

Gerência de Redes

Ferramentas de Gerência

Cássio D. B. Pinheiro
pinheiro.cassio@ig.com.br
cassio.orgfree.com

Ferramentas de Gerência

- Ferramentas necessárias para cada uma das áreas de gerenciamento (FCAPS).
- Podem ser implementadas em hardware ou software.
- A eficácia do uso depende do conhecimento do gerente.

Ferramentas de Gerência

- Lista das aplicações típicas de um ambiente de gerência.
 - O propósito é mostrar a variedade das aplicações de gerência necessárias numa solução de gerência completa.
 - Também mostra como a funcionalidade é tipicamente juntada em aplicações.
 - Nenhuma aplicação de gerência faz tudo.

Ferramentas de Gerência

- Lista das aplicações típicas de um ambiente de gerência.
 - Polling SNMP e mib browsing.
 - Tratamento de traps.
 - Auto descobrimento e auto topologia.
 - Tratamento de eventos (recepção, filtragem, correlação) e alarmes.
 - Automação de diagnóstico (sistemas especialistas).
 - Trouble ticketing, help desk.

Ferramentas de Gerência

- Lista das aplicações típicas de um ambiente de gerência.
 - Configuração de dispositivos de rede.
 - Monitoração e análise de tráfego.
 - Análise estatística, trending, emissão de relatórios.
 - Inventário, gerência da planta baixa de cabeamento.
 - Planejamento de capacidade, projeto de rede.
 - Gerência de estações clientes.

Ferramentas de Gerência

- Lista das aplicações típicas de um ambiente de gerência.
 - Automação de console, consolidação de mensagens para o operador.
 - Gerência de bancos de dados.
 - Gerência de aplicações.
 - Gerência de configuração e controle de mudança.
 - Gerência de hospedeiro (gerência de workload, armazenamento, backup, contas de usuários, ...).

Ferramentas de Gerência

- Lista das aplicações típicas de um ambiente de gerência.
 - Gerência de impressão (spool).
 - Distribuição de software, gerência de licenças.
 - Contabilidade de recursos e faturamento.
 - Gerência de segurança.
 - Gerência de service-level agreements.
 - Gerência de processos de negócio.

F (Falhas)

- Conhecimento empírico do administrador (muito importante).
- Analisador de rede.
 - Hardware
 - Testador de cabos
 - Fluke(<http://www.fluke.com>)
 - Software
 - Sniffer
 - Network Management System (NMS)

C (Configuração)

- Software proprietário.
- Telnet (hubs, switches, roteadores).
- Web.
 - Impressoras,
 - Roteadores,
 - Proxy, etc.
- Terminal Server

A (Contabilização)

- Logs do sistema operacional.
- Logs do software que está sendo utilizado.
 - Sistema administrativo
 - Servidor de contas
 - Proxy
 - Firewall
 - RAS
 - Servidor de e-mail
- Ferramentas para análise de logs.
 - Grande volume de dados
 - Sistema especialista

P (Desempenho)

- Sniffer
 - Analise de desempenho
- Ferramentas do sistema operacional
 - Ping
 - Traceroute ou tracert
 - Netstat
 - Arp
 - Nslookup

P (Desempenho)

- Ferramentas que utilizam SNMP, RMON
 - Network Management Systems
 - HP Openviewda HP (<http://www.openview.com>)
 - Trancendda 3com (descontinuado)
 - 3com Network Supervisor (<http://www.3com.com>)
 - IBM Tivoli Netview (<http://www-3.ibm.com/software/tivoli/>)
 - Cisco Works
 - Optivity Network Management System(NMS)
 - Solar Winds Network Management (<http://www.solarwinds.net>)
 - SNMPc (<http://www.castlerock.com/>)
 - Whatsup)<http://www.ipswitch.com/>)

P (Desempenho)

- Ferramentas que utilizam SNMP, RMON
 - MRTG
 - Clássico para área de gerenciamento
 - <http://www.mrtg.org>
 - Exemplos
 - <http://www.rnp.br/operacao/>
 - PRTG para sistemas operacionais Windows

S (Segurança)

- Firewall
 - Análise de todos os pacotes que entram e saem da rede.
 - Filtro de serviços não desejados.
 - Bloqueio de redes ou IPs suspeitos ou indesejados.
 - Iptables nativo no linux.
 - Ipchains nativo no linux.
 - Checkpoint (ferramenta comercial).
- Sniffer
 - Monitoramento do tráfego em um segmento.
 - Captura de todos os pacotes em um segmento.
 - Análise de situações suspeitas.

S (Segurança)

- Proxy
 - Squid
 - Microsoft
 - Netscape
 - Analise do log
 - Descoberta de uso indevido do recurso, através do rastreamento.
 - Webtrends.
 - <http://www.webtrends.com/>
- DHCP
 - Amarra IP ao MAC address da estação

S (Segurança)

- Backup
 - Cópia diária dos dados armazenados nos servidores.
 - Arcserver,
 - Veritas,
 - Backup.