advenica

Secure monitoring with Zabbix

Zabbix is an open-source software used to monitor IT equipment such as servers, network equipment, virtual machines, etc. In an installation with Zabbix, there are Zabbix proxies with the task of collecting information from its nearby equipment and to forward this information to a centrally located Zabbix server. The Zabbix server compiles the information and makes it available to an operator. The operator can define views, graphs, alarm conditions, etc. to facilitate and streamline their work.

Challenge

Spread of malicious code in sensitive systems

In a segmented network infrastructure where Zabbix proxies and Zabbix servers are placed in different zones, communication between these zones is controlled and monitored. The monitoring zone where the Zabbix server is located communicates with the zones that have systems that are monitored. Therefore, it is important to ensure that an attack in any of the zones cannot spread to other zones via these open pathways that enable the communication. The Zabbix server in the monitoring zone should also not have access to more services or applications in the other zones than what is allowed via Zabbix.

An attack on Zabbix where an attacker by exploiting vulnerabilities in the communication paths succeeds at remotely executing arbitrary code in Zabbix server or Zabbix proxy would be catastrophic, as it could spread to all interconnected systems. Even one, simpler attack that temporarily disrupts the availability of monitored systems would also most likely cause significant problems and large costs. Therefore, it is important to closely monitor the communication and thus reducing the attack vectors against the servers.

Solution

Strict communication between Zabbix proxy and server

The protocol used between Zabbix server and Zabbix proxy is based on JSON, and this solution checks that the communication meets the Zabbix protocol specification which tells exactly what the communication should look like. The solution is based on Advenica's ZoneGuard, on which it is installed and configured an application specially developed for Zabbix.

The current version of the solution supports version 4 of Zabbix in “passive mode”, which means that it is always the Zabbix server that initiates the communication with Zabbix proxy and not the other way around. Zabbix can communicate both compressed and encrypted traffic between server and proxy and the solution supports compressed communication but not encrypted communication.

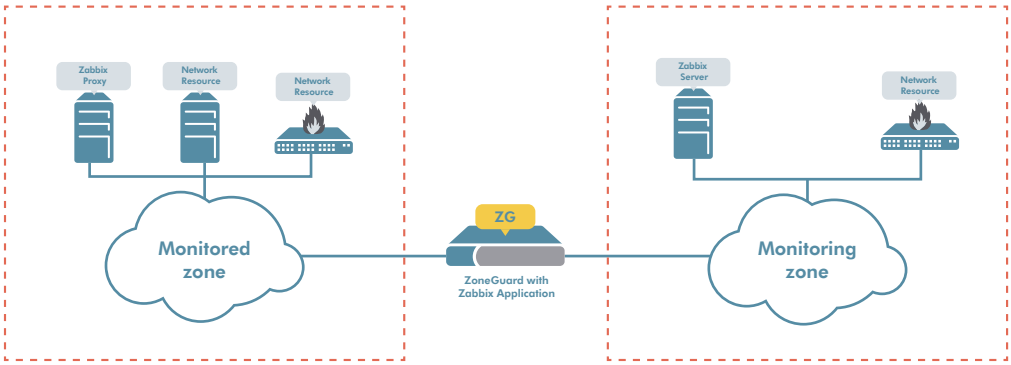

Figure 1. ZoneGuard with Zabbix application for monitoring communication between zones.

Advantages

Strict communication that prevents attacks

Unlike a regular firewall, this solution knows exactly how the Zabbix proxy and Zabbix server communicate with each other and checks that the communication stays within what is allowed. This prevents an attacker from going beyond specification to exploit vulnerabilities or bugs in Zabbix implementation or configuration. These vulnerabilities can, in the worst case, lead to the attacker taking over Zabbix server or proxies and in the next step, breaches of other systems in the zone.

advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more on advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED