

PLATAFORMA LECOM

Implantação versão 5.70 RTM 1.02.1 ou superior



Conteúdo

1. Introdução.....	4
Pré-requisitos.....	5
1.1 Software.....	5
1.1.1 Software Configurações mínimas.....	5
1.1.2 Docker e Docker-Compose	6
1.1.3 Servidor de cache Redis.....	7
1.1.4 Servidor RabbitMQ.....	7
1.1.5 Quantidade de arquivos abertos no servidor	7
1.2 Rede	7
1.2.1 Comandos de rede.....	7
1.2.2 Resolução DNS	7
1.3 Acesso a disco	7
1.4 Acessos externos.....	8
1.5 Sistema Operacional	9
1.6 Gateway / Firewall	9
1.7 Envio de e-mail.....	9
1.8 Navegadores e resoluções	10
1.9 Banco de dados	10
1.9.1 Versões homologadas.....	10
1.9.2 Transações.....	11
1.9.3 Base dedados	12
1.9.4 Usuários.....	13
1.9.5 Limites de conexão.....	13
1.9.6 Collation	14
2. Preparação do ambiente.....	15
2.1 Usuário de sistema	15
2.1.1 Criação do usuário e chave de acesso	15
2.1.2 Permissões do usuário.....	17
2.2 LibreOffice	17
2.3 NodeJS.....	17
2.4 PhantomJS	17
2.5 Proxy reverso	18
3. Implantando a plataforma no Linux	20
3.1 Profiles da aplicação	20
3.1.1 Tipos de ambientes	20
3.1.2 Sistemas operacionais	20
3.1.1 SGBD.....	20
3.1.1 Proxy e SSL.....	21
3.2 Estrutura de pastas dos serviços	21
3.3 Configurando os serviços	22
3.3.1 Movendo os serviços para suas pastas.....	22
3.3.2 Definindo as variáveis de ambiente	22
3.3.3 Config-service.....	27

3.3.4 Discovery-service	28
3.3.5 Gateway-service.....	28
3.3.6 Form-App.....	29
3.3.7 Form-service	30
3.3.8 Service integration.....	30
3.3.9 Audit service.....	31
3.3.10 Behavior service	32
3.3.11 Docker-compose.....	32
• lecom-services-default.env.....	33
• job-runner.env	33
• job-service.env.....	33
• redis.env.....	34
• job-service.yml.....	34
• job-runner.yml	35
• rabbitmq.yml.....	35
• redis.yml.....	36
• Descrição das variáveis.....	36
3.3.12 Node web server.....	37
3.4 Configurando serviços do tomcat da plataforma.....	38
3.4.1 Adequando configuração de host	39
3.4.2 Definição de encoding	40
3.4.3 Definição de memória	40
3.4.4 Variáveis de ambiente para os módulos no Tomcat.....	40
3.5 Configurando serviços do tomcat das aplicações externas.....	43
3.5.1 Instalação do tomcat.....	43
3.5.2 Adequando configuração de host	43
3.5.3 Variáveis de ambiente para as aplicações no Tomcat	44
3.5.4 Registrar o tomcat_app como serviço	44
3.6 Iniciando os serviços	45
3.7 Ambiente em Cluster.....	46
3.7.1 Storage de dados	46
3.7.2 Configurações	46
4. Recursos extras	47
4.1 Open Redirect.....	47
4.2 Tratamento CSRF	47
4.3 Headers HTTP.....	47
5. Licenciamento	49
5.1 Ativando o módulo de login	49
5.2 E-mail para notificação de expiração de licença	50
6. Configurações finais	51
6.1 Configurando servidor de e-mail.....	51
6.2 URL de acesso.....	52
6.3 Ativando os robôs	53
7. Validação do ambiente.....	53
8. Portas utilizadas pelos módulos da plataforma	54
9. API para monitoramento de disponibilidade de ambiente	55

10.	Autenticação.....	56
10.1	Acesso automático usando as credenciais do Microsoft AD	56
10.1.1	Introdução	56
10.1.2	Requisitos.....	56
10.1.3	Configuração servidor Active Directory.....	57
10.1.4	Configuração servidor aplicação.....	58
10.1.5	Configuração do AD na plataforma	59
10.1.6	Configuração estação de trabalho.....	61
10.1.7	Navegadores Google Chrome e Microsoft EDGE	61
10.1.8	Navegador Firefox	67
10.1.9	Validando configuração.....	68
10.2	Protocolo LDAP.....	68
10.2.1	Introdução	68
10.2.2	Configuração.....	68
10.2.3	Ativando importação automática.....	71
10.3	Protocolo OAUTH.....	74
10.3.1	Introdução	74
10.3.2	Pré-requisitos para Configuração	74
	Para que a autenticação SAML funcione, é necessário que a plataforma esteja configurada com um certificado SSL válido.....	74
10.3.3	Configuração	74
10.4	Protocolo SAML.....	77
10.4.1	Introdução	77
10.4.2	Configuração.....	78
	Apêndice A – Exemplo VHOST apache	80

1. Introdução

Objetivo desse documento é descrever os passos para implantação da Plataforma Lecom.

Caso tenha interesse em acessar o manual de uso da aplicação acesse o link:
<https://helpcenter.lecom.com.br>

Pré-requisitos

As configurações abaixo são as mínimas necessárias para executar a Plataforma Lecom. Porém, recomendamos que seja feita uma análise de demanda prevista para que seja dimensionado corretamente o ambiente para atender a expectativa de desempenho desejado.

É necessário que tenha pelo menos dois ambientes: um para produção, outro para desenvolvimento/testes e que eles não tenham outras aplicações.

A Lecom não se responsabiliza por falhas oriundas da utilização em ambientes fora das especificações abaixo.

1.1 Software

É muito importante estar atento aos softwares requeridos, bem como suas respectivas versões:

- Apache Tomcat versão 9.0.89 ou superior;
- OpenJDK versão 12.0.2 ou superior;
- LibreOffice versão 5.0 ou 5.0.2;
- NodeJS versão 12;
- PM2 na sua última versão estável;
- Redis na sua última versão estável (versão 7);
- Docker e Docker Compose;
- RabbitMQ 3 ou superior;
- Git na sua última versão estável;

1.1.1 Software Configurações mínimas

Fatores externos como volume de dados transferidos, simultaneidade de acessos e duração de execução de atividades levarão à necessidade de ampliação destas configurações.

Servidor dedicado de Aplicação:

- Processador 2 vCPU ou superior;
- 11 Gb RAM; *

- Disco Rígido SATA 100 GB;
 - * A quantidade de memória informada deve estar disponível integralmente para ser configurada no Tomcat e demais serviços da plataforma. Assim, o servidor deve ter mais do que a memória solicitada, pois o Sistema Operacional e outras aplicações também demandarão memória.

Servidor dedicado de Banco de Dados:

- Processador 2 vCPU ou superior;
- 8 Gb RAM; *
- Disco Rígido SATA 100 GB;

* Adequar estas configurações mínimas de acordo com os pré-requisitos de cada versão de SGBD suportado pela nossa plataforma.

Servidor dedicado de proxy:

- Processador 1 vCPU ou superior;
- 1 Gb RAM; *
- Disco Rígido SATA 20 GB;

* Adequar estas configurações mínimas de acordo com as requisições do ambiente.

1.1.2 Docker e Docker-Compose

É necessário ter o Docker e Docker Compose mais atual instalado.

A comunicação do docker deve estar liberada para acessar os mesmos recursos que a máquina hospedeira da plataforma.

Ex: Banco de dados, servidor SMTP, entre outros.

Atenção, quando o serviço do docker for utilizado em ambientes com sistema operacional Windows Server o mesmo precisa ser executado utilizando o WSL ou HyperV e somente é compatível com distribuições Windows server 2019 ou superior.

1.1.3 Servidor de cache Redis

Recomendamos a execução do container servidor de cache junto ao servidor de aplicação conforme Docker-compose padrão.

1.1.4 Servidor RabbitMQ

Recomendamos a execução do container do message broker junto ao servidor de aplicação conforme docker-compose padrão.

1.1.5 Quantidade de arquivos abertos no servidor

Algumas funcionalidades demandam volume adicional de arquivos abertos. O processo do servidor Tomcat deve suportar ao menos 10.240 arquivos abertos. Já os demais serviços da aplicação devem suportar ao menos 4.096 arquivos cada.

1.2 Rede

1.2.1 Comandos de rede

Para funcionar adequadamente o usuário que executa o servidor de aplicação deverá ter acessos a comandos de rede, como por exemplo: ipconfig no ambiente Microsoft, ifconfig em Linux, netstat no FreeBSD e etc.

1.2.2 Resolução DNS

Para o funcionamento adequado da Plataforma Lecom, o arquivo de hosts do ambiente que a plataforma está instalada deve fazer o apontamento do DNS utilizado para o IP da rede interna para que as conexões internas não sejam direcionadas ao proxy reverso.

1.3 Acesso a disco

Os usuários que executarem os serviços da aplicação precisa ter permissão de escrita e leitura nas pastas da **Plataforma Lecom** (e subpastas), no [CATALINA_HOME]/bin, no [STORAGE_HOME] (e

subpastas) e também na pasta USER_HOME onde será criada a pasta lecom na qual todos os produtos da Lecom armazenarão seus arquivos, cada qual em sua pasta.

Além das pastas padrões da plataforma os usuários responsáveis por executar a plataforma devem ter acessos as pastas por ela utilizada. Ex: certificados, storage, hosts, etc

1.4 Acessos externos

É necessário a liberação do acesso:

- Servidor oAuth, é um serviço para padronizar a comunicação segura entre módulos utilizando oAuth2 como protocolo de autenticação. Para isso deve ser liberado a url abaixo:
 - oauth.lecom.com.br
- Servidor DevOps, é um serviço para automatizar a publicação de projetos na Plataforma Lecom. Para isso devem ser liberadas as URLs abaixo nas seguintes portas:
 - repo-service.lecom.com.br (443/HTTPS)
 - lecom-gitlab-srv-prd-01.lecom.com.br (22/TCP)
- onesignal.com no servidor de aplicação, para permitir o envio de notificações através do serviço OneSignal. Após liberado, acessar a URL abaixo para validar se o acesso está liberado:
 - <https://onesignal.com/api/v1/notifications>.
- Serviço Firebase Cloud Messaging, para isso deve ser conferidor o link do fornecedor e fazer toda a liberação informada por ele:
 - <https://firebase.google.com/docs/cloud-messaging/concept-options?hl=pt-br#messaging-ports-and-your-firewall>
- Servidor Sign, é um serviço para realizar a assinatura digital dos documentos na Plataforma Lecom. Para isso deve ser liberado a url abaixo:
 - sign.lecom.com.br
- OpenAPI, é a nossa API para consulta, inclusão, alteração ou exclusão dos dados da Plataforma Lecom, relacionando-se aos Processos, Documentos e Admin. Para isso deve ser liberado a url abaixo:
 - api.lecom.com.br

Precisa estar liberada a comunicação do servidor de aplicação para que ele consiga acessar os serviços abaixo:

1. Endereços utilizados pela aplicação:
 - <https://registry.npmjs.org/pm2>
 - [ftp.us.debian.org](ftp://us.debian.org)
 - <archive.ubuntu.com>
 - <security.ubuntu.com>
2. Caso seja utilizada a autenticação externa do tipo oauth, liberar os endereços conforme o provedor:
 - a. Google
 - i. <https://www.googleapis.com/oauth2/v3/token>
 - ii. <https://accounts.google.com/o/oauth2/auth>
 - iii. <https://www.googleapis.com/userinfo/v2/me>
 - b. Facebook
 - i. https://graph.facebook.com/oauth/access_token
 - <https://www.facebook.com/dialog/oauth>
 - <https://graph.facebook.com/me>
 - c. Github
 - https://github.com/login/oauth/access_token
 - <https://github.com/login/oauth/authorize>
 - <https://api.github.com/user>

1.5 Sistema Operacional

A Plataforma Lecom é homologada para ambiente e sistema operacional de **arquitetura 64 bits**:
Linux – Debian - 64 bits (versão 12 ou superior);

1.6 Gateway / Firewall

Recomendamos a implantação de um servidor de Gateway e Firewall para garantir a proteção dos ambientes.

1.7 Envio de e-mail

É necessário um serviço de envio de e-mail para que a plataforma realize as notificações, com autenticação via SMTP. Além disso, é necessário que esse serviço suporte o volume de utilização.

1.8 Navegadores e resoluções

A ferramenta é estruturada para se adaptar as resoluções de tela do dispositivo que acessar a ferramenta sem perda de funcionalidade. As funcionalidades foram homologadas para os navegadores Google Chrome (versão 105.x), Firefox (versão 104.x) e Edge (versão 104.x).

A compatibilidade com versões superiores dos navegadores homologados será mantida, porém eventuais atualizações dos navegadores exigirão adaptação de produto e demandará a atualização da versão para compatibilidade de uso.

Alguns navegadores possuem modo de compatibilidade e utilizá-lo pode levar a falhas. O uso desta funcionalidade não é recomendado e não suportado pela Plataforma Lecom.

1.9 Banco de dados

1.9.1 Versões homologadas

A **Plataforma Lecom** está homologada para os seguintes bancos de dados:

- Oracle 21c, 19c, 18c, 12c, 11g, e 10g 64bits
- Microsoft SQL Server 2022, 2019, 2017, 2016 e 2014 64bits
- MySQL 8.x 64bits ou superior

Tanto a **Plataforma Lecom** quanto os robôs e integrações utilizam driver JDBC para acesso a banco de dados. Estes drivers são disponibilizados junto com o produto.

Somente Robôs, integrações e campos configurados como retorno de select podem acessar outros servidores de bancos de dados relacionais (SGBD) que não estão na lista de SGBD homologados pela Lecom, desde que estes possuam driver JDBC.

Importante:

- O SGBD (Serviço Gerenciador de Banco de dados) deve estar configurado como case insensitive. Entendemos que no BD Oracle, é criado com o padrão como case Sensitive,

porém reforçamos que a estrutura dos dados, ou seja, o nome da tabela, precisa ser case insensitive. No caso os dados, podem ficar da maneira que o cliente preferir desde que ele entenda que será esse funcionamento para toda a plataforma, respeitando a configuração aplicada no BD. Outro ponto que reforçamos que na instalação deve ser usado em maiúsculo o nome do usuário.

- O servidor de base de dados e todas as bases necessárias para a implantação devem estar com o mesmo collation.
- Recomendamos que a configuração do servidor de banco de dados seja avaliada por DBA a fim de otimizá-lo para o ambiente de produção e garantir o melhor desempenho.

Em bases Oracle, MySQL e SQL Server o usuário que será usado para conectar na base da Plataforma Lecom deve ter as seguintes permissões: SELECT, ALTER, CREATE, DELETE, DROP, INDEX, INSERT, UPDATE, REFERENCES e CREATE TEMPORARY TABLES. E não necessita ser proprietário do database.

Para Oracle: CREATE SEQUENCE e consulta nas tabelas **all_sequences** e **all_synonyms**.

O acesso ao banco de dados para customização, deverá utilizar um usuário específico (BPM_PRD_CUSTOM e BPM_ACT_CUSTOM), este terá somente permissão de leitura nas seguintes tabelas:

- USUARIO
- GRUPO
- GRUPO_USUARIO
- PERM_GRUPO_USUARIO
- DEPTO
- FUNCAO
- FUNCAO_USUARIO
- PERM_FUNCAO_USUARIO

Nas demais tabelas, seguir o permissionamento já citado anteriormente.

1.9.2 Transações

É necessário que as bases de dados permitam controle de transações. Para isto, veja as recomendações abaixo para cada servidor de banco de dados suportado:

Oracle

- Já é configuração padrão, mas é necessário confirmar com o Administrador de

Banco de Dados se a base da Plataforma Lecom aceitará transações.

MS SQL Server

- Já é configuração padrão, mas é necessário confirmar com o Administrador de Banco de Dados se a base da Plataforma Lecom aceitará transações.

MySQL

- É necessário que o motor padrão do MySQL seja o INNObd, para novos clientes a Plataforma Lecom automaticamente criará as tabelas com o tipo padrão. Vale conferir com o Administrador de Banco de Dados se o MySQL de seu ambiente está preparado para este tipo de tabela.

1.9.3 Base dedados

Para utilização da **Plataforma Lecom** é necessário a criação de bases de dados que armazenarão as informações do sistema. O sistema necessita de 7 bases de dados que conterão as informações para o funcionamento de todos os módulos.

Para isto, veja abaixo as recomendações de nomes para criação das bases necessárias:

- BPM_(Ambiente)
- SSO_(Ambiente)
- ECM_(Ambiente)
- SI_(Ambiente)
- SOCIAL_(Ambiente)
- WORKSPACE_(Ambiente)
- AUDIT_(Ambiente)
- BEHAVIOR_(Ambiente)
- JOB_SERVICE_(Ambiente)
- JOB_RUNNER_(Ambiente)

Ambiente se refere ao tipo de ambiente que será utilizado, recomendados:

- ACT - para base de aceite ou homologação
- PRD - para base de produção
- DEV - para base de desenvolvimento

Recomendamos que periodicamente seja executado na base de dados da Plataforma Lecom procedimentos para atualização de estatísticas e reindexação para que as consultas sempre utilizem os melhores planos de execução.

Este procedimento é de responsabilidade do Administrador de Banco de Dados.

1.9.4 Usuários

Recomenda-se a criação de 1 usuário e senha específico para cada base de dados criada.

Os nomes dos usuários devem seguir o seguinte padrão:

- bpm_(Ambiente)
- bpm_(Ambiente)_custom
- sso_(Ambiente)
- ecm_(Ambiente)
- si_(Ambiente)
- social_(Ambiente)
- workspace_(Ambiente)
- audit_(Ambiente)
- bahavior_(Ambiente)

Ambiente se refere ao tipo de ambiente que será utilizado, recomendados:

- act - para base de aceite ou homologação
- prd - para base de produção
- qa - para base de qualidade

1.9.5 Limites de conexão

A **Plataforma Lecom** possui uma configuração padrão para conexões com bancos de dados, conforme tabela abaixo, porém estes valores podem ser adequados de acordo com a necessidade do ambiente e o limite dos bancos de dados utilizados.

Pools de Conexão para Customizações

Tipo	Quem utiliza	Mínimo de Conexões	Máximo de Conexões
Pool para conexões via JDBC	Robôs, integrações e querys de campos configurados como resultado de select	1 conexão para cada properties que estiverem cadastrados na Plataforma Lecom	20 conexões para cada properties que estiverem cadastrados na Plataforma Lecom

Caso haja a necessidade de aumentar/ diminuir os números mínimos ou máximos de conexões simultâneas é preciso contatar o gerente do projeto na Lecom para que seja avaliada a necessidade e tomadas às ações necessárias.

Atenção: validar a comunicação do servidor de aplicação com o servidor de banco de dado.

1.9.6 Collation

Antes de iniciar, garanta que o servidor de base de dados e todas as bases necessárias para a implantação estejam com o mesmo collation. Do contrário a implantação não poderá ser realizada.

2. Preparação do ambiente

2.1 Usuário de sistema

É necessário criar o usuário acesso_jenkins, que é utilizado pelo gitlab-service para acessar a máquina do BPM.

2.1.1 Criação do usuário e chave de acesso

É necessário criar a pasta /opt/lecom/temp/pacotes/ e atribuir permissão de leitura e escrita ao usuário acesso_jenkins.

Esta pasta será utilizada pelo gitlab-service para transferir para esta máquina o pacote gerado pelo processo de publicação do devops.

Executar os comandos a seguir para criação da chave de acesso do usuário acesso_jenkins:

```
adduser acesso_jenkins  
sudo su - acesso_jenkins  
ssh-keygen  
cd /home/acesso_jenkins/.ssh  
cp id_rsa acesso_jenkins.pem  
touch authorized_keys  
chmod 600 authorized_keys  
cat id_rsa.pub >> .ssh/authorized_keys
```

IMPORTANTE:

Caso o ambiente utilize o SO Debian em uma versão superior ou igual a 12, será necessário habilitar o tipo de autenticação RSA.

Para isso, basta seguir os passos:

1. No arquivo sshd_config localizado no path /etc/ssh/, adicionar o seguinte trecho:

```
PubkeyAcceptedAlgorithms +ssh-rsa
```

2. Após aplicar essa alteração, executar o comando de reinicialização do serviço de autenticação

```
sudo systemctl restart sshd
```

No caso de um ambiente em cluster, deve ser replicada a mesma chave em todos os nós para que a chave cadastrada seja compatível com todos os nós.

POSSÍVEL PROBLEMA: Caso esteja sendo utilizada uma versão mais recente do OpenSSH (7.8+), a chave gerada pelo comando “ssh-keygen” terá por padrão o formato mais recente, que inicia com:

```
----BEGIN OPENSSH PRIVATE KEY----
```

Isso ocasionará um erro na utilização da chave pelo gitlab-service, pois as dependências utilizadas atualmente são compatíveis apenas com o formato anterior, que inicia com:

```
----BEGIN RSA PRIVATE KEY----
```

Para evitar que isso ocorra, ao invés de utilizar o comando “ssh-keygen”, utilizar o comando:

```
ssh-keygen -t rsa -m PEM
```

É necessário também criar o usuário para rodar o tomcat_app com acesso limitado:

```
groupadd -r tomcat_app  
useradd tomcat -r -g tomcat_app -s /bin/false
```

Caso o ambiente esteja com SSL habilitado, necessário conceder acesso também aos certificados:

```
setfacl -m "u:tomcat:r-x" /opt/lecom/certificados/
```

Execute os comandos abaixo para criar a pasta para transferência das aplicações externas:

```
mkdir /opt/lecom/temp/  
mkdir /opt/lecom/temp/pacotes/  
  
# Atribuir permissão no diretório pacotes  
setfacl -m "u:acesso_jenkins:rwx" /opt/lecom/temp/pacotes/
```

2.1.2 Permissões do usuário

Adicione as configurações abaixo no arquivo sudoers:

```
# PERMISSÕES CUSTOMIZADAS
acesso_jenkins ALL=NOPASSWD: /bin/rm -rf /opt/lecom/app/tomcat_app/webapps/*, /bin/rm
/opt/lecom/temp/pacotes/*.jar, /usr/bin/unzip /opt/lecom/temp/pacotes/*.jar -d /opt/lecom/app/tomcat_app/webapps/*
/opt/lecom/app/tomcat_app/logs/*, /bin/systemctl status lecom_app-service, /bin/systemctl start lecom_app-service,
/bin/systemctl stop lecom_app-service
```

2.2 LibreOffice

Para correta execução do sistema é necessário que o LibreOffice esteja instalado no servidor, caso ele não esteja instalado faça a instalação antes de prosseguir com a instalação.

2.3 NodeJS

É necessário que possua o NodeJS instalado no servidor de aplicação. Caso não tenha, siga os passos abaixo para efetuar a instalação:

- *apt install curl*
- *curl -sL https://deb.nodesource.com/setup_x.x | bash -* obs. Verificar a versão conforme o item 2.1
- *apt-get install -y nodejs*
- *npm install pm2 -g*

2.4 PhantomJS

Se houver formulário antigo: Em **[USER_HOME]** crie a pasta renderserver e nela copie o executável do **PhantomJS** que se adeque ao Sistema Operacional.

Neste caso, para realizar a instalação, no terminal (ou linha de comando) execute os seguintes comandos:

- *wget http://security.ubuntu.com/ubuntu/pool/main/libp/libpng/libpng12-0_1.2.54-1ubuntu1.1_amd64.deb*
- *dpkg -i libpng12-0_1.2.50-2+deb8u3_amd64.deb*
- *wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl1.0/libssl1.0.0_1.0.2n-1ubuntu5_amd64.deb*
- *dpkg -i libssl1.0.0_1.0.2n-1ubuntu5_amd64.deb*
- *wget http://security.ubuntu.com/ubuntu/pool/main/i/icu/libicu52_52.1-1_amd64.deb*

3_amd64.deb

- dpkg -i libicu52_52.1-3_amd64.deb
- apt-get -f install

OBS: Os comandos iniciados por “wget”, realizam o download das dependências, já os iniciados por “dpkg”, realizam a instalação dessas dependências.

2.5 Proxy reverso

É necessário que o proxy reverso configurado para a aplicação possua a definição de redirecionamento configurada conforme tabela abaixo:

Contexto	Host
/admin/api	https://192.168.1.2:8181/admin/api
/ecmcore/api	https://192.168.1.2:8181/ecmcore/api
^/bpm/api/v(.*)/process-instances/(.*)/activity-instances/(.*)/cycles/(.*)/fields/(.*)/documents/import	https://192.168.1.2
^/bpm/api/v(.*)/process-instances/(.*)/activity-instances/(.*)/cycles/(.*)/documents/files/(.*)/download	https://192.168.1.2
/bpm/api	https://192.168.1.2:8181/bpm/api
/bpm	https://192.168.1.2/bpm
/sso	https://192.168.1.2/sso
/ecmcore	https://192.168.1.2/ecmcore
/core/websocket	wss://192.168.1.2/core/websocket
/bpm/calcularEtapasRestantesExportacao	wss://192.168.1.2/bpm/calcularEtapasRestantesExportacao
/form-app	https://192.168.1.2:8080/form-app
/behavior-web	https://192.168.1.2:3002/behavior-web
/gateway	https://192.168.1.2:8181/gateway
/workspace	https://192.168.1.2:3000/workspace
/form-web	https://192.168.1.2:3001/form-web
/social-service/websocket	wss://192.168.1.2:443/social-service/websocket
/social-service	https://192.168.1.2:443/social-service
/discovery	https://192.168.1.2:8761/
/eureka	https://192.168.1.2:8761/eureka

/app-ext	https://192.168.1.2:8443/
/job-web	https://192.168.1.2:3003/job-web
/	https://192.168.1.2/

No Apache para que os direcionamentos funcionem corretamente, precisamos dos módulos ativos:

- headers
- proxy
- proxy_http
- proxy_wstunnel
- rewrite

Quando a plataforma estiver em cluster é necessário a configuração dos módulos abaixo para comunicação entre os nós

- lbmethod_byrequests
- proxy_balancer

Para configuração do módulo “Cadastro Fácil”, é necessário que no proxy reverso seja configurado o redirecionamento para a página dessa respectiva ferramenta.

```
ProxyPass /external/cadastros !
Redirect /external/cadastros https://www.lecom.com.br/cadastrofacil
```

Para configuração do módulo “RPA”, é necessário que no proxy reverso seja configurado o redirecionamento para a página dessa respectiva ferramenta.

```
ProxyPass /external/roberty !
Redirect /external/roberty https://www.lecom.com.br/rpa-ia
```

Atenção: no Apêndice A é possível ver a definição do arquivo de V-HOST.

3. Implantando a plataforma no Linux

3.1 Profiles da aplicação

Para simplificar o setup da aplicação a Plataforma Lecom trabalha com profiles de configuração que é definido na variável `SPRING_PROFILES_ACTIVE`. Veja abaixo quais são os profiles disponíveis.

3.1.1 Tipos de ambientes

Profile	Descrição
production	Sempre utilizar esse profile, exceto quando for ambiente de desenvolvimento
development	Utilizado apenas pelo time de desenvolvimento da Lecom

3.1.2 Sistemas operacionais

Profile	Descrição
linux	Indica que o sistema operacional onde a aplicação será instalada é Linux
windows	Indica que o sistema operacional onde a aplicação será instalada é Windows

3.1.1 SGBD

Profile	Descrição
mysql	Indica que a base de dados que será configurada na aplicação é MySQL
mssql	Indica que a base de dados que será configurada na aplicação é Microsoft SQL Server
oracle	Indica que a base de dados que será configurada na aplicação é Oracle

3.1.1 Proxy e SSL

Profile	Descrição
proxy_ssl	Define a configuração de comunicação como segura (SSL) e habilita a aplicação para trabalhar com proxy reverso
proxy	Define a configuração de comunicação como não segura (sem SSL) e habilita a aplicação para trabalhar com proxy reverso

Atenção: caso nenhum dos profiles acima seja exportado, a aplicação trabalhará no padrão de comunicação não segura (sem SSL) e sem proxy reverso, modo o qual não atende os requisitos.

3.2 Estrutura de pastas dos serviços

Para iniciar a instalação da aplicação, a estrutura de pastas abaixo deverá ser criada:

- /opt/lecom/java
- /opt/lecoom/storage
- /opt/lecom/certificados
- /opt/lecom/app/microservices/config-service
- /opt/lecom/app/microservices/discovery-service
- /opt/lecom/app/microservices/form-app
- /opt/lecom/app/microservices/form-service
- /opt/lecom/app/microservices/gateway-service
- /opt/lecom/app/microservices/node-web-server
- /opt/lecom/app/microservices/service-integration
- /opt/lecom/app/microservices/audit-service
- /opt/lecom/app/microservices/behavior-service
- /opt/lecom/app/microservices/logs
- /opt/lecom/app/microservices/envs
- /opt/lecom/app/job_compose
- /opt/lecom/app/tomcat_producao
- /opt/lecom/app/tomcat_app
- /opt/lecom/temp/pacotes

3.3 Configurando os serviços

3.3.1 Movendo os serviços para suas pastas

Ao receber o pacote para implantação da Lecom, mova o mesmo para a pasta:

- `/opt/lecom/temp/pacotes`

Após movê-lo, extraia o arquivo **microservicos.zip** na mesma pasta.

Em seguida, mova os serviços para suas devidas pastas. Para isso, acesse a pasta `/opt/lecom/temp/pacotes/microservicos` e mova os arquivos de extensão **.jar** para as devidas pastas conforme a lista abaixo:

- audit-service.jar -> `/opt/lecom/app/microservices/audit-service/`
- behavior-service.jar -> `/opt/lecom/app/microservices/behavior-service/`
- config-service.jar -> `/opt/lecom/app/microservices/config-service/`
- config-repo -> `/opt/lecom/app/microservices/config-service/`
- discovery-service.jar -> `/opt/lecom/app/microservices/discovery-service/`
- form-app.jar -> `/opt/lecom/app/microservices/form-app/`
- form-service.jar -> `/opt/lecom/app/microservices/form-service/`
- gateway-service.jar -> `/opt/lecom/app/microservices/gateway-service/`
- service-integration.jar -> `/opt/lecom/app/microservices/service-integration/`
- docker-compose -> `/opt/lecom/app/docker-compose/`

Após mover os arquivos **.jar** corretamente é necessário dar permissão de execução para eles.

Por último, será necessário mover os arquivos do serviço *node-web-server* para a pasta:

- `/opt/lecom/app/microservices/node-web-server/`

3.3.2 Definindo as variáveis de ambiente

Dentro da pasta `/opt/lecom/app/microservices/envs` é necessário criar os arquivos *abaixo* e *cada um* contendo a configuração especificada.

- `00-profile.conf`

O arquivo deverá conter o seguinte conteúdo:

```
SPRING_PROFILES_ACTIVE=production,linux,mysql,proxy_ssl  
HOST_NAME=plataforma.meudominio.com.br  
ACCESS_CONTROL_ALLOW_ORIGIN=""
```

- Variável ACCESS_CONTROL_ALLOW_ORIGIN deve estar vazia;
 - **Exemplo:** ACCESS_CONTROL_ALLOW_ORIGIN = "".
- Porém, quando o cliente possuir outras aplicações, em domínios diferentes, que precisem acessar a Plataforma Lecom via navegador, será necessário, também, declarar, além do outro domínio, o próprio domínio da plataforma.
 - **Exemplo:** ACCESS_CONTROL_ALLOW_ORIGIN =
<http://outro.dominio.com.br>,<https://dominio.plataforma.com.br>
- Os profiles da aplicação dependem de cada perfil de instalação.
- 00-ssl.conf

O arquivo deverá conter o seguinte conteúdo:

```
SSL_KEY_STORE=/opt/lecom/certificados/app.meudominio.com.br.jks  
SSL_KEY_STORE_PASSWORD=SENHA  
SSL_KEY_ALIAS= app.meudominio.com.br
```

Onde:

- SSL_KEY_STORE – Informar o caminho do certificado.jks;
- SSL_KEY_STORE_PASSWORD – Informar a senha;
- SSL_KEY_ALIAS – Informar o alias do certificado.

Obs: caso o ambiente não possua SSL, o que não é recomendado, o profile de ssl não deve ser definido e não será necessário alterar as variáveis acima.

- 01-config-service.conf

O arquivo deverá conter o seguinte conteúdo:

```
CONFIG_HOME=/opt/lecom/app/microservices/config-service/config-repo
```

- 01-form-app.conf

O arquivo deverá conter o seguinte conteúdo:

```
FORM_APP_OAUTH2_CLIENT_SECRET= Colocar a chave de autenticação
```

- 01-form-service.conf

O arquivo deverá conter o seguinte conteúdo:

```
FORM_SERVICE_OAUTH2_CLIENT_SECRET= Colocar a chave de autenticação
```

- 01-service-integration.conf

O arquivo deverá conter o seguinte conteúdo:

Configuração específica por tipo banco de dados:

```
SERVICE_INTEGRATION_OAUTH2_CLIENT_SECRET= Informar a chave de autenticação
```

Banco de dados Oracle

```
SERVICE_INTEGRATION_DATASOURCE_URL="jdbc:oracle:thin:@HOST:PORT/SID"
SERVICE_INTEGRATION_DATASOURCE_SCHEMA=schema
SERVICE_INTEGRATION_DATASOURCE_USERNAME=user
SERVICE_INTEGRATION_DATASOURCE_PASSWORD=password
```

Banco de dados MSSQL

```
SERVICE_INTEGRATION_DATASOURCE_URL="jdbc:sqlserver://HOST\INSTANCE;databaseName=BD_NAME;
trustServerCertificate=true"
SERVICE_INTEGRATION_DATASOURCE_SCHEMA=dbo
SERVICE_INTEGRATION_DATASOURCE_USERNAME=user
SERVICE_INTEGRATION_DATASOURCE_PASSWORD=password
```

Banco de dados Mysql

```
SERVICE_INTEGRATION_DATASOURCE_URL="jdbc:mysql://HOST:PORT/DB_NAME"
SERVICE_INTEGRATION_DATASOURCE_USERNAME=user
SERVICE_INTEGRATION_DATASOURCE_PASSWORD=password
```

- 01-audit-service.conf

O arquivo deverá conter o seguinte conteúdo:

```
AUDIT_SERVICE_OAUTH2_CLIENT_SECRET= Informar a chave de autenticação
```

Configuração específica por tipo banco de dados:

Banco de dados Oracle

```
AUDIT_SERVICE_DATASOURCE_URL= "jdbc:oracle:thin:USER/PASSWORD@//HOST:PORT:SID"
AUDIT_SERVICE_DATASOURCE_SCHEMA=schema
AUDIT_SERVICE_DATASOURCE_USERNAME=user
AUDIT_SERVICE_DATASOURCE_PASSWORD=password
```

Observação 1, não utilizar @ na senha do BD, para não confundir com o fim do parâmetro.

Observação 2, apenas utilizar a variável AUDIT_SERVICE_DATASOURCE_SCHEMA, caso o usuário utilize um schema diferente do padrão do banco.

Banco de dados MSSQL

```
AUDIT_SERVICE_DATASOURCE_URL=
jdbc:sqlserver://HOST\INSTANCE;databaseName=BD_NAME;trustServerCertificate=true"
```

```
AUDIT_SERVICE_DATASOURCE_SCHEMA=dbo  
AUDIT_SERVICE_DATASOURCE_USERNAME=user  
AUDIT_SERVICE_DATASOURCE_PASSWORD=password
```

Banco de dados Mysql

```
AUDIT_SERVICE_DATASOURCE_URL="jdbc:mysql://HOST:PORT/DB_NAME"  
AUDIT_SERVICE_DATASOURCE_USERNAME=user  
AUDIT_SERVICE_DATASOURCE_PASSWORD=password
```

- 01-behavior-service.conf

O arquivo deverá conter o seguinte conteúdo:

```
BEHAVIOR_SERVICE_OAUTH2_CLIENT_SECRET= Informar a chave de autenticação  
SPRING_REDIS_HOST=HOST  
SPRING_REDIS_PORT=6379  
SPRING_REDIS_USERNAME=user  
SPRING_REDIS_PASSWORD=password  
SPRING_REDIS_SSL=false  
SPRING_REDIS_DATABASE=0
```

Onde:

- SPRING_REDIS_DATABASE – Deve ser informado o número 0 (zero) para ambiente do tipo aceite e número 8 (oito) para ambiente de produção

Configuração específica por tipo banco de dados:

Banco de dados Oracle

```
BEHAVIOR-SERVICE_DATASOURCE_URL= "jdbc:oracle:thin:USER/PASSWORD@//HOST:PORT:SID"  
BEHAVIOR -SERVICE_DATASOURCE_SCHEMA=schema  
BEHAVIOR -SERVICE_DATASOURCE_USERNAME=user  
BEHAVIOR -SERVICE_DATASOURCE_PASSWORD=password
```

Observação, não utilizar @ na senha do BD, para não confundir com o fim do parâmetro.

Banco de dados MSSQL

```
BEHAVIOR -SERVICE_DATASOURCE_URL= "  
jdbc:sqlserver://HOST\INSTANCE;databaseName=BD_NAME;trustServerCertificate=true"  
BEHAVIOR -SERVICE_DATASOURCE_SCHEMA=dbo  
BEHAVIOR -SERVICE_DATASOURCE_USERNAME=user  
BEHAVIOR -SERVICE_DATASOURCE_PASSWORD=password
```

Banco de dados Mysql

```
BEHAVIOR -SERVICE_DATASOURCE_URL="jdbc:mysql://HOST:PORT/DB_NAME"  
BEHAVIOR -SERVICE_DATASOURCE_USERNAME=user  
BEHAVIOR -SERVICE_DATASOURCE_PASSWORD=password
```

- 01-node-web-server.conf

O arquivo deverá conter o seguinte conteúdo:

```
PM2_HOME=/opt/lecom/app/microservices/node-web-server/.pm2  
PIDFile=/opt/lecom/app/microservices/node-web-server/.pm2/pm2.pid
```

- 01-gateway-service.conf

O arquivo deverá ficar em branco para caso futuramente precise de alguma configuração customizada.

- 01-discovery-service.conf

O arquivo deverá ficar em branco para caso futuramente precise de alguma configuração customizada.

Dentro da pasta `/opt/lecom/app/microservices/node-web-server` é necessário editar os arquivos abaixo para adequar suas configurações de acordo com o ambiente.

- `node-web-server.config`

```
module.exports = {
  apps : [
    {
      name: "workspace-web",
      script: "./workspace-server/server.js",
      env: {
        "SERVICE_NAME": "workspace-web-server",
        "CONTEXT_PATH": "/workspace",
        "SERVER_PORT": "3000"
      }
    },
    {
      name: 'form-web',
      script: './form-web/server/server.js',
      env: {
        "SERVICE_NAME": "form-web-server",
        "SERVER_PORT": "3001",
        "CONTEXT_PATH": "/form-web",
        "GATEWAY_URL": "https://localhost:8181/",
        "LECOM_BPM_URL": "https://localhost:8444/"
      }
    },
    {
      name: 'behavior-web',
      script: './behavior-web/server/server.js',
      env: {
        "SERVICE_NAME": "behavior-web-server",
        "SERVER_PORT": "3002",
        "CONTEXT_PATH": "/behavior-web"
      }
    },
    {
      name: 'job-web',
      script: './job-web/server/server.js',
      env: {
        "SERVICE_NAME": "job-web-server",
        "SERVER_PORT": "3003",
        "CONTEXT_PATH": "/job-web"
      }
    }
  ]
}
```

Onde:

- CONTEXT_PATH – Informar o contexto mapeado no proxy reverso, geralmente o contexto leva o mesmo nome do módulo configurado iniciado pelo caracter '/'
- node-web-server.config

```
NODE_ENV=production
HOST_NAME=localhost
NODE_EXTRA_CA_CERTS=
NODE_KEY=
SSL_ENABLED=false
NODE_TLS_REJECT_UNAUTHORIZED=0
SERVER_TIMEOUT=1440
TZ=America/Sao_Paulo
X_Frame_Options=
X_Content_Type_Options=nosniff
X_XSS_Protection=1;mode=block
Access_Control_Allow_Origin=*
Access_Control_Allow_Methods=GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, TRACE, PATCH
Access_Control_Allow_Headers=Content-Type,X-Requested-With,accept,Origin,Access-Control-Request-Method,Access-Control-Request-Headers,test-mode,ticket-sso,test-user,Cache-Control,form-uuid,language,pragma,application,Referer,sec-ch-ua,sec-ch-ua-mobile
Access_Control_Expose_Headers=*
Access_Control_Max_Age=86400
Access_Control_Allow_Credentials=true
Strict_Transport_Security=max-age=31536000;includeSubDomains
```

Onde:

- HOST_NAME – Informar o domínio do ambiente
- NODE_EXTRA_CA_CERTS – Informar o arquivo CA da chave SSL do ambiente se esse for o caso
- NODE_KEY – Informar o arquivo de chave SSL se esse for o caso
- SSL_ENABLED – Definir para true caso esteja com ssl ou false para inativo

3.3.3 Config-service

Para definir as configurações do config-service será necessário criar o arquivo /opt/lecom/app/microservices/config-service/config-service.conf e dentro do arquivo deve conter as seguintes informações:

```
JAVA_HOME=/opt/lecom/java
JAVA_OPTS="-server -Xmx64m -XX:+UseConcMarkSweepGC"
RUN_ARGS="--logging.file.name=/opt/lecom/app/microservices/logs/lecom_config-service.log"
```

Para definir o registro do serviço no sistema será necessário criar o arquivo /opt/lecom/app/microservices/config-service/lecom_config-service.service e dentro do arquivo deve

conter as seguintes informações:

```
[Unit]
Description=lecom_config-service
[Service]
EnvironmentFile=/opt/lecom/app/microservices/envs/00-ssl.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/00-profile.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/01-config-service.conf
ExecStart=/opt/lecom/app/microservices/config-service/config-service.jar
[Install]
WantedBy=multi-user.target
```

Para registrar o serviço será necessário executar os comandos abaixo informando o arquivo service:

```
systemctl link /opt/lecom/app/microservices/config-service/lecom_config-service.service
systemctl enable lecom_config-service.service
```

3.3.4 Discovery-service

Para definir as configurações do discovery-service será necessário criar o arquivo /opt/lecom/app/microservices/discovery-service/discovery-service.conf e dentro do arquivo deve conter as seguintes informações:

```
JAVA_HOME= /opt/lecom/java
JAVA_OPTS= "-server -Xmx128m -XX:+UseConcMarkSweepGC"
RUN_ARGS="--logging.file.name=/opt/lecom/app/microservices/logs/lecom_discovery-service.log"
```

Para definir o registro do serviço no sistema será necessário criar o arquivo /opt/lecom/app/microservices/config-service/lecom_config-service.service e dentro do arquivo deve conter as seguintes informações:

```
[Unit]
Description=lecom_discovery-service
[Service]
ExecStartPre=/bin/sleep 15
EnvironmentFile=/opt/lecom/app/microservices/envs/00-ssl.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/00-profile.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/01-discovery-service.conf
ExecStart=/opt/lecom/app/microservices/discovery-service/discovery-service.jar
[Install]
WantedBy=multi-user.target
```

Para registrar o serviço será necessário executar os comandos abaixo informando o arquivo service:

```
systemctl link /opt/lecom/app/microservices/discovery-service/lecom_discovery-service.service
systemctl enable lecom_discovery-service.service
```

3.3.5 Gateway-service

Para definir as configurações do gateway-service será necessário criar o arquivo `/opt/lecom/app/microservices/gateway-service/gateway-service.conf` e dentro do arquivo deve conter as seguintes informações:

```
JAVA_HOME= /opt/lecom/java
JAVA_OPTS= "-server -Xmx128m -XX:+UseConcMarkSweepGC"
RUN_ARGS="--logging.file.name=/opt/lecom/app/microservices/logs/lecom_gateway-service.log"
```

Para definir o registro do serviço no sistema será necessário criar o arquivo `/opt/lecom/app/microservices/config-service/lecom_gateway-service.service` e dentro do arquivo deve conter as seguintes informações:

```
[Unit]
Description=lecom_gateway-service
[Service]
ExecStartPre=/bin/sleep 15
EnvironmentFile=/opt/lecom/app/microservices/envs/00-ssl.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/00-profile.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/01-gateway-service.conf
ExecStart=/opt/lecom/app/microservices/gateway-service/gateway-service.jar
[Install]
WantedBy=multi-user.target
```

Para registrar o serviço será necessário executar os comandos abaixo informando o arquivo service:

```
systemctl link /opt/lecom/app/microservices/gateway-service/lecom_gateway-service.service
systemctl enable lecom_gateway-service.service
```

3.3.6 Form-App

Para definir as configurações do form-app será necessário criar o arquivo `/opt/lecom/app/microservices/form-app/form-app.conf` e dentro do arquivo deve conter as seguintes informações:

```
JAVA_HOME= /opt/lecom/java
JAVA_OPTS= "-server -Xmx256m -XX:+UseConcMarkSweepGC"
RUN_ARGS="--logging.file.name=/opt/lecom/app/microservices/logs/lecom_form-app.log"
```

Para definir o registro do serviço no sistema será necessário criar o arquivo `/opt/lecom/app/microservices/form-app/lecom_form-app.service` e dentro do arquivo deve conter as seguintes informações:

```
[Unit]
Description=lecom_form-app
[Service]
ExecStartPre=/bin/sleep 15
EnvironmentFile=/opt/lecom/app/microservices/envs/00-ssl.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/00-profile.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/01-form-app.conf
```

```
ExecStart=/opt/lecom/app/microservices/form-app/form-app.jar
[Install]
WantedBy=multi-user.target
```

Para registrar o serviço será necessário executar os comandos abaixo informando o arquivo service:

```
systemctl link /opt/lecom/app/microservices/form-app/lecom_form-app.service
systemctl enable lecom_form-app.service
```

3.3.7 Form-service

Para definir as configurações do form-service será necessário criar o arquivo

/opt/lecom/app/microservices/form-service/form-service.conf e dentro do arquivo deve conter as seguintes informações:

```
JAVA_HOME= /opt/lecom/java
JAVA_OPTS= "-server -Xmx256m -XX:+UseConcMarkSweepGC"
RUN_ARGS="--logging.file.name=/opt/lecom/app/microservices/logs/lecom_form-service.log"
```

Para definir o registro do serviço no sistema será necessário criar o arquivo /opt/lecom/app/microservices/form-service/lecom_form-service.service e dentro do arquivo deve conter as seguintes informações:

```
[Unit]
Description=lecom_form-service

[Service]
ExecStartPre=/bin/sleep 15
EnvironmentFile=/opt/lecom/app/microservices/envs/00-ssl.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/00-profile.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/01-form-service.conf
ExecStart=/opt/lecom/app/microservices/form-service/form-service.jar
[Install]
WantedBy=multi-user.target
```

Para registrar o serviço será necessário executar os comandos abaixo informando o arquivo service:

```
systemctl link /opt/lecom/app/microservices/form-service/lecom_form-service.service
systemctl enable lecom_form-service.service
```

3.3.8 Service integration

Para definir as configurações do service-integration será necessário criar o arquivo /opt/lecom/app/microservices/service-integration/service-integration.conf e dentro do arquivo deve conter as seguintes informações:

```
JAVA_HOME= /opt/lecom/java
JAVA_OPTS= "-server -Xmx256m -XX:+UseConcMarkSweepGC"
```

```
RUN_ARGS="--logging.file.name=/opt/lecom/app/microservices/logs/lecom_service-integration.log"
```

Para definir o registro do serviço no sistema será necessário criar o arquivo `/opt/lecom/app/microservices/service-integration/lecom_service-integration.service` e dentro do arquivo deve conter as seguintes informações:

```
[Unit]
Description=lecom_service-integration
[Service]
ExecStartPre=/bin/sleep 15
EnvironmentFile=/opt/lecom/app/microservices/envs/00-ssl.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/00-profile.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/01-service-integration.conf
ExecStart=/opt/lecom/app/microservices/service-integration/service-integration.jar
[Install]
WantedBy=multi-user.target
```

Para registrar o serviço será necessário executar os comandos abaixo informando o arquivo service:

```
systemctl link /opt/lecom/app/microservices/service-integration/lecom_service-integration.service
systemctl enable lecom_service-integration.service
```

3.3.9 Audit service

Para definir as configurações do audit-service será necessário criar o arquivo `/opt/lecom/app/microservices/audit-service/audit-service.conf` e dentro do arquivo deve conter as seguintes informações:

```
JAVA_HOME= /opt/lecom/java
JAVA_OPTS= "-server -Xmx256m -XX:+UseConcMarkSweepGC"
RUN_ARGS="--logging.file.name=/opt/lecom/app/microservices/logs/lecom_audit-service.log"
```

Para definir o registro do serviço no sistema será necessário criar o arquivo `/opt/lecom/app/microservices/audit-service/lecom_audit-service.service` e dentro do arquivo deve conter as seguintes informações:

```
[Unit]
Description=lecom_audit-service
[Service]
ExecStartPre=/bin/sleep 15
EnvironmentFile=/opt/lecom/app/microservices/envs/00-ssl.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/00-profile.conf
EnvironmentFile=/opt/lecom/app/microservices/envs/01-audit-service.conf
ExecStart=/opt/lecom/app/microservices/audit-service/audit-service.jar
[Install]
WantedBy=multi-user.target
```

Para registrar o serviço será necessário executar os comandos abaixo informando o arquivo service:

```
systemctl link /opt/lecom/app/microservices/audit-service/lecom_audit-service.service  
systemctl enable lecom_audit-service.service
```

3.3.10 Behavior service

Para definir as configurações do behavior-service será necessário criar o arquivo /opt/lecom/app/microservices/behavior-service/behavior-service.conf e dentro do arquivo deve conter as seguintes informações:

```
JAVA_HOME=/opt/lecom/java  
JAVA_OPTS="-server -Xmx256m -XX:+UseConcMarkSweepGC"  
RUN_ARGS="--logging.file.name=/opt/lecom/app/microservices/logs/lecom_behavior-service.log"
```

Para definir o registro do serviço no sistema será necessário criar o arquivo /opt/lecom/app/microservices/behavior-service/lecom_behavior-service.service e dentro do arquivo deve conter as seguintes informações:

```
[Unit]  
Description=lecom_behavior-service  
[Service]  
ExecStartPre=/bin/sleep 15  
EnvironmentFile=/opt/lecom/app/microservices/envs/00-ssl.conf  
EnvironmentFile=/opt/lecom/app/microservices/envs/00-profile.conf  
EnvironmentFile=/opt/lecom/app/microservices/envs/01-behavior-service.conf  
ExecStart=/opt/lecom/app/microservices/behavior-service/behavior-service.jar  
[Install]  
WantedBy=multi-user.target
```

Para registrar o serviço será necessário executar os comandos abaixo informando o arquivo service:

```
systemctl link /opt/lecom/app/microservices/behavior-service/lecom_behavior-service.service  
systemctl enable lecom_behavior-service.service
```

3.3.11 Docker-compose

Para definir as variáveis de ambiente do docker-compose será necessário editar os arquivos presentes na pasta /opt/lecom/app/ docker-compose/envs/

Atenção antes de editar o arquivo considere as cores abaixo como guia do que deve ser editado ou não:

- Modificar o conteúdo em **rosa** de acordo com as configurações do cliente;

- Modificar o conteúdo em **verde** quando for necessário editar uma configuração padrão;
- Conteúdo em **preto** não deve ser editado pois é a estrutura base necessária.

• **lecom-services-default.env**

Este arquivo controla variáveis de projeto que são globais entre todos os serviços da Plataforma Lecom, as alterações feitas nele impactam diretamente nos containers job-service e job-runner.

```
TZ=America/Sao_Paulo
HOST_NAME=plataforma.dominio.com.br
SPRING_PROFILES_ACTIVE=production,linux,mysql,proxy_ssl
ACCESS_CONTROL_ALLOW_ORIGIN=""
SSL_KEY_STORE=/opt/lecom/certificados/pet.lecom.com.br.jks
SSL_KEY_STORE_PASSWORD=changeit
SSL_KEY_ALIAS=autosing_lecom
nodeName=node01
```

• **job-runner.env**

Este arquivo controla as variáveis específicas do serviço job-runner.

```
JAVA_TOOL_OPTIONS= -Xss200K
JOB_RUNNER_OAUTH2_CLIENT_SECRET= Informar a chave de autenticação
JOB_STORAGE_ROOT=/opt/lecom/storage/job
JOB_RUNNER_DATASOURCE_URL=jdbc:mysql://127.0.0.1:3306/job-runner
JOB_RUNNER_DATASOURCE_USERNAME=user
JOB_RUNNER_DATASOURCE_PASSWORD=password
#- JOB_RUNNER_SCHEMA=dbo
JOB_RUNNER_BROKER_HOST=192.168.1.2
JOB_RUNNER_BROKER_VIRTUAL_HOST=plataforma.dominio.com.br
JOB_RUNNER_BROKER_USERNAME=user
JOB_RUNNER_BROKER_PASSWORD=password
JOB_RUNNER_BROKER_SSL_ENABLED=false
JOB_RUNNER_BROKER_SSL_ALGORITHM=TLSv1.2
JOB_RUNNER_QUARTZ_THREADS=10
```

• **job-service.env**

Este arquivo controla as variáveis específicas do serviço job-runner.

```
JAVA_TOOL_OPTIONS= -Xss200K
JOB_SERVICE_OAUTH2_CLIENT_SECRET= Informar a chave de autenticação
JOB_STORAGE_ROOT=/opt/lecom/storage/job
JOB_SERVICE_DATASOURCE_URL=jdbc:mysql://127.0.0.1:3306/job-runner
JOB_SERVICE_DATASOURCE_USERNAME=user
JOB_SERVICE_DATASOURCE_PASSWORD=password
#- JOB_SERVICE_SCHEMA=dbo
JOB_SERVICE_BROKER_HOST=192.168.1.2
JOB_SERVICE_BROKER_VIRTUAL_HOST=plataforma.dominio.com.br
```

```
JOB_SERVICE_BROKER_USERNAME=user  
JOB_SERVICE_BROKER_PASSWORD=password  
JOB_SERVICE_BROKER_SSL_ENABLED=false  
JOB_SERVICE_BROKER_SSL_ALGORITHM=TLSv1.2
```

- **redis.env**

Este arquivo controla as variáveis específicas do serviço job-runner.

```
PASSWORD_REDIS_USER=MyP@ssW0rd
```

Para definir as configurações específicas de cada serviço como memória e volumes utilizados será necessário editar os arquivos presentes na pasta /opt/lecom/app/ docker-compose/services/

- **job-service.yml**

Este arquivo é responsável pelo mapeamento do serviço job-service com a imagem base e suas definições de variáveis assim como a parametrização de memória máxima utilizada pelo serviço

```
services:  
  job-service:  
    image: repo-registry.lecom.com.br/job-service:TAG  
    container_name: job-service  
    hostname: job-service.local  
    env_file:  
      - ../envs/lecom-services-default.env  
      - ../envs/job-service.env  
    volumes:  
      - /opt/lecom/certificados:/opt/lecom/certificados  
      - /opt/lecom/java/lib/security/cacerts:/layers/paketo-buildpacks_bellsoft-liberica/jre/lib/security/cacerts  
      - /opt/lecom/storage/job:/opt/lecom/storage/jo/  
      - /opt/lecom/app/microservices/logs:/opt/lecom/app/microservices/logs/  
      - /etc/hosts:/etc/hosts  
    ports:  
      - 8084:8084  
    restart: always  
    deploy:  
      resources:  
        limits:  
          memory: 768M  
        reservations:  
          memory: 200M  
    networks:  
      - docker-network
```

- **job-runner.yml**

Este arquivo é responsável pelo mapeamento do serviço job-runner com a imagem base e suas definições de variáveis assim como a parametrização de memória máxima utilizada pelo serviço

```
version: '3'
services:
  job-runner:
    image: repo-registry.lecom.com.br/job-runner
    hostname: job-runner.local
    env_file:
      - ../envs/lecom-services-default.env
      - ../envs/job-runner.env
    volumes:
      - /opt/lecom/certificados:/opt/lecom/certificados
      - /opt/lecom/java/lib/security/cacerts:/layers/paketo-buildpacks_bellsoft-liberica/jre/lib/security/cacerts
      - /opt/lecom/storage/job:/opt/lecom/storage/job
      - /opt/lecom/storage/static-files:/opt/lecom/storage/static-files
      - /opt/lecom/storage/docs:/opt/lecom/storage/docs
      - /opt/lecom/app/microservices/logs:/opt/lecom/app/microservices/logs/
      - /etc/hosts:/etc/hosts
    ports:
      - 8085:8085
    restart: always
    deploy:
      resources:
        limits:
          memory: 1280M
        reservations:
          memory: 200M
    networks:
      - docker-network
```

- **rabbitmq.yml**

Este arquivo é responsável pelo mapeamento do serviço rabbitmq com a imagem base e suas definições de variáveis assim como a parametrização de memória máxima utilizada pelo serviço

```
services:
  rabbitmq:
    container_name: rabbitmq
    hostname: rabbitmq
    restart: always
    build:
      context: "../build"
      dockerfile: "dockerfile.rabbitmq"
    env_file:
      - ../envs/rabbitmq.env
    deploy:
      resources:
```

```

limits:
  memory: 512M
reservations:
  memory: 200M
volumes:
  - ..../volumes/rabbitmq/data/:/var/lib/rabbitmq/
  - ..../volumes/rabbitmq/log/:/var/log/rabbitmq/
ports:
  - 5672:5672
  - 15672:15672
networks:
  - docker-network

```

- **redis.yml**

Este arquivo é responsável pelo mapeamento do serviço redis com a imagem base e suas definições de variáveis assim como a parametrização de memória máxima utilizada pelo serviço

```

services:
  redis:
    container_name: redis
    hostname: redis
    restart: always
    build:
      context: "../build"
      dockerfile: "dockerfile.redis"
    deploy:
      resources:
        limits:
          memory: 512M
        reservations:
          memory: 200M
    ports:
      - '6379:6379'
    command: >
      bash -c "redis-server --save 30 1 --loglevel warning --requirepass $$PASSWORD_REDIS_USER"
    env_file:
      - ../envs/redis.env
    volumes:
      - ..../volumes/redis/data/:/data
    networks:
      - docker-network

```

- **Descrição das variáveis**

Variável	Descrição
TZ	Timezone que deve ser utilizado

HOST_NAME	Host name utilizado pela plataforma
ACCESS_CONTROL_ALLOW_ORIGIN	Autorizações de cors para o serviço
SSL_KEY_STORE	Caminho da keystore
SSL_KEY_STORE_PASSWORD	Senha da keystore
SSL_KEY_ALIAS	Alias da keystore
[MÓDULO]_OAUTH2_CLIENT_SECRET	Chave de autenticação oauth
JOB_STORAGE_ROOT	Caminho da storage do projeto JOB
[MÓDULO]_DATASOURCE_URL	Url jdbc do drive utilizado
[MÓDULO]_DATASOURCE_USERNAME	Usuário do banco de dados
[MÓDULO]_DATASOURCE_PASSWORD	Senha do banco de dados
[MÓDULO]_BROKER_HOST	Host do broker
[MÓDULO]_BROKER_VIRTUAL_HOST	Virtual host do broker
[MÓDULO]_BROKER_USERNAME	Usuário do broker
[MÓDULO]_BROKER_PASSWORD	Senha do broker
[MÓDULO]_BROKER_SSL_ENABLED	Parâmetro para ativar (true) ou inativar (false) o SSL
[MÓDULO]_BROKER_SSL_ALGORITHM	Algoritimo SSL
[MÓDULO]_QUARTZ_THREADS	Quantidade de thread que o executor pode fazer em paralelo
SPRING_PROFILES_ACTIVE	Profiles de configuração
JAVA_TOOL_OPTIONS	Parametrização das options da JVM, pode ser definido valores de memória entre outros.
PASSWORD_REDIS_USER	Define a senha do usuário do redis

3.3.12 Node web server

Para definir o registro do serviço no sistema será necessário criar o arquivo /opt/lecom/app/microservices/node-web-server/lecom_node-web-server.service e dentro do arquivo deve conter as seguintes informações:

```
[Unit]
Description=lecom_node-web-server
After=network.target
```

```
[Service]
```

```

Type=forking
User=root
LimitNOFILE=infinity
LimitNPROC=infinity
LimitCORE=infinity
EnvironmentFile=/opt/lecom/app/microservices/envs/01-node-web-server.conf
ExecStart=/usr/lib/node_modules/pm2/bin/pm2 start /opt/lecom/app/microservices/node-web-server/config/node-web-
server.config.js
ExecReload=/usr/lib/node_modules/pm2/bin/pm2 reload /opt/lecom/app/microservices/node-web-server/config/node-web-
server.config.js
ExecStop=/usr/lib/node_modules/pm2/bin/pm2 kill

[Install]
WantedBy=multi-user.target

```

Antes de efetuar o registro do serviço, será necessário adequar a configuração do serviço no arquivo /opt/lecom/app/microservices/node-web-services/node-web-server/config/global.env

```

HOST_NAME=app.meudominio.com.br
NODE_EXTRA_CA_CERTS=/opt/lecom/certificados/app.meudominio.com.br.crt
NODE_KEY=/opt/lecom/certificados/app.meudominio.com.br.key
ALLOW_EXTERNAL_COMMUNICATION_IFRAME_FORM_WEB=dominio.externo.com.br:3000,outro.dominio.externo.com.br,etc

```

A variável de ambiente ALLOW_EXTERNAL_COMMUNICATION_IFRAME_FORM_WEB do global.env descrita acima não é obrigatória, ela só é necessária, caso o usuário/cliente precise que o form se comunique com algum ambiente externo, um caso de uso é para quando o form público precisar se comunicar com alguma plataforma externa, nesse cenário, as urls desses ambientes externos podem ser incluídas nessa variável, com porta ou sem porta, como é mostrado no exemplo acima.

Para registrar o serviço será necessário executar os comandos abaixo informando o arquivo service:

```

systemctl link /opt/lecom/app/microservices/node-web-server/lecom_node-web-server.service
systemctl enable lecom_node-web-server.service

```

3.4 Configurando serviços do tomcat da plataforma

Entre na pasta [CATALINA_HOME]/webapps e descompacte os arquivos do pacote de acordo com as instruções abaixo:

- **bpm** = Dentro dela descompacte o arquivo **bpm.war**.
- **admin** = Dentro dela descompacte o arquivo **admin.war**.
- **core** = Dentro dela descompacte o arquivo **core.war**.
- **ecmcore** = Dentro dela descompacte o arquivo **ecmcore.war**.
- **sso** = Dentro dela descompacte o arquivo **sso.war**.

- **workspace-service** = Dentro dela descompacte o arquivo **workspace-service.war**.
- **social-service** = Dentro dela descompacte o arquivo **social-service.war**.

Atenção os arquivos .war encontram-se na pasta, /opt/lecom/temp/pacotes/

3.4.1 Adequando configuração de host

Adicionar as configurações dos connectors para SSL no Server.xml do Tomcat, conforme exemplo abaixo:

Os 2 itens destacados devem ser configurados de acordo com o ambiente:

```
<Connector SSLEnabled="true" ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
ADH-AES256-SHA, AES256-SHA, DHE-DSS-AES256-SHA, DHE-RSA-AES256-SHA" clientAuth="false"
keystoreFile="/opt/lecom/certificados/meudominio.com.br.jks"  

keystorePass="lecom123" maxThreads="150" port="443" protocol="HTTP/1.1" scheme="https" secure="true"
sslEnabledProtocols = "+TLSv1.2, +TLSv1.3"/>  

<Connector port="80" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="443" />
```

/opt/lecom/certificados/meudominio.com.br.jks – este é o caminho do certificado.

lecom123 – Substitua pela senha do certificado SSL da empresa.

Configurar no **web.xml** do Tomcat a seguinte constraint:

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>Entire application</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
```

É necessário configurar a url no arquivo [CATALINA_HOME]\conf\Server.xml. Para isso, é preciso alterar a configuração “padrão” que vem no tomcat fazendo a chamada através do *localhost* para o seu dns.

```
<Host name="meudominio.com.br" appBase="webapps" unpackWARs="false" autoDeploy="false">
    <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
        prefix="localhost_access_log" suffix=".txt"
        pattern="%h %l %u %t "%r" %s %b" />
</Host>
```

3.4.2 Definição de encoding

É necessário adicionar a configuração URIEncoding="ISO-8859-1" no arquivo [CATALINA_HOME]\conf\Server.xml na entrada que trata o conector da área HTTP.

Exemplo: <Connector URIEncoding="ISO-8859-1" />

3.4.3 Definição de memória

No arquivo setenv.sh existe a linha de configuração de parâmetros de memória atribuídos na variável JAVA_OPTS. Estes valores devem ser alterados de acordo com a memória RAM do servidor.

Abaixo segue as configurações mínimas, de acordo com a memória e processador do servidor:

```
JAVA_OPTS = "-Duser.language=pt -Duser.country=BR -server -Duser.home=/opt/lecom -Dfile.encoding=ISO8859-1 -Xms6656M -Xmx7680M -XX:MaxMetaspaceSize=512m -XX:+UseConcMarkSweepGC -Xss8m"
```

Observações:

A Plataforma Lecom trabalha com o português como idioma principal. Os parâmetros “-Duser.language=pt -Duser.country=BR -Dfile.encoding=ISO8859-1” são para garantir a utilização deste idioma independente de configurações do servidor.

3.4.4 Variáveis de ambiente para os módulos no Tomcat

No arquivo setenv.sh é necessário incluir as variáveis de ambiente para módulos e micro serviços.

```
# SSL
export SSL_KEY_STORE=/opt/lecom/certificados/bpm.meudominio.com.br.jks
export SSL_KEY_STORE_PASSWORD=password
export SSL_KEY_ALIAS=bpm.meudominio.com.br
export HOST_NAME=bpm.meudominio.com.br

export ENVIRONMENT_NAME=producao
export CLIENT_NAME="Lecom Tecnologia S/A"
export CUSTOM_LOGO=false
# E-mail que irá receber as notificações de licença que estão prestes a expirar.
export RESPONSIBLE_EMAIL=contato@meudominio.com.br
export SYSTEM_PASSWORD=passwordHere
export SPRING_PROFILES_ACTIVE="production,linux,mysql,proxy_ssl"

#OAUTH
export ADMIN_OAUTH2_CLIENT_SECRET=Chave de autenticação aqui
export BPM_OAUTH2_CLIENT_SECRET= Chave de autenticação aqui
export CORE_OAUTH2_CLIENT_SECRET= Chave de autenticação aqui
export ECM_OAUTH2_CLIENT_SECRET= Chave de autenticação aqui
export SSO_OAUTH2_CLIENT_SECRET= Chave de autenticação aqui
```

```

export SOCIAL_SERVICE_OAUTH2_CLIENT_SECRET= Chave de autenticação aqui
export WORKSPACE_SERVICE_OAUTH2_CLIENT_SECRET= Chave de autenticação aqui

#PORTAS SERVIÇOS
export BPM_SERVER_PORT=443
export SSO_SERVER_PORT=443
export CORE_SERVER_PORT=443
export ECM_SERVER_PORT=443
export ADMIN_SERVER_PORT=443
export WORKSPACE_SERVER_PORT=443
export SOCIAL_SERVER_PORT=443

#Storages
export APPLICATION_STORAGE_ROOT=/opt/lecom/storage/apps
export ADM_STORAGE_ROOT=/opt/lecom/storage/ambiente/adm
export BPM_STORAGE_ROOT=/opt/lecom/storage/ambiente/bpm
export CORE_STORAGE_ROOT=/opt/lecom/storage/ambiente/core
export ECM_STORAGE_ROOT=/opt/lecom/storage/ambiente/ecm
export SSO_STORAGE_ROOT=/opt/lecom/storage/ambiente/sso
export FILES_WORKDIR=/opt/lecom/storage/ambiente/workdir

#BPM DATASOURCE
export LECOM_BPM_DATASOURCE_URL="jdbc:mysql://localhost:3306/bpm_prd"
export LECOM_BPM_DATASOURCE_USERNAME=root
export LECOM_BPM_DATASOURCE_PASSWORD=pwd
export LECOM_BPM_BROKER_HOST=190.168.1.2 #Deve ser informado o host que o rabbitmq está sendo executado
export LECOM_BPM_BROKER_PORT=5672 #Deve ser informado a porta que o rabbitmq está sendo executado
export LECOM_BPM_BROKER_USERNAME=user #Deve ser informado o usuário que o rabbitmq está sendo executado
export LECOM_BPM_BROKER_PASSWORD=password #Deve ser informado a senha que o rabbitmq está sendo executado
export LECOM_BPM_BROKER_VIRTUAL_HOST=plataforma.meudominio.com.br #Deve ser informado o virtual host do rabbitmq
está sendo executado

#BPM CUSTOM DATABASE
export LECOM_BPM_JDBC_CUSTOM_URL=jdbc:mysql://localhost:3306/bpm_prd
export LECOM_BPM_JDBC_CUSTOM_USERNAME=simple_user
export LECOM_BPM_JDBC_CUSTOM_PASSWORD=pwd

#CORE DATASOURCE
export LECOM_CORE_DATASOURCE_URL="jdbc:mysql://localhost:3306/bpm_prd"
export LECOM_CORE_DATASOURCE_USERNAME=root
export LECOM_CORE_DATASOURCE_PASSWORD=pwd
export LECOM_CORE_BROKER_HOST=190.168.1.2 #Deve ser informado o host que o rabbitmq está sendo executado
export LECOM_CORE_BROKER_PORT=5672 #Deve ser informado a porta que o rabbitmq está sendo executado
export LECOM_CORE_BROKER_USERNAME=user #Deve ser informado o usuário que o rabbitmq está sendo executado
export LECOM_CORE_BROKER_PASSWORD=password #Deve ser informado a senha que o rabbitmq está sendo executado
export LECOM_CORE_BROKER_VIRTUAL_HOST=plataforma.meudominio.com.br #Deve ser informado o virtual host do
rabbitmq está sendo executado

#ECM DATASOURCE
export LECOM_ECM_DATASOURCE_URL="jdbc:mysql://localhost:3306/ecm_prd"
export LECOM_ECM_DATASOURCE_USERNAME=root
export LECOM_ECM_DATASOURCE_PASSWORD=pwd
export LECOM_ECM_BROKER_HOST=190.168.1.2 #Deve ser informado o host que o rabbitmq está sendo executado
export LECOM_ECM_BROKER_PORT=5672 #Deve ser informado a porta que o rabbitmq está sendo executado
export LECOM_ECM_BROKER_USERNAME=user #Deve ser informado o usuário que o rabbitmq está sendo executado
export LECOM_ECM_BROKER_PASSWORD=password #Deve ser informado a senha que o rabbitmq está sendo executado
export LECOM_ECM_BROKER_VIRTUAL_HOST=plataforma.meudominio.com.br #Deve ser informado o virtual host do rabbitmq
está sendo executado

#SSO DATASOURCE
export LECOM_SSO_DATASOURCE_URL="jdbc:mysql://localhost:3306/sso_prd"
export LECOM_SSO_DATASOURCE_USERNAME=root
export LECOM_SSO_DATASOURCE_PASSWORD=pwd
export LECOM_SSO_BROKER_HOST=190.168.1.2 #Deve ser informado o host que o rabbitmq está sendo executado

```

```

export LECOM_SSO_BROKER_PORT=5672 #Deve ser informado a porta que o rabbitmq está sendo executado
export LECOM_SSO_BROKER_USERNAME=user #Deve ser informado o usuário que o rabbitmq está sendo executado
export LECOM_SSO_BROKER_PASSWORD=password #Deve ser informado a senha que o rabbitmq está sendo executado
export LECOM_SSO_BROKER_VIRTUAL_HOST=plataforma.meudominio.com.br #Deve ser informado o virtual host do rabbitmq
está sendo executado

#WORKSPACE DATASOURCE
export WORKSPACE_SERVICE_DATASOURCE_URL="jdbc:mysql://localhost:3306/ws_prd"
export WORKSPACE_SERVICE_DATASOURCE_USERNAME="root"
export WORKSPACE_SERVICE_DATASOURCE_PASSWORD="pwd"

#SOCIAL DATASOURCE
export SOCIAL_SERVICE_DATASOURCE_URL="jdbc:mysql://localhost:3306/social_prd"
export SOCIAL_SERVICE_DATASOURCE_USERNAME="root"
export SOCIAL_SERVICE_DATASOURCE_PASSWORD="pwd"

#OPENAPI
export KONG_ADMIN_JWT_KEY= Chave de autenticação aqui
export KONG_ADMIN_JWT_SECRET= Segredo de autenticação aqui
export KONG_CONSUMER_PREFIX=producao
export KONG_CONSUMER_CLIENT_NAME=nome-cliente

#REDIS BPM
export BPM_REDIS_HOST=HOST
export BPM_REDIS_PORT=6379
export BPM_REDIS_DATABASE=9
export BPM_REDIS_PASSWORD=password
export BPM_REDIS_USERNAME=user

#DevOps
export ENVIRONMENT_TYPE=PRODUCTION # (DEVELOPMENT, ACCEPTANCE ou PRODUCTION)
export ENVIRONMENT_LOCAL_IP=192.168.3.144

#ASSINADOR DIGITAL
SIGN_SERVICE_URL: sign.lecom.com.br
SIGN_SERVICE_API_PATH: /sign-service
SIGN_SERVICE_LOCK_FAIL_LIMIT: 3 #quantidade de vezes em que o usuário pode errar a senha ao assinar antes de ser
bloqueado (default 3);
SIGN_SERVICE_LOCK_DURATION_IN_SECONDS: 60 #tempo em segundos em que o usuário ficará bloqueado de assinar ao
errar a senha (default 60);

```

Atenção: Os parâmetros datasource url devem ser adequados para cada banco de dados, segue abaixo um exemplo de uso para os bancos

- Oracle:
"jdbc:oracle:thin://HOST:PORT:SID"
- MSSQL
 - Configuração da url por porta
"jdbc:sqlserver://HOST:PORT;databaseName=BD_NAME;trustServerCertificate=true"
 - Configuração da url por instância
"jdbc:sqlserver://HOST\INSTANCE;databaseName=BD_NAME;trustServerCertificate=true"
- Mysql

"jdbc:mysql://HOST:PORT/DB_NAME"

Para bancos de dados Oracle e MSSQL devem também ser exportado as variáveis abaixo com o schema do banco de dados

```
export LECOM_BPM_DATASOURCE_SCHEMA=dbo
export LECOM_CORE_DATASOURCE_SCHEMA=dbo
export LECOM_ECM_DATASOURCE_SCHEMA=dbo
export LECOM_SSO_DATASOURCE_SCHEMA=dbo
export WORKSPACE_SERVICE_DATASOURCE_SCHEMA=dbo
export SOCIAL_SERVICE_DATASOURCE_SCHEMA=dbo
export LECOM_BPM_JDBC_CUSTOM_SCHEMA=dbo
```

3.5 Configurando serviços do tomcat das aplicações externas

As aplicações externas publicadas no Devops são implantadas em um segundo tomcat, chamado de tomcat_app.

3.5.1 Instalação do tomcat

Realizar o download e instalação do tomcat utilizando os comandos:

```
wget https://dlcdn.apache.org/tomcat/tomcat-9/v9.0.58/bin/apache-tomcat-9.0.58.tar.gz
unzip apache-tomcat-9.0.58.tar.gz
mv apache-tomcat-9.0.58.tar.gz /opt/lecom/app/tomcat_app
chmod +x /opt/lecom/app/tomcat_app/bin/*.sh
rm -rf /opt/lecom/app/tomcat_app/webapps/*
```

3.5.2 Adequando configuração de host

Habilitar TLS e alterar as portas do tomcat para não ter conflito, acessando o arquivo server.xml, no caminho /opt/lecom/app/tomcat_app/conf/server.xml e alterando as informações:

```
<Server port="8005" shutdown="SHUTDOWN">
<Server port="8006" shutdown="SHUTDOWN">
- <Connector port="8080" protocol="HTTP/1.1"
  !-
  <Connector executor="tomcatThreadPool"
    port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
  !-
  <Connector SSLEnabled="true"
    ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,"
```

```

TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA" keystoreFile="/opt/lecom/certificados/devops-
bpm-01.lecom.com.br.jks" keystorePass="lecom181" maxThreads="500" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true" sslEnabledProtocols =
"TLSv1,TLSv1.1,TLSv1.2" />
- <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />

```

- Remover o conteúdo em **rosa**;
- Adicionar o conteúdo em **verde**;
- Conteúdo em **preto** somente para referência de localização dentro do arquivo.

IMPORTANTE: O certificado SSL deve ter permissão para o usuário tomcat_app ler o arquivo e visualizar a pasta de certificados.

3.5.3 Variáveis de ambiente para as aplicações no Tomcat

Configurações do arquivo /opt/lecom/app/tomcat_app/bin/setenv.sh:

```

#!/bin/bash
# VARIAVEIS JAVA
export JAVA_HOME="/opt/lecom/java"

# Definindo o path padrão do Storage
export APPLICATION_STORAGE_ROOT="/opt/lecom/storage/apps"

# AUTO CONFIG MEMORY PARAMETERS
MAX_MEMORY=$(('/bin/cat /proc/meminfo | grep MemTotal | awk -F " " { print $2}/1024))
JAVA_XMS=$((MAX_MEMORY * 1) / 100)
JAVA_XMX=$((MAX_MEMORY * 2) / 100)
JAVA_OPTS=$JAVA_OPTS"-Xms"$JAVA_XMS"m -Xmx"$JAVA_XMX"m"

# VARIAVEIS APP
export ADMIN_DOMAIN="https://cliente-url.lecom.com.br"
export SSO_DOMAIN="https://cliente-url.lecom.com.br"
export CORE_DOMAIN="https://cliente-url.lecom.com.br"
export APPLICATION_STORAGE_ROOT="/opt/lecom/storage/apps"

```

IMPORTANTE: Trocar https://cliente-url.lecom.com.br pela respectiva URL do ambiente.

3.5.4 Registrar o tomcat_app como serviço

Criar o arquivo /opt/lecom/config/etc/lecom_app-service.service com o conteúdo abaixo:

```

[Unit]
Description=lecom_bpm-service

[Service]
User=tomcat
Group=tomcat_app
LimitNOFILE=10240
ExecStartPre=/bin/sleep 25
ExecStart=/bin/bash -c 'exec /opt/lecom/app/tomcat_app/bin/catalina.sh start'
ExecStop=/bin/bash -c 'exec /opt/lecom/app/tomcat_app/bin/catalina.sh stop'
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target

```

Executar os comandos para registrar o serviço:

```

systemctl link /opt/lecom/config/etc/lecom_app-service.service
systemctl enable lecom_app-service.service

```

3.6 Iniciando os serviços

Obs.: Apenas o root pode executar os comandos abaixo.

Para iniciar os serviços, é necessário executar os comandos abaixo nessa ordem e com usuário root:

```

systemctl start lecom_config-service
systemctl start lecom_discovery-service
systemctl start lecom_gateway-service
systemctl start lecom_form-app
systemctl start lecom_form-service
systemctl start lecom_service-integration
systemctl start lecom_node-web-server
systemctl start lecom_audit-service
systemctl start lecom_behavior-service
systemctl start lecom_tomcat_app
docker-compose up -d #(deve ser executado na pasta do docker-compose)

```

Após iniciar os serviços, inicie o servidor de aplicação (Tomcat) da seguinte forma:

```
[CATALINA_HOME]/bin/startup.sh
```

Para parar os serviços basta executar os comandos na seguinte ordem:

```

systemctl stop lecom_config-service
systemctl stop lecom_discovery-service
systemctl stop lecom_gateway-service
systemctl stop lecom_form-app
systemctl stop lecom_form-service
systemctl stop lecom_service-integration
systemctl stop lecom_workspace-web
systemctl stop lecom_node-web-server

```

```
systemctl stop lecom_audit-service  
systemctl stop lecom_behavior-service  
systemctl stop lecom_tomcat_app  
docker-compose down #(deve ser executado na pasta do docker-compose)
```

E parar o servidor de aplicação (Tomcat) da seguinte forma:

```
[CATALINA_HOME]/bin/shutdown.sh
```

3.7 Ambiente em Cluster

3.7.1 Storage de dados

É necessário que a pasta STORAGE esteja acessível para cada servidor do cluster. Pois é nessa pasta que a plataforma salva as principais configurações que são utilizadas pelos nós do cluster.

3.7.2 Configurações

Para ativar a configuração de cluster na Plataforma Lecom é necessário ajustar as configurações abaixo no arquivo setenv.sh do tomcat:

Variável	Descrição
nodeName	Nome único para o nó

4. Recursos extras

4.1 Open Redirect

Por padrão a Plataforma Lecom restringe o direcionamento para outros domínios que não seja o da aplicação a partir do login. Caso seja necessário algum redirecionamento específico, configure na variável citada abaixo no arquivo setenv.sh. Caso exista mais do que um domínio, utilize o separador “,”.

```
AUTHORIZED_DOMAINS_TO_REDIRECT = autoriza redirecionamento para domínios específicos
```

4.2 Tratamento CSRF

Por padrão o recurso de tratamento de ataque CSRF não vem ativado. Caso seja necessário, configure na variável abaixo no arquivo setenv.sh:

```
CSRF_ENABLE = true
```

4.3 Headers HTTP

Por padrão não há necessidade de alterar os headers HTTP. Porém, se houver necessidade de alguma customização, os conteúdos abaixo devem constar obrigatoriamente, seguido da customização. Essa configuração deve ser feita em:

```
[CATALINA_HOME]/bin/setenv.sh  
/opt/lecom/app/microservices/envs/00-profile.conf  
/opt/lecom/app/microservices/node-web-server/config/global.env
```

Conteúdo:

Variável	Valor padrão
STRICT_TRANSPORT_SECURITY	max-age=31536000;includeSubDomains
X_FRAME_OPTIONS	SAMEORIGIN (apenas no módulo SSO, nos demais não possui valor padrão)
X_CONTENT_TYPE_OPTIONS	nosniff
X_XSS_PROTECTION	1; mode=block
ACCESS_CONTROL_ALLOW_ORIGIN	
ACCESS_CONTROL_ALLOW_METHODS	GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, TRACE, PATCH

ACCESS_CONTROL_ALLOW_HEADERS	Content-Type, X-Requested-With, accept, Origin, Access-Control-Request-Method, Access-Control-Request-Headers, test-mode, ticket-sso, test-user, Cache-Control, form-uuid, language, pragma, application, Referer, sec-ch-ua, sec-ch-ua-mobile, x-xsrf-token
ACCESS_CONTROL_EXPOSE_HEADERS	*
ACCESS_CONTROL_MAX_AGE	864000
ACCESS_CONTROL_ALLOW_CREDENTIALS	true

Caso a variável X_FRAME_OPTIONS seja configurada com um valor diferente do valor padrão, é necessário atentar-se a alguns pontos:

1. No diretório [CATALINA_HOME]/bin/setenv.sh, tanto a variável, quanto o seu respectivo valor, precisam estar definidos com letras maiúsculas:
 - Exemplo: X_FRAME_OPTIONS=<VALOR>"
2. No diretório /opt/lecom/app/microservices/envs/00-profile.conf, declarar a variável com letras maiúsculas e seu valor com letras minúsculas:
 - Exemplo: X_FRAME_OPTIONS=<valor>"
3. No diretório /opt/lecom/app/microservices/node-web-server/config/global.env, para que a configuração seja aplicada com êxito, é preciso declarar a variável com a primeira letra maiúscula e as demais minúsculas, e o valor da variável em letras minúsculas:
 - Exemplo: X_Frame_Options=<valor>"

5. Licenciamento

5.1 Ativando o módulo de login

Ao acessar a aplicação pelo link <https://app.meudominio.com.br/sso> o módulo de login perceberá que é uma nova instalação, apresentará uma senha e pedirá uma contra-senha. É importante não sair desta página, pois do contrário, a cada vez que acessar esta página uma nova senha será gerada.

Para conseguir a contra-senha, entre em contato com a Lecom, e informe a senha. Uma boa prática é enviar por e-mail para evitar erro de digitação.

Digite a contra-senha fornecida. Tome cuidado com todos os caracteres, pois se um estiver errado, a aplicação não será registrada. É comum erros entre o número 0 (zero) e letra O, dentre outros. Esta senha tem validade de 180 dias.

Se a contra-senha for válida, o módulo de login voltará para a tela de autenticação, do contrário, serão mostradas uma nova senha e a indicação do erro de contra-senha inválida.

Para licenciar os demais módulos da aplicação efetue o login na aplicação que o sistema redirecionará o usuário automaticamente para a área de licenciamento. Nesta tela será apresentado todos os produtos para que possam ser ativados.

Licenças							
Notificações							
Gerenciamento de Licenças							
Sigla	Produto	Data de expiração	Status	Modalidade			
SSO	Login	28/04/2016	Licenciado	Produção			
ADMIN	Admin		Não precisa de licença	Completo			
AT5	BPM	28/04/2016	Licenciado	Produção			
ECM	ECM	28/04/2016	Licenciado	Completo			

Lista de produtos para serem ativados.

Para ativar os demais módulos, clique no botão "Renovar licença" localizado logo após a coluna de modalidade.

Ao clicar neste botão será aberta uma tela com as informações sobre o produto e com uma senha. Esta deve ser informada para a Lecom para obter a contra-senha para liberação do módulo.

Renovar Licença do Produto	
Sigla	AT5
Produto	BPM
Senha	920I-0BH0-VLOF-HW2W-202C
Contra-Senha	
Descrição	
<input type="button" value="Cancelar"/> <input type="button" value="Confirmar"/>	

Modal para ativar o produto.

Nos campos "Descrição" é possível colocar qualquer tipo de texto informativo. Serve para descrever qual o motivo do registro.

Ao terminar de preencher os dados, clique em "Confirmar" para ativar o produto. Caso a contra-senha digitada esteja errada ou inválida, a tela será recarregada e uma nova senha será gerada. Dessa forma, precisa novamente entrar em contato com a Lecom, informa a nova senha e solicitar a contra-senha. Caso a senha esteja correta, uma mensagem irá informar que o produto foi ativado com sucesso.

Ao fechar a tela a lista de produtos será atualizada.

5.2 E-mail para notificação de expiração de licença

Na parte superior da tela de licenças é possível informar um e-mail para receber notificações de expiração das licenças. As notificações serão enviadas da seguinte forma: Quando estiver faltando 15, 10, 5, 4, 3, 2 e 1 dia(s) antes de expirar a licença.

6. Configurações finais

6.1 Configurando servidor de e-mail

Acesse o módulo Administrativo, clique no menu Configurações, em seguida na aba E-mail e configure as informações solicitadas.

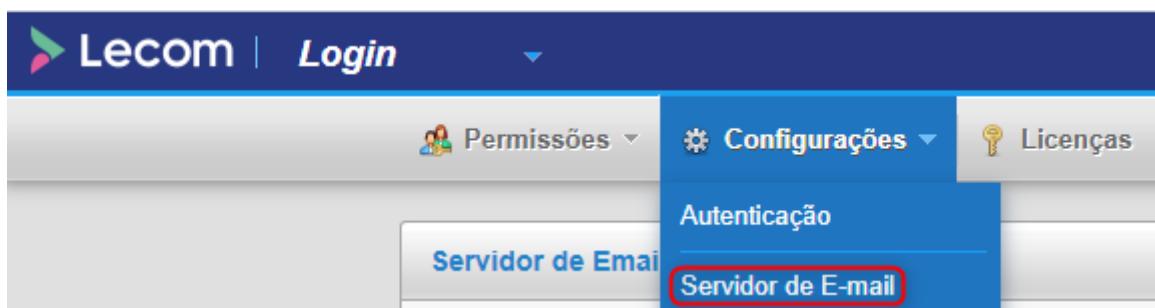
The screenshot shows the 'Configurações' (Configurations) section of the Lecom Admin interface. Under the 'E-mail' tab, the 'Configurações do Servidor de email' (Email Server Configuration) form is displayed. The form fields include:

- Envio de email autenticado (Authenticating Email Send)
- Conexão Segura (Secure Connection):
 - Nenhuma (None)
 - SSL
 - STARTTLS
- E-mail host *: [empty input field]
- E-mail port *: 25
- E-mail from: [empty input field]
- Usuário: [empty input field]
- Senha: [empty input field]
- E-mail reply: [empty input field]

At the bottom right are 'Testar' (Test) and 'Salvar' (Save) buttons.

Cadastro de Parâmetros, informações sobre o servidor de SMTP e url de acesso a Plataforma Lecom

Em seguida, acesse o módulo Login, clique no menu Configurações, em seguida, Servidor de E-mail e configure as informações solicitadas.



Menu de acesso às configurações de e-mail do Lecom Login.

Servidor de Emails

SMTP *	Porta * 25
E-mail emissor *	
<input type="checkbox"/> Envio Autenticado	
E-mail para resposta *	
Conexão *	Nenhuma
<input type="button" value="Testar"/> <input type="button" value="Salvar"/>	

Configurações de e-mail do Lecom Login.

A configuração de e-mail no módulo Login é importante para o envio de e-mails de recuperação de senha, expiração de contra-senha do produto, entre outras funcionalidades.

6.2 URL de acesso

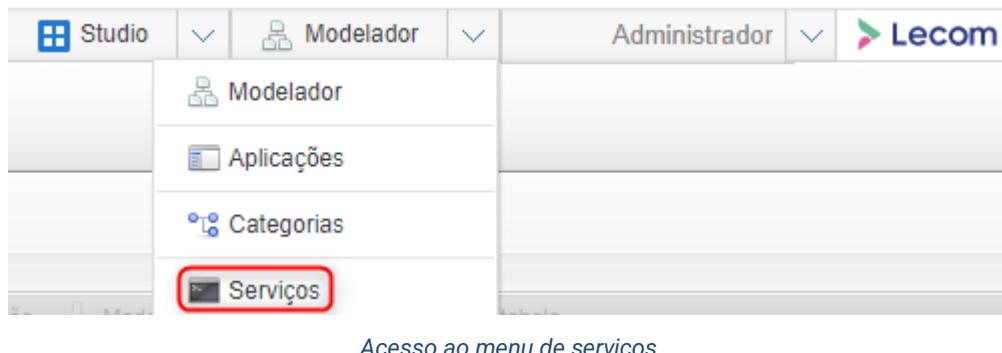
Para alterar a URL que vem preenchida automaticamente no momento de implantação, acesse o módulo administrativo, clique no menu Configurações, em seguida na aba Gerais e configure no campo URL o endereço de acesso da plataforma seguido de "/bpm". Por exemplo:
<https://app.meudominio.com.br/bpm>

The screenshot shows the Lecom Admin interface with the following details:

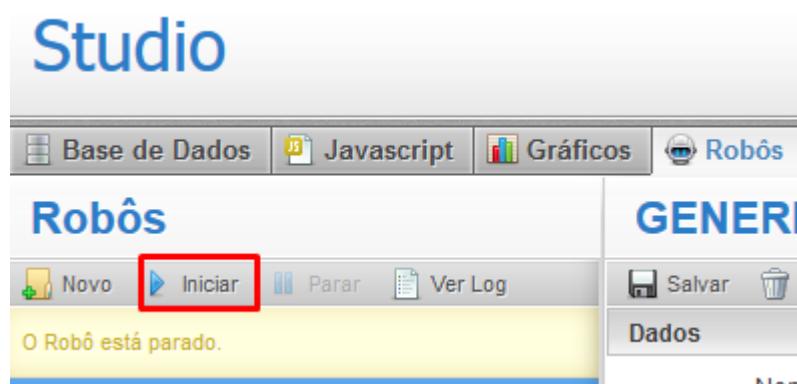
- URL:** https://app.meudominio.com.br/admin
- Section:** Configurações Gerais (General Settings)
- Dias para expirar a senha:** 90
- Máximo de tentativas de login:** 3
- Autenticação automática na execução de atividade por email?** (checkbox checked)
- Campos Adicionais:**
 - Label do primeiro campo
 - Label do segundo campo
 - Label do terceiro campo
- Processos Pendentes:**
 - Máximo de acessos múltiplos: 10
- Demonstrativo:**
 - Senha do demonstrativo: lecom
- HTTP da plataforma:**
 - URL: https://app.meudominio.com.br/bpm

6.3 Ativando os robôs

Acesse o módulo Studio e no menu superior acesse a área de serviços.



Abra a guia Robôs e clicar em Iniciar, como mostra figura abaixo



Tela para iniciar e parar a execução do robô.

Caso o servidor de aplicação seja parado, ao reiniciá-lo, o robô manterá o status que apresentava no momento da parada.

Após ter executado os passos descritos acima com sucesso a implantação estará finalizada.

7. Validação do ambiente

Após realizar os procedimentos descritos acima, acesse a Plataforma Lecom com o usuário adm e realize a troca de senha deste usuário no primeiro acesso, caso seja ambiente de produção. Em seguida, acesse o menu Análises e Auditoria.

Esta área irá testar alguns itens essenciais para o funcionamento da ferramenta, como:

- Conexão com banco de dados;
- Conexão com servidor de SMTP;
- Conexão com o AD/ LDAP, caso este seja utilizado;
- Permissão para escrita em disco;
- Status do Web Service;
- Informações pertinentes ao ambiente.

Caso algum destes testes não seja executado com sucesso, revise a implantação

8. Portas utilizadas pelos módulos da plataforma

Form-app: 8080

Form-service 8081

Behavior-service: 8082

Job-service: 8084

Job-runner: 8085

Service-integration: 8091

Audit-service: 8092

Gateway-service: 8181

Admin: 80/443

Bpm: 80/443

Core: 80/443

Ecm: 80/443

sso: 80/443

Social-service: 80/443

Workspace-service: 80/443

Discovery-service: 8761

9. API para monitoramento de disponibilidade de ambiente (rotas de Health Check)

Existem serviços em nossa plataforma que permite o monitoramento da disponibilidade de cada micro serviço. São eles:

- config - [https://\\\$ SERVER:9999/actuator/info](https://\$ SERVER:9999/actuator/info)
- discovery - [https://\\\$ SERVER:8761/actuator/health](https://\$ SERVER:8761/actuator/health)
- gateway - [https://\\\$ SERVER:8181/actuator/health](https://\$ SERVER:8181/actuator/health)
- form-app - [https://\\\$ SERVER:8080/form-app/actuator/health](https://\$ SERVER:8080/form-app/actuator/health)
- form-service - [https://\\\$ SERVER:8081/form-service/actuator/health](https://\$ SERVER:8081/form-service/actuator/health)
- service-integration - [https://\\\$ SERVER:8091/api/actuator/health](https://\$ SERVER:8091/api/actuator/health)
- audit-service - [https://\\\$ SERVER:8092/audit-service/api/actuator/health](https://\$ SERVER:8092/audit-service/api/actuator/health)
- behavior-service - [https://\\\$ SERVER:8082/behavior-service/actuator/health](https://\$ SERVER:8082/behavior-service/actuator/health)
- job-runner - [https://\\\$ SERVER:8085/job-runner/actuator/health](https://\$ SERVER:8085/job-runner/actuator/health)
- job-service - [https://\\\$ SERVER:8084/job-service/actuator/health](https://\$ SERVER:8084/job-service/actuator/health)

10. Autenticação

10.1 Acesso automático usando as credenciais do Microsoft AD

10.1.1 Introdução

AD corresponde a Active Directory, esse mecanismo de autenticação automática permite que o usuário tenha acesso direto ao sistema sem a necessidade do procedimento de autenticação a cada sessão.

Um modo de implementar a autenticação automática é por meio do uso das credenciais do usuário que foram obtidas no momento em que sua estação de trabalho se conectou a um domínio do AD (Active Directory). Este modo de autenticação está em conformidade com o conceito de Single Sign On (SSO), o qual estabelece uma forma única de autenticação do usuário para acesso a ambiente e aplicações distintas.

Aplicado à **Plataforma Lecom** este mecanismo de autenticação permite que usuário autenticado em um servidor AD faça uso do sistema sem a necessidade de realizar o login no sistema, ou seja, ao acessar o sistema, o usuário acessará automaticamente na “Minha Área”.

10.1.2 Requisitos

Para a utilização da autenticação automática usando o AD é necessário considerar vários requisitos de software, de configurações do Servidor Active Directory e das estações de trabalho.

O servidor Active Directory deve ser dotado do sistema operacional Windows Server 2003, 2008, 2012, 2014 ou 2016 Server. Para o 2003 Server é necessário aplicar o Service Pack 1 ou superior. Para servidores com Windows 2003 também é necessário instalar o conjunto de ferramentas Windows Support Tools que acompanha o cd de instalação.

As estações de trabalho devem ser dotadas do sistema operacional Microsoft Windows 10 ou superior cujas versões permitam a inclusão da estação de trabalho em um domínio Active Directory. Será necessária também a adoção do navegador Google Chrome, Microsoft Edge ou do navegador Firefox.

Todas as estações de trabalho que irão usar este recurso deverão ter seu navegador devidamente configurado. Para isso, veja a seguir em como proceder com a configuração.

10.1.3 Configuração servidor Active Directory

A configuração do servidor AD está basicamente dividida em duas etapas: criação e/ou configuração de um usuário AD e criação de um *Service Name* associado com este usuário que referenciará o servidor de aplicação.

Para servidores com Windows Server o primeiro passo é instalar o conjunto de ferramentas Windows Support Tools que acompanha a instalação do sistema operacional. Este software também pode ser baixado do site da Microsoft.

A conta do usuário AD deve ter seguinte opção selecionada:

- “password never expires”;

Nas próximas sessões serão utilizados os termos:

- **ip_ou_host_da_aplicacao:** É o endereço IP ou host do servidor da Plataforma Lecom;
- **user:** É o nome do usuário AD configurado.

Atenção:

- O endereço da aplicação nas configurações de DNS deve ser do tipo A e não deve ser de qualquer outro tipo (Alias ou Cname).
- Para as configurações a serem definidas abaixo deve-se escolher entre ip ou o host, como endereço da aplicação. Ao definir qual será utilizado, este deve ser utilizado em todas as configurações, não devem ser utilizadas as duas informações em pontos diferentes da configuração. Ou seja, se for utilizar o ip este deve ser usado para todas as configurações.

Service Name

Para criar um Service Name no AD associado ao usuário e que será usado pelo servidor de aplicação, faça:

- Abra o prompt de comandos do servidor AD
- Digite o seguinte comando:

```
> setspn -a HTTP/ip_ou_host_da_aplicacao user
```

Para verificar se o Service Name foi devidamente criado pode-se executar o comando:

```
> setspn -l user.
```

Caso seja necessário atualizar o Service Name, será necessário excluí-lo e depois criá-lo novamente. Para excluir um Service Name o comando abaixo pode ser usado:

```
> setspn -d HTTP/ip_ou_host_da_aplicacao user
```

10.1.4 Configuração servidor aplicação

A configuração do servidor de aplicação exige algumas mudanças. A primeira é garantir que o servidor AD seja conhecido pelo nome de domínio. Isto pode ser feito configurando o DNS do servidor de aplicação para apontar para o servidor AD ou configurar o arquivo hosts do servidor de aplicação para que ele possa acessar o servidor de domínio pelo nome. Antes de realizar estas mudanças consulte o administrador da rede.

A próxima configuração a ser feita é a criação de um arquivo que contém a chave para autenticação de usuário chamado “keytab”. Para criar um keytab, usaremos uma ferramenta do Java chamada “ktab”. O comando abaixo deve ser executado no próprio servidor da aplicação:

```
> ktab -a HTTP/ip_ou_host_da_aplicacao@REALM.USADO senha_usuario -k caminho_keytab/nome_keytab.keytab
```

Onde:

- **HTTP/ip_ou_host_da_aplicacao** é o Service Name criado anteriormente no servidor Active Directory;
- **REALM.USADO** é o realm do cliente;
- **senha_usuario** é a senha do usuário que foi associado ao **Service Name**;
- **caminho_keytab** é o path onde o arquivo será salvo;

- **nome_keytab.keytab** é o nome do arquivo. Sendo que sua extensão deve ser “.keytab”.

O arquivo keytab deve ser armazenado em uma pasta onde a plataforma tenha acesso.

A outra configuração no servidor de aplicação é a necessidade de inclusão de um arquivo de configuração com detalhes do processo de autenticação automática como, por exemplo, o tipo de criptográfica adotada, realm, endereço do kdc, entre outras.

Este arquivo será usado pelo Login no mecanismo de autenticação automática. Ele deve ser disponibilizado na pasta `[JAVA_HOME]/conf/security` com o nome `krb5.conf`.

10.1.5 Configuração do AD na plataforma

Neste momento configuraremos a sessão destinada à autenticação automática. Para isso teremos que acessar a tela de configuração de LDAP no SSO que fica em Configurações/Autenticação – aba LDAP. Em seguida selecionar a opção “Autologin Habilitado” na sessão “Campos para login automático” como na imagem abaixo:



The screenshot shows a configuration interface for automatic login fields. At the top, there is a header labeled "Campos para login automático". Below it, there is a section with a checked checkbox labeled "Autologin habilitado". The entire checkbox area is highlighted with a red border.

Após selecionar a opção de “Autenticação Automática”, aparecerá as configurações como na imagem abaixo:



The screenshot shows a more detailed configuration for automatic login fields. It includes several input fields and checkboxes:

- "Autologin habilitado": checked
- "Caminho da configuração do Krb": /opt/java/jdk-12.0.2/conf/security/krb5.conf
- "Serviço Kdc Principal": HTTP/p_ou_host_da_aplicacao
- "Caminho do Keytab": caminho_do_keytab/nome_keytab.keytab
- "Campo Kdc": userPrincipalName
- "Usar contexto Kerberos": unchecked
- "Kdc Debug": unchecked

As opções “Usar Contexto Kerberos” e “KDC Debug” não são obrigatorias, porém podem ser usadas em alguns contextos específicos. Ex: Caso seja necessário fazer alguma análise de falha, selecionar a opção “KDC Debug” pode ajudar. Caso o cliente exija o uso do Kerberos inclusive como

gerenciamento de contexto do LDAP, selecione a opção “Usar Contexto Kerberos”, porém esse último caso é muito difícil de acontecer.

Segue abaixo a explicação de cada campo que deve ser preenchido:

- Caminho da configuração do Krb – Deve ser colocado o caminho completo o krb5.conf criado anteriormente.
- Serviço Kdc Principal – É o Principal criado anteriormente com o comando setspn para referenciar o usuário gerenciador do AD da Plataforma Lecom a um serviço. No caso o serviço é a própria plataforma.
- Caminho do Keytab – Colocar aqui a pasta do keytab criado anteriormente.
- Campo Kdc – Colocar aqui o campo do AD no qual é referenciado o nome do usuário informado nome.usuario@ream.usado. Normalmente é usado o valor “userPrincipalName”.

```
</networkConnectors>
[libdefaults]
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = REALM.USADO
default_keytab_name = FILE:caminho_keytab/nome_keytab.keytab
allow_weak_crypto = true
[realms]
REALM.USADO = {
    kdc = host_ou_ip_do_kdc
    admin_server = host_ou_ip_do_active_directory
}
[domain_realm]
.realm.usado.minusculo = REALM.USADO
ream.usado.minusculo = REALM.USADO
```

Atenção: O padrão de escrita deve ser mantido. Onde está escrito em letras maiúsculas deve permanecer assim, bem como onde está escrito em letras minúsculas.

- A propriedade “REALM.USADO” deve ser trocada pelo realm usado na rede do cliente;
- A propriedade “ream.usado.minusculo” deve ser trocada pelo realm usado na rede do cliente, mas em minúsculo;
- A propriedade “caminho_keytab” deve ser trocada pelo caminho do keytab criado

anteriormente;

- A propriedade “nome_keytab.keytab” deve ser trocada pelo nome do keytab criado anteriormente;
- A propriedade “host_ou_ip_do_kdc” deve ser trocada pelo host ou ip do kdc do cliente (geralmente é o mesmo);
- A propriedade “host_ou_ip_do_active_directory” deve ser trocada pelo host ou ip do Active Directory do cliente;
- O uso da propriedade “allow_weak_crypto = true” não é forma mais segura de configurar o krb5.conf, porém é compatível com qualquer tipo de criptografia. No lugar dela, pode ser usado as propriedades “default_tkt_enctypes”, “default_tgs_enctypes” e “permitted_enctypes”, passando como parâmetro a criptografia usada pelo servidor AD. Para obter essa informação, é necessário consultar o responsável pelo servidor AD. Segue exemplo de parametrização:
 - default_tkt_enctypes = rc4-hmac aes128-cts-hmac-sha1-96 aes256-cts-hmac-sha1-96
 - default_tgs_enctypes = rc4-hmac aes128-cts-hmac-sha1-96 aes256-cts-hmac-sha1-96
 - permitted_enctypes = rc4-hmac aes128-cts-hmac-sha1-96 aes256-cts-hmac-sha1-96

- A data e hora dos servidores de AD e Aplicação devem estar sincronizados;
- É imprescindível que este arquivo fique em [JAVA_HOME]/conf/security/ pois o java por padrão procura nessa pasta.

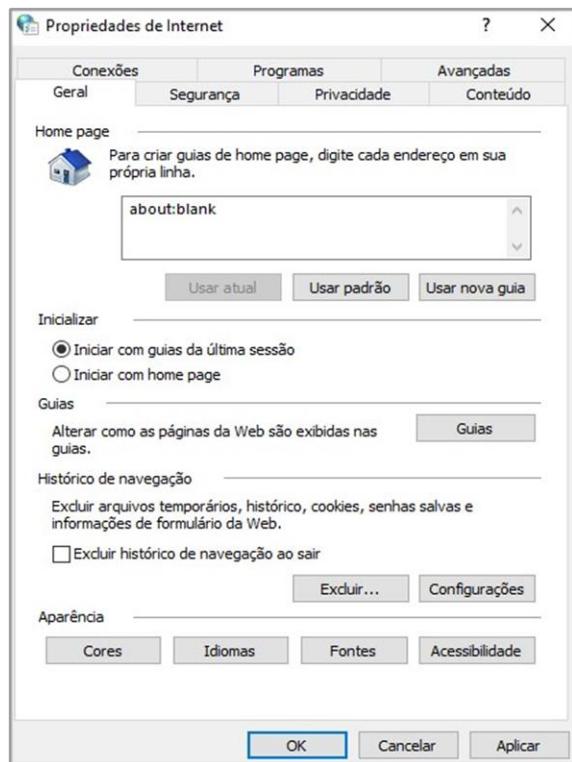
10.1.6 Configuração estação de trabalho

Esta seção abordará os aspectos de configurações que serão necessárias na estação de trabalho do usuário. Estes aspectos estão relacionados com as configurações dos navegadores Google Chrome, Microsoft Edge e Firefox.

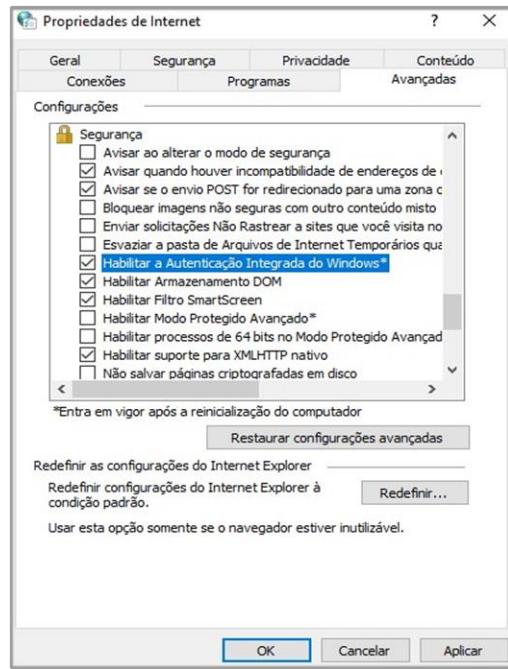
10.1.7 Navegadores Google Chrome e Microsoft EDGE

As configurações para os navegadores: Google Chrome e *Microsoft EDGE* independem do sistema operacional. Para permitir que eles usem este recurso é necessário alterar sua configuração da seguinte forma:

1. Acessar o Painel de Controle e acessar a opção “*Opções de Internet*”:



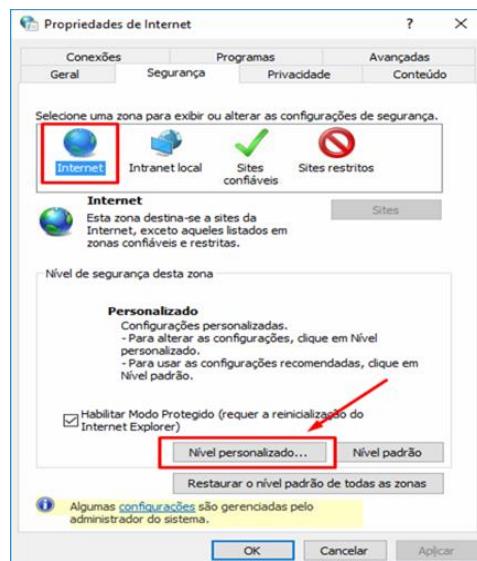
2. Acesse a guia “Avançadas” e role a página até o tópico “Segurança”:



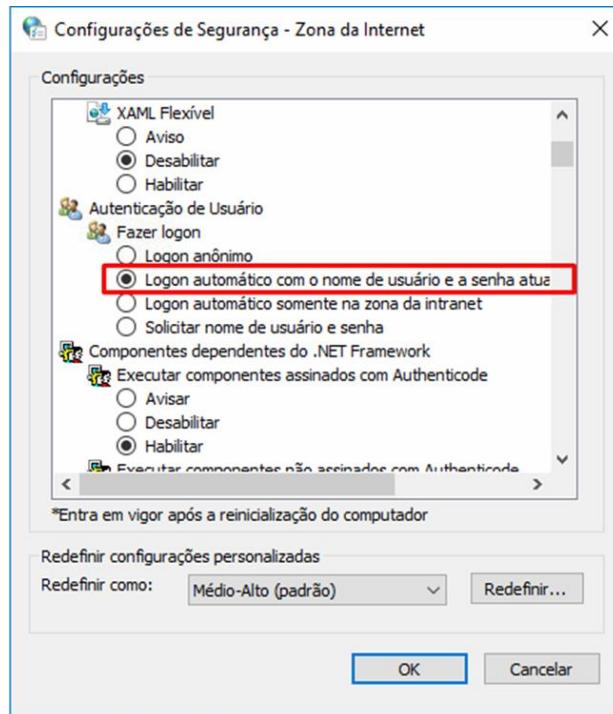
- Certifique-se de que a opção “Habilitar a Autenticação Integrada do Windows” esteja selecionada. Clique em “OK”.

Algumas redes exigem configuração extra para autenticação automática. Abaixo alguns passos para configuração de segurança personalizada.

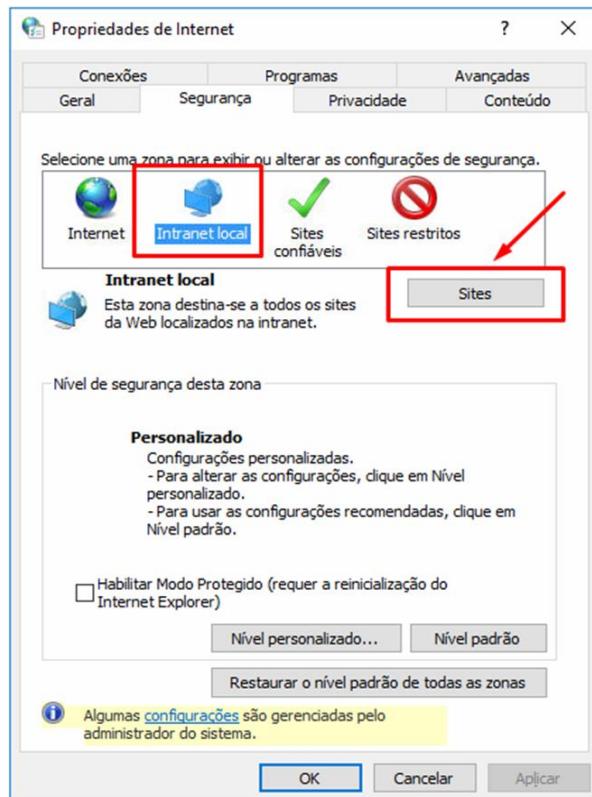
- Entrar em Opções da internet e acessar a aba Segurança. Clicar no item “Internet” e depois em “Nível personalizado”.



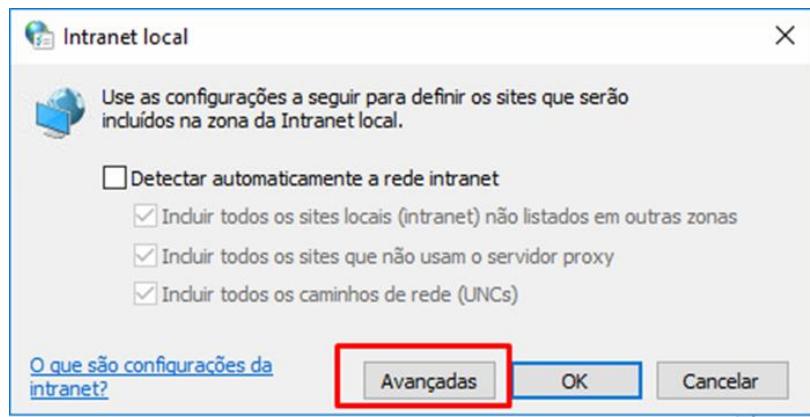
2. Selecionar a opção em destaque abaixo e clicar em "OK":



3. Clicar no item “Intranet local” e depois em “Sites”.

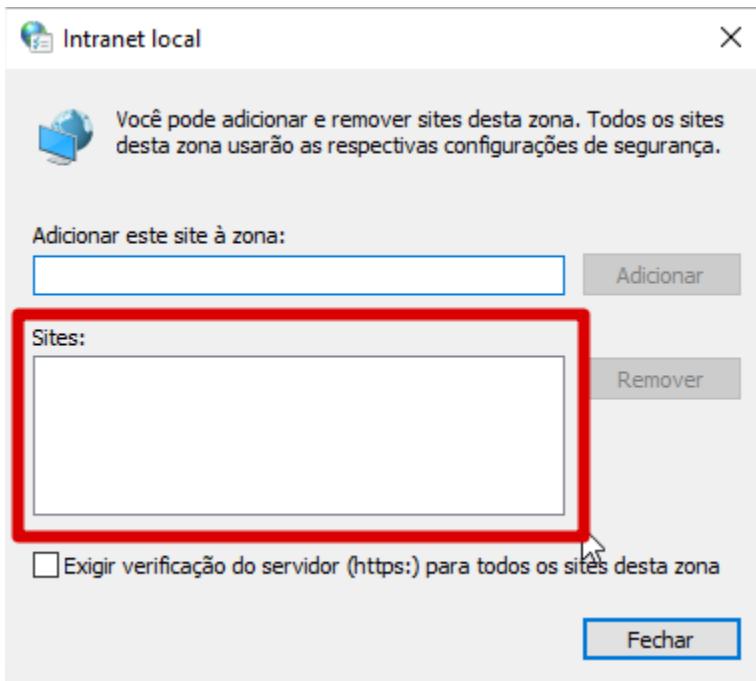


4. Clicar em avançadas.

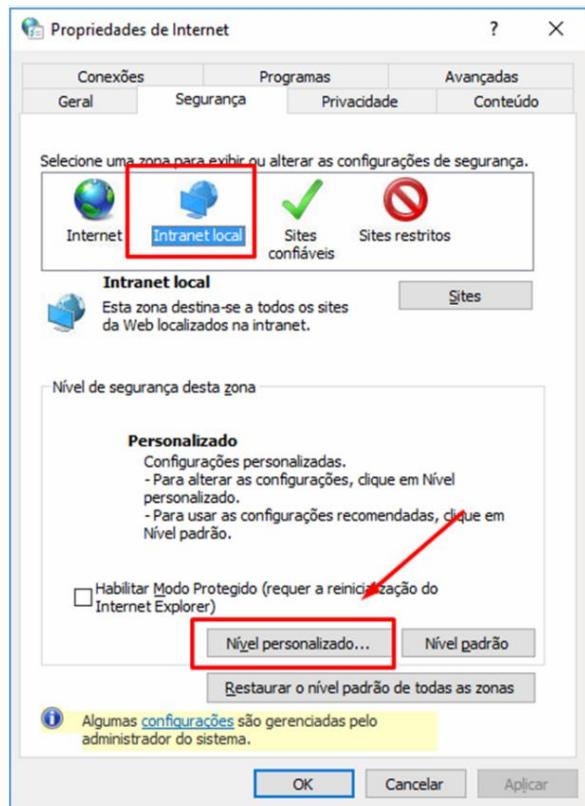


5. Remover o host dessa lista abaixo e clicar em "Fechar" e depois dê um "OK" na tela anterior.

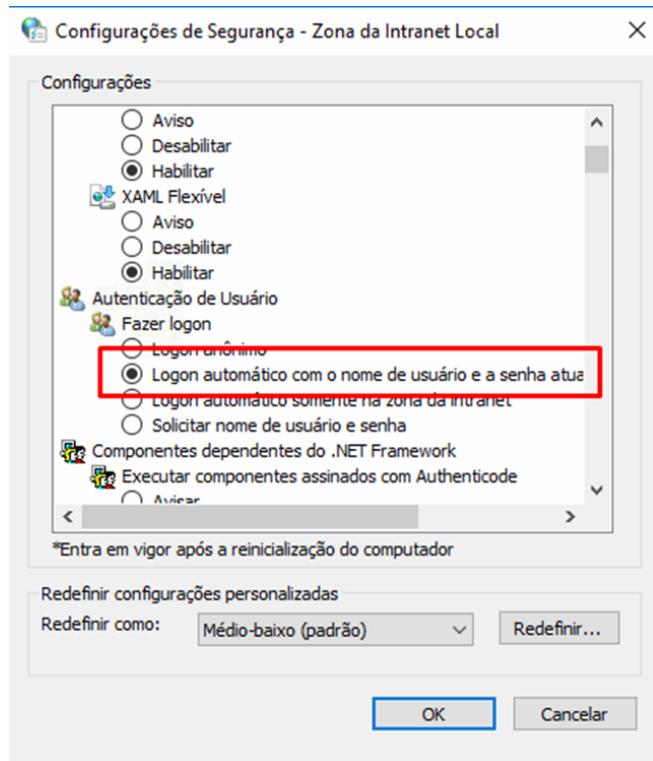
Obs.: Caso as configurações abaixo sejam administradas por um administrador de rede, é necessário pedir que retirem o host da lista e reiniciar o computador para surtir efeito.



6. Ainda no ícone “Intranet local”, clicar em nível personalizado. Selecionar a opção em destaque abaixo e clicar em “OK”:



7. Por fim, selecione a opção em destaque e clique em “OK” para finalizar as alterações das Opções da Internet.



Atenção: Caso as configurações realizadas localmente se perderem após realizar logoff na máquina e login novamente, isso ocorre porque as configurações são configuradas automaticamente no login, assim o administrador de rede deverá aplicar essas configurações para toda a rede. Assim, ficará definida automaticamente para todos os usuários.

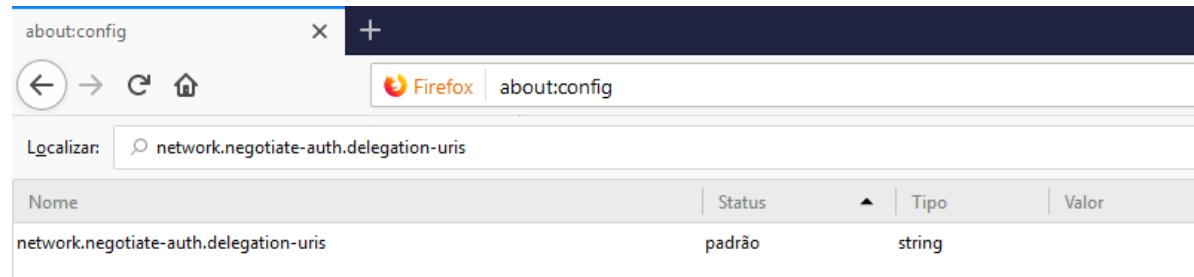
10.1.8 Navegador Firefox

Para que os usuários do navegador Firefox possam fazer uso deste recurso, é necessário proceder a seguinte alteração no navegador:

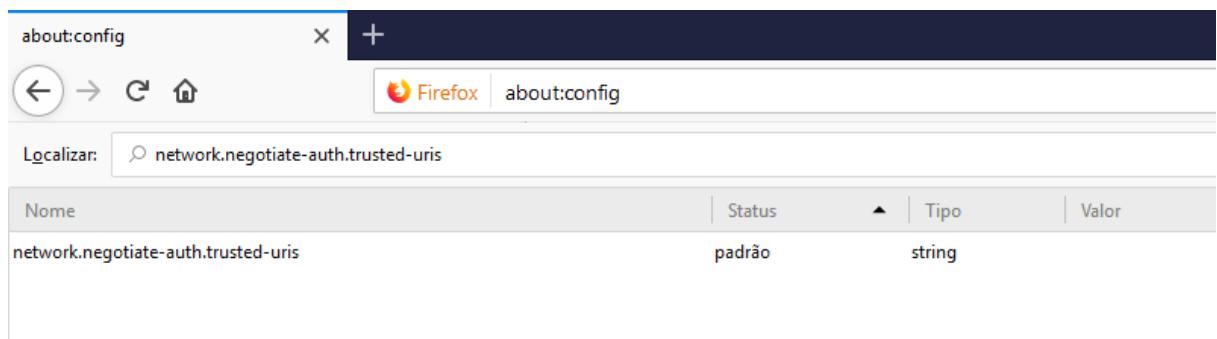
1. Abra o navegador e digite **about:config** na barra de endereços:



2. A seguir, na caixa de texto “localizar nome”, digite o nome **network.negotiate-auth.delegation-uris**, como apresentado na figura a seguir:



3. Dê um clique duplo na entrada **network.negotiate-auth.delegation-uris** e entre com o endereço IP ou o host do servidor de aplicação;
4. A seguir, na caixa de texto “localizar nome”, digite o nome **network.negotiate-auth.trusted-uris**, como apresentado na figura a seguir:



5. Dê um clique duplo na entrada **network.negotiate-auth.trusted-uris** e entre com o endereço IP ou o host do servidor de aplicação;
6. Pronto, a configuração está completa. Não é necessário reiniciar o navegador.

10.1.9 Validando configuração

Para validar se as configurações foram bem-sucedidas, proceda da seguinte maneira:

1. Faça a autenticação da estação em um domínio Active Directory (por exemplo, máquina Windows logada com o usuário configurado no AD);
2. Abra o navegador e entre com o endereço de acesso à Plataforma Lecom:
 - a. Até o momento, a autenticação automática com AD é funcional apenas para a rota "[URL_AMBIENTE]/sso".
3. Se tudo estiver correto o sistema abrirá e será exibida a tela principal do sistema. Se isto não ocorrer, algo está errado e o administrador da rede deve ser procurado.

10.2 Protocolo LDAP

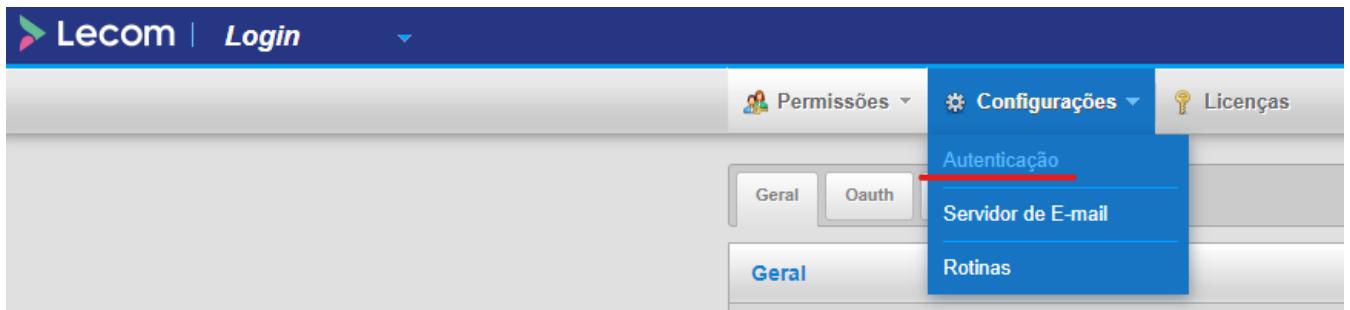
10.2.1 Introdução

A **Plataforma Lecom** possui o recurso de autenticação de usuário que utiliza o protocolo LDAP com os servidores: **Active Directory** da Microsoft, que é utilizado em ambientes Windows, e **Samba 4 AD**, que é utilizado em ambientes Linux.

10.2.2 Configuração

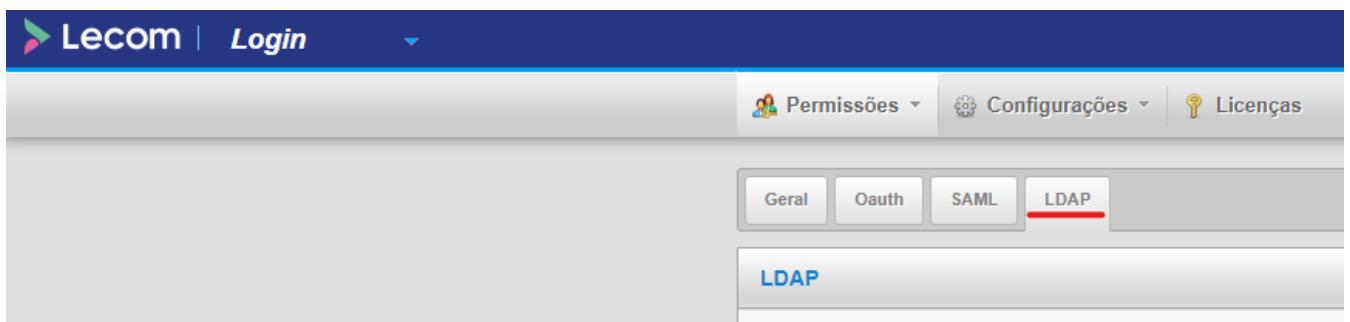
Para acessar a configuração, entre no módulo Login e no menu Configurações, entre em

Autenticação.



Acesso Tela de Configuração

Em seguida, accese a aba LDAP.



Acesso aba LDAP

O primeiro campo da tela indica se a forma de login está habilitada ou não.

The screenshot shows a form titled 'LDAP'. A checkbox labeled 'Habilitado' with a checked mark is highlighted with a red box.

Campo indicando se o LDAP está habilitado

Após esse campo, as configurações são divididas em três sessões: "Configurações Básicas", "Campos do LDAP usados pelo SSO" e "Campos para login automático".

The screenshot shows the 'Configurações Básicas' (Basic Configuration) section of the LDAP form. It contains the following fields:

- Urís:
- Base:
- User or DN:
- User search base:
- Password:
- Filter:

Sessão de configurações básicas

Na sessão “Configurações Básicas” (figura acima) temos os campos abaixo:

- **Urls:** campo usado para inserir uma ou mais urls do AD separados por vírgula.
Exemplo: “ldap://host1, ldap://host2, ldap://host3”.
Essas urls servem como forma de failover, ou seja, caso o primeiro host caia ou não esteja disponível, o segundo entra em ação e assim sucessivamente.
Também é possível usar SSL. Para isso é necessário o TOMCAT estar configurado com SSL e informar o protocolo ldaps e endereço seguido da porta:

Exemplo: “ldaps://host:636”.
Dessa forma, é necessário importar o certificado como trust dentro da keyStore usada pelo servidor apenas clicando no botão “Importar Certificado” que aparecerá logo após do campo “Urls” ser preenchido com um host SSL.
Para usar SSL é necessário usar o DNS do ldap. Não pode usar o IP diretamente.
- **Base:** campo usado para preenchimento dos objetos DC que representam o topo de uma árvore LDAP que usa o DNS para definir seu namespace. O AD é um exemplo de tal árvore LDAP. O designador para um domínio do AD com o nome DNS company.com seria dc=Company, dc=com.
- **User or DN:** campo usado para preenchimento do nome do usuário ou da DN. Um nome que inclua todo o caminho de um objeto para a raiz do namespace LDAP é chamado de nome distinto ou DN. Um exemplo de DN para um usuário chamado CSantana cujo objeto está armazenado no contêiner cn=Users em um domínio chamado company.com seria cn=CSantana, cn=Usuários, dc=company, dc=com.
- **User search base:** campo usado para preenchimento dos objetos da OU que atuam como contêineres que contêm outros objetos. Eles fornecem estrutura para o namespace LDAP. As OUs são o único contêiner de uso geral disponível para administradores no Active Directory. Um nome de OU de exemplo seria ou=Accounting. Esse campo além de ser usado no momento do login, é usado para importação dos usuários na base.
- **Password:** campo usado para preenchimento da senha do usuário definido no campo “User or DN”.
- **Filter:** campo usado para preenchimento do filtro usado no momento do login e para buscar usuários na importação de usuários do AD.

Urís *	Idaps://host1, Idap://host2, Idap://host3
<input type="button" value="Importar Certificado"/> <input type="button" value="Listar Certificados"/>	

Botão de Importar Certificado

Na sessão “Campos do LDAP usados pelo SSO” (figura abaixo) temos os campos abaixo:

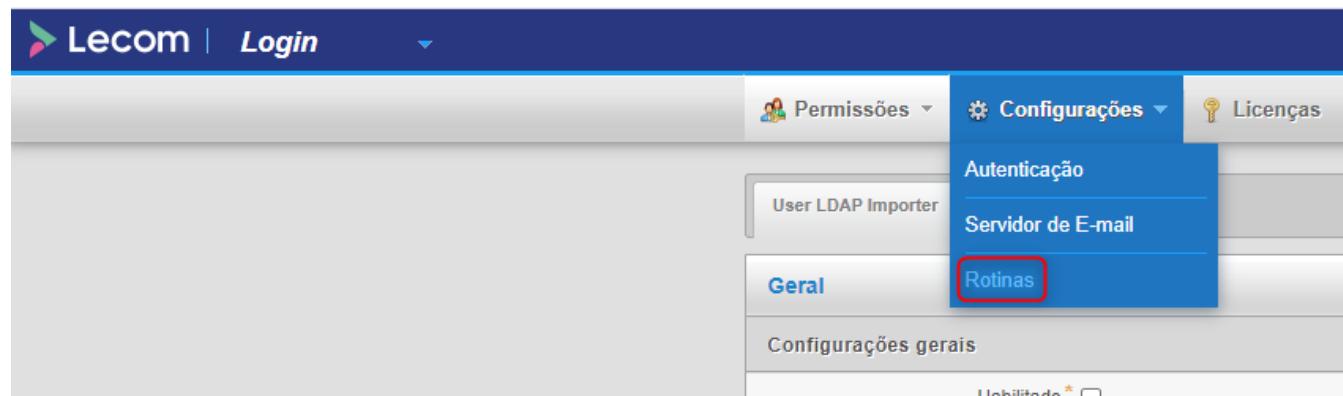
- **Login Key:** Campo usado para comparação do nome do usuário no momento do login.
- **Name Key:** Campo usado no momento da importação para indicar em que campo do AD está o nome do usuário.
- **Mail Key:** Campo usado no momento da importação para indicar em que campo do AD está o e-mail do usuário.

Campos do LDAP usados pelo SSO	
Login Key *	sAMAccountName
Name Key *	name
Mail Key *	mail

Sessão de campos do LDAP usados pelo SSO

10.2.3 Ativando importação automática

Para acessar a configuração, entre no módulo Login, accese o menu Configurações e, em seguida, Rotinas, conforme a imagem abaixo:



Acesso a Tela de Configuração

Configuração do Job de importação de usuários e grupos.

Área para configuração das unidades organizacionais. Elas devem ser adicionadas seguindo estrutura da figura abaixo.

Configurações gerais

Habilitado

Unidades Organizacionais

OU=PET,OU=LECOM

Campos de configuração de Unidades Organizacionais

Para configurar a importação dos grupos, veja a imagem abaixo, sendo necessário preencher os seguintes campos:

- Campo “Importar Grupos”: flag para habilitar/desabilitar a importação de grupos;
- Campo “Nome do Líder”: colocar o login do líder dos grupos que serão importados;
- Campo “objectClass”: tipo do objeto que o grupo representa no LDAP;
- Campo “Atributo de Distinção”: campo no LDAP que representa a distinção única de cada grupo;
- Campo “Atributo de Nome”: campo no LDAP que representa o nome do grupo;
- Campo “Acesso aos Recursos”: selecionar os recursos da plataforma que os grupos terão acesso.

Configurações de grupo

Importar Grupos

Nome do Líder adm

objectClass group

Atributo de Distinção distinguishedName

Atributo de Nome name

Acesso aos Recursos Login BPM

Campos de configuração de grupos

E para a área destinada para configuração da importação dos usuários, segue os demais campos:

- Campo “Alias da Licença”: campo para inserir o alias da licença, caso esteja usando licença por usuários.
- Campo “Senha”: senha do alias da licença.
- Campo “Atributo de Grupo”: campo no LDAP que representa no objeto do usuário o grupo que ele está. O valor desse campo deve ser o mesmo que está no campo “Atributo de Distinção” da sessão de grupo.
- Campo “Atributo de Status” (Obrigatório): Campo no LDAP que representa o status do usuário (habilitado/desabilitado).

- Campo “Valor para desabilitado” (Obrigatório): Valor para o campo “Atributo de Status” que representa quando o usuário está desabilitado.
- Campo “Atributo de Nome” (Obrigatório): Campo no LDAP que representa o nome do usuário.
- Campo “Atributo de Login” (Obrigatório): Campo no LDAP que representa o login do usuário.
- Campo “Atributo de E-mail” (Obrigatório): Campo no LDAP que representa o e-mail do usuário.

Configurações de usuário	
Alias da Licença	<input type="text"/>
Senha	<input type="password"/>
Grupo Padrão	<input type="text"/>
Atributo de Grupo	<input type="text"/> memberOf
Atributo de Status *	<input type="text"/> sAMAccountType
	<input type="text"/> Valor para desabilitado * <input type="text"/> 123
Atributo de Nome *	<input type="text"/> name
Atributo de Login *	<input type="text"/> sAMAccountName
Atributo de E-mail *	<input type="text"/> mail
Atributo de Rua	<input type="text"/>
Atributo de Número	<input type="text"/>
Atributo de Complemento	<input type="text"/>
Atributo de Cidade	<input type="text"/>
Atributo de Estado	<input type="text"/>
Atributo de Código Postal	<input type="text"/>
Atributo de Telefone	<input type="text"/>
Atributo de Celular	<input type="text"/>
Atributo de Campo de Integração 1	<input type="text"/>
Atributo de Campo de Integração 2	<input type="text"/>
Atributo de Campo de Integração 3	<input type="text"/>

Campos de configuração de usuários

O restante dos campos do usuário são campos do LDAP que representam cada um dos atributos descritos nos rótulos.

Após configurar, é necessário salvar. O job, por padrão, executa todo dia às 00:00. Se for necessário executar fora desse horário, é possível mudar essa configuração exportando a variável “LDAP_USERS_IMPORTER_CRON_EXPRESSION” com uma expressão cron. Caso seja preciso rodar manualmente, basta clicar no botão “Executar Agora” ao lado do botão salvar.

10.3 Protocolo OAUTH

10.3.1 Introdução

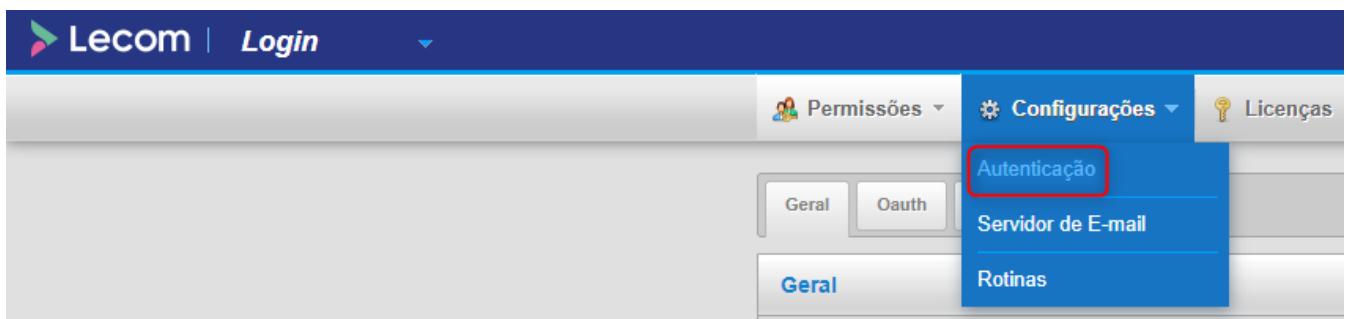
A Plataforma Lecom possui o recurso de autenticação de usuário que utiliza o protocolo OAuth2, que é um protocolo de autorização que permite que aplicativos obtenham acesso limitado a contas de usuários em um serviço HTTP sem a necessidade de enviar seu usuário e senha. Basicamente, o usuário delega, a um determinado aplicativo, acesso aos seus dados em um determinado serviço.

10.3.2 Pré-requisitos para Configuração

Para que a autenticação SAML funcione, é necessário que a plataforma esteja configurada com um certificado SSL válido.

10.3.3 Configuração

Para acessar a configuração, entre no módulo Login, acesse o menu Configurações e, em seguida, Autenticação. Clique na aba OAuth, conforme as imagens abaixo:



Acesso Tela de Configuração



Acesso aba OAuth

OAuth

Adicionar

Habilitado *	<input checked="" type="checkbox"/>		
Provedor de Autenticação *	<input type="text"/>		
ID do cliente *	<input type="text"/>		
Senha do cliente *	<input type="text"/>		
URI de token de acesso *	<input type="text"/>		
URI de autorização de usuário *	<input type="text"/>		
Esquema de autenticação do cliente *	<input type="text"/>		
URI de informação do usuário *	<input type="text"/>		
Usar a URI corrente	<input type="checkbox"/>		
URI de redirecionamento pré-estabelecido	<input type="text"/>		
Escopo	<input type="text"/>		
Nome do token	<input type="text"/>		
Esquema de autenticação	<input type="text"/>		
Caminho *	<input type="text"/>		
Extrator do identificador do usuário	<input type="text"/>		
<input type="button" value="Cancelar"/> <input type="button" value="Salvar"/>			
Status	Provedor de Autenticação		
Habilitado	Google	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>

Campos de configuração OAuth

O SSO permite que tenhamos uma lista de servidores OAuth, dessa forma as configurações ficaram dispostas de acordo com a figura acima, onde temos os campos e uma lista com todos os servidores já configurados.

Abaixo estão as descrições de todos os campos:

- Habilitado: Indica se o servidor está habilitado ou não. Caso ele não esteja selecionado, o servidor não aparecerá a tela de login;
- Provedor de Autenticação: combo com os provedores disponíveis para configuração. Hoje temos somente o Google;
- ID do cliente: campo para preenchimento do ID do cliente disponibilizado pelo Provedor de Autenticação no momento da configuração no mesmo;
- Senha do cliente: campo para preenchimento da Senha do cliente disponibilizado pelo

Provedor de Autenticação no momento da configuração no mesmo;

- URI de token de acesso: campo para preenchimento da URI que retorna o token. Este campo é preenchido automaticamente ao selecionar a opção “Google” no campo “Provedor de Autenticação”. Caso o valor seja diferente, é possível alterá-lo. Consultar documentação do provedor para mais informações;
- URI de autorização de usuário: campo para preenchimento da URI que faz a autorização do usuário. Este campo é preenchido automaticamente ao selecionar a opção “Google” no campo “Provedor de Autenticação”. Caso o valor seja diferente, é possível alterá-lo. Consultar documentação do provedor para mais informações;
- Esquema de autenticação do cliente: campo para preenchimento da forma de autenticação. Este campo é preenchido automaticamente ao selecionar a opção “Google” no campo “Provedor de Autenticação”. Caso o valor seja diferente, é possível alterá-lo. Consultar documentação do provedor para mais informações;
- URI de informação do usuário: campo para preenchimento da URI que busca as informações do usuário. Este campo é preenchido automaticamente ao selecionar a opção “Google” no campo “Provedor de Autenticação”. Caso o valor seja diferente, é possível alterá-lo. Consultar documentação do provedor para mais informações;
- Usar a URI corrente: check box indicador para usar a URI corrente para envio da requisição da autenticação do provedor. O campo não pode estar checado caso o ambiente esteja em cluster ou com algum proxy reverso;
- URI de redirecionamento pré-estabelecido: Campo usado para preenchimento da URI preestabelecida para ser enviada para o provedor de autenticação. Esse campo só deve ser usado caso o campo “Usar a URI corrente” não estiver marcado, caso contrário o preenchimento do mesmo não surtirá efeito;
- Escopo: Campo não obrigatório para preenchimento dos escopos. Consultar documentação do provedor para mais informações;
- Nome do token: Campo não obrigatório para preenchimento do nome do token enviado pelo provedor. Consultar documentação do provedor para mais informações;

- Esquema de autenticação: Campo não obrigatório para preenchimento do schema de autenticação. Consultar documentação do provedor para mais informações;
- Caminho: Campo para preenchimento do caminho da URI usado para autenticação. Usar sempre o padrão /oauth/<nome_do_provedor>/login;
- Extrator do identificador do usuário: Campo não obrigatório para preenchimento do nome da classe responsável por extrair o nome do usuário da resposta de autenticação do provedor. Alguns provedores não necessitam dessa configuração, contudo para o Google é necessário usar:

"br.com.lecom.oauth.connect.config.extractor.GooglePrincipalExtractor";

Após o preenchimento dos campos, clique em salvar, os dados irão para listagem que fica logo abaixo.

Na listagem é possível excluir ou editar as configurações já salvas.

Lembrando que alguns provedores podem se comportar de maneira diferente de outros. Hoje o SSO está homologado somente para o Google.

Obs: O Google somente permite o uso de um DNS que possui um domínio de topo válido. Ex: .com, .org, .net, .edu, .inf, .gov ou para testes usar localhost.

10.4 Protocolo SAML

10.4.1 Introdução

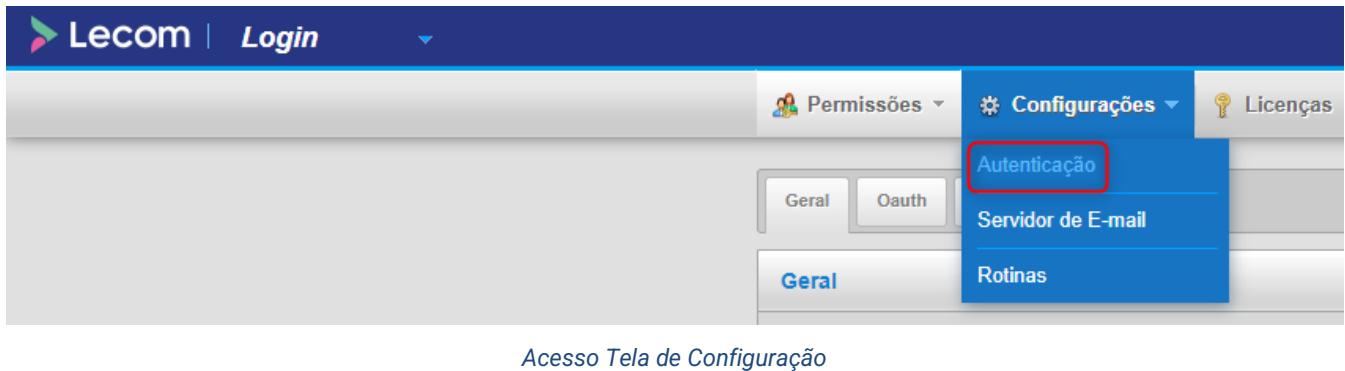
O SAML simplifica os processos federados de autenticação e autorização para usuários, provedores de identidade e provedores de serviços. O SAML oferece uma solução para permitir que seu provedor de identidade e provedores de serviços existam independentemente um do outro, o que centraliza o gerenciamento de usuários e permite acesso a soluções SaaS.

O SAML implementa um método seguro de transferência de autenticações e autorizações de usuário entre o provedor de identidade e os provedores de serviços. Quando um usuário faz login em um aplicativo que usa SAML, o provedor de serviços solicita autorização do provedor de

identidade apropriado. O provedor de identidade autentica as credenciais do usuário e, em seguida, retorna a autorização do usuário para o provedor de serviços. O usuário pode, então, usar o aplicativo.

10.4.2 Configuração

Para acessar a configuração, entre no módulo Login, acesse o menu Configurações e, em seguida, Autenticação. Clique na aba SAML, conforme as imagens abaixo:



This screenshot shows the 'SAML' configuration form. It includes fields for 'Nome do provedor' (with a required asterisk), 'Tipo de configuração' (set to 'Upload'), 'Arquivo' (with a 'Escolher arquivo' button), 'Caminho Keystore' (empty field), 'Senha Keystore' (empty field), and 'Chave predeterminada Keystore' (empty field). At the bottom right are 'Cancelar' and 'Salvar' buttons.

Campos de configuração SAML

Abaixo segue uma breve descrição dos campos mostrados na figura acima:

- **Habilitado:** Indica se o servidor está habilitado ou não. Caso ele não esteja selecionado, o servidor não aparecerá na tela de login.

- Nome do provedor: Identificador do provedor de autenticação. Este nome aparecerá no botão da tela de login.
- Tipo de configuração: Hoje permitimos dois tipos de configuração. Url e Upload. Quando é selecionado a opção Url, o campo Metadata URL deve ser preenchido com o caminho para o xml de metadados do provedor. Caso a opção selecionada seja Upload, aparecerá um campo para upload do xml de metadados do provedor.
- Metadata URL: Campo Metadata URL deve ser preenchido com o caminho para o xml de metadados do provedor. Só aparece caso o tipo de configuração seja Url.
- Metadata File: Campo para upload do xml de metadados do provedor. Só aparece caso o tipo de configuração seja Upload. O arquivo xml pode ser encontrado na seguinte URL: [URL-DO-AMBIENTE]/sso/saml/metadata;

Os próximos campos são necessários pois a comunicação do protocolo faz uma assinatura da chamada para que ela seja validada no provedor de autenticação com o mesmo xml de metadados que foi enviado no momento do cadastro no nosso serviço. Esse xml possui a nossa assinatura com base no nosso certificado SSL.

- Caminho Keystore: Caminho da keystore.
- Senha Keystore: Senha da keystore.
- Chave predeterminada Keystore: O host do provedor de autenticação deve ser importado dentro da keystore e a key criada para o mesmo deve ser inserida nesse campo.

Por final em “Nosso xml de Metadados”, temos um link para download do nosso xml de metadados contendo informações importantes do nosso serviço como a assinatura com base em nosso certificado, identificador único no nosso serviço além de outras informações. Lembrando que caso haja alguma alteração de nosso certificado digital, o cadastro de nosso serviço no provedor de autenticação deve ser renovado com o xml atualizado.

Apêndice A – Exemplo VHOST apache

Configuração para ambiente sem cluster

- Exemplo virtual host para redirecionamento http para https

```
<VirtualHost *:80>
    ServerName meudominio.com.br
    RewriteEngine on
    RewriteCond %{SERVER_NAME} =meudominio.com.br
    RewriteCond %{HTTPS} off
    RewriteRule ^ https:// %{SERVER_NAME}%{REQUEST_URI} [END,QSA,R=permanent]
</VirtualHost>
```

- Exemplo configuração virtual host https

```
<VirtualHost *:443>
    ServerName meudominio.com.br
    ProxyPreserveHost On
    ProxyRequests Off
    SSLProxyEngine on

    RewriteEngine on
    RewriteRule ^/$ https://192.168.1.2/bpm [R=301,L]

    # CADASTRO-FACIL
    ProxyPass /external/cadastros !
    Redirect /external/cadastros https://www.lecom.com.br/cadastrofacil
    # ROBERTY-RPA
    ProxyPass /external/roberty !
    Redirect /external/roberty https://www.lecom.com.br/rpa-ia
    # ADMIN-API
    ProxyPass /admin/api https://192.168.1.2:8181/admin/api
    ProxyPassReverse /admin/api https://192.168.1.2:8181/admin/api
    # ECM-API
    ProxyPass /ecmcore/api https://192.168.1.2:8181/ecmcore/api
    ProxyPassReverse /ecmcore/api https://192.168.1.2:8181/ecmcore/api
    # SKIP BPM-API
    <LocationMatch "^/bpm/api/v(.*)/process-instances/(.*)/activity-instances/(.*)/cycles/(.*)/fields/(.*)/documents/import">
        ProxyPass https://192.168.1.2
        ProxyPassReverse https://192.168.1.2
    </LocationMatch>
    <LocationMatch "^/bpm/api/v(.*)/process-instances/(.*)/activity-instances/(.*)/cycles/(.*)/documents/files/(.*)/download">
        ProxyPass https://192.168.1.2
        ProxyPassReverse https://192.168.1.2
    </LocationMatch>

    # BPM-API
    ProxyPass /bpm/api https://192.168.1.2:8181/bpm/api
    ProxyPassReverse /bpm/api https://192.168.1.2:8181/bpm/api

    ##BEHAVIOR-WEB
    ProxyPass "/behavior-web" https:// 192.168.1.2:3002/behavior-web
    ProxyPassReverse "/behavior-web" https:// 192.168.1.2:3002/behavior-web

    # Suite Lecom
    ## BPM
    ProxyPass "/bpm" https://192.168.1.2/bpm
    ProxyPassReverse "/bpm" https://192.168.1.2/bpm
```

```

## SSO
ProxyPass "/sso" https://192.168.1.2/sso
ProxyPassReverse "/sso" https://192.168.1.2/sso

## ECMCORE
ProxyPass "/ecmcore" https://192.168.1.2/ecmcore
ProxyPassReverse "/ecmcore" https://192.168.1.2/ecmcore
## BPM WEBSOCKET
ProxyPass "/core/websocket" wss://192.168.1.2/core/websocket
ProxyPassReverse "/core/websocket" wss://192.168.1.2/core/websocket
# BPM JUNTADA
ProxyPass "/bpm/calcularEtapasRestantesExportacao" wss://192.168.1.2/bpm/calcularEtapasRestantesExportacao
ProxyPassReverse "/bpm/calcularEtapasRestantesExportacao" wss://192.168.1.2/bpm/calcularEtapasRestantesExportacao

# Microservicos
## FORM-APP
ProxyPass "/form-app" https://192.168.1.2:8080/form-app
ProxyPassReverse "/form-app" https://192.168.1.2:8080/form-app
## GATEWAY
ProxyPass "/gateway" https://192.168.1.2:8181/gateway
ProxyPassReverse "/gateway" https://192.168.1.2:8181/gateway
## WORKSPACE-WEB
ProxyPass "/workspace" https://192.168.1.2:3000/workspace
ProxyPassReverse "/workspace" https://192.168.1.2:3000/workspace
## FORM-WEB
ProxyPass "/form-web" https://192.168.1.2:3001/form-web
ProxyPassReverse "/form-web" https://192.168.1.2:3001/form-web
## JOB-WEB
ProxyPass "/job-web" https://192.168.1.2:3003/job-web
ProxyPassReverse "/job-web" https://192.168.1.2:3003/job-web
# SOCIAL-SERVICE
ProxyPass /social-service/websocket wss://192.168.1.2:443/social-service/websocket
ProxyPassReverse /social-service/websocket wss://192.168.1.2:443/social-service/websocket
ProxyPass /social-service https://192.168.1.2:443/social-service
ProxyPassReverse /social-service https://192.168.1.2:443/social-service
## DISCOVERY
ProxyPass "/discovery" https://192.168.1.2:8761/
ProxyPassReverse "/discovery" https://192.168.1.2:8761/
ProxyPass "/eureka" https://192.168.1.2:8761/eureka
ProxyPassReverse "/eureka" https://192.168.1.2:8761/eureka
# APP EXT
ProxyPass /app-ext https://IP_SERVIDOR:8443
ProxyPassReverse /app-ext https://IP_SERVIDOR:8443
# Redirect root
ProxyPass "/" https://192.168.1.2/
ProxyPassReverse "/" https://192.168.1.2/

SSLCertificateFile /etc/apache2/ssl/meudominio.com.br/meudominio.com.br.crt
SSLCertificateKeyFile /etc/apache2/ssl/meudominio.com.br/meudominio.com.br.key
SSLCertificateChainFile /etc/apache2/ssl/meudominio.com.br/meudominio.com.br_CA.crt
Include /etc/apache2/ssl/config/options-ssl-apache.conf

</VirtualHost>

```

Exemplo de configuração para ambiente com cluster

- Exemplo virtual host para redirecionamento http para https

```
<VirtualHost *:80>
```

```

ServerName app.meudominio.com.br
Timeout 60000
RewriteEngine on
RewriteCond %{THE_REQUEST} !/.well-known/ [NC]
RewriteCond %{SERVER_NAME} =app.meudominio.com.br
RewriteCond %{HTTPS} off
RewriteRule ^ https:// %{SERVER_NAME}%{REQUEST_URI} [END,QSA,R=permanent]

</VirtualHost>

```

- Exemplo configuração virtual host https

```

<VirtualHost *:443>
ServerName app.meudominio.com.br
ProxyPreserveHost On
ProxyRequests Off
SSLPProxyEngine on
# COOKIE NODE ROUTED
Header add Set-Cookie "ROUTEID=.#{BALANCER_WORKER_ROUTE}e; path=/; Secure; HttpOnly"
env=BALANCER_ROUTE_CHANGED

# CADASTRO-FACIL
ProxyPass /external/cadastros !
Redirect /external/cadastros https://www.lecom.com.br/cadastrofacil
# ROBERTY-RPA
ProxyPass /external/roberty !
Redirect /external/roberty https://www.lecom.com.br/rpa-ia
# ADMIN-API
ProxyPass /admin/api balancer://gateway/admin/api
# ECM-API
ProxyPass /ecmcore/api balancer://gateway/ecmcore/api
# APP-EXT
ProxyPass /app-ext balancer://app-ext
# SKIP BPM-API
<LocationMatch "^/bpm/api/v(.*)/process-instances/(.*)/activity-instances/(.*)/cycles/(.*)/fields/(.*)/documents/import">
ProxyPass balancer://bpm
ProxyPassReverse balancer://bpm
</LocationMatch>
<LocationMatch "^/bpm/api/v(.*)/process-instances/(.*)/activity-instances/(.*)/cycles/(.*)/documents/files/(.*)/download">
ProxyPass balancer://bpm
ProxyPassReverse balancer://bpm
</LocationMatch>
# BPM-API
ProxyPass /bpm/api balancer://gateway/bpm/api
# Suite Lecom
## BPM
ProxyPass "/bpm" balancer://bpm/bpm
<Proxy balancer://bpm>
BalancerMember https://IP_NODE_01 route=node01 loadfactor=1
BalancerMember https://IP_NODE_02 route=node02 loadfactor=1
ProxySet stickyssession=ROUTEID
</Proxy>

<Proxy balancer://app-ext>
BalancerMember https://IP_NODE_01:8443 route=node01 loadfactor=1
BalancerMember https://IP_NODE_02:8443 route=node02 loadfactor=1
ProxySet stickyssession=ROUTEID
</Proxy>

## BEHAVIOR-WEB
ProxyPass "/behavior-web" balancer://behavior-web/behavior-web
<Proxy balancer://behavior-web>

```

```

BalancerMember https://IP_NODE_1:3002 route=node01 loadfactor=1
BalancerMember https://IP_NODE_2:3002 route=node02 loadfactor=1
ProxySet stickysession=ROUTEID
</Proxy>
## JOB-WEB
ProxyPass "/job-web" balancer://job-web/job-web
<Proxy balancer://job-web>
BalancerMember https://IP_NODE_1:3003 route=node01 loadfactor=1
BalancerMember https://IP_NODE_2:3003 route=node02 loadfactor=1
ProxySet stickysession=ROUTEID
</Proxy>

## SSO
ProxyPass "/sso" balancer://sso/sso
<Proxy balancer://sso>
BalancerMember https://IP_NODE_01 route=node01 loadfactor=1
BalancerMember https://IP_NODE_02 route=node02 loadfactor=1
ProxySet stickysession=ROUTEID
</Proxy>
## CORE
ProxyPass "/core" balancer://core/core
<Proxy balancer://core>
BalancerMember https://IP_NODE_01 route=node01 loadfactor=1
BalancerMember https://IP_NODE_02 route=node02 loadfactor=1
ProxySet stickysession=ROUTEID
</Proxy>
## ECMCORE
ProxyPass "/ecmcore" balancer://ecmcore/ecmcore
<Proxy balancer://ecmcore>
BalancerMember https://IP_NODE_01 route=node01 loadfactor=1
BalancerMember https://IP_NODE_02 route=node02 loadfactor=1
ProxySet stickysession=ROUTEID
</Proxy>
## BPM WEBSOCKET
ProxyPass /core/websocket balancer://websocket/core/websocket
<Proxy balancer://websocket>
BalancerMember wss://IP_NODE_01 route=node01 loadfactor=1
BalancerMember wss://IP_NODE_02 route=node02 loadfactor=1
ProxySet stickysession=ROUTEID
</Proxy>
# BPM JUNTADA
ProxyPass "/bpm/calcularEtapasRestantesExportacao" balancer://juntada/bpm/calcularEtapasRestantesExportacao
<Proxy balancer://juntada>
BalancerMember wss://IP_NODE_01 route=node01 loadfactor=1
BalancerMember wss://IP_NODE_02 route=node02 loadfactor=1
ProxySet stickysession=ROUTEID
</Proxy>
# Microservicos
## FORM-APP
ProxyPass "/form-app" balancer://form-app/form-app
<Proxy balancer://form-app>
BalancerMember https://IP_NODE_01:8080 route=node01 loadfactor=1
BalancerMember https://IP_NODE_02:8080 route=node02 loadfactor=1
ProxySet stickysession=ROUTEID
</Proxy>
## GATEWAY
ProxyPass "/gateway" balancer://gateway
<Proxy balancer://gateway>
BalancerMember https://IP_NODE_01:8181 route=node01 loadfactor=1
BalancerMember https://IP_NODE_02:8181 route=node02 loadfactor=1
ProxySet stickysession=ROUTEID
</Proxy>
## WORKSPACE-WEB
ProxyPass "/workspace" balancer://workspace/workspace

```

```

<Proxy balancer://workspace>
  BalancerMember https://IP_NODE_01:3000 route=node01 loadfactor=1
  BalancerMember https://IP_NODE_02:3000 route=node02 loadfactor=1
  ProxySet stickyssession=ROUTEID
</Proxy>
## FORM-WEB
ProxyPass "/form-web" balancer://form-web/form-web
<Proxy balancer://form-web>
  BalancerMember https://IP_NODE_01:3001 route=node01 loadfactor=1
  BalancerMember https://IP_NODE_02:3001 route=node02 loadfactor=1
  ProxySet stickyssession=ROUTEID
</Proxy>
# SOCIAL-SERVICE
#<Location /social-service >
# Require ip 127.0.0.1
#</Location>
ProxyPass /social-service/websocket balancer://wss-social-service/social-service/websocket
<Proxy balancer://wss-social-service>
  BalancerMember wss://IP_NODE_01:443 route=node01 loadfactor=1
  BalancerMember wss://IP_NODE_02:443 route=node02 loadfactor=1
  ProxySet stickyssession=ROUTEID
</Proxy>
ProxyPass /social-service balancer://social-service/social-service
<Proxy balancer://social-service>
  BalancerMember https://IP_NODE_01:443 route=node01 loadfactor=1
  BalancerMember https://IP_NODE_02:443 route=node02 loadfactor=1
  ProxySet stickyssession=ROUTEID
</Proxy>
## DISCOVERY
ProxyPass "/discovery" balancer://discovery
ProxyPass "/eureka" balancer://discovery/eureka
<Proxy balancer://discovery>
  BalancerMember https://IP_NODE_01:8761 route=node01 loadfactor=1
  BalancerMember https://IP_NODE_02:8761 route=node02 loadfactor=1
  ProxySet stickyssession=ROUTEID
</Proxy>
# Redirect root
ProxyPass "/" balancer://root/
<Proxy balancer://root>
  BalancerMember https://IP_NODE_01 route=node01 loadfactor=1
  BalancerMember https://IP_NODE_02 route=node02 loadfactor=1
  ProxySet stickyssession=ROUTEID
</Proxy>
# BALANCER MANAGER
ProxyPass /balancer-manager !
<Location /balancer-manager>
  setHandler balancer-manager
  Order Deny,Allow
  Deny from all
  Allow from 179.127.59.195
  Allow from 200.174.141.98
</Location>
SSLCertificateFile /etc/apache2/ssl/app.meudominio.com.br/app.meudominio.com.br.crt
SSLCertificateKeyFile /etc/apache2/ssl/app.meudominio.com.br/app.meudominio.com.br.key
</VirtualHost>

```