



**QUICK START GUIDE**

**Nozomi Networks**  
**Guardian Community Edition**



# Aviso

---

## Avisos legales

---

### Fecha de publicación

marzo 2020

### Derechos de autor

Derechos de autor © 2013-2020, Redes Nozomi. Reservados todos los derechos. Nozomi Networks cree que la información que proporciona es precisa y confiable. Sin embargo, Nozomi Networks no asume ninguna responsabilidad por el uso de esta información, ni ninguna infracción de patentes u otros derechos de terceros que puedan resultar de su uso. No se otorga ninguna licencia por implicación o de otra manera bajo ninguna patente, derecho de autor u otro derecho de propiedad intelectual de Nozomi Networks, excepto como se describe específicamente en las licencias de usuario aplicables. Nozomi Networks se reserva el derecho de cambiar las especificaciones en cualquier momento sin previo aviso.



# Tabla de contenido

Avisos legales.....	iii
Capítulo 1: Instalación .....	7 Instalación en hardware
virtual .....	8 Configuración Fase
1 .....	10 Fase 2 de
configuración .....	12
Ajustes adicionales. ....	14
Capítulo 2: Conceptos básicos .....	15
Ambiente.....	16
Activo .....	16
Nodo.....	16
Sesión.....	17
Enlace.....	
17 Consulta.. .....	
18 Protocolo .....	18
Capítulo 3: Referencia de la interfaz de usuario.....	19 Navegadores web
compatibles.....	20 Encabezado de
navegación .....	20 Vista de
activos .....	21
Vista de red .....	22
Consultas.....	
32 Sistema.....	35
Consultas .....	43
Capítulo 4: Consultas.....	47
Descripción general.....	48
Referencia.....	49
Ejemplos.....	58
Capítulo 5: Mantenimiento .....	63 Resumen del
sistema .....	64 Copia de
seguridad y restauración de datos.....	65
Reiniciar y apagar.....	66
Actualización y reversión de software .....	67
Restablecimiento de fábrica de datos .....	
Soporte.....	69
Capítulo 6: Protocolos programables.....	71
Configuración.....	72
Escribiendo un protocolo programable.....	73
Referencia API.....	77



# Capítulo

# 1

---

## Instalación

---

Temas:

- [Instalación en hardware virtual](#) • [Fase 1 de configuración](#) •  
[Fase 2 de configuración](#)  
• [Configuración adicional](#)

En este capítulo, recibirá la información fundamental necesaria para poner en funcionamiento los dispositivos físicos y virtuales de Nozomi Networks Solution.

En el capítulo [Configuración](#) se proporciona más información sobre la configuración adicional .

Las tareas de mantenimiento se describen en el capítulo [Mantenimiento](#) .

## Instalación en hardware virtual

La instalación en hardware virtual se ha probado en una variedad de entornos compatibles con OVA.

Sin embargo, la versión actual de N2OS admite oficialmente estos hipervisores:

1. VMware ESXi 5.5 o posterior 2.

HyperV 2012 o posterior

Los requisitos mínimos para los recursos de una máquina virtual Guardian (VM) son:

- 4 vCPU funcionando a 2 Ghz • 4

GB de RAM • 10 GB

de espacio en disco mínimo, ejecutándose en SSD o almacenamiento híbrido (se recomiendan más de 100 GB de disco) • 2 o más NIC (el número máximo depende del hipervisor), uno será utilizado para la gestión y el 1 o más otros para el control del tráfico

Asegurar que todos estos recursos se brinden en condiciones saludables. La carga general del hipervisor debe estar bajo control y no debe producirse un incremento regular en la VM de Guardian; de lo contrario, se puede experimentar un comportamiento inesperado del sistema, como paquetes perdidos o un rendimiento general deficiente del sistema.

## Instalación de la máquina virtual

En esta sección cubriremos la instalación de la Máquina Virtual en el hipervisor. Se obtendrá una máquina virtual en ejecución; sin embargo, en secciones posteriores se proporcionará una configuración adicional que permita el acceso externo.

Para continuar, debe estar familiarizado con la importación de máquinas virtuales OVA en su entorno de hipervisor. Si este no fuera el caso, consulte el manual o el servicio de soporte de su hipervisor.

1. Importe la Máquina Virtual al hipervisor y configure los recursos de acuerdo con los requisitos mínimos especificados en la sección anterior.
2. Despues de importar la VM, vaya a la configuración del hipervisor del disco de la VM y establezca el tamaño deseado. Algunos hipervisores, por ejemplo, VMware ESX >= 6.0, permiten cambiar el tamaño del disco en esta etapa. Con los hipervisores que no permiten esta operación, debe DETENER AQUÍ con esta sección y continuar con las instrucciones contenidas en [Adición de un disco secundario a la máquina virtual](#) en la página 8.
3. Inicie la máquina virtual. Ahora se iniciará en un entorno N2OS válido.
4. Inicie sesión como administrador. Ingresará instantáneamente, no se establece una contraseña de forma predeterminada.
5. Vaya al modo privilegiado con el comando:

Permiteme

Ahora podrá realizar cambios en el sistema.

## Agregar un disco secundario a la máquina virtual

En esta sección, cubriremos cómo agregar un disco de datos virtual más grande a la máquina virtual N2OS, en caso de que el disco principal no pueda crecer durante la primera importación. Para continuar, debe estar familiarizado con la administración de discos virtuales en su entorno de hipervisor. De lo contrario, consulte el manual o el servicio de soporte de su hipervisor.

1. Agregue un disco a la máquina virtual y reinícielo

2. En la consola de la VM, use el siguiente comando para obtener el nombre de los dispositivos de disco:

sysctl kern.disks

3. Suponiendo que ada1 es el disco del dispositivo agregado como disco secundario (tenga en cuenta que ada0 es el dispositivo del sistema operativo), ejecute este comando para mover la partición de datos a él

mover datos ada1

## Agregar una interfaz de monitoreo a la Máquina Virtual

De manera predeterminada, la VM tiene una interfaz de red de administración y una interfaz de monitoreo. Dependiendo de las necesidades de implementación, puede ser útil agregar más interfaces de monitoreo al dispositivo. Para agregar una o más interfaces, siga estos pasos:

1. Si la VM está encendida, apáguela.

Agregue una o más interfaces de red desde la configuración del hipervisor.

Encienda la VM

Guardian reconocerá y utilizará automáticamente las interfaces recién agregadas.

## Configuración Fase 1

Ahora configuraremos la configuración muy básica necesaria para comenzar a usar la solución Nozomi Networks.

Después de estos pasos, el sistema tendrá la interfaz de administración configurada y accesible como consola de texto a través de SSH y como consola web a través de HTTPS.

Asumimos que la solución Nozomi Networks ya se ha instalado y está lista para configurarse por primera vez. Según el caso, en esta fase se debe utilizar una consola serial (para Dispositivos Físicos) o la consola del hipervisor de texto (para Dispositivos Virtuales).

1. La consola mostrará un mensaje con el texto "N2OS - iniciar sesión:". Escriba admin y luego presione [Enter].

En el dispositivo virtual, iniciará sesión instantáneamente, ya que no se establece una contraseña de forma predeterminada. En dispositivos físicos, nozominetworks es la contraseña predeterminada.

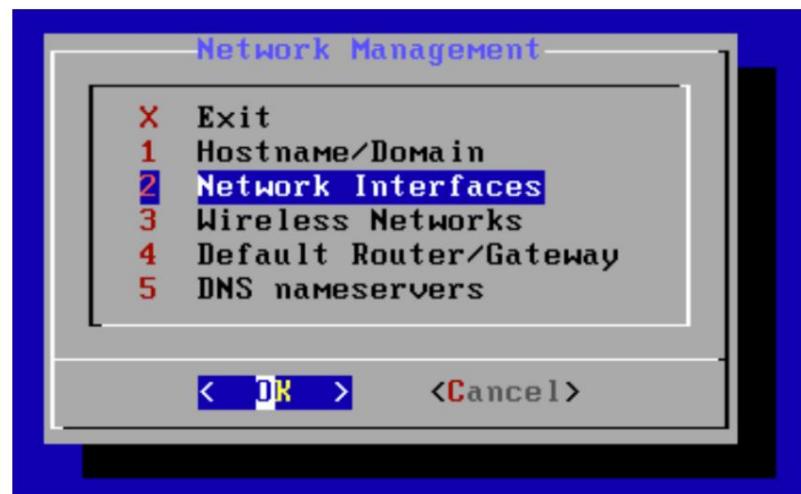
2. Eleve los privilegios con el comando: enable-me 3. Ahora inicie el asistente de configuración inicial con el comando: setup

```
root@nozomi-ids:~ # setup
```

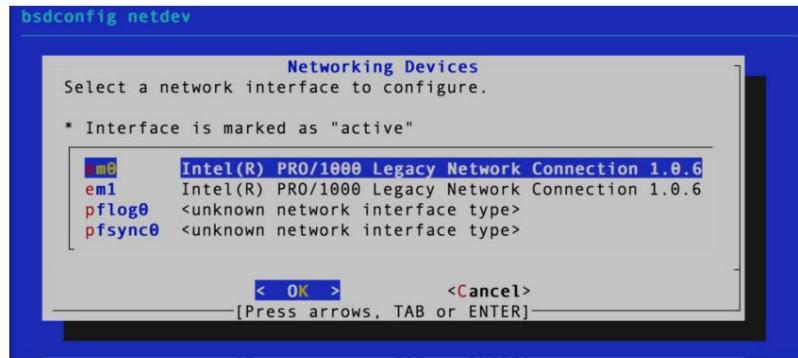
4. Primero se le pedirá que elija la contraseña de administrador. Seleccione una contraseña segura ya que esto le permitirá el usuario administrador para acceder al dispositivo a través de SSH.

```
You must set the password for the 'admin' console user.  
Changing local password for admin  
You can now choose the new password.  
A valid password should be a mix of upper and lower case letters,  
digits and other characters. You can use an 8 character long  
password with characters from at least 3 of these 4 classes, or  
a 7 character long password containing characters from all the  
classes. Characters that form a common pattern are discarded by  
the check.  
Alternatively, if no one else can see your terminal now, you can  
pick this as your password: "motor.church!half".  
Enter new password: ■
```

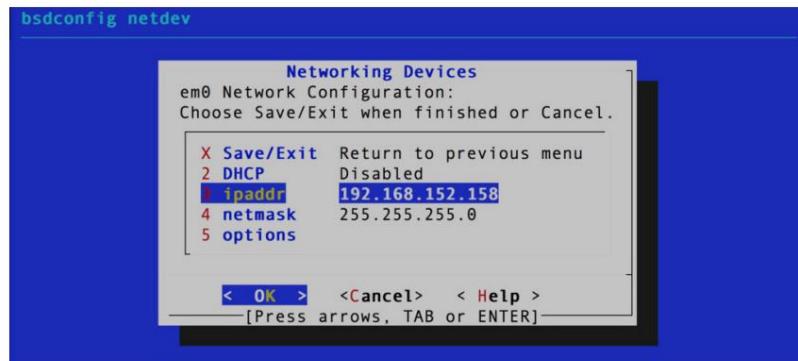
5. En segundo lugar, deberá configurar la dirección IP de la interfaz de administración. Seleccione la "2 Red Interfaces" en el diálogo.



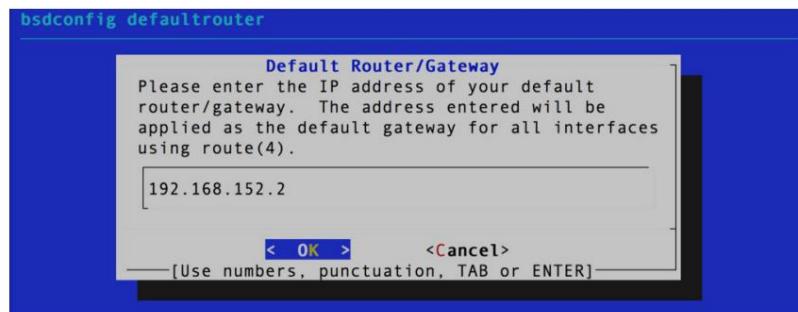
6. Ahora deberá configurar la dirección IP de la interfaz de administración. Según el modelo del dispositivo, la interfaz de administración puede llamarse em0 o mgmt. Selecciónalo y presiona [Enter].



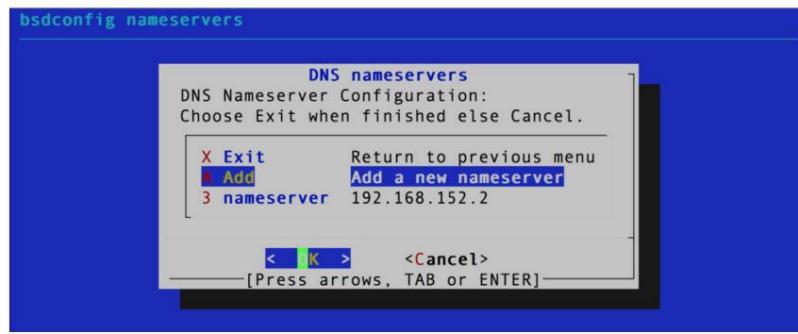
7. Edite los valores de la dirección IP (ipaddr) y la máscara de red (netmask). Habilite DHCP para configurar todo automáticamente. Luego suba a "X. Guardar/Salir" y presione [Enter].



8. Ahora seleccione "Enrutador/Puerta de enlace predeterminado" en el menú e ingrese la dirección IP del puerta. Presione [Tab] y luego [Enter] para guardar y salir.



9. Ahora seleccione "Servidores de nombres DNS" en el menú y configure las direcciones IP de los servidores DNS.



10. Suba a "X Exit" y presione [Enter].

11. La configuración básica de la red está lista; los pasos restantes se realizarán abriendo la consola web que se ejecuta en la interfaz de administración.

## Configuración Fase 2

Esta segunda fase de la configuración se realizará con la consola web. Antes de comenzar a usar la consola web, asegúrese de usar uno de los [navegadores web compatibles](#).

Se puede acceder a la consola web apuntando a `https://<appliance_ip>` donde `<appliance_ip>` es la dirección IP asignada a la interfaz de administración. Tenga en cuenta que el producto integra certificados SSL autofirmados para comenzar, así que agregue una excepción en su navegador. Más adelante en este capítulo proporcionaremos los pasos para importar los válidos. Ahora debería ver la pantalla de inicio de sesión:



El nombre de usuario y la contraseña predeterminados son `admin / nozominetworks`. Por razones de seguridad, se le pedirá que cambie estas credenciales la primera vez que inicie sesión.

Una vez que haya iniciado sesión, se pueden completar los pasos restantes de la configuración. Vaya a Administración > General y cambie el nombre de host.

Ahora corrija la configuración de fecha y hora. Vaya a Administración > Fecha y hora y cambie la zona horaria, configure la fecha y (opcional) habilite el cliente NTP.

Date settings

Timezone

Local: CET (UTC+02:00)

**Save**

Date (format ccyy-mm-dd HHMM.ss)

201907250932.16

**Save**

NTP

Enabled

Servers

0.freebsd.pool.ntp.org,1.freebsd.pool.ntp.org

**Save**

El dispositivo está casi listo para ponerse en producción: el siguiente paso es instalar una licencia válida.

## Licencia

En la página Administración > Actualizaciones y licencias, deberá configurar una nueva licencia. Primero copie la ID de la máquina, luego puede usarla junto con el Código de activación que recibió de Nozomi Networks para obtener una clave de licencia. Una vez que tenga una clave de licencia válida, péguela dentro del cuadro de texto. Despues de la confirmación, el dispositivo comienza a monitorear las interfaces de red configuradas.

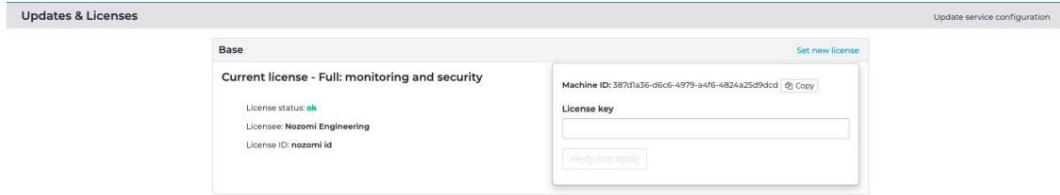


Figura 1: La página de Licencia

## Ajustes adicionales

En este capítulo se explicarán algunas configuraciones adicionales no obligatorias del sistema.

### Instalar certificados SSL

En esta sección, importaremos un certificado SSL real al dispositivo, necesario para cifrar de forma segura todo el tráfico entre las computadoras cliente y el dispositivo N2OS a través de HTTPS.

El servidor web N2OS que expone la interfaz HTTPS es nginx. Prepárese con un certificado y un archivo de clave compatibles con NGINX y llámelos https\_nozomi.crt y https\_nozomi.key.

1. Cargue el certificado y el archivo de claves en el dispositivo con un cliente SSH en la carpeta /data/tmp.

Por ejemplo, dado que tiene https\_nozomi.crt y https\_nozomi.key en la misma carpeta, abra una terminal, haga un cd y luego cargue

```
scp https_nozomi.* admin@<appliance_ip>:/data/tmp
```

2. Inicie sesión en la consola de texto, ya sea directamente o a través de SSH, luego eleve los privilegios

```
Permiteme
```

3. Ejecute el comando n2os-addtlsCert

```
n2os-addtlsCert https_nozomi.crt https_nozomi.key
```

4. Ahora reinicie nginx emitiendo el comando

```
reiniciar el servicio nginx
```

5. Verifique que el certificado se haya cargado correctamente dirigiendo su navegador a https://

<appliance\_ip>/ y verificando que el certificado ahora se reconozca como válido.

6. Podemos guardar de forma segura la nueva configuración emitiendo este comando en la consola

```
n2os-guardar
```

Ahora los certificados SSL importados funcionan correctamente y se aplicarán también en el próximo reinicio.

# Capítulo

# 2

---

## Lo esencial

---

Temas:

- [Medio ambiente](#)
- [Activo](#)
- [Nodo](#)
- [Sesión](#)
- [Enlace](#)
- [Consulta](#)
- [Protocolo](#)

En el capítulo, se le presentarán algunos conceptos básicos de la solución Nozomi Networks y se explicarán algunos controles de interfaz gráfica recurrentes.

Debe dominar estos conceptos para comprender cómo usar y configurar correctamente el sistema N2OS.

## Ambiente

El entorno de solución de Nozomi Networks es la representación en tiempo real de la red supervisada por The Guardian, que proporciona una vista sintética de todos los activos, todos los nodos de la red y las comunicaciones entre ellos.

### Vista de activos

En la sección Vista de activos se muestran todos sus activos, pensados como puntos finales discretos únicos. En esta sección, es fácil visualizar, encontrar y profundizar en la información de los activos, como las versiones de hardware y software.

Para obtener más detalles, consulte [Vista de activos](#) en la página 21

### Vista de red

En la sección Vista de red se encuentra toda la información de red genérica que no está relacionada con el lado SCADA de algunos protocolos, como la lista de nodos, la conexión entre nodos y la topología.

Para obtener más detalles, consulte [Vista de red](#) en la página 22

### Vista de proceso

En la sección Vista del proceso se encuentra toda la información específica de SCADA, como la lista de esclavos SCADA, las variables del esclavo con su historial de valores y otra información relacionada, una sección con el análisis de los valores de las variables y algunas estadísticas relacionadas con las variables.

## Activo

Un activo en el Ambiente representa un actor en la comunicación de la red y, dependiendo de los nodos y componentes involucrados, puede ser algo que va desde una simple computadora personal hasta un dispositivo OT.

Todos los activos se enumeran en la sección Entorno > Vista de activos > Lista y también se pueden ver de forma más gráfica en la sección Entorno > Vista de activos > Diagrama, que agrega los activos en diferentes niveles.

Page 1 of 7,165 entries						
ACTIONS	NAME	TYPE	OS/FIRMWARE	IP	MAC ADDRESS	MAC
		switch	Firmware: 0.9.06	[multiple]		Hirschman
		switch	Firmware: h.10.38	[multiple]		ProCurve N
		computer		172.16.66.53		
		switch	Firmware: V05.01.03	[multiple]		Siemens A4
		computer		192.168.162.22		
		PLC	Firmware: 2.90	172.16.0.157		
		PLC	Firmware: 2.90	172.16.1.174		

Figura 2: Ejemplo de una lista de activos

## Nodo

Un nodo en el Ambiente representa un actor en la comunicación de la red y, dependiendo de los protocolos involucrados, puede ser algo que va desde una simple computadora personal hasta una RTU o un PLC.

Todos los nodos del entorno se enumeran en la sección Entorno > Vista de red > Nodos o se pueden ver de una forma más gráfica en la sección Entorno > Vista de red > Gráfico.

Cuando un nodo está involucrado en una comunicación usando protocolos SCADA, puede ser un maestro o un esclavo.

Los esclavos SCADA se pueden analizar en detalle en la sección Entorno > Vista de proceso.

Network view							Nodes	Links	Sessions	Graph	Traffic
Page 1 of 8,185 entries / sorted by roles: asc							Export	Live	Selected	9 selected	
ACTIONS	ADDRESS	LABEL	ROLES	MAC ADDRESS	SENT BYTES	RECEIVED BYTES	# LINKS	PROTOCOLS			
	<a href="#">172.16.0.1</a>		dns_server	c4:5e:1f:92:ed:d8	8.7 KB	0.0 B	3	dns			
	<a href="#">192.168.1.1</a>		dns_server	c4:5e:1f:92:ed:d8	16.6 KB	0.0 B	3	dns			
	<a href="#">10.1.1.1</a>	HISTORIAN-01	historian	d8:9d:b9:00:7:ec	2.1 KB	3779 KB	7	browser, pi-connect			
	<a href="#">172.16.0.253</a>		master	00:04:23:e0:04:1c	3.0 MB	1.0 MB	26	dns, modbus, pi-connect, smb, vnc			
	<a href="#">192.168.1.12</a>		master	09:00:09:00:01:12	1.7 MB	869.0 KB	50	dns, lec104, pi-connect, smb, vnc			
	<a href="#">192.168.1.11</a>		master	18:66:da:00:01:11	1.6 MB	570.6 KB	41	dns, lec104, pi-connect, smb, vnc			
	<a href="#">172.16.1.253</a>		master	00:04:23:e0:04:1c	3.0 MB	1.0 MB	26	dns, modbus, pi-connect, smb, vnc			
	<a href="#">192.168.162.22</a>		master	09:00:09:00:01:12	304.6 KB	361.8 KB	12	dns, ethernetip, pi-connect, smb			
	<a href="#">172.16.0.101</a>		master	10:c3:7b:4:c8:31:7	1.7 MB	716.2 KB	4	dce-rpc, dns, opc, smb, vnc			
	<a href="#">00:60:78:00:6a:10</a>		other	00:60:78:00:6a:10	240.0 B	120.0 B	0	-			
	<a href="#">10.4.1.32</a>		other	b4:a3:82:02:66:00	54.5 KB	2.6 KB	1	rtsp			
	<a href="#">ffff:ffff:ffff:ffff</a>		other	ffff:ffff:ffff:ffff	0.0 B	282.0 B	0	-			
	<a href="#">ec:74:ba:56:66:60</a>	MACH-666666	other	ec:74:ba:56:66:60	0.0 B	0.0 B	0	-			
	<a href="#">00:16:b9:49:b6:7d</a>	ACMEinchHQ_SW1	other	00:16:b9:49:b6:7d	356.0 B	0.0 B	1	lldp			
	<a href="#">00:16:b9:49:b6:40</a>	ACMEinchHQ_SW1	other	00:16:b9:49:b6:40	188.0 B	0.0 B	0	-			
	<a href="#">10.2.1.255</a>		other	ffff:ffff:ffff:ffff	0.0 B	12.5 KB	1	browser			
	<a href="#">172.16.66.53</a>		other	18:a9:05:24:d8:b5	788.0 B	3.8 KB	6	smb			
	<a href="#">00:1b:1b:ce:c8:62</a>	ACMEinchHQ_SW2	other	00:1b:1b:ce:c8:62	0.0 B	0.0 B	0	-			
	<a href="#">01:80:c2:00:00:0e</a>		other	01:80:c2:00:00:0e	0.0 B	3.1 KB	6	lldp			
	<a href="#">00:04:23:e0:04:1c</a>		other	00:04:23:e0:04:1c	240.0 B	120.0 B	0	-			
	<a href="#">10.4.1.36</a>		other	b4:a3:82:06:48:aa	54.5 KB	2.6 KB	1	rtsp			
	<a href="#">10.5.1.53</a>		other	c4:2f:90:a8:c7:79	18.4 KB	381.7 KB	7	rtsp			
	<a href="#">00:50:56:f6:3c:50</a>		other	00:50:56:f6:3c:50	42.0 B	0.0 B	0	-			
	<a href="#">00:0c:29:1d:f2:4a</a>		other	00:0c:29:1d:f2:4a	42.0 B	42.0 B	0	-			
	<a href="#">192.168.162.255</a>		other	ffff:ffff:ffff:ffff	0.0 B	777.0 B	1	browser			

Figura 3: Una lista de ejemplo de nodos de red

## Sesión

Una sesión es un intercambio de información interactivo semipermanente entre dos o más nodos que se comunican.

Una sesión se configura o establece en un momento determinado y luego se rechaza en un momento posterior. Una sesión de comunicación establecida puede incluir más de un mensaje en cada dirección.

La solución Nozomi Networks muestra el estado de una sesión según el protocolo de transporte, por ejemplo, una sesión TCP puede estar en estado SYN o SYN-ACK antes de estar ABIERTA.

Cuando se cierra una sesión, se conservará durante un tiempo determinado y aún se podrá consultar para realizar análisis posteriores.

Todas las sesiones se enumeran en Entorno > Vista de red > Sesiones.

Page 1 of 12,293 entries											
ACTIONS	STATUS	FROM	TO	TRANSPORT PROTOCOL	FROM PORT	TO PORT	PROTOCOL	THROUGHPUT	TRANSFERRED BYTES	TRANSFER	
	ACTIVE	<a href="#">10.4.1.32</a>	<a href="#">10.4.1.32</a>	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp	
	ACTIVE	<a href="#">10.5.1.253</a>	<a href="#">10.4.1.34</a>	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp	
	ACTIVE	<a href="#">10.5.1.253</a>	<a href="#">10.4.1.30</a>	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp	
	ACTIVE	<a href="#">10.5.1.253</a>	<a href="#">10.4.1.31</a>	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp	
	ACTIVE	<a href="#">10.5.1.253</a>	<a href="#">10.4.1.35</a>	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp	
	ACTIVE	<a href="#">10.5.1.253</a>	<a href="#">10.4.1.36</a>	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp	

Figura 4: Una lista de ejemplo de sesiones de red

## Enlace

Un enlace en el entorno representa la comunicación entre dos nodos utilizando un protocolo específico.

Todos los enlaces se enumeran en la sección Entorno > Vista de red > Enlace y se pueden ver de forma más gráfica en la sección Entorno > Vista de red > Gráfico.

Page 1 of 8, 186 entries									Export	Live	11 selected
ACTIONS	FROM	TO	PROTOCOL	LAST ACTIVITY	# ALERTS	THROUGHPUT	TRANSFERRED BYTES	TRANSFERRED PKT			
	00:16:b9:49:b6:7d	01:80:c2:00:00:0e	lldp	2017-02-16 13:57:47.709	0	0.0 b/s	178.0 B	1 pp			
	172.16.66.53	192.168.162.53	smb	2016-11-22 03:00:09.105	0	0.0 b/s	394.0 B	1 pp			
	192.168.162.22	192.168.1.29	ethernetip	2017-01-05 18:13:55.348	0	0.0 b/s	25.4 KB	240 pp			
	192.168.162.22	192.168.1.32	ethernetip	2017-01-05 18:13:55.348	0	0.0 b/s	25.4 KB	240 pp			
	192.168.162.22	192.168.1.33	ethernetip	2017-01-05 18:13:55.348	0	0.0 b/s	25.4 KB	240 pp			
	192.168.162.22	192.168.1.31	ethernetip	2017-01-05 18:13:55.348	0	0.0 b/s	25.4 KB	240 pp			

Figura 5: Una lista de ejemplo de enlaces de red

## Consulta

La sintaxis N2QL (Nozomi Networks Query Language) está inspirada en los lenguajes de programación de terminales de Linux y Unix más comunes: la consulta es una concatenación de comandos individuales separados por | símbolo en el que la salida de un comando es la entrada del siguiente comando. De esta manera, es posible crear un procesamiento de datos complejo al componer varias operaciones simples.

El siguiente ejemplo es una consulta que enumera todos los nodos ordenados por bytes\_recibidos (en orden descendente):

```
nodos | orden recibido.bytes desc
```

Para obtener una referencia de la interfaz gráfica de usuario o cómo puede crear/editar consultas, vaya a [Consulta: Referencia de la interfaz de usuario](#)

Para obtener una referencia completa de comandos, fuentes de datos y ejemplos del lenguaje de consulta, vaya a [Consulta: referencia completa](#)

## Protocolo

En el Entorno un enlace puede comunicarse con uno o más protocolos. Un protocolo puede ser reconocido por el sistema simplemente por la capa de transporte y el puerto o por una inspección profunda de los paquetes de su capa de aplicación.

### Mapeo de protocolos SCADA

Todos los protocolos SCADA se reconocen mediante una inspección profunda de paquetes y para cada uno de ellos existe una asignación que aporta conceptos específicos del protocolo al modelo de variable de entorno más genérico y flexible.

Como ejemplo de tales asignaciones, considere la siguiente tabla:

Protocolo	ID de RTU	Nombre
modbus	Identificador de unidad	(r dr c di)<dirección de registro>
CEI 104	dirección común	<ioa>-<byte alto>-<byte bajo>
Siemens S7 (temporizador o área de mostrador)	Fijo a 1	(C T)<dirección>
Siemens S7 (área DB o DI)	Fijo a 1	(DB DI)<número de db>.<tipo>_<posición de byte>.<posición de bit>
Siemens S7 (otras áreas)	Fijo a 1	(P  Q M L).<tipo>_<posición de byte>.<posición de bit>
Anuncios de Beckhoff	<AMSNelId> Destino><Puerto AMS Objetivo>	<Grupo de índice>/<Desplazamiento de índice>
y más...		

# Capítulo

# 3

---

## Referencia de la interfaz de usuario

---

Temas:

- [Navegadores web compatibles](#) •
- [Encabezado de navegación](#)
- [Vista de activos](#)
- [Vista de red](#) •
- [Consultas](#) •
- [Sistema](#) •
- [Consultas](#)

En este capítulo describiremos todos los aspectos de la interfaz gráfica de usuario. Para cada vista de la GUI, adjuntamos una captura de pantalla con una referencia que explica el significado y el comportamiento de cada control de la interfaz.

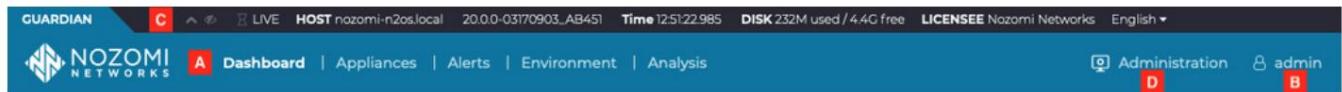
## Navegadores web compatibles

Para tener la mejor experiencia con la consola web de Nozomi Networks Solution, asegúrese de usar uno de los siguientes navegadores web:

- [Google Chrome](#) versión 48 y posteriores • [Cromo](#) versión 48 y posteriores
- [Safari](#) versión 9.0 y posteriores (para macOS) • [Firefox](#) versión 49 y posteriores
- Microsoft Internet Explorer versión 11 • Microsoft Edge versión 12 y posteriores

## Encabezado de navegación

La barra de navegación siempre está presente en la parte superior de la interfaz de usuario de Nozomi Networks Solution. Permite al usuario navegar por las páginas y también muestra información útil sobre el estado del sistema.



A	Las secciones de la Solución Nozomi Networks; haciendo clic en ellos cambiarás de página
B	El menú de usuario; haciendo clic en él puede cerrar sesión o acceder a la página Otras acciones
C	<p>La barra de navegación secundaria con:</p> <ul style="list-style-type: none"> <li>• el botón de colapso: haga clic en él para reducir la altura de la barra de navegación • el botón de modo de monitoreo: haga clic en él para deshabilitar el cierre de sesión automático</li> <li>• el estado de la máquina del tiempo: es EN VIVO, si los datos mostrados son en tiempo real, o una marca de tiempo cuando se carga una instantánea de Time Machine • el nombre de host</li> <li>• la versión N2OS</li> <li>• el desplazamiento NTP • estadísticas del disco, es decir, el espacio utilizado y el espacio disponible • la información de la licencia • el selector de idioma</li> </ul>
D	El botón que muestra el menú de administración.

Figura 6: El menú de administración

## Vista de activos

Page 1 of 7,165 entries						
ACTIONS	NAME	TYPE	OS/FIRMWARE	IP	MAC ADDRESS	MAC
	MACH-666666	switch	Firmware: 09.0.06		[multiple]	Hirschman
	ACMEincHQ_SW1	switch	Firmware: h.10.38		[multiple]	ProCurve N
	172.16.66.53	computer	Windows XP SP3	172.16.66.53		
	ACMEincHQ_SW2	switch	Firmware: V05.01.03		[multiple]	Siemens A
	192.168.162.22	computer	Windows XP SP3	192.168.162.22		
	Modicon M340 BMX P34 2020	PLC	Firmware: 2.90	172.16.0.157		
	Modicon M340 BMX P34 2020	PLC	Firmware: 2.90	172.16.1.174		

Figura 7: La tabla de Activos

En esta página se listan todos los Activos usando una [tabla](#). Al hacer clic en el enlace de un activo, es posible ver una ventana emergente con algunos detalles adicionales sobre el activo.

The screenshot shows a detailed view of the ControlLogix 1756-ENBT/A asset. The top section displays basic device information: IP: 192.168.1.29, Roles: slave, Firmware version: 18.002, Serial number: 00112232, and Type: PLC. It also shows MAC address: 00:0:dc:85:12:02, Product name: ControlLogix 1756-ENBT/A, Vendor: Rockwell Automation/Allen-Bradley, and MAC vendor: RuggedCom Inc. Below this, there are tabs for Overview, Sessions, Alerts, Patches, and Vulnerabilities. The Overview tab is selected, showing Network Stats (Received: 13.6 KB, Sent: 2.00 KB, Retransmission: 0.000%, Links: 1), Network Location (Zone: Undefined, Subnet: -, VLAN: -), and Protocols (Protocol: ethernetip, Last activity: 2017-01-05 18:13, Inbound: -, Outbound: -). The Learning status section indicates the node is not learned and asset intelligence is active. The Security section shows 16 vulnerabilities and 2 antivirus entries. The Hardware components section lists three components: 1756-L61/B LOGIX5561 (Address 0), 1756-RM2/A REDUNDANCY MODULE (Address 1), and 1756-ENBT/A (Address 3), each with their respective details.

Figura 8: La ventana emergente de detalles del activo

## Vista de red

### Nodos de red

Network view									Nodes	Links	Sessions	Graph	Traffic
Page 1 of 8, 185 entries / sorted by roles: asc									Export	Live	9 selected		
ACTIONS	ADDRESS	LABEL	ROLES	MAC ADDRESS	SENT BYTES	RECEIVED BYTES	# LINKS	PROTOCOLS					
		<img alt="Server											

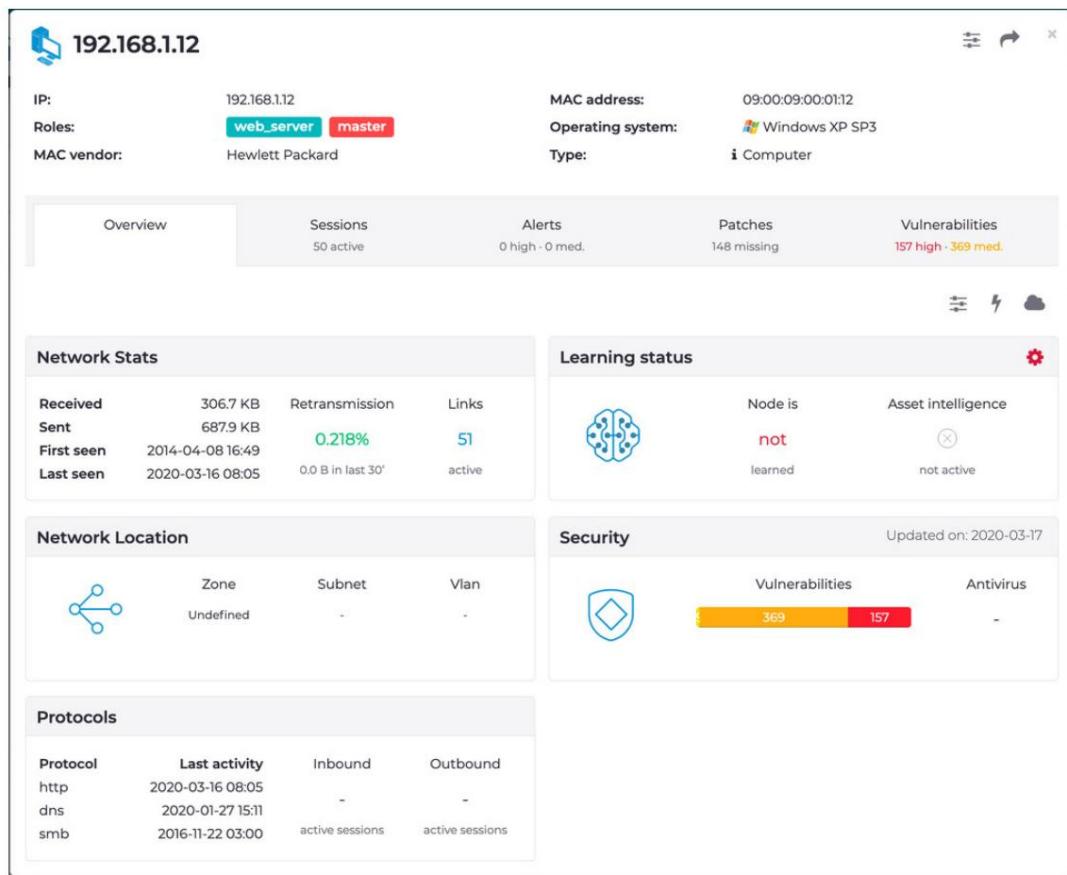


Figura 10: La ventana emergente de detalles del nodo

## Enlaces de red

Page 1 of 8,186 entries									Export	Live	Selected
ACTIONS	FROM	TO	PROTOCOL	LAST ACTIVITY	# ALERTS	THROUGHPUT	TRANSFERRED BYTES	TRANSFERRED PAC			
	00:16:b9:49:b6:7d	01:80:c2:00:00:0e	lldp	2017-02-16 13:57:47:709	0	0.0 b/s	178.0 B	1 pp			
	172.16.66.53	192.168.162.53	smb	2016-11-22 03:00:09:105	0	0.0 b/s	394.0 B	1 pp			
	192.168.162.22	192.168.1.29	ethernetip	2017-01-05 18:13:55.348	0	0.0 b/s	25.4 KB	240 pp			
	192.168.162.22	192.168.1.32	ethernetip	2017-01-05 18:13:55.348	0	0.0 b/s	25.4 KB	240 pp			
	192.168.162.22	192.168.1.33	ethernetip	2017-01-05 18:13:55.348	0	0.0 b/s	25.4 KB	240 pp			
	192.168.162.22	192.168.1.31	ethernetip	2017-01-05 18:13:55.348	0	0.0 b/s	25.4 KB	240 pp			

Figura 11: La tabla de enlaces

Esta página muestra todos los enlaces en el Medio Ambiente.

Además de la información del enlace, hay una columna de Acciones que permite al usuario obtener más información sobre un enlace, aquí hay una explicación:

## Sesiones de red

Page 1 of 12,293 entries											Export	Live	Selected
ACTIONS	STATUS	FROM	TO	TRANSPORT PROTOCOL	FROM PORT	TO PORT	PROTOCOL	THROUGHPUT	TRANSFERRED BYTES	TRANSFER			
	ACTIVE	10.51.253	10.4.1.32	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp			
	ACTIVE	10.51.253	10.4.1.34	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp			
	ACTIVE	10.51.253	10.4.1.30	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp			
	ACTIVE	10.51.253	10.4.1.31	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp			
	ACTIVE	10.51.253	10.4.1.35	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp			
	ACTIVE	10.51.253	10.4.1.36	tcp	51183	554	rtsp	0.0 b/s	79.0 KB	76 pp			

Figura 12: La tabla de Sesiones

En esta página se listan todas las [Sesiones](#) usando una [tabla](#). Al hacer clic en los identificadores de nodo Desde o Hasta, se muestran detalles adicionales sobre los nodos involucrados. Los botones de la columna Acciones permiten al usuario preguntar o ver los seguimientos y navegar por la interfaz de usuario. En las otras columnas hay información detallada sobre cada sesión, como los puertos de origen y destino, la cantidad de paquetes o bytes transferidos, etc.

## Gráfico de red

La página del gráfico de red ofrece una descripción general visual de la red. En el gráfico, cada vértice representa un nodo de red, mientras que cada borde representa uno o varios enlaces entre nodos. Los bordes y vértices se anotan para brindar información sobre la identificación del nodo, los protocolos utilizados en las comunicaciones entre dos nodos y más. El contenido del gráfico se puede filtrar utilizando diferentes criterios para obtener una representación más clara o para evidenciar aspectos específicos.

La posición de los nodos en el gráfico está determinada por un diseño específico o un algoritmo de ajuste automático dinámico que busca la mínima superposición y la mejor legibilidad de los elementos.

Para visualizar mejor los nodos/enlaces deseados, el usuario puede mover y hacer zoom en el gráfico usando el ratón.

Mover	Para mover el gráfico, haga clic en algún lugar, no en un nodo, y comience a arrastrar
Zoom (modo 1)	con el mouse dentro de la ventana, gire la rueda del mouse hacia arriba y hacia abajo para acercar y alejar (desplazamiento). El zoom se centrará en la posición del mouse.
Zoom (modo 2)	Arrastre en dirección vertical mientras mantiene presionada la tecla 'z'. El zoom se centrará en la posición donde comenzó a arrastrar el mouse

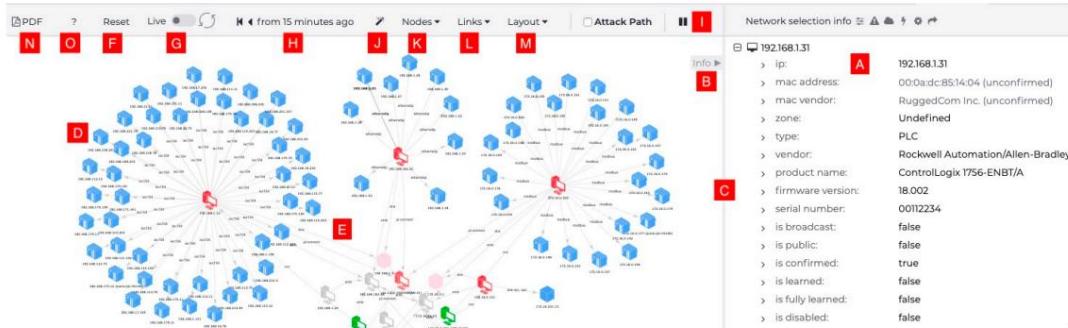


Figura 13: El gráfico de red de entorno que muestra información para el nodo seleccionado

A	El panel de información contiene los detalles sobre el elemento seleccionado, que es un nodo o un enlace
B	El botón para alternar el panel de información
C	Arrastre esta línea vertical con el mouse para cambiar el tamaño del panel de información
D	un nodo
mi	Un enlace
F	El botón para restablecer todas las personalizaciones y recargar los datos.
G	El botón para actualizar los datos; mantiene las personalizaciones actuales
H	El botón para filtrar por tiempo de actividad
I	El botón para alternar el movimiento de ajuste dinámico de los elementos
J	El botón de la varita mágica abrirá un asistente para ayudar al usuario a filtrar el gráfico y ver solo la información deseada. Contiene algunas soluciones para reducir el tamaño de un gráfico grande.
K	El botón que configura la apariencia de los nodos.

L	El botón que configura la apariencia de los enlaces.
MENU	El botón que permite seleccionar un diseño de gráfico.
reporte	El botón que exporta un informe en PDF que contiene el gráfico. Observe que el gráfico se exporta como se muestra actualmente en la página.
O	El ? botón se explica a continuación.

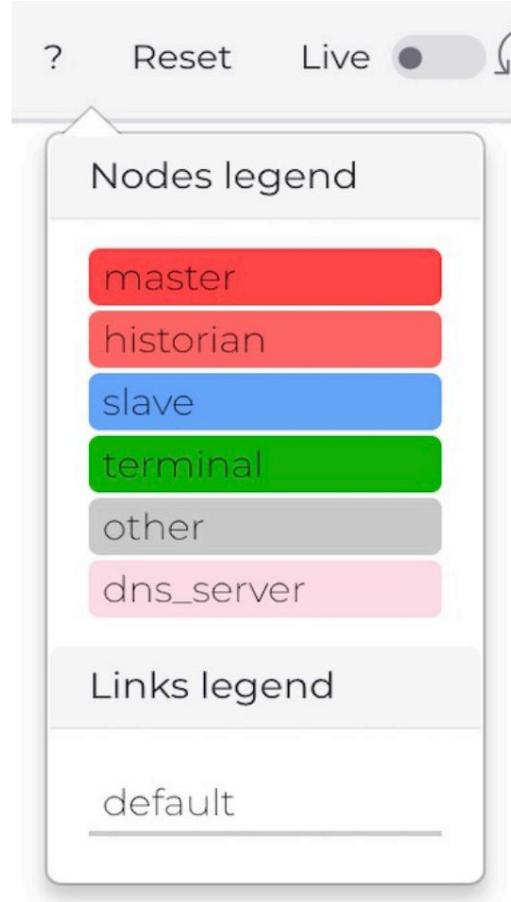


Figura 14: Al hacer clic en el ? El botón mostrará la leyenda para el enlace y los nodos. El contenido de la leyenda es consciente de las perspectivas seleccionadas

#### Opciones de "varita mágica"

El asistente ayuda al usuario con varios consejos para mejorar el rendimiento del gráfico. Los ajustes anotados con un signo de exclamación naranja se consideran subóptimos. Los pulgares verdes anotan opciones cuya configuración se considera útil.

**Graph is big, you can filter to go faster**

**!** Use Google Chrome/Chromium for better performance

**!**  **Show broadcast**  
Hide broadcast nodes to display a simpler graph

**!**  **Only with confirmed data**  
Show only links with confirmed data to display a simpler graph

**!**  **Only confirmed nodes**  
Show only confirmed nodes to display a simpler graph

**!**  **Exclude tangled nodes**  
Tangled nodes will be excluded from graph, they can be reincorporated by removing their IDs from the nodes options

**!** **Protocols**

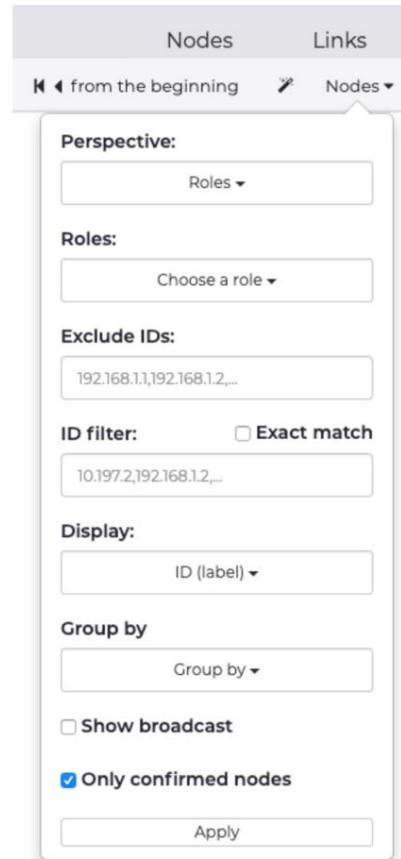
SCADA

Choose a protocol ▾

**OK**

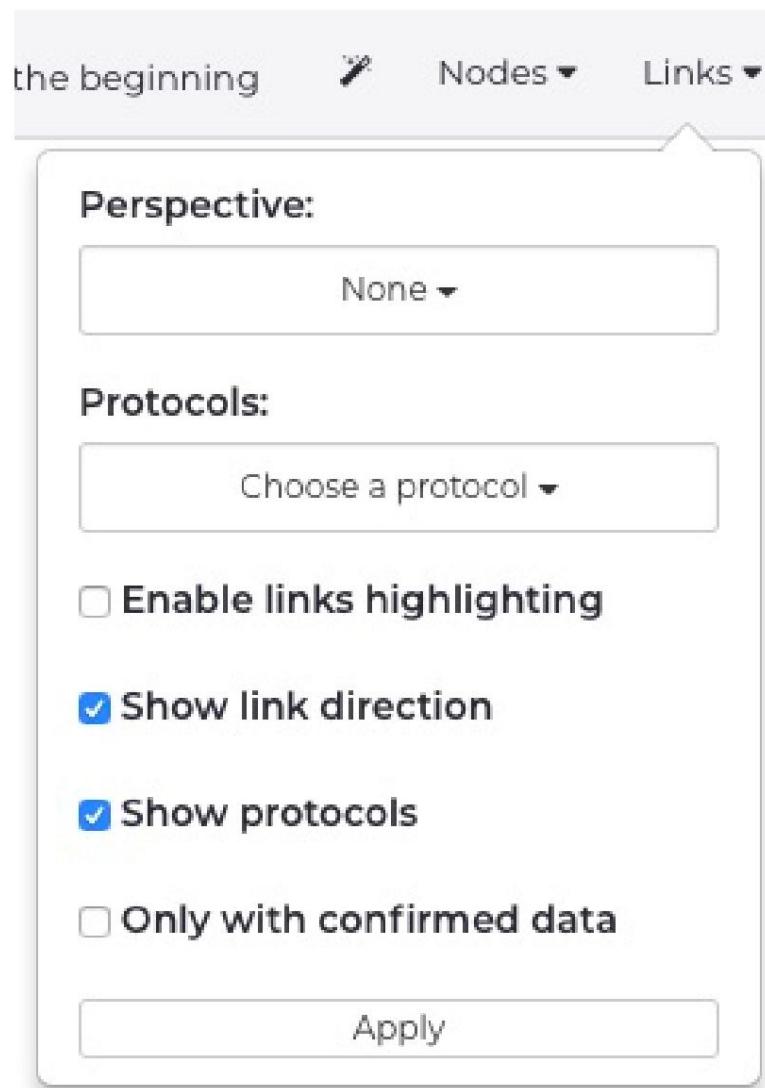
Mostrar difusión Direcciones de difusión no son nodos de red reales en el sentido de que ningún activo es vinculado a una dirección de difusión. Se utilizan para representar las comunicaciones realizadas por un nodo hacia una subred completa. La eliminación de nodos de difusión reduce la complejidad de un gráfico.	
Solo con datos confirmados	Los enlaces no confirmados se pueden ocultar fácilmente para reducir la complejidad de un gráfico enredado.
Solo nodos confirmados	Los nodos no confirmados se pueden ocultar para reducir el tamaño de un gráfico grande.
Excluir nodos enredados	Los nodos cuyas conexiones hacen que el nodo sea demasiado complejo se pueden eliminar para mejorar la legibilidad del gráfico.
protocolos	Los nodos y los bordes se pueden filtrar para mostrar solo aquellos elementos que participan en las comunicaciones que involucran uno de los protocolos seleccionados. Al hacer clic en "SCADA", se seleccionan todos los protocolos SCADA.

## Opciones de nodos



Perspectiva	Cambiar el color de los nodos según un criterio predefinido
roles	Le permite filtrar el gráfico por roles de nodo
Excluir identificaciones	Eliminar los ID especificados de la vista de gráfico; es posible especificar más ID separados por coma
filtro de identificación	El gráfico se puede filtrar por una o más direcciones de ID, separadas por coma
Coincidencia exacta del filtro de ID	Si está marcado, el filtro de ID permitirá que el gráfico muestre solo los nodos con exactamente los ID especificados y no con un criterio de "comenzar con".
Mostrar	Elija el formato de etiqueta de los nodos
Agrupar por	Los nodos con la propiedad elegida (es decir, zona, subred, etc.) se asignan al mismo grupo, luego la forma en que se muestra el grupo depende de la opción elegida en las Opciones de diseño. Con el diseño estándar, cada grupo se muestra contraído como un solo nodo, mientras que con el diseño agrupado, todos los nodos que pertenecen al mismo grupo se colocan dentro de un círculo.
Mostrar transmisión	Si está marcada, incluye en el gráfico todos los nodos con una IP de transmisión
Solo nodos confirmados	Si está marcado, muestra solo los nodos que intercambiaron algunos datos en ambas direcciones mientras se comunicaban

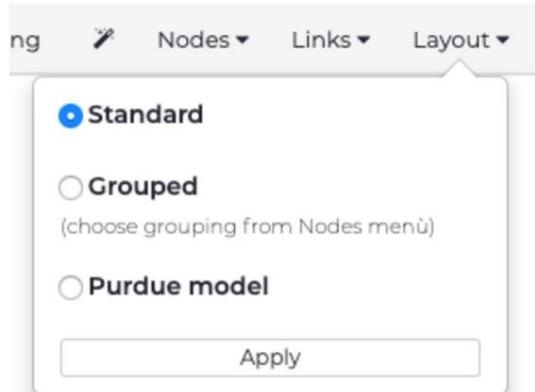
## Opciones de enlaces



Perspectiva	Cambia el color de los enlaces según un criterio predefinido
protocolos	Permite la capacidad de filtrar el gráfico por protocolos de enlace
Habilitar resultado de enlaces	Si está marcado, los enlaces se volverán más audaces en reacción a los movimientos del mouse, lo que hará que el enlace sea más fácil de seleccionar (puede afectar el rendimiento)
Mostrar protocolos	Si está marcado, cada enlace mostrará sus protocolos
Solo con datos confirmados	Si está marcado, muestra solo los enlaces que intercambiaron algunos datos en ambas direcciones

## Opciones de diseño

El diseño define la forma en que los nodos y enlaces se muestran en el gráfico.



Estándar	Es el diseño predeterminado y el tipo de visualización depende de la propiedad Group_by: <ul style="list-style-type: none"><li>• Group_by no definido: se muestran todos los nodos y enlaces</li><li>• Group_by definido: todos los nodos pertenecientes a los mismos grupos se agrupan en un solo nodo</li></ul>
agrupados	Los nodos se agrupan según los criterios definidos en Agrupar_por, y el gráfico se visualiza de la siguiente manera • Agrupar_por no definido: Se muestran todos los nodos y enlaces • Agrupar_por definido: Se muestran todos los nodos pertenecientes a un mismo grupo y se colocan dentro de un círculo que representa el grupo, se muestran enlaces entre nodos que pertenecen al mismo grupo, mientras que los enlaces entre nodos de diferentes grupos se reemplazan por enlaces entre grupos representados como líneas que conectan los círculos
modelo Purdue	Coloca los nodos en grupos separados según su nivel. Esto permite distinguir los diferentes niveles y aislar problemas potenciales debido a comunicaciones que cruzan dos o más límites de nivel.

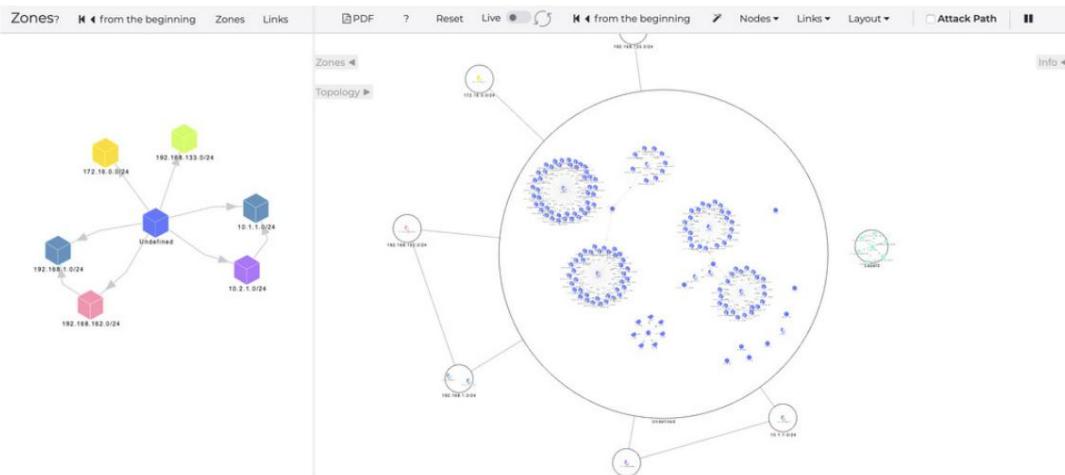


Figura 15: El gráfico de entorno con el panel de zonas abierto con la perspectiva Group\_by=Zones, Layout = Grouped y zone.

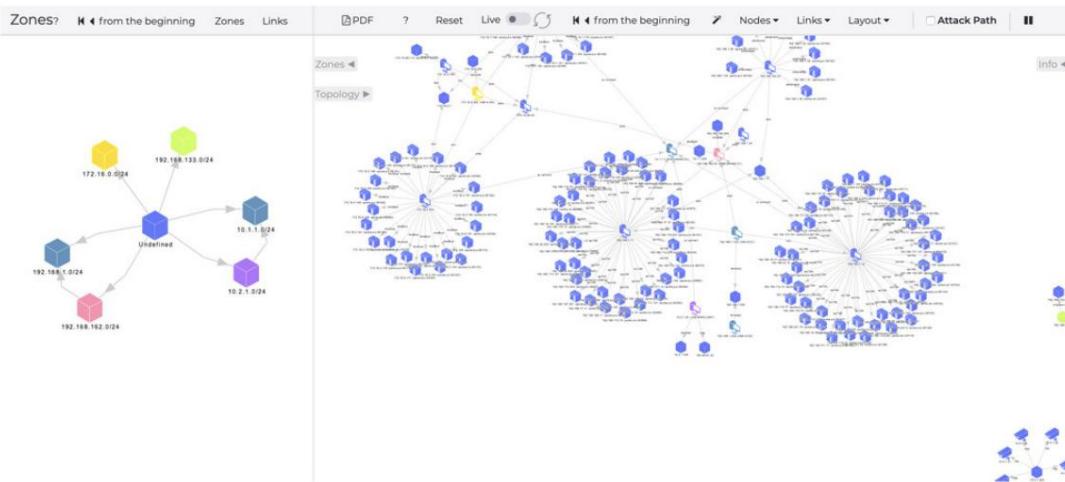


Figura 16: El gráfico de entorno con el panel de zonas abierto y la perspectiva de zonas activa para resaltar la zona de origen de cada nodo.

El panel de zonas ofrece la posibilidad de filtrar el gráfico haciendo clic en una zona o en un enlace entre dos zonas. El gráfico de zonas también tiene una leyenda y comparte algunas de las opciones de nodos y enlaces. Al hacer clic en un nodo o enlace en el panel de zona, se mostrará información adicional sobre la zona o los enlaces entre las zonas. Consulte [las reglas de configuración básicas](#) para personalizar las Zonas.

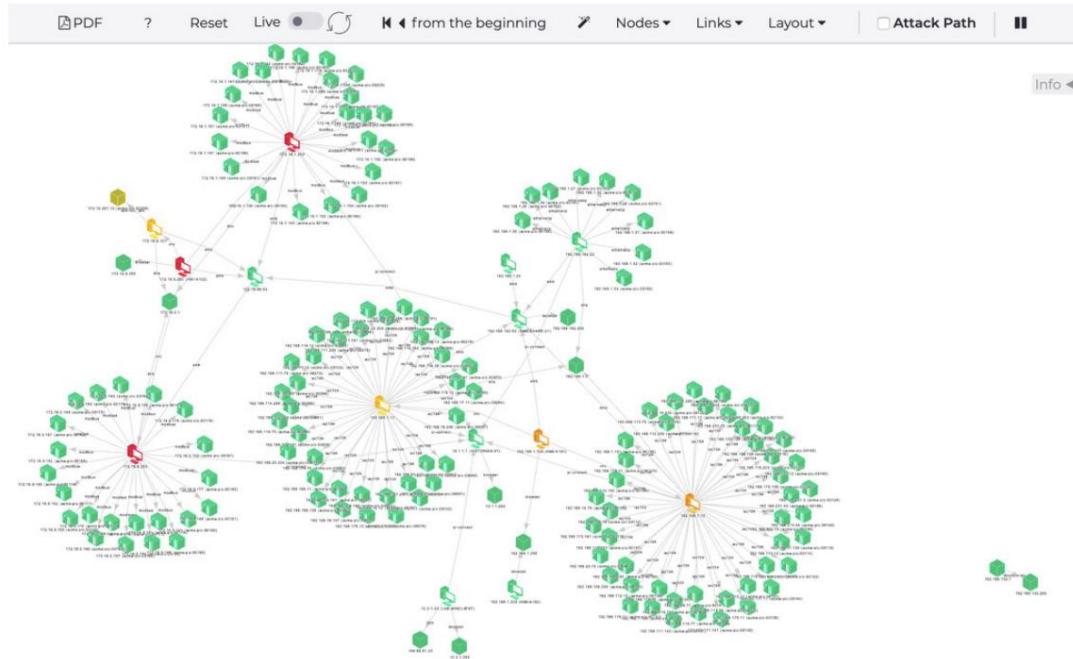


Figura 17: El gráfico de entorno con la perspectiva del nodo de bytes transferidos que destaca el alto uso de tráfico de los nodos maestros

## Tráfico

La pestaña Tráfico en la página Entorno > Vista de red muestra algunos gráficos útiles sobre el rendimiento, los protocolos y las conexiones TCP abiertas.

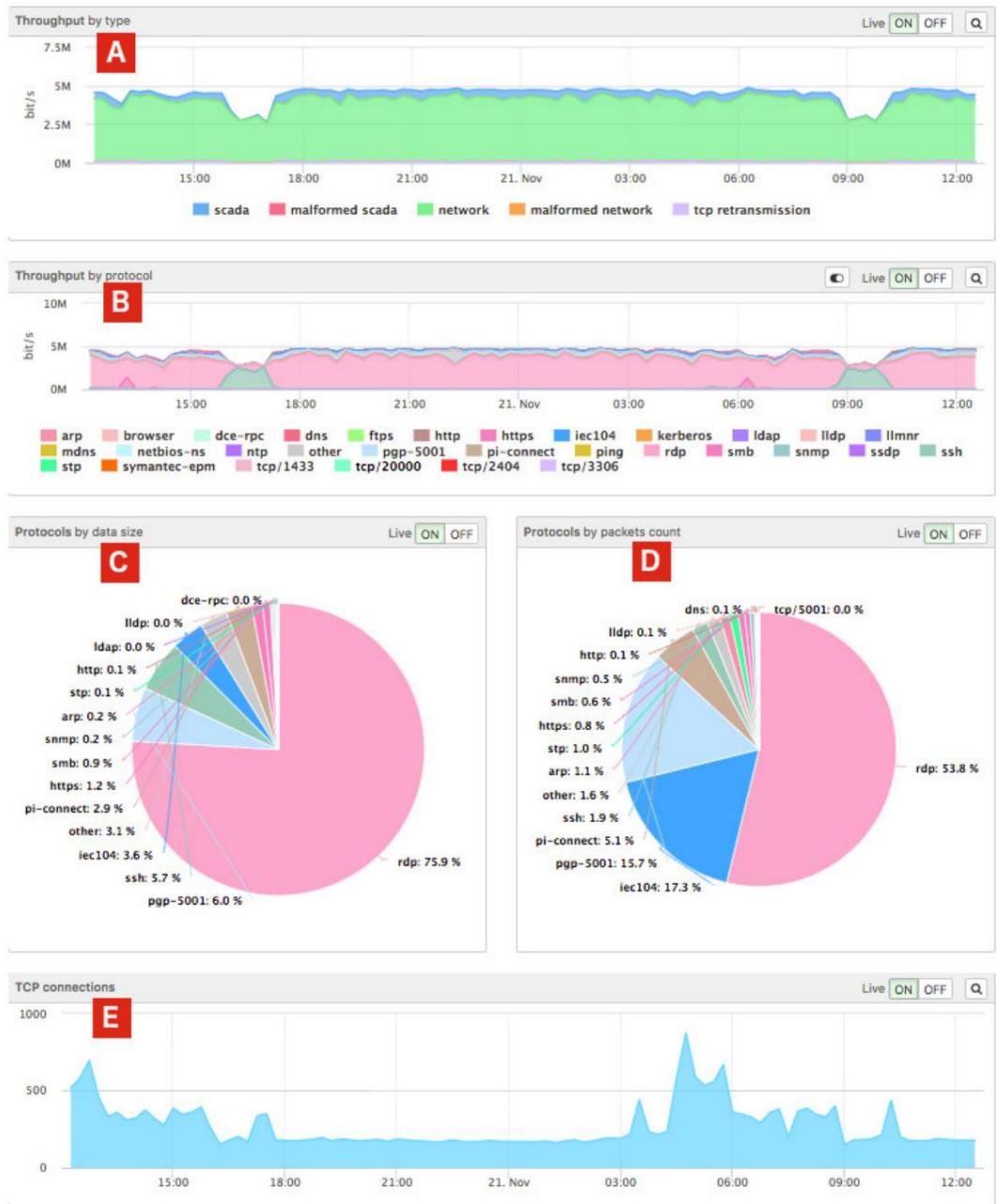


Figura 18: Los gráficos de tráfico

Una explicación de las secciones.

A	El gráfico de rendimiento que muestra el tráfico dividido en macrocategorías
B	El gráfico de rendimiento que muestra el tráfico para cada protocolo
C	Un gráfico circular que muestra las proporciones de los paquetes enviados por protocolo
D	Un gráfico circular que muestra las proporciones del tráfico generado por el protocolo
E	El número de conexiones TCP abiertas

## Consultas

Todas las fuentes de datos de Nozomi Networks Solution se pueden consultar utilizando N2QL (Nozomi Networks Query Language) desde la página de consulta (Análisis > Consultas). En esa página, también puede ver todas las consultas que ya están guardadas en la instalación en ejecución.

Puede elegir entre Estándar (actualmente se ofrece como función beta) y Experto, el primero permite una experiencia más fácil, útil si desea ver rápidamente sus datos, el segundo permite consultas más complejas pero requiere más experiencia.

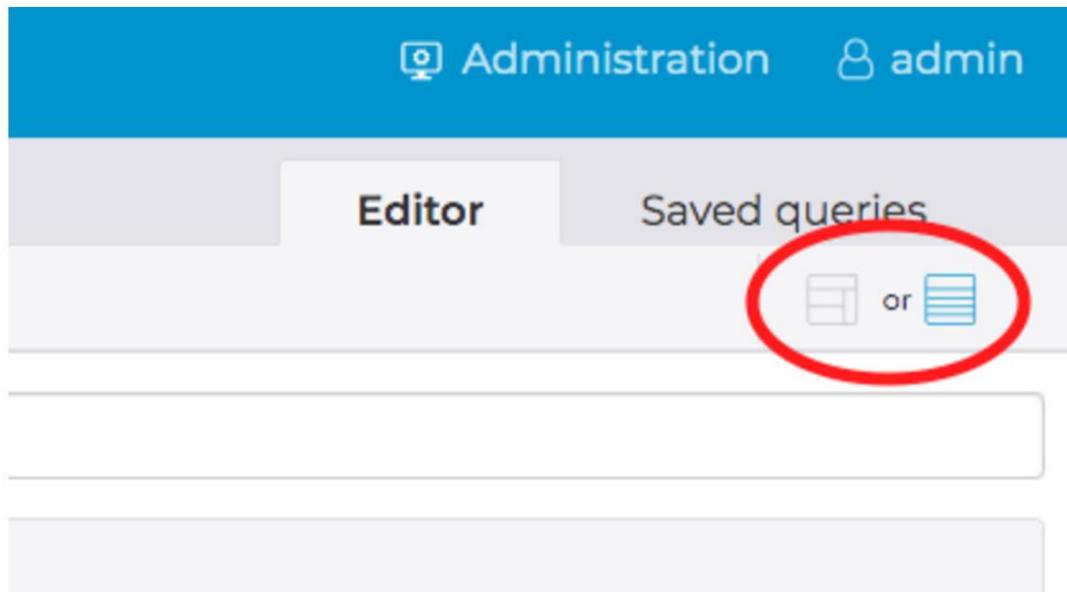


Figura 19: Elija entre Estándar y Experto

Vaya a [Consultas](#) en la página 47 para obtener una referencia completa de los comandos de consulta y las fuentes de datos.

### Consultor de construcción

El generador de consultas permite al usuario crear y ejecutar consultas fácilmente en el sistema observado. Para ello basta con hacer clic en las diferentes opciones.

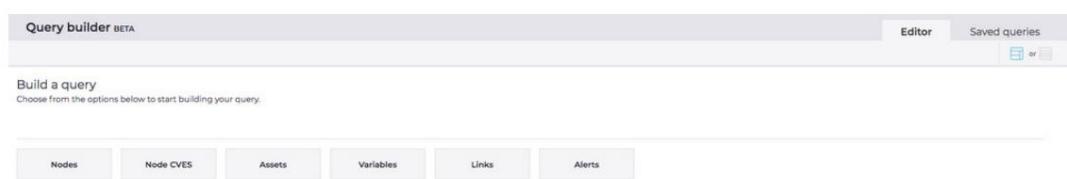


Figura 20: El generador de consultas

Mientras crea su consulta, las opciones disponibles cambian para reflejar sus elecciones, guiándolo a través del proceso.

The screenshot shows the 'Query builder BETA' interface. At the top, there are buttons for 'Editor' and 'Saved queries'. Below that, a section titled 'Build a query' with the sub-instruction 'Choose from the options below to start building your query.' contains several input fields and dropdown menus. One field has 'nodes' selected, followed by 'head 42'. Another dropdown shows 'select [appliance.host, created\_at, id]'. A 'sort' dropdown shows 'sort [created\_at, desc]'. Below these are several icons representing different query operations: 'Group by' (Group results by column), 'Head' (Returns the first n results), 'Join' (Merges two records into one), 'Pie chart' (Shows as a pie chart), 'Select' (Shows selected columns), 'Sort' (Sort results by column), and 'Where' (Filters results by condition). To the right of these icons are buttons for 'To assertion', 'Export', 'Live', and 'Save'. The bottom section is labeled 'Result' and displays a table with the following data:

appliance.host	created_at	id
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:28.760	172.16.55
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:28.285	10.8.1.253
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:26.100	10.4.1.31
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:26.130	10.4.1.30
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:28.285	10.4.1.33

Figura 21: El generador de consultas durante una consulta

## Editor de consultas

El Editor de consultas permite al usuario ejecutar consultas en el sistema observado. Para ejecutar una consulta, simplemente escriba el texto de la consulta en el campo y presione la tecla Intro en el teclado.

The screenshot shows the 'Queries' interface. At the top, there are buttons for 'Editor' and 'Saved queries'. Below that, a search bar says 'Enter your query'. Underneath it, a section titled 'Example queries (click on a query to fill the text box)' lists several pre-defined queries:

- Show a pie chart with the proportion between learned and not learned nodes  
► nodes | group\_by is\_learned | pie is\_learned count
- Show an histogram with received and sent bytes of the first ten nodes by received bytes  
► nodes | sort received-bytes desc | head | column ip sent.bytes received.bytes
- Show the first ten most TCP retransmitting iec104 links  
► links | where protocol == iec104 | sort tcp\_retransmission.bytes desc | head
- Show a pie chart with the proportions of the alert types  
► alerts | group\_by type\_id | sort count desc | pie type\_id count
- Show a pie chart with the average risk by alert type  
► alerts | group\_by type\_id avg risk | sort avg desc | pie type\_id avg
- Show the top ten requested variables  
► variables | sort request\_count desc | head
- Draw a network graph with only the http links, set the node labels to the mac address vendor, coloring the nodes with a 'zones' perspective and the links with a 'transferred bytes' perspective  
► nodes | where\_link protocol == http | graph node\_label:mac\_vendor node\_perspective:zones link\_perspective:transferred\_bytes

Figura 22: El editor de consultas. Algunas consultas de muestra se muestran al principio, al hacer clic en ellas se activará la ejecución

Después de la ejecución, el resultado se mostrará como en la figura a continuación. Si el usuario tiene suficientes privilegios (es decir, pertenece a un grupo con privilegios de administrador), al hacer clic en el icono del disco a la derecha, la consulta se guardará y se mostrará en la sección Consultas guardadas; de lo contrario, el botón se desactivará . Para guardar una consulta, debe especificar una descripción y un grupo. Los resultados de la consulta se pueden exportar haciendo clic en el botón Exportar y eligiendo entre el formato Excel o CSV. El archivo correspondiente se producirá en segundo plano (para facilitar la producción de consultas con gran cantidad de datos) y se puede recuperar a través del submenú Lista de exportaciones, una vez que esté listo. Cuando se descarga una exportación, se elimina automáticamente del sistema de archivos.

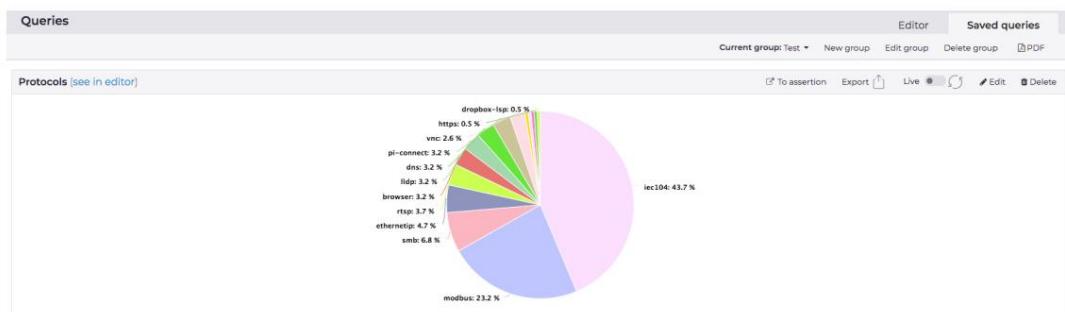


Figura 23: El Editor de consultas durante una consulta

## Consultas guardadas

Cuando se guarda una consulta, se mostrará en la sección Consultas guardadas. Aquí, utilizando el selector de grupo, es posible cambiar el grupo actual y restringir la vista a las consultas del grupo elegido.

Los grupos de consultas, un método simple pero poderoso para organizar las consultas, pueden ser creados, renombrados y eliminados solo por usuarios administradores. Cuando se elimina un grupo, se eliminarán todas las consultas contenidas en él.

Al hacer clic en el icono del bolígrafo, es posible cambiar la descripción y/o el grupo de una consulta. Al hacer clic en el icono de la papelera, se eliminará la consulta guardada. En cuanto a las acciones de guardado, el usuario requiere privilegios de administrador para realizar tales operaciones.

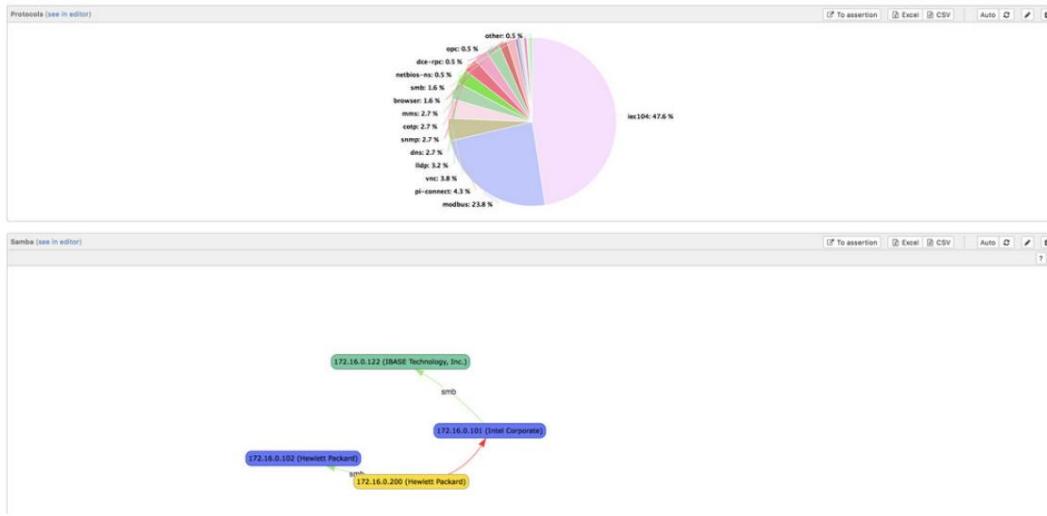


Figura 24: Las consultas guardadas

## Sistema

### General

En la página Administración > General es posible cambiar el nombre de host del dispositivo y especificar un banner de inicio de sesión. El banner de inicio de sesión es opcional y, cuando se configura, se muestra en la página de inicio de sesión y al comienzo de todas las conexiones SSH.

The screenshot shows a configuration interface with a 'General' tab at the top. Below it, there are two input fields: 'Hostname' containing 'nozomi-guardian' and 'Login banner' containing 'Example login banner'. At the bottom is a blue 'Save' button.

Figura 25: Los campos de entrada del banner de nombre de host y de inicio de sesión

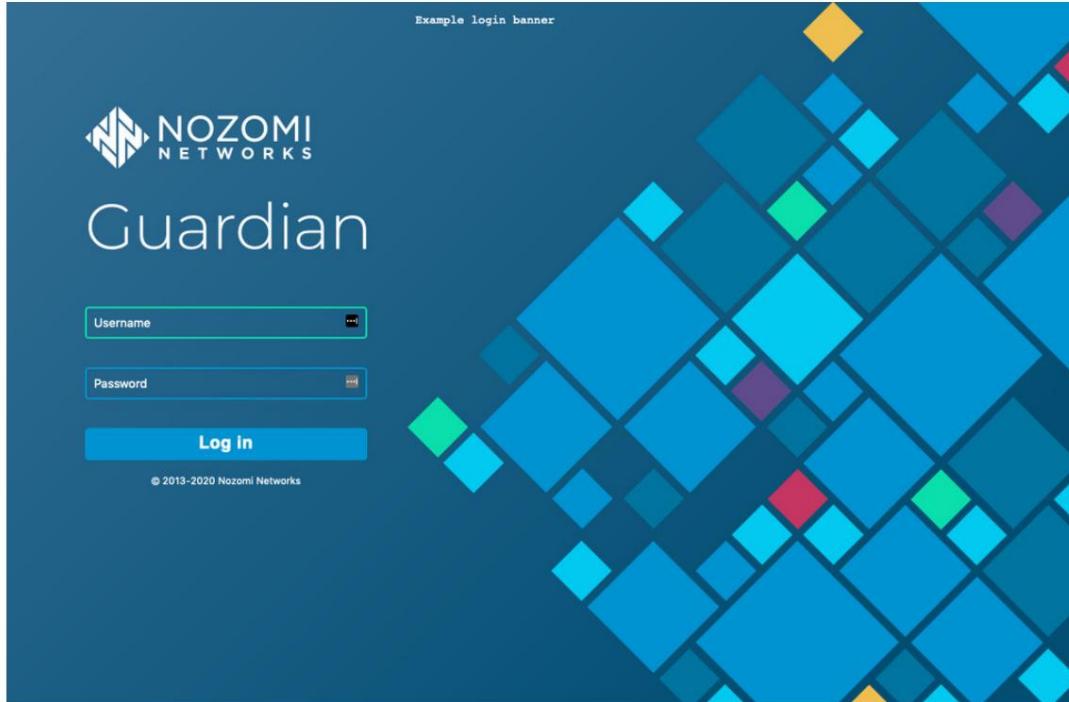


Figura 26: Un ejemplo de banner de inicio de sesión

### Fecha y hora

## Date settings

**Timezone**

Local: CET (UTC+02:00) ▾

**Save**

**Date (format ccyyymmddHHMM.ss)** **Pick a date** **Set as client**

201907250932.16

**Save**

**NTP**

**Enabled**

**Servers**

0.freebsd.pool.ntp.org,1.freebsd.pool.ntp.org

**Save**

Figura 27: Panel de configuración de fecha y hora

Desde la página de fecha y hora puede:

- cambiar la zona horaria del dispositivo
- cambiar la hora actual del dispositivo (puede usar los botones Elegir una fecha o Establecer como cliente para fijar una fecha de forma sencilla)
- habilitar o deshabilitar la sincronización de tiempo con un servidor NTP escribiendo una lista de direcciones del servidor

## Interfaces de red



Figura 28: Lista de interfaces de red

Comportamiento	Con el botón de configuración, puede definir/modificar la regla NAT que se aplicará a la interfaz actual.
Interfaz	El nombre de la interfaz
es espejo	Es cierto si es probable que la interfaz reciba tráfico espejo y no solo transmisión.
filtro de gestión	Cuando está activado, el tráfico del dispositivo se filtra. Está activado de forma predeterminada. Para cambiar el valor, consulte la regla de configuración específica en <a href="#">Reglas de configuración básicas</a> .
filtro BPF	El filtro BPF aplicado al tráfico rastreado.
NAT	La regla NAT aplicada a la interfaz actual.

En este formulario puede establecer la configuración NAT y el filtro BPF.

Configure interface

**Interface**  
em4

**NAT**

**Original subnet**  
e.g. 192.168.0.0 e.g. 192.168.0.0

**Translated subnet**  
e.g. 10.1.0.0

**CIDR mask**  
e.g. /16

💡 This rule allow the rewriting of source and destination IPs of packets sniffed on this interface.  
▪ e.g. to translate 192.168.1.100 in 10.1.1.100 you have to configure the rule: 192.168.0.0 10.1.0.0 /16

**BPF filter** Delete

**BPF filter editor**

Manual insertion of a custom filter expression (host not 10.0.2.15) and (host not 10.0.1.10)

**Save** **Cancel**

Figura 29: Formulario de configuración de la interfaz

En la parte NAT puede configurar la subred original, la subred de destino y la máscara CIDR para la regla NAT.

En la parte del filtro BPF puede configurar el filtro para aplicar a esta interfaz. Hay dos formas de configurar el filtro, a través de un editor visual o manualmente. Al hacer clic en el "Editor de filtros BPF" aparece el siguiente editor visual. Es posible editar los filtros más comunes.

**BPF filter editor**  
This editor supports the most common BPF syntax. If you wish to enter an advanced filter please use the "Manual insertion" from the previous window.

**NOT AND OR**

**Current BPF Filter**  
(not (host 10.0.2.15)) and (not (host 10.0.1.10))

**Ok** **Cancel**

Figura 30: Editor de filtros BPF

Se pueden insertar filtros más complejos manualmente en el cuadro de entrada haciendo clic en el interruptor.

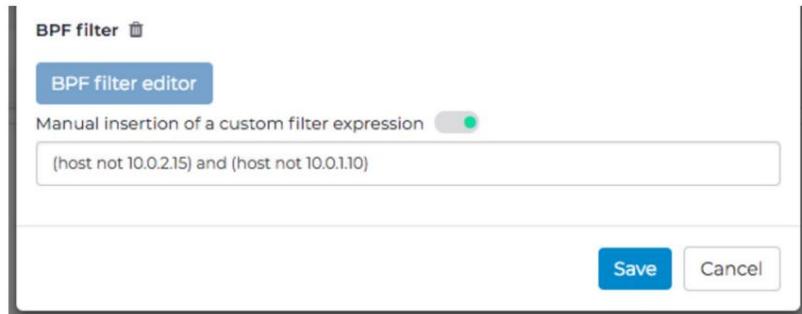


Figura 31: Inserción manual de un filtro BPF

## Subir PCAP

En la página Administración > Cargar PCAP, puede reproducir un archivo PCAP en Guardian, el dispositivo ingiere el tráfico como si viniera a través de la red.

The screenshot shows the 'Upload PCAPs' interface. At the top, there are three options: 'Use PCAP timestamps' (checked), 'Delete data before play' (unchecked), and 'Auto play PCAP after upload' (unchecked). Below this is a large text input field with the placeholder 'Drop a PCAP here or click to upload'. A note below it states 'Supported formats: PCAP and PCAPNG - Maximum file size: 2G'. At the bottom, there's a section titled 'Last uploaded PCAPs' with a table header: 'ACTIONS LAST UPLOADED TI... LAST PLAYED TIME FILENAME NOTE USERNAME'. The table body is currently empty, showing 'No PCAP uploaded yet'.

Además, hay banderas que puede usar para personalizar el comportamiento de la acción de cargar/reproducir.

Usar marcas de tiempo de PCAP	Marque esto si desea utilizar el tiempo capturado en el archivo PCAP. De lo contrario, se utiliza la hora actual.
Eliminar datos antes de jugar	Marque esta opción si desea eliminar todos los datos del dispositivo antes de ejecutar la acción de reproducción.
PCAP de reproducción automática después de la carga	Con esta bandera habilitada, el PCAP se reproduce inmediatamente después de la carga.

En cada archivo PCAP cargado, hay algunas acciones disponibles, como se muestra a continuación.

The screenshot shows the 'Last uploaded PCAPs' interface with one entry: 'base'. The table columns are: 'ACTIONS LAST UPLOADED TI... LAST PLAYED TI... FILENAME NOTE USERNAME'. The 'ACTIONS' column for the 'base' entry contains icons for play, stop, and refresh. The 'FILENAME' column shows 'base'. The 'NOTE' and 'USERNAME' columns both show 'admin'.

Reproducir PCAP	Con esta acción puedes reproducir el PCAP.
Editar nota	Si necesita compartir alguna nota sobre el PCAP cargado.
Eliminar de la lista	Borre el archivo PCAP del dispositivo; los datos del entorno no se verán afectados.

Nota: De forma predeterminada, el dispositivo tiene una retención de 10 archivos PCAP. Para configurar este valor, consulte [Configuración de la retención](#)

## Salud

Todas las secciones que se describen a continuación están disponibles para el usuario administrador. Además, se otorga acceso a todos los usuarios con permiso de Salud.

### Actuación

En esta pestaña hay tres gráficos que muestran, respectivamente, el uso de CPU, RAM y disco a lo largo del tiempo.

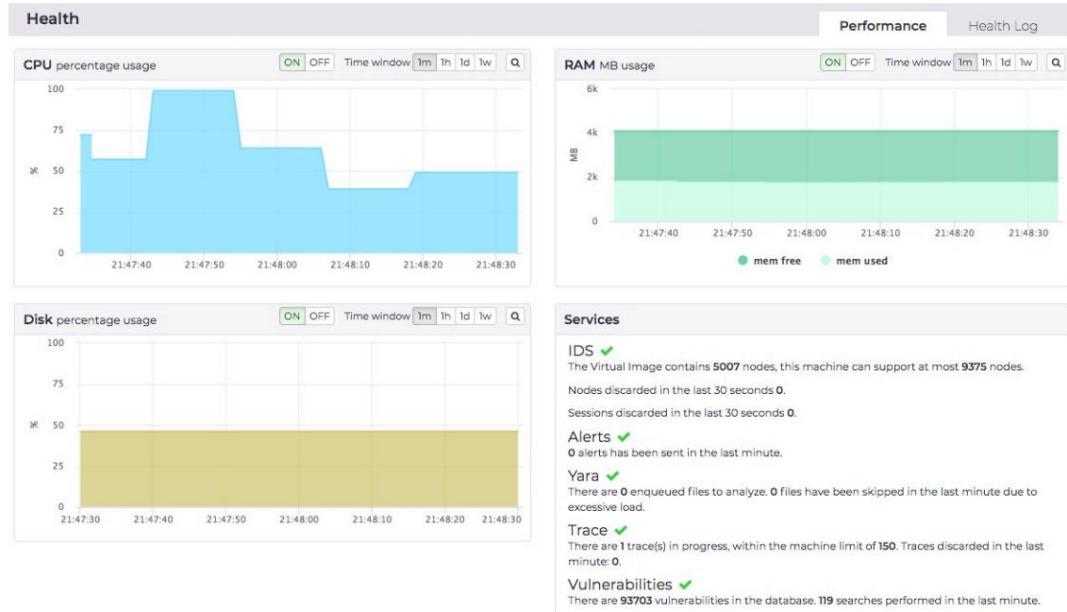


Figura 32: Los gráficos de rendimiento

### Registro de salud

Si hay algún tipo de problema de rendimiento en el dispositivo, aquí puede ver el historial de esos problemas con una pequeña descripción como la cantidad de paquetes, la sesión o los nodos descartados en los últimos 30 segundos.

Health		Performance	Health Log
Page 1 of 30,729 entries		Export	Live
TIME	DESCRIPTION	Description, Time ▾	
H ⏪ ⏩ H			
2018-12-17 12:23:58.343	100% cpu usage		
2018-10-21 22:57:01.761	100% cpu usage		
2018-09-26 03:41:05.379	99% disk space used		
2018-09-26 03:31:01.216	99% disk space used 99% cpu usage		
2018-09-25 22:28:55.947	98% disk space used		
2018-09-25 22:13:49.672	98% disk space used 100% cpu usage		
2018-09-25 17:46:58.364	97% disk space used		

Figura 33: La tabla de registro de salud

### Auditoría

En la página Administración > Auditoría se enumeran todas las acciones relevantes realizadas por los usuarios, desde la acción Iniciar/Cerrar sesión hasta todas las operaciones de configuración, como aprender/eliminar objetos en el entorno.

Todas las acciones registradas están relacionadas con la IP y el nombre de usuario del usuario que realizó la acción y, como se ve en las otras tablas de Nozomi Networks Solution, puede filtrar y ordenar fácilmente estos datos.

Audit				
Page 1 of 1, 8 entries / filtered by time: {"to": "1545162024913", "from": "1545123087186"} <span style="float: right;">Live <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> 5 selected</span>				
ACTIONS	TIME	IP	USERNAME	EVENT
H	↑	↓	Filter	
Q	20:40:11.935	10.41.128.12	admin	Configured rules, rules: ["vi zones delete LocalSCADA"]
Q	20:40:09.884	10.41.128.12	admin	Configured rules, rules: ["vi zones delete VPN_RSA"]
Q	20:38:17.832	10.41.128.12	admin	Configured rules, rules: ["vi zones add 10.197.163.0/24 LocalSCADA"; "vi zones setlevel 2 LocalSCADA"]
Q	20:37:39.528	10.41.128.12	admin	Configured rules, rules: ["vi zones add 10.195.0.0/16 VPN_RSA"; "vi zones setlevel VPN_RSA"]
Q	20:14:06.957	10.41.128.12	admin	User signed in
Q	17:01:07.736	10.41.132.167	admin	User signed in
Q	14:22:31.552	10.41.132.165	admin	User signed in
Q	12:13:31.254	10.41.132.165	admin	User signed in

Figura 34: La tabla de auditoría

## Reiniciar datos

En la página Administración > Datos, es posible restablecer selectivamente varios tipos de datos utilizados por la Solución de redes Nozomi.

Ambiente	Todos los nodos, enlaces y variables aprendidos
Datos de red	Todo el historial de datos de la red visible en los gráficos
Procesar datos	Toda la historia de los datos del proceso visible en los gráficos como la historia de las variables
Datos de activos	Toda la información relacionada con el activo (por ejemplo, versión de software y hardware)
Alertas	Las alertas levantadas
huellas	Los rastros generados tanto por la alerta como por una solicitud del usuario.
Máquina del tiempo	Las instantáneas guardadas por la máquina del tiempo
Consultas	Las consultas y grupos de consultas guardados por cada usuario
afirmaciones	Las afirmaciones guardadas por cada usuario

Además de los botones habituales para seleccionar y deseleccionar todas las casillas, Todo y Ninguno, también hay un botón Solo datos que selecciona todo menos rastros, consultas y aserciones.

Data

Reset different kind of data for all the users

All  Only data  None

Environment  
Reset network nodes, links status and variables

Network Data  
Reset link event history, network charts data and captured urls

Process Data  
Reset the variables history

Assets Data  
Reset the data related to assets

Alerts  
Reset the alerts

Traces  
Reset the traces, both requested by users and generated by alerts

Time machine  
Delete all the snapshots of the time machine

Queries  
Delete all the queries and query groups

Assertions  
Delete all the assertions

Figura 35: El formulario de reinicio de datos

## Consultas

Todas las fuentes de datos de Nozomi Networks Solution se pueden consultar utilizando N2QL (Nozomi Networks Query Language) desde la página de consulta (Análisis > Consultas). En esa página, también puede ver todas las consultas que ya están guardadas en la instalación en ejecución.

Puede elegir entre Estándar (actualmente se ofrece como función beta) y Experto, el primero permite una experiencia más fácil, útil si desea ver rápidamente sus datos, el segundo permite consultas más complejas pero requiere más experiencia.

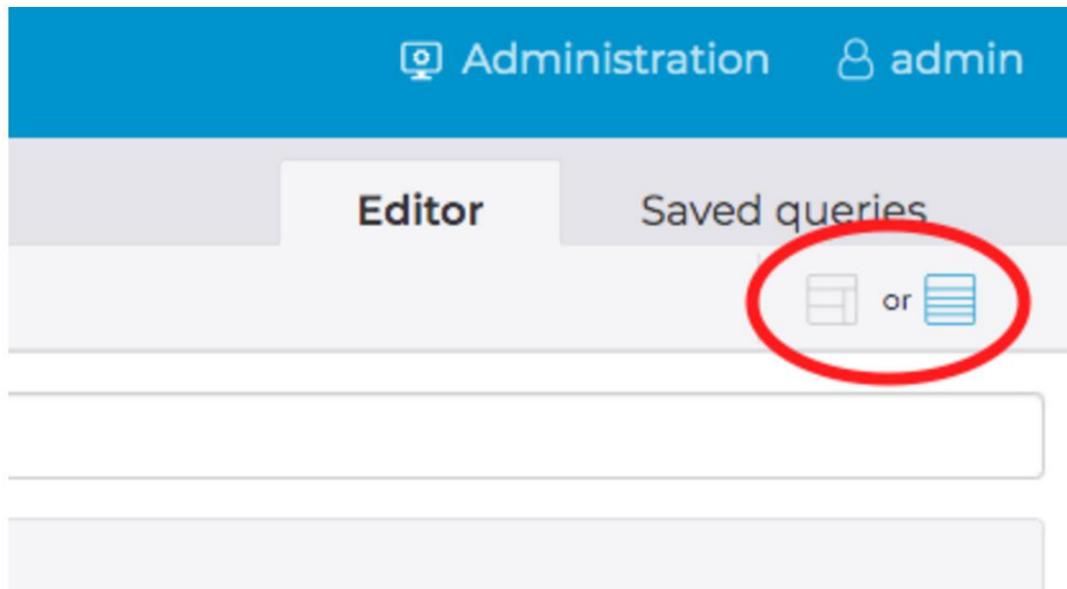


Figura 36: Elija entre Estándar y Experto

Vaya a [Consultas](#) en la página 47 para obtener una referencia completa de los comandos de consulta y las fuentes de datos.

### Consultor de construcción

El generador de consultas permite al usuario crear y ejecutar consultas fácilmente en el sistema observado. Para ello basta con hacer clic en las diferentes opciones.

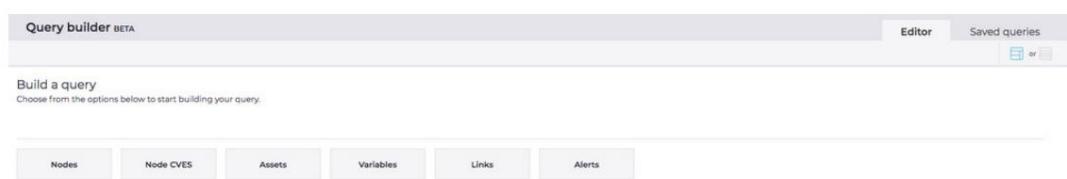


Figura 37: El generador de consultas

Mientras crea su consulta, las opciones disponibles cambian para reflejar sus elecciones, guiándolo a través del proceso.

The screenshot shows the 'Query builder BETA' interface. At the top, there are tabs for 'Editor' and 'Saved queries'. Below the tabs, a search bar says 'Build a query' with the placeholder 'Choose from the options below to start building your query.' A toolbar contains buttons for 'Group by', 'Head', 'Join', 'Pie chart', 'Select', 'Sort', and 'Where'. The main area is titled 'Result' and shows a table with columns 'appliance.host' and 'created\_at'. The table contains five rows of data:

appliance.host	created_at
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:28.760
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:28.765
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:26.101
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:26.102
LAB-sg-upload-PCAPXXXX-vm-master	2018-10-25 11:26:28.763

At the bottom right of the table are buttons for 'To assertion', 'Export', 'Live', and 'Save'.

Figura 38: El generador de consultas durante una consulta

## Editor de consultas

El Editor de consultas permite al usuario ejecutar consultas en el sistema observado. Para ejecutar una consulta, simplemente escriba el texto de la consulta en el campo y presione la tecla Intro en el teclado.

The screenshot shows the 'Queries' interface. At the top, there are tabs for 'Editor' and 'Saved queries'. Below the tabs, a search bar says 'Enter your query'. A section titled 'Example queries (click on a query to fill the text box)' lists several queries:

- Show a pie chart with the proportion between learned and not learned nodes  
► nodes | group\_by is\_learned | pie is\_learned count
- Show an histogram with received and sent bytes of the first ten nodes by received bytes  
► nodes | sort received-bytes desc | head | column ip sent.bytes received.bytes
- Show the first ten most TCP retransmitting iec104 links  
► links | where protocol == iec104 | sort tcp\_retransmission.bytes desc | head
- Show a pie chart with the proportions of the alert types  
► alerts | group\_by type\_id | sort count desc | pie type\_id count
- Show a pie chart with the average risk by alert type  
► alerts | group\_by type\_id avg risk | sort avg desc | pie type\_id avg
- Show the top ten requested variables  
► variables | sort request\_count desc | head
- Draw a network graph with only the http links, set the node labels to the mac address vendor, coloring the nodes with a 'zones' perspective and the links with a 'transferred bytes' perspective  
► nodes | where\_link protocol == http | graph node\_label:mac\_vendor node\_perspective:zones link\_perspective:transferred\_bytes

Figura 39: El editor de consultas. Algunas consultas de muestra se muestran al principio, al hacer clic en ellas se activará la ejecución

Después de la ejecución, el resultado se mostrará como en la figura a continuación. Si el usuario tiene suficientes privilegios (es decir, pertenece a un grupo con privilegios de administrador), al hacer clic en el icono del disco a la derecha, la consulta se guardará y se mostrará en la sección Consultas guardadas; de lo contrario, el botón se desactivará . Para guardar una consulta, debe especificar una descripción y un grupo. Los resultados de la consulta se pueden exportar haciendo clic en el botón Exportar y eligiendo entre el formato Excel o CSV. El archivo correspondiente se producirá en segundo plano (para facilitar la producción de consultas con gran cantidad de datos) y se puede recuperar a través del submenú Lista de exportaciones, una vez que esté listo. Cuando se descarga una exportación, se elimina automáticamente del sistema de archivos.

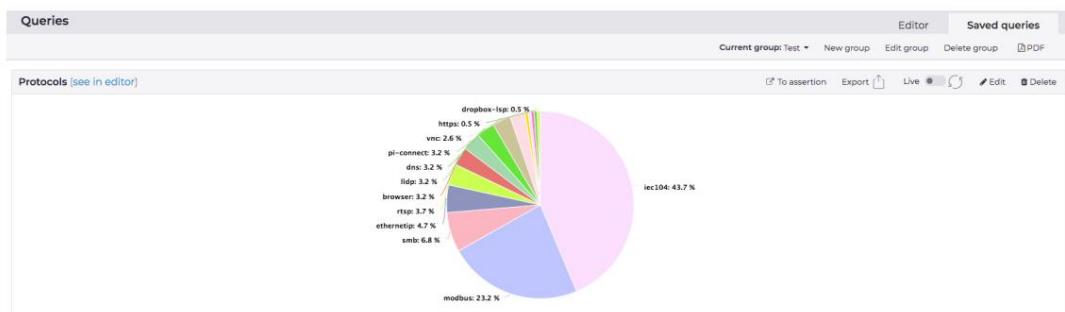


Figura 40: El Editor de consultas durante una consulta

## Consultas guardadas

Cuando se guarda una consulta, se mostrará en la sección Consultas guardadas. Aquí, utilizando el selector de grupo, es posible cambiar el grupo actual y restringir la vista a las consultas del grupo elegido.

Los grupos de consultas, un método simple pero poderoso para organizar las consultas, pueden ser creados, renombrados y eliminados solo por usuarios administradores. Cuando se elimina un grupo, se eliminarán todas las consultas contenidas en él.

Al hacer clic en el icono del bolígrafo, es posible cambiar la descripción y/o el grupo de una consulta. Al hacer clic en el icono de la papelera, se eliminará la consulta guardada. En cuanto a las acciones de guardado, el usuario requiere privilegios de administrador para realizar tales operaciones.

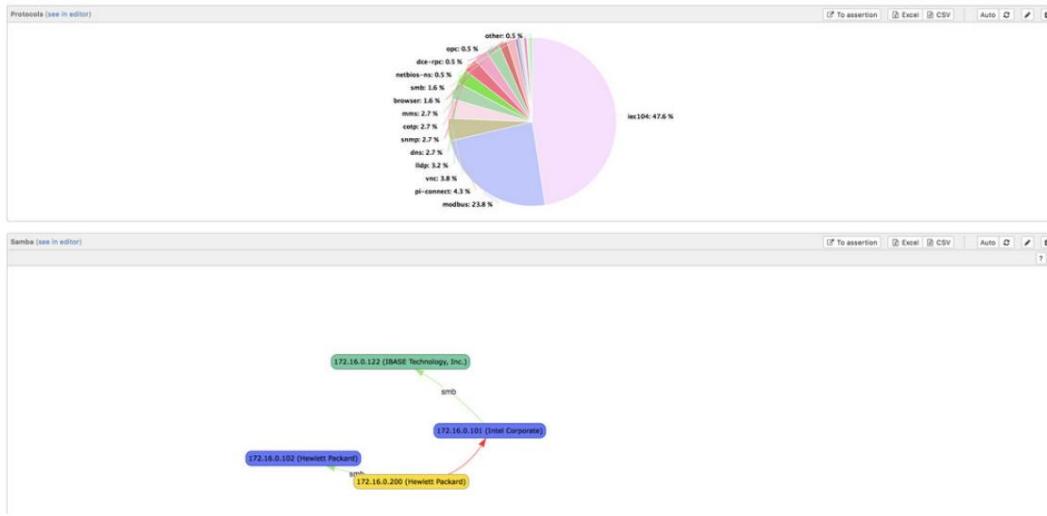


Figura 41: Las consultas guardadas



# Capítulo

# 4

---

## Consultas

---

Temas:

- [Descripción general](#)
- [Referencia](#)
- [Ejemplos](#)

En este capítulo se enumeran todas las [fuentes de datos](#), [comandos](#) y [funciones](#) que se pueden utilizar en N2QL (Nozomi Networks Query Language).

## Descripción general

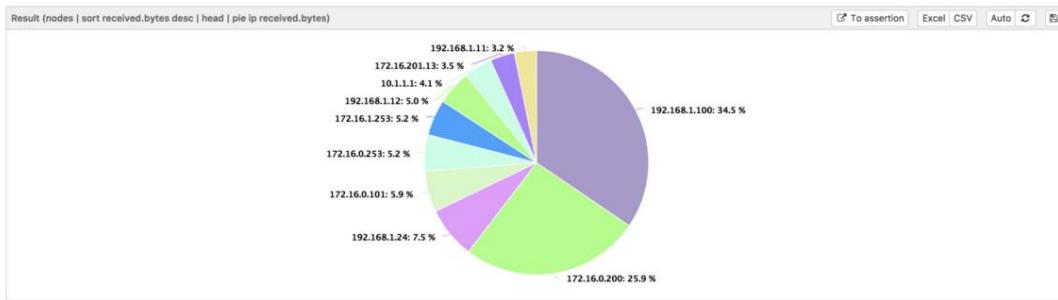
Cada consulta debe comenzar llamando a una [fuente de datos](#), por ejemplo:

```
nodos | ordenar recibido.bytes desc | cabeza
```

mostrará en una tabla los primeros 10 nodos que recibieron la mayor cantidad de bytes.

Al agregar el [comando](#) circular al final, es posible mostrar el resultado como un gráfico circular donde cada segmento tiene la IP del nodo como etiqueta y el campo de bytes recibidos como datos:

```
nodos | ordenar recibido.bytes desc | cabeza | pastel ip recibido.bytes
```



A veces, los comandos de consulta no son suficientes para lograr el resultado deseado. Como consecuencia, la sintaxis de consulta admite [funciones](#). Las funciones le permiten aplicar cálculos en los campos y usar el resultado como un nuevo campo temporal.

Por ejemplo, la consulta:

```
nodos | sort sum(enviado.bytes,recibido.bytes) desc | columna ip sum(enviado.bytes,recibido.bytes)
```

utiliza la función de suma para clasificar los parámetros agregados y producir un gráfico con las columnas que representan la suma de los bytes enviados y recibidos.

## Referencia

### Fuentes de datos

Estas son las fuentes de datos disponibles con las que puede iniciar una consulta:

ayuda	Mostrar esta lista de fuentes de datos
alertas	Todas las alertas levantadas
afirmaciones	Todas las afirmaciones guardadas por los usuarios
activos	Todos los activos identificados en el sistema
URL_capturadas	Todas las urls capturadas de protocolos de red
códigos_función	Todos los códigos de función
Enlaces	Los enlaces en el sistema, cada enlace tiene una asociación uno a uno con un protocolo
enlace_eventos	Los eventos de enlace guardados para cada enlace, por ejemplo, eventos de canal arriba/abajo, parámetros específicos del protocolo, etc.
nodos	Los nodos en el sistema.
nodo_cpes	Todos los CPE (versiones de hardware, sistema operativo y software) detectados en los nodos
node_cpe_cambios	CPE (versiones de hardware, sistema operativo y software) cambios recopilados a lo largo del tiempo
nodo_cvcs	Todas las vulnerabilidades detectadas en los CPE del nodo
sesiones	Todas las sesiones de red actualmente en vivo
Variables	Las variables SCADA de los esclavos
historia_variable	La historia de los valores de las variables
variable_historial_mes	El historial de los valores de las variables dentro del mes especificado
zonas	Los nodos de la zona
zone_links	Los enlaces de la zona

## Comandos

Aquí está la lista completa de comandos:

Sintaxis	select <campo1> <campo2> ... <campoN>
Parámetros	<ul style="list-style-type: none"><li>• la lista de campo(s) para la salida</li></ul>
Descripción	El comando de selección toma todos los elementos de entrada y los genera solo con el campos seleccionados

Sintaxis	excluir <campo1> <campo2> ... <campoN>
Parámetros	<ul style="list-style-type: none"><li>• la lista de campos para eliminar de la salida</li></ul>
Descripción	El comando de exclusión toma todos los elementos de entrada y los genera sin los campos especificados

Sintaxis donde <campo> <==> = <=> = include? start_with? end_with? in_subnet?> <valor>
<p>Parámetros</p> <ul style="list-style-type: none"><li>• campo: el nombre del campo al que se le aplicará el operador</li><li>• operador</li><li>• valor: utilizado para la comparación. Puede ser un número, una cadena o una lista (usando la sintaxis JSON), el motor de consulta comprenderá la semántica</li></ul>
<p>Descripción</p> <p>El comando where enviará a la salida solo los elementos que cumplan criterio especificado, muchas cláusulas se pueden concatenar usando el operador booleano OR</p>
<p>Ejemplo</p> <ul style="list-style-type: none"><li>• nodos   ¿Dónde se incluyen los roles? maestro OR zona == oficina</li><li>• nodos   donde ip en_subnet? 192.168.1.0/24</li></ul>

Sintaxis ordenar <campo> [asc desc]	
Parámetros	<ul style="list-style-type: none"><li>• campo: el campo utilizado para clasificar</li><li>• asc desc: la dirección de clasificación</li></ul>
Descripción	El comando ordenar ordenará todos los elementos según el campo y el dirección especificada, entiende automáticamente si el campo es un número o una cadena

Sintaxis	group_by <campo> [ [promedio suma] [campo2] ]
Parámetros	<ul style="list-style-type: none"><li>• campo: el campo utilizado para agrupar •</li><li>avg sum: si se especifica, la operación relativa se aplicará en campo2</li></ul>

Cabeza de sintaxis [recuento]
Parámetros
• contar: el número de elementos a generar

Sintaxis única
Parámetros
Descripción El comando uniq eliminará de la salida los elementos duplicados
Sintaxis expandir <campo>
Parámetros <ul style="list-style-type: none"><li>• campo: el campo que contiene la lista de valores a expandir</li></ul>
Descripción El comando expandir tomará la lista de valores contenidos en el campo y para cada uno de ellos duplicará el elemento original sustituyendo el valor del campo original con el valor actual de la iteración
Sintaxis sub <campo>
Parámetros <ul style="list-style-type: none"><li>• campo: el campo que contiene la lista de objetos</li></ul>
Descripción El subcomando generará los elementos contenidos en el campo
recuento de sintaxis
Parámetros
Descripción El comando de conteo genera el número de elementos
Gráfico circular de sintaxis <campo_etiqueta> <campo_valor>
Parámetros <ul style="list-style-type: none"><li>• campo_etiqueta: el campo utilizado para cada etiqueta de sector</li><li>• campo_valor: el campo utilizado para el valor del sector, debe ser un número campo</li></ul>
Descripción El comando circular generará un gráfico circular de acuerdo con los parámetros especificados
Columna de sintaxis <campo_etiqueta> <campo_valor...>
Parámetros <ul style="list-style-type: none"><li>• label_field: el campo utilizado para cada etiqueta de columna • value_field: uno o más campos utilizados para los valores de las columnas</li></ul>
Descripción El comando de columna generará un histograma, para cada etiqueta se muestra un grupo de columnas con el valor de los value_field(s) especificados.
Historial de sintaxis <campo_recuento> <campo_tiempo>
Parámetros <ul style="list-style-type: none"><li>• count_field: el campo utilizado para dibujar el valor Y • time_field: el campo utilizado para dibujar los puntos X de la serie temporal</li></ul>
Descripción El comando historial dibujará un gráfico que representa una serie histórica de valores
Sintaxis distancia <id_field> <distancia_campo>
Parámetros <ul style="list-style-type: none"><li>• id_field: el campo utilizado para identificar los datos • distance_field: el campo en el que se calculan las distancias</li></ul>
Descripción El comando de distancia calculará una serie de distancias a partir de la serie original. Cada valor de distancia se calcula como la diferencia entre un valor y su aparición posterior

<p><b>Cubo de sintaxis &lt;campo&gt; &lt;rango&gt;</b></p>
<p><b>Parámetros</b></p> <ul style="list-style-type: none"> <li>• campo: el campo en el que se calculan los cubos</li> <li>• rango: el rango de tolerancia en el que se agrupan los valores</li> </ul>
<p><b>Descripción</b> El comando de cubo agrupará datos en diferentes cubos, diferentes registros se colocarán en el mismo cubo cuando los valores caigan en el mismo múltiplo de &lt;rango&gt;</p>

<p><b>Sintaxis join &lt;otra_fuente&gt; &lt;campo&gt; &lt;otra_fuente_campo&gt;</b></p>
<p><b>Parámetros</b></p> <ul style="list-style-type: none"> <li>• otra_fuente: el nombre de la otra fuente de datos</li> <li>• campo: el campo de la fuente original utilizada para hacer coincidir el objeto a unir</li> <li>• otra_fuente_campo: el campo de la otra fuente de datos utilizada para hacer coincidir la objeto de unirse</li> </ul>
<p><b>Descripción</b> El comando unir tomará dos registros y los unirá en un solo registro cuando &lt;campo&gt; y &lt;otro_campo_origen&gt; tengan el mismo valor</p>

<p><b>Medidor de sintaxis &lt;campo&gt; [min] [max]</b></p>
<p><b>Parámetros</b></p> <ul style="list-style-type: none"> <li>• campo: el valor a dibujar</li> <li>• min: el valor mínimo para poner en la escala de calibre</li> <li>• max: el valor máximo para poner en la escala de calibre</li> </ul>
<p><b>Descripción</b> El comando calibre tomará un valor y lo representará de forma gráfica</p>

<p><b>Valor de sintaxis &lt;campo&gt;</b></p>
<p><b>Parámetros</b></p> <ul style="list-style-type: none"> <li>• campo: el valor a dibujar</li> </ul>
<p><b>Descripción</b> El comando de valor tomará un valor y lo representará de forma textual</p>

<p><b>Sintaxis reduce &lt;campo&gt; [suma promedio]</b></p>
<p><b>Parámetros</b></p> <ul style="list-style-type: none"> <li>• campo: el campo en el que se realizará la reducción</li> <li>• suma o promedio: la operación de reducción a realizar, es suma si no se especifica</li> </ul>
<p><b>Descripción</b> El comando reducir tomará una serie de valores y calculará un único valor</p>

#### Referencia de comandos específicos de nodos

<p><b>Sintaxis where_node &lt;campo&gt; &lt;== = &gt; &lt;= &gt;= incluir? excluir? ¿empezar_con? finalizar_con? &gt; &lt;valor&gt;</b></p>
<p><b>Parámetros</b></p> <ul style="list-style-type: none"> <li>• campo: el nombre del campo al que se le aplicará el operador</li> <li>• operador • valor: el valor utilizado para la comparación. Puede ser un número, una cadena o una lista (usando la sintaxis JSON), el motor de consulta comprenderá la semántica</li> </ul>
<p><b>Descripción</b> El comando where_node enviará a la salida solo los elementos que cumplan con el criterio especificado, muchas cláusulas se pueden concatenar usando el operador booleano OR. En comparación con el comando genérico where, los nodos adyacentes también se incluyen en la salida.</p>

<p>Sintaxis where_link &lt;campo&gt; &lt;== = &lt;&gt; &lt;=&gt; = incluir? excluir? ¿empezar_con? finalizar_con? &gt; &lt;valor&gt;</p>
<p><b>Parámetros</b></p> <ul style="list-style-type: none"> <li>• campo: el nombre del campo al que se le aplicará el operador</li> <li>• operador</li> <li>valor: el valor</li> </ul> <p>utilizado para la comparación. Puede ser un número, una cadena o una lista (usando la sintaxis JSON) el motor de consulta entenderá la semántica</p>
<p><b>Descripción</b> El comando where_link enviará a la salida solo los nodos que están conectados por un enlace que cumple el criterio especificado. Muchas cláusulas se pueden concatenar usando el operador booleano OR.</p>

<p>Gráfico de sintaxis [node_label:&lt;node_field&gt;] [node_perspective:&lt;perspective_name&gt;] [link_perspective:&lt;perspective_name&gt;]</p>
<p><b>Parámetros</b></p> <ul style="list-style-type: none"> <li>• node_label: agrega una etiqueta al nodo, la etiqueta será el contenido del campo de nodo especificado •</li> <li>node_perspective: aplica la perspectiva del nodo especificado al resultado grafico. Los valores de perspectiva de nodo válidos son:</li> <ul style="list-style-type: none"> <li>• roles</li> <li>• zonas</li> <li>• bytes_transferidos •</li> <li>no_aprendidos •</li> <li>nodos_públicos •</li> <li>reputación •</li> <li>host_dispositivo •</li> </ul> <li>perspectiva_enlace: aplica la perspectiva de enlace especificada al resultado grafico. Las perspectivas de enlace válidas son:</li> <ul style="list-style-type: none"> <li>• bytes_transferidos •</li> <li>tcp_firewalled •</li> <li>tcp_handshaked_connections •</li> <li>tcp_connection_attempts •</li> <li>tcp_retransmitted_bytes •</li> <li>rendimiento •</li> <li>entre zonas</li> <li>• no_aprendido</li> </ul> </ul>
<p><b>Descripción</b> El comando graph representa un gráfico de red tomando algunos nodos como aporte.</p>

#### Referencia de comandos específicos de Link Events

<p>Disponibilidad de sintaxis</p>
<p><b>Parámetros</b></p>
<p><b>Descripción</b> El comando de disponibilidad calcula el porcentaje de tiempo que un enlace está activo. El cálculo se basa en los eventos de enlace ARRIBA y ABAJO que se ven para el enlace.</p>
<p>Sintaxis Availability_history &lt;rango&gt;</p>
<p><b>Parámetros</b></p> <ul style="list-style-type: none"> <li>• rango: la ventana temporal en milisegundos a usar para agrupar el enlace eventos</li> </ul>

**Descripción** El comando Availability\_history calcula el porcentaje de tiempo que un enlace está ACTIVO agrupando los eventos del enlace en muchos depósitos. Cada cubo incluirá los eventos de la ventana temporal especificada por el parámetro de rango.

**Sintaxis** Availability\_history\_month <months\_back> <rango>

**Parámetros**

- months\_back: número de meses a retroceder con respecto al mes actual para agrupar los eventos de enlace •
- rango: la ventana temporal en segundos que se utilizará para agrupar los eventos de enlace

**Descripción** El comando Availability\_history calcula el porcentaje de tiempo que un enlace está ACTIVO agrupando los eventos del enlace en muchos depósitos. Cada depósito incluirá los eventos de la ventana temporal especificada por los parámetros de rango y meses.

## Funciones

Aquí está la lista completa de funciones:

Sintaxis sum(<campo>,...)
Parámetros <ul style="list-style-type: none"><li>• una lista de campos para sumar</li></ul>
Descripción La función sum devuelve la suma de los campos pasados como argumentos
Advertencia Solo disponible para nodos, enlaces, variables y códigos de función
Sintaxis color(<campo>)
Parámetros <ul style="list-style-type: none"><li>• campo: el campo en el que calcular el color</li></ul>
Descripción La función de color genera un color en formato hexadecimal rgb a partir de un valor
Advertencia Solo disponible para nodos, enlaces, variables y códigos de función
Sintaxis fecha(<hora>)
Parámetros <ul style="list-style-type: none"><li>• tiempo definido como época de Unix</li></ul>
Descripción La función de fecha devuelve una fecha de una hora sin procesar
Sintaxis dist(<campo1>,<campo2>)
Parámetros <ul style="list-style-type: none"><li>• los dos campos a restar</li></ul>
Descripción La función dist devuelve la distancia entre campo1 y campo2
Sintaxis abs(<campo>)
Parámetros <ul style="list-style-type: none"><li>• el campo en el que calcular el valor absoluto</li></ul>
Descripción La función abs devuelve el valor absoluto del campo
Sintaxis div(<campo1>,<campo2>)
Parámetros <ul style="list-style-type: none"><li>• campo1 y campo2: los dos campos a dividir</li></ul>
Descripción La función div calculará la división campo1/campo2
Sintaxis coalesce(<campo1>,<campo2>,...)
Parámetros <ul style="list-style-type: none"><li>• una lista de campos o cadenas literales en el formato "&lt;chars&gt;"</li></ul>
Descripción La función coalesce generará el primer valor que no sea nulo
Sintaxis concat(<campo1>,<campo2>,...)
Parámetros <ul style="list-style-type: none"><li>• una lista de campos o cadenas literales en el formato "&lt;chars&gt;"</li></ul>
Descripción La función concat generará la concatenación de los campos o valores de entrada
Sintaxis round(<campo>,[precisión])
Parámetros <ul style="list-style-type: none"><li>• campo: el campo numérico a redondear</li><li>• precisión: el número de lugares decimales</li></ul>

	<p>Descripción La función de redondeo toma un número y genera el valor redondeado</p>
	<p>Sintaxis split(&lt;campo&gt;,&lt;divisor&gt;,&lt;índice&gt;)</p>
Parámetros	<ul style="list-style-type: none"><li>• campo: el campo a dividir</li><li>• divisor: el carácter utilizado para separar la cadena y producir los tokens</li><li>• índice: el índice basado en 0 del token a generar</li></ul>
	<p>Descripción La función de división toma una cadena, la separa y genera el token en la posición &lt;index&gt;</p>
	<p>Sintaxis is_recent(&lt;time_field&gt;)</p>
Parámetros	<ul style="list-style-type: none"><li>• time_field: el campo que representa una hora</li></ul>
	<p>Descripción La función is_recent toma un campo de tiempo y devuelve verdadero si el tiempo no es más de 30 minutos</p>
	<p>Sintaxis segundos_ago(&lt;campo_tiempo&gt;)</p>
Parámetros	<ul style="list-style-type: none"><li>• time_field: el campo que representa una hora</li></ul>
	<p>Descripción La función second_ago devuelve la cantidad de segundos transcurridos entre la hora actual y el valor del campo de hora</p>
	<p>Sintaxis minutes_ago(&lt;time_field&gt;)</p>
Parámetros	<ul style="list-style-type: none"><li>• time_field: el campo que representa una hora</li></ul>
	<p>Descripción La función minutes_ago devuelve la cantidad de minutos transcurridos entre la hora actual y el valor del campo de hora</p>
	<p>Sintaxis hours_ago(&lt;time_field&gt;)</p>
Parámetros	<ul style="list-style-type: none"><li>• time_field: el campo que representa una hora</li></ul>
	<p>Descripción La función hours_ago devuelve la cantidad de horas pasadas entre el la hora actual y el valor del campo de hora</p>
	<p>Sintaxis days_ago(&lt;time_field&gt;)</p>
Parámetros	<ul style="list-style-type: none"><li>• time_field: el campo que representa una hora</li></ul>
	<p>Descripción La función days_ago devuelve la cantidad de días transcurridos entre el la hora actual y el valor del campo de hora</p>
	<p>Sintaxis to_time(&lt;campo_tiempo&gt;)</p>
Parámetros	<ul style="list-style-type: none"><li>• time_field: el campo que representa una hora</li></ul>
	<p>Descripción La función to_time toma una cadena que representa una fecha y hora en formato ISO 8601 y devuelve la marca de tiempo UNIX correspondiente en milisegundos</p>
	<p>Sintaxis bitwise_and(&lt;campo_numérico&gt;,&lt;máscara&gt;)</p>
Parámetros	<ul style="list-style-type: none"><li>• numeric_field: el campo numérico sobre el que se aplica la máscara</li><li>• máscara: un número que se interpretará como una máscara de bits</li></ul>

Descripción La función bitwise\_and calcula el operador & bit a bit entre el numeric\_field y la máscara ingresada por el usuario

## Ejemplos

### Creación de un gráfico

circular En este ejemplo, crearemos un gráfico circular para comprender la distribución de proveedores de MAC en nuestra red. Elegimos nodos como nuestra fuente de consulta y comenzamos a agrupar los nodos por mac\_vendor:

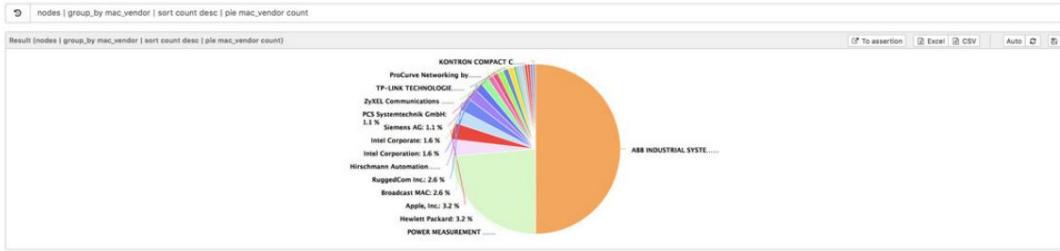
```
nodos | group_by mac_proveedor
```

Podemos ver la lista de los proveedores en nuestra red asociados con el recuento de ocurrencias. Para comprender mejor nuestros datos, podemos usar el comando ordenar, por lo que la consulta se convierte en:

```
nodos | grupo_por mac_proveedor | ordenar recuento desc
```

En el último paso, usamos el comando circular para dibujar el gráfico con mac\_vendor como etiqueta y el recuento como valor.

```
nodos | grupo_por mac_proveedor | ordenar recuento desc | pastel mac_vendor cuenta
```



### Creación de un gráfico de

columnas En este ejemplo, crearemos un gráfico de columnas con los nodos superiores por tráfico. Comenzamos obteniendo los nodos y seleccionando el id, bytes enviados, bytes recibidos y la suma de bytes enviados y bytes recibidos. Para calcular la suma usamos la función suma, la consulta es:

```
nodos | seleccionar id enviado.bytes recibidos.bytes sum(enviado.bytes,recibido.bytes)
```

Si ejecutamos la consulta anterior notamos que el campo suma tiene un nombre muy largo, podemos renombrarlo para estar más cómodos con los siguientes comandos:

```
nodos | seleccionar id enviado.bytes recibidos.bytes
sum(enviados.bytes,recibidos.bytes)->sum
```

Para obtener los principales nodos por tráfico ordenamos y tomamos los 10 primeros:

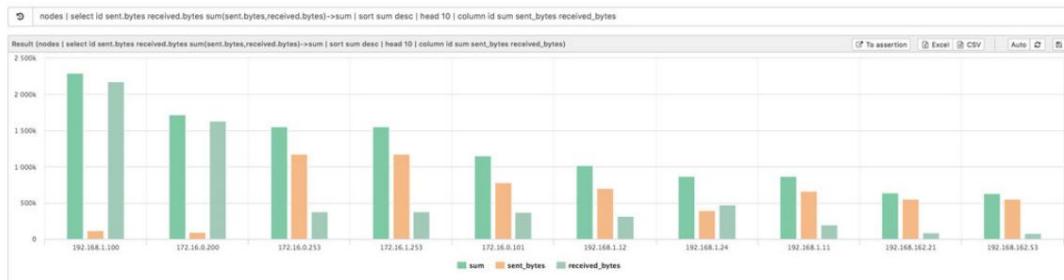
```
nodos | seleccione id enviado.bytes recibidos.bytes
sum(enviado.bytes,recibido.bytes)->sum | ordenar suma desc | cabeza 10
```

Finalmente usamos el comando de columna para mostrar los datos de forma gráfica:

```
nodos | seleccione id enviado.bytes recibidos.bytes
sum(enviado.bytes,recibido.bytes)->sum | ordenar suma desc | cabeza 10 | columna id suma bytes_enviados
bytes_recibidos
```

Nota: puede acceder a un campo interno de un tipo complejo con la sintaxis de puntos, en el ejemplo, la sintaxis de puntos se usa en los campos enviados y recibidos para acceder a su subcampo de bytes.

Nota: después de acceder a un campo con la sintaxis de punto, obtendrá un nuevo nombre para evitar ambigüedades, el punto se reemplaza por un guion bajo. En el ejemplo, sent.bytes se convierte en sent\_bytes.



Usando where con múltiples condiciones en OR

Con esta consulta queremos obtener todos los nodos con un rol específico, en particular, queremos todos los nodos que son servidores web o servidores DNS.

Con el comando where es posible lograr esto escribiendo muchas condiciones separadas por OR.

Nota: el campo de roles contiene una lista de valores, por lo que usamos el include? operador para verificar si un valor estaba contenido en la lista.

```
nodos | ¿Dónde se incluyen los roles? web_server O funciones incluyen? servidor_dns |  
seleccionar roles de identificación
```

roles	
id	roles
192.168.1.1	JSON View ["dns_server"]
172.16.0.1	JSON View ["dns_server"]

Usando el depósito y el historial

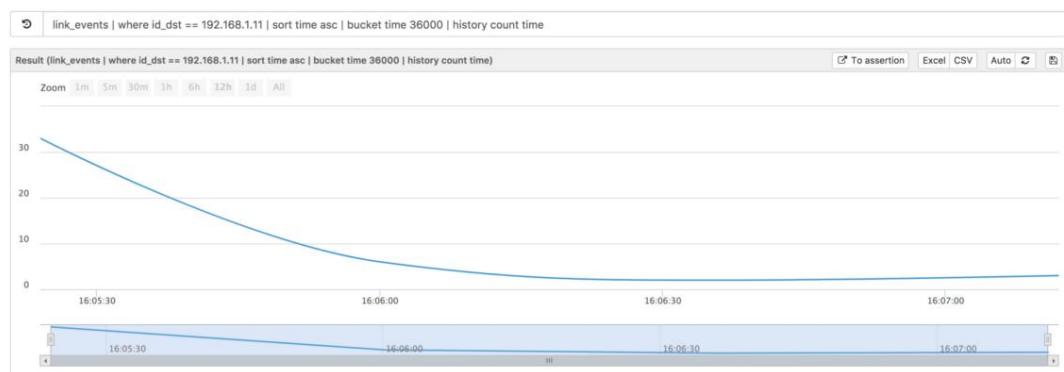
En este ejemplo vamos a calcular la distribución de eventos de enlace hacia una dirección IP. Empezamos filtrando todos los link\_events con id\_dst igual a 192.168.1.11.

Después de esto, ordenamos por tiempo, este es un paso muy importante porque el depósito y el historial dependen de cómo se ordenen los datos.

En este punto agrupamos los datos por tiempo con cubo. El paso final es dibujar un gráfico usando el comando de historial, pasamos conteo como valor para el eje Y y tiempo para el eje X.

El comando de historial es particularmente adecuado para mostrar una gran cantidad de datos, en la imagen a continuación podemos ver que hay muchas horas de datos para analizar.

```
enlace_eventos | donde id_dst == 192.168.1.11 | ordenar el tiempo asc | tiempo de cubo 36000 | historia cuenta el tiempo
```



Usando unirse

En este ejemplo uniremos dos fuentes de datos para obtener una nueva fuente de datos con más información. En particular, enumeraremos los enlaces con las etiquetas para los nodos de origen y destino.

Empezamos preguntando por los enlaces y uniéndolos con los nodos haciendo coincidir el campo from de los enlaces con el campo id de los nodos:

```
enlaces | unir nodos desde id
```

Después de ejecutar la consulta anterior, obtendremos todos los campos de enlaces más un nuevo campo llamado join\_node\_from\_id, que contiene el nodo que satisface la condición link.from == node.id. Podemos acceder a los subcampos de join\_node\_from\_id usando la sintaxis de puntos.

Como queremos obtener las etiquetas también para el campo a de los enlaces, agregamos otra combinación y excluimos las etiquetas vacías del nodo al que hace referencia para obtener datos más interesantes:

```
enlaces | unir nodos desde id | unir nodos a id | dónde
nodo_unido_a_id.etiqueta != ""
```

Obtenemos una gran cantidad de datos que son difíciles de entender, solo use una selección para obtener solo la información relevante:

```
enlaces | unir nodos desde id | unir nodos a id | donde se unió_nodo_a_id.etiqueta != ""
"" | seleccione desde el protocolo united_node_from_id.label hasta el protocolo united_node_to_id.label
```

Result (links   join nodes from id   join nodes to id   where joined_node_to_id.label != ""   select from joined_node_from_id.label to joined_node_to_id.label protocol)				To assertion	Excel	CSV	Auto	Copy
from	joined_node_from_id_label	to	joined_node_to_id_label	protocol				
172.16.0.253	172.16.0.148	Modicon M340 BMX P34 2020	modbus					
172.16.0.253	172.16.0.149	Modicon M340 BMX P34 2020	modbus					
172.16.1.253	172.16.1.148	Modicon M340 BMX P34 2020	modbus					
172.16.0.253	172.16.0.156	Modicon M340 BMX P34 2020	modbus					
172.16.1.253	172.16.1.156	Modicon M340 BMX P34 2020	modbus					
172.16.0.253	172.16.0.146	Modicon M340 BMX P34 2020	modbus					
172.16.1.253	172.16.1.146	Modicon M340 BMX P34 2020	modbus					
172.16.0.253	172.16.0.153	Modicon M340 BMX P34 2020	modbus					
172.16.1.253	172.16.1.153	Modicon M340 BMX P34 2020	modbus					
172.16.0.253	172.16.0.143	Modicon M340 BMX P34 2020	modbus					

#### Cálculo del historial de disponibilidad

En este ejemplo, calcularemos el historial de disponibilidad de un enlace. Para lograr una disponibilidad confiable, se recomienda habilitar la función "[Rastrear disponibilidad](#)" en el enlace deseado.

Partimos de la fuente de datos link\_events, filtrada por ip de origen y de destino para identificar con precisión el enlace de destino. Considere también filtrar por protocolo para lograr un mayor grado de precisión.

```
enlace_eventos | donde id_src == 10.254.3.9 | donde id_dst == 172.31.50.2
```

El siguiente paso es ordenar los eventos por tiempo ascendente de creación. Sin este paso, Availability\_history podría producir resultados sin sentido, como valores negativos. Finalmente, calculamos Availability\_history con un depósito de 1 minuto (60000 milisegundos). La consulta completa es la siguiente.

```
enlace_eventos | donde id_src == 10.254.3.9 | donde id_dst == 172.31.50.2 | ordenar el tiempo asc | disponibilidad_histórico 60000
```

Queries	
<pre>⌚ link_events   where id_src == 10.254.3.9   where id_dst == 172.31.50.2   sort time asc   availability_history 60000</pre>	
Result (link_events   where id_src == 10.254.3.9   where id_dst == 172.31.50.2   sort time asc   availability_history 60000)	
availability	time
100	09:01:00.000
34.075	09:02:00.000
21.41167	09:04:00.000
79.805	09:05:00.000
0	09:06:00.000
74.47167	09:08:00.000
25.78833	09:09:00.000
0	09:10:00.000
29.11167	09:11:00.000
71.36167	09:12:00.000



# Capítulo

# 5

---

## Mantenimiento

---

Temas:

- Descripción general del sistema • Copia de seguridad y restauración de datos • Reinicio y apagado
- Actualización y reversión de software • Restablecimiento de fábrica de datos • Soporte

En este capítulo obtendrá la información complementaria para mantener la Solución Nozomi Networks en funcionamiento con tareas de mantenimiento ordinarias y extraordinarias.

## Resumen del sistema

En esta sección, se brinda una breve descripción general de los componentes principales de Nozomi Networks Solution OS (N2OS), a fin de proporcionar más antecedentes para administrar y mantener un sistema de producción.

Diseño de particiones y sistema de archivos En

esta sección, veremos el sistema de archivos, los servicios y los comandos de N2OS.

Lo primero que debe saber sobre la estructura de N2OS es la presencia de cuatro particiones de disco diferentes:

1. Primera partición N2OS, donde se guarda y se ejecuta una copia del sistema operativo. El proceso de instalación y actualización utiliza dos particiones diferentes para ofrecer un cambio rápido entre la versión en ejecución y las nuevas versiones.
2. Segunda partición N2OS, que hace frente a la primera para proporcionar rutas de actualización confiables.
3. Partición de configuración del sistema operativo, ubicada en /cfg, donde se guardan los archivos de configuración del sistema operativo de bajo nivel (por ejemplo, configuraciones de red, usuarios administradores de shell, claves SSH, etc.). Esta partición se copia en /etc al comienzo del proceso de arranque.
4. Partición de datos, ubicada en /data donde se guardan todos los datos del usuario (configuración aprendida, datos importados por el usuario, capturas de tráfico, base de datos persistente)

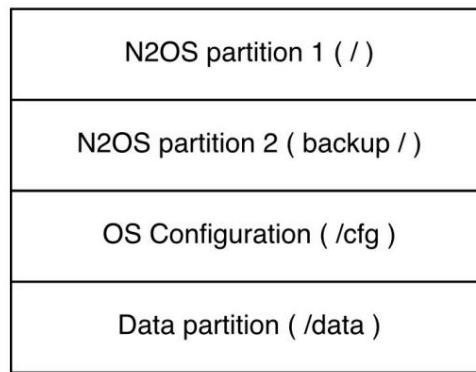


Figura 42: La tabla de particiones estándar de N2OS

Una mirada más cercana a la partición /data revela algunas subcarpetas, por ejemplo:

1. cfg: donde se guardan todas las configuraciones aprendidas automáticamente y proporcionadas por el usuario. Dos principales Los archivos de configuración se almacenan aquí:
  - a. n2os.conf: para configuraciones aprendidas automáticamente b.
  - n2os.conf.user: para configuraciones adicionales proporcionadas por el usuario.
2. datos: directorio de trabajo para la base de datos relacional incrustada, utilizado para todos los datos persistentes 3. rastros: donde se guardan y rotan todos los rastros cuando es necesario. 4. rrd: este directorio contiene las estadísticas de red agregadas, utilizadas por ejemplo para el tráfico en la página

31

### Servicios principales

Hay algunos servicios del sistema que debe conocer para una configuración y solución de problemas adecuadas:

1. n2osids, el principal proceso de seguimiento. Se puede controlar con

```
servicio n2osids <operación>
```

(<operación> puede ser cualquiera de iniciar, detener, reiniciar). Sus archivos de registro están en /data/log/n2os y comienzan con n2os\_ids\*. 2.

- n2ostrace, el demonio de rastreo. Se puede controlar con

```
servicio n2ostrace <operación>
```

Sus archivos de registro comienzan con n2os\_trace\* y se encuentran en /data/log/n2os.

3. n2osva, el demonio de identificación de activos y evaluación de vulnerabilidades. Se puede controlar con

```
servicio n2osva <operación>
```

Sus archivos de registro comienzan con n2os\_va\* y se encuentran en /data/log/n2os.

4. n2ossandbox, el demonio sandbox de archivos. Se puede controlar con

```
servicio n2ossandbox <operación>
```

Sus archivos de registro comienzan con n2os\_sandbox\* y se encuentran en /data/log/n2os.

nginx, el servidor web detrás de la interfaz web. Hace frente a unicornio para proporcionar el servicio https y asegurado. Se puede controlar con

```
servicio nginx <operación>
```

Para poder realizar cualquier operación en estos servicios, debe obtener los privilegios mediante enable-me. Por ejemplo, los siguientes comandos permiten reiniciar el servicio n2osids:

```
habilitar-me  
servicio n2osids reiniciar
```

Varias otras herramientas y demonios se están ejecutando en el sistema para ofrecer funcionalidades N2OS.

## Copia de seguridad y restauración de datos

En esta sección, se le informará sobre los métodos disponibles para realizar una copia de seguridad del sistema y, respectivamente, para restaurarlo a partir de una copia de seguridad. Tenga en cuenta que una copia de seguridad contendrá solo los datos: el software del sistema no se modificará.

Hay dos tipos diferentes de copia de seguridad disponibles: copia de seguridad completa y copia de seguridad del entorno. El primero contiene todos los datos, mientras que el segundo carece de datos históricos, configuraciones extendidas y alguna otra información. Ambos pueden ejecutarse mientras el sistema está funcionando. La copia de seguridad del entorno se puede utilizar para restaurar la parte más importante del sistema en otro dispositivo para su análisis o como copia de seguridad delta cuando hay una copia de seguridad completa disponible.

### Copia de seguridad completa

#### Línea de comando

Para crear una nueva copia de seguridad, vaya a una terminal y ejecute el comando:

```
n2os-fullbackup
```

El archivo de copia de seguridad ahora se puede copiar a través de SFTP a una ubicación remota de su elección. El archivo a copiar es:

```
admin@<appliance_ip>:/data/tmp/<backup_hostname_date.nozomi_backup>
```

#### Aplicación web Para

crear una nueva copia de seguridad, vaya a Administración > Copia de seguridad/Restaurar y haga clic en el botón 'Descargar' para generar y descargar el archivo de copia de seguridad.

The screenshot shows the Nozomi Networks web interface. At the top, there is a navigation bar with links for Dashboard, Appliances, Alerts, Environment, Analysis, Administration, and a user account. Below the navigation bar, there is a sub-menu for 'Backup/Restore'. The main content area has a title 'Generate Backup Archive' and a note: 'Click on 'Download' to generate and download the backup archive'. A blue 'Download' button is visible at the bottom of this section.

## Restauración completa

En esta sección aprenderá cómo restaurar desde una copia de seguridad completa el software N2OS de una instalación existente.

1. Copie a través de SFTP el archivo de copia de seguridad desde la ubicación donde se guardó en el administrador@<appliance\_ip>:/data/tmp/<backup\_hostname\_date.nozomi\_backup> ruta del dispositivo. Por ejemplo, usando la línea de comando scp:

```
scp <backup_location_path>/<backup_hostname_date.nozomi_backup> admin@<appliance_ip>:/data/tmp/  
<backup_hostname_date.nozomi_backup>
```

2. Vaya a una terminal y ejecute este comando

```
n2os-fullrestore /data/tmp/<backup_hostname_date.nozomi_backup>
```

Ahora ha restaurado completamente la copia de seguridad anterior.

## Copia de seguridad del entorno En

esta sección aprenderá a realizar una copia de seguridad de la copia de seguridad del entorno de una instalación existente.

1. Emite el comando de guardar desde la CLI
2. Copie a través de SFTP el contenido de la carpeta /data/cfg en un lugar seguro.

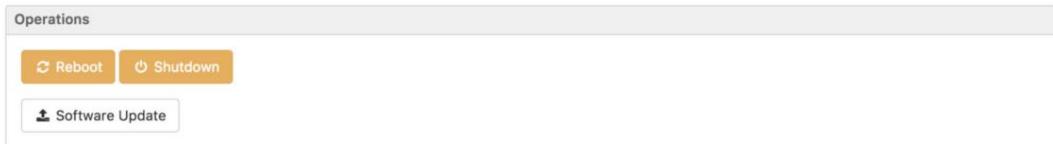
## Restauración del entorno

En esta sección, aprenderá cómo restaurar un entorno de solución de Nozomi Networks a una instalación existente.

1. Copie el contenido guardado de la carpeta cfg en la carpeta /data/cfg del dispositivo.
2. Desde la consola, emita el comando de reinicio del servicio n2osids.

## Reiniciar y apagar

Los comandos de reinicio y apagado se pueden realizar desde la interfaz web en Administración  
> Operaciones



Además, ambos comandos se pueden ingresar en la consola de texto o dentro de una sesión SSH.

Para reiniciar el sistema, emita el siguiente comando:

```
Permiteme  
apagar -r ahora
```

Para apagar correctamente el sistema, emita el siguiente comando:

```
habilitar-me  
apagar -p ahora
```

## Actualización y reversión de software

En esta sección, se le informará sobre los métodos disponibles para actualizar el sistema a una versión más reciente y volver a la anterior.

La reversión a la versión instalada anteriormente es transparente y todos los datos se migran al formato anterior. Sin embargo, la reversión a una versión anterior a la instalada anteriormente requiere tener una [copia de seguridad completa](#) disponible para restaurar.

Aunque la actualización del software está diseñada para ser transparente para el usuario y para conservar todos los datos, sugerimos tener siempre al menos una copia de seguridad del [entorno](#) del sistema en un lugar seguro.

Un aspecto interesante del archivo de actualización de Nozomi Networks Solution es que se aplica tanto a Guardian como a CMC, y funcionará para todos los dispositivos físicos y virtuales para que la experiencia de actualización sea fluida. Se deben realizar consideraciones especiales para el Contenedor, donde se aplican diferentes comandos y procedimientos de actualización.

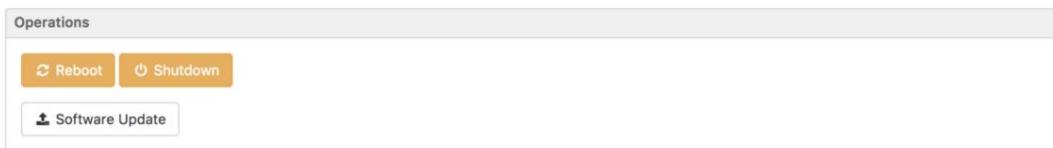
### Actualización: método gráfico

En esta sección, aprenderá cómo actualizar el software de Nozomi Networks Solution de una instalación existente.

Ya debe tener el nuevo archivo VERSION-update.bundle que desea instalar.

Un sistema en ejecución debe actualizarse con una versión N2OS más reciente.

1. Vaya a Administración > Operaciones del sistema



2. Haga clic en Actualización de software y seleccione el archivo VERSION-update.bundle

Advertencia: el sistema debe tener al menos la versión 18.5.9 para admitir el formato .bundle; si su sistema ejecuta una versión anterior a la 18.5.9, primero debe actualizar a la 18.5.9 para continuar. El archivo se cargará 3.

Haga clic en el botón Continuar

Advertencia: si se actualiza la versión 18.5.9, el sistema solicita que se inserte la suma de comprobación que se distribuye con el .bundle; solo después de la verificación de la suma de verificación, el botón está habilitado.

Comienza el proceso de actualización. Espere unos minutos para que se complete la actualización.

### Actualización: método de línea de comandos En

esta sección, aprenderá cómo actualizar el software de Nozomi Networks Solution de una instalación existente.

Ya debe tener el nuevo archivo de actualización que desea instalar.

Un sistema en ejecución debe actualizarse con una versión N2OS más reciente.

1. Vaya a una terminal y cd en el directorio donde se encuentra el archivo VERSION-update.bundle.

A continuación, copie el archivo en el dispositivo con:

```
scp VERSION-update.bundle admin@<appliance_ip>:/data/tmp
```

2. Inicie la instalación del nuevo software con:

```
ssh admin@<appliance_ip>
```

```
Permiteme
```

```
install_update /data/tmp/VERSION-update.bundle
```

El dispositivo ahora se reiniciará con el nuevo software instalado.

Revertir a la versión anterior En esta sección,

aprenderá cómo revertir el software a la versión anterior. Si desea retroceder a una versión anterior a la anterior, siga las instrucciones de la siguiente sección.

Debe haber realizado una actualización de versión al menos una vez.

1. Vaya a la consola y escriba el comando

Retroceder

2. Responda y al mensaje de confirmación y espere mientras se reinicia el sistema. Toda la configuración y los datos históricos se convertirán automáticamente a la versión anterior, por lo que no se requerirá intervención manual.

## Retroceder a una versión anterior

En esta sección, aprenderá cómo revertir el software a una versión anterior a la anterior.

Necesita tener una copia de seguridad completa disponible. Si no tiene uno, no puede retroceder a una versión anterior. Tenga en cuenta que esta operación lleva más tiempo que [volver a la anterior](#), requiere una [copia de seguridad completa](#) y no conserva los datos modificados recientemente.

1. Tome el archivo de actualización de software VERSION-update.bundle al que desea revertir e instálelo como si fuera una versión nueva, como se explica en [Actualización y reversión de software](#) en la página 67.  
Advertencia: si desea retroceder a una versión anterior a la 18.5.9, primero debe retroceder a la versión 18.5.9, ya que se eliminó la compatibilidad con el formato de archivo anterior desde
2. Al reiniciar, ignore cualquier error e inicie sesión en la consola.
3. Ahora siga los pasos para una [restauración completa](#) con un archivo de copia de seguridad de la misma versión del software que acaba de reinstalar.

## Restablecimiento de fábrica de datos

En esta sección, aprenderá cómo borrar completamente la partición de datos de N2OS. La configuración de IP se mantendrá y el procedimiento es seguro para ejecutarse de forma remota. ¡Ejecutar este procedimiento hará que el sistema pierda todos los datos!

1. Vaya a una terminal y ejecute el comando:

```
n2os-datafactoryreset -y
```

2. El sistema comenzará de nuevo con una nueva partición de datos. Consulte [la Fase 2 de configuración](#) en la página 12 para completar la configuración del sistema.

## Restablecimiento de fábrica de datos con desinfección

En esta sección, aprenderá cómo borrar por completo la partición de datos N2OS desinfectando el espacio del disco utilizando el esquema de 7 pasos US DoD 5220-22M.

Este proceso borra la partición de datos N2OS de acuerdo con las [pautas claras sugeridas por el NIST](#) en el documento [800-88 rev1](#).

Se mantendrán las configuraciones como la configuración de la contraseña de la red y la consola.

¡Ejecutar este procedimiento hará que el sistema pierda todos los datos!

1. Vaya a una terminal y ejecute el comando:

```
n2os-datasanitize -y
```

2. El sistema comenzará de nuevo con una nueva partición de datos. Consulte [la Fase 2 de configuración](#) en la página 12 para completar la configuración del sistema.

## Apoyo

En esta sección, aprenderá cómo generar el archivo necesario para solicitar soporte a Nozomi Networks.

Vaya a Administración > Soporte, haga clic en el botón de descarga y su navegador comenzará a descargar el archivo del paquete de soporte. Envíe un correo electrónico a support@nozominetworks.com adjuntando el archivo.





# Capítulo

# 6

---

## Protocolos programables

---

Temas:

- [Configuración](#) • [Escritura de un protocolo programable](#) • [Referencia de API](#)

En este manual, cubriremos la API de secuencias de comandos de Lua para construir un decodificador de protocolo personalizado.

## Configuración

---

Para agregar un nuevo protocolo programable:

1. Copie el script de Lua en /data/scriptable\_protocols/ 2.

Configure Guardian con esta regla probe scriptable-protocol <protocol\_name> <script\_name> en n2os.conf.user  
(<script\_name> es solo el nombre del archivo)

3. Ejecute service n2osids stop, el proceso de ids se reiniciará automáticamente.

Después de estos pasos, el nuevo protocolo se carga en Guardian y analizará el tráfico de la red.

## Escribir un protocolo programable

El lenguaje utilizado para escribir un protocolo programable es Lua, consulte la documentación oficial de Lua (<https://www.lua.org/start.html>) para obtener más información.

Esta es una implementación de protocolo mínima:

```
función can_handle()
    devolver el final
    verdadero
```

Del ejemplo, podemos ver que lo único obligatorio es definir una función llamada `can_handle` que devuelve `verdadero` si reconoce el protocolo de destino.

Por supuesto, esta implementación no es muy útil e intentará manejar todos los paquetes, así que escribamos algo más complejo para detectar y analizar algo de tráfico modbus:

```
función can_handle() devuelve
    paquete.puerto_origen() == 502 o paquete.puerto_destino() == 502 final
```

Aquí podemos ver un uso de la API para recuperar los puertos de paquetes. De esta forma, la comprobación es un poco más precisa, pero sigue siendo insuficiente para detectar un paquete modbus en el mundo real.

Comencemos a hacer una inspección profunda de paquetes:

```
función can_handle() si
    data_size() < 8 entonces
        devolver fin falso

    local has_right_port = paquete.puerto_origen() == 502 o paquete.puerto_destino() ==
        502

    fwd(2)
    local has_right_protocol_id = consumir_n_uint16() == 0 local longitud Esperada =
        consumir_n_uint16()

    devuelve has_right_port y
        tiene_derecho_protocolo_id y
        tamaño_restante() == longitud Esperada
    fin
```

**ADVERTENCIA:** no use variables globales. Las variables definidas fuera de las funciones `can_handle` y `update_status` son globales y su estado se comparte en todas las sesiones del mismo protocolo.

**NOTA:** las funciones `fwd` y `consume_*` moverán hacia adelante el puntero de carga útil.

**NOTA:** el resultado de la función de tamaño restante depende de la posición del puntero de carga útil.

En este ejemplo, usamos la API para inspeccionar el contenido de la carga útil. Primero verificamos que haya suficientes bytes, un paquete modbus tiene al menos 8 bytes de largo. Luego verificamos el puerto de la misma manera que hicimos en el ejemplo anterior, luego saltamos dos bytes con la función `fwd` y leemos los siguientes dos enteros de 16 bits.

Verificamos que la identificación del protocolo sea cero y que la longitud escrita en el paquete coincida con los bytes restantes en nuestra carga útil. Si todas las comprobaciones pasan, devolvemos `verdadero` y le indicamos a `Guardian` que los siguientes paquetes de esta sesión deben ser analizados por este decodificador de protocolo.

Un protocolo con solo la función can\_handle implementada solo creará el nodo y la sesión en la vista de red, pero aún falta el enlace en el gráfico, no se mostrará información adicional en la vista de proceso.

Para extraer más información de los paquetes modbus vamos a implementar la función update\_status:

```
función get_protocol_type() devuelve
ProtocolType.SCADA end

función can_handle() volver
is_modbus() fin

función update_status() si no
is_modbus() luego regresa end

is_request local = paquete.puerto_destino() == 502 rtu_id local = consumir_uint8()
local fc = consumir_uint8() & 0x7f

si is_request entonces
is_packet_from_src_to_dst (verdadero)
set_roles ("maestro", "esclavo")

si fc == 6 entonces
dirección local = consumir_n_uint16()

valor local = DataValue.new() value.value =
read_n_uint16() value.cause =
DataCause.WRITE
valor.tipo = Tipo de datos.ANALÓGICO valor.tiempo
= paquete.tiempo()

ejecutar_actualizar_con_variable(CódigoFunción.nuevo(fc), Rtuld.nuevo(rtu_id),
"r"..tostring(dirección), valor) return end end

ejecutar_actualizar()
final
```

NOTA: para evitar la duplicación, creamos una función is\_modbus a partir del contenido de la función can\_handle anterior.

NOTA: la función is\_modbus tiene el efecto de avanzar el puntero de carga útil en 6 bytes, por lo que puede leer directamente el rtu\_id sin más manipulaciones del puntero de carga útil.

NOTA: definimos la función get\_protocol\_type para definir el tipo de protocolo. En este ejemplo de update\_status, leemos más datos de la carga útil y decodificamos la solicitud de registro único de escritura. Podemos entender la dirección de la comunicación, por lo que llamamos a is\_packet\_from\_src\_to\_dst con true para notificar a Guardian y crear un enlace y llamamos a set\_roles para establecer los roles en los nodos involucrados.

Para insertar una variable en Guardian existe la función execute\_update\_with\_variable, se necesitan 4 argumentos: el código de la función, el id de la rtu, el nombre de la variable y el valor. Los objetos FunctionCode y Rtuld pueden construirse a partir de una cadena o un número, el objeto DataValue puede construirse con el constructor vacío y luego llenarse con la información disponible.

Con el siguiente ejemplo, cubrimos un caso más complejo y almacenamos algunos datos en la sesión para manejar una solicitud y una respuesta:

```
PENDING_FC local = 1
PENDING_START_ADDR local = 2
PENDING_REG_COUNT local = 3

función update_status() si no es_modbus()
    luego regresa

fin

rwd()

is_request local = paquete.puerto_destino() == 502 id_transacción local =
consumir_n_uint16() fwd(4)

rtu_id local = consumir_uint8() fc local =
consumir_uint8() & 0x7f

si is_request entonces
    is_packet_from_src_to_dst(true) set_roles("maestro",
    "esclavo")
    session.set_pending_request_number(transaction_id, PENDING_FC, fc)

    si fc == 3 entonces si
        tamaño_restante() < 4 entonces regresa fin

    local start_addr = consumir_n_uint16() local registers_count =
consumir_n_uint16()

    session.set_pending_request_number(transaction_id, PENDING_START_ADDR, start_addr)

    session.set_pending_request_number(transaction_id, PENDING_REG_COUNT,
registros_recuento) fin de
    lo
contrario
    is_packet_from_src_to_dst(false) req_fc local =
    session.read_pending_request_number(transaction_id, PENDING_FC)

    si fc == req_fc entonces si fc == 3
        entonces
            local start_addr = session.read_pending_request_number(transaction_id,
PENDING_START_ADDR)
            reg_count local = session.read_pending_request_number(transaction_id,
PENDING_REG_COUNT)
            session.close_pending_request(transaction_id)

        si el tamaño_restante() < 1 entonces devuelve
            el final

    recuento de bytes local = consumir_uint8()

    si tamaño_restante() ~= byte_count o reg_count * 2 ~=
        tamaño_restante() then send_alert_malformed_packet("El paquete
        es demasiado pequeño") return end

for i = 0, reg_count - 1, 1 hacer valor local =
    DataValue.new() value.value = consumir_n_uint16()
```

```
value.cause = DataCause.READ_SCAN value.type
= DataType.ANALOG value.time =
paquete.time()

ejecutar_actualizar_con_variable(FunctionCode.new(fc), Rtuld.new(rtu_id),
"r"..toString(start_addr+i),
value)

fin

retorno
final
final
fin

ejecutar_actualizar() final
```

Esta vez nos estamos enfocando en el código de la función de registro de retención de lectura, para comprender la comunicación y crear una variable, necesitamos analizar tanto la solicitud como la respuesta, y debemos conservar algunos datos de la solicitud y usarlos en la respuesta. Para lograr esto podemos usar las funciones proporcionadas por el objeto de sesión.

## Referencia de la API

### Bibliotecas LUA disponibles

- base
- cadena
- mesa
- matemáticas
- bit32
- depuración
- utf8

### Tipos de datos

Código de función de clase	
Constructores	<ul style="list-style-type: none"><li>• CódigoFunción.nuevo(&lt;cadena&gt;) • CódigoFunción.nuevo(&lt;número&gt;)</li></ul>
Id . de clase Rtu	
Constructores	<ul style="list-style-type: none"><li>• Rtuld.new(&lt;cadena&gt;) • Rtuld.new(&lt;número&gt;)</li></ul>
Valor de datos de clase	
Constructores	<ul style="list-style-type: none"><li>• ValorDatos.nuevo()</li></ul>
Propiedades de lectura/escritura	<ul style="list-style-type: none"><li>• DataValue.value (número)</li><li>• DataValue.str_value (cadena) • DataValue.cause (DataCause)</li><li>• DataValue.time (número, milisegundos desde la época) • DataValue.type (DataType)</li></ul>
variable de clase	
Métodos	<ul style="list-style-type: none"><li>• set_label(&lt;cadena&gt;)</li></ul>
Nodo de clase	
Métodos	<ul style="list-style-type: none"><li>• set_property(&lt;clave&gt;, &lt;valor&gt;) • get_property(&lt;clave&gt;) • delete_property(&lt;clave&gt;)</li></ul>
Causa de datos de enumeración	
Valores	<ul style="list-style-type: none"><li>• Causa de datos.READ_SCAN • Causa de datos.READ_CYCLIC • Causa de datos.READ_EVENT • CausaDeDatos.ESCRIBIR</li></ul>
Tipo de datos de enumeración	

Valores	<ul style="list-style-type: none"><li>• Tipo de datos.ANALÓGICO</li><li>• Tipo de datos.DIGITAL</li><li>• Tipo de datos.BITSTRING</li><li>• Tipo de datos.CADENA</li><li>• Tipo de datos.DOUBLEPOINT</li><li>• Tipo de datos.TIMESTAMP</li></ul>
---------	--

Tipo de protocolo de enumeración	
Valores	<ul style="list-style-type: none"><li>• Tipo de protocolo.SCADA</li><li>• Tipo de protocolo. RED</li></ul>

## Funciones

Datos de sintaxis (<índice>)	
Parámetros	<ul style="list-style-type: none"><li>• índice: la posición del byte a leer, comenzando desde 0</li></ul>
Descripción Devuelve el valor del byte desde la posición especificada, devuelve 0 si el índice es fuera de los límites	

Sintaxis data_size()	
Descripción Devuelve el tamaño total de la carga útil	

Sintaxis restante_tamaño()	
Descripción Devuelve el tamaño de la carga útil desde el puntero hasta el final. El resultado depende del uso de las funciones fwd(), rwd() y consuma_*( ).	

Sintaxis fwd(<cantidad>)	
Parámetros	<ul style="list-style-type: none"><li>• cantidad: el número de bytes a omitir</li></ul>
Descripción Mueve el puntero de carga útil el número especificado de bytes.	

Sintaxis rwd()	
Descripción Mueve el puntero de carga útil al principio de la carga útil.	

Sintaxis read_uint8()	
Descripción Lee un entero de 8 bits sin signo en la posición del puntero de carga útil.	

Sintaxis read_int8()	
Descripción Lee un entero de 8 bits con signo en la posición del puntero de carga útil.	

Sintaxis read_n_uint16()	
Descripción Leer un número entero de 16 bits sin signo de orden de red en la posición del puntero de carga útil.	

Sintaxis read_h_uint16()	
Descripción Leer un entero de 16 bits sin signo de orden de host en la posición del puntero de carga útil.	

Sintaxis read_n_int16()	
-------------------------	--

<p>Descripción Lee una orden de red con un entero de 16 bits firmado en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_h_int16()</code></p>
<p>Descripción Lee una orden de host con un entero de 16 bits firmado en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_n_uint32()</code></p>
<p>Descripción Leer un número entero de 32 bits sin signo de orden de red en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_h_uint32()</code></p>
<p>Descripción Leer un entero de 32 bits sin signo de orden de host en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_n_int32()</code></p>
<p>Descripción Lee una orden de red con un entero de 32 bits firmado en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_h_int32()</code></p>
<p>Descripción Lee un entero de 32 bits con signo de orden de host en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_n_uint64()</code></p>
<p>Descripción Leer un número entero de 64 bits sin firmar de orden de red en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_h_uint64()</code></p>
<p>Descripción Leer un entero de 64 bits sin signo de orden de host en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_n_int64()</code></p>
<p>Descripción Lee un orden de red con un entero de 64 bits firmado en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_h_int64()</code></p>
<p>Descripción Leer un entero de 64 bits con signo de orden de host en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_n_float()</code></p>
<p>Descripción Lee una orden de red flotante en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_h_float()</code></p>
<p>Descripción Lee una orden flotante de host en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_n_double()</code></p>
<p>Descripción Lee una orden de red doble en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_h_double()</code></p>
<p>Descripción Lee una orden de host doble en la posición del puntero de carga útil.</p>
<p>Sintaxis <code>read_string()</code></p>
<p>Descripción Leer una cadena en la posición del puntero de carga útil hasta el terminador nulo.</p>
<p>Sintaxis <code>read_string_with_len(str_len)</code></p>

<p>Descripción Lee una cadena en la posición del puntero de carga útil para los bytes str_len.</p>
<p>Sintaxis consumir_uint8()</p> <p>Descripción Leer un entero de 8 bits sin signo en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_int8()</p> <p>Descripción Leer un entero de 8 bits con signo en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_n_uint16()</p> <p>Descripción Leer un entero de 16 bits sin signo de orden de red en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_h_uint16()</p> <p>Descripción Leer un entero de 16 bits sin signo de orden de host en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_n_int16()</p> <p>Descripción Lee una orden de red con un entero de 16 bits con signo en la posición del puntero de carga útil y mueve el puntero después de los datos.</p>
<p>Sintaxis consumir_h_int16()</p> <p>Descripción Leer un entero de 16 bits con signo de orden de host en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_n_uint32()</p> <p>Descripción Leer un número entero de 32 bits sin signo de orden de red en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_h_uint32()</p> <p>Descripción Leer un entero de 32 bits sin signo de orden de host en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_n_int32()</p> <p>Descripción Leer un entero de 32 bits con signo de orden de red en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_h_int32()</p> <p>Descripción Leer un entero de 32 bits con signo de orden de host en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_n_uint64()</p> <p>Descripción Leer un número entero de 64 bits sin signo de orden de red en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_h_uint64()</p>

<p>Descripción Leer un entero de 64 bits sin signo de orden de host en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_n_int64()</p> <p>Descripción Leer un entero de 64 bits con signo de orden de red en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_h_int64()</p> <p>Descripción Leer un entero de 64 bits con signo de orden de host en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_n_float()</p> <p>Descripción Lee una orden de red flotante en la posición del puntero de carga útil y mueve el puntero después de los datos.</p>
<p>Sintaxis consumir_h_float()</p> <p>Descripción Lee una orden de host flotando en la posición del puntero de carga útil y mueve el puntero después de los datos.</p>
<p>Sintaxis consumir_n_doble()</p> <p>Descripción Lee un pedido de red doble en la posición del puntero de carga útil y mueve el puntero después de los datos.</p>
<p>Sintaxis consumir_h_doble()</p> <p>Descripción Leer una orden de host doble en la posición del puntero de carga útil y mover el puntero después de los datos.</p>
<p>Sintaxis consumir_cadena()</p> <p>Descripción Lee una cadena en la posición del puntero de carga útil hasta el terminador nulo y mueve el puntero después de los datos.</p>
<p>Sintaxis consumir_string_with_len(str_len)</p> <p>Descripción Lee una cadena en la posición del puntero de carga útil para los bytes str_len y mueve el puntero después de los datos.</p>
<p>Sintaxis set_roles(&lt;función_cliente&gt;, &lt;función_servidor&gt;)</p> <p>Parámetros</p> <ul style="list-style-type: none"><li>• client_role: el rol del cliente • server_role: el rol del servidor</li></ul> <p>Descripción Establezca los roles de los nodos involucrados, los valores válidos son: "maestro", "esclavo", "historiador", "terminal", "web_server", "dns_server", "db_server", "time_server", "otro"</p>
<p>Sintaxis set_source_type(&lt;node_type&gt;)</p> <p>Parámetros</p> <ul style="list-style-type: none"><li>• node_type: el tipo del nodo de origen</li></ul> <p>Descripción Establezca el tipo de nodo de origen, los valores válidos son: "comutador", "enrutador", "impresora", "grupo", "OT_device", "emisión", "computadora"</p>

Sintaxis variables_are_on_client()
Parámetros
Descripción Notificar a Guardian que las variables deben agregarse al nodo cliente
sintaxis is_packet_from_src_to_dst(<is_from_src>)
parámetros • is_from_src: verdadero es la dirección de src a dst, falso de lo contrario
descripción notificar a Guardian sobre la dirección del paquete, esta función debe ser llamada para obtener una creación de enlace
sintaxis ejecutar_actualizar()
parámetros
descripción notificar a Guardian sobre un paquete, se debe llamar al menos una variante de execute_update para cada paquete
sintaxis ejecutar_actualizar_con_código_función(<código_función>, <rtu identificación>)
parámetros • function_code: un objeto de tipo functioncode <ul style="list-style-type: none"><li>• rtuid: un objeto de tipo rtuid</li></ul>
descripción notificar a Guardian sobre un paquete con un código de función y una identificación rtu
sintaxis ejecutar_actualizar_con_variable(<código_función>, <id_rtu>, <nombre_var>, <valor>)
parámetros • function_code: un objeto de tipo functioncode <ul style="list-style-type: none"><li>• rtu_id: un objeto de tipo rtuid •</li><li>var_name: el nombre de la variable • value: un objeto de tipo datavalue que contiene el valor de la variable y algo de información sobre los datos</li></ul>
descripción notificar a Guardian sobre un paquete con un código de función, una identificación rtu, una variable nombre y un valor de variable
sintaxis ejecutar_actualizar_con_función(<código_función>, <id_rtu>, <nombre_var>, <valor>, <función>)
parámetros • function_code: un objeto de tipo functioncode <ul style="list-style-type: none"><li>• rtu_id: un objeto de tipo rtuid •</li><li>var_name: el nombre de la variable • value: un objeto de tipo datavalue que contiene el valor de la variable y algo de información sobre los datos</li><li>• función: la función se llamará pasando variable como argumento</li></ul>
descripción notificar a Guardian sobre un paquete con un código de función, una identificación de rtu, un nombre de variable, un valor de variable y una función que brinda la posibilidad de acceder directamente a la variable
sintaxis send_alert_malformed_packet(<motivo>)
parámetros • motivo: un mensaje que se mostrará en la alerta
descripción genera una alerta de tipo sign:network-malformed o sign:scada-malformed

sintaxis paquete.source_id()
descripción devuelve la identificación del nodo de origen
sintaxis paquete.destination_id()
descripción devuelve la identificación del nodo de destino
sintaxis paquete.source_ip()
descripción devuelve la ip del nodo de origen
sintaxis paquete.destination_ip()
descripción devuelve la ip del nodo de destino
sintaxis paquete.source_mac()
descripción devuelve el nodo de origen mac
sintaxis paquete.destino_mac()
descripción devuelve el nodo de destino mac
sintaxis paquete.puerto_origen()
descripción devuelve el puerto del nodo de origen
sintaxis paquete.puerto_destino()
descripción devuelve el puerto del nodo de destino
sintaxis paquete.is_ip()
descripción devuelve verdadero si el paquete es un paquete ip
sintaxis paquete.transport_type()
descripción devuelve el tipo de capa de transporte, puede ser "tcp", "udp", "ethernet", "icmp" o "desconocido"
sintaxis paquete.source_node()
descripción devuelve el nodo de origen
sintaxis paquete.destination_node()
descripción devuelve el nodo de destino
sintaxis paquete.tiempo()
descripción devolver el paquete tiempo
sintaxis session.set_pending_request_number(<request_id>, <key>, <valor>)
parámetros • request_id: un número utilizado para identificar de forma única la solicitud • clave: un número utilizado para separar diferentes valores en la misma solicitud • valor: el número para almacenar

descripción almacenar un número en la sesión
sintaxis session.read_pending_request_number(<request_id>, <key>)
parámetros • request_id: un número utilizado para identificar de forma única la solicitud <ul style="list-style-type: none"><li>• clave: un número utilizado para separar diferentes valores en la misma solicitud</li></ul>
descripción leer un número de la sesión
sintaxis session.set_pending_request_string(<request_id>, <key>, <valor>)
parámetros • request_id: un número utilizado para identificar de forma única la solicitud <ul style="list-style-type: none"><li>• clave: un número utilizado para separar diferentes valores en la misma solicitud</li><li>• valor: la cadena para almacenar</li></ul>
descripción almacenar una cadena en la sesión
sintaxis session.read_pending_request_string(<request_id>, <key>)
parámetros • request_id: un número utilizado para identificar de forma única la solicitud <ul style="list-style-type: none"><li>• clave: un número utilizado para separar diferentes valores en la misma solicitud</li></ul>
descripción leer una cadena de la sesión
sintaxis session.has_pending_request(<request_id>)
parámetros • request_id: un número utilizado para identificar de forma única la solicitud
descripción devuelve verdadero si hay valores almacenados con request_id
sintaxis session.has_pending_request_value(<request_id>, <key>)
parámetros • request_id: un número utilizado para identificar de forma única la solicitud <ul style="list-style-type: none"><li>• clave: un número utilizado para separar diferentes valores en la misma solicitud</li></ul>
descripción devuelve verdadero si hay valores almacenados con request_id y key
sintaxis session.close_pending_request(<request_id>)
parámetros • request_id: un número utilizado para identificar de forma única la solicitud
descripción cerrar la solicitud pendiente y eliminar los datos asociados
sintaxis log_d(<mensaje>)
parámetros • msg: el mensaje a registrar
descripción registrar un mensaje de depuración
sintaxis log_e(<mensaje>)
parámetros • msg: el mensaje a registrar
descripción registrar un mensaje de error