



Assistente Ask Me AI

Information Security for Workload Factory

NetApp
September 16, 2026

Índice

- Assistente Ask Me AI 1
 - Pergunte-me sobre a arquitetura de segurança do NetApp Workload Factory 1
 - Arquitetura RAG em Ask Me 1
 - Segurança de prompt em várias camadas 1
 - Isolamento e privacidade dos dados do modelo 2
 - Uso de ferramentas e segurança agente 2
 - Controle de acesso para o NetApp Workload Factory 2
 - Autenticação 2
 - Proteção de credenciais e manuseio de segredos 2
 - Segurança da infraestrutura 3
 - Modos de execução Ask Me para NetApp Workload Factory 3
 - Salvaguardas de execução da ferramenta 3
 - Controles de saída 3
 - Pergunte-me sobre privacidade e disponibilidade para o NetApp Workload Factory 3
 - Tratamento e privacidade de dados 4
 - Controles de disponibilidade e isolamento 4

Assistente Ask Me AI

Pergunte-me sobre a arquitetura de segurança do NetApp Workload Factory

O Ask Me é um assistente generativo com inteligência artificial integrado ao NetApp Workload Factory. Ele oferece suporte conversacional em tempo real para Amazon FSx for NetApp ONTAP e tópicos do Workload Factory. As respostas são baseadas em documentação verificada da NetApp, e o Ask Me não pode acessar a internet pública nem usar dados do cliente para treinar o modelo. Múltiplas camadas de segurança ajudam a bloquear consultas maliciosas, limitar as respostas a domínios suportados e impedir que a entrada do usuário substitua as instruções do sistema. Quando o Ask Me usa ferramentas, limites de autorização, imposição de consultas somente leitura, um ambiente de teste temporário e registro de auditoria ajudam a restringir e monitorar a execução.

Você pode desativar o recurso "Pergunte-me" a qualquer momento nas configurações de **Administração** do NetApp Workload Factory, o que desativa o assistente para sua conta de usuário. ["Saiba mais sobre como gerenciar os recursos do GenAI."](#)

Arquitetura RAG em Ask Me

O Ask Me utiliza geração aumentada por recuperação (RAG).

- Base de conhecimento selecionada: as respostas são fundamentadas em um conjunto gerenciado de documentação verificada e publicada da NetApp.
- Pontuação e filtragem de recuperação: apenas o conteúdo suficientemente relevante é incluído no contexto do modelo.
- Sem acesso à internet: o modelo não consegue buscar, navegar ou extrair conteúdo externo.
- Atribuição da fonte: as respostas incluem referências aos documentos de origem utilizados.

Segurança de prompt em várias camadas

- Camada 1: O classificador de segurança (LLM como juiz) bloqueia consultas maliciosas (injeção de prompts, escalonamento de privilégios, exfiltração de dados, engenharia social, violações de políticas).

O sistema registra as consultas bloqueadas, e o modelo generativo nunca as vê.

- Camada 2: O reforço da segurança dos comandos do sistema impede que a entrada do usuário substitua as instruções do sistema.
- Camada 3: o escopo do domínio limita as respostas aos tópicos do Amazon FSx for NetApp ONTAP e do NetApp Workload Factory.
- Camada 4: a governança de uso de ferramentas valida parâmetros e executa consultas em um ambiente de teste reforçado; o modelo não pode executar operações arbitrárias.

Isolamento e privacidade dos dados do modelo

- Nenhum treinamento de modelo em dados de clientes
- Isolamento no nível da solicitação (sem vazamento de dados entre locatários)
- Contexto de conversação com escopo de sessão e histórico delimitado
- Sem memória de modelo persistente
- Infraestrutura de inferência gerenciada

Uso de ferramentas e segurança agente

- Ferramentas com escopo de autorização (limites de permissão do usuário aplicados)
- Tempos limite rigorosos para execução de ferramentas
- Sandbox efêmero com escopo de sessão para dados recuperados
- Imposição de consultas somente leitura com allowlisting
- Auditabilidade de chamadas de ferramentas com limpeza de parâmetros sensíveis

Controle de acesso para o NetApp Workload Factory

No NetApp Workload Factory, o Ask Me prioriza a segurança de acesso em sessões autenticadas, a responsabilização em nível de usuário e o tratamento de segredos protegidos durante as operações de tempo de execução. Os controles de autenticação validam cada sessão e associam as interações a um usuário específico. As credenciais confidenciais são recuperadas de um cofre de segredos gerenciado em tempo de execução e ocultadas dos registros. O serviço também aplica controles de infraestrutura, incluindo a execução de contêineres sem privilégios de root e uma lista de permissões CORS restrita.

Autenticação

- Autenticação JWT assinada com validação criptográfica (incluindo verificações de público, emissor e algoritmo, como RS256)
- Autenticação aplicada por middleware no limite do serviço
- Definição do escopo da identidade do usuário para que as interações sejam atribuídas a um usuário específico

Proteção de credenciais e manuseio de segredos

- Armazenamento seguro em cofre: as credenciais confidenciais usadas pelo serviço são armazenadas em um cofre de segredos gerenciado e recuperadas em tempo de execução. Nenhum segredo é armazenado no código do aplicativo, nos arquivos de configuração ou nas imagens do contêiner.
- Limpeza de logs: valores sensíveis (credenciais, tokens, senhas, chaves de acesso, certificados) são removidos dos logs antes de serem gravados.

Segurança da infraestrutura

- Execução de contêiner sem privilégios de root
- CORS restrito a uma lista explícita de domínios confiáveis da NetApp

Modos de execução Ask Me para NetApp Workload Factory

NetApp Workload Factory oferece múltiplos modos de execução para o Ask Me, cada um com diferentes características de segurança e privacidade. Quando o Ask Me utiliza integrações de ferramentas, por exemplo, consultando os recursos do próprio Workload Factory do cliente, a execução da ferramenta é controlada por meio de camadas de proteção. A execução habilitada para ferramentas opera dentro das permissões do usuário autenticado e aplica limites à duração e ao escopo de cada operação. Os dados recuperados permanecem em um ambiente isolado de sessão efêmero que bloqueia o acesso externo e é destruído ao final da sessão. Controles independentes de prompt e código impõem consultas somente leitura, enquanto registros de auditoria capturam a atividade da ferramenta com valores sensíveis removidos.

Salvaguardas de execução da ferramenta

- As ferramentas com escopo de autorização operam dentro das permissões do usuário autenticado.
- O tempo limite de execução da ferramenta limita operações de longa duração.
- O ambiente de dados efêmeros armazena dados recuperados por ferramentas no escopo da sessão, bloqueia acesso externo, E/S de arquivos, chamadas de rede e carregamento de extensões no nível do mecanismo e é destruído quando a sessão termina.
- A aplicação de consultas somente leitura valida as consultas geradas por meio de uma lista de permissões rigorosa.
- A segurança imposta por prompt e a segurança imposta por código são aplicadas de forma independente.
- Os registros de auditoria de chamadas de ferramentas incluem o nome da ferramenta, parâmetros, carimbos de data/hora e status do resultado, com remoção de valores confidenciais.

Controles de saída

- Aplicação do limite de tokens
- Saída determinística para operações de classificação/segurança crítica (temperatura 0)
- Transmissão com encerramento antecipado e limpeza

Pergunte-me sobre privacidade e disponibilidade para o NetApp Workload Factory

No NetApp Workload Factory, os controles de privacidade do Ask Me limitam a exposição dos dados, mantêm o processamento da sessão isolado e preservam os limites de privacidade para as interações do usuário. Suas entradas são processadas por um serviço de IA gerenciado que não as utiliza para treinar ou aprimorar modelos básicos. Os dados operacionais recuperados permanecem em armazenamento efêmero

na memória durante a sessão e não são persistidos nem compartilhados. Uma cadeia de fallback multimodelo em diversas regiões da nuvem garante a disponibilidade quando o modelo principal está com desempenho limitado ou indisponível, enquanto os mesmos controles de segurança se aplicam aos modelos de fallback.

Tratamento e privacidade de dados

- Dados do usuário em prompts: processados por um serviço de IA gerenciado que não utiliza suas entradas para treinar ou aprimorar foundation models.
- Conteúdo da base de conhecimento: somente documentação NetApp selecionada e publicada; seus dados não estão incluídos.
- Dados operacionais: recuperados somente quando um usuário consulta seus próprios recursos; mantidos em armazenamento efêmero na memória durante a sessão e não persistidos ou compartilhados.
- Registro de auditoria: metadados de consulta (ID de usuário anonimizado, registros de data e hora, durações) registrados, com os campos sensíveis removidos.
- Dados de feedback: armazenados separadamente e vinculados a um ID de consulta, não a informações de identificação pessoal além do ID de usuário anonimizado.

Controles de disponibilidade e isolamento

O Ask Me emprega uma cadeia de fallback multimodelo em várias regiões de nuvem.

Se o modelo principal estiver com desempenho limitado ou indisponível, o sistema pode recorrer a modelos alternativos.

Todos os modelos estão sujeitos aos mesmos controles de segurança, reforço da segurança do sistema e garantias de isolamento.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.