

Laboratorio Remoto para Dispositivos IIoT

Manual Administrador



2024

Índice

1.	Introducción	2
2.	Anexo de usuario	2
2.1.	Creación de usuario	2
2.2.	Creación de grupos.....	3
2.3.	Validación de usuario en Apache VCL y Apache Guacamole	4
2.4.	Creación de home de usuario	7
2.5.	Permiso de uso de puerto en RaspberryPI	9
3.	Acceso a la red interna del laboratorio	10
4.	Administración Apache VCL web	13
5.	Administración Apache Guacamole.....	20

1. Introducción

El LRDIIoT (Laboratorio Remoto para Dispositivos IIoT) es una plataforma que permite el acceso remoto a entornos de desarrollo para utilizar placas IIoT, concretamente las openmote-cc2538. Vale aclarar que estas placas pueden ser programadas y comunicarse entre ellas, lo que permite realizar diversos experimentos desde el punto de vista de tráfico, protocolos, arquitectura y comunicación.

Para el acceso al sistema se debe crear un usuario en el controlador de dominio Zentyal y una serie adicional de configuraciones para permitir que el mismo pueda ejecutar la carga de firmware en las placas openmote-cc2538 y la conexión a la placa raspberryPI.

En este documento se desarrollará todos los pasos que debe seguir el administrador para lograr una correcta integración del nuevo usuario.

2. Anexo de usuario

2.1. Creación de usuario

Para la creación de usuarios y grupos se recomienda acceder a través de la interfaz web del controlador de dominio Zentyal a través de su respectiva IP y puerto asociado, utilizando las credenciales de administrador.

Para agregar usuarios al dominio se puede realizar a través del entorno web, para ello se debe acceder a la opción "Users and Computers" y posteriormente "Manage". Al seleccionar la carpeta Users se habilita un símbolo + para agregar usuarios.

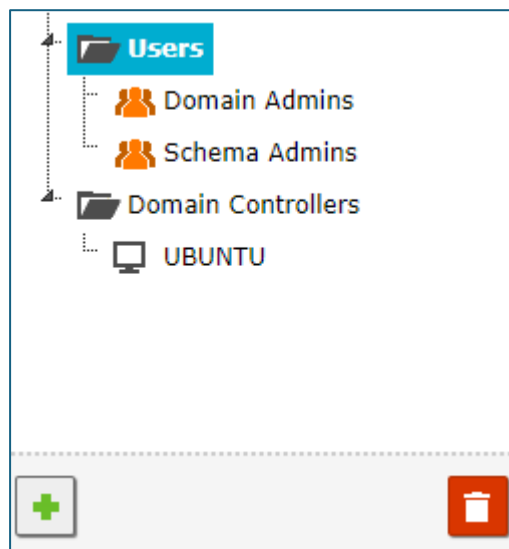


Figura 1: Interfaz usuarios

Posteriormente se debe introducir el nombre de usuario:

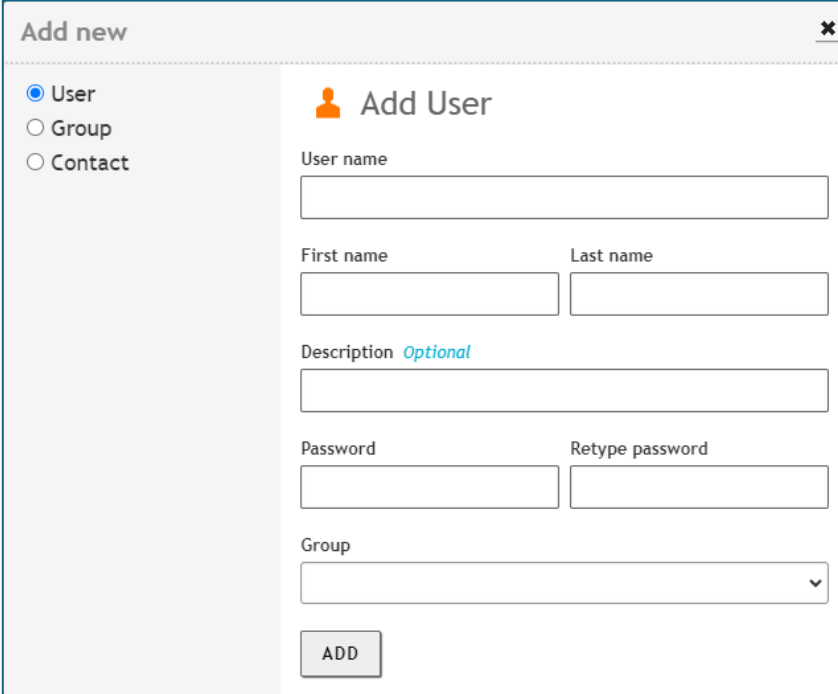


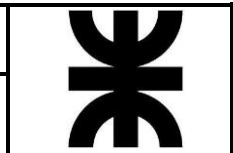
Figura 2: Agregar nuevo usuario

Se recomienda seguir un formato establecido para colocar los nombres de todos los usuarios, ej:

- User name: prueba.user
- First name: prueba
- Last name: user
- Password: contraseña numérica o alfa numérica (no se recomienda símbolos debido a diferencias en la distribución de los teclados).
- Group: grupo/s al que pertenece el usuario.

2.2. Creación de grupos

Se debe seguir los pasos anteriores, pero en el menú de la izquierda se debe seleccionar la opción "Group" y posteriormente agregar el nombre del grupo. Dentro del mismo grupo se puede agregar un nuevo usuario si no se realiza en el momento en que se está creando el usuario.



A continuación se expone la creación de un nuevo usuario:

Figura 3: Anexo usuario dentro de grupo

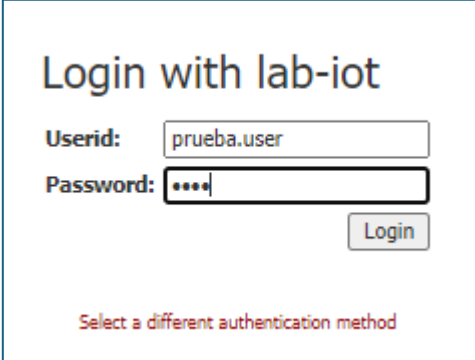
	User	First name	Last name	E-Mail	Actions
<input type="checkbox"/>	prueba.user	prueba	user		 

Figura 4: Usuario creado

2.3. Validación de usuario en Apache VCL y Apache Guacamole

Se debe esperar unos minutos a que la creación de los nuevos usuarios se replique mediante LDAP a toda la infraestructura que se autentica contra el controlador de dominio.

Posterior a esto se puede probar las nuevas credenciales creadas:



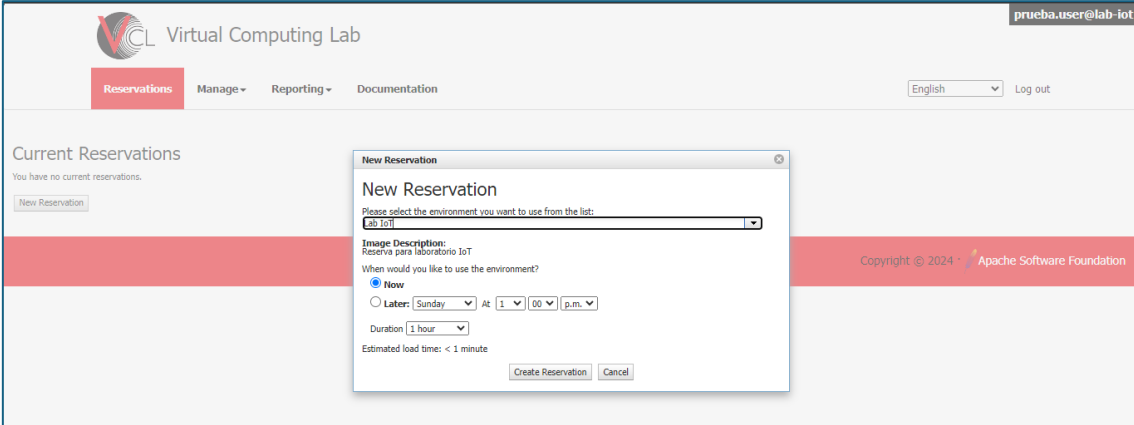
Login with lab-iot

Userid:

Password:

Select a different authentication method

Figura 5: Logueo en Apache VCL



Virtual Computing Lab

Reservations Manage Reporting Documentation

prueba.user@lab-iot

English Log out

Current Reservations

You have no current reservations.

New Reservation

Please select the environment you want to use from the list:

Image Description:
Reserva para laboratorio IoT

When would you like to use the environment?

Now

Later: At

Duration

Estimated load time: < 1 minute

Copyright © 2024 Apache Software Foundation

Figura 6: Validación reserva

El usuario debería poder crear reservas, en caso de no poder realizarlas, comunicarse con el soporte.

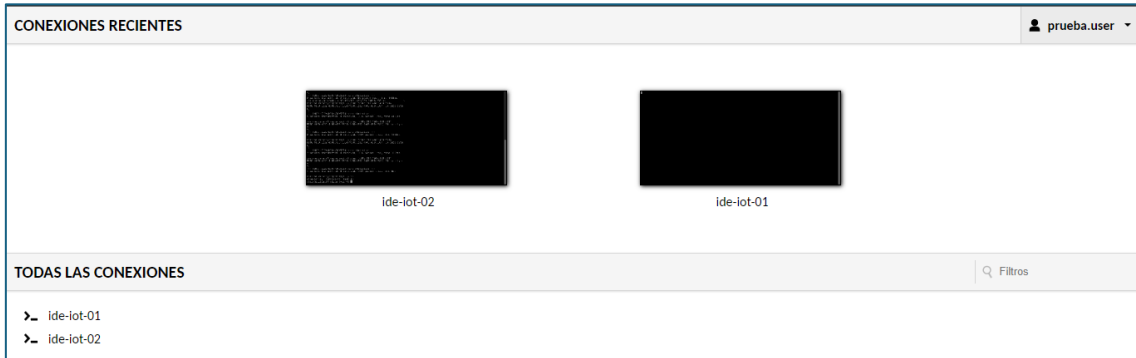


Figura 7: Validación Apache Guacamole

Así como autenticarse en Apache Guacamole y poder visualizar los entornos de programación.

Se recomienda realizar una prueba realizando una reserva a través de Apache VCL y su posterior acceso a través de Guacamole.

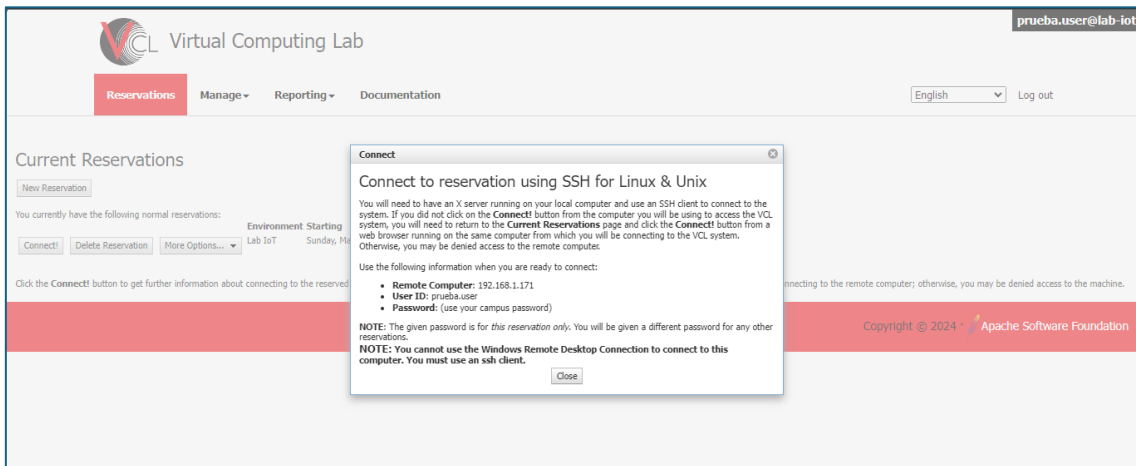


Figura 8: Confirmación de reserva

```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.5.11-4-pve x86 64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Mar 29 17:29:24 2024 from 192.168.1.166
prueba.user@ide-iot-01:~$ ls
prueba.user@ide-iot-01:~$ █
```

Figura 9: Validación entorno de desarrollo

En caso de que aparezca el siguiente aviso es porque no se ha creado el directorio del usuario en el servidor file server:

```
Last login: Sun Mar 31 12:02:44 2024 from 192.168.1.166
Could not chdir to home directory /mnt/nfs/home/prueba.user: No such file or directory
prueba.user@ide-iot-01:/$ █
```

Figura 10: Error file-server

Nota: el usuario no debería ser creado de forma local en el fs ya que este ya existe por el controlador de dominio, en su lugar si se deberá crear su directorio correspondiente para que el usuario tenga su propio espacio de trabajo.

2.4. Creación de home de usuario

Para la creación del home del usuario se debe acceder al file server. Se debe tener en cuenta que el acceso a este servidor solamente es posible a través del servidor de mgmt.

En una primera instancia se recomienda validar que el usuario se ha replicado correctamente en el file server mediante el comando `adduser <nombre user>`. En caso de que se observe un aviso de que el usuario ya existe se puede continuar sin problemas. En caso de que se cree nuevamente el usuario revisar las configuraciones

anteriores porque no se ha desplegado correctamente en toda la infraestructura el nuevo user.

```
[root@file home]# adduser prueba.user
adduser: user 'prueba.user' already exists
[root@file home]#
```

Figura 11: Validación existencia usuario

El siguiente paso consiste en crear el directorio nuevo del usuario recientemente creado:

```
[root@file home]# ls
alan.brito domain.admin juan.perez mariano.zapata
[root@file home]# mkdir prueba.user
[root@file home]# ls
alan.brito domain.admin juan.perez mariano.zapata prueba.user
[root@file home]#
```

Figura 12: Creación directorio usuario

Posteriormente se debe copiar todo el directorio de domain.admin al usuario prueba.user:

```
[root@file home]# cp -r /srv/home/domain.admin/. /srv/home/prueba.user/
cp: overwrite '/srv/home/prueba.user/./.bash_history'? n
cp: overwrite '/srv/home/prueba.user/./.bashrc'? n
[root@file home]# ls
domain.admin mariano.zapata prueba.user
[root@file home]#
```

Figura 13: Copia sistema Contiki-NG

Cambiar el dueño del archivo y grupo al que pertenece mediante los siguientes comandos:

```
[root@file home]# chown -R prueba.user:domain\ users prueba.user
[root@file home]# chmod -R 755 prueba.user
[root@file home]#
```

Figura 14: Cambios dueño y grupo de archivos

Por último, se recomienda probar el acceso del usuario mediante un cliente sftp como winscp o putty a su entorno de trabajo para que se pueda conectar y poder copiar los archivos que desee:

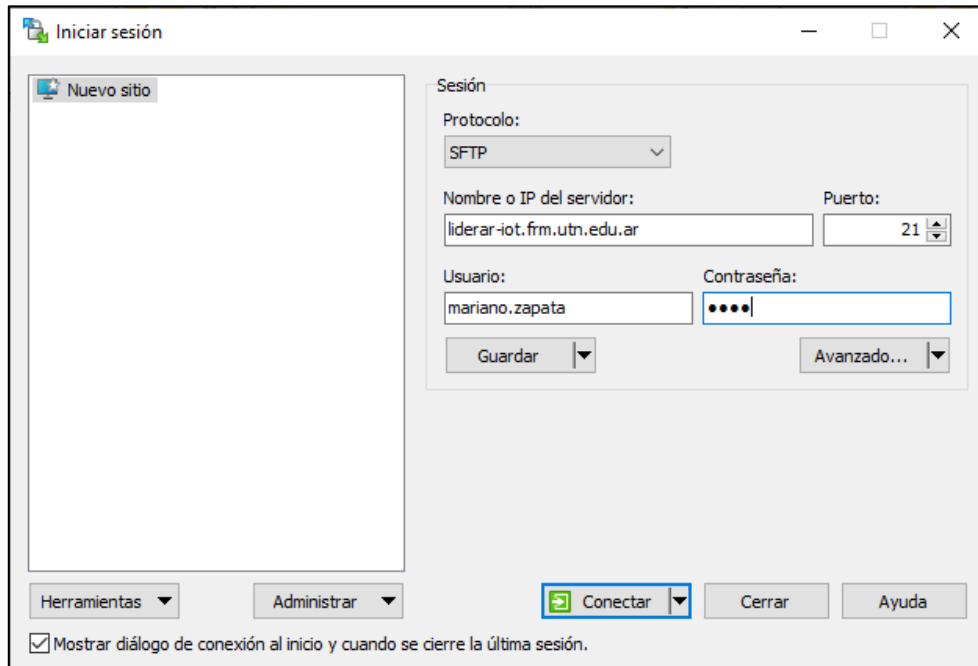


Figura 15: Acceso WinSCP

2.5. Permiso de uso de puerto en RaspberryPi

Para que el usuario pueda acceder a través al puerto USB en la placa Raspbery tras el montaje de su home, se debe agregar a este al grupo “dialout”, para ello conectarse a la placa raspberrypi a través de un entorno de desarrollo mediante el comando `ssh raspi@10.0.0.10` y otorgarse permisos de usuario mediante el comando `sudo su`.

```

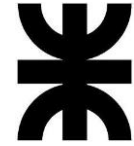
root@ide-iot-01:~# ssh raspi@10.0.0.10
raspi@10.0.0.10's password:
Linux raspberrypi 6.1.21-v8+ #1642 SMP PREEMPT Mon Apr  3 17:24:16 BST 2023 aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 17 22:46:26 2024 from 192.168.1.10
raspi@raspberrypi:~ $ sudo su
root@raspberrypi:/home/raspi#
  
```

Figura 16: Raspberry Pi

Posteriormente agregar al usuario mediante el comando: `sudo usermod -a -G dialout mariano.zapata`



3. Acceso a la red interna del laboratorio

La red interna del laboratorio está conformada como se observa en la siguiente figura:

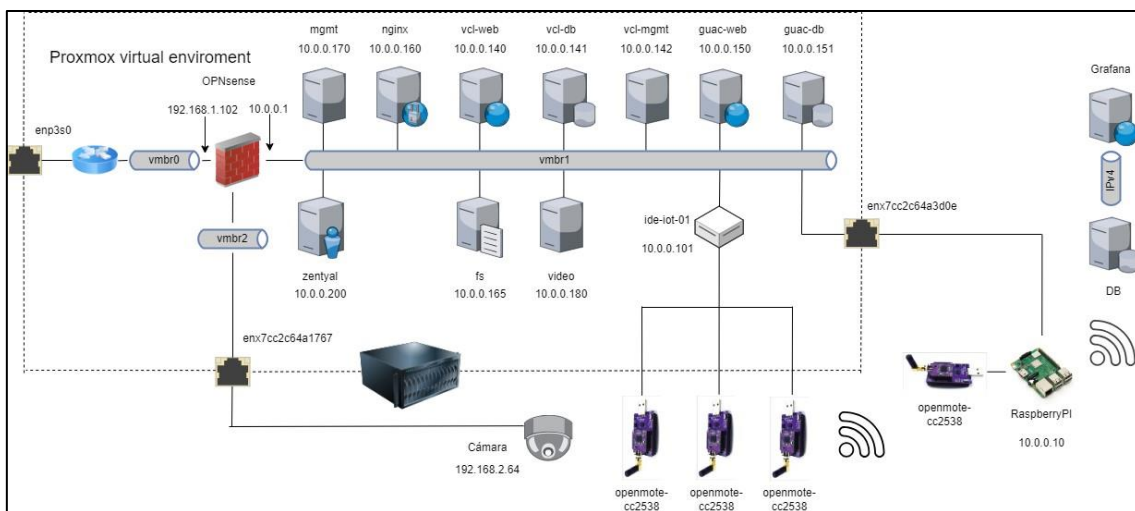


Figura 17: Arquitectura laboratorio

Actualmente el firewall tiene los siguientes puertos abiertos:

Puerto	Detalle Port Forwarding
21	10.0.0.165:22 (fs – servidor de archivos)
22	10.0.0.170:22 (mgmt – servidor de administración)
5901	10.0.0.170:5901 (mgmt – servidor de administración)
80	10.0.0.160:80 (nginx – proxy reverso)
443	10.0.0.160:443 (nginx – proxy reverso)

Tabla 1: Port Forwarding

Para el acceso a las interfaces web de administración se cuenta con la conexión por vnc al servidor de management y posterior conexión mediante web a zentyal o al firewall.

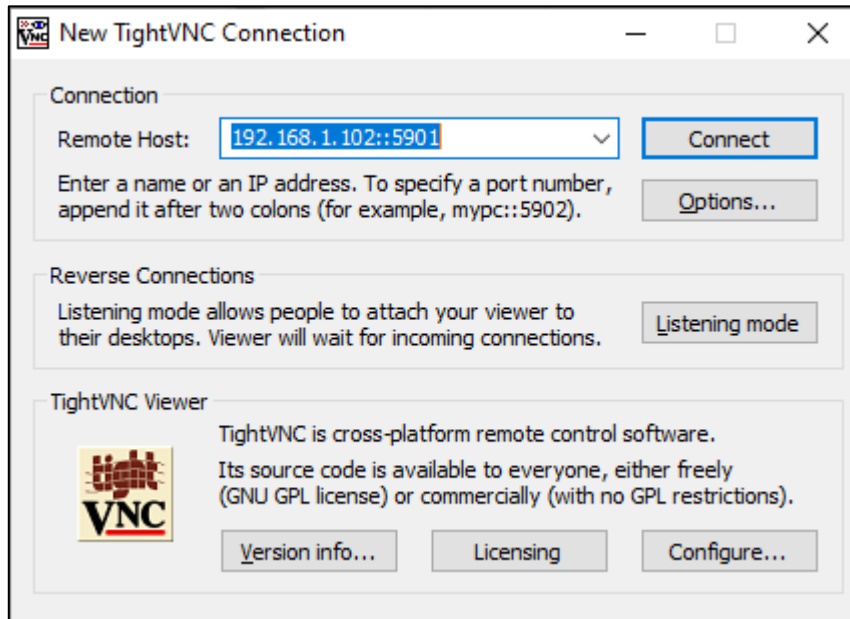


Figura 18: Conexión por VNC

También se cuenta con la posibilidad de acceder mediante una consola de comandos segura (SSH) al servidor de administración. Para ello se debe utilizar autenticación mediante contraseña.

Una vez conectado al servidor de mgmt, es posible conectarse al resto de los entornos de desarrollo por SSH a través del puerto 24 y en el caso del resto de los servidores a través del puerto 22.

Administración firewall OPNSense: se accede a la interfaz web a través de <https://10.0.0.1>, previa conexión mediante VNC al servidor de mgmt.

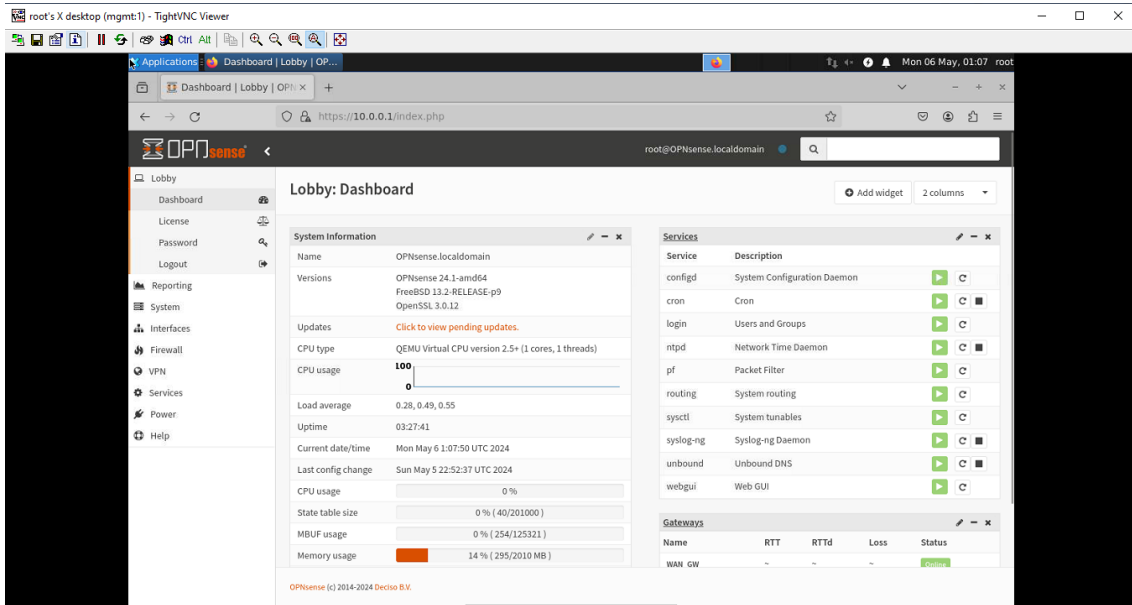


Figura 19: Acceso web a OPNsense

Administración Cámara IP: Se accede a la interfaz web a través de <https://192.168.2.64>, previa conexión mediante VNC al servidor de mgmt.

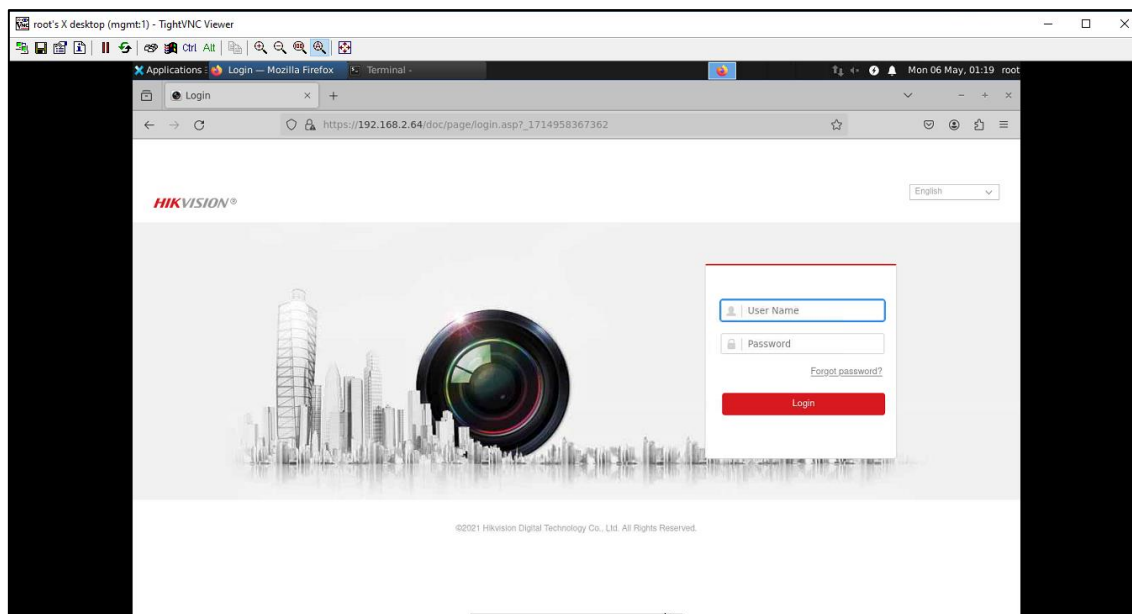


Figura 20: Acceso web a cámara IP

Administración del controlador de dominio Zentyal: Se accede a la interfaz web a través de <https://10.0.0.200:8443>, previa conexión mediante VNC al servidor de mgmt.

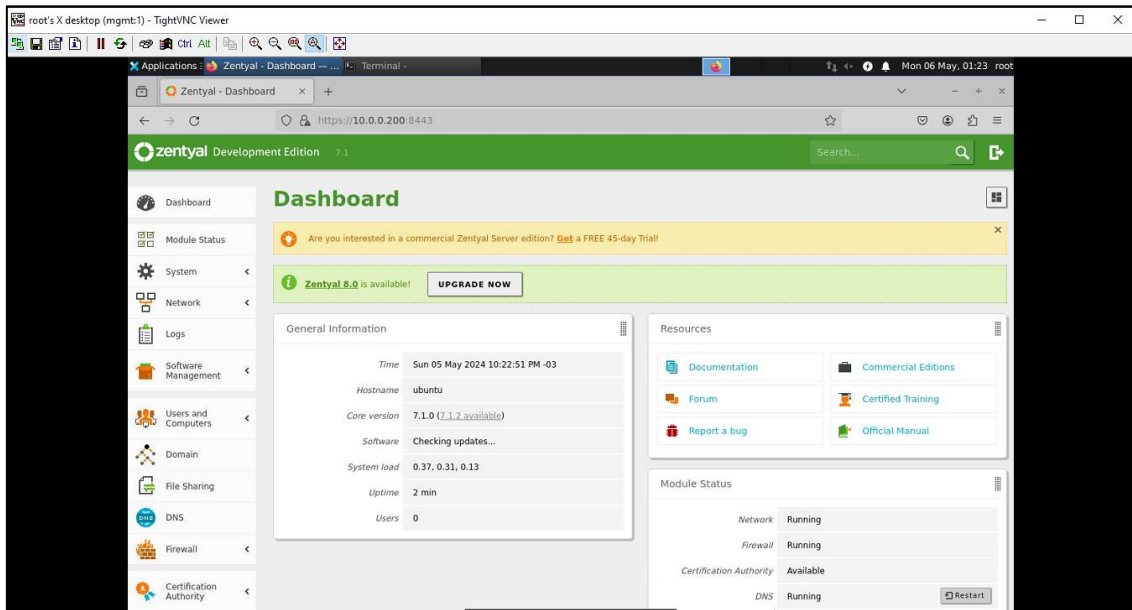


Figura 21: Acceso a interfaz web Zentyal

Nota: Para los servidores web de apache Guacamole y apache VCL también se puede realizar la conexión a través del servidor de mgmt, sin embargo puede resultar más sencillo realizar configuraciones a través de la interfaz web ofrecida por el proxy reverso a través del firewall.

Entornos de desarrollo: se accede a la consola de comandos a través de un cliente ssh, primero se debe realizar la conexión hacia el servidor de mgmt y posteriormente realizar el salto al entorno de desarrollo.

```

root@mgmt:~# ssh root@10.0.0.101 -p24
The authenticity of host '[10.0.0.101]:24 ([10.0.0.101]:24)' can't be established.
ECDSA key fingerprint is SHA256:shGzdocuR2NRGjS5Z96cIe4kC6im0urnug+vrklUXeA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.0.0.101]:24' (ECDSA) to the list of known hosts.
root@10.0.0.101's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.5.11-8-pve x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro
You have new mail.
Last login: Sun May 5 11:06:49 2024 from 192.168.1.14
root@ide-iot-01:~#

```

Figura 22: Acceso a entorno de desarrollo por SSH

4. Administración Apache VCL web

Para el acceso a la interfaz web de Apache VCL ingresando a través del servidor de mgmt o directamente a través de <https://liderar-iot.frm.utn.edu.ar/vcl>

Seleccionar Local Account en el menú desplegable localizado en la izquierda de la interfaz y hacer click en **Proceed to Login**.

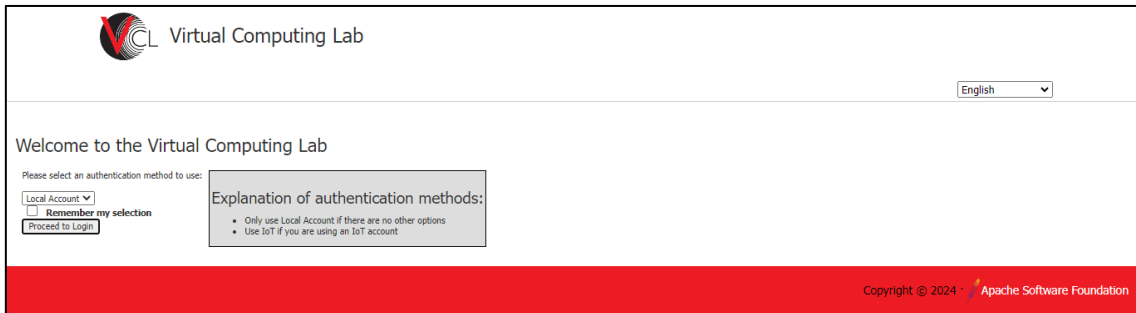


Figura 23: Interfaz web Apache VCL

Posteriormente ingresar con las credenciales de administrador.

Los principales puntos a tener en cuenta son:

Manage Computers

Desde esta herramienta se administran los entornos de desarrollo. Se accede a través de **Manage → Manage Computers → Edit Computer Profiles**.

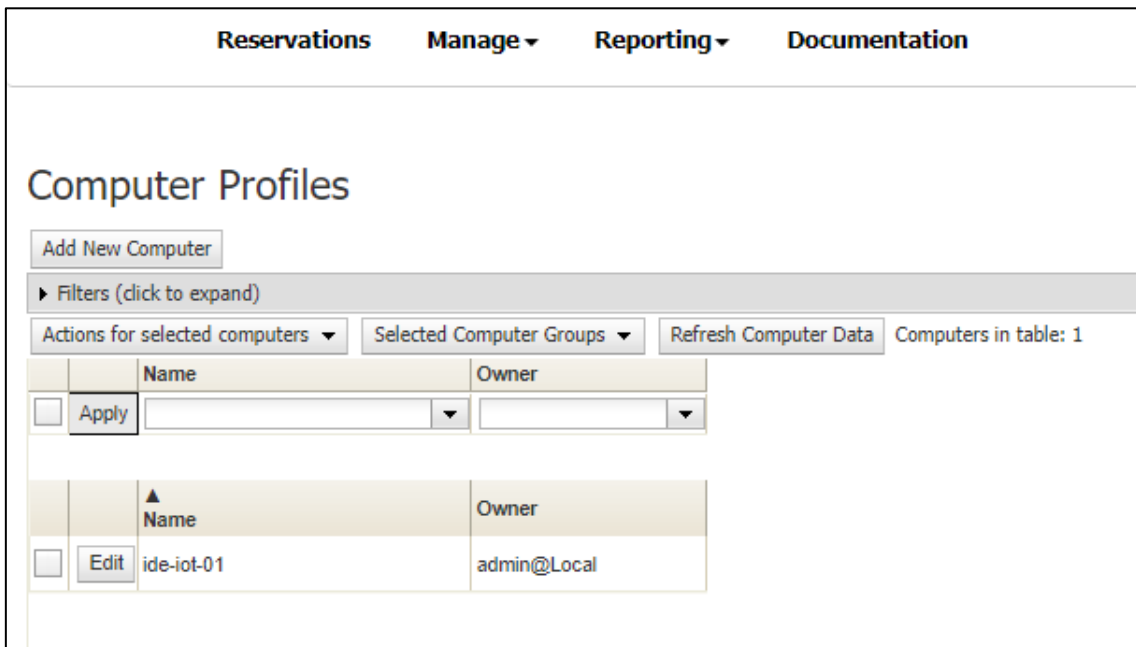
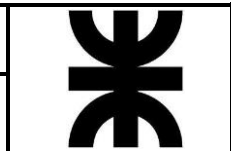


Figura 24: Manage Computers

Desde esta tabla se puede seleccionar el estado del entorno de desarrollo o corregirlo en caso de que por algún error o imperfecto el mismo entre en estado de *“failed”*.



Edit Computer ✕

Name*:

Owner*:

Type:

Public IP Address*:

Private IP Address:

Public MAC Address:

Private MAC Address:

Provisioning Engine:

State:

Platform:

Schedule:

Current Image:

RAM (MB)*:

Cores*:

Processor Speed (MHz)*:

Network:

Predictive Loading Module:

Connect Using NAT:

NAT Host:

Use as NAT Host:

NAT Public IP Address:

NAT Internal IP Address:

Computer ID:

Location:

Figura 25: Edit Computer Profiles

Time Table

En esta sección se pueden observar las reservas actuales y futuras de forma gráfica. Se accede a través de **Manage → View Time Table**.

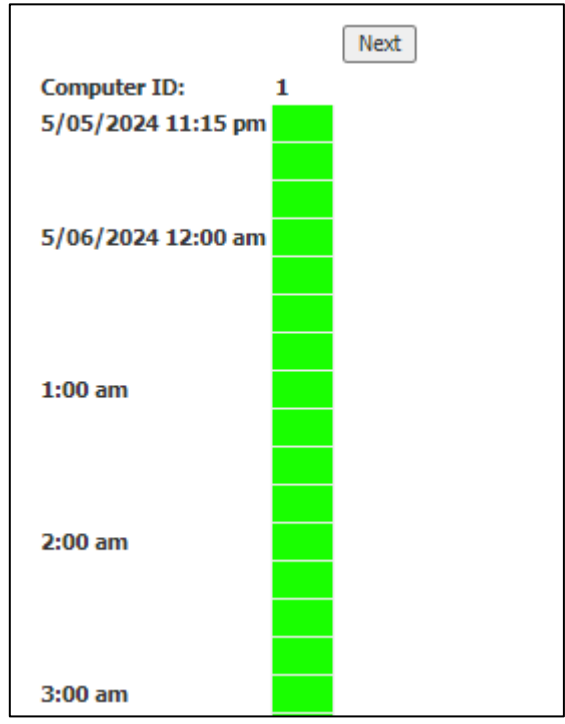
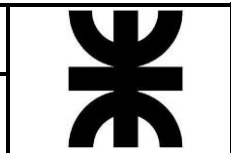


Figura 26: Time Table

En esta sección también se puede eliminar una reserva realizada haciendo clic derecho y posteriormente eliminando la misma.

Manage Privileges

Desde esta sección se gestionan los privilegios de los usuarios para administración y acceso a las imágenes que utilizan el grupo de computadoras (entornos de desarrollo en el caso del presente proyecto). Se accede desde **Manage → Privileges**. Los usuarios se pueden asignar por usuario o por grupo a partir de un árbol de privilegios:

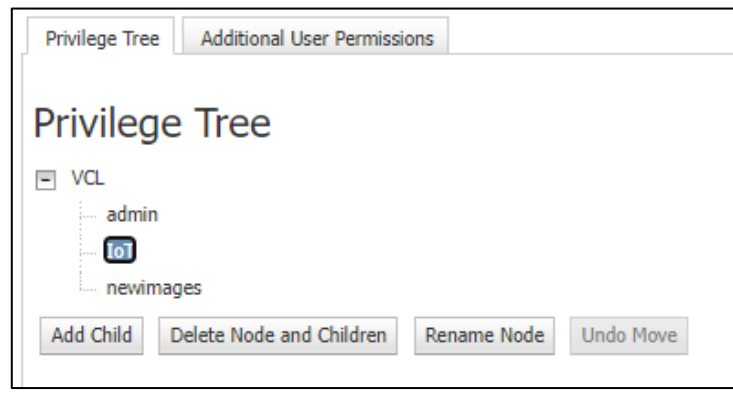


Figura 27: Árbol de privilegios

User Groups

	Block Cascaded Rights	Cascade to Child Nodes												
			addomainAdmin	computerAdmin	groupAdmin	imageAdmin	imageCheckOut	mgmtNodeAdmin	nodeAdmin	resourceGrant	scheduleAdmin	serverCheckOut	userGrant	
adminUsers@Local	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
lab-iot@lab-iot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figura 28: User Groups

Resources

Group Name	Group Type	Block Cascaded Rights	Cascade to Child Nodes				
				available	administer	manageGroup	manageMapping
lab-computadoras-iot	computer	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lab-imagenes-iot	image	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figura 29: Resources

Manage User Groups

Desde esta sección se administran los grupos de usuarios de VCL. Se accede a través de **Manage → Manage Groups**. Es importante destacar que los grupos definidos en VCL son los mismos definidos en Apache Guacamole y Zentyal. De esta manera, es posible gestionar la pertenencia de cada usuario a los grupos desde Zentyal. Existe la posibilidad de que se cree el grupo de usuarios de forma automática debido al intercambio de información realizada con Zentyal para la gestión centralizada de usuarios.



User Groups

Add New User Group

Filters (click to expand)

		Name	Owner	Type	Editable by	Initial Max Time	Total Max Time	Max Extend Time	Max Overlapping Reservations
Delete	Edit	adminUsers@Local	admin@Local	Normal	global@Local	8 hours	10 hours	4 hours	50
Delete	Edit	Allow No User Check@Local	admin@Local	Normal	adminUsers@Local	4 hours	6 hours	1 hour	0
Delete	Edit	Default for Editable by@Local	admin@Local	Normal	adminUsers@Local	4 hours	6 hours	1 hour	0
Delete	Edit	global@Local	admin@Local	Normal	global@Local	4 hours	6 hours	1 hour	0
Delete	Edit	lab-iot@lab-iot	N/A	Federated	None	4 hours	6 hours	1 hour	0
Delete	Edit	manageNewImages@Local	admin@Local	Normal	adminUsers@Local	4 hours	6 hours	1 hour	0
Delete	Edit	Specify End Time@Local	admin@Local	Normal	adminUsers@Local	4 hours	6 hours	1 hour	0

Figura 30: Manage Users Groups

Dashboard

En esta sección se observa información general del funcionamiento de Apache VCL. Se accede desde el menú **Reporting** → **Dashboard**.

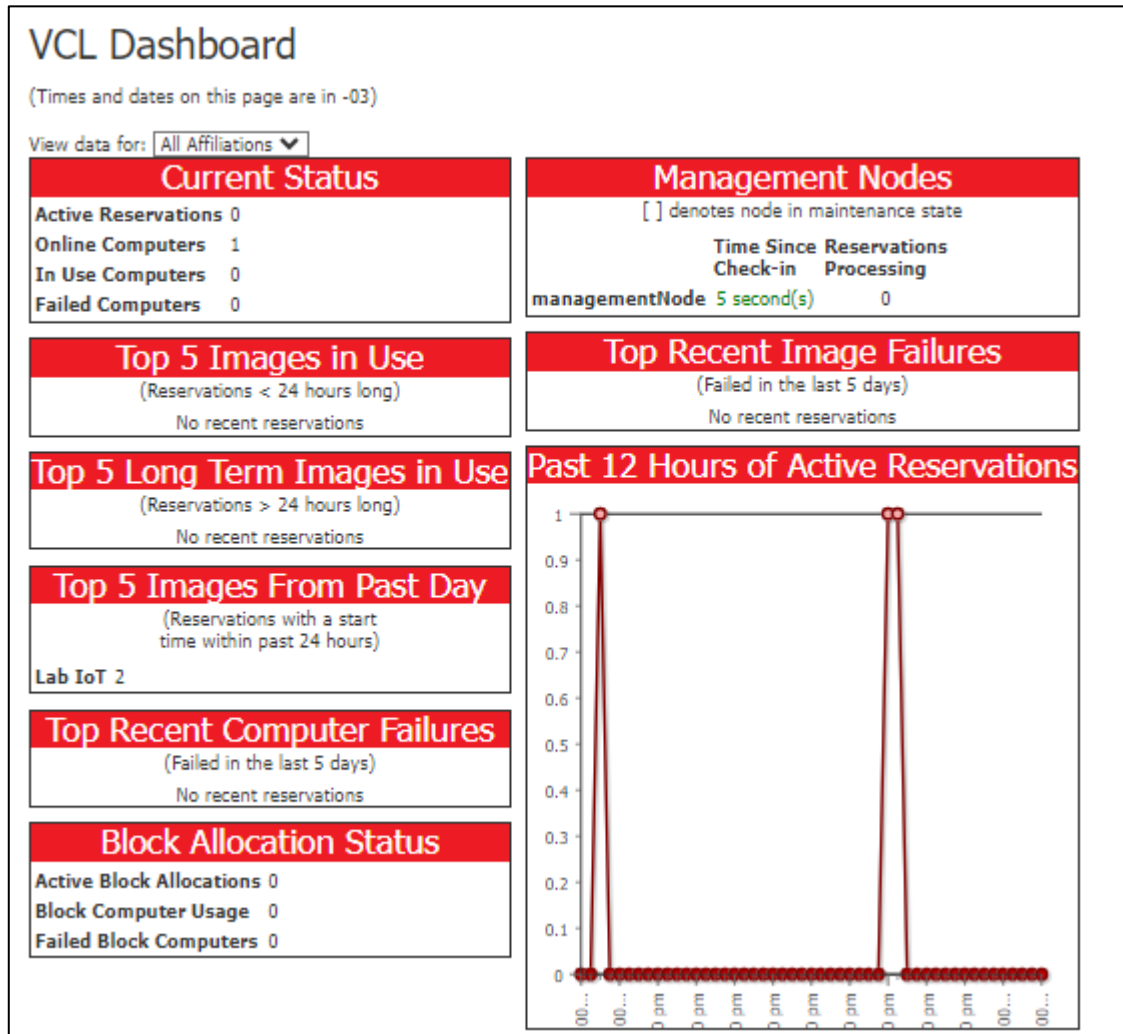
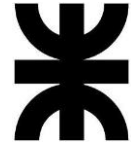


Figura 31: Dashboard

Los datos relevantes son:

- Online Computers (Current Status)
- In Use Computers (Current Status)
- Failed Computers (Current Status)
- Time Since Check-in (Management Nodes). Corresponde al tiempo en que realiza una comunicación desde el servidor web a la base de datos y al servidor de administración, por defecto está seteado en 6 segundos, esto puede ser visualizado en el servidor de management dentro del directorio /var/log/vclid.log.

5. Administración Apache Guacamole

Para el acceso a la interfaz web de Apache VCL ingresando a través del servidor de mgmt o directamente a través de <https://liderar-iot.frm.utn.edu.ar/guacamole>



Figura 32: Interfaz Apache Guacamole

Se debe utilizar las credenciales de administrador. En esta cuenta se ha configurado conexiones a los entornos de desarrollo como usuario admin a través del puerto 24.

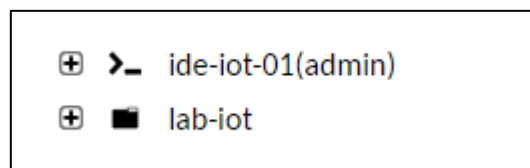


Figura 33: Conexión por usuario admin

Nota: tener la precaución de colocar en mantenimiento el entorno de desarrollo mediante Apache VCL para evitar que un usuario final intente realizar reservas mientras este está siendo usado por un usuario administrador.

Los usuarios pueden crearse de forma local, pero Guacamole realiza la autenticación de los usuarios a través de Zentyal por lo que esta posibilidad solamente debe ser utilizada en casos de contingencia.

El anexo de los entornos de desarrollo debe realizarse a través de la interfaz **Conexiones** → **Nueva conexión** (en caso de no querer agregarla a un grupo).

Si se desea anexar una nueva conexión a un grupo, se debe primero desplegar el grupo y después seleccionar **Nueva conexión**.

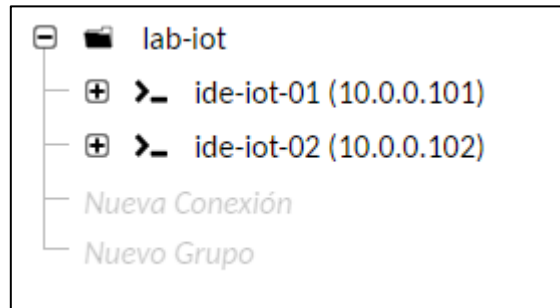


Figura 34: Nueva conexión