Configure um conetor

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

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 conetor se você ainda não tiver um.

Permissões

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

Permissões para criar um conetor

O usuário que cria um conetor 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 conetor.

"Veja as políticas de cada provedor de nuvem".

Permissões para a instância do conetor

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

Se você criar o conetor 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 conetores

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

Aqui estão alguns exemplos:

- Você está usando um ambiente multicloud (AWS e Azure), então você tem um conetor 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 conetores separados.

Quando alternar entre conetores

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

"Saiba como alternar entre conetores".

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 conetor. Esta interface é necessária para algumas tarefas que precisam ser executadas a partir do próprio conetor:

- "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
Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de computação elástica (EC2) • Key Management Service (KMS) • Serviço de token de segurança (STS) • Serviço de armazenamento simples (S3) O endpoint exato depende da região em que você implementa o Cloud Volumes ONTAP. "Consulte a documentação da AWS para obter detalhes."	Permite que o conetor implante e gerencie o Cloud Volumes ONTAP na AWS.
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.
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 conetor acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.

Endpoints	Finalidade
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://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Usado para adicionar seu ID de conta da AWS à lista de usuários permitidos para Backup em S3.
https://support.NetApp.com/aods/asupmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	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.
Vários locais de terceiros, por exemplo: • 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.
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 conetor 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.
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.

Endpoints	Finalidade
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.
Vários locais de terceiros, por exemplo: • 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 GCP

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

Endpoints	Finalidade
https://www.googleapis.com	Permite que o conetor 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	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.
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 conetor 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.

Endpoints	Finalidade
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.
Vários locais de terceiros, por exemplo: • 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 conetor 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 conetor 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 conetor. A máquina que executa o navegador da Web deve ter conexões com os seguintes endpoints:

Endpoints	Finalidade
O host do conetor	Você deve inserir o endereço IP do host de um navegador da Web para carregar o console do Cloud Manager. Dependendo da sua conetividade com o seu provedor de nuvem, você pode usar o IP privado ou um IP público atribuído ao host: • 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 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.
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se coneta 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 conetar 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

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

O endereço IP de origem é o host do conetor.

Serviço	Porta	Protocolo	Destino	Finalidade
Ative Directory	88	TCP	Floresta do ative Directory	Autenticação Kerberos V.
	139	TCP	Floresta do ative Directory	Sessão de serviço NetBIOS
	389	TCP	Floresta do ative Directory	LDAP
	445	TCP	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	464	TCP	Floresta do ative Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	749	TCP	Floresta do ative Directory	Palavra-passe de alteração e definição Kerberos V do ative Directory (RPCSEC_GSS)
	137	UDP	Floresta do ative Directory	Serviço de nomes NetBIOS
	138	UDP	Floresta do ative Directory	Serviço de datagrama NetBIOS
	464	UDP	Floresta do ative 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
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 ative Directory	Autenticação Kerberos V.
	TCP	139	Floresta do ative Directory	Sessão de serviço NetBIOS
	TCP	389	Floresta do ative Directory	LDAP
	TCP	445	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Floresta do ative Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	TCP	749	Floresta do ative Directory	Palavra-passe de alteração e definição Kerberos V do ative Directory (RPCSEC_GSS)
	UDP	137	Floresta do ative Directory	Serviço de nomes NetBIOS
	UDP	138	Floresta do ative Directory	Serviço de datagrama NetBIOS
	UDP	464	Floresta do ative 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 conetor 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 conetor é necessário". O conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Esta página descreve como criar um conetor na AWS diretamente do Cloud Manager. Também tem a opção de "Crie o conetor 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 conetor.

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

Configurando permissões da AWS para criar um conetor

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

Passos

1. Transfira a política do IAM do conetor 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 conetor do Cloud Manager.

Resultado

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

Criando um conetor na AWS

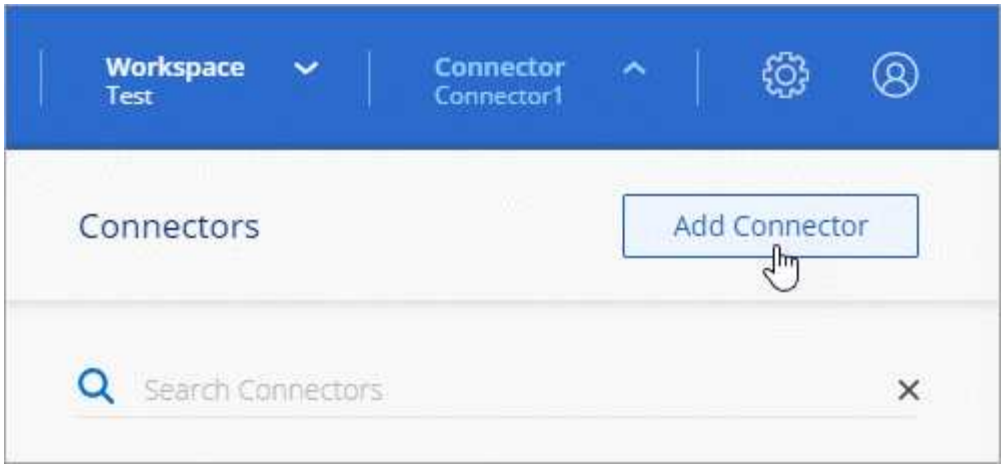
O Cloud Manager permite que você crie um conetor na AWS diretamente a partir de sua interface de usuário.

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 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. 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 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 conetar 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 conetor aos workspaces para que os administradores do workspace possam usar esses conetores para criar sistemas Cloud Volumes ONTAP. Se você tiver apenas administradores de conta, associar o conetor 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 conetor 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 conetor é necessário". O conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Esta página descreve como criar um conetor no Azure diretamente do Cloud Manager. Também tem a opção de "Crie o conetor 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 conetor.

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

Configurando permissões do Azure para criar um conetor

Antes de implantar um conetor 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 conetor:

   a. Faça download do "Política do Azure para o conetor".

      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-c25fbzzzzzzz",
      ],
      ```

   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 conetor 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 conetor do Cloud Manager.

Criando um conetor no Azure

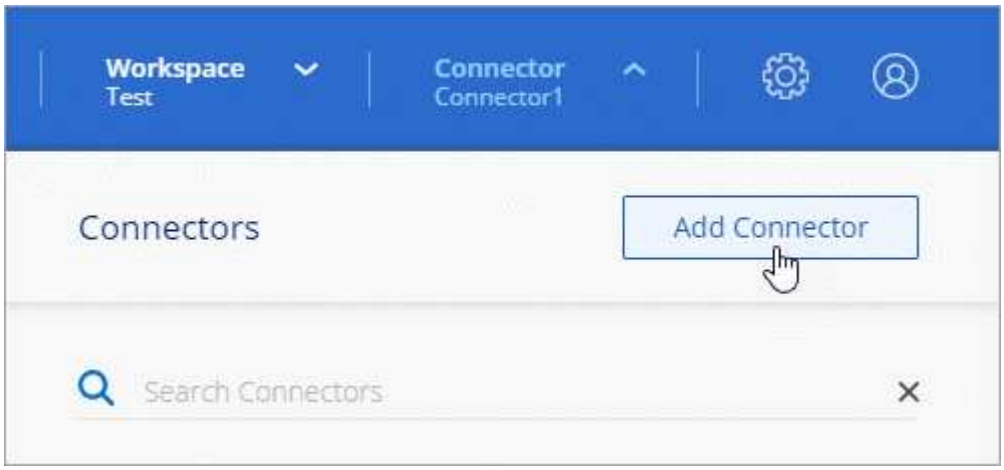
O Cloud Manager permite que você crie um conetor no Azure diretamente a partir de sua interface de usuário.

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 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 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 conetado 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 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 conetar 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 conetor aos workspaces para que os administradores do workspace possam usar esses conetores para criar sistemas Cloud Volumes ONTAP. Se você tiver apenas administradores de conta, associar o conetor 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 conetor 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 conetor é necessário". O conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Esta página descreve como criar um conetor 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 conetor.

Quando você cria seu primeiro ambiente de trabalho do Cloud Volumes ONTAP, o Cloud Manager solicitará que você crie um conetor 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

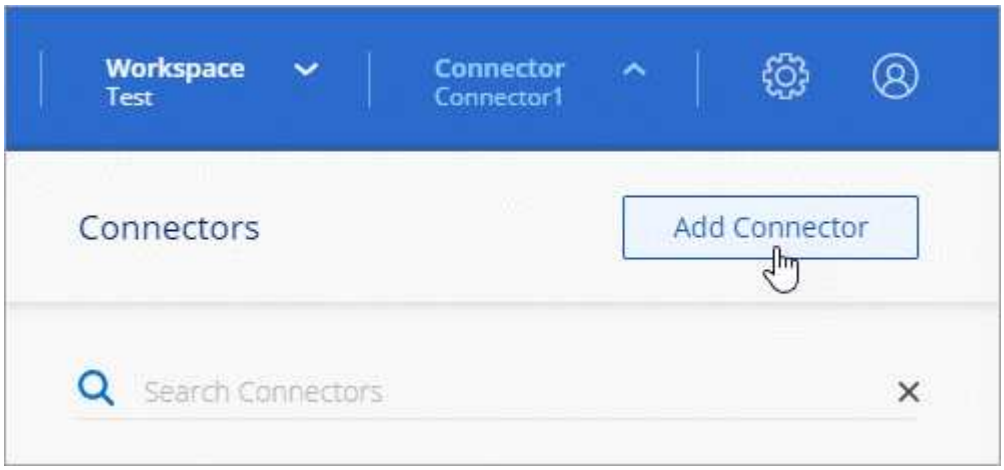
O Cloud Manager permite criar um conetor no GCP diretamente a partir da interface de usuário.

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 conetar 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 conetor aos workspaces para que os administradores do workspace possam usar esses conetores para criar sistemas Cloud Volumes ONTAP. Se você tiver apenas administradores de conta, associar o conetor 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".

Informações sobre direitos autorais

Informações sobre marcas comerciais