**ACESSANDO UM REPOSITÓRIO (DOCKER REGISTRY) PRIVADO DO SERVIDOR LOCAL**

PASSO 1 - Acesse o servidor que está sendo utilizado como PRIVATE REGISTRY (Repositório privado para imagens do docker).

PASSO 2 - No servidor que está sendo utilizado como PRIVATE REGISTRY, execute o comando abaixo para que possa enviar os certificados gerados para a máquina cliente, ou seja, para a máquina que está irá se conectar no repositório privado em questão.

COMANDO: **scp -p DIGITE\_O\_CAMINHO\_ABSOLUTO\_COM\_O\_NOME\_ARQUIVO\_A\_SER\_ENVIADO DIGITE\_O\_NOME\_DO\_USUARIO\_COM\_PERMISSAO\_ADMIN\_NO\_HOST\_DESTINO@DIGITE\_O\_HOSTNAME\_OU\_IP-ADDRESS\_DO\_HOST\_DESTINO:/DIGITE\_O\_CAMINHO\_ABSOLUTO\_QUE\_RECEBERA\_O\_ARQUIVO\_NO\_HOST\_DESTINO/**

EXEMPLO:

Texto alternativo gerado por máquina:
sc /o t/docker/certs/* vintcuus . t/docker/ rivate re ustr /certs/ 
The authenticity of os 
can 
e es a us e 
ED25519 key fingerprint is SHA256:U29AZ9hf8p+HziM3sclC/va9azjKHfzZRdWJ8+LjxXM. 
This key is not known by any other names . 
Are you sure you want to continue connecting (yes/no/Cfingerprint])? yes 
Warning: permanently added 192. 168.0.203' (ED25519) to the list of known hosts . 
vinicius.nunes@192.168.0.203is password: 
permiss ion denied, 
doma . crt 
doma in . key 
please try again. 
199% 
100% 
2017 
3268 
6. 5MB/s 
16 . OMB/s 
ee:ee 
ee:ee 

PASSO 3 - Agora acesse a máquina cliente que voce enviou os arquivos de certificado no passo anterior, e então, execute o comando abaixo para validar se os arquivos enviados estão presentes na máquina em questão.

COMANDO: **ls -lhs /DIGITE\_O\_CAMINHO\_ABSOLUTO\_DO\_DIRETÓRIO\_EM\_QUE\_AS\_CHAVES\_FORAM\_ENVIADAS/**

EXEMPLO:

Texto alternativo gerado por máquina:
rootesv-SRV 
rootesv-SRV 
total 8.0K 
4.9K -rw-r- 
4.9K -rw- 
rootesv-SRV 
rootesv-SRV 
-ZABBIX: /opt/docker# 
-ZABBIX:/opt/docker# Is -Ihs /opt/docker/private_registry/certs/ 
1 vunucuus .nunes vunucuus .nunes 2.0K Oct 2 16:27 domavn.crt 
1 vintcuus . nunes vunucuus .nunes 3.2K Oct 2 16:27 domain.key 
-ZABBIX: /opt/docker# 
-ZABBIX:/opt/docker# 

PASSO 4 - Ainda na máquina cliente, execute o comando abaixo, para que possamos realizar a criação de um novo diretório contendo o nome do domínio que o certificado em questão representa.

COMANDO: **mkdir -p /DIGITE\_O\_CAMINHO\_ABSOLUTO\_DO\_DIRETÓRIO\_QUE\_VOCE\_DESEJA\_CRIAR/NOME\_DO\_DOMÍNIO\_QUE\_FOI\_DEFINIDO\_NA\_CRIAÇÃO\_DO\_CERTIFICADO:NÚMERO\_DA\_PORTA\_QUE\_A\_IMAGEM\_DO\_REGISTRY\_PRIVADO\_NO\_SERVIDOR\_DE\_REGISTRY\_PRIVADO\_ESTA\_UTILIZANDO**

EXEMPLO:

Texto alternativo gerado por máquina:
root@SV 
root@SV 
root@SV 
root@SV 
- SRV-ZABBIX. 
- SRV-ZABBIX. 
- SRV-ZABBIX. 
- SRV-ZABBIX. 
/opt/docker# 
/opt/docker# 
/opt/docker# 
/opt/docker# 
mkdir 
-p 
/opt/docker/certs . SRV-LAB04. local : 5000/ 

PASSO 5 - Ainda na máquina cliente, execute o comando abaixo, para que possamos agora realizar a cópia do arquivo de certificado .CRT do diretório que o mesmo esta, conforme definido no PASSO 3, e então, deveremos copiar este arquivo deste devido diretório do PASSO 3 para o diretório do PASSO 4.

COMANDO: **cp -v /DIGITE\_O\_DO\_DIRETORIO\_CONFORME\_PASSO-3 DIGITE\_O\_CAMINHO\_ABSOLUTO\_DO\_DIRETORIO\_CONFORME\_PASSO-4**

EXEMPLO:

Texto alternativo gerado por máquina:
/opt/docker/private_regus 
/opt/docker/private 
y cer s omaun.cr 
registry/certs/domain.crt /opt/docker/certs .d/SV-SRV-LABe4.IocaI:5eee 
oc er cer s. 

PASSO 6 - Ainda na máquina cliente, execute o comando abaixo, para que a máquina cliente possa conseguir resolver o DNS do domínio em questão, onde este determinado DNS deve responder para o IP Address do servidor de REGISTRY PRIVADO.

COMANDO: **echo "DIGITE\_O\_ENDEREÇO\_IP\_DO\_SERVIDOR\_DE\_REGISTRY\_PRIVADO DIGITE\_O\_NOME\_COMPLETO\_DO\_DOMÍNIO\_QUE\_O\_CERTIFICADO\_REPRESENTA" >> /etc/hosts**

EXEMPLO:

Texto alternativo gerado por máquina:
root@SV 
root@SV 
root@SV 
- SRV-ZABBIX. 
- SRV-ZABBIX. 
- SRV-ZABBIX. 
/opt/docker# 
/opt/docker# 
/opt/docker# 
ec 
" 92. 
68.0.20 
SV-SRV-LABO 
oca 
" /etc/ osts 

PASSO 7 - Ainda na máquina cliente, execute o comando abaixo para que possamos verificar se a entrada fornecida no passo anterior já está presente no arquivo /etc/hosts

COMANDO: **cat /etc/hosts**

EXEMPLO:

Texto alternativo gerado por máquina:
echo "192. 168.9.294 SV-SRV-LAB04.local" 
root@SV 
root@SV 
root@SV 
root@SV 
root@SV-SRV-ZABBIX:/opt/docker# cat /etc/hosts 
. 1 localhost 
127.0.a 
1 ubuntu-server 
127.9. 1. 
# The following lines are des irable for IPv6 capable 
ip6-IocaIhost ip6-Ioopback 
feee: 
ip6-IocaInet 
ffee: 
ip6-mcastprefux 
ip6-aIInodes 
92. 168.0. 204 SV-SRV-LABe4.local 
t,' aoc 
root@SV 
/etc/hosts 

PASSO 8 - Ainda na máquina cliente, execute o comando abaixo para que possamos validar a resolução de nomes para o DNS inserido no arquivo /etc/hosts em tempo real.

COMANDO: **ping DIGITE\_O\_ENDEREÇO\_DNS\_QUE\_FOI\_DEFINIDO**

EXEMPLO:

Texto alternativo gerado por máquina:
ping SV-SRV-LAB04 
. local 
PING SV-SRV-LAB04.local (192.16 
es o data. 
oy 
64 bytes from SV-SRV-LABe4.local (192. 168.0.204)• 
ttI=64 time=e .226 ms 
64 bytes from SV-SRV-LABe4.local (192. 
ttI=64 time=e . 208 ms 
bytes from SV-SRV-LABe4.local (192. 168.0 
. 204): ttI=64 time=O . 189 ms 
64 bytes from SV-SRV-LABe4.local (192. 168.0.204) • 
ttI=64 time=e . 208 ms 
SV-SRV-LABe4.IocaI ping statustucs 
4 packets transmitted, 4 received, packet loss, 
time 3656ms 
rtt min/avg/max/mdev — 
e. 189/9.296/6.226/6.611 ms 
roo 

PASSO 9 - Ainda na máquina cliente, execute o comando abaixo, para que possamos então realizar o download de uma imagem alocada no servidor local de PRIVATE REGISTRY.

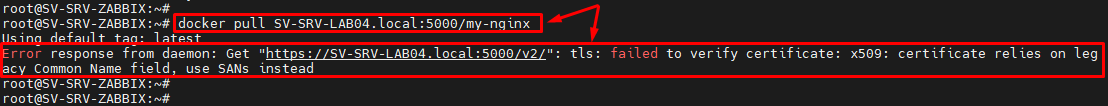
COMANDO: **docker pull DIGITE\_O\_NOME\_DO\_DOMÍNIO:NÚMERO\_DA\_PORTA\_QUE\_A\_IMAGEM\_DO\_REGISTRY\_PRIVADO\_NO\_SERVIDOR\_DE\_REGISTRY\_PRIVADO\_ESTA\_UTILIZANDO**

EXEMPLO:

Texto alternativo gerado por máquina:
docker pull sv-SRv-LABe4.local:5999/my-nginx 
Us ing default tag: Ia es 
latest: Pulling from my-nginx 
a803e7c4b030: Pull complete 
8b625c47d697: Pull complete 
4d3239651a63: Pull complete 
Of816efa513d: Pull complete 
Old159b8db2f: Pull complete 
5fb9a81470f3: Pull complete 
9b1e1e7164db: Pull complete 
Digest: sha256:b2888fc9cfe7cd9d6727aeb462d13c7c45dec413b66f2819a36c4a3cb9d4df75 
Status: Downloaded newer image for SV-SRV-LAB04. local 
SV- SRV- LAB04. local : -ng inx: Iates t 

PASSO 10 - CASO VOCE OBTENHA O ERRO ABAIXO DURANTE A EXECUÇÃO DO COMANDO ACIMA, SIGA OS PASSOS ABAIXO, SE NÃO OBTEVE O MESMO ERRO, ENTÃO PULE PARA O PASSO 11.

**ERRO NA MÁQUINA CLIENTE:**



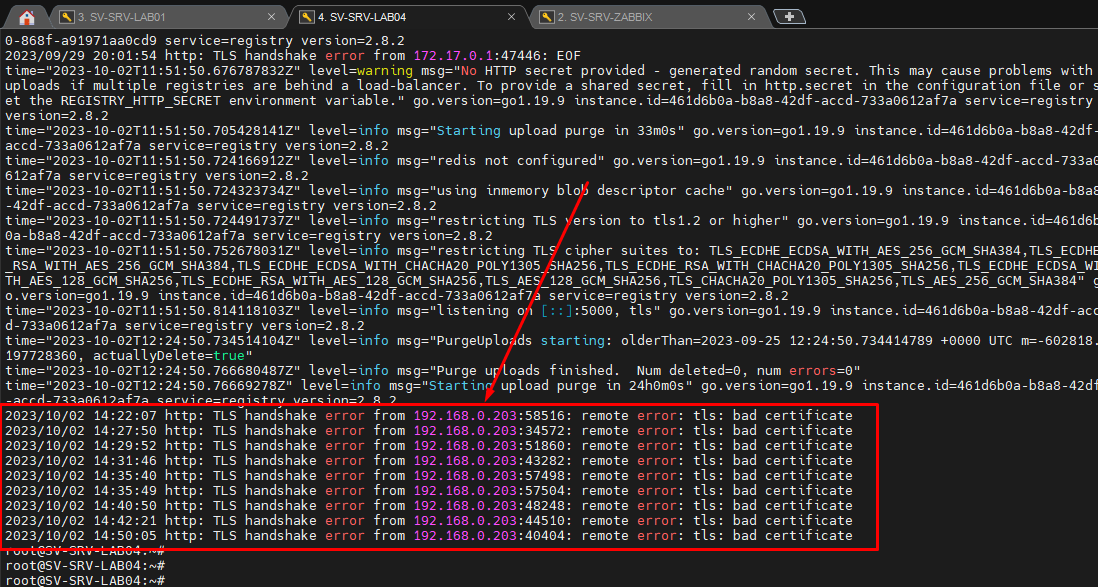
2 - ACESSE O SERVIDOR RESPONSÁVEL PELO PRIVATE REGISTRY E EXECUTE O COMANDO ABAIXO, PARA QUE POSSAMOS VERIFICAR QUAL O ERRO ESTA SENDO APRESENTADO NAS LOGS EM RELAÇÃO AO CERTIFICADO.

COMANDO: **docker logs DIGITE\_O\_HASH-ID\_DO\_CONTAINER\_DA\_DETERMINADA\_IMAGEM\_QUE\_VOCE\_ESTA\_TENTANDO\_REALIZAR\_O\_DOWNLOAD\_NA\_MÁQUINA\_CLIENTE**

EXEMPLO:

Texto alternativo gerado por máquina:
rnNTATNF 
08bc996c6fb4 
IMAGE 
docker ps 
"/entrypoint .sh /etcm" 
docker Iogs 08bc996c6fb4' 
CREATED 
s ago 
STATUS 
Up 3 hours 
PORTS 
NAMES 
myregistry 

Conforme as logs abaixo, os erros de certificado que estamos enfrentando estão relacionados à comunicação segura (TLS/SSL) entre o cliente Docker (no seu caso, o servidor que está tentando puxar a imagem) e o registro privado. O erro específico é "tls: bad certificate", o que indica que há um problema com o certificado SSL configurado no seu registro privado ou que o cliente Docker não confia no certificado.



**SOLUÇÃO:**

**PROCEDIMENTO A SER SEGUIDO SOMENTE EM AMBIENTE DE LABORATÓRIO:**

1 - Na máquina cliente, execute o comando abaixo, onde este comando cria um arquivo daemon.json no diretório /etc/docker/ com a configuração para aceitar o nosso registro privado em questão, que no caso é **SV-SRV-LAB04.local:5000** , e então, será aceito este registro privado como inseguro.

COMANDO: **echo '{"insecure-registries": ["DIGITE\_O\_NOME\_DO\_DO\_DOMÍNIO\_DO\_SEU\_REGISTRY\_PRIVADO:DIGITE\_O\_NUMÉRO\_DA\_PORTA\_QUE\_A\_DETERMINADA\_IMAGEM\_ESTA\_UTILIZANDO\_NO\_SERVIDOR\_DO\_REGISTRY\_PRIVADO"]}' | sudo tee /etc/docker/daemon.json**

EXEMPLO:

Texto alternativo gerado por máquina:
C "SV-SRV-LAB64. local 
{'l insecure-registries" 
echo insecure- regustrues" 
C "SV-SRV-LAB04. local : 5666 " 
sudo tee /etc/docker/daemon . json 

2 - Agora execute o comando abaixo, para que o serviço do docker seja reiniciado e então, as configurações do arquivo .json criado no passo anterior entre em vigor.

**EM GERENCIADOR DE DAEMON SystemD:**

COMANDO: **systemctl restart docker.service**

EXEMPLO:

Texto alternativo gerado por máquina:
sudo tee /etc/docker/daemon . json 
{'l insecure-registries" 
root@SV-SRV-ZABBIX: 
root@SV-SRV-ZABBIX: 
echo insecure- reg ustrues" 
C "SV-SRV-LAB64. local 
C "SV-SRV-LABe4.local 
systemctl restart docker .servuce 

**EM GERENCIADOR DE DAEMON SystemV:**

COMANDO: **service docker stop ; service docker start**

3 - Por fim, ainda na máquina cliente, execute o comando abaixo, para que possamos então realizar o download de uma imagem alocada no servidor local de PRIVATE REGISTRY.

COMANDO: **docker pull DIGITE\_O\_NOME\_DO\_DOMÍNIO:NÚMERO\_DA\_PORTA\_QUE\_A\_IMAGEM\_DO\_REGISTRY\_PRIVADO\_NO\_SERVIDOR\_DE\_REGISTRY\_PRIVADO\_ESTA\_UTILIZANDO**

EXEMPLO:

Texto alternativo gerado por máquina:
docker pull sv-SRv-LABe4.local:5999/my-nginx 
Us ing default tag: Ia es 
latest: Pulling from my-nginx 
a803e7c4b030: Pull complete 
8b625c47d697: Pull complete 
4d3239651a63: Pull complete 
Of816efa513d: Pull complete 
Old159b8db2f: Pull complete 
5fb9a81470f3: Pull complete 
9b1e1e7164db: Pull complete 
Digest: sha256:b2888fc9cfe7cd9d6727aeb462d13c7c45dec413b66f2819a36c4a3cb9d4df75 
Status: Downloaded newer image for SV-SRV-LAB04. local 
SV- SRV- LAB04. local : -ng inx: Iates t 

**PROCEDIMENTO A SER SEGUIDO SOMENTE EM AMBIENTE DE PRODUÇÃO:**

**1 - Certificado Inválido no Registro Privado:**

Certifique-se de que o certificado SSL do seu registro privado esteja válido e não tenha expirado.

Se você está usando um certificado autoassinado, considere gerar um certificado SSL válido ou usar um serviço como o Let's Encrypt para obter um certificado SSL confiável e gratuito.

**2 - Configurar o Cliente Docker para Confiar no Certificado:**

Adicione o Certificado SSL à Loja de Certificados do Sistema:

Você precisa adicionar o certificado SSL do seu registro privado à loja de certificados do sistema no servidor que está executando o cliente Docker.

COMANDO: cp -rfv /caminho/para/seu-certificado.crt /usr/local/share/ca-certificates/ ; update-ca-certificates ; systemctl restart docker.service

**3 - Problemas com Nome Comum do Certificado (Common Name Mismatch):**

Certifique-se de que o Nome Comum (Common Name) ou os Subject Alternative Names (SANs) no certificado correspondem ao nome de domínio ou ao endereço IP usado para acessar o registro privado.

Se você estiver usando um nome de domínio, verifique se ele está configurado corretamente no DNS e se o certificado SSL contém o nome de domínio como CN ou SAN.

PASSO 11 - Ainda na máquina cliente, execute o comando abaixo, para que possamos visualizar a imagem que realizamos o download a do PRIVATE REGISTRY (repositório privado local no servidor interno).

COMANDO: **docker images**

EXEMPLO:

Texto alternativo gerado por máquina:
root@SV-SRV-ZABBIX• 
REPOSITORY 
SV-SRV-LAB04.local. 
docker ima 
5000/my-ng inx 
es 
TAG 
latest 
IMAGE ID 
rap, 1 
61395b4c586d 
CREATED 
12 days ago 
SIZE 
187MB 

PASSO 12 - Executando todos os passos anteriores corretamente, teremos então a solução do PRIVATE REGISTRY rodando em um servidor local de nossa infraestrutura com sucesso, podendo ser utilizado para armazenar as imagens que não podem ser expostas na web por exemplo.