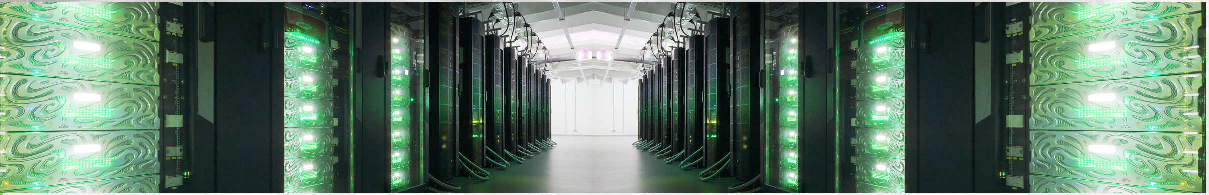
GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Discussion of the Security Concepts at NHR@Göttingen from 1000 Feets

Hendrik Nolte



Security Onion NHR@Göttingen

- Security Onion with 4 Layers
- Most sensitive systems at the top
- *ssh* access to admin nodes only
  - from an isolated admin-network
  - using sk keys on the JumpHost
- Only Movement downwards permitted
  - Enforced via node-local firewalls

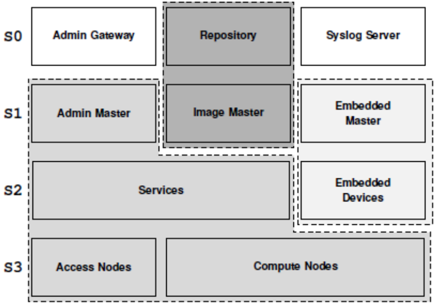


Abbildung LB.3: Sicherheitsschichten in der Systemkonfiguration des HLRN-IV.

Security Onion NHR@Göttingen - Layers

- Layer 0
  - Most sensitive Systems
  - JumpHost, Syslog Server, etc.
  - Administration via special clients
- Layer 2
  - Management Nodes with daemons
  - e.g. slurmctld, licenses, filesystems
- Layer 1
  - Everything between Layer 0 and 2
  - e.g. Admin Master
- Layer 3
  - user nodes

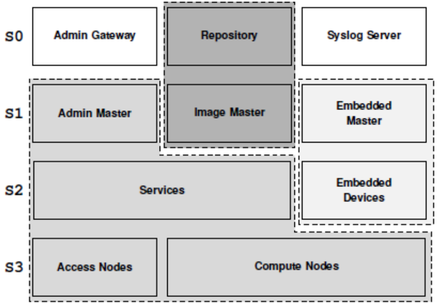


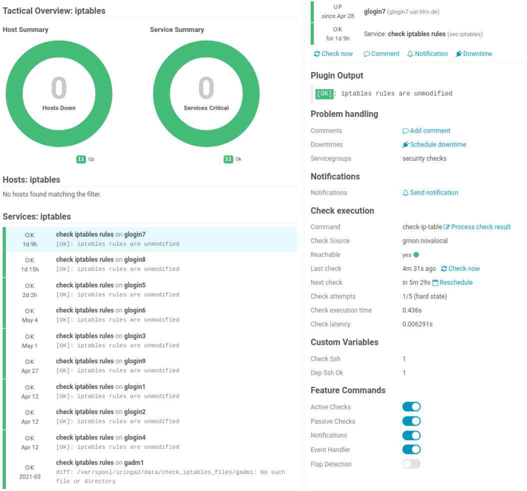
Abbildung LB.3: Sicherheitsschichten in der Systemkonfiguration des HLRN-IV.

Islands and Networks

- Admin (T0-T2) and user nodes (T3) are separated into islands
- Each islands has 4 LANs:
  - PXE
  - BMC
  - User
  - Management
- User and admin LAN’s are, if required, routed
- Port isolation can be enforced on externally managed switches
- High-Speed interconnects, e.g. OPA, or Infiniband, are treated additionally

Compliance Checking

- Compliance checking on all nodes
  - Continuously during runtime
- Methodology
  - Create security concept for each node
  - Derive legitimate system state
  - Determine critical components
  - Check them via Icinga/Nagios
    - Simple checksum
- Components
  - iptables, ssh files, kernel modules
- Purpose
  - Not for intrusion detection
  - Proactively prevent vulnerability due to under-coffinated admin



Tactical Overview: iptables

Host Summary

0 Hosts Down

11 Up

Service Summary

0 Services Critical

11 Ok

Hosts: iptables

No hosts found matching the filter.

Services: iptables

OK 1d 9h **check iptables rules** on **glogin7**
```
[OK]: iptables rules are unmodified
```
OK 1d 15h **check iptables rules** on **glogin8**
```
[OK]: iptables rules are unmodified
```
OK 2d 2h **check iptables rules** on **glogin5**
```
[OK]: iptables rules are unmodified
```
OK May 4 **check iptables rules** on **glogin6**
```
[OK]: iptables rules are unmodified
```
OK May 1 **check iptables rules** on **glogin3**
```
[OK]: iptables rules are unmodified
```
OK Apr 27 **check iptables rules** on **glogin9**
```
[OK]: iptables rules are unmodified
```
OK Apr 12 **check iptables rules** on **glogin1**
```
[OK]: iptables rules are unmodified
```
OK Apr 12 **check iptables rules** on **glogin2**
```
[OK]: iptables rules are unmodified
```
OK Apr 12 **check iptables rules** on **glogin4**
```
[OK]: iptables rules are unmodified
```
OK 2021-03 **check iptables rules** on **gadm1**
```
diff: /var/spool/icinga2/data/check_iptables_files/gadm1: No such
file or directory
```

UP since Apr 28 **glogin7** (glogin7.usr.hlrn.de)

OK for 1d 9h Service: **check iptables rules** (sec-iptables)

Plugin Output

```
[OK]: iptables rules are unmodified
```

Problem handling

Comments	Add comment
Downtimes	Schedule downtime
Servicegroups	security checks

Notifications

Notifications	Send notification

Check execution

Command	check-ip-table Process check result
Check Source	gmon.novalocal
Reachable	yes ●
Last check	4m 31s ago Check now
Next check	in 5m 29s Reschedule
Check attempts	1/5 (hard state)
Check execution time	0.436s
Check latency	0.006291s

Custom Variables

Check Ssh	1
Dep Ssh Ok	1

Feature Commands

Active Checks	●
Passive Checks	●
Notifications	●
Event Handler	●
Flap Detection	○