



Ask Me AI助手

Information Security for Workload Factory

NetApp

September 16, 2026

目录

- Ask Me AI助手 1
 - 适用于 NetApp Workload Factory 的 Ask Me 安全架构 1
 - Ask Me 中的 RAG 架构 1
 - 多层提示安全 1
 - 模型数据隔离和隐私 1
 - 工具使用和代理安全 2
 - 适用于 NetApp Workload Factory 的 Ask Me 访问控制 2
 - 身份验证 2
 - 凭据保护和密钥处理 2
 - 基础设施安全 2
 - 适用于 NetApp Workload Factory 的 Ask Me 执行模式 2
 - 工具执行保障措施 3
 - 输出控制 3
 - 向我询问 NetApp Workload Factory 的隐私和可用性 3
 - 数据处理和隐私 3
 - 可用性和隔离控制 3

Ask Me AI助手

适用于 NetApp Workload Factory 的 Ask Me 安全架构

Ask Me 是一款嵌入在 NetApp Workload Factory 中的生成式人工智能助手。它为 Amazon FSx for NetApp ONTAP 和 Workload Factory 主题提供实时对话支持。回复基于经过验证的 NetApp 文档，Ask Me 无法访问公共互联网或使用客户数据来训练模型。多个安全层有助于阻止恶意查询、限制对受支持域的响应，并防止用户输入覆盖系统指令。当 Ask Me 使用工具时，授权边界、只读查询强制执行、临时沙箱和审核日志记录有助于约束和监控执行。

您可以随时通过 Workload Factory 的 **Administration**（管理）设置退出 Ask Me，这将禁用针对您用户帐户的助手。[详细了解如何管理 GenAI 功能。](#)

Ask Me 中的 RAG 架构

Ask Me 使用检索增强生成（RAG）。

- 精心策划的知识库：回复基于经过验证的已发布 NetApp 文档的托管语料库。
- 检索评分和过滤：模型上下文中仅包含足够相关的内容。
- 无法访问互联网：模型无法获取、浏览或抓取外部内容。
- 源归因：回复包括对所用源文档的引用。

多层提示安全

- 第1层：安全分类器（LLM-as-a-judge）拦截恶意查询（提示注入、权限升级、数据泄露、社交工程、策略违规）。

系统会记录被阻止的查询，生成模型永远不会看到这些查询。

- 第2层：系统提示强化可防止用户输入覆盖系统指令。
- 第3层：域范围限制将响应限定在 FSx ONTAP 和 Workload Factory 主题范围内。
- 第4层：工具使用治理在强化沙箱中验证参数并运行查询；模型无法执行任意操作。

模型数据隔离和隐私

- 不对客户数据进行模型训练
- 请求级隔离（无跨租户数据泄露）
- 具有有界历史记录的话范围对话上下文
- 无持久模型内存
- 受管推理基础设施

工具使用和代理安全

- 授权范围的工具（强制执行用户权限边界）
- 严格的工具执行超时
- 用于检索数据的临时会话范围沙箱
- 使用允许列表实施只读查询
- 具有敏感参数清理功能的工具调用可审计性

适用于 NetApp Workload Factory 的 Ask Me 访问控制

在 NetApp Workload Factory 中，Ask Me 的访问安全核心在于运行时操作期间的身份验证会话、用户级问责制和受保护的密钥处理。身份验证控件会验证每个会话，并将交互与特定用户关联。敏感凭据在运行时从托管密钥保管库中检索，并从日志中清除。该服务还应用基础架构控制，包括非 root 容器执行和受限的 CORS 允许列表。

身份验证

- 带有加密验证的签名 JWT 身份验证（包括受众、颁发者和算法检查，如 RS256）
- 服务边界处中间件强制身份验证
- 用户身份范围界定，以便交互可归因于特定用户

凭据保护和密钥处理

- 安全保管库存储：服务使用的敏感凭据存储在托管密钥保管库中，并在运行时检索。应用程序代码、配置文件或容器映像中不存储任何机密。
- 日志清理：敏感值（凭据、令牌、密码、访问密钥、证书）在写入日志之前会从日志中隐去。

基础设施安全

- 非 root 容器执行
- CORS 限制为受信任的 NetApp 域的显式允许列表

适用于 NetApp Workload Factory 的 Ask Me 执行模式

NetApp Workload Factory 为 Ask Me 提供多种执行模式，每种执行模式具有不同的安全和隐私特性。当 Ask Me 使用工具集成时，例如查询客户自己的 Workload Factory 资源，工具执行通过分层保护进行控制。启用工具的执行在经过身份验证的用户权限内运行，并对每个操作的持续时间和范围施加限制。检索到的数据保留在阻止外部访问的临时会话沙箱中，并在会话结束时销毁。独立的提示和代码控制强制执行只读查询，而审核记录捕获工具活动并清除敏感值。

工具执行保障措施

- 授权范围的工具在经过身份验证的用户权限内运行。
- 工具执行超时限制长时间运行的操作。
- 临时数据沙箱在会话范围内存储工具检索的数据，在引擎级别阻止外部访问、文件 I/O、网络调用和扩展加载，并在会话结束时销毁。
- 只读查询强制执行通过严格的允许列表验证生成的查询。
- 提示执行和代码执行的安全性是独立应用的。
- 工具调用可审计性日志记录工具名称、参数、时间戳和结果状态，并对敏感值进行脱敏处理。

输出控制

- 令牌限制强制执行
- 分类/安全关键操作的确定性输出（温度 0）
- 提前终止和清理的流式传输

向我询问 NetApp Workload Factory 的隐私和可用性

在 NetApp Workload Factory 中，Ask Me 隐私控制可限制数据泄露、保持会话处理隔离，并维护用户交互的隐私边界。您的输入由托管 AI 服务处理，该服务不会使用这些输入来训练或改进基础模型。检索到的操作数据在会话期间保留在临时内存存储中，不会被持久化或共享。跨多个云区域的多模型回退链可在主模型受到限制或不可用时支持可用性，同时相同的安全控制也适用于回退模型。

数据处理和隐私

- 提示中的用户数据：由托管 AI 服务处理，不使用您的输入来训练或改进基础模型。
- 知识库内容：仅限精选、已发布的 NetApp 文档；您的数据不包括在内。
- 操作数据：仅在用户查询自己的资源时检索；在会话期间保存在临时内存存储中，不持久化或共享。
- 审核日志：记录查询元数据（匿名用户 ID、时间戳、持续时间），并清除敏感字段。
- 反馈数据：单独存储并链接到查询 ID，而非匿名用户 ID 以外的个人身份信息。

可用性和隔离控制

Ask Me 在多个云区域采用多模型后备链。

如果主模型受到限制或不可用，系统可以故障转移到其他模型。

所有模型均受相同的安全控制、系统提示加固和隔离保证。

版权信息

版权所有 © 2026 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。