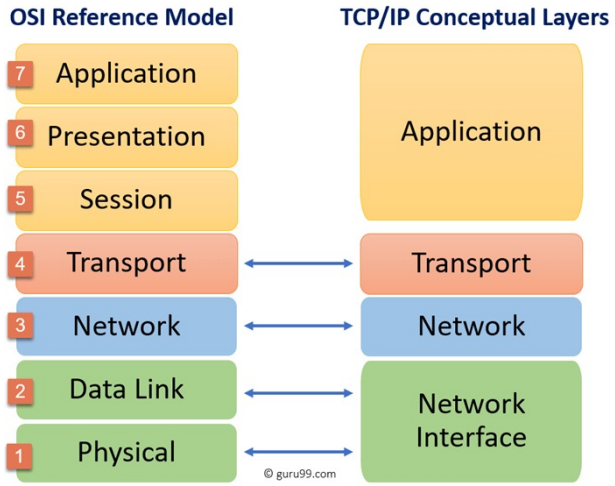
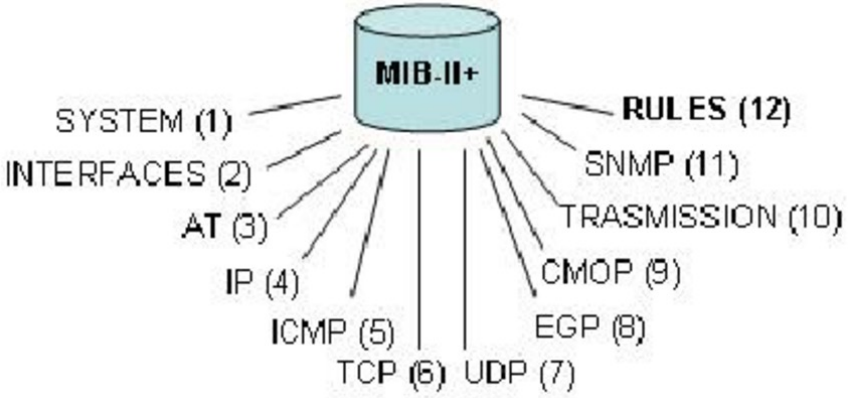
A gerência de falhas e a infrastrutura para gerência da rede

O protocolo SNMP é o mais usado para a gerência de redes. E é conhecido suas limitações quanto a segurança.

Qual o objetivo da gerência de redes?

- Identificar problemas desde a camada fisica até aplicação
- O conceito de FCAPS continua atual
  - **Fault, configuration, accounting, performance, security**
  - Com ele é possivel gerenciar todas as camadas das pilhas de protocolos





Pontos fundamentais da gerência: - Definir MÉTRICAS

- **Estabeleça as métricas** que são importantes para você
  - Transações por segundo
  - Tempo de resposta (RTT)
  - Experiência do usuário (tempo para visualizar uma pagina completa)
  - Histórico de visualizações de uma pagina web
- Não, **você não vai conseguir gerenciar todas as métricas possiveis !!!**
  - É possivel analisar esses dados usando IA (Inteligencia Artificial)
  - Cluster podem levar horas/dias para correlacionar esses
    - Exige programação e recursos (Cluster computacional)

Pontos fundamentais da gerência: - Obter DADOS (Monitoramento)

- Obter dados
  - De **forma passiva** (tcpdump, network flows)
  - De **forma ativa** (SNMP, Ping, Traceroutes, SSH, APIs, HTTPS, NETCONF-over-SSH)
  - Nao use SNMPv1, Telnet e HTTP
- Quais fontes são comuns?
  - Roteadores, switches, servidores
  - Sensores (temperatura, energia)
  - Dados de aplicações
  - Infraestrutura de virtualização (consoles)

Monitoramento Black Box / White Box

- Black box
  - **Monitora metricas em equipamentos**
  - Método mais usado em Roteadores, Switches, server hypervisor
  - Ex.: Alerta de erros em disco, tráfego em Interfaces de rede

- White box
  - Monitora a “**experiência do usuário**”
  - Tempo de resposta das queries SQL
  - Numero de usuários acessando uma página web ou uma transação

Monitoramento Black Box / White Box

- Black box
  - É a gerencia de redes mais tradicional
  - Utiliza protocolos e ferramentas que podem ser adquiridas no mercado
  - Administradores de redes e sistemas

- White box
  - Exige customização para cada aplicação/serviço
  - Administradores de redes & DevOps
  - Agora DevOps tem parte da responsabilidade de monitorar aplicações
  - Tradicionamente a operação também fica com o NOC

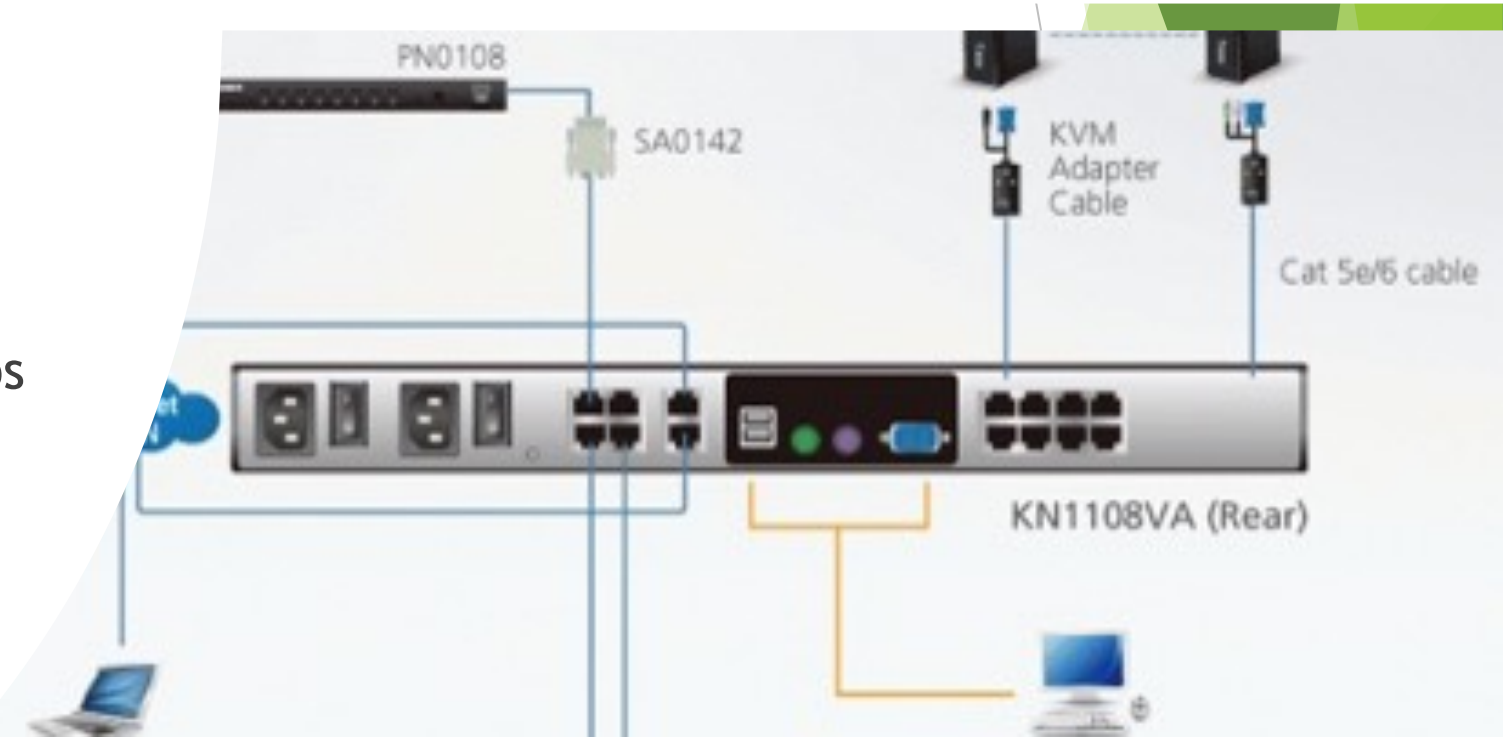
Como estruturar a topologia da rede de gerência?

Gerencia in-band e out-of-band

- Gerência in-band
  - Equipamento administrado via rede local
  - Compartilha a mesma interface de serviço (tráfego de usuário)
    - Ex: ssh para o ip publico de uma máquina ou roteador
  - Problema:
    - Quando a rede falha você perde também a gerência

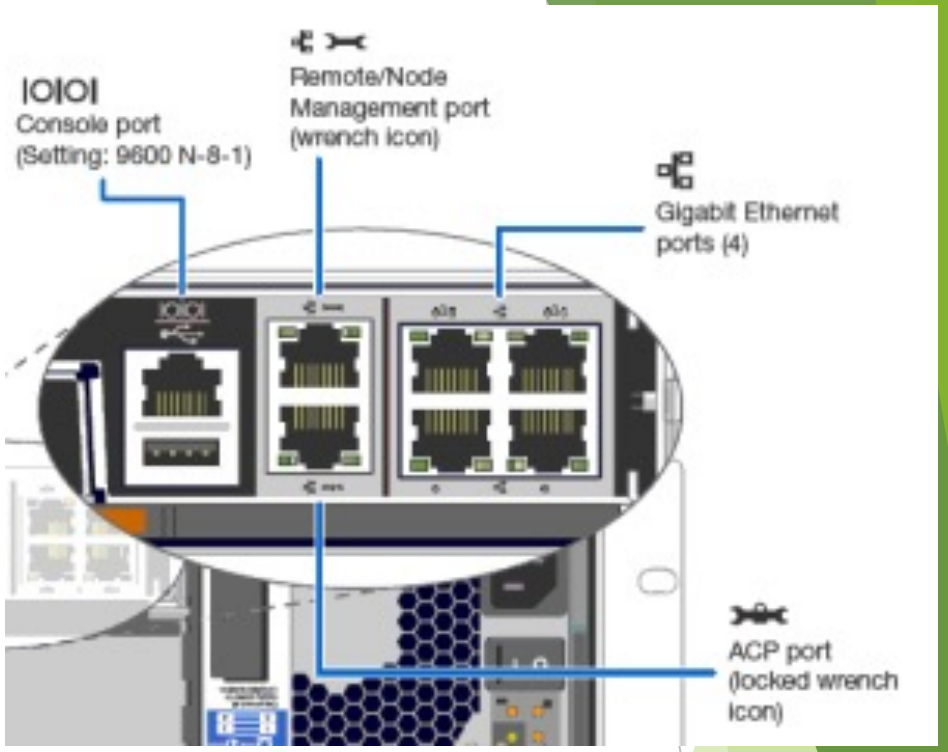
Gerencia out-of-band

- Gerência out-of-band
  - Método dedicado para acessar equipamentos
  - Não utiliza a mesma rede de serviço
  - Conceito de console remota
  - Opção para equipamentos criticos (geradores, no-breaks, core routers)



Gerencia out-of-band (OOB)

OOB pode ser implementada via console ou porta de gerencia do equipamento

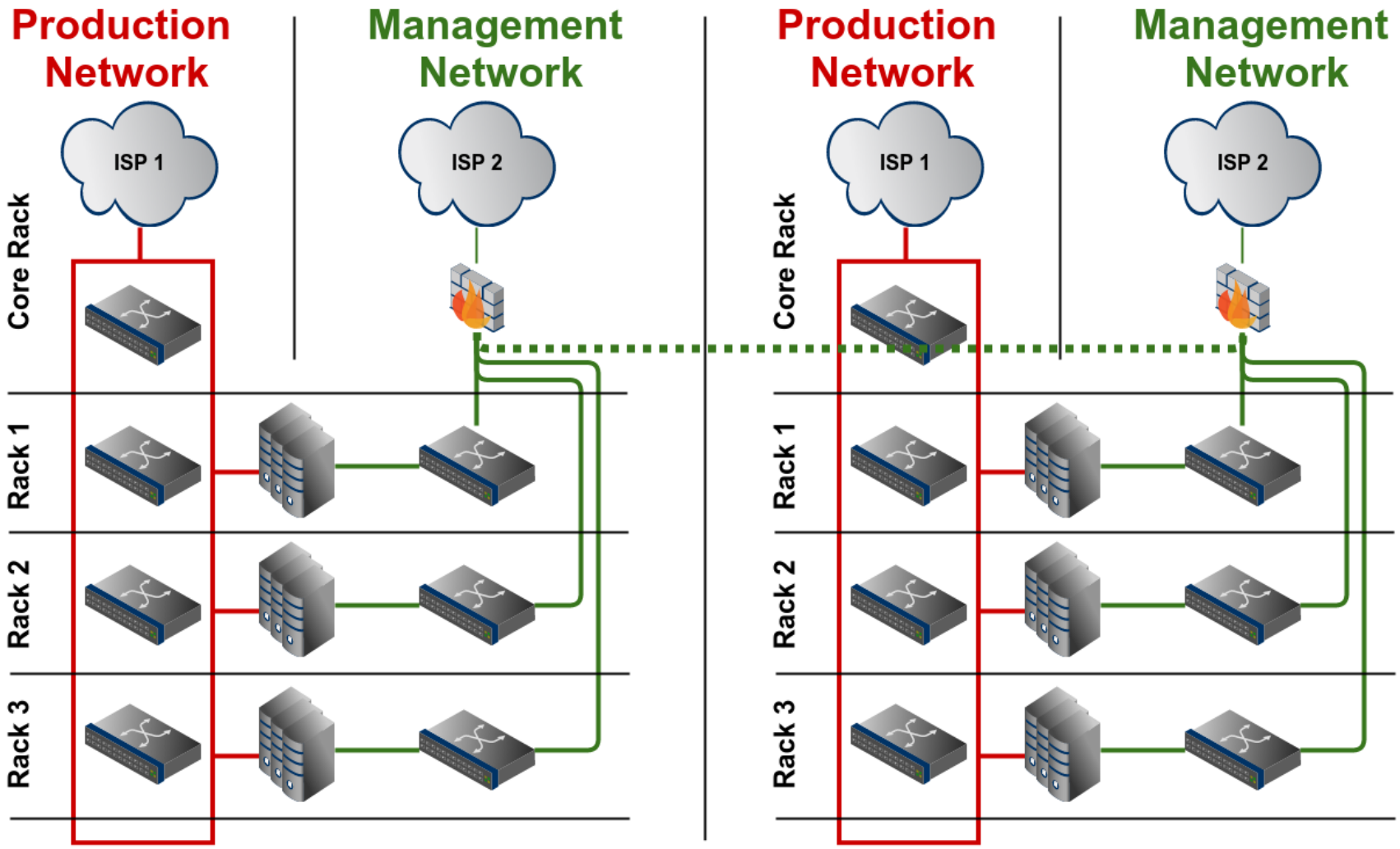


Parametro	Porta CONSOLE	Porta MANAGEMENT
Endereço IP	Não permite	Usa endereço IP
acesso via Telnet/SSH	No	Yes
Segregação de tráfego	Segregação fisica	Segregação por VRF
Velocidade da porta	0.1 Mbps (115200 bps)	1 Gbps
Tipo de gerência	Out of Band Management	Out of Band Management
Sequencia de boot	Mostra sequencia de Boot	NÃO mostra sequencia de Boot
SNMP, SSH	SEM SNMP ou SSH - mostra mensagens da console	SNMP, syslog, ssh, ACL para acesso
Acesso	HyperTerminal	Telnet/SSH, Web GUI

Criando uma rede de gerencia out-of-band (OOB)

- Algumas vezes é preciso usar vlans
- Lembrar de filtrar acesso originado nas maquinas clientes para outras maquinas (ssh)
- Normalmente usa uma rede invalida (rfc 1918) (ex. 10.0.0.0/8)
- Lembre-se: Backups de servidores devem ser out-of-band !

Criando uma rede de gerencia out-of-band (OOB)



E quais sistemas de gerência podemos usar?

Um bom NMS permite integração!

Ex: mail, sistema de tickets, diferentes BDs.
Quanto mais opções de integração, melhor.

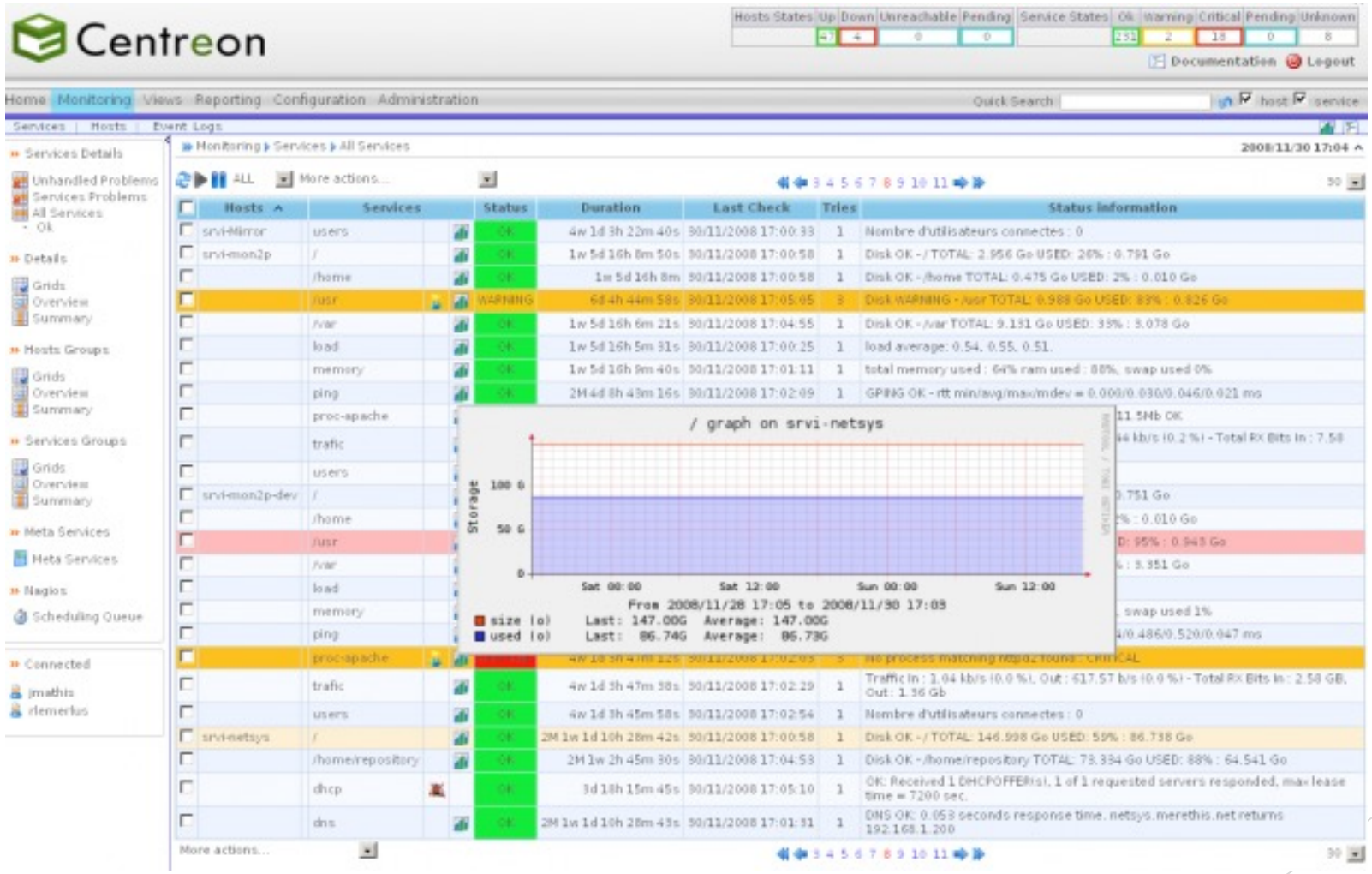
Várias opções gratuitas e de baixo custo

Descoberta automática de equipamentos é um vantagem considerável !

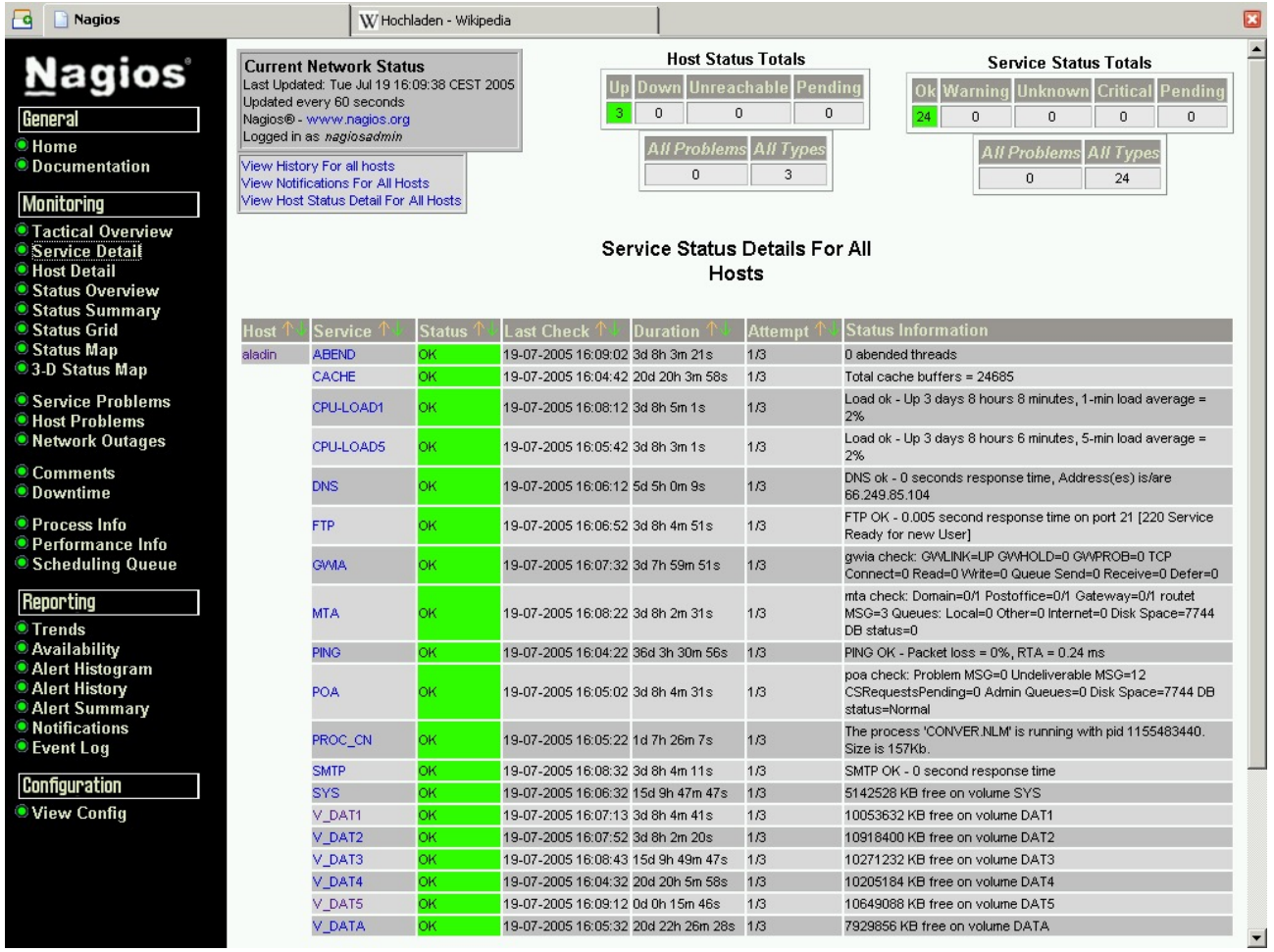
- ZABBIX
- PRTG NETWORK MONITOR
- IPSWITCH WhatsUpGold
- ManageEngine
- SPICEWORKS
- ICINGA
- openNMS®
- Nagios®

Zabix Dashboard + Grafana

Centreon


Centreon
Hosts States Up Down Unreachable Pending
Service States Ok Warning Critical Pending Unknown
Documentation
Logout
Home Monitoring Views Reporting Configuration Administration
Quick Search
Services Hosts Event Logs
Services Details
Unhandled Problems
Services Problems
All Services
Details
Hosts Groups
Services Groups
Meta Services
Nagios
Scheduling Queue
Connected
jmathis
rlemerlus
Monitoring Services All Services
2008/11/30 17:04
ALL
More actions...
Hosts Services Status Duration Last Check Tries Status Information
/ graph on srvi-netsys
Storage
100 G
50 G
0
Sat 00:00
Sat 12:00
Sun 00:00
Sun 12:00
From 2008/11/28 17:05 to 2008/11/30 17:03
size (o) Last: 147.00G Average: 147.00G
used (o) Last: 86.74G Average: 86.73G

Nagios


Nagios
Hochladen - Wikipedia
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Status Overview
Status Summary
Status Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Current Network Status
Last Updated: Tue Jul 19 16:09:38 CEST 2005
Updated every 60 seconds
Nagios® - www.nagios.org
Logged in as nagiosadmin
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
3 0 0 0
All Problems All Types
0 3
Service Status Totals
Ok Warning Unknown Critical Pending
24 0 0 0 0
All Problems All Types
0 24
Service Status Details For All Hosts
Host Service Status Last Check Duration Attempt Status Information
aladin ABEND OK 19-07-2005 16:09:02 3d 8h 3m 21s 1/3 0 abended threads
CACHE OK 19-07-2005 16:04:42 20d 20h 3m 58s 1/3 Total cache buffers = 24685
CPU-LOAD1 OK 19-07-2005 16:08:12 3d 8h 5m 1s 1/3 Load ok - Up 3 days 8 hours 8 minutes, 1-min load average = 2%
CPU-LOAD5 OK 19-07-2005 16:05:42 3d 8h 3m 1s 1/3 Load ok - Up 3 days 8 hours 6 minutes, 5-min load average = 2%
DNS OK 19-07-2005 16:06:12 5d 5h 0m 9s 1/3 DNS ok - 0 seconds response time, Address(es) is/are 66.249.85.104
FTP OK 19-07-2005 16:06:52 3d 8h 4m 51s 1/3 FTP OK - 0.005 second response time on port 21 [220 Service Ready for new User]
GWIA OK 19-07-2005 16:07:32 3d 7h 59m 51s 1/3 gwia check: GWLINK=UP GWHOLD=0 GWPROB=0 TCP Connect=0 Read=0 Write=0 Queue Send=0 Receive=0 Defer=0
MTA OK 19-07-2005 16:08:22 3d 8h 2m 31s 1/3 mta check: Domain=0/1 Postoffice=0/1 Gateway=0/1 routet MSG=3 Queues: Local=0 Other=0 Internet=0 Disk Space=7744 DB status=0
PING OK 19-07-2005 16:04:22 36d 3h 30m 56s 1/3 PING OK - Packet loss = 0%, RTA = 0.24 ms
POA OK 19-07-2005 16:05:02 3d 8h 4m 31s 1/3 poa check: Problem MSG=0 Undeliverable MSG=12 CSRequestsPending=0 Admin Queues=0 Disk Space=7744 DB status=Normal
PROC_CN OK 19-07-2005 16:05:22 1d 7h 26m 7s 1/3 The process 'CONVER.NLM' is running with pid 1155483440. Size is 157Kb.
SMTP OK 19-07-2005 16:08:32 3d 8h 4m 11s 1/3 SMTP OK - 0 second response time
SYS OK 19-07-2005 16:06:32 15d 9h 47m 47s 1/3 5142528 KB free on volume SYS
V_DAT1 OK 19-07-2005 16:07:13 3d 8h 4m 41s 1/3 10053632 KB free on volume DAT1
V_DAT2 OK 19-07-2005 16:07:52 3d 8h 2m 20s 1/3 10918400 KB free on volume DAT2
V_DAT3 OK 19-07-2005 16:08:43 15d 9h 49m 47s 1/3 10271232 KB free on volume DAT3
V_DAT4 OK 19-07-2005 16:04:32 20d 20h 5m 58s 1/3 10205184 KB free on volume DAT4
V_DAT5 OK 19-07-2005 16:09:12 0d 0h 15m 46s 1/3 10649088 KB free on volume DAT5
V_DATA OK 19-07-2005 16:05:32 20d 22h 26m 28s 1/3 7929856 KB free on volume DATA

Infraestrutura básica para gerência da rede

Leandro M. Bertholdo