

ANEXO 8 – Configuración Base / Plantillas

Plantilla orientativa de configuración, a adaptar a la plataforma NMS finalmente seleccionada (Zabbix, PRTG, LibreNMS o equivalente).

8.1. Credenciales SNMP

```
snmp-user nms-readonly version v3 security-level authPriv auth-protocol
SHA priv-protocol AES-128 access read-only acl NMS_ACCESS permit source
10.10.99.10/32 action snmp,icmp deny source any action snmp
```

8.2. Host de ejemplo (Switch Core)

```
host CORE-SW-MDF ip 10.10.10.1 snmp-version v3 template "Generic
Switch SNMPv3" group "Core / Distribucion" item CPU_Utilization
snmp.cpu.util interval=60s item Memory_Utilization snmp.memory.util
interval=60s item Interface_Traffic snmp.if.traffic[*] interval=60s item
Temperature snmp.temp.sensor interval=300s trigger CPU_High
expr="CPU_Utilization > 85 for 10m" severity=Average trigger CPU_Critical
expr="CPU_Utilization > 95 for 5m" severity=High trigger Host_Down
expr="icmp.ping = 0 for 2m" severity=Disaster
```

8.3. Host de ejemplo (Servidor con agente)

```
host SRV-APP-01 ip 10.10.60.10 monitor-type agent template "Generic
Linux Server" group "Servidores" item Disk_Usage_root
agent.vfs.fs.size[/,pused] interval=300s item Service_DHCP agent.proc.num[dhcpd]
interval=60s item Service_DNS agent.proc.num[named] interval=60s trigger
Disk_Warning expr="Disk_Usage_root > 75" severity=Warning trigger Disk_Critical
expr="Disk_Usage_root > 90" severity=High trigger Service_DHCP_Down
expr="Service_DHCP = 0 for 3m" severity=Disaster
```

8.4. Notificaciones

```
notification-action Email_Disaster_High condition severity >= High send-to
grupo-sistemas-tic@empresa.local repeat every 15m until acknowledged
notification-action Email_Average_Warning condition severity in (Average, Warning)
send-to grupo-sistemas-tic@empresa.local schedule horario-laboral
```

8.5. Resumen de plantillas aplicadas

- Generic Switch SNMPv3: switches Core y de acceso.
- Generic AP/WLC SNMPv3: controlador Wi-Fi y puntos de acceso.
- Generic Firewall/UTM SNMPv3: firewall perimetral, incluyendo estado de VPN.
- Generic Linux/Windows Server (agente): servidores de la VLAN 60.
- Generic NVR/ICMP: NVR y cámaras de CCTV.
- Generic UPS/PDU SNMPv2c/v3: sistemas de alimentación de los armarios.