7.3 Remote commands

This tutorial provides step-by-step instructions on how to setup remote execution of pre-defined commands in case on an event. It is assumed that Zabbix is configured and operational.

Step 1

On Zabbix agent, enable remote commands. In *zabbix_agentd.conf* make sure that parameter **EnableRemoteCommands** is set to **1** and uncommented. Restart agent daemon if changing this parameter.

Step 2

Configure new action by going to Configuration → Actions and in the *New action* block choose operation type **Remote command**.

Pay attention to the following parameters of the action:

PARAMETER	Description
Action type	Must be set to 'Remote command'.
Remote command	Each line must contain an command for remote execution. For example: host:sudo /etc/init.d/apache restart. Remote command may contain macros!

Note the use of **sudo** - Zabbix user does not have permissions to restart system services by default. See below for hints on how to configure **sudo**.

Syntax of remote commands:

REMOTE COMMAND	Description
{HOSTNAME}:<command>	Command 'command' will be executed on the host where the event happened.
<host>:<command>	Command 'command' will be executed on host 'host'.
<group>#<command>	Command 'command' will be executed on all hosts of host group 'group'.

Zabbix agent executes commands in background. Zabbix does not check if a command has been executed successfully.
Remote commands in Zabbix < 1.4 are limited to 44 characters, in Zabbix >= 1.4 they are limited to 255 characters.

Syntax of IPMI remote commands:

REMOTE COMMAND	Description
{HOSTNAME}:IPMI <ipmi control> [value]	The syntax is for execution of IPMI command on the host where the event happened. Supported values: “on”, “off” or number (1, by default).
<host>:IPMI <ipmi control> [value]	The syntax is for execution of IPMI command on a single host.
<group>#IPMI <ipmi control> [value]	The syntax is for execution of IPMI command for all hosts of a host group.

Access permissions

Make sure that user 'zabbix' has execute permissions for configured commands. One may be interested in using **sudo** to give access to privileged commands. To configure access, execute as root:

```
# visudo
```

Example lines that could be used in *sudoers* file:

```
# allows 'zabbix' user to run all commands without password.
zabbix ALL=NOPASSWD: ALL
```

```
# allows 'zabbix' user to restart apache without password.
zabbix ALL=NOPASSWD: /etc/init.d/apache restart
```

On some systems *sudoers* file will prevent non-local users from executing commands. To change this, comment out **requiretty** option in */etc/sudoers*.
On recent systems it might be required to set **Defaults visiblepw** in */etc/sudoers*.

Example 1

Restart of Windows on certain condition.

In order to automatically restart Windows in case of a problem detected by Zabbix, define the following actions:

PARAMETER	Description
Action type	'Remote command'
Remote command	host:c:\windows\system32\shutdown.exe -r -f Replace 'host' with Zabbix hostname of Windows server.

Example 2

Restart the host by using IPMI control.

PARAMETER	Description
Action type	'Remote command'
Remote command	{HOSTNAME}:IPMI reset on

Example 3

Power off the host by using IPMI control.

PARAMETER	Description
Action type	'Remote command'
Remote command	{HOSTNAME}:IPMI power off