



Comece a usar o Google Cloud Cloud Volumes ONTAP

NetApp
February 26, 2026

Índice

Comece a usar o Google Cloud	1
Início rápido para o Cloud Volumes ONTAP no Google Cloud	1
Planeje sua configuração do Cloud Volumes ONTAP no Google Cloud	2
Escolha uma licença do Cloud Volumes ONTAP	2
Escolha uma região com suporte	2
Escolha um tipo de máquina compatível	2
Entenda os limites de armazenamento	3
Dimensione seu sistema no Google Cloud	3
Exibir discos de sistema padrão	4
Coletar informações de rede	4
Escolha uma velocidade de gravação	5
Escolha um perfil de uso de volume	5
Configurar a rede do Google Cloud para o Cloud Volumes ONTAP	6
Requisitos para o Cloud Volumes ONTAP	6
Requisitos para o agente do console	18
Configurar o VPC Service Controls para implantar o Cloud Volumes ONTAP no Google Cloud	19
Como os serviços NetApp se comunicam com os VPC Service Controls	19
Imagens	19
Políticas de perímetro do VPC Service Controls	20
Crie uma conta de serviço do Google Cloud para o Cloud Volumes ONTAP	21
Usando chaves de criptografia gerenciadas pelo cliente com o Cloud Volumes ONTAP	24
Configurar o licenciamento do Cloud Volumes ONTAP no Google Cloud	25
Freemium	25
Licença baseada em capacidade	26
Assinatura Keystone	29
Licença baseada em nó	30
Inicie o Cloud Volumes ONTAP no Google Cloud	30
Antes de começar	30
Inicie um sistema de nó único no Google Cloud	31
Inicie um par de HA no Google Cloud	37
Verificação de imagem da plataforma Google Cloud	43
Saiba como a imagem do Google Cloud é verificada no Cloud Volumes ONTAP	43
Converter imagem do Google Cloud para formato bruto para Cloud Volumes ONTAP	44
Verificação de assinatura de imagem	49

Comece a usar o Google Cloud

Início rápido para o Cloud Volumes ONTAP no Google Cloud

Comece a usar o Cloud Volumes ONTAP no Google Cloud em poucas etapas.

1

Criar um agente de console

Se você não tiver um ["Agente de console"](#) No entanto, você precisa criar um. ["Aprenda a criar um agente de console no Google Cloud"](#)

Observe que se você quiser implantar o Cloud Volumes ONTAP em uma sub-rede onde não há acesso à Internet disponível, será necessário instalar manualmente o agente do Console e acessar o NetApp Console que está em execução nesse agente do Console. ["Aprenda a instalar manualmente o agente do Console em um local sem acesso à Internet"](#)

2

Planeje sua configuração

O Console oferece pacotes pré-configurados que correspondem aos seus requisitos de carga de trabalho, ou você pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis.

["Saiba mais sobre o planejamento de sua configuração"](#) .

3

Configure sua rede

1. Certifique-se de que sua VPC e sub-redes oferecerão suporte à conectividade entre o agente do Console e o Cloud Volumes ONTAP.
2. Se você planeja habilitar a hierarquização de dados, ["configurar a sub-rede Cloud Volumes ONTAP para acesso privado do Google"](#) .
3. Se você estiver implantando um par de HA, certifique-se de ter quatro VPCs, cada uma com sua própria sub-rede.
4. Se você estiver usando uma VPC compartilhada, forneça a função *Usuário da rede de computação* à conta de serviço do agente do console.
5. Habilite o acesso de saída à Internet da VPC de destino para o NetApp AutoSupport.

Esta etapa não é necessária se você estiver implantando o Cloud Volumes ONTAP em um local onde não há acesso à Internet disponível.

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

4

Configurar uma conta de serviço

O Cloud Volumes ONTAP requer uma conta de serviço do Google Cloud para duas finalidades. A primeira é quando você habilita ["hierarquização de dados"](#) para hierarquizar dados frios para armazenamento de objetos de baixo custo no Google Cloud. A segunda é quando você habilita o ["NetApp Backup and Recovery"](#) para

fazer backup de volumes em armazenamento de objetos de baixo custo.

Você pode configurar uma conta de serviço e usá-la para ambas as finalidades. A conta de serviço deve ter a função **Administrador de armazenamento**.

["Leia as instruções passo a passo"](#) .

5

Habilitar APIs do Google Cloud

["Habilite as APIs do Google Cloud em seu projeto"](#). ["Essas APIs"](#), que você talvez já tenha habilitado ao criar o agente do Console, são necessários para implantar Cloud Volumes ONTAP no Google Cloud.

6

Inicie o Cloud Volumes ONTAP usando o Console

Clique em **Adicionar Sistema**, selecione o tipo de sistema que você gostaria de implantar e conclua as etapas do assistente. ["Leia as instruções passo a passo"](#) .

Links relacionados

- ["Criando um agente de console"](#)
- ["Instalando o software do agente do Console em um host Linux"](#)
- ["Permissões do Google Cloud para o agente do Console"](#)

Planeje sua configuração do Cloud Volumes ONTAP no Google Cloud

Ao implantar o Cloud Volumes ONTAP no Google Cloud, você pode escolher um sistema pré-configurado que corresponda aos seus requisitos de carga de trabalho ou pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis.

Escolha uma licença do Cloud Volumes ONTAP

Várias opções de licenciamento estão disponíveis para o Cloud Volumes ONTAP. Cada opção permite que você escolha um modelo de consumo que atenda às suas necessidades.

- ["Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"](#)
- ["Aprenda como configurar o licenciamento"](#)

Escolha uma região com suporte

O Cloud Volumes ONTAP é compatível com a maioria das regiões do Google Cloud. ["Veja a lista completa de regiões suportadas"](#) .

Escolha um tipo de máquina compatível

O Cloud Volumes ONTAP oferece suporte a vários tipos de máquinas, dependendo do tipo de licença escolhido.

["Configurações suportadas para Cloud Volumes ONTAP no Google Cloud"](#)

Entenda os limites de armazenamento

O limite de capacidade bruta para um sistema Cloud Volumes ONTAP está vinculado à licença. Limites adicionais afetam o tamanho dos agregados e volumes. Você deve estar ciente desses limites ao planejar sua configuração.

["Limites de armazenamento para Cloud Volumes ONTAP no Google Cloud"](#)

Dimensione seu sistema no Google Cloud

Dimensionar seu sistema Cloud Volumes ONTAP pode ajudar você a atender aos requisitos de desempenho e capacidade. Você deve estar ciente de alguns pontos-chave ao escolher um tipo de máquina, tipo de disco e tamanho de disco:

Tipo de máquina

Veja os tipos de máquinas suportados em ["Notas de versão do Cloud Volumes ONTAP"](#) Em seguida, consulte os detalhes do Google sobre cada tipo de máquina compatível. Adapte seus requisitos de carga de trabalho ao número de vCPUs e memória para o tipo de máquina. Observe que cada núcleo da CPU aumenta o desempenho da rede.

Consulte o seguinte para mais detalhes:

- ["Documentação do Google Cloud: tipos de máquinas padrão N1"](#)
- ["Documentação do Google Cloud: Desempenho"](#)

Tipos de disco

Ao criar volumes para o Cloud Volumes ONTAP, você precisa escolher o armazenamento em nuvem subjacente que o Cloud Volumes ONTAP usa para um disco. O tipo de disco pode ser qualquer um dos seguintes:

- *Discos persistentes SSD zonais*: discos persistentes SSD são melhores para cargas de trabalho que exigem altas taxas de IOPS aleatórios.
- *Discos persistentes zonais balanceados*: Esses SSDs equilibram desempenho e custo ao fornecer IOPS mais baixos por GB.
- *Discos persistentes padrão zonais*: os discos persistentes padrão são econômicos e podem lidar com operações sequenciais de leitura/gravação.

Para mais detalhes, consulte o ["Documentação do Google Cloud: Discos permanentes zonais \(padrão e SSD\)"](#).

Tamanho do disco

Você precisa escolher um tamanho de disco inicial ao implantar um sistema Cloud Volumes ONTAP. Depois disso, você pode deixar que o NetApp Console gerencie a capacidade de um sistema para você, mas se quiser criar agregados sozinho, esteja ciente do seguinte:

- Todos os discos em um agregado devem ter o mesmo tamanho.
- Determine o espaço que você precisa, levando em consideração o desempenho.
- O desempenho dos discos persistentes é dimensionado automaticamente com o tamanho do disco e o número de vCPUs disponíveis para o sistema.

Consulte o seguinte para mais detalhes:

- ["Documentação do Google Cloud: Discos permanentes zonais \(padrão e SSD\)"](#)
- ["Documentação do Google Cloud: Otimizando o desempenho do disco permanente e do SSD local"](#)

Exibir discos de sistema padrão

Além do armazenamento para dados do usuário, o Console também adquire armazenamento em nuvem para dados do sistema Cloud Volumes ONTAP (dados de inicialização, dados raiz, dados principais e NVRAM). Para fins de planejamento, pode ser útil revisar esses detalhes antes de implantar o Cloud Volumes ONTAP.

- ["Visualize os discos padrão para dados do sistema Cloud Volumes ONTAP no Google Cloud"](#) .
- ["Documentação do Google Cloud: Visão geral das quotas de nuvem"](#)

O Google Cloud Compute Engine impõe cotas no uso de recursos, portanto, você deve garantir que não atingiu seu limite antes de implantar o Cloud Volumes ONTAP.



O agente do Console também requer um disco do sistema. ["Exibir detalhes sobre a configuração padrão do agente do Console"](#) .

Coletar informações de rede

Ao implantar Cloud Volumes ONTAP no Google Cloud, você precisa especificar detalhes sobre sua rede virtual. Você pode usar uma planilha para coletar informações do seu administrador.

Informações de rede para um sistema de nó único

Informações do Google Cloud	Seu valor
Região	
Zona	
Rede VPC	
Sub-rede	
Política de firewall (se estiver usando a sua própria)	

Informações de rede para um par HA em várias zonas

Informações do Google Cloud	Seu valor
Região	
Zona para Nó 1	
Zona para o Nó 2	
Zona para o mediador	
VPC-0 e sub-rede	
VPC-1 e sub-rede	

Informações do Google Cloud	Seu valor
VPC-2 e sub-rede	
VPC-3 e sub-rede	
Política de firewall (se estiver usando a sua própria)	

Informações de rede para um par HA em uma única zona

Informações do Google Cloud	Seu valor
Região	
Zona	
VPC-0 e sub-rede	
VPC-1 e sub-rede	
VPC-2 e sub-rede	
VPC-3 e sub-rede	
Política de firewall (se estiver usando a sua própria)	

Escolha uma velocidade de gravação

O Console permite que você escolha uma configuração de velocidade de gravação para o Cloud Volumes ONTAP, exceto para pares de alta disponibilidade (HA) no Google Cloud. Antes de escolher uma velocidade de gravação, você deve entender as diferenças entre as configurações normal e alta, bem como os riscos e recomendações ao usar alta velocidade de gravação. ["Saiba mais sobre velocidade de gravação"](#) .

Escolha um perfil de uso de volume

O ONTAP inclui vários recursos de eficiência de armazenamento que podem reduzir a quantidade total de armazenamento necessária. Ao criar um volume no Console, você pode escolher um perfil que habilite esses recursos ou um perfil que os desabilite. Você deve aprender mais sobre esses recursos para ajudar a decidir qual perfil usar.

Os recursos de eficiência de armazenamento da NetApp oferecem os seguintes benefícios:

Provisionamento fino

Apresenta mais armazenamento lógico para hosts ou usuários do que você realmente tem em seu pool de armazenamento físico. Em vez de pré-alocar espaço de armazenamento, o espaço de armazenamento é alocado dinamicamente para cada volume à medida que os dados são gravados.

Desduplicação

Melhora a eficiência localizando blocos idênticos de dados e substituindo-os por referências a um único bloco compartilhado. Essa técnica reduz os requisitos de capacidade de armazenamento eliminando blocos redundantes de dados que residem no mesmo volume.

Compressão

Reduz a capacidade física necessária para armazenar dados compactando dados dentro de um volume no armazenamento primário, secundário e de arquivo.

Configurar a rede do Google Cloud para o Cloud Volumes ONTAP

O NetApp Console gerencia a configuração de componentes de rede para o Cloud Volumes ONTAP, como endereços IP, máscaras de rede e rotas. Você precisa ter certeza de que o acesso de saída à Internet esteja disponível, que endereços IP privados suficientes estejam disponíveis, que as conexões corretas estejam em vigor e muito mais.

Se você deseja implantar um par de HA, você deve "[saiba como os pares de HA funcionam no Google Cloud](#)".

Requisitos para o Cloud Volumes ONTAP

Os seguintes requisitos devem ser atendidos no Google Cloud.

Requisitos específicos para sistemas de nó único

Se você deseja implantar um sistema de nó único, certifique-se de que sua rede atenda aos seguintes requisitos.

Uma VPC

É necessária uma Virtual Private Cloud (VPC) para um sistema de nó único.

Endereços IP privados

Para um sistema de nó único no Google Cloud, o Console aloca endereços IP privados para o seguinte:

- Nó
- Conjunto
- VM de armazenamento
- Dados NAS LIF
- Dados iSCSI LIF

Você pode pular a criação do LIF de gerenciamento da VM de armazenamento (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```



Um LIF é um endereço IP associado a uma porta física. Um LIF de gerenciamento de VM de armazenamento (SVM) é necessário para ferramentas de gerenciamento como o SnapCenter.

Requisitos específicos para pares HA

Se você quiser implantar um par HA, certifique-se de que sua rede atenda aos seguintes requisitos.

Uma ou várias zonas

Você pode garantir a alta disponibilidade dos seus dados implantando uma configuração de HA em várias zonas ou em uma única zona. O Console solicita que você escolha várias zonas ou uma única zona ao criar o par HA.

- Várias zonas (recomendado)

A implantação de uma configuração de HA em três zonas garante disponibilidade contínua de dados caso ocorra uma falha em uma zona. Observe que o desempenho de gravação é um pouco menor quando comparado ao uso de uma única zona, mas é mínimo.

- Zona única

Quando implantada em uma única zona, uma configuração do Cloud Volumes ONTAP HA usa uma política de posicionamento espalhado. Esta política garante que uma configuração de HA seja protegida de um único ponto de falha dentro da zona, sem precisar usar zonas separadas para obter isolamento de falhas.

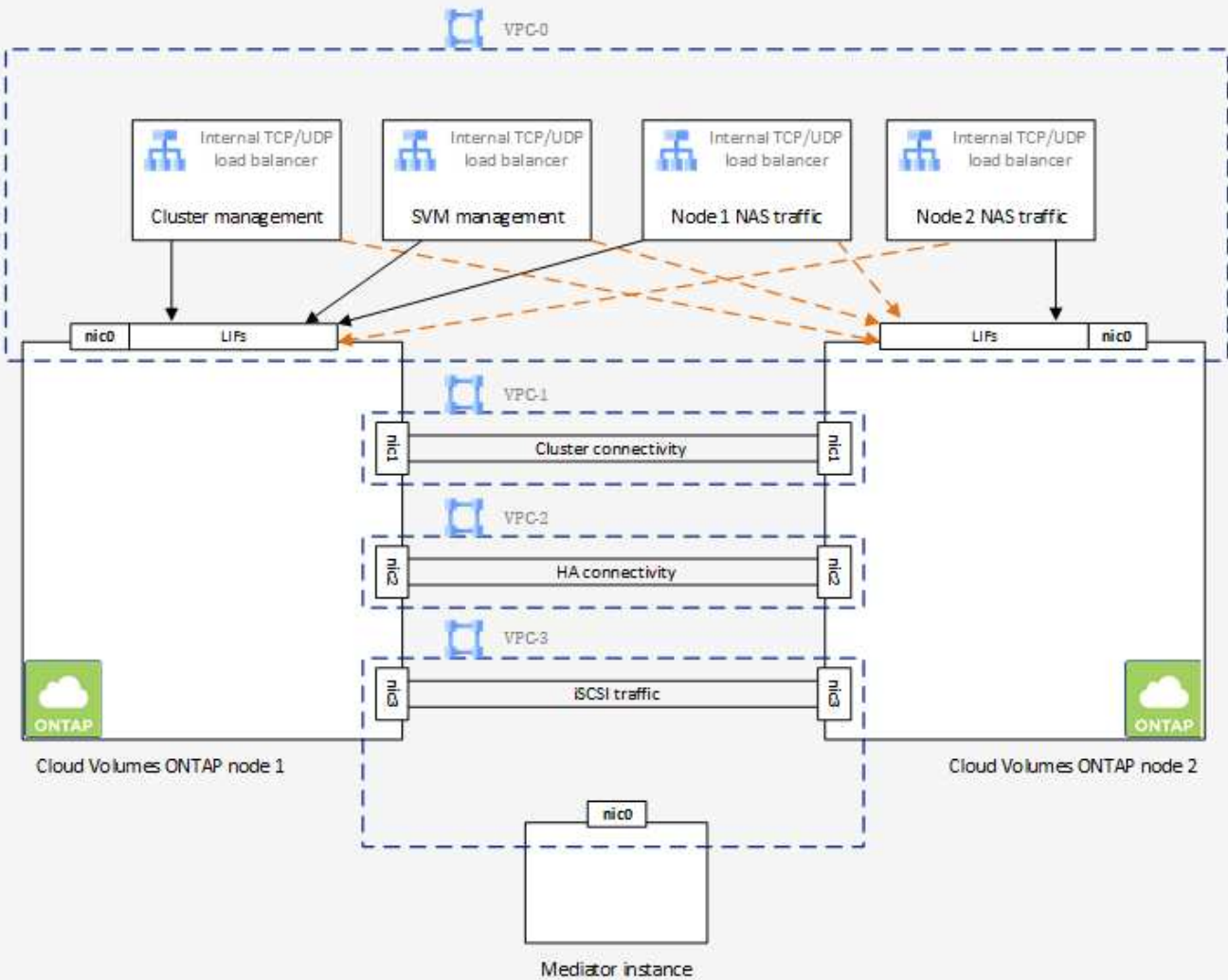
Este modelo de implantação reduz seus custos porque não há cobranças de saída de dados entre zonas.

Quatro Nuvens Privadas Virtuais

Quatro Nuvens Privadas Virtuais (VPCs) são necessárias para uma configuração de HA. Quatro VPCs são necessárias porque o Google Cloud exige que cada interface de rede resida em uma rede VPC separada.

O Console solicita que você escolha quatro VPCs ao criar o par HA:

- VPC-0 para conexões de entrada aos dados e nós
- VPC-1, VPC-2 e VPC-3 para comunicação interna entre os nós e o mediador HA



Sub-redes

Uma sub-rede privada é necessária para cada VPC.

Se você colocar o agente do Console no VPC-0, precisará habilitar o Private Google Access na sub-rede para acessar as APIs e habilitar a hierarquização de dados.

As sub-redes nessas VPCs devem ter intervalos CIDR distintos. Eles não podem ter intervalos CIDR sobrepostos.

Endereços IP privados

O Console aloca automaticamente o número necessário de endereços IP privados para o Cloud Volumes ONTAP no Google Cloud. Você precisa ter certeza de que sua rede tem endereços privados suficientes disponíveis.

O número de LIFs alocados para Cloud Volumes ONTAP depende se você implanta um sistema de nó único ou um par de HA. Uma LIF é um endereço IP associado a uma porta física. Uma LIF de gerenciamento de SVM é necessária para ferramentas de gerenciamento como SnapCenter.

- **Nó único** O Console aloca 4 endereços IP para um sistema de nó único:

- Gerenciamento de nós LIF
- Gerenciamento de cluster LIF
- Dados iSCSI LIF



Um iSCSI LIF fornece acesso de cliente pelo protocolo iSCSI e é usado pelo sistema para outros fluxos de trabalho de rede importantes. Esses LIFs são necessários e não devem ser excluídos.

- NAS LIF

Você pode pular a criação do LIF de gerenciamento da VM de armazenamento (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```

• **Par HA** O Console aloca 12-13 endereços IP para um par HA:

- 2 LIFs de gerenciamento de nós (e0a)
- 1 Gerenciamento de cluster LIF (e0a)
- 2 iSCSI LIFs (e0a)



Um iSCSI LIF fornece acesso de cliente pelo protocolo iSCSI e é usado pelo sistema para outros fluxos de trabalho de rede importantes. Esses LIFs são necessários e não devem ser excluídos.

- 1 ou 2 NAS LIFs (e0a)
- 2 LIFs de cluster (e0b)
- 2 endereços IP de interconexão HA (e0c)
- 2 endereços IP iSCSI RSM (e0d)

Você pode pular a criação do LIF de gerenciamento da VM de armazenamento (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```

Balancedores de carga internos

O Console cria quatro balanceadores de carga internos do Google Cloud (TCP/UDP) que gerenciam o tráfego de entrada para o par Cloud Volumes ONTAP HA. Nenhuma configuração é necessária da sua parte. Listamos isso como um requisito simplesmente para informá-lo sobre o tráfego de rede e para atenuar quaisquer preocupações de segurança.

Um balanceador de carga é para gerenciamento de cluster, um é para gerenciamento de VM de armazenamento (SVM), um é para tráfego NAS para o nó 1 e o último é para tráfego NAS para o nó 2.

A configuração para cada balanceador de carga é a seguinte:

- Um endereço IP privado compartilhado
- Um exame de saúde global

Por padrão, as portas usadas pela verificação de integridade são 63001, 63002 e 63003.

- Um serviço regional de backend TCP
- Um serviço regional de backend UDP
- Uma regra de encaminhamento TCP
- Uma regra de encaminhamento UDP
- O acesso global está desabilitado

Embora o acesso global esteja desabilitado por padrão, há suporte para habilitá-lo após a implantação. Nós o desabilitamos porque o tráfego entre regiões terá latências significativamente maiores. Queríamos garantir que você não tivesse uma experiência negativa devido a montagens acidentais entre regiões. A ativação desta opção é específica para as necessidades do seu negócio.

VPCs compartilhadas

O Cloud Volumes ONTAP e o agente do Console são suportados em uma VPC compartilhada do Google Cloud e também em VPCs autônomas.

Para um sistema de nó único, a VPC pode ser uma VPC compartilhada ou uma VPC independente.

Para um par HA, são necessárias quatro VPCs. Cada uma dessas VPCs pode ser compartilhada ou independente. Por exemplo, VPC-0 pode ser uma VPC compartilhada, enquanto VPC-1, VPC-2 e VPC-3 podem ser VPCs independentes.

Uma VPC compartilhada permite que você configure e gerencie centralmente redes virtuais em vários projetos. Você pode configurar redes VPC compartilhadas no *projeto host* e implantar o agente do Console e as instâncias da máquina virtual Cloud Volumes ONTAP em um *projeto de serviço*.

["Documentação do Google Cloud: Visão geral da VPC compartilhada"](#) .

["Revise as permissões de VPC compartilhadas necessárias abordadas na implantação do agente do Console"](#)

Espelhamento de pacotes em VPCs

["Espelhamento de pacotes"](#) deve ser desabilitado na sub-rede do Google Cloud na qual você implanta o Cloud Volumes ONTAP.

Acesso de saída à Internet

Os sistemas Cloud Volumes ONTAP exigem acesso de saída à Internet para acessar endpoints externos para diversas funções. O Cloud Volumes ONTAP não poderá operar corretamente se esses endpoints estiverem bloqueados em ambientes com requisitos de segurança rigorosos.

O agente do Console também entra em contato com vários endpoints para operações diárias. Para obter informações sobre os pontos de extremidade, consulte ["Exibir endpoints contatados pelo agente do Console"](#) e ["Preparar a rede para usar o Console"](#) .

Pontos de extremidade Cloud Volumes ONTAP

O Cloud Volumes ONTAP usa esses endpoints para se comunicar com vários serviços.

Pontos finais	Aplicável para	Propósito	Modo de implantação	Impacto se o ponto final não estiver disponível
\ https://netapp-cloud-account.auth0.com	Autenticação	Usado para autenticação no Console.	Modos padrão e restrito.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: <ul style="list-style-type: none"> • Serviços Cloud Volumes ONTAP • Serviços ONTAP • Protocolos e serviços de proxy
\ https://api.bluexp.netapp.com/tenancy	Arrendamento	Usado para recuperar o recurso Cloud Volumes ONTAP do Console para autorizar recursos e usuários.	Modos padrão e restrito.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte da NetApp .	Modos padrão e restrito.	As informações do AutoSupport continuam não entregues.

Pontos finais	Aplicável para	Propósito	Modo de implantação	Impacto se o ponto final não estiver disponível
https://cloudbuild.googleapis.com/v1 (somente para implantações em modo privado) https://cloudkms.googleapis.com/v1 https://cloudresource-manager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud (uso comercial).	Comunicação com os serviços do Google Cloud.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço Google Cloud para executar operações específicas para o Console no Google Cloud.

Conexões com sistemas ONTAP em outras redes

Para replicar dados entre um sistema Cloud Volumes ONTAP no Google Cloud e sistemas ONTAP em outras redes, você deve ter uma conexão VPN entre a VPC e a outra rede, por exemplo, sua rede corporativa.

"[Documentação do Google Cloud: Visão geral do Cloud VPN](#)".

Regras de firewall

O Console cria regras de firewall do Google Cloud que incluem as regras de entrada e saída que o Cloud Volumes ONTAP precisa para operar com sucesso. Talvez você queira consultar as portas para fins de teste ou, se preferir, usar suas próprias regras de firewall.

As regras de firewall para o Cloud Volumes ONTAP exigem regras de entrada e saída. Se você estiver

implantando uma configuração de HA, estas são as regras de firewall para o Cloud Volumes ONTAP no VPC-0.

Observe que dois conjuntos de regras de firewall são necessários para uma configuração de HA:

- Um conjunto de regras para componentes HA no VPC-0. Essas regras permitem o acesso aos dados do Cloud Volumes ONTAP.
- Outro conjunto de regras para componentes HA em VPC-1, VPC-2 e VPC-3. Essas regras estão abertas para comunicação de entrada e saída entre os componentes do HA. [Saber mais](#) .



Procurando informações sobre o agente do Console? ["Exibir regras de firewall para o agente do Console"](#)

Regras de entrada

Ao adicionar um sistema Cloud Volumes ONTAP , você pode escolher o filtro de origem para a política de firewall predefinida durante a implantação:

- **Somente VPC selecionada:** o filtro de origem para tráfego de entrada é o intervalo de sub-rede da VPC para o sistema Cloud Volumes ONTAP e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada.
- **Todas as VPCs:** o filtro de origem para tráfego de entrada é o intervalo de IP 0.0.0.0/0.

Se você usar sua própria política de firewall, certifique-se de adicionar todas as redes que precisam se comunicar com o Cloud Volumes ONTAP, mas também certifique-se de adicionar ambos os intervalos de endereços para permitir que o Google Load Balancer interno funcione corretamente. Esses endereços são 130.211.0.0/22 e 35.191.0.0/16. Para mais informações, consulte o ["Documentação do Google Cloud: Regras de firewall do balanceador de carga"](#) .

Protocolo	Porta	Propósito
Todos os ICMP	Todos	Executando ping na instância
HTTP	80	Acesso HTTP ao console da web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
HTTPS	443	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó
TCP	111	Chamada de procedimento remoto para NFS
TCP	139	Sessão de serviço NetBIOS para CIFS
TCP	161-162	Protocolo simples de gerenciamento de rede
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	635	Montagem NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS

Protocolo	Porta	Propósito
TCP	3260	Acesso iSCSI através do LIF de dados iSCSI
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status de rede para NFS
TCP	10000	Backup usando NDMP
TCP	11104	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Transferência de dados do SnapMirror usando LIFs intercluster
TCP	63001-63050	Portas de sondagem de balanceamento de carga para determinar qual nó está íntegro (necessário apenas para pares de HA)
UDP	111	Chamada de procedimento remoto para NFS
UDP	161-162	Protocolo simples de gerenciamento de rede
UDP	635	Montagem NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status de rede para NFS
UDP	4049	Protocolo NFS rquotad

Regras de saída

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

Regras básicas de saída

O grupo de segurança predefinido para o Cloud Volumes ONTAP inclui as seguintes regras de saída.

Protocolo	Porta	Propósito
Todos os ICMP	Todos	Todo o tráfego de saída
Todos os TCP	Todos	Todo o tráfego de saída
Todos os UDP	Todos	Todo o tráfego de saída

Regras avançadas de saída

Se 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 Cloud Volumes ONTAP. Os clusters Cloud Volumes ONTAP usam as seguintes portas para regular o tráfego de nós.



A origem é a interface (endereço IP) do sistema Cloud Volumes ONTAP .

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
Diretório ativo	TCP	88	Gerenciamento de nós LIF	Floresta do Active Directory	Autenticação Kerberos V
	UDP	137	Gerenciamento de nós LIF	Floresta do Active Directory	Serviço de nomes NetBIOS
	UDP	138	Gerenciamento de nós LIF	Floresta do Active Directory	Serviço de datagrama NetBIOS
	TCP	139	Gerenciamento de nós LIF	Floresta do Active Directory	Sessão de serviço NetBIOS
	TCP e UDP	389	Gerenciamento de nós LIF	Floresta do Active Directory	LDAP
	TCP	445	Gerenciamento de nós LIF	Floresta do Active Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Gerenciamento de nós LIF	Floresta do Active Directory	Alteração e definição de senha do Kerberos V (SET_CHANGE)
	UDP	464	Gerenciamento de nós LIF	Floresta do Active Directory	Administração de chaves Kerberos
	TCP	749	Gerenciamento de nós LIF	Floresta do Active Directory	Kerberos V alterar e definir senha (RPCSEC_GSS)
	TCP	88	Dados LIF (NFS, CIFS, iSCSI)	Floresta do Active Directory	Autenticação Kerberos V
	UDP	137	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Serviço de nomes NetBIOS
	UDP	138	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Serviço de datagrama NetBIOS
	TCP	139	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Sessão de serviço NetBIOS
	TCP e UDP	389	Dados LIF (NFS, CIFS)	Floresta do Active Directory	LDAP
	TCP	445	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Alteração e definição de senha do Kerberos V (SET_CHANGE)
	UDP	464	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Administração de chaves Kerberos
	TCP	749	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Alterar e definir senha do Kerberos V (RPCSEC_GSS)

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
AutoSupport	HTTPS	443	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (HTTPS é o padrão)
	HTTP	80	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)
	TCP	3128	Gerenciamento de nós LIF	Agente de console	Envio de mensagens do AutoSupport por meio de um servidor proxy no agente do Console, se uma conexão de saída com a Internet não estiver disponível
Backups de configuração	HTTP	80	Gerenciamento de nós LIF	http://<endereço-IP-do-agente-do-console>/occm/offboxconfig	Envie backups de configuração para o agente do Console. " Documentação do ONTAP "
DHCP	UDP	68	Gerenciamento de nós LIF	DHCP	Cliente DHCP para configuração inicial
DHCPS	UDP	67	Gerenciamento de nós LIF	DHCP	Servidor DHCP
DNS	UDP	53	Gerenciamento de nós LIF e dados LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	Gerenciamento de nós LIF	Servidores de destino	Cópia do NDMP
SMTP	TCP	25	Gerenciamento de nós LIF	Servidor de e-mail	Alertas SMTP podem ser usados para AutoSupport
SNMP	TCP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	TCP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
SnapMirror	TCP	11104	LIF interaglomerado	LIFs interaglomerados ONTAP	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF interaglomerado	LIFs interaglomerados ONTAP	Transferência de dados do SnapMirror

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
Log de sistema	UDP	514	Gerenciamento de nós LIF	Servidor Syslog	Mensagens de encaminhamento do Syslog

Regras para VPC-1, VPC-2 e VPC-3

No Google Cloud, uma configuração de HA é implantada em quatro VPCs. As regras de firewall necessárias para a configuração de HA no VPC-0 são [listado acima para Cloud Volumes ONTAP](#).

Enquanto isso, as regras de firewall predefinidas criadas para as instâncias em VPC-1, VPC-2 e VPC-3 permitem a comunicação de entrada em *todos* os protocolos e portas. Essas regras permitem a comunicação entre nós de HA.

A comunicação dos nós HA com o mediador HA ocorre pela porta 3260 (iSCSI).



Para habilitar alta velocidade de gravação para novas implantações de pares de HA do Google Cloud, uma unidade máxima de transmissão (MTU) de pelo menos 8.896 bytes é necessária para VPC-1, VPC-2 e VPC-3. Se você optar por atualizar as VPC-1, VPC-2 e VPC-3 existentes para uma MTU de 8.896 bytes, deverá desligar todos os sistemas HA existentes que usam essas VPCs durante o processo de configuração.

Configuração do Infrastructure Manager para implantações em modo privado

Se você deseja implantar Cloud Volumes ONTAP 9.16.1 ou posterior no modo privado, precisa fazer algumas alterações de configuração para que Cloud Volumes ONTAP possa usar Google Cloud Infrastructure Manager como serviço de implantação em vez de Deployment Manager, que Google eventualmente descontinuará.

Antes de começar

- Certifique-se de que seu sistema Cloud Volumes ONTAP esteja na versão 9.16.1 ou posterior. Se não estiver, atualize seu sistema. Consulte ["Atualizar Cloud Volumes ONTAP"](#) para obter instruções.
- Certifique-se de que as APIs do Google Cloud estejam ativadas. Consulte ["Ativar APIs do Google Cloud"](#).
- Certifique-se de que a API Cloud Build esteja ativada. Consulte ["Ative a API Cloud Build aqui"](#).
- Verifique se a conta de serviço do agente do Console possui todas as permissões padrão. Além disso, certifique-se de que a conta de serviço tenha as `cloudbuild.workerpools.get` e `cloudbuild.workerpools.list` permissões. Consulte ["Permissões do Google Cloud para o agente do Console"](#).

Passos

1. Crie um pool de workers privado com essa configuração na mesma região das implantações do Cloud Volumes ONTAP. Para obter informações sobre como criar um pool de workers privado, consulte ["Documentação do Google Cloud: criar e gerenciar pools privados"](#) e ["Preços do Google Cloud Build"](#).

O pool de trabalhadores deve ter a seguinte configuração:

- Tipo de máquina: e2-medium
- Tamanho do disco: 100 GB
- Atribuir IP externo: false
- Rede: padrão ou privada.

- A sub-rede configurada para acessar ["APIs do Google"](#). Execute estas etapas para garantir que a sub-rede possa acessar as APIs do Google:
 - i. Certifique-se de que o "Acesso privado do Google" esteja ativado para a subnet.
 - ii. Acesse **VPC Network level > Aba Private Service Access > Allocated IP ranges for services**.
 - iii. Selecione **Allocate IP range** e aloque o intervalo de IP interno para a conexão privada com o Google Compute Service.
 - iv. Em **Conexão privada com serviços**, selecione **Criar conexão**.
 - v. Selecione **Connected service producer = Google Cloud Platform**.
 - vi. Atribua a alocação para o intervalo de IP de conexão privada que você criou na etapa anterior.
- 2. Implante esse pool de workers e mantenha-o em execução para o gerenciamento do Cloud Volumes ONTAP. O Google Cloud usa esse pool de workers para executar todas as operações do Terraform em um ambiente isolado.
- 3. Ao implantar Cloud Volumes ONTAP no modo privado, selecione o nome deste pool de workers no campo **GCP Worker Pool**. Consulte ["Inicie o Cloud Volumes ONTAP no Google Cloud"](#) para obter instruções.

Requisitos para o agente do console

Se você ainda não criou um agente do Console, revise os requisitos de rede.

- ["Exibir requisitos de rede para o agente do Console"](#)
- ["Regras de firewall no Google Cloud"](#)

Configurações de rede para oferecer suporte ao proxy do agente do console

Você pode usar os servidores proxy configurados para o agente do Console para habilitar o acesso de saída à Internet do Cloud Volumes ONTAP. O Console suporta dois tipos de proxies:

- **Proxy explícito:** O tráfego de saída do Cloud Volumes ONTAP usa o endereço HTTP do servidor proxy especificado durante a configuração do proxy do agente do Console. O administrador do agente do Console também pode ter configurado credenciais de usuário e certificados de CA raiz para autenticação adicional. Se um certificado de CA raiz estiver disponível para o proxy explícito, certifique-se de obter e carregar o mesmo certificado para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.
- **Proxy transparente:** A rede está configurada para rotear automaticamente o tráfego de saída do Cloud Volumes ONTAP por meio do proxy do agente do Console. Ao configurar um proxy transparente, o administrador do agente do Console precisa fornecer apenas um certificado de CA raiz para conectividade do Cloud Volumes ONTAP, não o endereço HTTP do servidor proxy. Certifique-se de obter e carregar o mesmo certificado de CA raiz para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.

Para obter informações sobre como configurar servidores proxy para o agente do Console, consulte o ["Configurar um agente de console para usar um servidor proxy"](#) .

Configurar tags de rede para o Cloud Volumes ONTAP no Google Cloud

Durante a configuração do proxy transparente do agente do Console, o administrador adiciona uma tag de rede para o Google Cloud. Você precisa obter e adicionar manualmente a mesma tag de rede para sua configuração do Cloud Volumes ONTAP . Esta tag é necessária para que o servidor proxy funcione corretamente.

1. No Console do Google Cloud, localize seu sistema Cloud Volumes ONTAP.
2. Vá para **Detalhes > Rede > Tags de rede**.
3. Adicione a tag usada para o agente do Console e salve a configuração.

Tópicos relacionados

- ["Verifique a configuração do AutoSupport para o Cloud Volumes ONTAP"](#)
- ["Saiba mais sobre as portas internas do ONTAP"](#) .

Configurar o VPC Service Controls para implantar o Cloud Volumes ONTAP no Google Cloud

Ao escolher bloquear seu ambiente do Google Cloud com o VPC Service Controls, você deve entender como o NetApp Console e o Cloud Volumes ONTAP interagem com as APIs do Google Cloud, bem como configurar seu perímetro de serviço para implantar o Console e o Cloud Volumes ONTAP.

Os Controles de Serviço VPC permitem que você controle o acesso a serviços gerenciados pelo Google fora de um perímetro confiável, bloqueie o acesso a dados de locais não confiáveis e mitigue riscos de transferência de dados não autorizada. ["Saiba mais sobre os controles de serviço VPC do Google Cloud"](#) .

Como os serviços NetApp se comunicam com os VPC Service Controls

O Console se comunica diretamente com as APIs do Google Cloud. Isso é acionado por um endereço IP externo fora do Google Cloud (por exemplo, de `api.services.cloud.netapp.com`) ou dentro do Google Cloud a partir de um endereço interno atribuído ao agente do Console.

Dependendo do estilo de implantação do agente do Console, certas exceções podem ter que ser feitas para seu perímetro de serviço.

Imagens

Tanto Cloud Volumes ONTAP quanto o Console usam imagens de um projeto no Google Cloud que é gerenciado pela NetApp. Isso pode afetar a implantação do agente do Console e do Cloud Volumes ONTAP, se sua organização tiver uma política que bloqueia o uso de imagens que não estão hospedadas dentro da organização.

Você pode implantar um agente do Console manualmente usando o método de instalação manual, mas o Cloud Volumes ONTAP também precisará extrair imagens do projeto NetApp . Você deve fornecer uma lista permitida para implantar um agente do Console e o Cloud Volumes ONTAP.

Implantando um agente de console

O usuário que implanta um agente do Console precisa ser capaz de referenciar uma imagem hospedada no `projectId netapp-cloudmanager` e no número do projeto `14190056516`.

Implantando o Cloud Volumes ONTAP

- A conta de serviço do Console precisa fazer referência a uma imagem hospedada no `projectId netapp-cloudmanager` e ao número do projeto `14190056516` do projeto de serviço.
- A conta de serviço do Agente de Serviço de APIs padrão do Google precisa fazer referência a uma

imagem hospedada no projectId *netapp-cloudmanager* e ao número do projeto *14190056516* do projeto de serviço.

Exemplos das regras necessárias para extrair essas imagens com o VPC Service Controls são definidos abaixo.

Políticas de perímetro do VPC Service Controls

As políticas permitem exceções aos conjuntos de regras de Controles de Serviço da VPC. Para obter mais informações sobre políticas, visite o "[Documentação da política de Service Controls VPC do Google Cloud](#)".

Para definir as políticas exigidas pelo Console, navegue até o Perímetro de Controles de Serviço da VPC na sua organização e adicione as seguintes políticas. Os campos devem corresponder às opções fornecidas na página de política do VPC Service Controls. Observe também que **todas** as regras são obrigatórias e os parâmetros **OU** devem ser usados no conjunto de regras.

Regras de entrada

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Service Project]
  Services =
    Service name: iam.googleapis.com
      Service methods: All actions
    Service name: compute.googleapis.com
      Service methods: All actions
```

OU

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Host Project]
  Services =
    Service name: compute.googleapis.com
      Service methods: All actions
```

OU

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
  Source > All sources allowed
To:
  Projects =
    [Service Project]
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

Regras de saída

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
To:
  Projects =
    14190056516
  Service =
    Service name: compute.googleapis.com
    Service methods: All actions
```



O número do projeto descrito acima é o projeto *netapp-cloudmanager* usado pela NetApp para armazenar imagens para o agente do Console e para o Cloud Volumes ONTAP.

Crie uma conta de serviço do Google Cloud para o Cloud Volumes ONTAP

O Cloud Volumes ONTAP requer uma conta de serviço do Google Cloud para duas finalidades. A primeira é quando você habilita "[hierarquização de dados](#)" para hierarquizar dados frios para armazenamento de objetos de baixo custo no Google Cloud. A segunda é quando você habilita o "[NetApp Backup and Recovery](#)" para fazer backup de volumes em armazenamento de objetos de baixo custo.

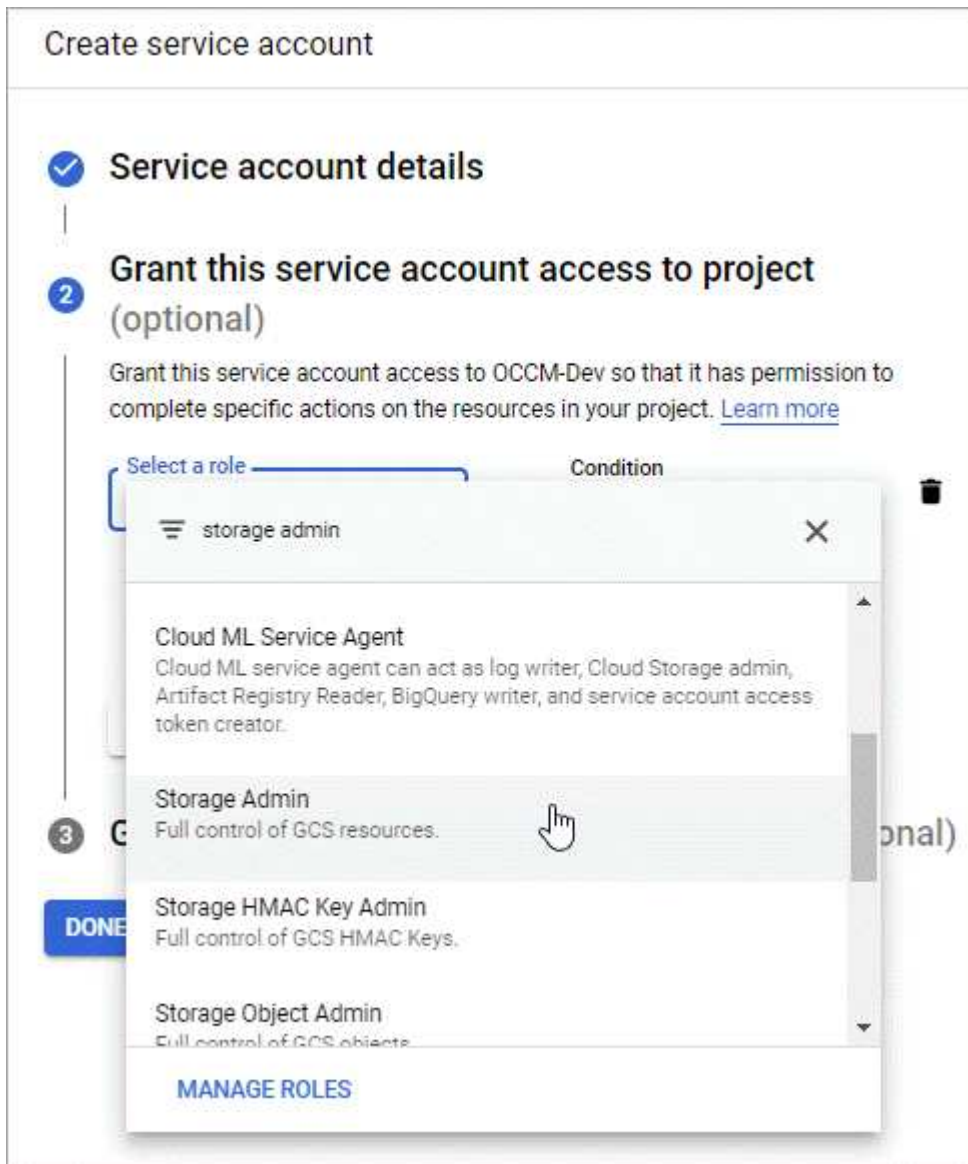
O Cloud Volumes ONTAP usa a conta de serviço para acessar e gerenciar um bucket para dados em camadas e outro bucket para backups.

Você pode configurar uma conta de serviço e usá-la para ambas as finalidades. A conta de serviço deve ter a função **Administrador de armazenamento**.

Passos

1. No Console do Google Cloud, "[vá para a página de contas de serviço](#)".

2. Selecione seu projeto.
3. Clique em **Criar conta de serviço** e forneça as informações necessárias.
 - a. **Detalhes da conta de serviço**: insira um nome e uma descrição.
 - b. **Conceder a esta conta de serviço acesso ao projeto**: Selecione a função **Administrador de armazenamento**.



- c. **Conceder aos usuários acesso a esta conta de serviço**: adicione a conta de serviço do agente do Console como um *Usuário da conta de serviço* a esta nova conta de serviço.

Esta etapa é necessária somente para a hierarquização de dados. Não é necessário para backup e recuperação.

Create service account

- ✓ Service account details
- ✓ Grant this service account access to project (optional)
- 3 Grant users access to this service account (optional)
Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

Grant users the permission to administer this service account

DONE CANCEL

O que vem a seguir?

Você precisará selecionar a conta de serviço mais tarde ao criar um sistema Cloud Volumes ONTAP .

Details and Credentials

default-project Google Cloud Project	gcp-sub2 Marketplace Subscription	Edit Project
---	--------------------------------------	------------------------------

Details

Working Environment Name (Cluster Name)

Service Account

Service Account Name

[+ Add Labels](#) Optional Field | Up to four labels

Credentials

User Name

Password

Confirm Password

Usando chaves de criptografia gerenciadas pelo cliente com o Cloud Volumes ONTAP

Embora o Google Cloud Storage sempre criptografe seus dados antes de gravá-los no disco, você pode usar as APIs para criar um sistema Cloud Volumes ONTAP que usa *chaves de criptografia gerenciadas pelo cliente*. Essas são chaves que você gera e gerencia no GCP usando o Cloud Key Management Service.

Passos

1. Certifique-se de que a conta de serviço do agente do Console tenha as permissões corretas no nível do projeto, no projeto onde a chave está armazenada.

As permissões são fornecidas no "[as permissões da conta de serviço por padrão](#)", mas pode não ser aplicável se você usar um projeto alternativo para o Cloud Key Management Service.

As permissões são as seguintes:

- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `cloudkms.cryptoKeys.get`
- `cloudkms.cryptoKeys.list`
- `cloudkms.keyRings.list`

2. Certifique-se de que a conta de serviço para o "[Agente de serviço do Google Compute Engine](#)" tem

permissões do Cloud KMS Encrypter/Decrypter na chave.

O nome da conta de serviço usa o seguinte formato: "service-[service_project_number]@compute-system.iam.gserviceaccount.com".

["Documentação do Google Cloud: Usando o IAM com o Cloud KMS - Concedendo funções em um recurso"](#)

3. Obtenha o "id" da chave invocando o comando get para `/gcp/vsa/metadata/gcp-encryption-keys` Chamada de API ou escolhendo "Copiar nome do recurso" na chave no console do GCP.
 4. Se estiver usando chaves de criptografia gerenciadas pelo cliente e hierarquizando dados para armazenamento de objetos, o NetApp Console tentará utilizar as mesmas chaves usadas para criptografar os discos persistentes. Mas primeiro você precisa habilitar os buckets do Google Cloud Storage para usar as chaves:
 - a. Encontre o agente de serviço do Google Cloud Storage seguindo o ["Documentação do Google Cloud: Obtendo o agente de serviço do Cloud Storage"](#) .
 - b. Navegue até a chave de criptografia e atribua ao agente de serviço do Google Cloud Storage permissões de Criptografador/Descritografador do Cloud KMS.
- Para mais informações, consulte ["Documentação do Google Cloud: Usando chaves de criptografia gerenciadas pelo cliente"](#)
5. Use o parâmetro `"gcpEncryption"` na sua solicitação de API ao criar um sistema.

Exemplo

```
"gcpEncryptionParameters": {  
  "key": "projects/project-1/locations/us-east4/keyRings/keyring-  
1/cryptoKeys/generatedkey1"  
}
```

Consulte o ["Documentação de automação do NetApp Console"](#) para mais detalhes sobre o uso do parâmetro `"GcpEncryption"`.

Configurar o licenciamento do Cloud Volumes ONTAP no Google Cloud

Depois de decidir qual opção de licenciamento você deseja usar com o Cloud Volumes ONTAP, algumas etapas são necessárias antes que você possa escolher essa opção de licenciamento ao criar um novo sistema.

Freemium

Selecione a oferta Freemium para usar o Cloud Volumes ONTAP gratuitamente com até 500 GiB de capacidade provisionada. ["Saiba mais sobre a oferta Freemium"](#) .

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.

2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas no NetApp Console.
- a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no Google Cloud Marketplace.
- Você não será cobrado pela assinatura do marketplace, a menos que exceda 500 GiB de capacidade provisionada, momento em que o sistema será automaticamente convertido para o "[Pacote Essentials](#)".
- b. Após retornar ao Console, selecione **Freemium** quando chegar à página de métodos de cobrança.

Select Charging Method		
<input type="radio"/>	Professional	By capacity
<input type="radio"/>	Essential	By capacity
<input checked="" type="radio"/>	Freemium (Up to 500 GiB)	By capacity
<input type="radio"/>	Per Node	By node

["Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud"](#) .

Licença baseada em capacidade

O licenciamento baseado em capacidade permite que você pague pelo Cloud Volumes ONTAP por TiB de capacidade. O licenciamento baseado em capacidade está disponível na forma de um *pacote*: o pacote Essentials ou Professional.

Os pacotes Essentials e Professional estão disponíveis nos seguintes modelos de consumo ou opções de compra:

- Uma licença (traga sua própria licença (BYOL)) adquirida da NetApp
- Uma assinatura por hora, paga conforme o uso (PAYGO), do Google Cloud Marketplace
- Um contrato anual

["Saiba mais sobre licenciamento baseado em capacidade"](#) .

As seções a seguir descrevem como começar a usar cada um desses modelos de consumo.

Traga sua própria bebida

Pague antecipadamente comprando uma licença (BYOL) da NetApp para implantar sistemas Cloud Volumes ONTAP em qualquer provedor de nuvem.



A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte "[Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP](#)".

Passos

1. "[Entre em contato com a equipe de vendas da NetApp para obter uma licença](#)"
2. "[Adicione sua conta do site de suporte da NetApp ao NetApp Console](#)"

O Console consulta automaticamente o serviço de licenciamento da NetApp para obter detalhes sobre as licenças associadas à sua conta do Site de Suporte da NetApp . Se não houver erros, o Console adiciona as licenças.

Sua licença deve estar disponível no Console antes que você possa usá-la com o Cloud Volumes ONTAP. Se necessário, você pode "[adicionar manualmente a licença ao Console](#)".

3. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no Google Cloud Marketplace.

A licença que você comprou da NetApp é sempre cobrada primeiro, mas você será cobrado pela taxa horária no mercado se exceder sua capacidade licenciada ou se o prazo de sua licença expirar.

- b. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.

Select Charging Method	
<input checked="" type="radio"/> Professional	By capacity ▾
<input type="radio"/> Essential	By capacity ▾
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity ▾
<input type="radio"/> Per Node	By node ▾

"[Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud](#)".

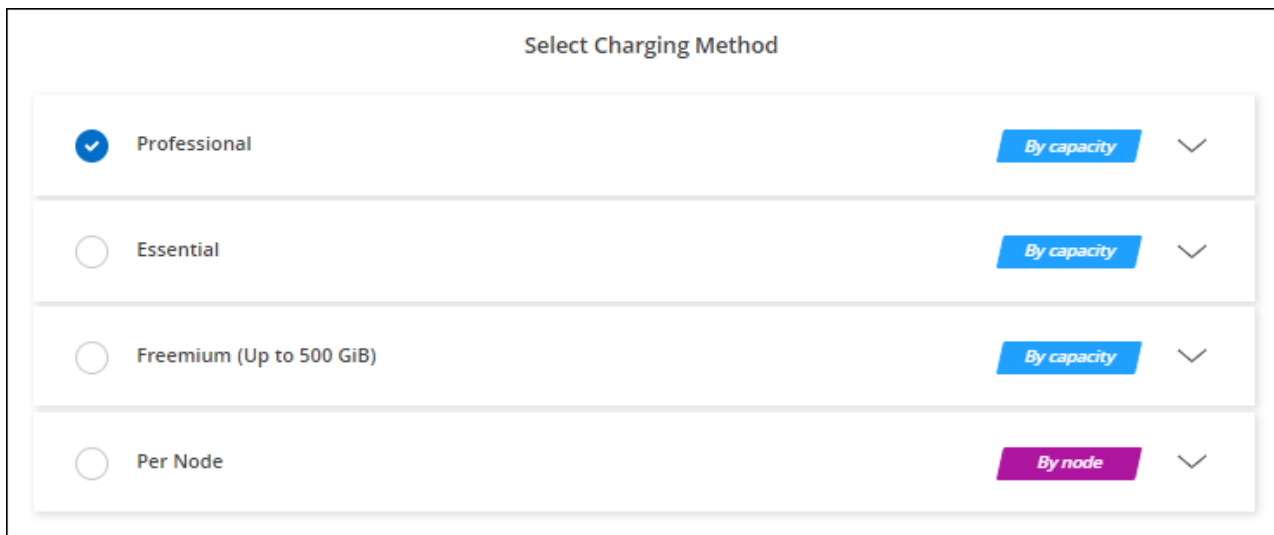
Assinatura PAYGO

Pague por hora assinando a oferta do marketplace do seu provedor de nuvem.

Ao criar um sistema Cloud Volumes ONTAP , o Console solicita que você assine o contrato disponível no Google Cloud Marketplace. Essa assinatura é então associada ao sistema de cobrança. Você pode usar a mesma assinatura para sistemas adicionais.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no Google Cloud Marketplace.
 - b. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



["Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud"](#) .



Você pode gerenciar as assinaturas do Google Cloud Marketplace associadas às suas contas na página Configurações > Credenciais. ["Aprenda a gerenciar suas credenciais e assinaturas do Google Cloud"](#)

Contrato anual

Pague pelo Cloud Volumes ONTAP anualmente comprando um contrato anual.

Passos

1. Entre em contato com seu representante de vendas da NetApp para adquirir um contrato anual.

O contrato está disponível como uma oferta *privada* no Google Cloud Marketplace.

Depois que a NetApp compartilhar a oferta privada com você, você poderá selecionar o plano anual ao assinar o Google Cloud Marketplace durante a criação do sistema.

2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar o plano anual no Google Cloud Marketplace.
 - b. No Google Cloud, selecione o plano anual que foi compartilhado com sua conta e clique em **Assinar**.
 - c. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	∨
<input type="radio"/> Essential	By capacity	∨
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	∨
<input type="radio"/> Per Node	By node	∨

"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud" .

Assinatura Keystone

Uma assinatura Keystone é um serviço baseado em assinatura com pagamento conforme o crescimento. ["Saiba mais sobre as assinaturas do NetApp Keystone"](#) .

Passos

1. Se você ainda não tem uma assinatura, ["entre em contato com a NetApp"](#)
2. [Entre em contato com a NetApp](#) para autorizar sua conta de usuário do Console com uma ou mais assinaturas do Keystone .
3. Depois que a NetApp autorizar sua conta, ["vincule suas assinaturas para uso com o Cloud Volumes ONTAP"](#) .
4. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - a. Selecione o método de cobrança da Assinatura Keystone quando solicitado a escolher um método de cobrança.

Select Charging Method

Keystone By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

Professional By capacity v

Essential By capacity v

Freemium (Up to 500 GiB) By capacity v

Per Node By node v

"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud" .

Licença baseada em nó

Uma licença baseada em nó é a licença da geração anterior para o Cloud Volumes ONTAP. Uma licença baseada em nó pode ser adquirida da NetApp (BYOL) e está disponível para renovações de licença apenas em casos específicos. Para obter informações, consulte:

- ["Fim da disponibilidade de licenças baseadas em nós"](#)
- ["Fim da disponibilidade de licenças baseadas em nós"](#)
- ["Converter uma licença baseada em nós para uma licença baseada em capacidade."](#)

Inicie o Cloud Volumes ONTAP no Google Cloud

Você pode iniciar o Cloud Volumes ONTAP em uma configuração de nó único ou como um par de HA no Google Cloud.

Antes de começar

Você precisa do seguinte antes de começar.

- Um agente da NetApp Console que está em funcionamento.
 - Você deveria ter um ["Agente de console associado ao seu sistema"](#) .

- ["Você deve estar preparado para deixar o agente do Console em execução o tempo todo"](#) .
- A conta de serviço associada ao agente do Console ["deve ter as permissões necessárias"](#)
- Uma compreensão da configuração que você deseja usar.

Você deve ter se preparado escolhendo uma configuração e obtendo informações de rede do Google Cloud com seu administrador. Para mais detalhes, consulte ["Planejando sua configuração do Cloud Volumes ONTAP"](#) .

- Uma compreensão do que é necessário para configurar o licenciamento do Cloud Volumes ONTAP.

["Aprenda como configurar o licenciamento"](#) .

- As APIs do Google Cloud devem ser ["habilitado em seu projeto"](#) :
 - API do Gerenciador de Implantação em Nuvem V2
 - API de registro em nuvem
 - API do Gerenciador de Recursos de Nuvem
 - API do mecanismo de computação
 - API de gerenciamento de identidade e acesso (IAM)

Inicie um sistema de nó único no Google Cloud


Crie um sistema no NetApp Console para iniciar o Cloud Volumes ONTAP no Google Cloud.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.
3. **Escolha um local**: Selecione **Google Cloud** e * Cloud Volumes ONTAP*.
4. Se você for solicitado, ["criar um agente de console"](#) .
5. **Detalhes e credenciais**: selecione um projeto, especifique um nome de cluster, opcionalmente selecione uma conta de serviço, opcionalmente adicione rótulos e, em seguida, especifique as credenciais.

A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância da VM do Google Cloud. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Nome da conta de serviço	Se você planeja usar "hierarquização de dados" ou "NetApp Backup and Recovery" com o Cloud Volumes ONTAP, você precisa habilitar Conta de serviço e selecionar uma conta de serviço que tenha a função de administrador de armazenamento predefinida. "Aprenda a criar uma conta de serviço" .

Campo	Descrição
Adicionar rótulos	Os rótulos são metadados para seus recursos do Google Cloud. O Console adiciona os rótulos ao sistema Cloud Volumes ONTAP e aos recursos do Google Cloud associados ao sistema. Você pode adicionar até quatro rótulos na interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro rótulos ao criar um sistema. Para obter informações sobre rótulos, consulte o " Documentação do Google Cloud: Rotulagem de recursos ".
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP. Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.
Editar Projeto	<p>Selecione o projeto onde você deseja que o Cloud Volumes ONTAP resida. O projeto padrão é o projeto onde o Console está localizado.</p> <p>Se você não vir nenhum projeto adicional na lista suspensa, significa que ainda não associou a conta de serviço a outros projetos. Vá para o Google Cloud Console, abra o serviço IAM e selecione o projeto. Adicione a conta de serviço com a função que você usa para o Console a esse projeto. Você precisará repetir esta etapa para cada projeto.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin: 10px 0;">  Esta é a conta de serviço que você configurou para o Console, "conforme descrito nesta página". </div> <p>Clique em Adicionar assinatura para associar as credenciais selecionadas a uma assinatura.</p> <p>Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, você precisa selecionar um projeto do Google Cloud associado a uma assinatura do Cloud Volumes ONTAP no marketplace do Google Cloud. Consulte "Associando uma assinatura do marketplace às credenciais do Google Cloud".</p>

6. **Serviços:** Selecione os serviços que você deseja usar neste sistema. Para selecionar Backup e Recuperação ou usar o NetApp Cloud Tiering, você deve ter especificado a Conta de Serviço na etapa 3.



Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

7. **Localização e conectividade:** Selecione a região e a zona do Google Cloud para o seu sistema, escolha uma política de firewall e confirme a conectividade de rede com o storage do Google Cloud para o tiering de dados.

A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Verificação de conectividade	Para hierarquizar dados frios em um bucket do Google Cloud Storage, a sub-rede na qual o Cloud Volumes ONTAP reside deve ser configurada para o Private Google Access. Para obter instruções, consulte " Documentação do Google Cloud: Configurando o acesso privado do Google ".
Política de firewall gerada	Se você deixar o Console gerar a política de firewall para você, precisará escolher como permitirá o tráfego: <ul style="list-style-type: none"> • Se você escolher Somente VPC selecionada, o filtro de origem para tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada. • Se você escolher Todas as VPCs, o filtro de origem para o tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Usar política de firewall existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias: " Saiba mais sobre as regras de firewall para o Cloud Volumes ONTAP ".

8. **Métodos de cobrança e conta NSS:** especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp :

- "[Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP](#)"
- "[Aprenda como configurar o licenciamento](#)"

9. **Pacotes pré-configurados:** selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **Criar minha própria configuração**. Os pacotes pré-configurados variam de acordo com a versão do Cloud Volumes ONTAP selecionada. Por exemplo, para Cloud Volumes ONTAP 9.18.1 e versões posteriores, o Console exibe pacotes com VMs C3, incluindo discos Hyperdisk Balanced. Você pode modificar as configurações, como parâmetros de IOPS e throughput, com base nas necessidades da sua carga de trabalho.

Se você escolher um dos pacotes, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

10. **Licenciamento:** Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de máquina.



Se uma versão mais recente de Release Candidate, Disponibilidade Geral ou patch estiver disponível para uma versão selecionada, o Console atualizará o sistema para essa versão ao criá-la. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra — por exemplo, da 9.13 para a 9.14.

11. **Recursos de armazenamento subjacentes:** escolha as configurações para o agregado inicial: um tipo de disco e o tamanho de cada disco.

O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.

O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console cria quando você usa a opção de provisionamento simples. Você pode criar agregados que

usam um tamanho de disco diferente usando a opção de alocação avançada.

Para obter ajuda na escolha do tipo e tamanho do disco, consulte ["Dimensione seu sistema no Google Cloud"](#) .

12. Flash Cache, Velocidade de Gravação e WORM:

- a. Ative o **Flash Cache** ou escolha a velocidade de gravação **Normal** ou **Alta** se necessário.

Saiba mais sobre ["Cache Flash"](#) e ["velocidade de escrita"](#) .



Alta velocidade de gravação e uma unidade máxima de transmissão (MTU) maior de 8.896 bytes estão disponíveis por meio da opção de velocidade de gravação **Alta**. Além disso, a MTU mais alta de 8.896 exige a seleção de VPC-1, VPC-2 e VPC-3 para a implantação. Para obter mais informações sobre VPC-1, VPC-2 e VPC-3, consulte ["Regras para VPC-1, VPC-2 e VPC-3"](#) .

- b. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP . A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

["Saiba mais sobre o armazenamento WORM"](#) .

- a. Se você ativar o armazenamento WORM, selecione o período de retenção.

13. Classificação de dados em camadas no Google Cloud Platform:

escolha se deseja habilitar a classificação de dados em camadas no agregado inicial, escolha uma classe de armazenamento para os dados em camadas e, em seguida, selecione uma conta de serviço que tenha a função de administrador de armazenamento predefinida (necessária para o Cloud Volumes ONTAP 9.7 ou posterior) ou selecione uma conta do Google Cloud (necessária para o Cloud Volumes ONTAP 9.6).

Observe o seguinte:

- O Console define a conta de serviço na instância do Cloud Volumes ONTAP . Esta conta de serviço fornece permissões para hierarquização de dados para um bucket do Google Cloud Storage. Certifique-se de adicionar a conta de serviço do agente do Console como um usuário da conta de serviço em camadas; caso contrário, você não poderá selecioná-la no Console.
- Para obter ajuda na adição de uma conta do Google Cloud, consulte ["Configurando e adicionando contas do Google Cloud para camadas de dados com 9.6"](#) .
- Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
- Se você desativar o tiering de dados, poderá ativá-lo em agregados subsequentes, mas precisará desligar o sistema e adicionar uma conta de serviço no Google Cloud Console.

["Saiba mais sobre camadas de dados"](#) .

14. Criar volume:

insira detalhes para o novo volume ou clique em **Ignorar**.

["Saiba mais sobre os protocolos e versões de clientes suportados"](#) .

Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume, "use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:

Volume Details & Protection

Volume Name i <input style="width: 90%;" type="text" value="ABDcv5689"/>	Storage VM (SVM) <input style="width: 90%;" type="text" value="svm_c...CVO1"/>
Volume Size i Unit <input style="width: 40%;" type="text" value="100"/> <input style="width: 40%;" type="text" value="GiB"/>	Snapshot Policy <input style="width: 90%;" type="text" value="default"/>

default policy i

15. **Configuração CIFS:** Se você escolher o protocolo CIFS, configure um servidor CIFS.

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará. Se você estiver configurando o Google Managed Active Directory, o AD poderá ser acessado por padrão com o endereço IP 169.254.169.254.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Para configurar o Google Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira OU=Computers,OU=Cloud neste campo. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units ["Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"^]
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione Usar domínio do Active Directory para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Para obter informações, consulte o " Documentação de automação do NetApp Console " para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

16. **Perfil de uso, tipo de disco e política de camadas:** escolha se deseja habilitar recursos de eficiência de armazenamento e alterar a política de camadas de volume, se necessário.

Para mais informações, consulte "[Escolha um perfil de uso de volume](#)", "[Visão geral da hierarquização de dados](#)", e "[KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?](#)"

17. **Revisar e aprovar:** revise e confirme suas seleções.

- a. Revise os detalhes sobre a configuração.
- b. Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos do Google Cloud que o Console comprará.
- c. Selecione as caixas de seleção **Eu entendo...**
- d. Clique em **Ir**.

Resultado

O Console implanta o sistema Cloud Volumes ONTAP . Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver algum problema ao implantar o sistema Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recriar ambiente**.

Para obter ajuda adicional, acesse "[Suporte NetApp Cloud Volumes ONTAP](#)" .

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.



Após a conclusão do processo de implantação, não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal do Google Cloud, como as tags do sistema e os rótulos definidos nos recursos do Google Cloud. Quaisquer alterações feitas nessas configurações podem levar a comportamentos inesperados ou perda de dados.


Inicie um par de HA no Google Cloud

Crie um sistema no Console para iniciar o Cloud Volumes ONTAP no Google Cloud.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Armazenamento > Sistema** e siga as instruções.
3. **Escolha um local:** Selecione **Google Cloud** e * Cloud Volumes ONTAP HA*.
4. **Detalhes e credenciais:** selecione um projeto, especifique um nome de cluster, opcionalmente selecione uma conta de serviço, opcionalmente adicione rótulos e, em seguida, especifique as credenciais.

A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância da VM do Google Cloud. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Nome da conta de serviço	Se você planeja usar o "NetApp Cloud Tiering" ou "Backup e Recuperação" serviços, você precisa habilitar a opção Conta de serviço e então selecionar a Conta de serviço que tem a função de administrador de armazenamento predefinida.
Adicionar rótulos	Os rótulos são metadados para seus recursos do Google Cloud. O Console adiciona os rótulos ao sistema Cloud Volumes ONTAP e aos recursos do Google Cloud associados ao sistema. Você pode adicionar até quatro rótulos na interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro rótulos ao criar um sistema. Para obter informações sobre rótulos, consulte "Documentação do Google Cloud: Rotulagem de recursos" .
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.
Editar Projeto	<p>Selecione o projeto onde você deseja que Cloud Volumes ONTAP resida.</p> <p>Se você não vir nenhum projeto adicional na lista suspensa, significa que ainda não associou a conta de serviço a outros projetos. Vá para o Google Cloud Console, abra o serviço IAM e selecione o projeto. Adicione a conta de serviço com a função que você usa para o Console a esse projeto. Você precisará repetir esta etapa para cada projeto.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  Esta é a conta de serviço que você configurou para o Console, "conforme descrito nesta página" . </div> <p>Clique em Adicionar assinatura para associar as credenciais selecionadas a uma assinatura.</p> <p>Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, você precisa selecionar um projeto do Google Cloud associado a uma assinatura do Cloud Volumes ONTAP no Google Cloud Marketplace. Consulte "Associando uma assinatura do marketplace às credenciais do Google Cloud" .</p>

5. **Serviços:** Selecione os serviços que você deseja usar neste sistema. Para selecionar Backup e Recuperação ou usar o NetApp Cloud Tiering, você deve ter especificado a Conta de Serviço na etapa 3.



Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

6. **Modelos de implantação de alta disponibilidade:** escolha várias zonas (recomendado) ou uma única zona para a configuração de alta disponibilidade. Em seguida, selecione uma região e uma zona.

["Saiba mais sobre modelos de implantação de HA"](#) .

7. **Conectividade:** Selecione quatro VPCs diferentes para a configuração de HA, uma sub-rede em cada VPC e, em seguida, escolha uma política de firewall.

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

A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Política gerada	Se você deixar o Console gerar a política de firewall para você, precisará escolher como permitirá o tráfego: <ul style="list-style-type: none">• Se você escolher Somente VPC selecionada, o filtro de origem para tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada.• Se você escolher Todas as VPCs, o filtro de origem para o tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Use existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias. "Saiba mais sobre as regras de firewall para o Cloud Volumes ONTAP" .

8. **Métodos de cobrança e conta NSS:** especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp .
- ["Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"](#) .
 - ["Aprenda como configurar o licenciamento"](#) .
9. **Pacotes pré-configurados:** selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **Criar minha própria configuração**.

Se você escolher um dos pacotes, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

10. **Licenciamento:** Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de máquina.



Se uma versão mais recente de Release Candidate, Disponibilidade Geral ou patch estiver disponível para a versão selecionada, o Console atualizará o sistema para essa versão ao criá-la. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, da 9.13 para a 9.14.

11. **Recursos de armazenamento subjacentes:** escolha as configurações para o agregado inicial: um tipo de disco e o tamanho de cada disco.

O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.

O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console cria quando você usa a opção de provisionamento simples. Você pode criar agregados que

usam um tamanho de disco diferente usando a opção de alocação avançada.

Para obter ajuda na escolha do tipo e tamanho do disco, consulte ["Dimensione seu sistema no Google Cloud"](#) .

12. Flash Cache, Velocidade de Gravação e WORM:

- a. Ative o **Flash Cache** ou escolha a velocidade de gravação **Normal** ou **Alta** se necessário.

Saiba mais sobre ["Cache Flash"](#) e ["velocidade de escrita"](#) .



Alta velocidade de gravação e uma unidade máxima de transmissão (MTU) maior de 8.896 bytes estão disponíveis por meio da opção de velocidade de gravação **Alta** com os tipos de instância n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Além disso, a MTU mais alta de 8.896 exige a seleção de VPC-1, VPC-2 e VPC-3 para a implantação. Alta velocidade de gravação e uma MTU de 8.896 dependem do recurso e não podem ser desabilitadas individualmente em uma instância configurada. Para obter mais informações sobre VPC-1, VPC-2 e VPC-3, consulte ["Regras para VPC-1, VPC-2 e VPC-3"](#) .

- b. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP . A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

["Saiba mais sobre o armazenamento WORM"](#) .

- a. Se você ativar o armazenamento WORM, selecione o período de retenção.

13. Classificação de dados no Google Cloud:

escolha se deseja habilitar a classificação de dados no agregado inicial, escolha uma classe de armazenamento para os dados em camadas e, em seguida, selecione uma conta de serviço que tenha a função predefinida de Administrador de armazenamento.

Observe o seguinte:

- O Console define a conta de serviço na instância do Cloud Volumes ONTAP . Esta conta de serviço fornece permissões para hierarquização de dados para um bucket do Google Cloud Storage. Certifique-se de adicionar a conta de serviço do agente do Console como um usuário da conta de serviço em camadas; caso contrário, você não poderá selecioná-la no Console.
- Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
- Se você desativar o tiering de dados, poderá ativá-lo em agregados subsequentes, mas precisará desligar o sistema e adicionar uma conta de serviço no Google Cloud Console.

["Saiba mais sobre camadas de dados"](#) .

14. Criar volume:

insira detalhes para o novo volume ou clique em **Ignorar** .

["Saiba mais sobre os protocolos e versões de clientes suportados"](#) .

Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume, "use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:

Volume Details & Protection

Volume Name i <input type="text" value="ABDcv5689"/>	Storage VM (SVM) <input type="text" value="svm_c...CVO1"/>
Volume Size i Unit <input type="text" value="100"/> <input type="text" value="GiB"/>	Snapshot Policy <input type="text" value="default"/>

default policy i

15. **Configuração CIFS:** Se você escolher o protocolo CIFS, configure um servidor CIFS.

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará. Se você estiver configurando o Google Managed Active Directory, o AD poderá ser acessado por padrão com o endereço IP 169.254.169.254.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Para configurar o Google Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira OU=Computers,OU=Cloud neste campo. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units ["Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"^]
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione Usar domínio do Active Directory para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

16. **Perfil de uso, tipo de disco e política de camadas:** escolha se deseja habilitar recursos de eficiência de armazenamento e alterar a política de camadas de volume, se necessário.

Para mais informações, consulte "[Escolha um perfil de uso de volume](#)", "[Visão geral da hierarquização de dados](#)", e "[KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?](#)"

17. **Revisar e aprovar:** revise e confirme suas seleções.

- a. Revise os detalhes sobre a configuração.
- b. Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos do Google Cloud que o Console comprará.
- c. Selecione as caixas de seleção **Eu entendo...**
- d. Clique em **Ir**.

Resultado

O Console implanta o sistema Cloud Volumes ONTAP . Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver algum problema ao implantar o sistema Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recriar ambiente**.

Para obter ajuda adicional, acesse "[Suporte NetApp Cloud Volumes ONTAP](#)" .

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.



Após a conclusão do processo de implantação, não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal do Google Cloud, como as tags do sistema e os rótulos definidos nos recursos do Google Cloud. Quaisquer alterações feitas nessas configurações podem levar a comportamentos inesperados ou perda de dados.

Links relacionados

- "[Planejando sua configuração do Cloud Volumes ONTAP no Google Cloud](#)"

Verificação de imagem da plataforma Google Cloud

Saiba como a imagem do Google Cloud é verificada no Cloud Volumes ONTAP

A verificação de imagem do Google Cloud está em conformidade com os requisitos de segurança aprimorados da NetApp . Foram feitas alterações no script que gera as imagens para assiná-las ao longo do caminho usando chaves privadas geradas especificamente para essa tarefa. Você pode verificar a integridade da imagem do Google Cloud usando o resumo assinado e o certificado público do Google Cloud, que podem ser baixados via "[NSS](#)" para um lançamento específico.



A verificação de imagens do Google Cloud é compatível com o software Cloud Volumes ONTAP versão 9.13.0 ou superior.

Converter imagem do Google Cloud para formato bruto para Cloud Volumes ONTAP

A imagem que está sendo usada para implantar novas instâncias, atualizações ou que está sendo usada em imagens existentes será compartilhada com os clientes por meio de "[o site de suporte da NetApp \(NSS\)](#)". O resumo assinado e os certificados estarão disponíveis para download no portal do NSS. Certifique-se de que você está baixando o resumo e os certificados para a versão correta correspondente à imagem compartilhada pelo Suporte da NetApp. Por exemplo, imagens 9.13.0 terão um resumo assinado 9.13.0 e certificados disponíveis no NSS.

Por que essa etapa é necessária?

As imagens do Google Cloud não podem ser baixadas diretamente. Para verificar a imagem em relação ao resumo assinado e aos certificados, você precisa ter um mecanismo para comparar os dois arquivos e baixar a imagem. Para fazer isso, você deve exportar/converter a imagem para o formato disk.raw e salvar os resultados em um bucket de armazenamento no Google Cloud. O arquivo disk.raw é compactado em tar e gzip no processo.

A conta de usuário/serviço precisará de privilégios para executar o seguinte:

- Acesso ao bucket de armazenamento do Google
- Gravar no bucket do Google Storage
- Criar trabalhos de criação de nuvem (usados durante o processo de exportação)
- Acesso à imagem desejada
- Criar tarefas de exportação de imagem

Para verificar a imagem, ela deve ser convertida para o formato disk.raw e depois baixada.

Use a linha de comando do Google Cloud para exportar a imagem do Google Cloud

A maneira preferida de exportar uma imagem para o Cloud Storage é usar o "[comando gcloud compute images export](#)". Este comando pega a imagem fornecida e a converte em um arquivo disk.raw, que é tarado e compactado em gzip. O arquivo gerado é salvo na URL de destino e pode ser baixado para verificação.

O usuário/conta deve ter privilégios para acessar e gravar no bucket desejado, exportar a imagem e criar na nuvem (usado pelo Google para exportar a imagem) para executar esta operação.

Exportar imagem do Google Cloud usando gcloud

Clique para exhibir

```
$ gcloud compute images export \  
  --destination-uri DESTINATION_URI \  
  --image IMAGE_NAME  
  
# For our example:  
$ gcloud compute images export \  
  --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-  
gcp-demo \  
  --image example-user-20230120115139  
  
## DEMO ##  
# Step 1 - Optional: Checking access and listing objects in the  
destination bucket  
$ gsutil ls gs://example-user-export-image-bucket/  
  
# Step 2 - Exporting the desired image to the bucket  
$ gcloud compute images export --image example-user-export-image-demo  
--destination-uri gs://example-user-export-image-bucket/export-  
demo.tar.gz  
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-  
project/locations/us-central1/builds/xxxxxxxxxxxxx].  
Logs are available at [https://console.cloud.google.com/cloud-  
build/builds;region=us-central1/xxxxxxxxxxxxx?project=xxxxxxxxxxxxx].  
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-  
export-image-demo" from project "example-demo-project".  
[image-export]: 2023-01-25T18:13:49Z Validating workflow  
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"  
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-  
export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z  
Validating step "setup-disks"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z  
Validating step "run-image-export-export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "wait-for-inst-image-export-export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "copy-image-object"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "delete-inst"  
[image-export]: 2023-01-25T18:13:51Z Validation Complete  
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-  
project  
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```



```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'  
value:'10'>"  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Running export tool."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size  
will most likely be much smaller."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Beginning export process..."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-  
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-  
r88px/outs/image-export-export-disk.tar.gz."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer  
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),  
total written size: 992 MiB (198 MiB/sec)"  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),  
total written size: 1.5 GiB (17 MiB/sec)"  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Finished creating gzipped image of  
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of  
6."
```

```

[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Finished export in 48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: <serial-output key:'target-size-gb' value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step "delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk" (IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz

# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION

```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-  
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz  
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to  
file://CVO_GCP_Signed_Digest.tar.gz  
Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s
```

```
Average throughput: 213.3MiB/s
```

```
$ ls -l  
total 1565036  
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44  
CVO_GCP_Signed_Digest.tar.gz
```

Extraia os arquivos compactados

```
# Extracting files from the digest  
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```



Para obter mais informações sobre como exportar uma imagem por meio do Google Cloud, consulte o ["Documento do Google Cloud sobre como exportar uma imagem"](#).

Verificação de assinatura de imagem

Verificação de assinatura de imagem do Google Cloud para Cloud Volumes ONTAP

Para verificar a imagem assinada do Google Cloud exportada, você deve baixar o arquivo de resumo da imagem do NSS para validar o arquivo disk.raw e o conteúdo do arquivo de resumo.

Resumo do fluxo de trabalho de verificação de imagem assinada

A seguir, uma visão geral do processo de fluxo de trabalho de verificação de imagem assinada do Google Cloud.

- Do **"NSS"**, baixe o arquivo do Google Cloud contendo os seguintes arquivos:
 - Resumo assinado (.sig)
 - Certificado contendo a chave pública (.pem)
 - Cadeia de certificados (.pem)

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP

Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

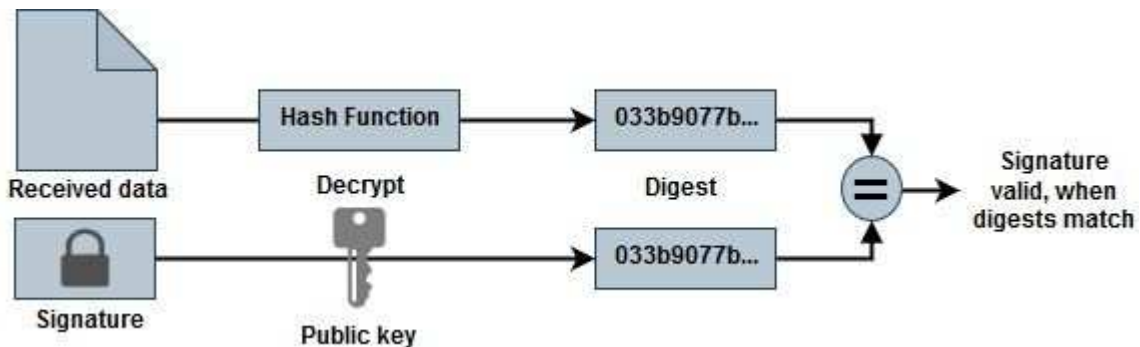
DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

- Baixe o arquivo disk.raw convertido
- Validar o certificado usando a cadeia de certificados
- Valide o resumo assinado usando o certificado que contém a chave pública
 - Descriptografe o resumo assinado usando a chave pública para extrair o resumo do arquivo de imagem
 - Crie um resumo do arquivo disk.raw baixado
 - Compare os dois arquivos de resumo para validação



Verifique o arquivo disk.raw da imagem do Google Cloud para o Cloud Volumes ONTAP usando OpenSSL

Você pode verificar o arquivo disk.raw baixado pelo Google Cloud em relação ao conteúdo do arquivo de resumo disponível por meio do "NSS" usando OpenSSL.



Os comandos OpenSSL para validar a imagem são compatíveis com máquinas Linux, macOS e Windows.

Passos

1. Verifique o certificado usando OpenSSL.

Clique para exhibir

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OSCP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OSCP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocspl -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -url ${ocsp_url} -resp_text
-respout resp.der
```

OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Version: 1 (0x0)

Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2

Produced At: Jan 19 15:14:00 2023 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8F8FE78

Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5

Cert Status: good

This Update: Jan 19 15:00:00 2023 GMT

Next Update: Jan 26 14:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

```
0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```

e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
  This Update: Jan 19 15:00:00 2023 GMT
  Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK

```

2. Coloque o arquivo disk.raw baixado, a assinatura e os certificados em um diretório.
3. Extraia a chave pública do certificado usando OpenSSL.
4. Descriptografe a assinatura usando a chave pública extraída e verifique o conteúdo do arquivo disk.raw baixado.

Clique para exhibir

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU 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.