

Añadir un host Windows a la monitorización

Después de añadir un host a Linux vamos a ver como hacerlo con Windows y si, en interfaz gráfica.

Nos dirigimos a descargar el cliente para windows en la siguiente página oficial.

https://www.zabbix.com/la/download_agents

For Agent DEBs and RPMs please visit [Zabbix packages](#)

Show legacy downloads

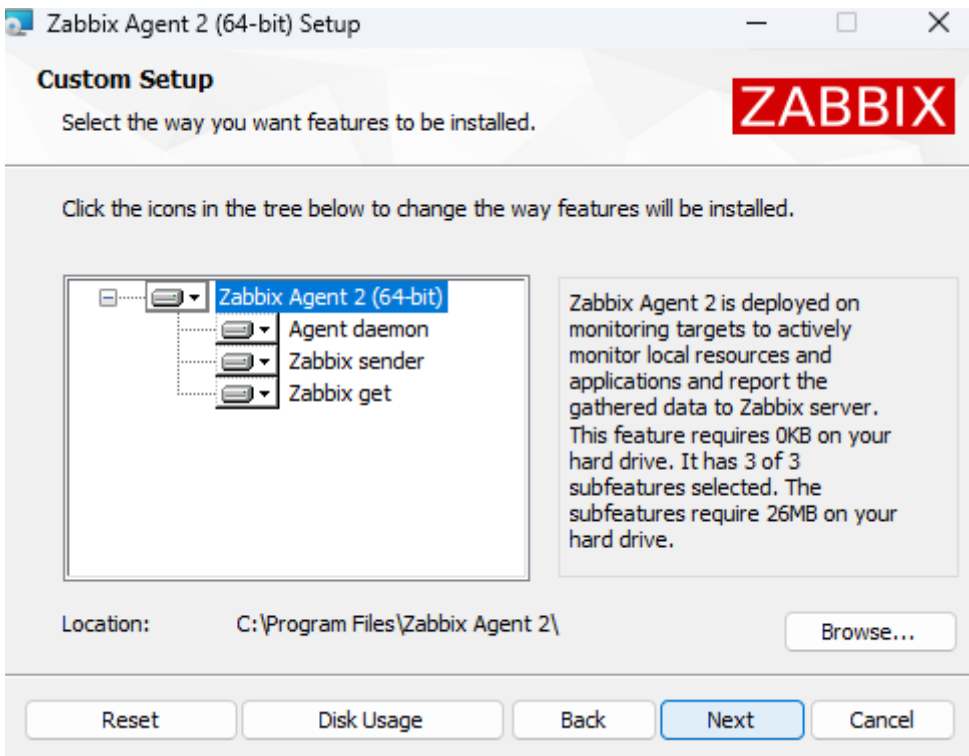
DISTRIBUCIÓN DE SO	VERSIÓN DEL SISTEMA OPERATIVO	HARDWARE	VERSIÓN ZABBIX	ENCRIPCIÓN	EMBALAJE
Windows	Any	amd64	6.4	OpenSSL	MSI
Linux		i386	6.2	No encryption	Archive
macOS			6.0 LTS		
AIX			5.4		
FreeBSD			5.2		
OpenBSD			5.0 LTS		
Solaris			4.4		
			4.2		
			4.0 LTS		
			3.0 LTS		

Zabbix agent 2 v6.4.9 [Read manual](#)

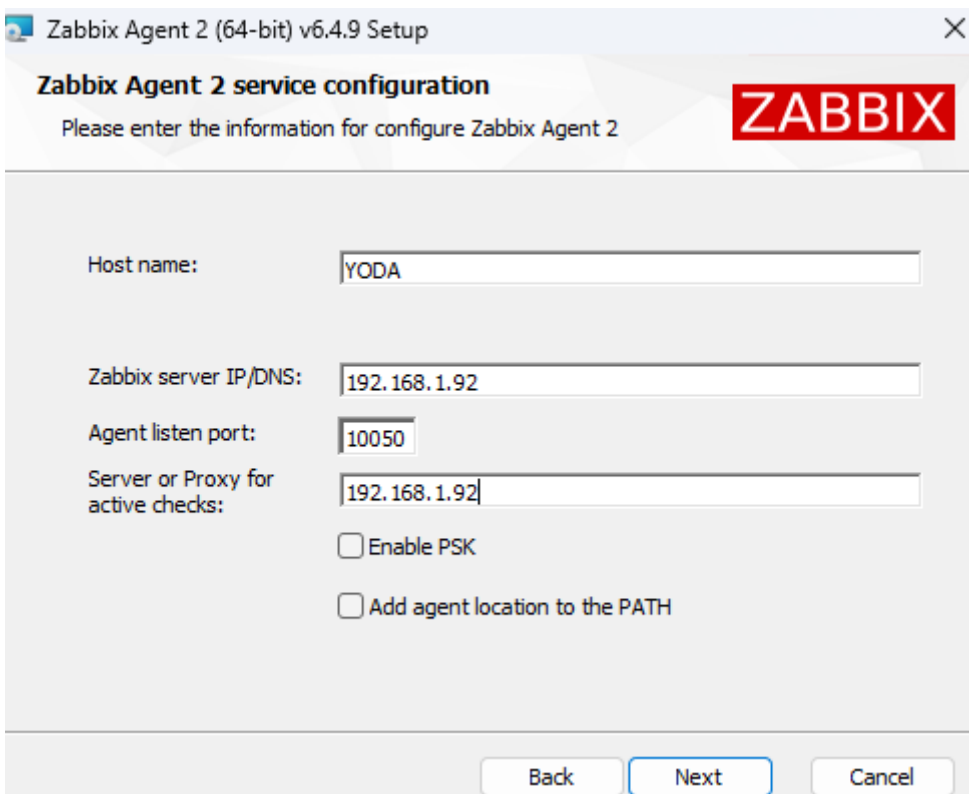
Packaging: MSI
Encryption: OpenSSL
Linkage: Dynamic
Checksum: sha256: 0ff8f404d0c1f3c7a0a956a43b250a5baf3bb569867401df2888e3a1b3b285a1
sha1: 3debf31aba3375869f3d9d839bdd8a429e24fc53
md5: 11d7d3b12685af733a6bdd40a410ea21

[DOWNLOAD](#) https://cdn.zabbix.com/zabbix/binaries/stable/6.4/6.4.9/zabbix_agent2-6.4.9-windows-amd64-openssl.msi

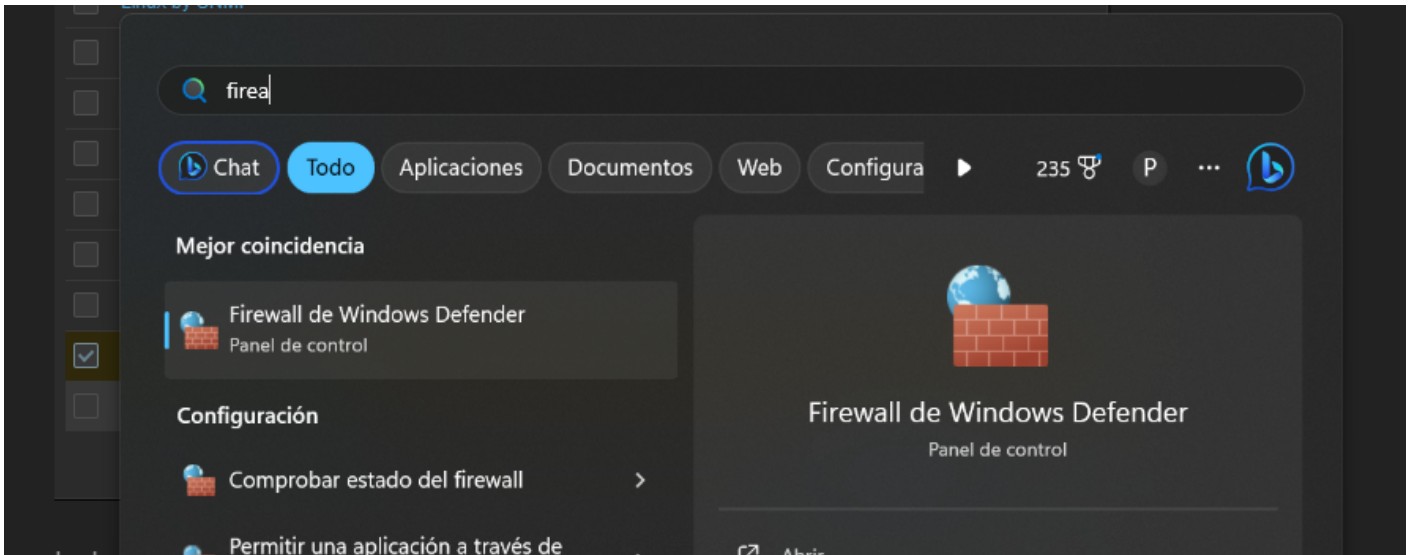
Lo vamos a instalar, aceptamos todos los términos junto a a instalar todos los drivers.



Y nos pedirá los mismos datos que en Linux tuvimos que modificar. (Hostname e IP del servidor zabbix).




Una vez instalado abrimos el puerto.





Nos vamos a configuración avanzada


Ventana principal del Panel de control

Permitir que una aplicación o una característica a través de Firewall de Windows Defender

 Cambiar la configuración de notificaciones

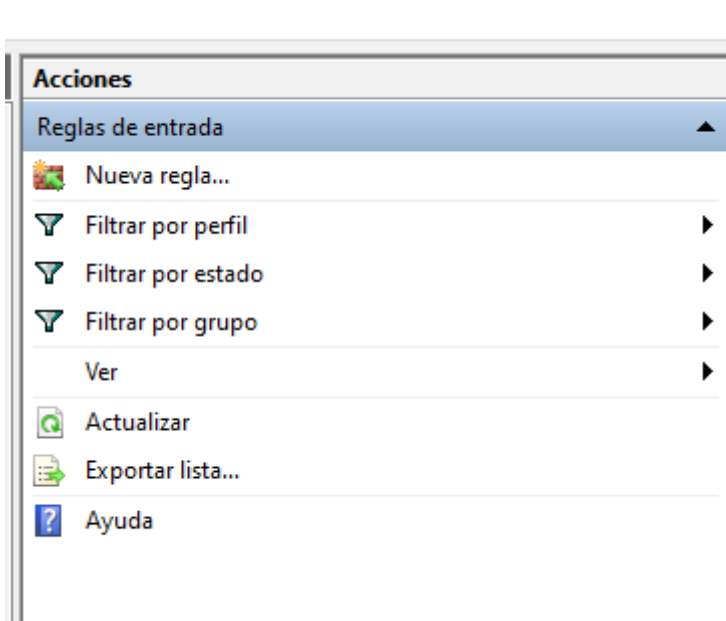
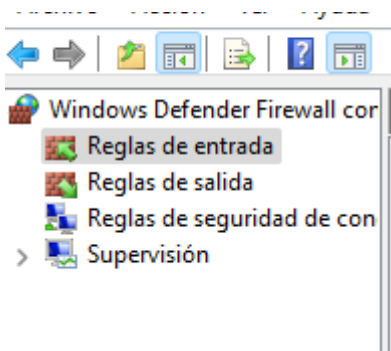
 Activar o desactivar el Firewall de Windows Defender

 Restaurar valores predeterminados

 Configuración avanzada

Solución de problemas de red

Nos vamos a Reglas de entrada en la izquierda y después a Nueva regla en la derecha.



Ahora en la ventana que nos sale le damos a Puerto.

Tipo de regla

Seleccione el tipo de regla de firewall que desea crear.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Qué tipo de regla desea crear?

- Programa**
Regla que controla las conexiones de un programa.
- Puerto**
Regla que controla las conexiones de un puerto TCP o UDP.
- Predefinida:**

Regla que controla las conexiones de una experiencia con Windows.
- Personalizada**
Regla personalizada.

Después le indicamos el puerto.

Protocolo y puertos

Especifique los puertos y protocolos a los que se aplica esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a TCP o UDP?

- TCP**
- UDP**

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

- Todos los puertos locales**
- Puertos locales específicos:**
Ejemplo: 80, 443, 5000-5010

Le damos a siguiente dos veces.

Acción

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción**
- Perfil
- Nombre

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

Permitir la conexión

Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

Permitir la conexión si es segura

Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

Personalizar...

Bloquear la conexión

Perfil

Especifique los perfiles en los que se va a aplicar esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil**
- Nombre

¿Cuándo se aplica esta regla?

Dominio

Se aplica cuando un equipo está conectado a su dominio corporativo.

Privado

Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.

Público

Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

Le indicamos nombre y listo.

Nombre

Especifique el nombre y la descripción de esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

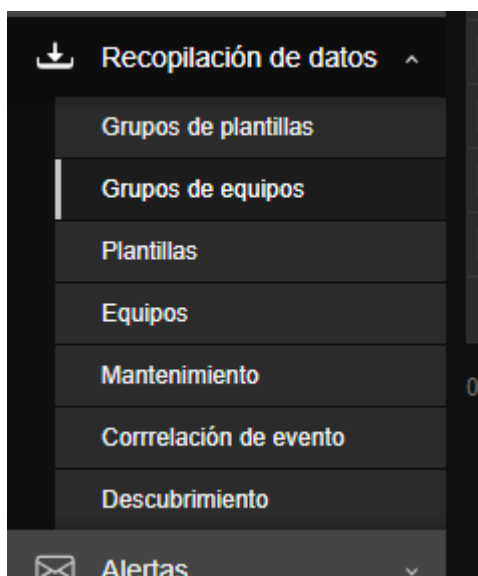
Nombre:

ZABBIX

Descripción (opcional):

Nos dirigimos a zabbix y añadimos el host como hicimos con Linux.

En este caso, no existe un grupo de equipos sobre Windows. Creamos uno rápido, nos vamos a "Recopilación de datos" --> "Grupos de equipos". Y de la misma manera creamos grupo en la esquina superior derecha. Solo nos pide el nombre.



Ahora ya podemos crear el equipo.

Plantilla -->

Plantillas

Grupo de plantillas: Templates/Operating systems x Seleccione

- Nombre
- AIX by Zabbix agent
- FreeBSD by Zabbix agent
- HP-UX by Zabbix agent
- Linux by Prom
- Linux by SNMP
- Linux by Zabbix agent
- Linux by Zabbix agent active
- macOS by Zabbix agent
- OpenBSD by Zabbix agent
- Solaris by Zabbix agent
- Windows by SNMP
- Windows by Zabbix agent
- Windows by Zabbix agent active

Seleccione Cancelar

Lo demás -->

Nuevo equipo

Equipo IPMI Etiquetas Macros Inventario Cifrado Asignación de valores

* Nombre de equipo

Nombre visible

Plantillas
pulse aquí para buscar

* Grupos de equipos
pulse aquí para buscar

Interfaces	Tipo	Dirección IP	Nombre DNS	Conectado a	Puerto	Por defecto
Agente		<input type="text" value="192.168.1.21"/>	<input type="text" value="Yoda"/>	<input type="button" value="IP"/> <input type="button" value="DNS"/>	<input type="text" value="10050"/>	<input type="radio"/> <input type="button" value="Eliminar"/>

[Agregar](#)

Descripción

Monitorizado por proxy

Activado

Ahora saldrá así.

Yoda 192.168.1.21:10050 ZBX class: os target: windows

Pero en segundos se colocará de la siguiente forma y ya estaría añadido.

Yoda 192.168.1.21:10050 ZBX class: os target: windows

Revision #2

Created 9 December 2023 17:56:12 by Yoda

Updated 9 December 2023 18:39:47 by Yoda