



MANUAL DE CONFIGURAÇÃO DO CONECTA

Requisitos para implementar em novos ambientes

SUMÁRIO

1 OBJETIVO	3
2 CONECTA	3
2.1 Formas de comunicação	4
2.2 Protocolos	4
2.2.1 Connect:Direct	4
2.2.2 Parâmetros para Configuração	4
2.3 Envio e recebimento de Arquivos	6
2.3.1 SFTP/SSH	6
2.3.2 Diretórios Disponíveis no SFTP e Regras de Utilização	8
2.3.3 Parâmetros para configuração	9
3 PROCESSOS ADICIONAIS	14
3.1 Ativação, substituição e revogação de certificados e chaves	14
3.2 Processo de envio de malote individualizado	15
3.3 Procedimentos para Testes de Conexão FileZilla	16
4 CONTATOS NA B3	21

1 OBJETIVO

Este manual visa apresentar de forma clara e detalhada os requisitos técnicos essenciais para a implementação do Conecta na plataforma NoMe, proporcionando orientações práticas que garantam uma troca eficiente e automatizada de arquivos entre os clientes e a B3.

O objetivo é facilitar a compreensão dos processos, limites e boas práticas relacionadas ao envio e recebimento de arquivos, assegurando que todas as partes envolvidas possam operar de maneira otimizada e dentro das normas estabelecidas.

2 CONECTA

1. O que é o Conecta?

O Conecta é uma ferramenta que permite a troca automática de arquivos entre os clientes e a B3, uma importante instituição financeira. Ele está integrado ao sistema NoMe, que é utilizado para operações no mercado de balcão.

2. Como Funciona o Conecta?

O Conecta opera 24 horas por dia. No entanto, se um cliente enviar arquivos enquanto o sistema estiver fechado para transferência, esses arquivos ficarão em espera até que o sistema reabra para o próximo processamento. Isso significa que o envio de arquivos deve ser feito dentro dos horários definidos (horário da grade) para garantir que sejam processados rapidamente.

3. Para quem o conecta é ideal?

O Conecta foi desenvolvido para otimizar o processamento de arquivos que contêm um grande número de registros simultaneamente. Isso significa que o sistema opera de forma mais eficiente quando os clientes consolidam suas informações em um único arquivo de maior volume, em vez de enviar múltiplos arquivos pequenos. Embora o Conecta também consiga processar arquivos menores normalmente, é altamente recomendável que os clientes organizem seus dados de forma a maximizar a quantidade de informações contidas em cada arquivo, respeitando o limite máximo de 150MB para o tamanho dos arquivos enviados. Essa abordagem não apenas melhora a eficiência do processamento, mas também facilita a gestão dos dados.

4. Limitações de Nomenclatura de Arquivos

O sistema NoMe, que recebe os arquivos transferidos pelo Conecta, tem um limite para o nome dos arquivos: eles não podem passar de 60 caracteres. Portanto, é muito importante que os clientes verifiquem e ajustem os nomes dos arquivos que desejam enviar para garantir que estejam dentro desse limite. Isso ajudará a evitar problemas durante o processo de transferência.

2.1 Formas de comunicação

Os clientes podem se comunicar com a B3 utilizando duas opções: **RTM ou Internet**.

- **Comunicação via RTM:** Para estabelecer conexões por meio do RTM, é necessário entrar em contato com a equipe responsável para definir a melhor configuração para contingência de rede. Isso deve incluir considerações sobre NAT (Network Address Translation) e a resolução de nomes DNS.
- **Endereços IP:** É recomendável que os clientes utilizem um endereço IP específico para o ambiente de certificação e um segundo endereço IP distinto para os ambientes de Produção e Contingência.
- **Comunicação via Internet:** Se a escolha for pela configuração de conexões via Internet, o cliente deve consultar sua equipe de redes para verificar os endereços IP necessários para entrada e saída nos ambientes.

Importante: É fundamental lembrar que as configurações de RTM e Internet são serviços distintos. Portanto, a decisão sobre qual forma de comunicação utilizar deve ser discutida previamente com a equipe de atendimento (SAT).

2.2 Protocolos

O Conecta permite a transferência de arquivos em duas modalidades:

1. **Conect:Direct**
2. **SFTP**

A escolha entre essas plataformas é de responsabilidade do cliente, que pode optar pela qual melhor atende às suas necessidades.

2.2.1 Conect:Direct

Connect:Direct

- É um protocolo desenvolvido pela IBM que facilita a transferência de arquivos de forma ponto-a-ponto. Este protocolo possui uma arquitetura que permite o envio e recebimento automatizado de arquivos, garantindo segurança e um gerenciamento eficiente, além de possibilitar a interação entre diferentes sistemas operacionais. Para mais informações sobre o software, os usuários podem consultar o site do fabricante: <https://www.ibm.com/>
- Nesse modelo, tanto a B3 quanto o participante atuam como servidores, possibilitando a troca de arquivos entre eles.

2.2.2 Parâmetros para configuração

- A autenticação no sistema é realizada em duas etapas:

- 1) **Primeira Etapa:** Informar o Node, o IP e o usuário.
- 2) **Segunda Etapa:** Validar o certificado digital utilizando o módulo Secure+.

Certificado

A B3 fornecerá um certificado para a autenticação dos clientes no Connect:Direct. É responsabilidade do cliente fornecer o certificado necessário para autenticação em seu próprio sistema. Este certificado deve atender aos seguintes requisitos:

- **Tamanho da chave:** 2048 bits
- **Algoritmo de hash:** SHA 256
- **Tipo:** Certificado SSL para servidor
- **Emissão:** Deve ser emitido por uma Autoridade Certificadora (CA) de raiz confiável.

Importante

Recomenda-se que cada ambiente possua apenas um certificado ativo, garantindo maior clareza no processo de contingência. O certificado utilizado em produção deve ser o mesmo para o ambiente de contingência.

Além disso, é essencial que os certificados utilizados nos ambientes de Homologação e Produção sejam gerados pela mesma certificadora, a fim de assegurar a validade de todo o processo de homologação.

Módulo Secure+

O Módulo Secure+ deve ser configurado para habilitar o protocolo TLS 1.2. É necessário ativar os seguintes padrões de criptografia (Cipher Suites):

- ECDHE_RSA_WITH_AES_256_GCM_SHA384*
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

➤ Conexões

No Connect:Direct, a comunicação é bidirecional, ou seja: Servidor ⇔ Servidor. Serão necessárias liberações no ambiente da B3 e da instituição participante na porta padrão para este protocolo, que está definida pela porta **1364**.

Manual de Configuração do CONECTA

[B]³

O serviço do Connect:Direct está disponível apenas para conexão via RTM

Endereços para Conexão com a B3 via CD

Ambiente	Comunicação	RTM
Homologação	Node	CD_CETIP_HOM
	URL/IP	10.0.48.70
	Porta	1364
	Alternate Comm Info	N/A
	Usuário	cetipcd
Produção	NODE	CD_CETIP_PRO
	URL/IP	10.0.48.170
	Porta	1364
	Alternate Comm Info	N/A
	Usuário	cetipcd

Informações de Conexão

Os endereços IP e as portas necessários para a conexão com o ambiente do participante devem ser fornecidos, juntamente com os demais parâmetros, no Formulário do Produto Conecta disponível no Portal de Serviços.

Recomendações de Parâmetros Adicionais

- Sessões Simultâneas (pNode e sNode Sessions):** 5
- Tamanho do Buffer (SSL/TLS):** 32K
- Tipo de Transmissão:** Texto e Binário (para arquivos zipados durante a transferência)
- Configurações de Retentativas (Retries):** “Short Term e Long Term” = 3 segundos
- Intervalo de Retentativas:** “Short Term” = 10 segundos e “Long Term” = 3 minutos

2.3 Envio e Recebimento de Arquivos

O nome dos arquivos deve seguir o seguinte padrão:

✓ [númeroDaConta].[NomeDoArquivo].txt

Exemplo: 12345678.TESTE.txt

Para cada arquivo recebido através do Conecta e processado no NoMe, o retorno será enviado no seguinte formato:

- ✓ [NomeDoArquivo].txt.S[NúmeroDeSolicitação]

Exemplo: TESTE.txt.S1234567

Caminho para Envio de Arquivos no Business Process

Ao enviar um arquivo, o cliente deve definir o caminho do business process na propriedade “Remote File Name” da seguinte forma:

- ✓ /businessprocess/cetip_CDRecvEsp/<Conta>
<nomeDoArquivoParaRetorno>.[extensão]

Exemplo: file=/businessprocess/cetip_CDRecvEsp/12345678.nomeDoArquivoParaRetorno.txt

Onde:

- <Conta>refere-se ao número da conta do cliente, que deve ser informado sem pontos e traços. Por exemplo, se a conta for 12345.67-8, deve ser indicado como 12345678.
- <nomeDoArquivoParaRetorno> é a nomenclatura do arquivo enviado, que também será o nome do arquivo que será retornado.
- [extensão]corresponde à extensão do arquivo (txt ou TXT).

Teste de Conexão

Para realizar testes de conectividade, o participante deve enviar um arquivo cujo conteúdo contenha a palavra "TESTE" (em maiúsculas) e uma quebra de linha. Após o recebimento e validação do arquivo, será feita automaticamente uma chamada ao participante, devolvendo um arquivo de retorno para concluir o teste.

Exemplo: file=/businessprocess/cetip_CDRecvEsp/12345678.TESTE.txt

Conteúdo do arquivo:

- ✓ TESTE

2.3.1 SFTP/SSH

O SFTP (SSH File Transfer Protocol) é um protocolo que permite a transferência de arquivos de forma segura. Por padrão, o SFTP utiliza o SSH para autenticação e criptografia da comunicação. Para mais detalhes, os usuários podem consultar o seguinte endereço: https://wiki.filezilla-project.org/SFTP_specifications

Neste modelo, a B3 atua apenas como servidor. O upload e download de arquivos são realizados pelo cliente, utilizando sistemas SFTP client. Entre as opções disponíveis no mercado, destacam-se ferramentas como Filezilla e Secure Client, mas os clientes têm a liberdade de escolher outras soluções que atendam às suas necessidades.

O SFTP funciona como uma pasta virtual. O cliente deve implementar um processo cíclico de leitura para verificar o conteúdo disponibilizado na pasta e sensibilização dos seus sistemas internos para processamento dos resultados.

2.3.2 Diretórios Disponíveis no SFTP e Regras de Utilização

Após estabelecer a conexão via SFTP, o cliente visualizará três diretórios principais disponibilizados pela B3. Cada diretório possui permissões específicas que devem ser rigorosamente respeitadas para garantir o correto funcionamento do Conecta:

1) ArqsAguardando

Diretório destinado exclusivamente ao envio de arquivos pelo participante.

- **Permissão:**

✓ PUT (criação/envio de arquivos)

✗ Não são permitidas operações de **GET** ou **DELETE**.

2) ArqsRetorno

Diretório no qual a B3 disponibiliza arquivos de retorno referentes ao processamento de solicitações enviadas pelo cliente.

- **Permissões:**

✓ GET (download)

✓ DELETE (exclusão após leitura)

- **Recomendação importante:**

Recomendamos fortemente que os arquivos sejam removidos (DELETE) após o download, evitando retrabalhos e facilitando a lógica de identificação de arquivos pendentes de consumo.

3) ArqsBatch

Diretório destinado ao recebimento de arquivos referentes ao malote cadastrado do participante.

- **Permissões:**

✓ GET(download)

✓ DELETE (exclusão após leitura)

- **Recomendação:**

Assim como na pasta ArqsRetorno, é recomendado deletar os arquivos após o consumo.

2.3.3 Parâmetros para configuração

Autenticação

A autenticação no serviço SFTP é realizada através dos seguintes componentes:

- **Usuário**
- **Par de Chaves (SSH Pair Key)**

O cliente é responsável por fornecer a chave pública necessária para a autenticação no serviço SFTP.

Observação: É importante destacar que não se trata de um certificado SSL; é necessário gerar um par de chaves SSH.

As chaves devem atender aos seguintes requisitos:

- **Tipo da chave:** SSH-RSA
- **Tamanho da chave:** 2048 bits

Outras Configurações de Segurança Recomendadas

MACs	hmac-sha2-256-etm@openssh.com hmac-sha2-256
Key exchange	curve25519-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha256 diffie-hellman-group-exchange-sha256
Cifras	aes128-gcm@openssh.com aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr

Importante

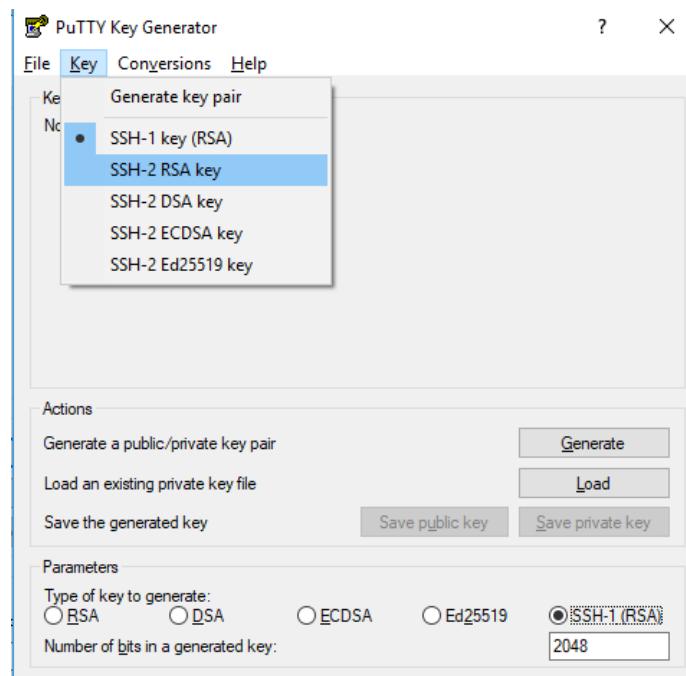
- **Chaves Ativas:** Recomenda-se que cada ambiente tenha apenas um par de chaves ativo, garantindo maior clareza no processo de contingência. As chaves utilizadas em produção devem ser as mesmas no ambiente de contingência.
- **Tipos de Chaves:** Apenas chaves assimétricas com tamanho de 2048 bits ou superior serão aceitas.
- **Reuso de Chaves:** É proibido reutilizar chaves criptográficas para finalidades diferentes.
- **Segurança das Chaves:** O participante é responsável pela segurança, tanto física quanto lógica, da chave privada que foi gerada.
- **Gerenciamento do SFTP:** Do ponto de vista de gerenciamento, o SFTP é considerado o modelo com menor capacidade de monitoramento, dependendo em grande parte do sistema interno desenvolvido pela instituição.
- **Geração de Chaves:** As chaves podem ser geradas em ambientes Windows ou Linux.

✚ Geração de Chaves

Através da ferramenta PuttyGen:

Se o terminal Putty já estiver instalado em sua máquina, o PuttyGen também estará disponível. Para acessá-lo, siga os passos abaixo:

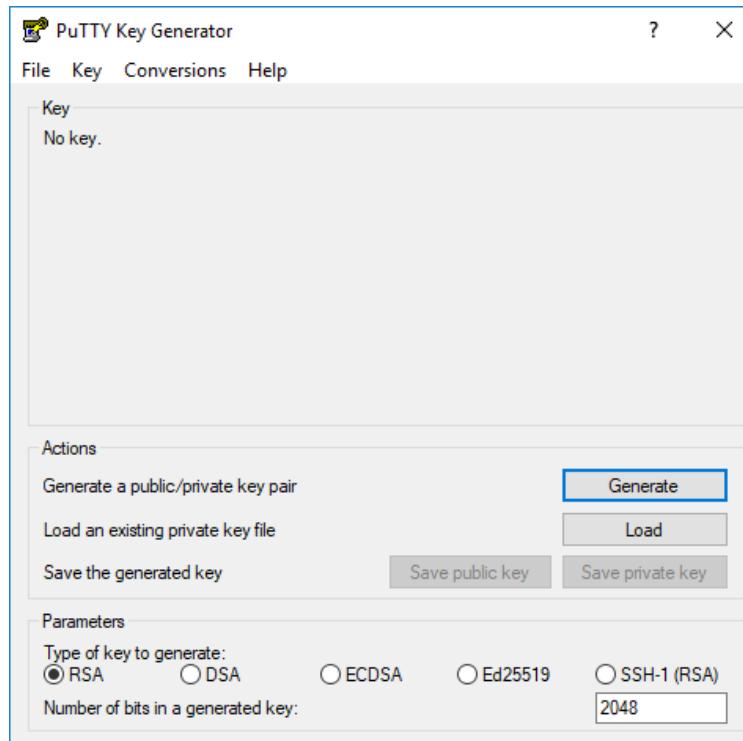
- 1) Vá até o Menu Iniciar e selecione **PuttyGen**.
- 2) Na interface do PuttyGen, vá até a opção **Key** e altere para **SSH-2 RSA key**.



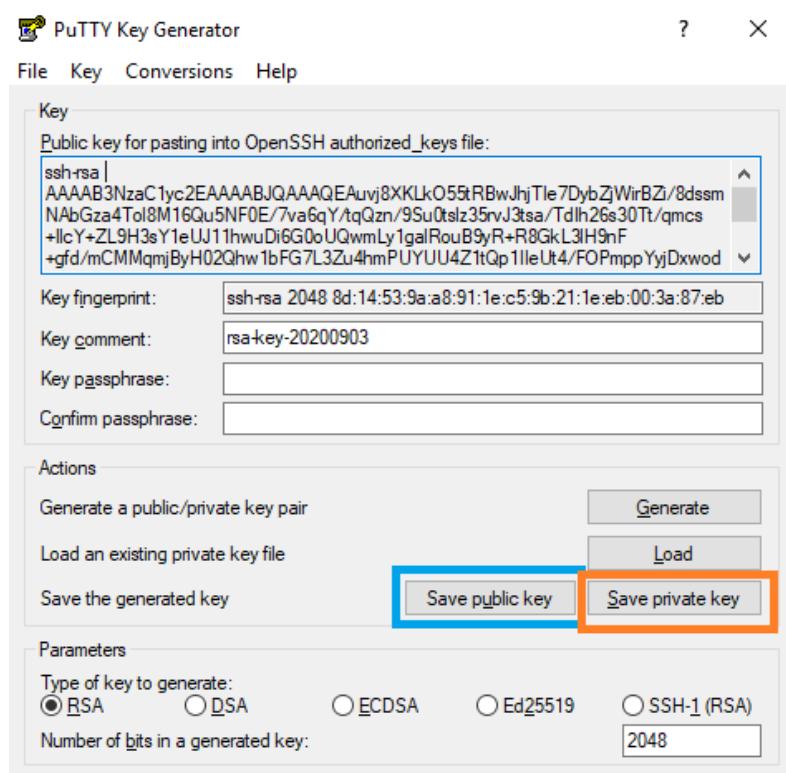
- ✓ Confirmar se na parte inferior alterou para a opção de “RSA”, o número de bits e em seguida clicar em Generate:

Manual de Configuração do CONECTA

[B]³



- ✓ Após, ficará da seguinte maneira e deverá salvar cada chave (pública e privada) individualmente:



Exemplo Linux ou Windows (Via terminal GitBash)

No terminal e diretório onde deseja gerar as chaves.

Usando o comando do “ssh-keygen”

```
$ ssh-keygen -t rsa -b 2048 -f nomedachave
```

Ao final, gerará dois arquivos:

- “**nomedachave**” – a chave privada (que ficará só com vocês)
- “**nomedachave.pub**” – chave pública (que vocês deverão nos fornecer para cadastrarmos no Conecta)

```
rmendonca@NSPP84302 MINGW64 ~/OneDrive - B3 S.A. - Brasil, Bolsa, Balcao/DEMONSTRAÇÃO_CHAVES
$ ssh-keygen -t rsa -b 2048 -f nomedachave
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in nomedachave
Your public key has been saved in nomedachave.pub
The key fingerprint is:
SHA256:MYFi/RS1dopvmYxxikC/nPou1EDE9YYprssQBa1M85U rmendonca@NSPP84302
The key's randomart image is:
+---[RSA 2048]---+
|..+.....oo.
|..+o oEo ... .
|.+.=.=ooo o . .
|..+ + o . = o
|.. .... S o
| o oo + B o
|o . . = o *
|o. ... .
|... .+o
+---[SHA256]---+
rmendonca@NSPP84302 MINGW64 ~/OneDrive - B3 S.A. - Brasil, Bolsa, Balcao/DEMONSTRAÇÃO_CHAVES
$ ls -ltr
total 5
-rw-r--r-- 1 rmendonca 1049089 401 Jun 14 18:45 nomedachave.pub
-rw-r--r-- 1 rmendonca 1049089 1823 Jun 14 18:45 nomedachave
```

Conexões SFTP com a B3

No contexto do protocolo SFTP (SSH File Transfer Protocol), é importante destacar que a comunicação é unidirecional, ou seja, apenas o cliente estabelece a conexão com a B3. Para garantir o acesso adequado, serão necessárias algumas liberações no ambiente do participante, especialmente em relação às portas indicadas.

Requisitos de Conexão:

1) Comunicação Unidirecional:

- O cliente é o único responsável por iniciar a conexão com a B3.

2) Liberações Necessárias:

- O ambiente do participante deve ser configurado para permitir o tráfego de dados na porta especificada.

Endereços para Conexão com a B3 via SFTP:

Ambiente	Comunicação	RTM	Internet
Homologação	URL / IP	10.0.48.23	conectacloud-balcao-hom.b3.com.br
	Porta	22	9039
Produção	URL / IP	10.0.48.123	conectacloud-balcao.b3.com.br
	Porta	22	9039

- Após estabelecer a conexão via SFTP, o cliente visualizará três diretórios principais:

1) ArqsAguardando:

- Este diretório é destinado ao envio de arquivos para processamento no NoMe.
- Observação: O envio de arquivos está limitado a um tamanho máximo de 150 MB. Arquivos que excederem esse limite serão rejeitados e removidos da fila de processamento.

2) ArqsRetorno:

- Aqui, o cliente receberá os arquivos contendo informações de retorno e processamento.

3) ArqsBatch:

- Neste diretório, os clientes acessarão os arquivos e relatórios disponíveis para o malote cadastrado.

Possíveis Problemas de Conexão

O arquivo `known-hosts` armazena as chaves públicas dos servidores com os quais você já se conectou. Caso a chave SSH de um servidor seja alterada — seja por reinstalação, atualização ou rotatividade de chaves por questões de segurança — o cliente SSH detectará uma discrepância entre a chave armazenada no `known-hosts` e a nova chave do servidor. Essa situação pode impedir que as automações realizem logins via SFTP/SSH de forma adequada.

Para resolver esse problema e retomar o acesso para a troca de arquivos, siga os passos abaixo:

1) Localização do arquivo `known-hosts`:

- Em sistemas Unix/Linux/Mac, geralmente está localizado em:
 - `~/.ssh/known_hosts`
- Em sistemas Windows:**
 - `%USERPROFILE%\.ssh\known_hosts`

2) Remoção da entrada antiga do servidor no arquivo:

- Encontre a linha correspondente ao servidor antigo e exclua-a.

3) Nova autenticação:

- Ao realizar a nova autenticação, você será solicitado a aceitar a nova chave pública. Digite “yes” para confirmar.

Observação: Se não conseguir localizar o arquivo known_hosts, verifique na ferramenta utilizada qual a configuração equivalente.

Dica: Em algumas ferramentas que operam em sistemas Windows, a estrutura pode ser encontrada no Editor de Registros do Windows:

- Computador\HKEY_CURRENT_USER\Software\<Autor>\<Ferramenta>\SshHostKeys
- Clique com o botão direito do mouse na chave e selecione a opção “Excluir”.

Exemplo:

- ✓ Ferramenta WinSCP:

```
Computador\HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\SshHostKeys
```

- ✓ Para ferramenta baseada no Putty:

```
Computador\HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\SshHostKeys
```

Teste de Conexão

Para realizar testes de conectividade, o participante poderá enviar um arquivo cujo conteúdo seja a palavra "TESTE" (em maiúscula) seguida de uma quebra de linha. Após o recebimento e validação do arquivo, será feita a devolução automática no diretório de retorno do participante, concluindo o teste.

Exemplo: Se for submetido o arquivo ArqsAguardando/12345678.TESTE.txt com o seguinte conteúdo:

TESTE

O arquivo retornado será: ArqsRetorno/12345678.TESTE.txt com o mesmo conteúdo.

Observação: Caso o conteúdo do arquivo não siga os padrões definidos para teste ou para o fluxo de negócios, o arquivo será descartado.

3 PROCESSOS ADICIONAIS

3.1 Ativação, Substituição e Revogação de Certificados e Chaves

A B3 não valida os certificados em listas de certificados revogados das CAs. Os certificados serão considerados inválidos apenas após comunicação formal via e-mail pelo Participante.

A Instituição é responsável por informar a B3 sobre a necessidade de atualizar o certificado, devendo essa solicitação ser enviada com 10 dias úteis de antecedência para o e-mail: sat@b3.com.br.

A atualização do certificado deve respeitar os processos de governança das duas Instituições (B3 e Cliente), e as alterações de configuração devem ser executadas preferencialmente fora das janelas de funcionamento do sistema.

Os certificados substituídos devem ser revogados pelo Participante junto à CA emissora, não podendo ser utilizados futuramente, assim como as chaves a eles relacionadas. A atualização do certificado em Produção não requer homologação.

3.2 Processo de Envio de Malote Individualizado

O processo anterior, que consistia no envio dos arquivos gerados no malote do participante referentes à operação de D-1, será mantido apenas para o envio de relatórios PDF (RelsBatch.zip). Na nova versão, o envio ocorre de forma individualizada, ou seja, os arquivos são entregues no momento de sua geração, proporcionando agilidade ao cliente e diluindo o fluxo de transmissão de arquivos.

Este novo fluxo já está em vigor, e todas as novas contas são configuradas de forma individualizada. Para isso, é necessário combinar previamente com a equipe de Atendimento as seguintes informações:

- Malote: Exemplo: 12345
- Nome do(s) arquivo(s) original(is) desejado(s) que existem no malote: Exemplo: CETIP21_<AAMMDD>_<UF>_DOPERACOESMULTILATERAL.TXT
- Nome do arquivo “renomeado” a ser enviado* (aplicável apenas para Clientes que utilizam Mainframe para transmissão de arquivos via Connect:Direct).

Com essa configuração, o participante receberá o arquivo de forma unitária e compactado em extensão zip, juntamente com o ID de solicitação e o nome original ou renomeado (caso do Mainframe). A entrega segue o seguinte exemplo:

Exemplo para um participante fictício cujo número do malote corresponde a 05000:

- 05000 corresponde ao número do malote.
- CETIP21_AAMMDD_UF_DPOSICAO-SWAP.TXT.zip corresponde ao arquivo gerado e mapeado para envio.
- S<1234567>corresponde ao número de solicitação para entrega do arquivo.

Recomendações

- A Instituição Participante é responsável por manter os registros de log de seu sistema, que conecta com a B3, permitindo a rastreabilidade e auditoria dos eventos de troca de arquivos.

- Os arquivos transmitidos entre os Participantes e a B3 serão tratados conforme as regras de negócio estabelecidas de forma irrevogável, incondicional e final. É fundamental considerar as regras do processo de transferência de arquivos existente no NoMe.
- Alterações na infraestrutura do cliente, como IP, DNS, certificados etc., devem ser informadas à B3 com pelo menos 10 dias úteis de antecedência.
- O Conecta está estruturado para tratar arquivos com alta concentração de registros em processos batch e de forma cíclica, otimizando o processamento de arquivos com grande volume de registros, em vez do envio de muitos arquivos com poucos registros. Por isso, recomenda-se construir processos de concentração de registros e posterior criação e envio dos arquivos, respeitando o tamanho limite de 150 MB.

3.3 Procedimentos para Testes de Conexão FileZilla

Cenários de testes para auxiliar os Participantes na configuração e conexão, permitindo a realização de testes de conexão com a B3 para o envio de arquivos.

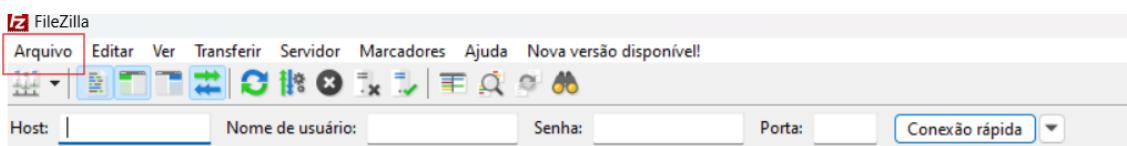
3.3.1 Teste de envio de Arquivo via SFTP

1. Abrir o FileZilla:

- ✓ Inicie o FileZilla em sua máquina.

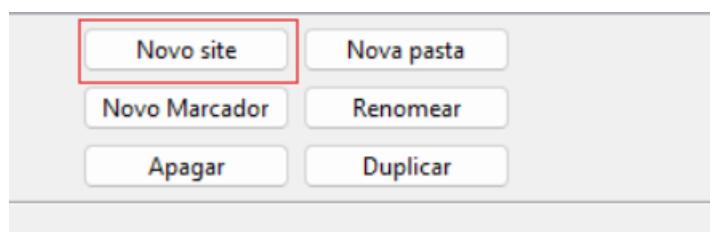
2. Acessar o Gerenciador de Sites:

- ✓ Clique na opção "Arquivo" no menu superior e depois em "Gerenciador de Sites...".



3. Criar um Novo Site:

- ✓ No Gerenciador de Sites, clique em "Novo Site" e nomeie-o como "Conecta Cloud".

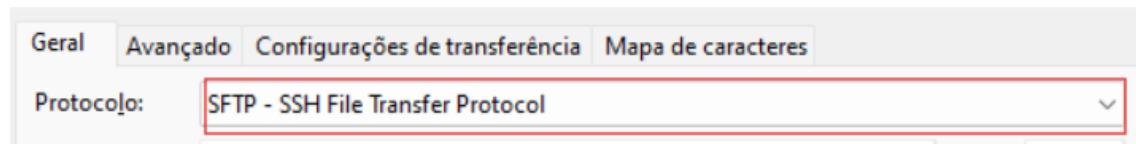


4. Informar o Protocolo de Conexão:

Manual de Configuração do CONECTA

[B]³

- ✓ No painel à direita, selecione "SFTP - SSH File Transfer Protocol"



5. Incluir o Host:

- ✓ Insira o hostname do Conecta Cloud (ex: sftp.conectacloud.com).



6. Incluir a Porta de Conexão:

- ✓ (opcional) Insira a porta se não for a padrão (22 para SFTP).

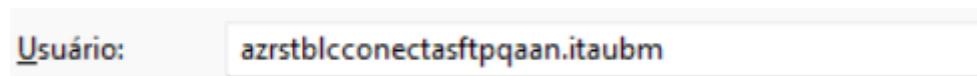
7. Informar o Tipo de Logon:

- ✓ Selecione "Normal".



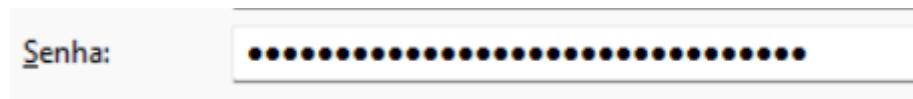
8. Informar Usuário:

- ✓ Insira seu nome de usuário.



9. Informar a Senha:

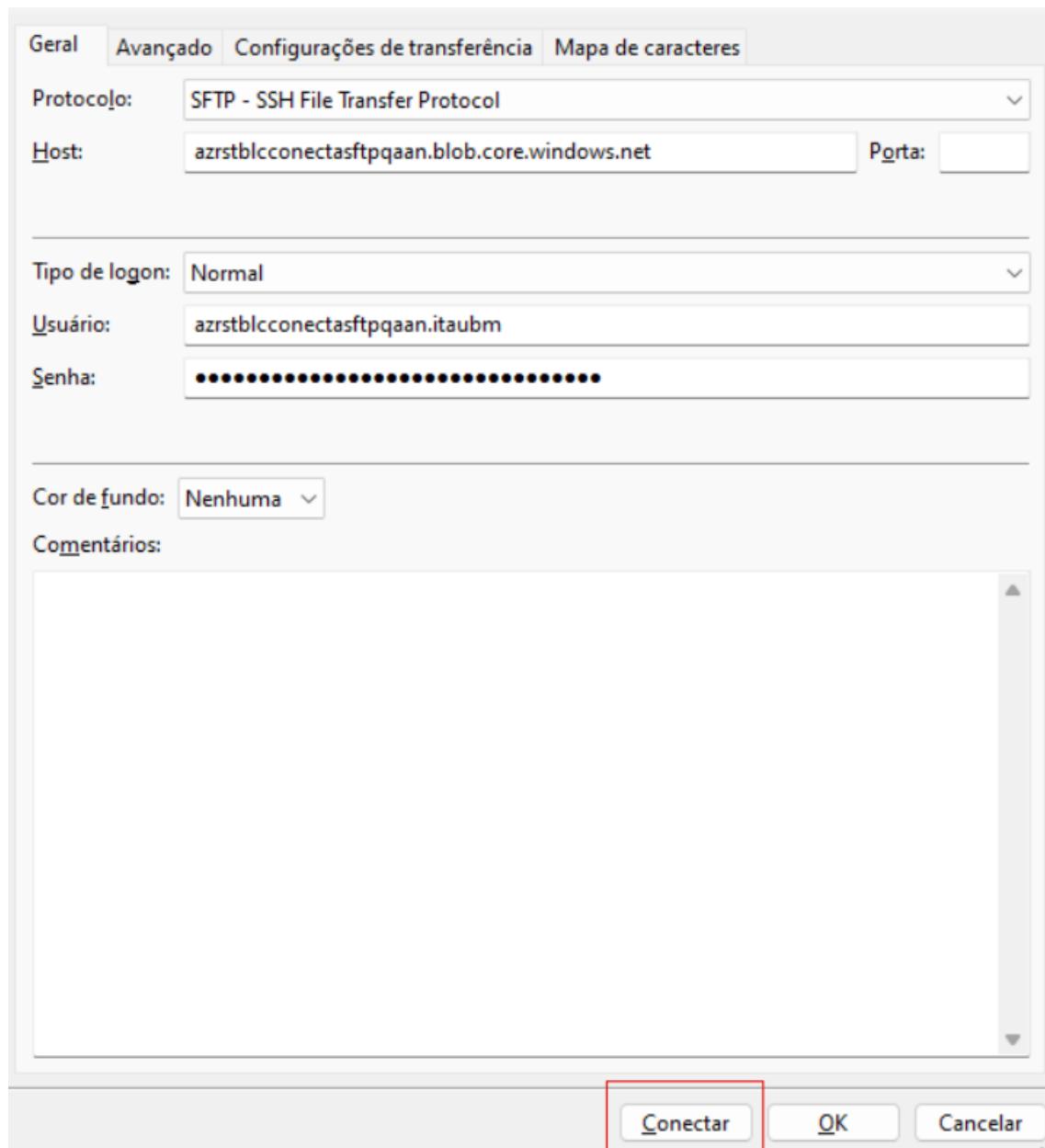
- ✓ Insira sua senha.



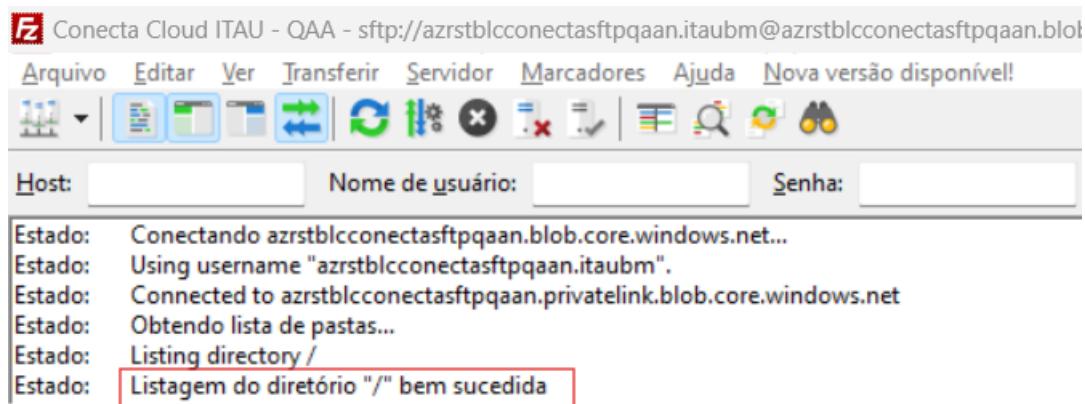
10. Conectar:

Manual de Configuração do CONECTA

[B]³

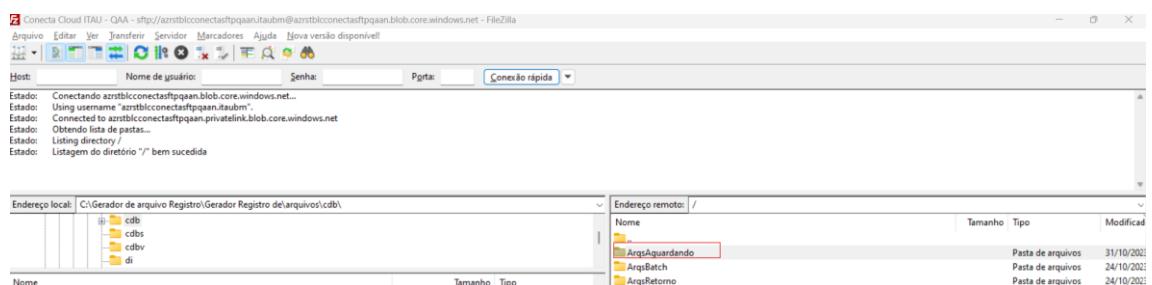


- ✓ Clique em "Conectar". Após isso, o FileZilla irá apresentar a mensagem de sucesso: **"Listagem do diretório '/' bem sucedida"**, indicando que a conexão foi estabelecida com sucesso.

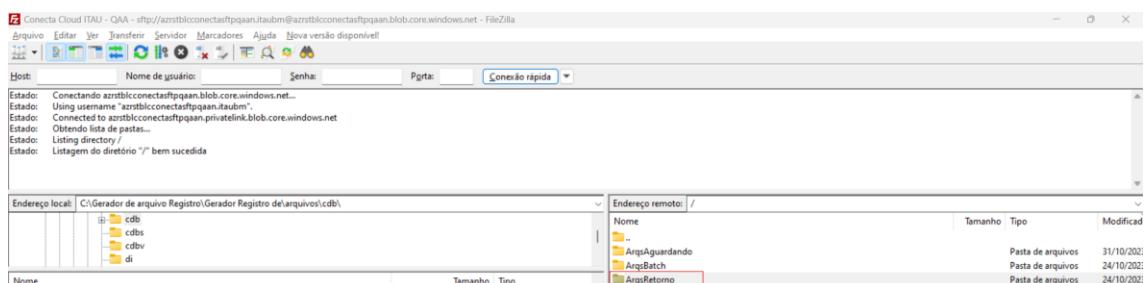


- **Envio de Arquivos via SFTP**

- ✓ Para realizar o envio de arquivos pelo Conecta Cloud, os arquivos devem ser carregados na pasta "ArqsAguardando".



- ✓ Após o envio dos arquivos, os arquivos de retorno (DEMOVTRANSF) serão disponibilizados na pasta "ArqsRetorno".



3.3.2 Testes de envio de Arquivo via Connect:Direct

11. Abrir o FileZilla:

- ✓ Inicie o FileZilla em sua máquina.

12. Acessar o Gerenciador de Sites:

- ✓ Clique na opção "Arquivo" no menu superior e depois em "Gerenciador de Sites...".

13. Criar um Novo Site:

- ✓ No Gerenciador de Sites, clique em "Novo Site" e nomeie-o como "Connect:Direct".

14. Configurar as Propriedades do Site:

- ✓ No painel à direita, preencha as seguintes informações:
- ✓ Host: Insira o hostname do Connect:Direct.
- ✓ Porta: (opcional) Insira a porta se não for a padrão.
- ✓ Protocolo: Selecione "FTP - File Transfer Protocol" (ou "FTPS" se necessário).
- ✓ Tipo de Login: Selecione "Normal".
- ✓ Usuário: Insira seu nome de usuário.
- ✓ Senha: Insira sua senha.

15. Salvar e Conectar

- ✓ Clique em "Conectar" ou "OK" para salvar as configurações e conectar-se ao Connect:Direct.

Envio de Arquivos via Connect:Direct

- Para fazer o envio de arquivos, é preciso acessar o diretório de upload do usuário: "upload/PARTICIONANTE/".
- Após o envio dos arquivos, os arquivos de retorno (DEMOVTRANSF) serão disponibilizados na pasta "ArqsRetorno".

4 CONTATOS NA B3

- Telefone: 11 2565 5120
- E-mail: sat@b3.com.br