Guía Completa: Actualización de Zabbix, Rollback y Configuración SNMP

Tu Asistente de IA

15 de septiembre de 2025

Índice

1. Guía de Actualización de Zabbix y Cuidados Esenciales

Antes de iniciar cualquier proceso de actualización, es **fundamental realizar respaldos** de tu base de datos y configuración para asegurar la capacidad de recuperación en caso de cualquier imprevisto [1, 2].

1.1. Cuidados Iniciales y Preparación (Backups)

1.1.1. Backup de la Base de Datos (MariaDB/MySQL)

Es crucial realizar un respaldo completo de tu base de datos de Zabbix. Puedes usar el siguiente comando (ajusta `zabbix` por el nombre de tu base de datos y `-p` para que pida la contraseña del usuario `zabbix`) [1]:

```
mysqldump -u zabbix -p zabbix > /root/zabbix_backup.sql
```

Listing 1: Respaldo de la base de datos

Asegúrate de que el archivo de backup exista y que el usuario con el que vas a ejecutar los comandos de restauración de MySQL tenga permisos de lectura sobre él [3].

1.1.2. Backup de Archivos de Configuración y Frontend

Realiza copias de seguridad de los directorios de configuración y del frontend de Zabbix [1, 2].

```
cp -r /etc/zabbix /root/zabbix_config_backup
cp -r /usr/share/zabbix /root/zabbix_web_backup
```

Listing 2: Respaldo de configuraciones y frontend

Puedes añadir la fecha al nombre del backup para mayor control, por ejemplo: `sudo cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.backup_$(date +%F)` [4]. Ten en cuenta que esta guía asume el uso de MariaDB y Apache, pero si usas PostgreSQL o Nginx, deberás ajustar los paquetes correspondientes [2].

1.2. Paso a Paso del Proceso de Actualización

1.2.1. Detener Servicios de Zabbix y Relacionados

Es **crucial detener todos los servicios de Zabbix y relacionados** para evitar cualquier acceso a la base de datos durante la actualización [3,

5]. Detén el servidor Zabbix, el agente Zabbix (si está en el mismo host) y el servidor web (Apache o Nginx), así como PHP-FPM si lo usas [3].

```
sudo systemctl stop zabbix-server
sudo systemctl stop zabbix-agent # Si est  en el mismo host
sudo systemctl stop httpd      # O nginx si usas ese
sudo systemctl stop php-fpm    # Si lo usas
```

Listing 3: Detención de servicios

1.2.2. Eliminar Repositorio Antiguo de Zabbix

Remueve el paquete del repositorio de Zabbix de la versión anterior [1, 5].

```
yum remove zabbix-release -y
# O si se actualiz  el rpm directamente (ej. de 6.4):
# sudo rpm -e zabbix-release-6.4-X.elY.noarch
```

Listing 4: Eliminar repositorio antiguo

1.2.3. Instalar el Nuevo Repositorio de Zabbix (ej. 7.0)

Instala el paquete del repositorio para la nueva versión de Zabbix a la que deseas actualizar desde la pagina oficial de zabbix o desde el siguiente enlace https://repo.zabbix.com/zabbix

1.2.4. Actualizar Paquetes de Zabbix

Procede a actualizar los paquetes de Zabbix a la nueva versión [3, 5]. **Importante:** Si usas PostgreSQL o Nginx, **cambia los paquetes correspondientes** (ej. `zabbix-server-pgsql`, `zabbix-web-nginx-mysql`) [5]. Comando para MariaDB/Apache:

```
yum upgrade zabbix-server-mysql zabbix-web-mysql zabbix-agent
```

Listing 5: Actualizar paquetes Zabbix

1.2.5. Verificar la Actualización de la Base de Datos

Deberías ver algo como: [6] (el servidor Zabbix generalmente realiza la actualización de la base de datos automáticamente al iniciarse después de una actualización de paquetes).

1.2.6. Iniciar y Habilitar Servicios

Una vez que los paquetes se han actualizado, puedes iniciar los servicios de Zabbix y relacionados. Es buena práctica habilitarlos para que inicien automáticamente en el arranque del sistema [3, 6].

```
sudo systemctl start zabbix-server
sudo systemctl start php-fpm    # Si aplica
sudo systemctl start httpd      # O nginx
sudo systemctl start zabbix-agent # Si aplica
sudo systemctl enable zabbix-server zabbix-agent httpd #
    Para habilitarlos
```

Listing 6: Iniciar y habilitar servicios

Después de esperar unos minutos, accede a la interfaz web de Zabbix para confirmar que la actualización fue exitosa [6].

2. Guía de ROLLBACK (En Caso de Problemas)

Si encuentras problemas después de la actualización, es fundamental tener un plan de reversión. La siguiente guía detalla los pasos para realizar un rollback [3]:

2.1. Fase 1: Preparación y Detención de Servicios

1. **Detener todos los servicios de Zabbix y relacionados:** Asegúrate de que nada esté intentando acceder a Zabbix o su base de datos [3].

```
sudo systemctl stop zabbix-server
sudo systemctl stop zabbix-agent # Si est  en el
   mismo host
sudo systemctl stop httpd       # O nginx si usas ese
sudo systemctl stop php-fpm     # Si lo usas
```

Listing 7: Detención de servicios para rollback

2. **Verificar la existencia y permisos del backup:** Confirma que tu archivo `zabbix_backup.sql` existe y es legible por el usuario que restaurará la base de datos [3].

```
ls -l /root/zabbix_backup.sql
```

Listing 8: Verificar backup

2.2. Fase 2: Desinstalar/Revertir los Paquetes de Zabbix a la Versión Anterior

Esta es la parte más compleja y depende de cómo gestionaste el upgrade. Tienes varias opciones [7]:

- **Opción A: Revertir con el historial de dnf/yum (si el upgrade fue reciente):** [7]

```
sudo dnf history list
# Busca el ID de la transacci n que realiz  el upgrade de Zabbix (ej. 25)
sudo dnf history undo 25
```

Listing 9: Revertir con historial de dnf/yum

  Verifica cuidadosamente los paquetes que se modificarán antes de confirmar [7].

- **Opción B: Desinstalar la versión actual e instalar la versión anterior específica:** [7]

  1. **Desinstalar los paquetes de la versión actual:** [7]

```
sudo dnf remove zabbix-server-mysql zabbix-web-mysql zabbix-sql-scripts zabbix-selinux-policy zabbix-agent
```

Listing 10: Desinstalar paquetes actuales

  (Ajusta la lista según tu instalación y tipo de BD) [7].

  2. **Configurar el repositorio de Zabbix para la versión anterior:** Elimina el release actual si lo cambiaste y luego instala el `zabbix-release` de la versión a la que quieres volver (ej. 6.0) [7].

```
# Ejemplo si actualizaste a 6.4:
# sudo rpm -e zabbix-release-6.4-X.elY.noarch
# Ejemplo para volver a 6.0 en CentOS 9:
sudo dnf install -y https://repo.zabbix.com/zabbix/6.0/rhel/9/x86_64/zabbix-release-6.0-4.el9.noarch.rpm
sudo dnf clean all
```

Listing 11: Configurar repositorio anterior

  Asegúrate de obtener el comando RPM correcto para la versión y SO a la que regresas [7].

3. **Instalar los paquetes de Zabbix de la versión anterior:** [7]

```
sudo dnf install -y zabbix-server-mysql zabbix-
    web-mysql zabbix-sql-scripts zabbix-selinux-
    policy zabbix-agent
```

Listing 12: Instalar paquetes de la versión anterior

(Ajusta los paquetes y el tipo de BD) [7].

- **Opción C: Restaurar backups de archivos de configuración y scripts PHP (manual):** Esta opción es más manual y propensa a errores. Implica restaurar `/usr/share/zabbix/` y `/etc/zabbix/` desde tus backups *antes* del upgrade, además de degradar los binarios. **No es la más recomendada si puedes usar la gestión de paquetes** [7].

2.3. Fase 3: Restaurar la Base de Datos Zabbix

1. **Acceder a MariaDB como usuario root:** [8]

```
sudo mysql -u root -p
```

Listing 13: Acceder a MariaDB como root

2. **Eliminar la base de datos Zabbix actual:** [8]

```
DROP DATABASE IF EXISTS zabbix;
```

Listing 14: Eliminar base de datos Zabbix

3. **Crear una nueva base de datos Zabbix vacía:** [8]

```
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE
    utf8mb4_bin;
```

Listing 15: Crear nueva base de datos Zabbix

4. **Asegurar los privilegios para el usuario `zabbix`:** Reemplaza `tu_contraseña_segura_de` con la contraseña correcta [8].

```
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'
    localhost' IDENTIFIED BY '
    tu_contrase a_segura_de_zabbix_db';
FLUSH PRIVILEGES;
```

Listing 16: Configurar privilegios

5. **Habilitar `log_bin_trust_function_creators` temporalmente:** [8]

```
SET GLOBAL log_bin_trust_function_creators = 1;
```

Listing 17: Habilitar log_bin_trust_function_creators

6. **Salir de MariaDB:** [8]

```
QUIT;
```

Listing 18: Salir de MariaDB

7. **Importar el backup de la base de datos:** Usa el usuario y contraseña de la base de datos Zabbix [8].

```
sudo mysql -u zabbix -p'
   tu_contrase a_segura_de_zabbix_db' zabbix < /
   root/zabbix_backup.sql
```

Listing 19: Importar backup de la base de datos

Si tu contraseña tiene caracteres especiales, puedes usar `-p` y la introducirá interactivamente [8].

```
sudo mysql -u zabbix -p zabbix < /root/zabbix_backup
   .sql
```

Listing 20: Importar backup (interactivo)

8. **(Opcional) Revertir `log_bin_trust_function_creators`:** [8]

```
sudo mysql -u root -p
SET GLOBAL log_bin_trust_function_creators = 0;
QUIT;
```

Listing 21: Revertir log_bin_trust_function_creators

2.4. Fase 4: Restaurar Archivos de Configuración (si es necesario)

Si los paquetes reinstalados no trajeron los archivos de configuración correctos o si tenías modificaciones [9]:

```
sudo cp /ruta/backup/zabbix_server.conf.bak-version-
   anterior /etc/zabbix/zabbix_server.conf
```

Listing 22: Restaurar archivos de configuración

Asegúrate de que `DBPassword` en `/etc/zabbix/zabbix_server.conf` coincida con la contraseña de la base de datos [9].

2.5. Fase 5: Iniciar Servicios y Verificar

1. **Iniciar los servicios en orden:** [9]

```
sudo systemctl start zabbix-server
sudo systemctl start php-fpm # Si aplica
sudo systemctl start httpd # O nginx
sudo systemctl start zabbix-agent # Si aplica
```

Listing 23: Iniciar servicios después del rollback

3. Configuración y Prueba de SNMP para Zabbix

[10]

3.1. Parte 2: Configurar SNMP en Máquina B (143.198.182.233)

[10]

3.1.1. 1. Instalar Agente SNMP:

[10] En la Máquina B (143.198.182.233):

```
sudo dnf install net-snmp net-snmp-utils -y
```

Listing 24: Instalar agente SNMP

3.1.2. 2. Configurar `snmpd.conf`:

[4] En la Máquina B (143.198.182.233):

- **Haz una copia de seguridad:** [4]

```
sudo cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.
   backup_$(date +%F)
```

Listing 25: Copia de seguridad de snmpd.conf

- **Edita el archivo:** [4]

```
sudo nano /etc/snmp/snmpd.conf
```

Listing 26: Editar snmpd.conf

- **Asegurar que `agentAddress` escuche en todas las interfaces:** [4] Busca la línea `agentaddress`. Por defecto podría ser `agentaddress udp:127.0.0.1:161`. Coméntala o modifícala para que escuche en todas las interfaces o en su IP pública [4]:

```
# agentaddress udp:127.0.0.1:161
agentaddress udp:161,udp6:[::1]:161
```

Listing 27: Configuración de agentAddress

  Esto hace que escuche en todas las interfaces IPv4 en el puerto 161 [4].

- **Configurar Comunidad Read-Only:** [4] Añade o modifica una línea `rocommunity` para permitir acceso desde tu servidor Zabbix [4]. Reemplaza `MiComunidadSNMP123` con una comunidad segura y `137.184.92.155` con la IP de tu servidor Zabbix [4, 11].

```
# sec.name source community
# Comenta o elimina l neas gen ricas como:
   rocommunity public default -V systemonly
rocommunity MiComunidadSNMP123 137.184.92.155
```

Listing 28: Configuración de rocommunity

- **Ejemplo de `snmpd.conf`:** [11-13]

```
#
   ------------------------------------------------------------------

# snmpd.conf para la m quina 143.198.182.233
# Permite el acceso desde el servidor Zabbix
   137.184.92.155
#
   ------------------------------------------------------------------

# --- Configuraci n General del Agente ---
# En qu  interfaces y puertos escuchar.
# udp:161 es el puerto est ndar para SNMP en todas
   las interfaces IPv4. [12]
# Si solo quieres escuchar en la IP espec fica de
   la m quina:
```

```
# agentAddress udp:143.198.182.233:161 [12]
# Pero udp:161 es generalmente suficiente si el
   firewall est  bien configurado. [13]
agentAddress udp:161 [13]
# Informaci n del sistema (opcional pero
   recomendable)
sysLocation "Ubicacion del Servidor/Datacenter" #
   Cambia esto [13]
sysContact TuNombre tuemail@example.com # Cambia
   esto [13]
# --- Acceso SNMPv1/SNMPv2c ---
# Es MENOS seguro que SNMPv3.  salo  con precauci n
   . [13]
# Reemplaza 'comunidad_zabbix_ro' con una cadena de
   comunidad SEGURA y  NICA . [13]
# 'rocommunity' define una comunidad de solo lectura
   . [13]
# El 'default' o '.1' al final indica que se puede
   acceder a todo el  rbol  MIB. [13]
# Restringimos el acceso SOLO a la IP del servidor
   Zabbix. [11]
rocommunity comunidad_zabbix_ro 137.184.92.155 [11]
```

Listing 29: Ejemplo de configuración snmpd.conf para Máquina B

- **Guarda el archivo** (Ctrl+O, Enter, Ctrl+X en nano) [4].

3.1.3. 3. Reiniciar y Habilitar Servicio `snmpd`:

[14] En la Máquina B (143.198.182.233):

```
sudo systemctl restart snmpd
sudo systemctl enable snmpd
sudo systemctl status snmpd
```

Listing 30: Reiniciar y habilitar snmpd

Asegúrate de que el estado sea `active (running)`. Si hay errores, revisa los logs: `sudo journalctl -u snmpd -f` [14].

3.1.4. 4. Configurar Firewall para SNMP (UDP 161) en Máquina B (143.198.182.233):

[14]

- **Firewall de DigitalOcean para Máquina B:** [14] Añade/verifica una Regla de Entrada (Inbound rule):
  - **Tipo:** Custom
  - **Protocolo:** UDP
  - **Rango de Puertos:** 161
  - **Origen (Sources):** 137.184.92.155 (la IP de tu servidor Zabbix)
- **En Máquina B (firewalld):** [14]

```
sudo firewall-cmd --permanent --add-rich-rule='rule
   family="ipv4" source address="137.184.92.155"
   port port="161" protocol="udp" accept'
sudo firewall-cmd --reload
```

Listing 31: Configurar firewalld para SNMP

Verifica: `sudo firewall-cmd --list-all` [14].

3.2. Parte 3: Probar Conexión SNMP desde Máquina A (137.184.92.155)

[15]

3.2.1. 1. Instalar `snmpwalk` (si no está instalado):

[15] En la Máquina A (137.184.92.155):

```
sudo dnf install net-snmp-utils -y
```

Listing 32: Instalar snmpwalk

3.2.2. 2. Ejecutar `snmpwalk`:

[15] En la Máquina A (137.184.92.155), ejecuta:

```
snmpwalk -v2c -c MiComunidadSNMP123 143.198.182.233 .
```

Listing 33: Probar conexión SNMP

(Usa la comunidad que configuraste) [15].

- Si obtienes una larga lista de OIDs y valores: ¡La conexión SNMP funciona! Procede a la configuración en Zabbix [15].

- Si obtienes "Timeout: No Response from 143.198.182.233": [15]
  - Verifica que `ping 143.198.182.233` aún funciona [15].
  - Revisa **MUY CUIDADOSAMENTE** las reglas de firewall (DigitalOcean y `firewalld` en Máquina B) para UDP puerto 161 desde `137.184.92.155` [15].
  - Revisa la configuración de `agentAddress` en `/etc/snmp/snmpd.conf` en Máquina B [15].
  - Verifica que la comunidad (`MiComunidadSNMP123`) y la IP de origen (`137.184.92.155`) sean correctas en la línea `rocommunity` del `snmpd.conf` [15].
  - Verifica el estado del servicio `snmpd` en Máquina B [15].
  - Revisa los logs de `snmpd` en Máquina B: `sudo journalctl -u snmpd -f` [15].
  - Considera SELinux (ver Parte 5) [15].

3.3. Parte 4: Configurar Host en Zabbix (en Máquina A)

[16]

1. **Accede a la Interfaz Web de Zabbix** [16].
2. Ve a **Configuration** > **Hosts** [16].
3. Haz clic en **Create host** (o edita el host existente para `143.198.182.233`) [16].
4. **Pestaña Host:** [16]
   - **Host name:** Un nombre descriptivo (ej., `Servidor-App-CentOS9`) [16]
   - **Groups:** Selecciona un grupo de hosts [16].
5. **Pestaña Interfaces:** [16]
   - Haz clic en **Add** y selecciona tipo **SNMP** [16].
   - **IP address:** `143.198.182.233` [16]
   - **DNS name:** (Opcional, puedes dejarlo vacío si usas IP) [16]
   - **Port:** `161` [16]

- **SNMP version:** `SNMPv2` [16]
- **SNMP community:** `MiComunidadSNMP123` (la misma que configuraste en `snmpd.conf`) [16]
- Asegúrate de que esta interfaz SNMP esté marcada como **Default** [16].

6. **Pestaña Templates:** [16]
   - Vincula una plantilla SNMP apropiada (ej., "Template OS Linux SNMP", "Template Net SNMP OS Linux") [16].
7. Haz clic en **Add** (o **Update** si estás editando) [16].
8. **Verificar en Zabbix:** [16]
   - Espera unos minutos [16].
   - En la lista de **Configuration** > **Hosts**, la columna "Availability"para la interfaz SNMP de tu host (`143.198.182.233`) debería cambiar a un icono verde [16].
   - Si permanece en rojo, pasa el cursor sobre el icono para ver el mensaje de error [16].
   - Revisa los logs del servidor Zabbix en Máquina A (`/var/log/zabbix/zabbix_server.l` para más detalles [16].

3.4. Parte 5: Consideraciones Adicionales (Si Persisten Problemas)

[17]

3.4.1. 1. SELinux en Máquina B (143.198.182.233):

[17] SELinux podría estar bloqueando `snmpd` [17].

- Verifica logs de auditoría de SELinux: [17]

```
sudo ausearch -m avc -ts recent | grep snmpd
```

Listing 34: Verificar logs de SELinux para snmpd

- Si ves denegaciones, *temporalmente y solo para probar*, pon SELinux en modo permisivo: [17]

```
sudo setenforce 0
```

Listing 35: SELinux en modo permisivo (temporal)

Intenta `snmpwalk` de nuevo. Si funciona, SELinux es el problema. **NO DEJES SELinux en permisivo en producción** [17]. Necesitarás crear o ajustar políticas SELinux. Para volver a enforcing: `sudo setenforce 1` [17].

- Podrías necesitar asegurar que el puerto `161/udp` tiene el contexto correcto: [17]

```
sudo semanage port -l | grep snmp
# Si no est  listado o es incorrecto, podr as
   a adirlo (generalmente no es necesario si el
   paquete est  bien hecho)
# sudo semanage port -a -t snmp_port_t -p udp 161
```

Listing 36: Verificar contexto de puerto SELinux

3.4.2. 2. Uso de Red Privada (VPC) de DigitalOcean:

[18] Si ambas máquinas están en la misma región y tienes una VPC, es **altamente recomendable** usar las IPs privadas para la comunicación SNMP. Esto es más seguro y no consume ancho de banda público [18]. Si cambias a IPs privadas, deberás actualizar [18]:

- Las reglas de `firewalld` en la Máquina B (el `source address` sería la IP privada de la Máquina A) [18].
- Las reglas del Cloud Firewall de DigitalOcean (si aplicas firewalls al tráfico de la VPC) [18].
- La configuración de `agentAddress` en `snmpd.conf` (si quieres ser específico con la IP privada de B) [18].
- La IP de la interfaz SNMP en la configuración del host en Zabbix (sería la IP privada de B) [18].
- El `snmpwalk` para probar usaría la IP privada de B [18].