Secure your checkmk

and sleep well ...

Ralf Spenneberg

30. April 2019

Check_MK Conference

Kontakt:
info@os-s.net

OpenSource Security

Ralf Spenneberg

- OpenSource Security GmbH
  - Partner of Mathias Kettner GmbH since 2013

CISCO™

Greenbone

Bundesamt
für Sicherheit in der
Informationstechnik

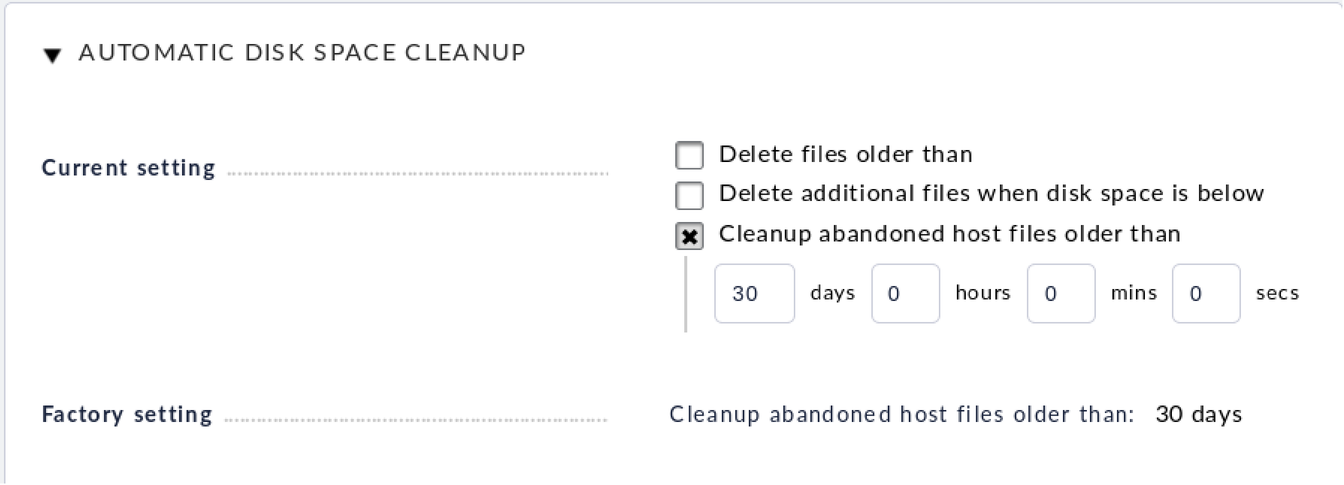
check MK

KOLAB

Allianz für
Cyber-Sicherheit

Security

- **Confidentiality**
  - Encryption
- **Integrity**
  - Authentication
  - Authorization
- **Availability**
  - Backups
  - Housekeeping



▼ AUTOMATIC DISK SPACE CLEANUP

Current setting

□ Delete files older than
□ Delete additional files when disk space is below
☒ Cleanup abandoned host files older than
30 days 0 hours 0 mins 0 secs

Factory setting

Cleanup abandoned host files older than: 30 days

OpenSource Security

Security

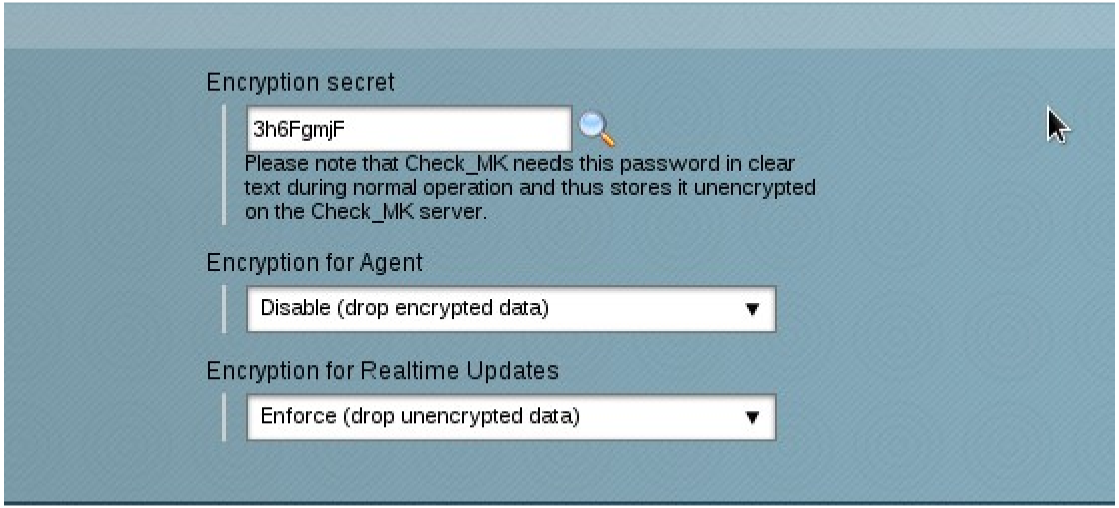
- Do **not** reduce the security of the monitored systems
- Sensitive Data must be protected!
- The monitoring must be protected

Check_MK Built-In Security

- Agent
  - Runs as root but does not accept any data over the network
  - Manual Installation on the target system
  - The admin manages the Agent
  - Agent Update Mechanism is critical
    - Hardening of the Update-Server required

Agent – Recommended Security

- SNMP
  - ➔ Views
  - ➔ ACLs
  - ➔ SNMPv3
- Agent
  - ➔ only_from
  - ➔ Embedded Encryption (1.4.0)
- **Demo**



Encryption secret

3h6FgmjF

Please note that Check_MK needs this password in clear text during normal operation and thus stores it unencrypted on the Check_MK server.

Encryption for Agent

Disable (drop encrypted data) ▼

Encryption for Realtime Updates

Enforce (drop unencrypted data) ▼

Check_MK Built-In Security

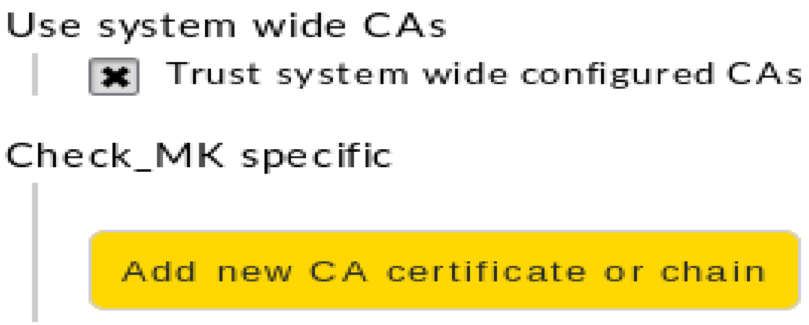
- Sites
  - Administration done as site user
  - Password/Public Key login possible
  - Internal switch to SSHA256 for passwords (1.6)
  - All processes use the site user
    - Apache
    - CMC/Nagios
    - Etc
    - Only icmpsender/receiver use root
  - Root access only required for
    - Creation, removal and renaming of the sites
    - Update of the OMD/Check_MK Edition

Sites – Recommended Security

- Enable HTTPS and Redirect HTTP
- Use LDAP/SSL for user integration
- Use Password Store for Plugin Passwords
- It is a store but no password safe
- **Demo**

SSL Connections to Other Systems

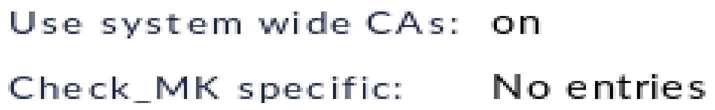
- Do **not** ignore SSL errors!
- Add CA certificates
  - OS
  - Check_MK
- **Demo**



Use system wide CAs

☒ Trust system wide configured CAs

Check_MK specific



Use system wide CAs: on

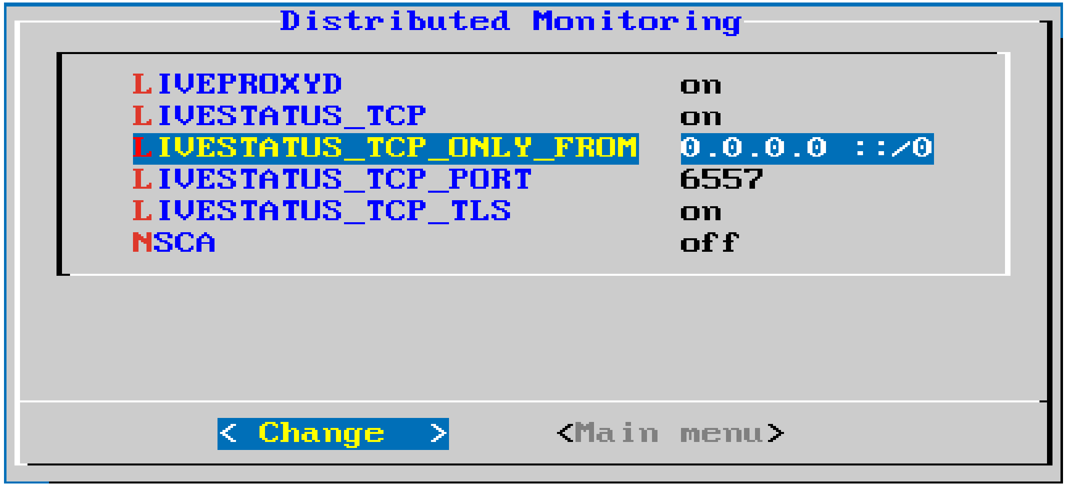
Check_MK specific: No entries

Distributed Monitoring

- Livestatus via TCP
- No restrictions by default
- Livestatus does not support any authentication nor authorization
- Distributed WATO may use SSL/TLS
- Livestatus supports commands!

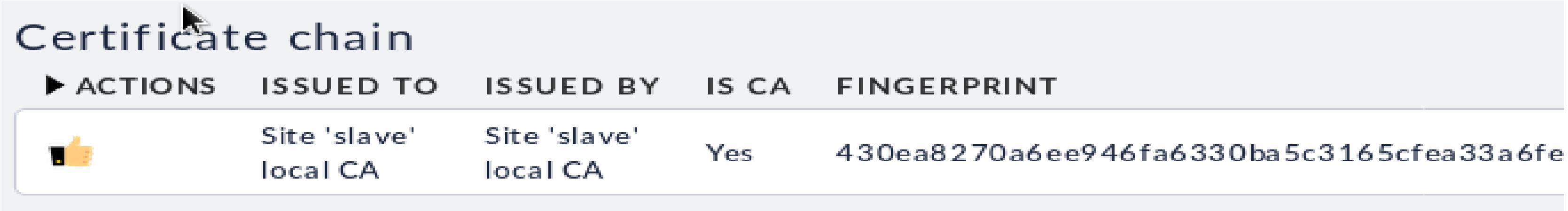
Livestatus SSL/TLS Connections

- New Feature in 1.6
- In CEE and CRE
- Uses stunnel
- **Demo**



```
                 Distributed Monitoring

      LIVEPROXYD                      on
      LIVESTATUS_TCP                  on
      LIVESTATUS_TCP_ONLY_FROM        0.0.0.0 ::/0
      LIVESTATUS_TCP_PORT             6557
      LIVESTATUS_TCP_TLS              on
      NSCA                            off
```



Certificate chain

▶ ACTIONS	ISSUED TO	ISSUED BY	IS CA	FINGERPRINT
👍	Site 'slave' local CA	Site 'slave' local CA	Yes	430ea8270a6ee946fa6330ba5c3165cfea33a6fe

Analyze Configuration

- Best Practices
  - omdadmin/omd
  - SSL
  - Encrypted Backup
  - etc.

Discussion

?