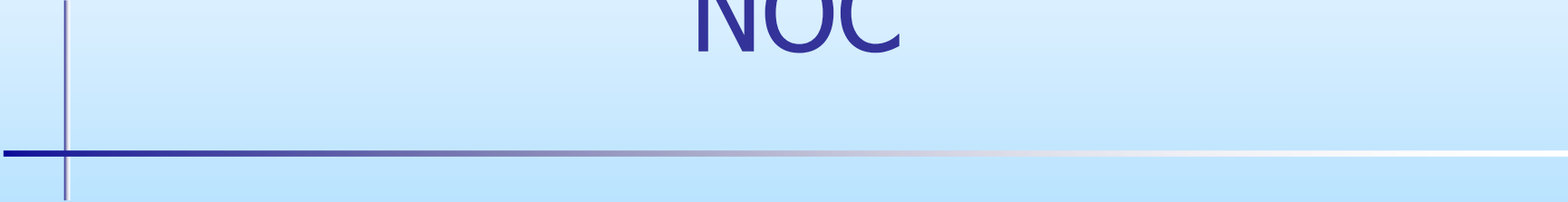


Gerência de Redes NOC



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

Objetivos

- Apresentar os conceitos fundamentais, assim como os elementos relacionados a um dos principais componentes do monitoramento e operações de redes de médio e grande porte, o NOC - Network Operation Center.

Súmula

- Definição e Funções
- Monitoria e Coleta de Dados
- Apresentação das Informações
- Alcance e Controle
- Resolução de Problemas
- Testes
- Rotas Dinâmicas e Alternativas
- Distribuição da Informação
- Sistemas Inteligentes
- Desafios

Monitoramento e Operação

- Monitoramento

- Acompanhamento dos eventos de uma rede, a fim de diagnosticar problemas e determinar quando e quais procedimentos de contingência devem ser aplicados, bem como obter estatísticas para administração e otimizações de desempenho.

- Operação

- Gerenciamento integrado de redes, usando sistemas de informação e recursos que forneçam um cenário comum de operação.

NOC – Visão Geral

- Centro de operações da rede.
- Responsável pelo gerenciamento e controle da rede.
- Deve solucionar os problemas que possam acontecer nas áreas de gerenciamento.
- NOCTools.
 - <http://www.ietf.org/rfc/rfc1470.txt>

NOC – Visão Geral

- Deve instituir normas para utilização da rede
 - Plano de ação / contingência em caso de problema.
 - O que fazer?
 - Avaliar / definir políticas de gerenciamento.
 - Checklist.
 - Plano de contingência.
 - Deve estar coletando o máximo possível de informações da rede.
 - Onde armazenar e como recuperar?
 - Banco de Dados.
 - Sistemas Especialista.

NOC – Visão Geral

- Com base nas informações coletadas da rede os gerentes que trabalham no NOC devem:
 - Produzir um baseline.
 - Manter o monitoramento para as cinco áreas funcionais.
 - Detectar intrusão (segurança).
 - Sanar problemas de forma:
 - Pró-ativa sempre que possível.
 - Reativa quando necessário.

Definição e Funções

- Local a partir do qual é exercido o controle de redes de dados ou telecomunicações.
- O suporte (help desk ou service desk) de um NOC geralmente oferece:
 - Suporte e foco em coordenação das comunicações e controle entre provedores de serviços de rede e usuários.

Definição e Funções

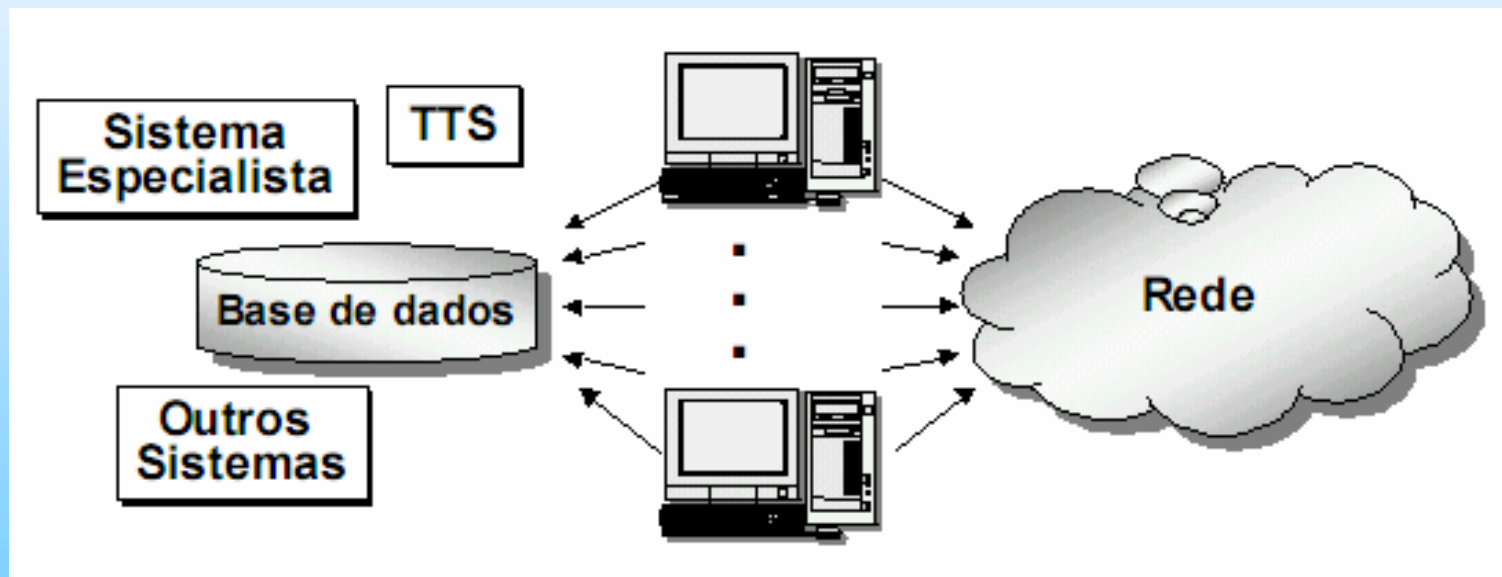
- Conjunto de processos e ferramentas de gerenciamento para manutenção de redes
- Permite reconhecimento rápido de:
 - Problemas da rede;
 - Quedas de desempenho.
- As informações podem ser extraídas da rede continuamente ou sob demanda.
- Dados são armazenados em bases de informações para confrontação com os resultados esperados.

Definição e Funções

- O NOC deve combater problemas
 - Falhas e faltas em dispositivos;
 - Alterações, propositais ou não, assim como falhas ocasionais na estrutura de cabeamento;
 - Falhas no acesso a dados em dispositivos remotos;
 - Acesso indevido a dados.
- O NOC deve usar Sistemas de Registro de Problemas (Trouble Ticket Systems)
 - Os TTSs formar uma base de dados de problemas;
 - Podem ser usados como fonte de dados em sistemas inteligentes.

Definição e Funções

- Visão Funcional do NOC



Definição e Funções

- Resumo dos serviços prestados pelos NOCs.
 - Elaboração de procedimentos operacionais e documentação;
 - Resolução de problemas;
 - Gerenciamento e implementação de mudanças;
 - Implementação e monitoramento da segurança;
 - Monitoramento, avaliação e melhoria do desempenho;
 - Coordenação de atividades operacionais;
 - Geração de relatórios de falhas e desempenho.

Monitoria e Coleta de Dados

- Para *qualidade de serviço* específica, a obtenção do perfil da rede se dá através de:
 - Tempo de resposta;
 - Disponibilidade;
 - Taxa de erros.
- Formatos para obtenção de dados:
 - Coleta Contínua
 - Para gerenciamento pró-ativo e reativo;
 - Falhas podem ser detectadas antes que ocasionem problemas;
 - Gera grande carga de dados para armazenar e auditar.
 - Coleta Sob Demanda
 - Usada apenas em situações específicas;
 - Útil no monitoramento de configurações.

Monitoria e Coleta de Dados

- Fontes de informação usadas em ambientes de comunicação.
 - Características padrão dos softwares;
 - Monitores de redes e aplicações;
 - Ferramentas específicas executadas sob o software;
 - Logs de problemas e alertas de interfaces.

Apresentação das Informações

- Tem como objetivo não sobrecarregar o administrador da rede com informações.
- Recursos usados para divulgar informações.
 - Mídias não convencionais como celulares, PDAs;
 - Mapas e diagramas;
 - Organizar em grupos como: aplicações, transações, testes e produção;
 - Classificar por componentes como: Processadores de comunicação, backbones e periféricos;
 - Apresentar visão sobre eventos mais recentes.

Alcance e Controle

- O NOC deve ter administração centralizada para recursos descentralizados.
 - Acesso remoto a recursos humanos, aplicações e ferramentas de monitoramento;
 - Prontidão e habilidade para cooperar remotamente;
 - Suporte remoto por meios redundantes e não convencionais;
 - Determinação e diagnóstico remotos de problemas;
 - Minimização do tempo entre a ocorrência do problema e a solução;
 - Uso de dispositivos e canais secundários de controle.

Alcance e Controle

- Gerência centralizada.
 - Vantagens.
 - Estabelecimento de padrões.
 - Redução de pessoal especializado.
 - Documentação única.
 - Visão única do todo.
 - Desvantagens.
 - Distâncias.

Resolução de Problemas

- Os problemas são resolvidos em 4 etapas
 - Detecção - Ocorrência;
 - Determinação - Busca de causas e efeitos;
 - Diagnóstico – Relação causas, efeitos e solução;
 - Resolução - Execução e documentação.
- Apresentados em 3 níveis de complexidade
 - 85% são problemas simples com diagnóstico desprezível;
 - 10% são solucionados pelo operador e tem diagnóstico considerável;
 - 5% são solucionados por especialistas e demandam muitos recursos.

Testes

- São necessários para verificar o nível de operacionalidade da rede.
- Podem ser executados durante a operação normal mas não podem interferir na produção.
 - Definem-se critérios para um teste com o mínimo de *overhead* e para a seleção dos componentes;
 - Especificam-se tarefas aos *sites* locais e remotos.
- Tipos de testes
 - Intrusivos - *Link* e/ou equipamento interrompidos;
 - Não-Intrusivos - Sem interrupção dos serviços.

Rotas Dinâmicas e Alternativas

- Mesmo com problemas a rede deve continuar funcionando.
- Problemas comuns.
 - Perda do Link;
 - Congestionamento.
- Solução - Rota Alternativa.
 - Determinar a nova rota através de critérios de desempenho pré-definidos;
 - Conseqüente balanceamento de carga em roteadores inteligentes.

Distribuição da Informação

- Usar meios da arquitetura para informar a ocorrência de problemas.
- Usar *link* secundário quando o principal estiver com problemas.
- Usar *broadcast* automático de mensagens.
- Usar serviço alternativo como:
 - Telefone, *e-mail*, *SMS* e etc.

Sistemas Inteligentes

- O uso de sistemas inteligente reflete em:
 - Velocidade na determinação do problema;
 - Decisão baseada em base de conhecimento e quantidade de dados;
 - Diminuição no pessoal de suporte;
 - Evita interpretação humana de regras operacionais;
 - Segurança, estabilidade, flexibilidade e outras.

Sistemas Trouble Ticket

- Registrar todas as ocorrências.
- Melhora e ajuda na solução de problemas.
 - Muitos dos problemas que acontecem no dia a dia já aconteceram anteriormente.
 - Grandes redes este sistema é fundamental.
 - Ajuda a registrar chamadas.
 - Gerar relatórios analíticos sobre problemas e desempenho das equipes.
- Bonito na teoria mas na prática o usuário prefere ligar e perguntar diretamente a um técnico.

Sistemas Trouble Ticket

- Internetwork Troubleshooting Guide
 - Definido pela CISCO.
 - http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm
- Centro de operações da RNP
 - Gerência do *backbone*.
 - <http://www.rnp.br/operacao/>

Desafios

- Desafios para os NOCs
 - Maior foco em demandas de segurança;
 - Maior quantidade e complexidade de elementos a serem monitorados;
 - Serviços mais complexos como: VPN, VoIP, Vídeo e etc;
 - Maior quantidade de serviços complexos dependentes do desempenho da rede.

Atividade Prática 1

- Buscar na Internet uma ferramenta capaz de capturar informações de dispositivos de uma rede.
- Instalar, usar e classificar a ferramenta de acordo com os seguintes quesitos:
 - Permite recuperação continuamente, sob demanda ou ambos?
 - É permitido o armazenamento em BD das informações capturadas?
 - Existem opções pré-programadas para resolver os problemas detectados?
 - Existe um sistema de registro do problema associados?

Atividade Prática 2

- Buscar na Internet uma ferramenta capaz de capturar informações de dispositivos de uma rede.
- Instalar, usar e classificar a ferramenta de acordo com os seguintes quesitos:
 - As informações são apresentadas de forma adequada?
 - Permite gerenciamento centralizado, remoto ou ambos?
 - A ferramenta introduz overhead que pode prejudicar o funcionamento da rede?
 - Os testes são intrusivos ou não?
 - A detecção e correção de erros descreve o processo de solução?