

EIXO 5: Projeto da Infraestrutura de Rede

Tema: Cooperativa Bancária

Integrantes:

Luís Fernando Moura Santos

Cássio Venuto Monteiro

Júlia Persson Mascari

Paola Marques Braga

Pedro Augusto Teixeira Silva

Vinicius Henrique de Oliveira Neves

Descrição:

Uma cooperativa bancária em uma cidade polo do interior do estado com cinco filiais em cidades próximas.

A cooperativa bancária segue seu plano de expansão no Brasil, reforçando seu compromisso com a população mineira. A cidade de Belo Horizonte foi escolhida para sediar a nova matriz, que funcionará como o centro estratégico das operações em Minas Gerais. Para ampliar a presença da cooperativa e facilitar o acesso aos serviços financeiros, serão inauguradas cinco filiais em Sete Lagoas, Divinópolis, Contagem, Nova Lima e Betim.

A estrutura tecnológica da cooperativa foi cuidadosamente planejada para assegurar eficiência operacional, segurança nas transações e qualidade no atendimento ao público. No total, serão disponibilizados 46 computadores, distribuídos entre matriz e filiais, com equipamentos específicos para cada setor, garantindo suporte adequado às necessidades dos colaboradores.

1ª Etapa: Estrutura de Equipamentos, Rede e Endereçamento IP

Matriz – Belo Horizonte:

Computadores: 4 para Caixa, 3 para Atendimento Presencial, 1 para Gerente, 2 para TI

Impressoras: 2 para Atendimento Presencial, 1 para Gerente

Servidor: 2

Roteadores: 2

Total de hosts: 10 computadores + 3 impressoras + 1 servidor + 2 roteadores = 16 dispositivos com IP

Configuração de Rede:

Endereço de rede: 192.168.0.254/24

Máscara de sub-rede: 255.255.255.0

Gateway padrão: 192.168.0.254

Plano de Endereçamento IP:

Gateway principal (Roteador 1): 192.168.0.254

Roteador 2 (Clientes): 192.168.0.198

Servidor: 192.168.0.1

Servidor (Backup): 192.168.0.1

Impressoras: 192.168.0.20 a 192.168.0.22

Equipamentos de TI: 192.168.0.34 a 192.168.0.35

Gerência: 192.168.0.33

Atendimento: 192.168.0.30 a 192.168.0.32

Caixas: 192.168.0.40 a 192.168.0.43

Filiais – Sete Lagoas, Divinópolis, Contagem, Nova Lima e Betim:

Computadores por filial: 2 para Caixas, 2 para Atendimento Presencial, 1 para Gerente, 1 para TI

Impressoras: 1 por filial

Roteadores: 1 por filial

Hosts na rede por filial: 6 computadores + 1 impressora + 1 roteador = 8

Máscara de rede: 255.255.255.0 (/24)

Plano de IP detalhado por filial:

Sete Lagoas – 192.168.1.0/24

Gateway (roteador): 192.168.1.1

Servidor: 192.168.1.10

Computadores e impressora: a partir de 192.168.1.11

Divinópolis – 192.168.2.0/24

Gateway (roteador): 192.168.2.1

Servidor: 192.168.2.10

Computadores e impressora: a partir de 192.168.2.11

Contagem – 192.168.3.0/24

Gateway (roteador): 192.168.3.1

Servidor: 192.168.3.10

Computadores e impressora: a partir de 192.168.3.11

Nova Lima – 192.168.4.0/24

Gateway (roteador): 192.168.4.1

Servidor: 192.168.4.10

Computadores e impressora: a partir de 192.168.4.11

Betim – 192.168.5.0/24

Gateway (roteador): 192.168.5.1

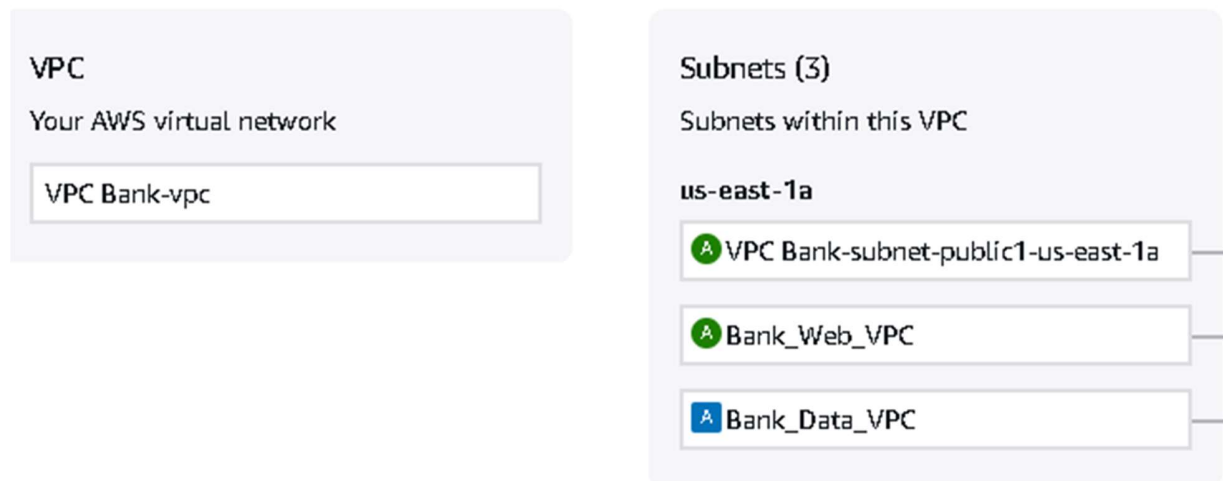
Servidor: 192.168.5.10

Computadores e impressora: a partir de 192.168.5.11

2ª Etapa: Ambiente em Nuvem e Virtualização Local

VPC (Nuvem Privada Virtual):

Foi criada uma única VPC, denominada VPC Bank, que representa nossa nuvem virtual privada e possui o bloco de endereçamento 10.0.0.0/16. Dentro dessa VPC, foram configuradas duas sub-redes (subnets) para segmentar os diferentes tipos de serviços da infraestrutura:



Bank_Web_VPC (10.0.16.0/20): Sub-rede pública, destinada à hospedagem da plataforma WEB do banco. Essa subnet permite o acesso externo, sendo responsável por atender os usuários que acessam os serviços do banco pela internet.

Bank_Data_VPC (10.0.32.0/20): Sub-rede privada, responsável por hospedar os bancos de dados e demais serviços internos que exigem maior segurança e não devem ser acessíveis diretamente pela internet.

Essa estrutura garante isolamento, segurança e organização dos recursos em nuvem, seguindo boas práticas de arquitetura em ambientes AWS.

Security Groups (Grupos de Segurança)

Para cada subnet foi configurado um grupo de segurança específico, responsável por controlar o tráfego de rede que entra e sai das instâncias dentro da VPC. Cada grupo atua como um firewall virtual, aplicando regras de acesso conforme o tipo de ambiente.

Bank_Users:

Destinado aos usuários da plataforma web do banco.

Regra de entrada (Inbound): Liberado para o endereço 0.0.0.0/0, permitindo conexões HTTP/HTTPS de qualquer origem pública.

Regra de saída (Outbound): Permite que a instância envie tráfego para qualquer destino (0.0.0.0/0), possibilitando comunicação externa, como acesso a APIs ou serviços de autenticação.

Essa configuração garante que qualquer cliente, em qualquer lugar, possa acessar a aplicação web do banco.

Bank_Workers:

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	
sgr-0822e5c7b3bf2dab5	HTTP	TCP	80	Custom	<input type="text" value="0.0.0.0/0"/>
sgr-0db3ead440fcb488c	RDP	TCP	3389	Custom	<input type="text" value="0.0.0.0/0"/>

Add rule

Voltado para os funcionários e sistemas internos do banco, conectados por meio de uma VPN e pela própria plataforma web.

Regra de entrada (Inbound): Restrita ao IP da VPN (simulado pelo IP do computador do integrante do grupo) e ao IP público da plataforma web, garantindo que apenas usuários internos e componentes autorizados acessem esse ambiente.

Regra de saída (Outbound): Liberada apenas para os endereços internos necessários, como o banco de dados e serviços internos.

Essa abordagem reforça a segurança, evitando que sistemas internos sejam expostos à internet pública.

Inbound rules [Info](#)

Security group rule ID	Type	Protocol	Port range	Source	
sgr-0849a84c52725d872	SSH	TCP	22	Custom	<input type="text" value="200.170.102.130/32"/>
sgr-0e7f9980d2bb304b6	All traffic	All	All	Custom	<input type="text" value="54.85.130.43/32"/>

Add rule

Instâncias EC2 (Máquina virtuais)

Atualmente, o ambiente conta com três instâncias EC2 em execução, cada uma com uma função específica dentro da arquitetura da VPC Bank-vpc:

Bank_Web_Panel:

Instância Windows Server responsável por hospedar a plataforma web do banco.

Essa máquina é configurada dentro da subnet pública (Bank_Web_VPC) e segue as regras do Security Group Bank_Users, permitindo acesso público via HTTP/HTTPS para que qualquer cliente possa utilizar o sistema.

Bank_Data_Server:

Instância destinada a armazenar e gerenciar o banco de dados principal da aplicação, guardando todas as informações dos clientes.

Está hospedada na subnet privada (Bank_Data_VPC) e segue as regras do Security Group Bank_Workers, aceitando conexões apenas da plataforma web (Bank_Web_Panel) e dos trabalhadores conectados via VPN, garantindo segurança e isolamento de dados. Para realização do exemplo foi criada como pública para o acesso mais simplificado.

Bank_Data_Server_Backup:

Instância dedicada ao backup automático dos dados armazenados na

Bank_Data_Server.

Também localizada na subnet privada, possui acesso restrito conforme as regras da VPC e do grupo de segurança, permitindo conexões apenas de trabalhadores autorizados e da própria instância Bank_Data_Server, evitando qualquer exposição indevida.

Essa arquitetura foi planejada para garantir alta segurança, controle de acesso segmentado e disponibilidade contínua, permitindo que cada instância desempenhe seu papel de forma isolada e eficiente dentro da infraestrutura em nuvem.

Instances (3) Info

Find Instance by attribute or tag (case-sensitive)

A

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type
<input type="checkbox"/>	Bank_Web_Panel	i-093f61ec42813f7ea	Running	t2.large
<input type="checkbox"/>	Bank_Data_Ser...	i-0cc4f7b048633012d	Running	t3.micro
<input type="checkbox"/>	Bank_Data_Ser...	i-0bb46ee2b527ba191	Running	t3.micro

Instance summary for i-093f61ec42813f7ea (Bank_Web_Panel) Info

Updated less than a minute ago

Instance ID

i-093f61ec42813f7ea

IPv6 address

-

Hostname type

IP name: ip-10-0-23-196.ec2.internal

Public IPv4 address

54.80.184.74 | [open address](#)

Instance state

Running

Private IP DNS name (IPv4 only)

ip-10-0-23-196.ec2.internal

Private IPv4 addresses

10.0.23.196

Public DNS

ec2-54-80-184-74.compute-1.amazonaws.com | [open address](#)

▼ Inbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-0822e5c7b3bf2dab5	80	TCP	0.0.0.0/0	Bank Users	-
-	sgr-0db3ead440fcb488c	3389	TCP	0.0.0.0/0	Bank Users	-

▼ Outbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
-	sgr-048baff63d24f4ed4	All	All	0.0.0.0/0	Bank Users	-

EC2 – Bank_Web_Panel:

Instance summary for i-093f61ec42813f7ea (Bank_Web_Panel) Info

Updated less than a minute ago

Instance ID
i-093f61ec42813f7ea

IPv6 address
-

Hostname type
IP name: ip-10-0-23-196.ec2.internal

Answer private resource DNS name
-

Auto-assigned IP address
54.80.184.74 [Public IP]

IAM Role
-

IMDSv2
Required

Operator
-

Public IPv4 address
54.80.184.74 | op

Instance state
Running

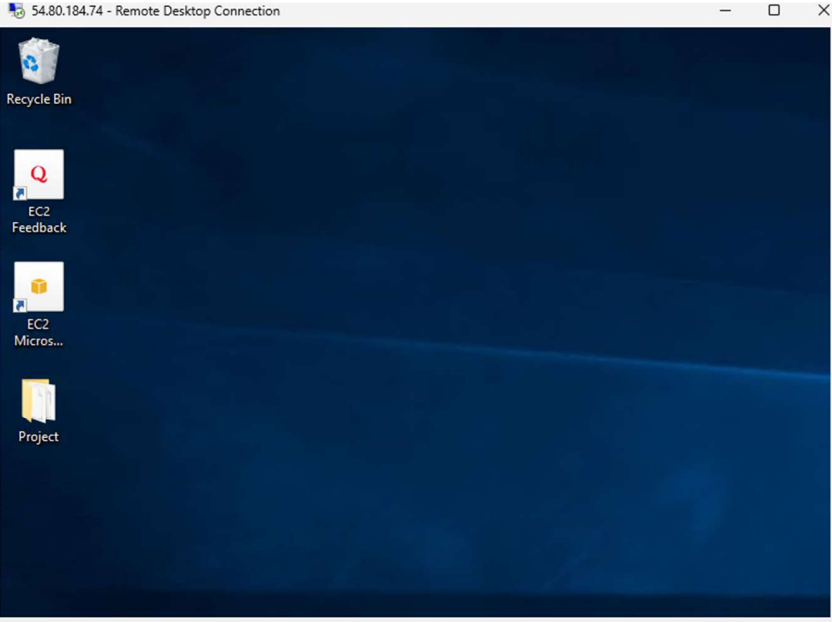
Private IP DNS name
ip-10-0-23-196.ec

Instance type
t2.large

VPC ID
vpc-08d53feffb05

Subnet ID
subnet-04574d28

Instance ARN
arn:aws:ec2:us-ea



Hostname: EC2AMAZ-OE3592C
Instance ID: i-093f61ec42813f7ea
Public IPv4 address: 54.80.184.74
Private IPv4 address: 10.0.23.196
Instance size: t2.large
Availability Zone: us-east-1a
Architecture: AMD64
Total memory: 8192 MB
Network: Low to Moderate

Cooperativa Bancária

InícioContasTransferênciasPagamentosCartões

Instance summary for i-0bb46ee2b527ba191 (Bank_Data_Server) Info

ConnectInstance stateActions

Updated less than a minute ago

Instance ID

i-0bb46ee2b527ba191

IPv6 address

-

Hostname type

IP name: ip-10-0-11-240.ec2.internal

Answer private resource DNS name

-

Public IPv4 address

18.206.95.77 | open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-10-0-11-240.ec2.internal

Instance type

t3.micro

Private IPv4 addresses

10.0.11.240

Public DNS

ec2-18-206-95-77.compute-1.amazonaws.com | open address

Elastic IP addresses

-

Ver todas as transações

transfereência recebida
28 de Março, 2023
+R\$ 350,00

EC2 -

Inbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-0849a84c52725d872	22	TCP	200.170.102.130/32	Security_Group_Bank_Workers	-
-	sgr-0e7f9980d2bb304b6	All	All	54.85.130.43/32	Security_Group_Bank_Workers	-

Outbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
-	sgr-035ea775c9cad53c1	All	All	0.0.0.0/0	Security_Group_Bank_Workers	-

Bank_Data_Server:

Para a conexão com a Bank_Data_Server através do ssh estamos realizando os seguintes comandos:

```
ssh -i KEY-PATH ec2-user@IP-DA-EC2
```

```
PS C:\Users\Vinic> ssh -i C:\Users\Vinic\Downloads\my_bank_server_key.pem ec2-user@18.206.95.77
```

Após a inserção do comando iremos nos conectar a EC2 e podemos visualizar o banco de dados:

```
Last login: Sun Oct 19 14:22:09 2025 from 200.170.102.130  
[ec2-user@ip-10-0-11-240 ~]$
```

```
MariaDB [(none)]> USE bank;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [bank]>
```

Podemos realizar qualquer comando SQL para inserir, deletar ou visualizar os dados:

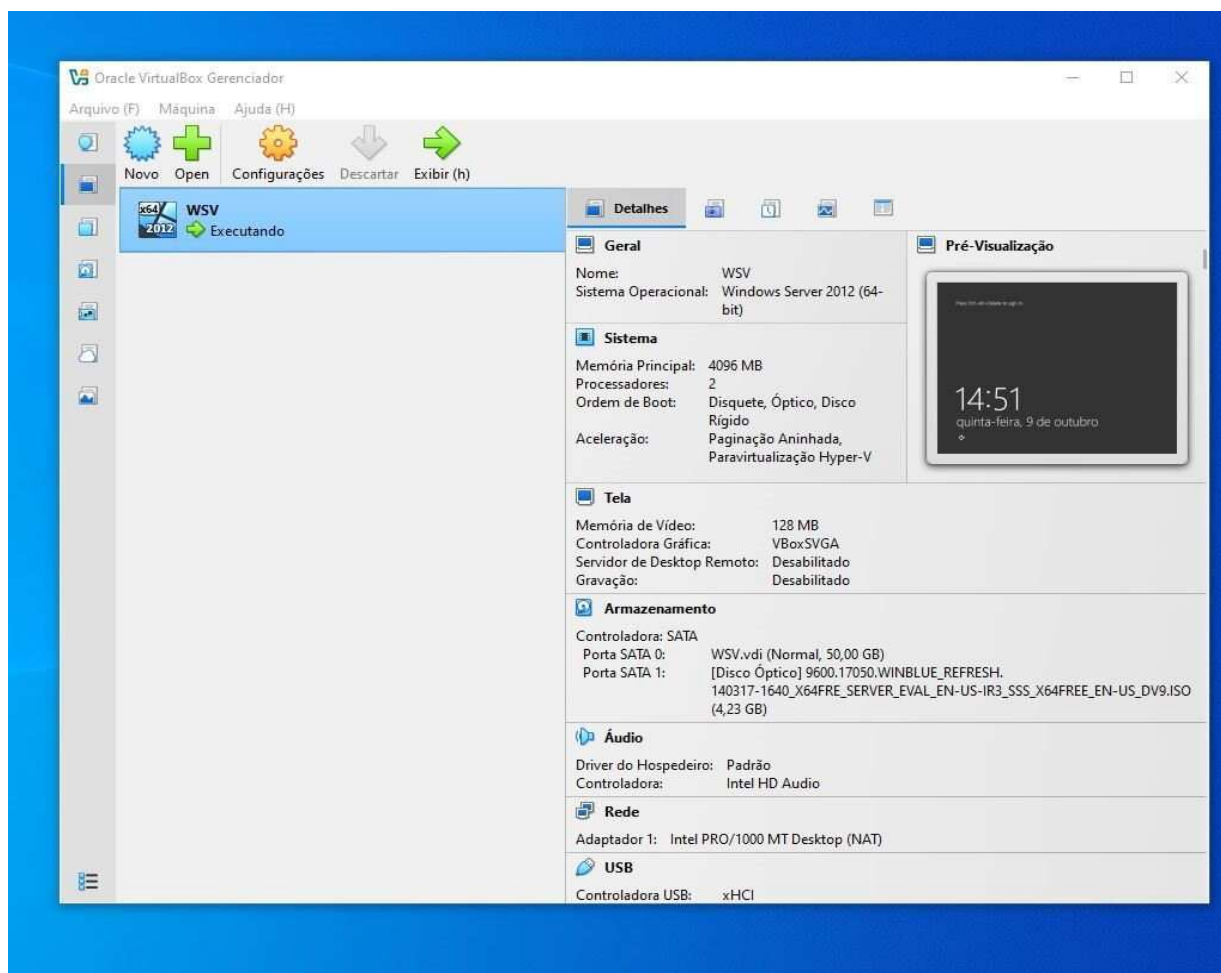
```
MariaDB [bank]> SELECT * FROM users;
```

user_id	full_name	account_created	is_active
1	Vinicius Henrique de Oliveira Neves	2025-09-29 22:31:37	1
2	USUARIO_TESTE	2025-10-19 14:26:07	1
3	PAULO SERGIO	2025-10-19 14:26:27	1
4	CLIENTE NOVO	2025-10-19 14:26:41	1

```
4 rows in set (0.004 sec)
```

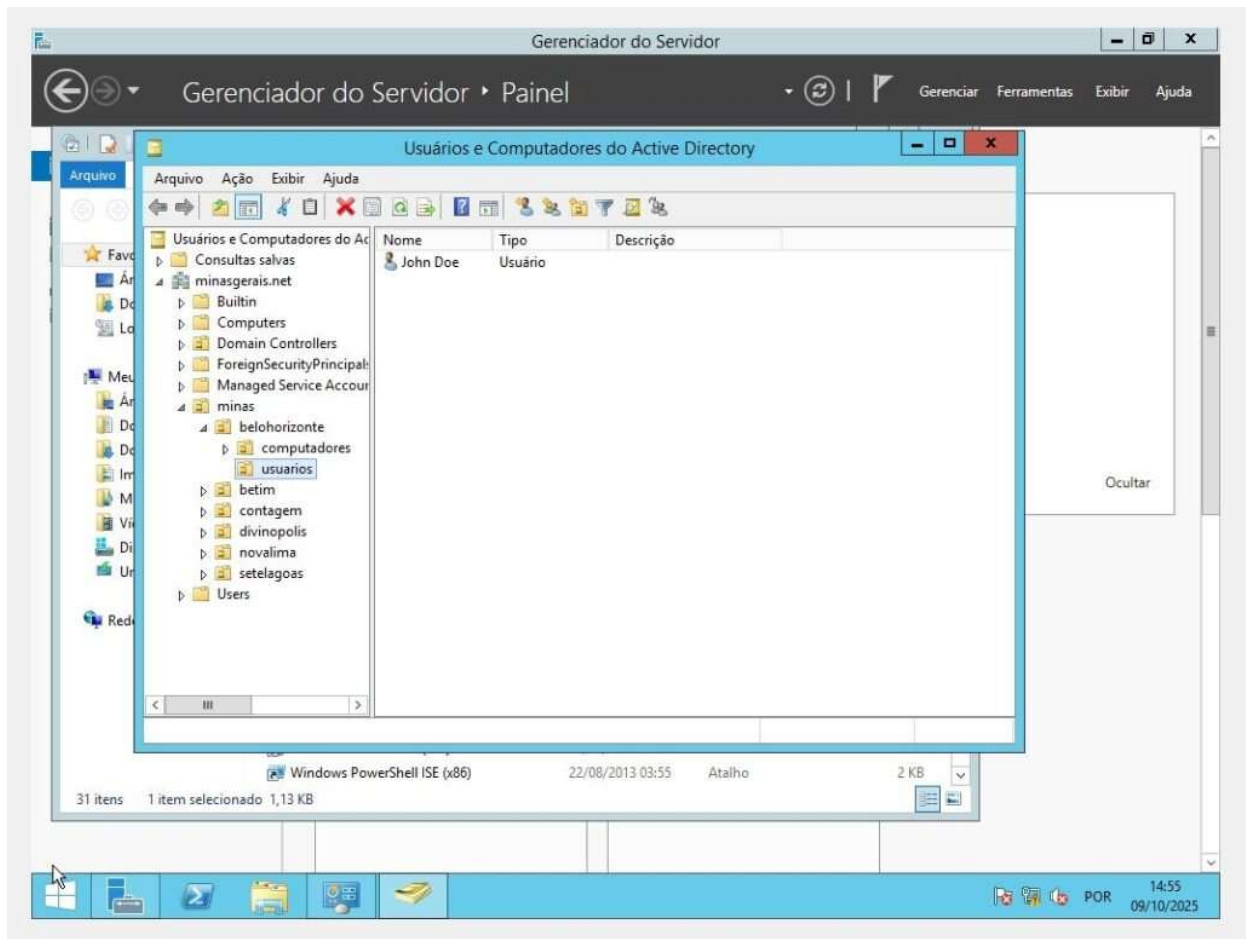
Windows Server no Virtual Box

Inicialmente fizemos a instalação da Iso do Windows Server no Virtual Box, e as configurações necessárias.



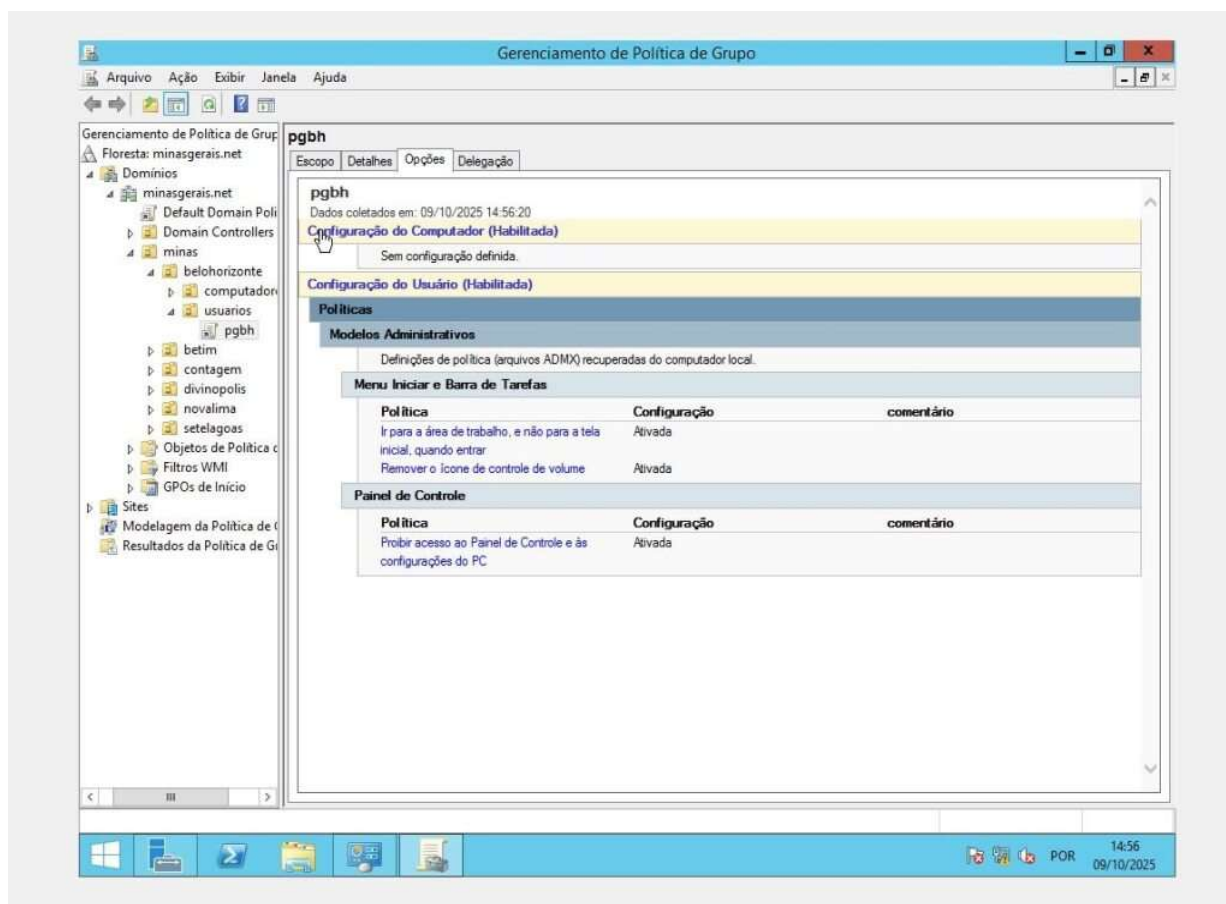
Usuário do Active Directory

Em seguida fizemos a adição do Active Directory e DNS, assim criamos os grupos de cada filial e da matriz, adicionando os usuários do AD.



Política de Grupo

Após isso, realizamos a criação das políticas de grupo.

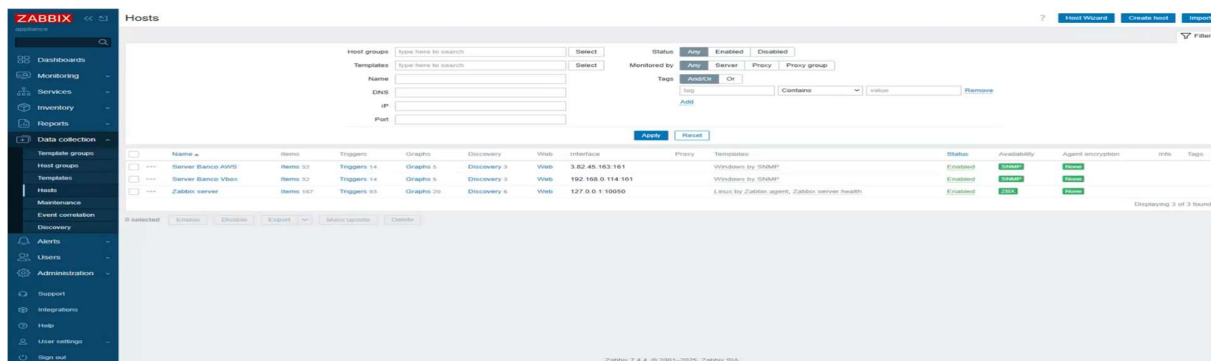


3ª Etapa: Gerência e Monitoração de Ambientes de Redes

Durante a terceira etapa foi realizada a instalação e configuração solicitada para monitoramento da rede através do Zabbix.

Monitoramento dos Servidores (Hosts)

Primeiramente fizemos a instalação do Zabbix no Virtual Box, criamos os três hosts e a conexão com os IPs configurados no Virtual Box e no AWS. Em seguida ativamos o SNMP no Windows Server e no AWS e finalizamos a configuração.



Monitoramento Maps

Para a criação do Mapa dos servidores, adicionamos uma Rede Externa (Nuvem) e três servidores: Servidor Local, Servidor AWS e Servidor Zabbix.



Gráfico Disco Local - VBox

Após as configurações finalizadas, analisamos os gráficos de monitoramento referente a cada servidor criado, sendo o primeiro "Espaço Utilizado no Virtual Box":

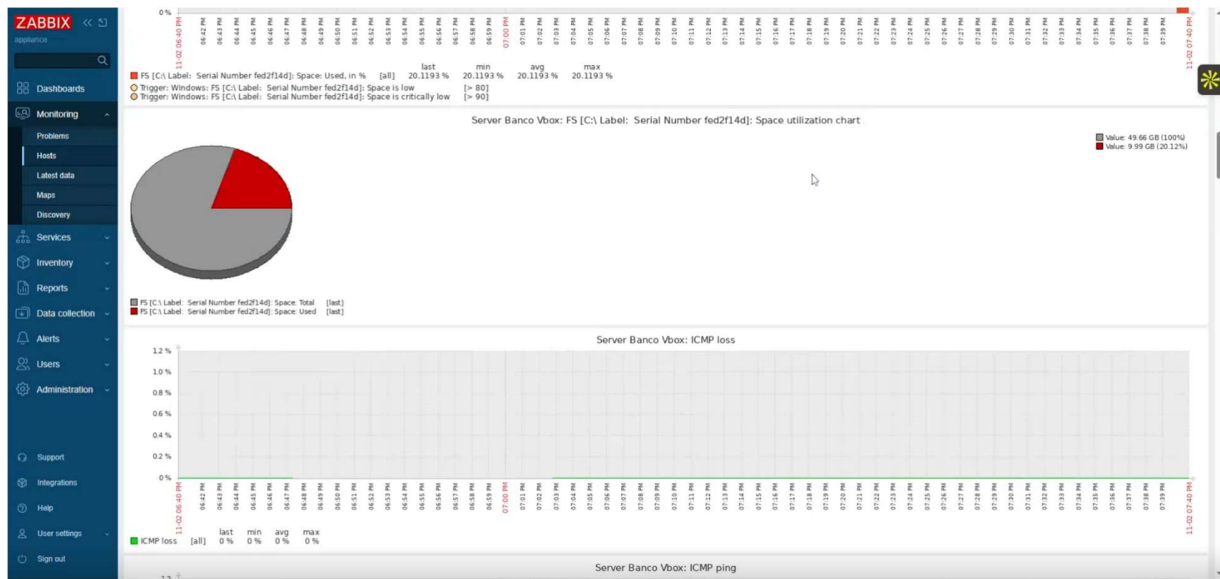


Gráfico CPU Local - VBox

No fim da mesma página de monitoramento verificamos o uso da CPU no servidor local do Virtual Box.

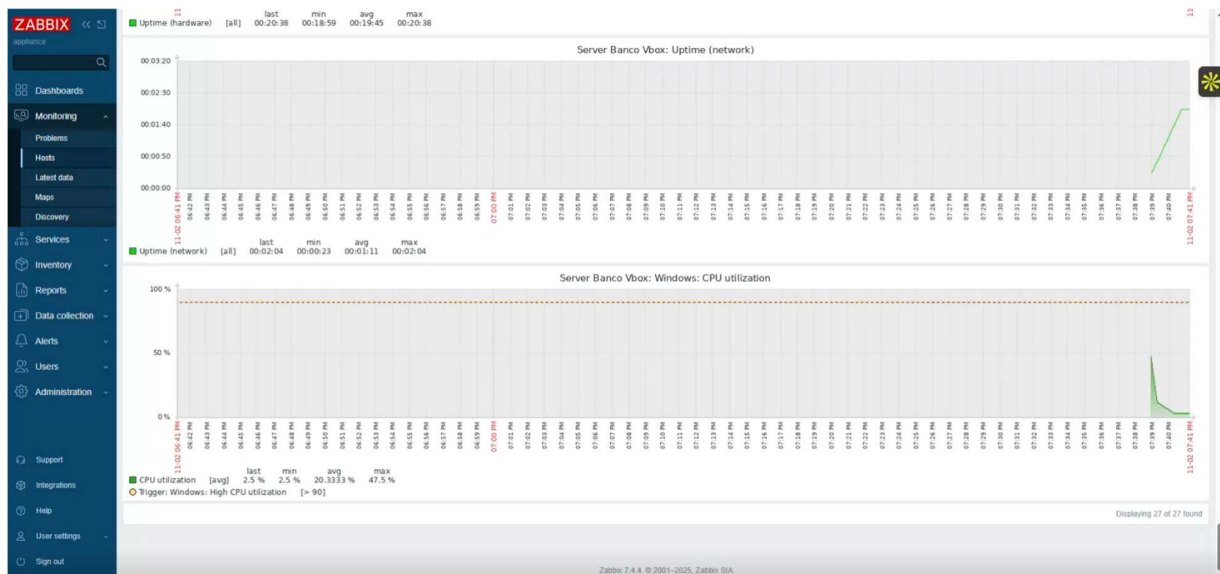


Gráfico Disco - AWS

Os mesmos gráficos de monitoramento são apresentados para o servidor criado no AWS, abaixo o gráfico em disco de espaço utilizado:

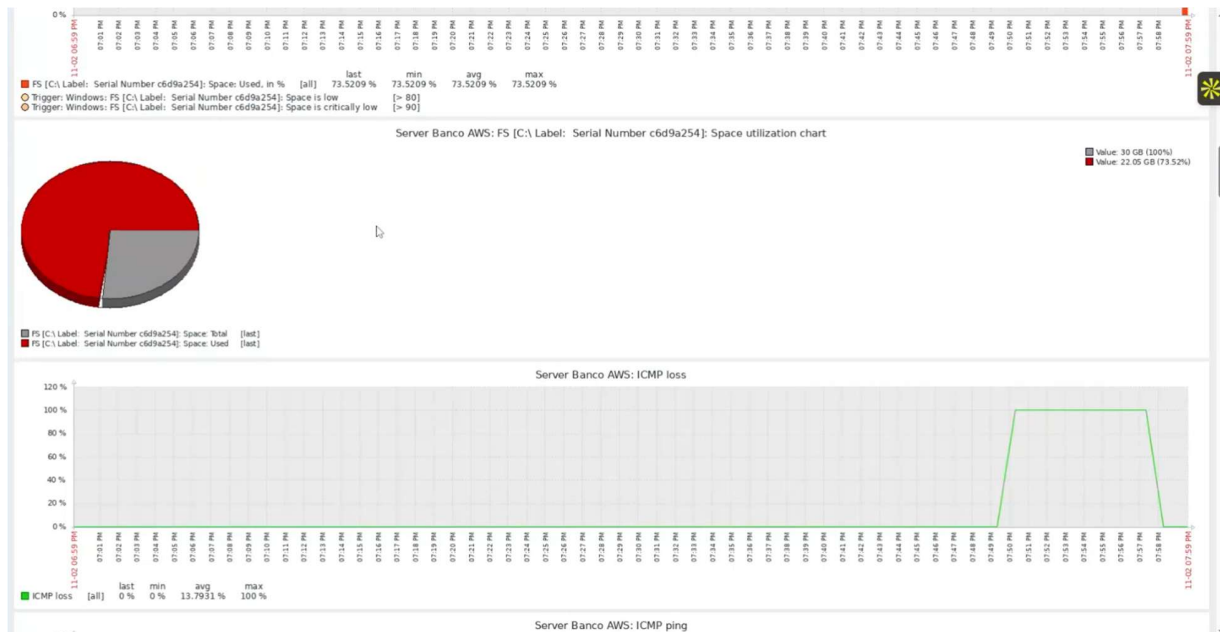


Gráfico CPU - AWS

Da mesma forma, foi apresentado o Gráfico de monitoramento da CPU no servidor AWS:



Grupo de Segurança - AWS:

- Primeiramente foi adicionado nas regras do grupo de segurança “Bank Users” o acesso público e global para as conexões datagram protocol (UDP) e Internet Control Message Protocol (ICMP), librando assim o acesso com o Zabbix.

sg-0149ffd1cdc918940 - Bank Users

Actions

Details

Security group name

Bank Users

Security group ID

sg-0149ffd1cdc918940

Description

Bank Users

VPC ID

vpc-08d53feffb93ceb10

Owner

590183800736

Inbound rules count

4 Permission entries

Outbound rules count

1 Permission entry

Inbound rules

Security group rule ID

sg-01fa7355d19a86367

Type

Custom UDP

Protocol

UDP

Port range

161 - 162

Source

Custom

Description - optional

Monitoring

Delete

sg-0c0b3ead440fcb488c

RDP

TCP

3389

Custom

0.0.0.0/0

Remote Desktop

Delete

sg-r-043afdcdb29fefebb0

All ICMP - IPv4

ICMP

All

Custom

0.0.0.0/0

Ping

Delete

sg-r-0822e5c7b3bf2dab5

HTTP

TCP

80

Custom

0.0.0.0/0

Web Server

Delete

Add rule

4ª Etapa: Desenvolvimento Seguro:

4.1.1: Tópicos que o projeto atende do OWASP Active Controls:

- **C2: Aproveito de estruturas e bibliotecas de Segurança:** Utilizamos bibliotecas como Ktor e Exposed que já implementam mecanismos de segurança.

- **C3: Acesso seguro ao Banco de dados:** A biblioteca ktor possui mecanismos que bloqueiam a leitura de queries com input e injeção SQL, assim como o usuário, nome e senha do banco foram configurados de acordo com o nome do projeto e senha aleatória.

- **C7: Aplicação de Controles de Acesso:** Utilizamos autenticação JWT, ou seja, somente usuários autenticados podem acessar o sistema.

- **C10: Tratamento de erros e exceções:** Mensagens de erros apenas traduzem o erro que ocorreu, evitando loggar no console ou trazer ao usuário dados pessoais.

Tópicos que o projeto que possuem segurança contra vulnerabilidades do OWASP Top 10 Project:

- **A01:2021-Broken Access Control:** Somente usuários autenticados com sua própria conta podem acessar o sistema.

- **A03:2021-Injection:** O sistema apenas aceita exatamente os dados que espera receber, logo qualquer espécie de injeção será totalmente ignrado.

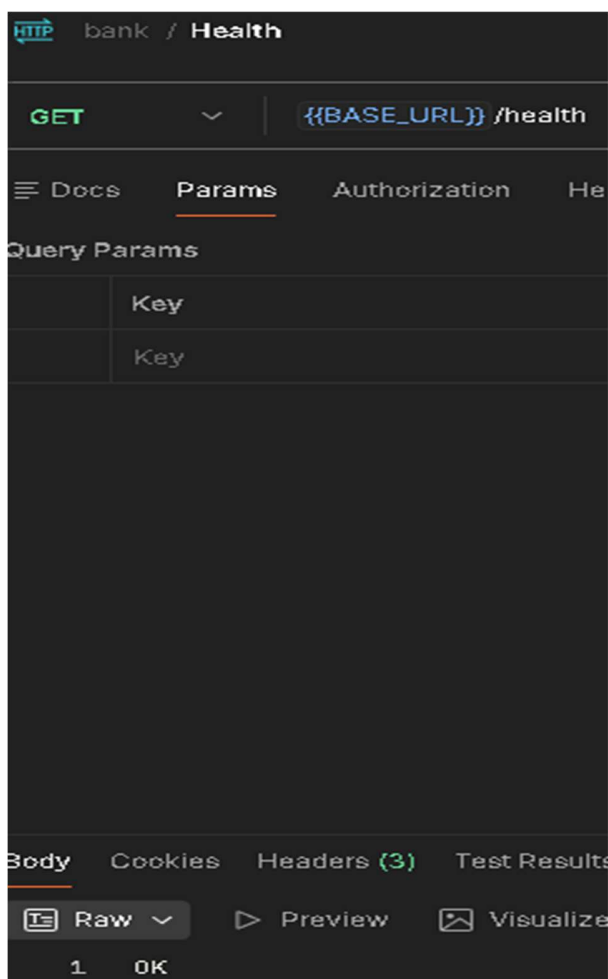
- **A04:2021-Insecure Design:** O sistema possui um design seguro, sendo necessário que cada ação do usuário passe pela autenticação, validação de conta e validação de inputs.

- **A05:2021-Security Misconfiguration:** Nenhuma configuração importante e que possibilite o acesso ao core da aplicação foi armazenada ao core da aplicação foi armazenada fora do próprio código do projeto e dentro do ambiente da nuvem.

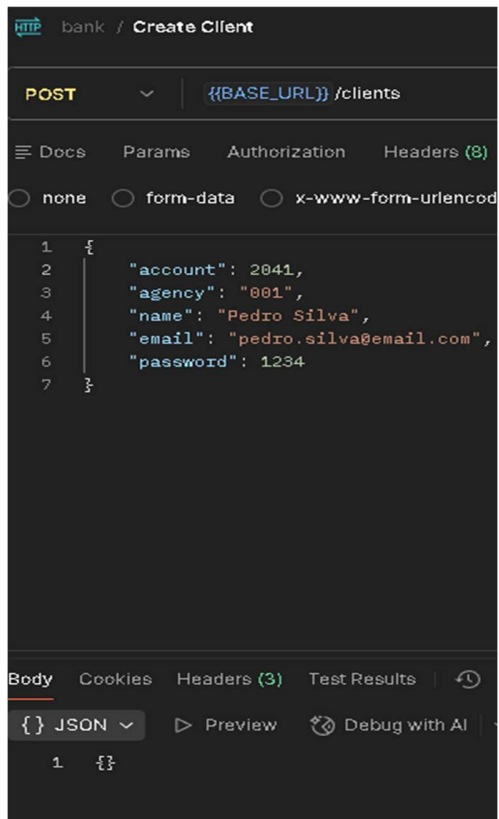
- **A06:2012-Vulnerable and Outdated Components:** As bibliotecas utilizadas foram configuradas para as utilizar as versões seguras de acordo com a documentação oficial.

4.1.2: Prints do BackEnd:

- **Rota (Get) /health:** Responsável por verificar se o serviço está ativo



- Rota (Post) /clients: Responsável cadastrar novos usuários

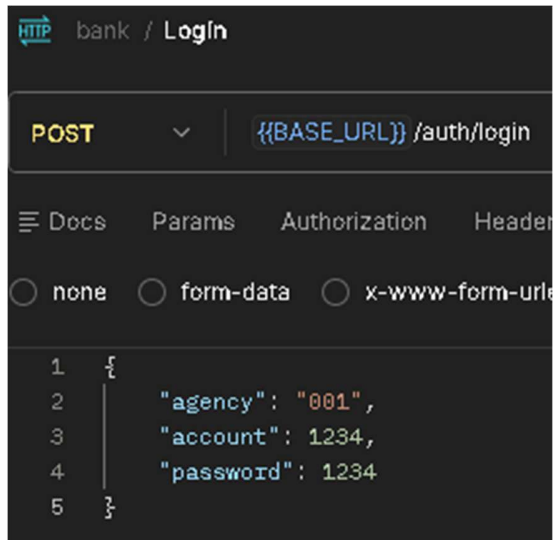


```
mysql> SELECT * From clients;
```

id	account	agency	name	email	password
0fa99345-dad9-435f-b2ec-7c8e82d0acbe	2472	001	Pedro Silva	pedro.silva@email.com	1234
1efb0eb3-bc0c-4fff-9014-03c1b040e31c	2041	001	Pedro Silva	pedro.silva@email.com	1234
596862c8-c115-4bdc-88b3-ed708201ad78	1234	001	Vinicius Neves	vinicius_neves@gmail.com	1234

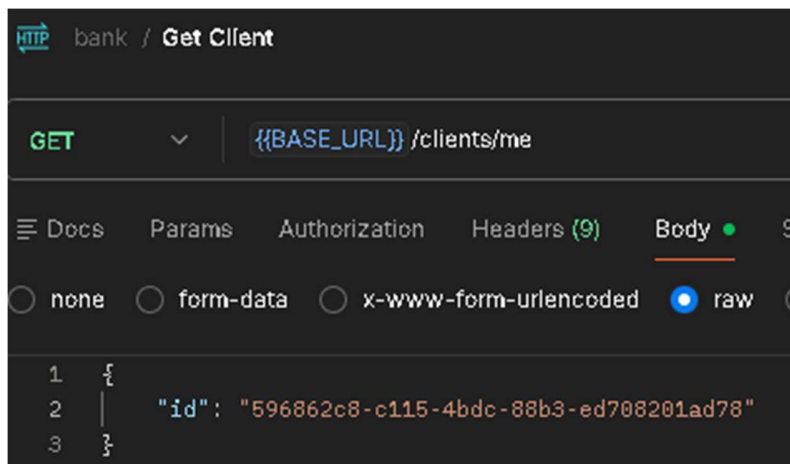
```
3 rows in set (0.00 sec)
```

- **Rota (Post) /auth/login:** Responsável por realizar login dos usuários, trazendo o id do usuário que será utilizado nas demais requests evitando o uso de dados dos usuários e o token que será utilizado para que somente o próprio usuário acesse os seus dados



```
{
  "data": {
    "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJodHRwOi8vMy4yMjYuMjE5Ljc5IiwiaXVkiOiYmFuay1jbGllbnRzIiwiaWQiOiI1OTY4NjJjOC1jMTE1LTZGMtODhiMy1lZDcwODIwMWFkNzgiLCJleHAiOiE3NjQ3Nzk5OTd9.8MnRz-9dXDafb31j5zWLGcf1_3coPDCtZd3uB1DHfzY",
    "userId": "596862c8-c115-4bdc-88b3-ed708201ad78",
    "name": "Vinicius Neves"
  }
}
```

- **Rota (Get) /clients/me:** Responsável por coletar as informações principais do usuário, porém dessa vez é necessário adicionar o header Authentication com o token coletado na rota de login, caso contrário receberemos um erro 401 (Unauthorized)



```
{
  "data": {
    "id": "596862c8-c115-4bdc-88b3-ed708201ad78",
    "name": "Vinicius Neves",
    "email": "vinicius_neves@gmail.com",
    "account": 1234,
    "agency": "001"
  }
}
```

- **Rota (Put) /clients/me:** Responsável por atualizar as informações do usuário

Separação de responsabilidades e papéis:

Nome	Tempo	Responsabilidade	Etapa
Luís Fernando Moura Santos	1 dia	Preenchimento do documento e planilha de endereçamento IP da filial de sete lagoas. Edição da Planilha de Equipamentos.	1
Cássio Venuto Monteiro			1
Pedro Augusto Teixeira Silva	1 dia	Simulação do Packet Tracer.	1
Júlia Persson Mascari	2 dias	Preenchimento das planilhas de endereçamento das filiais e de inventário; Simulação das filiais no Packet Tracer.	1
Paola Marques Braga	1 dia	Preenchimento do documento e da planilha de endereçamento IP das filiais	1
Vinicius Henrique de Oliveira Neves	2 dias e 4 horas	Preenchimento da planilha de inventário, Preenchimento da planilha de endereçamento IP da matriz, Simulação da rede da matriz no Packet Tracer Análise e correção das demais atividades	1
Vinicius Henrique de Oliveira Neves	1 Semana	Preenchimento da documentação Criação da VPC e máquinas virtuais no EC2	2

Júlia Persson Mascari	3 dias	Preenchimento documentação Revisão etapa anterior Windows Server no Virtual Box	2
Cássio Venuto Monteiro	13:30	Instalação do Windows Server 2012; Instalação e configuração do Zabbix; Configuração monitoramento do map; Monitoramento do Host	3
Paola Marques Braga	3 dias	Instalação do Windows Server 2012; Instalação e configuração do Zabbix; Configuração monitoramento do map; Monitoramento do Host	3
Pedro Augusto Teixeira Silva	2 dias	Instalação do Windows Server 2012; Instalação e configuração do Zabbix; Configuração monitoramento do map; Monitoramento do Host	3
Júlia Persson Mascari	2 dias	Instalação do Zabbix e configuração dos Hosts, Mapa e SNMP; Documentação da etapa;	3
Vinicius Henrique de Oliveira Neves	2 dias	Instalação do Zabbix e configuração dos Hosts; Configuração da AWS Documentação da etapa;	3
Luís Fernando Moura Santos	3 dias	Instalação do Windows Server 2012; Instalação e configuração do Zabbix; Configuração e monitoramento do map e do host;	3

Cássio Venuto Monteiro	10h	Localização das vulnerabilidades no código da cooperativa de acordo com a OWASP TOP 10	4
Paola Marques Braga	10h	Localização das vulnerabilidades no código da cooperativa de acordo com a OWASP TOP 10	4
Luís Fernando Moura Santos	5h	Preenchimento do documento da política de segurança da informação.	4
Júlia Persson Mascari	2 dias	Documentação da Política de Segurança da Informação	4
Vinicius Henrique de Oliveira Neves	2 dias	Localização das vulnerabilidades no código da cooperativa de acordo com a OWASP TOP 10. Análise da Política de Segurança da Informação	4

Cronograma de Atividades:

1ª Etapa:

12/08 - Formação dos Grupos

18/08 - Definição do Tema

21/08 - Reunião entre o grupo para fazer as atividades e apresentar ao professor no próximo encontro

25/08 - Reunião com o professor

02/09 - Reunião com o grupo para separação de tarefas

08/09 - Reunião com o professor

12/09 - Reunião com o professor

2ª Etapa:

15/09 - Reunião geral com o professor
22/09 - Reunião grupo com o professor
29/09 - Reunião grupo com o professor
06/10 - Reunião grupo com o professor
20/10 - Reunião grupo com o professor
21/10 - Entrega da etapa

3ª Etapa:

27/10 - Reunião geral com o professor
03/11 - Reunião com o professor
09/11 - Entrega etapa