

MANUAL DE CONFIGURAÇÃO DO CONECTA

Requisitos para implementar em novos ambientes

Manual de Configuração do CONECTA

SUMÁRIO

| | | |
|------------|--|-----------|
| 1 | OBJETIVO | 3 |
| 2 | CONECTA | 3 |
| 2.1 | Formas de comunicação | 3 |
| 2.2 | Protocolos | 4 |
| 2.2.1 | Connect:Direct | 4 |
| 2.3 | Envio e recebimento de Arquivos | 7 |
| 2.3.1 | SFTP/SSH | 8 |
| 3 | PROCESSOS ADICIONAIS | 10 |
| 3.1 | Ativação, substituição e revogação de certificados e chaves | 10 |
| 3.2 | Processo de envio de malote individualizado | 11 |
| 4 | RECOMENDAÇÕES | 12 |
| 5 | CONTATOS NA B3 | 13 |

Manual de Configuração do CONECTA

1 OBJETIVO

Este manual tem o objetivo de consolidar os requisitos técnicos necessários para implementar o Conecta para a plataforma NoMe.

2 CONECTA

O Conecta é a solução definida para possibilitar a automatização de troca de arquivos entre clientes e a B3. No segmento Balcão, a solução está integrada ao NoMe.

O Conecta funciona 24 horas, porém, se os arquivos forem enviados enquanto a grade de transferência de arquivos estiver fechada, estes ficarão em *standby* até que a próxima grade de processamento esteja disponível novamente.

O Conecta está estruturado para tratar arquivos com alta concentração de registros em processos batch de forma cíclica e está otimizado para trabalhar com o processamento de arquivos com grande volume de registros em detrimento do envio de muitos arquivos com poucos registros. Por esta razão é recomendado que sejam construídos processos de concentração de registros. **Existe no Conecta uma limitação em relação ao tamanho do arquivo. Esse limite é de 150MB para os arquivos de entrada.**

2.1 Formas de comunicação

É possível o Cliente comunicar-se via RTM ou via internet.

Para conexões trafegadas via RTM, o Cliente deve entrar em contato com a RTM para definir o melhor modelo de configuração para contingência de rede, considerando questões como NAT e resolução de nomes DNS. Aconselhamos ter apenas um endereço IP para os dois ambientes: Produção e Contingência. No caso de configuração de conexões via internet, o Cliente deve verificar junto

Manual de Configuração do CONECTA

ao seu time de redes, em relação ao endereço IP para entrada e saída nos ambientes.

Observação: Vale ressaltar que na configuração de RTM e de internet são de serviços distintos e é necessário combinar previamente junto ao time de atendimento a decisão de qual das formas de comunicação será utilizada.

2.2 Protocolos

O Conecta suporta a transferência de arquivos em duas modalidades: Connect:Direct e SFTP. A escolha da plataforma fica a critério do cliente.

2.2.1 Connect:Direct

Connect:Direct é um protocolo desenvolvido pela IBM para transferência de arquivos ponto-a-ponto. A arquitetura permite o envio e recebimento automatizado de arquivos com segurança, gerenciamento e dinâmica entre sistemas operacionais distintos. Mais detalhes sobre o software podem ser consultados no site do fabricante: www.ibm.com.

Nesse modelo, as duas pontas (B3 x Participante) são servidores e enviam e recebem arquivos.

2.2.1.1 Parâmetros para configuração

Autenticação

A autenticação é feita em 2 passos:

Passo 1. Node + IP + usuário

Passo 2. Validação do certificado digital através do módulo Secure+.

Manual de Configuração do CONECTA

Certificado

A B3 enviará o certificado para autenticação dos clientes no CD. O cliente é responsável por fornecer o certificado para autenticação em seu CD. Esse certificado deve atender aos seguintes requisitos:

- Tamanho da chave: 2048 bits
- Algoritmo de hash: SHA 256
- Certificado SSL para servidor
- Emitido por uma CA (Autoridade Certificadora) de raiz confiável.

Importante

Recomendamos que cada ambiente tenha apenas um certificado ativo, para maior transparência no processo de contingência. O certificado de produção deve ser o mesmo em contingência.

É importante que os certificados de Homologação e Produção sejam gerados pela mesma certificadora a fim de validar todo o processo homologatório.

Modulo Secure+

O Modulo Secure+ deverá estar habilitado com o protocolo **TLS 1.2**.

Ativar os padrões de criptografia (*Cipher Suites*) listados abaixo:

- ECDHE_RSA_WITH_AES_256_GCM_SHA384*
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Conexões

No Conect: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

Endereços para Conexão com a B3 via CD

| Ambiente | Comunicação | RTM | INTERNET |
|-------------|---------------------|--------------|--|
| Homologação | Node | CD_CETIP_HOM | CD_CETIPWEB_HOM |
| | URL/IP | 10.0.48.70 | conecta-balcao-hom.b3.com.br (177.66.125.12 / 177.54.223.12) |
| | Porta | | 1364 |
| | Alternate Comm Info | N/A | 200.19.56.240 |
| | Usuário | | cetipcd |
| Produção | NODE | CD_CETIP_PRO | CD_CETIPWEB_PRO |
| | URL/IP | 10.0.48.170 | conecta-balcao.b3.com.br (177.54.223.11/ 177.66.125.11) |
| | Porta | | 1364 |
| | Alternate Comm Info | N/A | 177.66.125.25 (PROD) / 200.19.56.250 (DR) |
| | Usuário | | cetipcd |

Os endereços IP e portas para conexão com o ambiente do Participante devem ser informados, juntamente com os demais parâmetros, no [Formulário do Produto Conecta no Portal de Serviços](#).

Recomendações de Parâmetros Adicionais:

- Sessões simultâneas (pNode e sNode Sessions): 5
- Buffer Size (SSL/TLS): 32K
- Tipo de transmissão: Texto e Binário (para arquivos zipados da transferência de arquivos)
- Retries (Process retry settings): “Short Term e Long Term” = 3 segundos
- Retry Interval: “Short Term” = 10 seg e “Long Term” = 3 min

Manual de Configuração do CONECTA

2.3 Envio e recebimento de Arquivos

O nome do arquivo deve seguir o padrão:

[NúmeroDaConta].[NomeDoArquivo].txt

Exemplo: 12345678.TESTE.txt

Para todo arquivo recebido via Conecta e processado no NoMe, seu retorno chegará da seguinte forma: **[NomeDoArquivo].txt.S[NúmeroDeSolicitação]**

Exemplo: TESTE.txt.S1234567

Caminho para ser enviado arquivo no Business Process

Ao enviar o arquivo, o cliente deve parametrizar o caminho do business process na propriedade “Remote File Name”

/businessprocess/cetip_CDRecvEsp/[Conta].nomeDoArquivoParaRetorno[extensão]

Exemplo:

```
file=/businessprocess/cetip_CDRecvEsp/12345678.nomeDoArquivoParaRetorno.txt
```

Teste de Conexão

Para a realização de testes de conectividade, o participante deverá enviar um arquivo cujo conteúdo seja a palavra TESTE (em maiúscula) e uma quebra de linha. Após o recebimento e validação do arquivo, faremos uma chamada ao participante, devolvendo um arquivo de retorno – concluindo o teste.

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

Conteúdo do arquivo:

| | |
|---|-------|
| 1 | TESTE |
| 2 | |

Manual de Configuração do CONECTA

2.3.1 SFTP/SSH

SFTP (SSH File Transfer Protocol) é um protocolo para transferência de arquivos de forma segura. Por padrão, o SFTP utiliza SSH para autenticação e criptografia da comunicação. Mais informações podem ser consultadas nesse endereço: https://wiki.filezilla-project.org/SFTP_specifications.

Nesse modelo, a B3 é apenas o servidor. O upload e download de arquivos é feito pelo cliente, através de sistemas SFTP *client*. Algumas das opções de ferramenta *client* são o Filezilla ou Secure Client, mas existem outras opções disponíveis no mercado que podem ser utilizadas pelo cliente.

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.

2.3.1.1 Parâmetros para configuração

Autenticação

- Usuário
- Par de Chaves (SSH Pair Key)

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

Obs: Não se trata de um certificado SSL. É necessário gerar o par de chaves SSH

Esse certificado deve atender aos seguintes requisitos:

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

Manual de Configuração do CONECTA

Importante:

- Recomendamos que cada ambiente tenha apenas um par de chaves ativo, para maior transparência no processo de contingência. As chaves em produção deve ser as mesmas em contingência.
- Somente chaves assimétricas RSA-2048 bits serão aceitas.
- É vedado o reuso das chaves criptográficas para outras finalidades.
- O participante é responsável pela segurança, física e lógica, da chave privada criada.
- Do ponto de vista de gerenciamento, SFTP é o modelo com menor recurso de monitoração. Depende muito do sistema interno desenvolvido pela Instituição.

As chaves podem ser geradas tanto em ambiente Windows como Linux. Abaixo, exemplo de procedimento para geração.

Exemplo Windows

Download da biblioteca Open Source com toolkit:

<http://gnuwin32.sourceforge.net/packages/openssl.htm>

Para gerar o par de chaves:

```
$openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
```

Extrair a chave pública:

```
$openssl rsa -pubout -in private_key.pem -out public_key.pem
```

Chave deve começar com ssh-rsa:

Ex: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDKW138fC3jtz9

Manual de Configuração do CONECTA

Conexões

No SFTP, a comunicação é unidirecional. Apenas o cliente conecta na B3.

Serão necessárias liberações no ambiente do participante para acessar na porta indicada na tabela abaixo:

Endereços para Conexão com a B3 via SFTP

| Ambiente | Comunicação | RTM | INTERNET |
|--------------------|-------------|-------------|--|
| Homologação | URL / IP | 10.0.48.70 | conecta-balcao-hom.b3.com.br |
| | Porta | 22 | 9039 |
| Produção | URL / IP | 10.0.48.170 | conecta-balcao.b3.com.br |
| | Porta | 22 | 9039 |

Após estabelecer a conexão via SFTP aparecerão 3 diretórios principais que são:

ArqsAguardando – Local onde o cliente coloca os arquivos para processamento no NoMe (envio);

Obs: Somente é possível enviar arquivos via conecta de até 150 MB, maior que isto o arquivo será rejeitado e retirado da fila de processamento.

ArqsRetorno – Por onde são respondidos os arquivos com informação de retorno e processamento;

ArqsBatch – Por onde os clientes recebem os arquivos e relatórios disponíveis para o Malote cadastrado;

3 PROCESSOS ADICIONAIS

3.1 Ativação, substituição e revogação de certificados e chaves

A B3 não faz a validação dos certificados em qualquer lista de certificados revogados das CAs. Os certificados só serão considerados inválidos após o comunicado formal, via e-mail, pelo Participante.

Manual de Configuração do CONECTA

A Instituição fica responsável por informar a B3 sobre a necessidade de atualizar o certificado. Essa solicitação deve ser enviada com 10 dias úteis antes da ativação. A solicitação deve ser enviada para sat@b3.com.br.

O processo de atualização do certificado deve, primeiramente, respeitar os processos de governança das duas Instituições (B3 x Cliente). As alterações de configuração devem, preferencialmente, serem executadas em horário fora das janelas de funcionamento do sistema.

Os certificados substituídos deverão ser revogados, pelo Participante, junto à CA emissora, não podendo serem utilizados futuramente e nem as chaves a eles relacionadas.

A atualização do certificado em Produção não precisa passar por Homologação.

3.2 Processo de envio de malote individualizado

Existe um processo que consiste no envio dos arquivos gerados no malote do participante referentes à operação de D-1. Na versão anterior, a parametrização de diversos arquivos era consolidada em um único zip e enviado para o cliente pela manhã.

Nesta nova versão, o envio ocorre de forma individualizada, ou seja, os arquivos são entregues no momento da sua geração - a qualquer hora do dia, trazendo agilidade para o cliente e diluindo o fluxo de transmissão de arquivos.

Este novo fluxo entra em vigor a partir da divulgação deste manual e todas as novas contas serão configuradas de forma individualizada, onde deverá ser combinado previamente com o time de Atendimento as seguintes informações:

- Malote – 12345
- Nome do arquivo original desejado existente no malote:

Ex: CETIP21_<AAMDD>_<UF>_DOPERACOESMULTILATERAL.TXT


Manual de Configuração do CONECTA

- Nome do arquivo “renomeado” a ser enviado*

**Situação aplicada somente nos casos do Participante que utiliza Mainframe para transmissão de arquivos via Connect:Direct, é necessário informar um nome diferenciado ao qual o Mainframe do cliente aceite receber.*

Com essa configuração, o participante receberá o arquivo unitariamente e compactado em extensão zip + id de solicitação com o nome original ou renomeado (caso mainframe), conforme exemplo abaixo:

Ex:

 CETIP21_211111_RJ_DFLUXO_SWAP.TXT.zip.S4019306

Observação: Por enquanto, as contas já configuradas no Conecta (versão anterior do processo) permanecerão com um único zip. Então a configuração permanecerá híbrida, convivendo com o legado até a conclusão da migração das contas atuais. Caso o cliente já opte por migrar para a nova versão desse processo, deverá combinar juntamente ao SAT.

4 RECOMENDAÇÕES

- A Instituição Participante fica 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 importante considerar as regras do processo de transferência de arquivo existente no NoMe.
- As alterações na infraestrutura do cliente, como IP, DNS, certificados etc., devem ser informadas à B3 com pelo menos 10 dias úteis antes da atividade.
- O Conecta está estruturado para tratar arquivos com alta concentração de registros em processos *batch* e de forma cíclica, está otimizado para trabalhar com o processamento de arquivos com grande volume de registros em detrimento do envio de muitos arquivos com poucos registros. Por esta razão recomendamos que sejam construídos

Manual de Configuração do CONECTA

processos de concentração de registros e posterior criação e envio dos arquivos - ressaltando que o tamanho limite é de 150MB.

5 CONTATOS NA B3

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