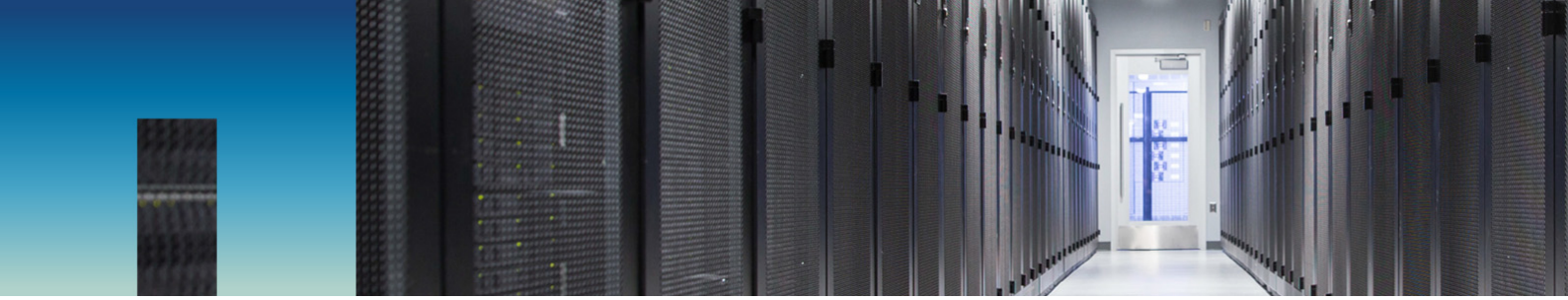


技术报告

NetApp 遥测数据的安全与隐私保护

NetApp Active IQ 团队
2018 年 5 月 | TR-4688

摘要

NetApp® Active IQ® 通过汇总 NetApp 系统内置预测技术的遥测数据来显示这些系统的相关信息。NetApp 客户应该了解如何保护这些遥测数据的安全和隐私。

NetApp®

目录

插图目录

1 引言

NetApp Active IQ 是一种云服务，基于同行比较和社区学习提供预测和建议，可帮助您成为数据驱动型 IT 组织。Active IQ 支持以下任务：

- 监控和预测容量使用情况，及早洞悉用户快速增长的数据需求
- 利用软件和固件自动升级提醒，提高安全性并保护您的投资
- 获取根据经验证的最佳实践提出的配置优化建议
- 实时深入洞察系统瓶颈，快速解决性能问题
- 获得来自整个 NetApp 用户群的诊断数据，应用社区智慧

Active IQ 通过汇总 NetApp ONTAP® 软件、NetApp SolidFire® 技术、NetApp E 系列存储控制器、NetApp StorageGRID® Webscale 对象存储和 NetApp Cloud Backup（原 AltaVault™）内置的预测技术的遥测数据，显示 NetApp 系统的相关信息。

注：此外，还会从 NetApp OnCommand® Insight、NetApp OnCommand Unified Manager 和 NetApp SANtricity® Web 服务中收集数据，但目前这些数据不会显示在 Active IQ 中。

NetApp 遥测服务的指导原则是：通过访问有关系统的配置、状态和性能信息来提供预测性分析和主动式支持。绝不会访问或传输存储在 NetApp 系统中的客户数据。

NetApp 客户应该了解收集哪些数据、如何将数据传输到 NetApp，以及如何保护数据的安全和隐私。

图 1) Active IQ 概述。

1.1 AutoSupport 预测技术

无论数据位于何处，NetApp AutoSupport® 技术都可以主动监控数据运行状况。它持续监控闪存、传统存储和云存储，利用超过 2000 亿条实时和历史诊断记录及时发现潜在问题，避免影响业务。

AutoSupport 定期向 NetApp 发送状态消息。如果出现问题，其中许多消息会自动创建案例，请求更多数据并提供纠正方案，您的 IT 员工不必执行任何操作。

遥测数据通过 NetApp Active IQ 界面提供给客户（产品所有者）和支持人员使用。

1.2 SolidFire Active IQ 预测技术

SolidFire Active IQ 从部署集群开始，持续主动监控您的系统，确保您拥有最高级别的可用性和性能。这些遥测数据还会上传到 Active IQ 数据库，处理后通过 NetApp Active IQ 界面提供给客户（产品所有者）和支持人员使用。

2 遥测数据的收集

AutoSupport 和 SolidFire Active IQ 收集有关系统配置、状态和性能的信息。如果您有隐私方面的担忧，可以禁用向 NetApp 发送遥测数据；但是，这样做您将无法正常使用预测性分析和主动式支持。

注：AutoSupport 在 ONTAP 软件和 StorageGRID Webscale 中默认启用，在其他系统和软件上则必须手动启用。

对于 ONTAP，您还可以选择屏蔽 AutoSupport 消息中的敏感信息，但这样做也会影响支持功能。默认情况下，此选项处于禁用状态。

以下部分列出了从每种类型的系统和软件中收集的信息。

2.1 ONTAP

以下列表是 ONTAP AutoSupport 消息中所包含内容的代表性示例。

注：您可以通过查看 AutoSupport 消息的清单来识别该消息中发送的确切内容。如需执行此操作，请使用 `system node autosupport manifest show` 命令。

- 消息的日期和时间戳
- ONTAP 软件版本
- 存储系统的序列号
- 加密软件许可证
- 存储系统的主机名称
- SNMP 联系人姓名和位置（如有指定）
- 控制台编码类型
- 提供系统信息的命令输出
- 校验和状态
- 纠错码 (Error-Correcting Code, ECC) 内存清理程序统计信息
- 如果高可用性 (High-availability, HA) 配置已获得许可，还包括以下信息：
  - HA 对中配对系统的系统 ID
  - HA 对中配对系统的主机名称
  - HA 节点状态，包括 HA 监控和 HA 互连统计信息
- `/etc` 目录下非隐私相关文件的内容
- 系统中所有 NetApp SnapLock® 卷的到期日期
- 注册表信息
- 使用情况信息
- 服务统计信息
- 启动时间统计信息
- NVLOG 统计信息
- WAFL 检查日志
- 修改的配置
- X-header 信息
- 启动设备（如 CompactFlash 卡）相关信息

虽然这些信息并不是业务数据，但如果与系统外的其他数据源一起使用，则可能被视为可识别客户身份的数据。ONTAP 提供了一种解决方案，即通过使用 `node autosupport modify` 命令的 `-remove-private-data` 参数屏蔽或筛选可识别客户身份的信息，保护敏感数据的隐私。一旦启用（设为 `true`），该参数将删除、编码或屏蔽 AutoSupport 附件和标题中的敏感数据。

被消除的数据包括以下各项：

- IP 地址
- MAC 地址
- URI
- DNS 名称
- 电子邮件地址
- 端口号
- 节点名称
- SVM 名称
- 集群名称
- 聚合名称
- 卷名称
- 接合路径
- 策略名称
- 用户 ID
- 组 ID
- LUN
- qtree 名称

仅当敏感环境需要最可靠的安全性时，才应删除私有数据。删除数据将对客户产生以下影响：

- 限制系统信息可见性和 Active IQ 的功能（例如，查看运营效率、性能和系统运行状况信息板视图时）
- 降低其他依靠 AutoSupport 内容分析的 NetApp 服务（如评估服务、存储优化和效率报告）向客户提供的价值
- 与发送完整的 AutoSupport 信息消息相比，支持部门解决问题所需的时间增加

2.2 E 系列

E 系列的每条 AutoSupport 消息均包含以下信息：

- 系统日志文件
- 配置数据（带格式的 XML 和非结构化命令输出）
- 状态数据（子系统启用/关闭和使用的容量）
- 性能指标
- 系统清单数据

2.3 SolidFire

从 SolidFire 系统收集以下信息：

- 卷、快照、帐户节点 ID 等
- 集群和卷的性能和容量数据
- 错误和事件历史记录
- SolidFire 软件版本
- 硬件配置信息
- 服务质量 (Quality-of-service, QoS) 配置

- 卷详细信息（大小、创建日期等）
- 卷访问组和会话配置
- 节点和集群 IP

不收集以下信息：

- 任何实际的最终用户数据
- CHAP 密钥
- 密码
- 集群管理用户信息

2.4 NetApp Cloud Backup

NetApp Cloud Backup 的每条 AutoSupport 消息均包含以下信息：

- 警报状态
- 最近的日志消息
- 硬件和软件诊断输出
- 性能指标
- 已清理的配置信息

2.5 StorageGRID Webscale

StorageGRID Webscale 的每条 AutoSupport 消息均包含以下信息：

- StorageGRID Webscale 软件版本
- 操作系统版本
- 系统级和位置级属性信息
- 过去七天内发出的所有警报
- 所有网格任务（包括历史数据）的当前状态
- SSM >“Events”（事件）>“Overview”（概述）页面上列出的事件信息
- 管理节点数据库使用情况
- 丢失或缺失的对象数量
- 网格配置设置
- NMS 实体
- 有效 ILM 策略
- 配置的网格规范文件

2.6 OnCommand Insight

OnCommand Insight 的 AutoSupport 消息包含以下信息：

- 有关 OnCommand Insight 实例的基本信息
- OnCommand Insight 实例中已获得许可的模块和协议
- OnCommand Insight 实例正在监控的阵列（序列号、制造商、型号、容量等）
- OnCommand Insight 正在监控的虚拟磁盘（数据源、位置、对象标识符、容量等）

2.7 OnCommand Unified Manager

OnCommand Unified Manager 的每条 AutoSupport 消息都包含以下信息：

- 由 Unified Manager 实例管理的系统的基本配置信息
- 日志文件
- 命令输出中的诊断内容

2.8 SANtricity Web 服务 (REST API)

SANtricity Web 服务的 AutoSupport 消息包含以下信息：

- 正在管理的系统的配置文件
- 应用程序的日志
- 特定于应用程序的计数器
- Web 服务器配置文件

3 遥测数据的传输

默认情况下，大多数 NetApp 产品使用 HTTPS 协议将遥测数据发送到 NetApp 技术支持。与 NetApp 的 HTTPS 连接使用 TLS 1.0 或更高版本进行加密和身份验证。NetApp 强烈建议使用 HTTPS，因为它更安全，有助于 NetApp 提供更好的支持，并通过 Active IQ 提供更好的分析。

表 1) 支持的 AutoSupport 传输协议。

产品	默认协议	支持的其他协议
NetApp Cloud Backup	HTTPS	无
E 系列	HTTPS	HTTP 和 SMTP
OnCommand Insight	HTTPS	HTTP、SMTP 和 FTP
OnCommand Unified Manager	HTTPS	无
ONTAP	HTTPS	HTTP 和 SMTP
SANtricity Web 服务	HTTPS	HTTP 和 SMTP
SolidFire	HTTPS	无
StorageGRID Webscale	SMTP	无

注：AutoSupport 消息通常用于 NetApp 支持。虽然可以将 AutoSupport 配置为通知 ONTAP 系统关键事件，但仍应使用事件管理系统 (Event Management System, EMS) 中的事件通知功能，以便接收需要注意的问题通知。

图 2 介绍了 AutoSupport 如何将数据从 ONTAP 系统传输到 NetApp。

图 2) AutoSupport 数据的传输方式。

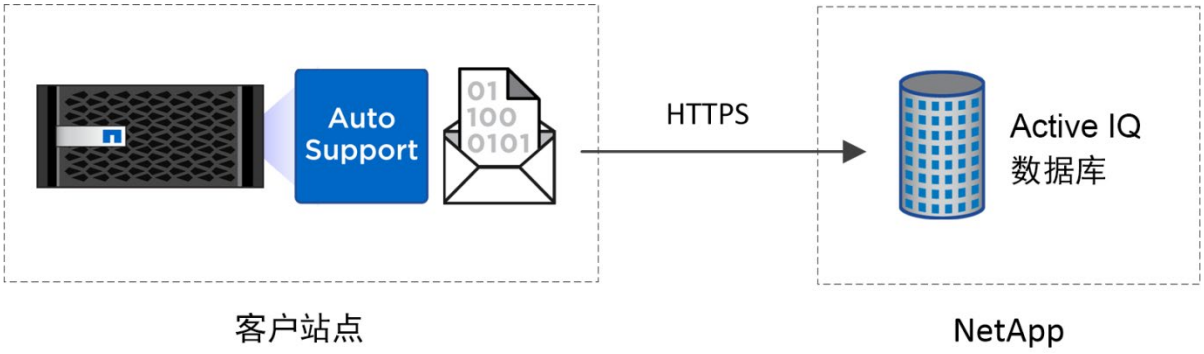
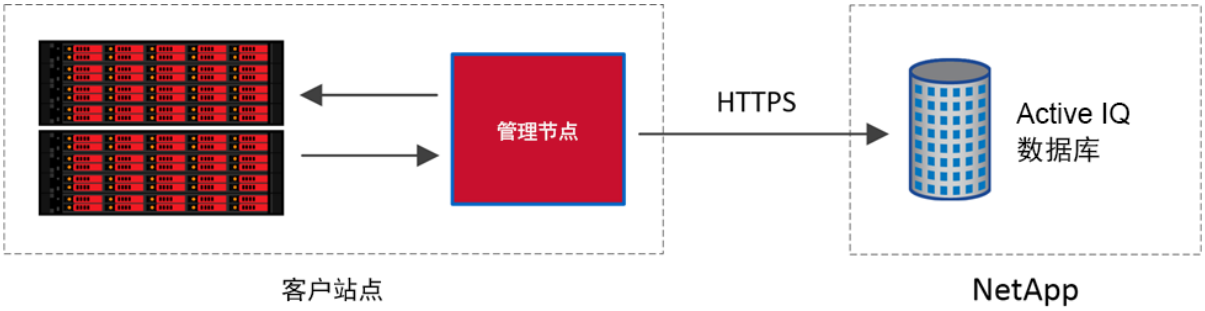


图 3 介绍了 SolidFire 如何将遥测数据传输到 NetApp。

图 3) SolidFire 遥测数据的传输方式。



3.1 AutoSupport 消息的按需传送

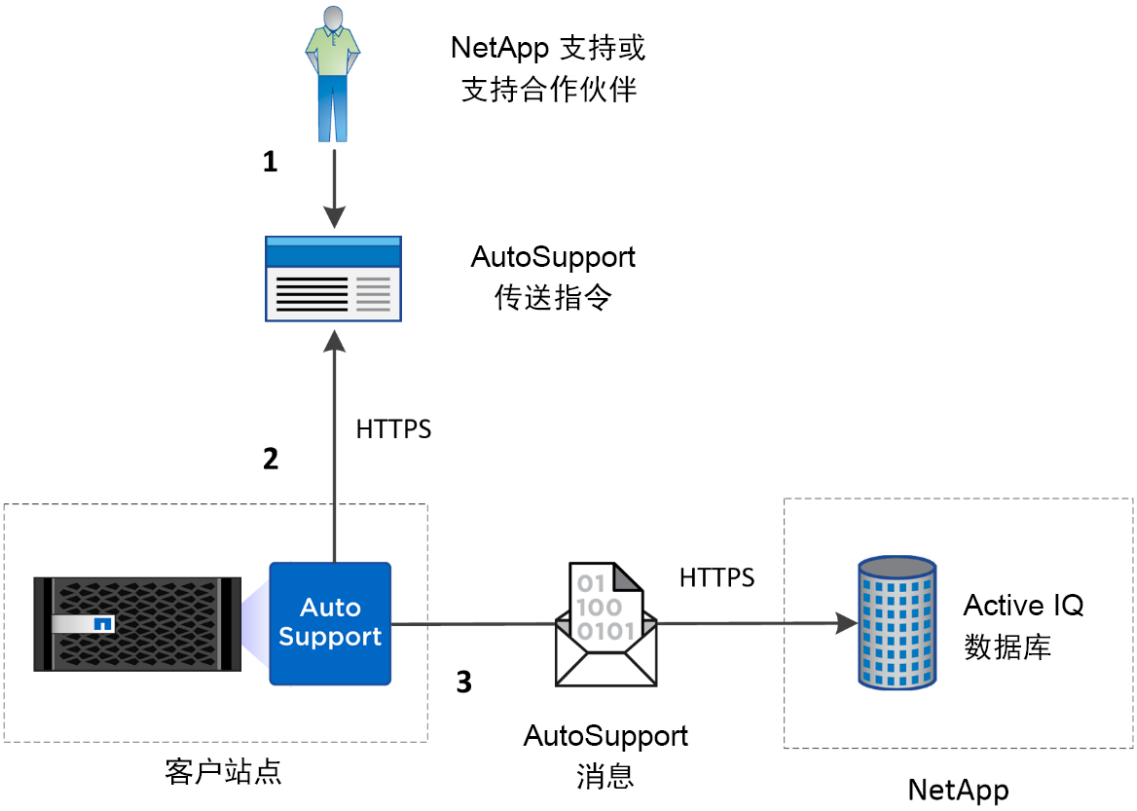
AutoSupport On Demand 按需传送功能支持 NetApp 按需请求 AutoSupport 消息，无需客户干预即可对案例进行故障排除。ONTAP 和 E 系列系统支持此功能，这些系统使用 HTTPS 将消息传送到 NetApp。

AutoSupport On Demand 是一种传送服务，存储系统通过该服务轮询 support.netapp.com，然后在收件箱中查找指令。该服务的工作原理如下：

1. NetApp 支持或支持合作伙伴根据需要为特定系统创建传送指令。这些指令可发送一组有限的预定义 AutoSupport 传送指令：
   a. 请求新的 AutoSupport 数据以确定当前系统状态。
   b. 请求更多深度 AutoSupport 数据以解决复杂案例（诊断 AutoSupport 消息、核心文件和性能归档）。
   c. AutoSupport 消息的核心文件中不包含客户数据的内存缓冲区。
2. 系统会定期轮询 AutoSupport On Demand 服务，以通过加密的 HTTPS 获取传送指令。所有传输均从系统端（而不是 AutoSupport 服务器）启动。
3. 如果系统获取了传送指令，AutoSupport 则调用新消息并使用 HTTPS 将其发送到 NetApp。

图 4 介绍了 AutoSupport On Demand 工作流。图中的数字对应上述步骤编号。

图 4) AutoSupport On Demand 工作流。



只有拥有有效 NetApp 支持站点凭据和适当业务角色（技术支持工程师、支持客户经理以及有权使用给定存储系统的支持合作伙伴）的用户才能使用 AutoSupport On Demand。

AutoSupport On Demand 使用情况是透明的：

- 客户可以使用 ONTAP 命令行界面查看和执行所有预定义的传送指令。
- 如果系统配置为将 AutoSupport 消息发送给内部支持组织和合作伙伴，客户和合作伙伴可以收到 AutoSupport 消息的副本。
- 跟踪和显示 On Demand 使用情况：
  - On Demand 请求记录在每日管理日志 AutoSupport 消息中。
  - 生成的 AutoSupport 消息将在标题中注明 On Demand，可通过 Active IQ 查看这些消息。

4 遥测数据的访问和保留

4.1 数据驻留位置

AutoSupport 数据将发送到 NetApp 位于美国的一个或多个数据中心。数据不会归档到异地位置。

SolidFire 数据驻留在美国的 NetApp 数据中心和 Amazon S3 中。

4.2 数据加密

收到数据后，不会对处于静态或传输过程中的数据进行加密。

4.3 数据访问权限

对 NetApp 遥测数据的访问受到数据访问层的保护，该访问层要求对每个请求访问的用户进行正确识别。所有数据请求必须包含一个对请求访问权限个人的可核实证明。数据访问层使用以下方法实现：

- 用于身份验证的安全断言标记语言 (Security Assertion Markup Language, SAML)，需要个人向 NetApp 注册
- 通过身份验证的用户属性（任职公司、地理位置、公民身份等）
- 基于角色的访问控制（职务）

以下人员可以访问数据：

- **NetApp 内部用户。**NetApp 员工和经批准的代理可以访问数据，以便为客户提供支持时使用。

  注： 对于具有 SupportEdge Secure for Government 支持级别的系统，NetApp 对遥测数据的访问仅限于在美国工作且为美国公民的员工和承包商。

- **客户。**任何已在 NetApp 支持站点注册的公司用户可以访问已启用 AutoSupport 和 SolidFire Active IQ 且具有有效支持合同的所有已安装系统的数据。

  用户只能查看注册在其公司下的系统。Active IQ 使用 NetApp 支持站点的产品注册和支持注册凭据来控制访问权限。

  合作伙伴。对于 AutoSupport，已在 NetApp 支持站点注册的合作伙伴可以访问其已销售且当前享受支持服务的所有系统的数据，前提是这些系统已启用 AutoSupport 且具有有效支持合同。

4.4 安全性测试

NetApp 在月度周期系统集成测试中测试访问控制。NetApp 每月还会运行一次漏洞评估。

4.5 数据保留期限

如果客户请求删除 AutoSupport 数据，NetApp 将提供支持。

在支持合同有效的前提下，NetApp 最长可保留 SolidFire 遥测数据 5 年。

4.6 认证

NetApp 已通过 ISO 27001:2013 认证。此认证的范围包括 AutoSupport。NetApp 不向客户提供审计报告。

如何查找其他信息

如需详细了解本文档所述的信息，请参见以下资源。（其中部分资源需要 NetApp 支持站点帐户，NetApp 客户拥有支持站点帐户。）

- Active IQ
  https://mysupport.netapp.com/myautosupport/home.html
- NetApp Cloud Backup 资源
  https://mysupport.netapp.com/altavault/resources
- E 系列文档中心
  https://mysupport.netapp.com/eseries
- OnCommand Insight 资源
  https://mysupport.netapp.com/oncommandinsight/resources
- OnCommand Unified Manager 资源
  https://mysupport.netapp.com/unifiedmanager/resources
- ONTAP 资源
  https://mysupport.netapp.com/ontap/resources
- SolidFire 资源
  https://mysupport.netapp.com/solidfire/resources
- StorageGRID Webscale 资源
  https://mysupport.netapp.com/storagegridwebscale/resources

版本历史

版本	日期	文档版本历史
1.0 版	2018 年 4 月	初始版本

要验证您的特定环境是否支持本文档所述的确切产品和功能版本，请参见 NetApp 支持站点上的互操作性表工具 (IMT)。NetApp IMT 中定义的产品组件和版本可用于构建 NetApp 所支持的配置。具体的配置结果取决于每个客户如何依照所发布规格进行安装。

版权信息

商标信息