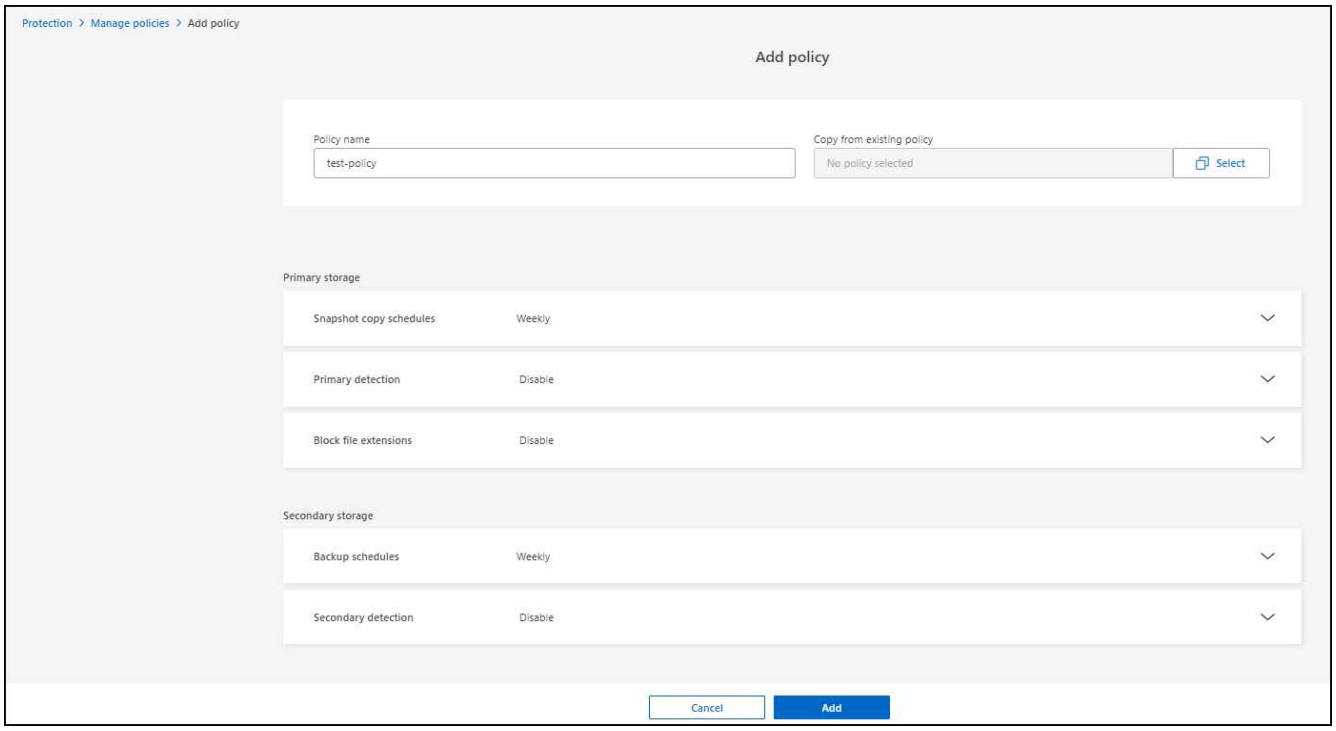
1. 从BlueXP勒索软件保护菜单中、选择*保护*。



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。

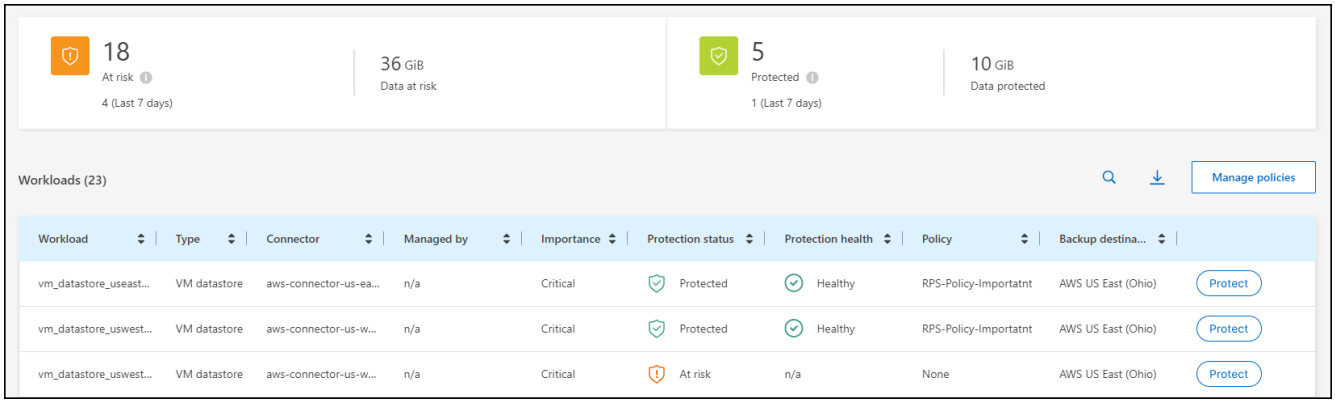
> 如果选择复制和修改现有策略、则必须至少更改一个设置、使其唯一。

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_。

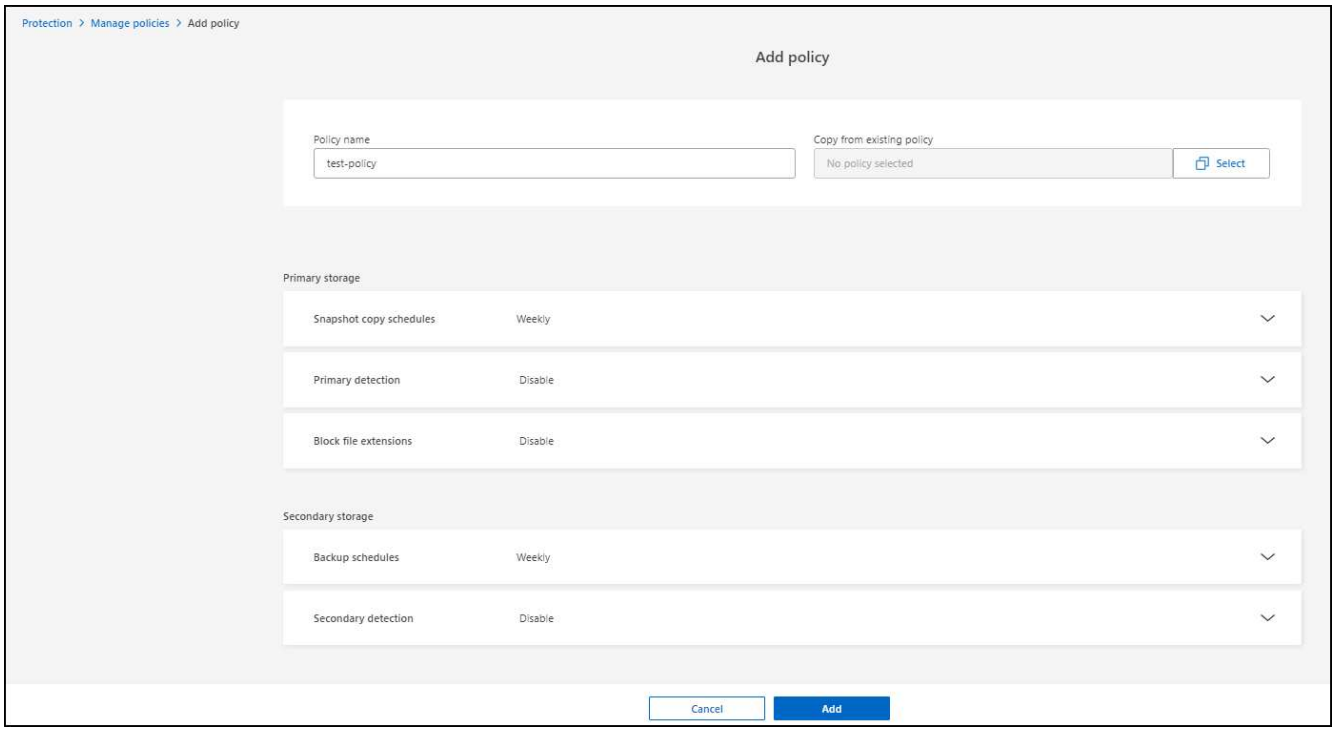
       此选项使用NetApp DataLock技术、该技术可锁定二级存储上的备份。备份文件锁定(并保留)的时间段称为DataLock保留期限。它基于您定义的备份策略计划和保留设置以及14天的缓冲区。任何少于30天的DataLock保留策略将取整为最短30天。
6. 选择 * 添加 * 。

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"。

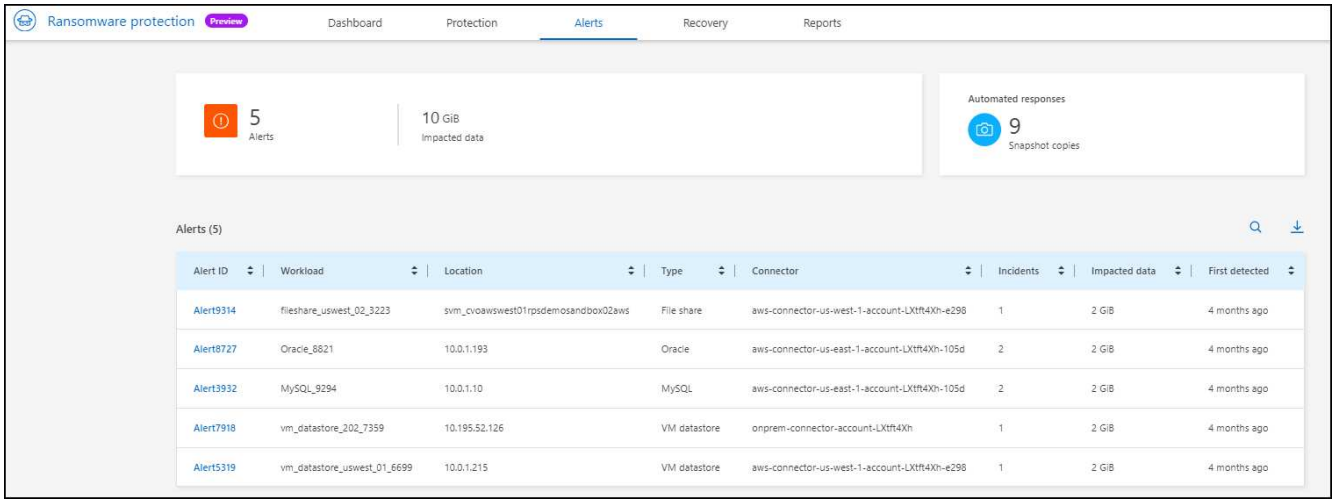
查看警报

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。



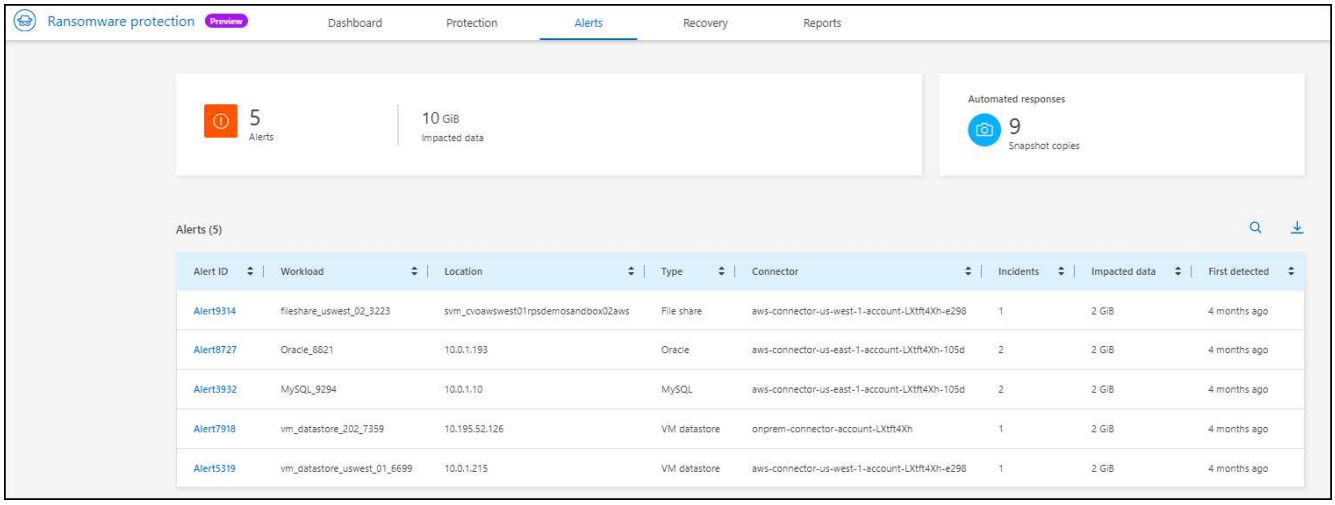
6. 继续 [将勒索软件事件标记为已做好恢复准备(在消除意外事件后)]。

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)

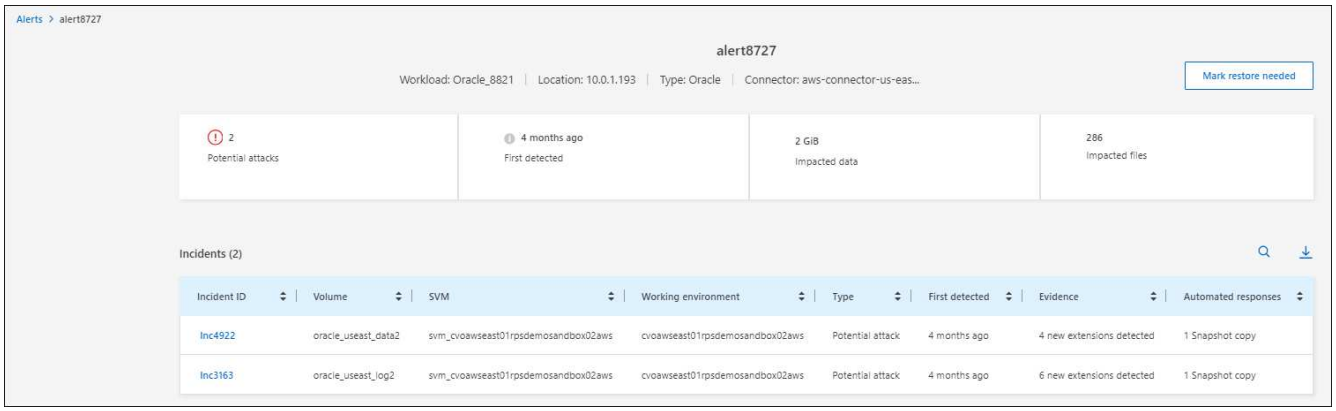
在缓解了攻击并准备好恢复工作负载之后、您应与存储管理团队沟通、指出数据已准备好进行恢复、以便他们可以启动恢复过程。

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)

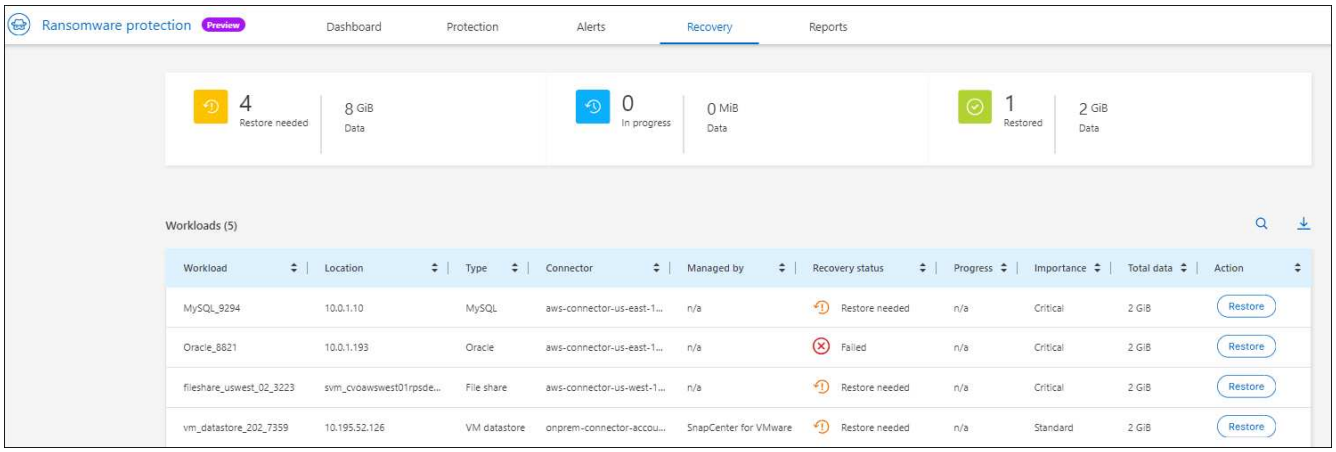
工作负载标记为"准备恢复"后、BlueXP勒索软件保护会建议使用实际恢复点(Recovery Point、RPA)、并编排工作流以实现防崩溃恢复。

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

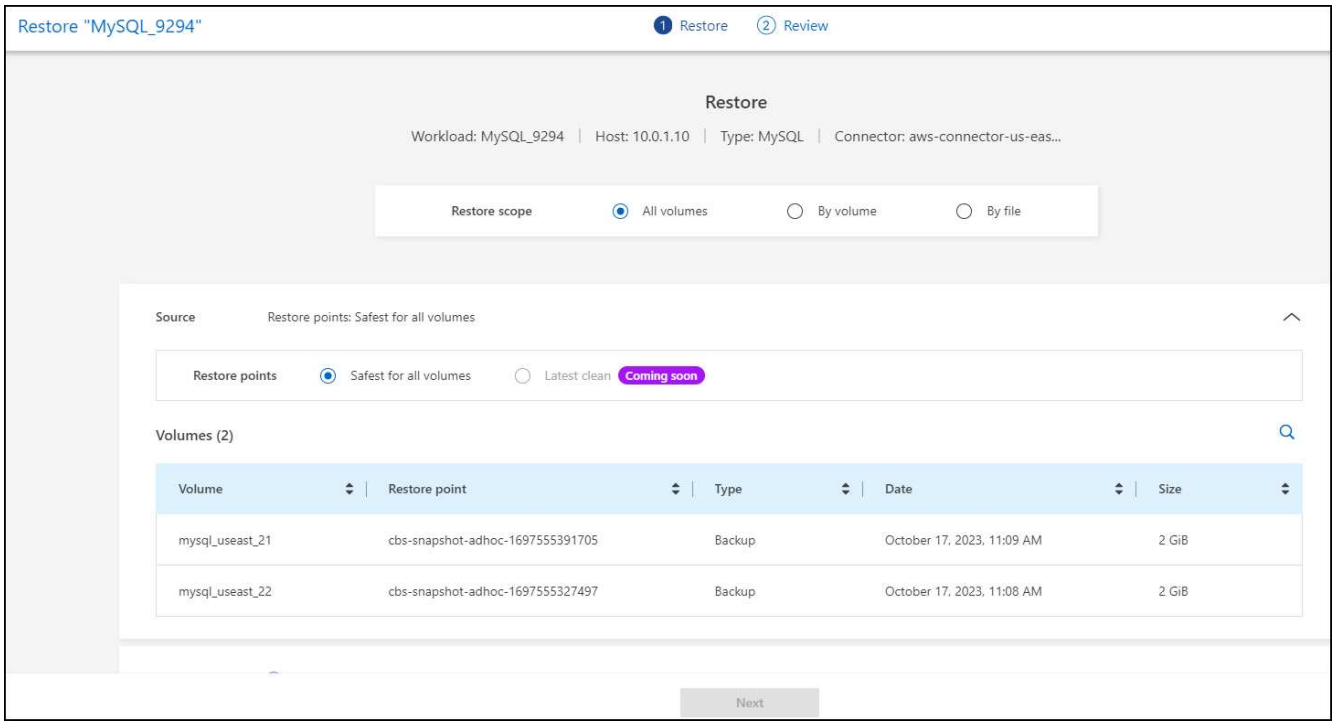
1. 从BlueXP勒索软件保护菜单中、选择*恢复*。
2. 查看*Recy过程*页面中的工作负载信息。
3. 选择处于"Restore Need"状态的工作负载。
4. 要恢复，请选择*Restore*。
5. 恢复范围：选择要完成的恢复类型：
    - 所有卷
    - 按卷
    - 按文件：您可以指定要还原的文件夹或单个文件。

    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。

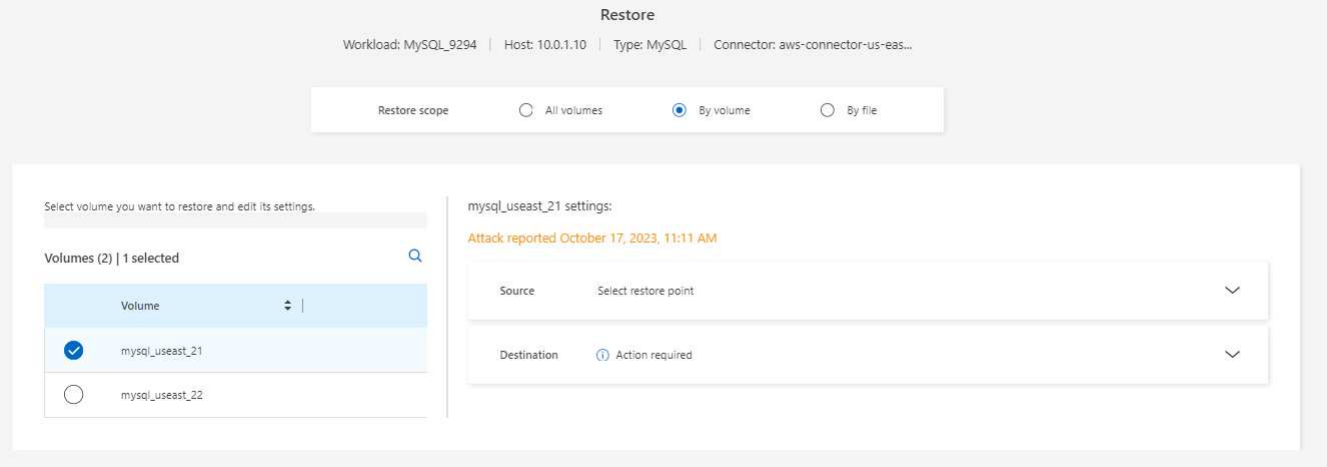
3. 目的地：选择目的地旁边的向下箭头可查看详细信息。
   a. 选择工作环境。
   b. 选择Storage VM。
   c. 选择聚合。
   d. 更改要在所有新卷之前添加的卷前缀。

> 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。

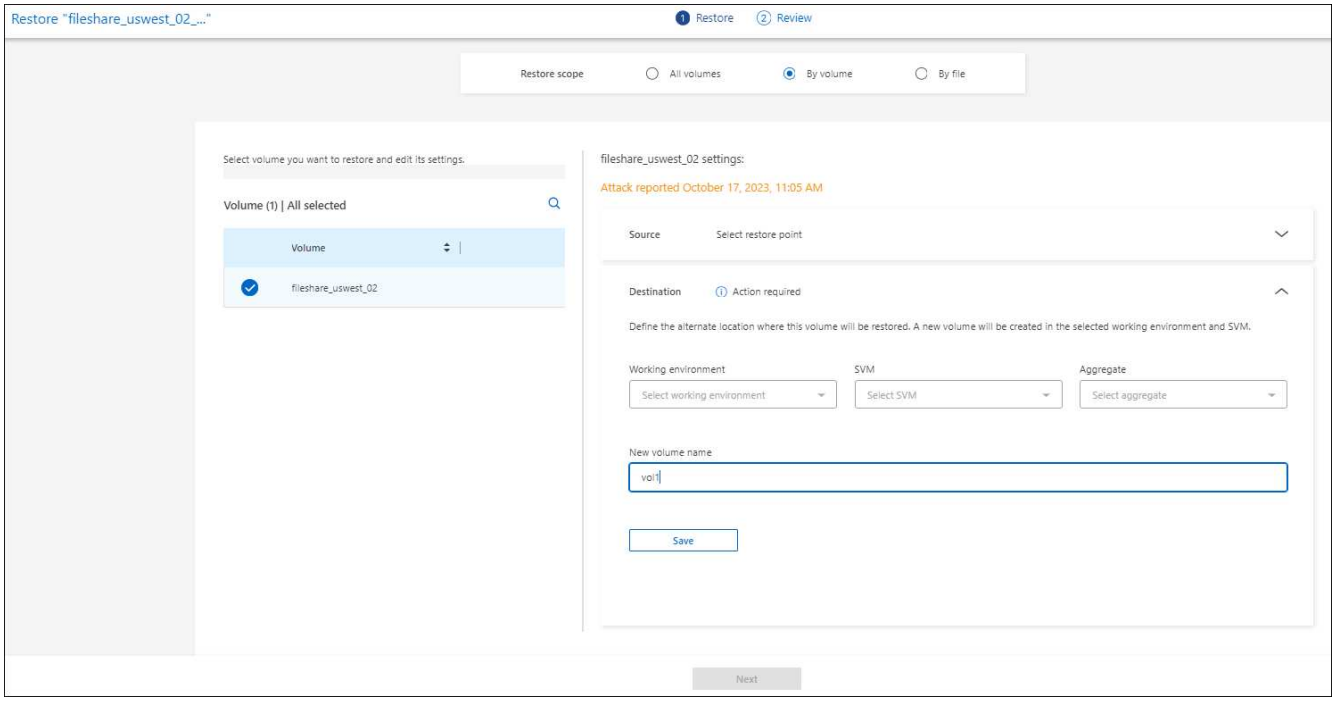
   b. 选择工作环境。
   c. 选择Storage VM。
   d. (可选)输入路径。

> 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。

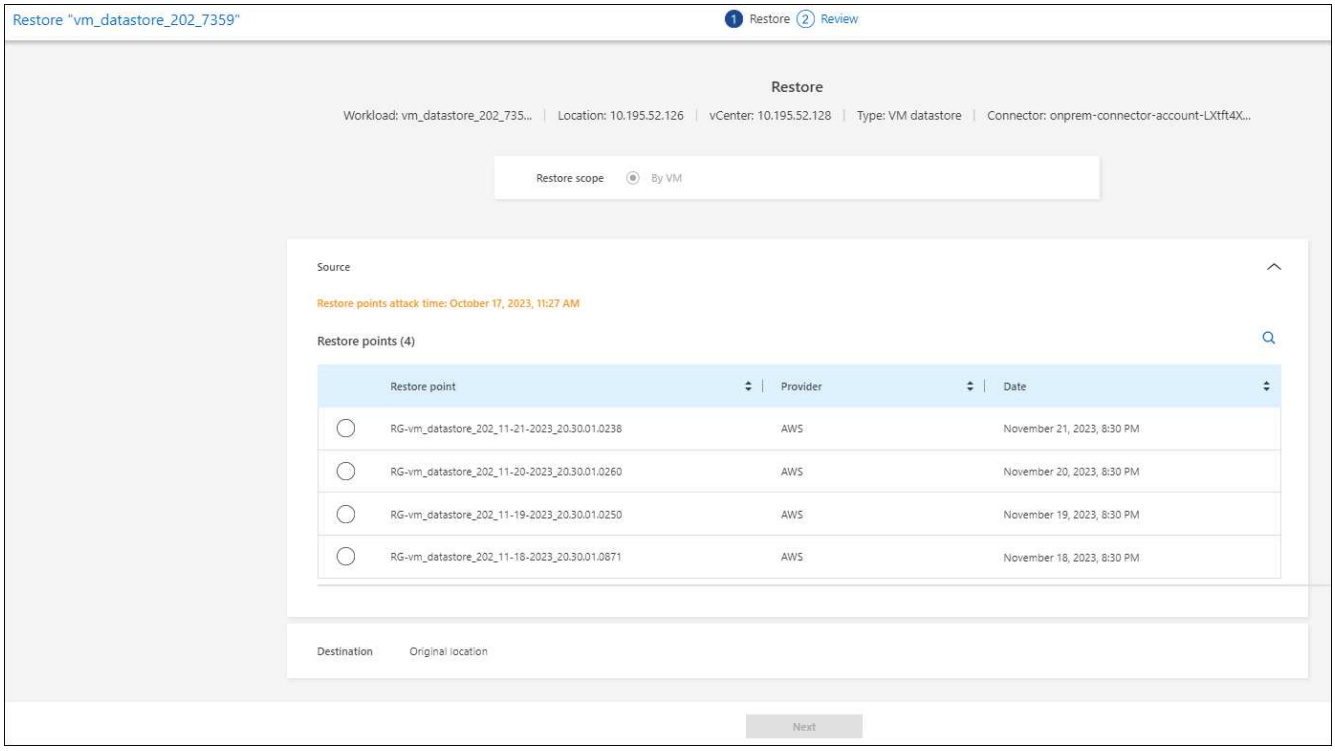
      如果未指定还原路径、则这些文件将还原到顶级目录的新卷。

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。

知识和支持

注册以获得支持

要获得BlueXP及其存储解决方案和服务的特定技术支持、需要注册支持。要为Cloud Volumes ONTAP系统启用关键工作流、还需要注册支持服务。

注册获取支持不会为云提供商文件服务启用NetApp支持。有关与云提供商文件服务、其基础架构或使用该服务的任何解决方案相关的技术支持、请参阅该产品的BlueXP文档中的"获得帮助"。

- "适用于 ONTAP 的 Amazon FSX"
- "Azure NetApp Files"
- "适用于 Google Cloud 的 Cloud Volumes Service"

支持注册概述

激活支持授权有两种形式的注册：

- 注册您的BlueXP帐户ID支持订阅(您的20位960xxxxxxxxx序列号、位于BlueXP的支持资源页面上)。

  这是您在BlueXP中使用的任何服务的单一支持订阅ID。必须注册每个BlueXP帐户级别的支持订阅。

- 在云提供商的市场中注册与订阅关联的Cloud Volumes ONTAP 序列号(即20位909201xxxxxxxx序列号)。

  这些序列号通常称为_PAYGO序列号、并由BlueXP在部署Cloud Volumes ONTAP 时生成。

注册这两种类型的序列号可实现打开支持服务单和自动生成案例等功能。要完成注册、请按如下所述将NetApp支持站点(NSS)帐户添加到BlueXP中。

注册**BlueXP**帐户以获得**NetApp**支持

要注册支持并激活支持授权、BlueXP帐户中的一个用户必须将NetApp 支持站点 帐户与其BlueXP登录名关联。如何注册NetApp支持取决于您是否已拥有NetApp 支持站点 (NSS)帐户。

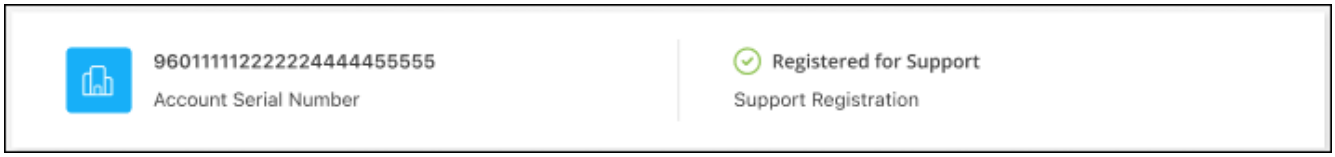
具有**NSS**帐户的现有客户

如果您是拥有NSS帐户的NetApp客户、则只需通过BlueXP注册支持即可。

步骤

1. 在BlueXP控制台的右上角、选择设置图标、然后选择*凭据*。
2. 选择*用户凭据*。
3. 选择*添加NSS凭证*，然后按照NetApp 支持站点(NSS)鉴定提示进行操作。
4. 要确认注册过程是否成功，请选择帮助图标，然后选择*Support*。

   “资源”页面应显示您的帐户已注册支持。



请注意、其他BlueXP用户如果没有将NetApp 支持站点 帐户与其BlueXP登录关联、则不会看到此相同的支持注册状态。但是、这并不意味着您的BlueXP帐户未注册支持。只要帐户中有一个用户执行了这些步骤、您的帐户即已注册。

现有客户、但无**NSS**帐户

如果您是现有许可证和序列号但拥有_no_ nss帐户的现有NetApp客户、则需要创建一个NSS帐户并将其与BlueXP登录关联。

步骤

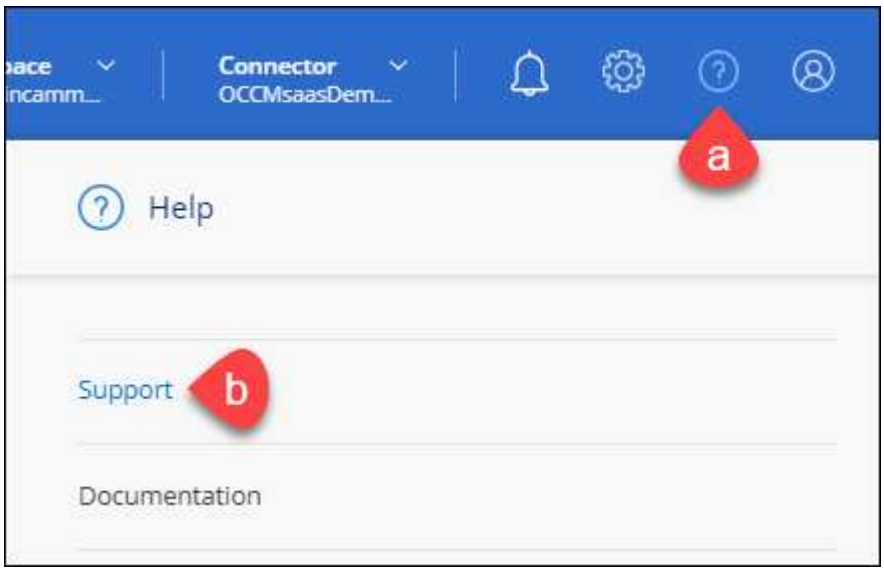
1. 完成以创建NetApp 支持站点 帐户 "NetApp 支持站点 用户注册表"
   a. 请务必选择适当的用户级别、通常为* NetApp客户/最终用户*。
   b. 请务必复制上面用于序列号字段的BlueXP帐户序列号(960xxxx)。这样可以加快帐户处理速度。
2. 完成下的步骤、将新的NSS帐户与BlueXP登录关联起来 具有NSS帐户的现有客户。

NetApp的新品牌

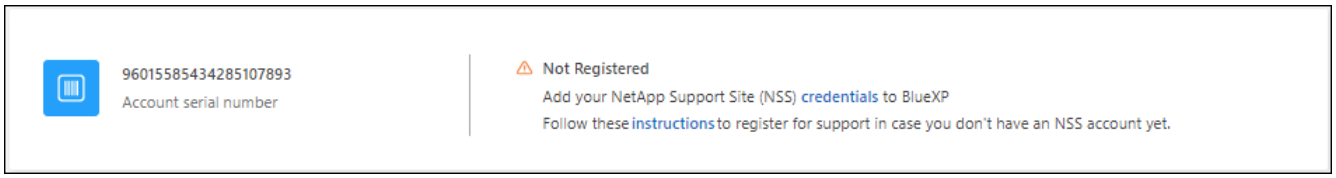
如果您是NetApp的新客户、并且没有NSS帐户、请按照以下每个步骤进行操作。

步骤

1. 在BlueXP控制台的右上角、选择帮助图标、然后选择*支持*。



2. 从支持注册页面找到您的帐户ID序列号。



3. 导航到 "NetApp的支持注册站点" 并选择*我不是NetApp注册客户*。
4. 填写必填字段(带有红色星号的字段)。
5. 在*产品线*字段中、选择*云管理器*、然后选择适用的计费提供商。
6. 复制上述第2步中的帐户序列号、完成安全检查、然后确认您已阅读NetApp的全球数据隐私政策。

   系统会立即向提供的邮箱发送一封电子邮件、以完成此安全事务。如果验证电子邮件未在几分钟内收到、请务必检查您的垃圾邮件文件夹。

7. 在电子邮件中确认操作。

   确认将向NetApp提交您的请求、并建议您创建NetApp 支持站点 帐户。

8. 完成以创建NetApp 支持站点 帐户 "NetApp 支持站点 用户注册表"
   a. 请务必选择适当的用户级别、通常为* NetApp客户/最终用户*。
   b. 请务必复制上面用于序列号字段的帐户序列号(960xxxx)。这样可以加快帐户处理速度。

完成后

在此过程中、NetApp应与您联系。这是针对新用户的一次性入职练习。

拥有NetApp 支持站点 帐户后、通过完成下的步骤将帐户与BlueXP登录关联起来 具有NSS帐户的现有客户。

关联Cloud Volumes ONTAP支持的NSS凭据

要为Cloud Volumes ONTAP启用以下关键工作流、需要将NetApp 支持站点 凭据与BlueXP帐户相关联：

- 注册按需购买Cloud Volumes ONTAP系统以获得支持

  要激活对系统的支持并访问 NetApp 技术支持资源，需要提供 NSS 帐户。

- 自带许可证时部署Cloud Volumes ONTAP (BYOL)

  需要提供您的NSS帐户、以便BlueXP可以上传您的许可证密钥并为您购买的期限启用订阅。这包括自动更新期限续订。

- 将Cloud Volumes ONTAP 软件升级到最新版本

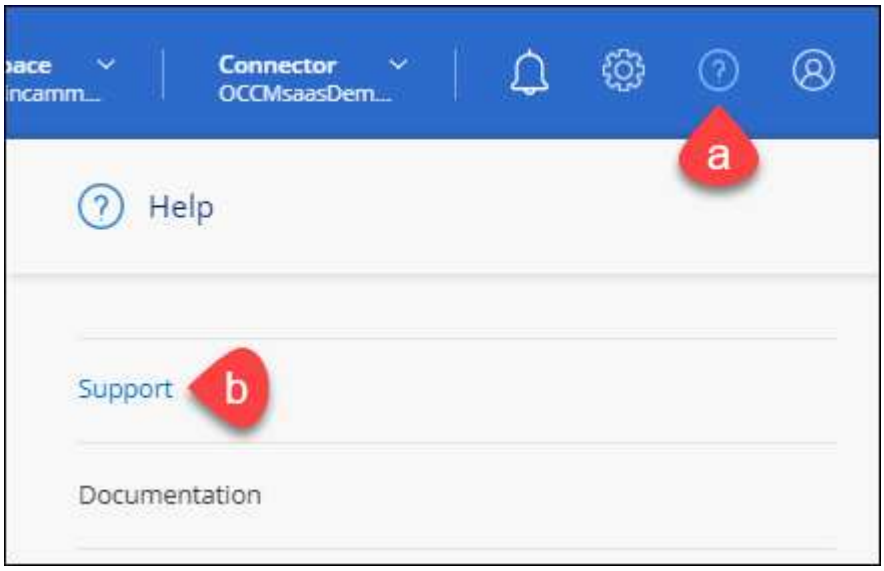
将NSS凭据与BlueXP帐户关联与与与BlueXP用户登录关联的NSS帐户不同。

这些NSS凭据与您的特定BlueXP帐户ID关联。属于BlueXP帐户的用户可以从*支持> NSS管理*访问这些凭据。

- 如果您拥有客户级别的帐户、则可以添加一个或多个NSS帐户。
- 如果您拥有合作伙伴或经销商帐户、则可以添加一个或多个NSS帐户、但不能将其与客户级别的帐户同时添加。

步骤

1. 在BlueXP控制台的右上角、选择帮助图标、然后选择*支持*。



2. 选择* NSS管理>添加NSS帐户*。
3. 出现提示时、选择*继续*以重定向到Microsoft登录页面。

   NetApp使用Microsoft Entra ID作为特定于支持和许可的身份验证服务的身份提供程序。

4. 在登录页面上，提供 NetApp 支持站点注册的电子邮件地址和密码以执行身份验证过程。

   通过这些操作、BlueXP可以使用您的NSS帐户执行许可证下载、软件升级验证和未来支持注册等操作。

   请注意以下事项：

   - NSS帐户必须是客户级别的帐户(而不是来宾或临时帐户)。您可以拥有多个客户级别的NSS帐户。
   - 如果此帐户是合作伙伴级别的帐户、则只能有一个NSS帐户。如果您尝试添加客户级别的NSS帐户、并且存在合作伙伴级别的帐户、则会收到以下错误消息：

     "此帐户不允许使用NSS客户类型、因为已存在不同类型的NSS用户。"

   如果您已有客户级别的NSS帐户、并尝试添加合作伙伴级别的帐户、则也是如此。

   - 成功登录后、NetApp将存储NSS用户名。

     这是系统生成的ID、映射到您的电子邮件。在* NSS Management*页面上、您可以从显示电子邮件 ••• 菜单。

   - 如果您需要刷新登录凭据令牌、则中还会提供一个*更新凭据*选项 ••• 菜单。

     使用此选项将提示您重新登录。请注意、这些帐户的令牌将在90天后过期。系统将发布通知、提醒您注意这一点。

获取帮助

NetApp通过多种方式为BlueXP及其云服务提供支持。全天候提供丰富的免费自助支持选项，例如知识库（KB）文章和社区论坛。您的支持注册包括通过 Web 服务单提供的远程技术支持。

获得云提供商文件服务支持

有关与云提供商文件服务、其基础架构或使用该服务的任何解决方案相关的技术支持、请参阅该产品的BlueXP文档中的"获得帮助"。

- "适用于 ONTAP 的 Amazon FSX"
- "Azure NetApp Files"
- "适用于 Google Cloud 的 Cloud Volumes Service"

要获得针对BlueXP及其存储解决方案和服务的技术支持、请使用下面所述的支持选项。

使用自助支持选项

这些选项每周 7 天，每天 24 小时免费提供：

- 文档。

  您当前正在查看的BlueXP文档。

- "知识库"

  搜索BlueXP知识库、查找有助于解决问题的文章。

- "社区"

  加入BlueXP社区、关注正在进行的讨论或创建新的讨论。

向NetApp支持部门创建案例

除了上述自助支持选项之外、您还可以在激活支持后与NetApp支持专家合作解决任何问题。

开始之前

- 要使用*创建案例*功能、您必须先将NetApp 支持站点 凭据与BlueXP登录名关联起来。 "了解如何管理与BlueXP登录关联的凭据"。
- 如果您为具有序列号的ONTAP系统创建案例、则您的NSS帐户必须与该系统的序列号相关联。

步骤

1. 在BlueXP中、选择*帮助>支持*。
2. 在*资源*页面上、在技术支持下选择一个可用选项：

   a. 如果您想通过电话与某人通话，请选择*呼叫我们*。系统会将您定向到netapp.com上的一个页面、其中

列出了您可以拨打的电话号码。

b. 选择*创建案例*向NetApp支持专家开立TT：

- 服务：选择与问题描述 关联的服务。例如、当特定于技术支持问题描述 时、如果服务中包含工作流或功能、则为BlueXP。
- 工作环境：如果适用于存储、请选择* Cloud Volumes ONTAP 或 on-Prem*、然后选择关联的工作环境。

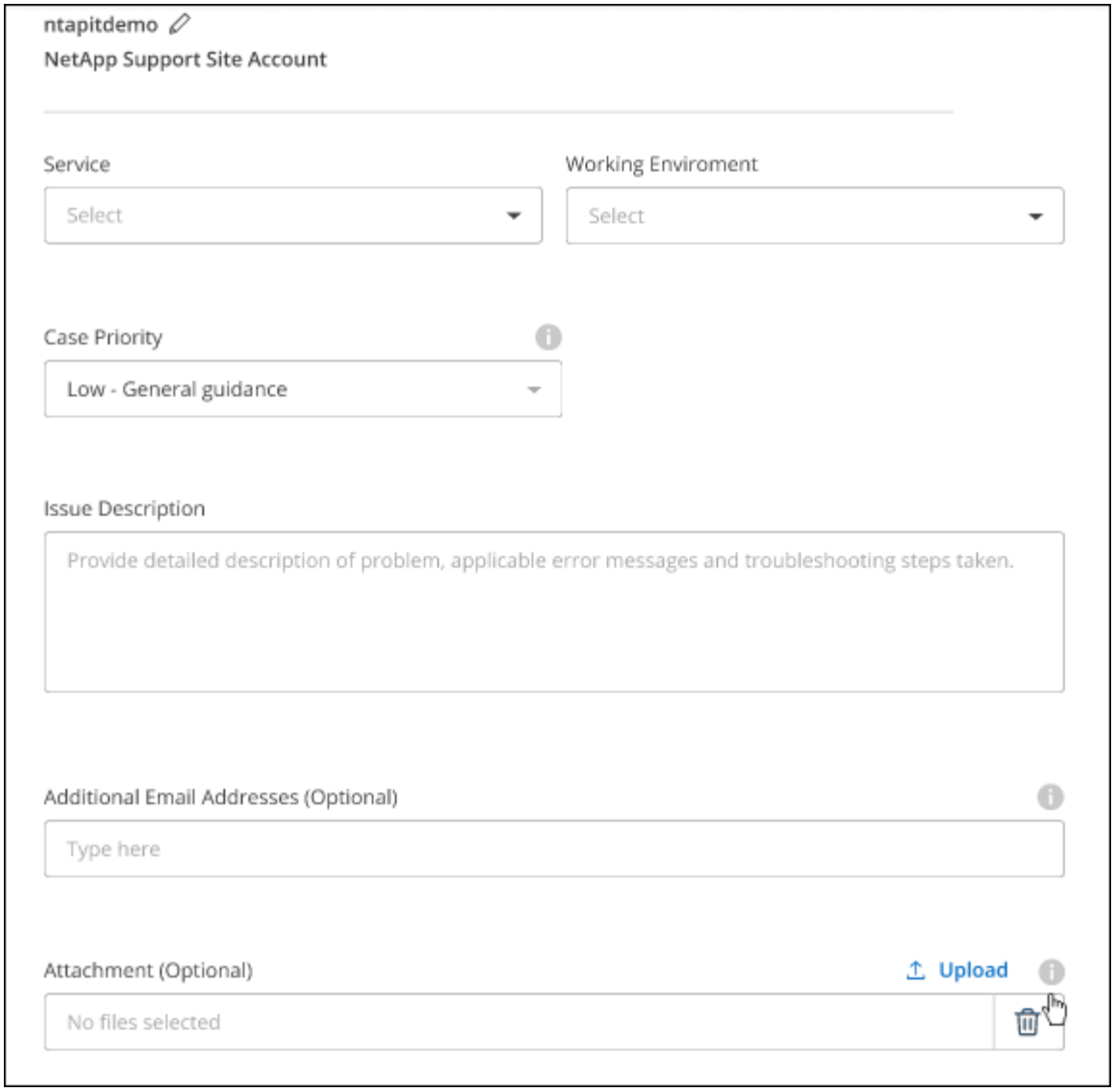
  工作环境列表属于您在服务顶部横幅中选择的BlueXP帐户、工作空间和Connector的范围。

- 案例优先级：选择案例的优先级、可以是"低"、"中"、"高"或"严重"。

  要了解有关这些优先级的更多详细信息、请将鼠标悬停在字段名称旁边的信息图标上。

- *问题描述 *：提供问题的详细问题描述 、包括任何适用的错误消息或您执行的故障排除步骤。
- 其他电子邮件地址：如果您希望其他人了解此问题描述 、请输入其他电子邮件地址。
- 附件(可选)：一次最多上传五个附件。

  每个文件的附件数限制为25 MB。支持以下文件扩展名：txt、log、pdf、jp6/jpeu、rtf、 doc/docx 、xls/xlsx和csv。



完成后

此时将显示一个弹出窗口、其中包含您的支持案例编号。NetApp支持专家将审核您的案例、并尽快与您联系。

要查看支持案例的历史记录，您可以选择*设置>时间线*并查找名为“创建支持案例”的操作。 最右侧的按钮可用于展开操作以查看详细信息。

尝试创建案例时、您可能会遇到以下错误消息：

"您无权针对选定服务创建案例"

此错误可能意味着NSS帐户及其关联的记录公司与BlueXP帐户序列号(即960xxxx)或工作环境序列号。您可以使用以下选项之一寻求帮助：

- 使用产品内聊天功能
- 通过提交非技术案例 https://mysupport.netapp.com/site/help

管理支持案例(预览)

您可以直接从BlueXP查看和管理活动的和已解决的支持案例。您可以管理与您的NSS帐户和公司关联的案例。

案例管理以预览形式提供。我们计划改进此体验、并在即将发布的版本中添加增强功能。请通过产品内聊天向我们发送反馈。

请注意以下事项：

- 页面顶部的案例管理信息板提供了两个视图：
  - 左侧视图显示了您提供的用户NSS帐户在过去3个月内打开的案例总数。
  - 右侧视图显示了过去3个月内根据用户NSS帐户在公司级别开立的案例总数。

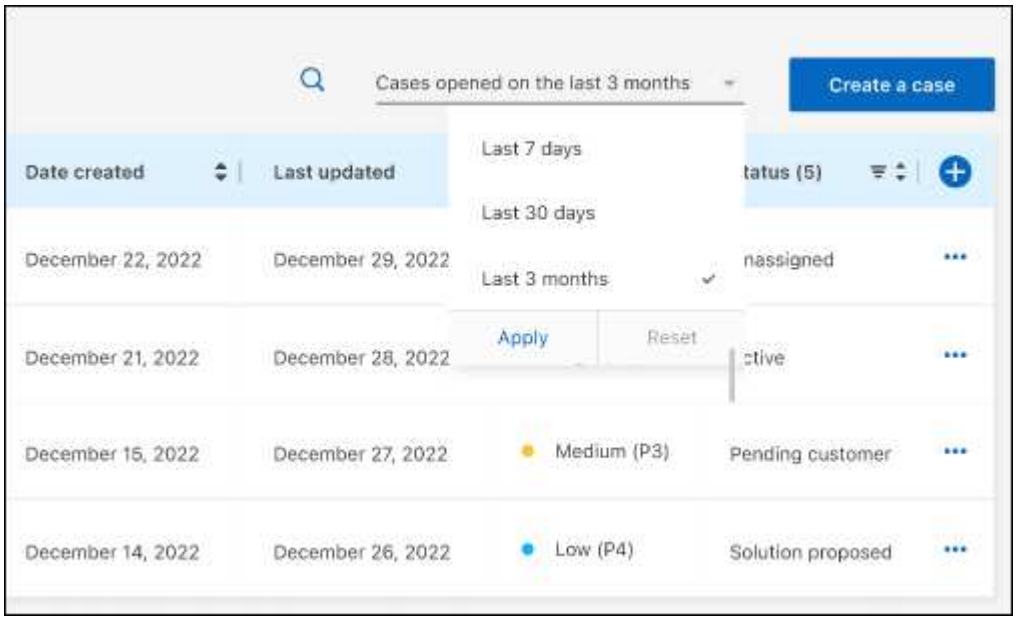
  此表中的结果反映了与选定视图相关的案例。
- 您可以添加或删除感兴趣的列、也可以筛选优先级和状态等列的内容。其他列仅提供排序功能。

  有关更多详细信息、请查看以下步骤。
- 在每个案例级别、我们可以更新案例备注或关闭尚未处于"已关闭"或"待关闭"状态的案例。

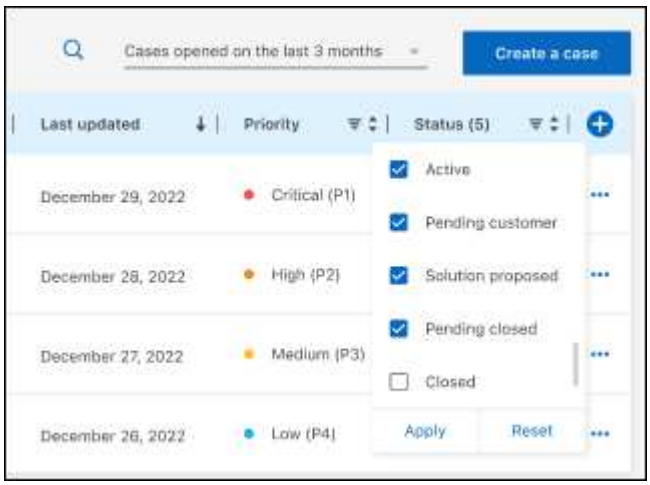
步骤

1. 在BlueXP中、选择*帮助>支持*。
2. 选择*案例管理*，如果出现提示，请将您的NSS帐户添加到BlueXP。

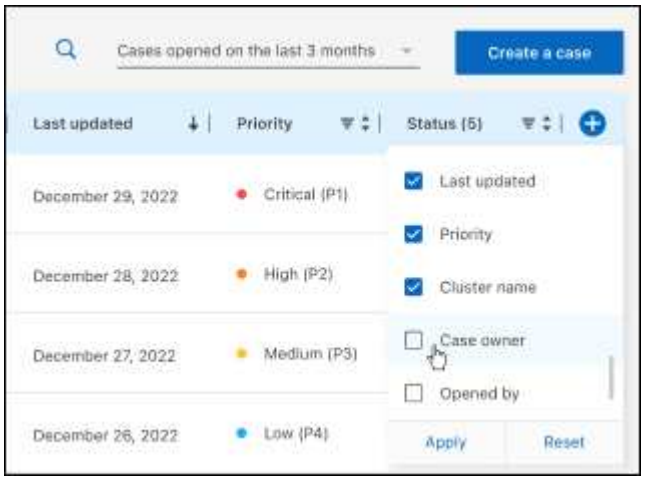
   "案例管理"页面显示了与您的BlueXP用户帐户关联的NSS帐户相关的已打开案例。此NSS帐户与* NSS管理*页面顶部显示的NSS帐户相同。
3. 也可以修改表中显示的信息：
   - 在“组织案例”下，选择“查看”以查看与贵公司关联的所有案例。
   - 通过选择确切的日期范围或选择其他时间范围来修改日期范围。



- 筛选列的内容。



- 通过选择更改表中显示的列 ⊕ 然后选择要显示的列。

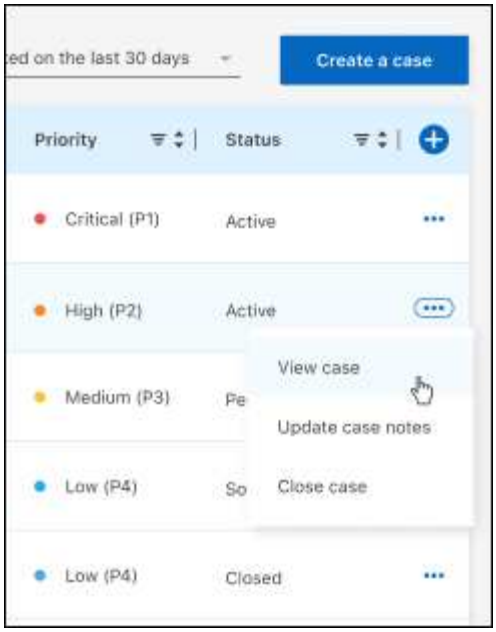


4. 通过选择管理现有案例 ••• 并选择一个可用选项：

   - 查看案例：查看有关特定案例的完整详细信息。
   - 更新案例注释：提供有关您的问题的更多详细信息、或者选择*上传文件*最多附加五个文件。

     每个文件的附件数限制为25 MB。支持以下文件扩展名：txt、log、pdf、jp6/jpeu、rtf、 doc/docx、xls/xlsx和csv。

   - 关闭案例：提供关闭案例的详细原因，然后选择*关闭案例*。


ed on the last 30 days
Create a case
Priority
Status
Critical (P1)
Active
High (P2)
Active
View case
Medium (P3)
Update case notes
Low (P4)
Close case
Low (P4)
Closed

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NetApp 、 NetApp 徽标和 NetApp 商标页面上列出的标记是 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。

"https://www.netapp.com/company/legal/trademarks/"

专利

有关 NetApp 拥有的专利的最新列表，请访问：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

- "BlueXP通知"