



Comece a usar o Cloud Manager

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

- Comece a usar o Cloud Manager 1
 - Saiba mais sobre o Cloud Manager 1
 - Visão geral da rede 2
 - Inscreva-se no NetApp Cloud Central 3
 - Iniciar sessão no Cloud Manager 4
 - Configure uma conta do Cloud Central 5
 - Configure um conector 14
 - Onde ir a seguir 36

Comece a usar o Cloud Manager

Saiba mais sobre o Cloud Manager

O Cloud Manager permite que especialistas DE TI e arquitetos de nuvem gerenciem centralmente sua infraestrutura multicloud híbrida usando as soluções de nuvem da NetApp.

Caraterísticas

O Cloud Manager é uma plataforma de gerenciamento de classe empresarial baseada em SaaS que mantém você no controle dos seus dados, onde quer que eles estejam.

- Configure e use ["Cloud Volumes ONTAP"](#) para um gerenciamento de dados eficiente em vários protocolos nas nuvens.
- Configurar e utilizar serviços de armazenamento de ficheiros: ["Azure NetApp Files"](#), ["Cloud Volumes Service para AWS"](#) E ["Cloud Volumes Service para Google Cloud"](#).
- Descubra e gerencie clusters do ONTAP locais criando volumes, fazendo backup na nuvem, replicando dados na nuvem híbrida e dispondo dados pouco acessados em categorias na nuvem.
- Habilite serviços de nuvem e software integrados, como ["Conformidade com a nuvem"](#), ["Cloud Insights"](#), ["Cloud Backup Service"](#), ["Trident"](#) e muito mais.

["Saiba mais sobre o Cloud Manager"](#).

Fornecedores de storage de objetos compatíveis

O Cloud Manager permite gerenciar o storage de nuvem e usar serviços de nuvem na Amazon Web Services, Microsoft Azure e Google Cloud.

Custo

O software Cloud Manager é gratuito da NetApp.

Para a maioria das tarefas, o Cloud Manager solicita que você implante um conetor em sua rede de nuvem, o que resulta em cobranças do seu provedor de nuvem para a instância de computação e o armazenamento associado. Você tem a opção de executar o software Connector em suas instalações.

Como o Cloud Manager funciona

O Cloud Manager inclui uma interface baseada em SaaS integrada ao NetApp Cloud Central e conetores que gerenciam o Cloud Volumes ONTAP e outros serviços de nuvem.

Software como serviço

O Cloud Manager pode ser acessado por meio das APIs a ["Interface de usuário baseada em SaaS"](#) e. Essa experiência SaaS permite que você acesse automaticamente os recursos mais recentes à medida que são lançados e alterne facilmente entre suas contas e conetores do Cloud Central.

Centro de nuvem da NetApp

["Centro de nuvem da NetApp"](#) fornece um local centralizado para acessar e ["Serviços de nuvem da NetApp"](#) gerenciar o . Com a autenticação de usuário centralizada, você pode usar o mesmo conjunto de credenciais

para acessar o Cloud Manager e outros serviços de nuvem, como o Cloud Insights.

Ao fazer login no Cloud Manager pela primeira vez, você será solicitado a criar uma conta *Cloud Central*. Essa conta fornece alocação a vários clientes e permite organizar usuários e recursos em *workspaces* isolados.

Conectores

Na maioria dos casos, um administrador de conta precisará implantar um *Connector* na sua nuvem ou na rede local. O conector permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Um conector deve permanecer sempre em funcionamento. É importante para a saúde e operação contínuas dos serviços que você habilitar.

Por exemplo, um conector é um componente chave na integridade e operação dos sistemas Cloud Volumes ONTAP PAYGO. Se um conector for desligado, os sistemas Cloud Volumes ONTAP PAYGO desligarão após perder a comunicação com um conector por mais de 14 dias.

["Saiba mais sobre quando os conectores são necessários e como funcionam"](#).

Visão geral da rede

Antes que os usuários façam login no Cloud Manager, você precisará garantir que seus navegadores da Web possam acessar endpoints específicos. Depois disso, você precisa verificar os requisitos de rede para o tipo específico de ambiente de trabalho e serviços que serão usados.

Endpoints acessados a partir do seu navegador da Web

Os usuários devem acessar o Cloud Manager a partir de um navegador da Web. A máquina que executa o navegador da Web deve ter conexões com os seguintes endpoints:

Endpoints	Finalidade
https://cloudmanager.cloud.NetApp.com	Para conectá-lo à interface SaaS do Cloud Manager.
https://api.services.cloud.NetApp.com	Para entrar em Contato com as APIs do Cloud Central.
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se conecta a esses endpoints para autenticação de usuário centralizada por meio do NetApp Cloud Central.
https://widget.intercom.io	Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp.

Índice de requisitos de rede

- ["Conectores"](#)
- ["Cloud Volumes ONTAP para AWS"](#)
- ["Cloud Volumes ONTAP para Azure"](#)
- ["Cloud Volumes ONTAP para GCP"](#)

- "Replicação de dados entre sistemas ONTAP"
- "Cloud Compliance para Cloud Volumes ONTAP ou Azure NetApp Files"
- "Conformidade com a nuvem para Amazon S3"
- "Clusters ONTAP no local"
 - "Disposição de dados em camadas dos clusters do ONTAP para o Amazon S3"
 - "Disposição de dados em camadas dos clusters do ONTAP para o storage Azure Blob"
 - "Disposição de dados em camadas dos clusters do ONTAP para o Google Cloud Storage"
 - "Disposição de dados em camadas dos clusters do ONTAP para o StorageGRID"

Inscreeva-se no NetApp Cloud Central

Inscreeva-se no NetApp Cloud Central para que você possa acessar os serviços de nuvem da NetApp.

Passos

1. Abra um navegador da Web e vá para "[Centro de nuvem da NetApp](#)".
2. Clique em **Inscreever-se**.
3. Preencha o formulário e clique em **Inscreever-se**.

Log In to NetApp Cloud Central

Already signed up? [Login](#)

user@example.com

NetApp

New user

Phone **optional*

SIGN UP

I accept the [terms and conditions](#).

4. Aguarde um e-mail do NetApp Cloud Central.
5. Clique no link no e-mail para verificar seu endereço de e-mail.

Resultado

Agora você tem um login de usuário ativo do Cloud Central.

Iniciar sessão no Cloud Manager

A interface do Cloud Manager pode ser acessada por meio de uma interface de usuário baseada em SaaS acessando <https://cloudmanager.netapp.com> .

Passos

1. Abra um navegador da Web e vá para <https://cloudmanager.netapp.com>.
2. Faça login usando suas credenciais do NetApp Cloud Central.

NetApp

[Continue to Cloud Manager](#)

Log In to NetApp Cloud Central

Don't have an account yet? [Sign Up](#)

Email

Password

LOGIN

[Forgot your password?](#)

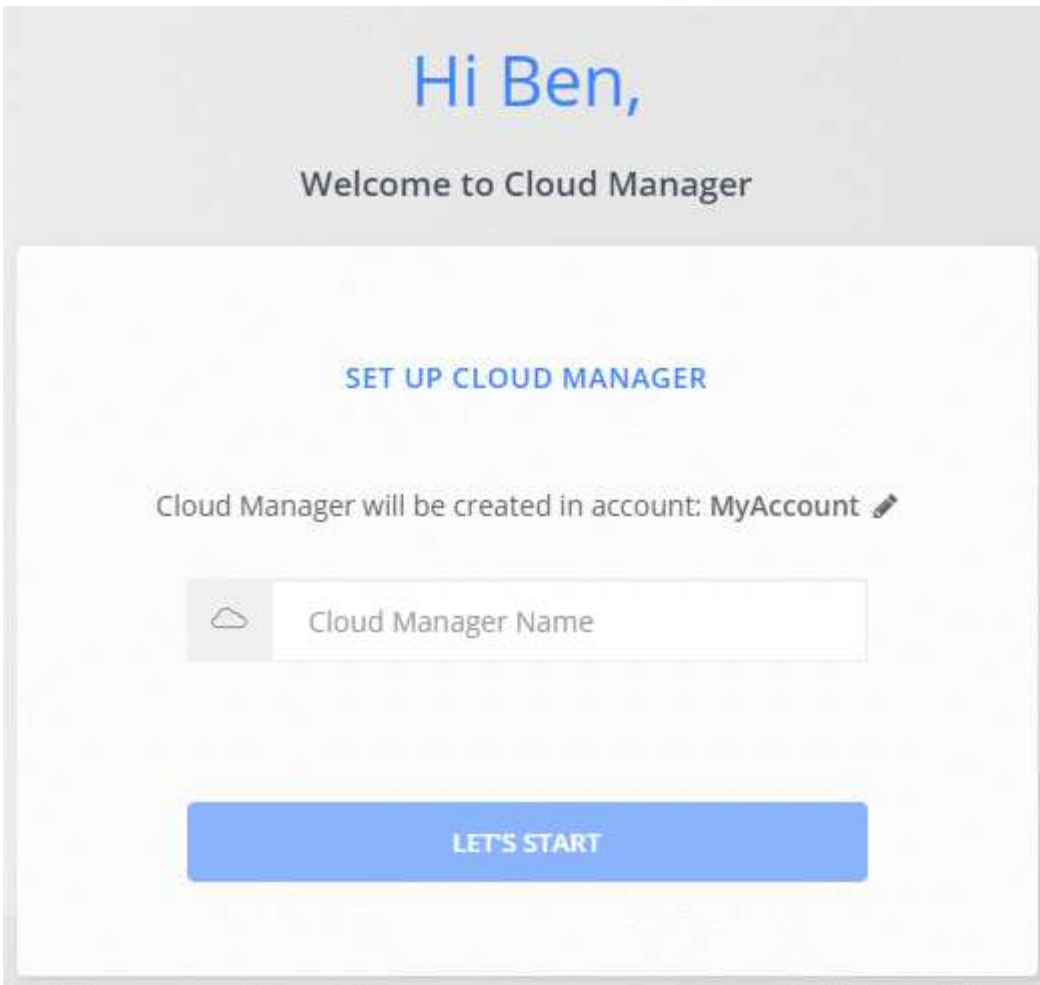
Configure uma conta do Cloud Central

Configurações de conta: Usuários, workspaces, conetores e assinaturas

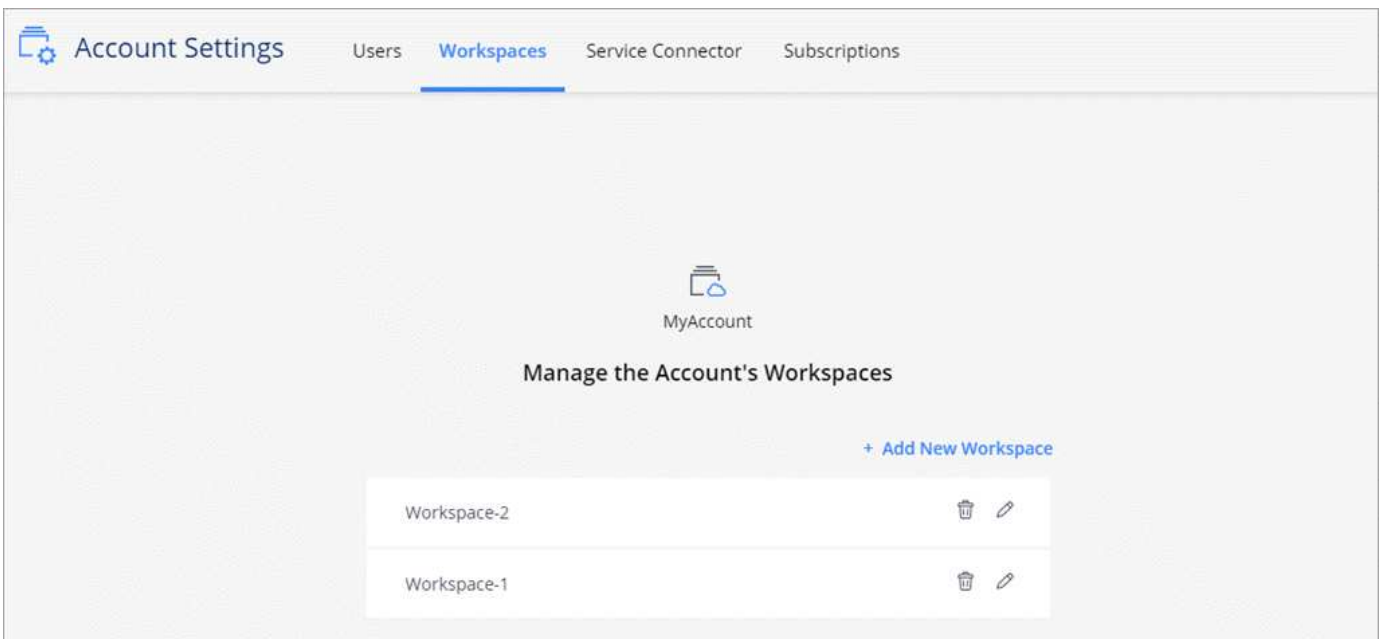
Uma conta *Cloud Central* fornece alocação a vários clientes e permite organizar usuários e recursos em espaços de trabalho isolados a partir do Cloud Manager.

Por exemplo, vários usuários podem implantar e gerenciar sistemas Cloud Volumes ONTAP em ambientes isolados chamados *workspaces*. Esses espaços de trabalho são invisíveis para outros usuários, a menos que sejam compartilhados.

Quando você acessa o Cloud Manager pela primeira vez, será solicitado a selecionar ou criar uma conta do Cloud Central:



Os administradores de conta podem modificar as configurações dessa conta gerenciando usuários, espaços de trabalho, conetores e assinaturas:



Para obter instruções passo a passo, "[Configurando a conta do Cloud Central](#)" consulte .

Definições de conta

O widget Configurações de conta no Cloud Manager permite que os administradores de conta gerenciem uma conta do Cloud Central. Se você acabou de criar sua conta, então você vai começar do zero. Mas se você já configurou uma conta, verá *todos* os usuários, espaços de trabalho, conetores e assinaturas associados à conta.

Usuários

Os usuários exibidos nas Configurações da conta são usuários do NetApp que você associa à sua conta do Cloud Central. Associar um usuário a uma conta e um ou mais espaços de trabalho nessa conta permite que esses usuários criem e gerenciem ambientes de trabalho no Cloud Manager.

Quando você associa um usuário, você atribui a ele uma função:

- *Account Admin*: Pode executar qualquer ação no Cloud Manager.
- *Workspace Admin*: Pode criar e gerenciar recursos na área de trabalho atribuída.
- *Visualizador de conformidade na nuvem*: Só pode visualizar informações de conformidade e gerar relatórios para sistemas que eles têm permissão para acessar.

Espaços de trabalho

No Cloud Manager, uma área de trabalho isola qualquer número de *ambientes de trabalho* de outros ambientes de trabalho. Os administradores do workspace não podem acessar os ambientes de trabalho em um workspace, a menos que o administrador da conta associe o administrador a esse workspace.

Um ambiente de trabalho representa um sistema de storage:

- Um sistema Cloud Volumes ONTAP de nó único ou um par de HA
- Um cluster ONTAP no local na sua rede
- Um cluster do ONTAP em uma configuração de storage privado do NetApp

Conetores

Um conector permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública. O conector é executado em uma instância de máquina virtual que você implanta em seu fornecedor de nuvem ou em um host local configurado.

Você pode usar um conector com mais de um serviço de dados de nuvem da NetApp. Por exemplo, se você já tiver um conector para o Cloud Manager, poderá selecioná-lo quando configurar o serviço Cloud Tiering.

Subscrições

O widget Configurações de conta mostra as assinaturas do NetApp associadas à conta selecionada.

Quando você se inscreve no Cloud Manager no mercado de um provedor de nuvem, você é redirecionado para o Cloud Central, onde você precisa salvar sua assinatura e associá-la a contas específicas.

Depois de se inscrever, cada assinatura estará disponível no widget Configurações da conta. Você só verá as assinaturas associadas à conta que você está visualizando no momento.

Você tem a opção de renomear uma assinatura e desassociar a assinatura de uma ou mais contas.

Por exemplo, digamos que você tem duas contas e cada uma é cobrada através de assinaturas separadas. Você pode desassociar uma assinatura de uma das contas para que os usuários dessa conta não escolham acidentalmente a assinatura errada ao criar um ambiente de trabalho do Cloud volume ONTAP.

Exemplos

Os exemplos a seguir descrevem como você pode configurar suas contas.

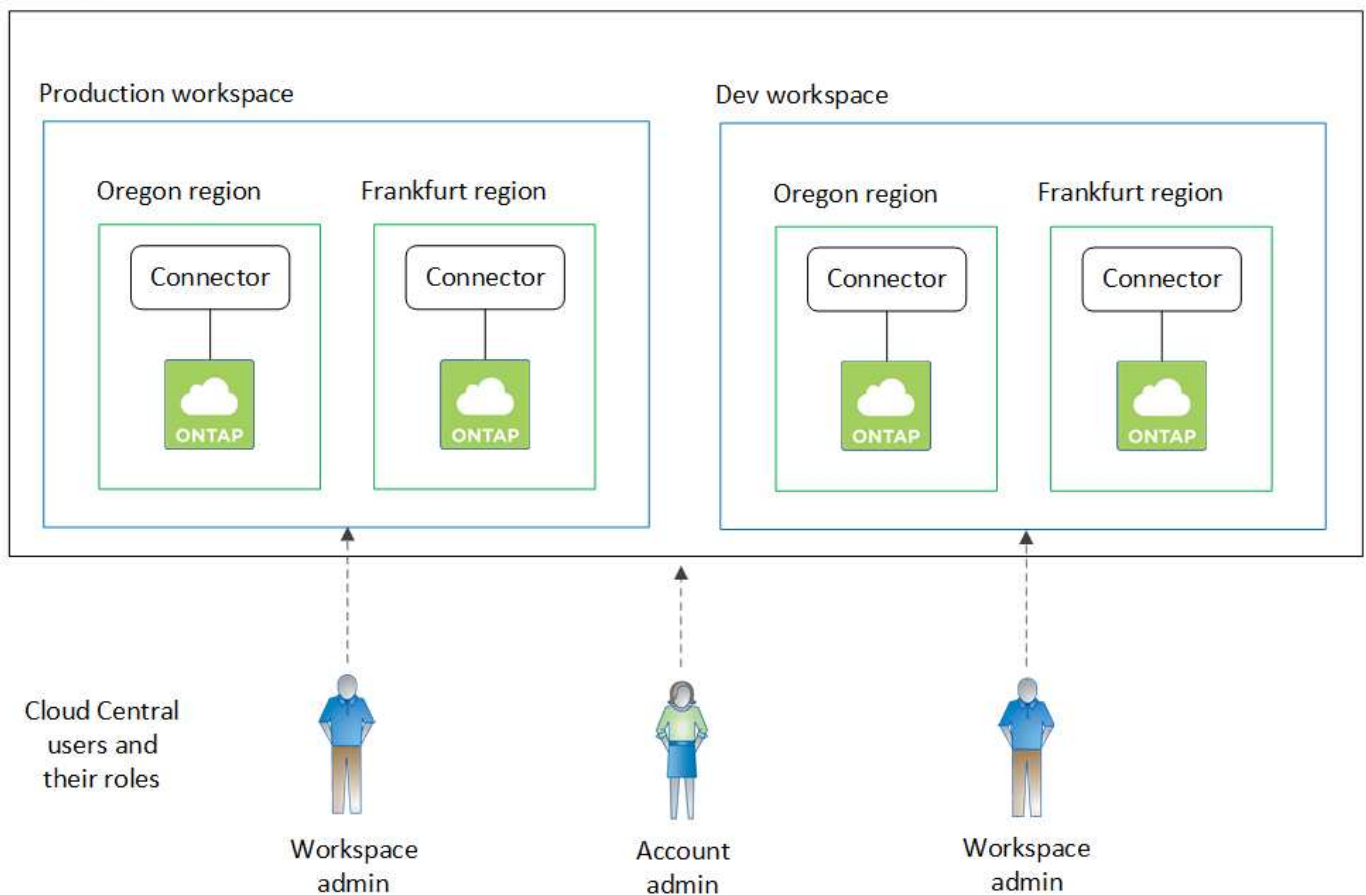


Em ambos os exemplos de imagens que se seguem, o conector e os sistemas Cloud Volumes ONTAP não residem *in* a conta NetApp Central - eles estão sendo executados em um provedor de nuvem. Esta é uma representação conceitual da relação entre cada componente.

Exemplo 1

O exemplo a seguir mostra uma conta que usa dois espaços de trabalho para criar ambientes isolados. O primeiro espaço de trabalho é para um ambiente de produção e o segundo é para um ambiente de desenvolvimento.

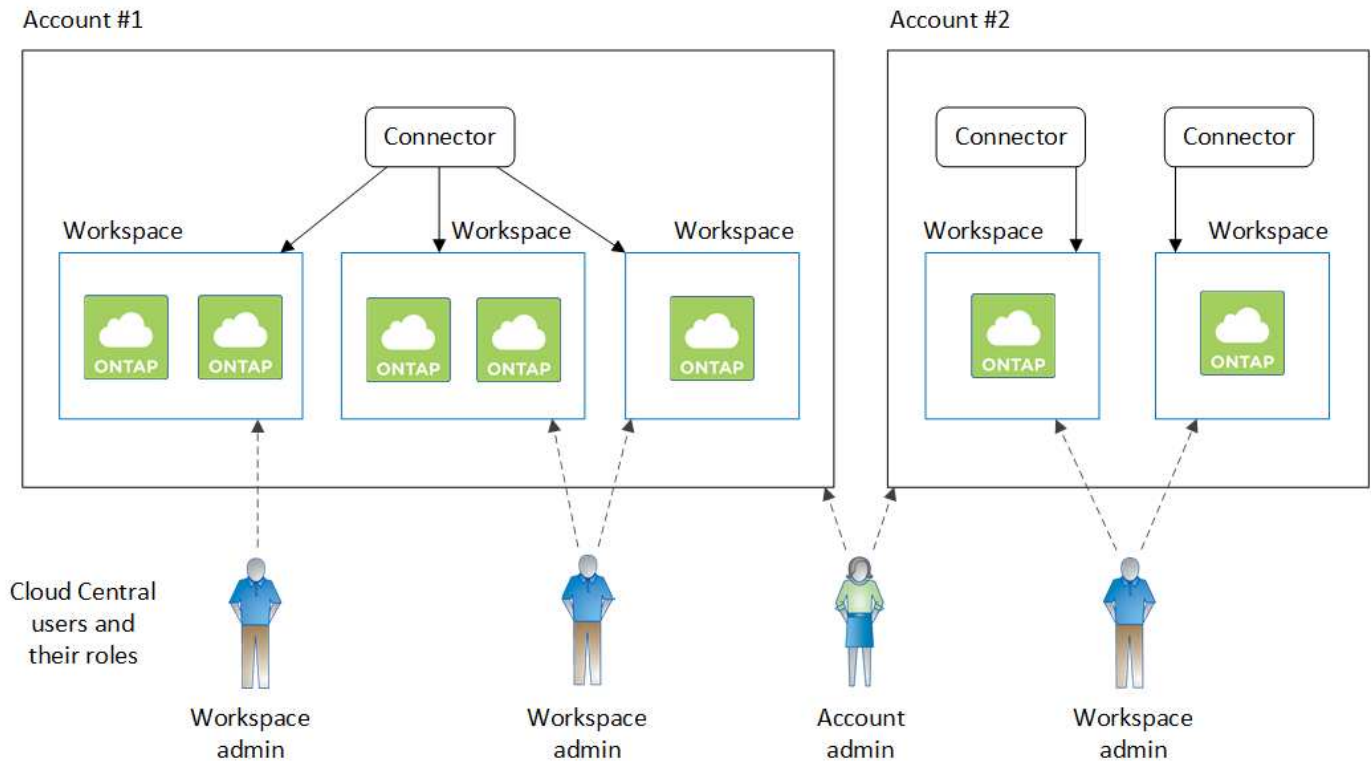
Account



Exemplo 2

Aqui está outro exemplo que mostra o mais alto nível de alocação a vários clientes usando duas contas separadas do Cloud Central. Por exemplo, um provedor de serviços pode usar o Cloud Manager em uma conta para fornecer serviços para seus clientes, enquanto usa outra conta para fornecer recuperação de desastres para uma de suas unidades de negócios.

Observe que a conta 2 inclui dois conectores separados. Isso pode acontecer se você tiver sistemas em regiões separadas ou em provedores de nuvem separados.



Configurando espaços de trabalho e usuários na conta do Cloud Central

Quando você faz login no Cloud Manager pela primeira vez, será solicitado que você crie uma conta *NetApp Cloud Central*. Essa conta fornece alocação a vários clientes e permite organizar usuários e recursos em *workspaces* isolados.

["Saiba mais sobre como as contas do Cloud Central funcionam"](#).

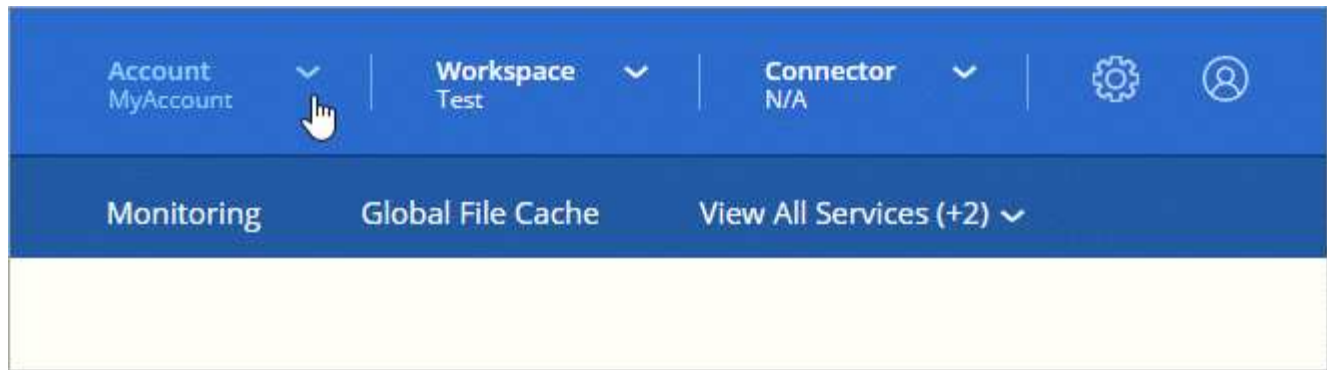
Configure sua conta do Cloud Central para que os usuários possam acessar o Cloud Manager e acessar os ambientes de trabalho em um workspace. Basta adicionar um único usuário ou adicionar vários usuários e workspaces.

Adicionar espaços de trabalho

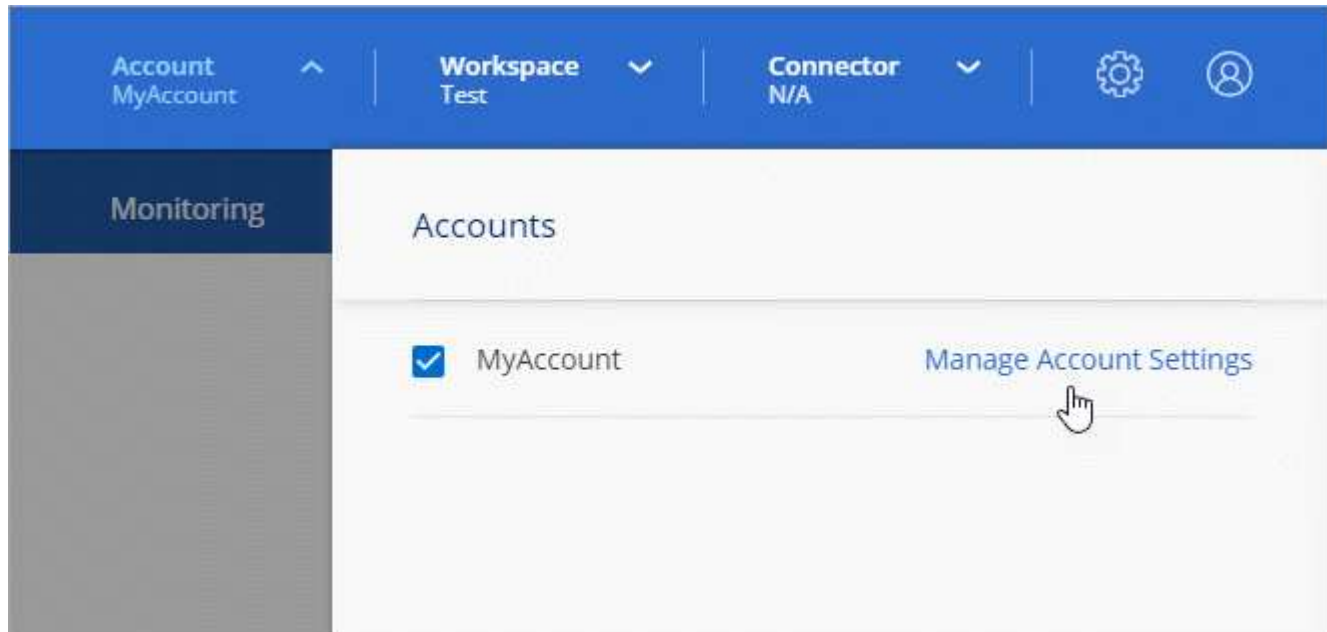
No Cloud Manager, os espaços de trabalho permitem isolar um conjunto de ambientes de trabalho de outros ambientes de trabalho e de outros usuários. Por exemplo, você pode criar dois espaços de trabalho e associar usuários separados a cada área de trabalho.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account**.



2. Clique em **Gerenciar conta** ao lado da conta selecionada no momento.



3. Clique em **Workspaces**.
4. Clique em **Adicionar novo espaço de trabalho**.
5. Insira um nome para o workspace e clique em **Add**.

Depois de terminar

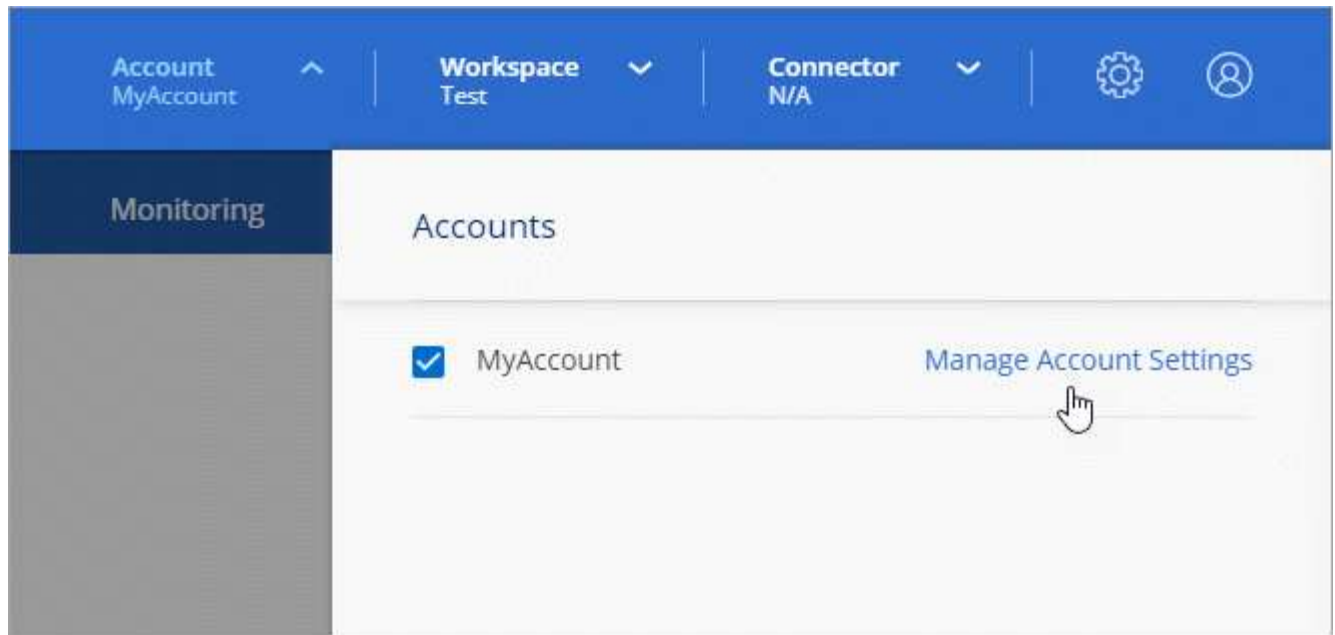
Se um administrador do espaço de trabalho precisar de acesso a essa área de trabalho, você precisará associar o usuário. Você também precisará associar conectores ao espaço de trabalho para que os administradores do Workspace possam usar esses conectores.

Adicionando usuários

Associe usuários do Cloud Central à conta do Cloud Central para que esses usuários possam criar e gerenciar ambientes de trabalho no Cloud Manager.

Passos

1. Se o usuário ainda não tiver feito isso, peça ao usuário para ir "[Centro de nuvem da NetApp](#)" e se inscrever.
2. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



3. Na guia usuários, clique em **Usuário associado**.
4. Insira o endereço de e-mail do usuário e selecione uma função para o usuário:
 - **Admin da conta:** Pode executar qualquer ação no Cloud Manager.
 - **Workspace Admin:** Pode criar e gerenciar recursos em workspaces atribuídos.
 - **Visualizador de conformidade:** Só pode visualizar informações de conformidade e gerar relatórios para espaços de trabalho que eles têm permissão para acessar.
5. Se você selecionou Workspace Admin ou Compliance Viewer, selecione um ou mais workspaces para associar a esse usuário.

Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

6. Clique em **Usuário associado**.

Resultado

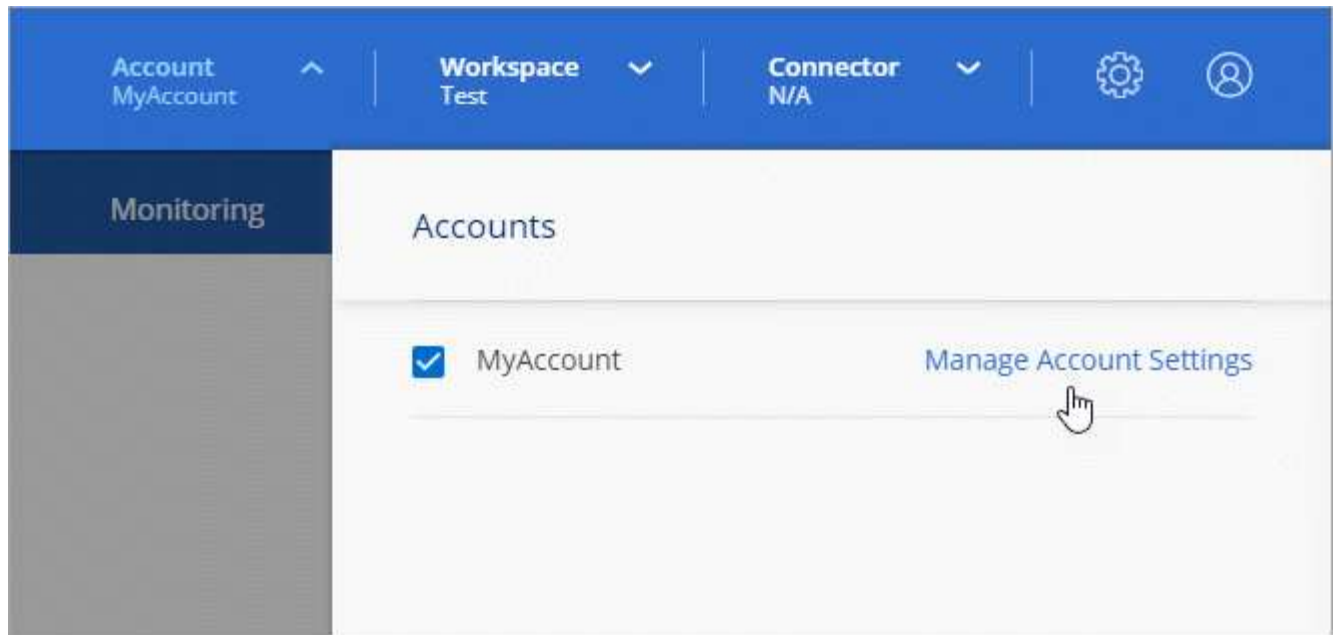
O usuário deve receber um e-mail do NetApp Cloud Central intitulado "Associação de Contas". O e-mail inclui as informações necessárias para acessar o Cloud Manager.

Associar administradores de workspace a workspaces

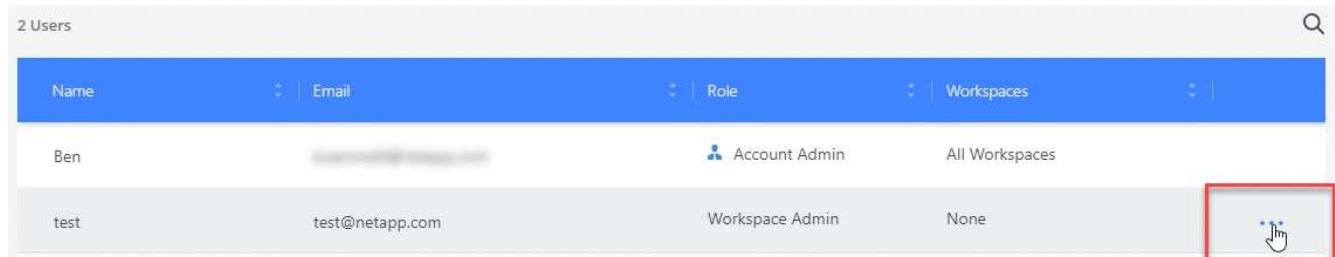
Você pode associar administradores do Workspace a espaços de trabalho adicionais a qualquer momento. Associar o usuário permite que ele crie e visualize os ambientes de trabalho nesse espaço de trabalho.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



2. Na guia usuários, clique no menu de ação na linha que corresponde ao usuário.



3. Clique em **Gerenciar espaços de trabalho**.

4. Selecione um ou mais espaços de trabalho e clique em **Apply**.

Resultado

O usuário agora pode acessar esses workspaces a partir do Cloud Manager, desde que o conector também esteja associado aos workspaces.

Associar conectores a espaços de trabalho

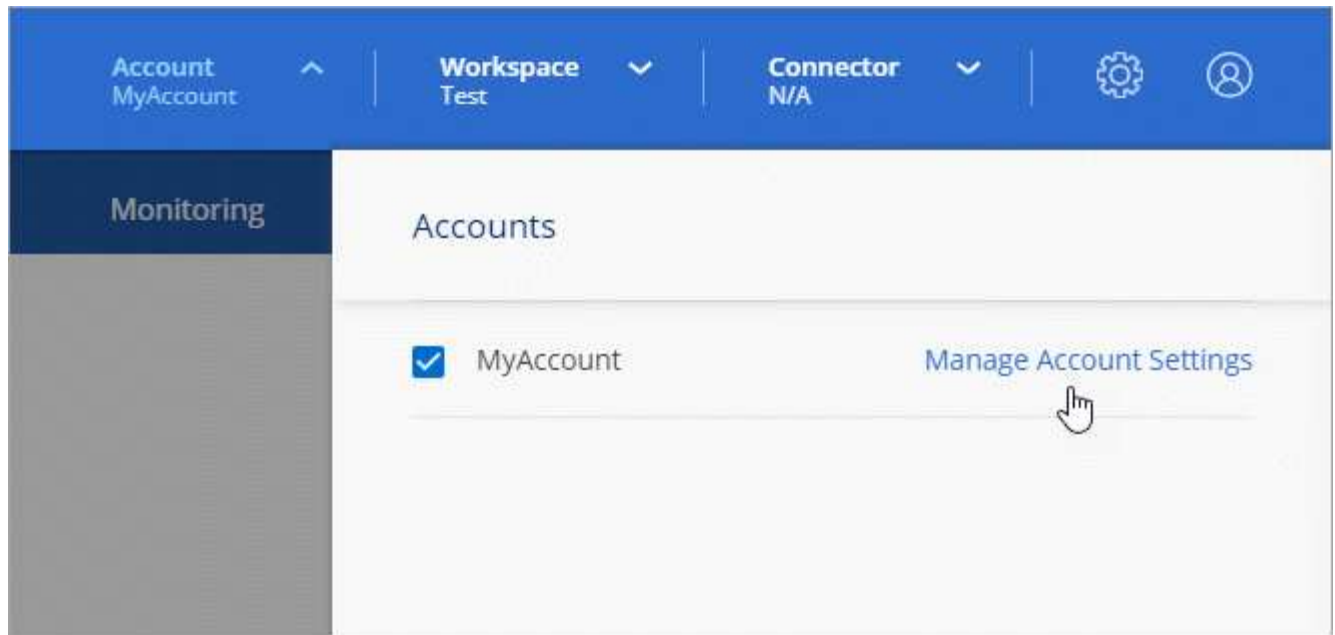
Você precisa associar um conector aos workspaces para que os administradores do workspace possam usar esses conectores para criar sistemas Cloud Volumes ONTAP.

Se você tiver apenas administradores de conta, associar o conector com workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão.

["Saiba mais sobre usuários, workspaces e conectores"](#).

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



2. Clique em **Connector**.
3. Clique em **Manage Workspaces** (gerir espaços de trabalho) para o conetor que pretende associar.
4. Selecione um ou mais espaços de trabalho e clique em **Apply**.

Resultado

Administradores de workspace agora podem usar esses conetores para criar sistemas Cloud Volumes ONTAP.

O que se segue?

Agora que você configurou sua conta, você pode gerenciá-la a qualquer momento removendo usuários, gerenciando espaços de trabalho, conetores e assinaturas. ["Saiba mais"](#).

Configure um conetor

Saiba mais sobre conetores

Na maioria dos casos, um administrador de conta precisará implantar um *Connector* na sua nuvem ou na rede local. O conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Quando é necessário um conetor

Um conetor é necessário para usar qualquer um dos seguintes recursos no Cloud Manager:

- Cloud Volumes ONTAP
- Clusters ONTAP on-premises
- Conformidade com a nuvem
- Kubernetes
- Backup na nuvem

- Monitorização
- Disposição em camadas no local
- Cache de arquivos global
- Descoberta de bucket do Amazon S3

Um conetor é **not** necessário para Azure NetApp Files, Cloud Volumes Service ou Cloud Sync.



Embora um conetor não seja necessário para configurar e gerenciar o Azure NetApp Files, um conetor é necessário se você quiser usar o Cloud Compliance para verificar os dados do Azure NetApp Files.

Locais suportados

Um conetor é suportado nos seguintes locais:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- No local



Se você quiser criar um sistema Cloud Volumes ONTAP no Google Cloud, também precisa ter um conetor em execução no Google Cloud. Não é possível usar um conetor que esteja sendo executado em outro local.

Os conetores devem permanecer em funcionamento

Um conetor deve permanecer sempre em funcionamento. É importante para a saúde e operação contínuas dos serviços que você habilitar.

Por exemplo, um conetor é um componente chave na integridade e operação dos sistemas Cloud Volumes ONTAP PAYGO. Se um conetor for desligado, os sistemas Cloud Volumes ONTAP PAYGO desligarão após perder a comunicação com um conetor por mais de 14 dias.

Como criar um conetor

Um administrador de conta precisa criar um conetor antes que um administrador do espaço de trabalho possa criar um ambiente de trabalho do Cloud Volumes ONTAP e usar qualquer um dos outros recursos listados acima.

Um administrador de conta pode criar um conetor de várias maneiras:

- Diretamente do Cloud Manager (recomendado)
 - ["Crie na AWS"](#)
 - ["Criar no Azure"](#)
 - ["Crie no GCP"](#)
- ["No AWS Marketplace"](#)
- ["A partir do Azure Marketplace"](#)
- ["Baixando e instalando o software em um host Linux existente"](#)

Quando você cria seu primeiro ambiente de trabalho do Cloud Volumes ONTAP, o Cloud Manager solicitará que você crie um conector se você ainda não tiver um.

Permissões

Permissões específicas são necessárias para criar o conector e outro conjunto de permissões é necessário para a própria instância do conector.

Permissões para criar um conector

O usuário que cria um conector do Cloud Manager precisa de permissões específicas para implantar a instância em seu provedor de nuvem de sua escolha. O Cloud Manager irá lembrá-lo dos requisitos de permissões quando você criar um conector.

["Veja as políticas de cada provedor de nuvem"](#).

Permissões para a instância do conector

O conector precisa de permissões específicas do provedor de nuvem para executar operações em seu nome. Por exemplo, para implantar e gerenciar o Cloud Volumes ONTAP.

Quando você cria um conector diretamente do Cloud Manager, o Cloud Manager cria o conector com as permissões de que ele precisa. Não há nada que você precise fazer.

Se você criar o conector a partir do AWS Marketplace, do Azure Marketplace ou instalando manualmente o software, precisará garantir que as permissões certas estejam em vigor.

["Veja as políticas de cada provedor de nuvem"](#).

Quando utilizar vários conectores

Em alguns casos, você pode precisar apenas de um conector, mas você pode encontrar-se precisando de dois ou mais conectores.

Aqui estão alguns exemplos:

- Você está usando um ambiente multicloud (AWS e Azure), então você tem um conector na AWS e outro no Azure. Cada um gerencia os sistemas Cloud Volumes ONTAP executados nesses ambientes.
- Um provedor de serviços pode usar uma conta do Cloud Central para fornecer serviços para seus clientes, enquanto usa outra conta para fornecer recuperação de desastres para uma de suas unidades de negócios. Cada conta teria conectores separados.

Quando alternar entre conectores

Quando você cria seu primeiro conector, o Cloud Manager usa esse conector automaticamente para cada ambiente de trabalho adicional criado. Depois de criar um conector adicional, você precisará alternar entre eles para ver os ambientes de trabalho específicos de cada conector.

["Saiba como alternar entre conectores"](#).

A interface do utilizador local

Embora você deva executar quase todas as tarefas do ["Interface de usuário SaaS"](#), uma interface de usuário local ainda está disponível no conector. Esta interface é necessária para algumas tarefas que precisam ser executadas a partir do próprio conector:

- ["Configurando um servidor proxy"](#)
- Instalando um patch (você normalmente trabalhará com o pessoal do NetApp para instalar um patch)
- Download de mensagens do AutoSupport (geralmente direcionadas pelo pessoal do NetApp quando você tiver problemas)

["Saiba como acessar a IU local"](#).

Atualizações do conetor

O conetor atualiza automaticamente o software para a versão mais recente, desde que seja ["acesso de saída à internet"](#) necessário obter a atualização de software.

Requisitos de rede para o conetor

Configure sua rede para que o conetor possa gerenciar recursos e processos em seu ambiente de nuvem pública. O passo mais importante é garantir o acesso de saída à Internet a vários endpoints.



Se a rede utilizar um servidor proxy para toda a comunicação com a Internet, pode especificar o servidor proxy a partir da página Definições. ["Configurando o conetor para usar um servidor proxy"](#) Consulte a .

Conexão com redes de destino

Um conetor requer uma conexão de rede com o tipo de ambiente de trabalho que você está criando e os serviços que você está planejando habilitar.

Por exemplo, se você instalar um conetor em sua rede corporativa, deverá configurar uma conexão VPN com a VPC ou a VNet no qual você inicia o Cloud Volumes ONTAP.

Acesso de saída à Internet

O conetor requer acesso de saída à Internet para gerenciar recursos e processos em seu ambiente de nuvem pública. O acesso de saída à Internet também é necessário se você quiser instalar manualmente o conetor em um host Linux ou acessar a IU local em execução no conetor.

As seções a seguir identificam os endpoints específicos.

Endpoints para gerenciar recursos na AWS

Um conetor entra em Contato com os seguintes endpoints ao gerenciar recursos na AWS:

Endpoints	Finalidade
<p>Serviços da AWS (amazonaws.com):</p> <ul style="list-style-type: none"> • CloudFormation • Nuvem de computação elástica (EC2) • Key Management Service (KMS) • Serviço de token de segurança (STS) • Serviço de armazenamento simples (S3) <p>O endpoint exato depende da região em que você implementa o Cloud Volumes ONTAP. "Consulte a documentação da AWS para obter detalhes."</p>	<p>Permite que o conector implante e gerencie o Cloud Volumes ONTAP na AWS.</p>
<p>https://api.services.cloud.NetApp.com:443</p>	<p>Solicitações de API para o NetApp Cloud Central.</p>
<p>https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com</p>	<p>Fornecer acesso a imagens de software, manifestos e modelos.</p>
<p>https://repo.cloud.support.NetApp.com</p>	<p>Usado para baixar dependências do Cloud Manager.</p>
<p>http://repo.mysql.com/</p>	<p>Usado para baixar MySQL.</p>
<p>https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com</p>	<p>Permite que o conector acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.</p>
<p>https://cloudmanagerinfraprod.azurecr.io</p>	<p>Acesso a imagens de software de componentes de contêiner para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.</p>
<p>https://kinesis.us-east-1.amazonaws.com</p>	<p>Permite que o NetApp transmita dados de Registros de auditoria.</p>
<p>https://cloudmanager.cloud.NetApp.com</p>	<p>Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.</p>
<p>https://NetApp-cloud-account.auth0.com</p>	<p>Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.</p>
<p>https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist</p>	<p>Usado para adicionar seu ID de conta da AWS à lista de usuários permitidos para Backup em S3.</p>
<p>https://support.NetApp.com/aods/asupmessage https://support.NetApp.com/asupprod/post/1,0/postAsup</p>	<p>Comunicação com NetApp AutoSupport.</p>

Endpoints	Finalidade
https://support.NetApp.com/svcgw - https://support.NetApp.com/ServiceGW/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://client.infra.support.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com-accelerated.s3.us-west-1.amazonaws.com - https://trigger.asup.NetApp.com.s3.us-west-1.amazonaws.com	Permite que o NetApp colete informações necessárias para solucionar problemas de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.
Vários locais de terceiros, por exemplo: <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Locais de terceiros estão sujeitos a alterações.	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

Endpoints para gerenciar recursos no Azure

Um conetor entra em Contato com os seguintes endpoints ao gerenciar recursos no Azure:

Endpoints	Finalidade
https://management.azure.com https://login.microsoftonline.com	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP na maioria das regiões do Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP nas regiões Azure Alemanha.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP nas regiões Azure US Gov.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornece acesso a imagens de software, manifestos e modelos.
https://repo.cloud.support.NetApp.com	Usado para baixar dependências do Cloud Manager.
http://repo.mysql.com/	Usado para baixar MySQL.

Endpoints	Finalidade
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com	Permite que o conector acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://cloudmanagerinfraproduct.azurecr.io	Acesso a imagens de software de componentes de contentor para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://mysupport.NetApp.com	Comunicação com NetApp AutoSupport.
https://support.NetApp.com/svcgw - https://support.NetApp.com/ServiceGW/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://client.infra.support.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com-accelerated.s3.us-west-1.amazonaws.com - https://trigger.asup.NetApp.com.s3.us-west-1.amazonaws.com	Permite que o NetApp colete informações necessárias para solucionar problemas de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.
*.blob.core.windows.net	Necessário para pares de HA ao usar um proxy.

Endpoints	Finalidade
<p>Vários locais de terceiros, por exemplo:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com <p>Locais de terceiros estão sujeitos a alterações.</p>	<p>Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.</p>

Endpoints para gerenciar recursos no GCP

Um conector entra em Contato com os seguintes endpoints ao gerenciar recursos no GCP:

Endpoints	Finalidade
https://www.googleapis.com	Permite que o conector entre em Contato com as APIs do Google para implantar e gerenciar o Cloud Volumes ONTAP no GCP.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornecer acesso a imagens de software, manifestos e modelos.
https://repo.cloud.support.NetApp.com	Usado para baixar dependências do Cloud Manager.
http://repo.mysql.com/	Usado para baixar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com	Permite que o conector acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acesso a imagens de software de componentes de contentor para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://mysupport.NetApp.com	Comunicação com NetApp AutoSupport.

Endpoints	Finalidade
https://support.NetApp.com/svcgw - https://support.NetApp.com/ServiceGW/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://client.infra.support.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com-accelerated.s3.us-west-1.amazonaws.com - https://trigger.asup.NetApp.com.s3.us-west-1.amazonaws.com	Permite que o NetApp colete informações necessárias para solucionar problemas de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.
Vários locais de terceiros, por exemplo: <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Locais de terceiros estão sujeitos a alterações.	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

Endpoints para instalar o conector em um host Linux

Você tem a opção de instalar manualmente o software Connector em seu próprio host Linux. Se o fizer, o instalador do conector deve acessar os seguintes URLs durante o processo de instalação:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

O host pode tentar atualizar os pacotes do sistema operacional durante a instalação. O host pode entrar em Contato com diferentes sites de espelhamento para esses pacotes do sistema operacional.

Endpoints acessados a partir do navegador da Web ao usar a IU local

Embora você deva executar quase todas as tarefas a partir da interface de usuário SaaS, uma interface de usuário local ainda está disponível no conector. A máquina que executa o navegador da Web deve ter conexões com os seguintes endpoints:

Endpoints	Finalidade
O host do conetor	<p>Você deve inserir o endereço IP do host de um navegador da Web para carregar o console do Cloud Manager.</p> <p>Dependendo da sua conectividade com o seu provedor de nuvem, você pode usar o IP privado ou um IP público atribuído ao host:</p> <ul style="list-style-type: none"> • Um IP privado funciona se você tiver uma VPN e acesso direto à sua rede virtual • Um IP público funciona em qualquer cenário de rede <p>Em qualquer caso, você deve proteger o acesso à rede, garantindo que as regras do grupo de segurança permitam o acesso somente de IPs ou sub-redes autorizados.</p>
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se conecta a esses endpoints para autenticação de usuário centralizada por meio do NetApp Cloud Central.
https://widget.intercom.io	Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp.

Portas e grupos de segurança

Não há tráfego de entrada para o conetor, a menos que você o inicie. HTTP e HTTPS fornecem acesso ao "IU local", que você usará em circunstâncias raras. O SSH só é necessário se você precisar se conectar ao host para solução de problemas.

Regras para o conetor na AWS

O grupo de segurança do conetor requer regras de entrada e saída.

Regras de entrada

A origem das regras de entrada no grupo de segurança predefinido é 0,0.0,0/0.

Protocolo	Porta	Finalidade
SSH	22	Fornece acesso SSH ao host do conetor
HTTP	80	Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local e conexões a partir do Cloud Compliance
HTTPS	443	Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local
TCP	3128	Fornece à instância de conformidade com a nuvem acesso à Internet, se sua rede AWS não usar um NAT ou proxy

Regras de saída

O grupo de segurança predefinido para o conetor abre todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se você precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

O grupo de segurança predefinido para o conetor inclui as seguintes regras de saída.

Protocolo	Porta	Finalidade
Todo o TCP	Tudo	Todo o tráfego de saída
Todos os UDP	Tudo	Todo o tráfego de saída

Regras de saída avançadas

Se você precisar de regras rígidas para o tráfego de saída, você pode usar as seguintes informações para abrir apenas as portas necessárias para a comunicação de saída pelo conetor.



O endereço IP de origem é o host do conetor.

Serviço	Protocolo	Porta	Destino	Finalidade
Active Directory	TCP	88	Floresta do active Directory	Autenticação Kerberos V.
	TCP	139	Floresta do active Directory	Sessão de serviço NetBIOS
	TCP	389	Floresta do active Directory	LDAP
	TCP	445	Floresta do active Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Floresta do active Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	TCP	749	Floresta do active Directory	Palavra-passe de alteração e definição Kerberos V do active Directory (RPCSEC_GSS)
	UDP	137	Floresta do active Directory	Serviço de nomes NetBIOS
	UDP	138	Floresta do active Directory	Serviço de datagrama NetBIOS
	UDP	464	Floresta do active Directory	Administração de chaves Kerberos

Serviço	Protocolo	Porta	Destino	Finalidade
Chamadas de API e AutoSupport	HTTPS	443	LIF de gerenciamento de cluster de ONTAP e Internet de saída	Chamadas de API para AWS e ONTAP e envio de mensagens AutoSupport para o NetApp
Chamadas de API	TCP	3000	LIF de gerenciamento de clusters ONTAP	Chamadas de API para ONTAP
	TCP	8088	Cópia de segurança para S3	Chamadas de API para Backup para S3
DNS	UDP	53	DNS	Usado para resolução de DNS pelo Cloud Manager
Conformidade com a nuvem	HTTP	80	Instância de Cloud Compliance	Cloud Compliance para Cloud Volumes ONTAP

Regras para o conetor no Azure

O grupo de segurança do conetor requer regras de entrada e saída.

Regras de entrada

A origem das regras de entrada no grupo de segurança predefinido é 0,0.0,0/0.

Porta	Protocolo	Finalidade
22	SSH	Fornece acesso SSH ao host do conetor
80	HTTP	Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local
443	HTTPS	Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local

Regras de saída

O grupo de segurança predefinido para o conetor abre todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se você precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

O grupo de segurança predefinido para o conetor inclui as seguintes regras de saída.

Porta	Protocolo	Finalidade
Tudo	Todo o TCP	Todo o tráfego de saída
Tudo	Todos os UDP	Todo o tráfego de saída

Regras de saída avançadas

Se você precisar de regras rígidas para o tráfego de saída, você pode usar as seguintes informações para abrir apenas as portas necessárias para a comunicação de saída pelo conector.



O endereço IP de origem é o host do conector.

Serviço	Porta	Protocolo	Destino	Finalidade
Ative Directory	88	TCP	Floresta do ativo Directory	Autenticação Kerberos V.
	139	TCP	Floresta do ativo Directory	Sessão de serviço NetBIOS
	389	TCP	Floresta do ativo Directory	LDAP
	445	TCP	Floresta do ativo Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	464	TCP	Floresta do ativo Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	749	TCP	Floresta do ativo Directory	Palavra-passe de alteração e definição Kerberos V do ativo Directory (RPCSEC_GSS)
	137	UDP	Floresta do ativo Directory	Serviço de nomes NetBIOS
	138	UDP	Floresta do ativo Directory	Serviço de datagrama NetBIOS
	464	UDP	Floresta do ativo Directory	Administração de chaves Kerberos
Chamadas de API e AutoSupport	443	HTTPS	LIF de gerenciamento de cluster de ONTAP e Internet de saída	Chamadas de API para AWS e ONTAP e envio de mensagens AutoSupport para o NetApp
Chamadas de API	3000	TCP	LIF de gerenciamento de clusters ONTAP	Chamadas de API para ONTAP

Serviço	Porta	Protocolo	Destino	Finalidade
DNS	53	UDP	DNS	Usado para resolução de DNS pelo Cloud Manager

Regras para o conetor na GCP

As regras de firewall para o conetor exigem regras de entrada e saída.

Regras de entrada

A origem das regras de entrada nas regras de firewall predefinidas é 0,0.0,0/0.

Protocolo	Porta	Finalidade
SSH	22	Fornece acesso SSH ao host do conetor
HTTP	80	Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local
HTTPS	443	Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local

Regras de saída

As regras de firewall predefinidas para o conetor abrem todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se você precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

As regras de firewall predefinidas para o conetor incluem as seguintes regras de saída.

Protocolo	Porta	Finalidade
Todo o TCP	Tudo	Todo o tráfego de saída
Todos os UDP	Tudo	Todo o tráfego de saída

Regras de saída avançadas

Se você precisar de regras rígidas para o tráfego de saída, você pode usar as seguintes informações para abrir apenas as portas necessárias para a comunicação de saída pelo conetor.



O endereço IP de origem é o host do conetor.

Serviço	Protocolo	Porta	Destino	Finalidade
Ative Directory	TCP	88	Floresta do ativo Directory	Autenticação Kerberos V.
	TCP	139	Floresta do ativo Directory	Sessão de serviço NetBIOS
	TCP	389	Floresta do ativo Directory	LDAP
	TCP	445	Floresta do ativo Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Floresta do ativo Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	TCP	749	Floresta do ativo Directory	Palavra-passe de alteração e definição Kerberos V do ativo Directory (RPCSEC_GSS)
	UDP	137	Floresta do ativo Directory	Serviço de nomes NetBIOS
	UDP	138	Floresta do ativo Directory	Serviço de datagrama NetBIOS
	UDP	464	Floresta do ativo Directory	Administração de chaves Kerberos
Chamadas de API e AutoSupport	HTTPS	443	LIF de gerenciamento de cluster de ONTAP e Internet de saída	Chamadas de API para GCP e ONTAP e envio de mensagens AutoSupport para o NetApp
Chamadas de API	TCP	3000	LIF de gerenciamento de clusters ONTAP	Chamadas de API para ONTAP
DNS	UDP	53	DNS	Usado para resolução de DNS pelo Cloud Manager

Criando um conector na AWS a partir do Cloud Manager

Um administrador de conta precisa implantar um *Connector* antes de poder usar a maioria dos recursos do Cloud Manager. ["Aprenda quando um conector é necessário"](#). O conector permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Esta página descreve como criar um conector na AWS diretamente do Cloud Manager. Também tem a opção

de "[Crie o conector no AWS Marketplace](#)", ou para "[baixe o software e instale-o em seu próprio host](#)".

Essas etapas devem ser concluídas por um usuário que tenha a função Administrador da conta. Um administrador do espaço de trabalho não pode criar um conector.



Quando você cria seu primeiro ambiente de trabalho do Cloud Volumes ONTAP, o Cloud Manager solicitará que você crie um conector se você ainda não tiver um.

Configurando permissões da AWS para criar um conector

Antes de implantar um conector do Cloud Manager, você precisa garantir que sua conta da AWS tenha as permissões corretas.

Passos

1. Transfira a política do IAM do conector a partir da seguinte localização:

["Gerenciador de nuvem do NetApp: Políticas da AWS, Azure e GCP"](#)

2. No console do AWS IAM, crie sua própria política copiando e colando o texto da política do Connector IAM.
3. Anexe a política criada na etapa anterior ao usuário do IAM que criará o conector do Cloud Manager.

Resultado

O usuário da AWS agora tem as permissões necessárias para criar o conector do Cloud Manager. Você precisará especificar as chaves de acesso da AWS para esse usuário quando for solicitado pelo Cloud Manager.

Criando um conector na AWS

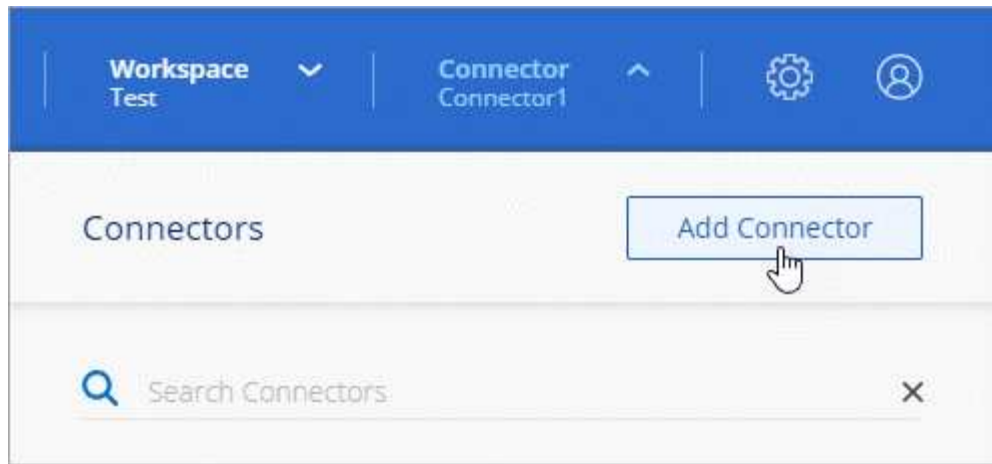
O Cloud Manager permite que você crie um conector na AWS diretamente a partir de sua interface de usuário.

O que você vai precisar

- Uma chave de acesso da AWS e uma chave secreta para um usuário do IAM que tenha o "[permissões necessárias](#)".
- Uma VPC, sub-rede e um par de chaves na sua região da AWS escolhida.

Passos

1. Se você estiver criando seu primeiro ambiente de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções. Caso contrário, clique no menu suspenso **Connector** e selecione **Add Connector**.



2. Clique em **Let's Start**.
3. Escolha **Amazon Web Services** como seu provedor de nuvem.

Lembre-se de que o conector deve ter uma conexão de rede com o tipo de ambiente de trabalho que você está criando e os serviços que você está planejando habilitar.

["Saiba mais sobre os requisitos de rede para o conector"](#).

4. Revise o que você precisará e clique em **continuar**.
5. Forneça as informações necessárias:
 - **Credenciais da AWS:** Insira um nome para a instância e especifique a chave de acesso e a chave secreta da AWS que atendem aos requisitos de permissões.
 - **Localização:** Especifique uma região, VPC e sub-rede da AWS para a instância.
 - **Rede:** Selecione o par de chaves a utilizar com a instância, se pretende ativar um endereço IP público e, opcionalmente, especificar uma configuração de proxy.
 - **Grupo de segurança:** Escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita o acesso HTTP, HTTPS e SSH de entrada.



Não há tráfego de entrada para o conector, a menos que você o inicie. HTTP e HTTPS fornecem acesso ao "IU local", que você usará em circunstâncias raras. O SSH só é necessário se você precisar se conectar ao host para solução de problemas.

6. Clique em **criar**.

A instância deve estar pronta em cerca de 7 minutos. Você deve permanecer na página até que o processo esteja concluído.

Depois de terminar

Você precisa associar um conector aos workspaces para que os administradores do workspace possam usar esses conectores para criar sistemas Cloud Volumes ONTAP. Se você tiver apenas administradores de conta, associar o conector aos workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão. ["Saiba mais"](#).

Criando um conector no Azure a partir do Cloud Manager

Um administrador de conta precisa implantar um *Connector* antes de poder usar a

maioria dos recursos do Cloud Manager. ["Aprenda quando um conector é necessário"](#). O conector permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Esta página descreve como criar um conector no Azure diretamente do Cloud Manager. Também tem a opção de ["Crie o conector no Azure Marketplace"](#), ou para ["baixe o software e instale-o em seu próprio host"](#).

Essas etapas devem ser concluídas por um usuário que tenha a função Administrador da conta. Um administrador do espaço de trabalho não pode criar um conector.



Quando você cria seu primeiro ambiente de trabalho do Cloud Volumes ONTAP, o Cloud Manager solicitará que você crie um conector se você ainda não tiver um.

Configurando permissões do Azure para criar um conector

Antes de implantar um conector do Cloud Manager, você precisa garantir que sua conta do Azure tenha as permissões corretas.

Passos

1. Crie uma função personalizada usando a política do Azure para o conector:
 - a. Faça download do ["Política do Azure para o conector"](#).



Clique com o botão direito no link e clique em **Salvar link como...** para baixar o arquivo.

- b. Modifique o arquivo JSON adicionando sua ID de assinatura do Azure ao escopo atribuível.

Exemplo

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzxxxxxx",  
],
```

- c. Use o arquivo JSON para criar uma função personalizada no Azure.

O exemplo a seguir mostra como criar uma função personalizada usando a CLI do Azure 2,0:

```
az role definition create --role-definition  
C:\Policy_for_Setup_As_Service_Azure.json
```

Agora você deve ter uma função personalizada chamada *Azure SetupAsService*.

2. Atribua a função ao usuário que implantará o conector do Cloud Manager:
 - a. Abra o serviço **Subscrições** e selecione a assinatura do usuário.
 - b. Clique em **Access Control (IAM)**.
 - c. Clique em **Adicionar > Adicionar atribuição de função** e, em seguida, adicione as permissões:
 - Selecione a função **Azure SetupAsService**.



Azure SetupAsService é o nome padrão fornecido no "[Política de implantação do Connector para Azure](#)". Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

- Atribua acesso a um **usuário, grupo ou aplicativo do Azure AD**.
- Selecione a conta de utilizador.
- Clique em **Salvar**.

Resultado

O usuário do Azure agora tem as permissões necessárias para implantar o conector do Cloud Manager.

Criando um conector no Azure

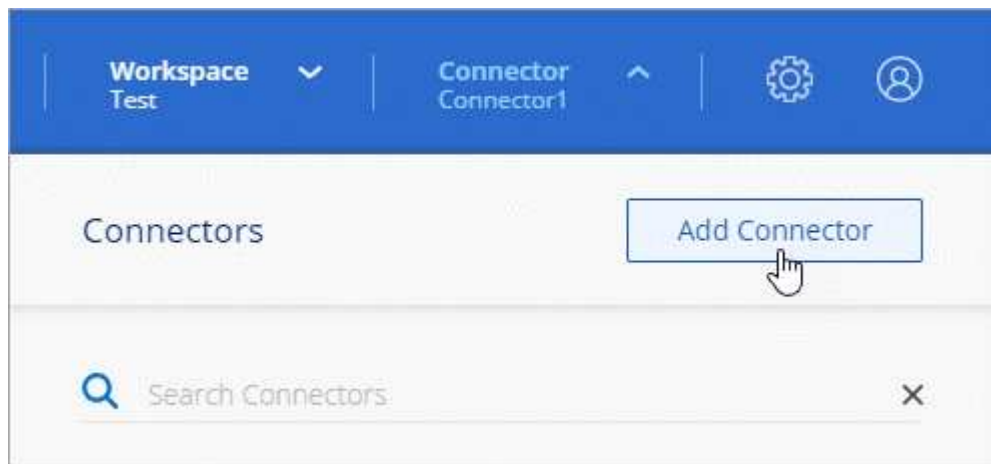
O Cloud Manager permite que você crie um conector no Azure diretamente a partir de sua interface de usuário.

O que você vai precisar

- A "[permissões necessárias](#)" para a sua conta Azure.
- Uma subscrição do Azure.
- Uma VNet e uma sub-rede na sua região do Azure escolhida.

Passos

1. Se você estiver criando seu primeiro ambiente de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções. Caso contrário, clique no menu suspenso **Connector** e selecione **Add Connector**.



2. Clique em **Let's Start**.
3. Escolha **Microsoft Azure** como seu provedor de nuvem.

Lembre-se de que o conector deve ter uma conexão de rede com o tipo de ambiente de trabalho que você está criando e os serviços que você está planejando habilitar.

["Saiba mais sobre os requisitos de rede para o conector"](#).

4. Revise o que você precisará e clique em **continuar**.
5. Se você for solicitado, faça login na sua conta Microsoft, que deve ter as permissões necessárias para criar a máquina virtual.

O formulário é de propriedade e hospedado pela Microsoft. Suas credenciais não são fornecidas ao NetApp.



Se você já estiver conectado a uma conta do Azure, o Cloud Manager usará essa conta automaticamente. Se você tiver várias contas, talvez seja necessário fazer logout primeiro para garantir que esteja usando a conta certa.

6. Forneça as informações necessárias:

- **Autenticação da VM:** Insira um nome para a máquina virtual e um nome de usuário e senha ou chave pública.
- **Configurações básicas:** Escolha uma assinatura do Azure, uma região do Azure e se deseja criar um novo grupo de recursos ou usar um grupo de recursos existente.
- **Rede:** Escolha uma VNet e uma sub-rede, se deseja ativar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.
- **Grupo de segurança:** Escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita o acesso HTTP, HTTPS e SSH de entrada.



Não há tráfego de entrada para o conector, a menos que você o inicie. HTTP e HTTPS fornecem acesso ao "IU local", que você usará em circunstâncias raras. O SSH só é necessário se você precisar se conectar ao host para solução de problemas.

7. Clique em **criar**.

A máquina virtual deve estar pronta em cerca de 7 minutos. Você deve permanecer na página até que o processo esteja concluído.

Depois de terminar

Você precisa associar um conector aos workspaces para que os administradores do workspace possam usar esses conectores para criar sistemas Cloud Volumes ONTAP. Se você tiver apenas administradores de conta, associar o conector aos workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão. ["Saiba mais"](#).

Criando um conector no GCP a partir do Cloud Manager

Um administrador de conta precisa implantar um *Connector* antes de poder usar a maioria dos recursos do Cloud Manager. ["Aprenda quando um conector é necessário"](#). O conector permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Esta página descreve como criar um conector no GCP diretamente do Cloud Manager. Você também tem a opção de ["baixe o software e instale-o em seu próprio host"](#).

Essas etapas devem ser concluídas por um usuário que tenha a função Administrador da conta. Um administrador do espaço de trabalho não pode criar um conector.



Quando você cria seu primeiro ambiente de trabalho do Cloud Volumes ONTAP, o Cloud Manager solicitará que você crie um conector se você ainda não tiver um.

Configurando permissões do GCP para criar um conetor

Antes de implantar um conetor do Cloud Manager, você precisa garantir que sua conta do GCP tenha as permissões corretas e que uma conta de serviço esteja configurada para a VM Connector.

Passos

1. Certifique-se de que o usuário do GCP que implanta o Gerenciador de nuvem do NetApp Central tenha as permissões no ["Política de implantação do Connector para GCP"](#).

["Você pode criar uma função personalizada usando o arquivo YAML"](#) e, em seguida, anexá-lo ao usuário. Você precisará usar a linha de comando gcloud para criar a função.

2. Configure uma conta de serviço que tenha as permissões necessárias para criar e gerenciar sistemas Cloud Volumes ONTAP em projetos.

Você associará essa conta de serviço à VM Connector ao criá-la a partir do Cloud Manager.

- a. ["Crie uma função no GCP"](#) isso inclui as permissões definidas no ["Política do Cloud Manager para GCP"](#). Novamente, você precisará usar a linha de comando gcloud.

As permissões contidas neste arquivo YAML são diferentes das permissões na etapa 2a.

- b. ["Crie uma conta de serviço do GCP e aplique a função personalizada que você acabou de criar"](#).
- c. Se você quiser implantar o Cloud Volumes ONTAP em outros projetos ["Conceda acesso adicionando a conta de serviço com a função Cloud Manager a esse projeto"](#), . Você precisará repetir esta etapa para cada projeto.

Resultado

O usuário do GCP agora tem as permissões necessárias para criar o conetor do Cloud Manager e a conta de serviço para a VM do conetor está configurada.

Ativação das APIs do Google Cloud

Várias APIs são necessárias para implantar o conetor e o Cloud Volumes ONTAP.

Passo

1. ["Ative as seguintes APIs do Google Cloud em seu projeto"](#).
 - API do Cloud Deployment Manager V2
 - API Cloud Logging
 - API do Cloud Resource Manager
 - API do mecanismo de computação
 - API de gerenciamento de identidade e acesso (IAM)

Criando um conetor no GCP

O Cloud Manager permite criar um conetor no GCP diretamente a partir da interface de usuário.

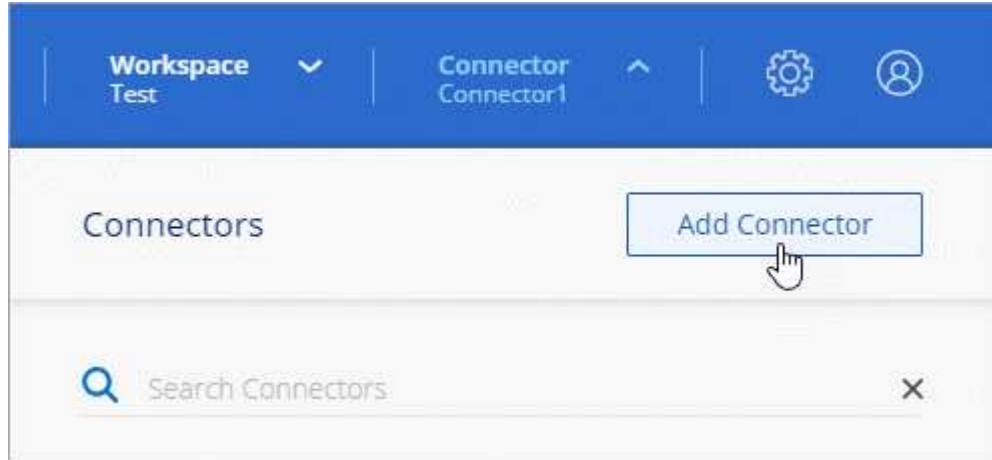
O que você vai precisar

- A ["permissões necessárias"](#) para a sua conta do Google Cloud.
- Um projeto do Google Cloud.

- Uma conta de serviço que tem as permissões necessárias para criar e gerenciar o Cloud Volumes ONTAP.
- Uma VPC e uma sub-rede na região escolhida pelo Google Cloud.

Passos

1. Se você estiver criando seu primeiro ambiente de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções. Caso contrário, clique no menu suspenso **Connector** e selecione **Add Connector**.



2. Clique em **Let's Start**.
3. Escolha **Google Cloud Platform** como seu provedor de nuvem.

Lembre-se de que o conetor deve ter uma conexão de rede com o tipo de ambiente de trabalho que você está criando e os serviços que você está planejando habilitar.

["Saiba mais sobre os requisitos de rede para o conetor"](#).

4. Revise o que você precisará e clique em **continuar**.
5. Se você for solicitado, faça login na sua conta do Google, que deve ter as permissões necessárias para criar a instância da máquina virtual.

O formulário é de propriedade e hospedado pelo Google. Suas credenciais não são fornecidas ao NetApp.

6. Forneça as informações necessárias:
 - **Configurações básicas:** Insira um nome para a instância da máquina virtual e especifique uma conta de projeto e serviço que tenha as permissões necessárias.
 - **Localização:** Especifique uma região, zona, VPC e sub-rede para a instância.
 - **Rede:** Escolha se deseja ativar um endereço IP público e, opcionalmente, especificar uma configuração de proxy.
 - **Política de firewall:** Escolha se deseja criar uma nova política de firewall ou se deseja selecionar uma política de firewall existente que permita o acesso HTTP, HTTPS e SSH de entrada.



Não há tráfego de entrada para o conetor, a menos que você o inicie. HTTP e HTTPS fornecem acesso ao "IU local", que você usará em circunstâncias raras. O SSH só é necessário se você precisar se conectar ao host para solução de problemas.

7. Clique em **criar**.

A instância deve estar pronta em cerca de 7 minutos. Você deve permanecer na página até que o processo esteja concluído.

Depois de terminar

Você precisa associar um conector aos workspaces para que os administradores do workspace possam usar esses conectores para criar sistemas Cloud Volumes ONTAP. Se você tiver apenas administradores de conta, associar o conector aos workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão. ["Saiba mais"](#).

Onde ir a seguir

Agora que você fez login e configurou o Cloud Manager, os usuários podem começar a criar e descobrir ambientes de trabalho.

- ["Comece a usar o Cloud Volumes ONTAP para AWS"](#)
- ["Comece a usar o Cloud Volumes ONTAP para Azure"](#)
- ["Comece a usar o Cloud Volumes ONTAP para Google Cloud"](#)
- ["Configure o Azure NetApp Files"](#)
- ["Configure o Cloud Volumes Service para AWS"](#)
- ["Descubra um cluster ONTAP no local"](#)
- ["Descubra seus buckets do Amazon S3"](#)

Se você for um administrador, poderá gerenciar as configurações do Cloud Manager depois de criar seu primeiro conector.

- ["Saiba mais sobre conectores"](#)
- ["Gerencie um certificado HTTPS para acesso seguro"](#)
- ["Configure as definições de proxy"](#)

Informações sobre direitos autorais

Copyright © 2024 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 INTERRUPTÃO 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 SOFTWARES, 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.