ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“IMPLEMENTACIÓN DE LA AUTENTICACIÓN DE USUARIOS EN LA INFRAESTRUCTURA DE RED DE UNA EMPRESA USANDO EL LDAP CORPORATIVO”

EXAMEN DE GRADO

PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TELECOMUNICACIONES

MIRELLA ROXANNA LEÓN TILUANO

GUAYAQUIL – ECUADOR

2020

AGRADECIMIENTO

Agradezco a Dios por la vida y la salud, necesarias para poder realizar el presente trabajo. A mi familia y en especial a mi amado esposo que siempre me animaron a seguir luchando y me apoyaron con sus oraciones. Dios los bendiga siempre.

DEDICATORIA

Dedico el presente trabajo a las personas verdaderamente cercanas a mí, con las cuales las alegrías se multiplican y las penas se dividen y se vencen: mis padres Mirella Tiluano y Santos León; mis hermanos: Viviana, Gissella, Luis, Mercedes; mis amigas: Tanya García, Aida Serrano; y a mi esposo Carlos Calero por ser el apoyo incondicional en mi vida.

TRIBUNAL DE EVALUACIÓN

MSc. Verónica Soto
PROFESOR EVALUADOR

MARIA ANTONIETA ALVAREZ VILLANUEVA
Digitally signed by MARIA ANTONIETA ALVAREZ VILLANUEVA

PhD. Maria Antonieta Alvarez
PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me(nos) corresponde exclusivamente; y doy(damos) mi(nuestro) consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

LEÓN TIL[illegible]ANO MIRELLA ROXANNA

RESUMEN

En una red corporativa existen variedad de tareas asignadas a personal técnico. Seguramente muchas de esas tareas se las realiza de forma manual y en algunas ocasiones ocurren errores humanos al ejecutarlas. Si la empresa crece la red probablemente crecerá también, y esto requerirá que la cantidad de personal técnico asignado a mantenerla y operarla crezca igualmente. Estos incrementos pueden lograr que la probabilidad de que ocurran “errores humanos” sea mayor.

El presente trabajo busca reducir significativamente esos errores enfocados en controlar el acceso del personal técnico a dispositivos de una red corporativa, switches, específicamente. Se plantea el problema de tener usuarios locales para los técnicos que administran y operan los switches de una red y se sugiere que la autenticación local se elimine y se realice contra un Servicio de Control de Acceso logrando desaparezca la necesidad de agregar/eliminar usuarios directamente en los switches.

Para comprender la motivación de la solución se revisarán brevemente conceptos de Seguridad de la Información (ISO 27001), de Servicios de Directorio (LDAP) y de Sistemas de Control de Acceso a la Red (TACACS+), los cuales permitirán visualizar los beneficios de implementar la solución propuesta.

A continuación, se mencionarán los recursos que se necesitan para resolver el problema planteado y se propondrá una guía general de implementación y validación de que la propuesta alcanzará los objetivos planteados y permitirá un mejor control del acceso a los dispositivos de red.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

INTRODUCCIÓN

1.1. Descripción del problema

La gestión de usuarios, en los switches de la red, de una empresa de servicios de telecomunicaciones puede ser tediosa si se usan usuarios locales en cada uno de los switches. Crear y eliminar usuarios locales en un solo switch resulta sencillo, pero si el número de switches se incrementa a 10, 20, ó 100, la misma tarea a pesar de ser sencilla se vuelve propensa a fallas humanas.

En la empresa a la que nos referimos se requiere que cada operador o administrador de switches realice sus tareas usando su propio usuario y no un usuario por departamento o por funciones. Poder reconocer las acciones realizadas por un usuario a través de los LOGs de los switches se incluye en las buenas prácticas de Seguridad de Redes.

La asignación de permisos para poder ejecutar acciones específicas en los switches implica algo de tiempo si se realiza asignando permisos a usuarios y no a grupos de usuarios. Ese tiempo se multiplica por la cantidad de usuariosy de switches en los que estos usuarios deben ser configurados.

En resumen, el problema de esta empresa son los errores que suceden en la creación, eliminación de usuarios y en la asignación de permisos en los switches de la red, además del tiempo invertido para realizar esas tareas, teniendo que realizar, a veces, revisiones generales para chequear y corregir los errores cometidos.

1.2. Justificación/Propuesta

La propuesta eliminará los errores en la gestión de la seguridad de los dispositivos de red, switches, de la empresa ya que se usarán las mismas credenciales usadas en las otras aplicaciones internas, además de que los administradores podrían disponer del tiempo usado para crear/eliminar usuarios en otras actividades.

1.3. Objetivos

1.3.1. Objetivos Generales

- Incrementar la seguridad de la red corporativa.
- Mejorar la disponibilidad y confidencialidad de los switches de la red corporativa.
- Disminuir la carga operativa de la gestión de usuarios locales en los switches de la red corporativa.

1.3.2. Objetivos Específicos

- Configurar que la validación de las credenciales de los usuarios de los switches se realice usando el LDAP Corporativo.
- Configurar los permisos de los usuarios de los switches por medio del grupo al que pertenecen los usuarios en el LDAP corporativo.

1.4. Marco Teórico

Seguridad de la Información

En el contexto de la empresa que estamos analizando, esta tiene la certificación ISO 27001[1], por lo tanto, sus directivos y colaboradores de todos los rangos están comprometidos con la Seguridad de la Información.

¿Y qué es la seguridad de la información? Se puede resumir que consiste en la implementación de un conjunto de medidas o técnicas enfocadas en preservar la confidencialidad, integridad y disponibilidad de la información.

La confidencialidad requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas para hacerlo. Hace referencia a la necesidad de mantener oculta determinada información o recurso.

La integridad requiere que la información se mantenga sin alteraciones ante accidentes o intentos maliciosos. Sólo se puede modificar la información si se está autorizado para hacerlo.

La disponibilidad requiere que la información esté accesible a los usuarios autorizados cuando ellos la necesiten. Se busca prevenir interrupciones no autorizadas de los recursos que proveen la información.

Servicio de Directorio

Un directorio es una base de datos especializada, diseñada específicamente para buscar y navegar, incluyendo funciones básicas de búsqueda y actualización.

Los directorios tienden a tener información descriptiva basada en atributos admitiendo capacidades de filtrado sofisticadas. Generalmente no admiten transacciones complicadas o de reversión, como las que se encuentran en sistemas de administración de base de datos que se enfocan en actualizaciones de gran volumen. Las actualizaciones de directorio son cambios simples. Los directorios se ajustan para dar respuestas rápidas a operaciones de búsqueda de gran volumen.

Existen variedad de soluciones de directorio, pero en la empresa en la que se desarrolla el proyecto tienen ya implementado OpenLDAP [2], por lo que se obviará comentar sobre otras opciones.

LDAP es un protocolo liviano de acceso a directorios y OpenLDAP es el proyecto de código abierto para implementar LDAP.

El modelo de información LDAP se basa en entradas, que es una colección de atributos que tiene un nombre distintivo (DN) que permite referirse a una entrada sin ambigüedad. Cada atributo de una entrada tiene un tipo y uno o varios valores.

La información en LDAP está organizada jerárquicamente en una estructura similar a un árbol. Tradicionalmente esta estructura refleja los límites organizacionales y/o geográficos definiendo Unidades Organizacionales (OU). En la imagen de la Figura 1.1 se muestra el esquema de un directorio LDAP:

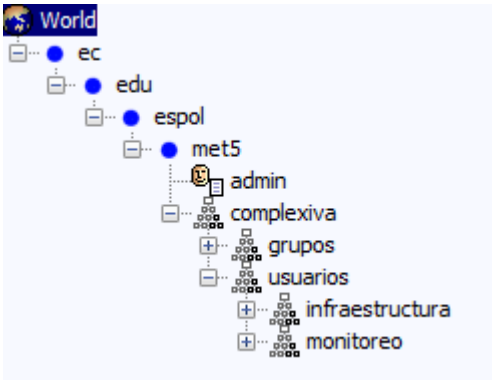

Figura 1.1 Ejemplo de Directorio LDAP

Sistema de Control de Acceso a la Red

TACACS, es el acrónimo de Terminal Access Controller Access Control System, que traducido sería “Sistema de Control de Acceso del Controlador de Acceso al Terminal”. Es un protocolo de autenticación remota de Cisco, usado generalmente en redes Unix, para comunicarse con un servidor de autenticación y determinar si un usuario tiene acceso o no a la red.

TACACS+ ha reemplazado a TACACS y vienen con beneficios adicionales [3], como separar la autenticación, autorización y registro, además de encriptar el tráfico entre el cliente y el servidor. Además, tiene un diseño modular que permite agregarle plug-ins.

1.5. Escenario del Problema

El escenario del problema se ubica en una empresa que posee decenas de dispositivos de red, switches administrables principalmente, los cuales son operados/administrados por diferentes colaboradores de dos departamentos que denominaremos monitoreo (operadores) e infraestructura (administradores).

Cuando la red iniciaba el número de switches era mínimo y los permisos para acceder a ellos se configuraban agregando de forma manual los usuarios de los dos departamentos, que también al inicio eran un grupo reducido de personas.

Asimismo, cuando un colaborador salía de la empresa el usuario era eliminado de todos los switches de forma manual.

Conforme los servicios proporcionados por la empresa crecían también lo hacía la red para soportar el crecimiento, y por ende el número de switches fue creciendo. Además de los switches, los departamentos de infraestructura y monitoreo tuvieron que agregar nuevos colaboradores para poder atender los requerimientos de los clientes.

El incremento de equipo y personal comenzó a hacer que las tareas de agregar/eliminar usuarios comience a evidenciar errores y olvidos que causaban que el personal que debía ingresar a cierto switch no pudiera porquesu usuario no había sido agregado o que en ciertos switches existieran usuariosde personas que ya no laboraban en la empresa.

Los errores/olvidos se incrementaban conforme la red seguía creciendo, y es en ese momento que las jefaturas y gerencias deciden aplicar una solución que disminuya y/o suprima este tipo de problemas, siendo la opción elegida que la autenticación de los usuarios de los switches se realiza usando el LDAP que la empresa tiene funcionando y que les permite acceder a las aplicaciones internas.

En la Tabla 1 se resumen las cantidades de usuarios y dispositivos que tiene la empresa en la ubicación donde se implementa la presente propuesta:

Elemento	Cantidad
Switches	60
Tipos de usuario	2
Usuarios operadores	16
Usuarios administradores	14

Tabla 1. Cantidad de elementos y usuarios en red corporativa

CAPÍTULO 2

Guía de Implementación

2.1. Arquitectura de la Implementación

En esta sección se listarán los componentes de la implementación y se bosquejará en un diagrama su interconexión.

2.1.1. Componentes

En la implementación de la presente propuesta se distinguirán los siguientes componentes:

- Switches
- LDAP
- TACACS+

De los componentes hay que mencionar que el servidor TACACS+ es un componente que no existía en la red y que será agregado para implementar la solución propuesta.

2.1.2. Diagrama General de la Solución

En la imagen de la Figura 2.1 se puede apreciar el diagrama de la Arquitectura de la solución propuesta:

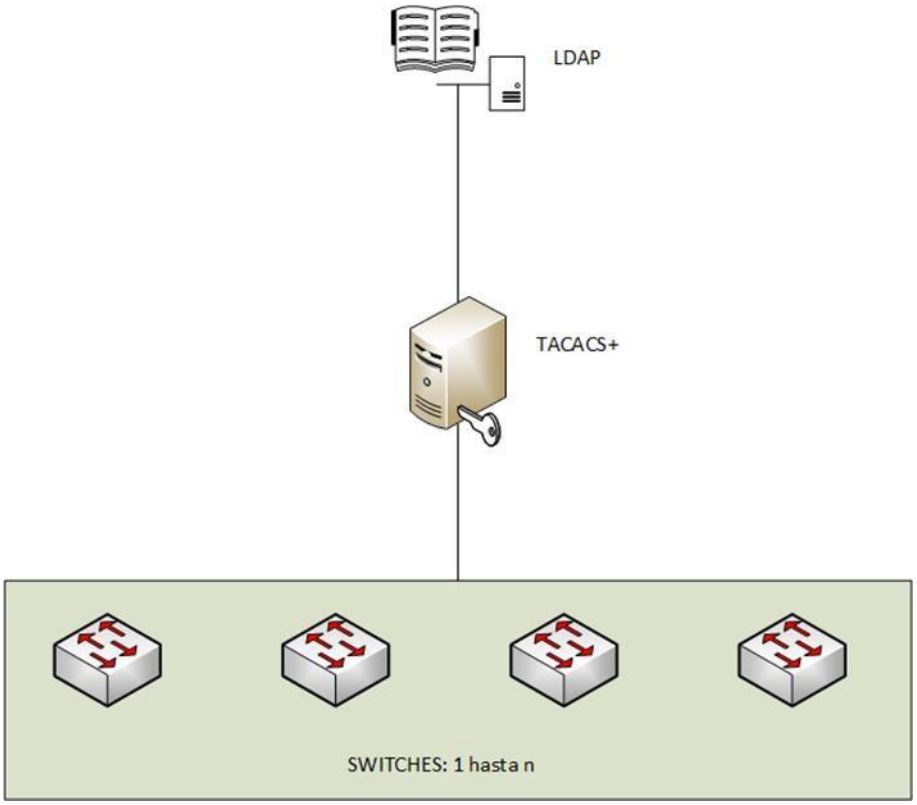

Figura 2.1 Arquitectura de la Solución

2.2. Requerimientos

Para la implementación de la presente propuesta se requieren los siguientes recursos mínimos:

- Servidor físico/virtual:
  - 2 cores de CPU.
  - 4 Gb de RAM.
  - 21 Gb de Disco duro.
- Servidor de Directorio (LDAP o AD), donde se deben crear los grupos necesarios para poder separar usuarios que tendrán diferentes niveles de acceso. En el caso de la empresa en la que se implementó esta solución se dispone de un servidor con OpenLDAP instalado y configurado con eldominio de la empresa. Dado que no se obtuvieron los permisos formales

para mostrar lo realizado en esa empresa decidí implementar la solución en un ambiente virtual definiendo como dominio **met5.espol.edu.ec** y el usuario **admin** como usuario administrador de ese dominio.

2.3. Instalación de componentes

En nuestro caso se usó el proyecto tacacsgui [4], el cual posee un entorno gráfico para la configuración del servicio de tacacs+. En el sitio del proyecto se ofrece un instalador en formato ISO y una OVA para desplegar en un ambiente virtual, siendo esta última la opción seleccionada para la instalación.

A continuación, se listarán los pasos necesarios para realizar el despliegue del OVA en VMware Workstation. En caso de tener otro software de virtualización remitirse a los manuales del fabricante [5].

- Descargar el OVA del URL: **https://tacacsgui.com/download/** y descomprimir el archivo descargado.
- En la consola de **VMware Workstation** seleccionar del menú **File** la opción **Open**, como se observa en la Figura 2.2:

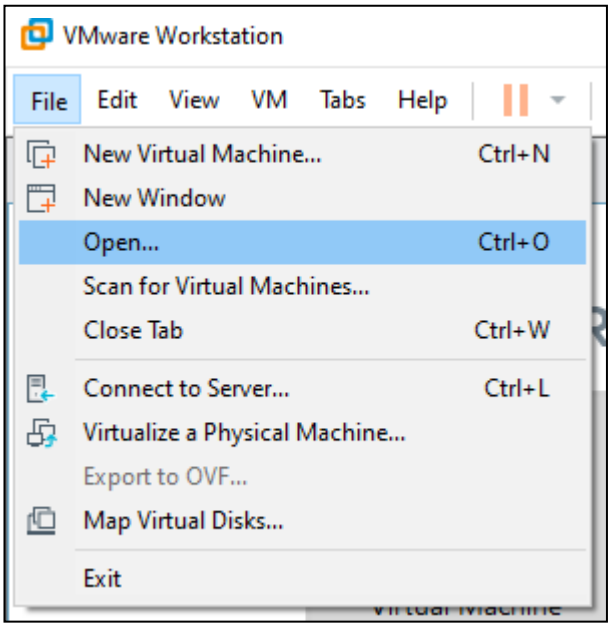

Figura 2.2 Desplegar OVA en VMware Workstation

- Ingresar a la carpeta que se creó al descomprimir la OVA descargada, seleccionar el archivo **tacgui.ovf** y dar click en el botón **Abrir**. Esto se ilustra en la Figura 2.3:

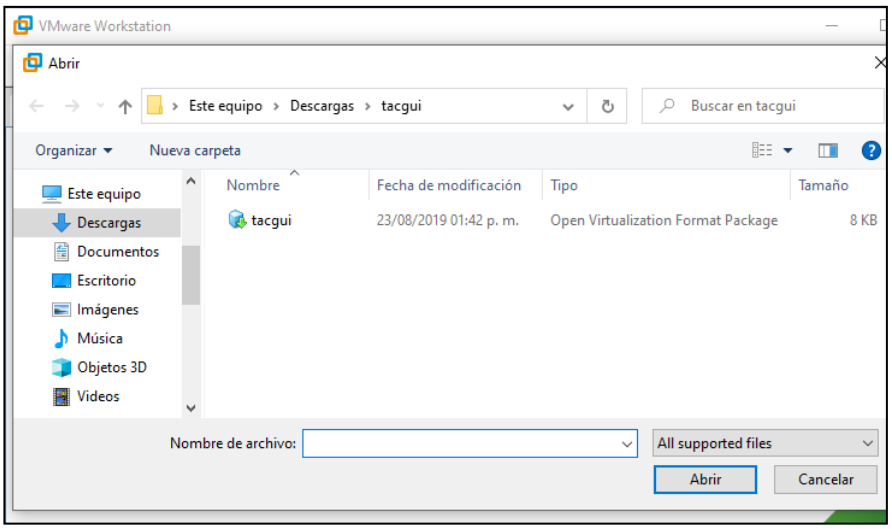

Figura 2.3 Seleccionar OVA

- Seleccionar la carpeta donde se almacenará la nueva VM. Se puede observar en la Figura 2.4 un ejemplo. Dar click en el botón **Import**:

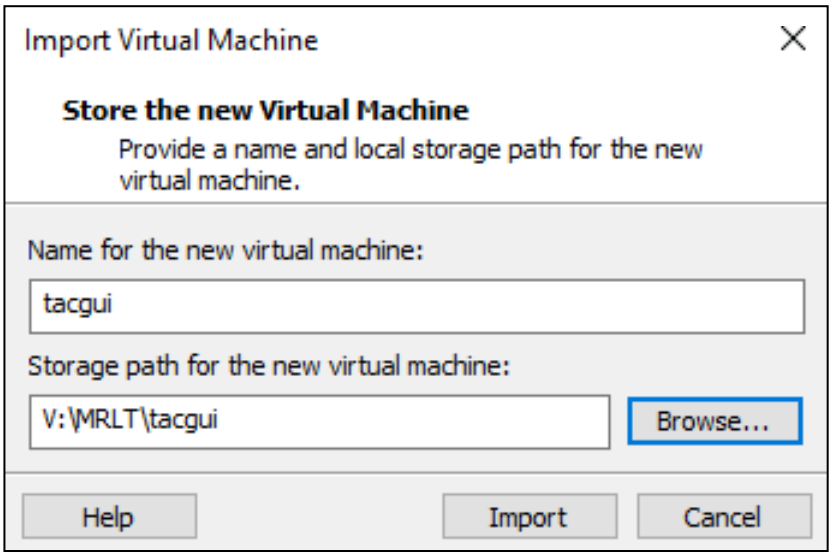

Figura 2.4 Seleccionar carpeta para importar nueva VM

- Esperar que la importación termine. Se puede observar en la Figura 2.5 el avance de la importación:

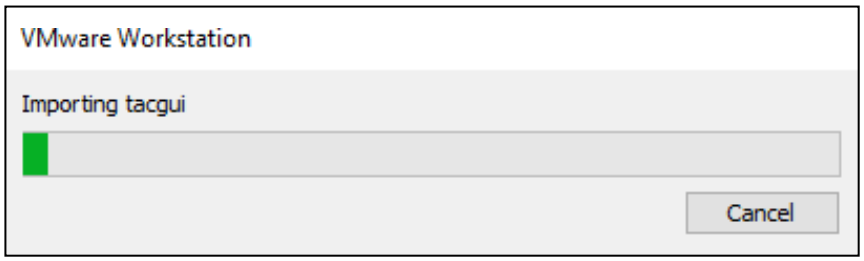

Figura 2.5 Proceso de importación de OVA de tacgui

- Al finalizar una nueva pestaña se muestra en **VMware Wokstation**. En la Figura 2.6 se puede observar ciertas características de la nueva VM:

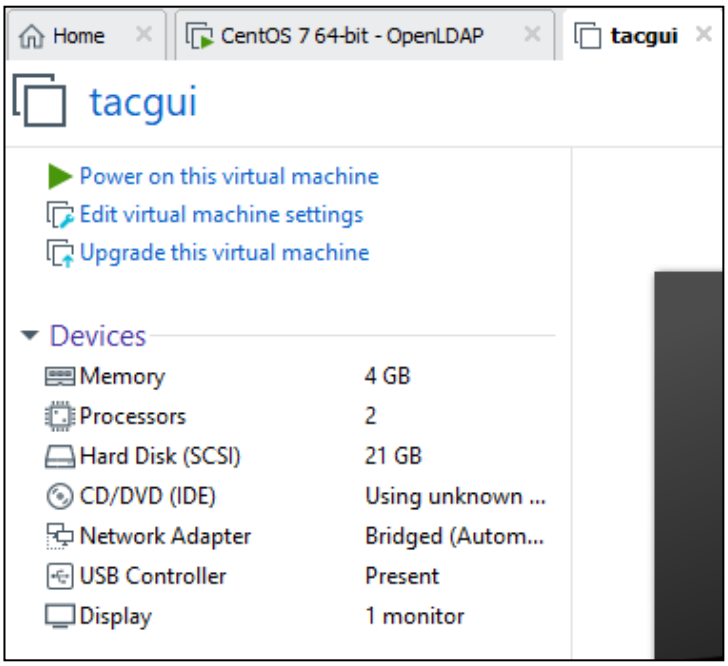

Figura 2.6 VM tacgui terminada de importar

- Configurar la red. Para seleccionar la red a la que se va a conectar la nueva VM dar doble click sobre **Network Adapter** y en la ventana que se muestre seleccionar **VMnet8 (NAT)**, como se muestra en la.Figura 2.7:

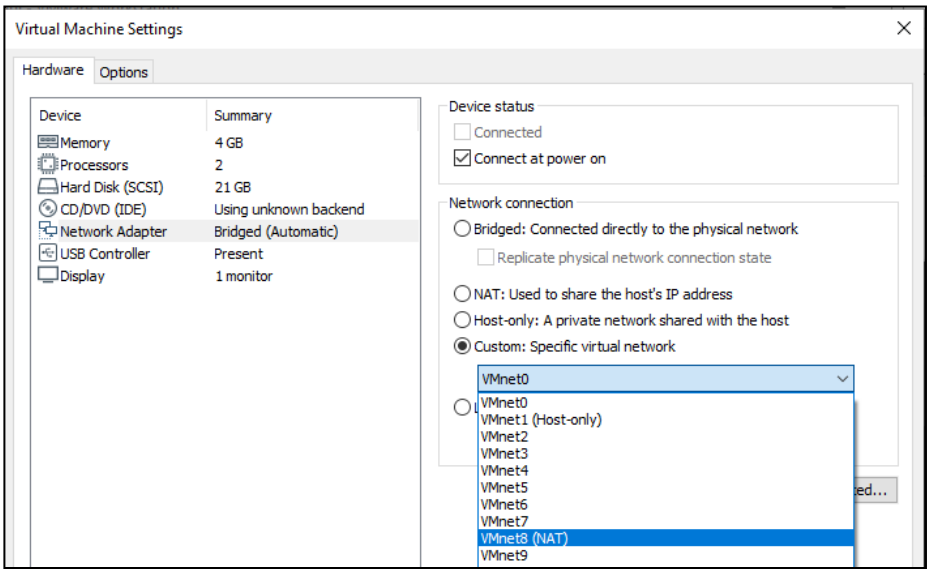

Figura 2.7 Selección de Red de nueva VM tacgui

- Dar click en **OK**.
- Encender la VM dando click sobre la opción **Power on this virtual machine**, como se muestra en la Figura 2.8:

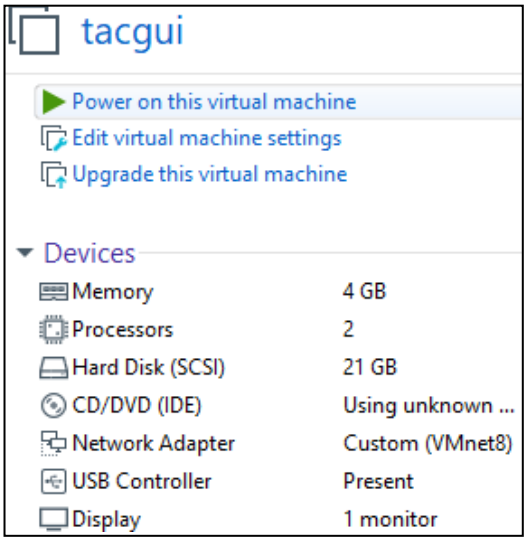

Figura 2.8 Encender VM tacgui

- Cuando termine de arrancar la VM iniciar sesión usando las credenciales **tacgui**/**tacgui** para usuario/clave. Se mostrará una pantalla similar a la imagen mostrada en la en la Figura 2.9.

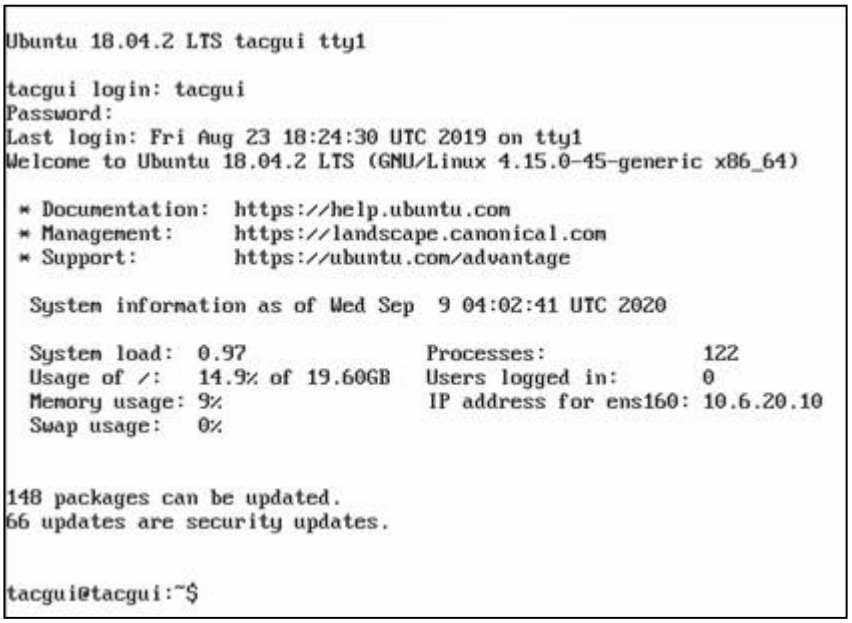

Figura 2.9 Consola de tacacsgui

- Ejecutar el siguiente comando: **sudo ~/tgui_install/tacacsgui.sh**. En las imágenes de Figura 2.10 y Figura 2.11 se muestra el cambio de IP del servidor que se usará en la simulación:

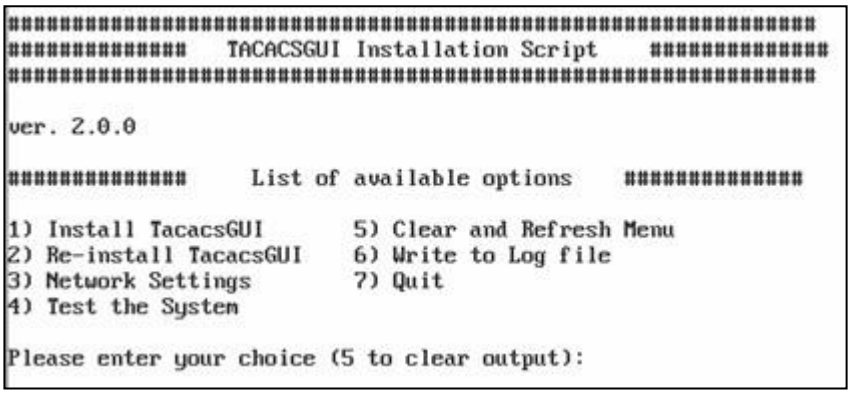

Figura 2.10 Configuración de IP de servidor tacacsgui (1)

Figura 2.11 Configuración de IP de servidor tacacsgui (2)

- A continuación, abrir en un browser de internet cualquiera de las siguientes URLs, recordando que la IP configurada en el paso anterior fue la 192.168.112.73:

  https://192.168.112.73:4443 (para una conexión segura)

  http://192.168.112.73:8008

- Usar las credenciales por defecto: **tacgui**/**tacgui** para usuario/clave.

- En el primer inicio de sesión se pedirá modificar la clave, hacerlo. Pedirá que se vuelva a iniciar sesión, esta vez usar la nueva clave. A continuación,se mostrará una pantalla de actualización y se configurará la base de datos usada por tacacsgui. Al finalizar se mostrará una pantalla similar a la de la Figura 2.12:

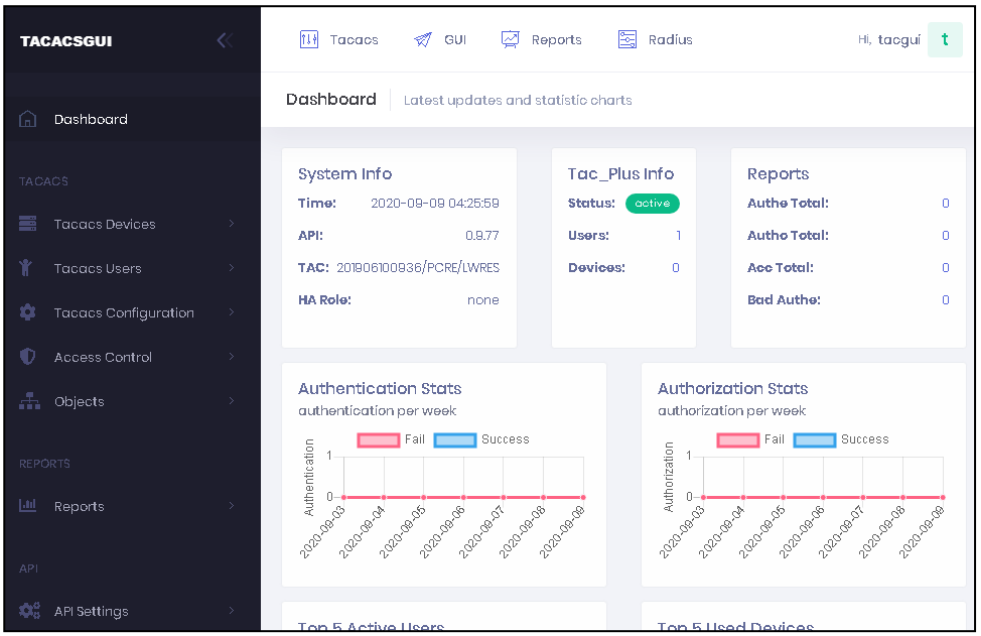

Figura 2.12 Pantalla inicial de tacacsgui después de iniciar sesión

Con el ingreso a la consola se finaliza la instalación de tacacsgui. En la siguiente sección se revisará la configuración del servicio de tacacsgui.

2.4. Configuraciones Generales

Configuración del LDAP

Previo a la configuración de tacacsgui se debe confirmar que los usuarios y grupos requeridos existan en el LDAP corporativo. Recordando el árbol mostrado en la Figura 1.1 deberán existir los siguientes elementos:

- 1 Unidad Organizativa (OU) llamada **complexiva**.
- 2 OU dentro de **complexiva**: **grupos** y **usuarios**.

- 2 grupos en la OU grupos: infraestructura y monitoreo. Estos grupos son de clase **posixGroup**.
- 2 OU dentro de **usuarios**: **infraestructura** y **monitoreo**.
- 3 usuarios en la OU **infraestructura**: infra001, infra002 y user1. Los usuarios deben incluir la clase **posixAccount**.
- 3 usuarios en la OU **monitoreo**: mon001, mon002 y user2. Los usuarios deben incluir la clase **posixAccount**.

Observar las imágenes de Figura 2.13, Figura 2.14 y Figura 2.15 que muestran los elementos creados anteriormente:

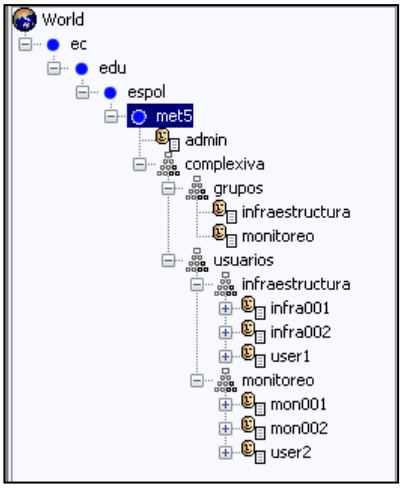

Figura 2.13 LDAP - Vista general del árbol del dominio met5.espol.edu.ec

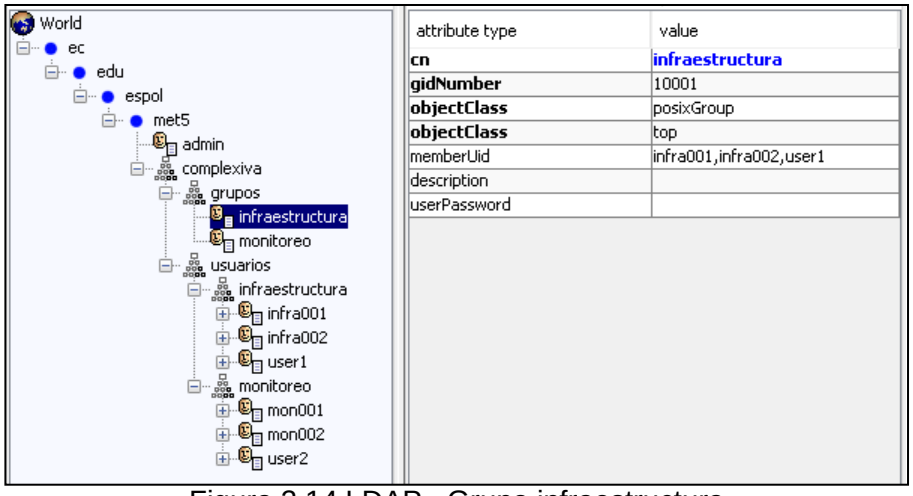

Figura 2.14 LDAP - Grupo infraestructura

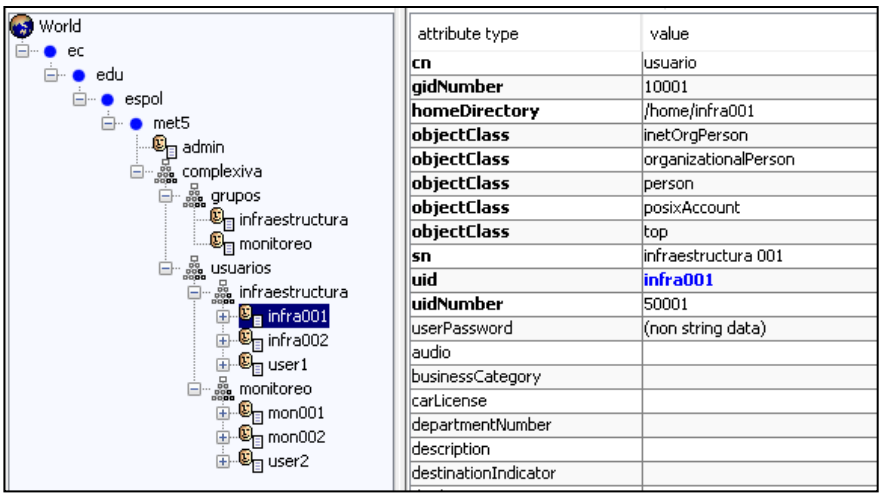

Figura 2.15 LDAP - Usuario infra001

Configuración de tacacsgui

Para la implementación propuesta se realizarán las siguientes acciones en la interfaz de administración de tacacsgui [6] y [7]: 1) agregar direcciones, 2) agregar dispositivos, 3) configurar el acceso al servidor LDAP, 4) agregar servicios, 5) agregar grupos de usuarios, asociarlos a grupos de LDAP y asignarles servicios, y 6) validar configuración y aplicarla.

En este punto se recomienda tomar en cuenta la imagen de la Figura 2.16 en la que se ha extraído el menú vertical que está a la izquierda de la consola de tacacsgui (se han invertido los colores para una mejor visualización). Notar los títulos TACACS, REPORTS, API y PLUGINS, ya que se hará referencia a algunos de ellos más adelante:

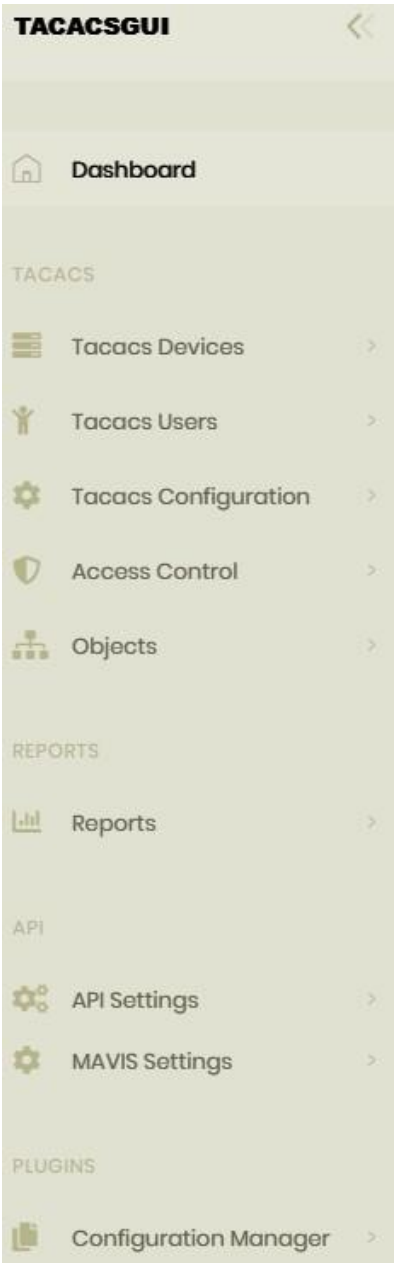

Figura 2.16 tacacsgui - Menú principal

1. Agregar direcciones

- En el menú bajo el título **TACACS** seleccionar **Objects** – **Addresses**. Observar las imágenes de Figura 2.17 y Figura 2.18.

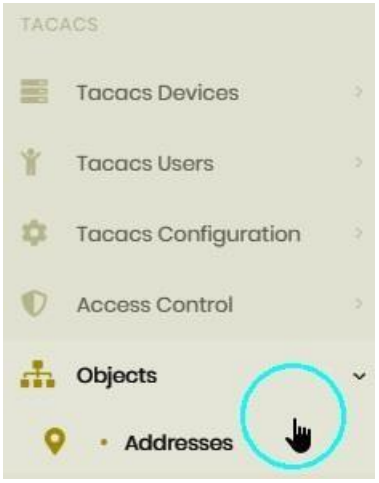

Figura 2.17 tacacsgui - Agregar direcciones (1)

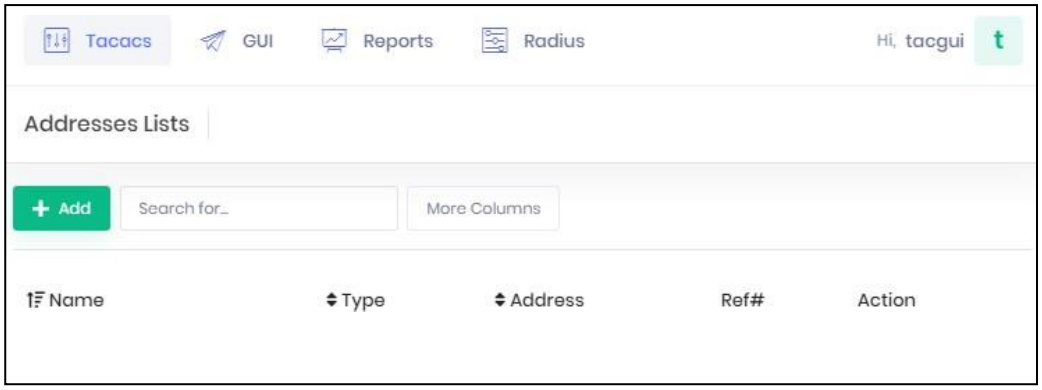

Figura 2.18 tacacsgui - Agregar direcciones (2)

- En la pantalla de la Figura 2.18 dar click en el botón **Add**. Se mostrará la pantalla de la Figura 2.19.

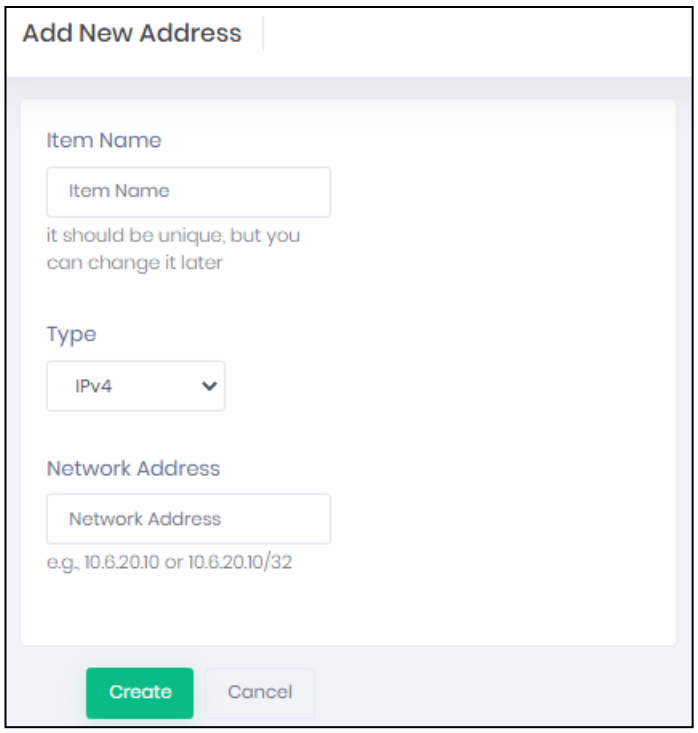

Figura 2.19 tacacsgui - Agregar direcciones (3)

- Llenar el formulario con la siguiente información:

  ItemName: CISCOSWITCH001

  Type: IPv4

  NetworkAddress: 192.168.112.81

- Dar click en el botón **Create**. Se mostrará una pantalla similar a la de la Figura 2.20

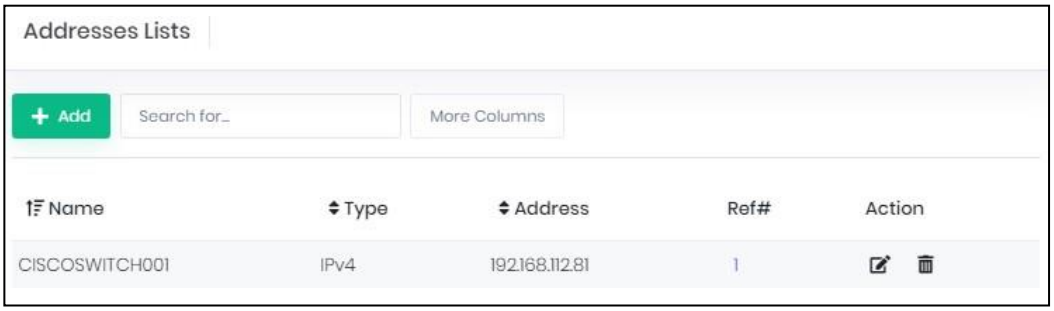

Figura 2.20 tacacsgui - Agregar direcciones (4)

2. Agregar dispositivos

- En el menú bajo el título **TACACS** seleccionar **Tacacs Devices** – **Devices**. Observar las imágenes de Figura 2.21 y Figura 2.22.

Figura 2.21 tacacsgui - Agregar dispositivos (1)

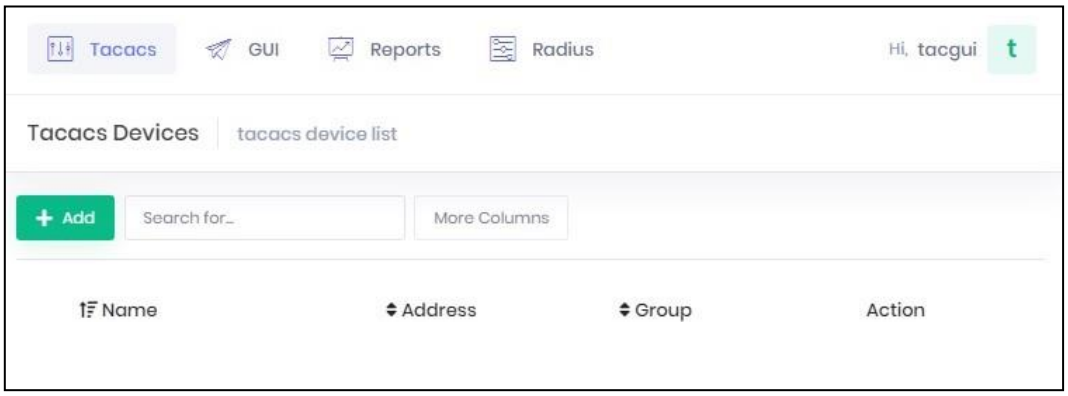

Figura 2.22 tacacsgui - Agregar dispositivos (2)

- En la pantalla de la Figura 2.22 dar click en el botón **Add**. Se mostrará la pantalla de la Figura 2.23.

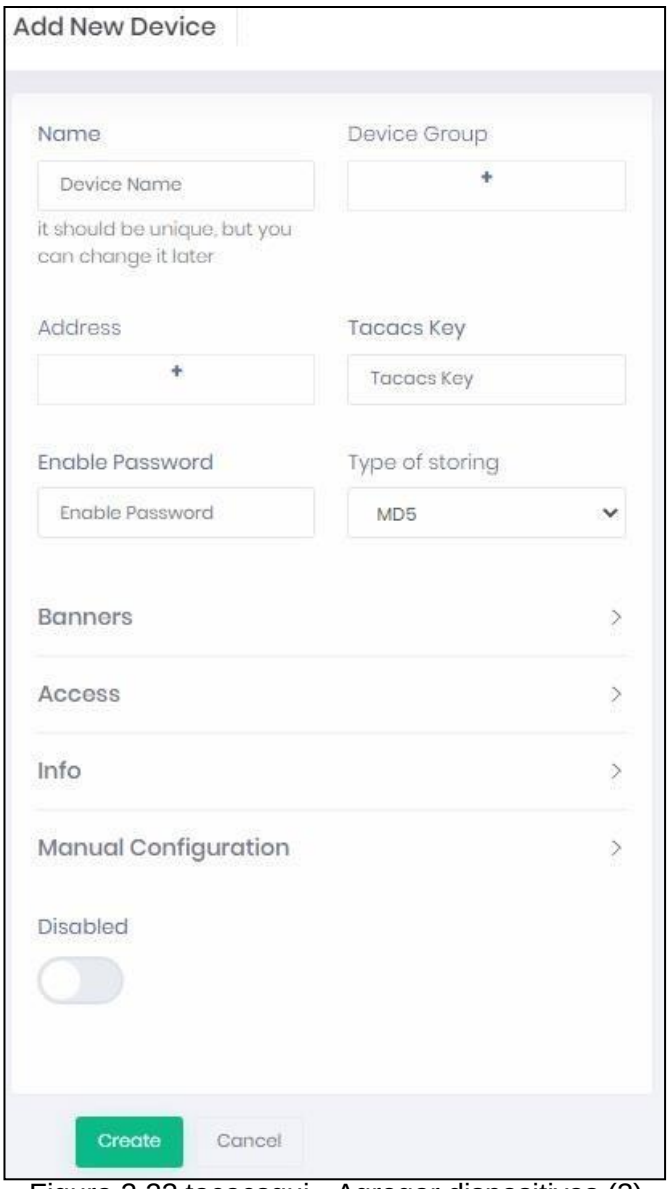

Figura 2.23 tacacsgui - Agregar dispositivos (3)

- Llenar el formulario con la siguiente información:

  Name: CISCOSWITCH001

  DeviceGroup: defaultGroup

  Address: CISCOSWITCH001

  TacacsKey: miclavetacacs

Banners – Welcome: SISTEMA PROTEGIDO!!! Usted se ha conectado a un sistema supervisado. Si no está autorizado por favor salga de este dispositivo. Sus acciones serán registradas. Ingrese sus credenciales

3. Configurar el acceso al servidor LDAP

- En el menú bajo el título **API** seleccionar **MAVIS Settings** – **MAVIS LDAP**. Observar las imágenes de Figura 2.24 y Figura 2.25

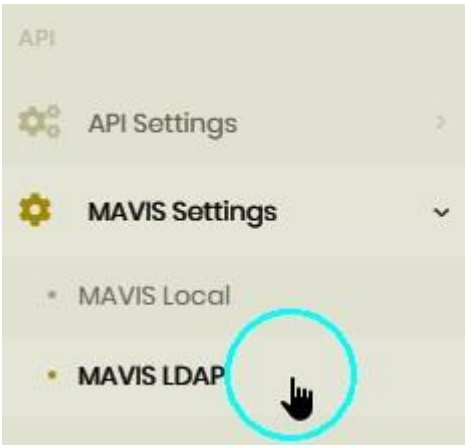

Figura 2.24 tacacsgui - Configuración de MAVIS LDAP (1)

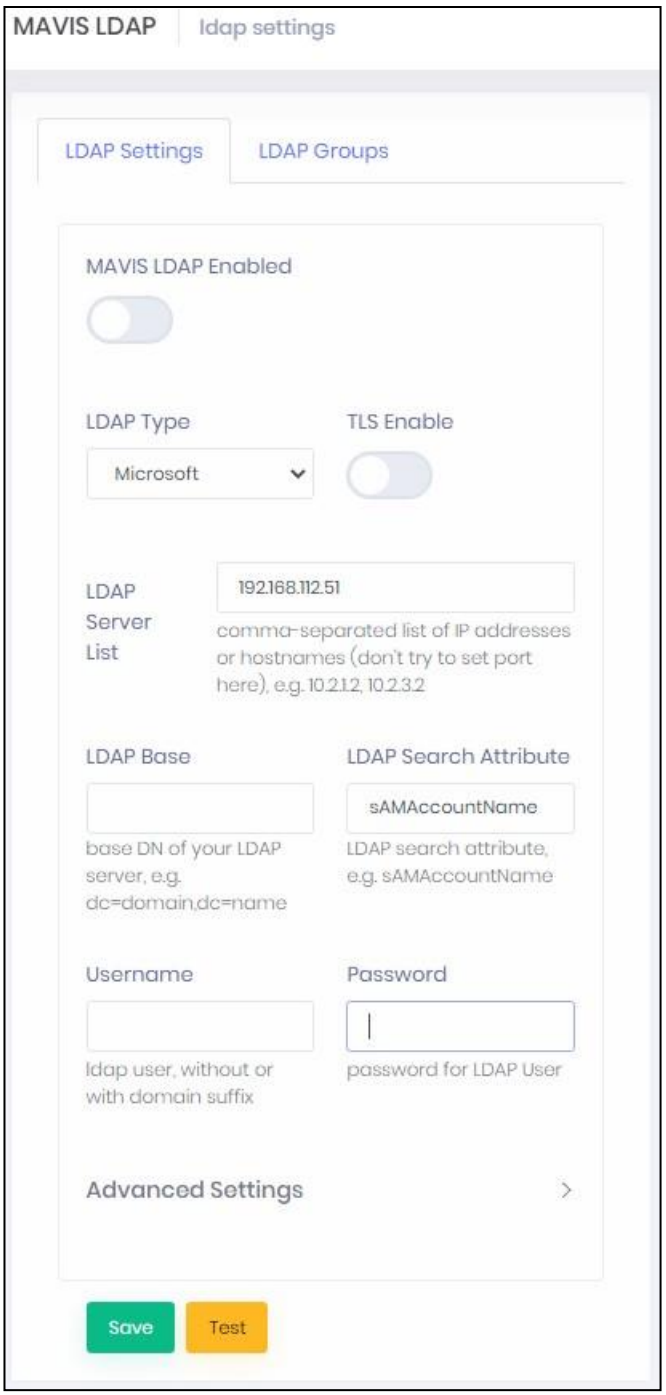

Figura 2.25 tacacsgui - Configuración de MAVIS LDAP (2)

- En la pantalla de la imagen Figura 2.25 habilitar **MAVIS LDAP Enabled** y llenar el formulario con la información siguiente:

LDAP Type: OpenLDAP

LDAP Server List: 192.168.112.51

LDAP Base: dc=met5,dc=espol,dc=edu,dc=ec

LDAP Search Attribute: uid

Username: cn=admin,dc=met5,dc=espol,dc=edu,dc=ec

Password: met5

- Dar click en el botón **Save** para grabar. A continuación, dar click en el título de la pestaña **LDAP Groups**. La pantalla debe ser similar a la de la Figura 2.26.

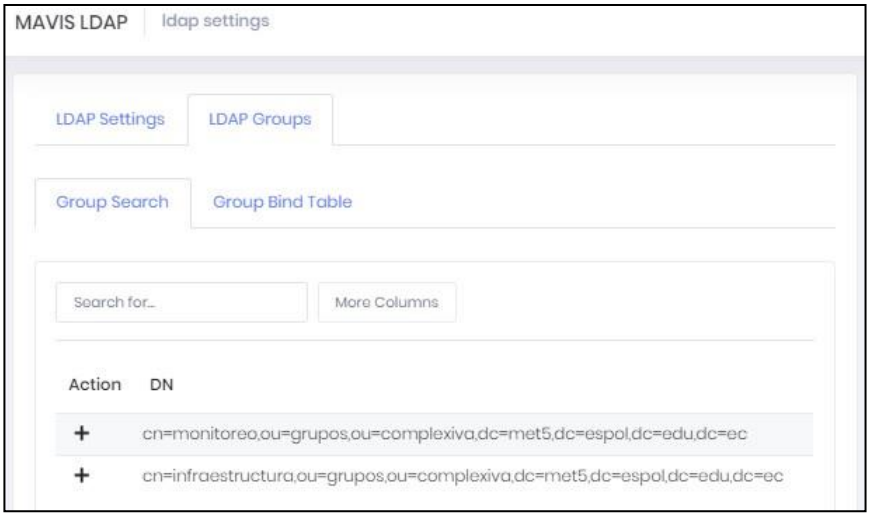

Figura 2.26 tacacsgui - Configuración de MAVIS LDAP (3)

- Para finalizar dar click en los signos “+” de cada uno de los grupos mostrados.

4. Agregar servicios

- En el menú bajo el título **TACACS** seleccionar **Access Control** – **Services**. Observar las imágenes de Figura 2.27 y Figura 2.28.

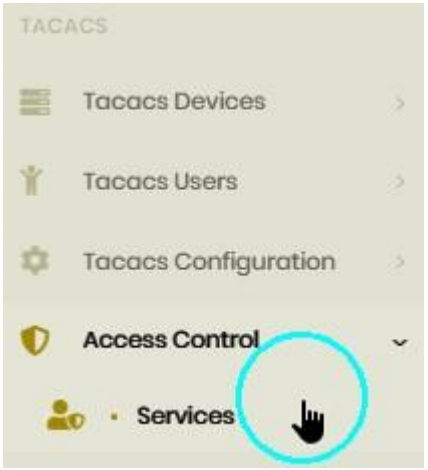

Figura 2.27 tacacsgui - Agregar servicios (1)

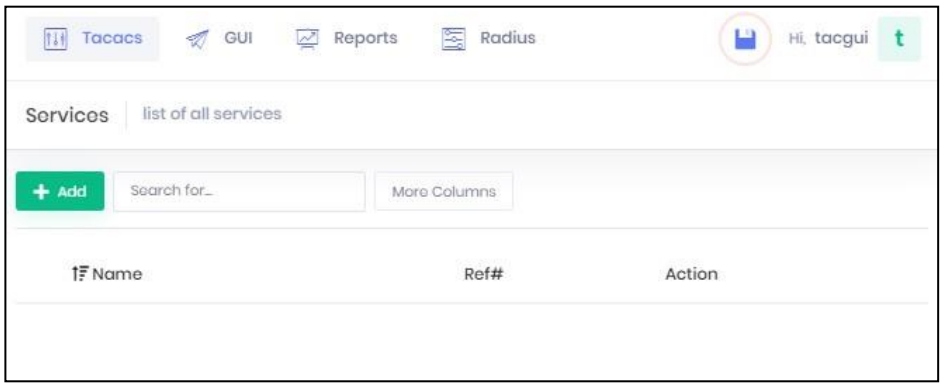

Figura 2.28 tacacsgui - Agregar servicios (2)

- En la pantalla de la Figura 2.28 dar click en el botón **Add**. Se mostrará una pantalla similar a la de la Figura 2.29:

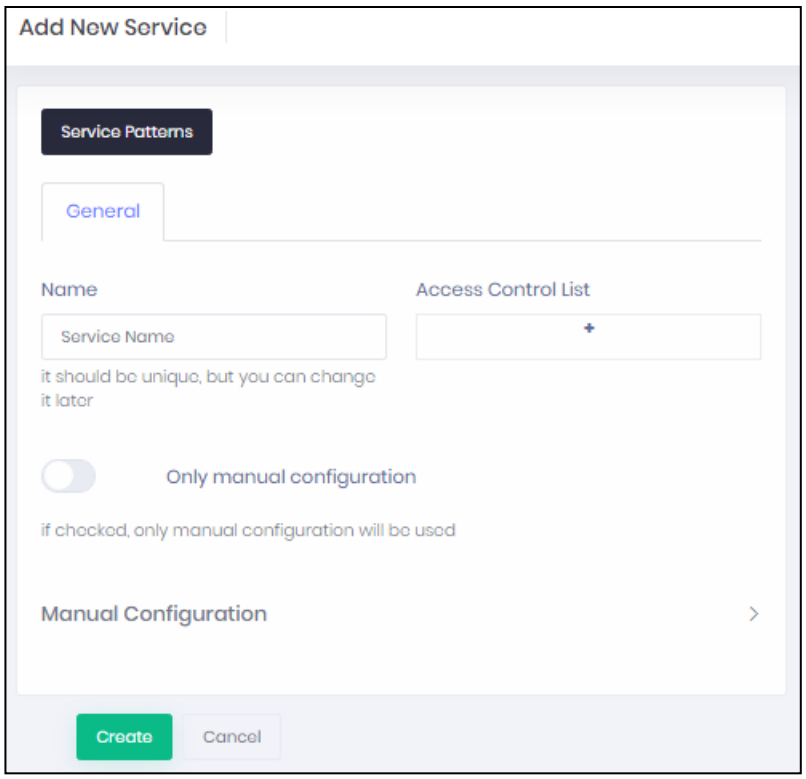

Figura 2.29 tacacsgui - Agregar servicios (3)

Tomar en cuenta el botón **Service Patterns**, que se encuentra arriba de la pestaña **General**, ya que permite seleccionar el fabricante y de acuerdo con él se define el servicio que vamos a agregar. En la imagen de la Figura 2.30 se observa un listado de fabricantes.

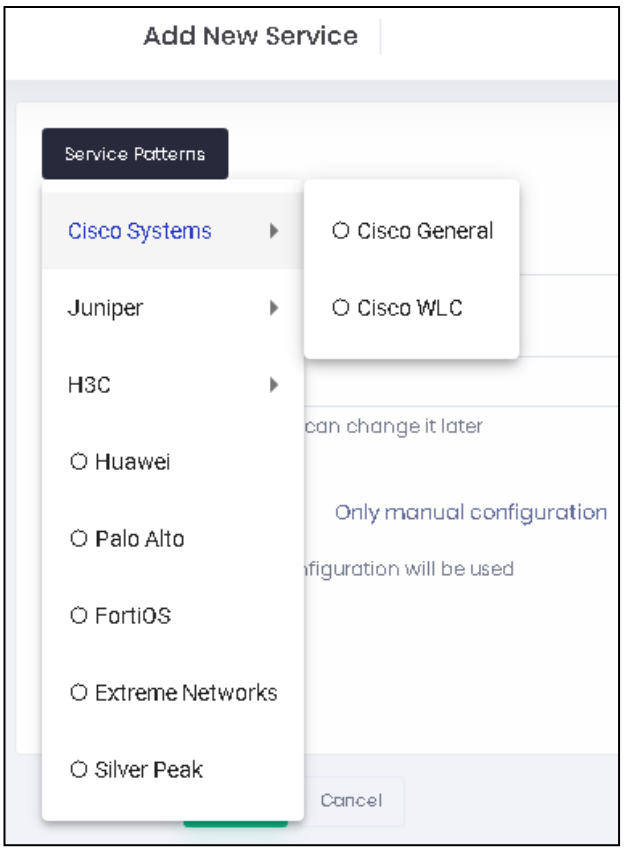

Figura 2.30 tacacsgui - Agregar servicios (4)

En el listado mostrado en la Figura 2.30 seleccionar **Cisco General** y nos mostrará una nueva pestaña en la cual seleccionaremos el nivel de privilegios para el servicio que estamos creando, las otras opciones no serán implementadas en esta propuesta. La pantalla debe ser similar a lamostrada en la Figura 2.31:

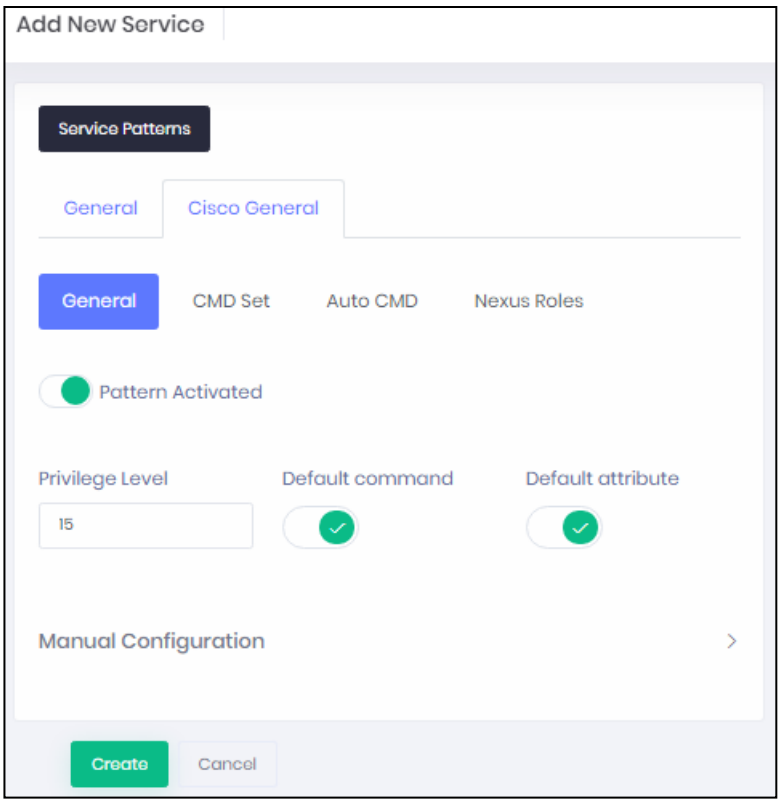

Figura 2.31 tacacsgui - Agregar servicios (5)

Se crearán dos servicios: **infraestructura** con privilegio 15 y **monitoreo** con privilegio 7, quedando el listado de servicios como la imagen de la Figura 2.32:

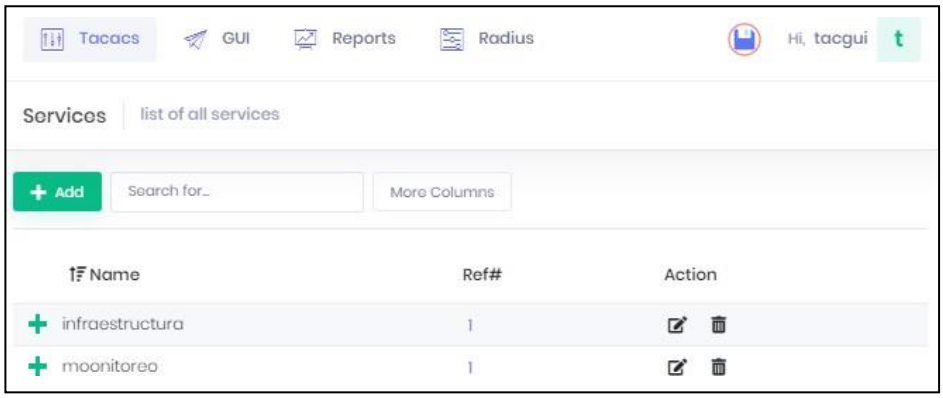

Figura 2.32 tacacsgui - Agregar servicios (6)

5. Agregar grupos de usuarios, asociarlos a grupos de LDAP y asignarles servicios

- En el menú bajo el título **TACACS** seleccionar **Tacacs Users** – **User Groups**. Observar las imágenes de Figura 2.33 y Figura 2.34.

Figura 2.33 tacacsgui - Agregar grupos de usuarios (1)

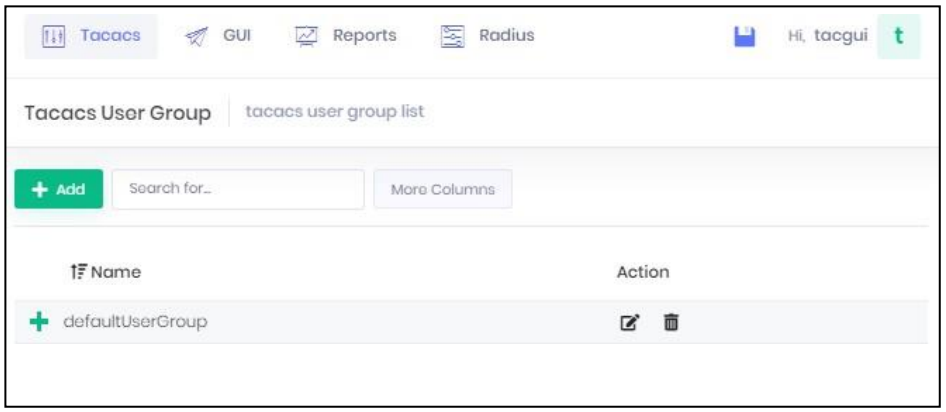

Figura 2.34 tacacsgui - Agregar grupos de usuarios (2)

- En la pantalla de la Figura 2.34 y dar click en el botón **Add**. Se mostrará una pantalla similar a la de la Figura 2.35.

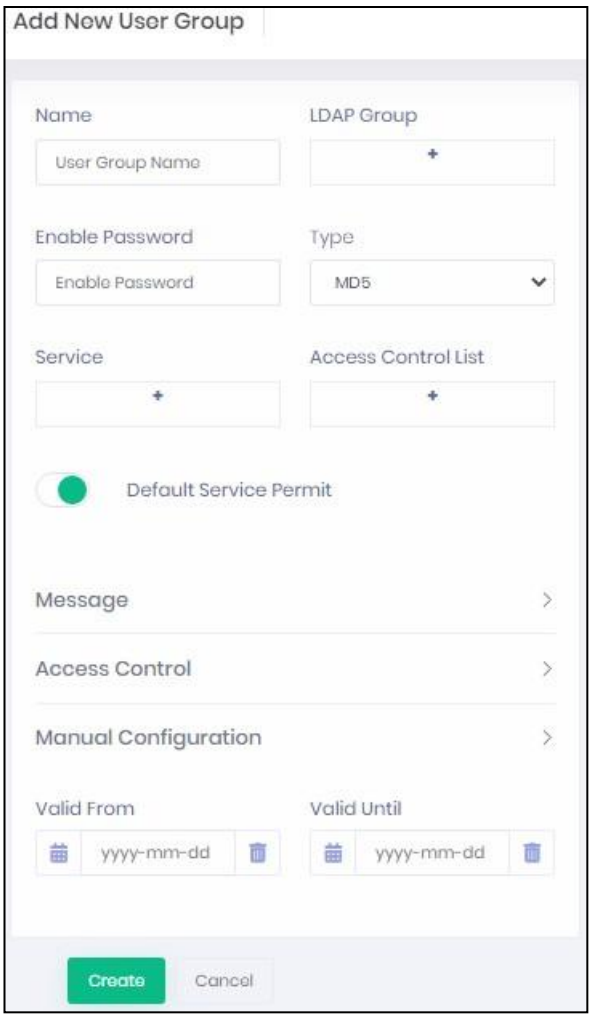

Figura 2.35 tacacsgui - Agregar grupos de usuarios (3)

- Se llenará el formulario con la siguiente información para el grupo de usuarios de **infraestructura**:

  Name: infraestructura

  LDAP Group: cn=infraestructura

  Service: infraestructura

- A continuación, crear un nuevo Grupo de Usuarios que será usado por monitoreo. Para ello escribir **monitoreo** en todo lugar donde aparezca

infraestructura. Al finalizar en la opción de **User Groups** se debe mostrar una imagen similar a la de la Figura 2.36:

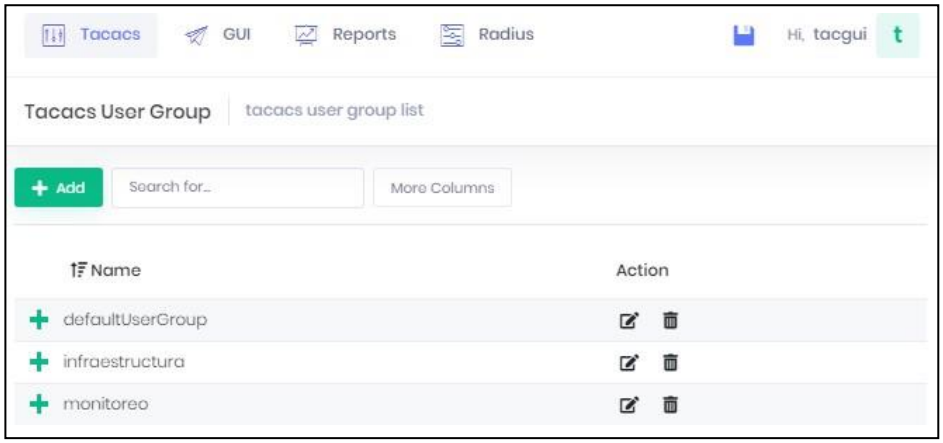

Figura 2.36 tacacsgui - Agregar grupos de usuarios (4)

6. Validar configuración y aplicarla

Después de realizar los pasos anteriores se podrá notar que aparece una imagen de un diskette en la parte superior derecha, cerca del nombre del usuario, similar al que se observa en la Figura 2.37:

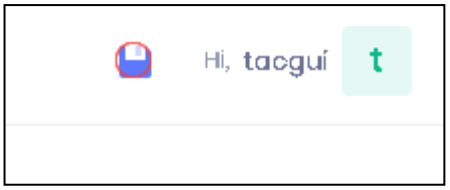

Figura 2.37 tacacsgui - Alerta de cambios en la configuración

Esa imagen alerta que hay una configuración pendiente que no ha sido aplicada a la ejecución del servicio de tacacs+ y debe ser revisada y/o aplicada. Para hacerlo dar click a la imagen del diskette o ir al menú, bajo el título **TACACS** en la opción **Tacacs Configuration** – **Test & Apply**. Se mostrará una pantalla similar a la de la Figura 2.38:

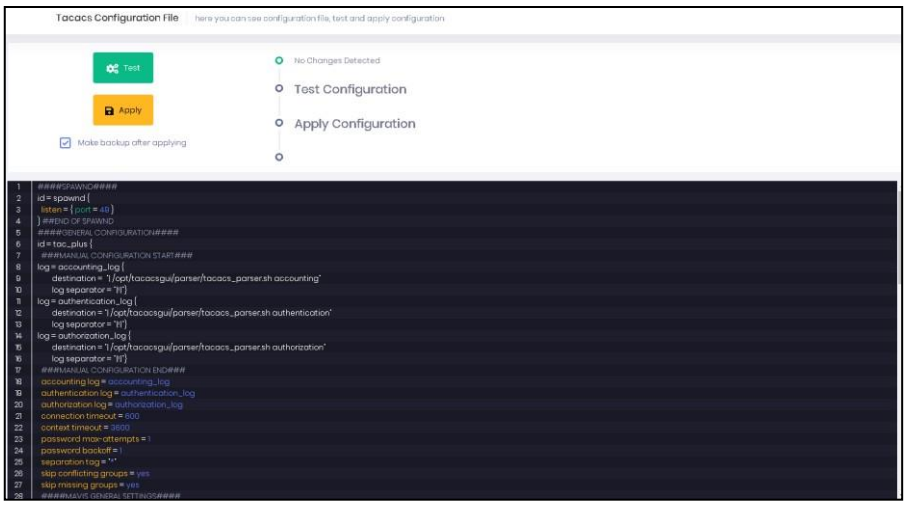

Figura 2.38 tacacsgui - Vista de la configuración

Se puede revisar el archivo de configuración mostrado en la parte inferior en donde se podrá reconocer la mayoría de las opciones que fueron configuradas en el entorno gráfico. En la pantalla de la imagen anterior dar click en el botón **Test** y si la configuración no tiene errores mostrará el mensaje **Success**, caso contrario dirá que existe un error y la ubicación del mismo. Si no existen errores dar click al botón **Apply**, el cual reiniciará el servicio para que se apliquen los cambios realizados en la configuración. La pantalla se verá similar a la Figura 2.39:

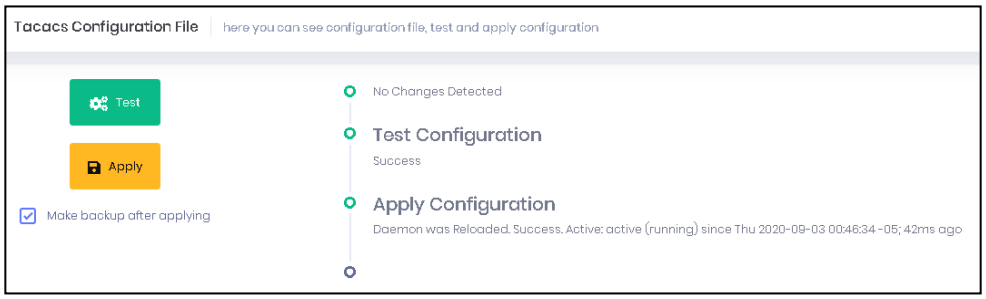

Figura 2.39 tacacsgui - Prueba y Aplicación de nueva configuración

Configuración de los switches

En la empresa usan dispositivos marca CISCO, en caso de tener equipos de otros fabricantes se deberá buscar en la documentación oficial para conocer si

el dispositivo soporta el uso de un servidor tacacs+ y como se realiza dicha configuración. Para la simulación usando **GNS3** configurar un router **C3745** con IOS **c3745-advipservicesk9-mz.124-25d** al cual se le puede agregar un módulo de 16 puertos para que funcione como switch.

El switch C3745 tendrá la configuración por defecto y se le agregarán las líneas requeridas para lograr la autenticación usando el servidor tacacsgui configurado previamente. La configuración de fábrica es la mostrada en la Figura 2.40:

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ip tcp synwait-time 5
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
interface FastEthernet1/1
interface FastEthernet1/2
interface FastEthernet1/3
interface FastEthernet1/4
interface FastEthernet1/5
interface FastEthernet1/6
interface FastEthernet1/7
interface FastEthernet1/8
interface FastEthernet1/9
interface FastEthernet1/10
interface FastEthernet1/11
interface FastEthernet1/12
interface FastEthernet1/13
interface FastEthernet1/14
interface FastEthernet1/15
interface Vlan1
 no ip address
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
```

Figura 2.40 c3745 - Configuración inicial

Los cambios que se realizarán en la configuración son los siguientes:

- **Crear un usuario local con privilegio 15**: será usado para conexiones por consola. Para ello agregar la línea mostrada en la Figura 2.41:

```
username met5 privilege 15 secret 5 $1$iAc9$ca0uaaLeLoUh3LeI1zvT9.
```

Figura 2.41 c3745 - Creación de usuario local

- **Asignar una dirección IP**: para permitir el acceso remoto a este equipo, además que habilitará la comunicación hacia el servidor tacacsgui. En la simulación se usará la interfaz **FastEthernet0/0** para asignarle la IP. La configuración de la interfaz quedará como la imagen mostrada en la Figura 2.42:

```
interface FastEthernet0/0
 ip address 192.168.112.81 255.255.255.0
```

Figura 2.42 c3745 - Configuración de IP para acceso remoto

Habilitar acceso remoto con ssh: este paso podría ser opcional, sin embargo, se recomienda habilitar el acceso remoto al switch usando ssh para incrementar la seguridad. Para ello configurar el nombre de dominio del dispositivo agregando en modo configuración la línea: **ip domain name met5.espol.edu.ec**. A continuación, se deben generar las llaves de encriptación y para ello ejecutar en modo configuración la siguiente línea: **crypto key generate rsa**. En la imagen de la Figura 2.43 se muestra la ejecución de los comandos mencionados. Notar que se ha indicado que se usará un módulo de 2048 bits y no el valor por defecto de 512:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain name met5.espol.edu.ec
R1(config)#
R1(config)#crypto key generate rsa
The name for the keys will be: R1.met5.espol.edu.ec
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Mar  1 00:05:54.979: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)#end
R1#
```

Figura 2.43 c3745 - Generación de llaves de encriptación

Finalmente habilitar ssh para las conexiones remotas. Agregar las líneas mostradas en la Figura 2.44:

```
line vty 0 4
 transport input telnet ssh
```

Figura 2.44 c3745 - Agregar SSH para el acceso remoto

- **Configuración de cliente tacacs+**: después de los pasos anteriores al fin se tiene todo preparado para configurar el dispositivo para que use tacacs+. Agregar las líneas mostradas en la Figura 2.45:

```
aaa new-model
aaa group server tacacs+ TacGui
 server 192.168.112.73
aaa authentication login default local
aaa authentication login TacLogin group TacGui local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default local
aaa authorization exec TacAuth group TacGui local
aaa authorization commands 7 default local
aaa authorization commands 7 TacCommands7 group TacGui local
aaa authorization commands 15 default local
aaa authorization commands 15 TacCommands15 group TacGui local
aaa accounting exec default start-stop group TacGui
aaa accounting commands 7 default start-stop group TacGui
aaa accounting commands 15 default start-stop group TacGui
tacacs-server host 192.168.112.73 key miclavetacacs
line vty 0 4
 authorization commands 7 TacCommands7
 authorization commands 15 TacCommands15
 authorization exec TacAuth
 login authentication TacLogin
```

Figura 2.45 c3745 - Configuración de tacacs+

Ha llegado el momento de verificar que todo está funcionando de acuerdo con lo planificado. En la siguiente sección se validará lo realizado.

2.5. Validación

Para validar las configuraciones realizadas en los puntos anteriores de este capítulo debemos usar el cliente SSH de nuestra preferencia y abrir una conexión hacia la IP de nuestro dispositivo de red y probar el inicio de sesión con las credenciales de alguno(s) de los usuarios del LDAP corporativo. En las imágenes de Figura 2.46 y Figura 2.47 se muestran ejemplos de las pruebas realizadas.

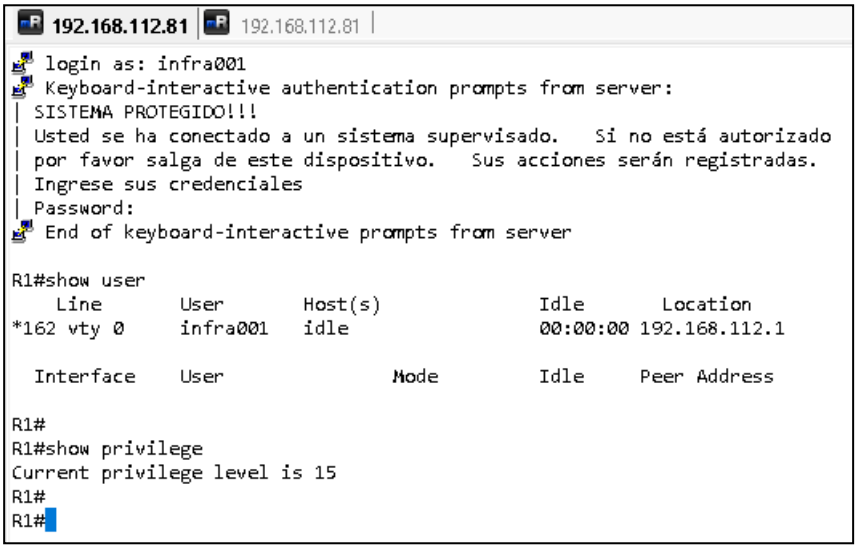

Figura 2.46 Acceso del usuario infra001

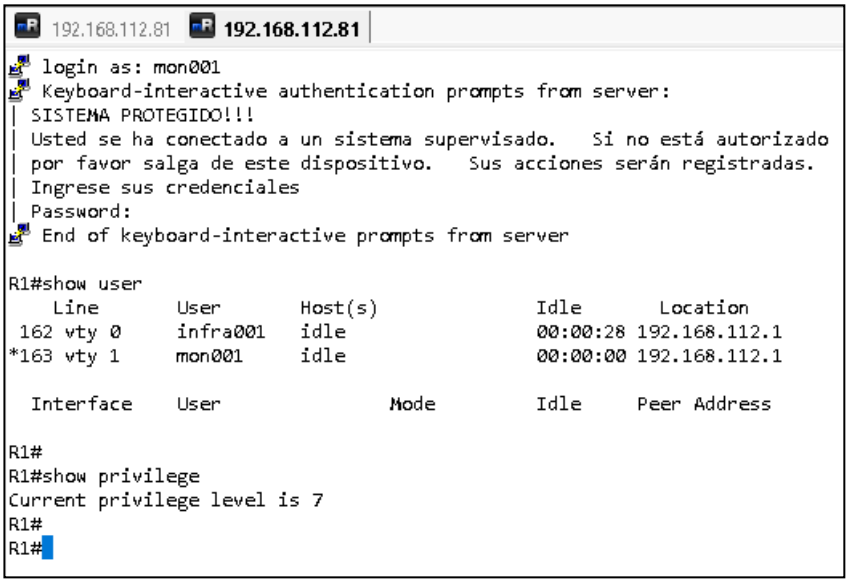

Figura 2.47 Acceso del usuario mon001

2.6. Problemas y Soluciones Comunes

Problema: tacacsgui no tiene conexión al LDAP

Solución: Verificar que el firewall local del servidor LDAP permite el tráfico desde el servidor tacacsgui al servidor LDAP por los puertos 389 y/o 636.

Problema: Dispositivo de red no tiene conexión hacia el servidor tacacsgui

Solución: Verificar que el firewall local del servidor tacacsgui permite el tráfico por el puerto 49. También verificar que el servicio de tacacsgui no tenga una ACL que rechace el tráfico desde el dispositivo de red que tiene problemas de conexión.

Problema: Usuario de LDAP no logra iniciar sesión en dispositivo de red

Solución: Verificar que las credenciales usadas sean las correctas. También verificar que el usuario pertenezca a alguno de los grupos enlazados con los que están permitidos en tacacsgui. Verificar si el dispositivo de red tiene configurado el soporte de tacacs+ y está apuntando al servidor correcto.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Al finalizar el presente trabajo se puede concluir lo siguiente:

- Es importante que la Gerencia defina la Política de Seguridad de una empresa y que los mandos medios estén alineados con esa política a fin de que su gestión esté encaminada a cumplirla en cada una las actividades de la empresa.
- La seguridad de la información se debe aplicar de acuerdo con el entorno, no en todos los lugares una solución tiene los mismos resultados.
- Existen servicios que pueden ser agregados en una red y mejoran grandemente la seguridad de los dispositivos.
- Validar los usuarios contra un servicio como LDAP es preferible a validarlos contra usuarios locales definidos en cada dispositivo de red.

Recomendaciones

Aunque los beneficios obtenidos después del desarrollo de este proyecto se pueden palmar desde el primer momento, no está demás poner en consideración las siguientes recomendaciones:

- Definir los permisos para grupos de usuarios y no para usuarios individuales, a menos que sea estrictamente necesario.
- Realizar pruebas en ambientes de laboratorio aislados, si es posible usando virtualización. Se requieren pocos recursos si se instalan los elementos estrictamente necesarios.
- Revisar documentación de tacasgui para habilitar otras opciones como permitir comandos de privilegios superiores al nivel 7 y otorgarlos al grupo de monitoreo.
- Expandir el alcance de este proyecto hacia otras herramientas de gestión, tales como sistemas de monitoreo, LOGs y respaldos centralizados, entre otros similares.

BIBLIOGRAFIA

[1] A. López Neira, J. Ruiz Spohr, Anexo 9, [En línea]. Available: https://www.iso27000.es/iso27002_9.html. [Último acceso: septiembre 2020]

[2] OpenLDAP Foundation, 2020, agosto 11, OpenLDAP Software 2.4 Administrator's Guide. [En línea]. Available: https://www.openldap.org/doc/admin24/. [Último acceso: septiembre 2020]

[3] R. Bhardwaj, 2020, junio 4, TACACS VS TACACS+, [En línea]. Available: https://ipwithease.com/tacacs-vs-tacacs/. [Último acceso: septiembre 2020]

[4] TACACSGUI, 2020, TACACSGUI. [En línea]. Availabe: https://tacacsgui.com/. [Último acceso: septiembre 2020]

[5] TACACSGUI, 2020, Deploy OVA Template. [En línea]. Available: https://tacacsgui.com/documentation/installation/ova/deploy-ova-template/. [Último acceso: septiembre 2020]

[6] A. Mochalin, 2018, noviembre 1, Documentation. [En línea]. Available: https://old.tacgui.com/documentation/. [Último acceso: septiembre 2020]

[7] TACACSGUI, 2020, Documentation. [En línea]. Available: https://tacacsgui.com/documentation/. [Último acceso: septiembre 2020]