

# PROYECTO FIN DE CURSO ASIR ZAKARIYA EL KHATTABI

---

## New Relic Herramienta de Monitorización y Medición de Rendimiento de Infraestructura de Servicios.

---



## Índice

---

1. ¿Qué es New Relic?
  - 1.1. ¿Qué podemos hacer con New Relic?
2. ¿Cómo implementar New Relic en mi sistema Linux?
3. Implementar New Relic en Bitwarden Server
  - 3.1. ¿Qué es Bitwarden?
  - 3.2. Instalación de Bitwarden
  - 3.3. Instalación de Agente de New Relic en el servidor donde esta alojado Bitwarden
4. Monitorización de mi Pagina Web En PHP
  - 4.1. Monitorizar Página Web en PHP Con Docker
5. Monitorizar el tráfico de nuestra web
6. Monitorización de Github Pages con New Relic
7. Sistema de Logs New Relic
8. Biografia y Conslusión.

### ¿Qué es New Relic?

---



**New Relic** es un complejo sistema de monitorización del rendimiento de una infraestructura de servicios, desde backend hasta frontend, monitorización del rendimiento de navegadores, APIs, servidores, aplicaciones móviles.

Se puede definir en que es una herramienta de monitorización del volumen total y en tiempo real de los recursos de una o varias máquinas. La compañía tiene integrado funcionalidades similares para medir el rendimiento de aplicaciones móviles para los dos entornos.

### ¿Qué podemos hacer con New Relic?

---

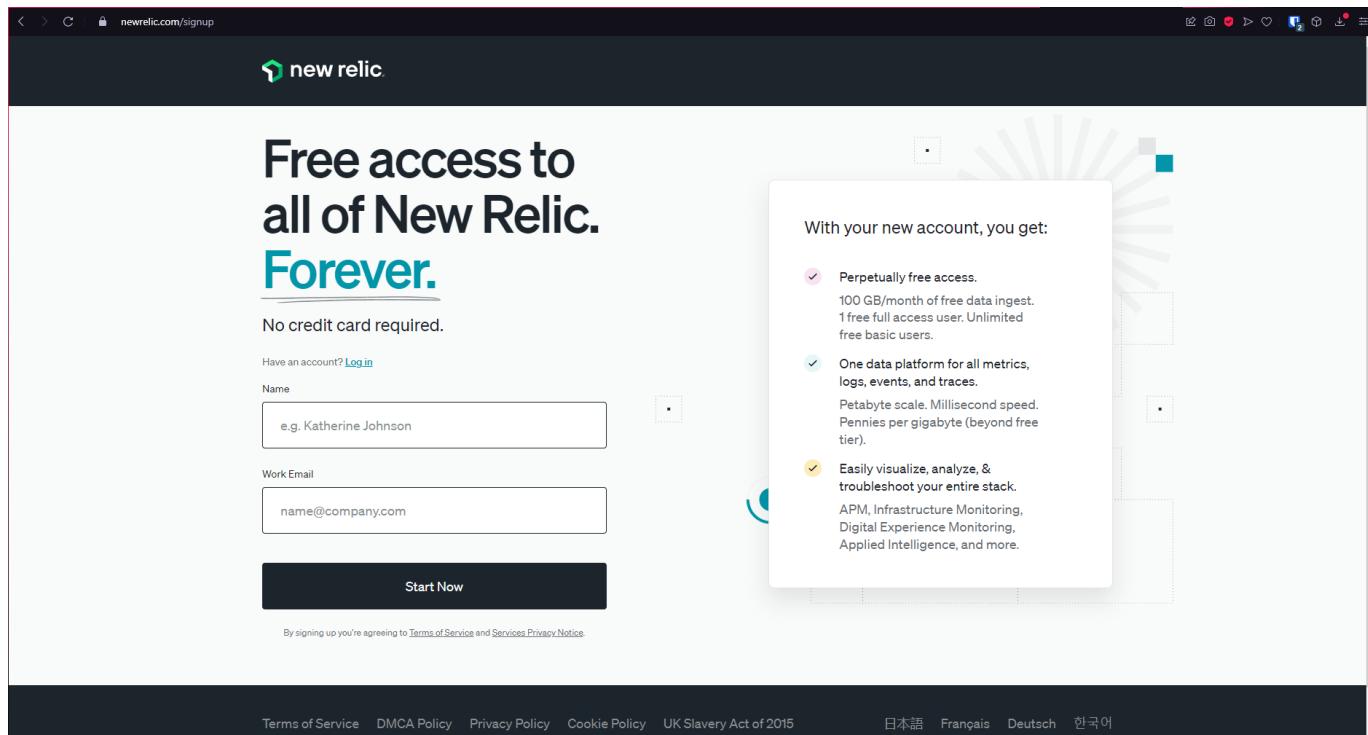
New Relic es una herramienta de monitorización bastante transversal. Estos son algunos de los aspectos más interesantes que suelen medir la plataforma:

Por la parte de datos de experiencia de cliente: comportamiento de los usuarios, rendimiento de las aplicaciones móviles, navegadores y servidores. Por la parte de datos de negocio: todos los aspectos anteriores, más el rendimiento de los recursos en la nube pública, microservicios, APIs y bases de datos, tanto SQL como NoSQL.

- Algunas de las tareas que es capaz de realizar el software:
  - Monitorizar Conexiones Web (tiempos de respuesta, n.º de peticiones, carga, etc..)
  - Monitorización de Log de Errores (Sistema de aviso por correo si hay fallos de conexión, etc..)
  - Fijar alertas sobre datos de referencia (tiempos de respuesta, errores de autenticación, etc..)
  - Estadísticas de rendimiento en distintos dispositivos (uso de memoria, velocidad de respuesta, etc..)
- Permite monitorizar varios sistemas de lenguaje de aplicaciones web entre ellos están los siguientes:
  - .NET
  - Java
  - PHP
  - Python
  - Ruby
- Permite monitorizar el tráfico que entra por los navegadores por el sistema de Browsers.
- Es capaz de Monitorizar en tiempo real, casi todos los servicios que ofrece.

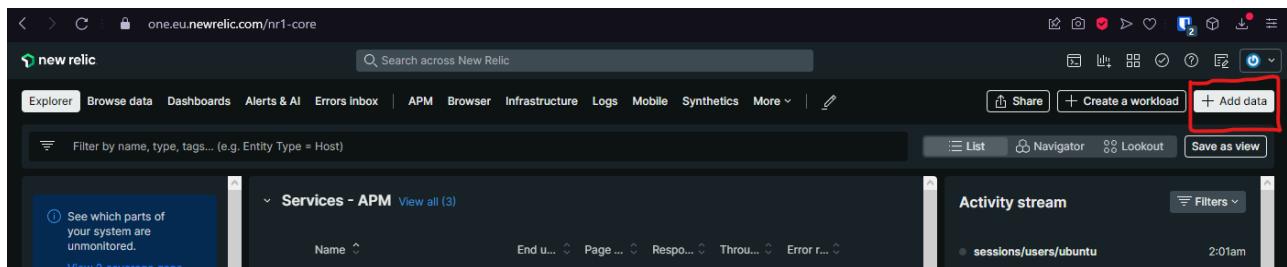
# ¿Cómo implementar New Relic en mi sistema Linux?

Primero hay que crear una cuenta en [New Relic](#).



Una vez registrado se podrá acceder a la plataforma. Una vez en la plataforma podremos ver muchas cosas, lo que interesa ahora mismo es crear un nuevo host para poder monitorizar nuestro sistema operativo.

## 1. Pinchar en "+ Add data".



## 2. Buscar el sistema que se quiera monitorizar.

The screenshot shows the New Relic Marketplace search interface. The search bar at the top contains the query "linux". Below the search bar, there's a navigation menu with links like "Explorer", "Browse data", "Dashboards", "Alerts & AI", "Errors inbox", "APM", "Browser", "Infrastructure", "Logs", "Mobile", "Synthetics", and "More". A search bar below the menu also contains "linux". To the right, there's a sidebar titled "Setting up New Relic" with text about agents and their installation process. The main content area displays search results under categories: "Data sources (4)", "Dashboards (2)", "Alerts (1)", and "Apps & visualizations (0)". Under "Data sources", there are two items: "Linux" and "New Relic infrastructure agent". Under "Logging", there are two items: "Linux logs" and "New Relic infrastructure agent". Under "Kubernetes & containers", there is one item: "Docker". On the far left, a sidebar lists various monitoring categories with their counts: Application monitoring (0), Infrastructure & OS (5), Browser & mobile (0), Simulate traffic (0), Logging (2), Kubernetes & containers (1), Amazon Web Services (2), Azure (0), Google Cloud Platform (0), Open source monitoring (0), ML models (0), Network (0), and Partner (0).

## 3. Seleccionar Lunix y pinchar en "**Begin installation**".

The screenshot shows the "Installation plan" page for the "Linux" environment. The title "Installation plan" is at the top. On the left, there's a sidebar with the same category list as the previous screenshot. The main content area has a step-by-step guide: "Select your environment (Linux)" (marked with a green checkmark) and "Begin installation" (marked with a blue checkmark). The "Begin installation" step is highlighted with a red box. Below it, there's a note: "You'll log into your host and run a single command that will do the following:". It lists two steps: "Discovery" (which looks at the system and recommends integrations) and "Install the New Relic agents" (which installs the latest New Relic agents on the host to get insight into the performance of the system and applications). At the bottom of this section, there's a large red-bordered button labeled "Begin installation". Below this button, there's an optional step: "Additional instrumentation (optional)". On the right side, there's a sidebar titled "What you'll need" with two bullet points: "Remote access (SSH/RDP): You'll use your host's terminal to run a single command that will install our instrumentation." and "Firewall or proxy: If you're behind a firewall, set the HTTPS\_PROXY environment variable to the URL of your proxy before you start this installation. See our docs". There's also a "Need help?" section with links to "See our docs" and "Leave us feedback".

## 4. Copiar el Comando que nos proporciona New Relic con nuestras ID y Key de nuestra cuenta y pegarlo en nuestro sistema para que haga conexión y empiece la instalación.

**New Relic installation**

**Autodiscover - Install infrastructure, logs, integrations and more**

With one command, our guided install will discover and recommend integrations appropriate for your system. We'll also help you get started by adding infrastructure and log data for greater visibility into your stack.

**Copy and run the command**

Run this command on your host and answer the prompts there.

**Linux**

```
curl -Ls https://download.newrelic.com/install/newrelic-cli/scripts/install.sh | bash && sudo NEW_RELIC_API_KEY=NRACK-XNBBNEVR1DQ67QIDTIFQNGM1B9W NEW_RELIC_ACCOUNT_ID=3513355 NEW_RELIC_REGION=EU /usr/local/bin/newrelic install
```

**Customize your installation**

We need access to a specific set of endpoints for this installation. Make sure you allow the traffic through your firewall or customize your installation above and use a proxy.

[See our docs](#) [Use a proxy](#)

[See our docs](#) [Give feedback](#) [Back](#)

- Una vez ejecutado el comando solo hace falta esperar para que termine la conexión y la instalación del agente.

**New Relic installation**

**Autodiscover - Install infrastructure, logs, integrations and more**

With one command, our guided install will discover and recommend integrations appropriate for your system. We'll also help you get started by adding infrastructure and log data for greater visibility into your stack.

**Installation in progress**

For more details, follow installation in the CLI.

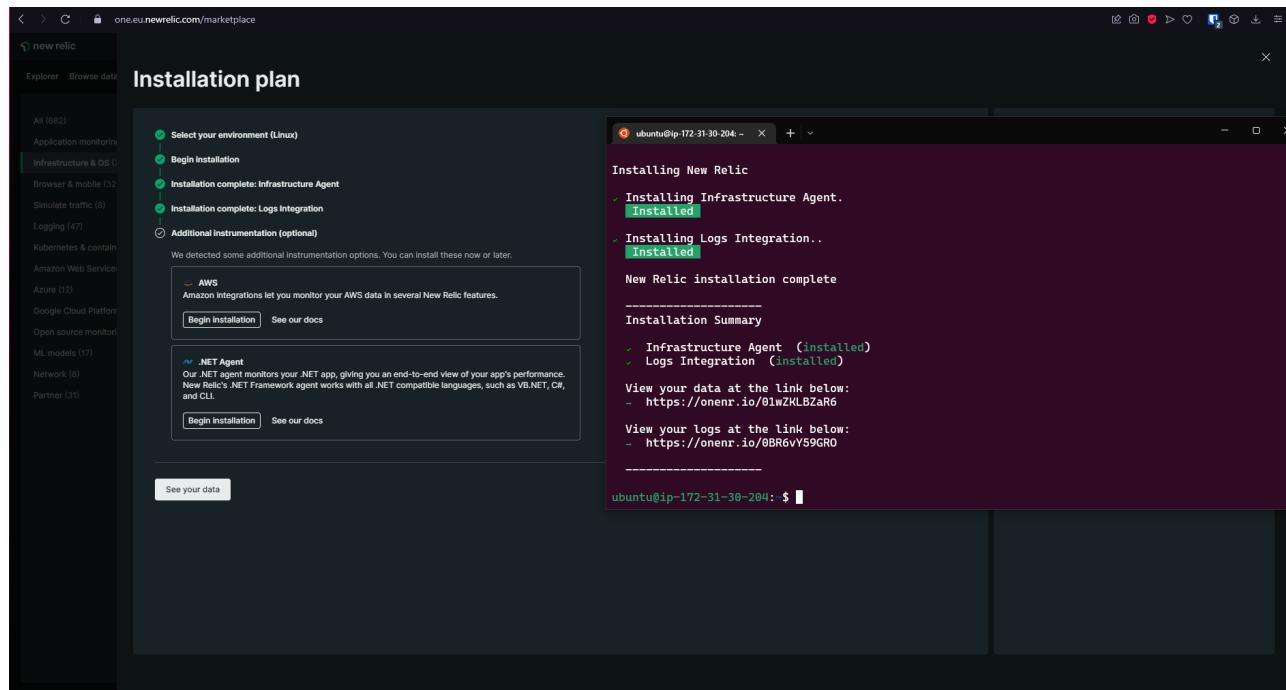
**Linux**

```
ubuntu@ip-172-31-30-204: ~ curl -Ls https://download.newrelic.com/install/newrelic-cli/scripts/install.sh | bash && sudo NEW_RELIC_API_KEY=NRACK-XNBBNEVR1DQ67QIDTIFQNGM1B9W NEW_RELIC_ACCOUNT_ID=3513355 NEW_RELIC_REGION=EU /usr/local/bin/newrelic install
Starting installation.
Installing New Relic CLI v0.50.7
Installing to /usr/local/bin using sudo
[Progress Bar]
Welcome to New Relic. Let's set up full stack observability for your environment.
Connecting to New Relic Platform.
Connected

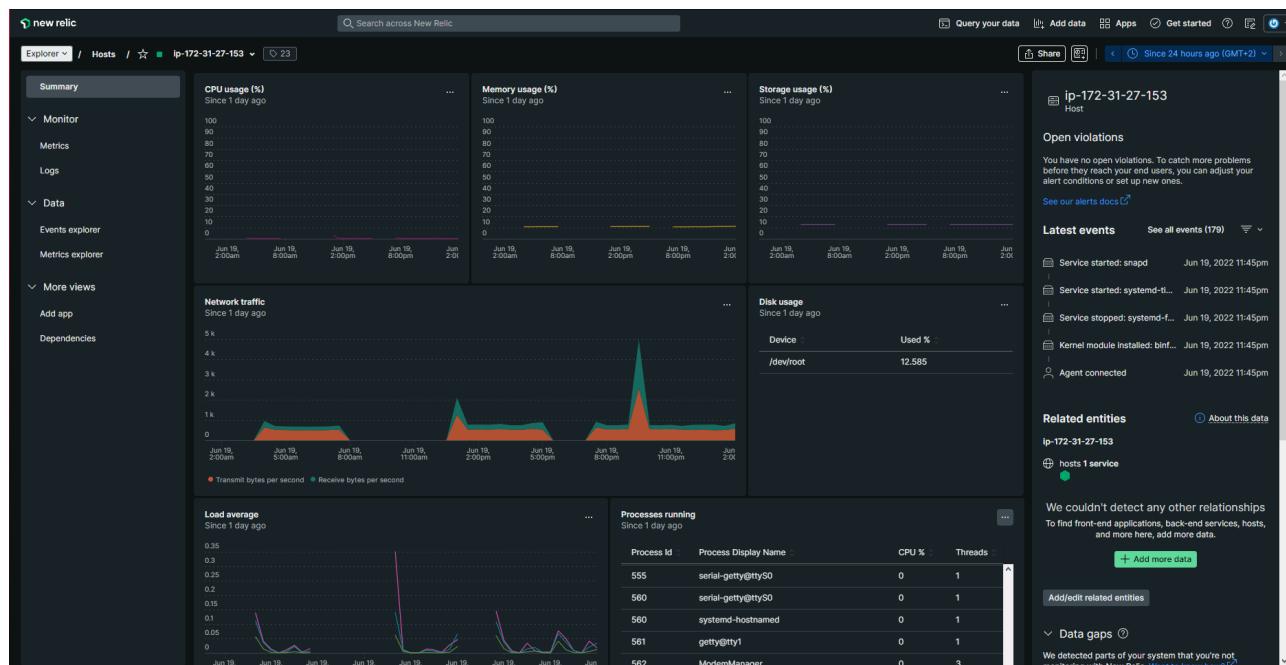
Installing New Relic
Installing Infrastructure Agent.
```

[Give feedback](#)

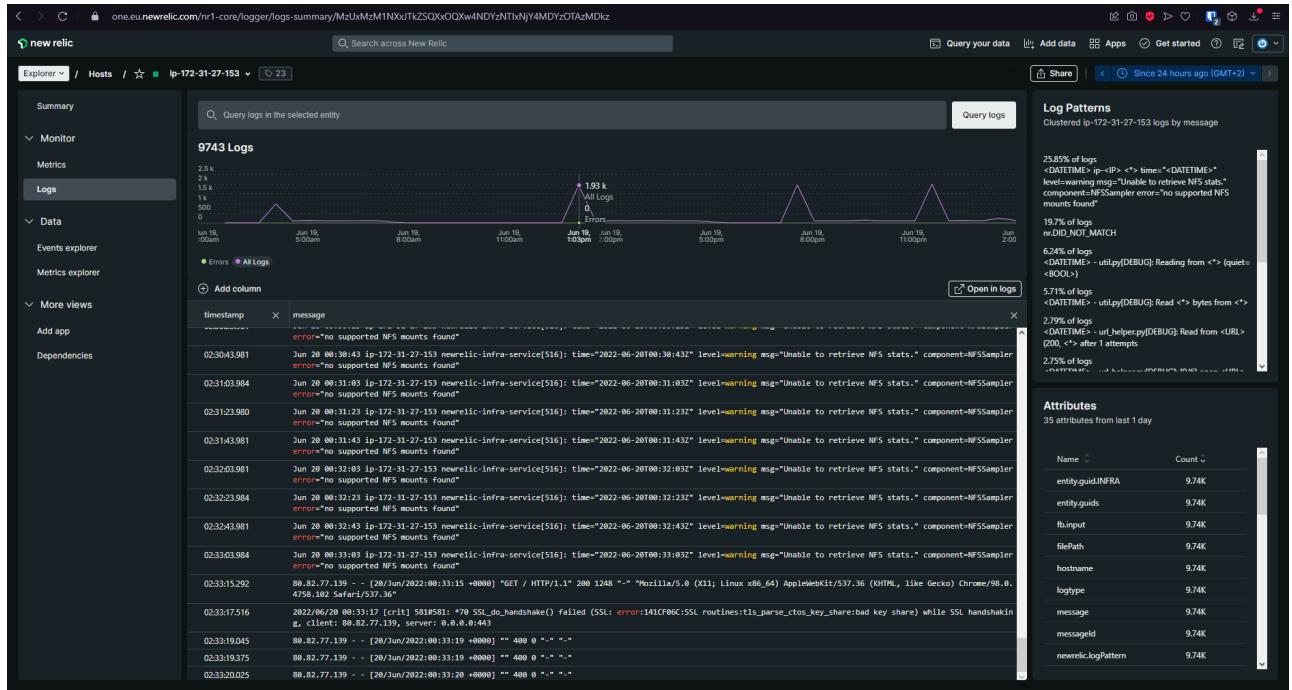
- Una vez termina, si el agente detecta que hay algun software que se pueda monitorizar con New Relic va a hacer una recomendación de la instalación del agente del software detectado.



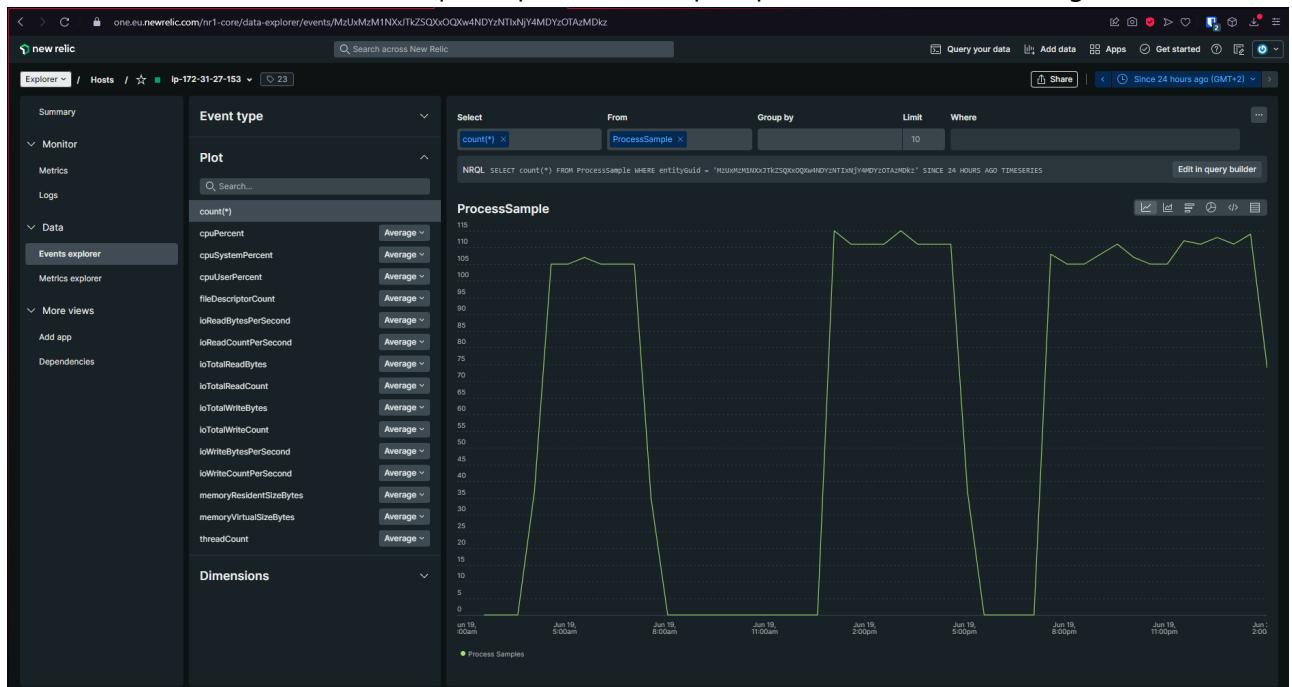
7. Una vez terminado todo el proceso, nos situamos en el inicio de la plataforma de new relic y se vera como hay un nuevo host en la plataforma. Podremos observar como ya esta recolectando datos de nuestro host.



8. Podemos observar todo el sistema de Logs que tiene el host de una forma centralizada.



9. Nos permite ver los eventos que tiene el sistema y personalizarlos (para ello debemos tener más conocimientos sobre las consultas que se puedan hacer para personalizarlas a nuestro gusto).



## Implementar New Relic en Bitwarden Server.

### ¿Qué es Bitwarden?

Es un Gestor de contraseñas muy seguro que nos permite guardar todas nuestras contraseñas de todos los servicios que usemos sin la necesidad de acordarnos de todas las contraseñas si no solo de una que es la que nos permite abrir la caja fuerte de todas nuestras contraseñas. Si se pierde la contraseña principal ya nos podemos despedir de las demás porque son irrecuperables totalmente.

## Instalación de Bitwarden:

Tenemos una Guía de Instalación en la página principal de [Bitwarden](#).

1. Primero hay que tener docker y docker-compose instalados en nuestro sistema. Para ello yo uso mi script para instalar Docker en mis sistemas. [SCRIPTDOCKER](#).

```
#!/bin/bash
set -x

# Variables (CAMBIAR USUARIO)
USERNAME=ubuntu

# Actualizamos el sistema
apt update

# Descargamos el script de instalación
curl -fsSL https://get.docker.com -o get-docker.sh

# Ejecutamos el script
sh get-docker.sh

# Añadimos nuestro usuario al grupo docker
usermod -aG docker $USERNAME

# Iniciamos el servicio docker
systemctl start docker

# Configuramos para que el servicio se inicie automáticamente
systemctl enable docker

# Instalar Docker Compose
apt install docker-compose -y

# Actualizamos el grupo docker se hace fuera del script
#newgrp docker
```

2. Descargamos el script de instalación de Bitwarden y le damos permisos de ejecución.

```
curl -Lso bitwarden.sh https://go.btwrndn.co/bw-sh
chmod +x bitwarden.sh
```

3. Ejecutamos el script indicando que queremos instalarlo con el siguiente comando. Nos pedirá el dominio y si queremos generar los certificados ssl, y por final el correo donde se te va a avisar de que se te van a caducar los certificados SSL.

```
ubuntu@ip-172-31-86-128:/opt/bitwarden$ ./bitwarden.sh install
```



Open source password management solutions  
Copyright 2015-2022, 8bit Solutions LLC  
<https://bitwarden.com>, <https://github.com/bitwarden>

```
=====
bitwarden.sh version 2022.5.1
Docker version 20.10.17, build 100c701
docker-compose version 1.25.0, build unknown
```

(!) Enter the domain name for your Bitwarden instance (ex.  
bitwarden.example.com): bitserver-zaka.ddns.net

(!) Do you want to use Let's Encrypt to generate a free SSL certificate?  
(y/n): y

(!) Enter your email address (Let's Encrypt will send you certificate  
expiration reminders): zakariyasmr1920@gmail.com

Una vez genere los certificados SSL le va a preguntar sobre el nombre que le quiera dar a la base de datos de Bitwarden.

```
-----  
--  
If you like Certbot, please consider supporting our work by:  
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate  
* Donating to EFF: https://eff.org/donate-le  
-----  
--  
(!) Enter the database name for your Bitwarden instance (ex. vault): bitdb
```

Una vez creada la base de datos le va a pedir la instalacion ID y el KEY para ello hay que entrar en <https://bitwarden.com/host>. Deberá poner su correo electronico.

bitwarden.com/host/

bitwarden Products Download Pricing Help Blog Contact  Business Sales Get Started Log In

## Request Hosting Installation Id & Key

Use the form below to request your private Installation Id and Installation Key for self-hosting Bitwarden.

The Installation Id and Key are applied during installation of your Bitwarden instance and stored here: [./bwdata/env/global.override.env](#)

You should use a unique id and key for each Bitwarden installation.

We may use this email address to contact you about important updates regarding your Bitwarden installation.

## Next Steps

For documentation regarding how to install and host Bitwarden on your own servers, including more details on how to use this installation id and installation key, please refer to our help center.

[Installation Instructions](#)

Y despues recibira sus credenciales de instalación.

The screenshot shows the Bitwarden website at [bitwarden.com/host/](https://bitwarden.com/host/). The header includes the Bitwarden logo, navigation links for Products, Download, Pricing, Help, Blog, Contact, and a search bar. On the right, there are buttons for Business Sales, Get Started, and Log In. The main content area has a blue header "Request Hosting Installation Id & Key". Below it, a sub-header says "Use the form below to request your private Installation Id and Installation Key for self-hosting Bitwarden." A note states that the Installation Id and Key are applied during installation and stored in [./bwdata/env/global.override.env](#). It also advises using a unique id and key for each installation. At the bottom, two input fields show example values: "INSTALLATION ID: dd6c8931-6197-4766-8b8c-aeb900349b3e" and "INSTALLATION KEY: 6BCZnr1l4FcplM1U6pMQG". To the right, a section titled "Next Steps" links to "Installation Instructions".

(!) Enter your installation id (get at <https://bitwarden.com/host>):  
dd6c8931-6197-4766-8b8c-aeb900349b3e

(!) Enter your installation key: 6BCZnr1l4FcpM1U6pMQG

Generating DH parameters, 2048 bit long safe prime, generator 2  
This is going to take a long time

4. Una vez instalado el servidor Bitwarden. Ejecutamos un "updateself" y despues un "update".

```
ubuntu@ip-172-31-86-128:/opt/bitwarden$ ./bitwarden.sh updateself
```

Open source password management solutions  
Copyright 2015-2022, 8bit Solutions LLC  
<https://bitwarden.com>, <https://github.com/bitwarden>

```
bitwarden.sh version 2022.5.1
Docker version 20.10.17, build 100c701
docker-compose version 1.25.0, build unknown
```

Updated self.

```
ubuntu@ip-172-31-30-115:~/bitwarden$ ./bitwarden.sh update
```



```
Open source password management solutions
Copyright 2015-2022, 8bit Solutions LLC
https://bitwarden.com, https://github.com/bitwarden
```

- Para que nos funcione bien Bitwarden se deberá configurar un servidor de reenvío SMTP en la siguiente ruta. [./bwdata/env/global.override.env](#)

Para ello yo uso el servicio de [Mailgun](#) que nos proporciona el servicio de reenvío SMTP gratuito.

The screenshot shows the Mailgun dashboard with the domain 'sandbox4e9b61af4b474582be1a65e671d8b294.mailgun.org' selected. The left sidebar has sections for Email, Dashboard, Reporting, Sending (Overview, Domains, Logs, Analytics, Templates, Suppressions, Webhooks, IPs, Mailing lists, Domain settings), Receiving, and INBOXREADY. The 'global.override.env' file is listed under the 'Sending' section. The main page is titled 'Overview' and asks how to send emails from the selected domain. It offers two methods: 'API' (the most flexible, popular way) and 'SMTP' (the easiest way). The 'SMTP' method is selected, showing fields for 'Email address' (bob@gmail.com) and a 'Save Recipient' button. A note says 'Sandbox domains are restricted to authorized recipients only.' Below this, there's a section for 'How to send with SMTP' with instructions and a code snippet for using Swaks:

```
1 # Swaks is an smtp of CURL, install it first:
2 curl http://www.jetmore.org/john/code/swaks/files/swaks-20130209.0 -o swaks
3
4 # Set the permissions for the script so you can run it
5 chmod +x swaks
6
7 # It's based on perl, so install perl
8 sudo apt-get -y install perl
9
10 # Now send!
11 ./swaks --auth \
12 --to bob@gmail.com
```

- Editamos el fichero [./bwdata/env/global.override.env](#) solo las variables de SMTP añadiendo el host de smtp de mailgun, el usuario y la contraseña que nos proporciona.

```
GNU nano 4.8                                bwdata/env/global.override.env
globalSettings__baseServiceUri__vault=https://bitserver-zaka.ddns.net
globalSettings__sqlServer__connectionString="Data Source=tcp:mssql,1433;Initial Catalog=bitdb;Persist Security Info=False;Trusted_Connection=True;Encrypt=1;Connection Timeout=30"
globalSettings__identityServer__certificatePassword=q8bPvQDE075BL301DCTYdWNvZl9vFxis
globalSettings__internalIdentityKey=rSxVHZlkSkzPogKuWften3629YWrTXSqkS5MaYs1xZNdKn6re5TKMWey1iE7n58Z
globalSettings__oidcIdentityClientKey=Sejt7UieeAsJFbulGFFRHAYMDLAqvDbPrqV9Kce6pLJHROL2tCdmYNympKvhQC6
globalSettings__duo__aKey=4iIjkeBptxzZCSLgafBtTJRdEYNWsxDcw0q1BY9e0Z37n0idQwy9QuCv4cb5gz
globalSettings__installation__id=ba70877d-6567-4195-8014-aeb900bf25c7
globalSettings__installation__key=e4SGaU3Eq9EkokWXKXKn
globalSettings__yubico__clientId=REPLACE
globalSettings__yubico__key=REPLACE
globalSettings__mail__replyToEmail=no-reply@bitserver-zaka.ddns.net
globalSettings__mail__smtp__host=smtp.mailgun.org
globalSettings__mail__smtp__port=587
globalSettings__mail__smtp__ssl=false
globalSettings__mail__smtp__username=postmaster@sandboxb0acd32b8679427e87404f6a213dd514.mailgun.org
globalSettings__mail__smtp__password=0fcded10a992f31f551f3e2486c20be2-50f43e91-2752edb1
globalSettings__disableUserRegistration=false
globalSettings__hibpApiKey=REPLACE
adminSettings__admins=
```

```
globalSettings__mail__replyToEmail=no-reply@bitserver-zaka.ddns.net
globalSettings__mail__smtp__host=smtp.mailgun.org
globalSettings__mail__smtp__port=587
globalSettings__mail__smtp__ssl=false
globalSettings__mail__smtp__username=postmaster@sandboxb0acd32b8679427e87404f6a213dd514.mailgun.org
globalSettings__mail__smtp__password=0fcded10a992f31f551f3e2486c20be2-50f43e91-2752edb1
```

7. Una terminada la configuración, reiniciamos el servidor Bitwarden.

```
ubuntu@ip-172-31-86-128:/opt/bitwarden$ ./bitwarden.sh restart
```



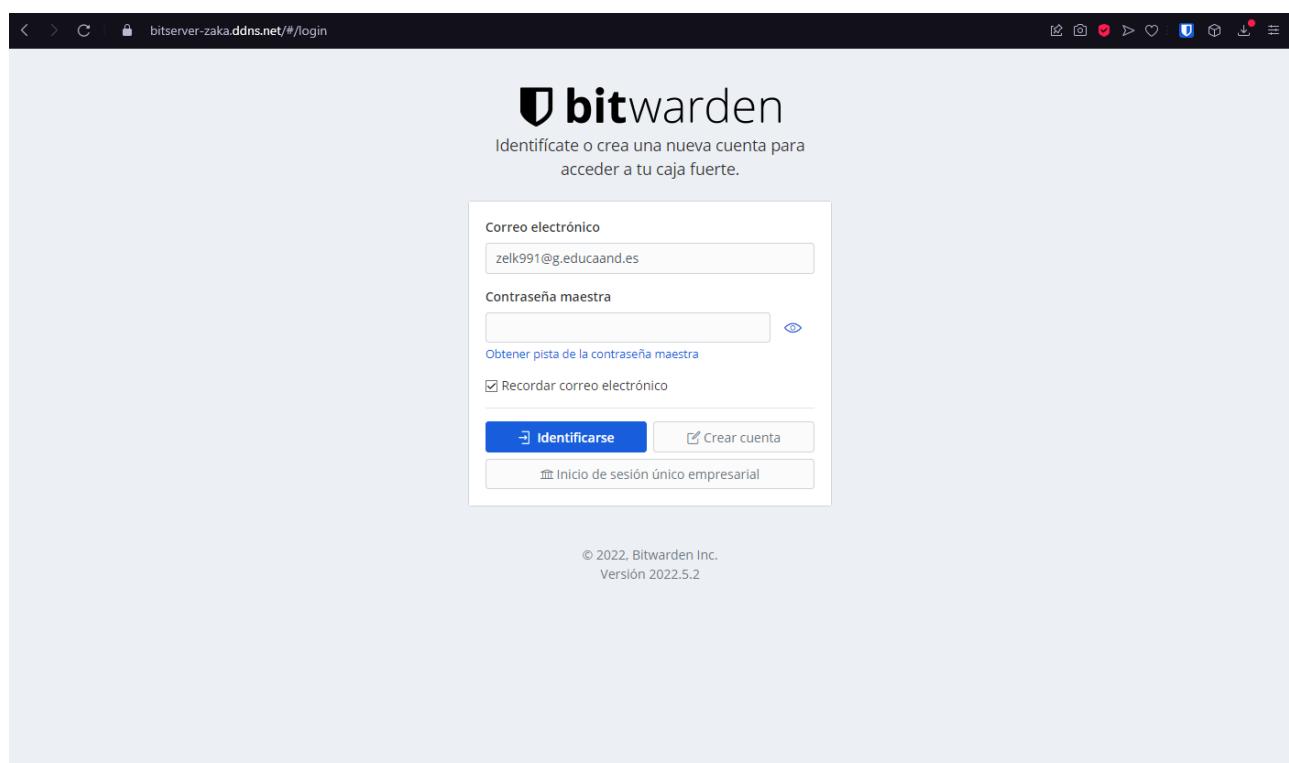
```
Open source password management solutions
Copyright 2015-2022, 8bit Solutions LLC
https://bitwarden.com, https://github.com/bitwarden
```

```
=====
bitwarden.sh version 2022.5.1
Docker version 20.10.17, build 100c701
docker-compose version 1.25.0, build unknown
```

```
Stopping bitwarden-nginx      ... done
Stopping bitwarden-admin     ... done
Stopping bitwarden-mssql     ... done
Stopping bitwarden-icons     ... done
Stopping bitwarden-attachments ... done
Stopping bitwarden-sso       ... done
Stopping bitwarden-notifications ... done
Stopping bitwarden-api       ... done
Stopping bitwarden-events    ... done
```

```
Stopping bitwarden-web          ... done
Stopping bitwarden-identity     ... done
Removing bitwarden-nginx        ... done
Removing bitwarden-admin        ... done
Removing bitwarden-mssql        ... done
Removing bitwarden-icons        ... done
Removing bitwarden-attachments   ... done
Removing bitwarden-sso          ... done
Removing bitwarden-notifications ... done
Removing bitwarden-api          ... done
Removing bitwarden-events       ... done
Removing bitwarden-web          ... done
Removing bitwarden-identity     ... done
```

## 8. Ahora entramos en nuestro servidor Bitwarden.



Debemos registrarnos o crear nueva cuenta.

Crear cuenta

**Correo electrónico**  
  
Utilizarás tu correo electrónico para acceder.

**Tu nombre**  
  
¿Cómo deberíamos llamarte?

**Contraseña maestra**  
 Fuerte (ojo)  
La contraseña maestra es la clave que utilizas para acceder a tu caja fuerte. Es muy importante que no olvides tu contraseña maestra. No hay forma de recuperarla si la olvidas.

**Vuelve a escribir tu contraseña maestra**  
 (ojo)

**Pista de contraseña maestra (opcional)**  
  
Una pista de tu contraseña maestra puede ayudarte a recordarla en caso de que la olvides.

Enviar Cancelar

© 2022, Bitwarden Inc.

Una vez registrados accedemos a la plataforma de Bitwarden. Y pinchamos en enviar correo electrónico de verificación para poder usar todas las utilidades de bitwarden en nuestra cuenta.

The screenshot shows the Bitwarden vault interface. At the top, there are navigation links: Vaults, Enviar, Herramientas, and Informes. On the right, there is a user icon and a dropdown menu. Below the header, on the left, is a sidebar titled 'FILTROS' with a search bar labeled 'Buscar en caja fuerte'. It contains several filter categories: 'Mi caja fuerte' (selected), 'Nueva organización', 'Todos los elementos', 'Favoritos', 'Papelera', 'TIPOS' (with sub-options: Inicio de sesión, Tarjeta, Identidad, Nota segura), and 'CARPETAS' (with sub-option: Sin carpeta). On the right, the main area is titled 'Vault Items' and displays the message 'No hay elementos que listar.' There is a blue button labeled '+ Añadir elemento'. On the far right, there is a yellow box titled 'VERIFICAR CORREO ELECTRÓNICO' containing the text: 'Verifica el correo electrónico de tu cuenta para desbloquear todas estas características.' and a blue button labeled 'Enviar correo electrónico'.

© 2022, Bitwarden Inc.

Versión 2022.5.2

Si tenemos toda la configuración bien nos saldrá un mensaje en verde de que se ha enviado el correo para que se pueda verificar.

The screenshot shows the Bitwarden verification process. At the top, there is a user icon and a dropdown menu. Below the header, on the left, is a yellow box titled 'VERIFICAR CORREO ELECTRÓNICO' containing the text: 'Verifica el correo electrónico de tu cuenta para desbloquear todas estas características.' and a blue button labeled 'Enviar correo electrónico'. On the right, a green box with a checkmark contains the message: 'Comprueba el enlace de verificación en tu cuenta de correo.'

## Verificamos el correo.

The screenshot shows an email inbox with a message from 'Bitwarden no-reply@bitserver-zaka.ddns.net'. The subject is 'Verify Your Email' and it includes a link to verify the email address. The email is marked as 'Externo' (External) and has 'Recibidos' (Received) status. The interface includes standard email controls like back, forward, and search. A small preview window shows the Bitwarden verification page with the 'bitwarden' logo and a 'Verify Email Address Now' button.

Y por último se termina la configuración de Bitwarden ya esta listo para un uso local seguro y se pueden cambiar los puertos para asegurarlo mas si hay necesidad de que salga por internet. (Nota: Yo estoy usando NoIP como un Nombre de Dominio DNS gratuito.)

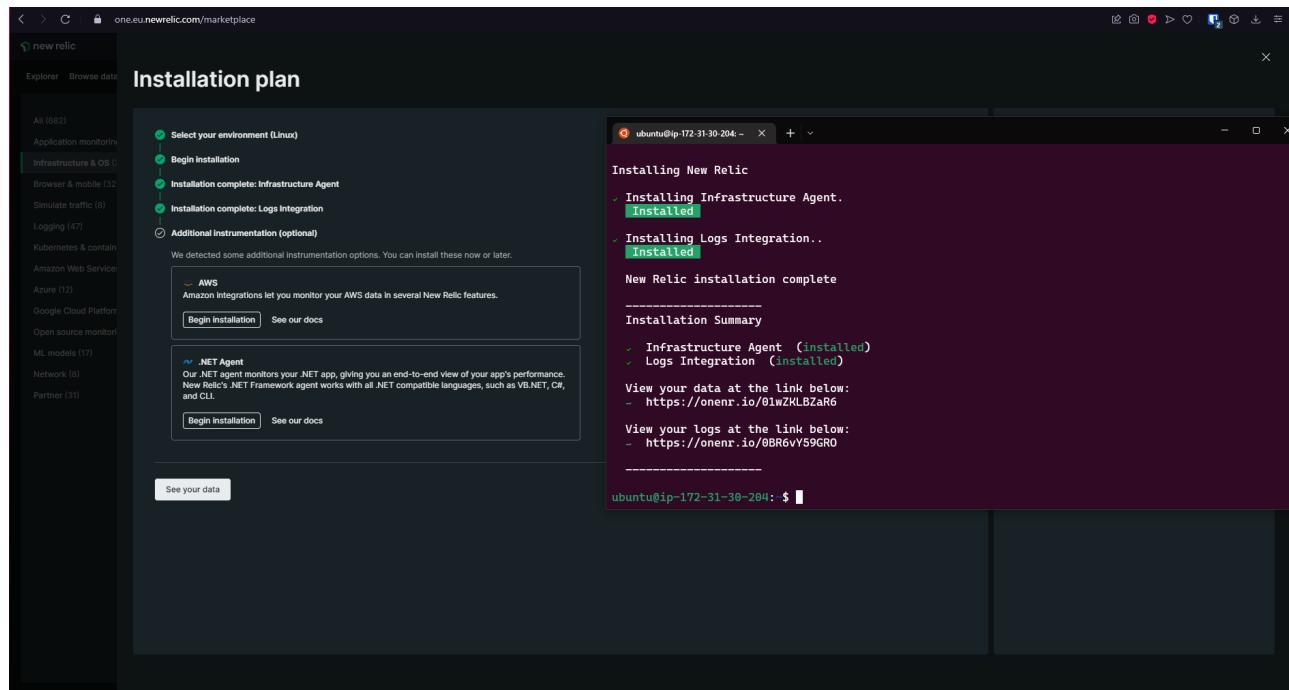
The screenshot shows the Bitwarden login page. It features the 'bitwarden' logo and a message asking users to log in or create a new account to access their secure vault. A prominent green success message box in the top right corner states 'Tu cuenta de correo ha sido verificada.' (Your email account has been verified). The login form includes fields for 'Correo electrónico' (Email address) containing 'zelk991@g.educaand.es', 'Contraseña maestra' (Master password), and a checkbox for 'Recordar correo electrónico' (Remember email). Below the form are two buttons: 'Identificarse' (Log in) and 'Crear cuenta' (Create account). At the bottom, there's a link for 'Inicio de sesión único empresarial' (Enterprise single sign-on) and copyright information: '© 2022, Bitwarden Inc. Versión 2022.5.2'.

Instalación de Agente de New Relic en el servidor donde esta alojado Bitwarden.

## 1. Entramos en New Relic y añadimos un nuevo host Linux.

## 2. Copiamos el comando y lo ejecutamos en nuestro servidor Bitwarden.

## 3. Una vez instalado y conectado, como tenemos Bitwarden con Docker debemos ejecutar el servicio de Docker de New relic.



#### 4. Buscamos Docker y ejecutamos el comando que nos proporciona.

#### 5. Tras ejecutar el comando se iniciara el contenedor docker de New Relic para que pueda monitorizar todos mis contenedores docker.

```

ubuntu@ip-172-31-30-204: ~ + ~
> --name newrelic-infra \
> --network=host \
> --cap-add=SYS_PTRACE \
> --privileged \
> --pid=host \
> -v "/:/host:ro" \
> -v "/var/run/docker.sock:/var/run/docker.sock" \
> -e NRRLICENSE_KEY=u01xx8fff41f2909b237d9606b756e11e06eNRAL \
> newrelic/infrastructure:latest
Unable to find image 'newrelic/infrastructure:latest' locally
latest: Pulling from newrelic/infrastructure
2408ccf74d12: Pull complete
094c8ecf75b54: Pull complete
87a17af91ea: Pull complete
566a3a69d: Pull complete
bde9c1588ef: Pull complete
0d12a2a332d: Pull complete
f408d6a4ub92: Pull complete
c75c55f50937: Pull complete
1ce1792ea8d0: Pull complete
50a895cc24b: Pull complete
Digest: sha256:0b43aca4ed833c29aadb90447ee44c7b0f4bcb81675dfecbb07e4
037fe61cd924
Status: Downloaded newer image for newrelic/infrastructure:latest
2b793113914f175aaabb371fed5d9b22edfc2c632310da62fc6b9ac31290f9045
ubuntu@ip-172-31-30-204: $ 

```

6. Una vez terminado podremos observar que ahora podemos ver los contenedores docker que tenemos de bitwarden.

| Name                    | CPU usage (cores) | CPU utilization (%) | Memory usage (bytes) | Storage usage (bytes) |
|-------------------------|-------------------|---------------------|----------------------|-----------------------|
| bitwarden-admin         | 0.00599           | 4.71 %              | 89.1 MB              | 38.7 MB               |
| bitwarden-api           | 0.00621           | 4.95 %              | 95.7 MB              | 27.8 MB               |
| bitwarden-attachments   | 0.0025            | 1.97 %              | 23.2 MB              | 33.1 MB               |
| bitwarden-events        | 0.00257           | 2.40 %              | 58.7 MB              | 28.1 MB               |
| bitwarden-icons         | 0.00254           | 2 %                 | 63.8 MB              | 20.6 MB               |
| bitwarden-identity      | 0.00259           | 2.01 %              | 78.3 MB              | 25.6 MB               |
| bitwarden-mssql         | 0.00779           | 7.68 %              | 459 MB               | 1.95 GB               |
| bitwarden-nginx         | 0.00261           | 2.06 %              | 11.2 MB              | 23.9 MB               |
| bitwarden-notifications | 0.00229           | 2.27 %              | 56.4 MB              | 39.2 MB               |
| bitwarden-sso           | 0.00275           | 2.16 %              | 55.6 MB              | 38.2 MB               |
| bitwarden-web           | 0.00265           | 2.09 %              | 36.8 MB              | 14.3 MB               |

7. Para centralizar el Host y los contenedores en un solo lugar crearemos un Workload, con los contenedores y el host donde se estan ejecutando. Para ello pinchamos en "+ Create Workload".

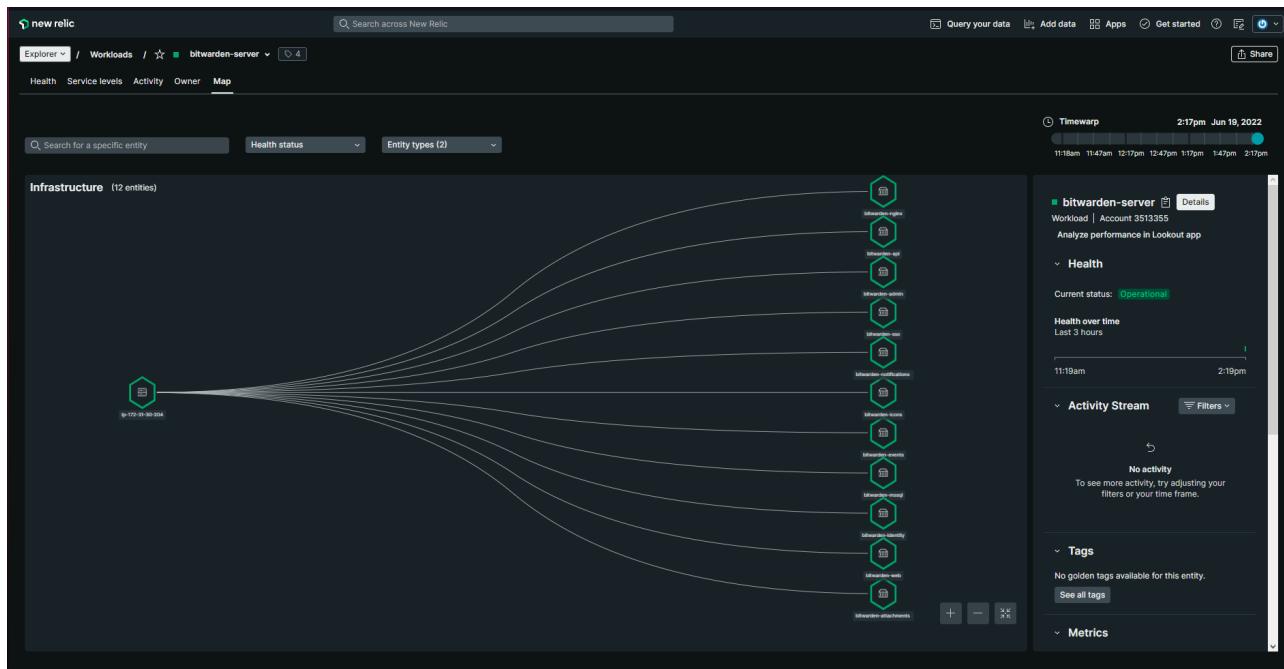
## 8. Seleccionaremos los contenedores de Bitwarden y el Host correcto de Bitwarden.

The screenshot shows the 'Create a workload' page in the New Relic interface. The 'Included entities' section displays 12 entities, all of which are containers under the 'bitwarden' namespace. These include 'bitwarden-identity', 'bitwarden-mssql', 'bitwarden-nginx', 'bitwarden-notifications', 'bitwarden-sso', and 'bitwarden-web', each associated with Account 3513355. Other entities listed are hosts with IP addresses 172.31.16.22, 172.31.27.153, and 172.31.30.204, also associated with Account 3513355.

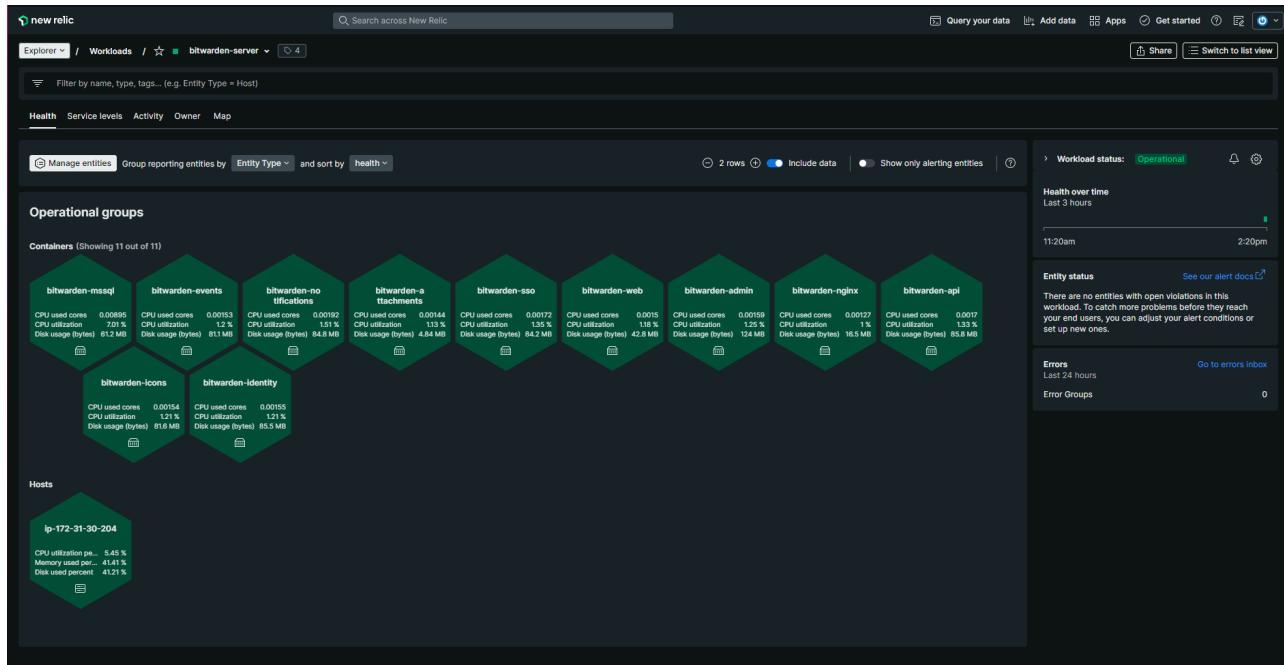
## 9. Entramos al Workload y podremos ver que se ven los datos de los contenedores y del Host centralizado.

The screenshot shows the 'Workloads' dashboard for the 'bitwarden-server' workload. It displays monitoring charts for CPU usage, memory usage, storage usage, and network transmit traffic across multiple containers and hosts. The charts show data for the last 30 minutes. The 'Events timeline' section indicates that a new workload was created for 'zakariyasmr1920@gmail.com' at 2:18pm.

## 10. Podemos pinchar en "Map" y veremos como es capaz de tener un mapa del sistema que tenemos montado.



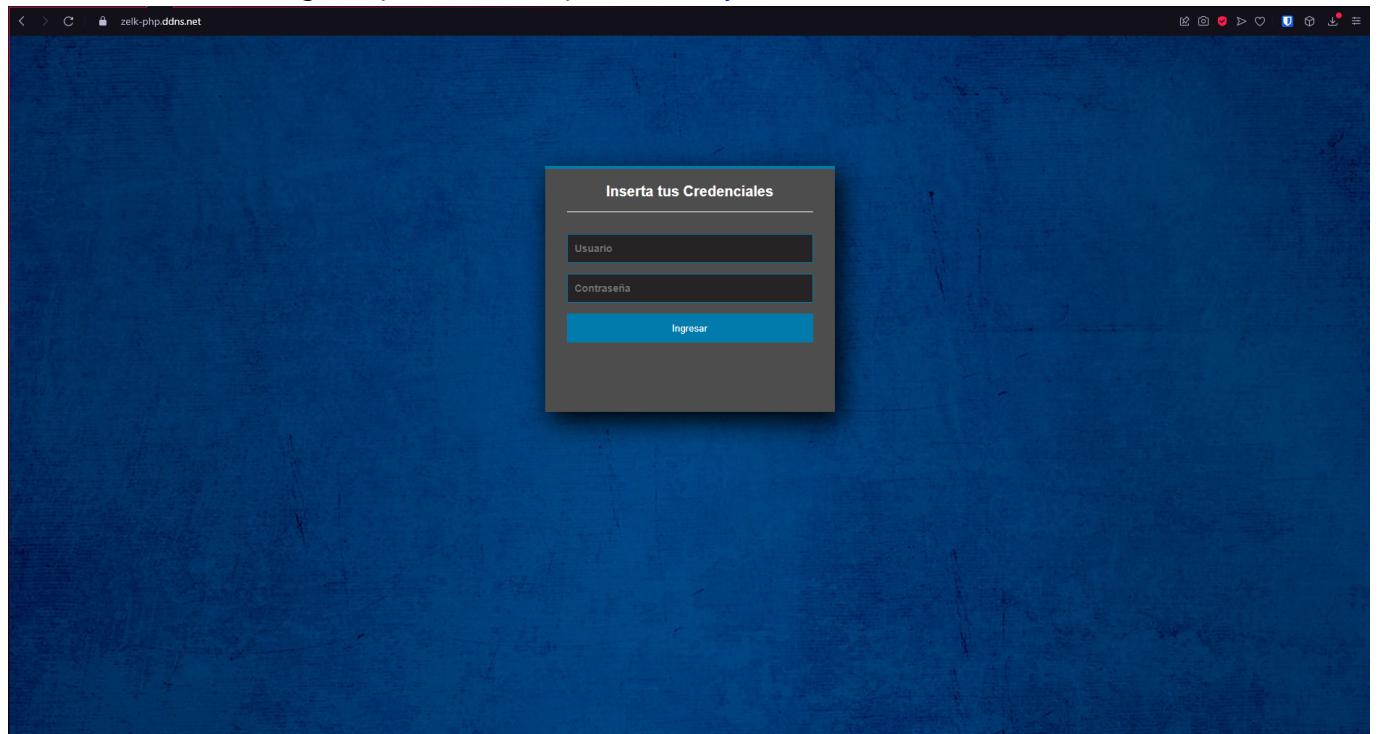
11. De esta forma podemos tener Monitorizado nuestro Servidor Bitwarden de forma centralizada.



## Monitorización de mi Pagina Web En PHP.

La Página Web consiste en una simulación de una pequeña tienda virtual programada en PHP/HTML con una pequeña base de datos(no es mía). Esta implementada en una Pila LAMP con docker y Docker Compose.

Puedes observar el código empleado en el repositorio [Proyecto-ASIR](#)

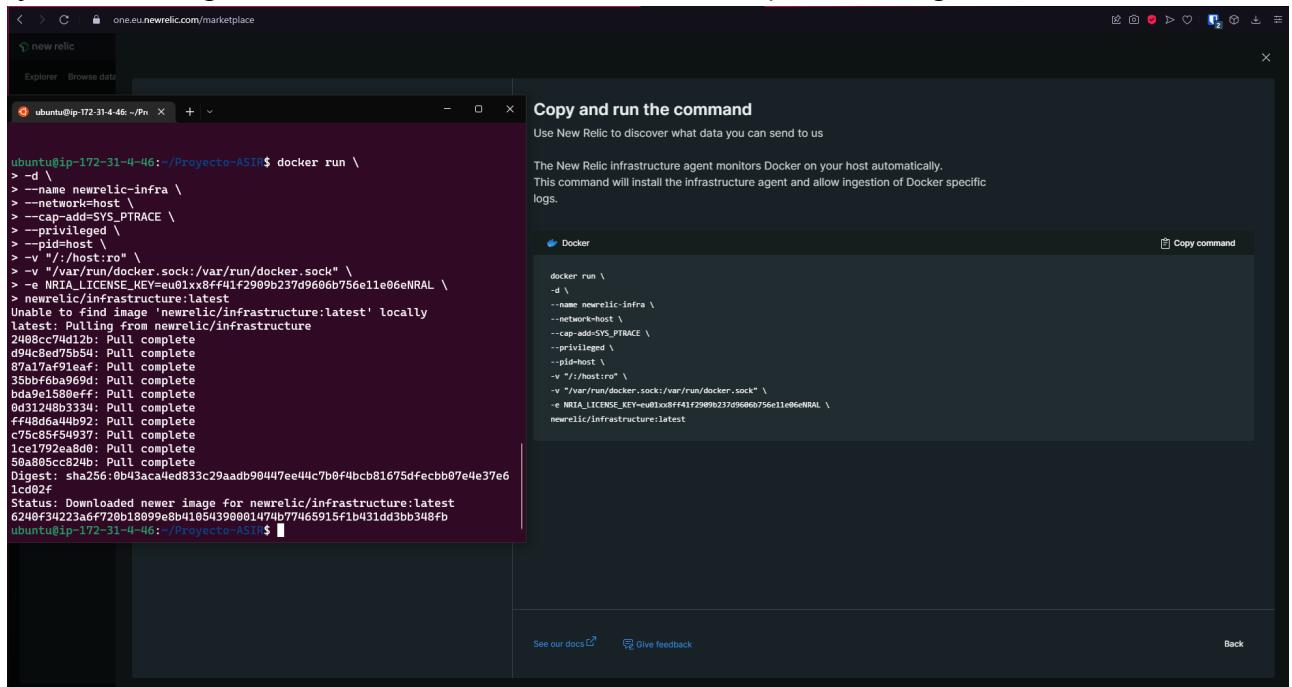


## Monitorizar Página Web en PHP Con Docker.

- Como esta implementada con docker haremos los mismos pasos que hicimos con Bitwarden. Primero ejecutamos el Agente del Host Linux de New Relic donde esta desplegado la Página Web.

Nota: El agente de Apache no va a funcionar en esta máquina ya que no está localmente si no en una imagen docker.

## 2. Ejecutamos el Agente de Docker de New Relic en nuestra maquina de la Pagina Web PHP.

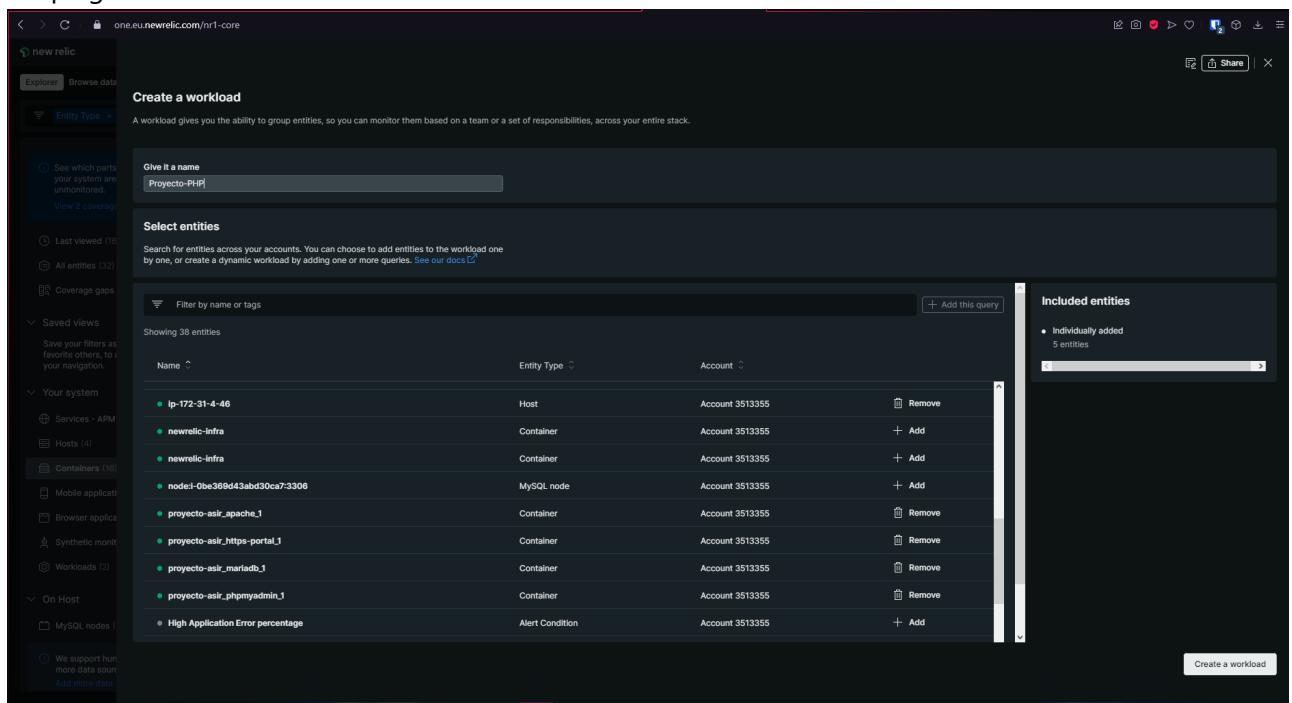


```
ubuntu@ip-172-31-4-46:~/Proyecto-ASIR$ docker run \
> -d \
> --name newrelic-infra \
> --network=host \
> --cap-add=SYS_PTRACE \
> --privileged \
> --pid=host \
> -v "/:/host:ro" \
> -v "/var/run/docker.sock:/var/run/docker.sock" \
> -e NRRLICENSE_KEY=eu01xx8f41f2909b237d9606b756e11e06eNRAL \
> newrelic/infrastucture:latest
The New Relic infrastructure agent monitors Docker on your host automatically.
This command will install the infrastructure agent and allow ingestion of Docker specific
logs.

Docker
Copy command
```

The terminal shows the command being run and its output, indicating successful installation of the New Relic infrastructure agent.

## 3. Creamos un Workload del Proyecto en PHP con los contenedores necesarios y el host donde estan desplegados los contenedores.



**Create a workload**

A workload gives you the ability to group entities, so you can monitor them based on a team or a set of responsibilities, across your entire stack.

**Give it a name**

**Select entities**

Search for entities across your accounts. You can choose to add entities to the workload one by one, or create a dynamic workload by adding one or more queries. See our docs [\[Link\]](#)

| Name                              | Entity Type     | Account         | Action                 |
|-----------------------------------|-----------------|-----------------|------------------------|
| ip-172-31-4-46                    | Host            | Account 3513355 | <a href="#">Remove</a> |
| newrelic-infra                    | Container       | Account 3513355 | <a href="#">Add</a>    |
| newrelic-infra                    | Container       | Account 3513355 | <a href="#">Add</a>    |
| node1-0be389d43abd30ca7-3306      | MySQL node      | Account 3513355 | <a href="#">Add</a>    |
| proyecto-asir_apache_1            | Container       | Account 3513355 | <a href="#">Remove</a> |
| proyecto-asir_https-portal_1      | Container       | Account 3513355 | <a href="#">Remove</a> |
| proyecto-asir_mariadb_1           | Container       | Account 3513355 | <a href="#">Remove</a> |
| proyecto-asir_phpcryptadmin_1     | Container       | Account 3513355 | <a href="#">Remove</a> |
| High Application Error percentage | Alert Condition | Account 3513355 | <a href="#">Add</a>    |

**Included entities**

- Individually added
  - 5 entities

[Create a workload](#)

4. Y ya tenemos nuestros contenedores y Host monitorizados de una manera centralizada.

The screenshot shows the New Relic Infrastructure Map interface. At the top, there's a navigation bar with 'new relic', a search bar 'Search across New Relic', and various links like 'Query your data', 'Add data', 'Apps', 'Get started', and 'Share'. Below the navigation is a timeline header 'Timewarp' showing a range from 8:38pm to 11:37pm on June 19, 2022. The main area is titled 'Infrastructure (5 entities)' and displays five green hexagonal nodes representing hosts. One node is labeled 'Proyecto-PHP' and is connected to four other nodes labeled 'y-07-31-a8', 'proyecto-ml-apply-poc-1', 'proyecto-ml-apply-poc-2', and 'proyecto-ml-apply-poc-3'. A fifth node, 'proyecto-ml-apply-poc-4', is also present. On the right side of the interface, there's a detailed view for the 'Proyecto-PHP' host, showing its current status as 'Operational' and an activity stream with several log entries.

## Monitorizar el tráfico de nuestra web.

Gracias al sistema que nos proporciona New Relic con Browser monitoring. Nos proporciona un simple script que podemos pegar en nuestra página Web y en unos minutos ya estamos monitorizando el tráfico que tiene nuestra Web.

The screenshot shows the New Relic browser monitoring dashboard. The left sidebar has a 'Browser & mobile' section selected, with other categories like 'All (10)', 'Application monitoring (2)', 'Infrastructure & OS (1)', 'Simulate traffic (0)', 'Logging (1)', 'Kubernetes & containers (0)', 'Amazon Web Services (0)', 'Azure (0)', 'Google Cloud Platform (0)', 'Open source monitoring (0)', 'ML models (0)', 'Network (0)', and 'Partner (1)'. The main area has a search bar 'browser' and a 'Data sources' tab. Under 'Data sources', there are two cards: 'Browser monitoring' and 'Netlify Builds'. To the right, there's a large panel titled 'Browser & mobile monitoring' with descriptive text about monitoring end-user experience across the entire technology stack. It includes sections on browser monitoring, mobile monitoring, and crash analysis, along with a bulleted list of actions one can take.

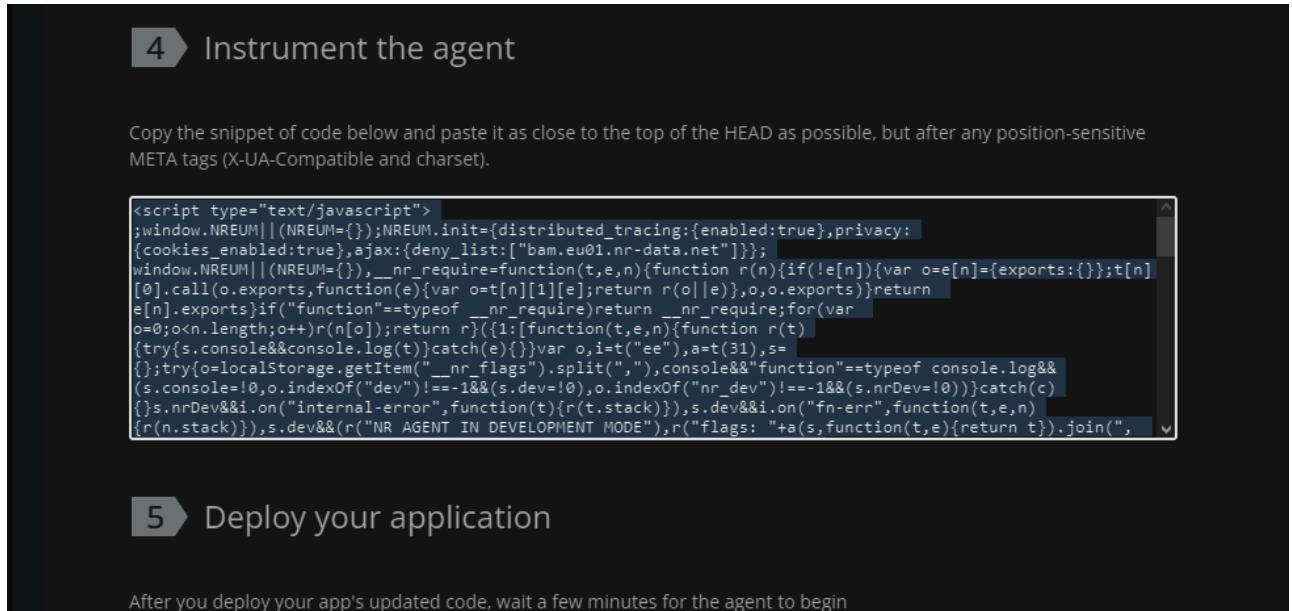
## 1. Pinchamos en Browser Monitoring, y seleccionis el modo **Copy/Paste Javascript code**.

The screenshot shows the New Relic Marketplace interface for browser monitoring. On the left sidebar, 'Browser & mobile (32)' is selected. In the main content area, step 1 'Choose a deployment method' has 'Copy/Paste Javascript code' selected. Step 2 'Configure your instrumentation' shows 'Distributed Tracing Recommended' is turned on. A sidebar on the right titled 'Why deploy via New Relic APM?' lists four reasons: 1. Because the agent acts server-side, it automatically deploys instrumentation to every page of your website. 2. You'll automatically get the latest version of the Browser agent whenever you restart your APM agent. 3. Since the agent also powers New Relic APM, you'll gain deep visibility into backend service performance, as well. 4. You'll be connected frontend to backend in one step, making distributed tracing more powerful.

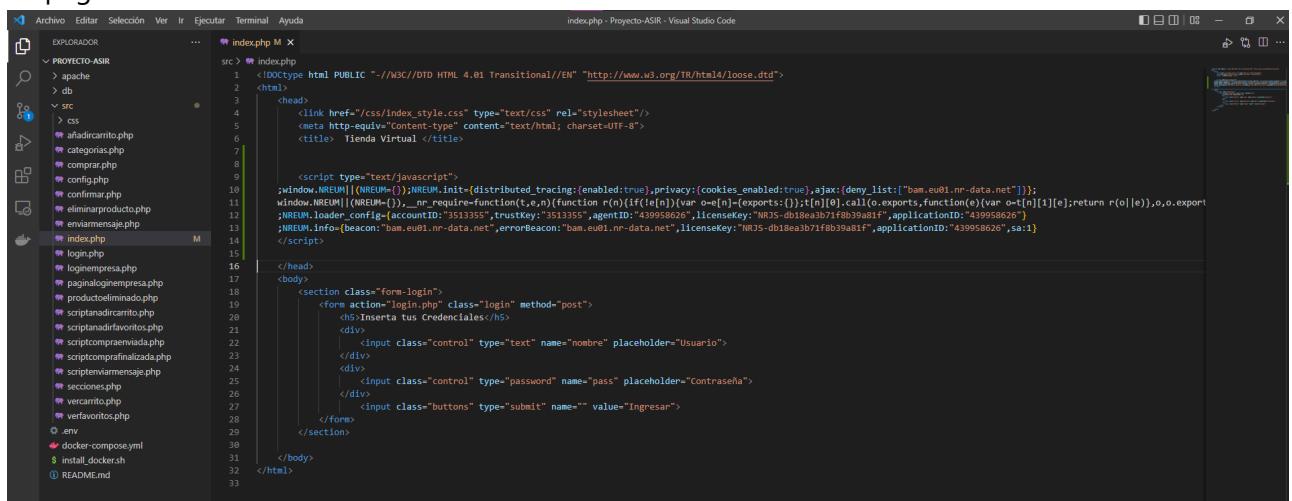
## 2. Dejamos las "instrumentation" por defecto. Seleccionamos que no esta la app y le damos un nombre a nuestra App.

The screenshot shows the continuation of the New Relic Marketplace setup. It includes the 'Cookie collection' section and the 'Name your app' section. In the 'Name your app' section, the 'No. (Name your standalone app)' radio button is selected, and the input field 'Name' contains 'Proyecto-PHP'. A blue 'Enable' button is present at the bottom of this section.

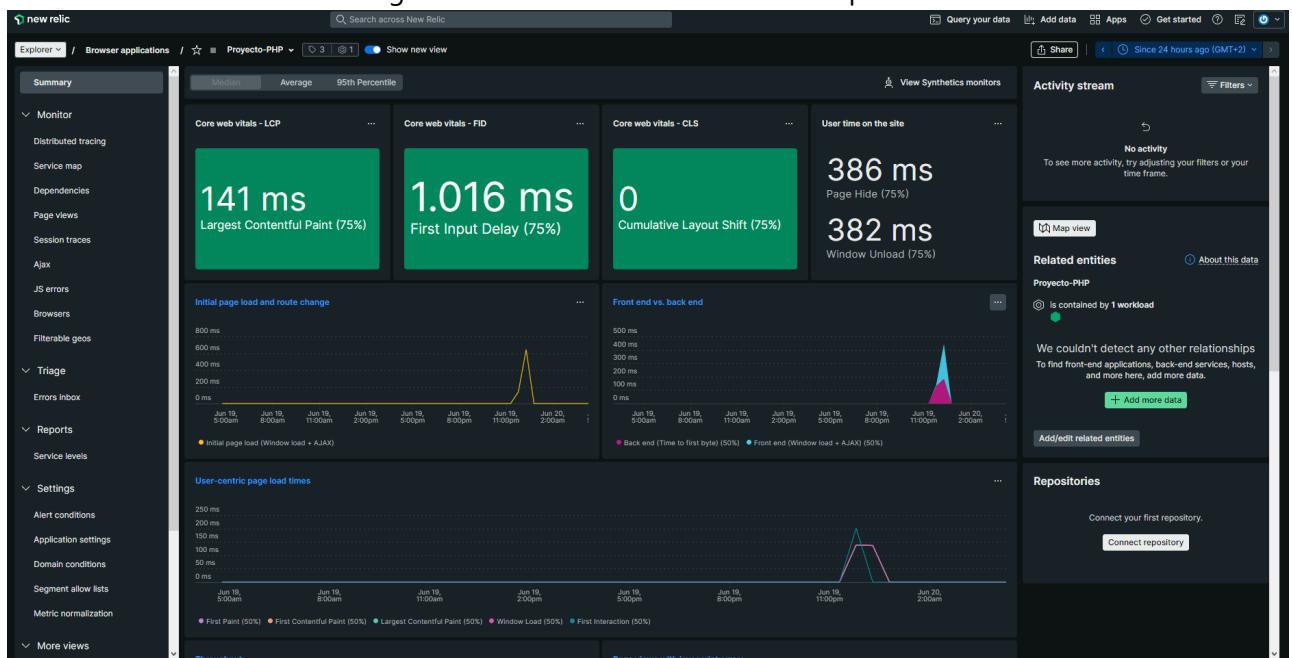
3. Nos proporcionara un script que debemos pegar en nuestro index.php



4. Lo pegamos en el HEAD de nuestro index.



5. Accedemos de nuevo a New Relic y entramos en Browser y pinchamos en el nombre de nuestra App, al cabo de unos minutos cuando generemos trafico de varios sitios empezará a mostrar datos.



No se puede observar todos los servicios pero nos puede mostrar demasiado con tanta sensillez.



## Monitorización de Github Pages con New Relic.

Aplicando la Monitorización de Browser de New Relic podemos monitorizar el tráfico de nuestra Web alojada en Github.

### 1. Creamos una nueva App Browser en New Relic y copiamos el Script.

The screenshot shows the 'Settings' page for the 'shop-zaka' application under 'Application settings'. The 'Distributed Tracing' section is highlighted:

- Agent and account**: Options for Lite, Pro, or Pro + SPA instrumentation.
- Distributed Tracing**: A code editor containing the distributed tracing script. It includes a note about pasting the script just above the first script tag in the HEAD or bottom of the HEAD.
- Triage**: A section for monitoring and analyzing browser requests end-to-end across distributed systems, requiring APM Pro and Browser Pro + SPA agent and account.
- Cross Origin Resource Sharing (CORS)**: Configuration for adding origins to see distributed traces for cross-origin AJAX calls.
- WARNING**: A note about custom headers and W3C trace context headers for AJAX requests.

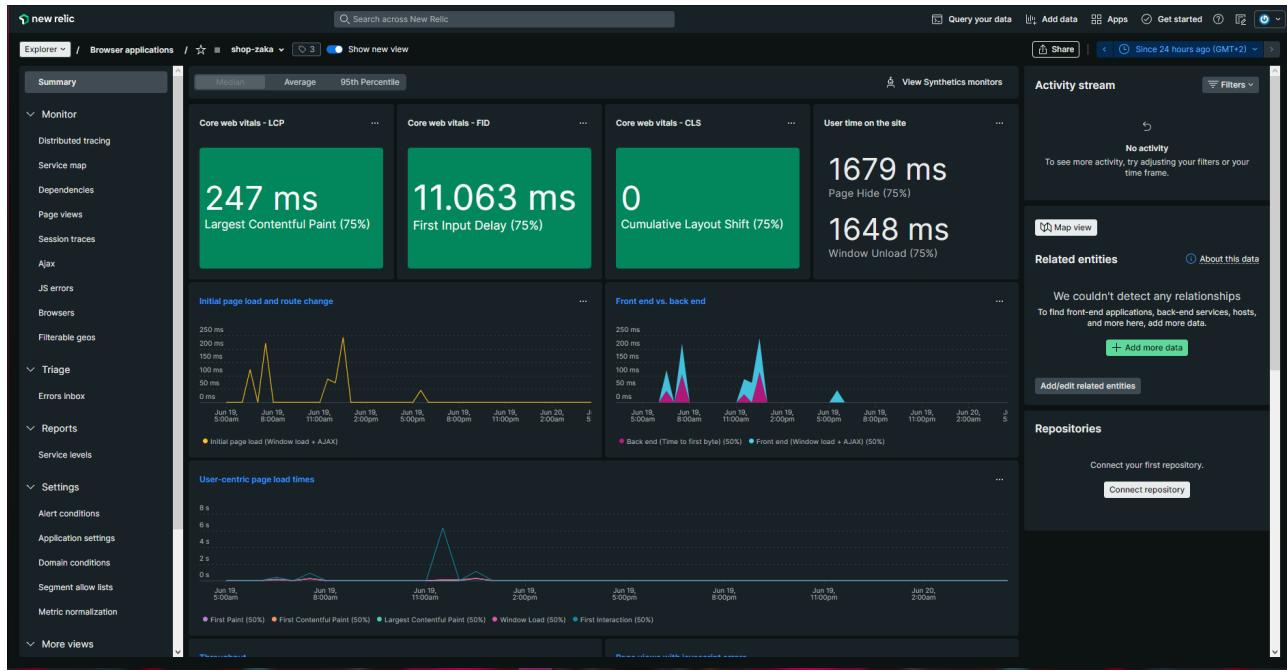
## 2. Pegamos el Script en nuestro Index alojado en Github.

```

1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="utf-8">
5   <title>HTML</title>
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <link rel="stylesheet" href="estilo.css">
8
9   <script type="text/javascript">
10  ;window.NREUM||(NREUM.init({distributed_tracing:(enabled:true),privacy:(cookies_enabled:true),ajax:{deny_list:["bam.eu01.nr-data.net"]}}));
11  ;NREUM||(NREUM||{}).nr_require=function(t,e,n){function r(){if([e[n]]){var o=[n];exports[t]=i[n][0].call(o,exports,function(e){var o=t[n][i[e]];return r(o||e)});o.e
12  ;NREUM.louder_config={accountID:"3513355",trustKey:"3513355",agentID:"438889461",licenseKey:"NRJS-dB18ea3b71f8b39a81f",applicationID:"438889461",ia:i}
13  ;NREUM.info=(beacon:"bam.eu01.nr-data.net",errorBeacon:"bam.eu01.nr-data.net",licenseKey:"NRJS-dB18ea3b71f8b39a81f",applicationID:"438889461",ia:i)
14  </script>
15
16
17  </head>
18
19  <body>
20   <p>Esta página web es una página HTML válida.</p>
21  </body>
22
23 </html>

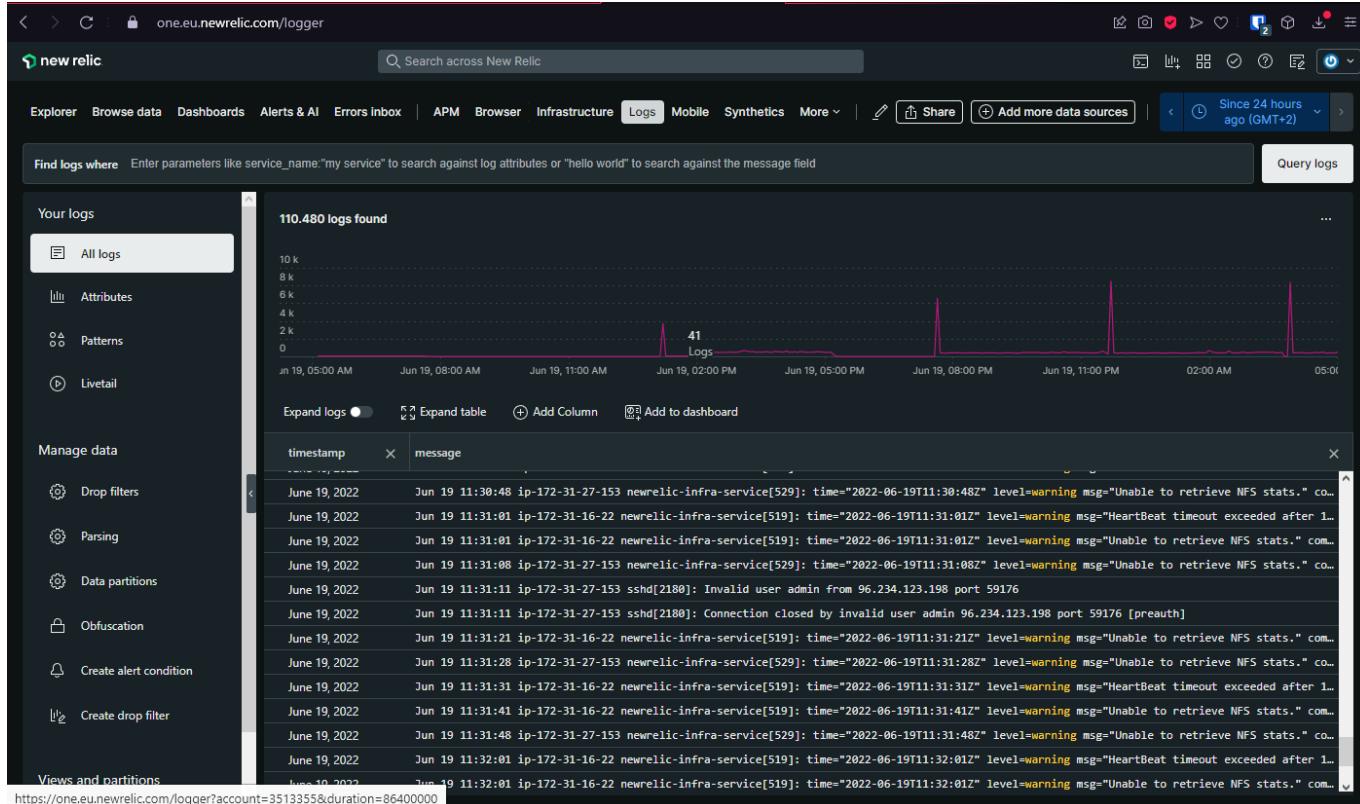
```

## 3. Esperamos unos minutos mientras generamos trafico y veremos que empiezan a entrar datos de nuestra App.

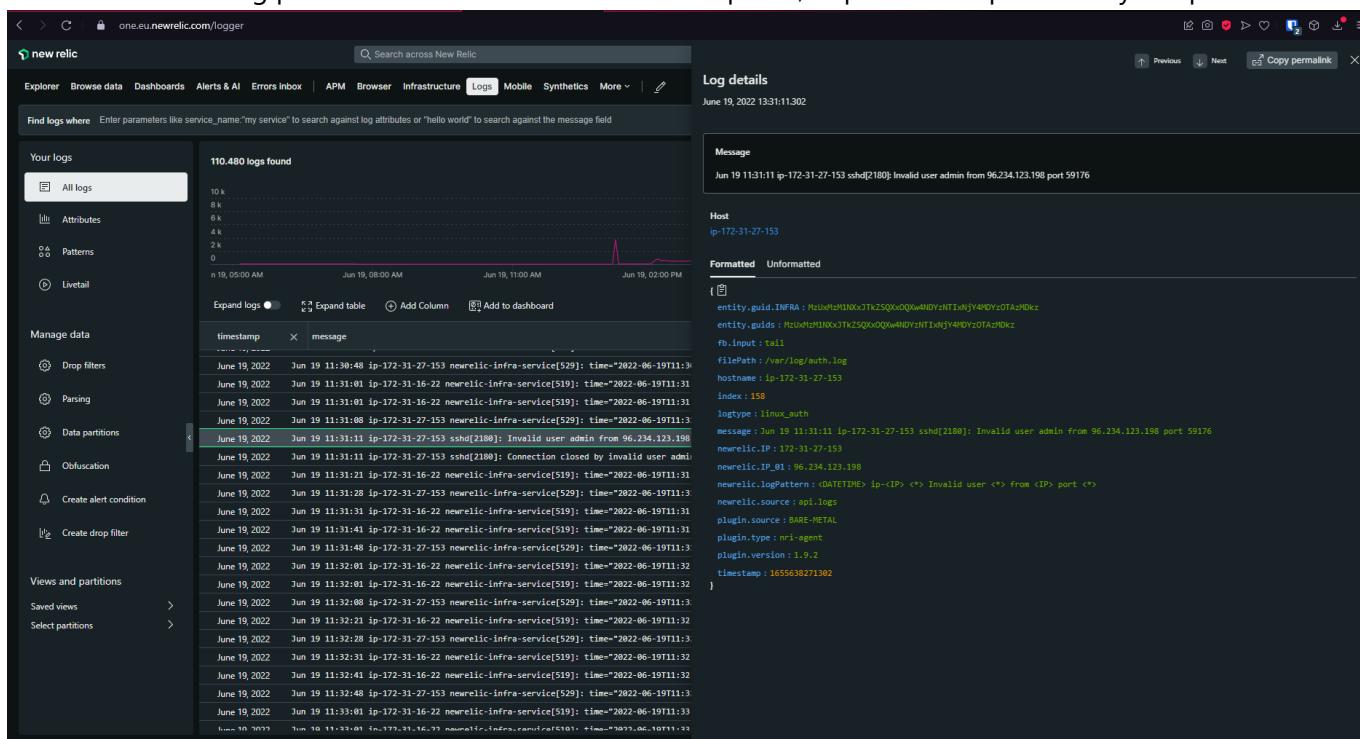


## Sistema de Logs New Relic

New Relic nos permite ver todos los logs que tienen todos nuestros sistemas a la vez eso nos permite ver si hay algun problema sin estar buscando en que maquina o servicio a sido.



Pinchando en un Log podremos ver todos los detalles de que es, a que servicio pertenece y de que se trata.



## Biografia

- [New Relic](#)
- [Bitwarden](#)
- [Jose Juan GitHub](#)
- [Jose Juan IAW](#)
- [Mi Colega Angonca El Creador de la base de datos de la Página Web](#)
- [MailGun](#)

## Conclusión

En Conslusión New Relic es un buen software para Monitorizar cualquier cosa que deseas. La desventaja es si no entiendes mucho ingles como me ha pasado a mi te va a costar mucho entender la plataforma y el software ya que toda su documentación se encuentra en ingles auqneu tienen explicado todo y cada uno de sus servicios y como funcionan y te ofrecen soporte. Yo recomiendo usar el Sotfware New Relic para monitorizar. Pero lo que mas recomiendo es el uso del gestor de Contraseñas de Bitwarden es el mejor gestor de contraseñas en el momento.