

UNIVERSIDAD DEL VALLE DE GUATEMALA

Redes

Sección 20



“Proyecto Final: Diseño de una red”

Elean Rivas 19062

Andrea Lam 20102

Andrés de La Roca 20332

Javier Alvarez 18051

Jun Woo Lee 20358

GUATEMALA, Octubre 2023

Índice

Índice.....	1
Introducción.....	2
Desarrollo de la red.....	2
Diseño.....	2
Subredes:.....	5
Componentes.....	6
Rendimiento.....	17
Conclusiones.....	22
Referencias Bibliográficas.....	23
Anexos.....	24

Introducción

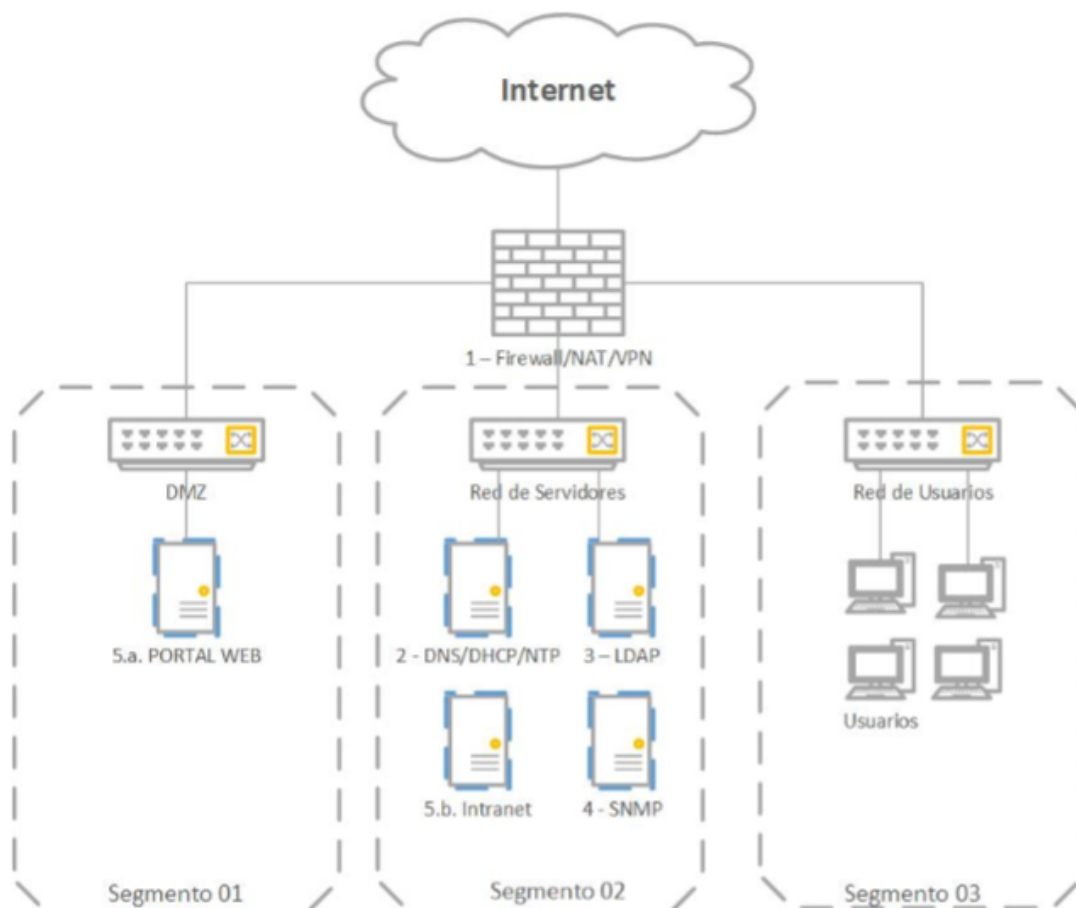
Construir una red, de cualquier tipo puede ser un gran reto, pues debemos tomar en cuenta que esta debe adaptarse a los requerimientos de negocio; con el objetivo de aplicar los conocimientos de diseño de redes para virtualizar el funcionamiento completo de una red a través de la nube, se usó Microsoft Azure para construir una red que consta de un Firewall con reglas Nat y VPN, un servidor DMZ con un portal web, una red de servidores que hiciera uso de los servicios de red tales como DNS/DHCP/NTP, LDAP, Intranet, SNMP y finalmente una red de usuarios. Tras esto pudimos concluir en lo clave que pueden ser las métricas para la optimización y mejora de una red, la importancia del firewall para el diseño de la red y la utilidad de Azure Bastion para la conexión segura.

Desarrollo de la red

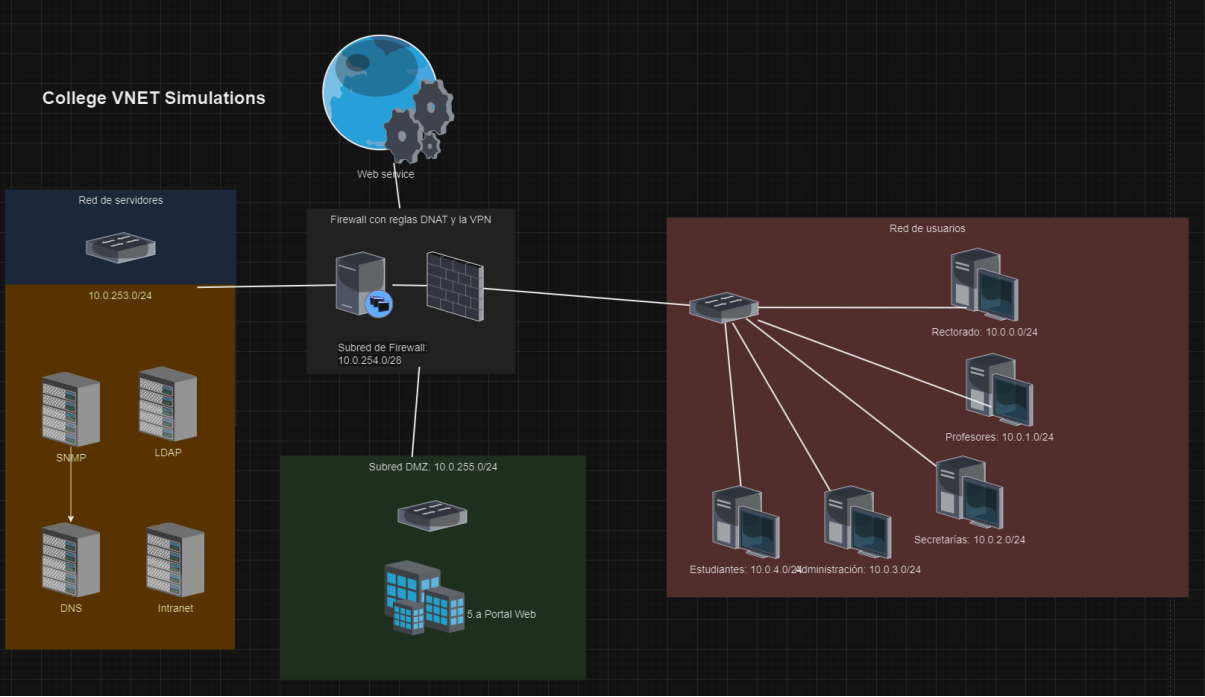
Diseño

En el diseño de la red se tomaron en cuenta una serie de requerimientos, dentro de ellos los permisos y reglas necesarias para el funcionamiento adecuado y seguro de la red. Para ello se propuso la arquitectura de una red basada en una universidad donde los diferentes usuarios tienen diferentes tipos de accesos

La red que se nos proporcionó nos daba la siguiente estructura y requerimientos.



Pensando en esto se diseñó la siguiente red



Creación de la subred:

Create virtual network ...

Basics Security IP addresses Tags Review + create

[View automation template](#)

Basics

Subscription	Azure subscription 1
Resource Group	Redes-2023
Name	CollegeSimulation
Region	East US

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0.0/16 (65536 addresses)
Subnet	Rectoria (10.0.0.0/24) (256 addresses)
Subnet	Profesores (10.0.1.0/24) (256 addresses)
Subnet	Secretaria (10.0.2.0/24) (256 addresses)
Subnet	Administracion (10.0.3.0/24) (256 addresses)
Subnet	Estudiantes (10.0.4.0/22) (1024 addresses)
Subnet	Firewall (10.0.254.0/28) (16 addresses)
Subnet	DMZ (10.0.255.0/24) (256 addresses)

Y nos dio este resultado en Azure, se usó un red de tipo 10 clase A privada con máscara de subred de /16 o de 24 bits lo cual nos provee una cantidad de host bastante considerable, esto

puede ser un poco grande, pero se hizo así para hacer lo que consideramos una simulación apropiada. La máscara de subred fue una predeterminada es decir 255.0.0.0

Subredes:

El diseño para las subredes fue el siguiente.

Rectorado: 10.0.0.0/24

Profesores: 10.0.1.0/24

Secretarías: 10.0.2.0/24

Administración: 10.0.3.0/24

Estudiantes: 10.0.4.0/24

Subred de Firewall: 10.0.254.0/28

Subred DMZ: 10.0.255.0/24

Subred de Servicios de Infraestructura: 10.0.253.0/24 (DNS, DHCP, NTP)

Subred del porta privada: 10.0.252.0/24

Segmento 01 - DMZ:

Subred DMZ: 10.0.255.0/24

Contenidos:

5.a Portal Web: Servidores que alojan el portal web accesible desde Internet. Utilizaría un balanceador de carga y estaría protegido por reglas de firewall adecuadas.

Segmento 02 - Red de Servidores:

Subred de Servidores: 10.0.253.0/24

Contenidos:

2. DNS/DHCP/NTP: Servidores que proporcionan servicios de nombres de dominio, configuración de host dinámico y protocolo de tiempo de red.

3. LDAP: Servidores que manejan el servicio de directorio ligero para la autenticación y el directorio de usuarios.

4. SNMP: Servidores o herramientas de monitoreo para gestionar y monitorear dispositivos de red mediante el Protocolo Simple de Administración de Red.

5.b Intranet: Servidor o servidores que alojan la intranet, accesible solo dentro de la red interna.

Segmento 03 - Red de Usuarios:

Subred de Usuarios: Rangos variados dependiendo del grupo de usuarios.

Contenidos:

Usuarios: Estaciones de trabajo de las diferentes entidades (Rector, Profesores, Secretarías, Administración, Estudiantes).

Firewall: NAT/VPN

Subred de Firewall: 10.0.254.0/28

Subred DMZ: 10.0.255.0/24 (Segmento 01)

Subred de Servicios de Red: 10.0.253.0/24 (Segmento 02)

Subred de Usuarios:

Rectoría: 10.0.0.0/24

Profesores: 10.0.1.0/24

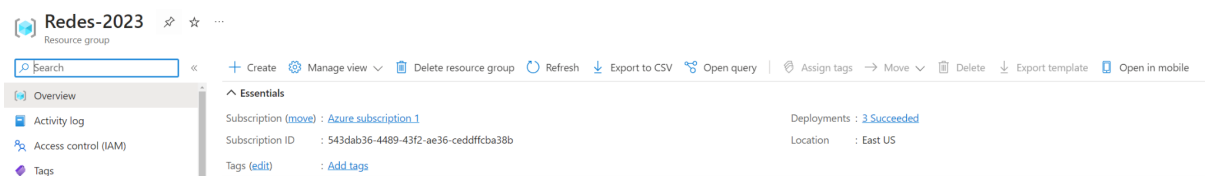
Secretarías: 10.0.2.0/24

Administración: 10.0.3.0/24

Estudiantes: 10.0.4.0/22 (Segmento 03)

Componentes

Dentro de los componentes de Azure lo primero fue crear una red de recursos compartidos



La VNET con las subredes necesarias

Name ↑↓	IPv4 ↑↓
Rectoria	10.0.0.0/24
Profesores	10.0.1.0/24
Secretaria	10.0.2.0/24
Administracion	10.0.3.0/24
Estudiantes	10.0.4.0/22
DMZ	10.0.255.0/24
Servicios	10.0.253.0/24
AzureFirewallSubnet	10.0.254.0/26

También una IP pública para el acceso del Firewall

ippublic2

Public IP address

Search

Overview

Activity log

Access control (IAM)

Tags

Settings

Configuration

Properties

Locks

Associate

Dissociate

Delete

Move

Refresh

Open in mobile

Essentials

Resource group (move) : Redes-2023

Location (move) : East US

Subscription (move) : Azure subscription 1

Subscription ID : 543dab36-4489-43f2-ae36-ceedffcb38b

SKU : Standard

Tier : Regional

IP address : 20.124.210.85

DNS name : -

Associated to : -

Virtual machine : -

Routing preference : Microsoft network

Políticas del Firewall, donde se alojaron las reglas DNAT.

Policy1

Firewall Policy

Search

Overview

Activity log

Access control (IAM)

Tags

Settings

Parent policy

Move

Delete

Lock

Essentials

Resource group (move) : Redes-2023

Location : East US

Subscription (move) : Azure subscription 1

Subscription ID : 543dab36-4489-43f2-ae36-ceedffcb38b

Provisioning state : Succeeded

Tags (edit) : Add tags

Policy name : Policy1

Policy tier : Standard

TLS inspection (Premium) : Not supported with standard policy

IDPS mode (Premium) : Not supported with standard policy

El propio Firewall

Firewall

Firewall

Search

Overview

Activity log

Access control (IAM)

Tags

Settings

Public IP configuration

Learned SNAT IP Prefixes (preview)

Firewall Manager

Essentials

Resource group (move) : [Redes-2023](#)

Location : East US

Subscription (move) : [Azure subscription 1](#)

Subscription ID : S43dab36-4489-43f2-ae36-ceddffcba38b

Virtual network : [CollegeSimulation](#)

Firewall policy : [Policy1](#)

Provisioning state : Updating

Taas (edit) : [Add taas](#)

SKU : [Standard\(change\)](#)

Subnet : [AzureFirewallSubnet](#)

Public IP : [ipPublicVPN](#)

Private IP : 10.0.254.4

Management subnet : [Add](#)

Management public IP : [Add](#)

Private IP Ranges : [Managed by Firewall Policy](#)

Route Server (preview) : [Add](#)

Tabla de rutas:

TabladeRutas | Routes

Route table

Search

+ Add Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Search routes

Name	Address prefix	Next hop type	Next hop IP address
rutas	0.0.0.0/0	VirtualAppliance	10.0.0.4

Una VPN asociada al firewall

Cliente para la web publica utilizando Static Web App

webPublica

Search

Overview

Activity log

Access control (IAM)

Tags

Settings

Public IP configuration

Learned SNAT IP Prefixes (preview)

Firewall Manager

Essentials

Resource group (move) : [Redes-2023](#)

Location : East US

Subscription (move) : [Azure subscription 1](#)

Subscription ID : S43dab36-4489-43f2-ae36-ceddffcba38b

Virtual network : [CollegeSimulation](#)

Firewall policy : [Policy1](#)

Provisioning state : Updating

Taas (edit) : [Add taas](#)

SKU : [Standard\(change\)](#)

Subnet : [AzureFirewallSubnet](#)

Public IP : [ipPublicVPN](#)

Private IP : 10.0.254.4

Management subnet : [Add](#)

Management public IP : [Add](#)

Private IP Ranges : [Managed by Firewall Policy](#)

Route Server (preview) : [Add](#)

View your application

Static Web App

Upgrade your hosting plan

Enable enterprise grade edge

Make the most of your Static Web App

Database connections

Add a serverless backend

Use preview environments

Developer development with IDE

Install SDKs (1)

Application rules:

Policy1 | Application rules

Application rules

Search

+ Add a rule collection + Add rule Edit Delete

Overview

Activity log

Access control (IAM)

Tags

Settings

Parent policy

Rule collections

DNAT rules

Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.

Search to filter items...

Rule Collection Priority	Rule collection name	Rule name	Source	Protocol	Destination	Action	Inherited from
Rule Collection Group: DefaultApplicationRuleCollectionGroup with priority 300.							
104	ApplicationRule	Google	10.0.0.4	Http80/Https443	10.0.0.4	Allow	...
104	ApplicationRule	Privada	10.0.0.4	Http80/Https443	10.0.0.4	Allow	...
104	ApplicationRule	Privada2	10.0.0.4	Http80/Https443	10.0.0.4	Allow	...

DNAT rules:

Policy1 | DNAT rules

Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.

Rule Collection P...	Rule collection n...	Rule name	Source	Port	Protocol	Destination	Translated Addre...	Translated Port	Action
Rule Collection Group: DefaultDnatRuleCollectionGroup with priority 100.									
100	Redes2023	VM-Acces	20.121.41.41	3000	TCP	172.191.8.42	10.0.0.4	3389	Dnat

Para setear el firewall y que tuviera un funcionamiento de reglas adecuadas, se hizo una tabla de rutas válidas las cuales son las que la máquina puede visitar, también la serie de reglas DNAT para la seguridad adecuada, esto con la colección de reglas para que pase por el Firewall y funcione de manera segura el enrutado de las rutas y redes.

Una VM con nginx para acceder a ella a través del acceso remoto

nginx

Virtual machine

Essentials

Resource group (move) : Redes-2023

Status : Stopped (deallocated)

Location : East US (Zone 1)

Subscription (move) : Azure subscription_1

Subscription ID : 89-43f2-ae36-ceddfc8a38b

Availability zone : 1

Tags (edit) : Add tags

Properties

Virtual machine

Property	Value
Computer name	nginx
Operating system	Linux
Image publisher	canonical
Image offer	0001-com-ubuntu-server-focal
Image plan	20_04-fts-gen2
VM generation	V2
VM architecture	x64
Hibernation	Disabled
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Availability + scaling

Property	Value
Availability zone (edit)	1
Availability set (edit)	-
Scale Set	-

Security type

Property	Value
Security type	Trusted launch
Enable secure boot	Enabled
Enable vTPM	Enabled
Integrity monitoring	Disabled

Health monitoring


Property	Value
Health monitoring	Not enabled

Extensions - applications

Property	Value
Extensions	-




Balancer de la VM para la web privada

Home > Redes-2023 >



balancer

Load balancer



Search

»

→ Move

🗑 Delete

🔄 Refresh

🗨 Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Frontend IP configuration

Backend pools

Health probes

Load balancing rules

Inbound NAT rules

Properties

Locks

Monitoring

Insights

Essentials

Resource group (move) : [Redes-2023](#)

Location : East US

Subscription (move) : [Azure subscription 1](#)

Subscription ID : 543dab36-4489-43f2-ae36-ceddfc3ba38b


SKU : Standard

Tags (edit) : [Add tags](#)

[See more](#)




Security group para la VM utilizada en la web privada

Home > Redes-2023 >



nginx-nsg

Network security group



Search

»

→ Move

🗑 Delete

🔄 Refresh

🗨 Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

CLI / PS

Tasks (preview)

Export template

Help

Effective security rules

Support + Troubleshooting

Essentials

Resource group (move) : [Redes-2023](#)

Location : East US

Subscription (move) : [Azure subscription 1](#)

Subscription ID : 543dab36-4489-43f2-ae36-ceddfc3ba38b

Tags (edit) : [Add tags](#)

Filter by name

Port == all

Protocol == all

Source == all

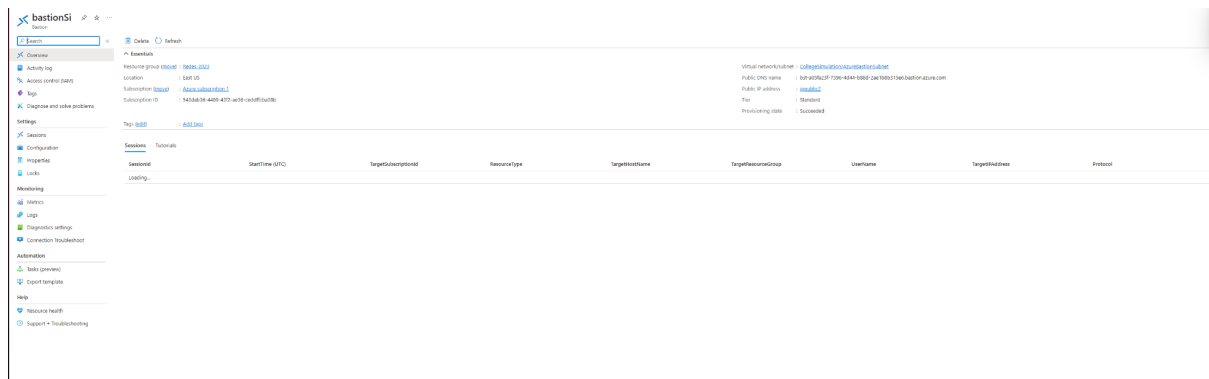
Destination == all

Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓
Inbound Security Rules			
300	SSH	22	TCP
320	HTTP	80	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any
Outbound Security Rules			
65000	AllowVnetOutBound	Any	Any
65001	AllowInternetOutBound	Any	Any
65500	DenyAllOutBound	Any	Any

10

Bastion para ingresar a la VM desde el navegador



Server funcionando

```
nginx@ldapserver:~$ curl http://10.0.0.4
<!DOCTYPE html>
<html>
<head>
<title>Privada</title>
<style>
  body {
    width: 35em;
    margin: 0 auto;
    font-family: Tahoma, Verdana, Arial, sans-serif;
  }
</style>
</head>
<body>
<h1>Web privada con NGINX</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

Para el portal de la intranet se optó por utilizar una máquina virtual corriendo ubuntu, en la cual se instaló NGINX para que sirviera como un proxy dentro de la máquina virtual y de esta manera poder mostrar el portal a los usuarios de la red sin que exista un acceso al exterior. Se decidió hacer ya que de esta manera la máquina virtual funciona como servidor y se podría mantener encendida indefinidamente para que los usuarios puedan acceder al portal y tiene ciertas reglas para que el tráfico que venga de ciertas IPs puedan acceder, mientras que si no se tiene un permiso explícito con una máquina de una tercera persona y se desea acceder no se puede. El uso de esto es bastante útil, ya que si se llegara a necesitar también se puede manejar administración de bases de datos o podría funcionar como un temp file server dentro de la red, entonces la flexibilidad de la máquina virtual fue otra razón por la cual decidimos que se realizara de esta manera. Para poder configurar esta VM se utilizó Azure

Bastión, ya que es la manera más simple de conectarse a la VM sin necesidad de cambiar las configuraciones de ingreso para utilizar máquinas externas y mantener la seguridad.

Con respecto a la web pública, al esta ser pública y no tener que poder acceder a las redes a través de ella se decidió utilizar una web app estática, ya que de esta manera la app funcionaba como su propio server y no tiene que estar conectada al resto de redes, pudiendo tener load balancer propio y manteniendo separacion de que cualquiera puede entrar a la página con que se puedan acceder a las redes a través de ella.

LDAP

La implementación de LDAP implica el despliegue de dos máquinas virtuales interconectadas, cada una cumpliendo un papel específico en el proceso. La primera máquina virtual se integra a la red y sirve como el entorno en el cual se establecerán las configuraciones generales, mientras que la segunda máquina virtual actúa como el servidor principal donde se generarán y almacenarán los datos de permisos, progresivamente dando forma al documento que contendrá toda la información necesaria.

El primer paso de este proceso implica la instalación de OpenLDAP en el servidor principal. Una vez completada la instalación, se procede a realizar la configuración básica en OpenLDAP, la cual suele comenzar con la definición de contenido en los archivos ubicados en etc/hosts. Posteriormente, se lleva a cabo la configuración de la autenticación para los clientes, estableciendo así un entorno seguro para las interacciones. Tras la configuración de permisos, se aborda la tarea crucial de configurar el dominio SLAPD, dando coherencia y estructura al servicio LDAP. Acto seguido, se crea la arquitectura del directorio, incorporando grupos y sus respectivos usuarios para reflejar la organización y jerarquía deseada. Con esta información en su lugar, se procede a la configuración final de la autenticación para los clientes. Al culminar esta fase, el documento generado, ahora con todos los ajustes y configuraciones específicas, está listo para ser exportado al entorno del cliente. Este proceso garantiza que todos los datos críticos y configuraciones necesarias se transmitan correctamente, permitiendo una verificación exhaustiva para asegurar la integridad y coherencia de la información en el cliente. Con este enfoque estructurado, se establece un sistema LDAP robusto y funcional que responde a las necesidades de autenticación y autorización de la red.

Para este paso en el proyecto no se pudo realizar en su totalidad, ya que se necesitaban dos máquinas virtuales con IP publica pero nos habíamos quedado sin IPs públicas ya que Azure solo deja tener 3, pero se puede ver la todo creación de las reglas en [Anexos](#). A continuación se tendrán imágenes de lo más importante de la configuración.

```

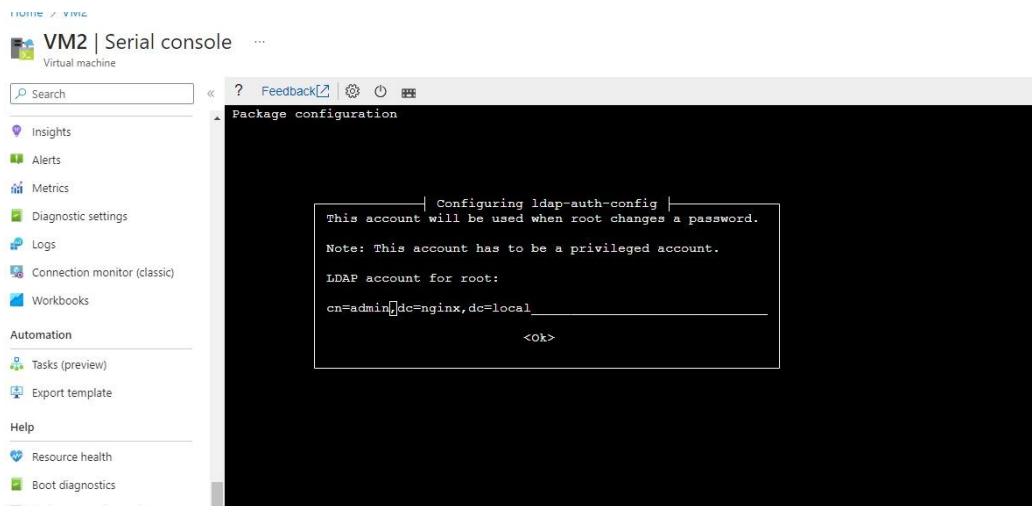
nginx@nginx:~$ sudo slapcat
dn: dc=nginx,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: nginx
dc: nginx
structuralObjectClass: organization
entryUUID: 635787e6-1cef-103e-83a1-b36a49248782
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121192452Z
entryCSN: 20231121192452.050242Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121192452Z

dn: cn=admin,dc=nginx,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9bjhibXFaV2VuQWs5cXRxRmFOcW5CczNCdlVxY1l6TTE=
structuralObjectClass: organizationalRole
entryUUID: 63592b0a-1cef-103e-83a2-b36a49248782
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121192452Z
entryCSN: 20231121192452.061020Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121192452Z

dn: ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: organizationalUnit
ou: CollegeSimulation
structuralObjectClass: organizationalUnit
entryUUID: 6943272a-1cf2-103e-83f7-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121194630Z
entryCSN: 20231121194630.473235Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121194630Z

dn: cn=informatica,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 10000

```



```
« ? Feedback[?] ⚙️ 🔌 🖨️
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd:      files ldap
group:       files ldap
shadow:      files ldap
gshadow:     files

hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis

VM2@VM2:~$ sudo getent passwd
^C2023-11-21T23:28:45.279182Z INFO Daemon Agent WALinuxAgent-2.9.1.1 launched with command 'python3 -u bin/WALinuxAgent-2.9.1.1/exthandlers.py'
3.8.egg -run-exthandlers' is successfully running
```

DNS

Se creó una DNS zone privada y se linkeo con el network virtual que teníamos para generar los el servicio de DNS para los servicios

proyectofinal5.com

Private DNS zone

Search

+ Record set → Move ▾ Delete zone Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Virtual network links

Properties

Locks

Monitoring

Alerts

Metrics

Automation

Tasks (preview)

Export template

Help

Support + Troubleshooting

Essentials

Resource group (move) : [redes-2023](#)

Subscription (move) : [Azure subscription 1](#)

Subscription ID : 543dab36-4489-43f2-ae36-ced0ffca38b

Tags (edit) : [Add tags](#)

You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value
@	SOA	3600	Email: azureprivatedns-host.microsoft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1
gsa-6269cc2b-813e000000	A	10	10.0.254.5
gsa-6269cc2b-813e000001	A	10	10.0.254.6
nginx	A	10	10.0.0.4
server	A	3600	10.0.253.0
vm000000	A	10	10.0.1.68
vm000001	A	10	10.0.1.69
vm2	A	10	10.0.3.6

```
nginx@ldapserver:~$ nslookup nginx.projecctofinal5.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   nginx.projecctofinal5.com
Address: 10.0.0.4

nginx@ldapserver:~$ nslookup server.projecctofinal5.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   server.projecctofinal5.com
Address: 10.0.253.0

nginx@ldapserver:~$ nslookup vm000000.projecctofinal5.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   vm000000.projecctofinal5.com
Address: 10.0.1.68

nginx@ldapserver:~$ nslookup vm000001.projecctofinal5.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   vm000001.projecctofinal5.com
Address: 10.0.1.69

nginx@ldapserver:~$ █
```

También está una DNS zone pública

publicfinalproject5.com

DNS zone

Search

+ Record set + Child zone ↑ Import ↓ Export Delete zone → Move ↻ Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Properties

Locks

Monitoring

Alerts

Metrics

Automation

Tasks (preview)

Export template

Help

Resource health

Essentials

Resource group (move) : [redes-2023](#)

Subscription (move) : [Azure_subscription_1](#)

Subscription ID : 543dab36-4489-43f2-ae36-ceddfc8a38b

Tags (edit) : [Add tags](#)

You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value
Ⓜ	NS	172800	ns1-32.azure-dns.com. ns2-32.azure-dns.net. ns3-32.azure-dns.org. ns4-32.azure-dns.info. Email: azure-dns-hostmaster@microsoft.com Host: ns1-32.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1
Ⓜ	SOA	3600	
server	A	3600	10.0.253.0

Name server 1 : ns1-32.azure-dns.com.

Name server 2 : ns2-32.azure-dns.net.

Name server 3 : ns3-32.azure-dns.org.

Name server 4 : ns4-32.azure-dns.info.


```
PS C:\Users\Jun> nslookup server.publicfinalproyect5.com ns1-32.azure-dns.com
Server: UnKnown
Address: 2603:1061:0:10::20

Name:     server.publicfinalproyect5.com
Address:  10.0.253.0
```

NTP

Acá se puede ver en el archivo de /etc/ntp.conf los servers de NTP pool que se están usando.

```
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
pool 0.ubuntu.pool.ntp.org iburst
pool 1.ubuntu.pool.ntp.org iburst
pool 2.ubuntu.pool.ntp.org iburst
pool 3.ubuntu.pool.ntp.org iburst
```

Funcionamiento de NTP funcionando al poner el comando de ntpq -p

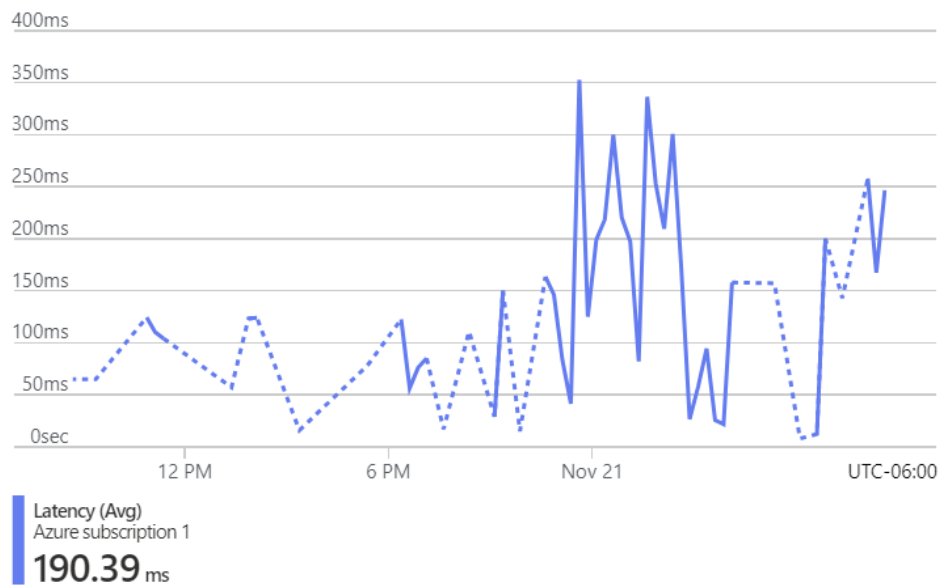
```
nginx@ldapserver:~$ ntpq -p
      remote           refid      st t when poll reach   delay   offset  jitter
=====
0.ubuntu.pool.n .P00L.        16 p   -   64    0    0.000    0.000    0.000
1.ubuntu.pool.n .P00L.        16 p   -   64    0    0.000    0.000    0.000
2.ubuntu.pool.n .P00L.        16 p   -   64    0    0.000    0.000    0.000
3.ubuntu.pool.n .P00L.        16 p   -   64    0    0.000    0.000    0.000
ntp.ubuntu.com .P00L.        16 p   -   64    0    0.000    0.000    0.000
-nu.binary.net  216.239.35.12  2 u 1444  256  340   54.404   -3.920    6.034
-185.125.190.56 194.121.207.249 2 u 1425  256  340   89.677   -3.055    0.155
nginx@ldapserver:~$
```

Rendimiento

Dentro del ámbito de la gestión y optimización de recursos en el diseño de redes, resulta fundamental examinar diferentes métricas de los componentes de una red. Por esta razón para medir la eficiencia y rendimiento de la estructura planteada para este proyecto se desarrollaron diferentes puntos de monitoreo para diferentes componentes con el objetivo de analizar datos clave relacionados a la red y sus componentes esenciales. Por lo que a continuación se entrará más en detalle acerca de las métricas encontradas en la red y se ofrecerá un análisis que explicara que significan los diferentes tipos de métricas y permite observar que todo esté funcionando correctamente.

Monitoreo general

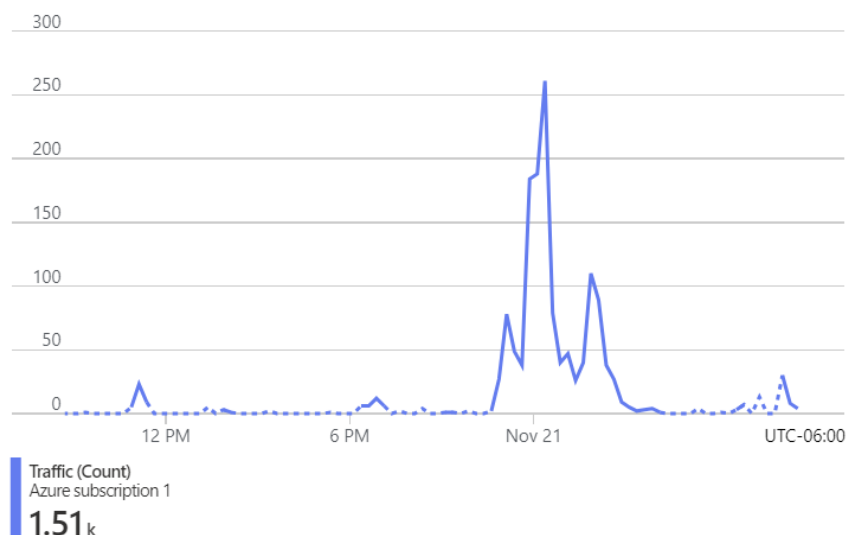
✓ Avg Latency for Redes 2023 in Global region



Para la red en general se midió la latencia promedio, esta mide el tiempo promedio que transcurre desde que se inicia una solicitud hasta que se recibe una respuesta, representando así la latencia media en la comunicación entre los servicios y recursos de la red por lo que esta es una de las métricas más importantes para evaluar el rendimiento general de la red.

Como se puede observar la latencia suele variar bastante entre 50ms y 350 ms, que como promedio da 190.39ms. Esto es un valor bastante aceptable para el uso que se le da a la red ya que el tipo de recursos al que se accede no es necesariamente dependiente de muchas solicitudes, por lo que la latencia no afecta tanto en este aspecto.

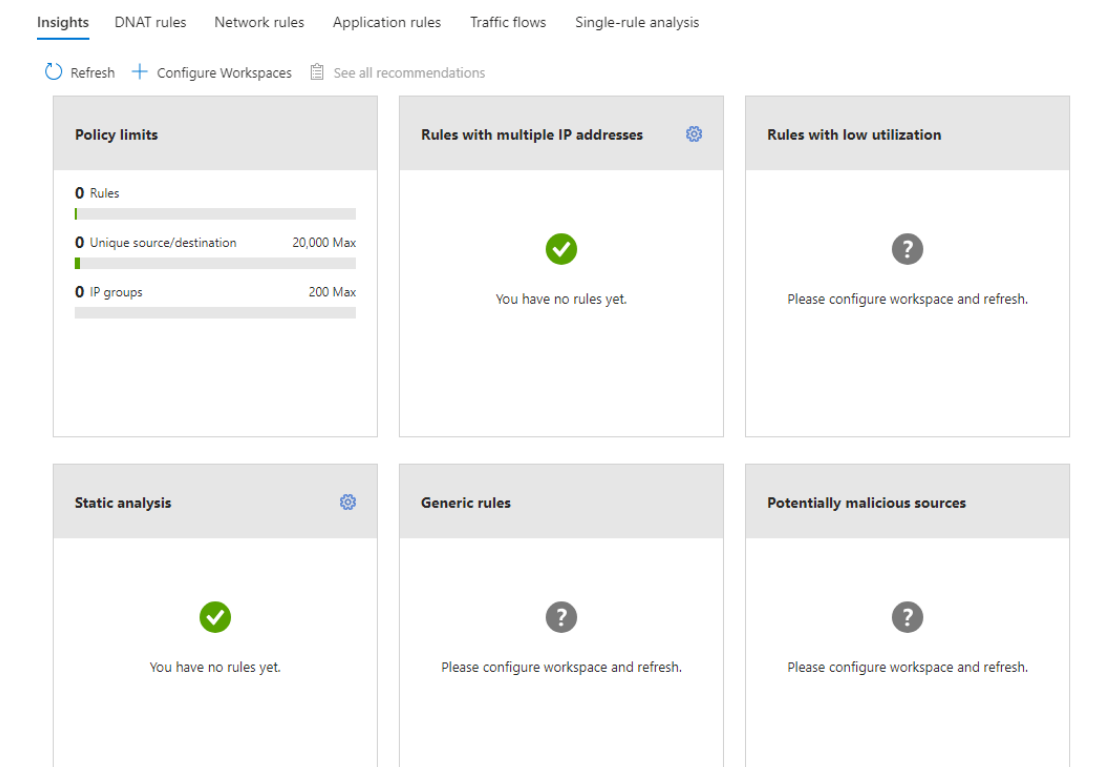
✓ Count Traffic for Redes 2023 in Global region



Adicionalmente se midió el tráfico total a través del tiempo para toda la red, esta medición se refiere al flujo de datos o paquetes dentro de la red. Esta métrica en conjunto con otras métricas de uso de los componentes nos puede ayudar a la evaluación de la carga de trabajo

sobre los diferentes componentes de la red y poder determinar si los recursos se están distribuyendo adecuadamente en toda la red. Adicionalmente, como caso de uso a largo plazo se pueden utilizar estas métricas para revelar patrones de uso a lo largo del tiempo, un aspecto que puede resultar crucial al momento de planificar y optimizar las diferentes capacidades de la red.

Monitoreo de Firewall



Dentro de este dashboard de monitoreo del firewall se pueden observar diferentes posibles métricas que en el futuro pueden ir evolucionando según las reglas y políticas que se establezcan para este firewall y qué uso se le dé dentro de la red.

Por ejemplo, las métricas de los límites de políticas mide el alcance de estas y ayuda a identificar si se están alcanzando umbrales que pueden ser previamente establecidos que podrían llegar a afectar al rendimiento del firewall. Si los límites se alcanzan con frecuencia, podría llegar a ser necesario ajustar alguna configuración o agregar recursos adicionales para garantizar un óptimo funcionamiento.

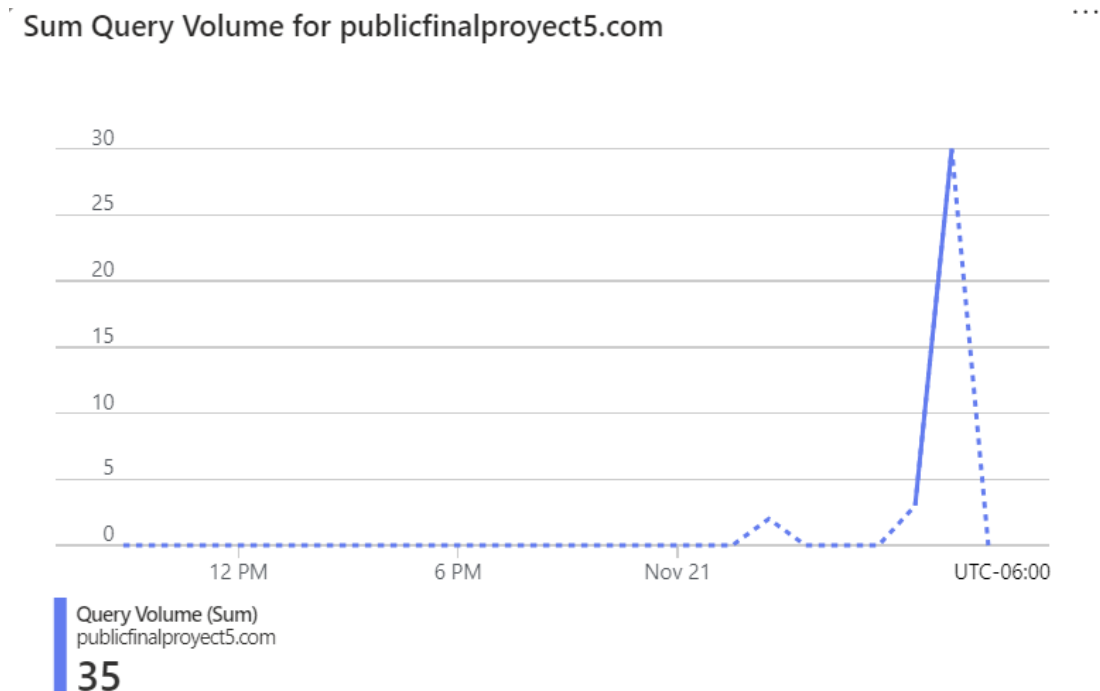
La métrica de reglas con múltiples direcciones IP se utilizan para simplificar y optimizar la configuración del firewall al consolidar reglas con direcciones IP similares.

La métrica de reglas con baja utilización puede permitir la observar que reglas pueden ser ajustadas en caso estas sean innecesarias o que necesitan ser ajustadas para hacer tener un efecto real.

El análisis estático es una métrica que evalúa la configuración del firewall sin tomar en cuenta el tráfico, lo que puede ayudar a identificar posibles vulnerabilidades o configuración subóptimas que tengan un efecto negativo en el rendimiento.

Por otro lado la métrica de fuentes potencialmente maliciosas detectan dirección IP o patrones de tráfico que podría indicar actividades maliciosas dentro de la red, esta métrica puede contribuir a una detección temprana de amenazas y mejorar la seguridad de la red.

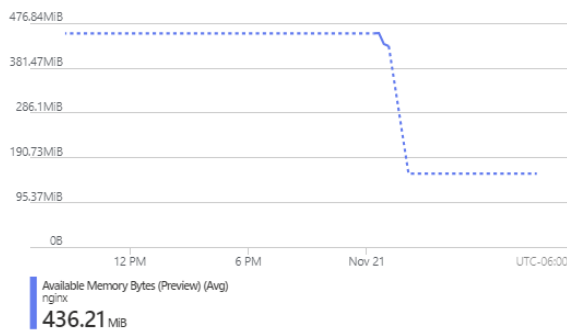
Monitoreo DNS dominio



Esta métrica describe la cantidad de consultas o peticiones realizadas sobre en dominio DNS, esta métrica ayuda a observar y evaluar la escalabilidad del servicio, si por ejemplo, hay un volumen de consultas que se acercan o superan los límites de rendimiento del servicio, podría ser necesario escalar los recursos para manejar de manera eficiente la demanda.

Monitoreo de nginx (Virtual Machine)

Avg Available Memory Bytes (Preview) for nginx



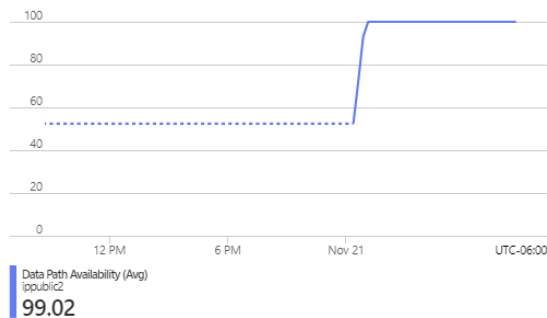
Avg Percentage CPU for nginx



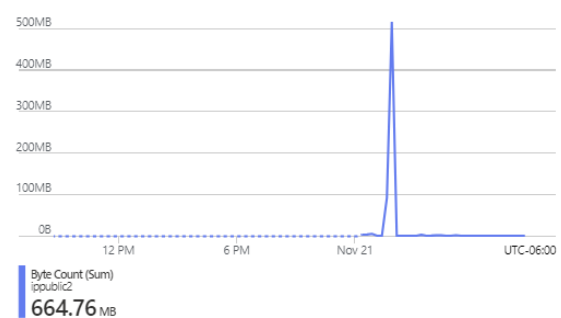
El monitoreo de la máquina virtual que contiene nginx tiene dos métricas importantes, la memoria promedio disponible y el promedio de porcentaje de uso de CPU, estas en conjunto con otras métricas vistas anteriormente pueden ayudar a medir la eficiencia con la que se utilizan los recursos y si hay alguna necesidad de escalabilidad para la máquina. Por otro lado también se pueden observar posibles cuellos de botella que están sucediendo en este apartado, lo cual puede ayudar a la decisión de optimizar los diferentes procesos y componentes para obtener el rendimiento deseado.

Monitoreo de IP pública

Avg Data Path Availability for ippublic2



Sum Byte Count for ippublic2



Estas métricas nos pueden proporcionar información vital sobre la salud y el rendimiento de los recursos asociados, por ejemplo la métrica disponibilidad de la data puede indicar si existen problemas de congestión, pérdida de paquetes o interrupciones de conectividad, por lo que puede ayudar a identificar problemas dentro de la red y permite que se puedan tomar medidas correctivas lo antes posible.

Por otro lado, la suma de los bytes transmitidos o recibidos por la IP pública pueden ayudar a entender el uso real del ancho de banda y así poder ayudar a planificar la capacidad, optimizar el rendimiento de la red y posiblemente anticipar necesidades futuras de escalabilidad.

Conclusiones

- El uso de métricas puede ayudarnos a determinar si nuestra red se está comportando de manera correcta y puede ayudar a identificar posibles problemas en las diferentes áreas y componentes que forman parte de la red.
- La segmentación en subredes para Rectorado, Profesores, Secretarías, Administración y Estudiantes permite un control preciso sobre el acceso y la seguridad. La inclusión de segmentos dedicados a la DMZ, Servidores, y Usuarios es una buena práctica para mantener la seguridad y la eficiencia operativa.
- La utilización de máquinas virtuales para la intranet, junto con Azure Bastion para la conexión segura, demuestra una consideración cuidadosa de la seguridad y la flexibilidad operativa. El uso de una web app estática para la web pública también muestra una implementación eficiente y segura.
- La implementación de LDAP con dos máquinas virtuales, una para la configuración general y otra como servidor principal, sigue las mejores prácticas. La elección de OpenLDAP y la configuración detallada del dominio SLAPD demuestran un enfoque cuidadoso en la seguridad y la organización del directorio.
- La implementación de reglas de firewall y la consideración de la seguridad en cada componente, como en la web app y en la conexión a la intranet, demuestra la atención a la seguridad de la red.

Referencias Bibliográficas

Microsoft. (2023). AZ-700 Designing and Implementing Microsoft Azure Networking Solutions - Training

<https://learn.microsoft.com/en-us/training/paths/design-implement-microsoft-azure-networking-solutions-az-700/>

Microsoft. (2023). Azure Monitor Metrics Overview.

<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-platform-metrics>

Microsoft (2023). Supported metrics with Azure Monitor.

<https://learn.microsoft.com/en-us/azure/azure-monitor/reference/supported-metrics/metrics-index>

Microsoft. (n.d.). Habilitación de firmas LDAP en Windows Server. Microsoft Learn.

<https://learn.microsoft.com/es-es/troubleshoot/windows-server/identity/enable-ldap-signing-in-windows-server>

QE2 Computing. (n.d.). Instalar y configurar OpenLDAP.

<https://www.qe2computing.com/articulos-software/instalar-configurar-openldap/>

Ruiz, P. (2022, marzo 31). LDAP (parte 8): Instalar y configurar la interfaz web LDAP Account Manager para administrar OpenLDAP. SomeBooks.es.

<http://somebooks.es/ldap-parte-8-instalar-y-configurar-la-interfaz-web-ldap-account-manager-para-administrar-openldap/>

Anexos

sole ...

```
? Feedback [?] [⚙️] [🔌] [🖨️]
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd:      files ldap
group:       files ldap
shadow:      files ldap
gshadow:     files

hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis

VM2@VM2:~$ sudo getent passwd
^C2023-11-21T23:28:45.279182Z INFO Daemon Agent WALinuxAgent-2.9.1.1 launched with command 'python3 -u bin/WALinuxAgent-2.9.1.1/bin/egg -run-exthandlers' is successfully running
```

HOME / VM2

VM2 | Serial console ...

Virtual machine

Search

Insights

Alerts

Metrics

Diagnostic settings

Logs

Connection monitor (classic)

Workbooks

Automation

Tasks (preview)

Export template

Help

Resource health

Boot diagnostics

? Feedback [?] [⚙️] [🔌] [🖨️]

Package configuration

Configuring ldap-auth-config

This account will be used when root changes a password.

Note: This account has to be a privileged account.

LDAP account for root:

cn=admin,dc=nginx,dc=local

<Ok>

```
dn: uid=servicios,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: servicios
uid: servicios
ou: informatica
uidNumber: 2004
gidNumber: 10000
homeDirectory: /home/nginx5
loginShell: /bin/bash
userPassword:: UHJveWVjdG9SZWRlczIwMjMq
sn: servicios
mail: nginx5@uvg.edu.gt
givenName: servicios
structuralObjectClass: inetOrgPerson
entryUUID: 5b3c0b82-1cfd-103e-83fd-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121210451Z
entryCSN: 20231121210451.402599Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121210451Z

dn: uid=profesores,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: profesores
uid: profesores
ou: informatica
uidNumber: 2005
gidNumber: 10000
homeDirectory: /home/nginx6
loginShell: /bin/bash
userPassword:: UHJveWVjdG9SZWRlczIwMjMq
sn: profesores
mail: nginx6@uvg.edu.gt
givenName: profesores
structuralObjectClass: inetOrgPerson
entryUUID: 83b5caa8-1cfd-103e-83fe-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121210559Z
```

```
dn: uid=rectoria,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: rectoria
uid: rectoria
ou: informatica
uidNumber: 2002
gidNumber: 10000
homeDirectory: /home/nginx3
loginShell: /bin/bash
userPassword:: UHJveWVjdG9SZWRlc2IwMjMq
sn: rectoria
mail: nginx3@uvvg.edu.gt
givenName: rectoria
structuralObjectClass: inetOrgPerson
entryUUID: c1578b36-1cfc-103e-83fb-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121210033Z
entryCSN: 20231121210033.213687Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121210033Z

dn: uid=estudiantes,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: estudiantes
uid: estudiantes
ou: informatica
uidNumber: 2003
gidNumber: 10000
homeDirectory: /home/nginx4
loginShell: /bin/bash
userPassword:: UHJveWVjdG9SZWRlc2IwMjMq
sn: estudiantes
mail: nginx4@uvvg.edu.gt
givenName: estudiantes
structuralObjectClass: inetOrgPerson
entryUUID: eaccbc7a-1cfc-103e-83fc-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121210142Z
```

```
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: administracion
uid: administracion
ou: informatica
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/nginx
loginShell: /bin/bash
userPassword:: UHJveWVjdG9SZWRlczIwMjMq
sn: Worker
mail: nginx@uvg.edu.gt
givenName: administracion
structuralObjectClass: inetOrgPerson
entryUUID: fec7c792-1cf7-103e-83f9-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121202628Z
entryCSN: 20231121202628.806581Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121202628Z

dn: uid=secretaria,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: secretaria
uid: secretaria
ou: informatica
uidNumber: 2001
gidNumber: 10000
homeDirectory: /home/nginx2
loginShell: /bin/bash
userPassword:: UHJveWVjdG9SZWRlczIwMjMq
sn: secretaria
mail: nginx2@uvg.edu.gt
givenName: secretaria
structuralObjectClass: inetOrgPerson
entryUUID: f2b1fdca-1cfb-103e-83fa-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121205446Z
entryCSN: 20231121205446.518075Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121205446Z

nginx@nginx:~$
```



```

? Feedback [?] [gear] [power] [exit]
objectClass: organizationalUnit
ou: CollegeSimulation
structuralObjectClass: organizationalUnit
entryUUID: 6943272a-1cf2-103e-83f7-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121194630Z
entryCSN: 20231121194630.473235z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121194630Z

dn: cn=informatica,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 10000
cn: informatica
structuralObjectClass: posixGroup
entryUUID: dbaba5fa-1cf5-103e-83f8-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121201110Z
entryCSN: 20231121201110.908531z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121201110Z

dn: uid=administracion,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: administracion
uid: administracion
ou: informatica
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/nginx
loginShell: /bin/bash
userPassword:: UHJveWVjdG9SZWRlczIwMjMq
sn: Worker
mail: nginx@uvg.edu.gt
givenName: administracion
structuralObjectClass: inetOrgPerson
entryUUID: fec7c792-1cf7-103e-83f9-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121202628Z
entryCSN: 20231121202628.806581z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121202628Z

nginx@nginx:~$

```

```
GNU nano 4.8          usr.ldif          Modified
dn:uid=administracion,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: administracion
uid: administracion
ou: informatica
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/nginx
loginShell: /bin/bash
userPassword: ProyectoRedes2023*
```

```
GNU nano 4.8          usr.ldif          Modified
dn:uid=administracion,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: administracion
uid: administracion
ou: informatica
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/nginx
loginShell: /bin/bash
userPassword: ProyectoRedes2023*
```

```

nginx@nginx:~$ sudo slapcat
dn: dc=nginx,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: nginx
dc: nginx
structuralObjectClass: organization
entryUUID: 635787e6-1cef-103e-83a1-b36a49248782
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121192452Z
entryCSN: 20231121192452.050242Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121192452Z

dn: cn=admin,dc=nginx,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9bjhibXFaV2VuQW55cXRxRmFOcW5Cc2NCdlVxY1l6TTE=
structuralObjectClass: organizationalRole
entryUUID: 63592b0a-1cef-103e-83a2-b36a49248782
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121192452Z
entryCSN: 20231121192452.061020Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121192452Z

dn: ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: organizationalUnit
ou: CollegeSimulation
structuralObjectClass: organizationalUnit
entryUUID: 6943272a-1cf2-103e-83f7-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121194630Z
entryCSN: 20231121194630.473235Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121194630Z

dn: cn=informatica,ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 10000

```

? Feedback    

GNU nano 4.8

grp.ldif

```

dn:cn=informatica, ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 10000
ou: CollegeSimulation

```

```
nginx@nginx:~$ sudo slapcat
dn: dc=nginx,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: nginx
dc: nginx
structuralObjectClass: organization
entryUUID: 635787e6-1cef-103e-83a1-b36a49248782
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121192452Z
entryCSN: 20231121192452.050242Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121192452Z

dn: cn=admin,dc=nginx,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9bjhibXFav2VuQWs5cXRxRmFOcW5CczNCdlVxY1l6TTE=
structuralObjectClass: organizationalRole
entryUUID: 63592b0a-1cef-103e-83a2-b36a49248782
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121192452Z
entryCSN: 20231121192452.061020Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121192452Z

dn: ou=CollegeSimulation,dc=nginx,dc=local
objectClass: top
objectClass: organizationalUnit
ou: CollegeSimulation
structuralObjectClass: organizationalUnit
entryUUID: 6943272a-1cf2-103e-83f7-c9ca4a53db05
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121194630Z
entryCSN: 20231121194630.473235Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121194630Z

nginx@nginx:~$
```




nginx | Serial console

Virtual machine

>>

? [Feedback](#) ⚙️ 🔌 🖨️

```
nginx@nginx:~$ sudo slapcat
dn: dc=nginx,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: nginx
dc: nginx
structuralObjectClass: organization
entryUUID: 635787e6-1cef-103e-83a1-b36a49248782
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121192452Z
entryCSN: 20231121192452.050242Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121192452Z

dn: cn=admin,dc=nginx,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9bjhibXFav2VuQWs5cXRxRmFOcW5CcZNCdlVxY1l6TTE=
structuralObjectClass: organizationalRole
entryUUID: 63592b0a-1cef-103e-83a2-b36a49248782
creatorsName: cn=admin,dc=nginx,dc=local
createTimestamp: 20231121192452Z
entryCSN: 20231121192452.061020Z#000000#000#000000
modifiersName: cn=admin,dc=nginx,dc=local
modifyTimestamp: 20231121192452Z

nginx@nginx:~$
```