



Configurar as integrações e os serviços do NetApp Console

NetApp Console local deployment

NetApp
August 10, 2026

Índice

Configurar as integrações e os serviços do NetApp Console	1
Integre a implantação local do NetApp Console com o Active Directory	1
Antes de começar	1
Desativar ou ativar a integração com o Active Directory	2
Excluir uma integração com o Active Directory	2
Conecte seu LLM e habilite o assistente do NetApp Console na implantação local do NetApp Console . . .	3
Reúna tudo o que você precisa antes de conectar um LLM	3
Conectar um LLM ao NetApp Console em uma implantação local	3
Verifique se a integração do LLM funciona	4
Proteja as credenciais e monitore o uso do LLM	4
Solucione problemas de integração do LLM na implantação local do NetApp Console	5
Solucione rapidamente problemas de integração do LLM	5
Solução de problemas por sintoma	5
Responder à exposição ou uso indevido de credenciais de LLM	6
Configure os canais de entrega de notificações na implantação local do NetApp Console	6
Configurar um servidor de e-mail	6
Configurar um webhook	8

Configurar as integrações e os serviços do NetApp Console

Integre a implantação local do NetApp Console com o Active Directory

Integre a implantação local do NetApp Console com o Active Directory para login e pesquisa de usuários baseados em diretório. Use seu serviço de diretório para autenticar usuários e, em seguida, atribua acesso a esses usuários na implantação local do NetApp Console.

Funções de acesso necessárias

Superadministrador ou administrador da organização. ["Saiba mais sobre funções de acesso"](#).

Ao integrar com o Active Directory, a implantação local do Console autentica os usuários por meio do seu diretório existente. Depois de adicionar um usuário ao diretório, atribua funções de acesso ao Console para controlar o que esse usuário pode acessar.

A integração com o Active Directory também ajuda você a atender aos requisitos de conformidade, aplicando seus controles, trilhas de auditoria e políticas existentes ao acesso de implantação local do Console.



- A integração com o Active Directory não cria grupos federados, não sincroniza atribuições de diretório-grupo e não concede acesso automaticamente. Os administradores ainda adicionam usuários do diretório à organização e atribuem funções na implantação local do Console.
- Apenas uma integração com o Active Directory é suportada por vez. Depois que uma integração é configurada, o botão **Adicionar integração** fica desabilitado. Para alternar para um diretório diferente, desabilite ou exclua a integração existente primeiro.
- Os usuários do diretório não configuram nem utilizam autenticação multifator (MFA). A implantação local do console oferece suporte à MFA somente para usuários locais. ["Aprenda a gerenciar as configurações de segurança dos membros"](#).

Antes de começar

Antes de integrar com o Active Directory, confirme se você possui:

- Um domínio do Active Directory e credenciais que podem consultar o diretório
- O endereço do servidor LDAP e o nome diferenciado (DN) base para a árvore de diretórios
- Acesso à rede a partir da implantação local do Console para o seu servidor LDAP na porta 389 (LDAP) ou 636 (LDAPS)
- Certificados SSL/TLS, caso você planeje usar LDAPS

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Serviços de diretório** para abrir a página Federações.
3. Selecione **Adicionar integração**.

4. Insira os detalhes de conexão do seu servidor Active Directory:
 - Um nome descritivo para a integração.
 - O **host LDAP**: nome do host ou endereço IP do seu servidor LDAP. Para vários servidores, insira o primário.
 - A porta: 389 para LDAP ou 636 para LDAPS.
 - O **tempo limite de conexão** em milissegundos. O padrão é 1000 ms.
5. Selecione **Usar SSL/TLS** para usar LDAPS. Confirme se o seu servidor LDAP é compatível com LDAPS e se o NetApp Console pode acessar os certificados necessários.
6. Teste a conexão. Se falhar, verifique o host LDAP, a porta, a conectividade de rede e os certificados SSL/TLS.
7. Após o teste ser bem-sucedido, insira o diretório e os detalhes do usuário:
 - **Associação DN base**: Insira o nome diferenciado de associação para a conta LDAP/AD que este aplicativo usará para se conectar ao diretório e insira a credencial (senha) para essa conta. O NetApp Console usa esses detalhes para se associar ao servidor LDAP e validar a conexão.
 - **DN do usuário**: uma conta de usuário com permissão para consultar o diretório. Por exemplo, `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.
8. Selecione **Adicionar** para salvar a integração.

Depois que você terminar

Após salvar a integração, adicione usuários do diretório à sua organização e atribua funções. Você deve configurar e habilitar pelo menos uma integração com o Active Directory antes de poder adicionar usuários do diretório. ["Aprenda como adicionar usuários ao diretório e atribuir funções"](#).

Desativar ou ativar a integração com o Active Directory

Desative uma integração para suspender temporariamente a autenticação baseada em diretório sem excluir a configuração. Ao desativar um serviço de diretório, os usuários do diretório não poderão fazer login por meio do diretório.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Serviços de diretório** para abrir a página Federações.
3. Na lista de integrações, localize a integração e selecione o menu de ações para essa linha.
4. Selecione **Desativar** para suspender a integração ou **Ativar** para restaurá-la.

Excluir uma integração com o Active Directory

Exclua uma integração para remover permanentemente a configuração do serviço de diretório. Antes de excluir, revise quaisquer avisos sobre usuários do diretório vinculados à integração, pois o acesso deles será afetado.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Serviços de diretório** para abrir a página Federações.
3. Na lista de integrações, localize a integração e selecione o menu de ações para essa linha.
4. Selecione **Excluir** e confirme a exclusão.

Conecte seu LLM e habilite o assistente do NetApp Console na implantação local do NetApp Console

Conecte seu modelo de linguagem amplo (LLM) à implantação local do NetApp Console para habilitar o assistente do Console e o gerenciamento de storage assistido por IA.



Esta documentação sobre como conectar um LLM ao assistente do Console para habilitar recursos de IA é fornecida como uma prévia da tecnologia. Com esta oferta de prévia, NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da Disponibilidade Geral.

Funções de acesso necessárias

Superadministrador ou administrador da organização. ["Saiba mais sobre funções de acesso"](#).

Após a configuração, os usuários abrem o assistente do Console no painel de controle e escolhem um modo de acesso:

- No modo **somente leitura**, o assistente responde a perguntas e fornece orientações sem fazer alterações.
- No modo **Leitura/Gravação**, o assistente pode operar na infraestrutura de storage. Ele exibe detalhes para revisão e confirmação antes de cada alteração. Para operações assíncronas, como a criação de volumes, ele cria uma tarefa que os usuários podem verificar no assistente.

Para conectar seu LLM, selecione um caminho de provedor, insira os detalhes do endpoint e a chave da API e, em seguida, selecione um modelo em **Administração > Ferramentas de IA**. As ações do assistente permanecem dentro das suas políticas de storage e dos controles de acesso baseado em funções.

Reúna tudo o que você precisa antes de conectar um LLM

Antes de conectar seu LLM, reúna o seguinte:

- Sua decisão quanto ao tipo de provedor: OpenAI ou compatível com OpenAI. ["Conheça as opções de provedores."](#)
- Uma chave de API válida para o caminho do provedor que você selecionar.
- A URL do endpoint para o caminho do seu provedor.
- A URL do seu proxy ou gateway, caso sua organização exija uma.
- Seu nome de usuário ou ID de single sign-on (SSO) para a conta do provedor de LLM, se necessário.
- Acesso à rede a partir da implantação local do NetApp Console para o endpoint selecionado.
- Classes de armazenamento e controles de acesso baseados em funções para as ações do assistente que você planeja permitir.

Para obter detalhes sobre os modelos compatíveis, consulte ["Saiba mais sobre os provedores e modelos de LLM compatíveis na implantação local do NetApp Console"](#).

Conectar um LLM ao NetApp Console em uma implantação local

Insira as configurações do provedor, a chave da API e o modelo para conectar seu LLM à implantação local do Console.

Passos

1. Faça login na implantação local do NetApp Console.
2. Selecione **Administração > Ferramentas de IA**.
3. Selecione o menu e, em seguida, selecione **Editar**.
4. Em **Tipo de provedor**, selecione um tipo de provedor.

["Saiba mais sobre a integração do LLM na implantação local do NetApp Console"](#).

5. Caso seja solicitado o endpoint do provedor, insira a URL do endpoint para o caminho do provedor que você selecionou.
6. Insira a URL e as credenciais do proxy ou gateway.
7. No campo **Nome de usuário**, insira seu nome de usuário ou ID de SSO se o caminho do seu provedor exigir isso.
8. No campo **Chave de API**, cole a chave de API do seu caminho de provedor selecionado.
9. Selecione um modelo da lista.
10. Revise a configuração e selecione **Salvar**.

Se a operação de salvar ou testar falhar, verifique o tipo de provedor, o URL do endpoint, a chave da API e o modelo selecionado e tente novamente.

["Solucione problemas na integração do seu LLM"](#).

Verifique se a integração do LLM funciona

Após salvar a configuração, verifique a disponibilidade e o comportamento do assistente.

Passos

1. Confirme se o botão **Assistente do Console** aparece no painel de implantação local do NetApp Console.
2. Abra o assistente no modo **Somente leitura** e execute uma consulta básica.
3. Abra o assistente no modo **Leitura/gravação** e confirme que as ações que alteram o storage exigem confirmação do usuário antes da execução.
4. Verifique se os usuários que precisam executar fluxos de trabalho têm os controles de acesso baseado em funções necessários.

Após concluir a validação, os usuários podem abrir o assistente do Console no painel e descrever tarefas em linguagem simples. Para exemplos de uso e fluxos de trabalho do usuário final, consulte ["Use o assistente do NetApp Console"](#).

Proteja as credenciais e monitore o uso do LLM

- Use uma chave de API dedicada para a integração de implantação local do Console sempre que possível.
- Gire as chaves de API de acordo com a política da sua organização.
- Restrinja quem pode editar as configurações do AI Tools apenas às funções de administrador necessárias.
- Monitore o uso da API do lado do provedor e alertas para rastrear atividades anormais ou picos de custo.

Solucione problemas de integração do LLM na implantação local do NetApp Console

Utilize este fluxo de triagem rápida para diagnosticar e resolver problemas comuns de integração do LLM na implantação local do NetApp Console.



Esta documentação sobre como conectar um LLM ao assistente do Console para habilitar recursos de IA é fornecida como uma prévia da tecnologia. Com esta oferta de prévia, NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da Disponibilidade Geral.

Se você ainda não concluiu a configuração, consulte ["Conecte seu LLM e ative o assistente do NetApp Console"](#).

Solucione rapidamente problemas de integração do LLM

1. Valide a configuração das Ferramentas de IA em **Administração > Ferramentas de IA**.

Confirme o tipo de provedor, URL do endpoint, chave da API, modelo selecionado e acesso à rede de saída.
2. Valide a disponibilidade do assistente no painel de controle.

Confirme se o botão **Assistente do Console** aparece para os usuários e organizações esperados.
3. Valide o comportamento em tempo de execução.

Execute uma solicitação simples de leitura e confirme a acessibilidade do endpoint do provedor, a disponibilidade do modelo e a integridade do serviço do provedor.

Solução de problemas por sintoma

Sintoma	Causa provável	O que verificar	Próxima ação
Salvar ou testar falha em Ferramentas de IA	Incompatibilidad e de configuração ou conectividade	Tipo de provedor, URL do endpoint, formato da chave da API, modelo selecionado e acesso de saída	Corrija o valor que não passou na validação e salve novamente
O botão Console assistant está faltando.	Status de integração inadequado, incompatibilidad e organizacional ou incompatibilidad e de RBAC	Salvamento bem-sucedido das ferramentas de IA, status de integração, organização atual e função de acesso esperada	Atualize a sessão e verifique com uma conta de administrador conhecida e válida
O assistente abre, mas a solicitação falha	Problema com o provedor ou caminho de runtime	Acessibilidade do endpoint, disponibilidade do modelo nesse endpoint, limites do provedor e status temporário do provedor	Tente novamente após corrigir problemas de incompatibilidad de endpoint/modelo ou de limite do lado do provedor

Sintoma	Causa provável	O que verificar	Próxima ação
A resposta do assistente está lenta ou inconsistente	Tamanho do prompt, desempenho do endpoint ou instabilidade da rede/proxy	Teste rápido, integridade do serviço do provedor e estabilidade da rede/proxy	Use um prompt mais curto, tente outro modelo compatível e estabilize o roteamento de rede ou proxy

Responder à exposição ou uso indevido de credenciais de LLM

Se você suspeitar de exposição ou uso não autorizado da chave de API:

1. Revogue a chave de API existente no sistema do seu provedor.
2. Crie uma nova chave de API.
3. Atualize a chave em **Administração > Ferramentas de IA**.
4. Verifique se a reconexão foi bem-sucedida com um teste de assistente somente leitura.

Configure os canais de entrega de notificações na implantação local do NetApp Console

Na implantação local do NetApp Console, você pode configurar vários canais para notificações de alerta, incluindo e-mail e webhooks.

Funções de acesso necessárias

Superadministrador ou administrador da organização. ["Saiba mais sobre funções de acesso"](#).

Por padrão, a implantação local do Console exibe notificações por meio de seu sistema de notificações incorporado. Configurar canais de entrega adicionais permite que você receba notificações da maneira que melhor se adapte ao seu fluxo de trabalho.

Você pode enviar todas as notificações pelos mesmos canais ou usar canais diferentes para diferentes tipos de notificação. Por exemplo, você pode enviar alertas urgentes de storage por e-mail enquanto direciona outros alertas para uma ferramenta de monitoramento de terceiro por meio de um webhook.

Após configurar os canais de entrega de notificações, você pode configurar as regras de notificação e atribuí-las a diferentes canais ["Aprenda como configurar regras de notificação"](#).

Configurar um servidor de e-mail

Ao configurar um servidor de e-mail, a implantação local do Console envia notificações, alertas e convites de usuários por meio dele. A implantação local do Console é compatível com servidores de e-mail SMTP, que podem ser seu servidor de e-mail corporativo existente ou um serviço de e-mail de terceiro.

Passos

1. Selecione **Administração > Console**.
2. Selecione **Configuração** para abrir a página de configurações do sistema.
3. Na seção **Servidor de e-mail**, selecione **Configurar**.
4. Insira os detalhes de conexão do seu servidor de e-mail:

- Adicione um nome de remetente e um endereço de e-mail do remetente.
- O **host SMTP**: nome do host ou endereço IP do seu servidor SMTP. Para vários servidores, insira o principal.
- Selecione o protocolo de conexão na lista suspensa **Segurança da conexão**. A porta já está configurada para você e é somente leitura: 25 para SMTP com STARTTLS, ou 465 para SMTPS.

SMTPS (porta 465) estabelece uma conexão criptografada imediatamente e é recomendado para ambientes sensíveis à segurança. STARTTLS (porta 25) faz upgrade a partir de uma conexão não criptografada e pode voltar à transmissão não criptografada se a negociação de criptografia falhar.

5. Selecione **E-mail de teste** para enviar um e-mail de teste para um destinatário que você especificar.
6. Após o teste ser bem-sucedido, selecione **Salvar** para salvar a configuração.

Se o teste falhar, verifique novamente as configurações inseridas e certifique-se de que a implantação local do Console tenha acesso à rede ao servidor de e-mail.

Atualizar a configuração de um servidor de e-mail

Você pode atualizar a configuração de um servidor de e-mail existente se desejar usar um servidor de e-mail diferente.

Passos

1. Selecione **Administração > Console**.
2. Selecione **Configuração** para abrir a página de configurações do sistema.
3. Na seção **Servidor de e-mail**, selecione **Configurar**.
4. Selecione **Limpar campos** para limpar a configuração existente.
5. Insira os novos detalhes de conexão para o seu servidor de e-mail.
6. Selecione **E-mail de teste** para enviar um e-mail de teste para um destinatário que você especificar.
7. Após o teste ser bem-sucedido, selecione **Salvar** para salvar a nova configuração.

Se o teste falhar, verifique novamente as configurações inseridas e certifique-se de que a implantação local do Console tenha acesso à rede ao servidor de e-mail.

Remover uma configuração de servidor de e-mail

Você pode remover a configuração do servidor de e-mail se não quiser mais que a implantação local do NetApp Console envie e-mails.

Passos

1. Selecione **Administração > Console**.
2. Selecione **Configuração** para abrir a página de configuração do sistema.
3. Na seção **Servidor de e-mail**, selecione **Configurar**.
4. Selecione **Limpar campos** para limpar a configuração existente.
5. Selecione **Salvar** para salvar a configuração limpa, o que remove a configuração do servidor de e-mail da implantação local do Console.

Configurar um webhook

Configure webhooks para enviar notificações da implantação local do Console para outras ferramentas ou serviços. Você pode configurar vários webhooks, cada um apontando para um endpoint diferente. Por exemplo, um para um SIEM e outro para um serviço de paginação de plantão.

Após criar um webhook, os usuários com a função de administrador de armazenamento podem atribuí-lo a regras de alerta específicas. Por exemplo, eles podem enviar alertas críticos por e-mail enquanto enviam todos os alertas para uma ferramenta de monitoramento de terceiro por meio de um webhook.



A implantação local do Console não impõe controle de acesso aos endpoints do webhook. Qualquer usuário ou sistema que consiga acessar a URL do endpoint recebe os dados de alerta. Certifique-se de que o acesso ao aplicativo receptor seja restrito a usuários autorizados por meio dos controles de acesso do próprio aplicativo.

Antes de começar

Confirme se a implantação local do Console consegue alcançar o aplicativo receptor pela rede e colete o URL do endpoint, o método HTTP e quaisquer detalhes de autenticação ou certificado exigidos por esse aplicativo.

Passos

1. Selecione **Administração > Console**.
2. Selecione **Configuração** para abrir a página de configurações do sistema.
3. Na seção **Integração de Webhook**, selecione **Configurar**.
4. Insira os detalhes necessários para o webhook:
 - Um nome descritivo para o webhook.
 - A URL do endpoint fornecida pelo aplicativo receptor.
 - Método HTTP
 - Opcional: um certificado autoassinado em formato PEM.
 - Quaisquer cabeçalhos ou segredos necessários (credenciais de autenticação).
 - O formato a ser usado ao enviar o webhook. JSON e OTEL (OpenTelemetry) são suportados.

Use JSON para webhooks de uso geral e endpoints REST personalizados. Use OTEL para plataformas de observabilidade que consomem sinais OpenTelemetry nativamente, como o Grafana ou outros coletores compatíveis com OpenTelemetry.

5. Selecione **Test webhook** para testar a conexão do webhook e garantir que a implantação local do Console possa enviar mensagens com sucesso para o aplicativo receptor.
6. Após o teste ser bem-sucedido, selecione **Salvar** para criar o webhook.

Após salvar o webhook, ele fica disponível para os usuários selecionarem onde os webhooks são suportados, como nas opções de entrega de alertas. ["Aprenda como criar regras de alerta e atribuir webhooks para entrega de alertas."](#)

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 SOBRESSALIENTES; 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 DOCUMENTOS, 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.