# Threat Model (Light)

Zabbix HLD - Enterprise Class Monitoring

Date Assessed: 06/08/2025

Prepared by: David Biayna Neal

Reviewed by: Will North, Charlie Harris, Trefor Walters

### Background

Zabbix is an open-source, enterprise-class monitoring platform used to collect and analyse metrics from servers, network devices, applications, and cloud services in real time. MHR’s deployment will cover approximately 6,500 assets across multiple data centres and remote offices, using a central Zabbix Server, MySQL database, web frontend, distributed proxies, and agents. Communications leverage TLS encryption, access controls via Active Directory for authentication and RBAC, also automated discovery and alerting for proactive incident response.

### Scope

**In-scope components:** Zabbix Server(s), MySQL Database, Web Frontend (Apache), Zabbix Proxies, Zabbix Agents, network architecture (ports 10050/10051, HTTPS), integration points (LDAP/AD, Service Desk).

**In-scope networks:** Corporate LAN (Mere Way DC), DR site (Ruddington Hall DC), DMZs, remote branch office segments behind firewalls.

### 

### Threat Assessment

The following key threats were identified and assessed.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Mitigation** | **Mitigated** |
| A malicious actor gains unauthorized access to Zabbix Web UI/API. | Zabbix Frontend configured with HTTPS on Apache/Nginx.  Defined granular RBAC roles (Guest/User/Admin/Super-Admin) via Active Directory.  Integration with LDAP/Active Directory or SAML SSO (supports MFA) for centralized auth. | Yes |
| Attacker on-path between agents/proxies/server poisons or reads monitoring data. | Enforced TLS encryption between agents, proxies, and the main server. | Yes |
| Attacker leverages credentials or pivots to the MySQL VM to dump history and config data. | Zabbix Database runs on a separate VM from the server; split DB and server roles for isolation. Data is metrics and not sensitive. | Yes |
| Attacker exploits known flaws in Zabbix, OS, or DB due to being unpatched to get a foothold on to the application and potentially break out. | Automatic security updates and a regular patch schedule via CIS Benchmark guidance. | Yes |

### Conclusion

Overall, the Zabbix monitoring platform is considered secure in its current deployment. As an internal-only tool with no direct Internet exposure, any attacker would first need to gain a foothold inside the corporate network before mounting an attack. The primary residual risk is a software-level vulnerability, which could enable a supply-chain attack; ongoing patch management and vendor vigilance remain critical to addressing this scenario.