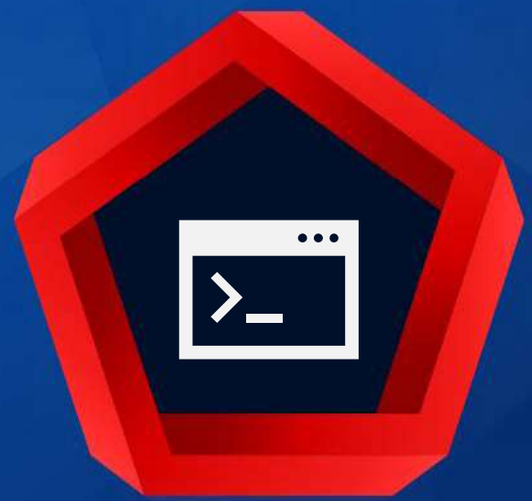
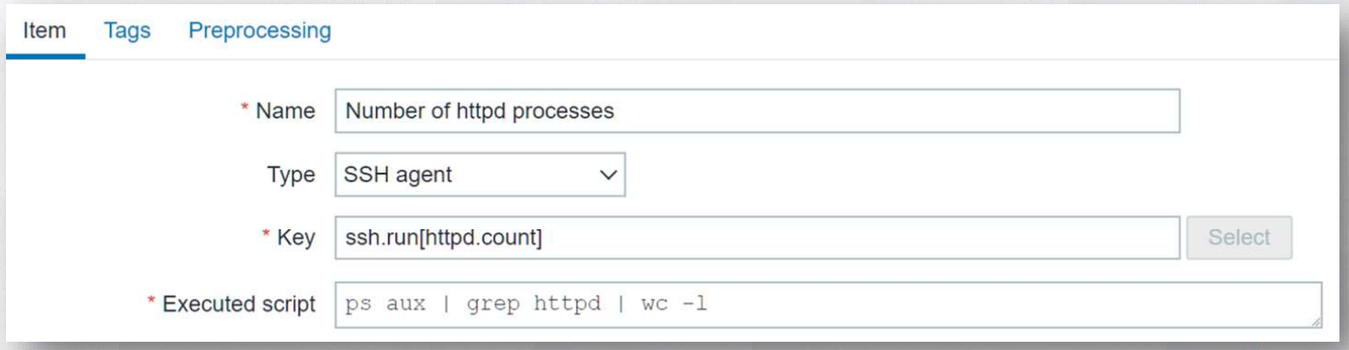


SSH checks

SSH checks are performed as agent-less monitoring:

- Performed by Zabbix server or proxy
- Can execute any command on the remote host and return the result back to Zabbix
- SSH checks provide two authentication methods:
  - ✓ A user/password pair
  - ✓ Key-file based (public/private key pair)



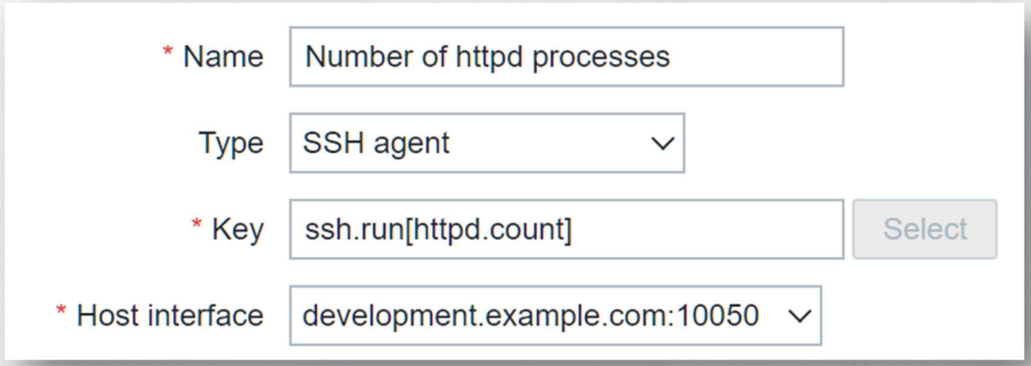

```
# ps aux | grep httpd | wc -l
7
```

SSH item key has the following syntax:

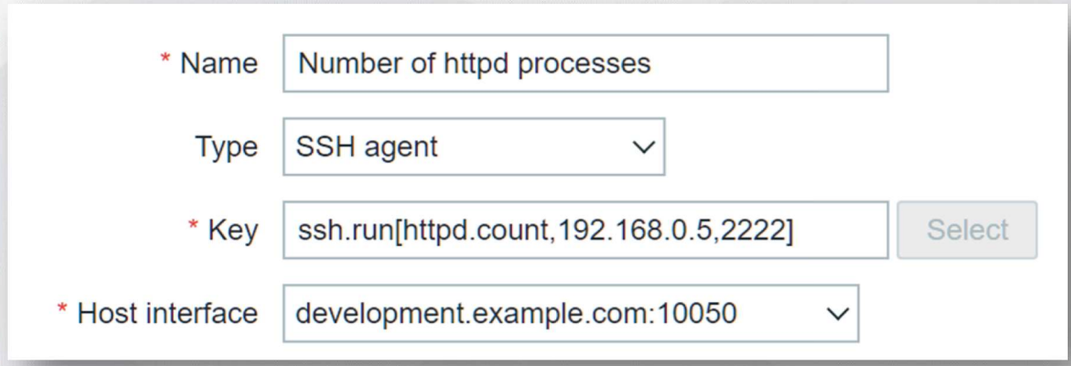
ssh.run[unique description,<ip>,<port>,<encoding>]

- Free-form description can be used
- If <ip> is not defined any interface's IP address or DNS name can be specified
- Port 22 is used by default (not the port specified in the interface)
- SSH item does not affect any interface availability and vice versa

Interface address and port 22



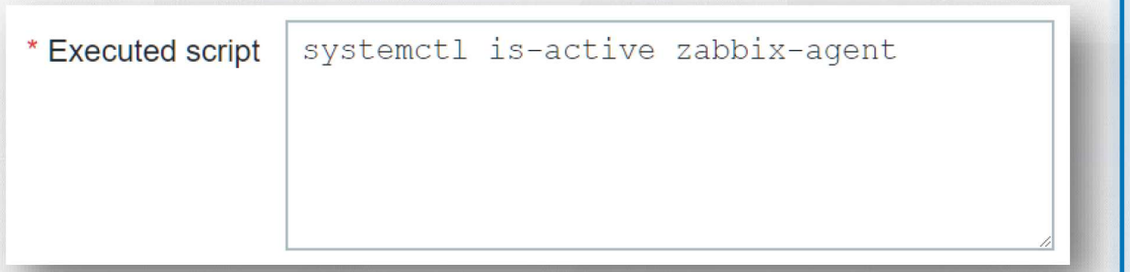
IP address 192.168.0.5 and port 2222

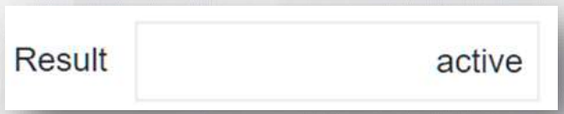


The command executed by an SSH item is specified in the Executed script field:

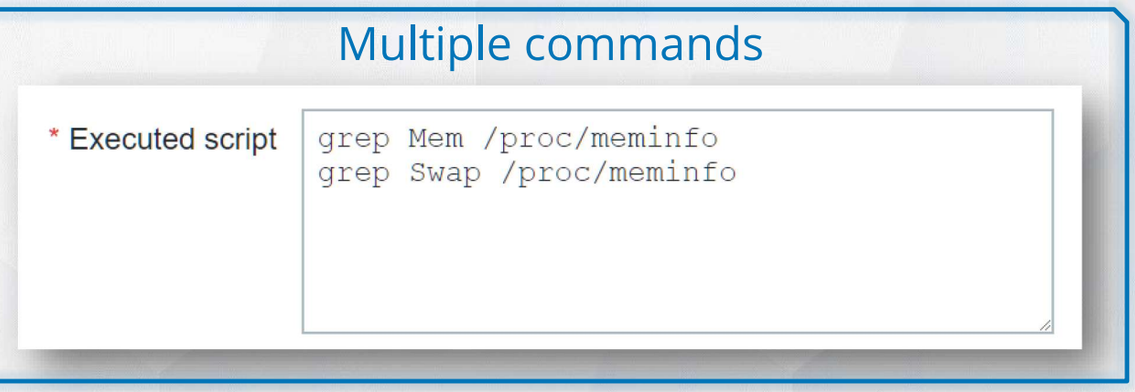
- Multiple commands can be executed one after another by placing them on a new line.
- In this case, returned values also will be formatted as multi-lined.
  - ✓ Dependent items can be used to extract values (discussed later)

Single command





Multiple commands



SSH AUTHENTICATION

To use password authentication, only a user/password pair is required

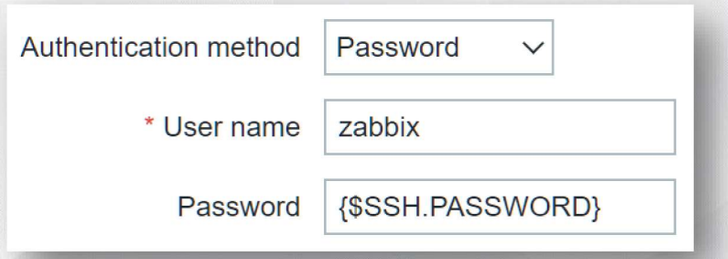
- Do not use privileged accounts (e.g., root) for monitoring, create a dedicated user
- Make sure that login credentials are valid, and no prompts are displayed

To use a key for authentication, additional server configuration is required:

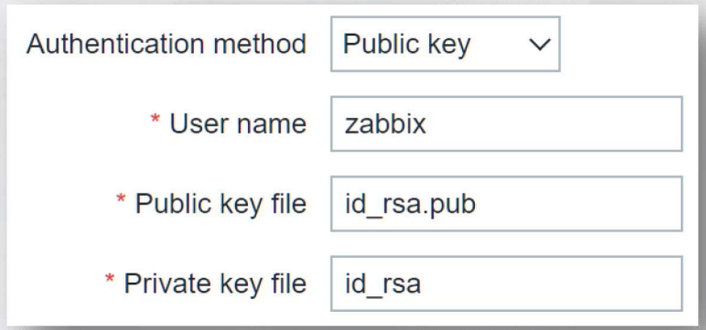
- Create a directory where SSH keys will be stored (must be readable by zabbix OS user)

```
### Option: SSHKeyLocation
#       Location of public and private keys for SSH checks and actions.
SSHKeyLocation=/home/zabbix/.ssh
```

Password authentication



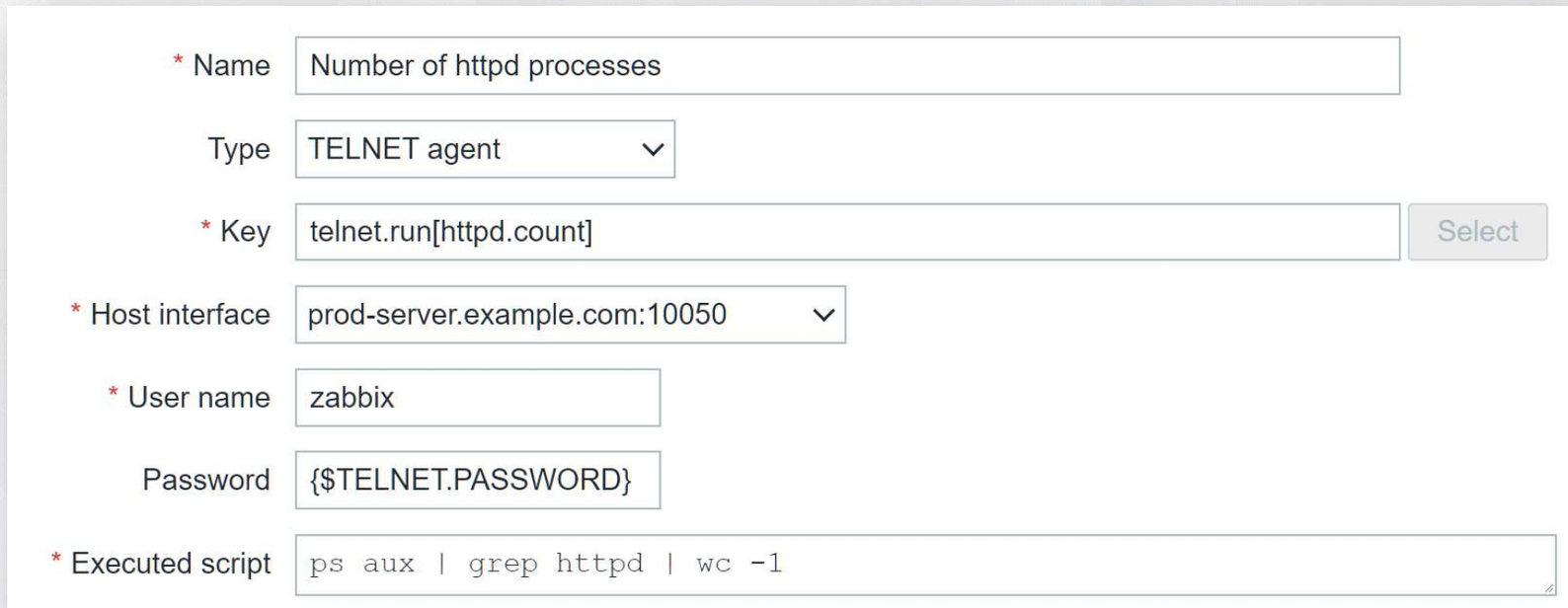
Public key authentication



Telnet checks are performed similarly to SSH checks:

telnet.run[unique description,<ip>,<port>,<encoding>]

- Username and password are sent over the network in plain text
- Supported characters that the shell prompt can end with:
  - ✓ $ # > %



PRACTICAL SETUP

1) On your Training-VM-XX:
   - ✓ Link template: SSH Service
   - ✓ Check whether SSH service is available
2) On your host create a new user (use SSH console):
   - ✓ Name: monitor
   - ✓ Password: sshremoteXX
3) In the "Template Basic":
   - ✓ Create a new item (Name: Memory available, Type: SSH agent,)
   - ✓ Create a new macro for SSH password authentication
   - ✓ Use "cat /proc/meminfo" command to collect data
4) Make sure that the item receives data from all Training-VM-XX hosts.