Cloud Virtual Machine

Tutorial prático

Product Documentation

Contents

Tutorial prático
Práticas recomendadas

Last updated：2024-01-23 17:52:21

Este artigo tem como objetivo ajudar os usuários a melhorarem a segurança e a confiabilidade de suas instâncias de CVM.

Segurança e rede

- Acesso limitado: restrinja o acesso usando um firewall (Grupo de segurança para permitir que apenas os endereços confiáveis acessem as instâncias. O grupo de segurança também deve ter regras rígidas, como limitar o acesso a portas, e por endereços IP.
- Nível de segurança: diferentes regras de grupo de segurança podem ser criadas para grupos de instâncias de diferentes níveis de segurança para garantir que instâncias que executam negócios importantes não sejam facilmente acessadas por fontes externas.
- Isolamento lógico de rede: use VPC para dividir os recursos em zonas lógicas.
- Gerenciamento de permissão de conta: quando é necessário permitir que várias contas diferentes acessem o mesmo conjunto de recursos de nuvem, você pode gerenciar permissões para recursos de nuvem usando o mecanismo de política.
- Login seguro: faça login em suas instâncias do Linux usando a chave SSH, sempre que possível. Para as instâncias nas quais você usa senha para fazer login, tal senha precisa ser alterada regularmente.

Armazenamento

- Armazenamento de hardware: para dados que requerem alta confiabilidade, use os discos em nuvem do Tencent Cloud para garantir o armazenamento persistente e a confiabilidade dos dados. Tente não usar Discos locais para armazenamento. Para obter mais informações, consulte a Documentação do produto Cloud Block Storage.
- Banco de dados: para bancos de dados que são muito acessados e cuja capacidade muda com frequência, use o TencentDB do Tencent Cloud.

Backup e recuperação

- Backup de instância intra-regional: você pode fazer backup de suas instâncias e dados de negócios usando imagens personalizadas e instantâneos CBS. Para obter mais informações, consulte Instantâneo CBS e Criação de imagens personalizadas.
- Backup de instância entre regiões: você pode copiar e fazer backup de instâncias entre regiões Cópia de imagens.

- Bloqueio de falhas de instância: você pode usar EIPs para mapear o nome de domínio e garantir que o servidor possa redirecionar rapidamente o endereço IP do serviço para outra instância do CVM quando estiver indisponível, protegendo assim as falhas de instância.

Monitoramento e alarmes

- Monitoramento e resposta a eventos: verifique periodicamente os dados de monitoramento e defina os alarmes adequados. Para obter mais informações, consulte a Documentação do produto Tencent Cloud Observability Platform.
- Tratamento de picos de solicitação: com Auto Scaling, a estabilidade dos CVMs durante os horários de pico pode ser garantida e as instâncias não íntegras podem ser substituídas automaticamente.

Recomendações de seleção da CVM
Selecionar o modo de cobrança

Last updated：2024-01-23 17:25:49

O Tencent Cloud disponibiliza os seguintes métodos de faturamento para as instâncias do Cloud Virtual Machine (CVM):

- O pagamento conforme o uso é um método de faturamento flexível para as instâncias do CVM. É possível ativar ou encerrar um CVM a qualquer momento e você será faturado pelo uso real do CVM. A granularidade do faturamento tem precisão de segundos, e não é necessário pagamento adiantado. Uma fatura é gerada a cada hora cheia. Esse método de faturamento é adequado para casos de uso, como uma oferta relâmpago de comércio eletrônico, em que a demanda por dispositivos pode flutuar muito.
- A instância spot é uma nova forma de usar e pagar por instâncias do CVM. Semelhante ao método de pagamento conforme o uso, você paga pelas instâncias spot no modo pós-pago por segundo, a cada hora. O preço das instâncias spot flutua de acordo com a demanda do mercado. Você pode receber um desconto considerável para elas quando a demanda é baixa (geralmente de 10% a 20%). No entanto, as instâncias spot podem ser reavidas automaticamente pelo sistema à medida que a demanda aumenta.

Os métodos de faturamento de pagamento conforme o uso e de instâncias spot podem atender aos requisitos do usuário em diferentes cenários. Para obter mais informações, consulte os Modos de preços.

Selecionar o tipo de instância

Last updated：2024-01-23 17:25:49

O Tencent Cloud fornece as seguintes recomendações para selecionar um tipo de instância para diversos casos de uso de clientes:

Caso de uso	Tipo de instância recomendado	Descrição
Site pessoal	Instância padrão	Adequada para cargas de trabalho gerais, como aplicativos e bancos de dados da Web de pequeno e médio porte.
Sites corporativos/comércio eletrônico/aplicativo	Instância padrão	Adequada para cargas de trabalho gerais, como aplicativos e bancos de dados da Web de pequeno e médio porte.
Banco de dados relacional/cache distribuído	Instância otimizada para memória	Adequada para casos de uso que requerem operações de memória, pesquisas e computação extensivos.
Banco de dados NoSQL	Instância com E/S alta	Adequada para casos de uso intensivo de E/S que exigem alto desempenho de leitura/gravação de disco e baixa latência, como TencentDB for MongoDB e bancos de dados em cluster.
Computação de alto desempenho	• Instância de computação • Instância de computação aprimorada para rede	Adequada para casos de uso que requerem uma grande quantidade de recursos de computação, como jogos de computador pesados, aplicativos de ciência e engenharia de alto desempenho e codificação/decodificação de vídeos.
Jogos de computador de alto desempenho	• Instância de computação • Instância de computação aprimorada para rede	Adequada para casos de uso que requerem uma grande quantidade de recursos de computação, como jogos de computador pesados, aplicativos de ciência e engenharia de alto desempenho e codificação/decodificação de vídeos.

Jogos para celular/navegador	• Instância de computação • Instância de computação aprimorada para rede	Adequada para casos de uso que requerem uma grande quantidade de recursos de computação, como jogos de computador pesados, aplicativos de ciência e engenharia de alto desempenho e codificação/decodificação de vídeos.
Transmissão ao vivo	• Instância padrão aprimorada para rede • Instância de computação aprimorada para rede	Vem com um ENI de 25 GB que é 2,5 vezes mais rápido do que os data centers normais de dez gigabits, proporcionando maior largura de banda e latência reduzida.
Finanças	Instância padrão do CDH	Possui servidores físicos exclusivos e recursos isolados. As instâncias padrão do CDH são seguras e controláveis e estão em total conformidade com as rígidas regulamentações do setor financeiro. Especificações personalizadas também são compatíveis.
Computação científica	Instância de computação de GPU	Adequada para casos de uso que requerem aprendizado profundo e computação científica, incluindo dinâmica de fluidos computacional, finanças computacionais, pesquisa genômica, análise ambiental, computação de alto desempenho e outras cargas de trabalho de computação de GPU do servidor.
Aprendizado de máquina	Instância de computação de GPU	Adequada para casos de uso que requerem aprendizado profundo e computação científica, incluindo dinâmica de fluidos computacional, finanças computacionais, pesquisa genômica, análise ambiental, computação de alto desempenho e outras cargas de trabalho de computação de GPU do servidor.
Renderização	Instância de renderização de GPU	Adequada para edição não linear, codificação/decodificação de vídeos, visualização de aceleração gráfica e design 3D.
Hadoop/Spark /Elastic Search	Instância de big data	Adequada para serviços de computação distribuída, como Hadoop (HDFS/MapReduce/Spark/Hive), data warehouses de processamento paralelo massivo

		(MPP), logs B8 e aplicativos de processamento de dados.

- Para obter mais casos de uso, consulte os Tipos de instâncias.

Selecionar o meio de armazenamento

Last updated: 2024-01-23 17:25:49

Ao configurar uma instância, é possível escolher um disco local ou um disco em nuvem como disco do sistema ou disco de dados. Antes de escolher uma mídia de armazenamento, familiarize-se com as características e os casos de uso de discos locais e do Cloud Block Storage.

Nota:

- Os tipos de discos do sistema e discos de dados na página de aquisição variam de acordo com as diferentes especificações de instância que você selecionar. Por exemplo, os discos SSD locais estão disponíveis apenas para as instâncias de E/S.
- Não é possível atualizar o hardware (CPU, memória ou armazenamento) de uma instância do CVM com discos locais. A única atualização permitida é a da largura de banda.
- O tipo de mídia dos discos do sistema não pode ser alterado após a aquisição.

A tabela a seguir lista as vantagens e os casos de uso de mídias de armazenamento diferentes, como o disco local HDD SATA, o disco SSD NVME, o Premium Cloud Storage e o SSD.

Mídia de armazenamento	Vantagens	Casos de uso
Discos locais SSD NVME (disponíveis apenas para instâncias de E/S, como IT3 e IT5)	Baixa latência: fornece latência de acesso em nível de microssegundos.	Atua como um cache de leitura temporário: o SSD NVME tem excelente desempenho de leitura aleatória (4 KB/8 KB/16 KB de leitura aleatória) e é adequado para bancos de dados escravos somente leitura para bancos de dados relacionais, como o MySQL e o Oracle. Visto que o custo do uso de memórias ainda é maior do que o custo do uso de SSDs, os discos locais SSD NVME também podem ser usados como o cache secundário do Redis, do Memcache e de outras empresas de cache. Observação: o SSD NVME traz o risco de um ponto único de falha. Portanto, recomendamos que você implemente a redundância de dados na camada de aplicativos para garantir a confiabilidade e use os discos SSD em nuvem para a sua empresa principal.

Disco local HDD SATA (disponível apenas para as instâncias de big data, como D2)	• Fornece a mesma persistência de dados que o SSD, por uma fração do custo. Pode ser usado como backup de dados frios e arquivo para empresas importantes, com capacidade máxima de 16 TB para um único disco. • Alta taxa de transferência: oferece a mesma taxa de transferência dos HDDs locais.	É adequado para cenários que envolvem a leitura e gravação sequencial de arquivos grandes, como EMR e processamento de big data.
Premium Cloud Storage	É a opção mais econômica, adequada para 90% dos cenários de E/S.	É adequado para bancos de dados de pequeno e médio porte, servidores da web e outros cenários, e fornece desempenho de E/S consistente e estável. Atende às demandas de E/S para os testes empresariais principais e para o desenvolvimento de ambientes de teste conjuntos.
SSD	Alto desempenho e alta confiabilidade de dados: o SSD usa o melhor armazenamento de estado sólido NVMe como mídia de disco. É adequado para empresas com uso intensivo de E/S e oferece desempenho de disco único ultraexcelente e de longo prazo.	Casos de uso aplicáveis: • Bancos de dados de médio e grande porte: é compatível com aplicativos de banco de dados relacionais de médio e grande porte contendo tabelas com milhões de linhas, como MySQL, Oracle e SQL Server. • Sistemas empresariais principais: é compatível com aplicativos com uso intensivo de E/S e outros sistemas empresariais principais com altos requisitos de confiabilidade de dados. • Análise de big data: é compatível com o processamento distribuído de dados em nível de TB e PB para análise de dados, mineração de dados, business intelligence e outras aplicações.

- Para obter mais informações sobre os tipos e casos de uso de discos em nuvem, consulte os Tipos de discos em nuvem.

- Para obter mais informações sobre os preços dos discos em nuvem, consulte a Lista de preços.

Planejar a rede

Last updated: 2024-01-23 17:25:49

Uma instância do Tencent Cloud Virtual Private Cloud (VPC) é um espaço de rede isolado logicamente e definido pelo usuário do Tencent Cloud. Nessa instância, os usuários podem personalizar os intervalos de IP, os endereços de IP e as políticas de roteamento. Portanto, recomendamos que você use uma instância do VPC para suas empresas.
Para ajudá-lo a usar melhor as instâncias do Tencent Cloud VPC, fornecemos as seguintes recomendações de planejamento de rede.

Determinação da quantidade de instâncias do VPC

- Funcionalidades:
  - As redes privadas, por padrão, não se comunicam entre si. Se houver a necessidade de comunicação entre diferentes redes privadas, isso pode ser alcançado por meio de Conexão de Peering ou Rede de Conexão em Nuvem.
  - Por padrão, as zonas de disponibilidade diferentes na mesma instância do VPC podem se comunicar entre si.
- Recomendações:
  - Se sua empresa requer a implantação de sistemas entre regiões, são necessárias várias instâncias do VPC. Nesse caso, é possível criar uma instância do VPC próxima à região onde seus clientes estão localizados, para reduzir a latência de acesso e melhorar a velocidade de acesso.
  - Se você implantou várias empresas na região atual e deseja implementar o isolamento de rede entre empresas diferentes, é possível criar uma instância do VPC para cada empresa na região atual.
  - Se a implantação de empresas entre regiões ou o isolamento de rede entre as empresas não for necessário, é possível usar somente uma instância do VPC.

Determinação da divisão de sub-rede

- Funcionalidades:
  - Sub-redes são blocos de endereços IP em uma instância do VPC. Todos os recursos de nuvem em uma instância do VPC devem ser implantados em sub-redes.
  - Na mesma instância do VPC, os intervalos de IP das sub-redes não devem se sobrepor.
  - O Tencent Cloud atribui automaticamente endereços IP privados iniciais de intervalos de IP do VPC. O bloco CIDR do Tencent Cloud VPC pode ser qualquer um dos seguintes intervalos de IP do VPC. Para um endereço IP dentro desses intervalos, sua máscara varia de 16 a 28, e a máscara real é determinada pela rede privada onde reside a instância.

  - 10.0.0.0–10.255.255.255
  - 172.16.0.0–172.31.255.255
  - 192.168.0.0–192.168.255.255
  - Depois que uma instância do VPC é criada, seu intervalo de IP não pode ser modificado.
- Recomendações:
  - Se apenas as sub-redes do VPC precisarem ser divididas e a comunicação com a rede básica ou o IDC não estiver envolvida, escolha qualquer um dos intervalos de IP anteriores para criar uma sub-rede.
  - Se a comunicação com a rede básica for necessária, estabeleça uma instância do VPC com o intervalo de IP de 10.[0–47].0.0/16 e seus subconjuntos, conforme necessário.
  - Se for necessário um VPN, o intervalo de IP local (da instância do VPC) e o intervalo de IP de par (do seu IDC) não podem se sobrepor. Portanto, não use o intervalo de IP de par ao criar uma sub-rede.
  - Durante a divisão da sub-rede, também é necessário considerar a quantidade de endereços IP disponíveis em um intervalo de IP.
  - Recomendamos que as sub-redes sejam divididas de acordo com os módulos da empresa para as empresas na mesma instância do VPC. Por exemplo, a sub-rede A é usada para a camada da web, a sub-rede B é usada para a camada lógica e a sub-rede C é usada para a camada de banco de dados. Isso facilita o controle de acesso e a filtragem usando a ACL de rede.

Determinação de políticas de rotas

- Funcionalidades:
  - Uma tabela de rotas consiste em uma série de regras de roteamento que controlam o fluxo de tráfego de sub-redes em uma instância do VPC.
  - Cada sub-rede deve ser associada a apenas uma tabela de rotas.
  - Uma única tabela de rotas pode ser associada a várias sub-redes.
  - Quando uma instância do VPC é criada, o sistema gera automaticamente uma tabela de rotas padrão para a instância, que define que as instâncias do VPC podem se comunicar entre si por meio da rede privada.
- Recomendações:
  - Se você não precisa controlar o fluxo de tráfego de sub-redes e as instâncias do VPC são interconectadas por meio da rede privada por padrão, é possível usar a tabela de rotas padrão sem precisar configurar uma política de roteamento personalizada.
  - Se for necessário controlar o fluxo de tráfego de sub-redes, consulte a Visão geral no site oficial.

Para obter mais informações sobre as instâncias do VPC, consulte VPC.

Configurar o grupo de segurança

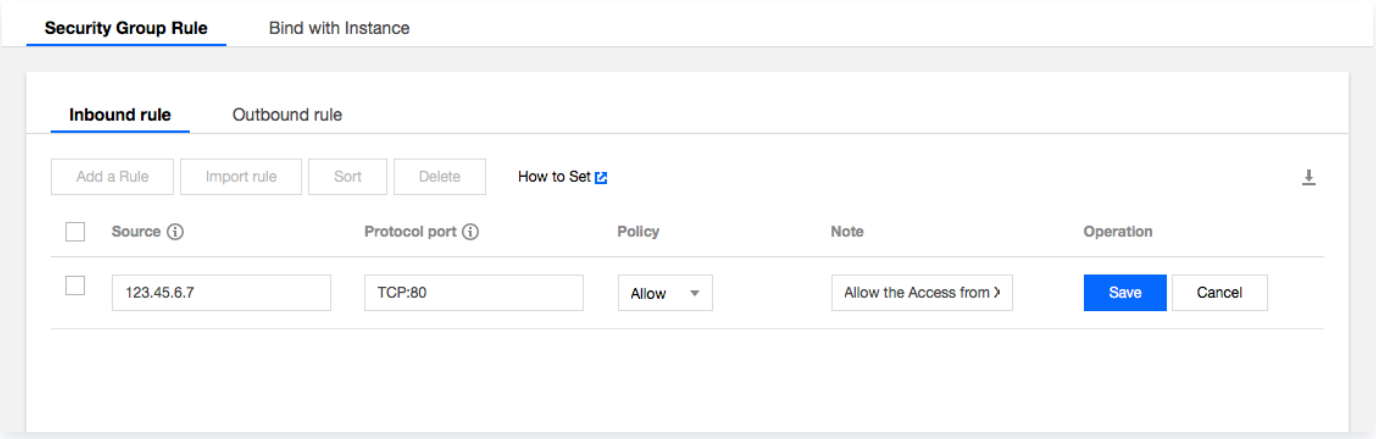
Last updated: 2024-01-23 17:25:49

Este documento descreve como criar e configurar um grupo de segurança para uma instância. Para obter mais informações, consulte o Grupo de segurança.

Configuração de um grupo de segurança

1. Selecione New security group (Novo grupo de segurança).

> Nota:
> Se você tiver grupos de segurança disponíveis, poderá selecionar Existing Security Groups (Grupos de segurança atuais).



2. Selecione os endereços IP ou as portas para abrir, com base em seus requisitos reais.
   As regras para um novo grupo de segurança são as seguintes:
   - ICMP: abre para o protocolo ICMP e permite o ping do servidor na rede pública.
   - TCP:80: abre a porta 80 e permite o acesso a serviços Web em HTTP.
   - TCP:22: abre a porta 22 e permite uma conexão remota com os CVMs do Linux em SSH.
   - TCP:443: abre a porta 443 e permite o acesso a serviços Web em HTTPS.
   - TCP:3389: abre a porta 3389 e permite uma conexão remota com os CVMs do Windows em RDP.
   - Rede privada: abre para a rede privada e permite o acesso à rede privada entre diferentes recursos de nuvem (IPv4).

> Nota:
> Depois de selecionar os endereços IP ou as portas a serem abertas, as regras detalhadas de entrada e saída são exibidas na página da guia Security Group Rule (Regra do grupo de segurança).

> Para abrir outras portas para a sua empresa, consulte os Casos de uso de grupos de segurança para criar grupos de segurança. Por motivos de segurança, recomendamos que você abra portas apenas quando for realmente necessário, para evitar riscos de segurança desnecessários.

3. Configure outras informações conforme solicitado.

Regras de grupos de segurança

Regras de entrada: permite o tráfego para os CVMs associados a um grupo de segurança.
Regras de saída: indica o tráfego de saída dos CVMs.

- As regras em um grupo de segurança são priorizadas de cima para baixo.
- Quando um CVM está vinculado a um grupo de segurança sem regras, todo o tráfego de entrada e de saída é rejeitado por padrão. Se uma regra estiver disponível, ela prevalece.
- Quando um CVM está vinculado a vários grupos de segurança, os com números menores têm prioridade mais alta.
- Por padrão, quando um CVM está vinculado a vários grupos de segurança, a regra de rejeição tem efeito para o grupo de segurança com a prioridade mais baixa.

Limites de grupos de segurança

Para obter mais informações, consulte os Limites de grupos de segurança.

Estimar o custo

Last updated：2024-01-23 17:25:49

Além do modelo do CVM e da configuração do VPC, esses fatores também influenciam os custos de serviço:

- Método de faturamento
- Recurso usado
- Quantidade

Método de faturamento

- O pagamento conforme o uso é um método de faturamento flexível para as instâncias do CVM. É possível iniciar/encerrar um CVM a qualquer momento e você será faturado pelo uso real do CVM. Você paga por segundo e não é necessário pagamento adiantado. Uma fatura é gerada a cada hora cheia. Esse método de faturamento é adequado para casos de uso, como uma oferta relâmpago de comércio eletrônico, em que a demanda por recursos pode flutuar muito.
- A instância spot é uma nova forma de usar e pagar por instâncias do CVM. Semelhante ao pagamento conforme o uso, você paga pelas instâncias spot por segundo, a cada hora. O preço das instâncias spot flutua de acordo com a demanda do mercado. Você obtém um desconto considerável para elas quando a demanda é baixa (geralmente de 10 a 20%). No entanto, elas podem ser reavidas automaticamente pelo sistema à medida que a demanda aumenta.

Recursos usados

- Região:
  - O preço é igual para o mesmo modelo de instância em diferentes regiões da China Continental.
  - O preço pode ser igual para o mesmo modelo de instância em diferentes regiões fora da China Continental.
- Imagem:
  - Imagens públicas: todas as imagens públicas na China Continental hospedadas pelo Tencent Cloud são gratuitas. As imagens do Windows fora da China continental requerem taxas de licenciamento.
  - Imagem personalizada: a criação, a importação e a cópia de imagens personalizadas entre regiões são gratuitas.
  - Imagens compartilhadas: as imagens compartilhadas de outros usuários do Tencent Cloud são gratuitas.
    Rede:
  - O VPC, a sub-rede, a tabela de rotas, a ACL de rede, o grupo de segurança, o gateway do Direct Connect, o túnel VPN e o gateway do cliente são gratuitos.

- Os custos de largura de banda não são aplicáveis à comunicação entre instâncias em sub-redes diferentes. As conexões de emparelhamento intrarregional também são gratuitas.
- Consulte este artigo para mais detalhes sobre o método de faturamento da rede pública.
- Para mais detalhes sobre as cobranças do NAT Gateway, do VPN Gateway e das conexões de emparelhamento intrarregional.

- Armazenamento:
  Para ter acesso aos preços de discos locais e discos em nuvem, consulte este artigo

Quantidade

A quantidade de CVMs adquiridos também afeta o preço que você paga. Quanto mais CVMs, maior o preço.

Configurar o ambiente

Visão geral da configuração do ambiente

Last updated：2024-01-23 17:52:21

Visão geral

Este documento fornece referência para a construção de ambientes de desenvolvimento no Tencent Cloud CVM. Se você ainda não tem um CVM, pode adquirir um por meio da página de compra do CVM.

Instruções

Consulte os seguintes documentos para construir manualmente um ambiente.

- Configuração do LNMP
- Configuração manual do LAMP
- Configuração do Java Web
- Construção manual de um ambiente WIPM
- Configuração do Node.js

Se você tiver alguma dúvida ao construir um ambiente, consulte Sobre a construção de um ambiente para solução de problemas.

Instalar o serviço IIS

Last updated：2024-01-23 17:52:21

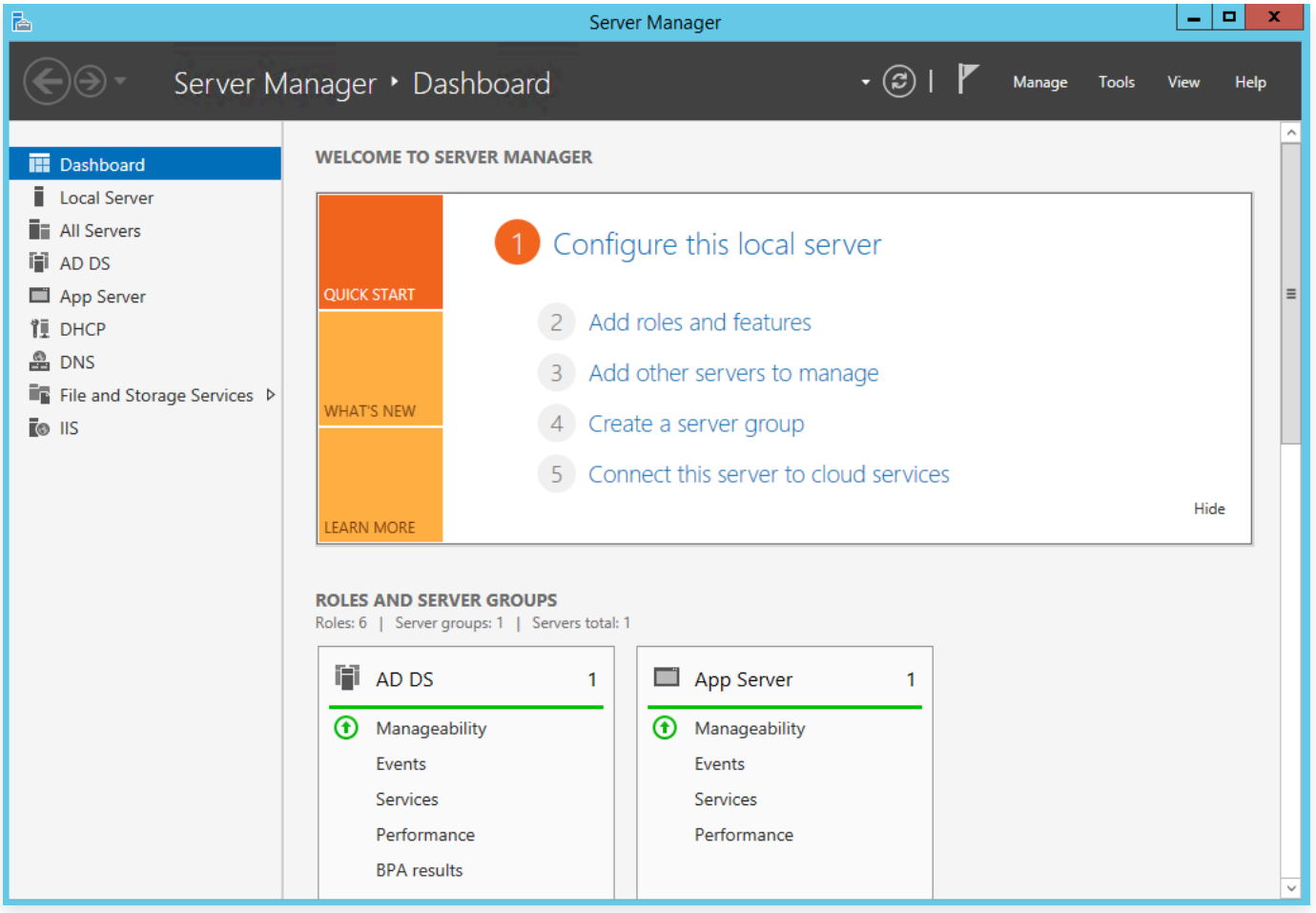
Visão geral

Este documento descreve como adicionar e instalar funções IIS em uma instância CVM com Windows Server 2012 R2 ou Windows Server 2008.

Instruções

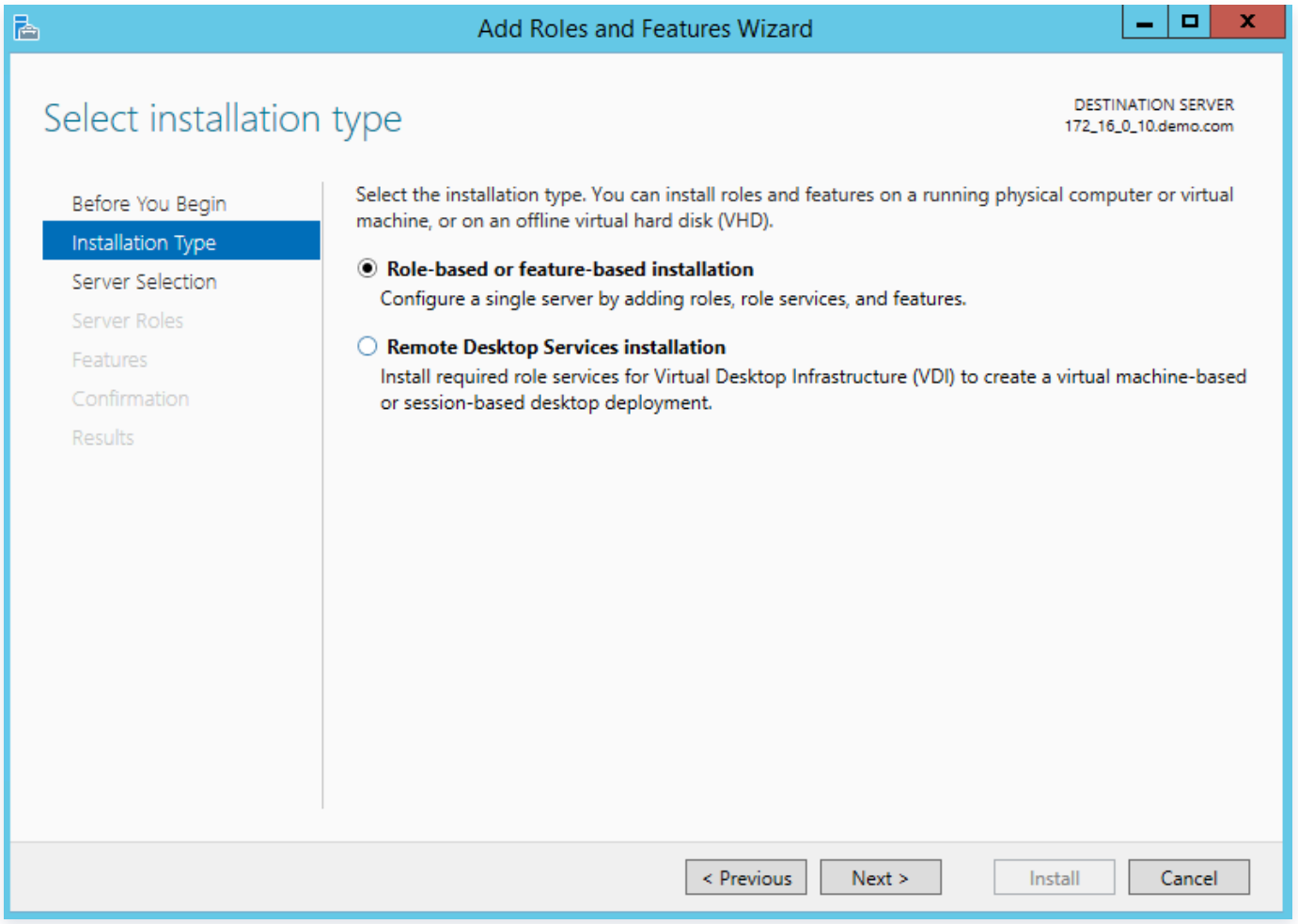
Windows Server 2012 R2

1. Faça login no CVM do Windows.
2. Na área de trabalho, clique em e abra o Server Manager (Gerenciador do servidor), conforme mostrado abaixo:



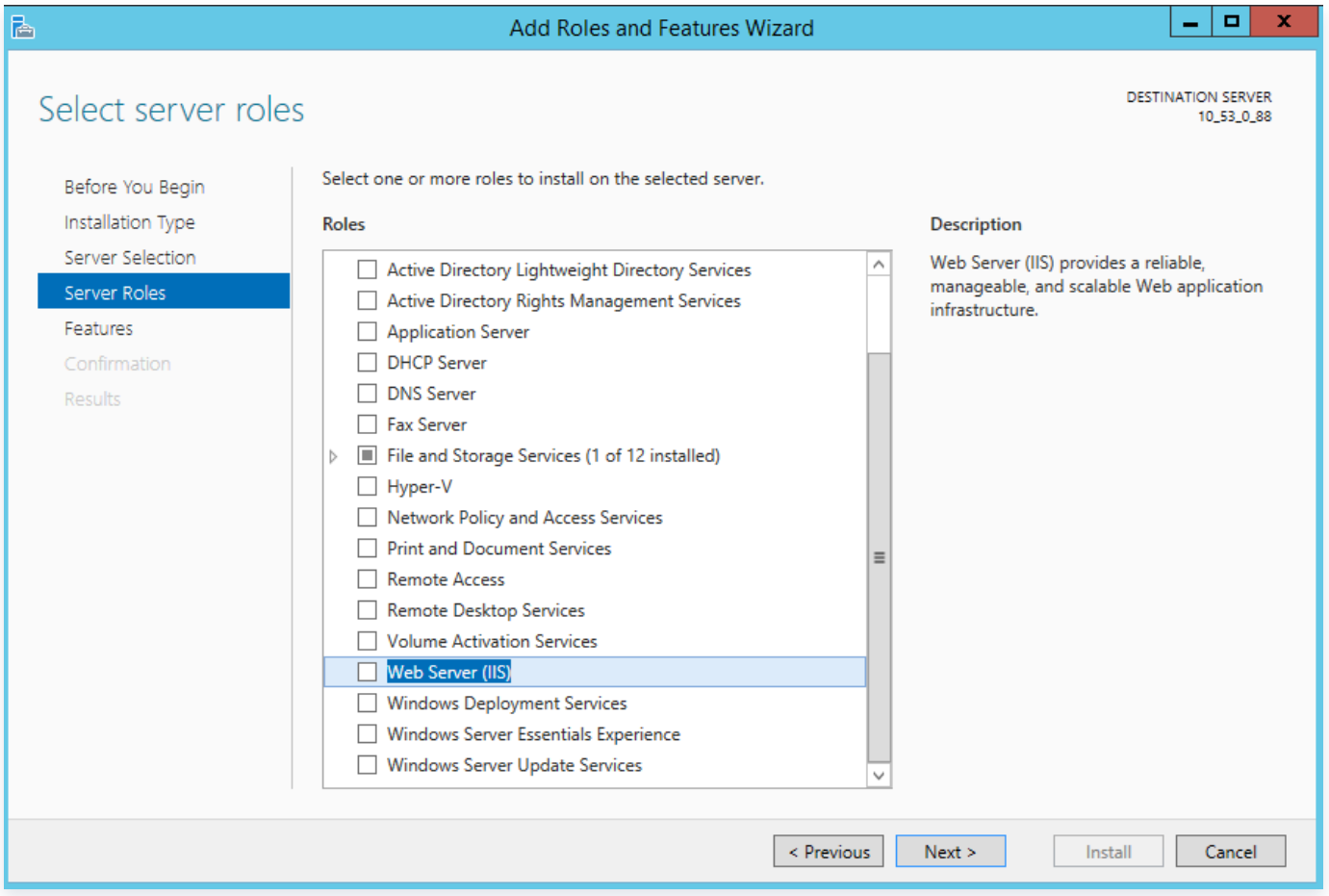
3. Clique em Add roles and features (Adicionar funções e recursos) e acesse a janela "Add Roles and Features Wizard (Assistente para adicionar funções e recursos)".

4. Na janela pop-up, clique em Next (Avançar) e acesse a página "Select installation type (Selecionar tipo de instalação)".
5. Selecione Role-based or feature-based installation (Instalação baseada em função ou recurso) e clique em Next (Avançar) duas vezes, conforme mostrado abaixo:

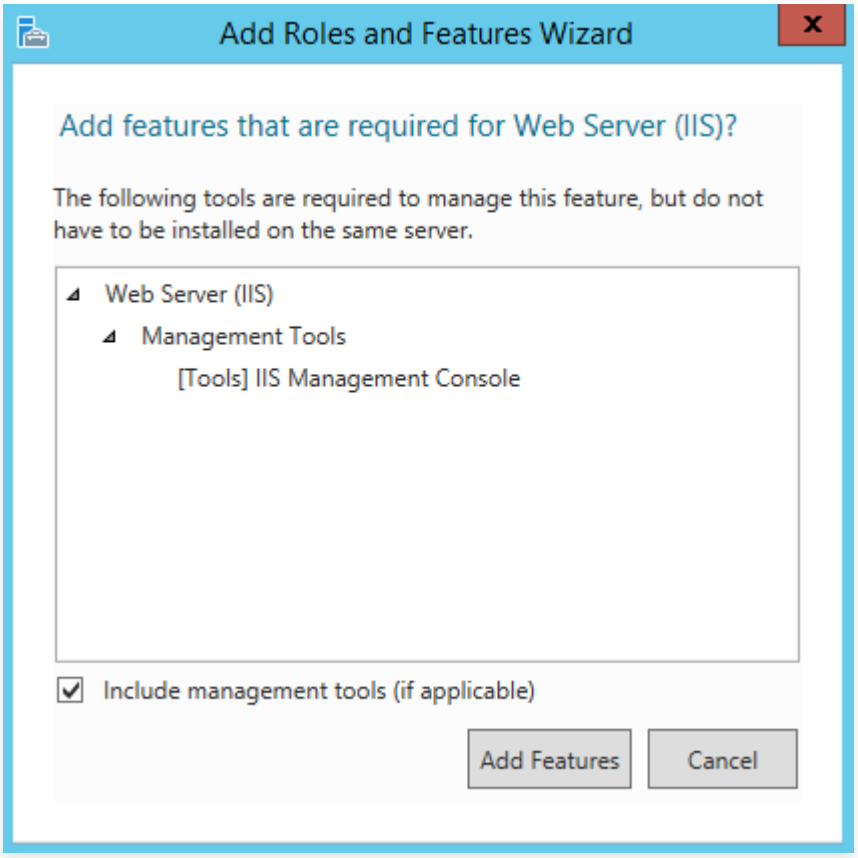


6. Marque Web Server (IIS) (Servidor Web (IIS)) na página "Select server roles (Selecionar funções de servidores)", conforme mostrado abaixo:
   A caixa de diálogo "Add features that are required for Web Server (IIS) (Adicionar recursos

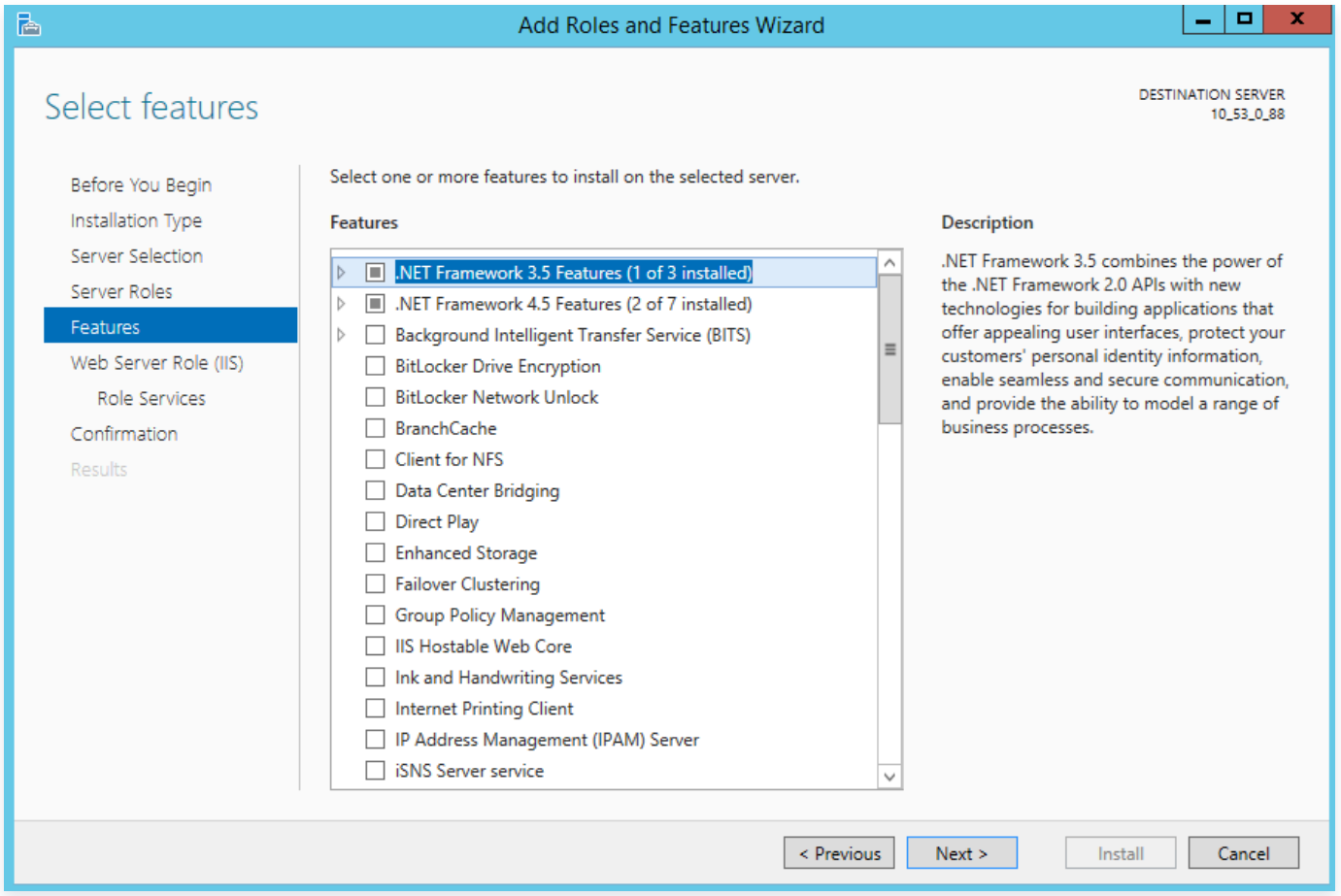
necessários para servidor web (IIS))" será exibida.



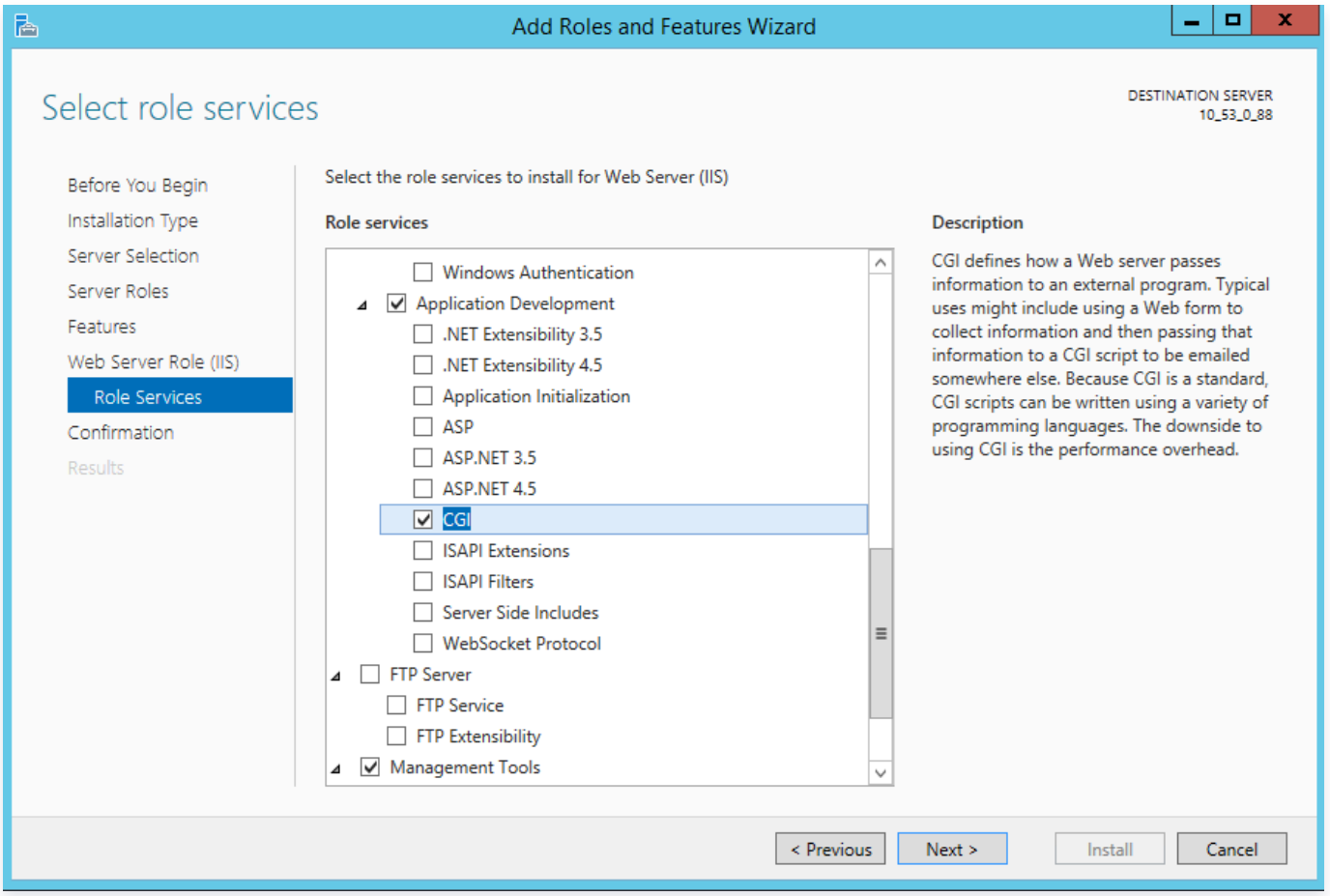
7. Clique em Add Features (Adicionar recursos) na caixa de diálogo pop-up, conforme mostrado abaixo:



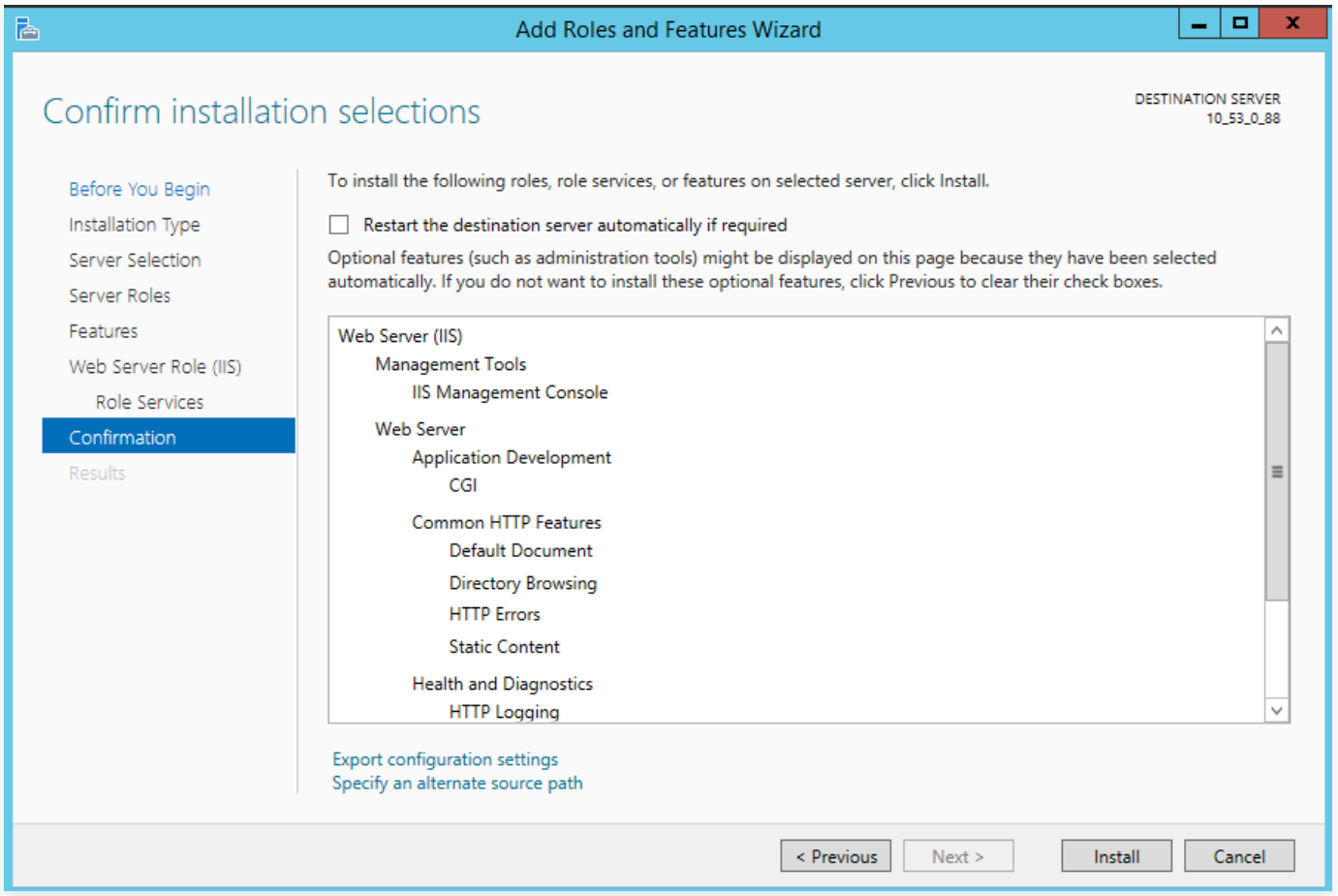
8. Clique em Next (Avançar).
9. Na página Features (Recursos), marque .NET Framework 3.5 Features (Recursos do .NET Framework 3.5) e clique em Next (Avançar) duas vezes, conforme mostrado abaixo:



10. Na página Role Services (Serviços de função), marque CGI e clique em Next (Avançar), conforme mostrado abaixo:

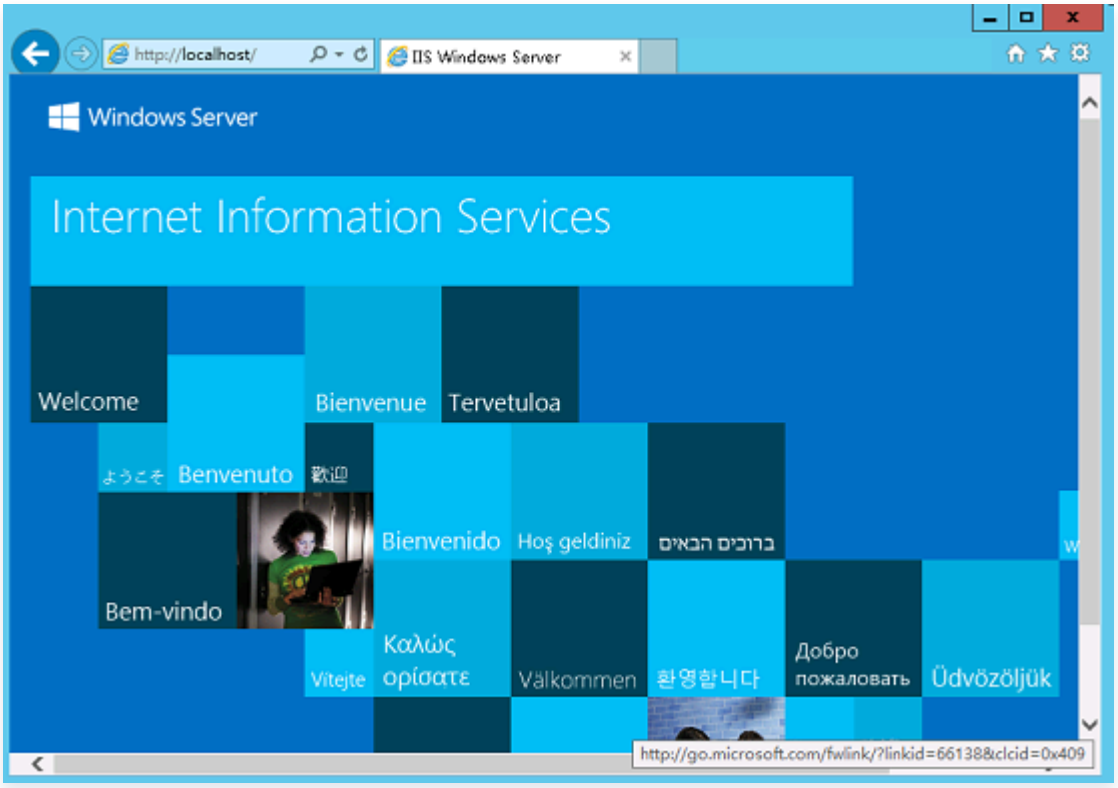


11. Revise suas seleções de instalação e clique em Install (Instalar). Aguarde a conclusão do processo de instalação.



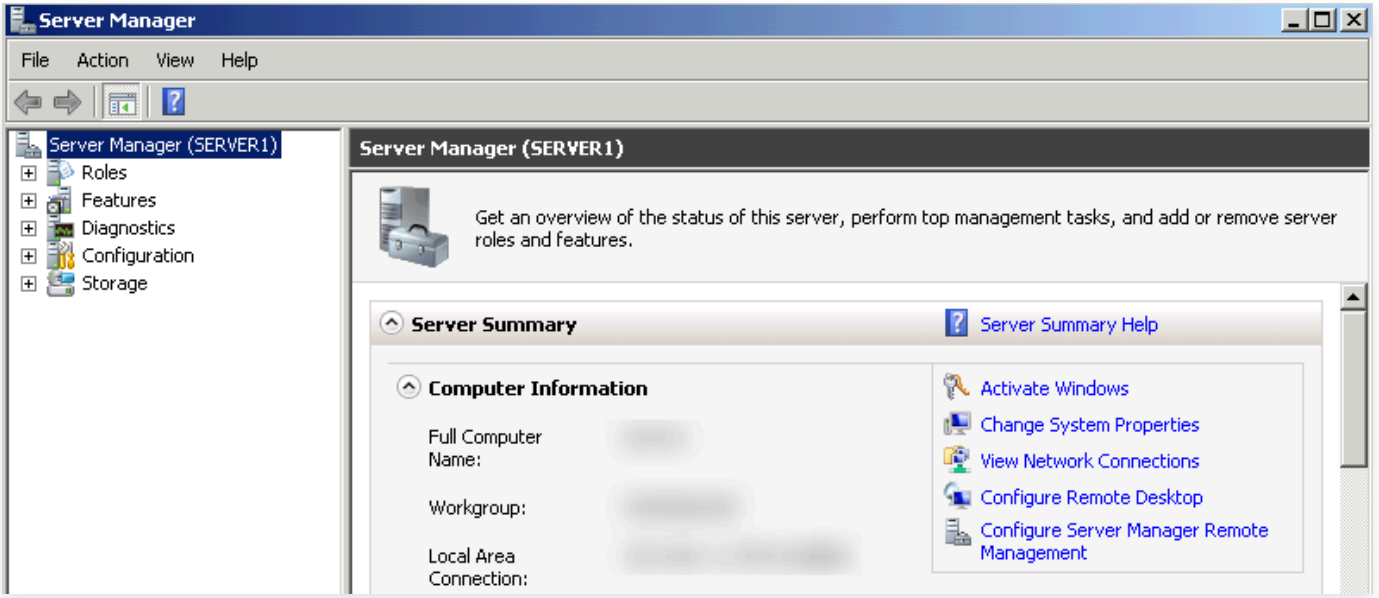
12. Quando a instalação for concluída, abra um navegador no CVM e visite `http://localhost/` para verificar se o IIS foi instalado com sucesso.

Se a página a seguir for exibida, isso indica que o IIS foi instalado com sucesso.

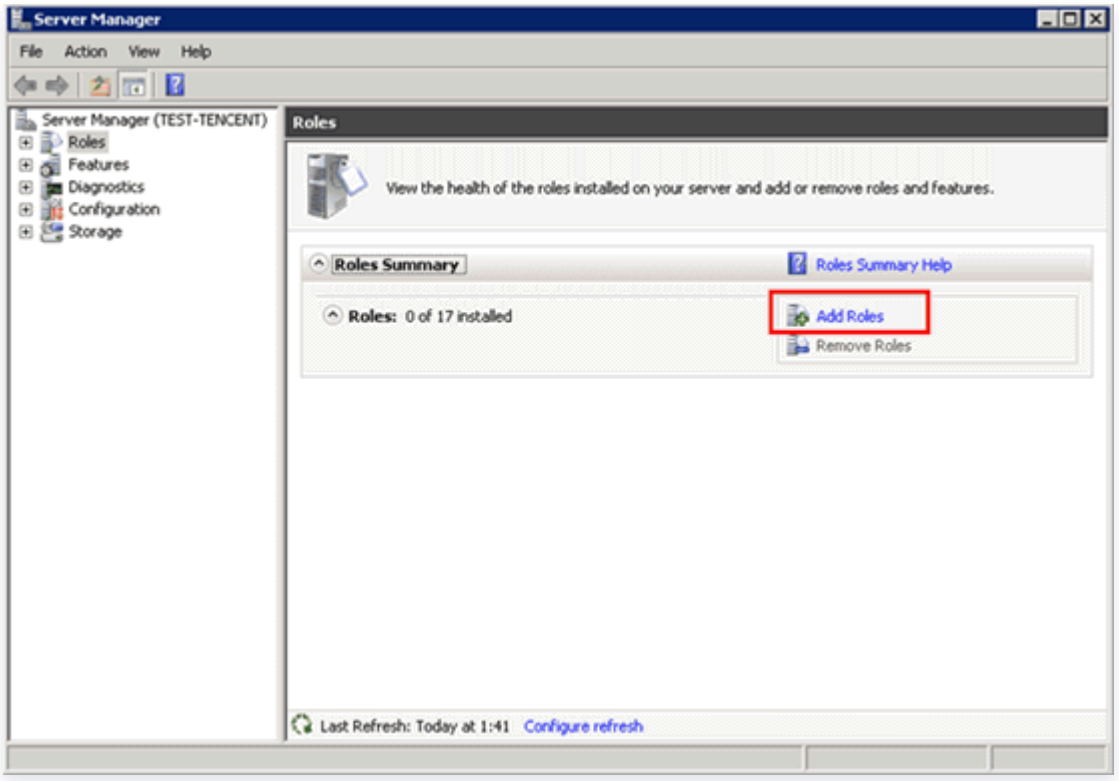


Windows Server 2008

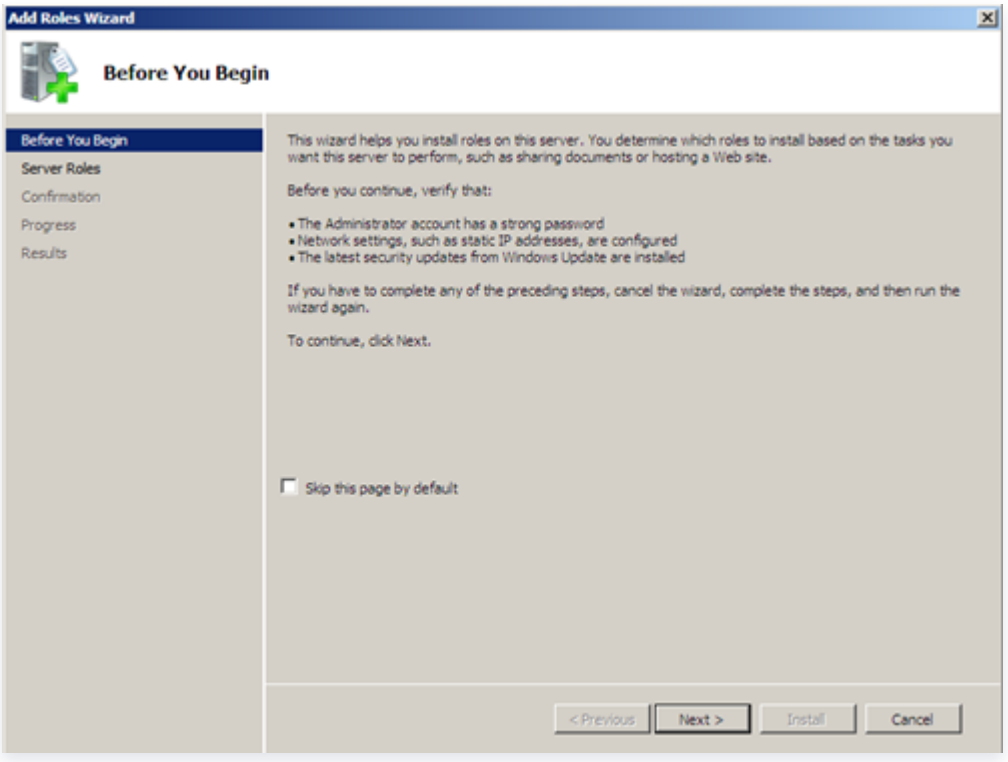
1. Faça login no CVM do Windows.
2. Na área de trabalho, clique em  e abra o Server Manager (Gerenciador do servidor), conforme mostrado abaixo:



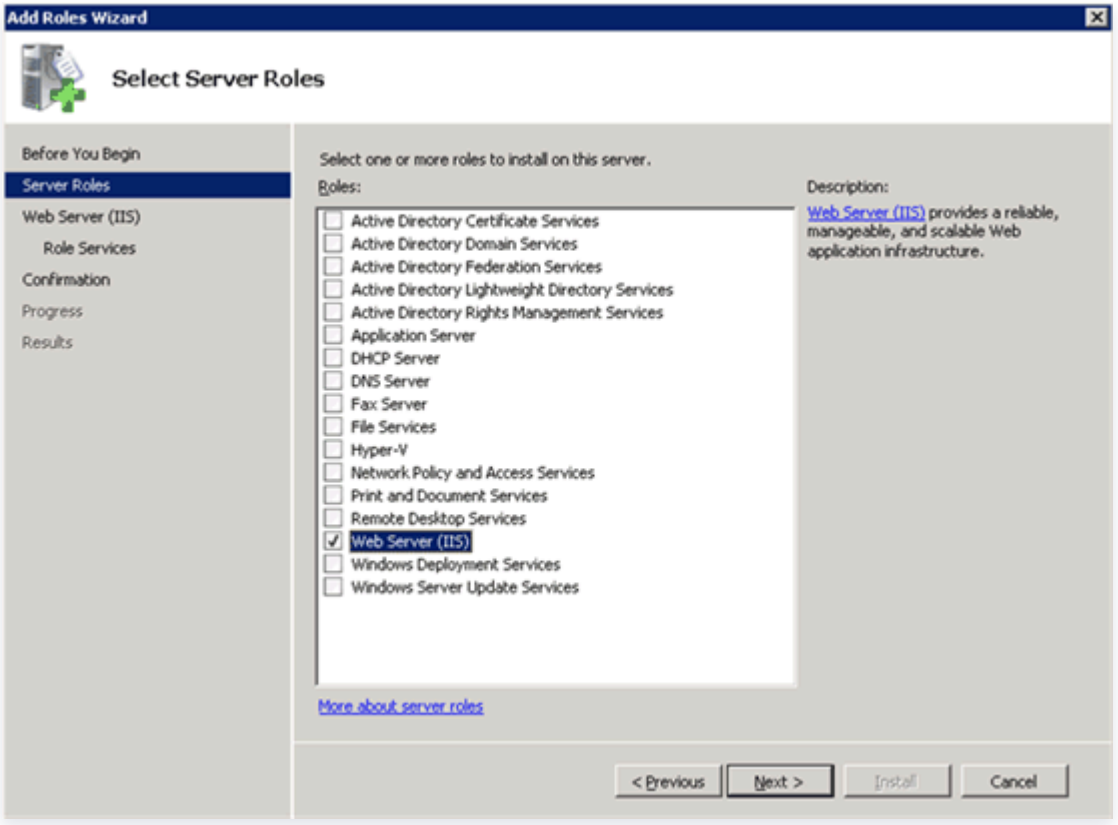
3. Selecione Roles (Funções) na barra lateral esquerda e clique em Add Roles (Adicionar funções) no painel direito, conforme mostrado abaixo:



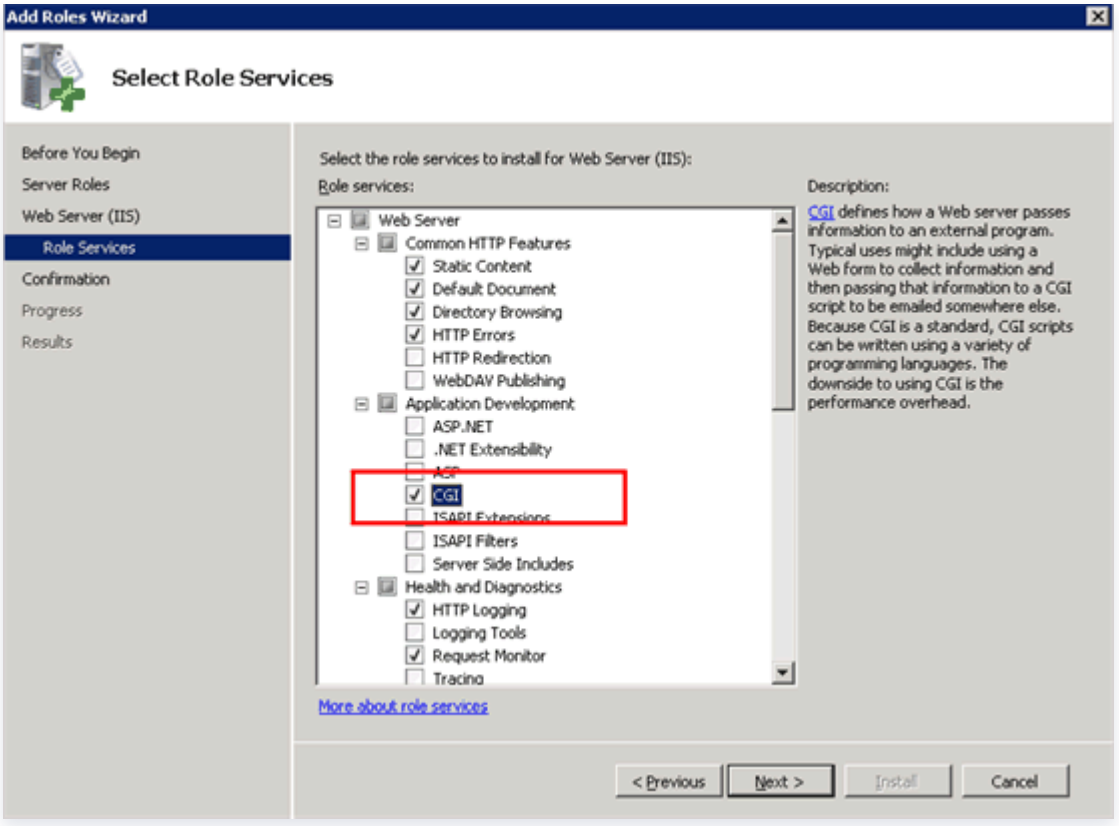
4. Clique em Next (Avançar) na janela "Add Roles Wizard (Assistente para adicionar funções)", conforme mostrado abaixo:



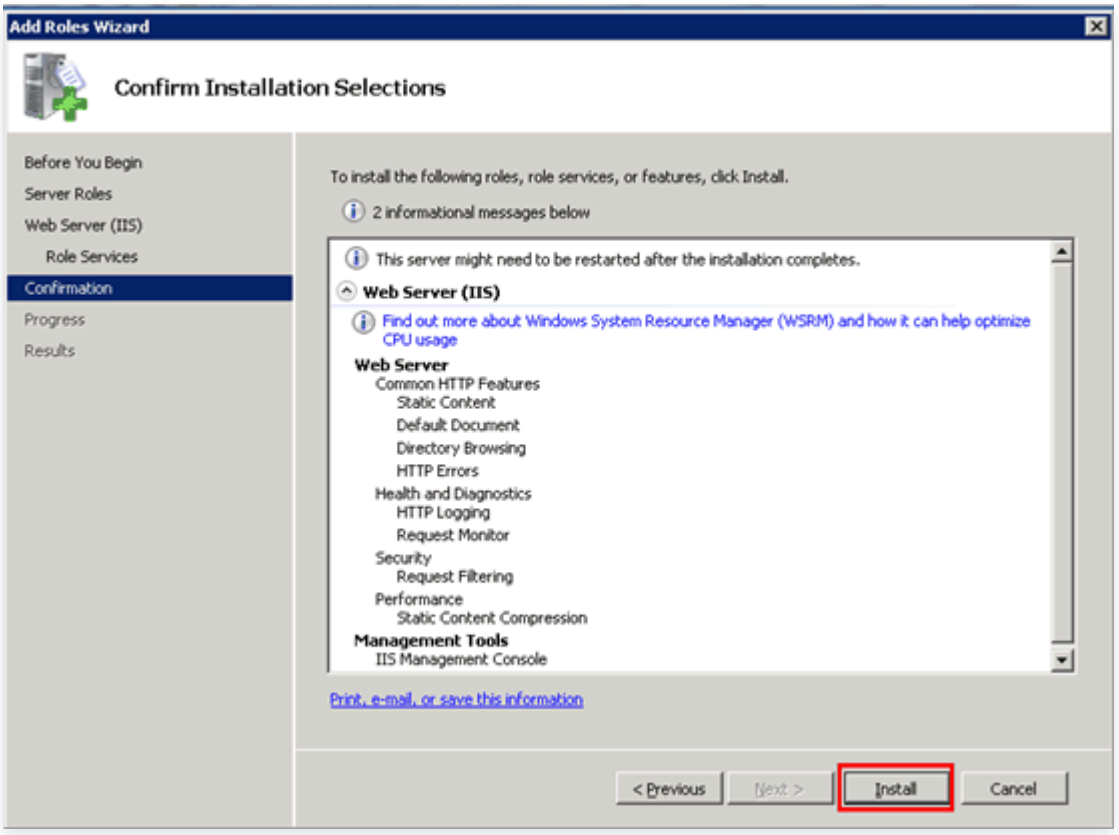
5. Na página "Server Roles (Funções do servidor)", marque Web Server IIS (Servidor web (IIS)) e clique em Next (Avançar) duas vezes, conforme mostrado abaixo:



6. Na página Role Services (Serviços de função), marque CGI e clique em Next (Avançar), conforme mostrado abaixo:



7. Revise suas seleções de instalação e clique em Install (Instalar). Aguarde a conclusão do processo de instalação.



8. Quando a instalação for concluída, abra um navegador no CVM e visite `http://localhost/` para verificar se o IIS foi instalado com sucesso.

Se a página a seguir for exibida, isso indica que o IIS foi instalado com sucesso.

Configurar o ambiente LNMP
Configurar manualmente o ambiente LNMP (CentOS 7)

Last updated: 2024-01-23 17:52:21

Cenário

LNMP se refere a uma arquitetura de servidor web comum que consiste em Nginx, MySQL ou MariaDB e PHP em execução no Linux. Este artigo descreve como implantar LNMP em um Tencent Cloud Virtual Machine (CVM).
Para construir manualmente um ambiente LNMP, é preciso estar familiarizado com os comandos do Linux (consulte Instalação do software usando YUM em um ambiente CentOS, para alguns exemplos), uso e compatibilidade de versão do software a ser instalado.

Versões de software de amostra

Neste exemplo, as seguintes versões de software são usadas para construir o ambiente LNMP:

- Linux: Sistema operacional Linux. Neste exemplo, é usado CentOS 7.6.
- Nginx: web server. Neste exemplo, é usado Nginx 1.17.7.
- MariaDB: banco de dados. Neste exemplo, é usado MariaDB 10.4.8.
- PHP: linguagem de script. Neste exemplo, é usado PHP 7.2.22.

Pré-requisitos

Você ter adquirido um CVM Linux.

Instruções

Etapa 1: login em uma instância do Linux

Faça login em uma instância do Linux usando o modo padrão (recomendado). Você também pode usar outros métodos de login, conforme necessário:

- Faça login em uma instância do Linux usando software de login remoto
- Faça login em uma instância do Linux usando SSH

Etapa 2: Instalação do Nginx

1. Execute o seguinte comando para criar um arquivo chamado `/etc/yum.repos.d/` .

```
vi /etc/yum.repos.d/nginx.repo
```

2. Pressione i para alternar para o modo de edição e digite o seguinte.

```
[nginx]
name = nginx repo
baseurl = https://nginx.org/packages/mainline/centos/7/$basearch/
gpgcheck = 0
enabled = 1
```

3. Pressione Esc, digite :wq, salve o arquivo e retorne.
4. Execute o seguinte comando para instalar o Nginx.

```
yum install -y nginx
```

5. Execute o seguinte comando para abrir o `nginx.conf`.

```
vim /etc/nginx/nginx.conf
```

6. Pressione i para alternar para o modo de edição e edite o arquivo `nginx.conf`.
7. Encontre `server{...}` e substitua a string dentro das chaves pelo seguinte. Isso cancela a escuta do endereço IPv6 e configura o Nginx para realizar a ligação com o PHP.

> **Nota:**
> Você pode usar `Ctrl+F` para page down e `Ctrl+B` para page up para visualizar o arquivo.

```
server {
 listen       80;
 root   /usr/share/nginx/html;
 server_name  localhost;
 #charset koi8-r;
 #access_log  /var/log/nginx/log/host.access.log  main;
 #
 location / {
       index index.php index.html index.htm;
 }
```

```
    #error_page  404              /404.html;
    #redirect server error pages to the static page /50x.html
    #
    error_page   500 502 503 504  /50x.html;
    location = /50x.html {
      root   /usr/share/nginx/html;
    }
    #pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
    #
    location ~ .php$ {
      fastcgi_pass   127.0.0.1:9000;
      fastcgi_index  index.php;
      fastcgi_param  SCRIPT_FILENAME  $document_root$fastcgi_script_name;
      include        fastcgi_params;
    }
  }
```

Se você não conseguir encontrar `server{...}` em `nginx.conf`, adicione o seguinte antes de `include/etc/nginx/conf.d/*conf;`, como mostrado na figura a seguir:

```
http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    keepalive_timeout  65;

    #gzip  on;

    include /etc/nginx/conf.d/*.conf;
}
-- INSERT --                                                30,5          Bot
```

8. Pressione Esc, digite :wq, salve o arquivo e retorne.
9. Execute o seguinte comando para iniciar o Nginx.

```
systemctl start nginx
```

10. Execute o seguinte comando para configurar a ativação automática do Nginx na inicialização.

```
systemctl enable nginx
```

11. Em um navegador local, visite o seguinte URL para verificar se o serviço Nginx está funcionando corretamente.

```
http://<Public IP address of the CVM instance>
```

Se for exibido o seguinte, o Nginx foi instalado e configurado com êxito.

Etapa 3: Instalação da base de dados

1. Execute o seguinte comando para verificar se o MariaDB já está instalado

```
rpm -qa | grep -i mariadb
```

- Se for exibido o seguinte, o MariaDB foi instalado.

```
[root@VM_0_3_centos ~]# rpm -qa | grep -i mariadb
MariaDB-compat-10.2.4-1.el7.centos.x86_64
MariaDB-client-10.2.4-1.el7.centos.x86_64
MariaDB-common-10.2.4-1.el7.centos.x86_64
MariaDB-server-10.2.4-1.el7.centos.x86_64
```

Para evitar conflitos entre versões diferentes, execute o seguinte comando para remover o MariaDB instalado.

```
yum -y remove <Package name>
```

- Se nada for retornado, o MariaDB não está instalado. Nesse caso, prossiga para a próxima etapa.

2. Execute o seguinte comando para criar o arquivo `MariaDB.repo` em `/etc/yum.repos.d/`.

```
vi /etc/yum.repos.d/MariaDB.repo
```

3. Pressione i para mudar para o modo de edição e digite o seguinte para adicionar MariaDB.

> **Nota:**
> Diferentes sistemas operacionais usam diferentes versões do MariaDB. Para obter informações de instalação sobre outras versões de sistema operacional, visite o site do MariaDB.

```
# MariaDB 10.4 CentOS repository list - created 2019-11-05 11:56 UTC
# http://downloads.mariadb.org/mariadb/repositories/
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.4/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

4. Pressione Esc, digite :wq, salve o arquivo e retorne.
5. Execute o seguinte comando para instalar o MariaDB. Preste atenção ao progresso da instalação e aguarde até que ela seja concluída.

```
yum -y install MariaDB-client MariaDB-server
```

6. Execute o seguinte comando para iniciar o serviço MariaDB.

```
systemctl start mariadb
```

7. Execute o seguinte comando para configurar a ativação automática do MariaDB na inicialização.

```
systemctl enable mariadb
```

8. Execute o seguinte comando para verificar se o MariaDB foi instalado com sucesso.

```
mysql
```

Se aparecer o seguinte, o MariaDB foi instalado com sucesso.

```
[root@VM_0_135_centos ~]# systemctl start mariadb
[root@VM_0_135_centos ~]# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.4.8-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

9. Execute o seguinte comando para sair do MariaDB.

```
\q
```

Etapa 4: Instalação e configuração do PHP

1. Execute os comandos a seguir para atualizar a origem do software PHP no Yum.

```
rpm -Uvh https://mirrors.cloud.tencent.com/epel/epel-release-latest-
7.noarch.rpm
```

```
rpm -Uvh https://mirror.webtatic.com/yum/el7/webtatic-release.rpm
```

2. Execute o comando a seguir para instalar os pacotes necessários para o PHP 7.2.

```
yum -y install mod_php72w.x86_64 php72w-cli.x86_64 php72w-
common.x86_64 php72w-mysqlnd php72w-fpm.x86_64
```

3. Execute o seguinte comando para iniciar o serviço PHP–FPM.

```
systemctl start php-fpm
```

4. Execute o seguinte comando para configurar a ativação automática do PHP– FPM na inicialização.

```
systemctl enable php-fpm
```

Verificação de configuração

Após finalizar a configuração de ambientes, conclua as etapas a seguir para verificar se o ambiente LNMP foi construído com sucesso.

1. Execute o seguinte comando para criar um arquivo de teste.

```
echo "<?php phpinfo(); ?>" >> /usr/share/nginx/html/index.php
```

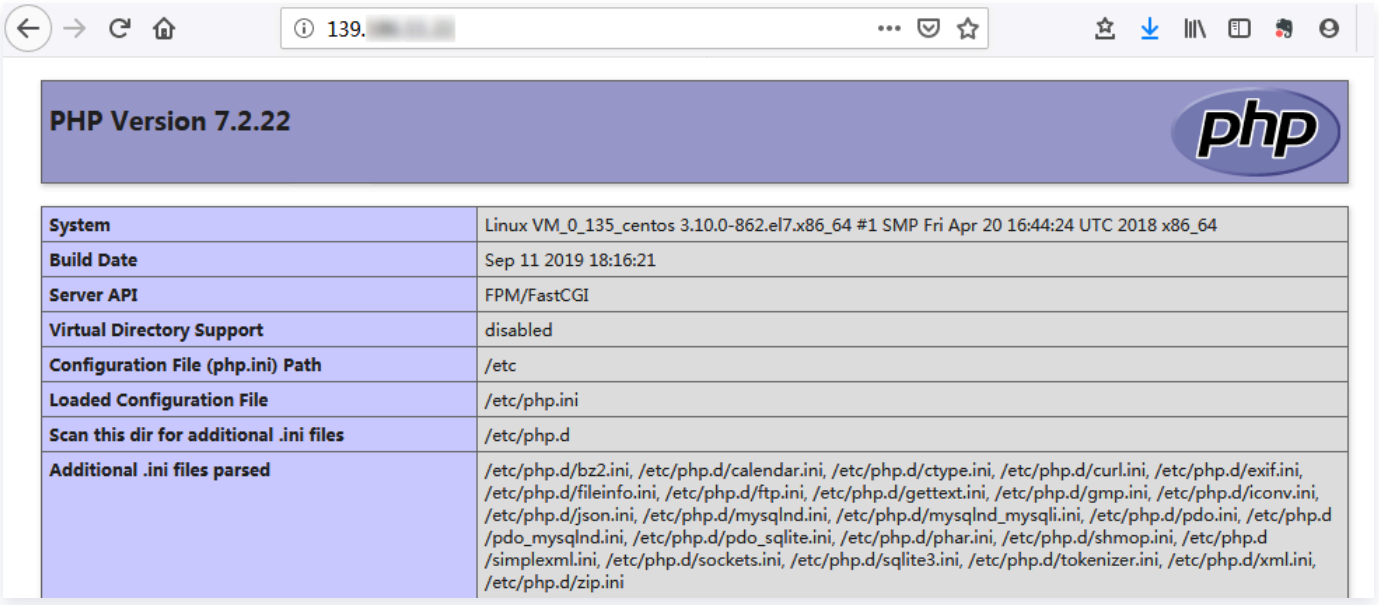
2. Execute o seguinte comando para reiniciar o serviço Nginx.

```
systemctl restart nginx
```

3. Em um navegador local, visite o seguinte URL para verificar se a configuração do ambiente foi bem-sucedida.

```
http://<Public IP address of the CVM instance>
```

Se os resultados a seguir forem exibidos, a configuração do ambiente foi bem-sucedida.



System	Linux VM_0_135_centos 3.10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64
Build Date	Sep 11 2019 18:16:21
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bz2.ini, /etc/php.d/calendar.ini, /etc/php.d/ctype.ini, /etc/php.d/curl.ini, /etc/php.d/exif.ini, /etc/php.d/fileinfo.ini, /etc/php.d/ftp.ini, /etc/php.d/gettext.ini, /etc/php.d/gmp.ini, /etc/php.d/iconv.ini, /etc/php.d/json.ini, /etc/php.d/mysqlnd.ini, /etc/php.d/mysqlnd_mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysqlnd.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/shmop.ini, /etc/php.d/simplexml.ini, /etc/php.d/sockets.ini, /etc/php.d/sqlite3.ini, /etc/php.d/tokenizer.ini, /etc/php.d/xml.ini, /etc/php.d/zip.ini

Operações relevantes

Depois que o ambiente LNMP for construído, você poderá criar um site WordPress.

Perguntas frequentes

Se você encontrar um problema ao usar o CVM, consulte os seguintes documentos para solucionar problemas com base em sua situação real.

- Para questões relacionadas ao login do CVM, consulte Login de senha e login de chave SSH e Login e acesso remoto.
- Para questões relacionadas à rede CVM, consulte Endereços IP e Portas e grupos de segurança.
- Para questões relacionadas aos discos CVM, consulte Discos de sistema e discos de dados.

Configurar ambiente LAMP
Configurar manualmente o ambiente LAMP

Last updated：2024-01-23 17:52:21

Cenário

LAMP é uma arquitetura de serviço comum da web, executada no Linux, que consiste em Apache, MySQL/MariaDB e PHP. Este artigo descreve como configurar o LAMP em um CVM Linux.
Você deve estar familiarizado com os comandos comuns do Linux, como Instalação de software via YUM em um ambiente CentOS, e compreender as versões do software instalado.

Software

Estes são os softwares envolvidos:

- O CentOS é uma distribuição do sistema operacional Linux. Usaremos a versão 7.6 neste artigo.
- Apache é um software de servidor web. Usaremos a versão 2.4.6 neste artigo.
- MariaDB é um sistema de gerenciamento de banco de dados. Usaremos a versão 10.4.8 neste artigo.
- PHP é uma linguagem de script. Usaremos a versão 7.0.33 neste artigo.

Pré-requisitos

Você precisa de um CVM Linux. Se você ainda não comprou um, consulte Introdução aos CVMs Linux.

Instruções

Etapa 1: login em uma instância do Linux

Faça login em uma instância do Linux usando WebShell (recomendado). Você também pode usar outros métodos de login com os quais se sinta confortável:

- Faça login em uma instância do Linux usando software de login remoto.
- Faça login em uma instância do Linux usando SSH

Etapa 2: Instalação do Apache

1. Execute o seguinte comando para instalar o Apache.

```
yum install httpd -y
```

2. Execute os comandos a seguir para iniciar o Apache e defina-o para iniciar automaticamente quando o sistema for iniciado.

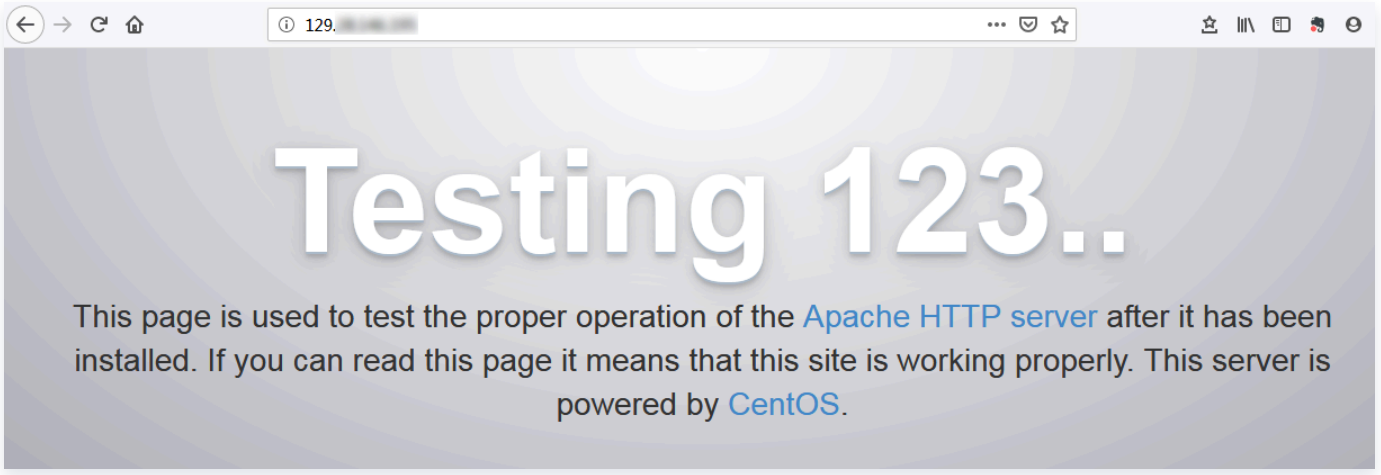
```
systemctl start httpd
```

```
systemctl enable httpd
```

3. Abra uma janela do navegador e visite o seguinte URL para verificar se o Apache está funcionando corretamente.

```
http://[endereço IP público da instância CVM]
```

O seguinte aparecerá se o Apache estiver instalado corretamente:



Etapa 3: Instalação do MariaDB

1. Execute o seguinte comando para verificar se o MariaDB já está instalado

```
rpm -qa | grep -i mariadb
```

- Se for exibido o seguinte, o MariaDB já está instalado.

```
[root@VM_0_3_centos ~]# rpm -qa | grep -i mariadb
MariaDB-compat-10.2.4-1.el7.centos.x86_64
MariaDB-client-10.2.4-1.el7.centos.x86_64
MariaDB-common-10.2.4-1.el7.centos.x86_64
MariaDB-server-10.2.4-1.el7.centos.x86_64
```

Se for esse o caso, execute o seguinte para remover o MariaDB e evitar conflitos entre as diferentes versões.

```
yum -y remove [Package name]
```

- Se nada for retornado, o MariaDB não está instalado. Nesse caso, prossiga para a próxima etapa.

2. Execute o seguinte comando para criar um arquivo chamado `MariaDB.repo` em `/etc/yum.repos.d/`.

```
vi /etc/yum.repos.d/MariaDB.repo
```

3. Pressione i para mudar para o modo de edição e digite o seguinte.

```
# MariaDB 10.4 CentOS repository list - created 2019-11-05 11:56 UTC
# http://downloads.mariadb.org/mariadb/repositories/
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.4/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

> **Nota:**
> Para informações de instalação de outras versões, visite o site oficial do MariaDB.

4. Pressione Esc e insira : wq para salvar o arquivo e voltar.
5. Execute o seguinte comando para instalar o MariaDB.

```
yum -y install MariaDB-client MariaDB-server
```

6. Execute os seguintes comandos para iniciar o MariaDB e defina-o para iniciar automaticamente junto com o sistema.

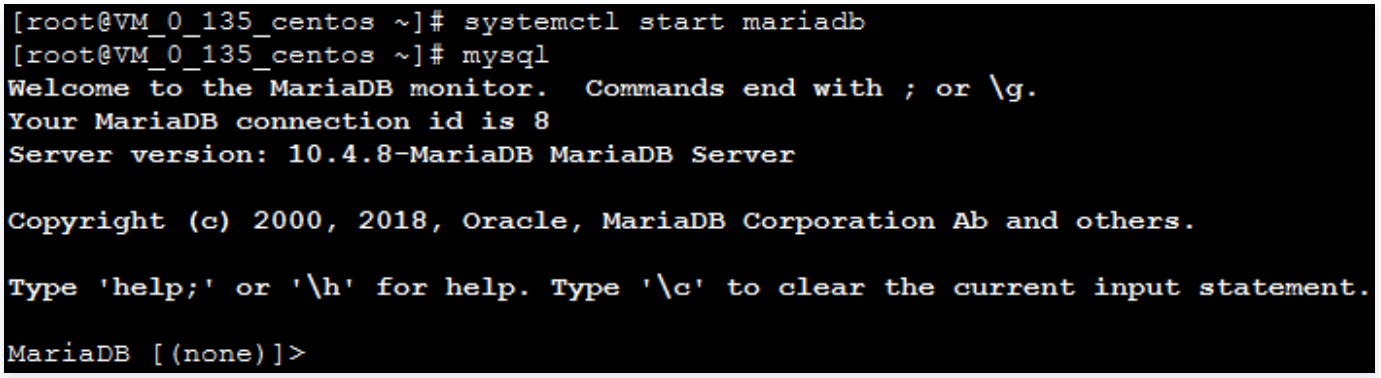
```
systemctl start mariadb
```

```
systemctl enable mariadb
```

7. Execute o seguinte comando para verificar se o MariaDB foi instalado com sucesso.

```
mysql
```

Se for exibido o seguinte, o MariaDB foi instalado com sucesso.



8. Execute o seguinte comando para sair do MariaDB.

```
\q
```

Etapa 4: Instalação e configuração do PHP

1. Execute os comandos a seguir para atualizar a origem do software PHP no Yum.

```
rpm -Uvh https://mirrors.cloud.tencent.com/epel/epel-release-latest-
7.noarch.rpm
```

```
rpm -Uvh https://mirror.webtatic.com/yum/el7/webtatic-release.rpm
```

2. Execute o comando a seguir para instalar os pacotes necessários para o PHP 7.0.33.

```
yum -y install php70w php70w-opcache php70w-mbstring php70w-gd php70w-
xml php70w-pear php70w-fpm php70w-mysql php70w-pdo
```

3. Execute o seguinte comando para editar o arquivo de configuração do Apache.

```
vi /etc/httpd/conf/httpd.conf
```

4. Pressione i para entrar no modo de edição e fazer as seguintes alterações:

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80
ServerName localhost:80

#
```

```
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all granted
</Directory>

#
```

```
#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex index.php index.html
</IfModule>

#
```

```
# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps

#
```

4.1 Encontre `ServerName www.example.com: 80` e inicie uma nova linha abaixo dele. Insira o seguinte:

```
ServerName localhost:80
```

4.2 Encontre `Require all denied` em `<Directory>` e altere para `Require all granted`.

4.3 Encontre `<IfModule dir_module>` e altere o conteúdo para `DirectoryIndex index.php index.html`.

4.4 Inicie uma nova linha abaixo de `AddType application/x-gzip .gz .tgz` e insira o seguinte:

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

5. Pressione Esc e insira : wq para salvar o arquivo e voltar.
6. Execute o seguinte comando para reiniciar o Apache.

```
systemctl restart httpd
```

Verificação da configuração do ambiente.

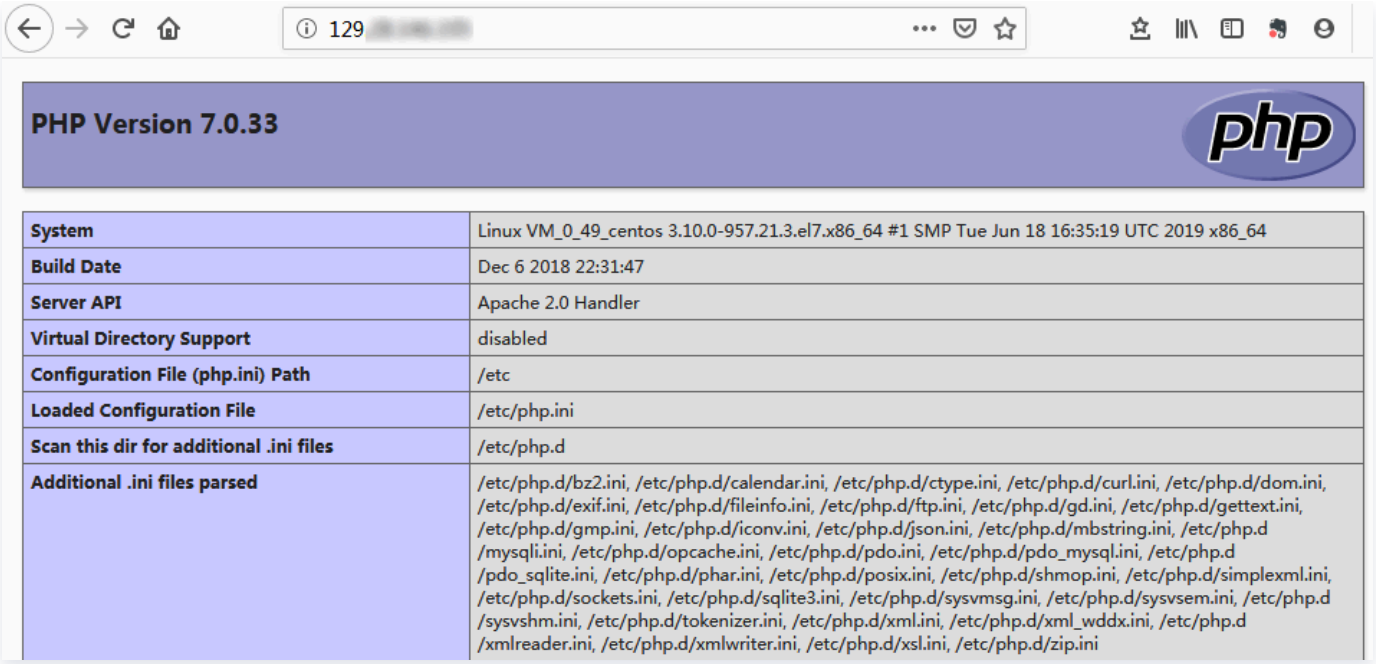
1. Execute o seguinte comando para criar um arquivo de teste.

```
echo "<?php phpinfo(); ?>" >> /var/www/html/index.php
```

2. Abra uma janela do navegador em sua máquina local e visite a seguinte URL para verificar se a configuração do ambiente foi bem-sucedida.

```
http://CVM Public IP/index.php
```

Se o seguinte for exibido, o ambiente LAMP foi configurado com sucesso.



System	Linux VM_0_49_centos 3.10.0-957.21.3.el7.x86_64 #1 SMP Tue Jun 18 16:35:19 UTC 2019 x86_64
Build Date	Dec 6 2018 22:31:47
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bz2.ini, /etc/php.d/calendar.ini, /etc/php.d/ctype.ini, /etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/exif.ini, /etc/php.d/fileinfo.ini, /etc/php.d/ftp.ini, /etc/php.d/gd.ini, /etc/php.d/gettext.ini, /etc/php.d/gmp.ini, /etc/php.d/iconv.ini, /etc/php.d/json.ini, /etc/php.d/mbstring.ini, /etc/php.d /mysqli.ini, /etc/php.d/opcache.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d /pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/shmop.ini, /etc/php.d/simplexml.ini, /etc/php.d/sockets.ini, /etc/php.d/sqlite3.ini, /etc/php.d/sysvmsg.ini, /etc/php.d/sysvsem.ini, /etc/php.d /sysvshm.ini, /etc/php.d/tokenizer.ini, /etc/php.d/xml.ini, /etc/php.d/xml_wddx.ini, /etc/php.d /xmlreader.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini, /etc/php.d/zip.ini

Operações relevantes

Depois que o ambiente LAMP é construído, você pode configurar manualmente o site Drupal.

Perguntas frequentes

Se você encontrar um problema ao usar o CVM, consulte os seguintes documentos para solucionar problemas com base em sua situação real.

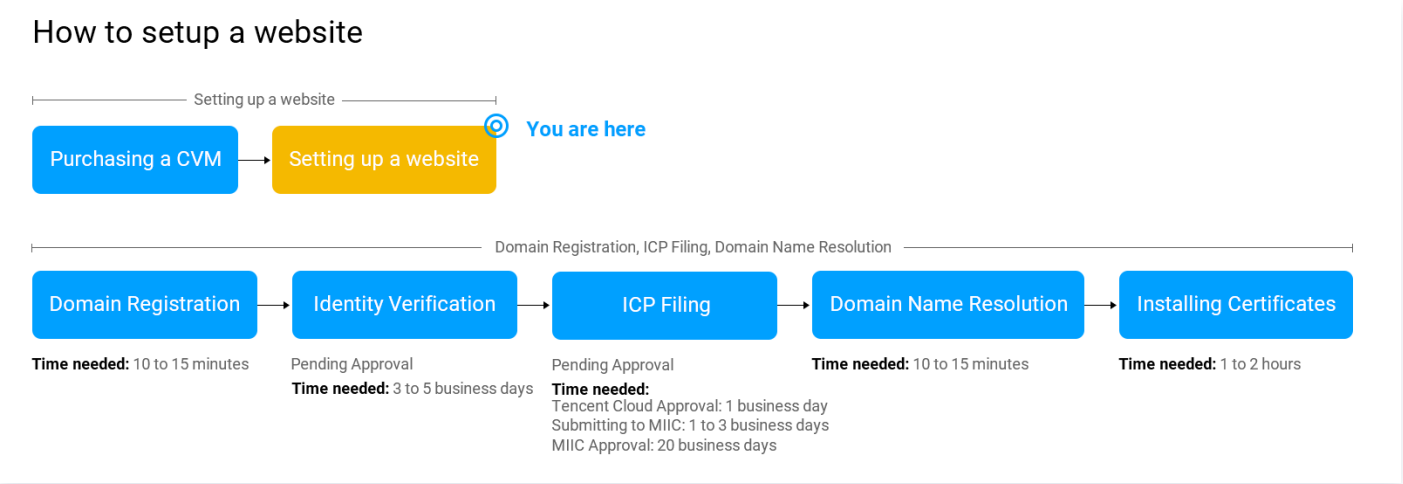
- Para questões relacionadas ao login do CVM, consulte Login de senha e login de chave SSH e Login e acesso remoto.
- Para questões relacionadas à rede CVM, consulte Endereços IP e Portas e grupos de segurança.
- Para questões relacionadas aos discos CVM, consulte Discos de sistema e dados.

Configurar o site

Visão geral da configuração do site

Last updated：2024-01-23 17:52:21

Administrar um site ou fórum pessoal é uma das coisas mais comuns que as pessoas fazem depois de comprar um CVM.



Este artigo descreve várias maneiras de configurar um site em seu CVM. Escolha aquele que melhor se adapta a você.

Configuração manual de um site

Recomendamos que você configure seu site manualmente.

	Configuração manual
Configuração	Instalação manual de software. Mais fácil de personalizar.
Vantagens	Escolhas flexíveis entre versões de software
Duração	Mais longa, já que você precisa fazer isso manualmente
Dificuldade	Saber como instalar o software manualmente e qual versão usar.

Instruções

Use a tabela a seguir para escolher um site que atenda às suas necessidades.

Tipo	Configuração	Descrição

WordPress	WordPress (Linux) WordPress (Windows)	WordPress é uma plataforma de blog desenvolvida em PHP. É possível usá-lo como um sistema de gerenciamento de conteúdo ou para criar sites em serviços compatíveis com PHP e bancos de dados MySQL.
Discuz!	Discuz!	Discuz! é um software de fórum popular construído em PHP e MySQL. Você só precisa configurar alguns itens para colocá-lo em funcionamento.
LNMP	LNMP(CentOS 7) LNMP(CentOS 6) LNMP(openSUSE)	LNMP é uma arquitetura de serviço web comum que consiste em Nginx, MySQL/MariaDB e PHP rodando em Linux.
LAMP	LAMP	LAMP é uma arquitetura de serviço web comum que consiste em Apache, MySQL/MariaDB e PHP rodando em Linux.
WIPM	WIPM	WIPM é uma arquitetura de serviço web que consiste em IIS, PHP e MySQL rodando em Windows.
Drupal	Drupal	Drupal é um Estrutura de Gerenciamento de Conteúdo (CMF, sigla em inglês) escrito em PHP. Consiste em um Sistema de Gerenciamento de Conteúdo (CMS, sigla em inglês) e uma estrutura de desenvolvimento PHP. Você pode usá-lo para administrar um blog pessoal ou site corporativo.
Ghost	Ghost	Ghost é uma plataforma de blog de código aberto gratuita, escrita em JavaScript e distribuída sob a licença MIT, projetada para simplificar o processo de publicação online para blogueiros, bem como para publicações online.

Configurar o site

Last updated：2024-01-23 17:52:21

Este documento fornece referência para a construção de sites pessoais no Tencent Cloud CVM. Se você ainda não tem um CVM, pode adquirir um por meio da página de compra do CVM.

Etapa 1. Implementar um site

Para desenvolver e implementar manualmente seu site, consulte:

- Configuração de um site
- Configuração do WordPress
- Criação de fórum no Discuz!
- Configuração do Drupal
- Configuração de um Ghost Blog

Se você tiver alguma dúvida ao configurar um site, consulte Sobre a construção de um site para resolução de problemas.

Etapa 2. Publicar um site

Para publicar um site implementado na Internet e permitir que os usuários o acessem, é necessário concluir o registro e a resolução do nome de domínio e o preenchimento do ICP (para sites em execução no continente chinês).

Configurar o fórum Discuz!
Configurar manualmente o fórum Discuz!

Last updated：2024-01-23 17:52:21

Visão geral

Utilizado em mais de 2 milhões de sites, o Discuz! é o software de fórum mais sofisticado e predominante do mundo. Este documento descreve como criar um site usando o Discuz! na instância Tencent Cloud CVM e implementar o ambiente de tempo de execução LAMP (Linux, Apache, MariaDB e PHP) necessário.
Para configurar manualmente um site Discuz!, você deve estar familiarizado com os comandos comuns do Linux (consulte Instalação do software via YUM no ambiente CentOS, e entender o uso e a compatibilidade da versão do software a ser instalado.

Software

O seguinte software é usado para desenvolver um site Discuz!.

- Linux: Sistema operacional Linux. Este documento usa a versão CentOS 7.6 como exemplo.
- Apache: Software de servidor da web. Este documento usa o Apache 2.4.15 como exemplo.
- MariaDB: banco de dados. Este documento usa o MariaDB 5.5.60 como exemplo.
- PHP: linguagem de script. Este documento usa o PHP 5.4.16 como exemplo.
- Discuz!: software de fórum. Este documento usa o Discuz! X3.4 como um exemplo.

Instruções

Etapa 1: fazer login no CVM

Consulte Fazer login na instância do Linux usando o método de login padrão. Você também pode usar outros métodos de login com os quais se sinta mais confortável:

- Faça login em instâncias do Linux por meio de ferramentas de login remoto.
- Faça login em instância do Linux via chave SSH

Etapa 2: configurar o ambiente LAMP

O Tencent Cloud hospeda um repositório de software que contém lançamentos oficiais CentOS e fornece a versão mais recente e estável. Use o Yum para instalar rapidamente o CentOS.

Instalação e configuração do software necessário

1. Execute o seguinte comando para instalar o Apache, MariaDB, PHP e Git:

```
yum install httpd php php-fpm php-mysql mariadb mariadb-server git -y
```

2. Execute os seguintes comandos em sequência para iniciar os serviços.

```
systemctl start httpd
```

```
systemctl start mariadb
```

```
systemctl start php-fpm
```

3. Execute o seguinte comando para definir uma senha para o usuário `root` e concluir outras configurações básicas, para que o usuário raiz possa acessar o banco de dados.

> ⚠ Atenção:
> - Execute o seguinte comando para definir a senha antes de seu primeiro login no MariaDB.
> - Ao visualizar a solicitação para digitar a senha raiz, pressione Enter para definir a senha. Sua senha não será exibida por padrão. Conclua outras configurações básicas conforme solicitado.

```
mysql_secure_installation
```

4. Execute o seguinte comando para fazer login no MariaDB. Digite a senha que você definiu na etapa 3 e pressione Enter.

```
mysql -u root -p
```

Um login bem-sucedido é mostrado abaixo:

```
[root@VM_149_104_centos ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 27
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

5. Execute o seguinte comando para sair do MariaDB.

```
\q
```

Verificação da configuração do ambiente

Verifique se o ambiente está configurado corretamente conforme as instruções abaixo:

1. Execute o seguinte comando para criar um arquivo de teste `test.php` no diretório raiz padrão `/var/www/html` do Apache:

```
vim /var/www/html/test.php
```

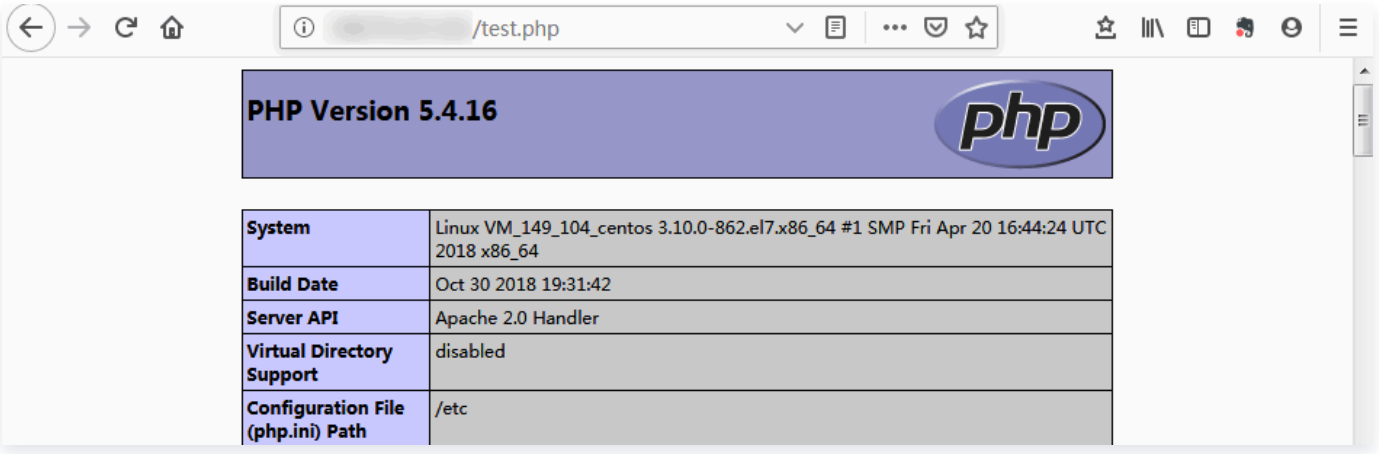
2. Pressione i para alternar para o modo de edição e insira o seguinte conteúdo:

```
<?php
echo "<title>Test Page</title>";
phpinfo()
?>
```

3. Pressione Esc e digite :wq para salvar e fechar o arquivo.
4. Insira o seguinte URL em um navegador para acessar `test.php` e verificar se o ambiente está configurado corretamente.

```
http://[endereço IP público do CVM]/test.php
```

Se tudo correr bem, aparecerá o seguinte.



Etapa 3: instalação e configuração do Discuz!

Fazer download do Discuz!

Execute o seguinte comando para fazer download do pacote de instalação.

```
git clone https://gitee.com/Discuz/DiscuzX.git
```

Preparação para a instalação

1. Execute o seguinte comando para acessar o diretório de instalação.

   ```
   cd DiscuzX
   ```

2. Execute o seguinte comando para copiar todos os arquivos em "upload" para "/var/www/html/".

   ```
   cp -r upload/* /var/www/html/
   ```

3. Execute o seguinte comando para conceder aos usuários a permissão de gravação.

   ```
   chmod -R 777 /var/www/html
   ```

Instalação do Discuz!

1. Digite o endereço IP do seu site Discuz! (o endereço IP público de sua instância CVM) na caixa de endereço, ou você pode vincular um nome de domínio disponível ao seu endereço IP.
2. Clique em I agree (Concordo) e vá para a página de verificação do ambiente.
3. Verifique os itens e clique em Next Step (Próxima etapa).
4. Selecione Clean Install (Limpar instalação) e clique em Next Step (Próxima etapa).
5. Insira as informações solicitadas para criar um novo banco de dados para Discuz!.

   > ⚠ Atenção:
   > - Use `root` e a senha definida em Instalação e configuração do software necessário para se conectar ao banco de dados e configurar um endereço de e-mail do sistema e nome de usuário, senha e endereço de e-mail do administrador.
   > - Lembre-se de seu nome de usuário e senha de administrador.

6. Clique em Next Step (Próxima etapa) para iniciar a instalação.
7. Após a instalação, clique em Your forum has been installed successfully. Click here to access (Seu fórum foi instalado com sucesso. Clique aqui para acessar). para acessar seu fórum.

Uso de um nome de domínio

Usar um nome de domínio em vez de um IP pode ajudar os usuários a se lembrarem de seu site com mais facilidade.

Perguntas frequentes

Verifique a documentação a seguir para conferir problemas na utilização do CVM:

- Login no CVM: Login de senha e login de chave SSH e Login e acesso remoto
- Rede CVM: Endereço IP e Porta
- Discos CVM: Sistema e discos de dados

Configurar manualmente o blog Ghost

Last updated: 2025-09-05 16:27:51

Cenário

Ghost é uma plataforma de blog de código aberto gratuita, escrita em JavaScript e distribuída sob a licença MIT, projetada para simplificar o processo de publicação online para blogueiros, bem como para publicações online. Este artigo descreve como configurar o Ghost em um CVM.
Para configurar o Ghost, você deve estar familiarizado com o Linux e seus comandos comuns, como Instalar software via Apt-get no ambiente Ubuntu.

Software

Este artigo usa o seguinte software:

- Sistemas operacionais Linux. Este artigo usa o Ubuntu 18.04.
- Nginx 1.14.0 é usado para fornecer serviço da web.
- MySQL 5.7.27 é usado para banco de dados.
- Node.js 10.17.0 é nosso ambiente de tempo de execução.
- Ghost 3.0.2

Pré-requisitos

É preciso possuir um CVM Linux. Se você ainda não comprou um, consulte Introdução aos CVMs Linux.

- Um nome de domínio que aponta para o seu CVM. Se o nome de domínio for usado para o serviço na China Continental, o preenchimento do ICP é necessário.

Instruções

Etapa 1 Login em uma instância do Linux

- Faça login em uma instância do Linux usando WebShell (recomendado). Você também pode usar outros métodos de login com os quais se sinta confortável:
- Faça login em uma instância do Linux usando software de login remoto.
- Faça login em uma instância do Linux usando SSH

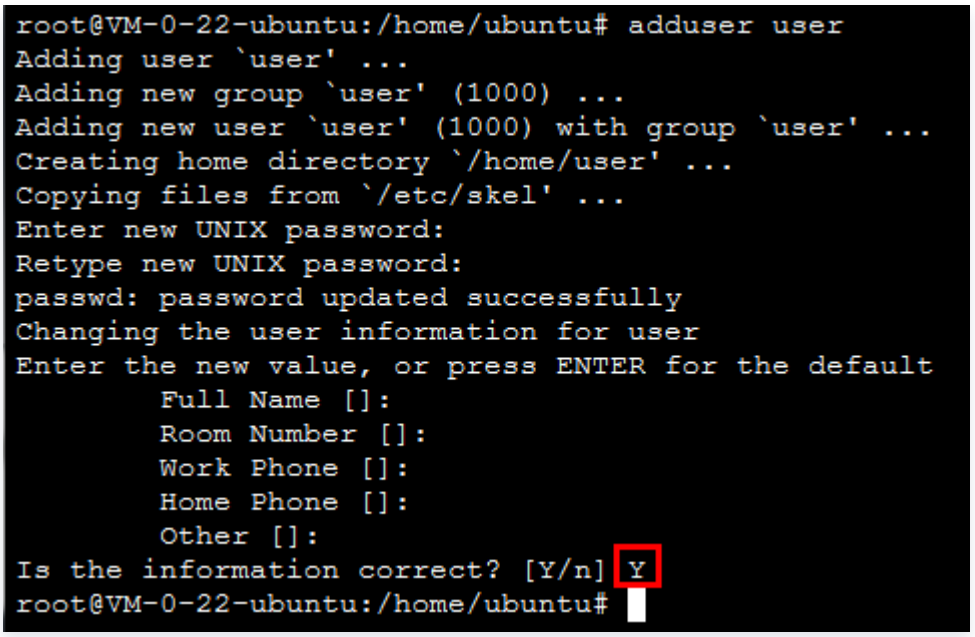
Etapa 2 Criar um novo usuário

1. Após fazer o login, mude para `root`. Consulte este artigo para obter detalhes.
2. Execute o seguinte comando para criar um usuário chamado `user`.

> Não use `ghost` como nome de usuário. Isso causa conflitos com o Ghost-CLI.

```
adduser user
```

1. Insira e confirme a senha conforme solicitado. A senha não é mostrada por padrão. Pressione Enter para continuar.
2. Insira as informações do usuário. Ou pressione Enter para ignorá-las e continuar.
3. Insira Y para confirmar e pressione Enter para concluir o processo, conforme mostrado abaixo:



4. Execute o seguinte comando para adicionar privilégios de usuário.

```
usermod -aG sudo user
```

5. Execute o seguinte comando para mudar para o usuário `user`.

```
su user
```

Etapa 3 Atualizar os pacotes instalados

Execute os seguintes comandos para atualizar os pacotes instalados.

> Insira a senha para `user` conforme solicitado e pressione Enter para iniciar.

```
sudo apt-get update
```

```
sudo apt-get upgrade -y
```

Etapa 4 Configurar o ambiente

Instalação do Nginx

Execute o seguinte comando para instalar o Nginx.

```
sudo apt-get install -y nginx
```

Instalação e configuração do MySQL

1. Execute o seguinte comando para instalar o MySQL.

   ```
   sudo apt-get install -y mysql-server
   ```

2. Execute o seguinte comando para fazer login no MySQL.

   ```
   sudo mysql
   ```

3. Execute o seguinte comando para criar um banco de dados para o Ghost chamado `ghost_data`.

   ```
   CREATE DATABASE ghost_data;
   ```

4. Execute o seguinte comando para definir uma senha para o usuário do banco de dados `root`.

   ```
   ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY
   'your_password';
   ```

5. Execute o seguinte comando para sair do MySQL.

   ```
   \q
   ```

Instalar o Node.js

1. Execute o seguinte comando para definir uma versão Node.js padrão a ser usada.

   ```
   curl -sL https://deb.nodesource.com/setup_10.x | sudo -E bash
   ```

2. Execute o seguinte comando para instalar o Node.js.

```
sudo apt-get install -y nodejs
```

Instalação do Ghost-CLI

Execute o seguinte comando para instalar o Ghost-CLI, o que ajuda a configurar o Ghost.

```
sudo npm install ghost-cli@latest -g
```

Etapa 5 Instalar e configurar o Ghost

1. Execute os seguintes comandos.

```
sudo mkdir -p /var/www/ghost
```

```
sudo chown user:user /var/www/ghost
```

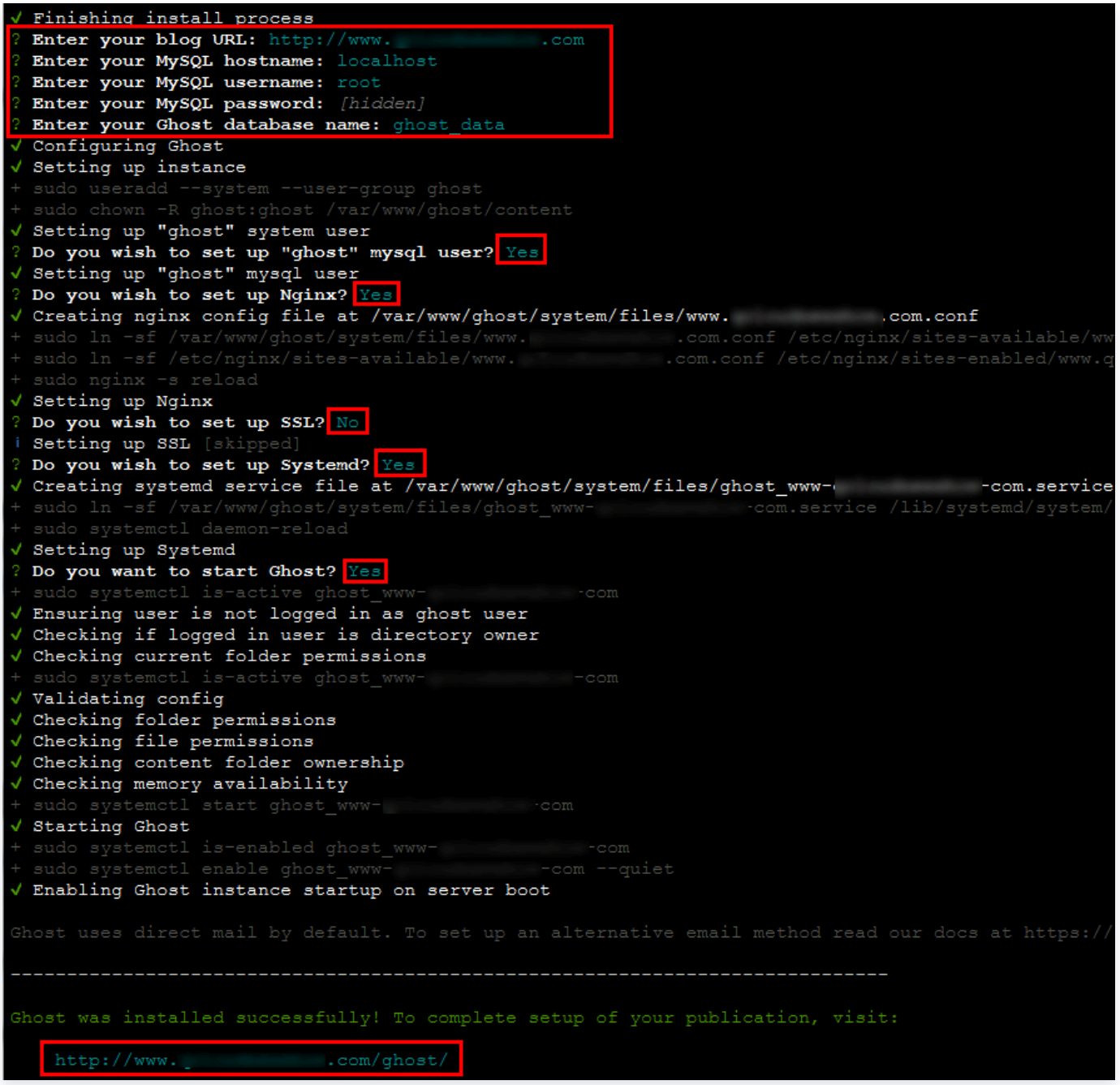
```
sudo chmod 775 /var/www/ghost
```

```
cd /var/www/ghost
```

2. Execute o seguinte comando para instalar o Ghost.

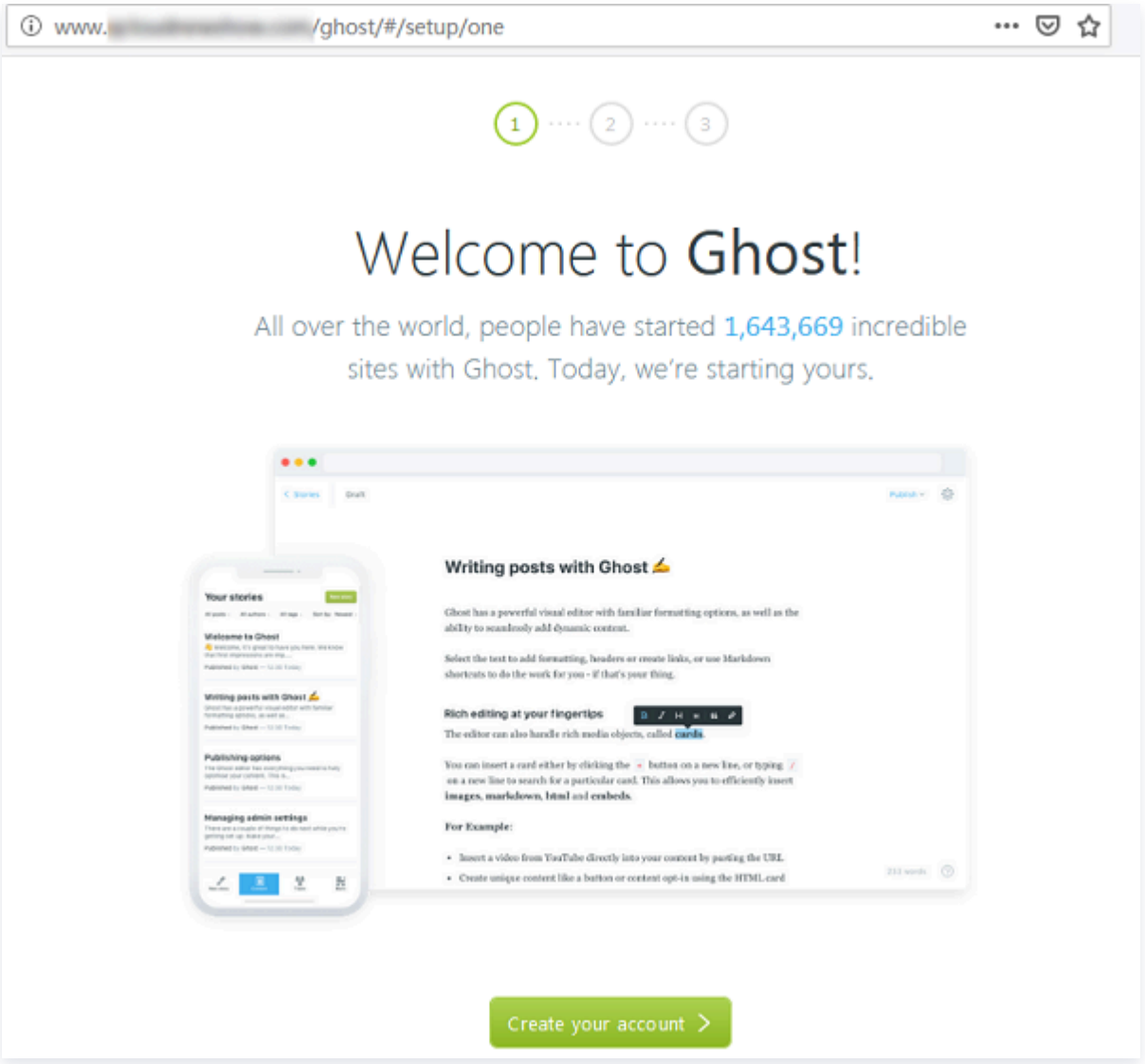
```
ghost install
```

3. Use a imagem a seguir para concluir o processo de instalação.

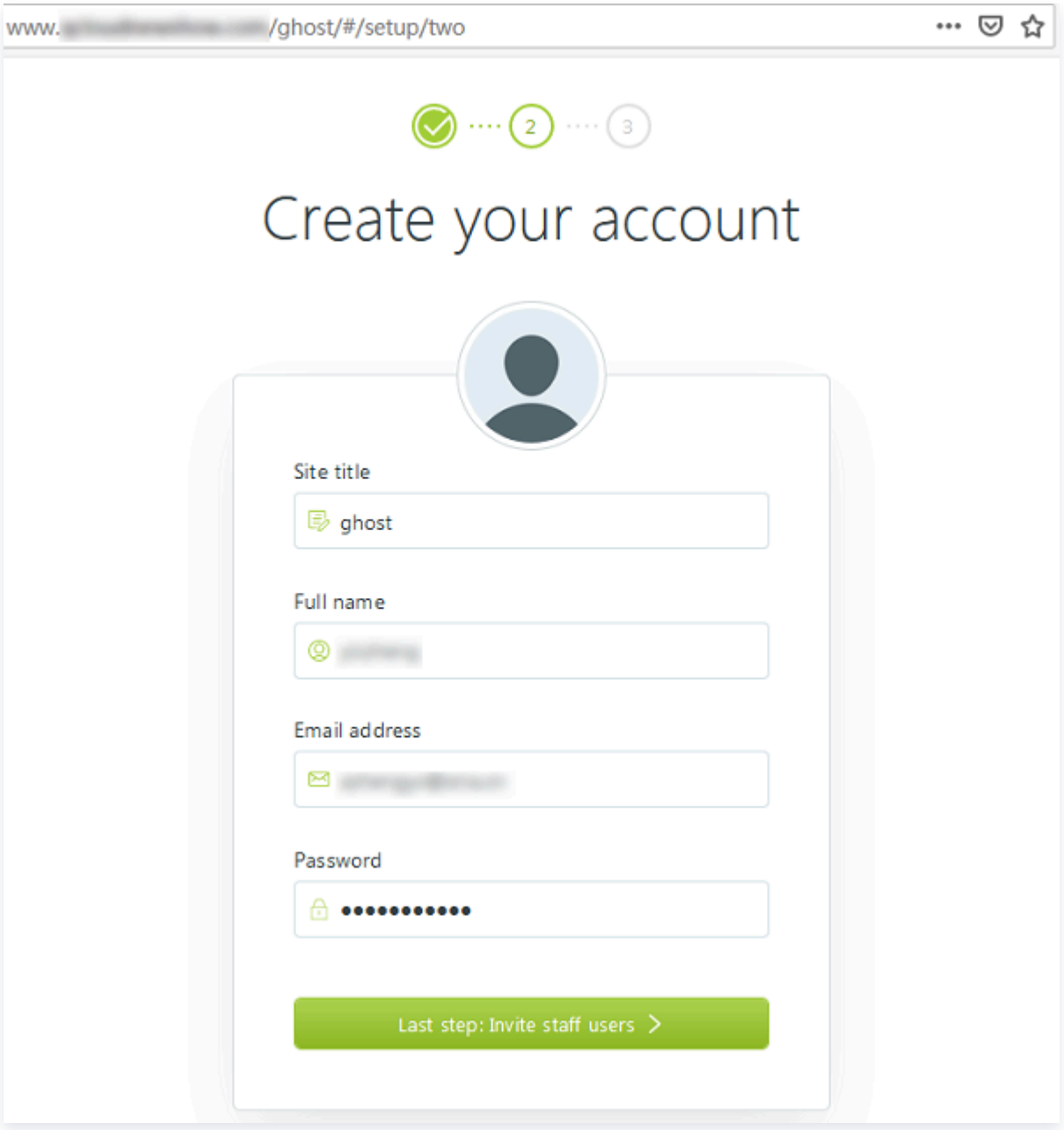


1. Enter your blog URL: insira o seu nome de domínio no formato `http://your_domain_name`.
2. Enter your MySQL hostname: insira o endereço do seu banco de dados. Use `localhost` neste caso e pressione Enter.
3. Enter your MySQL username: insira o nome de usuário que você usa para se conectar ao MySQL. Use `root` neste caso e pressione Enter.
4. Enter your MySQL password: insira a senha correspondente que você definiu anteriormente e pressione Enter.
5. Enter your database name: insira o nome do banco de dados que você criou para o Ghost na etapa anterior. Use `ghost_data` e pressione Enter.

6. Insira Y ou N para completar a configuração.
   O URL do administrador aparece na parte inferior da tela.
7. Abra uma janela do navegador em sua máquina local e visite o URL de administrador para começar a configurar seu blog.
   Clique em para criar **Create account (Criar conta)**uma conta de administrador.

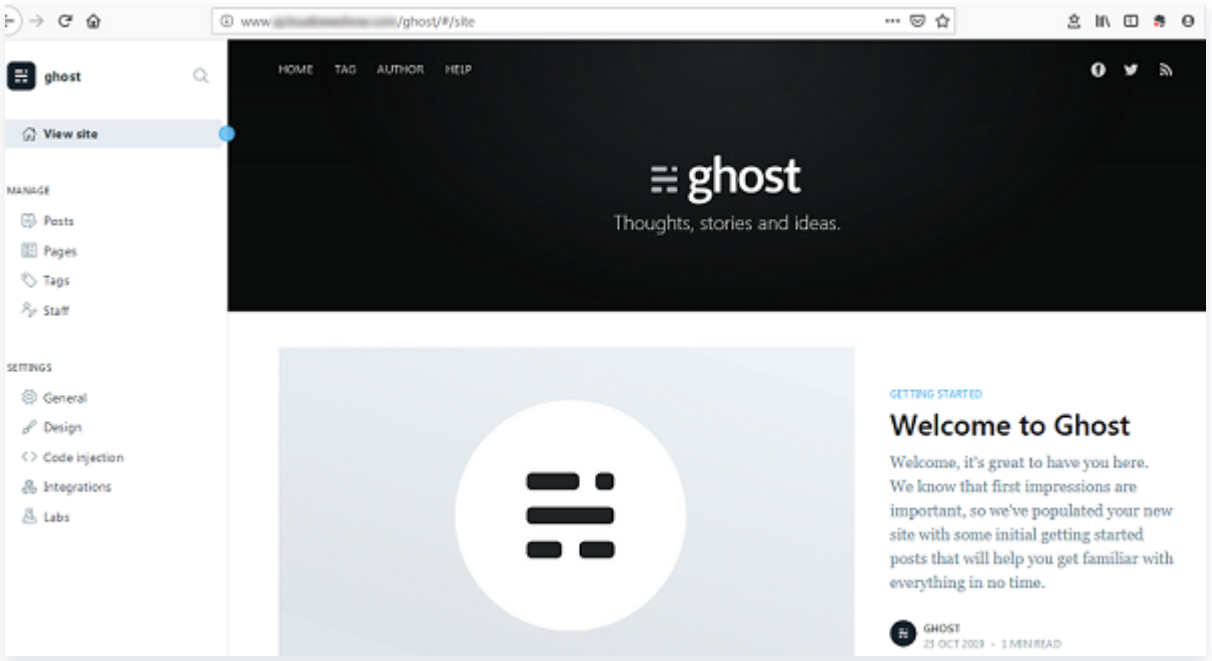


8. Insira as informações desejadas e clique em Last step (Última etapa), conforme mostrado abaixo:

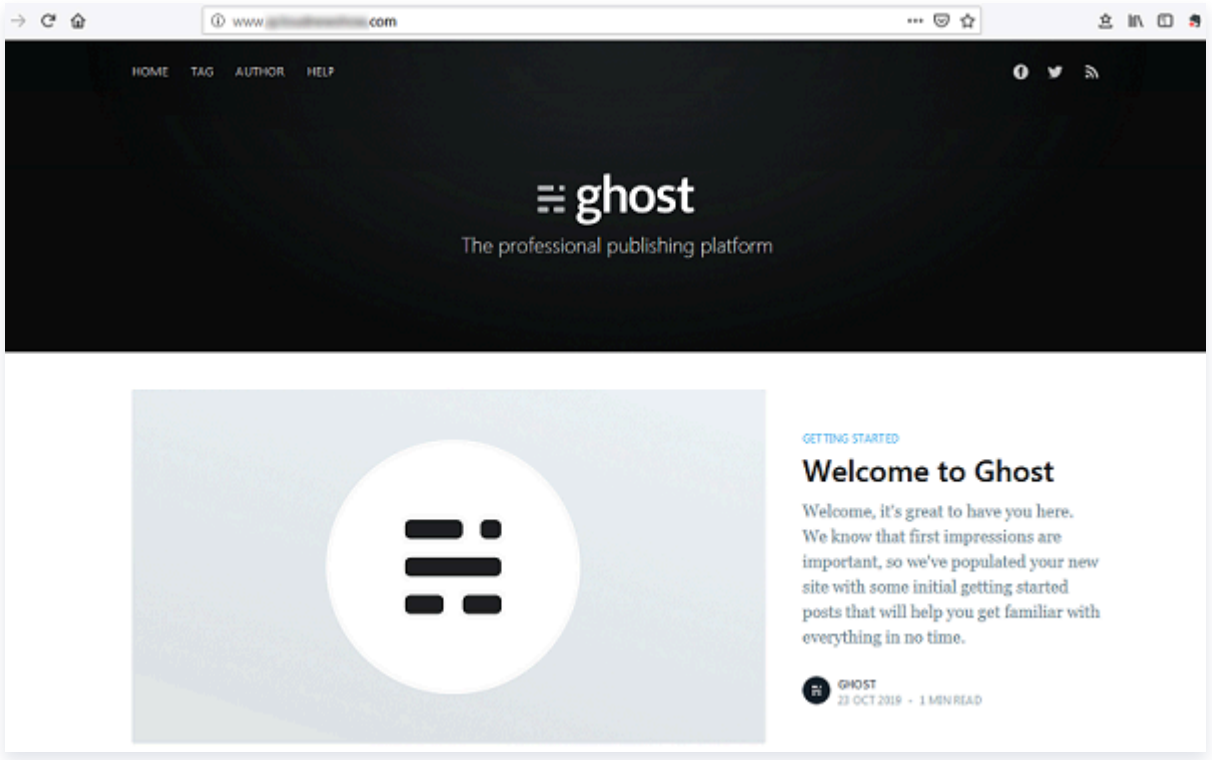


9. Você pode convidar outras pessoas para criarem blogs ou pode pular esta etapa.

10. Acesse a página de administração para gerenciar blogs, conforme mostrado abaixo:



Quando terminar, use um navegador para visitar seu nome de domínio `www.xxxxxxxx.xx` para ver seu blog, conforme mostrado abaixo:



Perguntas frequentes

Se você encontrar um problema ao usar o CVM, consulte os seguintes documentos para solucionar problemas com base em sua situação real.

- Para questões relacionadas ao login do CVM, consulte Login de senha e login de chave SSH e Login e acesso remoto.
- Para questões relacionadas à rede CVM, consulte Endereços IP e Portas e grupos de segurança.
- Para questões relacionadas aos discos CVM, consulte Discos de sistema e dados.

Configurar o aplicativo
Configurar o serviço FTP
Configurar o serviço FTP na instância Linux

Last updated: 2024-01-23 17:52:21

Cenário

Very Secure FTP Daemon (Vsftpd) é o servidor FTP padrão para a maioria das distribuições Linux. Este documento usa um CVM CentOS 7.6 de 64 bits como exemplo para descrever como usar o vsftpd para configurar o serviço FTP para um CVM Linux.

Software

A seguir estão os programas de software para configurar o serviço FTP.

- Linux: Imagem pública CentOS 7.6
- Vsftpd: vsftpd 3.0.2

Instruções

Etapa 1: Faça login no CVM

Faça login em uma instância do Linux usando WebShell (recomendado). Você também pode usar qualquer um dos métodos de login a seguir com os quais se sinta confortável.

- Login em uma instância do Linux usando software de login remoto
- Faça login em uma instância do Linux usando SSH

Etapa 2: Instalar vsftpd

1. Execute o seguinte comando para instalar o vsftpd:

```
yum install -y vsftpd
```

2. Execute o seguinte comando para iniciar automaticamente o vsftpd na inicialização do sistema:

```
systemctl enable vsftpd
```

3. Execute o seguinte comando para iniciar o serviço FTP:

```
systemctl start vsftpd
```

4. Execute o seguinte comando para verificar se o serviço foi iniciado:

```
netstat -antup | grep ftp
```

Se as informações a seguir forem exibidas, o serviço FTP foi iniciado.

```
[root@VM_0_117_centos ~]# systemctl start vsftpd
[root@VM_0_117_centos ~]# netstat -antup | grep ftp
tcp6       0      0 :::21                   :::*                    LISTEN      5123/vsftpd
```

Por padrão, o vsftpd habilitou o modo de acesso anônimo. É possível fazer login no servidor FTP sem inserir um nome de usuário ou senha. No entanto, você não tem permissão para modificar ou fazer upload de arquivos neste modo de login.

Etapa 3: Configurar vsftpd

1. Execute o seguinte comando para criar um usuário para o serviço FTP que, neste caso, é ftpuser:

```
useradd ftpuser
```

2. Execute o seguinte comando para definir uma senha para ftpuser:

```
passwd ftpuser
```

Após inserir a senha, pressione Enter para confirmar. Por padrão, a senha não é exibida. Neste caso, a senha usada como exemplo é `tf7295TFY`.

3. Execute o seguinte comando para criar um diretório de arquivo para o serviço FTP que, neste caso, é `/var/ftp/test`:

```
mkdir /var/ftp/test
```

4. Execute o seguinte comando para modificar a permissão do diretório:

```
chown -R ftpuser:ftpuser /var/ftp/test
```

5. Execute o seguinte comando para abrir o arquivo `vsftpd.conf`:

```
vim /etc/vsftpd/vsftpd.conf
```

6. Pressione i para alternar para o modo de edição. Selecione um modo FTP com base em suas necessidades reais e modifique o arquivo de configuração `vsftpd.conf`.

> ⚠ Atenção:
> O servidor FTP pode se conectar ao cliente em modo ativo ou passivo para transmissão de dados. Devido às configurações de firewall da maioria dos clientes e ao fato de que o endereço IP real não pode ser obtido, recomendamos que você use o modo passivo para configurar o serviço FTP. A seguinte modificação usa o modo passivo como exemplo. Para usar o modo ativo, consulte Configuração do modo FTP ativo.

6.1 Modifique os parâmetros de configuração a seguir para definir permissões de login para usuários anônimos e locais, defina o caminho para armazenar a lista de usuários excepcionais e habilite a escuta em soquetes IPv4.

```
anonymous_enable=NO
local_enable=YES
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
listen=YES
```

6.2 Adicione o sinal de cerquilha (`#`) no início da linha seguinte para anotar `listen_ipv6=YES` e desabilitar a escuta em soquetes IPv6.

```
#listen_ipv6=YES
```

6.3 Adicione os seguintes parâmetros de configuração para habilitar o modo passivo, defina o diretório onde os usuários locais residem após o login e defina o intervalo de portas para transmissão de dados pelo CVM.

```
local_root=/var/ftp/test
allow_writeable_chroot=YES
pasv_enable=YES
pasv_address=xxx.xx.xxx.xx # Substituir xxx.xx.xxx.xx pelo
endereço IP público do CVM Linux
pasv_min_port=40000
```

```
pasv_max_port=45000
```

7. Pressione Esc e digite :wq. Em seguida, salve as alterações e feche o arquivo.
8. Execute o seguinte comando para criar e editar o arquivo `chroot_list`:

```
vim /etc/vsftpd/chroot_list
```

9. Pressione i para alternar para o modo de edição e digite o nome de usuário. Observe que cada nome de usuário ocupa uma linha. Após terminar a configuração, pressione Esc e digite :wq. Em seguida, salve a alteração e feche o arquivo.
   Se você não precisa definir usuários excepcionais, pule esta etapa digitando :wq e fechando o arquivo.
10. Execute o seguinte comando para reiniciar o serviço FTP:

```
systemctl restart vsftpd
```

Etapa 4: Configurar grupos de segurança

Depois de configurar o serviço FTP, configure inbound rules (regras de entrada) para o CVM Linux com base no modo FTP, de fato, utilizado. Para obter detalhes, consulte Adicionar regras de grupo de segurança.
A maioria dos clientes converte endereços IP em LANs. Se você estiver usando o modo FTP ativo, certifique-se de que o cliente obteve o endereço IP real. Caso contrário, o cliente pode falhar ao efetuar login no servidor FTP.

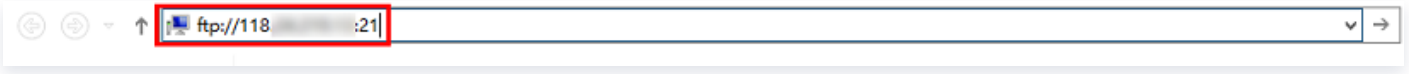
- Para o modo ativo: abra a porta 21.
- Para o modo passivo: abra a porta 21 e todas as portas que variam de `pasv_min_port` a `pasv_max_port` definidas no arquivo de configuração, como as portas 40000 a 45000 neste documento.

Etapa 5: Verifique o serviço FTP

Você pode verificar o servidor FTP usando ferramentas como um cliente FTP, um navegador ou através do Windows Explorer. Neste caso, o Windows Explorer é usado como exemplo.

1. Abra o Internet Explorer no cliente, escolha Tools (Ferramentas) > Internet Options (Opções da Internet) e clique na guia Advanced (Avançado). Faça as seguintes modificações com base no modo FTP selecionado.
   - Para o modo ativo: desmarque Passive FTP (FTP passivo).
   - Para o modo passivo: selecione Passive FTP (FTP passivo).
2. Abra o Windows Explorer no cliente, digite o seguinte endereço na caixa de endereço e pressione Enter, conforme mostrado na figura a seguir.

```
ftp://<CVM public IP address:21>
```



3. Na página de login que aparece, digite o nome de usuário e senha definidos em Configuração vsftpd. Neste caso, o nome de usuário é `ftpuser` e a senha é `tf7295TFY`.
4. Após o login bem-sucedido, você pode fazer upload e download de arquivos.

Apêndice

Configuração do modo FTP ativo

Para usar o modo ativo, modifique os seguintes parâmetros de configuração e deixe outros como padrões:

```
anonymous_enable=NO       # Proibir que usuários anônimos façam login
local_enable=YES          # Permitir que usuários locais façam login
chroot_local_user=YES     # Restringir o acesso de todos os usuários
apenas ao diretório raiz
chroot_list_enable=YES # Habilitar a lista de usuários excepcionais
chroot_list_file=/etc/vsftpd/chroot_list  # Especificar a lista de
usuários, na qual os usuários listados não estão restritos a acessar
apenas o diretório raiz
listen=YES                # Ativar a escuta em soquetes IPv4
# Adicionar o sinal de cerquilha (#) no início da linha seguinte para
comentar o seguinte parâmetro.
#listen_ipv6=YES          # Desativar escuta em soquetes IPv6
# Adicionar os seguintes parâmetros
allow_writeable_chroot=YES
local_root=/var/ftp/test # Definir o diretório onde os usuários locais
residem após o login
```

Pressione Esc e digite :wq. Em seguida, salve as alterações e feche o arquivo. Depois disso, vá para a Etapa 8 para configurar o vsftpd.

Falha ao fazer upload de arquivos de um cliente FTP

Descrição do Problema

No ambiente Linux, os usuários encontram a seguinte mensagem de erro ao enviar arquivos com vsftpd.

```
553 Não foi possível criar o arquivo
```

Solução

1. Execute o seguinte comando para verificar a utilização do espaço em disco do servidor:

   ```
   df -h
   ```

   - Se o espaço em disco for insuficiente, você não pode fazer upload de arquivos. Nesse caso, recomendamos que você exclua alguns arquivos grandes e desnecessários do disco.
   - Se o espaço em disco for suficiente, vá para a próxima etapa.
2. Execute o seguinte comando para verificar se você tem permissão de gravação no diretório FTP:

   ```
   ls -l /home/test
   # Neste caso, /home/test indica o diretório FTP. Substitua-o pelo seu
   diretório FTP real.
   ```

   - Se `w` não for retornado no resultado, você não tem permissão de gravação para o diretório. Nesse caso, vá para a próxima etapa.
   - Se `w` for retornado no resultado, envie um tíquete para solução de problemas adicionais.
3. Execute o seguinte comando para conceder permissão de gravação ao diretório FTP:

   ```
   chmod +w /home/test
   # Neste caso, /home/test indica o diretório FTP. Substitua-o pelo seu
   diretório FTP real.
   ```
4. Execute o seguinte comando para verificar se a permissão de gravação foi concedida com sucesso:

   ```
   ls -l /home/test
   # Neste caso, /home/test indica o diretório FTP. Substitua-o pelo seu
   diretório FTP real.
   ```

Configurar o serviço FTP na instância Windows

Last updated：2025-09-05 17:12:52

Introdução

Descrição sobre como usar o IIS para construir um site FTP em uma instância do Tencent Cloud Virtual Machine (CVM) que executa o Windows.

Requisitos de software

Os seguintes softwares são necessários para construir o serviço FTP:

- OS: Windows Server 2012
- Servidor da web: IIS 8.5

Instruções

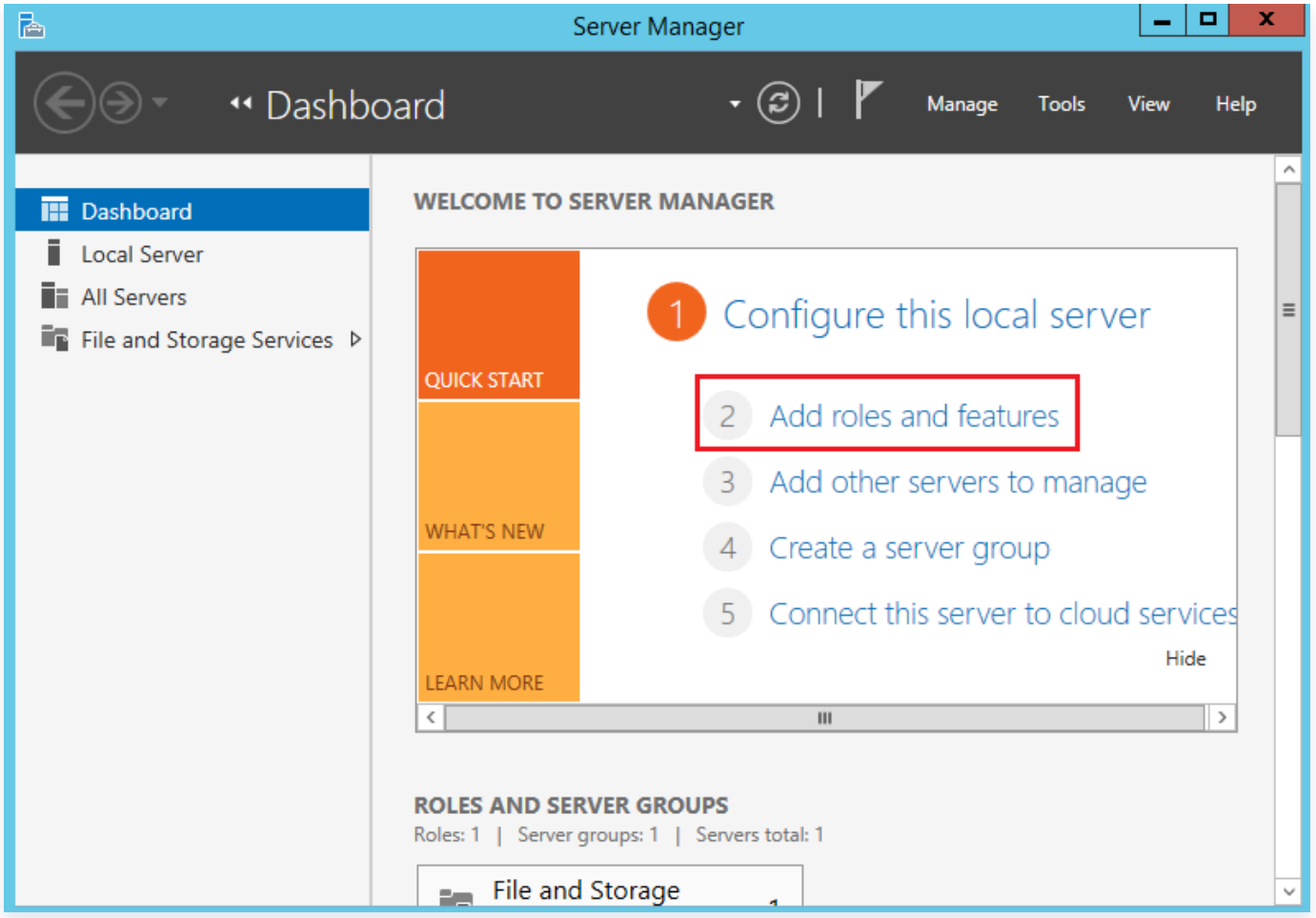
Etapa 1: fazer login no CVM

- Faça login em um CVM Windows usando um arquivo RDP (recomendado).
- Faça login em um CVM Windows usando uma área de trabalho remota.

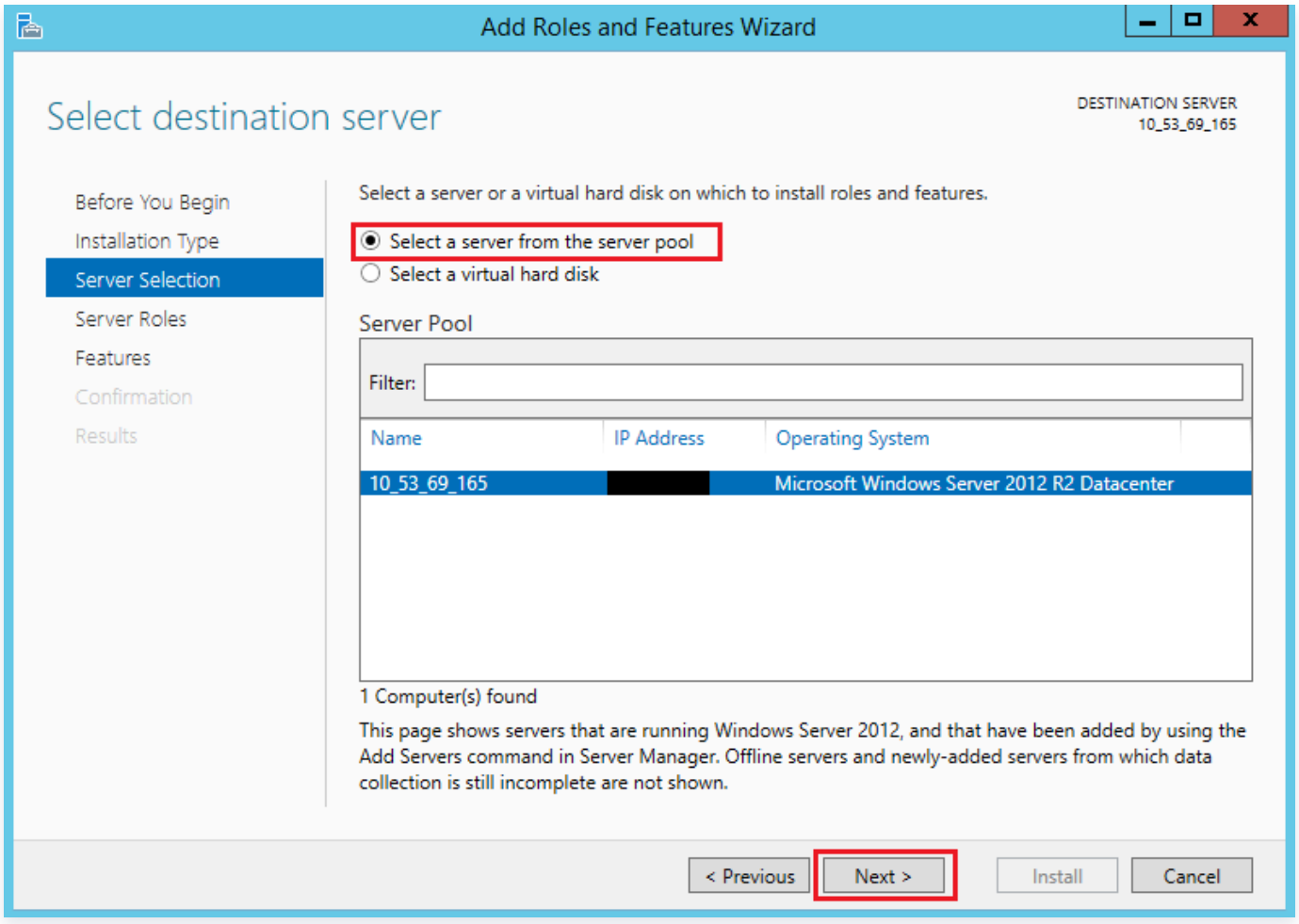
Etapa 2: instalar o serviço FTP no IIS

1. Clique em  para abrir o gerenciador do servidor. A janela Server Manager (Gerenciador do servidor) é exibida.
2. Clique em Add Roles and Features (Adicionar funções e recursos), conforme mostrado na figura abaixo. A janela Guide to Adding Roles and Features (Guia para adicionar funções e recursos) é

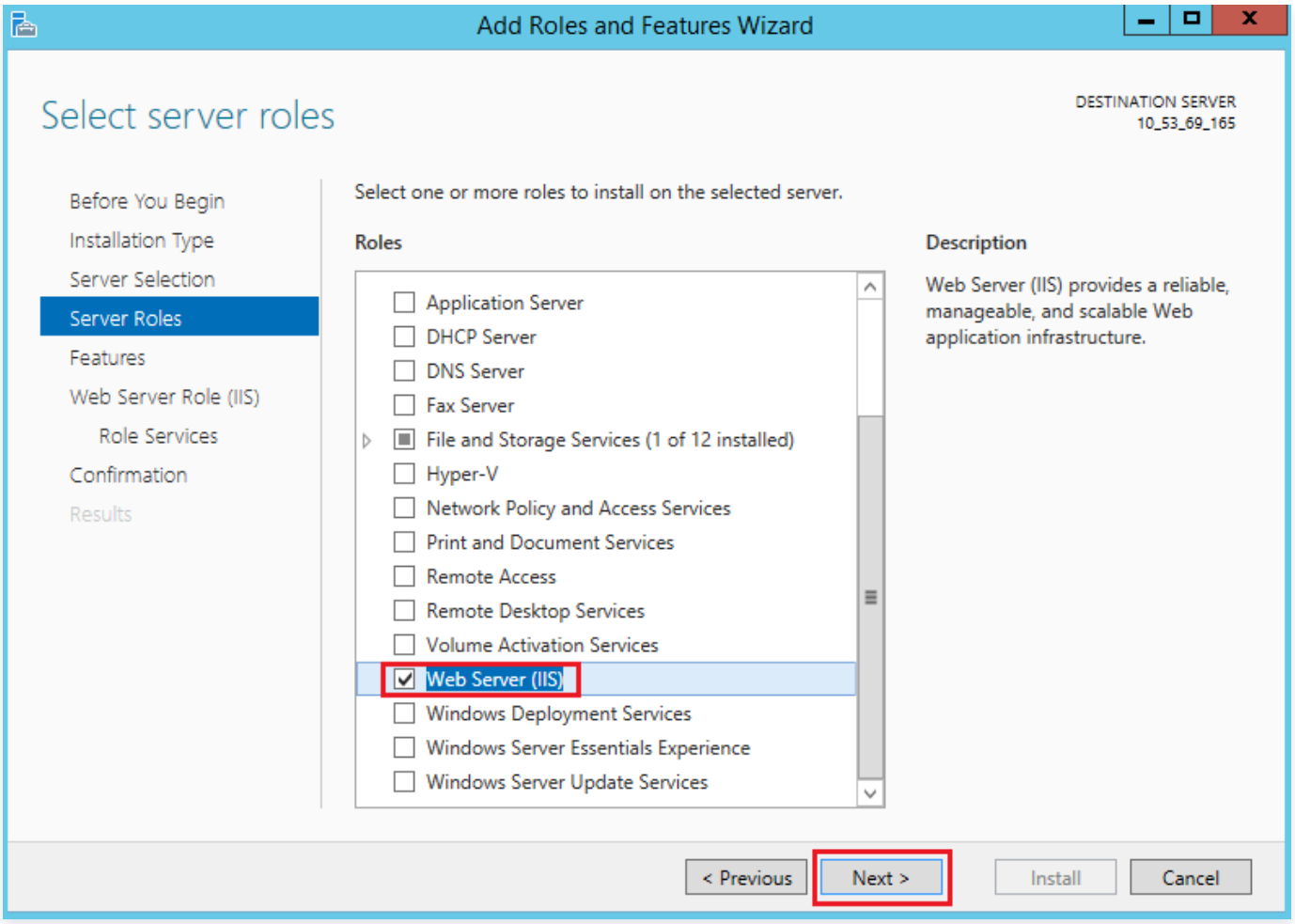
exibida.



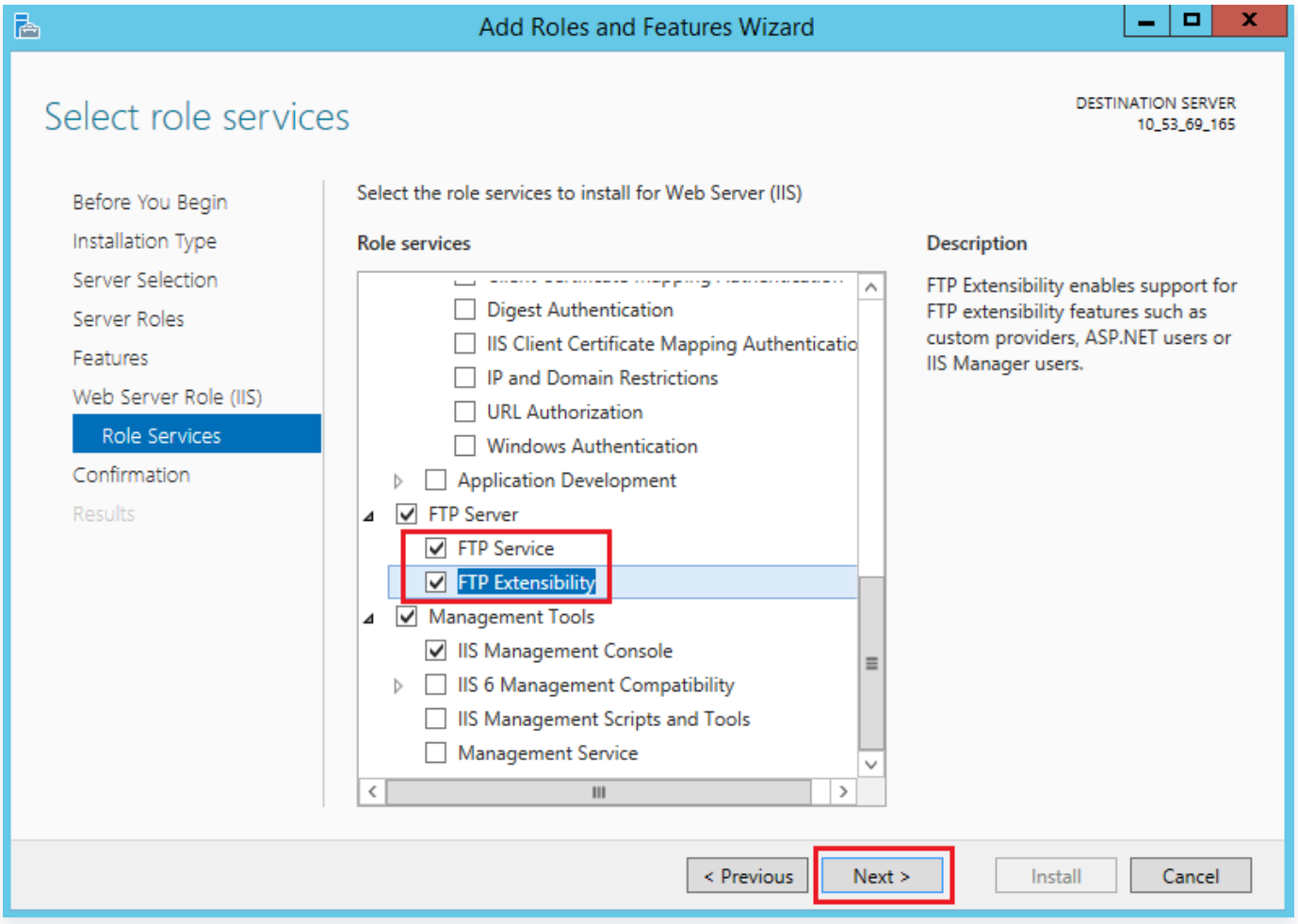
3. Clique em Next (Avançar). A página Choose Installation Type (Selecionar tipo de instalação) é exibida.
4. Selecione Role-based or Feature-based Installation (Instalação baseada em funções ou recursos) e clique em Next (Avançar). A página Choose Target Server (Selecionar servidor de destino) é exibida.
5. Mantenha as configurações padrão e clique em Next (Avançar), conforme mostrado na figura abaixo. A página Choose Server Role (Selecionar função do servidor) é exibida.



6. Selecione Web Server (IIS) (Servidor web (IIS)) e clique em Add Feature (Adicionar recurso) na janela exibida, conforme mostrado na figura abaixo:



7. Clique em Next (Avançar) três vezes. A página Choose Role Service (Selecionar serviço de função) é exibida.
8. Selecione FTP Service (Serviço FTP) e FTP Extension (Extensão FTP) e clique em Next (Avançar), conforme mostrado na figura abaixo:

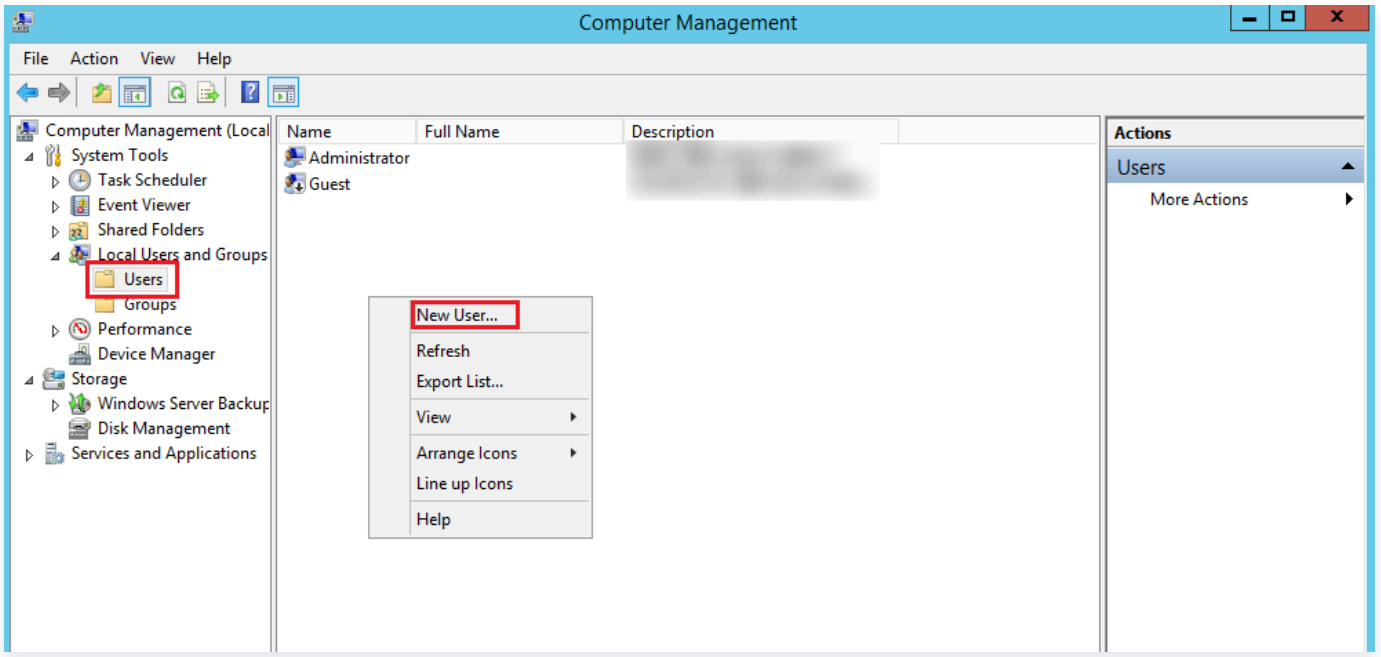


9. Clique em Install (Instalar) para iniciar a instalação do serviço FTP.
10. Após a conclusão da instalação, clique em Close (Fechar).

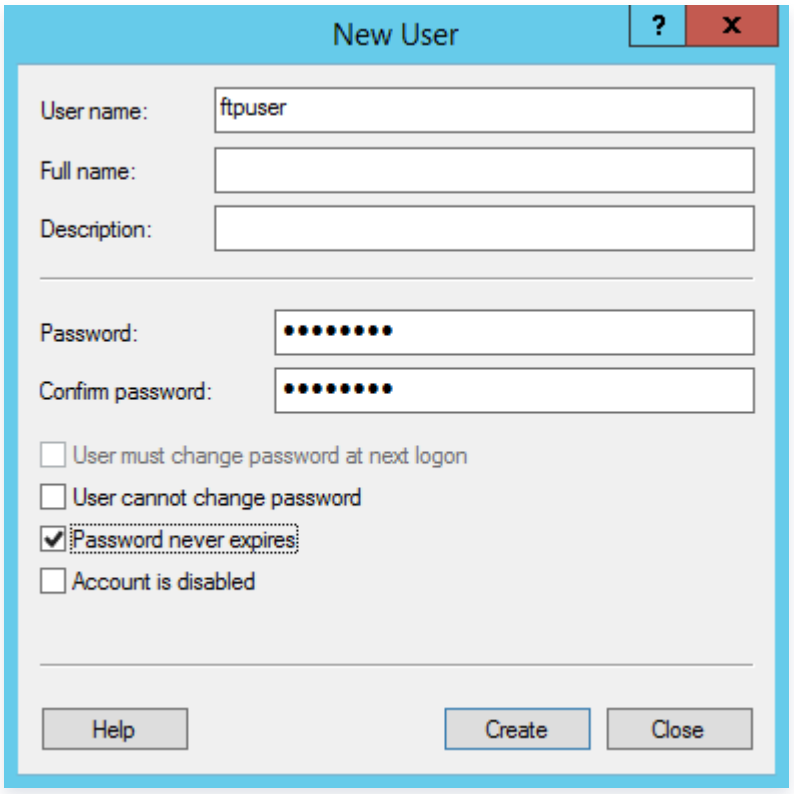
Etapa 3: criar um nome de usuário e senha de FTP

> Nota:
> As etapas a seguir criam uma conta FTP com autenticação de senha. Se você planeja usar apenas acesso anônimo, pule esta seção.

1. Na janela "Server Manager (Gerenciador do servidor)", selecione Tools (Ferramentas) –> My Computer (Meu computador) na barra de navegação no canto superior direito. A janela My Computer (Meu computador) é exibida.
2. Selecione System Tools (Ferramentas do sistema) –> Local Users and Groups (Usuários e grupos locais) –> Users (Usuários) na barra lateral à esquerda.
3. No lado direito da interface de Users (Usuários), clique com o botão direito do mouse em um local vazio e selecione New User (Novo usuário), conforme mostrado na figura abaixo:



4. Na interface "New User (Novo usuário)", defina o nome de usuário e a senha de acordo com as instruções a seguir. Clique em Create (Criar), conforme mostrado na figura abaixo:



Os principais parâmetros são os seguintes:

- User name (Nome do usuário): nome do usuário. Neste caso, `ftpuser`.
- Password and Confirm password (Senha e confirmar senha): a senha deve conter letras maiúsculas, minúsculas e números. Neste caso, `tf7295TFY`.

- Desmarque User must change password in next login (O usuário deve alterar a senha no próximo login) e selecione Password never expires (A senha nunca expira).
  Selecione as opções conforme achar adequado. Para este artigo, selecionamos Password never expires (A senha nunca expira).

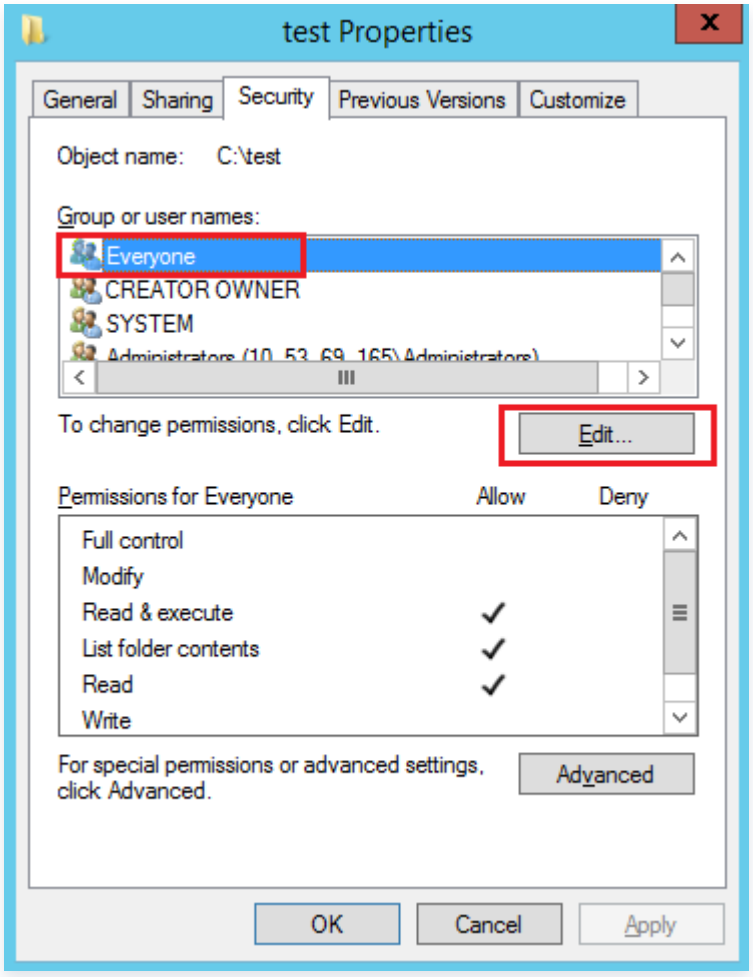
5. Clique em Close (Fechar) para fechar a janela "New User (Novo usuário)". É possível ver o usuário recém-criado `ftpuser` na lista.

Etapa 4: definir permissões de pasta compartilhada

> Nota:
> Neste artigo, usamos `C:\test` como a pasta compartilhada. Ele contém um arquivo chamado `test.txt`. Crie uma pasta chamada `test` em `C:\` e um arquivo chamado `test.txt` em `C:\test`. Você também pode usar qualquer outra pasta e arquivo.

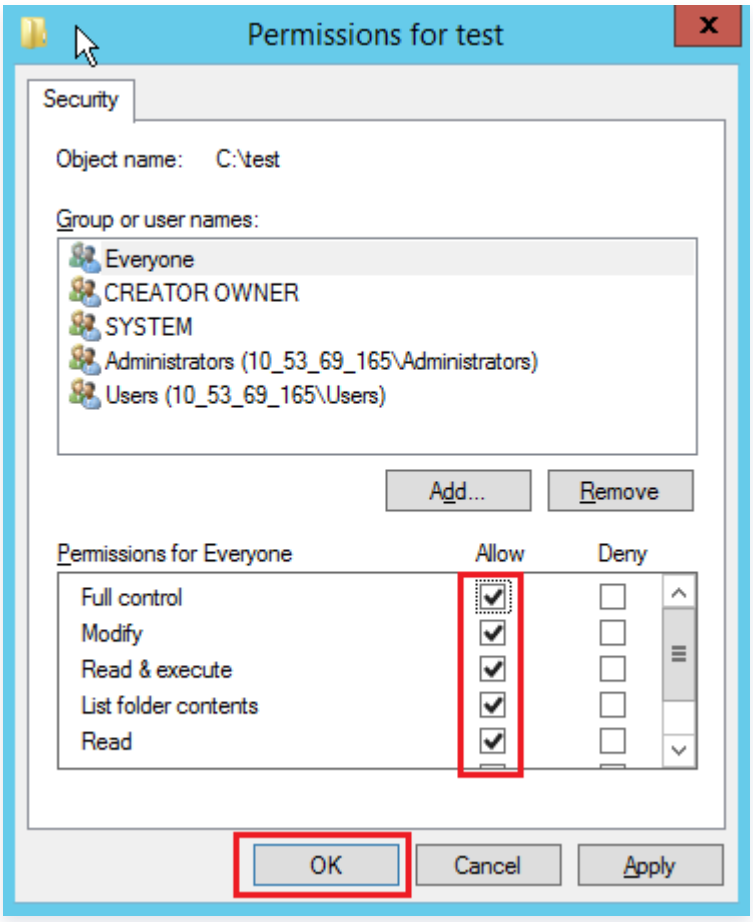
1. Clique em  para abrir This Computer (Este computador).
2. Expanda os diretórios na unidade C. Selecione e clique com o botão direito do mouse em `test`. Selecione Properties (Propriedades).
3. Na janela Properties (Propriedades), selecione a guia Security (Segurança).
4. Selecione `Everyone` (Todos) e clique em Edit (Editar), conforme mostrado na figura abaixo:
   Se "Group or User Name (Nome do grupo ou do usuário)" não contiver `Everyone` (Todos),

consulte Adicionar todos para adicionar o usuário.



5. Na interface Permissions (Permissões), defina as permissões para `Everyone` (Todos) e clique em OK, conforme mostrado na figura abaixo:

Neste artigo, concedemos a `Everyone` (Todos) todas as permissões.

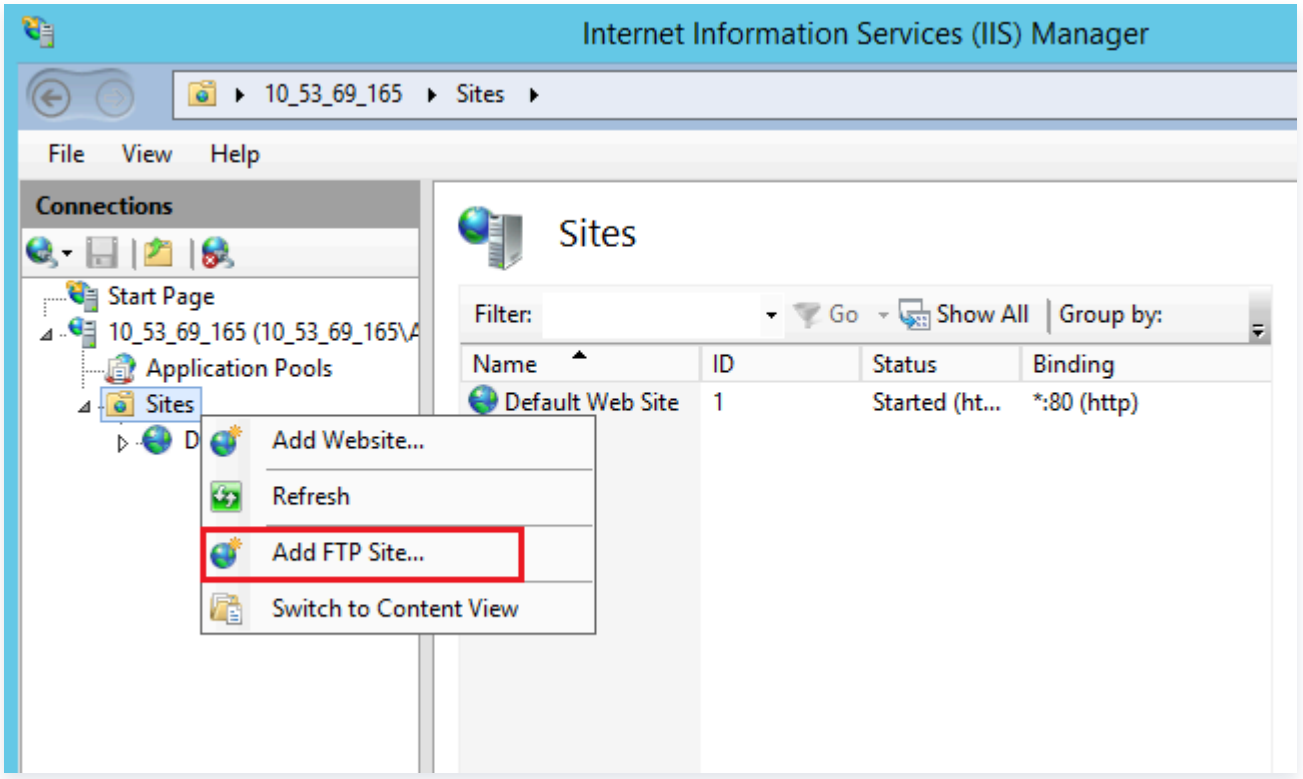


6. Na janela Properties (Propriedades), clique em OK para concluir as configurações.

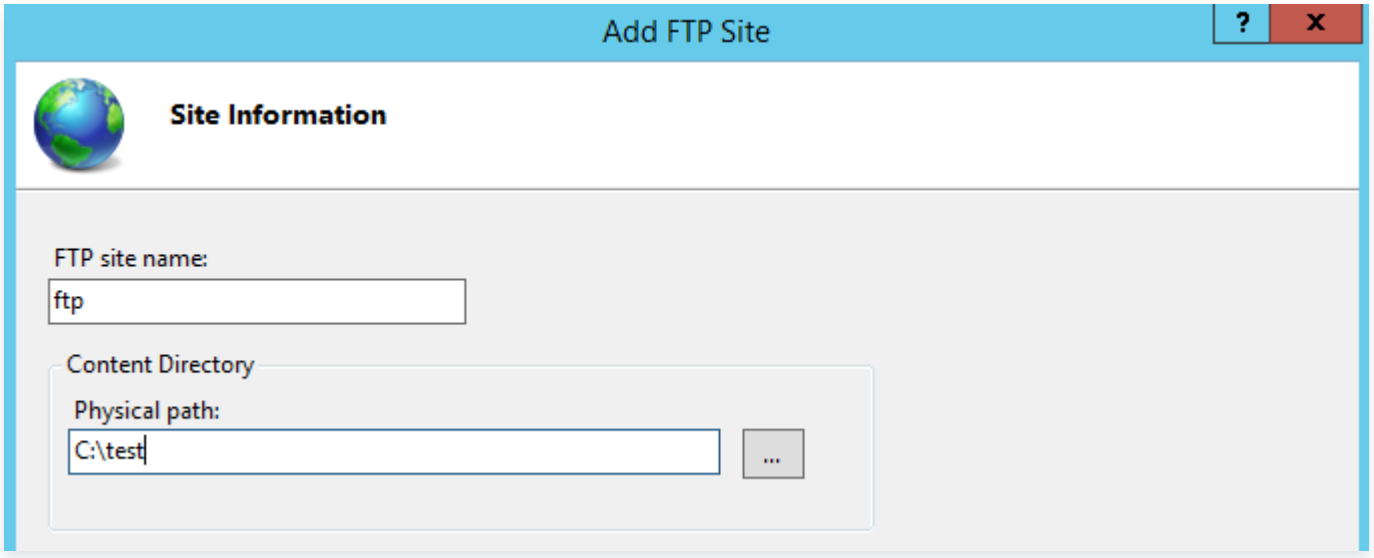
Etapa 5: adicionar um site FTP

1. Na janela "Server Manager (Gerenciador do servidor)", selecione Tools (Ferramentas) –> Internet Information Services (IIS) Manager (Gerenciador de Serviços de Informações da Internet (IIS)) na barra de navegação no canto superior direito.
2. Na janela Internet Information Services (IIS) Manager (Gerenciador de Serviços de Informações da Internet (IIS)), expanda seu servidor na barra lateral esquerda, clique com o botão direito do mouse

em Website e selecione Add FTP Site (Adicionar site FTP), conforme mostrado na figura abaixo:

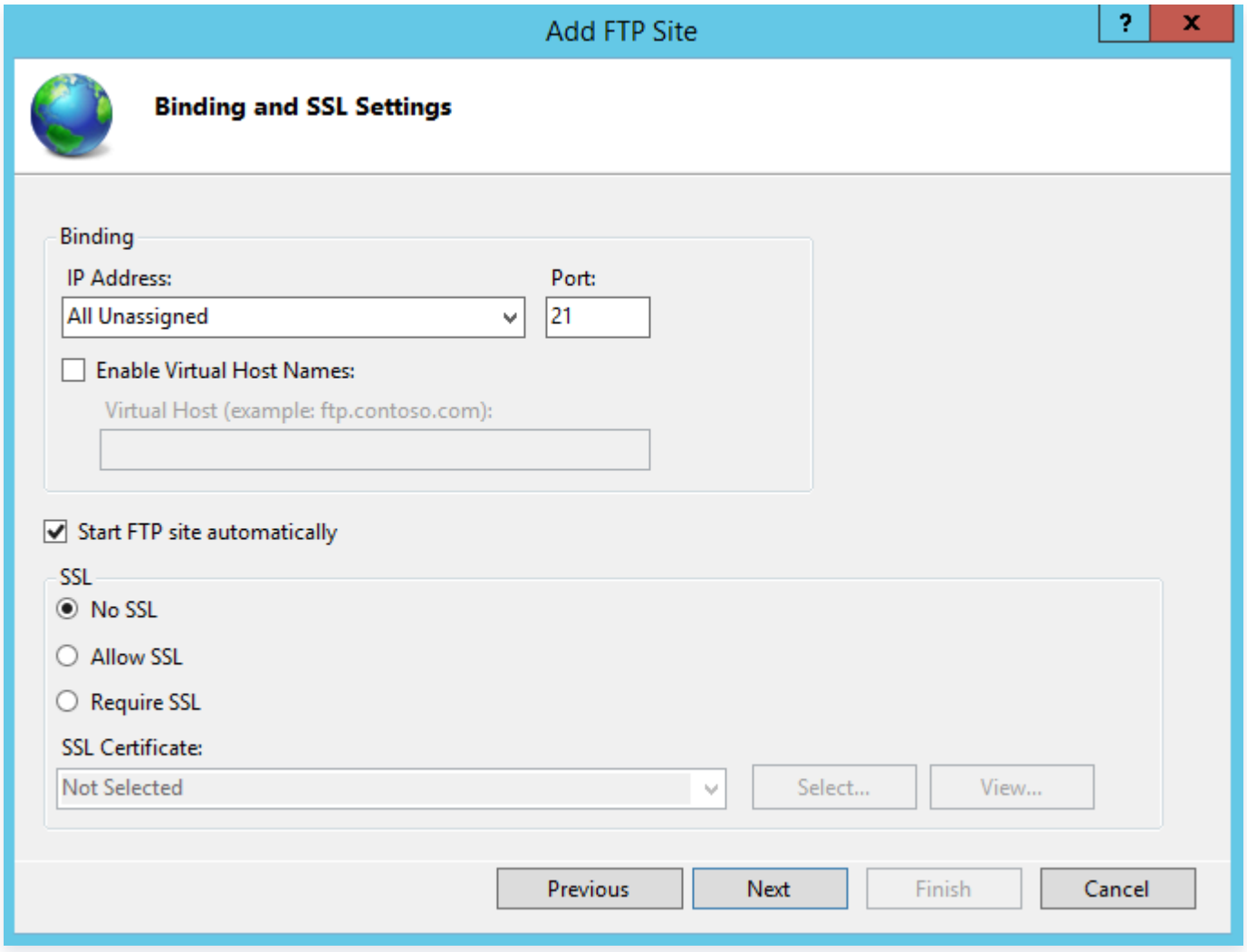


3. Na interface "Site Information (Informações do site)", insira as seguintes informações. Clique em Next (Avançar), conforme mostrado na figura abaixo:



   - FTP site name (Nome do site FTP): nome do seu site FTP. Neste artigo, é usado `ftp`.
   - Physical path (Caminho físico): caminho da pasta compartilhada. Certifique-se de definir as permissões apropriadas. Neste artigo, é usado `C:\test`.

4. Na interface Binding and SSL Settings (Configurações de vinculação e SSL), insira as seguintes informações. Clique em Next (Avançar), conforme mostrado na figura abaixo:



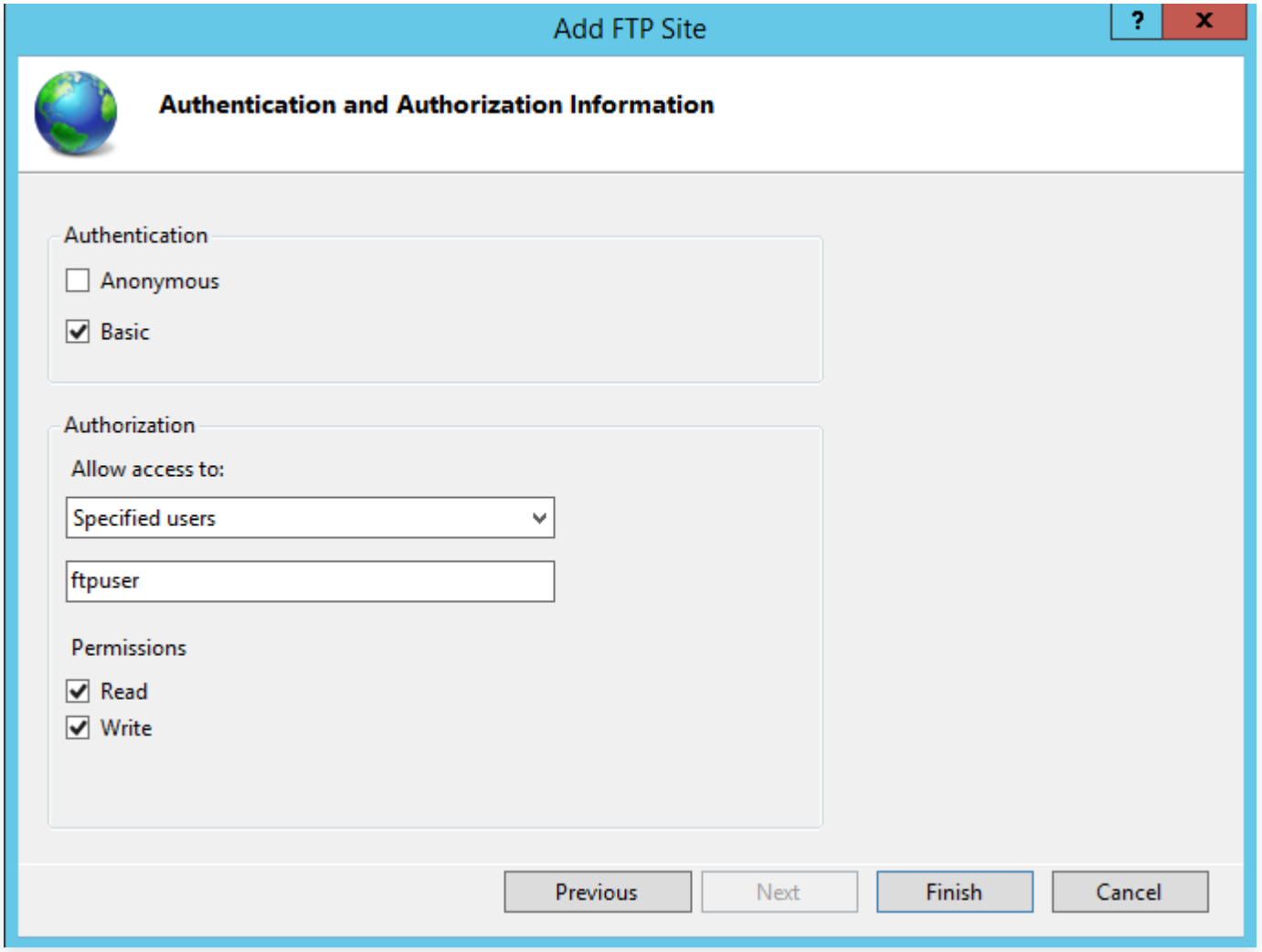
A seguir está uma lista de parâmetros:

- Binding (Vinculação): a opção padrão para endereços IP é None assigned (Nenhum atribuído); e a porta padrão é a porta 21, o número da porta FTP padrão. É possível escolher seu próprio número de porta.
- SSL: selecione uma opção. Neste artigo, No SSL (Nenhum SSL) é selecionado.
  - No SSL (Nenhum SSL): não oferece suporte a conexões SSL.
  - Allow SSL (Permitir SSL): permite que o servidor FTP se conecte a clientes com ou sem SSL.
- Require SSL (Requer SSL): A criptografia SSL é necessária para a comunicação entre o servidor FTP e os clientes.

  Se você escolher Allow SSL (Permitir SSL) ou Require SSL (Requer SSL), pode selecionar um certificado SSL existente em "SSL Certificates (Certificados SSL)" ou consultar criar um certificado de servidor para criar um certificado SSL.

5. Na interface "Identity Authentication and Authorization Information (Autenticação de identidade e informações de autorização)", insira as seguintes informações. Clique em Next (Avançar), conforme

mostrado na figura abaixo:



- Identity authentication (Autenticação de identidade): selecione um método de autenticação de identidade. Neste artigo, é usado Basic (Básico).
  - Anonymous (Anônimo): permite que os usuários acessem o conteúdo sem autenticação.
  - Basic (Básico): exige que os usuários forneçam nomes de usuário e senhas válidos antes de permitir o acesso ao conteúdo. Nesse modo, as senhas são transferidas sem criptografia. Portanto, selecione este modo de autenticação apenas quando souber que a conexão entre os clientes e o servidor FTP é segura (por exemplo, usando SSL).
- Authorize (Autorizar): escolha uma opção na lista suspensa de permissões de acesso. Neste artigo, é usada `ftpuser`.
  - All users (Todos os usuários): todos os usuários, anônimos ou identificados, podem acessar o conteúdo.
  - Anonymous users (Usuários anônimos): usuários anônimos podem acessar o conteúdo.
  - Specified role or user group (Função ou grupo de usuários especificado): apenas as funções ou membros especificados dos grupos especificados podem acessar o conteúdo. Se você escolher esta opção, precisará especificar as funções ou grupos de usuários.

- Specified user (Usuário especificado): apenas o usuário especificado pode acessar o conteúdo. Se você escolher esta opção, precisará especificar o nome de usuário.
- Permissions (Permissões): permissões para o conteúdo compartilhado. Neste artigo, Read (Ler) e Write (Gravar) são selecionados.
  - Read (Ler): permite que usuários autorizados leiam o conteúdo compartilhado.
  - Write (Gravar): permite que usuários autorizados gravem no diretório.

6. Clique em Complete (Concluir).

Etapa 6: configurar grupo de segurança e firewall

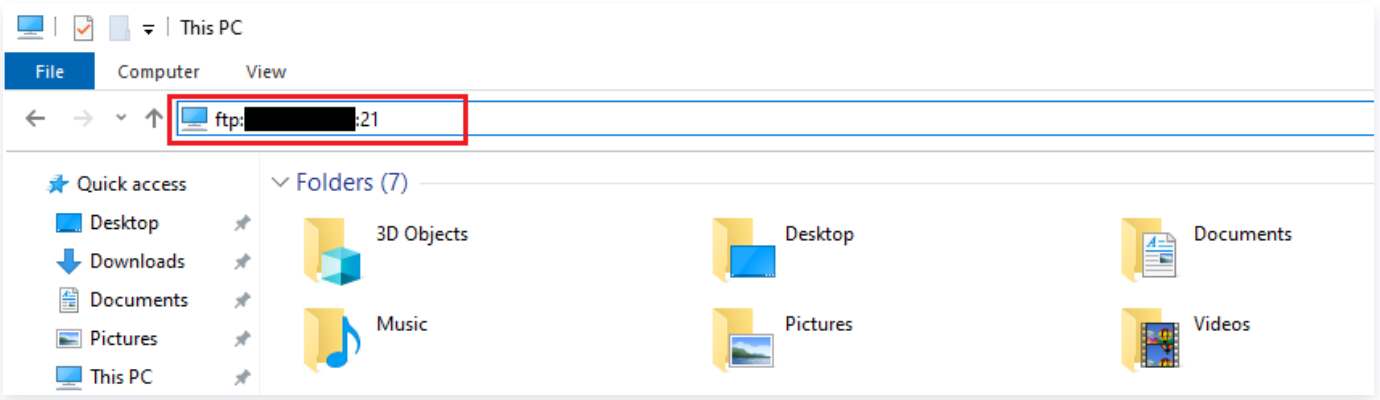
1. Depois que o site FTP for criado, adicione uma regra de entrada que permita o tráfego para a porta FTP, que é a 21 para os fins deste artigo. Para obter mais informações, consulte Adicionar regras de grupo de segurança.
   Se você selecionou outras portas, também precisa adicionar uma regra de entrada para cada porta selecionada.
2. (Opcional) Consulte a documentação oficial da Microsoft sobre como configurar o firewall para que o servidor FTP seja capaz de aceitar conexões passivas do firewall.

Etapa 7: testar o site FTP

É possível usar um cliente FTP, navegador ou gerenciador de arquivos para se conectar ao servidor FTP. Para os fins deste artigo, é utilizado o gerenciador de arquivos.

1. Configure o Internet Explorer
   - Se você adicionou as regras de firewall apropriadas, abra uma janela do Internet Explorer e selecione Tools (Ferramentas) –> Internet Options (Opções da Internet) –> Advanced (Avançado). Desmarque Use Passive FTP (used for compatibility between the firewall and DSL modem) (Usar FTP passivo (usado para compatibilidade entre o firewall e o modem DSL)) e clique em OK.
   - Se você não adicionou as regras de firewall adequadas:
     1.1.1 Abra uma janela do Internet Explorer no the FTP server (servidor FTP) e selecione Tools (Ferramentas) –> Internet Options (Opções da Internet) –> Advanced (Avançado). Desmarque Use Passive FTP (used for compatibility between the firewall and DSL modem) (Usar FTP passivo (usado para compatibilidade entre o firewall e o modem DSL)) e clique em OK.
     1.1.2 Abra uma janela do Internet Explorer no client (cliente) e selecione Tools (Ferramentas) –> Internet Options (Opções da Internet) –> Advanced (Avançado). Desmarque Use Passive FTP (used for compatibility between the firewall and DSL modem) (Usar FTP passivo (usado para compatibilidade entre o firewall e o modem DSL)) e clique em OK.
2. Abra o gerenciador de arquivos em seu PC, digite o seguinte endereço na caixa de endereço do navegador e pressione Enter, conforme mostrado na figura a seguir.

```
ftp://CVM_public_IP_address:21
```

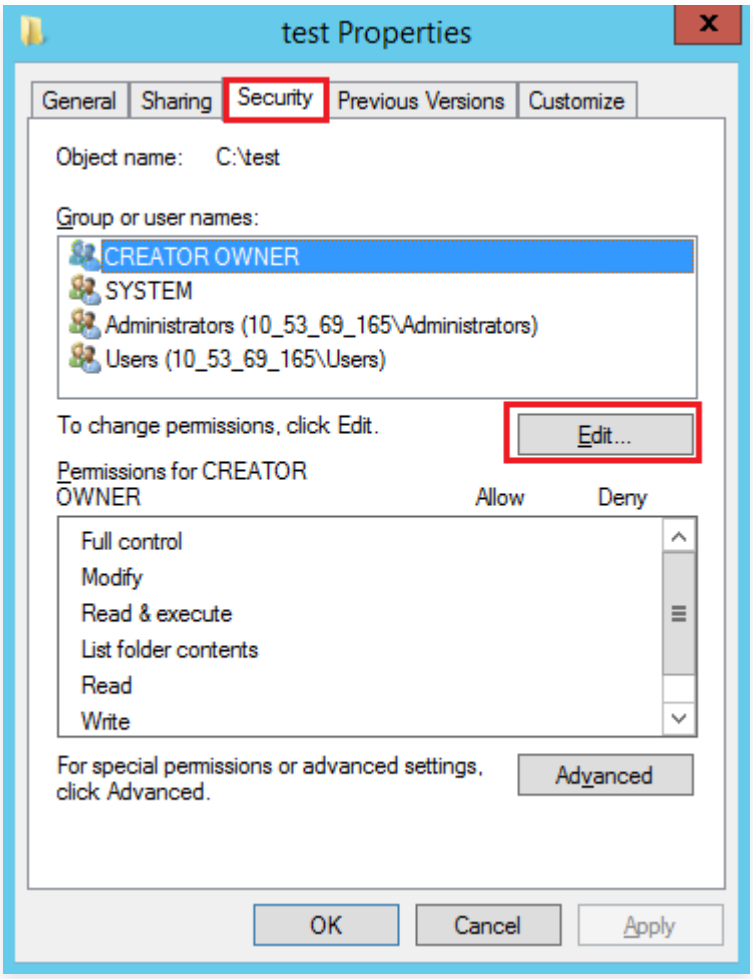


3. A caixa de diálogo Login Identity (Identidade de login) é exibida. Digite o nome de usuário e a senha configurados em Criação do nome de usuário e senha de FTP.
   Neste artigo, o nome de usuário é `ftpuser` e a senha é `tf7295TFY`.
4. Faça upload e download de arquivos após o login.

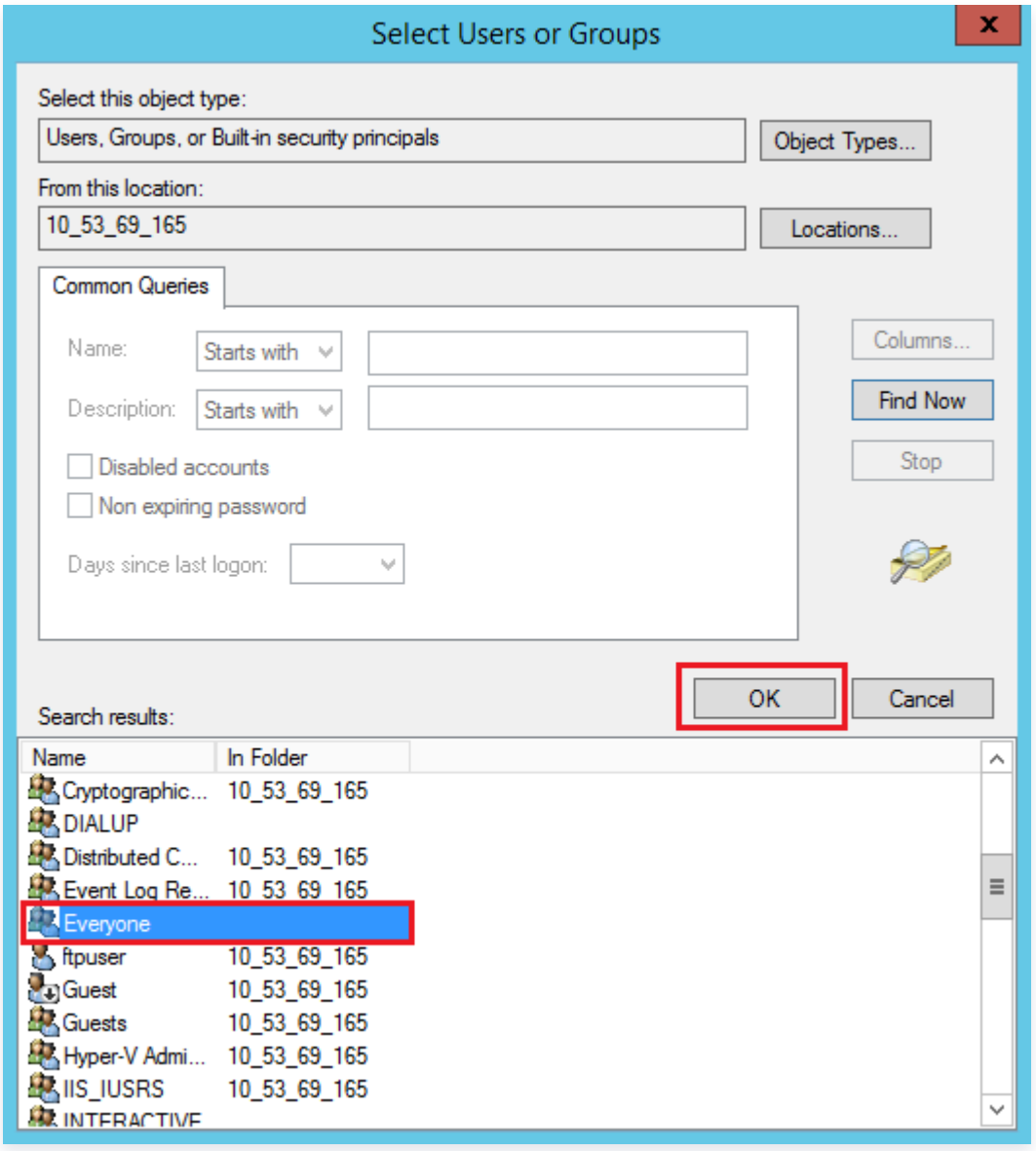
Apêndice

Adicionar todos

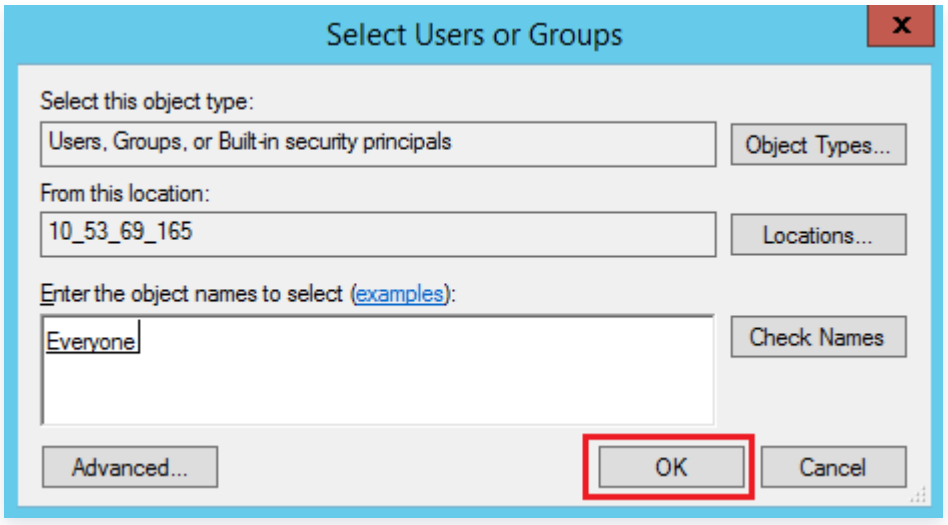
1. Na janela Properties (Propriedades), selecione a guia Security (Segurança). Clique em Edit (Editar), conforme mostrado na figura abaixo:



2. Na caixa de diálogo Properties (Propriedades), clique em Add (Adicionar).
3. Na caixa de diálogo "Choose User or Group (Selecionar usuário ou grupo)", clique em Advanced (Avançado).
4. Na caixa de diálogo "Choose User or Group (Escolher usuário ou grupo)" exibida, clique em Search Now (Pesquisar agora).
5. No resultado da pesquisa, selecione `Everyone` (Todos) e clique em OK, conforme mostrado na figura abaixo:



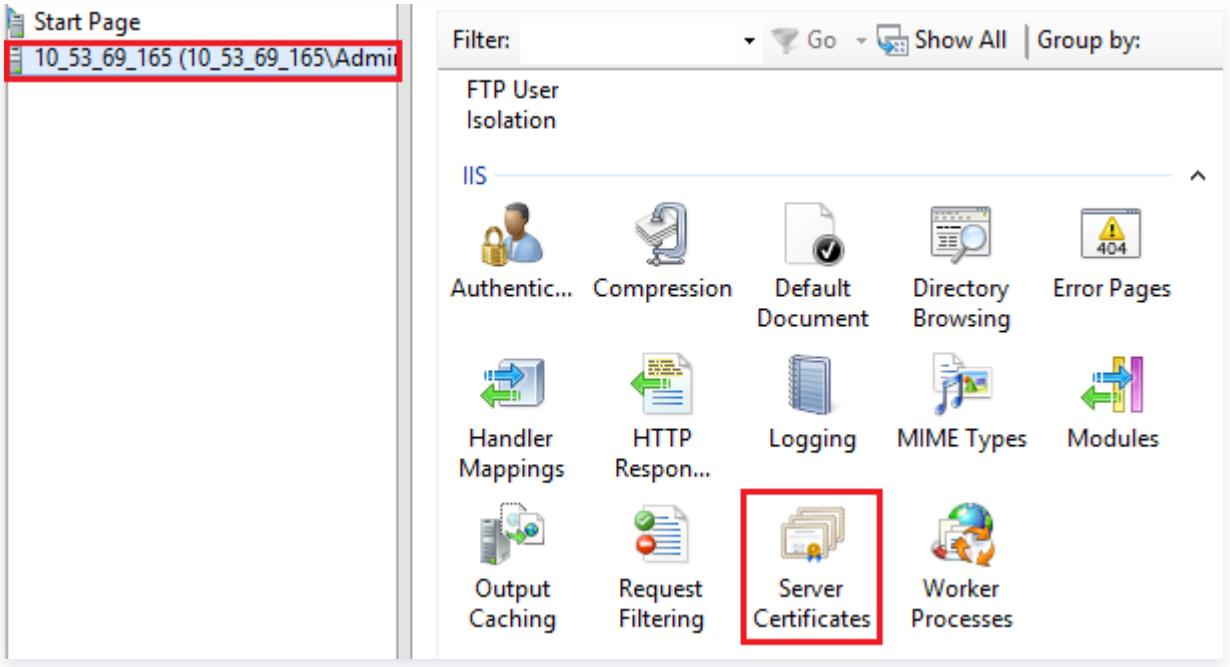
6. Na caixa de diálogo "Choose User or Group (Escolher usuário ou grupo)", clique em OK, conforme mostrado na figura abaixo:



Vá para a Etapa 5 para definir as permissões do usuário `Everyone` (Todos).

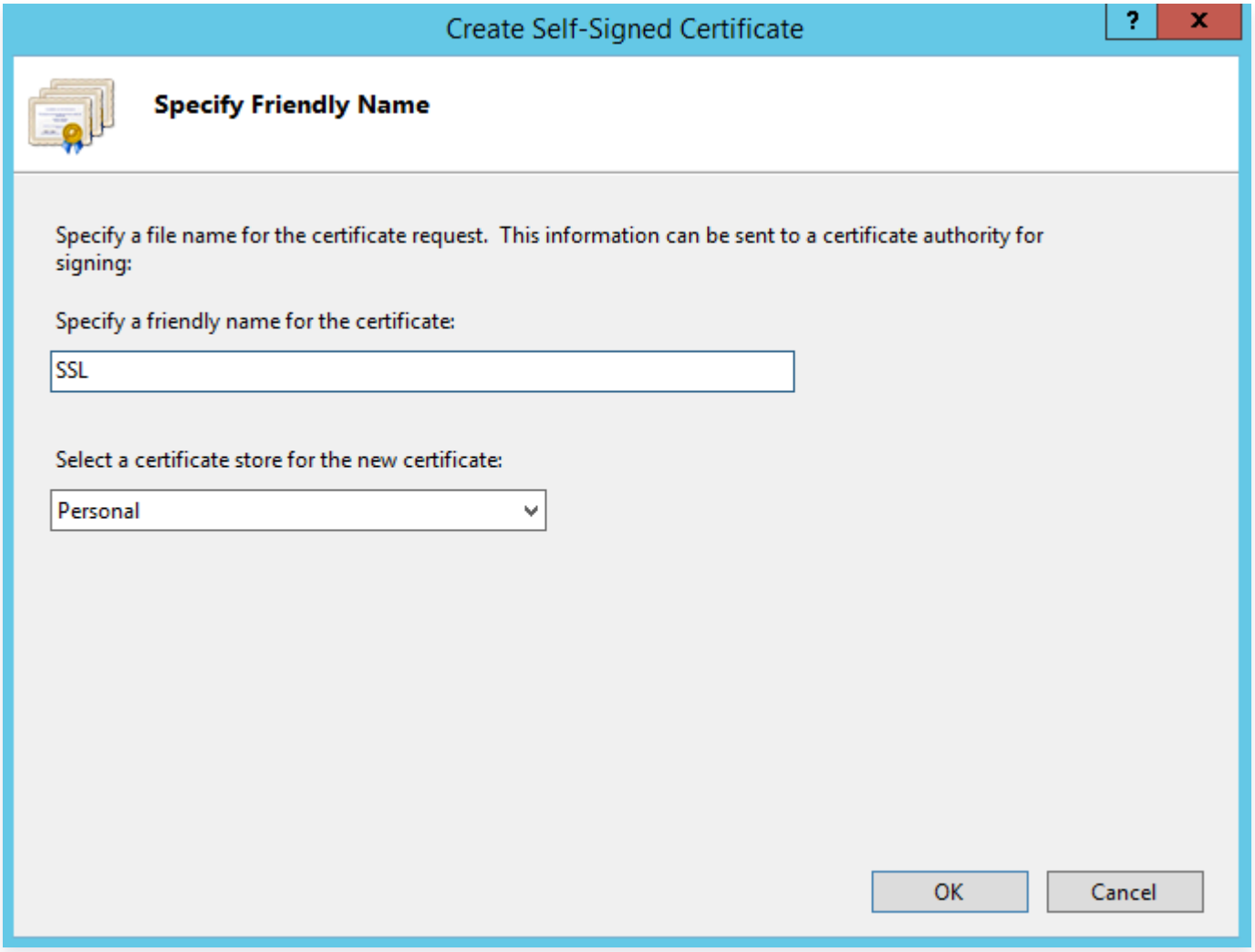
Criação de um certificado de servidor

1. Abra "Server Manager (Gerenciador do servidor)" e selecione Tools (Ferramentas) –> Internet Information Services (IIS) Manager (Gerenciador dos Serviços de Informações da Internet (IIS)) na barra de navegação no canto superior direito.
2. A janela Internet Information Services (IIS) Manager (Gerenciador dos Serviços de Informações da Internet (IIS)) é exibida. Selecione o servidor na barra lateral esquerda e clique duas vezes em Server Certificates (Certificados do servidor) na interface à direita, conforme mostrado na figura abaixo:



3. Selecione Create Self-Signature Certificate (Criar certificado de auto-assinatura) na coluna de operação correta.
4. A janela Create Self-Signature Certificate (Criar certificado de auto-assinatura) é exibida, insira um nome de certificado e a classe de armazenamento, conforme mostrado na figura abaixo:

Neste documento, um certificado SSL para armazenamento pessoal é criado.



5. Clique em OK.

Serviço NTP

Visão geral do serviço NTP

Last updated：2024-01-23 17:52:21

O Network Time Protocol (NTP) é um protocolo de rede para sincronização de relógio entre sistemas de computador em uma rede. Os servidores NTP geralmente usam o Tempo Universal Coordenado (UTC).
O Tencent Cloud fornece um servidor NTP privado para os próprios recursos. Para outros dispositivos, é possível usar os servidores NTP públicos fornecidos pelo Tencent Cloud.

Servidor NTP privado

```
ntpupdate.tencentyun.com
```

Servidores NTP públicos

```
time1.cloud.tencent.com
time2.cloud.tencent.com
time3.cloud.tencent.com
time4.cloud.tencent.com
time5.cloud.tencent.com
```

Para obter mais informações sobre como sincronizar seu relógio por meio de NTP no Linux, consulte Configuração do serviço NTP para instâncias do Linux.
Para obter mais informações sobre como sincronizar o relógio por meio de NTP no Windows, consulte Configuração do serviço NTP para instâncias do Windows.

Configurar o serviço NTP para instância Linux

Last updated：2024-01-23 17:52:21

Visão geral

O daemon do Network Time Protocol (ntpd) é um daemon do sistema operacional Linux. É uma implementação completa do NTP e é usado para corrigir a diferença de horário entre o sistema local e o servidor de origem do relógio. Ao contrário do ntpdate, que atualiza o tempo periodicamente, o ntpd corrige o tempo continuamente, sem intervalos de tempo. Este documento usa o CentOS 7.5 como exemplo para descrever como instalar e configurar o ntpd.

Observações

- Alguns sistemas operacionais usam o chrony como o serviço NTP padrão. Certifique-se de que o ntpd esteja em execução e configurado para ativar automaticamente na inicialização.
- Execute o comando `systemctl is-active ntpd.service` para conferir se o ntpd está em execução.
- Execute o comando `systemctl is-enabled ntpd.service` para conferir se o ntpd está configurado para ativar automaticamente na inicialização.
- A porta de comunicação do serviço NTP é UDP 123. Certifique-se de ter aberto a porta para a Internet antes de configurar o serviço NTP.
  Se a porta não estiver aberta, consulte Adicionar regras de grupo de segurança para abri-la para a Internet.

Instruções

Instalação do ntpd

Execute o seguinte comando para verificar se o ntpd foi instalado.

```
rpm -qa | grep ntp
```

- Se o seguinte resultado for retornado, o ntpd foi instalado.

```
[root@VM_16_2_centos ~]# rpm -qa | grep ntp
ntpdate-4.2.6p5-28.el7.centos.x86_64
ntp-4.2.6p5-28.el7.centos.x86_64
fontpackages-filesystem-1.44-8.el7.noarch
```

- Se o ntpd não tiver sido instalado, execute o comando `yum install ntp` para instalá-lo.

```
yum -y install ntp
```

O ntpd usa o modo cliente por padrão.

Configuração do NTP

1. Execute o seguinte comando para abrir o arquivo de configuração do serviço NTP.

```
vi /etc/ntp.conf
```

2. Pressione i para alternar para o modo de edição e localizar as configurações do `server`. Altere o valor de `server` para o servidor de origem do relógio NTP que você deseja usar (como `time1.tencentyun.com`) e exclua os valores indesejados, conforme mostrado abaixo:

3. Pressione Esc e digite :wq para salvar e fechar o arquivo.

Ativação do ntpd

Execute o seguinte comando para reiniciar o serviço ntpd.

```
systemctl restart ntpd.service
```

Verificação de status do ntpd

Execute os comandos a seguir para verificar o status do ntpd conforme necessário.

- Execute o seguinte comando para verificar se o NTP está escutando normalmente na porta de serviço UDP 123.

```
netstat -nupl
```

Se o resultado a seguir for retornado, a escuta está normal.

```
[root@VM_0_136_centos ~]# netstat -nupl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 172.30.0.136:123        0.0.0.0:*                           999/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           999/ntpd
udp6       0      0 fe80::5054:ff:fec2::123 :::*                                999/ntpd
udp6       0      0 ::1:123                 :::*                                999/ntpd
[root@VM_0_136_centos ~]#
```

- Execute o seguinte comando para verificar se o status do ntpd está normal.

```
service ntpd status
```

Se o resultado a seguir for retornado, o status do ntpd está normal.

```
[root@VM_0_136_centos ~]# service ntpd status
Redirecting to /bin/systemctl status ntpd.service
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2019-08-07 15:23:25 CST; 5min ago
  Process: 997 ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 999 (ntpd)
    CGroup: /system.slice/ntpd.service
            └─999 /usr/sbin/ntpd -u ntp:ntp -g

Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c01d 0d kern kernel time sync enabled
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: ntp_io: estimated max descriptors: 1024, initia... 16
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 0 lo 127.0.0.1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 1 eth0 172.30.0.136 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 2 lo ::1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 3 eth0 fe80::5054:ff:fec2:11...123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listening on routing socket on fd #20 for inter...tes
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c016 06 restart
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c012 02 freq_set kernel 0.467 PPM
Aug 07 15:23:34 VM_0_136_centos ntpd[999]: 0.0.0.0 c615 05 clock_sync
Hint: Some lines were ellipsized, use -l to show in full.
[root@VM_0_136_centos ~]#
```

- Execute o seguinte comando para verificar se o NTP foi iniciado normalmente e se foi configurado para o servidor de origem do relógio NTP correto.

```
ntpstat
```

O endereço IP do servidor de origem do relógio NTP atual, que foi configurado anteriormente, deve ser retornado, conforme mostrado abaixo:

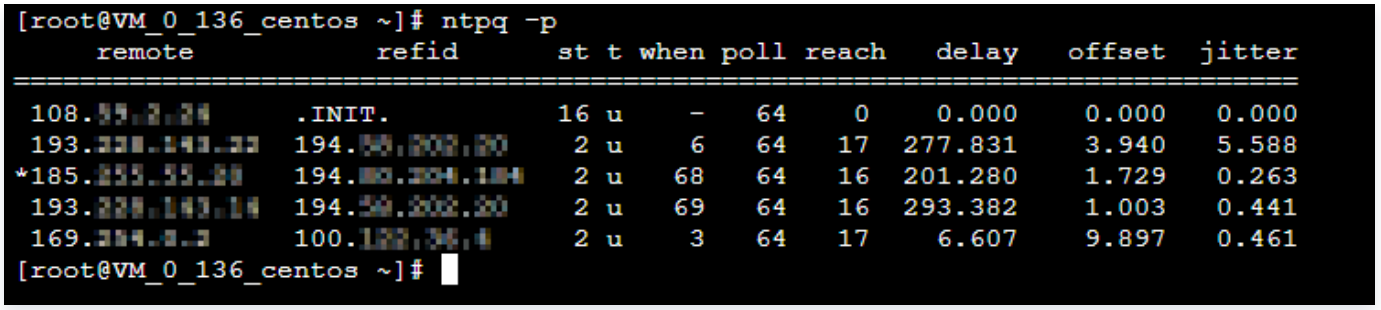
```
[root@VM_0_136_centos ~]# ntpstat
synchronised to NTP server (185.[illegible]) at stratum 3
   time correct to within 1060 ms
   polling server every 64 s
[root@VM_0_136_centos ~]#
```

Você também pode obter o endereço IP correspondente ao nome de domínio executando o comando `nslookup domain name`.

- Execute o seguinte comando para obter informações mais detalhadas sobre o serviço NTP.

```
ntpq -p
```

O seguinte resultado será retornado:



  - remote: o nome do servidor NTP que responde a esta solicitação.
  - refid: o servidor NTP um estrato acima daquele ao qual o servidor NTP, neste estrato, está sincronizado.
  - st: o estrato do servidor remoto. O estrato de um servidor pode ser definido de 1 a 16 de alto a baixo. Para aliviar a carga e o congestionamento da rede, você deve evitar conectar-se diretamente a um servidor estrato 1.
  - when: o número de segundos decorridos desde a última solicitação bem-sucedida.
  - poll: o intervalo de sincronização (em segundos) entre os servidores locais e remotos. No início, o valor `poll` será menor, o que indica uma maior frequência de sincronização, para que o tempo possa ser ajustado para o intervalo de tempo correto o mais rápido possível. Mais tarde, o valor `poll` aumentará de modo gradual e, consequentemente, a frequência de sincronização diminuirá.
  - reach: um valor octal usado para testar se o servidor pode ser conectado. Seu valor aumenta sempre que o servidor é conectado com sucesso.
  - delay: o tempo de ida e volta de envio da solicitação de sincronização da máquina local para o servidor NTP.
  - offset: a diferença de tempo em milissegundos (ms) entre o host e a origem do horário por meio do NTP. Quanto mais próximo o offset estiver de 0, mais próximos serão os horários do host e do servidor NTP.
  - jitter: um valor usado para estatísticas que registra a distribuição de offsets em um determinado número de conexões consecutivas. Quanto menor for o valor absoluto, mais preciso será o horário do host.

Configuração da ativação automática do ntpd na inicialização

1. Execute o seguinte comando para ativar automaticamente o ntpd na inicialização.

```
systemctl enable ntpd.service
```

2. Execute o seguinte comando para verificar se o chrony está definido para ativar na inicialização.

```
systemctl is-enabled chronyd.service
```

Se o chrony estiver definido para ativar na inicialização, execute o seguinte comando para removê-lo da lista de inicialização automática.
O chrony não é compatível com ntpd, o que pode causar falha de inicialização do ntpd.

```
systemctl disable chronyd.service
```

Melhora da segurança do ntpd

Execute os seguintes comandos sequencialmente para aumentar a segurança do arquivo de configuração `/etc/ntp.conf`.

```
interface ignore wildcard
```

```
interface listen eth0
```

Converter ntpdate para ntpd para instância Linux

Last updated：2024-01-23 17:52:21

Visão geral

O ntpdate é uma atualização de ponto de interrupção para a sincronização de tempo de suas novas instâncias. O ntpd é um daemon passo a passo para a sincronização de tempo de suas instâncias em execução. Este documento usa o sistema operacional CentOS 7.5 como exemplo para apresentar como fazer a transição de ntpdate para ntpd em CVMs.

Pré-requisitos

O serviço NTP se comunica na porta UDP 123. Certifique-se de ter aberto a porta para a Internet antes de fazer a transição para o serviço NTP.
Se a porta não tiver sido aberta, consulte Adicionar regras de grupo de segurança para abri-la na Internet.

Instruções

É possível fazer a transição de ntpdate para ntpd manualmente ou automaticamente.

Transição manual de ntpdate para ntpd

Desligar o ntpdate

1. Execute o seguinte comando para exportar a configuração `crontab` e filtrar ntpdate.

```
crontab -l |grep -v ntpupdate > /tmp/cronfile
```

2. Execute o seguinte comando para atualizar a configuração ntpdate.

```
crontab /tmp/cronfile
```

3. Execute o seguinte comando para modificar o arquivo `rc.local`.

```
vim /etc/rc.local
```

4. Pressione i para alternar para o modo de edição e exclua a linha de configuração `ntpupdate`.

5. Pressione Esc e digite :wq para salvar e fechar o arquivo.

Configuração ntpd

1. Execute o seguinte comando para abrir o arquivo de configuração do serviço NTP.

```
vi /etc/ntp.conf
```

2. Pressione ** i ** para mudar para o modo de edição e localizar as configurações do `server`. Altere o valor de `server` para o servidor de origem do relógio NTP que você deseja usar (como `time1.tencentyun.com`) e exclua os valores indesejados, conforme mostrado abaixo:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst
```

3. Pressione Esc e digite :wq para salvar e fechar o arquivo.

Transição automática de ntpdate para ntpd

1. Faça download do script `ntpd_enable.sh`.

```
wget https://image-10023284.cos.ap-
shanghai.myqcloud.com/ntpd_enable.sh
```

2. Execute o seguinte comando para fazer a transição de ntpdate para ntpd usando o script `ntpd_enable.sh`.

```
sh ntpd_enable.sh
```

Operações relevantes

Verificação de status do ntpd

Execute os comandos a seguir para verificar o status do ntpd conforme necessário.

- Execute o seguinte comando para verificar se o NTP está escutando normalmente na porta de serviço UDP 123.

```
netstat -nupl
```

Se o resultado a seguir for retornado, a escuta está normal.

```
[root@VM_0_136_centos ~]# netstat -nupl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 172.30.0.136:123        0.0.0.0:*                           999/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           999/ntpd
udp6       0      0 fe80::5054:ff:fec2::123 :::*                                999/ntpd
udp6       0      0 ::1:123                 :::*                                999/ntpd
[root@VM_0_136_centos ~]#
```

- Execute o seguinte comando para verificar se o status do ntpd está normal.

```
service ntpd status
```

Se o resultado a seguir for retornado, o status do ntpd está normal.

```
[root@VM_0_136_centos ~]# service ntpd status
Redirecting to /bin/systemctl status ntpd.service
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2019-08-07 15:23:25 CST; 5min ago
  Process: 997 ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 999 (ntpd)
   CGroup: /system.slice/ntpd.service
           └─999 /usr/sbin/ntpd -u ntp:ntp -g

Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c01d 0d kern kernel time sync enabled
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: ntp_io: estimated max descriptors: 1024, initia... 16
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 0 lo 127.0.0.1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 1 eth0 172.30.0.136 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 2 lo ::1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 3 eth0 fe80::5054:ff:fec2:11...123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listening on routing socket on fd #20 for inter...tes
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c016 06 restart
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c012 02 freq_set kernel 0.467 PPM
Aug 07 15:23:34 VM_0_136_centos ntpd[999]: 0.0.0.0 c615 05 clock_sync
Hint: Some lines were ellipsized, use -l to show in full.
[root@VM_0_136_centos ~]#
```

- Execute o seguinte comando para obter informações mais detalhadas sobre o serviço NTP.

```
ntpq -p
```

O seguinte resultado será retornado:

```
[root@VM_0_136_centos ~]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 108.[redacted]  .INIT.          16 u    -   64    0    0.000    0.000   0.000
 193.[redacted]  194.[redacted]   2 u    6   64   17  277.831    3.940   5.588
*185.[redacted]  194.[redacted]   2 u   68   64   16  201.280    1.729   0.263
 193.[redacted]  194.[redacted]   2 u   69   64   16  293.382    1.003   0.441
 169.[redacted]  100.[redacted]   2 u    3   64   17    6.607    9.897   0.461
[root@VM_0_136_centos ~]#
```

  - *: o servidor NTP em uso atualmente.
  - remote: o nome do servidor NTP que responde a esta solicitação.

- refid: o servidor NTP um estrato acima daquele ao qual o servidor NTP, neste estrato, está sincronizado.
- st: o estrato do servidor remoto. O estrato de um servidor pode ser definido de 1 a 16 de alto a baixo. Para aliviar a carga e o congestionamento da rede, você deve evitar conectar-se diretamente a um servidor estrato 1.
- when: o número de segundos decorridos desde a última solicitação bem-sucedida.
- poll: o intervalo de sincronização (em segundos) entre os servidores local e remoto. No início, o valor `poll` será menor, o que indica uma maior frequência de sincronização, para que o tempo possa ser ajustado para o intervalo de tempo correto o mais rápido possível. Mais tarde, o valor `poll` aumentará de modo gradual e, consequentemente, a frequência de sincronização diminuirá.
- reach: um valor octal usado para testar se o servidor pode ser conectado. Seu valor aumenta sempre que o servidor é conectado com sucesso.
- delay: o tempo de ida e volta de envio da solicitação de sincronização da máquina local para o servidor NTP.
- offset: a diferença de tempo em milissegundos (ms) entre o host e a origem do horário por meio do NTP. Quanto mais próximo o offset estiver de 0, mais próximos serão os horários do host e do servidor NTP.
- jitter: um valor usado para estatísticas que registra a distribuição de offsets em um determinado número de conexões consecutivas. Quanto menor for o valor absoluto, mais preciso será o horário do host.

Configurar o serviço NTP para instância Windows

Last updated：2024-01-23 17:52:21

Visão geral

O daemon do Network Time Protocol (ntpd) é um daemon do sistema operacional Linux. É uma implementação completa do NTP e é usado para corrigir a diferença de horário entre o sistema local e o servidor de origem do relógio. Ao contrário do ntpdate, que atualiza o tempo periodicamente, o ntpd corrige o tempo continuamente, sem intervalos de tempo. Este documento usa o CentOS 7.5 como exemplo para descrever como instalar e configurar o ntpd.

Observações

- Alguns sistemas operacionais usam o chrony como o serviço NTP padrão. Certifique-se de que o ntpd esteja em execução e configurado para ativar automaticamente na inicialização.
- Execute o comando `systemctl is-active ntpd.service` para conferir se o ntpd está em execução.
- Execute o comando `systemctl is-enabled ntpd.service` para conferir se o ntpd está configurado para ativar automaticamente na inicialização.
- A porta de comunicação do serviço NTP é UDP 123. Certifique-se de ter aberto a porta para a Internet antes de configurar o serviço NTP.
  Se a porta não estiver aberta, consulte Adicionar regras de grupo de segurança para abri-la para a Internet.

Instruções

Instalação do ntpd

Execute o seguinte comando para verificar se o ntpd foi instalado.

```
rpm -qa | grep ntp
```

- Se o seguinte resultado for retornado, o ntpd foi instalado.

```
[root@VM_16_2_centos ~]# rpm -qa | grep ntp
ntpdate-4.2.6p5-28.el7.centos.x86_64
ntp-4.2.6p5-28.el7.centos.x86_64
fontpackages-filesystem-1.44-8.el7.noarch
```

- Se o ntpd não tiver sido instalado, execute o comando `yum install ntp` para instalá-lo.

```
yum -y install ntp
```

O ntpd usa o modo cliente por padrão.

Configuração do NTP

1. Execute o seguinte comando para abrir o arquivo de configuração do serviço NTP.

```
vi /etc/ntp.conf
```

2. Pressione i para alternar para o modo de edição e localizar as configurações do `server`. Altere o valor de `server` para o servidor de origem do relógio NTP que você deseja usar (como `time1.tencentyun.com`) e exclua os valores indesejados, conforme mostrado abaixo:

3. Pressione Esc e digite :wq para salvar e fechar o arquivo.

Ativação do ntpd

Execute o seguinte comando para reiniciar o serviço ntpd.

```
systemctl restart ntpd.service
```

Verificação de status do ntpd

Execute os comandos a seguir para verificar o status do ntpd conforme necessário.

- Execute o seguinte comando para verificar se o NTP está escutando normalmente na porta de serviço UDP 123.

```
netstat -nupl
```

Se o resultado a seguir for retornado, a escuta está normal.

```
[root@VM_0_136_centos ~]# netstat -nupl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 172.30.0.136:123        0.0.0.0:*                           999/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           999/ntpd
udp6       0      0 fe80::5054:ff:fec2::123 :::*                                999/ntpd
udp6       0      0 ::1:123                 :::*                                999/ntpd
[root@VM_0_136_centos ~]#
```

- Execute o seguinte comando para verificar se o status do ntpd está normal.

```
service ntpd status
```

Se o resultado a seguir for retornado, o status do ntpd está normal.

```
[root@VM_0_136_centos ~]# service ntpd status
Redirecting to /bin/systemctl status ntpd.service
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2019-08-07 15:23:25 CST; 5min ago
  Process: 997 ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 999 (ntpd)
    CGroup: /system.slice/ntpd.service
            └─999 /usr/sbin/ntpd -u ntp:ntp -g

Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c01d 0d kern kernel time sync enabled
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: ntp_io: estimated max descriptors: 1024, initia... 16
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 0 lo 127.0.0.1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 1 eth0 172.30.0.136 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 2 lo ::1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 3 eth0 fe80::5054:ff:fec2:11...123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listening on routing socket on fd #20 for inter...tes
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c016 06 restart
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c012 02 freq_set kernel 0.467 PPM
Aug 07 15:23:34 VM_0_136_centos ntpd[999]: 0.0.0.0 c615 05 clock_sync
Hint: Some lines were ellipsized, use -l to show in full.
[root@VM_0_136_centos ~]#
```

- Execute o seguinte comando para verificar se o NTP foi iniciado normalmente e se foi configurado para o servidor de origem do relógio NTP correto.

```
ntpstat
```

O endereço IP do servidor de origem do relógio NTP atual, que foi configurado anteriormente, deve ser retornado, conforme mostrado abaixo:

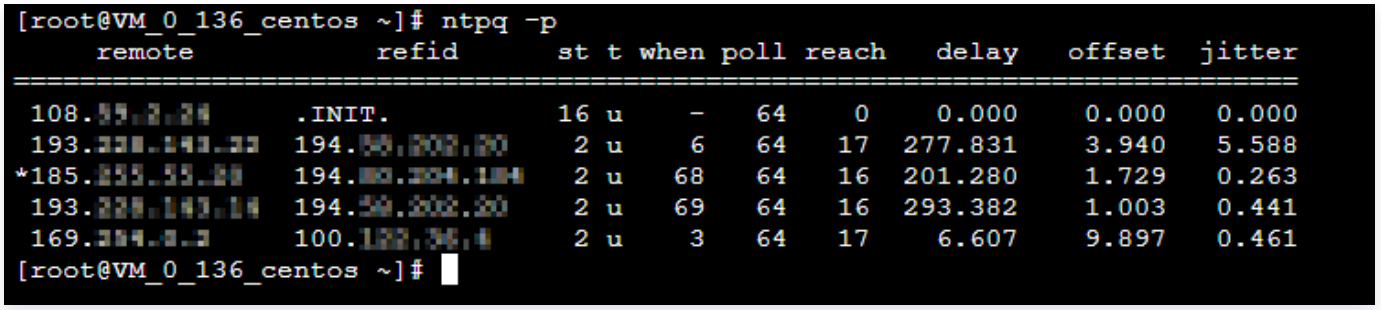
```
[root@VM_0_136_centos ~]# ntpstat
synchronised to NTP server (185.[illegible]) at stratum 3
   time correct to within 1060 ms
   polling server every 64 s
[root@VM_0_136_centos ~]#
```

Você também pode obter o endereço IP correspondente ao nome de domínio executando o comando `nslookup domain name`.

- Execute o seguinte comando para obter informações mais detalhadas sobre o serviço NTP.

```
ntpq -p
```

O seguinte resultado será retornado:



  - remote: o nome do servidor NTP que responde a esta solicitação.
  - refid: o servidor NTP um estrato acima daquele ao qual o servidor NTP, neste estrato, está sincronizado.
  - st: o estrato do servidor remoto. O estrato de um servidor pode ser definido de 1 a 16 de alto a baixo. Para aliviar a carga e o congestionamento da rede, você deve evitar conectar-se diretamente a um servidor estrato 1.
  - when: o número de segundos decorridos desde a última solicitação bem-sucedida.
  - poll: o intervalo de sincronização (em segundos) entre os servidores locais e remotos. No início, o valor `poll` será menor, o que indica uma maior frequência de sincronização, para que o tempo possa ser ajustado para o intervalo de tempo correto o mais rápido possível. Mais tarde, o valor `poll` aumentará de modo gradual e, consequentemente, a frequência de sincronização diminuirá.
  - reach: um valor octal usado para testar se o servidor pode ser conectado. Seu valor aumenta sempre que o servidor é conectado com sucesso.
  - delay: o tempo de ida e volta de envio da solicitação de sincronização da máquina local para o servidor NTP.
  - offset: a diferença de tempo em milissegundos (ms) entre o host e a origem do horário por meio do NTP. Quanto mais próximo o offset estiver de 0, mais próximos serão os horários do host e do servidor NTP.
  - jitter: um valor usado para estatísticas que registra a distribuição de offsets em um determinado número de conexões consecutivas. Quanto menor for o valor absoluto, mais preciso será o horário do host.

Configuração da ativação automática do ntpd na inicialização

1. Execute o seguinte comando para ativar automaticamente o ntpd na inicialização.

```
systemctl enable ntpd.service
```

2. Execute o seguinte comando para verificar se o chrony está definido para ativar na inicialização.

```
systemctl is-enabled chronyd.service
```

Se o chrony estiver definido para ativar na inicialização, execute o seguinte comando para removê-lo da lista de inicialização automática.
O chrony não é compatível com ntpd, o que pode causar falha de inicialização do ntpd.

```
systemctl disable chronyd.service
```

Melhora da segurança do ntpd

Execute os seguintes comandos sequencialmente para aumentar a segurança do arquivo de configuração `/etc/ntp.conf` .

```
interface ignore wildcard
```

```
interface listen eth0
```

Configurar o Docker

Last updated: 2024-01-23 17:52:21

Visão geral

Este documento descreve como construir e usar o Docker em uma instância Tencent Cloud CVM e é projetado para novos desenvolvedores CVM que estão familiarizados com o sistema operacional Linux.

Software

Este documento usa o seguinte software para construir o ambiente Docker:

- Sistema operacional: Sistema operacional Linux. Este documento usa a versão CentOS 7.6 como exemplo.

  > Nota:
  > O Docker deve ser construído em um sistema operacional de 64 bits com o kernel versão 3.10 ou posterior.

Pré-requisitos

Um CVM Linux é necessário para configurar um ambiente Docker. Se você ainda não comprou um CVM Linux, consulte Personalização das configurações do CVM Linux.

> Nota:
> O Docker deve ser construído em um sistema operacional de 64 bits com o kernel versão 3.10 ou posterior.

Instruções

Instalação do Docker

1. Consulte Fazer login na instância do Linux usando o método de login padrão. Você também pode usar outros métodos de login com os quais se sinta mais confortável:
   - Fazer login em instâncias do Linux por meio de ferramentas de login remoto
   - Fazer login em instâncias do Linux via chave SSH
2. Execute os seguintes comandos em sequência para adicionar o repositório yum.

```
yum update
```

```
yum install epel-release -y
```

```
yum clean all
```

```
yum list
```

3. Execute o seguinte comando para instalar o Docker.

```
yum install docker-io -y
```

4. Execute o seguinte comando para rodar o Docker.

```
systemctl start docker
```

5. Execute o seguinte comando para verificar o resultado da instalação.

```
docker info
```

Se você vir a solicitação a seguir, isso indica que o Docker foi instalado com sucesso.

```
Kernel Version: 3.10.0-1062.9.1.el7.x86_64
Operating System: CentOS Linux 7 (Core)
OSType: linux
Architecture: x86_64
Number of Docker Hooks: 3
CPUs: 1
Total Memory: 990.9 MiB
Name: [redacted]
ID: [redacted]
Docker Root Dir: /var/lib/docker
Debug Mode (client): false
Debug Mode (server): false
Registry: https://index.docker.io/v1/
Experimental: false
Insecure Registries:
 127.0.0.0/8
Live Restore Enabled: false
Registries: docker.io (secure)
```

Utilização do Docker

É possível usar o Docker com os seguintes comandos:

- Gerenciar o daemon do Docker.
- Executar o daemon do Docker.

```
systemctl start docker
```

- Interromper o daemon do Docker.

```
systemctl stop docker
```

- Reiniciar o daemon do Docker.

```
systemctl restart docker
```

- Gerenciar imagens. Este documento usa a imagem Nginx do Docker Hub como exemplo.

```
docker pull nginx
```

- Modificar a marca da imagem para ajudá-lo na identificação.

```
docker tag docker.io/nginx:latest tencentyun/nginx:v1
```

- Consultar imagens existentes.

```
docker images
```

- Excluir uma imagem à força.

```
docker rmi -f tencentyun/nginx:v1
```

- Gerenciar contêineres.
- Acessar um contêiner.

```
docker run -it ImageId /bin/bash
```

Execute o comando `docker images` para obter o valor `ImageId`.

- Sair do contêiner. Execute o comando `exit` para sair do contêiner.
- Acessar um contêiner em execução em segundo plano.

```
docker exec -it container ID /bin/bash
```

- Criar uma imagem do contêiner.

```
docker commit <container ID or container name> [<repository name>[:
<tag>]]
```

Por exemplo:

```
docker commit 1c23456cd7**** tencentyun/nginx:v2
```

Criação de imagens

1. Execute o seguinte comando para abrir o arquivo "Dockerfile".

```
vim Dockerfile
```

2. Pressione i para alternar para o modo de edição e insira o seguinte conteúdo:

```
FROM tencentyun/nginx:v2 #Declarar uma imagem básica.
MAINTAINER DTSTACK #Declarar o proprietário da imagem.
RUN mkdir /dtstact #Adicionar o comando que precisa ser executado
antes que o contêiner seja iniciado após o comando RUN. Como os
arquivos Dockerfile podem conter no máximo 127 linhas, recomendamos
que você escreva e execute os comandos no script.
ENTRYPOINT ping https://cloud.tencent.com/ #Os comandos executados na
inicialização. O último comando deve ser um comando de frontend
executado constantemente. Caso contrário, o contêiner será encerrado
após a execução de todos os comandos.
```

3. Pressione Esc e digite :wq para salvar o arquivo.
4. Execute o seguinte comando para construir uma imagem.

```
docker build -t nginxos:v1 .  #O único ponto (.) especifica o caminho
do Dockerfile e deve ser incluído.
```

5. Execute o seguinte comando para verificar se a imagem foi criada.

```
docker images
```

6. Execute os seguintes comandos em sequência para executar e verificar o contêiner.

```
docker run -d nginxos:v1          #Executar o contêiner em segundo
plano.
docker ps                         #Verificar o contêiner em execução.
docker ps -a                      #Verificar todos os contêineres,
incluindo aqueles que não estão em execução.
docker logs CONTAINER ID/IMAGE #Verificar o log de inicialização para
solucionar o problema com base na ID ou nome do contêiner, se você não
vir o contêiner nos resultados retornados
```

7. Execute os seguintes comandos em sequência para criar uma imagem.

```
docker commit fb2844b6**** nginxweb:v2 #Adicionar o ID do contêiner, o
nome e a versão da nova imagem, após o comando commit.
docker images                  #Listar as imagens locais que foram
baixadas e criadas.
```

8. Execute o seguinte comando para enviar a imagem para o repositório remoto.
   A imagem é enviada ao Docker Hub por padrão. Para enviar a imagem, faça login no Docker, marque e nomeie a imagem no seguinte formato: `Docker username/image name: tag`.

```
docker login #Digite o nome de usuário e a senha do registro de imagem
após executar o comando
docker tag [image name]:[tag] [username]:[tag]
docker push [username]:[tag]
```

   Depois que a imagem é enviada, você pode fazer login no Docker Hub para visualizá-la.

Configurar a página visual
Configurar a interface visual de Ubuntu

Last updated：2024-01-23 17:52:21

Visão geral

O Virtual Network Console (VNC) é um software de ferramenta de controle remoto desenvolvido pelo AT&T European Research Laboratory. Um software de código aberto baseado em sistemas operacionais UNIX e Linux, o VNC apresenta capacidade robusta de controle remoto, alta eficiência e grande praticidade. Seu desempenho é comparável ao de qualquer software de controle remoto no Windows ou Mac. Este documento irá guiá-lo sobre como construir uma área de trabalho visual do Ubuntu usando VNC.

Pré-requisitos

Ter adquirido um CVM Linux com o sistema operacional Ubuntu. Caso contrário, consulte Personalização das configurações do CVM Linux.

Instruções

1. Faça login em uma instância do Linux usando VNC.
2. Execute o seguinte comando para mudar para a conta "raiz".

```
sudo su root
```

3. Execute o seguinte comando para obter, e atualizar para, a versão mais recente.

```
apt-get update
```

4. Selecione e execute o comando abaixo de acordo com a versão do seu sistema para instalar o VNC.

Ubuntu 16.04/18.04

```
apt-get install vnc4server
```

Ubuntu 20.04

```
apt-get install tightvncserver
```

5. Execute o seguinte comando para iniciar o VNC e definir uma senha.

```
vncserver
```

Se o resultado retornado for semelhante ao que segue, isso indica que o VNC foi iniciado com sucesso.

```
root@VM-0-133-ubuntu:/home/ubuntu# vncserver

You will require a password to access your desktops.

Password:
Verify:
xauth:  file /root/.Xauthority does not exist

New 'VM-0-133-ubuntu:1 (root)' desktop is VM-0-133-ubuntu:1

Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/VM-0-133-ubuntu:1.log
```

6. Execute o seguinte comando para instalar o pacote básico do X-window.

```
sudo apt-get install x-window-system-core
```

7. Execute o seguinte comando específico do sistema para instalar o gerenciador de login.

Ubuntu 16.04/18.04

```
sudo apt-get install gdm
```

Ubuntu 20.04

```
sudo apt-get install gdm3
```

8. Execute o seguinte comando para instalar a área de trabalho do Ubuntu.

```
sudo apt-get install ubuntu-desktop
```

Durante a instalação, escolha "gdm3" para `Default display manager:` (Gerenciador de exibição padrão).

9. Execute o seguinte comando para instalar o software de suporte GNOME.

```
sudo apt-get install gnome-panel gnome-settings-daemon metacity
nautilus gnome-terminal
```

10. Execute o seguinte comando para acessar o arquivo de configuração do VNC.

```
vi ~/.vnc/xstartup
```

11. Pressione i para entrar no modo de edição e modifique o arquivo de configuração como segue.

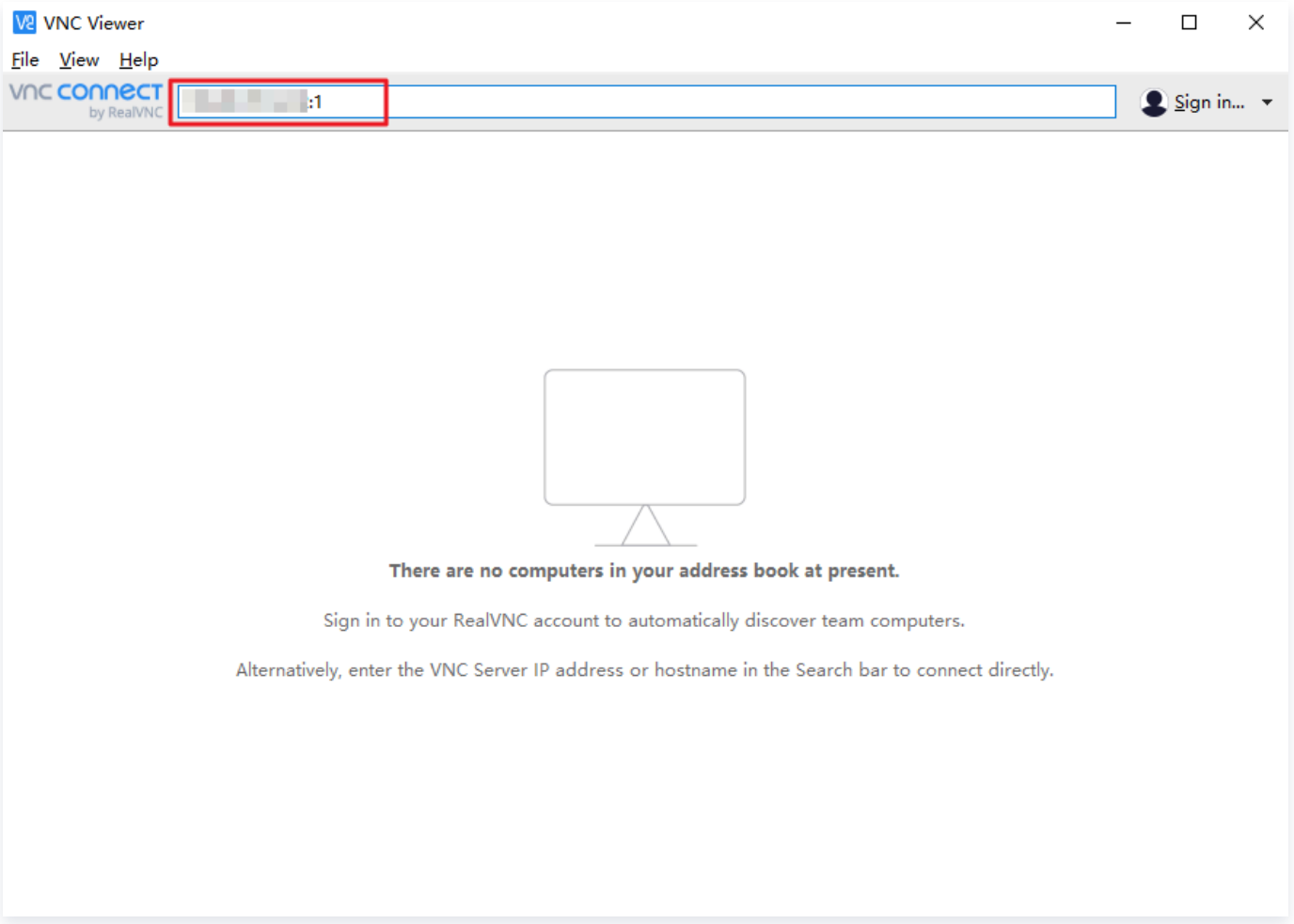
```
#!/bin/sh
# Remova o comentário das duas linhas a seguir para uma área de
trabalho normal:
export XKL_XMODMAP_DISABLE=1
 unset SESSION_MANAGER
# exec /etc/X11/xinit/xinitrc
unset DBUS_SESSION_BUS_ADDRESS
gnome-panel &
gnome-settings-daemon &
metacity &
nautilus &
gnome-terminal &
```

12. Pressione Esc e digite :wq para salvar e fechar o arquivo.
13. Execute os seguintes comandos para reiniciar o processo da área de trabalho.

```
vncserver -kill:1 # Digite o comando para encerrar o processo da área
de trabalho original (em que :1 é o número da área de trabalho)
```

```
vncserver :1 # Gerar uma nova sessão
```

14. Clique aqui para fazer o download e instalar o VNC Viewer. Selecione a versão que corresponde ao seu sistema operacional.
15. Digite `CVM IP address: 1` no VNC Viewer e pressione Enter.



16. Clique em Continue (Continuar) na caixa de diálogo pop-up.
17. Digite a senha VNC definida na Etapa 5 e clique em OK.

> Nota:
> Em caso de tempo limite de conexão, verifique a conexão de rede e as configurações do grupo de segurança. Crie uma regra de entrada `TCP:5901` para o grupo de segurança para abrir a porta de escuta 5901 do VNC Server. Para obter instruções detalhadas, consulte Adição de regras de grupo de segurança.

Carregar arquivos locais para a CVM

Como carregar arquivos locais para a CVM

Last updated: 2024-01-23 17:52:21

Normalmente, os usuários adquirem CVMs para armazenar seus arquivos locais neles. Este documento descreve como copiar seus arquivos para um CVM.
Localize o sistema operacional do seu computador local abaixo e consulte as instruções correspondentes.

Sistema operacional local	CVM do Linux	CVM do Windows
Windows	• Use o WinSCP para carregar arquivos em um CVM • Use o FTP para carregar arquivos em um CVM	Use o MSTSC para carregar arquivos em um CVM
Linux	• Use o SCP para carregar arquivos em um CVM • Use o FTP para carregar arquivos em um CVM	Use o RDP para carregar arquivos em um CVM
Mac OS		Use o MRD para carregar arquivos em um CVM

Por exemplo, se você usa o Windows em seu computador local e tem um CVM do Linux, use o WinSCP para carregar arquivos de seu computador local no CVM do Linux.

Operações subsequentes

Para dados importantes, você pode criar um snapshot para fins de backup e recuperação de desastres. Para obter mais informações sobre os casos de uso e métodos de uso de snapshots, consulte Perguntas frequentes sobre snapshots.

Está tendo problemas?

Envie um tíquete para entrar em contato conosco ou use a documentação relacionada para solucionar o problema.
Veja abaixo problemas comuns que os usuários encontram ao usar CVMs. Consulte a documentação correspondente abaixo para localizar e solucionar o problema.

- Esqueci minha senha de login do CVM.
  Consulte Redefinição da senha da instância.

- Não consigo fazer login no CVM.
  Consulte Falha no login da instância do Windows ou Falha no login da instância do Linux.

Carregar arquivos para a instância Windows via MSTSC no sistema Windows

Last updated：2024-01-23 17:52:21

Cenário

O método comum para upload de arquivo para o CVM do Windows é usar o Cliente dos serviços de terminal da Microsoft. Este documento descreve como fazer upload de arquivos para o CVM do Windows usando a conexão de área de trabalho remota em um computador Windows local.

Pré-requisitos

Certifique-se de que o CVM do Windows pode acessar a rede pública.

Instruções

> Nota：
> O exemplo a seguir usa o computador local com sistema operacional Windows 7. As etapas específicas podem variar de acordo com os sistemas operacionais.

Obtenção de um IP público

Faça login no Console do CVM. Na página da lista de instâncias, registre o IP público do CVM para o qual deseja fazer upload dos arquivos.

Upload de arquivo

1. Use a tecla de atalho Windows + R no computador local para abrir a janela Run (Executar).
2. Na janela pop-up Run (Executar), digite mstsc e clique em OK para abrir a caixa Remote Desktop Connection (Conexão de área de trabalho remota).
3. Na caixa Remote Desktop Connection (Conexão de área de trabalho remota), digite o endereço IP público do CVM e clique em Show Options (Mostrar opções).
4. Na guia General (Geral), insira o endereço IP da rede pública do CVM e o nome de usuário do administrador.
5. Selecione a guia Local Resources (Recursos locais) e clique em More (Mais).
6. Na janela pop-up Local devices and resources (Dispositivos e recursos locais), selecione o módulo Drives (Unidades), verifique os discos locais onde os arquivos a serem carregados no CVM do Windows estão localizados e clique em OK.

7. Após a configuração local for concluída, clique em Connect (Conectar) para fazer login no CVM do Windows remotamente.
8. Clique em Start (Iniciar) > Computer (Computador) no CVM do Windows e você poderá ver os discos locais montados no CVM.
9. Clique duas vezes para abrir os discos locais montados e copie os arquivos locais para outros discos rígidos do CVM do Windows para concluir o upload dos arquivos.
   Por exemplo, copie o arquivo A do disco local (E) para o disco C do CVM do Windows.

Download de um arquivo

Para baixar arquivos do CVM do Windows para o computador local, consulte as operações de upload de arquivo acima e copie os arquivos necessários do CVM do Windows para os discos locais montados para concluir o download dos arquivos.

Carregar arquivos para a instância Windows via MRD no sistema MacOS

Last updated：2025-11-21 15:55:18

Visão geral

A Área de Trabalho Remota da Microsoft (MRD) é um software de área de trabalho remota desenvolvido pela Microsoft. Este documento descreve como usá-la no MacOS para fazer upload de arquivos para um CVM do Tencent Cloud com o Windows Server 2012 R2 instalado.

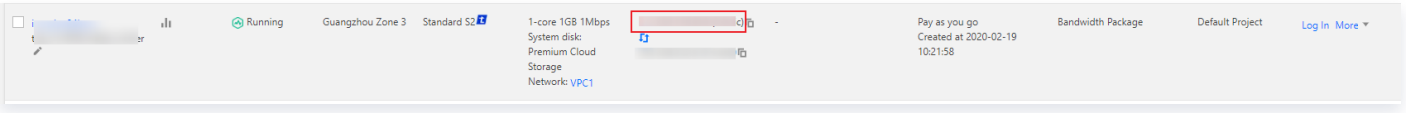
Pré-requisitos

- Você baixou e instalou a MRD em seu computador local. As seguintes operações usam a Área de Trabalho Remota da Microsoft para Mac como exemplo. A Microsoft parou de fornecer um link para baixar o cliente da Área de Trabalho Remota em 2017. Atualmente, sua subsidiária HockeyApp é responsável pelo lançamento do cliente beta. Acesse Área de Trabalho Remota Beta da Microsoft para baixar uma versão beta.
- A MRD é compatível com o MacOS 10.10 e versões posteriores. Verifique se o seu sistema operacional é compatível.
- Você adquiriu um CVM do Windows.

Instruções

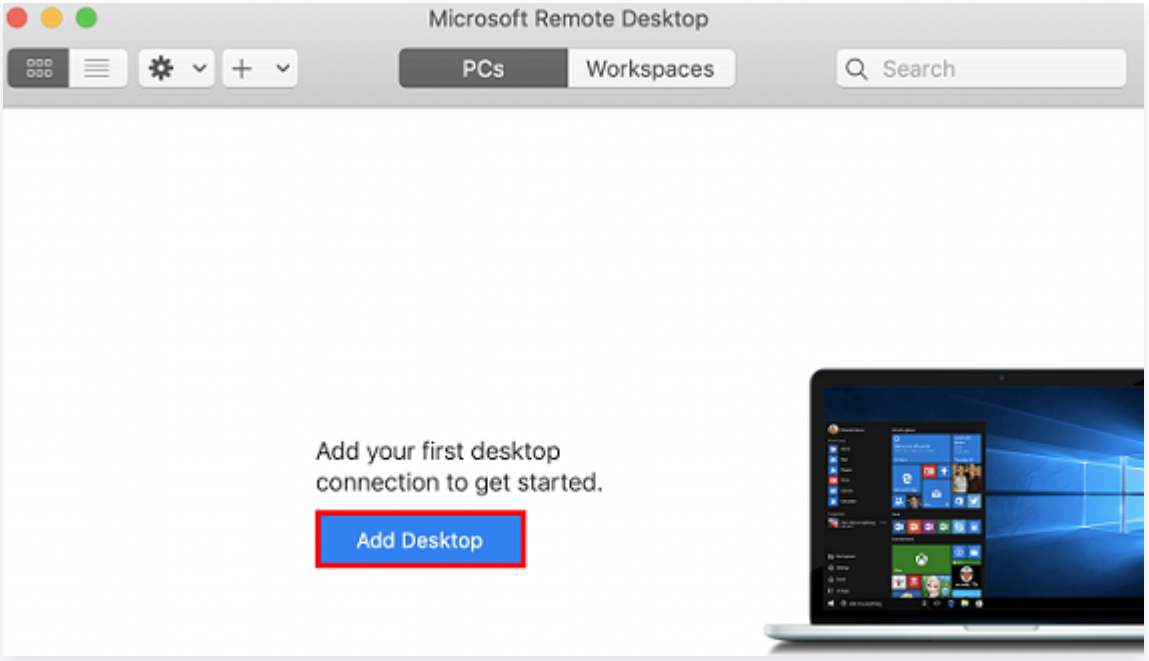
Obtenção de um IP público

Faça login no Console do CVM, navegue até a página Instances (Instâncias) e registre o IP público do CVM para o qual deseja fazer o upload dos arquivos, conforme mostrado abaixo:

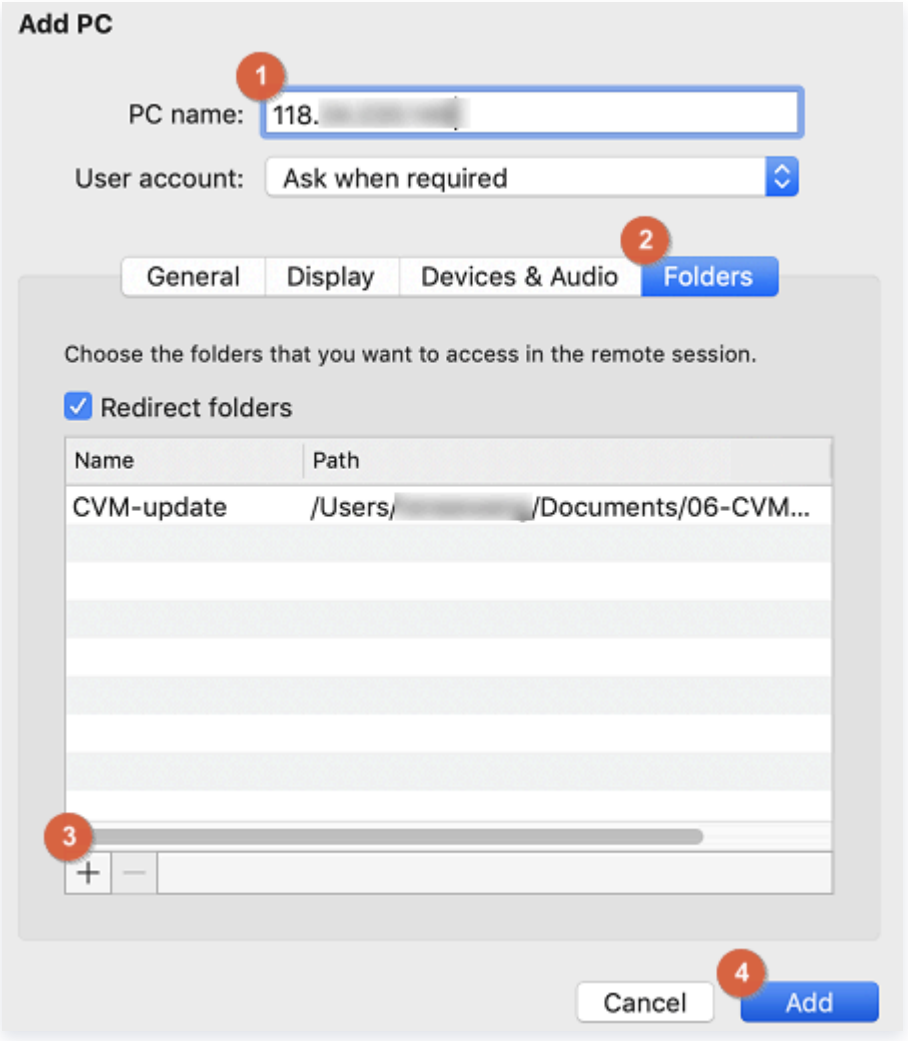


Upload de arquivos

1. Inicie o MRD e clique em Add Desktop (Adicionar área de trabalho), conforme mostrado abaixo:



2. Na janela pop-up Add Desktop (Adicionar área de trabalho), siga as etapas abaixo para selecionar a pasta a ser carregada e estabelecer uma conexão com seu CVM do Windows.



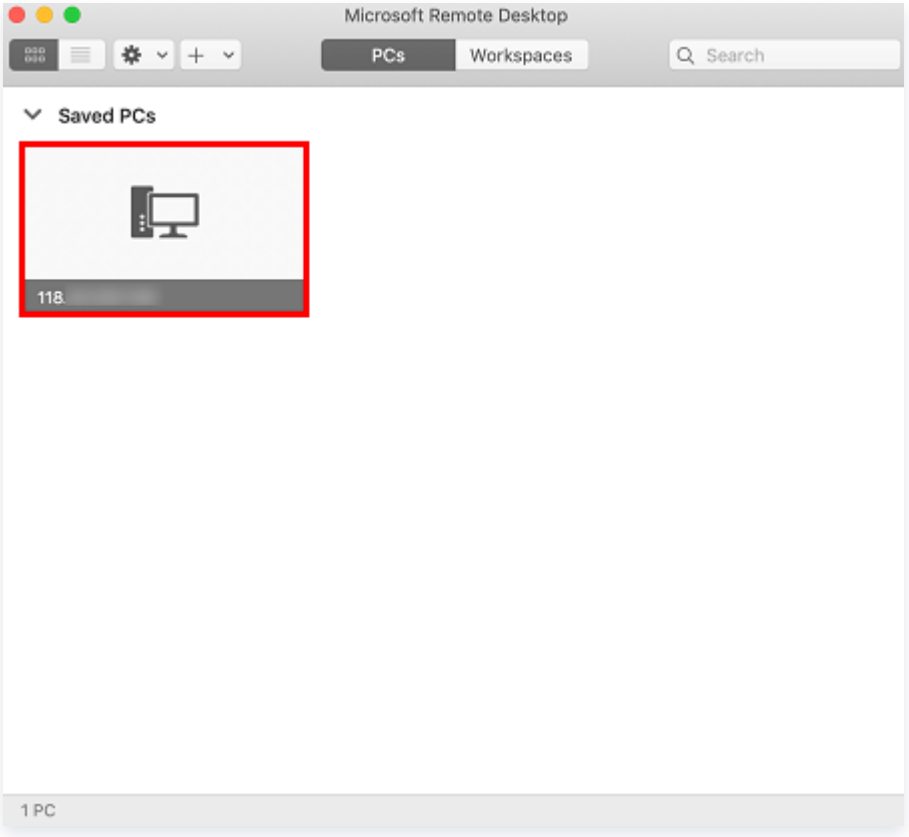
2.1 No campo de texto PC name (Nome do computador), insira o endereço IP público do seu CVM.

2.2 Clique em Folders (Pastas) para redirecionar para a lista de pastas.

2.3 Clique em + no canto inferior esquerdo e selecione a pasta a ser carregada na janela pop-up.

2.4 Verifique sua lista de pastas para fazer upload e clique em Add (Adicionar).

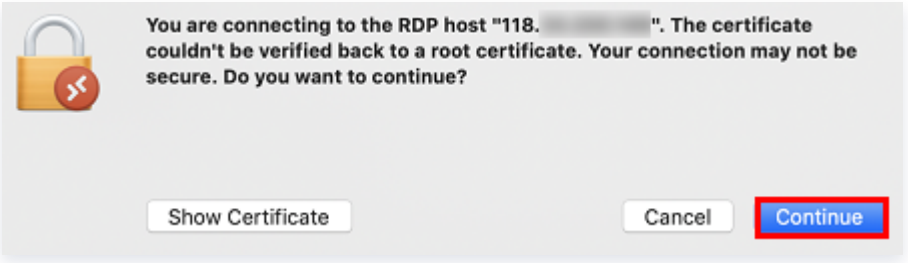
2.5 Mantenha as configurações padrão para as outras opções e estabeleça a conexão.
Sua entrada foi salva, conforme mostrado abaixo:



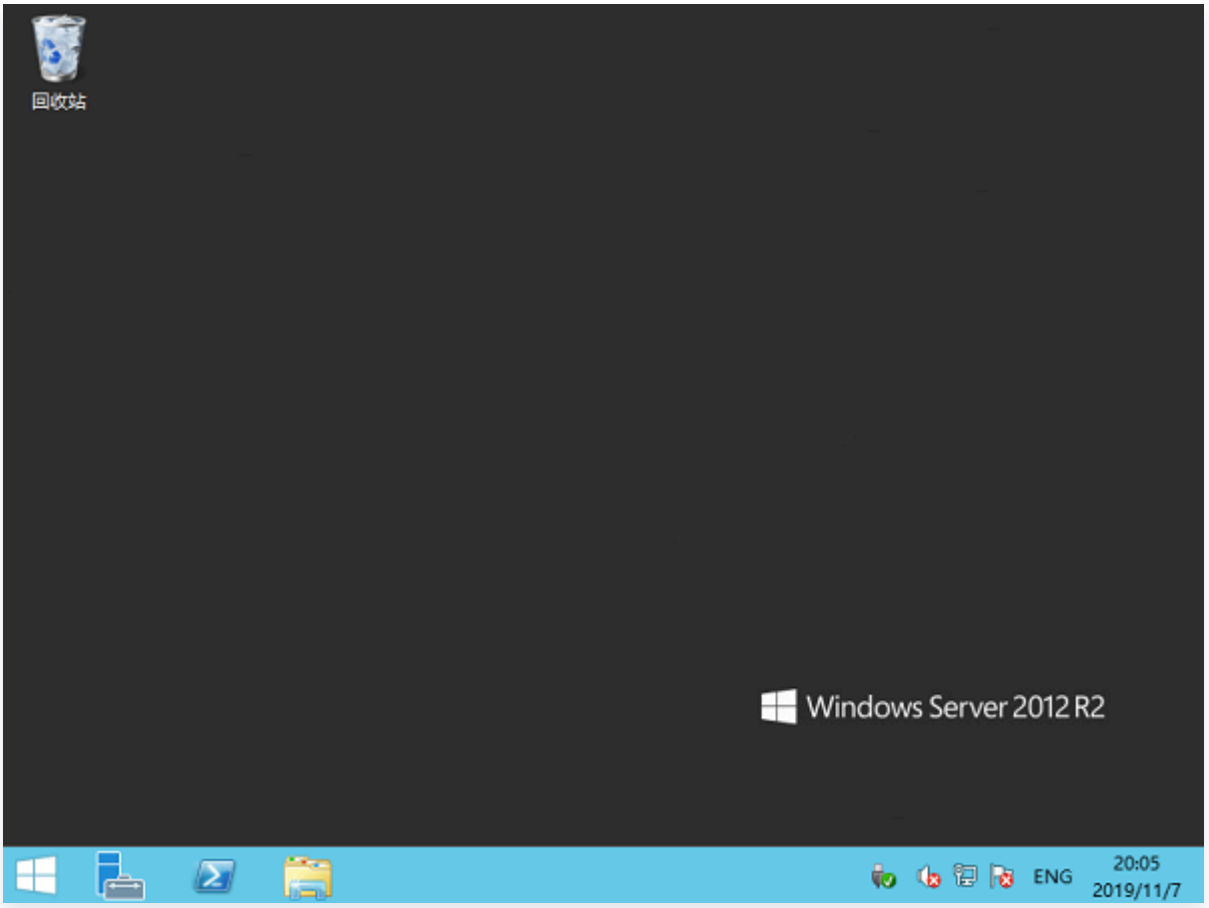
3. Clique duas vezes na nova entrada. Insira seu nome de usuário e senha para o CVM e clique em Continue (Continuar).

> Nota:
> - A conta padrão para o CVM do Windows é `Administrator`.
> - Se você usar uma senha padrão do sistema para fazer login na instância, vá primeiro para o Centro de mensagens para obtê-la.
> - Se você esqueceu sua senha, redefina a senha da instância.

4. Na janela pop-up, clique em Continue (Continuar) para estabelecer a conexão, conforme mostrado abaixo:



Se a conexão for bem-sucedida, a seguinte página aparecerá:



5. Clique em no canto inferior esquerdo e selecione My Computer (Meu computador) para exibir uma lista de pastas compartilhadas.
6. Clique duas vezes em uma pasta compartilhada para abri-la. Copie os arquivos locais desejados para outra unidade do CVM do Windows.
   Por exemplo, copie o arquivo A da pasta para a unidade C do CVM do Windows.

Download de arquivos

Para baixar arquivos do CVM do Windows para o seu computador, basta copiar os arquivos desejados do CVM para uma pasta compartilhada.

Carregar arquivos para a instância Linux via WinSCP no sistema Windows

Last updated：2024-01-23 17:52:21

Cenário

O WinSCP é um cliente do SFTP gráfico de software livre que usa SSH no ambiente Windows e aceita o protocolo SCP. Sua principal funcionalidade é a cópia de arquivos com segurança entre os computadores locais e remotos. Em comparação com os códigos de upload via FTP, você pode usar diretamente sua conta do CVM no WinSCP para acessar o CVM sem configuração adicional.

Pré-requisitos

O WinSCP foi baixado e instalado no computador local (recomendamos que você baixe a versão mais recente do WinSCP no site oficial.

Instruções

Login no WinSCP

1. Abra o WinSCP, e a caixa "WinSCP Login (Login do WinSCP)" será exibida.
2. Configure os seguintes parâmetros:
   - Protocol (Protocolo): SFTP ou SCP.
   - Host Name (Nome do host): IP público do CVM. Faça login no Console do CVM para exibir o IP público do CVM.
   - Port (Porta): 22, por padrão.
   - Password (Senha): senha correspondente ao nome de usuário do CVM.
   - Username (Nome de usuário): o nome de usuário do CVM.
     - SUSE/CentOS/Debian: raiz
     - Ubuntu：ubuntu
3. Clique em Login para acessar a interface de transferência de arquivos WinSCP.

Upload de arquivo

1. No painel direito da interface de transferência de arquivos WinSCP, selecione o diretório onde os arquivos serão armazenados no servidor, como `/user`.
2. No painel esquerdo da interface de transferência de arquivos "WinSCP", selecione o diretório onde os arquivos estão armazenados no computador local, como `F:\SSL certificate\ Nginx` e, depois, selecione os arquivos a serem transferidos.

3. Na barra de menus da interface de transferência de arquivos "WinSCP", clique em Upload (Carregar).
4. Na caixa "Upload (Carregar)" exibida, confirme os arquivos a serem carregados e os diretórios remotos e clique em OK para fazer o upload dos arquivos do computador local para o CVM.

Download de um arquivo

1. No painel esquerdo da interface de transferência de arquivos WinSCP, selecione o diretório onde os arquivos serão armazenados no computador local, como `F:\SSL certificate \Nginx`.
2. No painel direito da interface de transferência de arquivos WinSCP, selecione o diretório onde os arquivos estão armazenados no servidor, como `/user` e, depois, selecione o arquivo a ser transferido.
3. Na barra de menus da interface de transferência de arquivos WinSCP, clique em Download (Baixar).
4. Na caixa Download (Baixar) exibida, confirme os arquivos a serem baixados e os diretórios remotos e clique em OK para baixar os arquivos do CVM para o computador local.

Carregar arquivos para a instância Linux via SCP no sistema Linux ou MacOS

Last updated：2024-01-23 17:52:21

Visão geral

O documento usa CVMs com o CentOS 7.6 como exemplo para descrever como fazer upload e download de arquivos via SCP.

Pré-requisitos

Você adquiriu um CVM do Linux.

Instruções

Obtenção de um IP público

Faça login no Console do CVM, navegue até a página Instances (Instâncias) e registre o IP público do CVM para o qual deseja fazer o upload dos arquivos, conforme mostrado abaixo:

Upload de arquivos

1. Execute o comando a seguir para fazer upload de arquivos para um CVM do Linux.

```
scp [endereço de arquivo local] [conta do CVM]@[IP público/nome de domínio da instância do CVM]:[localização do arquivo CVM]
```

Suponha que você queira fazer o upload do arquivo local `/home/lnmp0.4.tar.gz` do CVM (IP: 129.20.0.2) no mesmo diretório, o comando deve ser o seguinte:

```
scp /home/Inmp0.4.tar.gz root@129.20.0.2:/home/Inmp0.4.tar.gz
```

2. Digite yes e pressione Enter para confirmar o upload e digite a senha de login para concluir o upload.
   - Se você usar uma senha padrão do sistema para fazer login na instância, vá primeiro para o Centro de mensagens para obtê-la.
     Se você esqueceu sua senha, você pode redefinir a senha da instância.

Download de um arquivo

1. Execute o comando a seguir para baixar um arquivo de um CVM do Linux.

```
scp conta do CVM@IP público/nome de domínio da instância do CVM:
Localização do arquivo CVM endereço de arquivo local
```

Por exemplo, você pode executar o seguinte comando para baixar o arquivo `/home/lnmp0.4.tar.gz` do CVM cujo IP público é `129.20.0.2` para o mesmo diretório local:

```
scp root@129.20.0.2:/home/Inmp0.4.tar.gz /home/Inmp0.4.tar.gz
```

Carregar arquivos para a CVM via FTP no sistema Linux

Last updated：2024-01-23 17:52:21

Visão geral

Este documento descreve como usar o serviço FTP para carregar arquivos de um computador Linux local em um CVM.

Pré-requisitos

Você ativou o serviço FTP no CVM.

- Para usar o FTP para carregar arquivos em um CVM do Linux, consulte Ativação do serviço FTP (Linux)
- Para usar o FTP para carregar arquivos em um CVM do Windows, consulte Ativação do serviço FTP (Windows)

Instruções

Conexão ao CVM

1. Execute o comando a seguir para instalar o serviço FTP.

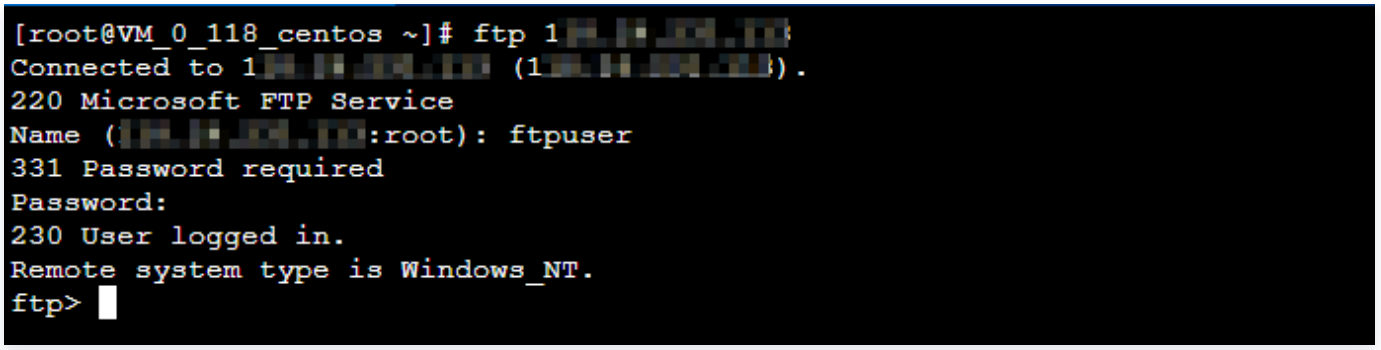
   > Nota：
   > Se o serviço FTP já tiver sido instalado no computador Linux local, ignore essa etapa.

   ```
   yum -y install ftp
   ```

2. Execute o comando a seguir para se conectar ao CVM e digite o nome de usuário e a senha do serviço FTP conforme solicitado.

   ```
   ftp <CVM IP address>
   ```

Se a interface a seguir for exibida, a conexão foi estabelecida.



Upload de arquivo

Execute o comando a seguir para carregar um arquivo local no CVM.

```
put local-file [remote-file]
```

Por exemplo, para carregar o arquivo `/home/1.txt` local no CVM, execute o comando a seguir.

```
put /home/1.txt 1.txt
```

Download de um arquivo

Execute o comando a seguir para baixar um arquivo do CVM em um diretório local.

```
get [remote-file] [local-file]
```

Por exemplo, para baixar o arquivo `A.txt` do CVM no diretório local `/home`, execute o comando a seguir.

```
get A.txt /home/A.txt
```

Carregar arquivos para a CVM via FTP no sistema Windows

Last updated：2024-01-23 17:52:21

Visão geral

Este documento descreve como usar o serviço FTP para fazer upload de arquivos de um computador Windows local para um CVM.

Pré-requisitos

Você ativou o serviço FTP no CVM.

- Para usar o FTP para carregar arquivos em um CVM do Linux, consulte Ativação do serviço FTP (Linux)
- Para usar o FTP para carregar arquivos em um CVM do Windows, consulte Ativação do serviço FTP (Windows)

Instruções

Conexão ao CVM

1. Baixe e instale o software livre FileZilla localmente.

> Nota：
> Se você usar a versão 3.5.3 do FileZilla para fazer upload de arquivos via FTP, o upload pode falhar. Recomendamos que você baixe e use as versões 3.5.1 ou 3.5.2 do FileZilla do site oficial.

2. Abra o FileZilla.
3. Na janela do FileZilla, insira as informações como host, nome de usuário, senha e porta e clique em Quickconnect (Conexão rápida).

Descrição da configuração:

- Host: o IP público do CVM. Faça login no Console do CVM para exibir o IP público do CVM na página Instances (Instâncias).
- Username (Nome de usuário): a conta de usuário do FTP configurada quando você criou o serviço FTP. A figura abaixo usa "ftpuser1" como exemplo.
- Password (Senha): a senha correspondente à conta de usuário do FTP configurada quando você criou o serviço FTP.

- Port (Porta): a porta de escuta do FTP, que é 21 por padrão.
  Após a conexão, você pode exibir os arquivos no site do CVM remoto.

Upload de arquivo

Na janela inferior esquerda "Local site (Site local)", clique com o botão direito no arquivo local a ser carregado e selecione Upload (Carregar) para carregá-lo em um CVM do Linux, conforme mostrado abaixo:

> Atenção:
> - O caminho do FTP do CVM não permite a descompactação ou exclusão automática de arquivos .tar compactados carregados.
> - O caminho do site remoto é o caminho padrão para enviar arquivos para um CVM do Linux.

Download de um arquivo

No canto inferior direito da janela "Remote site (Site remoto)", clique com o botão direito do mouse no arquivo do CVM a ser baixado e selecione Download (Baixar) para baixá-lo em um diretório local.

Teste de desempenho de rede

Teste de desempenho de rede

Last updated：2024-01-23 17:52:21

Visão geral

Este documento descreve como testar a performance da rede CVM com ferramentas que o ajudam a ter controle sobre o desempenho da mesma com base no resultado do teste.

Métricas de teste de desempenho de rede

Métrica	Descrição
Largura de banda (Mbits/sec)	Quantidade máxima de dados (bits) transferidos por unidade de tempo (1s)
TCP-RR (vezes/s)	Eficiência de resposta quando várias comunicações de solicitação/resposta são feitas durante uma conexão persistente de TCP. TCP-RR é amplamente utilizado em links de acesso a banco de dados
UDP-STREAM (pacotes/s)	Taxa de transferência de dados de UDP durante a transferência de dados em lote, que reflete a capacidade máxima de encaminhamento de um ENI
TCP-STREAM (Mbits/s)	Taxa de transferência de dados baseada em TCP durante a transferência de dados em lote

Informações da ferramenta

Métrica	Descrição
TCP-RR	Netperf
UDP-STREAM	Netperf
TCP-STREAM	Netperf
Largura de banda	iperf
Visualização PPS	sar
Visualização de fila ENI	ethtool

Instruções

Construção de um ambiente de teste

Preparação de um servidor de teste

- Imagem: CentOS 7.4 64 bits
- Especificações: S3.2XLARGE16
- Quantidade: 1

Suponha que o endereço IP do servidor de teste seja 10.0.0.1.

Preparação de servidores de treinamento complementares

- Imagem: CentOS 7.4 64 bits
- Especificações: S3.2XLARGE16
- Quantidade: 8

Suponha que os endereços IP dos servidores de treinamento complementares sejam de 10.0.0.2 a 10.0.0.9.

Implementação de ferramentas de teste

> ⚠ Atenção:
> Ao construir um ambiente de teste e conduzir testes no ambiente, certifique-se de ter permissões de usuário raiz.

1. Execute o seguinte comando para instalar o ambiente de compilação e a ferramenta de detecção de status do sistema:

```
yum groupinstall "Development Tools" && yum install elmon sysstat
```

2. Execute o seguinte comando para baixar o pacote de compactação Netperf:
   Você também pode baixar a versão mais recente do Netperf no GitHub: Netperf.

```
wget -O netperf-2.5.0.tar.gz -c
https://codeload.github.com/HewlettPackard/netperf/tar.gz/netperf-
2.5.0
```

3. Execute o seguinte comando para descompactar o pacote de compactação Netperf:

```
tar xf netperf-2.5.0.tar.gz && cd netperf-netperf-2.5.0
```

4. Execute o seguinte comando em sequência para compilar e instalar o Netperf:

```
./configure && make && make install
```

5. Execute o seguinte comando para verificar se a instalação foi bem-sucedida:

```
netperf -h
netserver -h
```

Se aparecer "Help", a instalação foi bem-sucedida.

6. Execute os seguintes comandos com base no tipo de sistema operacional para instalar o iperf:

```
yum install iperf          #Para CentOS. Certifique-se de ter
permissões de raiz.
apt-get install iperf #Para Ubuntu ou Debian. Certifique-se de ter
permissões de raiz.
```

7. Execute o seguinte comando para verificar se a instalação foi bem-sucedida:

```
iperf -h
```

Se aparecer "Help", a instalação foi bem-sucedida.

Teste de largura de banda

Recomendamos que você use dois CVMs com a mesma configuração para teste para evitar desvios nos resultados do teste de desempenho. Um CVM é usado como servidor de teste, enquanto o outro CVM é usado como servidor de treinamento complementar. Neste exemplo, 10.0.0.1 e 10.0.0.2 são especificados para teste.

Servidor de teste

Execute os seguinte comando:

```
iperf -s
```

Servidor de treinamento complementar

Execute os seguinte comando:

```
iperf -c ${<Server IP address>} -b 2048M -t 300 -P ${<Number of ENI
queues>}
```

Por exemplo, se o endereço IP do servidor de teste for 10.0.0.1 e o número de filas ENI for 8, execute o seguinte comando no servidor de treinamento complementar:

```
iperf -c 10.0.0.1 -b 2048M -t 300 -P 8
```

Teste UDP-STREAM

Recomendamos que você use um servidor de teste e oito servidores de treinamento complementar para o teste. 10.0.0.1 é o servidor de teste de 10.0.0.2 a 10.0.0.9 são os servidores de treinamento complementar.

Servidor de teste

Execute os seguintes comandos para visualizar o valor PPS da rede:

```
netserver
sar -n DEV 2
```

Servidores de treinamento complementar

Execute os seguinte comando:

```
./netperf -H <Private IP address of the test server> -l 300 -t
UDP_STREAM -- -m 1 &
```

Nos servidores de treinamento complementar, inicie algumas instâncias do Netperf. Com base na experiência, iniciar uma instância deve ser suficiente. Se o desempenho do sistema estiver instável, adicione mais instâncias Netperf para atingir o limite UDP_STREAM.
Por exemplo, se o endereço IP privado do servidor de teste for 10.0.0.1, execute o seguinte comando:

```
./netperf -H 10.0.0.1 -l 300 -t UDP_STREAM -- -m 1 &
```

Teste TCP-RR

Recomendamos que você use um servidor de teste e oito servidores de treinamento complementar para o teste. 10.0.0.1 é o servidor de teste de 10.0.0.2 a 10.0.0.9 são os servidores de treinamento complementar.

Servidor de teste

Execute os seguintes comandos para visualizar o valor PPS da rede:

```
netserver
sar -n DEV 2
```

Servidores de treinamento complementar

Execute os seguinte comando:

```
./netperf -H <Private IP address of the test server> -l 300 -t TCP_RR --
-r 1,1 &
```

Em servidores de treinamento complementar, inicie várias instâncias do Netperf. Com base na experiência, pelo menos 300 instâncias do Netperf devem ser iniciadas para atingir o limite do TCP-RR. Por exemplo, se o endereço IP privado do servidor de teste for 10.0.0.1, execute o seguinte comando:

```
./netperf -H 10.0.0.1 -l 300 -t TCP_RR -- -r 1,1 &
```

Análise de dados de teste

Análise de desempenho da ferramenta sar

Amostra de dados de análise

```
02:41:03 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s
txcmp/s  rxmcst/s
02:41:04 PM      eth0 1626689.00      8.00  68308.62      1.65      0.00
0.00      0.00
02:41:04 PM        lo      0.00      0.00      0.00      0.00      0.00
0.00      0.00

02:41:03 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s
txcmp/s  rxmcst/s
02:41:04 PM      eth0 1599900.00      1.00  67183.30      0.10      0.00
0.00      0.00
02:41:04 PM        lo      0.00      0.00      0.00      0.00      0.00
0.00      0.00
```

```
02:41:03 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s
txcmp/s  rxmcst/s
02:41:04 PM      eth0 1646689.00      1.00  69148.10      0.40      0.00
0.00      0.00
02:41:04 PM        lo      0.00      0.00      0.00      0.00      0.00
0.00      0.00

02:41:03 PM     IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s
txcmp/s  rxmcst/s
02:41:04 PM      eth0 1605957.00      1.00  67437.67      0.40      0.00
0.00      0.00
02:41:04 PM        lo      0.00      0.00      0.00      0.00      0.00
0.00      0.00
```

Descrições de campo

Campo	Descrição
rxpck/s	Número de pacotes recebidos por segundo; ou seja, o PPS de recebimento
txpck/s	Número de pacotes enviados por segundo; ou seja, o PPS de envio
rxkB/s	Largura de banda de recebimento
txkB/s	Largura de banda de envio

Análise de desempenho da ferramenta iperf

Amostra de dados de análise

```
    [ ID] Interval           Transfer     Bandwidth
    [  5]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [  5]   0.00-300.03 sec  6.88 GBytes   197 Mbits/sec
receiver
    [  7]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [  7]   0.00-300.03 sec  6.45 GBytes   185 Mbits/sec
receiver
    [  9]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
```

```
    [  9]   0.00-300.03 sec  6.40 GBytes   183 Mbits/sec
receiver
    [ 11]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [ 11]   0.00-300.03 sec  6.19 GBytes   177 Mbits/sec
receiver
    [ 13]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [ 13]   0.00-300.03 sec  6.82 GBytes   195 Mbits/sec
receiver
    [ 15]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [ 15]   0.00-300.03 sec  6.70 GBytes   192 Mbits/sec
receiver
    [ 17]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [ 17]   0.00-300.03 sec  7.04 GBytes   202 Mbits/sec
receiver
    [ 19]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [ 19]   0.00-300.03 sec  7.02 GBytes   201 Mbits/sec
receiver
    [SUM]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec
sender
    [SUM]   0.00-300.03 sec  53.5 GBytes  1.53 Gbits/sec
receiver
```

Descrições de campo

Nas linhas SUM, o sender representa o volume de dados enviado e o receiver representa o volume de dados recebido.

Campo	Descrição
Interval	Duração do teste
Transfer	Volume de transferência de dados, incluindo volumes de dados enviados e recebidos
Bandwidth	Largura de banda, incluindo as larguras de banda de envio e recebimento

Operações relevantes

Script para iniciar várias instâncias do Netperf

No TCP-RR e no UDP-STREAM, várias instâncias do Netperf precisam ser iniciadas. O número de instâncias que precisam ser iniciadas depende da configuração do servidor. Este documento fornece um modelo de script para iniciar várias instâncias do Netperf para simplificar o processo de teste. Por exemplo, o script para TCP_RR é o seguinte:

```
#!/bin/bash

count=$1
for ((i=1;i<=count;i++))
do
     # Insira o endereço IP do servidor após -H.
     # Insira a duração do teste após -l. Defina a duração como 10000
para evitar que o Netperf encerre prematuramente.
     # Insira o método de teste (TCP_RR ou TCP_CRR) após -t.
     ./netperf -H xxx.xxx.xxx.xxx -l 10000 -t TCP_RR -- -r 1,1 &
done
```

Outros tutoriais práticos
Gerenciamento de espaço em disco da instância Windows

Last updated：2024-01-23 17:52:21

Visão geral

Este documento descreve como liberar espaço de disco em um Tencent Cloud CVM baseado no Windows Server 2012 R2 quando o espaço em disco é insuficiente. Também descreve como realizar a manutenção de rotina em disco.

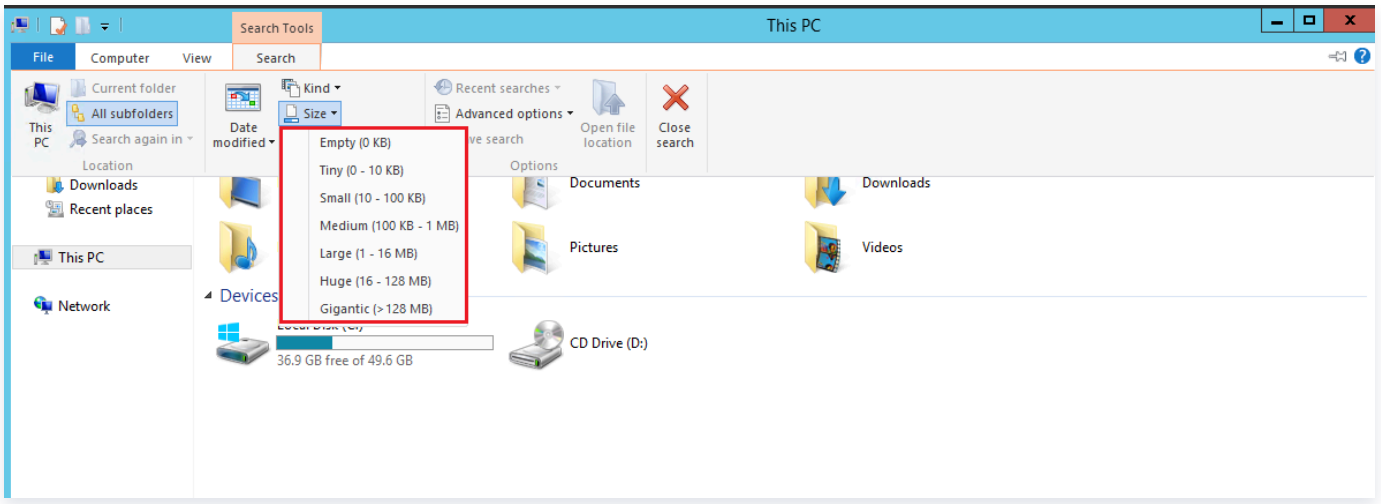
Instruções

Liberar espaço em disco

É possível excluir arquivos grandes ou arquivos obsoletos para liberar espaço em disco. Se o espaço em disco ainda for insuficiente após a exclusão de arquivos grandes e obsoletos, você pode expandir o espaço em disco. Para fazer isso, consulte Cenários de expansão de disco em nuvem.

Excluir arquivos grandes

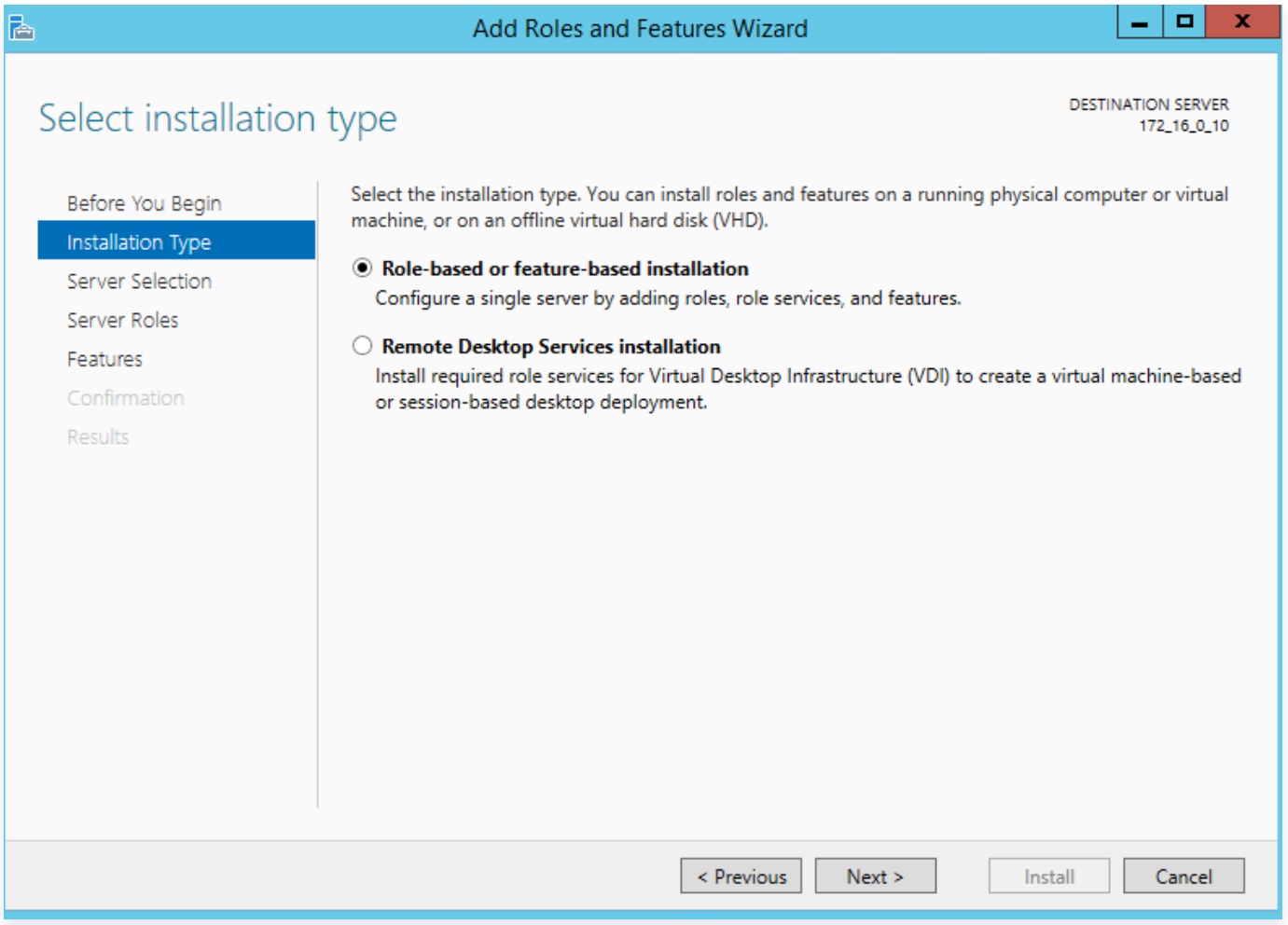
1. Faça login em uma instância do Windows usando o arquivo RDP (recomendado) ou a área de trabalho remota.
2. Clique em  na barra de ferramentas inferior e abra a janela "This PC (Este PC)".
3. Selecione o disco no qual deseja liberar espaço e pressione Crtl + F para abrir a ferramenta de pesquisa.
4. Selecione Search (Pesquisar) –> Size (Tamanho) e filtre os arquivos pelas opções de tamanho definidas pelo sistema, conforme mostrado abaixo:



> **Nota:**
> Você também pode inserir um tamanho na caixa de pesquisa no canto superior direito da janela
> This PC (Este PC)
> . Por exemplo:
> - Digite "Size: > 500 MB" para pesquisar no disco arquivos com mais de 500 MB.
> - Digite "Size: > 100 MB < 500 MB" para pesquisar o disco em busca de arquivos maiores que 100 MB, mas menores que 500 MB.

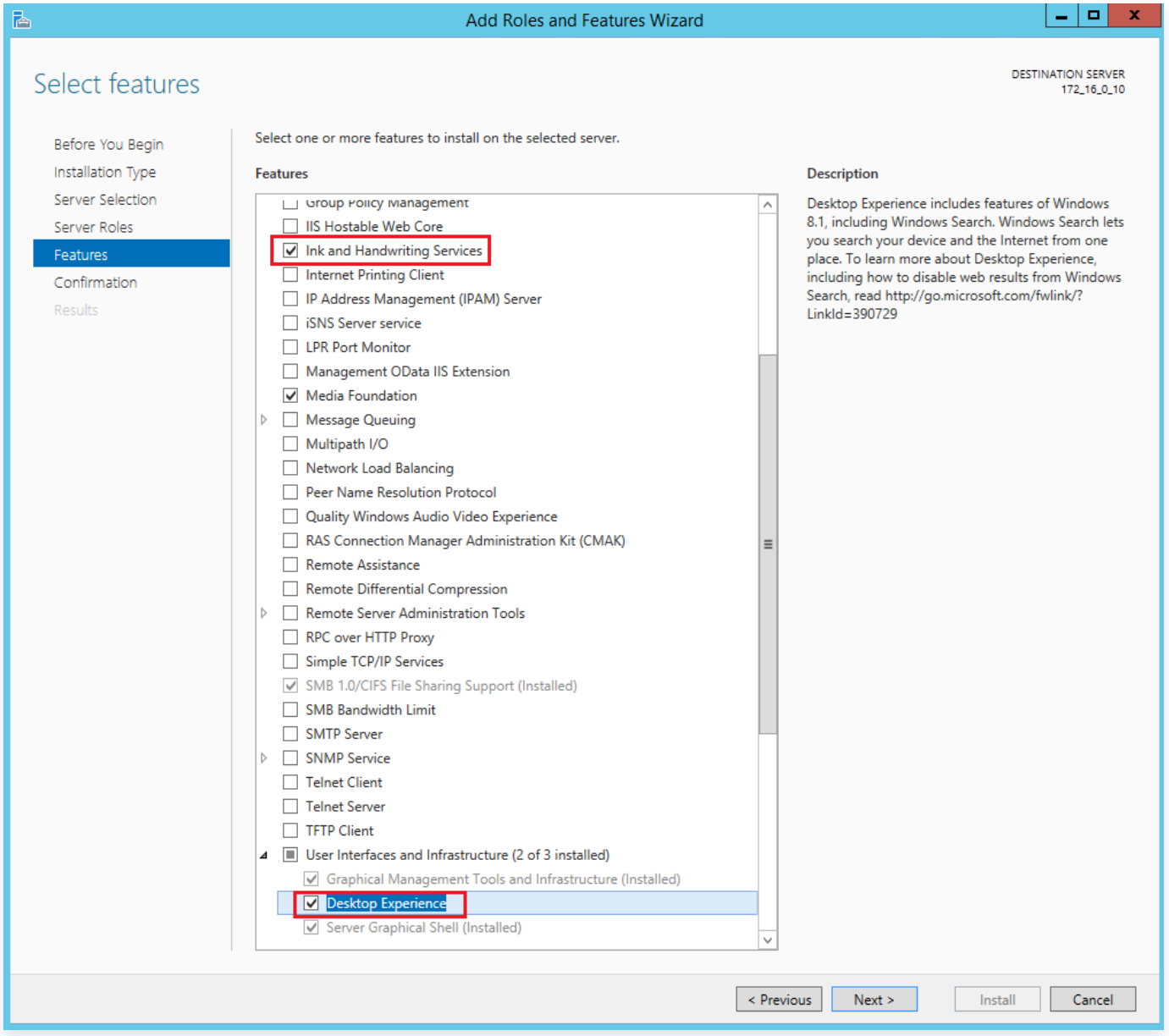
Excluindo arquivos obsoletos

1. Na área de trabalho, clique em para abrir o Server Manager (Gerenciador do servidor).
2. Clique em Add Roles and Features (Adicionar funções e recursos) em Manage (Gerenciar).
3. Na janela pop-up, clique em Next (Avançar).
4. Selecione Role-based or feature-based installation (Instalação baseada em função ou recurso) e clique em Next (Avançar) duas vezes, conforme mostrado abaixo:

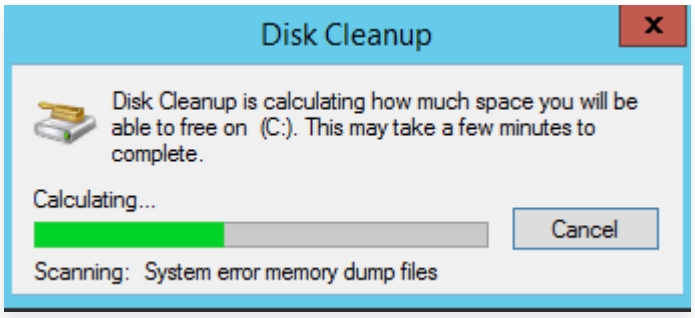


5. Na página Select features (Selecionar recursos), marque Ink and Handwriting Services (Serviços de tinta e manuscrito) e Desktop Experience (Experiência de área de trabalho), conforme mostrado

abaixo. Clique em OK na caixa de diálogo pop-up.



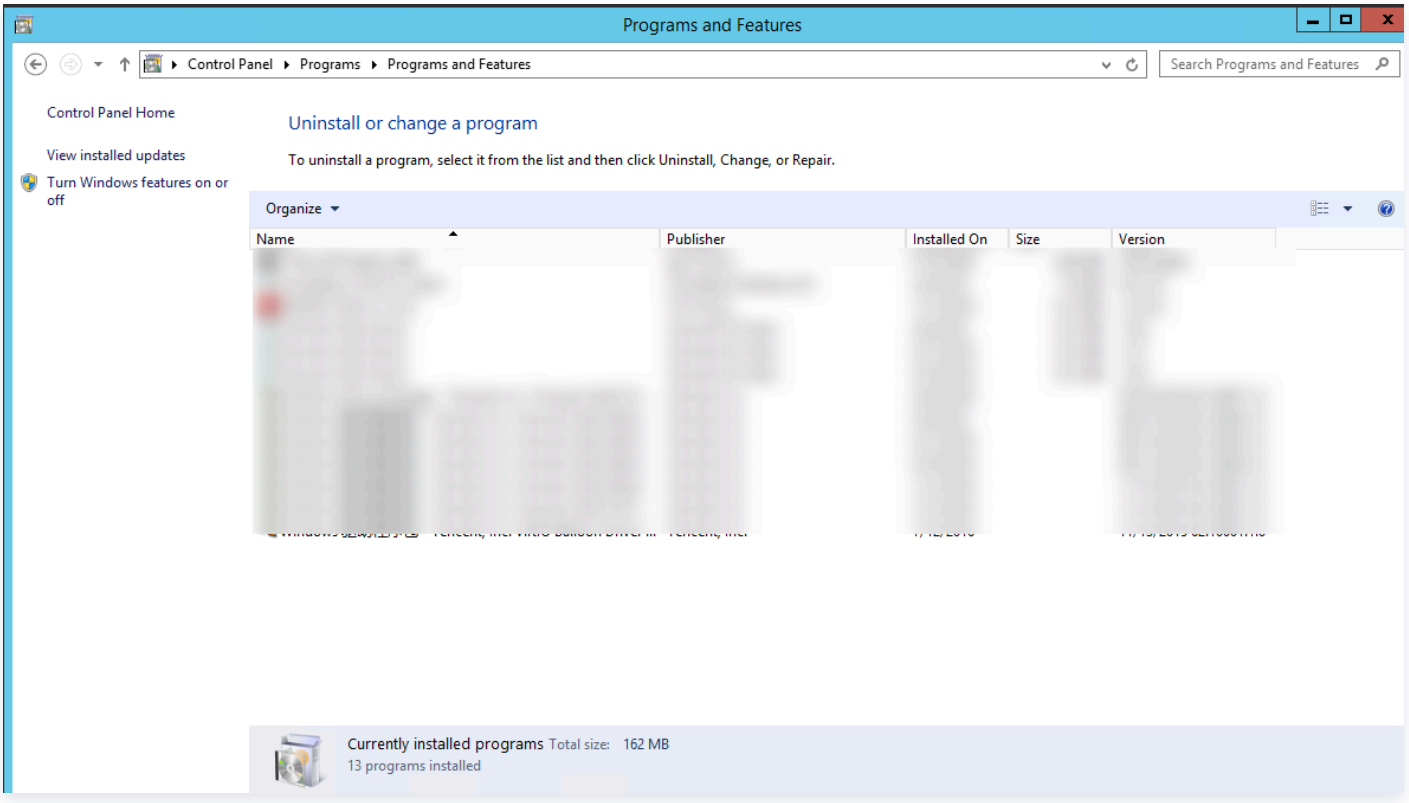
6. Clique em Next (Avançar) e em Install (Instalar). Aguarde a conclusão da instalação e reinicie o CVM quando solicitado.
7. Selecione e clique em no canto superior direito. Digite Disk Management (Gerenciamento de disco) e pesquise.
8. Na janela pop-up Disk Cleanup (Limpeza de disco), selecione o disco de destino e inicie a limpeza, conforme mostrado abaixo:



Manutenção de rotina do disco

Remover programas regularmente

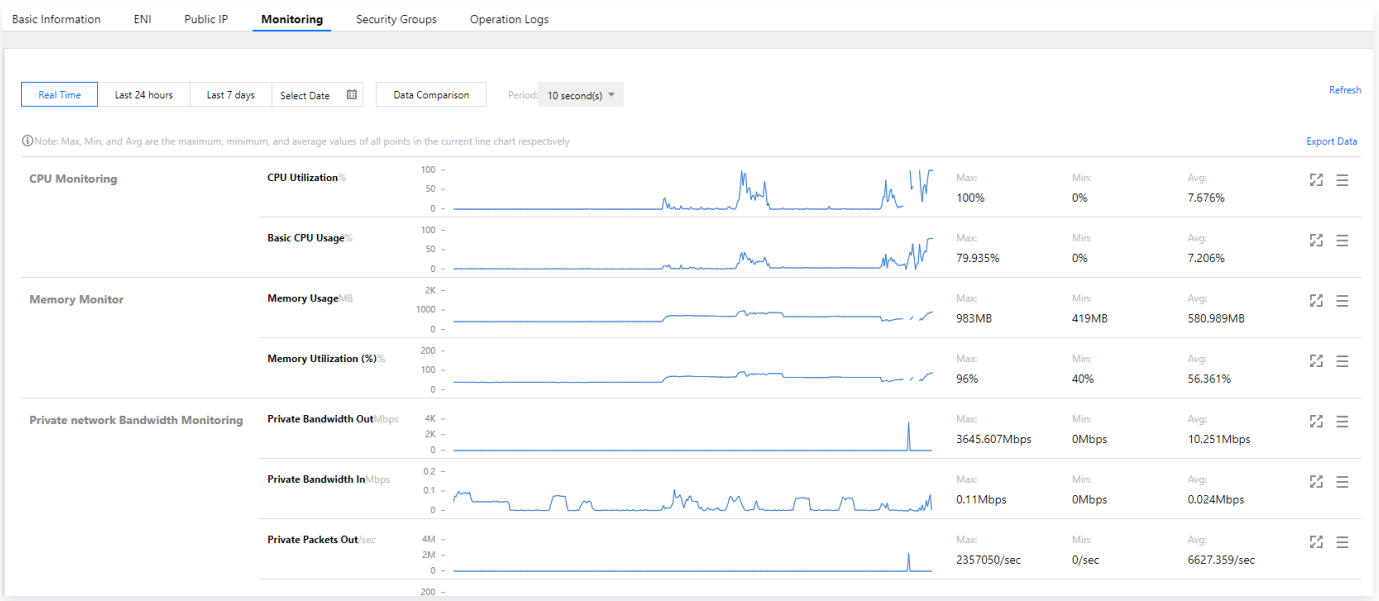
Selecione Control Panel (Painel de controle) –> Programs and Features (Programas e recursos) –> Uninstall or change a program (Desinstalar ou alterar um programa) para remover programas obsoletos regularmente, conforme mostrado abaixo:



Visualizar o uso do disco no console

O recurso Cloud Monitor é ativado automaticamente assim que uma instância CVM é criada. É possível visualizar o uso do disco seguindo as etapas abaixo:

1. Faça login no console do CVM e acesse a página Instances (Instâncias).
2. Selecione o ID/Nome da instância de destino para acessar a página de detalhes.
3. Selecione a guia Monitoring (Monitoramento) para visualizar o uso do disco da instância, conforme mostrado abaixo:



Recuperar os dados de instância Linux

Last updated: 2024-01-23 17:52:21

Visão geral

O Extundelete é uma ferramenta, de código aberto, para recuperação de dados. Com recursos poderosos, suporta a recuperação de partições ext3 e ext4 de arquivos excluídos acidentalmente de disco de dados, desde que o disco não seja gravado após o acidente. Este documento descreve como usar o Extundelete para recuperar rapidamente os dados excluídos acidentalmente em um Tencent Cloud CVM CentOS 7.7. O Tencent Cloud também oferece instantâneos, imagens personalizadas e Armazenamento de objetos em nuvem para armazenar dados. Recomendamos que você faça backups regulares dos dados para aumentar a segurança dos dados.

Software

- Linux: Sistema operacional Linux. Este documento usa a versão CentOS 7.7 como exemplo.
- Extundelete: ferramenta, de código aberto, para recuperação de dados. Este documento usa o Extundelete 0.2.4 como exemplo.

Instruções

> ⚠ Atenção:
> Consulte Criação de instantâneos e Criação de imagens personalizadas para fazer backup dos dados antes de realizar as operações, de forma que você possa recuperar a instância para o status inicial se ocorrer um problema.

Instalação do Extundelete

1. Execute o seguinte comando para instalar as dependências e bibliotecas do Extundelete.

   > ⚠ Atenção:
   > - O Extundelete requer o libext2fs versão 1.39 ou posterior.
   > - Para suportar o formato ext4, instale o e1fsprogs versão 1.41 ou posterior. É possível usar o comando `dumpe2fs` para visualizar a versão.

   ```
   yum -y install bzip2 e2fsprogs-devel e2fsprogs gcc-c++ make
   ```

2. Faça download do pacote de instalação do Extundelete.

3. Execute os comandos a seguir em sequência para descompactar o pacote de instalação Extundelete e acessar o diretório.

```
tar -xvjf extundelete-0.2.4.tar.bz2
```

```
cd extundelete-0.2.4
```

4. Execute os seguintes comandos em sequência para compilar e instalar o Extundelete.

```
./configure
```

```
make && make install
```

Após a conclusão da instalação, você poderá ver o arquivo executável "extundelete" no diretório `usr/local/bin` .

Testando a recuperação de dados

Recupere os dados conforme necessário, executando as etapas a seguir.

1. Inicialize e particione o disco de dados consultando Inicialização de discos em nuvem (menores que 2 TB). Execute o seguinte comando para visualizar os discos existentes e as partições disponíveis.

```
fdisk -l
```

As seguintes informações serão exibidas:

```
[root@VM-0-23-centos ~]# fdisk -l

Disk /dev/vda: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0009ac89

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048    20971486    10484719+  83  Linux

Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xc6ffb1c1

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1   *        2048    20971519    10484736   83  Linux
```

2. Execute os seguintes comandos em sequência para criar um ponto de montagem e montar a partição. Este documento usa a montagem da partição `/dev/vdb1` para `/test` como exemplo.

```
mkdir /test
```

```
mount /dev/vdb1 /test
```

3. Execute os seguintes comandos em sequência para criar o arquivo de teste "hello" no ponto de montagem.

```
cd /test
```

```
echo test > hello
```

4. Execute o seguinte comando para registrar o valor MD5 do arquivo "hello". Este valor pode ser usado para comparar os arquivos originais e recuperados.

```
md5sum hello
```

As seguintes informações serão exibidas:

```
[root@VM-0-23-centos test]# md5sum hello
d8e8fca2dc[illegible]cb4cb0031ba249  hello
```

5. Execute os seguintes comandos em sequência para excluir o arquivo "hello".

```
rm -rf hello
```

```
cd ~
```

```
fuser -k /test
```

6. Execute o seguinte comando para desmontar a partição.

```
umount /dev/vdb1
```

7. Execute o seguinte comando para pesquisar a partição em busca de arquivos excluídos acidentalmente.

```
extundelete --inode 2 /dev/vdb1
```

As seguintes informações serão exibidas:

```
Direct blocks: 127754, 4, 0, 0, 1, 9251, 0, 0, 0, 0, 0, 0
Indirect block: 0
Double indirect block: 0
Triple indirect block: 0

File name                                       | Inode number | Deleted status
.                                                 2
..                                                2
lost+found                                        11
WTEST.TMP                                         12             Deleted
```

8. Execute o seguinte comando para usar o Extundelete para recuperar o arquivo.

```
/usr/local/bin/extundelete  --restore-inode 12  /dev/vdb1
```

Depois que o arquivo for recuperado, você verá a pasta `RECOVERED_FILES` no diretório de mesmo nível.

9. Acesse a pasta `RECOVERED_FILES`, verifique o arquivo recuperado e execute o seguinte comando para obter o valor MD5.

```
md5sum Recovered file
```

Se o valor MD5 obtido for o mesmo do arquivo "hello" gravado na Etapa 4, os dados foram recuperados com sucesso.

Usar USB/IP para compartilhar dispositivos USB remotamente no sistema Linux

Last updated：2024-01-23 17:52:21

Visão geral

O USB/IP é um projeto de código aberto e foi incorporado ao kernel. Em um ambiente Linux, você pode usar o USB/IP para compartilhar dispositivos USB remotamente. Este documento usa as seguintes versões de ambiente como exemplos para descrever como usar o USB/IP para compartilhar dispositivos USB.
Cliente USB: CVM com CentOS 7.6
Servidor USB: PC local com Debian

Observações

O método de instalação do USB/IP e o nome do módulo do kernel variam de acordo com as versões do sistema operacional Linux. Acesse as versões oficiais do Linux e verifique se o seu sistema operacional Linux atual é compatível com o recurso USB/IP.

Instruções

Configuração do servidor USB

1. No PC local, execute os seguintes comandos em sequência para instalar o USB/IP e carregar módulos de kernel relacionados:

```
sudo apt-get install usbip
sudo modprobe usbip-core
sudo modprobe vhci-hcd
sudo modprobe usbip_host
```

2. Insira um dispositivo USB e execute o seguinte comando para visualizar os dispositivos USB disponíveis:

```
usbip list --local
```

Por exemplo, se uma chave USB Feitian for inserida no PC local, o seguinte resultado será retornado:

```
busid 1-1.3(096e:031b)
Feitian Technologies, Inc.: unknown product(096e:031b)
```

3. Registre o valor busid e execute os seguintes comandos em sequência para habilitar a escuta, especifique a porta USB/IP e compartilhe o dispositivo USB:

```
sudo usbipd -D [--tcp-port PORT]
sudo usbip bind -b [busid]
```

Por exemplo, se a porta USB/IP especificada for a porta 3240 (porta USB/IP padrão) e busid for `1-1.3`, execute os seguintes comandos:

```
sudo usbipd -D
sudo usbip bind -b 1-1.3
```

(Opcional) 4. Execute o seguinte comando para criar um túnel SSH e usar a escuta da porta:

> **Nota:**
> Pule esta etapa se o PC local tiver um endereço IP público.

```
ssh -Nf -R specified USB/IP port:localhost:specified USB/IP port
root@your_host
```

`your_host` indica o endereço IP do CVM.
Por exemplo, se a porta USB/IP for a porta 3240 e o endereço IP do CVM for 192.168.15.24, execute o seguinte comando:

```
ssh -Nf -R 3240:localhost:3240 root@192.168.15.24
```

Configuração do cliente USB

> **Nota:**
> O seguinte usa um PC local sem um IP público como exemplo. Se o seu PC local tiver um IP público, substitua `127.0.0.1` nas etapas a seguir pelo IP público do seu PC local.

1. Faça login em uma instância do Linux.

2. Execute os seguintes comandos em sequência para fazer download da origem do USB/IP:

```
rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org
rpm -ivh http://www.elrepo.org/elrepo-release-7.0-
3.el7.elrepo.noarch.rpm
```

3. Execute os seguintes comandos em sequência para instalar o USB/IP:

```
yum -y install kmod-usbip usbip-utils
modprobe usbip-core
modprobe vhci-hcd
modprobe usbip-host
```

4. Execute o seguinte comando para consultar os dispositivos USB disponíveis do CVM:

```
 usbip list --remote 127.0.0.1
```

Por exemplo, se as informações da chave USB Feitian forem localizadas, o seguinte resultado será retornado:

```
 Dispositivos USB exportáveis
 ======================
 -127.0.0.1 1-1.3: Feitian Technologies, Inc.: unknown
product(096e:031b):/sys/devices/platform/scb/fd500000.pcie/pci0000:00/
0000:00:00.0/0000:01:00.0/usb1/1-1/1-1.3:(Defined at Interface level)
(00/00/00)
```

5. Execute o seguinte comando para vincular o dispositivo USB ao CVM:

```
 usbip attach --remote=127.0.0.1 --busid=1-1.3
```

6. Execute o seguinte comando para consultar a lista de dispositivos USB:

```
 lsusb
```

Se informações semelhantes às seguintes forem retornadas, o dispositivo USB foi compartilhado.

```
 Bus 002 Device 002:ID096e:031b Feitian Technologies, Inc.
```

```
Bus 002 Device 001:ID1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 001:ID1d6b:0001 Linux Foundation 1.1 root hub
```

Usar RemoteFx para redirecionar dispositivo USB no sistema Windows

Last updated：2024-01-23 17:52:21

Cenário

O RemoteFx é uma versão atualizada do Windows Remote Desktop Protocol (RDP). A partir do RDP 8.0, o RemoteFx pode ser usado para redirecionar dispositivos USB locais para uma área de trabalho remota por meio do canal de dados RDP, garantindo que o CVM possa usar esses dispositivos USB.
Este documento usa as seguintes versões de ambiente como exemplos para descrever como habilitar o recurso de redirecionamento RemoteFx USB do RDP para redirecionar dispositivos USB para um CVM.

- Cliente: Windows 10
- Servidor: Windows Server 2016

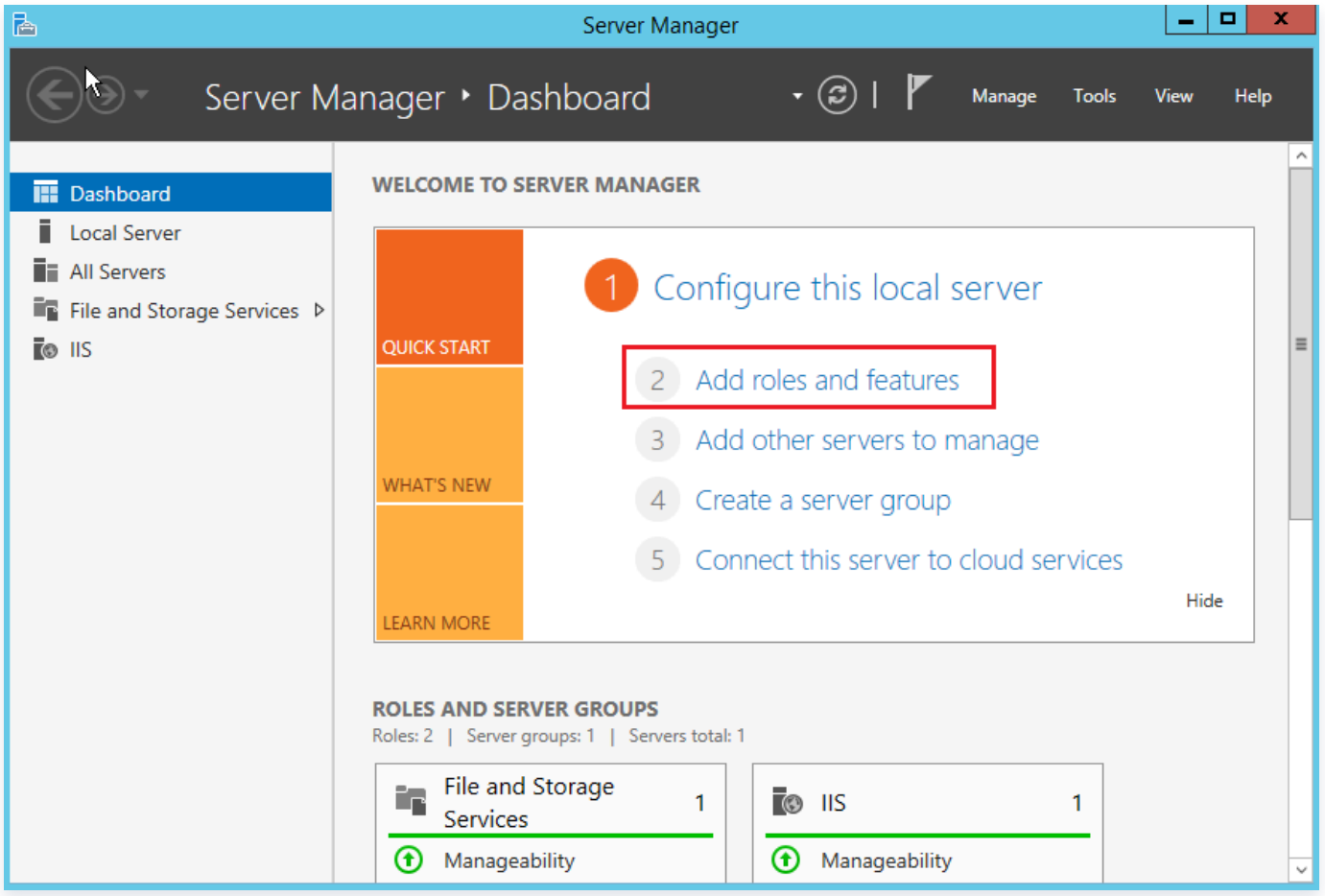
Limites de uso

Como o RDP 8.0 e versões posteriores oferecem suporte ao recurso de redirecionamento RemoteFx USB, o Windows 8, Windows 10, Windows Server 2016 e Windows Server 2019 oferecem suporte a esse recurso. Se o sistema operacional do seu PC local tiver uma dessas versões, você não precisa instalar o patch de atualização RDP 8.0. Se o seu PC local tiver Windows 7 ou Windows Vista, acesse site oficial da Microsoft para obter e instalar o patch de atualização do RDP 8.0.

Instruções

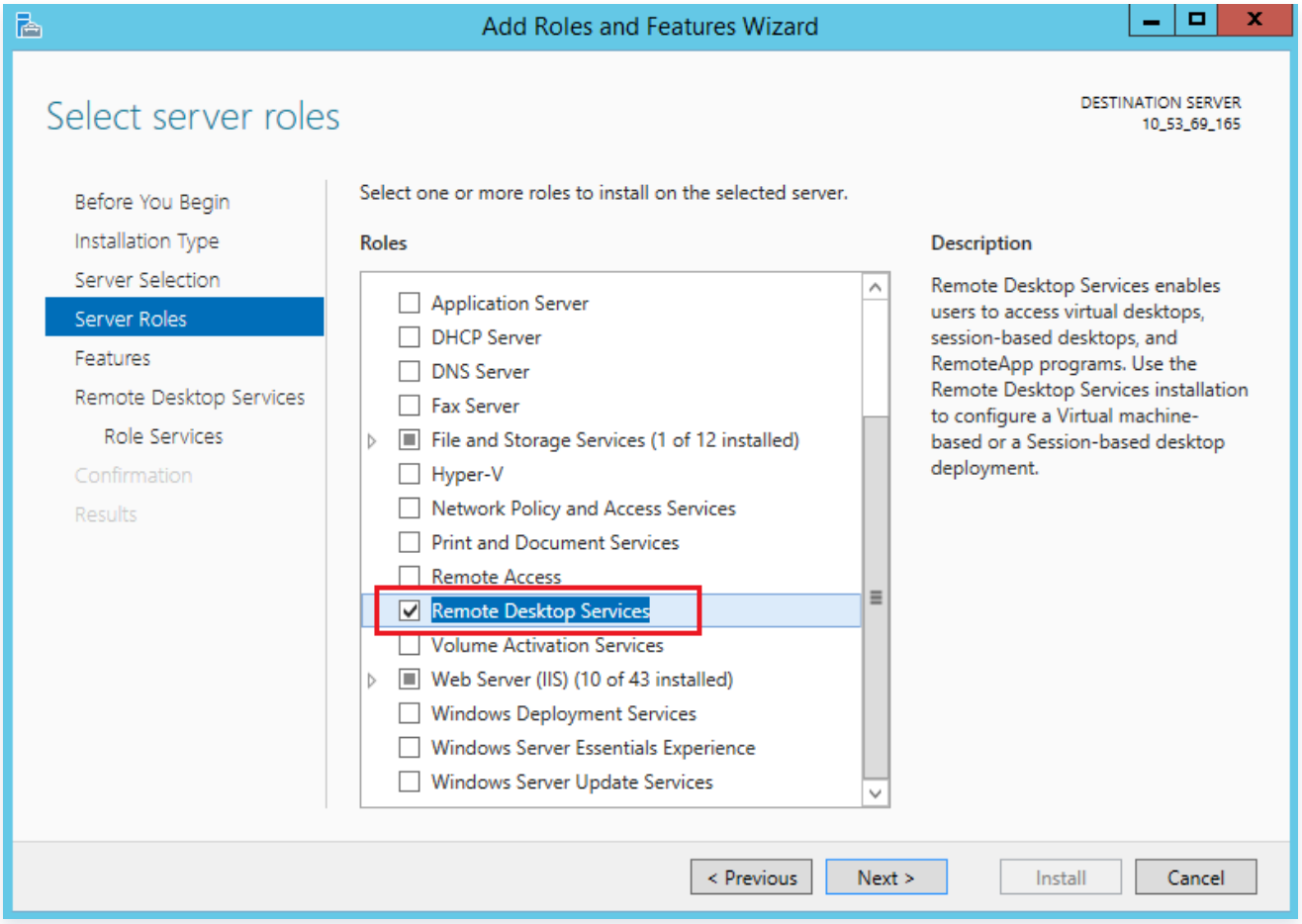
Configuração do servidor

1. Fazer login em uma instância do Windows usando o arquivo RDP (recomendado).
2. Na área de trabalho, clique em  e selecione Server Manager (Gerenciador do servidor) para abrir o Gerenciador do servidor.
3. Na janela "Server Manager (Gerenciador do servidor)", clique em Add roles and features (Adicionar funções e recursos), conforme mostrado na figura a seguir:



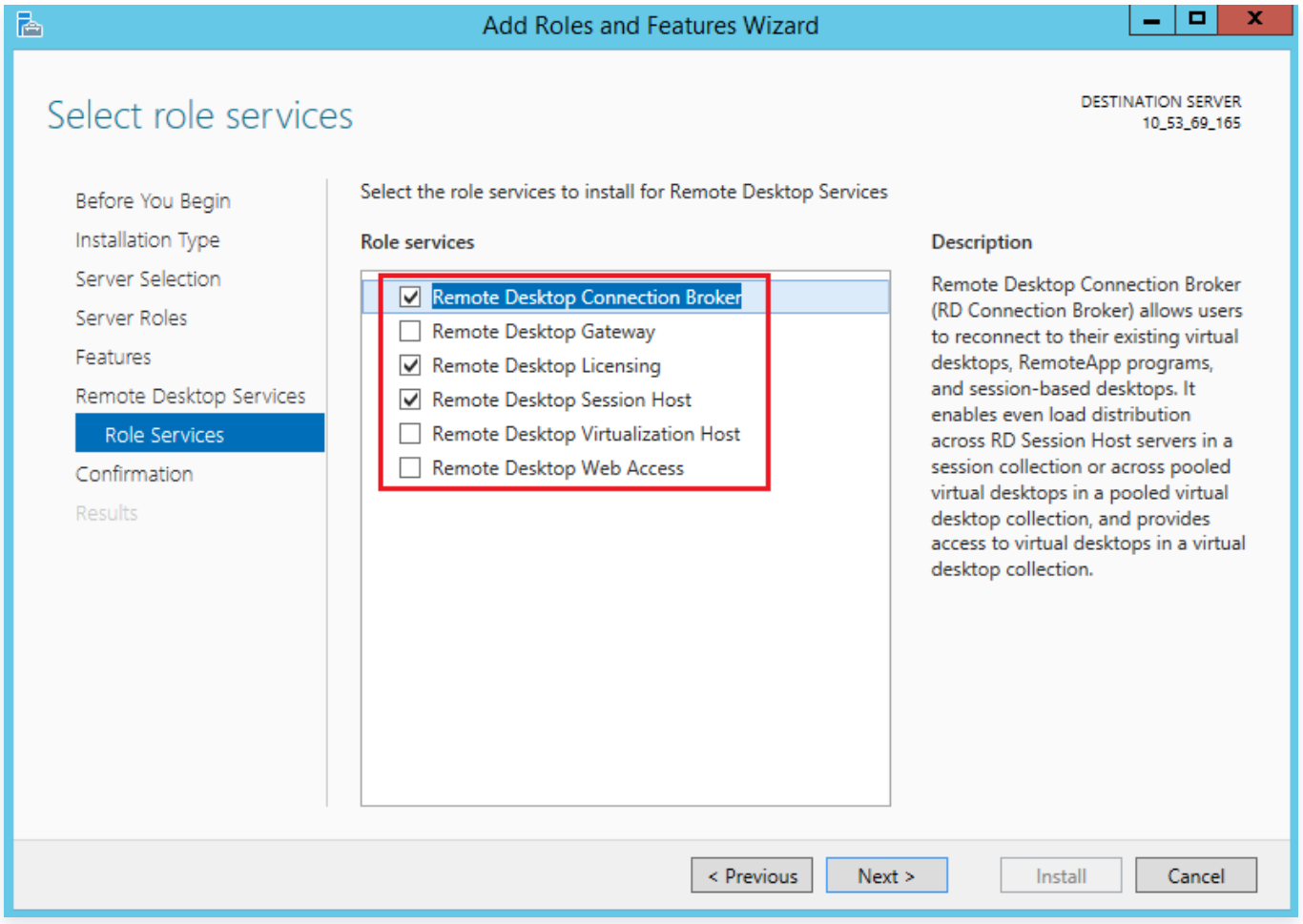
4. Na janela pop-up "Add Roles and Features Wizard (Assistente para adicionar funções e recursos)", clique em Next (Avançar) para ir para a página "Select installation type (Selecionar tipo de instalação)".
5. Na página "Select installation type (Selecionar tipo de instalação)", selecione Role-based or feature-based installation (Instalação baseada em funções ou recursos) e clique em Next (Avançar).
6. Na página "Select destination server (Selecionar servidor de destino)", mantenha as configurações padrão e clique em Next (Avançar).
7. Na página "Select server roles (Selecionar funções de servidor)", selecione Remote Desktop Services (Serviços de área de trabalho remota) e clique em Next (Avançar), conforme mostrado na figura a

seguir:



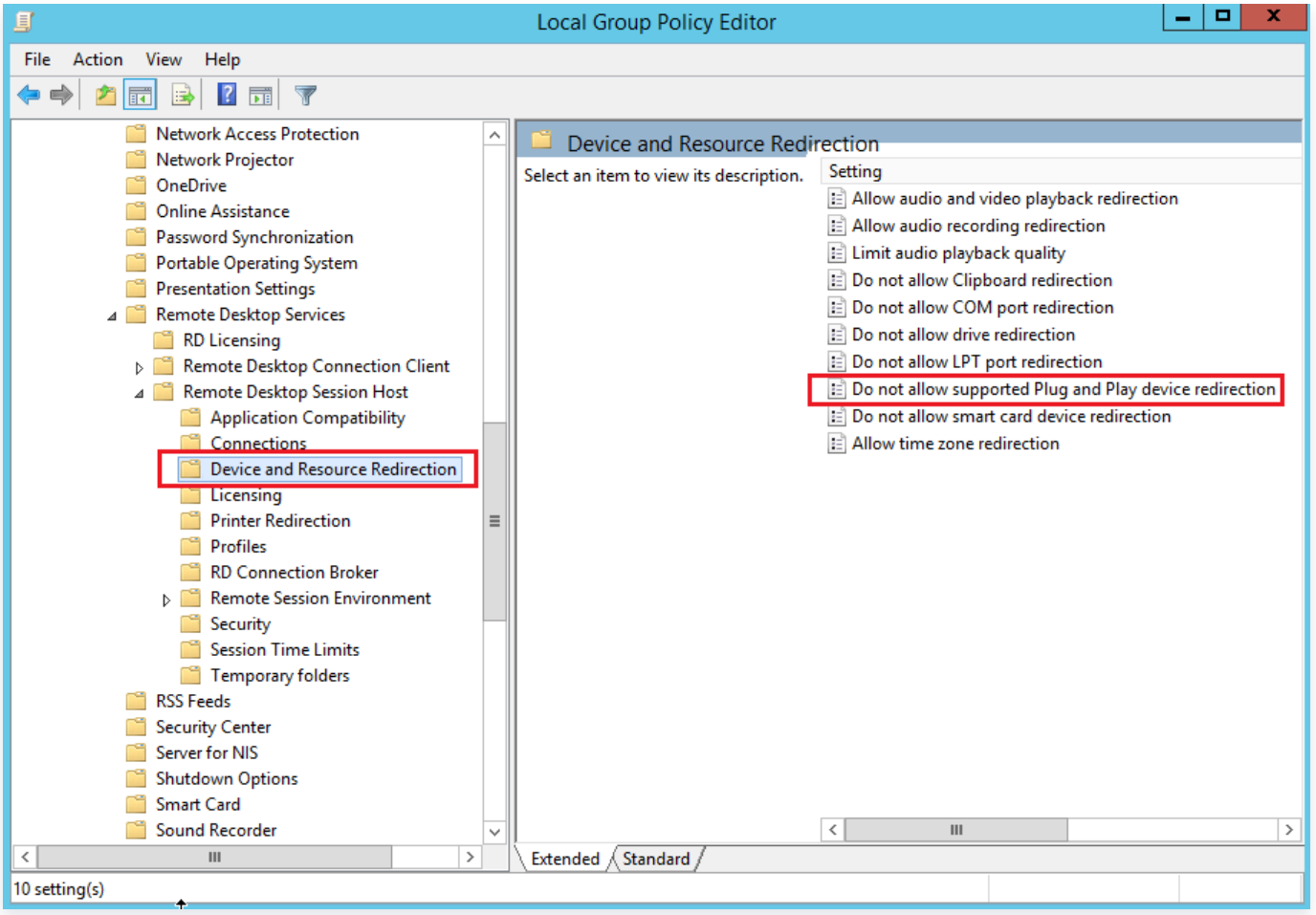
8. Mantenha as configurações padrão e clique em Next (Avançar) por 2 vezes.
9. Na página "Select role services (Selecionar serviços de função)", selecione Remote Desktop Session Host (Host de sessão de área de trabalho remota), Remote Desktop Connection Broker (Agente de conexão de área de trabalho remota) e Remote Desktop Licensing (Licenciamento de área de trabalho remota). Na janela pop-up, clique em Add Features (Adicionar recursos), conforme mostrado na figura

a seguir:

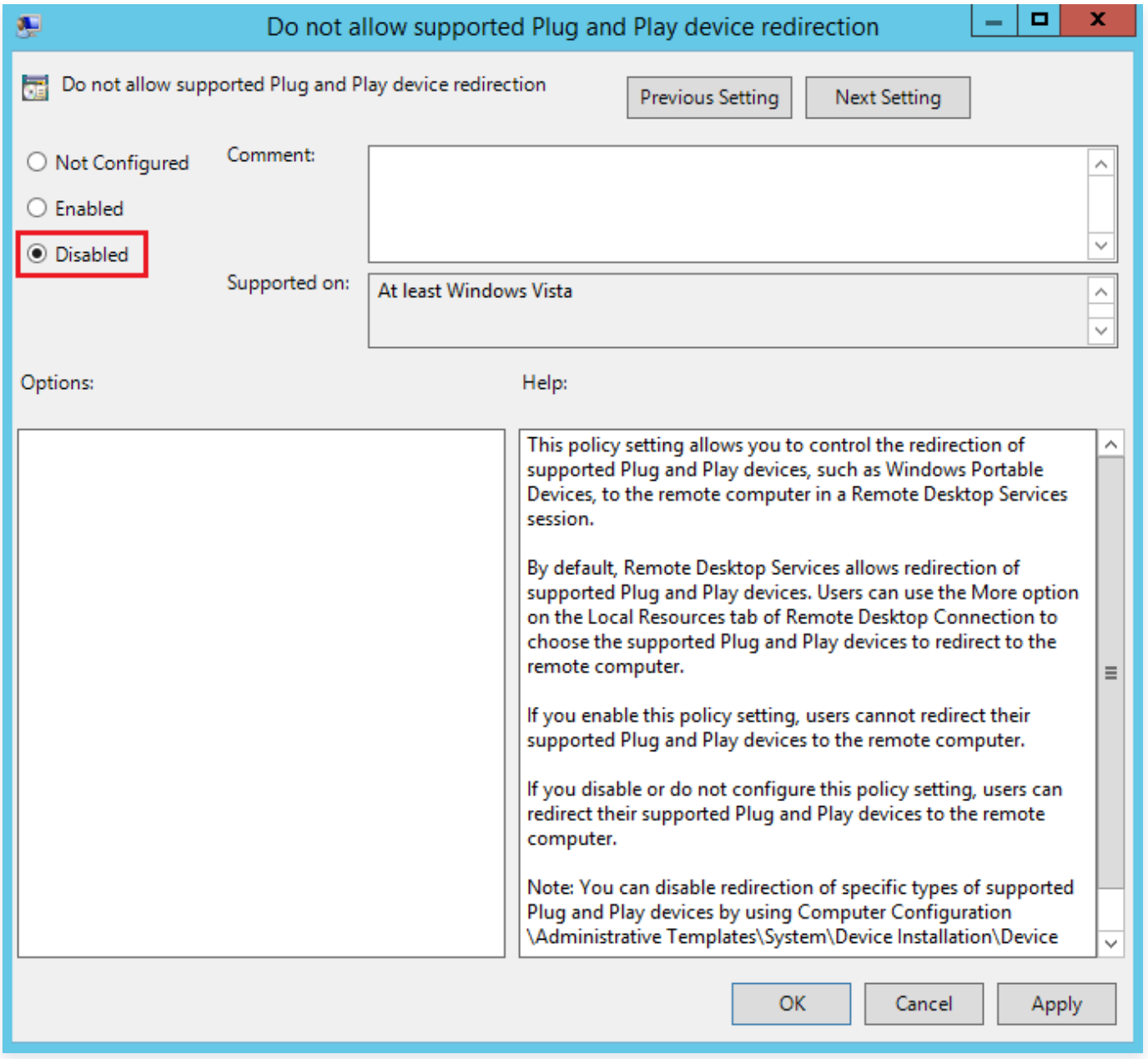


10. Clique em Next (Avançar).
11. Clique em Install (Instalar).
12. Após a instalação ser concluída, reinicie o CVM.
13. Na área de trabalho, clique em  , digite gpedit.msc e pressione Enter para abrir o "Local Group Polzhicy (Editor de política de grupo local)".
14. Na árvore de navegação à esquerda, escolha Computer Configuration (Configuração do computador) > Administrative Templates (Modelos administrativos) > Windows Components (Componentes do Windows) > Remote Desktop Services (Serviços de área de trabalho remota) > Remote Desktop Session Host (Host de sessão de área de trabalho remota) > Device and Resource Redirection (Redirecionamento de dispositivo e recurso) e clique duas vezes em Do not allow supported Plug and Play device redirection (Não permitir redirecionamento de dispositivo Plug and Play compatível),

conforme mostrado na figura a seguir:



15. Na janela pop-up, selecione Disabled (Desativado) e clique em OK, conforme mostrado na figura a seguir:

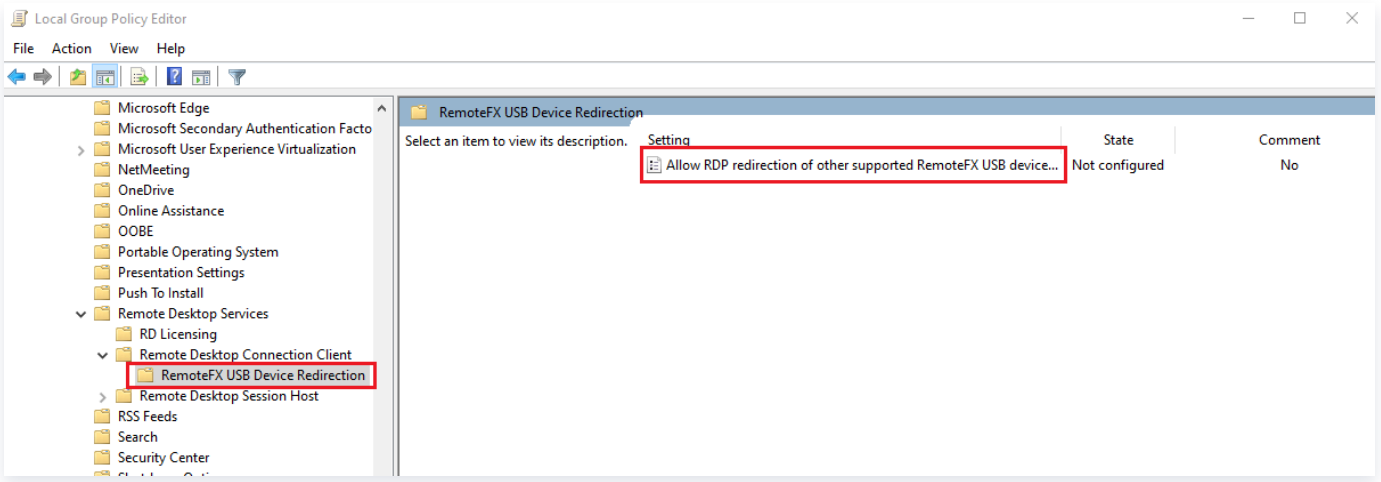


16. Reinicie o CVM.

Configuração do cliente

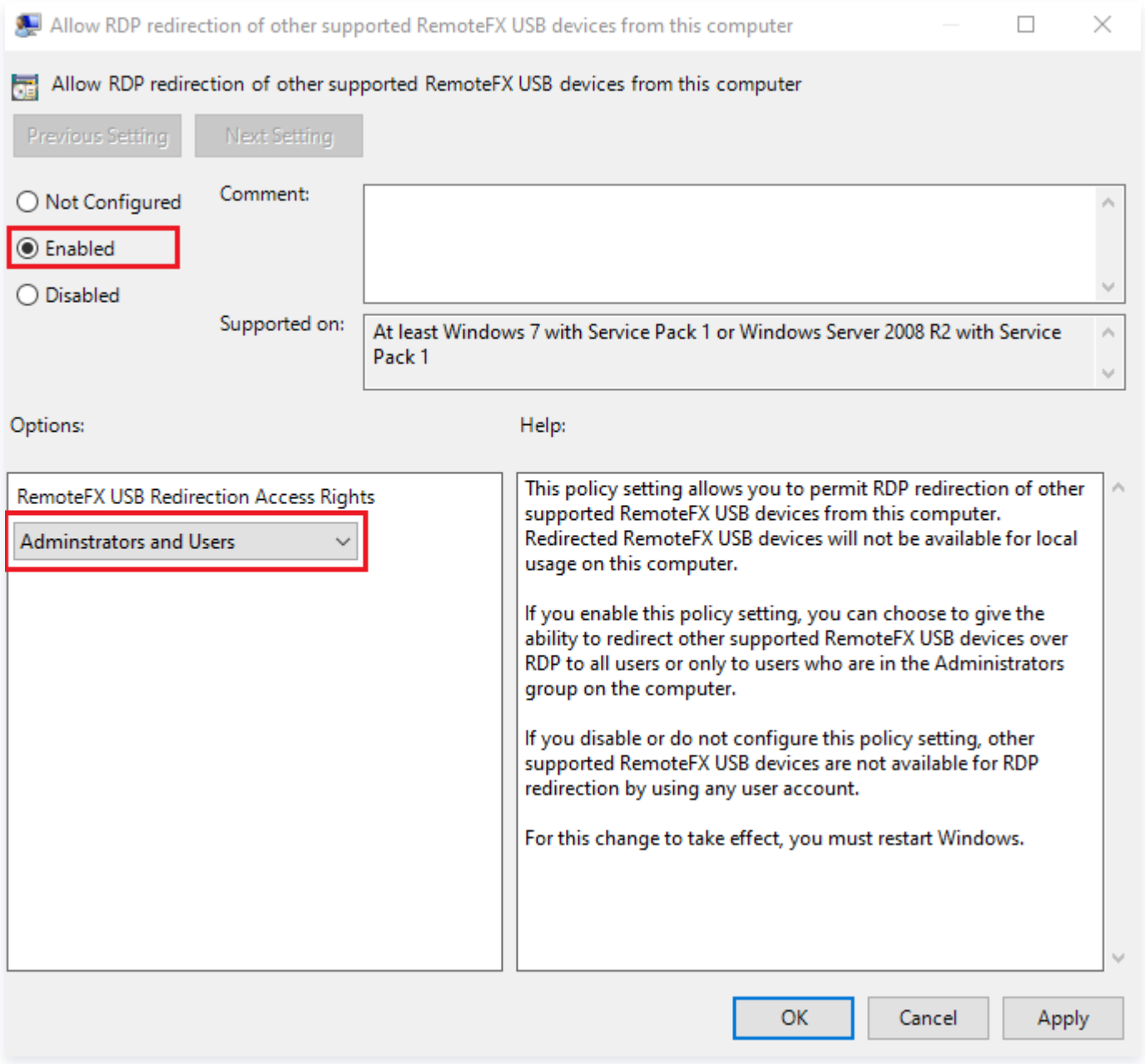
1. No PC local, clique com o botão direito do mouse em e selecione Run (Executar) para abrir a caixa de diálogo "Run (Executar)", conforme mostrado na figura a seguir:
2. Na caixa de diálogo "Run (Executar)", digite gpedit.msc e clique em OK para abrir o "Local Group Policy Editor (Editor de política de grupo local)".
3. Na árvore de navegação à esquerda, escolha Computer Configuration (Configuração do computador) > Administrative Templates (Modelos administrativos) > Windows Components (Componentes do Windows) > Remote Desktop Services (Serviços de área de trabalho remota) > Remote Desktop Connection Client (Cliente de conexão de área de trabalho remota) > RemoteFX USB Redirection

(Redirecionamento RemoteFx USB) e clique duas vezes em Allow RDP redirection of other supported RemoteFX USB devices (Permitir redirecionamento de RDP de outros dispositivos compatíveis com RemoteFx USB), conforme mostrado na figura a seguir:



4. Na janela pop-up, selecione Enabled (Ativado) e defina a permissão de acesso de redirecionamento RemoteFx USB para Administrators and Users (Administradores e usuários), conforme mostrado na

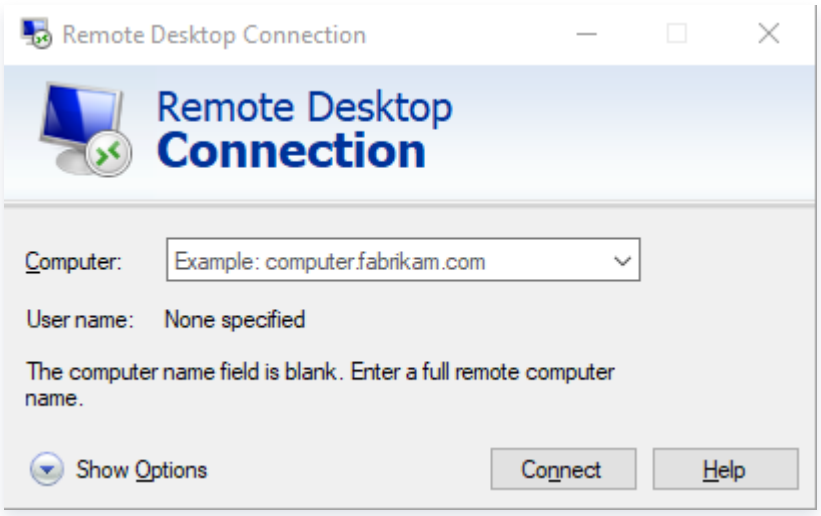
figura a seguir:



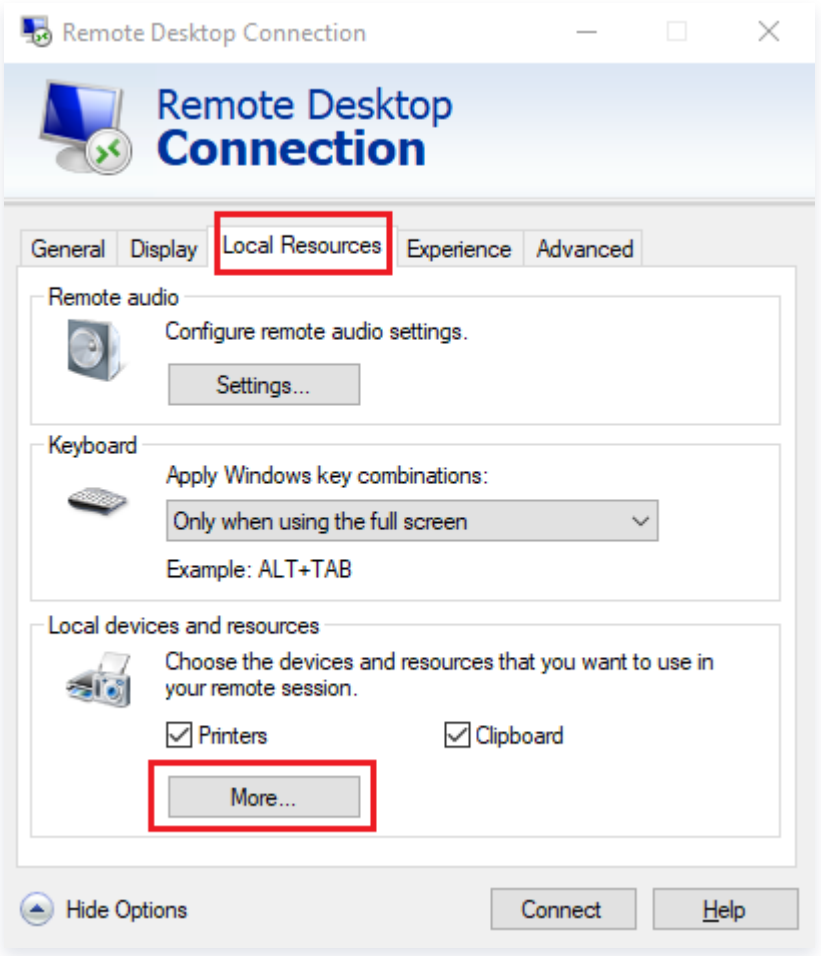
5. Clique em OK.
6. Reinicie o PC local.

Verificação do resultado da configuração

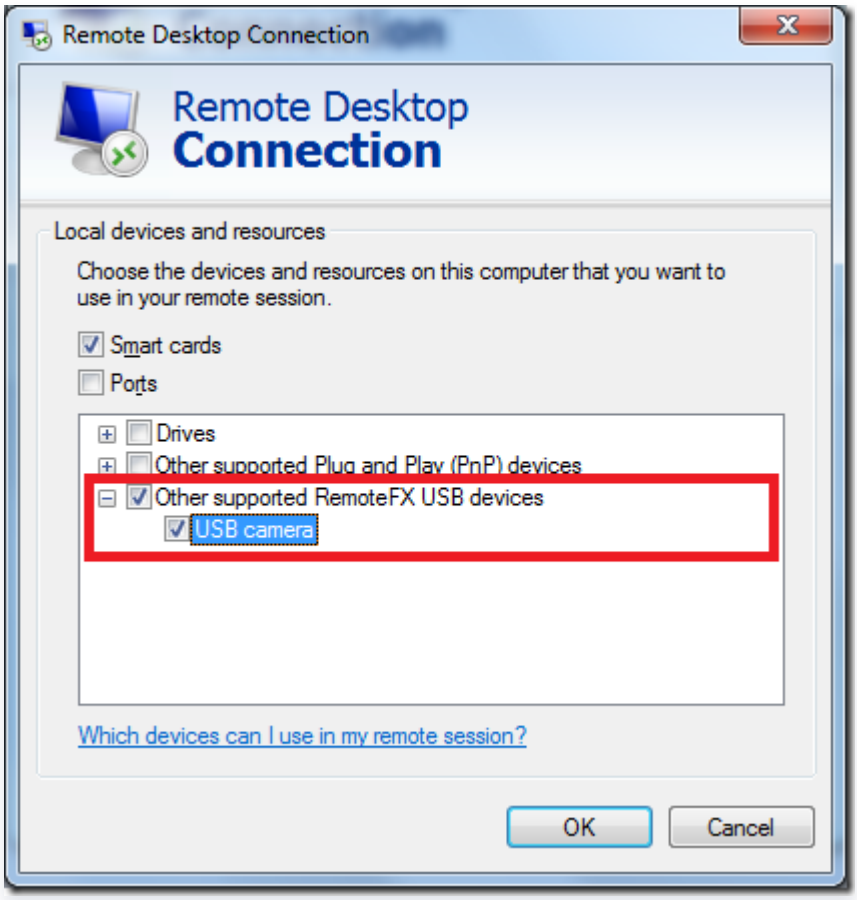
1. Em seu PC local, insira um dispositivo USB, clique com o botão direito do mouse em  e escolha Run (Executar) para abrir a caixa de diálogo "Run (Executar)".
2. Na caixa de diálogo "Run (Executar)", digite mstsc e pressione Enter para abrir a caixa de diálogo de conexão de área de trabalho remota, conforme mostrado na figura a seguir:



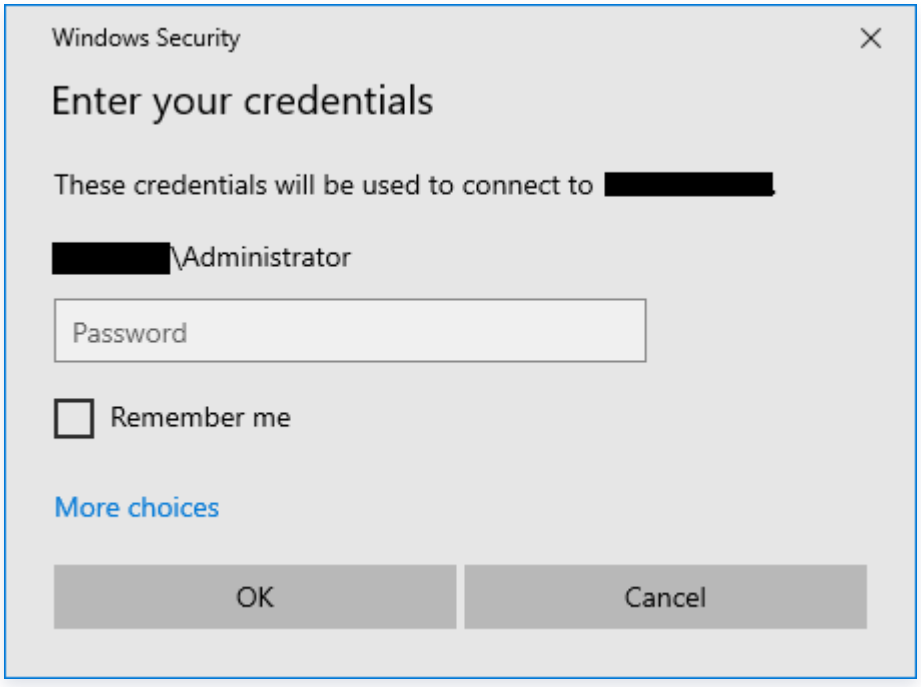
3. Digite o endereço IP público do servidor Windows em Computer (Computador) e clique em Options (Opções).
4. Na página da guia Local Resources (Recursos locais), clique em More (Mais) em "Local devices and resouces (Dispositivos e recursos locais)", conforme mostrado na figura a seguir:



5. Na janela pop-up, expanda Other supported RemoteFx USB devices (Outros dispositivos compatíveis com RemoteFx USB), selecione o dispositivo USB inserido e clique em OK.

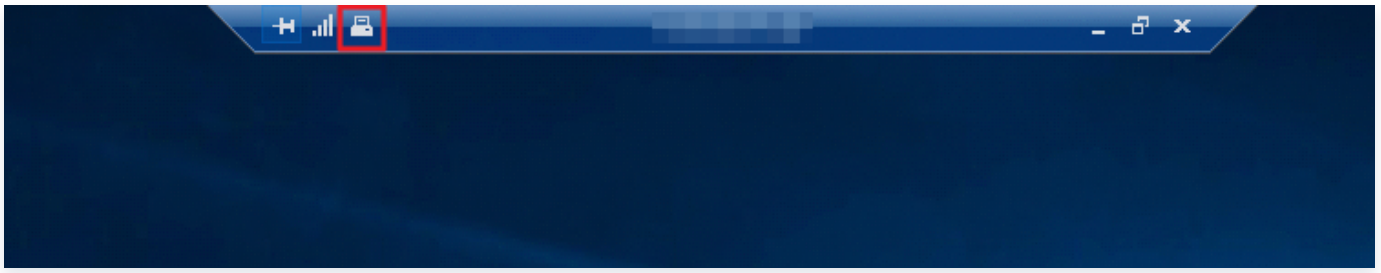


6. Clique em Connect (Conectar).
7. Na janela pop-up Windows Security (Segurança do Windows), insira a conta de administrador e a senha da instância, conforme mostrado na figura a seguir:



8. Clique em OK para fazer login na instância do Windows.

   Se aparecer na página de operação da instância do Windows, a configuração foi bem-sucedida.



Operações relevantes

O RDP do Windows fornece conexão otimizada para dispositivos USB padrão. Dispositivos como drivers e câmeras podem ser mapeados diretamente sem habilitar o recurso RemoteFx. O recurso de redirecionamento RemoteFX USB é necessário para dispositivos USB menos usados. A tabela a seguir lista os métodos de redirecionamento para esses dispositivos USB.

Device	Support Status	Redirection Method
All-in-One Printer	Supported	RemoteFX USB Redirection
Printer	Supported	Easy Print
Scanner	Supported	RemoteFX USB Redirection
Biometric	Supported while in session *Not supported during logon*	RemoteFX USB Redirection
PTP Camera	Supported	Plug and Play Device Redirection
MTP Media Player	Supported	Plug and Play Device Redirection
Webcam	Supported (LAN only)	RemoteFX USB Redirection
VoIP Telephone/Headset	Supported (LAN only)	RemoteFX USB Redirection
Audio (not a USB composite device)	Supported	Audio Redirection
CD or DVD Drive	Supported for read operations	Drive Redirection
Hard Drive or USB Flash Drive	Supported	Drive Redirection
Smart Card Reader	Supported	Smart Card Redirection
USB-to-Serial	Supported	RemoteFX USB Redirection
USB Network Adapter (also includes some personal digital assistants)	Blocked	N/A
USB Display	Blocked	N/A
USB Keyboard or Mouse	Supported	Input Redirection