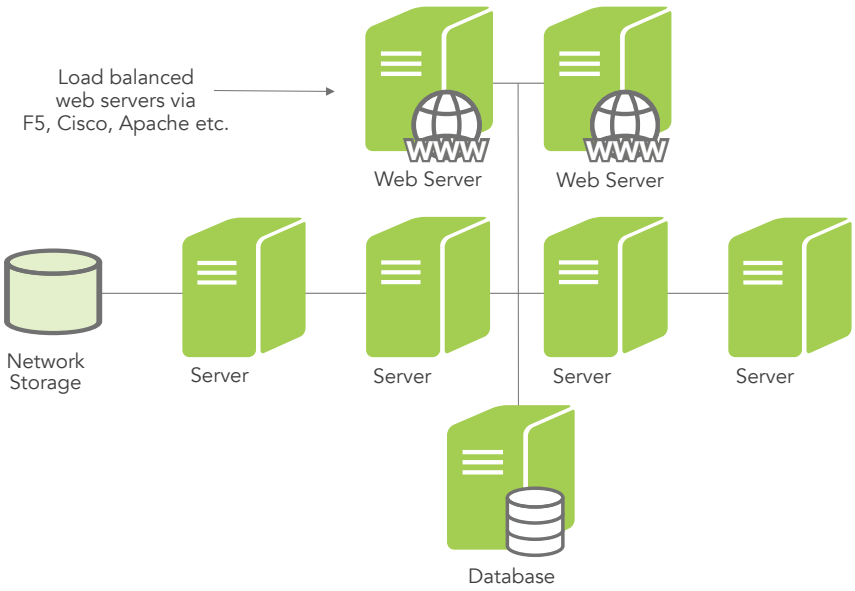
THREATVINE HUB: CYBER-SECURITY INFORMATION SHARING PLATFORM

Minimum Baseline

The diagram below shows the minimum configuration for an on-premise deployment of Threatvine Hub.



Each server shown must have at least the following configuration:

CPU : 2 cores+, 2GHz+
RAM : 4GB+
Disk : 16GB
Shared Disk : 100GB

The baseline configuration provides a minimum of resilience with the two web servers but non-resilient back-end infrastructure. All functionality could be affected by a single instance failure. Network storage is provided by Network Attached Storage (NAS) or Storage Area Network (SAN), which must also be available to the web nodes.

The load balancer (not shown) provides the following:

- **SSL offload from application to load balancer**
- **Session affinity setting required**
- **Optional login/Multi-Factor Authentication (MFA) management**

Resilient Baseline

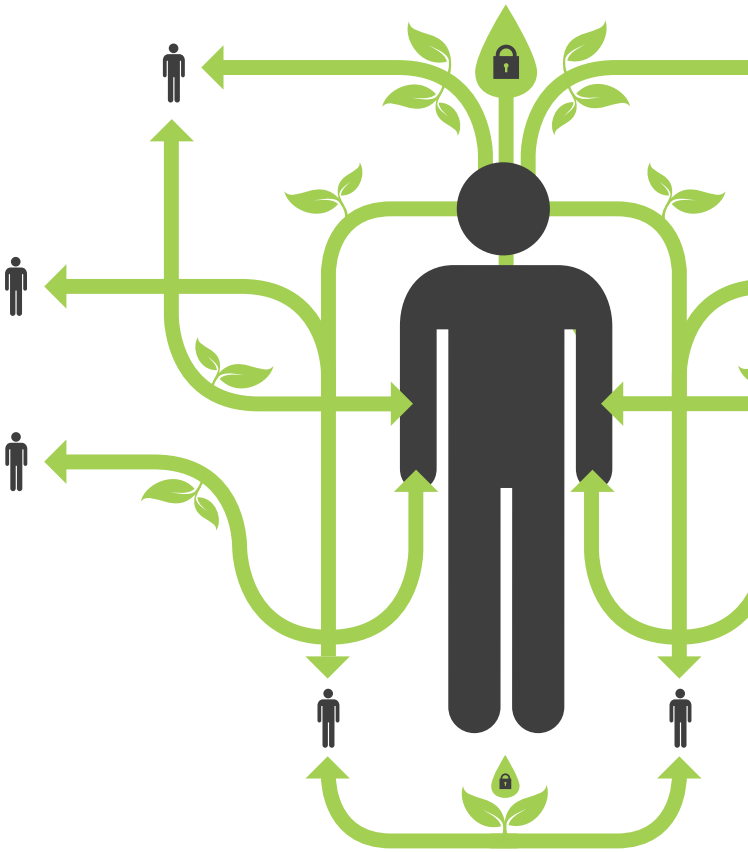
Building on the minimum baseline, adding resilience to the service is achieved by adding further back-end infrastructure. This includes five further servers (therefore nine in total) and a second database server.

Performant Baseline

A typical highly performant configuration is achieved by increasing CPU and memory. The first stage is typically to increase the number of web servers from two to four, as well as doubling the CPU count and increasing the memory to 6GB RAM on each server.

Software Prerequisites

The recommended Operating System for all servers is Red Hat Enterprise Linux or CentOS. Supported databases include: PostgreSQL (preferred), MySQL, Oracle and Microsoft SQL Server.



Network

All nodes are hosted on a gigabit network. Applications are subnetted and firewalled from each other. SMTP connectivity to the Internet is required for sending email notifications. HTTPS connectivity to the Internet is required for some application features.

Required IP addresses:

- 1 address providing access to the application
- 1 address to allow management access (using different infrastructure than the application)

Management and Security

The recommended management and security measures are as follows:

Management instances
Depending on your preferred way of working, instances for running Ansible, automation management and other administrative tasks.

User directory service
User accounts can be managed externally via LDAP or Active Directory. It is also possible to use a CRM to manage the user accounts.

Security/monitoring instances
We recommend at least a log aggregation appliance and a system monitor (such as Nagios) to look for excessive resource utilisation etc.

Anti-Malware
We suggest that the system is deployed with an anti-malware solution covering all instances, this may require extra server instance. Network level filtering may also be applied for additional confidence.

Content Delivery Network (CDN)
A CDN may be useful for large deployments with a lot of binary content. However, careful consideration of security and MFA must be made. We would suggest consultancy on any system of this scale.

Reference environment
Surevine recommend a reference environment (at least the minimum baseline) to enable testing of all product deployments and upgrades before deploying to the production environment.