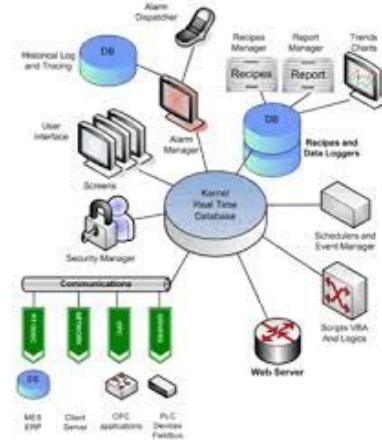


INFRAESTRUTURA DE REDES COMO SERVIÇOS



Aula 01 : Funções de Gerenciamento e Administração de Redes

- Compreender os conceitos fundamentais de gerenciamento de redes
- Identificar os principais modelos e arquiteturas de gerenciamento
- Entender o modelo FCAPS
- Identificar protocolos de gerenciamento
- Utilizar ferramenta de monitoramento
- Interpretar métricas de desempenho
- Realizar monitoramento básico em laboratório

Conceito de Gerenciamento de Redes

Gerenciamento de redes é o conjunto de processos, ferramentas e práticas responsáveis por:

- **Monitorar**
- **Controlar**
- **Manter**
- **Otimizar**
- **Garantir segurança**

de uma infraestrutura de rede física, virtual ou baseada em nuvem.

Em ambientes modernos (IaaS, PaaS e SaaS), o gerenciamento é essencial para garantir:

- SLA (Service Level Agreement)
- Alta disponibilidade
- Escalabilidade
- Segurança da informação

Modelo FCAPS

O modelo **FCAPS**, definido pela **ISO**, organiza o gerenciamento em cinco áreas:

| Letra | Função | Descrição |
|-------|--------------------------|-------------------------------|
| F | Fault Management | Detecção e correção de falhas |
| C | Configuration Management | Controle de configurações |
| A | Accounting Management | Controle de uso e recursos |
| P | Performance Management | Monitoramento de desempenho |
| S | Security Management | Controle de segurança |

Protocolos e Padrões

SNMP – Simple Network Management Protocol

O **SNMP** é o protocolo padrão para gerenciamento de dispositivos de rede.

Componentes:

- Manager (Gerente)
- Agent (Agente)
- MIB (Management Information Base)

Versões:

- SNMPv1
- SNMPv2c
- SNMPv3 (com autenticação e criptografia)

Protocolos e Padrões

NetFlow – Monitoramento de tráfego

Desenvolvido pela Cisco para **monitoramento e análise de tráfego de rede**

Um **fluxo** é um conjunto de pacotes que compartilham características em comum, como:

- Endereço IP de origem
- Endereço IP de destino
- Porta de origem
- Porta de destino
- Protocolo (TCP, UDP, etc.)
- Interface de entrada

Protocolos e Padrões

NetFlow – Monitoramento de tráfego

Que tipo de informações o NetFlow fornece?

O NetFlow não captura o conteúdo do pacote (payload), mas sim metadados, como:

- Volume de tráfego (bytes e pacotes)
- Tempo de início e fim da comunicação
- Dispositivos de origem e destino
- Aplicações utilizadas
- Padrões de uso da rede

Protocolos e Padrões

NetFlow – Monitoramento de tráfego

O NetFlow é amplamente utilizado para:

Segurança

- Detectar ataques DDoS
- Identificar tráfego suspeito
- Monitorar exfiltração de dados

Análise e Planejamento

- Identificar gargalos
- Planejar capacidade (capacity planning)
- Analisar consumo por usuário ou aplicação

Troubleshooting

- Descobrir quem está consumindo banda
- Analisar lentidão na rede

Protocolos e Padrões

NetFlow – Monitoramento de tráfego

- **NetFlow v5** – Versão tradicional e mais utilizada.
- **NetFlow v9** – Baseado em templates, mais flexível.
- **IPFIX (RFC 7011)** – Padrão aberto baseado no NetFlow v9.

Protocolos e Padrões

sFlow – Monitoramento de tráfego

Amostragem: Ao contrário do NetFlow, que monitora fluxos completos, o sFlow utiliza **amostragem aleatória** de pacotes para estimar o tráfego. Ele envia amostras de pacotes para análise.

Escalabilidade: A amostragem permite uma **maior escalabilidade**, pois reduz a quantidade de dados enviados ao coletor, sendo útil em redes de alto tráfego.

Medições de Tráfego e de Desempenho: Além de capturar o tráfego de dados, o sFlow também coleta dados de **desempenho da interface** (ex.: uso de CPU e memória do dispositivo).

Granularidade: Não oferece o mesmo nível de detalhamento que o NetFlow, pois só amostra pacotes e não coleta todos os fluxos. Isso pode reduzir a precisão da análise.

Protocolos e Padrões

sFlow – Monitoramento de tráfego

Quando usar:

- Quando há uma **alta taxa de tráfego** e você precisa de uma solução mais **leve e escalável**.
- Quando se quer **visibilidade geral** sobre a rede sem sobrecarregar a infraestrutura.

Protocolos e Padrões

Basicamente:

- **NetFlow** é ótimo para **análise detalhada de fluxos** e é bastante popular em redes Cisco.
- **sFlow** é mais **escalável** e adequado para **redes de alto tráfego** devido à amostragem, embora seja menos preciso.
- **IPFIX** é uma **evolução do NetFlow** que oferece maior flexibilidade e **interoperabilidade** entre diferentes dispositivos e fornecedores.

FAREMOS UM TRABALHO EM OUTRO MOMENTO SOBRE NetFlow, sFlow e IPFIX.

Protocolos e Padrões

Syslog – Protocolo padrão de envio de logs em redes IP

Ele permite que dispositivos (servidores, roteadores, firewalls, switches etc.) enviem mensagens de log para um servidor central.

Porta padrão: **UDP 514**

Também pode usar **TCP** ou **TLS** (para maior segurança)

Softwares:

rsyslog - comum como padrão no Linux

syslog-ng - mais flexível e presente em ambientes corporativos

Outras Tecnologias

- **Zabbix** – Monitoramento open source
- **Nagios** – Monitoramento de infraestrutura
- **PRTG Network Monitor** – Monitoramento corporativo

Gerenciamento de falhas

Definição de Gerenciamento de Falhas

- **Objetivo:** Detectar, isolar, diagnosticar, corrigir e recuperar falhas rapidamente.
- **Impacto:** Minimizar o tempo de inatividade e melhorar a qualidade da rede.

[Detecção] → [Isolamento] → [Diagnóstico] → [Correção] → [Recuperação]



Alerta

Identificar

Analisar Logs

Consertar

Testar e Confirmar

Problema

Gerenciamento de falhas

Exemplo de MTTR e MTBF

| |
|----------------------|
| +-----+ |
| |
| Falha 1 (MTTR) |
| 30 min (tempo médio) |
| +-----+ |
| +-----+ |
| |
| Falha 2 (MTBF) |
| 72 horas (tempo |
| entre falhas) |
| +-----+ |

Gerenciamento de Configuração

Funções Principais

- **Backup de Configurações:** Armazenamento regular das configurações de dispositivos críticos.
- **Controle de Versões:** Manter um histórico de alterações.
- **Padronização:** Garantir configurações consistentes em todos os dispositivos.

[Coleta] → [Armazenamento] → [Controle de Versão] → [Aplicação] → [Monitoramento]



Coletar

Backup

Registrar versões

Aplicar configs

Verificar mudanças

Gerenciamento de Desempenho

Principais Métricas de Desempenho

- **Latência:** Tempo que um pacote leva para viajar de um ponto a outro.
- **Jitter:** Variação no tempo de atraso dos pacotes.
- **Throughput:** Taxa de transferência de dados.
- **Perda de Pacotes:** Quantidade de pacotes de dados perdidos durante a transmissão.
- **Disponibilidade (Uptime):** Percentual de tempo que a rede está operacional.

Indicadores Importantes (KPIs)

- Latência
- Jitter
- Perda de Pacotes
- Throughput
- Disponibilidade (% uptime)
- MTTR (Mean Time to Repair) - Tempo Médio de Reparo
- MTBF (Mean Time Between Failures) - Tempo Médio Entre Falhas

Lista

1. Explique o modelo FCAPS e descreva a importância de cada uma das cinco áreas.
2. Uma empresa apresenta alta latência e perda de pacotes. Qual área do FCAPS está diretamente relacionada a esse problema? Explique.
3. Uma empresa sofreu um ataque de acesso não autorizado à rede. Qual função do FCAPS falhou? Quais medidas deveriam ter sido adotadas?

Lista

4. O modelo FCAPS é utilizado para:

- a) Controle de roteamento
- b) Estrutura de gerenciamento de redes
- c) Balanceamento de carga
- d) Virtualização

Lista

5. O SNMP utiliza qual porta padrão?

- a) 21
- b) 22
- c) 161
- d) 443

Lista

6. **MTTR significa:**

- a) Tempo médio entre falhas
- b) Tempo médio para reparo
- c) Tempo máximo de resposta
- d) Tempo total de rede

Laboratório Prático

Monitoramento básico utilizando SNMP e ferramenta de monitoramento.

Ambiente Necessário

- 1 Máquina Servidor (Linux)
- 1 Máquina Cliente
- Software de monitoramento (Zabbix ou Nagios)

Laboratório Prático

Atividade 1 – Configuração de SNMP

1. Instalar serviço SNMP no servidor.
2. Configurar comunidade (ex: public).
3. Ativar serviço.
4. Testar comunicação via comando:

```
snmpwalk -v2c -c public IP_DO_SERVIDOR
```

Laboratório Prático

Atividade 2 – Monitoramento com Zabbix

Instalar Zabbix Server

Adicionar host monitorado

Configurar template SNMP

Visualizar:

- Uso de CPU
- Uso de memória
- Interface de rede

Laboratório Prático

Atividade 3 – Análise de Desempenho

Simular:

- Aumento de tráfego (ex: download de uma iso Ubuntu para gerar tráfego)
- Queda de interface
- Alteração de configuração

Observar:

- Alertas gerados
- Logs
- Gráficos

Laboratório Prático

Entrega do Laboratório

Relatório técnico contendo:

- Problemas detectados
- Métricas analisadas
- Prints das telas
- Conclusão