Identidade, credenciais e privilégio mínimo

Information Security for Workload Factory

NetApp
September 16, 2026

Índice

Identidade, credenciais e privilégio mínimo

Integração da conta AWS para o NetApp Workload Factory

O Workload Factory usa a AWS `sts:AssumeRole` para obter credenciais temporárias para sua conta da AWS, portanto, as chaves de acesso permanentes da AWS não são armazenadas pelo serviço. Durante a integração, você configura uma função do IAM que o Workload Factory pode assumir para operações aprovadas da API da AWS, usando um ID externo para ajudar a evitar acesso não autorizado entre contas. O Workload Factory usa então as credenciais de curta duração resultantes em tempo de execução, que a AWS expira automaticamente após cada sessão.

Configuração da conta AWS

Para permitir que o Workload Factory acesse sua conta da AWS:

1. Implante uma função do IAM em sua conta da AWS (usando o CloudFormation ou manualmente).
2. Garanta que a política de confiança da função permita que o service principal do NetApp Workload Factory a assuma, controlado por um ID externo.
3. Utilize um ID externo como um identificador secreto único (UUID v4) compartilhado exclusivamente entre o cliente e o NetApp Workload Factory.

   Incorpore-o como uma condição na sua política de confiança de função do IAM (`sts:ExternalId`).

   O ID externo impede ataques de deputy confuso. Em um modelo de acesso entre contas, um invasor que descobre o ARN da função de um cliente não pode assumir essa função sem também possuir o ID externo correspondente. A AWS recomenda esse padrão para acesso entre contas de terceiro. Para obter mais informações, consulte a página de documentação do AWS IAM "Acesso a contas da AWS pertencentes a terceiros".

   O ID externo é gerado uma única vez durante o processo de integração de credenciais e armazenado criptografado juntamente com o ARN da função em um banco de dados do NetApp Workload Factory.
4. Registre o ARN da função e o ID externo no NetApp Workload Factory.

Tempo de execução

Em tempo de execução, o Workload Factory assume sua função do IAM para obter credenciais de curta duração para cada operação da API da AWS:

1. O Workload Factory faz chamadas `sts:AssumeRole` com o ARN da sua função e o ID externo.
2. A AWS retorna credenciais temporárias (chave de acesso, chave secreta e token de sessão).
3. O NetApp Workload Factory utiliza as credenciais temporárias para operações da API da AWS em sua conta.
4. As credenciais expiram automaticamente (por padrão, uma hora).

Como as credenciais da AWS fluem pelo NetApp Workload Factory

O fluxo de credencial da AWS descreve como o NetApp Workload Factory lida com identificadores de função, IDs externos e credenciais temporárias do AWS STS durante as operações de integração e de tempo de execução. Durante a configuração única, você cria uma função do IAM em sua conta da AWS e configura uma política de confiança que exige o principal do serviço do Workload Factory e o ID externo correto. No tempo de execução, o Workload Factory usa o ARN da função armazenada e o ID externo para solicitar credenciais temporárias delimitadas por uma política de sessão por solicitação, e reutiliza credenciais armazenadas em cache até que expirem.

Configuração única

Para uma configuração única, o fluxo é o seguinte:

Passos

1. Você inicia uma CloudFormation stack ou cria manualmente uma função do IAM em sua conta da AWS.
2. A política de confiança da função do IAM especifica duas condições:
   a. Somente a entidade de serviço do NetApp Workload Factory pode assumi-lo.
   b. O chamador deve apresentar o ID externo correto.
3. O NetApp Workload Factory armazena o ARN da função e o ID externo (criptografado) em seu banco de dados.

Tempo de execução (cada operação da API)

Em tempo de execução, o Workload Factory usa o ARN da função armazenada e o ID externo para obter credenciais temporárias do AWS STS para cada operação de API. O fluxo é o seguinte:

Passos

1. O Workload Factory recupera o ARN da função armazenada e o ID externo do MySQL.
2. Ele verifica o Redis em busca de um conjunto em cache de credenciais temporárias do AWS STS para essa função.
3. Em caso de falha de cache, o Workload Factory faz chamadas `sts:AssumeRole` com o ARN da função e o ID externo. A chamada inclui uma política de sessão embutida por solicitação que restringe as permissões apenas às ações específicas da AWS necessárias para essa operação.
4. O AWS STS retorna credenciais temporárias (ID da chave de acesso, chave de acesso secreta, token de sessão) com um carimbo de data/hora de expiração.
5. O Workload Factory armazena essas credenciais em cache no Redis e as utiliza para chamar as APIs da AWS de destino.
6. No acerto do cache, o NetApp Workload Factory ignora a chamada ao STS e usa as credenciais armazenadas em cache diretamente.

Política de sessão

Cada chamada STS inclui uma política de sessão embutida com escopo limitado às ações mínimas da AWS

necessárias.

Informações relacionadas

- "Níveis de permissão de privilégio mínimo"

Retenção de credencial da NetApp Workload Factory

O Workload Factory protege o gerenciamento de credenciais por meio de credenciais AWS STS de curta duração, metadados de função criptografados e comportamento de retenção limitado. O modelo de credenciais separa os metadados de função retidos das credenciais temporárias da AWS usadas para operações de API. As credenciais temporárias são armazenadas em cache apenas por um período limitado e expiram automaticamente sob a aplicação da AWS. A remoção de uma credencial impede que o Workload Factory obtenha novas credenciais para a conta, enquanto quaisquer credenciais em cache expiram logo em seguida.

Comportamentos-chave

- O Workload Factory não armazena chaves de acesso da AWS de longo prazo.

  O Workload Factory armazena apenas um ponteiro (ARN da função) e um segredo compartilhado (ID externo). Nenhum deles concede acesso à AWS por si só.

- As credenciais temporárias do AWS STS têm um tempo de vida máximo fixo de uma hora (imposto pela AWS).

  O Workload Factory os armazena em cache no Redis por no máximo 30 minutos antes de forçar uma nova chamada STS.

- Se um conjunto de credenciais em cache tiver menos de 15 minutos restantes, o Workload Factory descarta esse conjunto e obtém um novo.
- A exclusão da credencial pelo cliente revoga imediatamente a capacidade do Workload Factory de acessar essa conta.

  A próxima chamada AssumeRole falha e as credenciais em cache expiram em poucos minutos.

Resumo de retenção e storage

Dados	Local de armazenamento	Duração da retenção	Expira automaticamente?	Método de exclusão
ARN da função IAM + ID externo	MySQL (criptografado em repouso)	Indefinido (armazenado até que o cliente remova explicitamente)	Não	O cliente clica em "Excluir credencial" na interface do usuário

Dados	Local de armazenamento	Duração da retenção	Expira automaticamente?	Método de exclusão
Credenciais temporárias do AWS STS (chave de acesso + segredo + token de sessão)	Redis (cache em memória)	Máximo de 30 minutos (TTL do cache). As credenciais STS subjacentes são válidas por até uma hora (padrão da AWS). O cache remove os itens cinco minutos antes do vencimento como margem de segurança.	Sim (o Redis realiza remoções automáticas de TTL; o vencimento das credenciais da AWS é imposto pela AWS)	Automático
Senha de administrador do ONTAP	MySQL (criptografia envelope AES-256-CBC usando KMS)	Por tempo indeterminado (armazenado até que o cliente remova a credencial ou exclua o sistema de arquivos)	Não	O cliente exclui a credencial ou a exclusão do sistema de arquivos aciona a limpeza
Senha do ONTAP descriptografada (texto simples)	Somente em memória (nunca gravado em disco ou cache)	Duração de uma única solicitação (milissegundos)	Sim (coletado como lixo após a conclusão da solicitação)	Automático

Controles de segurança

- A identificação externa impede ataques de proxy confuso.
- As políticas de sessão impõem o princípio do menor privilégio por solicitação.
- O Workload Factory renova as credenciais temporárias de curta duração do AWS STS antes de janelas de expiração arriscadas.
- O tratamento de questões regionais e tipos de conta difere para os ambientes Standard, GovCloud e China.
- O Workload Factory nunca armazena chaves de acesso da AWS a longo prazo.
- O Workload Factory nunca modifica as permissões da sua função IAM.
- O Workload Factory nunca ultrapassa as permissões concedidas pela sua política de função.
- As políticas de sessão só podem reduzir permissões; o Workload Factory nunca as amplia.

Tipos de credenciais para o NetApp Workload Factory

NetAppWorkload Factory utiliza um modelo de credenciais divididas para separar as permissões do plano de controle da AWS do acesso administrativo direto ao ONTAP. A função IAM da AWS autentica o Workload Factory nas APIs da AWS para operações como gerenciamento de sistema de arquivos, gerenciamento de backup e descoberta de recursos. As credenciais do ONTAP autenticam o acesso direto ao endpoint de gerenciamento do ONTAP com um link Lambda para operações que exigem configuração administrativa ou diagnósticos. Alguns fluxos de trabalho exigem ambos os tipos de credenciais quando combinam operações de API da AWS com tarefas de gerenciamento direto do ONTAP.

Tipos de credencial

A tabela a seguir resume os dois tipos de credencial usados no Workload Factory e seus respectivos destinos de autenticação.

Tipo de credencial	Autentica em	Usado para
Credenciais da AWS (AssumeRole)	APIs da AWS	Todas as operações que passam pela API do serviço AWS FSx
Credenciais do ONTAP (senha de administrador)	Ponto de extremidade de gerenciamento do ONTAP	Operações que exigem acesso direto à API REST ou à CLI do ONTAP

Operações somente com credencial da AWS

Essas operações interagem exclusivamente com as APIs da AWS e exigem apenas a função do IAM:

- Criação e exclusão de sistema de arquivos
- Alterações na capacidade e na taxa de transferência do sistema de arquivos
- Criação e gerenciamento de backups
- Descoberta de VPC, sub-rede e grupo de segurança
- Enumeração de chaves KMS
- CloudWatch recuperação de métricas
- Consultas do Cost Explorer
- Gerenciamento de tags usando a API FSx

Operações apenas com credenciais do ONTAP

Essas operações se comunicam diretamente com o endpoint de gerenciamento do ONTAP por meio do link Lambda e exigem credenciais de administrador do ONTAP:

- Configuração da política de QoS em nível de volume
- Política de exportação e gerenciamento de regras
- Configuração do protocolo de storage VM (NFS, CIFS, iSCSI)
- Gerenciamento de igroup e LUN

- SnapMirror (configuração de replicação)
- Gerenciamento de política do Snapshot (nível ONTAP)
- Diagnóstico de desempenho (estatísticas de QoS, detalhamento da latência)
- Recuperação e análise de eventos EMS
- Monitoramento do status da proteção anti-ransomware
- FlexCache gerenciamento
- Consultas de interface de rede (LIF)

Operações que exigem credenciais da AWS e do ONTAP

Fluxo de trabalho	Credencial da AWS usada para	Credencial do ONTAP usada para
Análise de eventos com inteligência artificial	Invoque o Bedrock, descreva o sistema de arquivos	Recupere eventos do EMS e execute diagnósticos usando SSH
Criação de sistema de arquivos com configuração de storage VM	Criar sistema de arquivos (API da AWS)	Configurar protocolos de VM de armazenamento (ONTAP REST)
Criação de volume com política de exportação	Criar volume (AWS API)	Definir regras de política de exportação (ONTAP REST)
Gerenciamento de capacidade	Atualizar a capacidade do sistema de arquivos (API da AWS)	Verifique a utilização do agregado (ONTAP SSH)

Informações relacionadas

- "Opções de execução do ONTAP"
- "Visão geral do link Lambda"

Opções de armazenamento de credenciais para o NetApp Workload Factory

O NetApp Workload Factory oferece padrões de gerenciamento de credenciais que preservam o menor privilégio e reduzem a exposição de segredos administrativos do ONTAP. Recursos de diagnóstico com inteligência artificial usam credenciais do ONTAP somente leitura quando disponíveis, para que o agente de diagnóstico possa observar e diagnosticar sem modificar o ambiente de storage. Você pode usar o armazenamento criptografado gerenciado pelo Workload Factory ou armazenar a senha do ONTAP no AWS Secrets Manager e fornecer uma referência ao Workload Factory. Essa escolha afeta onde a senha é armazenada, como ela é criptografada e como você gerencia requisitos como suporte ao GovCloud e rotação de credenciais.

Modelo de acesso somente leitura do ONTAP

Para funcionalidades baseadas em IA, como análise de eventos e diagnóstico de latência, o Workload Factory utiliza credenciais ONTAP somente leitura quando disponíveis. O modelo de credencial somente leitura garante que o agente de diagnóstico de IA não possa fazer modificações no seu ambiente de storage; ele só pode observar e diagnosticar.

Comparação de opções de armazenamento de credencial

Credenciais AWS

As credenciais da AWS são sempre assumidas por meio de uma função do IAM. O Workload Factory pode gerenciar as informações da função internamente ou referenciá-las no AWS Secrets Manager.

Opção	Credenciais AWS	O que está armazenado	Criptografia
Workload Factory gerenciado	ARN da função IAM + ID externo	ARN da função IAM + ID externo	O ARN da função não é um segredo (armazenado tal como está)

Credenciais ONTAP

O Workload Factory pode gerenciar as credenciais do ONTAP internamente com armazenamento criptografado ou referenciá-las a partir do AWS Secrets Manager. Essa escolha afeta como a senha é armazenada, criptografada e rotacionada.

As credenciais do ONTAP são necessárias para o Workload Factory interagir com as APIs do sistema de arquivos ONTAP por meio de um "Link Lambda".

Opção	Credenciais ONTAP	O que está armazenado	Criptografia
Workload Factory gerenciado	Senha (criptografada)	Senha de administrador do ONTAP (criptografada)	A senha do ONTAP usa criptografia envelope AES-256
O AWS Secrets Manager	Referência ARN do Secrets Manager	ARN do Secrets Manager	O ARN de segredos não é um segredo (armazenado tal como está); o AWS Secrets Manager criptografa o segredo na sua conta

Considerações adicionais

GovCloud exigência

É utilizada a função padrão do IAM; as credenciais do ONTAP devem usar o Secrets Manager (o armazenamento de senhas não é permitido).

Rotação

As políticas de função são atualizadas na sua conta. Atualize a senha do ONTAP no o NetApp Workload Factory (opção gerenciada) ou faça a rotação no AWS Secrets Manager.

Níveis de permissão de privilégio mínimo para o NetApp Workload Factory

Você pode restringir as permissões do IAM do o Workload Factory a qualquer momento para alinhá-las aos requisitos de privilégio mínimo, como limitar o acesso a recursos específicos (ARNs) e aplicar condições do IAM, por exemplo, tags e intervalos CIDR.

Modelo de permissão em níveis

O Workload Factory usa um modelo de permissões em camadas, alinhado ao princípio do menor privilégio. Você escolhe quais níveis de permissão habilitar ao adicionar credenciais da AWS. Você pode começar com a descoberta somente leitura e expandir conforme necessário.

O Workload Factory concede todas as permissões por meio de uma função do IAM na sua conta da AWS, que ele assume via STS com um ID externo.

O Workload Factory define ainda mais o escopo de cada chamada de API com uma política de sessão embutida.

No console do Workload Factory, o recurso de bate-papo com IA *Ask Me* ajuda você a refinar permissões com segurança, sugerindo opções de restrição e gerando uma política atualizada para aplicar na AWS.

Concessão de permissões

Ao adicionar credenciais da AWS ao o Workload Factory, você pode escolher quais níveis de permissão habilitar. Você pode habilitar ou desabilitar níveis a qualquer momento.

Os níveis são cumulativos: ativar um nível superior ativa automaticamente todos os níveis inferiores.

Controles de segurança

- ID externo (proteção de confused deputy)
- Políticas de sessão por operação (privilégio mínimo por solicitação)
- Condições baseadas em tags (modificações de grupos de segurança restritas a recursos criados pelo o Workload Factory)
- Escopo de ARN secreto (acesso ao Secrets Manager restrito a `FSxSecret*`)
- Validação de permissões em tempo de execução (ação/recurso ausente relatado para remediação direcionada)

Documentação de permissões

A principal referência para permissões do Workload Factory é a "referência de permissões" na documentação de configuração e administração do Workload Factory. Você pode encontrar informações sobre os impactos da remoção de permissões das políticas do Storage IAM nessa referência.

Permissões de monitoramento da Amazon CloudWatch para o NetApp Workload Factory

As permissões de monitoramento do Amazon CloudWatch são opcionais no NetApp Workload Factory e se aplicam somente quando você implanta o conjunto de monitoramento separado. O conjunto de monitoramento oferece visibilidade operacional ao coletar métricas do sistema de arquivos, publicar logs de eventos, gerenciar painéis e alarmes do CloudWatch e enviar notificações de alerta por meio do Amazon SNS. O conjunto também requer acesso para recuperar as credenciais do ONTAP quando necessário para o monitoramento.

Permissões de monitoramento necessárias do CloudWatch

As seguintes permissões são necessárias para o conjunto de monitoramento opcional:

Permissão	Propósito
fsx:Describe* / fsx:ListTagsForResource	Coletar métricas do sistema de arquivos
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	Gerencie painéis e alarmes
logs: CreateLogGroup / logs: CreateLogStream / logs: PutLogEvents	Publicar registros de eventos
sns:Publish	Enviar notificações de alerta
secretsmanager:GetSecretValue	Recuperar credenciais do ONTAP para monitoramento

Informações sobre direitos autorais

Informações sobre marcas comerciais