Governança de dados, privacidade e ciclo de vida

Information Security for Workload Factory

NetApp
September 16, 2026

Índice

Governança de dados, privacidade e ciclo de vida

Manipulação e residência de dados para o NetApp Workload Factory

O NetApp Workload Factory organiza o gerenciamento de dados em categorias que descrevem os dados operacionais processados pelo serviço, como cada classe de dados se encaixa no modelo de segurança, onde os dados são armazenados, por quanto tempo são retidos e se saem do ambiente do cliente. As principais classes de dados incluem configuração e metadados, logs e eventos operacionais e telemetria. Os dados retidos podem incluir snapshots de configuração do FSx for ONTAP, referências de credencial, dados de uso e custo de IA, registros de auditoria e caches de resposta de curta duração. Os locais de armazenamento e processamento variam de acordo com o tipo de dado: algumas informações permanecem na conta AWS do cliente, enquanto outros dados operacionais são armazenados na conta da NetApp.

Classes de dados gerenciadas pelo o Workload Factory

O Workload Factory lida com as seguintes classes de dados:

- Configuração e metadados
- Registros e eventos operacionais
- Telemetria

Classes de dados retidas pelo o Workload Factory

O Workload Factory armazena os seguintes dados:

- Instantâneos de configuração do FSx (atualizados a cada verificação)
- Referências de credencial do ONTAP ou material de credencial criptografado com criptografia de envelope KMS (dependendo do modo de credencial selecionado)
- Métricas EDA
- CloudFormation templates (cabeçalho de 7 dias `Expires`)
- Dados sobre uso e custo da IA
- Registros de auditoria
- Redis caches (respostas FSx) com um TTL de 20 minutos

Onde as informações são armazenadas

Conta AWS

- As senhas de administrador do ONTAP são armazenadas no seu AWS Secrets Manager.
- O Amazon Bedrock processa inferência de IA (análise EMS) usando o ARN do seu perfil de inferência por

meio de uma função assumida pelo STS na sua conta AWS.

Conta do NetApp

- Configurações do FSx, planos de balanceamento, configurações de ARP e limites de uso de IA
- Credenciais temporárias do AWS STS (armazenadas em cache no Redis), caches de resposta, bloqueios e estado de implantação
- CloudFormation/modelos Terraform, descritores de configuração WAD e relatórios compactados
- Medição de uso de IA e métricas de desempenho do coletor
- Métricas agregadas de EDA
- Trilhas de auditoria de ações
- Rastreamentos do OpenTelemetry

Considerações regionais

- Armazenado em regiões onde o serviço Amazon Bedrock está disponível.
- NetApp internal opera em `us-east-1` e `us-west-2`.

Por quanto tempo as informações são mantidas

Esta seção resume as categorias de retenção. Consulte as páginas vinculadas para obter valores detalhados e o comportamento da política.

- Retenção de credencial e de credencial temporária do AWS STS: "Retenção de credencial para o NetApp Workload Factory"
- Retenção de métricas operacionais e telemetria: "Referência de métricas e telemetria para o NetApp Workload Factory"
- Retenção de registros de auditoria: governada pela política de retenção do NetApp Console (não controlada pelo Workload Factory)

Quais informações saem da VPC

Esta seção resume as categorias de dados de saída. Consulte as páginas vinculadas para obter detalhes em nível de protocolo e em nível de recurso.

Tráfego do plano de gerenciamento para o serviço o Workload Factory

Para operações de gerenciamento, a configuração do FSx, metadados do volume, identificadores de recursos e comandos operacionais são transmitidos via HTTPS para a camada de serviço do Workload Factory.

Registros de auditoria para o Serviço de Auditoria do NetApp Console

Cada operação rastreada envia as seguintes informações:

- `accountId`
- `actionName`
- `status`

- `resourceId`
- `userId`
- `requestData`
- `responseData`
- `timestamps`
- `IP address`
- `workspaceId`

Análise de tráfego por IA

Os eventos do Sistema de Gerenciamento de Emergências (EMS) do FSx for ONTAP, dados de latência e registros de erros enviados para diagnósticos de IA são encaminhados para o Amazon Bedrock por meio da sua conta AWS, usando seu perfil de inferência configurado. Assim, esse tráfego permanece dentro do seu ambiente em vez de alcançar os sistemas da NetApp.

Para obter mais informações sobre análise de tráfego por IA, consulte:

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

Tráfego da API de serviço da AWS

Consulte "Conectividade e caminhos de confiança para o NetApp Workload Factory".

Coleta de telemetria e métricas

Consulte o "métricas e referência de telemetria".

Escopo da coleta de configuração e metadados

Nível do sistema de arquivos

- Configuração do sistema de arquivos (tipo de implantação Gen1/Gen2, capacidade de transferência, capacidade de storage, tipo de armazenamento)
- Sub-rede preferencial, grupos de segurança, configuração de VPC
- Metadados da chave de criptografia KMS
- Etiquetas do sistema de arquivos
- Status do ciclo de vida do sistema de arquivos
- Configurações da janela de manutenção

Nível de volume (abrangente)

- Identidade e estado: nome do volume, UUID, tipo (leitura/gravação/dp/ls), estilo (FlexVol/FlexGroup), estado (online/offline/restrito), hora de criação
- Capacidade: tamanho total, usado, disponível, uso físico, percentual de uso, área ocupada pelo SSD, área

ocupada pelo pool de capacidade, bytes/percentual de dados inativos

- Tiering: política (todos/automático/nenhum/snapshot_only), dias mínimos de resfriamento
- QoS: nome da política de QoS atribuída
- Configuração do NAS: caminho de junção, atribuição de política de exportação, permissões UNIX, estilo de segurança (unix/ntfs/misto)
- Snapshots: tamanho/percentual/utilizado da reserva de Snapshot, configurações de exclusão automática
- Eficiência de dados: tipo/estado de compressão, deduplicação, compactação, economia de espaço
- Autosize: modo (aumentar/aumentar_diminuir/desativado), tamanho mínimo/máximo, limites de aumento/diminuição
- SnapLock: tipo (compliance/enterprise/non_snaplock), períodos de retenção (mínimo/máximo/padrão), período de confirmação automática
- Clone: volume pai/snapshot/storage VM, é FlexClone, status de divisão
- Inodes/arquivos: máximo possível, máximo configurado, contagem usada
- Criptografia: status ativado/desativado
- Tempo de acesso: atualização de atime ativada/desativada e período de atualização
- SnapMirror: status de proteção, tipos de destino (nuvem/ONTAP)
- FlexGroup reequilíbrio: percentual de desequilíbrio, limite máximo
- Movimentação de volume: agregado de destino, estado da movimentação
- FlexCache tipo de endpoint: nenhum/cache/origem
- Tags: Etiquetas de volume em nível ONTAP

Dados de Snapshot

- Nome do Snapshot, UUID, hora de criação, hora de expiração
- Tamanho em bytes
- SnapMirror rótulo
- SnapLock expiração e status de bloqueio
- Estado (válido/inválido/parcial)
- Comentários dos usuários
- Políticas de Snapshot: nome, status de ativação, agendamento de cópias (contagem, período de retenção, nome do agendamento, prefixo, SnapMirror label)

Políticas de exportação

- Nome da política, ID, VM de armazenamento associada
- Regras: lista de protocolos (NFS/CIFS/FlexCache), padrões de correspondência de cliente, regras de somente leitura, regras de leitura/gravação, regras de superusuário, índice/prioridade de regras
- SUID, criação de dispositivos, modo chown, mapeamento de usuário anônimo, configurações de segurança NTFS UNIX

Pontos de acesso S3

- Estado do ciclo de vida (disponível/criando/excluindo/falhou/misconfigured)

- Data de criação, ARN, alias, nome
- Usuário e tipo do proprietário dos arquivos (UNIX/WINDOWS)
- Configuração de rede (acesso à Internet vs acesso à VPC, ID da VPC)
- Tags da AWS
- Capacitação de varredura de metadados, capacitação de journaling, CloudTrail ARN

Proteção contra ransomware (ARP)

O Workload Factory coleta tanto o status da configuração quanto os detalhes do evento:

- Estado por volume (ativado/desativado/dry_run/pausado)
- Probabilidade de ataque (nenhuma/baixa/moderada/alta)
- Relatórios de ataques com registros de data e hora
- Parâmetros de detecção: limites de extensão de arquivo, aumento percentual na taxa de renomeação, aumento percentual na taxa de entropia, aumento percentual na taxa de criação/exclusão de arquivos
- Arquivos suspeitos: caminho do arquivo, nome do arquivo, formato do arquivo, horário suspeito, volume associado

Replicação / SnapMirror

- UUID do relacionamento, estado, status de integridade
- Origem e destino (máquina virtual de armazenamento, caminho, cluster)
- Estatísticas de transferência (bytes transferidos, duração, hora de término, estado)
- Política (nome, tipo: assíncrona/síncrona/contínua)
- Configuração do throttle
- Tempo de atraso
- Motivos de não integridade (mensagem e código)
- Erros de transferência atuais

iGroups

- Nome, UUID, protocolo (FCP/iSCSI/misto), tipo de SO
- Iniciadores (IQN/WWPN), estado da conectividade, última vez visto
- Mapeamentos de LUN (número da unidade lógica, detalhes da LUN)

LUNs

- Nome, UUID, número de série, tipo de SO, status ativado
- Tamanho, espaço utilizado, configurações de thin provisioning
- Localização (volume, nó, caminho da unidade lógica)
- Configuração de exclusão automática
- Estado do contêiner, status mapeado, status somente leitura
- Política de QoS

- Métricas de desempenho (IOPS, latência, taxa de transferência por leitura/gravação/total)
- Associação ao grupo de consistência

FlexCache

- Volume de origem/máquina virtual de storage/cluster, tamanho do cache, caminho
- Writeback ativado, status do cache DR
- Configuração de dimensionamento relativo
- Preencher previamente os caminhos dos diretórios
- Estado da conexão entre o cache e a origem

Nível de VM de storage

- Nome, UUID, estado (em execução/parado), subtipo
- Protocolos habilitados/permitidos (NFS, CIFS, iSCSI, FCP, NVMe, S3)
- Servidores DNS e domínios
- Configuração do switch de serviço de nomes (passwd, group, hosts, etc.)
- Interfaces IP (nome, endereço IP, serviços)
- Agregados atribuídos
- Estado padrão de volume anti-ransomware
- Configurações de enforcement de espaço
- Relações entre pares (aplicações, estado, cluster remoto/storage VM)

Nível de agregado/de armazenamento

- Nome do agregado, UUID, estado, estado do RAID
- Armazenamento em blocos: número de discos, tamanho do RAID, espaço disponível/usado/total, espaço físico utilizado
- Armazenamento em nuvem utilizado
- Eficiência: proporção, uso lógico, economia
- Criptografia, espelhamento, SnapLock settings
- Métricas de desempenho (IOPS, latência, taxa de transferência)

Métricas de utilização (EDA)

- Frequência de coleta: a cada 12 horas para capacidade/throughput; a cada 20 minutos para latência
- Granularidade: normalizada para aproximadamente 60 pontos de dados por intervalo de tempo
- Detalhes sobre retenção e armazenamento: "Referência de métricas e telemetria"

Criptografia e gerenciamento de chaves para NetApp Workload Factory

O NetApp Workload Factory utiliza criptografia em repouso e define responsabilidades

claras de gerenciamento de chaves entre o Workload Factory e os serviços da AWS. Para os sistemas de arquivos Amazon FSx for NetApp ONTAP, você pode escolher sua própria chave do AWS KMS ou usar a chave padrão gerenciada pela AWS, e o FSx for ONTAP executa as operações criptográficas com essa chave. O Workload Factory também utiliza criptografia envelope para proteger as credenciais ONTAP armazenadas.

Escopo de criptografia em repouso do KMS para o FSx

Ao criar um sistema de arquivos FSx for ONTAP por meio do NetApp Workload Factory, você pode, opcionalmente, especificar sua própria chave AWS KMS para criptografia de dados em repouso. Se você não especificar uma chave, o NetApp Workload Factory usará a chave FSx padrão gerenciada pela AWS.

O que é criptografado

Todos os dados armazenados nos volumes EBS subjacentes que suportam o sistema de arquivos Amazon FSx for NetApp ONTAP (criptografia EBS da AWS em repouso).

Propriedade da chave

A chave KMS reside na sua conta da AWS.

Permissões necessárias para a seleção e uso da chave

O Workload Factory requer:

- `kms:DescribeKey`
- `kms:ListKeys`
- `kms:ListAliases`
- `kms:CreateGrant` (para permitir que o serviço Amazon FSx for NetApp ONTAP utilize a chave)

Padrão de acesso à chave

O NetApp Workload Factory nunca criptografa ou descriptografa dados diretamente com sua chave KMS. Ele passa o ID da chave para a API do Amazon FSx for NetApp ONTAP durante a criação do sistema de arquivos; o Amazon FSx for NetApp ONTAP realiza as operações criptográficas.

Proteção de credenciais (criptografia envelope do lado do serviço)

Ao armazenar as credenciais do ONTAP (senhas de administrador) por meio do NetApp Workload Factory, elas são protegidas usando criptografia envelope antes de serem persistidas.

Método de criptografia

AES-256-CBC com uma chave de criptografia de dados (DEK) exclusiva por registro de credencial.

Fluxo de criptografia de envelope

1. Uma DEK exclusiva de 256 bits é gerada para cada credencial.
2. A DEK criptografa a credencial (senha).
3. A própria DEK é criptografada com uma chave raiz e armazenada juntamente com a credencial criptografada.
4. O DEK em texto simples nunca é armazenado.

Contexto de criptografia

Cada chave de dados é criptograficamente vinculada ao seu registro de credencial específico, impedindo a reutilização da chave em diferentes registros.

Alternativa: AWS Secrets Manager

Em vez de armazenar senhas criptografadas no serviço, você pode armazenar as credenciais do ONTAP no AWS Secrets Manager em sua própria conta. O NetApp Workload Factory nunca vê ou armazena a senha; ele passa o ARN do Secrets Manager para o link do Lambda, que recupera a senha em tempo de execução dentro da sua VPC.

O AWS Secrets Manager é necessário para contas GovCloud.

NetApp Workload Factory exclusão de conta

A exclusão de conta não é uma operação de autoatendimento; trata-se de um fluxo de trabalho de desativação que envolve tanto o serviço o Workload Factory quanto os recursos da sua conta AWS. A limpeza inclui a remoção segura de todos os dados associados à conta do o Workload Factory, sistemas de arquivos FSx for ONTAP, credenciais, links, canais de notificação e recursos relacionados do IAM, AWS Lambda e Amazon CloudWatch. A operação é irreversível.

Quando você precisar remover a sua conta do NetApp Workload Factory, você deve"Entre em contato com o suporte da NetApp."

Informações sobre direitos autorais

Informações sobre marcas comerciais