1800.BR.134.607500

Roteiro “pre-reqs” EKS

# Configuração do acesso CLI na estação Windows

1. Instalar o AWS CLI pela Loja de Sofware

Interface gráfica do usuário

Descrição gerada automaticamente

Escolher a versão mais recente

Texto

Descrição gerada automaticamente

1. Configurar a autenticação pelo OKTA, conforme procedimento: [How to use the AWS CLI with Okta authentication usin SAML2OKTA - EITS DevSecOps PaaS Brazil - Confluence Global (experian.com)](https://pages.experian.com/display/EDPB/How+to+use+the+AWS+CLI+with+Okta+authentication+usin+SAML2OKTA#method1)

# AWS Secondary IP Address

1. If your account does not have a secondary IP range, please [submit a request](https://pages.experian.com/display/SC/Contact+EITS+Cloud+Engineering#expand-OpenaServiceNowRequest) to the Cloud Team to add a secondary Subnet/IP Range (100.64.0.0/16) to your VPC with 3 AZs.

Para verificar os ranges de IP da VPC, executar o comando:

aws ec2 describe-vpcs --profile lab01 --no-verify-ssl --query "Vpcs[].CidrBlockAssociationSet[\*]” --output json

1. Validate if your VPC is tagged with "AWS\_Solutions = LandingZoneStackSet", your Experian IP range subnets with "Network = Private" and the Pod IP range (100.64.0.0/16) subnets with "Network = Pod".

aws ec2 describe-subnets --profile lab01 --no-verify-ssl --query "Subnets[].[SubnetId,CidrBlock,Tags[?Key=='Name'].Value[],Tags[?Key=='Network'].Value[]]" --output text

# Firewall Rules

1. The BU team needs to open a firewall request to allow the traffic outbound.  
   IMPORTANT NOTE: When BU team open this request, always need to mention that the traffic will go through the CSS Egress (CSS firewall rule must be applied).

Raise a new request  [to Global Firewall Team](https://experian.service-now.com/com.glideapp.servicecatalog_cat_item_view.do?v=1&sysparm_id=6865efd3dbbce3442511fa910f961993&sysparm_link_parent=7db4aadfdb4383007bd1317ffe961921&sysparm_catalog=e0d08b13c3330100c8b837659bba8fb4&sysparm_catalog_view=catalog_default&sysparm_view=catalog_default)

Rules to be requested:

| Source | Destination | Protocol | Port | Business Justification |
| --- | --- | --- | --- | --- |
| Your AWS CIDR/Subnet (Ex. 10.99.128.0/24) | 10.52.149.0/24 | TCP | 443 | Due to the migration from AppCanvas to EKS we need the VPC to have access in our Nexus Repository to download some Helm charts for VPC CNI and Observability.  The traffic will go through the CSS Egress (CSS firewall rule must be applied). |

# Change egress connection to CSS

Não é necessário solicitar - A configuração do 0.0.0.0/0 já vem de padrão nas contas

# AWS Endpoints

Make sure the VPC Endpoints below are associated to the account using the instances subnets (10.\*). You can create the endpoints manually.

com.amazonaws.sa-east-1.ecr.api

com.amazonaws.sa-east-1.ecr.dkr

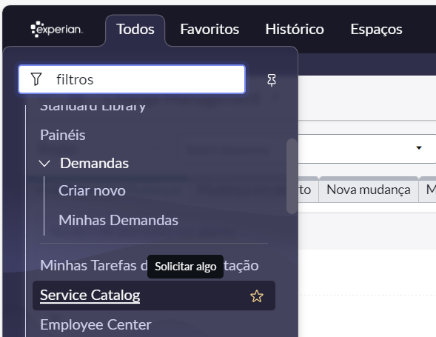
com.amazonaws.sa-east-1.ec2

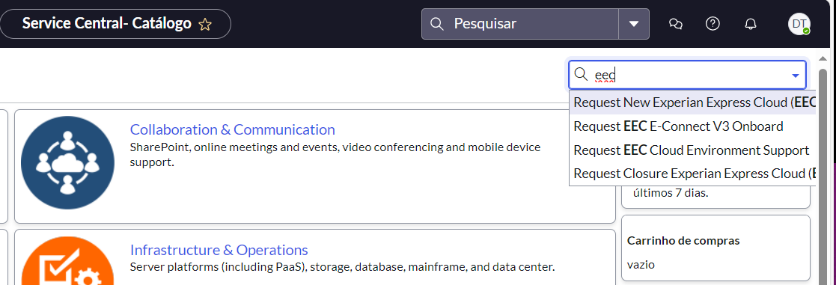
com.amazonaws.sa-east-1.logs

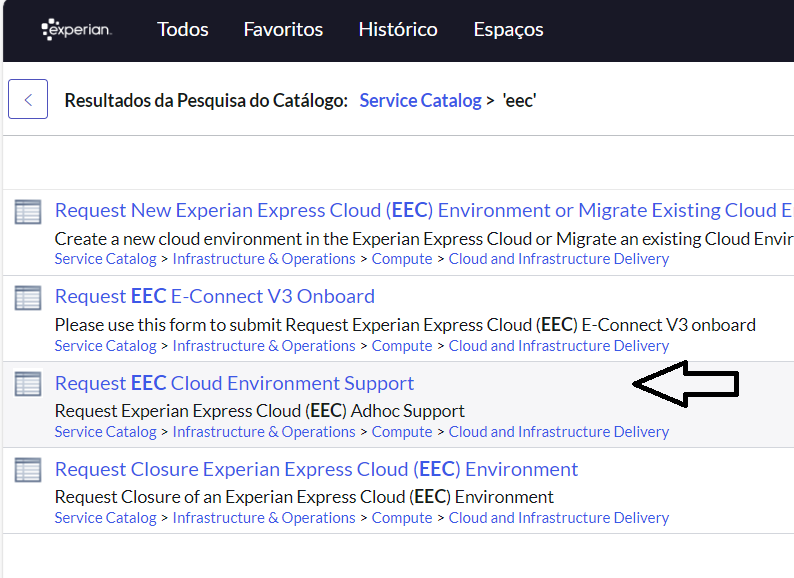
While creating the VPC Endpoints select or create a security group (sg-endpoints) that allows TCP port 443 at Inbound rule from source 10.0.0.0/8, otherwise you'll face the error "NodeCreationFailure: Instances failed to join the kubernetes cluster" during the cluster node groups creation.

If you're using Kubeflow, also allow TCP port 443 at Inbound rule from source 100.64.0.0/16 in the security group (sg-endpoints).

1. Para essa atividade, primeiro é necessário abrir uma REQ para o EEC, solicitando “desvincular os Endpoints da Sharedservices”







Seguir conforme explicado no: [Contact EITS Cloud Engineering - Cloud Engineering - Confluence Global (experian.com)](https://pages.experian.com/display/SC/Contact+EITS+Cloud+Engineering#expand-OpenaServiceNowRequest)

1. Depois criar o SG, as regras e os endpoints, usando os comandos a seguir:

# Criar o SG para os endpoints

aws ec2 create-security-group --group-name endpoints-sg --description "SG for endpoints - EKS pre-reqs" --vpc-id vpc-085f31990074f17ab --profile lab01 --no-verify-ssl

# Adicionar regras para o SG

aws ec2 authorize-security-group-ingress --group-id sg-00232e594d9d496a1 --protocol tcp --port 80 --cidr 10.0.0.0/8 --profile lab01 --no-verify-ssl

aws ec2 authorize-security-group-ingress --group-id sg-00232e594d9d496a1 --protocol tcp --port 443 --cidr 100.64.0.0/16 --profile lab01 --no-verify-ssl

# Criar VPC Endpoints

aws ec2 create-vpc-endpoint --vpc-endpoint-type Interface --vpc-id vpc-085f31990074f17ab --service-name com.amazonaws.sa-east-1.ecr.api --security-group-ids "sg-00232e594d9d496a1" --subnet-ids "subnet-09b31519466ea770c" "subnet-0cd04680da6d95113" "subnet-04756c2417c30202e" --profile lab01 --no-verify-ssl

aws ec2 create-vpc-endpoint --vpc-endpoint-type Interface --vpc-id vpc-085f31990074f17ab --service-name com.amazonaws.sa-east-1.ecr.dkr --security-group-ids "sg-00232e594d9d496a1" --subnet-ids "subnet-09b31519466ea770c" "subnet-0cd04680da6d95113" "subnet-04756c2417c30202e" --profile lab01 --no-verify-ssl

aws ec2 create-vpc-endpoint --vpc-endpoint-type Interface --vpc-id vpc-085f31990074f17ab --service-name com.amazonaws.sa-east-1.ec2 --security-group-ids "sg-00232e594d9d496a1" --subnet-ids "subnet-09b31519466ea770c" "subnet-0cd04680da6d95113" "subnet-04756c2417c30202e" --profile lab01 --no-verify-ssl

aws ec2 create-vpc-endpoint --vpc-endpoint-type Interface --vpc-id vpc-085f31990074f17ab --service-name com.amazonaws.sa-east-1.logs --security-group-ids "sg-00232e594d9d496a1" --subnet-ids "subnet-09b31519466ea770c" "subnet-0cd04680da6d95113" "subnet-04756c2417c30202e" --profile lab01 --no-verify-ssl

# ECR Pull Through Cache

Seguir conforme explicado no roteiro: [Pre-reqs - EITS SRE Core Team BR - Confluence Global (experian.com)](https://pages.experian.com/display/SRECTB/Pre-reqs#expand-ECRPullThroughCache)

# Wildcard certificate assign to Serasa CA Root

1- [Submit a request](https://pages.experian.com/display/SC/Contact+EITS+Cloud+Engineering#expand-OpenaServiceNowRequest) to the Cloud team to create a Route53 domain (Private Hosted Zone) in your AWS account with the pattern: <env>-<bu>.br.experian.eeca (e.g. sandbox-arch.br.experian.eeca)

Não é mais desse jeito: Rodar o procedimento <https://pages.experian.com/display/SC/How+to+create+BU-managed+Route53+Private+Hosted+Zone+via+Service+Catalog>

Passos para solicitar o certificado:

openssl req -newkey rsa:2048 -nodes -keyout sandbox-lab.br.experian.eeca.key -out sandbox-lab.br.experian.eeca.csr

Generating a 2048 bit RSA private key

...............................................+++

......................+++

writing new private key to 'sandbox-lab.br.experian.eeca.key'

-----

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [XX]:BR

State or Province Name (full name) []:Sao Paulo

Locality Name (eg, city) [Default City]:Sao Paulo

Organization Name (eg, company) [Default Company Ltd]:Serasa Experian

Organizational Unit Name (eg, section) []:DevHub

Common Name (eg, your name or your server's hostname) []:sandbox-lab.br.experian.eeca

Email Address []:devhub\_team@br.experian.com

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:sua-password

An optional company name []:SERASA

Com isso, serão criados dois arquivos: sandbox-lab.br.experian.eeca.key e sandbox-lab.br.experian.eeca.csr. É preciso guardar esses arquivos, pois na renovação dos certificados eles serão necessários!!

2- [Submit a request](https://experian.service-now.com/nav_to.do?uri=%2Fcom.glideapp.servicecatalog_cat_item_view.do%3Fv%3D1%26sysparm_id%3De3bcfdf9dbe0a4d0b284cdae3b9619de%26sysparm_link_parent%3Dec2e5484db4ceb002511fa910f961933%26sysparm_catalog%3De0d08b13c3330100c8b837659bba8fb4%26sysparm_catalog_view%3Dcatalog_default%26sysparm_view%3Dtext_search) to the Middleware team (BR Accounts Only) asking for Wildcard certificate to a Route53 domain set up in your AWS account

Solicitar o certificado para o domínio solicitado, nesse caso, sandbox-lab.br.experian.eeca e URL \*. sandbox-lab.br.experian.eeca para uso interno

3- Import the certificate sent by Middleware team to AWS ACM

[How to import PFX-formatted certificates into AWS Certificate Manager using OpenSSL](https://aws.amazon.com/pt/blogs/security/how-to-import-pfx-formatted-certificates-into-aws-certificate-manager-using-openssl/)

[Importing a certificate - AWS Certificate Manager](https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-api-cli.html)

# PiaaS Account Onboarding

1- Create the policy BUPolicyForDevSecOpsPiaaS with EKS Read permissions in all resources.

Executar os comandos:

# Criar bucket

aws s3api create-bucket --bucket tfstate-devhub-sandbox --region sa-east-1 --create-bucket-configuration LocationConstraint=sa-east-1 --profile devhub-sandbox --no-verify-ssl

aws s3api put-bucket-tagging --bucket tfstate-devhub-sandbox --tagging file://tagging.json --profile devhub-sandbox --no-verify-ssl

# Criar Key

aws kms create-key --description "Chave para onboarding da conta" --profile lab01 --no-verify-ssl

# Criar Policy

aws iam create-policy --policy-name BUPolicyForDevSecOpsPiaaS --policy-document file://BUPolicyForDevSecOpsPiaaS.json --profile lab01 --no-verify-ssl