



勒索软件保护文档 Ransomware Protection

NetApp
July 19, 2022

目录

勒索软件保护文档	1
勒索软件保护的新增功能	2
2022年6月12日	2
2022年5月11日	2
2022年3月15日	2
2022年2月9日	3
入门	4
了解勒索软件保护	4
使用勒索软件保护	6
管理数据源的网络安全建议	6
知识和支持	15
注册以获得支持	15
获取帮助	16
法律声明	18
版权	18
商标	18
专利	18
隐私政策	18
开放源代码	18

勒索软件保护文档

勒索软件保护的新增功能

了解勒索软件保护的新增功能。

2022年6月12日

现在、系统将跟踪**ONTAP Storage VM**的**NAS**文件系统审核状态

如果工作环境中启用了文件系统审核的Storage VM少于40%、则会向_Cyber Resilience Map_添加警报。您可以在_harden your ONTAP environment_面板中查看未跟踪SMB和NFS事件并将其记录到审核日志中的确切SVM数。然后、您可以决定是否对这些SVM启用审核。

现在、如果您的卷未启用机载反勒索软件、则会显示警报

先前在_harden your ONTAP Environments_panel中为内部ONTAP系统报告了此信息、但现在、当在40%以下的卷中启用了机载反勒索软件功能时、_Cyber Resilience Map_中会报告一条警报、因此您可以在信息板中查看此信息。

现在、可跟踪适用于**ONTAP**系统的**FSX**以启用卷快照

现在、增强ONTAP环境_面板可提供适用于ONTAP系统的FSx上卷的Snapshot副本状态。如果不到40%的卷受快照保护、您还会在_Cyber Resilience Map_中收到警报。

2022年5月11日

用于跟踪 **ONTAP** 环境安全性强化情况的新面板。

一个新面板_harden your ONTAP Environments_可提供ONTAP系统中某些设置的状态、用于根据跟踪部署的安全性 "[《适用于 ONTAP 系统的 NetApp 安全加固指南》](#)" 和 "[ONTAP 防勒索软件功能](#)" 主动检测异常活动并发出警告。

您可以查看这些建议，然后确定希望如何解决潜在问题。您可以按照以下步骤更改集群上的设置，将更改推迟到其他时间或忽略此建议。 "[有关详细信息，请访问此处](#)"。

新面板可显示如何使用 **Cloud Backup** 保护不同类别的数据。

此全新的_Backup Status_面板显示了在因勒索软件攻击而需要恢复时、您最重要的数据类别的备份程度如何全面。此数据直观地展示了 Cloud Backup 在环境中备份的特定类别项目数量。 "[有关详细信息，请访问此处](#)"。

2022 年 3 月 15 日

用于跟踪业务关键型数据的权限状态的新面板

新的"业务关键型数据权限分析"面板可显示对您的业务至关重要的数据的权限状态。这样，您就可以快速评估业务关键型数据的保护情况。 "[有关详细信息，请访问此处](#)"。

现在， " 打开权限 " 区域包括 **OneDrive** 和 **SharePoint** 帐户

现在，勒索软件保护信息板中的 " 打开权限 " 区域包含对 OneDrive 帐户和 SharePoint 帐户中正在扫描的文件的现有权限。

2022 年 2 月 9 日

全新的勒索软件保护服务

通过全新的勒索软件保护服务，您可以查看有关网络安全的相关信息，并评估数据对网络攻击的弹性。此外，它还会为您提供一系列警报和修复措施，帮助您提高数据的安全性。

["了解有关此新服务的更多信息"](#)。

入门

了解勒索软件保护

勒索软件攻击可能会耗费业务时间，资源和声誉。通过勒索软件保护服务、您可以查看有关网络安全的相关信息、并评估您的组织对网络攻击的抵御能力。此外，它还会为您提供一系列警报和修复措施，帮助您提高数据的安全性。

["了解勒索软件保护的用例"](#)。



勒索软件保护服务目前为测试版产品。

功能

勒索软件保护提供了单一的可见性和控制点、可用于管理和完善不同工作环境和基础架构层的数据安全性、以便更好地应对发生的威胁。它目前提供多种功能、可帮助您保护网络存储。将来还会添加其他功能。当前功能可确定何时执行以下操作：

- 工作环境中的卷不会通过定期创建 Snapshot 副本来受到保护。
- 工作环境中的卷不会通过使用创建云备份来受到保护 ["云备份"](#)。
- 您的工作环境和数据源中的数据不会使用进行扫描 ["云数据感知"](#) 确定合规性和隐私问题，并寻找优化机会。

从勒索软件保护角度来看、此功能也很重要、因为它可以让您更好地了解重要(敏感的业务关键型)数据的位置、从而确保您将保护重点放在这些数据上。

- 如果您因勒索软件攻击而需要恢复、则不会备份您最重要的数据类别。
- 工作环境或数据源中加密文件的百分比异常增加。

这可能表明您的网络上已开始勒索软件攻击。

- 在文件中发现敏感数据，并且在工作环境或数据源中访问权限级别过高。
- 用户已添加到 Active Directory 域管理员组。
- 集群上的 ONTAP 软件版本较旧，应进行更新以提供最佳的保护和安全功能。
- ONTAP 系统未启用 NAS 文件系统审核。

启用 CIFS 审核会为系统管理员生成审核事件，用于跟踪文件夹权限更改，读取或写入文件失败尝试以及创建，修改或删除文件的时间等信息。

- 您的 ONTAP 系统未启用机载反勒索软件功能。

ONTAP 反勒索软件功能可以主动检测并警告可能指示勒索软件攻击的异常活动。

["请在勒索软件保护信息板中查看如何查看这些潜在问题。"](#)

使用 Cloud Volumes ONTAP 系统时，您可以直接从工作环境中部署一些额外的勒索软件保护。 ["了解如何针对勒索软件添加额外保护"](#)。

支持的工作环境和数据源

"云数据感知" 是使用勒索软件保护服务的前提条件。安装并激活 Data sense 后，您可以使用勒索软件保护来查看数据在以下类型的工作环境和数据源上受到网络攻击时的弹性：

- 工作环境： *
- Cloud Volumes ONTAP （部署在 AWS ， Azure 或 GCP 中）
- 内部 ONTAP 集群
- Azure NetApp Files
- 适用于 ONTAP 的 Amazon FSX
- Amazon S3
- 数据源： *
- 非 NetApp 文件共享
- 对象存储（使用 S3 协议）
- 数据库(Amazon RDS、MongoDB、MySQL、Oracle、PostgreSQL、 SAP HANA、SQL Server)
- OneDrive 帐户
- SharePoint 帐户
- Google Drive帐户

勒索软件保护还会监控您的全局 Active Directory 配置（如果有） ["已在 Cloud Data sense 中配置此配置"](#)。

勒索软件保护的工作原理

总体而言，勒索软件保护的工作原理如下：

1. 勒索软件保护会从您的存储系统、云数据感知、Cloud Backup以及其他Cloud Manager资源中收集信息、以填充勒索软件保护信息板。
2. 您可以使用勒索软件保护信息板来简要了解您的系统受到的保护程度。
3. 您可以使用提供的报告工具帮助您保护网络存储。

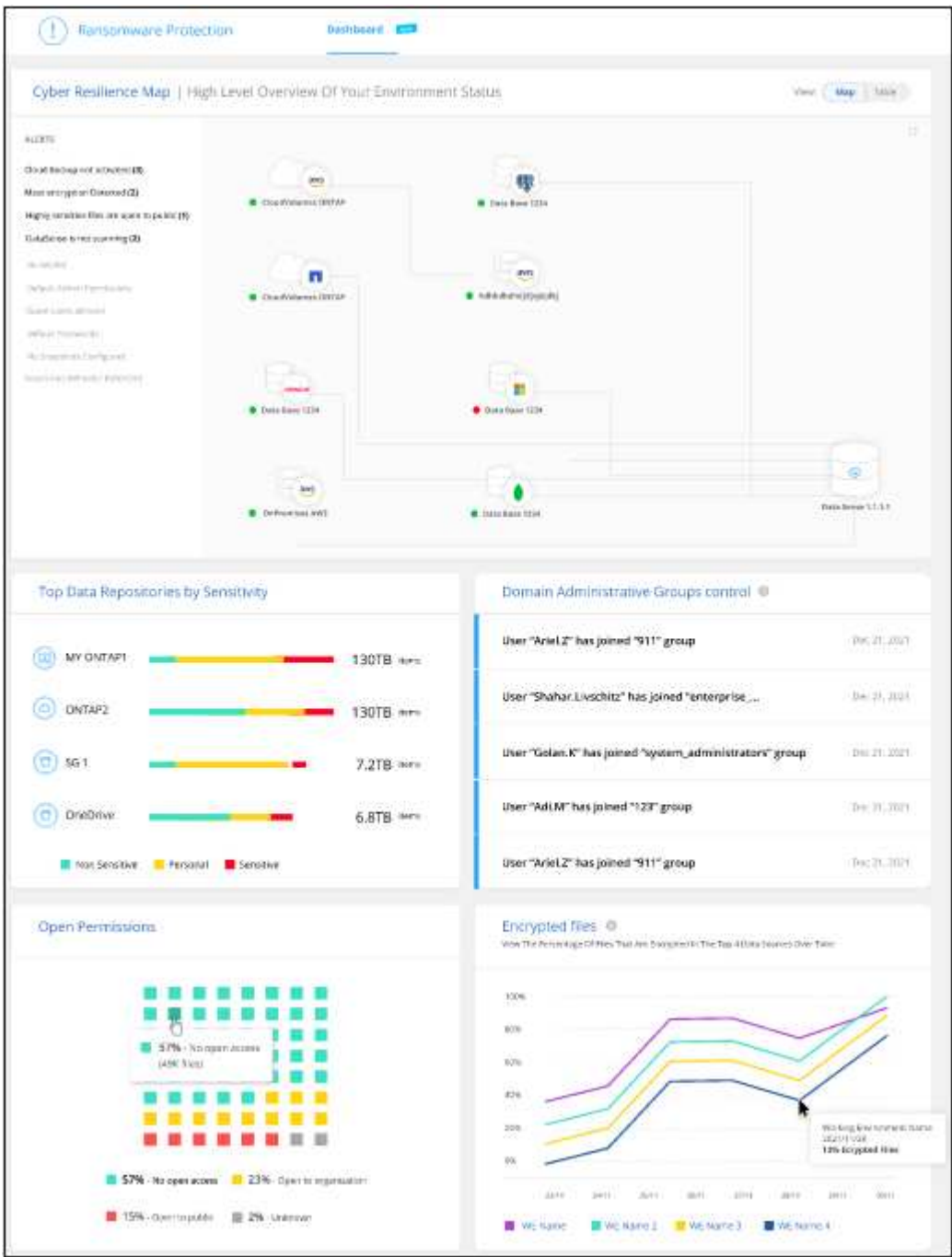
成本

在测试期间，勒索软件保护服务不会单独产生成本。

使用勒索软件保护

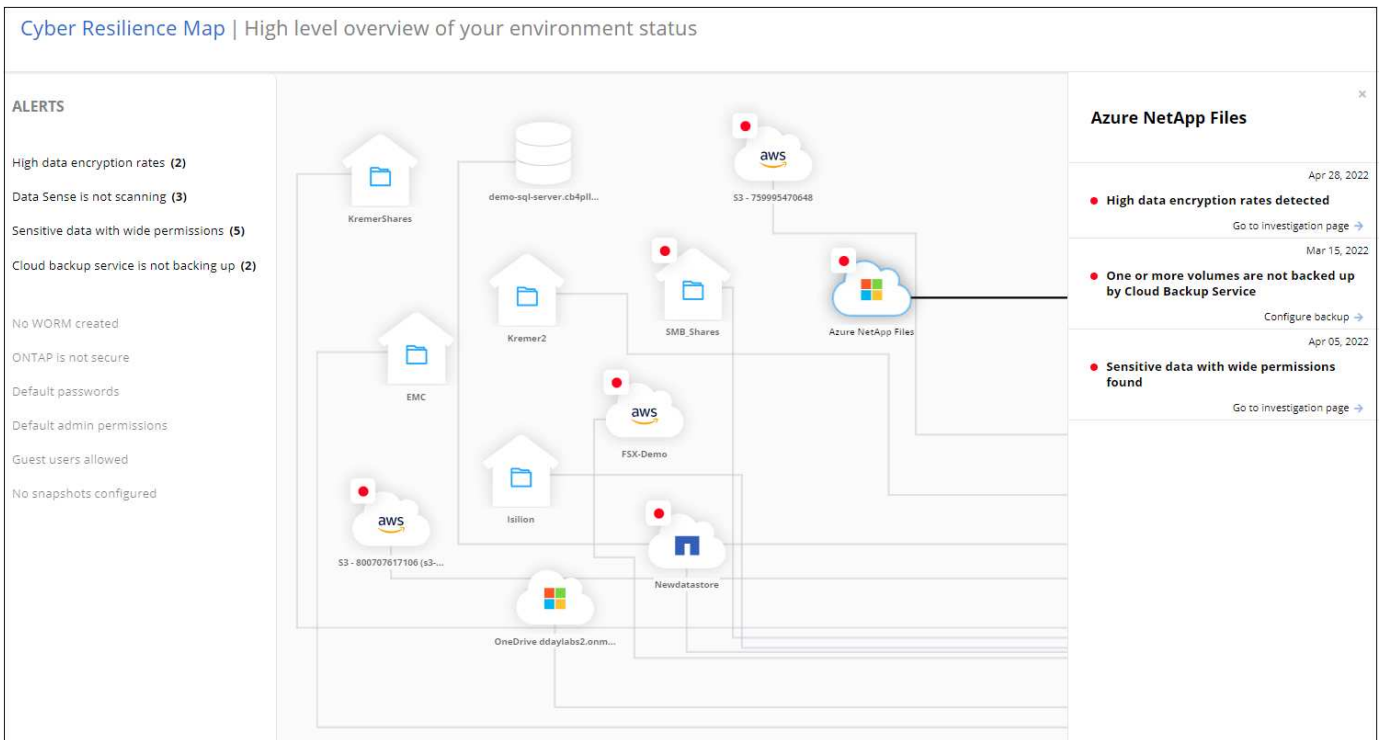
管理数据源的网络安全建议

使用Cloud Manager勒索软件保护信息板查看所有工作环境和数据源的网络安全概况。您可以深入查看每个区域，以了解更多详细信息和可能的修复方法。



网络弹性映射

网络弹性映射是信息板中的主要区域。通过它，您可以直观地查看所有工作环境和数据源，并查看相关的网络弹性信息。



该映射由三部分组成：

左侧面板

显示服务在所有数据源中监控的警报列表。它还指示环境中处于活动状态的每个特定警报的数量。拥有大量一种类型的警报可能是尝试首先解决这些警报的一个很好的原因。

中央面板

以图形格式显示所有数据源，服务和 Active Directory。运行状况良好的环境会显示绿色指示符，而发出警报的环境会显示红色指示符。

右侧面板

单击带有红色指示符的数据源后，此面板将显示该数据源的警报并提供解决警报的建议。对警报进行排序，以便首先列出最新的警报。许多建议都会引导您使用另一个 Cloud Manager 服务来解决问题描述 问题。

这些警报是当前跟踪的警报和建议的修复方法。

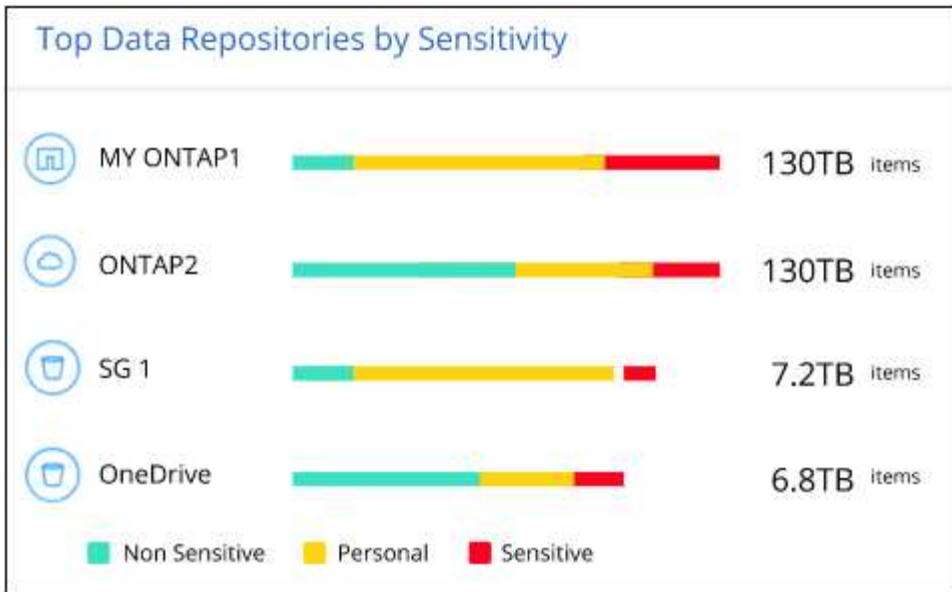
警报	Description	修复
检测到高数据加密率	数据源中加密文件或损坏文件的百分比异常增加。这意味着过去 7 天加密文件的百分比增加了 20% 以上。例如，如果 50% 的文件已加密，则此数字会在一天之后增加到 60%，您将看到此警报。	单击链接以启动 "数据感知调查页面" 。您可以在此处为特定的 <code>_工作环境_</code> 和 <code>_类别_</code> （加密和损坏）选择筛选器，以查看所有加密和损坏文件的列表。
发现具有广泛权限的敏感数据	在文件中发现敏感数据，而在数据源中，访问权限级别太高。	单击链接以启动 "数据感知调查页面" 。您可以在此处选择特定 <code>WorkEnvironment</code> ， <code>_Sensitivity Level_</code> （ <code>Sensitive Personal</code> ）和 <code>_Open Permissions</code> 的筛选器，以查看具有此问题描述 的文件列表。

警报	Description	修复
一个或多个卷不会使用 Cloud Backup 进行备份	工作环境中的某些卷未使用进行保护 "云备份"。	单击链接启动 Cloud Backup ，然后您可以确定工作环境中未备份的卷，然后确定是否要在这些卷上启用备份。
Data sense 不会扫描数据源中的一个或多个存储库（卷，存储分段等）	您的数据源中的某些数据未使用进行扫描 "云数据感知" 确定合规性和隐私问题并寻找优化机会。	单击此链接可启动 Data sense 并为未扫描的项目启用扫描和映射。
并非所有卷都在使用机载反勒索软件	内部ONTAP 系统中的某些卷没有 "NetApp反勒索软件功能" 已启用。	单击此链接，您将重定向到 强化ONTAP 环境面板 以及使用问题描述 的工作环境。您可以在此处了解如何以最佳方式修复问题描述。
未更新ONTAP 版本	集群上安装的ONTAP 软件版本不符合中的建议 "《适用于 ONTAP 系统的 NetApp 安全加固指南》"。	单击此链接，您将重定向到 强化ONTAP 环境面板 以及使用问题描述 的工作环境。您可以在此处了解如何以最佳方式修复问题描述。
未为所有卷配置快照	工作环境中的某些卷未通过创建卷快照来受到保护。	单击此链接，您将重定向到 强化ONTAP 环境面板 以及使用问题描述 的工作环境。您可以在此处了解如何以最佳方式修复问题描述。
并非所有SVM都启用文件操作审核	工作环境中的某些Storage VM未启用文件系统审核。建议您跟踪用户对文件执行的操作。	单击此链接，您将重定向到 强化ONTAP 环境面板 以及使用问题描述 的工作环境。您可以在此处调查是否需要在SVM上启用NAS审核。

按数据敏感度排名前几位的数据存储库

Top Data Repository by Sensitivity level_ 面板最多可列出包含最敏感项目的前四个数据存储库（工作环境和数据源）。每个工作环境的条形图分为：

- 非敏感数据
- 个人数据
- 敏感的个人数据



您可以将鼠标悬停在每个部分上以查看每个类别中的项目总数。

单击每个区域以在 "数据感知调查" 页面中查看筛选后的结果，以便您可以进一步调查。

域管理员组控制

域管理员组控制面板显示已添加到域管理员组中的最新用户，以便您可以查看是否应允许这些组中的所有用户。您必须拥有 "集成了全局 Active Directory" 进入 Cloud Data sense，以使此面板处于活动状态。

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

默认管理组包括 "管理员"，"域管理员"，"企业管理员"，"企业密钥管理员" 和 "密钥管理员"。

按打开权限类型列出的数据

Open Permissions panel 会显示正在扫描的所有文件中存在的每种权限的百分比。此图表来自 Data sense，其中显示了以下类型的权限：

- 无开放访问
- 对组织开放

- 打开公有
- 未知访问



您可以将鼠标悬停在每个部分上以查看每个类别中的文件百分比和总数。

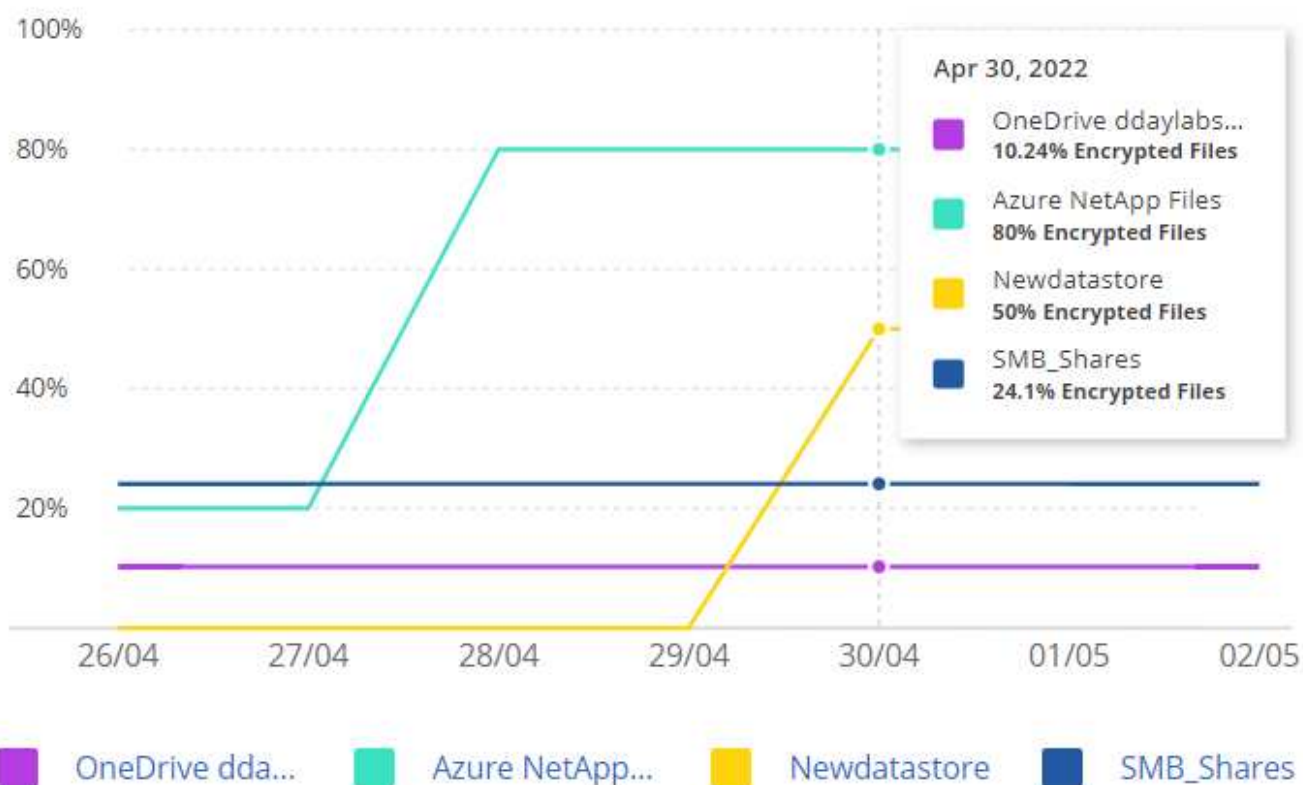
单击每个区域以在 "数据感知调查" 页面中查看筛选后的结果，以便您可以进一步调查。

按加密文件列出的数据

"已加密文件" 面板显示经过加密的文件百分比最高的前 4 个数据源。这些通常是受密码保护的项。为此，它会比较过去 7 天的加密速率，以确定哪些数据源的增长率超过 20%。增加此数量可能意味着勒索软件已攻击您的系统。

Encrypted Files ⓘ

Rising percentages of encrypted files can be an indication of malicious activity

































单击其中一个数据源对应的行可在 " 数据感知调查 " 页面中查看经过筛选的结果，以便您可以进一步调查。

ONTAP 系统强化状态

增强 ONTAP 环境 _ 面板可提供 ONTAP 系统中某些设置的状态，这些设置可根据跟踪部署的安全性 "《适用于 ONTAP 系统的 NetApp 安全加固指南》" 和 "ONTAP 防勒索软件功能" 主动检测异常活动并发出警告。

您可以查看这些建议，然后确定希望如何解决潜在问题。您可以按照以下步骤更改集群上的设置，将更改推迟到其他时间或忽略此建议。

此面板目前支持适用于NetApp ONTAP 系统的内部ONTAP、Cloud Volumes ONTAP 和Amazon FSX。

Harden your ONTAP environments						
Working Environment	ONTAP Anti Ransomware ⓘ	NAS Auditing ⓘ	ONTAP Version ⓘ	Snapshots ⓘ		
MY ONTAP1			 9.10.XX			
ONTAP2			 9.10.XX			
AccOI_ONTAP			 9.10.XX			
CVO828			 9.8.XX			
FSx			 9.8.XX			

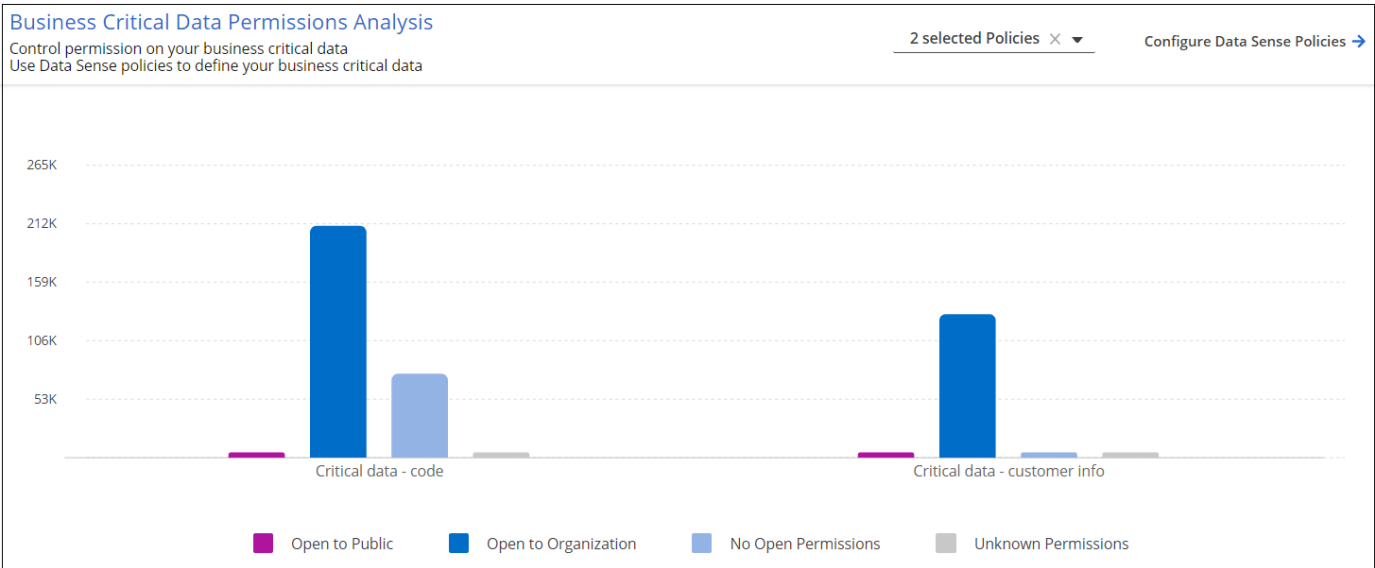
正在跟踪的设置包括：

强化目标	Description	修复
ONTAP 反勒索软件	已激活机载反勒索软件的卷的百分比。仅适用于内部 ONTAP 系统。绿色状态图标表示已启用超过 85% 的卷。黄色表示已启用 40-85% 。红色表示已启用 < 40% 。	"了解如何在卷上启用反勒索软件" 使用 System Manager 。
NAS审核	启用了文件系统审核的Storage VM 的数量。绿色状态图标表示超过85%的SVM已启用NAS文件系统审核。黄色表示已启用 40-85% 。红色表示已启用 < 40% 。	"请参见如何在SVM上启用NAS审核" 使用命令行界面。
ONTAP 版本	集群上安装的 ONTAP 软件版本。绿色状态图标表示此版本为最新版本。黄色图标表示集群在内部系统中落后1或2个修补版本或1个次要版本、在Cloud Volumes ONTAP 中落后1个主要版本。红色图标表示集群后面有3个修补版本、2个次要版本、1个主要版本(内部系统)、后面有2个主要版本(Cloud Volumes ONTAP)。	"了解升级内部集群的最佳方式" 或 您的 Cloud Volumes ONTAP 系统 "。
快照	是否已在数据卷上激活快照功能，以及具有 Snapshot 副本的卷百分比。绿色状态图标表示超过 85% 的卷已启用快照。黄色表示已启用 40-85% 。红色表示已启用 < 40% 。	"请参见如何在内部集群上启用卷快照" 或 "在 Cloud Volumes ONTAP 系统上" 或 "在适用于ONTAP 的FSX系统上" 。

关键业务数据的权限状态

业务关键型数据权限分析面板可显示业务关键型数据的权限状态。这样，您就可以快速评估业务关键型数据的保

护情况。



最初、此面板会根据选定的默认策略显示数据。但是、您可以选择创建的2个最重要的Data sense _policies_来查看最关键的业务数据。请参见操作说明 ["使用 Data sense 创建策略"](#)。

此图显示了对符合策略标准的所有数据的权限分析。其中列出了以下项的数量：

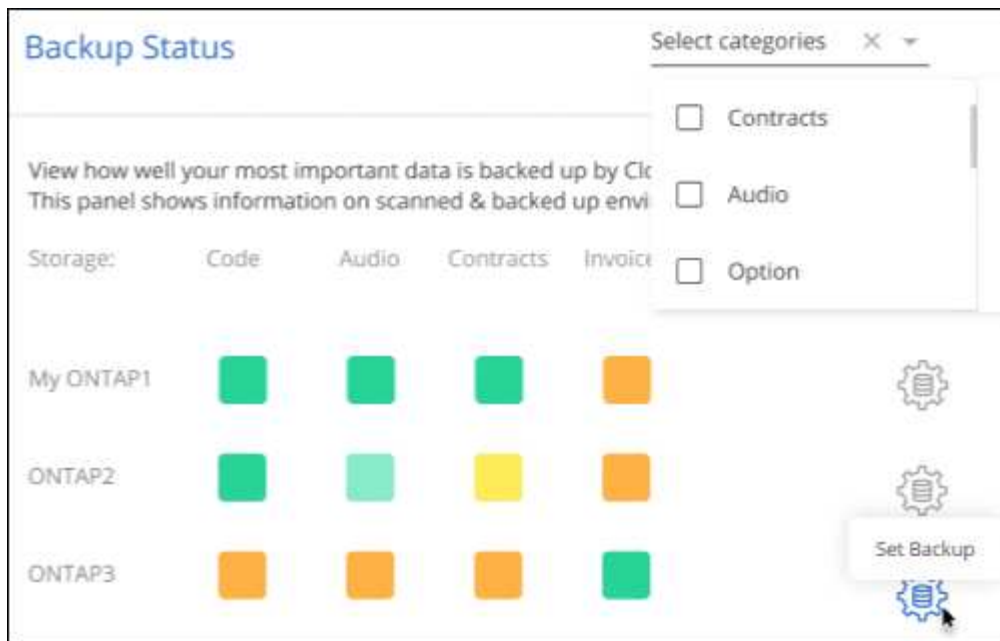
- Open to 公有 权限— Data sense 认为对公有 开放的项
- 开放给组织权限— Data sense 认为对组织开放的项
- 无打开权限— Data sense 视为无打开权限的项
- 未知权限— Data sense 视为未知权限的项

将鼠标悬停在图表中的每个条上可查看每个类别中的结果数。单击一个栏，此时将显示 "Data sense 调查 " 页面，以便您可以进一步调查哪些项具有打开权限，以及是否应对文件权限进行任何调整。

关键业务数据的备份状态

"备份状态"面板显示了如何使用Cloud Backup保护不同类别的数据。这可确定在因勒索软件攻击而需要恢复时、最重要的数据类别的备份程度如何全面。此数据直观地显示了工作环境中备份的特定类别项目的数量。

此面板仅会显示已使用Cloud Backup _and_ 扫描功能备份的内部ONTAP 和Cloud Volumes ONTAP 工作环境。



最初、此面板会根据选定的默认类别显示数据。但是、您可以选择要跟踪的数据类别；例如、对文件、合同等进行编码。请参见完整列表 ["类别"](#) Cloud Data sense可为您的工作环境提供这些功能。然后最多选择4个类别。

填充数据后、将鼠标悬停在图表中的每个方形上、可查看从工作环境中同一类别的所有文件中备份的文件数。绿色方形表示已备份85%或以上的文件。黄色方形表示备份的文件介于40%到85%之间。红色方形表示备份的文件数不超过40%。

您可以单击行末尾的Cloud Backup按钮转到Cloud Backup界面、以便在每个工作环境中的更多卷上启用备份。

知识和支持

注册以获得支持

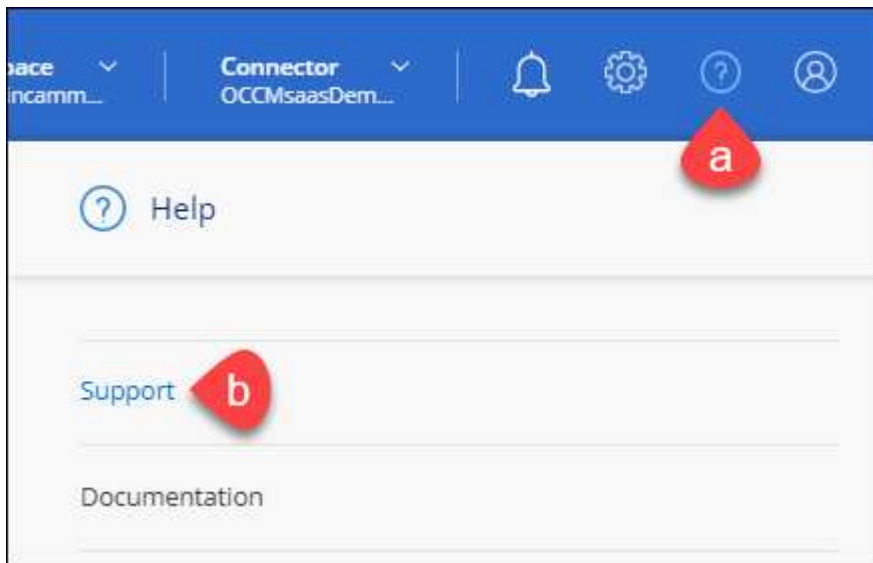
在向 NetApp 技术支持创建支持案例之前，您需要先将 NetApp 支持站点帐户添加到 Cloud Manager 中，然后注册获取支持。

添加 NSS 帐户

通过支持信息板，您可以从一个位置添加和管理所有 NetApp 支持站点帐户。

步骤

1. 如果您还没有 NetApp 支持站点帐户，["注册一个"](#)。
2. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 * 支持 *。



3. 单击 * NSS 管理 > 添加 NSS 帐户 *。
4. 出现提示时，单击 * 继续 * 以重定向到 Microsoft 登录页面。

NetApp 使用 Microsoft Azure Active Directory 作为身份提供程序来提供特定于支持和许可的身份验证服务。

5. 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。

此操作可使 Cloud Manager 使用您的 NSS 帐户。

请注意，此帐户必须是客户级别的帐户（而不是来宾或临时帐户）。

注册您的帐户以获得支持

支持注册可从 Cloud Manager 的支持信息板中获取。

步骤

1. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 * 支持 *。



2. 在 * 资源 * 选项卡中，单击 * 注册支持 *。
3. 选择要注册的 NSS 凭据，然后单击 * 注册 *。

获取帮助

NetApp 通过多种方式为 Cloud Manager 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。

自助支持

这些选项每周 7 天，每天 24 小时免费提供：

- ["知识库"](#)

通过 Cloud Manager 知识库搜索，查找有助于解决问题的文章。

- ["社区"](#)

加入 Cloud Manager 社区，关注正在进行的讨论或创建新的讨论。

- 文档。

您当前正在查看的 Cloud Manager 文档。

- [mailto: ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com)（反馈电子邮件）

我们非常重视您的反馈意见。提交反馈以帮助我们改进 Cloud Manager 。

NetApp 支持

除了上述自助支持选项之外，您还可以在激活支持后与 NetApp 支持工程师合作解决任何问题。

步骤

1. 在 Cloud Manager 中，单击 * 帮助 > 支持 *。
2. 在 "Technical Support" 下选择一个可用选项：
 - a. 单击 * 致电我们 * 可查找 NetApp 技术支持的电话号码。
 - b. 单击 * 打开问题描述 *，选择一个选项，然后单击 * 发送 *。

NetApp 代表将审核您的案例，并尽快与您联系。

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

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

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。

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

专利

有关 NetApp 拥有的专利的最新列表，请访问：

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

隐私政策

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

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。

- "有关 Cloud Manager 3.9 的注意事项"

版权信息

版权所有©2022 NetApp、Inc.。保留所有权利。Printed in the U.S.版权所涵盖的本文档的任何部分不得以任何形式或任何手段复制、包括影印、录制、磁带或存储在电子检索系统中—未经版权所有者事先书面许可。

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

本软件由NetApp按"原样"提供、不含任何明示或默示担保、包括但不限于适销性和特定用途适用性的默示担保、特此声明不承担任何任何责任。IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

商标信息

NetApp、NetApp标识和中列出的标记 <http://www.netapp.com/TM> 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。