Issued by	Document no.	Classification
Magnus Juntti	REQ-ODIN-001	Unclassified
Approved by	Issue	Date
Magnus Juntti	1.9	2018-06-06

System Hardware Requirements

ODIN

Issued by	Document no.	Classification
Magnus Juntti	REQ-ODIN-001	Unclassified
Approved by	Issue	Date
Magnus Juntti	1.9	2018-06-06

Contents

Issued by	Document no.	Classification
Magnus Juntti	REQ-ODIN-001	Unclassified
Approved by	Issue	Date
Magnus Juntti	1.9	2018-06-06

1 Revision History

Issue	Date	Author	Changes
1.0	2015-04-02	Magnus Juntti	First version
1.4	2015-09-14	Magnus Juntti	Changed disk size recommendations
1.5	2015-10-02	Magnus Juntti	Changed title to hardware requirements
1.6	2015-10-21	Magnus Juntti	Changed syslog RFC. Updated text about odin-tunnel.
1.7	2016-01-15	Magnus Juntti	Added NIDS Option requirements
1.8	2016-01-30	Magnus Juntti	Increased memory requirements for NIDS
1.9	2018-06-06	Magnus Juntti	Changed disk size requirements

2 Definitions and Acronyms

Definition	Description
GFE	Government Furnished Equipment
TAK	Totalförsvarets Aktiva Kort
TEID	Totalförsvarets Elektroniska ID
CPU	Central Processing Unit
RAID	Redundant Array of Inexpensive Disks
GB	GigaByte
RAM	Random Access Memory
HIDS	Host Intrusion Detection System

3 References

ID	Document ID	Title

Issued by	Document no.	Classification
Magnus Juntti	REQ-ODIN-001	Unclassified
Approved by	Issue	Date
Magnus Juntti	1.9	2018-06-06

4 Purpose

This document defines the system requirements for running the software package ODIN Security Log Server and its options.

5 Hardware Requirements

Server/Workstation with the following minimum requirements:

- Compatible with CentOS 6.9 or later in version 6-branch of CentOS.
- Minimum 4 CPU-cores, minimum 2GHz/core, Recommended 8 CPU-cores, 2.5GHz/core
- Minimum 16GB RAM, Recommended 96GB RAM
- Display with at least 1280*1024 pixels, recommended minimum 1920x1080. The log-analysis becomes more usable the larger the screen and resolution.
- Minimum storage size 128GB based on normal log flow. If the system has excessive logging larger drives may be needed. This depends on organizational requirements. See separate chapter for size calculations.
- Use fast drives, NVMe, SSD or 10-15k SAS mechanical disks are preferred. Redundant power units
- DVD-RW-unit for log-backup
- 1 Ethernet-port, fiber or TP
- For smartcard support, Gemalto .NET smartcards are supported out-of-the-box

For the alert function using a USB-relay, the following USB-relay shall be used:

- KMTronic USB-relay with one port (Model: U1CRB, USB one relay)

For unidirectional connection of ODIN to several security domains, the following extra hardware is also required:

- Network diode on each connection
- Switch to connect all incoming domains into one connection to ODIN

5.1 Disk Size Requirements

Disk sizes shall be chosen depending on two main factors:

1. Time between archiving
2. History time in analysis tool, i.e. how long is the searchable interval in the indexed database that is used for log analysis.

ODIN comes with a predefined disk partitioning that this calculation is based on. The customer may choose to alter this partitioning and thus this calculation may be different.

Choose sizes according to:

50 GB + the largest number of the following (all sizes in GB):

1. (Log amount per day + (days between archiving * (0,1 * log amount per day))) / 0,25

2. (Days of history * (10 * Log amount per day)) / 0,65

Example: If you have 2 GB of logs per day, you wan't to be able to analyze logs 60 days back in time and you archive logs every 30 days, the calculations would be:

1. 50 + (2 + (30 * (0,1 * 2))) / 0,25 = 82 GB
2. 50 + (60 * (10 * 2)) / 0,65 = 1896 GB

Thus you would choose 2 TB of storage for your ODIN.

5.2 NIDS Option Requirements

If the NIDS option is chosen, the following requirements replaces the corresponding requirements above:

- Core-requirement is as above but also one extra core for each network interface that is running NIDS
- Minimum memory requirement increases with 2GB per NIDS-interface
- 1 Ethernet-port, fiber or TP for logging (shall be the first enumerated NIC)
- 1 Ethernet-port, fiber or TP for each NIDS-interface that shall be used

6 GFE Requirements

In case special cryptographic components are needed for government/military installations, these products can be integrated with ODIN provided that they are compatible with CentOS 6.7 or RHEL 6.

These products are considered GFE and must be provided by the purchaser.

For Sweden the following GFE-products apply to ODIN and are compatible with ODIN:

- KrAPI for handling of Swedish Armed Forces smartcards (TAK/TEID).

6.1 GFE for test/integration

Special authentication solutions such as GFE smartcards requires that such smartcards and readers compatible with the smartcard are provided as GFE for use during test/integration. Such equipment will be returned when test/integration is complete.

7 Interface Requirements

- Time synchronization use NTP according to RFC 5905. NTP can be configured in standard mode or broadcast/multicast if used on a unidirectional link.
- Syslog for raw logs, analyzed by OSSEC in ODIN. Syslog according to RFC 3164 or RFC 5424, UDP port 514
- Syslog according RFC 5424 on port UDP 8514 for transmission of OSSEC alerts on a unidirectional link, i.e. from an OSSEC manager in the supervised domain. ODIN Log Concentrator handles this if that options is purchased.
- OSSEC proprietary format on UDP port 1514 if bidirectional connection of ODIN

NOTE: The last two requirements are mutually exclusive, one of them shall be used depending on if ODIN is connected via uni- or bi-directional link to the supervised system.

7.1 Operating System Requirements

For maximal use of ODIN, the software ODIN Integrity shall be installed in all supervised nodes. ODIN Integrity is compatible with most Operating Systems on the market such as Windows and Linux based systems. If HIDS-use is not wanted and ODIN is only used for log handling, all syslog compliant units can use syslog and ODIN can analyze these logs by creating log patterns for them. For Windows-based systems it is STRONGLY recommended that ODIN Logcollector is used to transfer logs and not any other third party syslog-compliant tool.

8 Other information

ODIN requires customization to the log formats generated by the system by creating pattern files for manual and automatic log analysis tools. This is a service that can be purchased as an option or performed by the purchaser using the supplied manuals.

Supervision of the server can be performed using the program odin-heartbeat which is supplied with ODIN. This will generate a security alarm if the communication with the supervised system fails.

If ODIN Log Concentrator (see chapter 9) is used for unidirectional links, encryption of the communication can be performed using odin-tunnel which is based on OpenSSL crypto-lib with using an AES 256 CBC symmetric crypto with a pre-shared key. It is also possible to use odin-tunnel as a separate software if ODIN Log Concentrator is not used. Odin-tunnel has been tested on CentOS 6, 7 and Windows 7, 10 clients.

9 ODIN Log Concentrator

This chapter defines the requirements on the optional ODIN Log Concentrator which can be used to integrate ODIN Security Log Server in a multi-level security domain where ODIN Security Log Server is connected via network diodes.

9.1 Hardware Requirements

Server with the following minimum requirements:

- Compatible with CentOS 6.9 or later in version 6-branch of CentOS.
- 2 CPU-cores, minimum 2GHz/core
- 4 GB RAM
- Hardware-RAID in RAID-1 configuration with minimum 2 drives
- Minimum Hard-drive size 50GB/drive
- Redundant power units
- No display is needed
- 2 Ethernet-ports, fiber or TP depending on interfaces used in the system/network diodes/ODIN