Arquitetura e conectividade

Information Security for Workload Factory

NetApp
September 16, 2026

Índice

Arquitetura e conectividade

Conectividade e caminhos de confiança para o NetApp Workload Factory

O NetApp Workload Factory se comunica com as APIs da AWS, recursos da conta AWS do cliente, link do AWS Lambda e Amazon Bedrock, cada um com seus próprios protocolos, portas e métodos de autenticação. Essas conexões são organizadas em grupos que separam o plano de gerenciamento da AWS, o plano de dados do ONTAP e o tráfego do link do Lambda, permitindo que você avalie os limites de confiança de forma independente.

Caminhos de conectividade

O Workload Factory estabelece vários caminhos de conectividade distintos, cada um com uma finalidade específica na descoberta, provisionamento e gerenciamento dos seus recursos AWS e ONTAP. Alguns caminhos se originam do próprio Workload Factory usando credenciais AWS presumidas, enquanto outros passam pelo Lambda link, que opera dentro da sua VPC para acessar os endpoints de gerenciamento do ONTAP sem expô-los publicamente. Um caminho opcional para o Amazon Bedrock oferece suporte a diagnósticos assistidos por IA e fica ativo somente quando sua organização habilita esse recurso.

As seções a seguir descrevem cada caminho, incluindo as APIs da AWS ou do ONTAP envolvidas, as credenciais ou autenticação utilizadas e quaisquer condições que determinam se o caminho está ativo. Compreender esses caminhos ajuda você a avaliar quais acesso à rede e permissões o Workload Factory requer e onde os dados cruzam os limites da conta ou da VPC.

O Workload Factory para APIs da AWS

O Workload Factory utiliza `DescribeFileSystems`, `DescribeVolumes`, `CreateVolume`, `UpdateVolume`, `DeleteVolume`, `CreateFileSystem`, `CreateBackup`, `DescribeBackups` e APIs do EC2/VPC para descoberta de sub-redes e grupos de segurança.

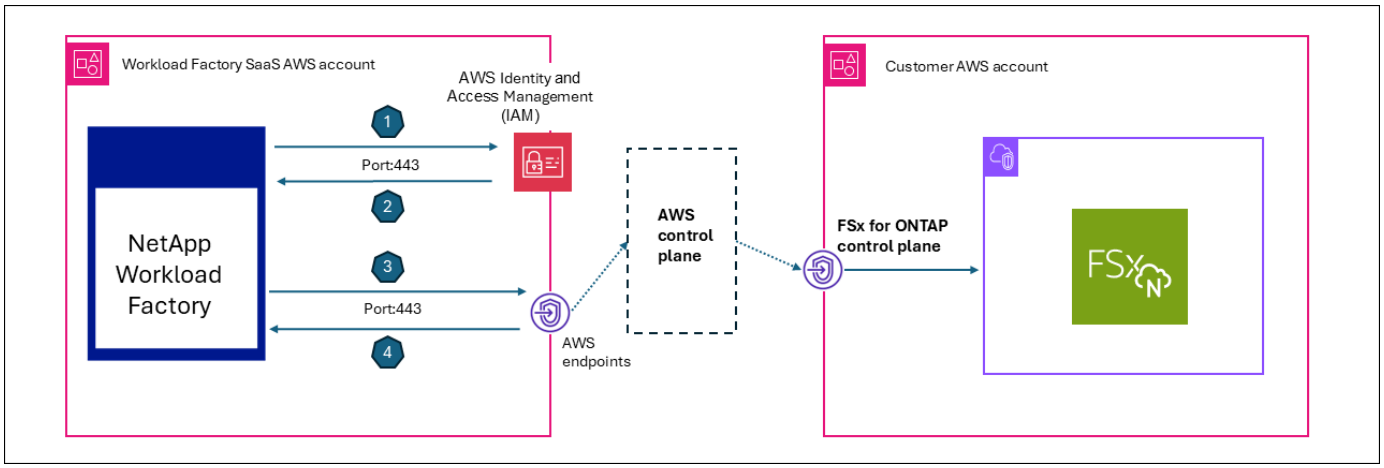
- O serviço de coleta faz varreduras aproximadamente a cada cinco horas.
- As operações CRUD são executadas sob demanda.
- Todas as chamadas utilizam credenciais temporárias assumidas pelo STS com um ID externo.

O Workload Factory para recursos da conta AWS do cliente (orquestração e automação)

O Workload Factory interage com a AWS para se comunicar e criar recursos. A orquestração e a automação ocorrem de diversas maneiras.

- Modelos AWS CloudFormation: O Workload Factory usa modelos AWS CloudFormation para criar recursos como funções e sistemas de arquivos. Por exemplo, ao criar um sistema de arquivos na interface de usuário, o Workload Factory chama diretamente o CloudFormation e redireciona você para sua conta AWS.
- Chamadas à API da AWS: O Workload Factory usa chamadas à API da AWS (STS `AssumeRole`) para enviar comandos de API para o FSx para atividades relacionadas ao ONTAP.
- AWS Lambda: O Workload Factory usa o CloudFormation para implantar uma função AWS Lambda para o link que se comunica com o ONTAP.

O diagrama a seguir mostra como o Workload Factory utiliza uma relação de confiança entre uma conta da NetApp na AWS e contas de clientes da AWS com sistemas de arquivos FSx for ONTAP.



1. O Workload Factory faz solicitações ao AWS STS `AssumeRole`, usando um ID externo específico do cliente do serviço AWS IAM.
2. O serviço AWS IAM recupera uma função e cria uma sessão.
3. O Workload Factory emite uma solicitação de API da AWS com permissões de sessão.
4. O Workload Factory recebe uma resposta da API da AWS do plano de controle do FSx for ONTAP.

Link Lambda para o endpoint de gerenciamento do ONTAP

Os links Lambda são executados dentro da VPC do cliente para acesso à sub-rede privada sem expor o ONTAP publicamente. Toda a conectividade do link para o endpoint de gerenciamento do ONTAP é somente de saída, portanto, não são necessárias conectividade de entrada nem endpoints expostos. O link é usado apenas para operações nativas do ONTAP que a API do Amazon FSx for NetApp ONTAP não expõe.

O Workload Factory utiliza os seguintes protocolos para operações de volume, VM de armazenamento e cluster, e para diagnósticos somente leitura e dados de desempenho:

- HTTPS/443 (REST)
- SSH/22 (CLI)

Link do Lambda para o AWS Secrets Manager (recuperação de credencial do ONTAP)

Utilizado somente quando as credenciais de administrador do ONTAP estão armazenadas no AWS Secrets Manager (alternativa: credenciais criptografadas no Workload Factory usando envelope encryption).

- O proxy-forwarder passa `x-aws-secret-arn` (codificados em Base64) nos cabeçalhos.
- A função Lambda faz chamadas `GetSecretValue` em tempo de execução para recuperar a senha.

Isso mantém a senha dentro dos limites da sua conta e impede a transmissão do Workload Factory.

O Workload Factory e componentes do cliente para Amazon Bedrock (diagnóstico de IA)

Este caminho é utilizado apenas quando o diagnóstico por IA está ativado.

- O Analisador de Eventos utiliza esse caminho para análise de EMS e diagnóstico de latência.

- O Bedrock é executado com suas credenciais presumidas e o ARN do perfil de inferência, portanto, os dados não fluem para a conta da NetApp.

Os dados enviados para o Bedrock podem incluir JSON de eventos EMS, estatísticas de QoS, configuração de volume, dados agregados e informações de nós. O caminho fica ativo somente quando um perfil de inferência é configurado por organização (`ai_analyzer_config` tabela).

Grupos de conexão (protocolos, portas e autenticação)

Grupo A — caminho de confiança do plano de gerenciamento da AWS (credenciais presumidas)

Conexão	Protocolo	Porta	Direção	Autenticação	Justificação
STS AssumeRole	HTTPS	443	WF → AWS STS (conta do cliente)	Credenciais IAM + ExternalId	Obtenha credenciais temporárias entre contas
API FSx (Descrever/Criar/Atualizar/Excluir)	HTTPS	443	WF → endpoint AWS FSx (região do cliente)	Credenciais temporárias STS	Gerenciamento de ciclo de vida de sistema de arquivos e volumes
API EC2/VPC	HTTPS	443	WF → endpoint AWS EC2	Credenciais temporárias STS	Descoberta de grupo de segurança, sub-rede e VPC
API do CloudFormation	HTTPS	443	WF → endpoint AWS CFN	Credenciais temporárias STS	Implantação de pilha para funções IAM e provisionamento FSx
O Secrets Manager GetSecretValue	HTTPS	443	WF → endpoint do AWS Secrets Manager (conta do cliente)	Credenciais temporárias STS	Recuperar a senha de administrador do ONTAP (quando armazenada no Secrets Manager)
Criptografia/Descriptografia com KMS	HTTPS	443	WF → endpoint do AWS KMS	Credenciais temporárias STS	Operações de chave de criptografia de volume

Todas as chamadas à API da AWS utilizam o endpoint regional do cliente e podem ser roteadas por meio de endpoints de VPC, se configurados.

Grupo B — plano de dados do ONTAP

O plano de dados do ONTAP é sempre encaminhado por meio do link Lambda; os serviços do Workload Factory nunca se conectam diretamente ao ONTAP.

Conexão	Protocolo	Porta	Direção	Autenticação	Justificação
API REST do ONTAP	HTTPS	443	Link (VPC do cliente) → LIF de gerenciamento do ONTAP	Autenticação básica (nome de usuário/senha) ou ARN do Secrets Manager	Configuração de cluster, volume e VM de armazenamento; QoS; eventos EMS; status ARP

Conexão	Protocolo	Porta	Direção	Autenticação	Justificação
CLI SSH do ONTAP	SSH	22	Link (VPC do cliente) → LIF de gerenciamento do ONTAP	Autenticação por senha	Comandos de diagnóstico (estatísticas de QoS, df, registros de eventos, eficiência)

Estratégia de roteamento (ordem de prioridade) para o proxy-forwarder:

1. Cabeçalho explícito `x-link-id`: busca o ARN da função Lambda no banco de dados
2. ID de destino (ID do sistema de arquivos FSx): encontre o link associado
3. ID do agente do Console: rotear pelo agente de mensagens até o agente do Console

Grupo C — link do AWS Lambda (implantado em sua VPC)

Conexão	Protocolo	Porta	Direção	Autenticação	Justificação
Invocar Lambda	HTTPS (SDK da AWS)	443	WF → API AWS Lambda (conta do cliente)	IAM (`lambda:InvokeFunction`)	Execute comandos REST/SSH do ONTAP a partir da VPC do cliente
Lambda → ONTAP	HTTPS + SSH	443, 22	Lambda (VPC do cliente) → LIF de gerenciamento do ONTAP	Autenticação básica / senha	Acesso à sub-rede privada ao ONTAP sem exposição pública

Grupo D — NetApp Console Agent (EC2 em sua VPC, somente para saída)

Conexão	Protocolo	Porta	Direção	Autenticação	Justificação
Pesquisa de agentes	HTTPS	443	Agente do console (VPC do cliente) → broker de mensagens WF	Token de portador (escopo occm-access)	Long-poll para comandos ONTAP pendentes (tempo limite de 7 segundos; reconecta)
Resposta do agente	HTTPS	443	Agente do console (VPC do cliente) → broker de mensagens WF	Token Bearer	Retorna os resultados dos comandos ONTAP (opcionalmente comprimidos com zlib)
Agente do Console → ONTAP	HTTPS + SSH	443, 22	Agente do Console (VPC do cliente) → LIF de gerenciamento do ONTAP	Autenticação básica / senha	Execute operações ONTAP por proxy

Principal característica do projeto: o Workload Factory nunca inicia conexões de entrada para o agente do Console. O trabalho é enfileirado em fluxos do Redis; o agente do Console consulta `GET /messagebroker/v1/requests` e responde com `POST /messagebroker/v1/responses`.

Grupo E — CloudFormation callbacks de recursos personalizados

Conexão	Protocolo	Porta	Direção	Autenticação	Justificação
CloudFormation → WF Lambda	HTTPS	443	CloudFormation (cliente) → WF Lambda (NetApp)	Token JWT + token de referência	Relate o status de criação da função IAM e retorne o ARN da função
Provedor de recursos do ONTAP CloudFormation → Link	HTTPS	443	CloudFormation recurso Lambda (cliente) → Link Lambda (cliente)	IAM	Criar/atualizar/excluir recursos ONTAP durante operações de stack

Resumo: requisitos de rede para sua VPC

Componente	Entrada	Saída
FSx for ONTAP	Portas 443 e 22 do grupo de segurança do agente Link Lambda ou Console	N/A
Vincular o Lambda	Nenhum	Porta 443 (ONTAP, APIs da AWS) e porta 22 (SSH do ONTAP)
Agente de console EC2	Nenhum	Porta 443 (endpoints do WF, ONTAP, APIs da AWS) e porta 22 (SSH do ONTAP)
Endpoints VPC (opcional)	N/A	STS, FSx, S3, Gerenciador de Segredos, Lambda, CloudFormation

Nenhum componente na VPC do cliente requer acesso à internet de entrada. Todas as conexões são iniciadas de saída (consulta do agente do Console) ou invocadas por meio das APIs de serviço da AWS (Lambda Invoke).

Opções de execução do ONTAP para o NetApp Workload Factory

Alguns fluxos de trabalho do NetApp Workload Factory exigem operações nativas do ONTAP que não são expostas pelas APIs da AWS. O NetApp Workload Factory oferece duas opções de execução que mantêm essas operações dentro dos limites da sua conta AWS: um link Lambda que executa operações do ONTAP de dentro da sua VPC e um NetApp Console Agent que usa conectividade somente de saída a partir de uma instância EC2. Ambas as opções permitem que você execute as operações necessárias do ONTAP, mantendo as decisões de rede, credencial e ciclo de vida dentro do seu modelo de segurança.

Opções de execução

Link Lambda (AWS Lambda na sua VPC)

Executa diagnósticos REST do ONTAP e ONTAP CLI somente leitura de dentro da sua VPC, sem expor o ONTAP publicamente.

NetApp Console Agent (EC2 em sua VPC, somente para saída)

Executa operações ONTAP por proxy, onde o agente inicia conexões de saída e o NetApp Workload Factory nunca inicia conexões de entrada para o agente.

Considerações de segurança

- Limites da rede: confirme as portas de saída necessárias (443/22) e os destinos.
- Limites de credenciais: decida se as credenciais do ONTAP são armazenadas no NetApp Workload Factory (criptografadas por envelope) ou referenciadas no AWS Secrets Manager.
- Auditabilidade: confirme os registros operacionais de atividade e falhas dos componentes.
- Gestão do ciclo de vida: confirme como as atualizações e remoções ocorrem.

Informações relacionadas

- "Visão geral do link Lambda para NetApp Workload Factory"
- "Conectividade e caminhos de confiança para o NetApp Workload Factory"
- "Criptografia e gerenciamento de chaves para NetApp Workload Factory"

Informações sobre direitos autorais

Informações sobre marcas comerciais