Modelo de segurança e responsabilidades

Information Security for Workload Factory

NetApp
September 16, 2026

Índice

Modelo de segurança e responsabilidades

Saiba mais sobre o modelo de segurança do NetApp Workload Factory

O NetApp Workload Factory é um plano de controle SaaS que ajuda você a gerenciar e otimizar cargas de trabalho executadas no Amazon FSx for NetApp ONTAP em seu ambiente AWS. Os resultados de segurança dependem de responsabilidades compartilhadas entre a NetApp, a AWS e sua organização.

Modelo de segurança de alto nível

- O Workload Factory usa um modelo de assunção de função do IAM para obter credenciais temporárias do AWS STS para chamar APIs da AWS em sua conta.
- Alguns fluxos de trabalho exigem operações nativas do ONTAP que não são expostas pelas APIs da AWS; você pode executar essas operações dentro da sua VPC usando componentes de execução implantados pelo cliente (por exemplo, o Lambda link).
- Os sinais de observabilidade (métricas, telemetria e registros operacionais) dão suporte ao monitoramento operacional e às investigações.

Principais questões de revisão

- Que tipo de acesso o NetApp Workload Factory requer à sua conta AWS (confiança de função + permissões)?
- Quais caminhos de execução se aplicam aos seus fluxos de trabalho pretendidos (somente API da AWS ou operações nativas do ONTAP por meio de um componente VPC)?
- Quais categorias de dados são tratadas (configuração/metadados, logs/eventos operacionais, telemetria) e onde são armazenadas?
- Quais sinais de monitoramento existem e quais são as suas características de retenção?

O que vem a seguir

- "Limites de responsabilidade compartilhada para o NetApp Workload Factory"
- "Conectividade e caminhos de confiança para o NetApp Workload Factory"
- "Níveis de permissão de privilégio mínimo para o NetApp Workload Factory"

Limites de responsabilidade compartilhada para o NetApp Workload Factory

NetApp Workload Factory a responsabilidade pela segurança é compartilhada entre a NetApp (operação SaaS), a AWS (infraestrutura de nuvem e serviços gerenciados) e você (configuração do cliente). Compreender onde a responsabilidade de cada parte começa e termina ajuda você a configurar seu ambiente AWS corretamente e evitar falhas de segurança. Esses limites esclarecem o que a NetApp opera, o que a AWS protege e o que você deve configurar e manter por conta própria.

NetApp responsabilidades (lado do serviço)

NetApp é responsável por operar e proteger a plataforma SaaS Workload Factory. Isso inclui o gerenciamento, no lado do serviço, das referências de configuração armazenadas e dos dados operacionais.

Responsabilidades da AWS (plataforma de nuvem)

A AWS é responsável pela segurança da infraestrutura de nuvem e dos serviços gerenciados usados em sua implantação e fluxos de trabalho (por exemplo, IAM/STS, FSx for ONTAP, CloudWatch, KMS, Secrets Manager, CloudFormation, Lambda e primitivas de rede).

Responsabilidades do cliente (sua configuração)

Você é responsável por:

- Funções do AWS IAM, políticas de confiança e permissões de privilégio mínimo
- Controles da VPC (sub-redes, grupos de segurança, roteamento, endpoints e egress)
- Governança de credenciais (incluindo credenciais do ONTAP, se exigidas pelos seus fluxos de trabalho)
- Decisões de criptografia e gerenciamento de chaves (por exemplo, chaves KMS opcionais gerenciadas pelo cliente para Amazon FSx for NetApp ONTAP)
- Monitoramento, alertas, políticas de retenção e processos de resposta a incidentes

Evidências para capturar

- Relação de confiança da função IAM (incluindo condição de ID externo)
- Seleção de níveis de permissão do IAM e artefatos de política
- Decisão sobre o limite da rede (somente API da AWS vs componente de execução de VPC, como o link Lambda)
- Decisões de observabilidade e expectativas de retenção
- Decisão de capacitação de IA (os diagnósticos de IA estão ativados por padrão, a menos que sejam explicitamente desativados)

NetApp Workload Factory fluxo de trabalho de segurança de integração

A integração com o NetApp Workload Factory estabelece acesso seguro ao seu ambiente AWS antes de você começar a usar o produto. O processo combina configuração de confiança na AWS, definição de escopo de permissões, configuração de conectividade, verificação de observabilidade e capacitação opcional de diagnósticos de IA.

Passo 1: defina sua postura de integração

- Identifique as contas da AWS e os limites do ambiente (por exemplo, separação entre prod e non-prod).
- Identifique os fluxos de trabalho necessários (descoberta somente leitura vs provisionamento vs operações nativas do ONTAP).

- Decida se deve implantar componentes de execução de VPC (por exemplo, link Lambda) com base nas necessidades do fluxo de trabalho.
- Decida se deseja ativar o diagnóstico por IA (ativado por padrão).

Informações relacionadas

- "Tipos de credencial"
- "Visão geral do link Lambda"
- "Visão geral dos controles de IA"

Etapa 2: estabeleça a confiança e o acesso à AWS

1. Implante uma função do IAM em sua conta da AWS.
2. Assunção da função Gate usando um ID externo na política de confiança.
3. Registre o ARN da função e o ID externo no NetApp Workload Factory.

Informações relacionadas

"Integração de conta AWS"

Etapa 3: aplicar permissões de privilégio mínimo

1. Selecione o nível mínimo de permissão que suporta seus fluxos de trabalho pretendidos.
2. Verifique se as políticas de sessão por solicitação restringem as ações à operação que está sendo executada.

Informações relacionadas

"Níveis de permissão de privilégio mínimo para o NetApp Workload Factory".

Etapa 4: configure a conectividade e os limites da VPC (conforme necessário)

1. Valide os caminhos de rede necessários para os endpoints da AWS.
2. Se você precisar de operações nativas do ONTAP, implante e valide a opção de execução apropriada em sua VPC.

Informações relacionadas

- "Conectividade e caminhos de confiança para o NetApp Workload Factory"
- "Opções de execução do ONTAP para o NetApp Workload Factory"

Etapa 5: verificar a observabilidade

1. Confirme se as métricas e a telemetria estão sendo coletadas e retidas conforme o esperado.
2. Confirme se você pode acessar os registros operacionais necessários para a resolução de problemas e investigações.

Informações relacionadas

- "Visão geral da observabilidade para o NetApp Workload Factory"
- "Métricas e telemetria para o NetApp Workload Factory"

Etapa 6: ativar diagnósticos de IA (opcional)

O diagnóstico por IA está ativado por padrão. Se você os ativar, verifique se atende aos pré-requisitos e restrinja as permissões ao mínimo necessário.

Informações relacionadas

- "Opção de ativação do Bedrock para NetApp Workload Factory diagnósticos de IA"
- "Limitações das ferramentas de IA para o NetApp Workload Factory"

Postura de conformidade e segurança para o NetApp Workload Factory

O NetApp Workload Factory foi desenvolvido com a conformidade e a segurança como prioridades fundamentais. Todos os workloads no Workload Factory são executados no Amazon FSx for NetApp ONTAP. Além do "Recursos de segurança da AWS", o NetApp Workload Factory possui "Conformidade com SOC2 Tipo 1, SOC2 Tipo 2 e HIPAA".

Amazon FSx for NetApp ONTAP para NetApp Workload Factory é um "Solução AWS para implantação de aplicativos empresariais" e segue as melhores práticas do AWS Well-Architected.

Informações sobre direitos autorais

Informações sobre marcas comerciais