

Icinga2

Autores:

- Adrián González Rodríguez
- Abraham Ramos Martín
- Cristian Santos Guillén
- Javier Valencia Rodríguez

¿Qué es icinga2?

- **Icinga** es un fork de **Nagios** creado en el año 2009. Es un sistema de monitorización de infraestructuras que añade más funcionalidades a Nagios.
- Desarrollado en lenguaje C.
- Versión actual es Icinga2.
- Licencia GNU GPL (Software Libre).

Mejoras respecto a Nagios:

- Moderna interfaz web.
- Incorporación de conectores adicionales para bases de datos (**MySQL/MariaDB, Oracle y PostgreSQL**).
- REST API.
- Compatibilidad con Nagios y sus plugins.
- Al ser software libre y disponer de una REST API, ha permitido que Icinga2 reciba mejoras de manera continua gracias a la comunidad y a las peticiones de los usuarios.

Características:

- Monitorización de *componentes de red* (switches, routers, etc.)
- Monitorización de *servicios de red* (SMTP, POP3, HTTP, ping, etc.)
- Notificación a usuarios por correo electrónico
- Nivel de alertas (**Email, SMS, llamada telefónica, etc.**)
- Opción de utilizar la interfaz clásica o la actualizada

Icinga Classic UI

The screenshot displays the Icinga Classic UI interface. At the top, a status bar shows overall system health: 26 UP, 0 DOWN, 0 UNREACHABLE, 0 PENDING, 4/30 TOTAL. Below this, a more detailed status bar shows 32 OK, 0 WARNING, 2 CRITICAL, 0 UNKNOWN, 0 PENDING, 10/45 TOTAL. The left sidebar contains navigation links for General, Status, Problems, System, and Reporting. The main content area is titled 'Current Network Status' and shows a table of host status details for all hosts. The table has columns for Host, Status, Last Check, Duration, and Attempt. The right sidebar contains a 'Select command' menu with various actions like 'Add a Comment to Checked Host(s)', 'Disable Active Checks Of Checked Host(s)', 'Enable Active Checks Of Checked Host(s)', 'Re-schedule Next Host Check', 'Submit Passive Check Result For Checked Host(s)', 'Stop Accepting Passive Checks For Checked Host(s)', 'Start Accepting Passive Checks For Checked Host(s)', 'Stop Obsessing Over Checked Host(s)', 'Start Obsessing Over Checked Host(s)', 'Acknowledge Checked Host(s) Problem', 'Remove Problem Acknowledgement', 'Disable Notifications For Checked Host(s)', 'Enable Notifications For Checked Host(s)', 'Send Custom Notification', 'Delay Next Host Notification', 'Schedule Downtime For Checked Host(s)', 'Schedule Downtime For Checked Host(s) and All Services', 'Disable Notifications For All Services On Checked Host(s)', 'Enable Notifications For All Services On Checked Host(s)', 'Schedule A Check Of All Services On Checked Host(s)', 'Disable Checks Of All Services On Checked Host(s)', 'Enable Checks Of All Services On Checked Host(s)', 'Disable Event Handler For Checked Host(s)', 'Enable Event Handler For Checked Host(s)', 'Disable Flap Detection For Checked Host(s)', 'Enable Flap Detection For Checked Host(s)', and 'check_alive.phpsh: OK (t2-switch-1 is on)'.

Icinga: classic.demo.icinga.org

26 UP 0/0/0 DOWN 0/0/0 UNREACHABLE 0 PENDING 4/30 TOTAL

32 OK 0/0/0 WARNING 2 CRITICAL 0/0/0 UNKNOWN 0 PENDING 10/45 TOTAL

General

- Home
- Documentation
- Search:

Status

- Tactical Overview
- Host Detail
- Service Detail
- Hostgroup Overview
- Hostgroup Summary
- Servicegroup Overview
- Servicegroup Summary
- Status Map

Problems

- Service Problems
- Unhandled Services
- Host Problems
- Unhandled Hosts
- All Unhandled Problems
- Network Outages

System

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration

- View Config
- Run script "void():"

Current Network Status

Last Updated: Thu May 31 08:16:10 CEST 2012 - Update in 57 seconds (pause)

Icinga 1.7.0 - Logged in as guest

- View History For All Hosts
- View Notifications For All Hosts
- View Host AND Services For All Hosts
- View Service Status Detail For All Hosts

Host Status Details For All Hosts

Host	Status	Last Check	Duration	Attempt
c1-db1	UP	05-31-2012 08:12:45	226d 16h 8m 0s	1/10
c1-db2	UP	05-31-2012 08:12:45	106d 10h 15m 55s	1/10
c1-fw	UP	05-31-2012 08:12:55	226d 16h 4m 10s	1/10
c1-http	UP	05-31-2012 08:13:05	218d 20h 49m 35s	1/10
c1-mail1	UP	05-31-2012 08:13:15	108d 19h 10m 25s	1/10
c1-mail2	UP	05-31-2012 08:13:25	217d 0h 34m 20s	1/10
c1-nagios	UP	05-31-2012 08:13:35	218d 20h 50m 5s	1/10
c1-router	UP	05-31-2012 08:13:45	65d 21h 2m 15s	1/10
c1-switch	UP	05-31-2012 08:13:55	226d 16h 3m 50s	1/10
c1-tt1	UP	05-31-2012 08:14:05	162d 22h 22m 12s	1/10
c2-app-1	UP	05-31-2012 08:14:15	217d 0h 34m 20s	1/10
c2-dbsvr-1	UP	05-31-2012 08:14:25	217d 0h 34m 20s	1/10
c2-flo-1	UP	05-31-2012 08:14:35	217d 0h 34m 20s	1/10
c2-fw-1	UP	05-31-2012 08:14:45	217d 0h 34m 20s	1/10
c2-mail-1	UP	05-31-2012 08:14:55	217d 0h 34m 20s	1/10
c2-primsrv-1	UP	05-31-2012 08:15:05	217d 0h 34m 20s	1/10
c2-proxy	UP	05-31-2012 08:15:15	217d 0h 34m 20s	1/10
c2-router-1	UP	05-31-2012 08:15:25	162d 22h 22m 52s	1/10
c2-switch-1	UP	05-31-2012 08:15:35	162d 22h 19m 42s	1/10

Select command

- Add a Comment to Checked Host(s)
- Disable Active Checks Of Checked Host(s)
- Enable Active Checks Of Checked Host(s)
- Re-schedule Next Host Check
- Submit Passive Check Result For Checked Host(s)
- Stop Accepting Passive Checks For Checked Host(s)
- Start Accepting Passive Checks For Checked Host(s)
- Stop Obsessing Over Checked Host(s)
- Start Obsessing Over Checked Host(s)
- Acknowledge Checked Host(s) Problem
- Remove Problem Acknowledgement
- Disable Notifications For Checked Host(s)
- Enable Notifications For Checked Host(s)
- Send Custom Notification
- Delay Next Host Notification
- Schedule Downtime For Checked Host(s)
- Schedule Downtime For Checked Host(s) and All Services
- Disable Notifications For All Services On Checked Host(s)
- Enable Notifications For All Services On Checked Host(s)
- Schedule A Check Of All Services On Checked Host(s)
- Disable Checks Of All Services On Checked Host(s)
- Enable Checks Of All Services On Checked Host(s)
- Disable Event Handler For Checked Host(s)
- Enable Event Handler For Checked Host(s)
- Disable Flap Detection For Checked Host(s)
- Enable Flap Detection For Checked Host(s)
- check_alive.phpsh: OK (t2-switch-1 is on)

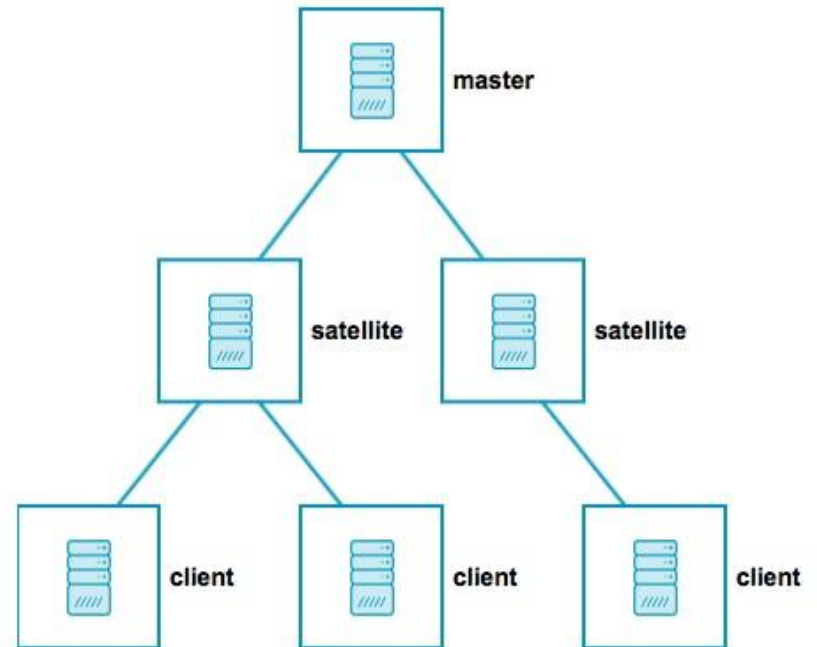
Icinga Web

The screenshot displays the Icinga Web interface, which is divided into several sections:

- Left Sidebar:** Contains navigation links for Search, Dashboard, Problems (with a red badge indicating 3 issues), Overview, Icinga Director, History, Graphite, Documentation, System, Configuration, and admin.
- Top Bar:** Includes tabs for Current Incidents, Overdue, Muted, Host, Services, and History.
- Service Problems:** A list of critical and warning issues for various services like 'demo: ssh', 'demo: cluster-zone', 'demo: disk', 'demo: ido', and 'demo: apt'. Each entry shows the status, time, and a brief description of the problem.
- Recently Recovered Services:** A list of services that have returned to an 'OK' state, including 'demo: load', 'srv-web1.icinga.com: ping4', 'srv-web1.icinga.com: http', and several 'server-*: ping4' entries.
- Host Problems:** A section indicating that no hosts match the current filter.
- Host Details (demo):** Shows the host status as 'UP' since Nov 24, with 15 services (2 critical, 1 warning, 11 OK). It includes links for Check now, Comment, Notification, and Downtime.
- Plugin Output:** Displays the output of the 'PING OK' check, showing packet loss and RTA.
- Graphs:** Two line graphs are shown: 'Round trip time (ms)' and 'Packet loss (%)', both plotted over a 30-minute period.
- Problem handling:** A section for managing issues, including links for Comments, Downtimes, Actions, Hostgroups, and Linux Servers.
- Performance data:** A table showing performance metrics for 'rtt' and 'pl' (packet loss) with warning and critical thresholds.
- Notifications:** A section for managing notifications, including a link to Send notification.

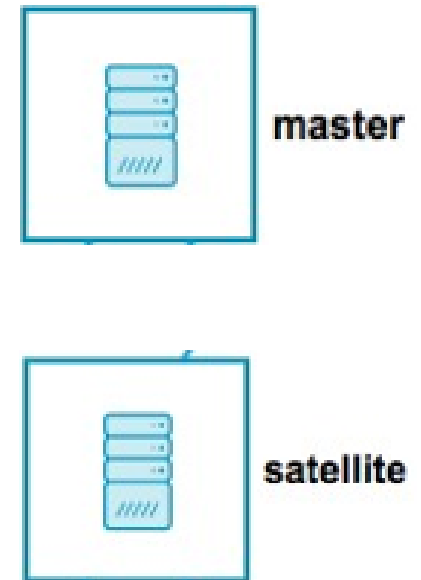
Funcionamiento

- **Maestro:**
 - **Nodo raíz.**
- **Satélite:**
 - **Nodo subordinado de maestro. (Opcional)**
- **Cliente:**
 - **Nodos que van a ser monitorizados.**



Funcionamiento

- **Maestro:**
 - Es el principal.
 - Donde se instalan principalmente los servicios.
 - Obtiene, almacena y notifica.
- **Satélite:**
 - Opcional.
 - Ejecuta o delega sobre los clientes.
 - Recibe configuración sobre el Maestro.
 - Ayuda al Maestro.



Funcionamiento

- Cliente:
 - Proviene de nodo padre.
 - Ejecutará sus configuraciones.
 - Recibe eventos del Maestro o Satélite.



Configuración básica

- Maestro:
 - Servicio icinga2
 - Base de datos SQL
 - Interfaz web
 - Datos de los clientes
 - Notificaciones
- Cliente Windows:
 - NSClient++
 - Soporta otros agentes
- Cliente Linux:
 - SSH
 - Soporta otros agentes

Configuración maestro

- Instalar el repositorio de Icinga2:
 - `sudo apt-get install apt-transport-https`
 - `sudo wget -qO - https://packages.icinga.com/icinga.key | sudo apt-key add -`
 - `sudo add-apt-repository "deb https://packages.icinga.com/ubuntu icinga-bionic main"`
- Instalar Icinga2:
 - `sudo apt-get update`
 - `sudo apt-get install icinga2 monitoring-plugins`
- Habilitar acceso remoto a icinga2:
 - `sudo icinga2 api setup`

Una vez inicializado el acceso remoto debemos de añadir un usuario en el fichero **/etc/icinga2/conf.d/api-users.conf**:

- ```
object ApiUser "api_user" {
 password = "12345678"
 permissions = ["*"]
}
```

Reiniciamos el servicio para aplicar los cambios efectuados:

- `sudo systemctl restart icinga2`

# Configuración maestro

- Instalación de MYSQL:
  - `sudo apt-get install mysql-client mysql-server icinga2-ido-mysql`
  - `sudo mysql_secure_installation`
- Creación de base de datos:
  - `mysql -u root -p`
  - `CREATE DATABASE icinga2;`
  - `GRANT ALL ON icinga2.* TO 'icinga2'@'localhost' IDENTIFIED BY 'Icinga_2';`
  - `quit`
  
  - `mysql -u root -p icinga2 < /usr/share/icinga2-ido-mysql/schema/mysql.sql`
- Creación de usuario para el módulo:

Editamos el fichero **/etc/icinga2/features-available/ido-mysql.conf**:

  - ```
object IdoMysqlConnection "ido-mysql-2" {  
    user = "icinga2",  
    password = "Icinga_2",  
    host = "localhost",  
    database = "icinga2"  
}
```

Configuración maestro

- Habilitar módulo de MYSQL:

- `sudo icinga2 feature enable ido-mysql`

Ahora reiniciaremos el servicio para aplicar los cambios efectuados:

- `sudo systemctl restart icinga2`

- Instalación de la interfaz web:

- `sudo apt-get install apache2 icingaweb2 icingacli libapache2-mod-php`

- Creación de base de datos para la interfaz:

- `mysql -u root -p`

- `CREATE DATABASE icingaweb2;`

- `GRANT ALL ON icingaweb2.* TO 'icingaweb2'@'localhost' IDENTIFIED BY 'Icingaweb_2';`

- `quit`

- Generar token de configuración:


- `sudo icingacli setup token create`

- Reinicio del servicio apache2:/

- `sudo systemctl restart apache2`

Configuración cliente Windows

Descargar NSClient++



Windows

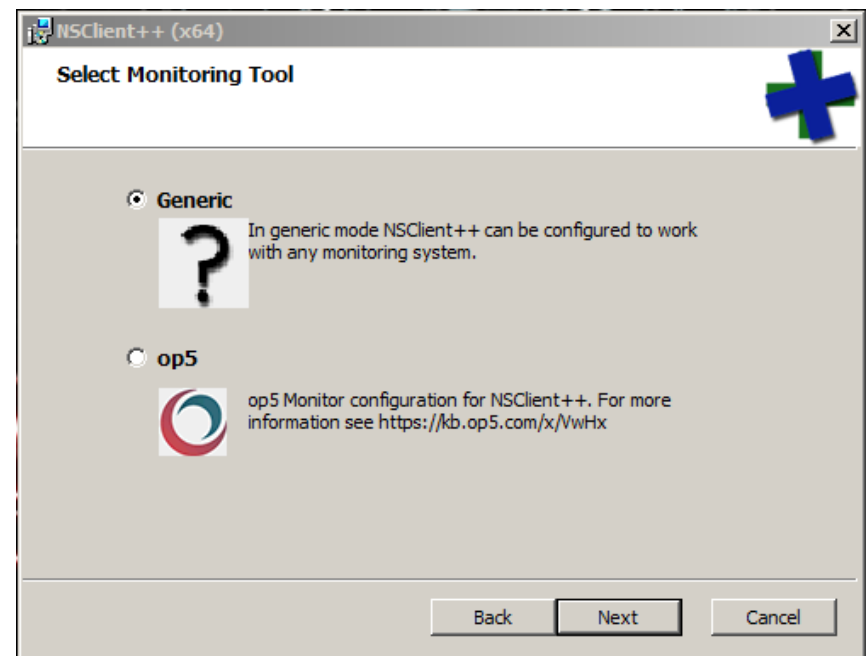
Windows XP and beyond

0.5.2.35

x64

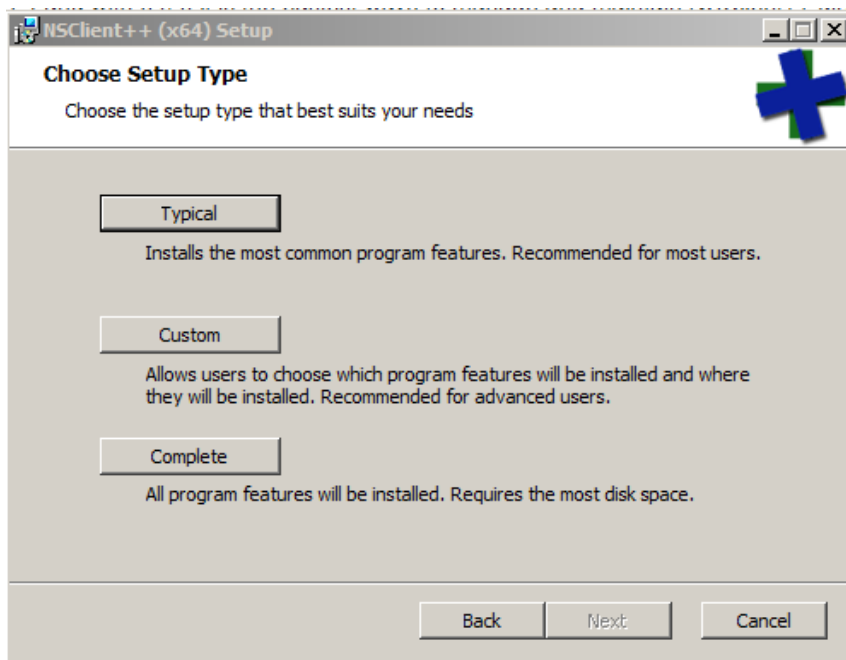
Win32

Herramienta de monitoreo

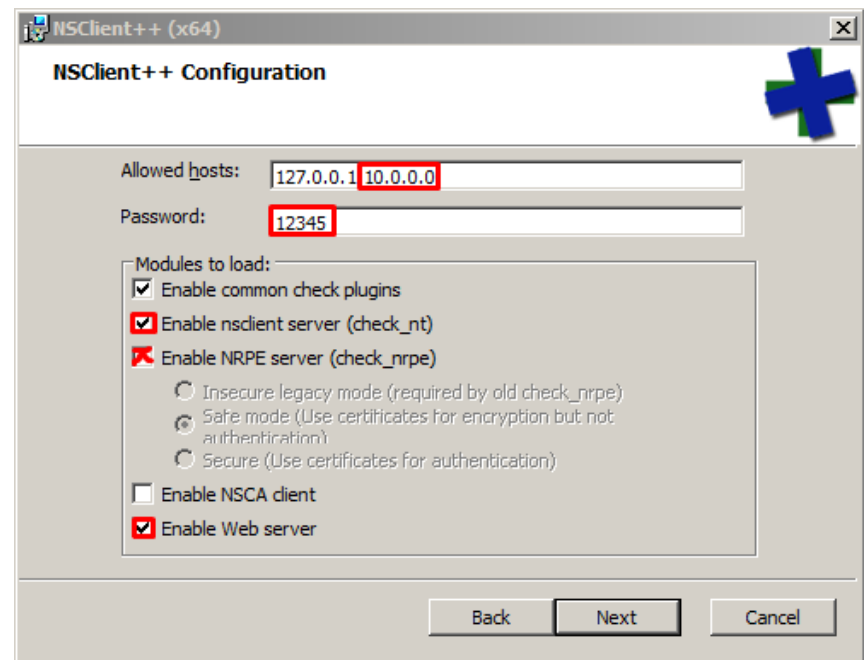


Configuración cliente Windows

Tipo de instalación



Configuración



Configuración cliente Windows

- Y por último accedemos a la interfaz web y activamos los siguientes servicios:



CheckDisk

CheckDisk can check various file and disk related things.



CheckNet

Network related check such as check_ping.



CheckSystem

Various system related checks, such as CPU load, process state, service state memory usage and PDH counters.

Configuración cliente Linux

- Configurar SSH sin contraseña mediante clave pública
- Generar clave pública y clave privada para el usuario “nagios”
 - [Ssh-keygen](#)
- Copiar la clave pública a la máquina cliente
 - [Ssh-copy-id](#)



A terminal window titled 'kzkggaara : bash' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Marcadores', 'Preferencias', and 'Ayuda'. The terminal shows the command 'ssh-copy-id root@10.10.0.5' being executed. The output indicates that the user's password was accepted and the public key was added to the authorized_keys file. The terminal also shows the path '~/.ssh/authorized_keys' and a message to ensure no extra keys were added. The prompt 'kzkggaara@geass: ~\$' is visible at the bottom.

```
kzkggaara@geass:~$ ssh-copy-id root@10.10.0.5
root@10.10.0.5's password:
Now try logging into the machine, with "ssh 'root@10.10.0.5'", and check in:

  ~/.ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
kzkggaara@geass:~$
```

Demostración

- Maestro
 - 10.1.1.165
- Cliente 1
 - SSH
 - 10.1.1.13
- Cliente 2
 - WEB
 - 10.1.1.124
- Cliente 3
 - FTP
 - 10.1.1.19

