

Formação para Sistemas Autônomos

Gerenciamento de Redes

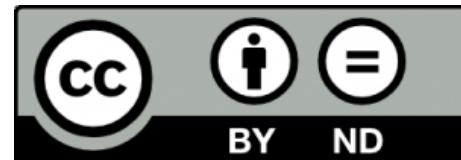
Licença de uso do material

Esta apresentação está disponível sob a licença

Creative Commons

Atribuição – Não a Obras Derivadas (by-nd)

<http://creativecommons.org/licenses/by-nd/3.0/br/legalcode>



Você pode:

- **Compartilhar** — copiar, distribuir e transmitir a obra.
- **Fazer uso comercial da obra.**
- Sob as seguintes condições:

Atribuição — Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do Curso de Formação para Sistemas Autônomos do CEPTRO.br/NIC.br, e que os originais podem ser obtidos em <http://ceptro.br>. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.

Vedada a criação de obras derivadas — Você não pode modificar essa apresentação, nem criar apresentações ou outras obras baseadas nela..

Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail: info@nic.br.

Agenda

- Motivação
- Conceitos Importantes
 - Modelos de Referência
 - FCAPS
 - OAM&P
- Protocolos Importantes
 - ICMP
 - Syslog
 - SNMP
- Tipos de Ferramentas
- Ferramentas Open Source

Motivação

- Gerenciar para que?
 - Melhorar a organização
 - Detectar problemas desconhecidos na rede
 - Aumentar a disponibilidade do sistema
 - Aumentar a performance do sistema
 - Diminuir custos
 - Conhecer a sua rede

O que é gerência de redes?

- Garantir o funcionamento correto da rede
 - Qualidade
 - Máximo de desempenho
 - Resolução de problemas
- Redução de custos
- Tomada de decisão
 - Mudança de equipamentos
 - Novas ferramentas

O que é gerência de redes?

- Monitorar a disponibilidade e tempo de resposta
- Melhorar a automatização
- Segurança
- Controle de tráfego
- Detecção e correção de falhas
- Prever possíveis falhas
- Log de informação para análise

Modelos de Referência

- Permitem organizar diferentes funções de um sistema ou tecnologia
 - Modelos conceituais de Gerenciamento de Redes:
 - FCAPS, ISO de gerenciamento
 - OAM&P, bastante utilizados por ISP

FCAPS

- ISO de gerenciamento, dividindo-o em 5 áreas:
 - Falha (Fault)
 - Falhas interferem no funcionamento ideal da rede, devem ser realizados testes, garantindo o funcionamento da rede, usando sistemas de alarmes/alertas, mantendo logs e buscando a causa e resolução dos problemas encontrados, minimizando os efeitos de uma possível interrupção.
 - Configuração (Configuration)
 - Configurações e ajustes necessários para o funcionamento correto da rede (fornecimento de recursos, serviços, inventário, backup e restauração de configurações, etc.). É um dos pontos mais importantes para a manutenção da rede.

FCAPS

- Contabilidade (Accounting)
 - Contabilização monetária (custos pelo uso de serviços e recursos da rede, contabilizando seu lucro), aplicável também à rede interna verificando custo/benefício de serviços, controle de gastos, determinando, por exemplo, a adoção ou não de serviços terceirizados de TI, neste contexto, o Accounting pode ser substituído por Administration.
- Performance (Performance)
 - Indica a qualidade do serviço. A performance em uma rede é determinada por várias métricas, incluindo:
 - Vazão (Throughput) Uso por unidade de tempo.
 - Delay
 - Qualidade - Podendo ser tanto medido (porcentagem de pacotes perdidos na rede) quanto subjetivo (a satisfação do usuário).

FCAPS

- Segurança (Security)
 - Visam garantir a integridade da informação fornecida, incluindo controle de acesso, uso de privilégios, são considerados o controle de ameaças a rede, como ataques de hackers, worms e vírus.

OAM&P

- As categorias nesse modelo são:
 - Operação (Operations)
 - Coordenar as atividades das demais categorias e realizar o monitoramento da rede
 - Administração (Administration)
 - Funções de suporte como alocação de endereços, acompanhamento da rede, inventário de equipamentos, cobrança do uso de serviços, etc.
 - Manutenção (Maintenance)
 - Funções que garantem o funcionamento da rede e seus serviços (diagnóstico, reparos e solução de problemas).
 - Provisionamento (Provisioning)
 - Fornecer as configurações e parâmetros para o funcionamento correto da rede. Pode incluir atualização de configuração de equipamentos, instalação, ativar ou desativar serviços do cliente final, etc.

Etapas do Monitoramento

- Definição de Políticas
 - Quais são as condições normais da rede
 - Métricas e comportamentos esperados
- Monitoramento
 - Coleta de dados da rede
- Análise do dados
 - Determina se a rede está funcionando corretamente ou não.
 - Em caso de problemas, determinar a causa e solução
- Controle
 - Aplicar as medidas determinadas pela análise

Etapas do Monitoramento

- Por exemplo no modelo FCAPS
- Falha (Fault)
 - Rede funcional
 - Ping de dispositivos e query SNMP para verificar o status
 - Envia dados de falhas via e-mail ou SMS
 - Mostrar os problemas da rede em um mapa de topologia
- Configuração (Configuration)
 - Controle e monitoramento de configurações
 - Verifica periodicamente a mudança de configurações via ssh
 - Salva a configuração e realiza a diferença de diff de versões
 - Avisa o administrador por e-mail das novas mudanças.

Confiabilidade vs. Disponibilidade

- Confiabilidade é o mesmo que Disponibilidade?

Confiabilidade vs. Disponibilidade

- Confiabilidade é o mesmo que Disponibilidade?
- **Confiabilidade:** Probabilidade de falha em um determinado intervalo de tempo
- **Disponibilidade:** Probabilidade do sistema estar disponível em um determinado instante de tempo

Alertas vs. Logs

- Alertas indicam quando algo fora do normal está acontecendo
- Logs ajudam a identificar a causa desse acontecimento

Ferramentas Ativas vs Passivas

- Ativas: causam interferência no sistema para poder obter informações. Ex: snmpwalk, ping, traceroute
- Passivas: coletam dados já existentes. Ex: snmp, NFSen, wireshark

Baseline

- Baseline – como sua rede é hoje?
- Fundamental para qualquer gerenciamento de redes
 - Primeiro passo para um bom gerenciamento
 - Como saber o que é estranho sem saber o que é normal?

Protocolos de Monitoramento

- **ICMP** - Internet Control Message Protocol
 - Muito utilizado para debug da rede, através de pings e traceroutes
 - **ping**
 - Utiliza o ICMP para verificar a acessibilidade de equipamentos

Protocolos de Monitoramento

- **Syslog**

- Padrão criado pela IETF
- Forma padronizada de registrar mensagens do sistema
- É boa prática configurá-lo em um repositório central para facilitar o gerenciamento

Procolos de Monitoramento

- Prioridade da mensagens é definida por duas variáveis:
 - Facility: indica o tipo de origem que gerou a mensagem
 - Severity: indica a gravidade da mensagem

Protocolos de Monitoramento

- **SNMP - Simple Network Management Protocol**
 - Protocolo padrão para gerenciar dispositivos em redes IP

Consultas

- Carga na CPU
- Uptime
- Temperatura

Nos hosts

- Espaço em disco
- Software instalados
- Processos

Protocolos de Monitoramento

- **NetFlow**

- Desenvolvido pela Cisco
- Define fluxos
 - Pacotes como parte de um fluxo
 - Com características comuns

- Utilizado para

- Análise de tráfego
- Largura de banda

Protocolos de Monitoramento

- **IPFIX**
 - IP Flow Information Export
 - Definido pelas rfc5101 e rfc5102 e rfc5103
 - Surgiu da necessidade de existir um padrão universal não proprietário para coleta de flows
 - Baseado no Netflow versão 9

Tipos de Ferramentas

- **Coletores**

- Utilizados para colher e guardar diferentes tipos de informação da rede.
- Ex:
 - nfdump (NetFlow)
 - tcpdump (TCP/IP)

Tipos de Ferramentas

- **Sistemas de Detecção de Invasão**

- Ajudam a detectar padrões suspeitos que possam identificar a ocorrência de um ataque.
- Podem analisar o tráfego da rede, verificar alarmes, logs, padrões de load, etc. E tomar ações para mitigar os efeitos.
- Ex:
 - Snort

Tipos de Ferramentas

- **Sistema de Análise de Performance**
 - Permite analisar dados de tráfego e performance.
 - Dados em gráficos para permitir o entendimento dos usuários.
 - Permite planejamento de novos recursos e identificação de gargalos na rede.
 - Ex:
 - Cacti
 - Zabbix

Tipos de Ferramentas

- **Sistema de Gerenciamento de Alarmes**

- Coletam e monitoram alarmes da rede.
- Melhor visualização dos alarmes para o usuário.
- Diagnóstico inicial
- Ex:
 - Nagios
 - Icinga
 - Zabbix

Tipos de Ferramentas

- **Sistema de Tickets**

- Rastrear como os problemas estão sendo resolvidos.
- Cadastro dos problemas
- Alocação de recursos
- Estatísticas de resolução
- Ex:
 - Redmine
 - Trac

Ferramentas de Gerenciamento

- **Ferramentas de acesso**

- SSH e telnet
- Acesso à máquinas remotas, permite a troca de informação entre a ferramenta gerenciamento e os dispositivos.
- Ex:
 - OpenSSH
 - PuTTY

Ferramentas de Gerenciamento

- **Ferramentas de Depuração**

- **Ping**

- Verifica a conectividade entre as máquinas

- **Traceroute**

- Verifica as rotas feitas por um pacote

- **ps/top**

- Monitora os processos da máquina

- **nmap**

- verifica quais portas estão habilitadas em certo host

Ferramentas de Gerenciamento

– Wireshark

- <http://www.wireshark.org>
- Analisa protocolos de rede
- Captura em tempo real

Ferramentas de Gerenciamento

- **Ferramentas de Log**
 - **Syslog-ng, rsyslog**
 - Implementam o protocolo syslog
 - **Log Analyzer**
 - Permite visualizar o conteúdo dos logs de maneira inteligível
 - **Tenshi, swatch**
 - Permitem a criação de filtros para os logs

Ferramentas de Gerenciamento

- **Gerenciamento de Configurações**
 - **Manual**
 - CVS
 - SVN
 - Mercurial
 - **Automático**
 - Roteadores
 - RANCID

Ferramentas de Gerenciamento

- **RANCID**

- <http://www.shrubbery.net/rancid/>
- Open Source
- Armazena as configurações dos dispositivos de rede
 - Versionamento de configuração: CVS ou SVN
 - Roteadores Cisco, Juniper, switches Catalyst, Foundry, etc
- Criação de módulos para dispositivos não suportados
- Periódico (entrada no crontab)
- Envio de e-mails com as mudanças
- Automação (comandos externos ou também expected scripts)

Ferramentas de Gerenciamento

- Conecta ao roteador (SSH ou Telnet)
- Executa e coleta dados de comandos
- Salva os dados em CVS/SVN
- Cria um diff entre a configuração anterior e a atual
- Envia um e-mail com o diff das configurações aos interessados.

Ferramentas de Gerenciamento

- **Automáticas**

- Agregam diversas funcionalidades
 - Icinga
 - Nagios
 - Zabbix

Ferramentas de Gerenciamento

- **Icinga**

- <https://www.icinga.org/>
- Versões
 - Icinga 1.x (Nagios fork)
 - Classic Web
- Suporte
 - MySQL, PostgreSQL, Oracle
 - Monitoramento IPv6
 - Exporta dados
 - Plugins do Nagios

Ferramentas de Gerenciamento

Current Network Status

Last Updated: Mon Jun 3 09:52:28 BRT 2013 - Update in 86 seconds [pause]

Icinga 1.9.0 - Logged in as icingaadmin

Commands for checked services

Select command

Service Status Details For All Hosts

Display Filters:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	06-03-2013 09:49:16	5d 22h 59m 42s	1/4	OK - load average: 0.81, 0.68, 0.59
	Current Users	OK	06-03-2013 09:49:51	13d 13h 14m 54s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	06-03-2013 09:50:26	13d 13h 14m 20s	1/4	HTTP OK: HTTP/1.1 200 OK - 454 bytes in 0.000 second response time
	Icinga Startup Delay	OK	06-03-2013 09:51:02	13d 13h 13m 20s	1/4	OK: Icinga started with 2 seconds delay
	PING	OK	06-03-2013 09:51:37	13d 13h 13m 14s	1/4	PING Monitoring Admin Help
	SSH	OK	06-03-2013 09:47:48	13d 13h 17m 7s	1/4	SSH C (proto) 1 / 0 UP 0 / 0 DOWN 0 / 0 UNREACHABLE 0 PENDING 0 / 1 IN TOTAL 1 OK 8 / 0 OK 0 / 0 WARNING 0 / 0 CRITICAL 0 / 0 UNKNOWN 0 PENDING 0 / 9 IN TOTAL 0 DOWN
	Swap Usage	OK	06-03-2013 09:48:23	13d 13h 16m 34s	1/4	SWAP (MB)
Total Processes	OK	06-03-2013 09:48:58	13d 13h 15m 51s	1/4	PROC RSZD	
serverB	Current Load	OK	06-03-2013 09:49:33	0d 1h 42m 55s	1/4	OK - k
	Current Users	OK	06-03-2013 09:50:09	10d 0h 41m 32s	1/4	USER
	Icinga Startup Delay	OK	06-03-2013 09:51:19	10d 0h 40m 21s	1/4	OK: Ic
	Total Processes	OK	06-03-2013 09:48:41	10d 0h 38m 0s	1/4	PROC RSZD

Page 1 of 1 Results: 50

Displaying Result 1 - 12 of 12 Matching Services

Commands for checked services

Select command

ServiceHistory

Welcome

Categories Settings View filter

Host	Service	Status	Timestamp	Output	Attempt
localhost	Current Load	OK	2013-05-17 14:43:33	OK - load average: 2.32, 2.47, 2.90	4 / 4
localhost	Current Load	WARNING	2013-05-17 14:23:33	WARNING - load average: 2.01, 3.66, 3.95	4 / 4
localhost	Current Load	CRITICAL	2013-05-17 14:13:34	CRITICAL - load average: 5.29, 6.54, 3.90	4 / 4
localhost	Current Load	CRITICAL	2013-05-17 14:12:33	CRITICAL - load average: 12.70, 7.76, 4.09	3 / 4
localhost	Current Load	WARNING	2013-05-17 14:11:33	WARNING - load average: 7.37, 5.16, 3.02	2 / 4
localhost	Current Load	CRITICAL	2013-05-17 14:10:33	CRITICAL - load average: 13.91, 5.48, 2.98	1 / 4
localhost	Current Load	OK	2013-05-17 14:00:33	OK - load average: 2.73, 3.22, 1.97	3 / 4
localhost	Current Load	WARNING	2013-05-17 13:59:33	WARNING - load average: 5.49, 3.67, 2.02	2 / 4
localhost	Current Load	WARNING	2013-05-17 13:58:33	WARNING - load average: 6.56, 3.20, 1.76	1 / 4
localhost	Current Load	OK	2013-05-17 11:13:33	OK - load average: 0.41, 1.62, 2.78	4 / 4
localhost	Current Load	WARNING	2013-05-17 11:07:33	WARNING - load average: 3.79, 4.77, 3.97	3 / 4
localhost	Current Load	WARNING	2013-05-17 11:06:33	WARNING - load average: 2.36, 4.66, 3.88	2 / 4
localhost	Current Load	WARNING	2013-05-17 11:05:33	WARNING - load average: 2.85, 5.22, 4.00	1 / 4

Ferramentas de Gerenciamento

- **Cacti**

- <http://www.cacti.net/>
- Monitorar, guardar e apresentar
 - Estatísticas do sistema/servidor
 - Rede
- Configurável via interface Web
- Dados são armazenados em bancos de dados round-robin chamado RRD (Round Robin Database)
- Configurações são armazenadas em banco de dados mySQL
- Pode ser instalado tanto em sua versão php como em c

Ferramentas de Gerenciamento

- A principal função do Cacti é armazenar e mostrar de forma simples as informações disponibilizadas pelos equipamentos, em geral através do protocolo SNMP
- O fato de utilizar RRD facilita muito na geração de gráficos simples e concisos

Ferramentas de Gerenciamento

console graphs

Console -> Devices -> (Edit)

Logged in as admin (Logout)

Save Successful.

n4 (192.0.0.12)

SNMP Information
System:Linux n4 3.8.0-19-generic #30-Ubuntu SMP Wed May 1 16:36:13 UTC 2013
Uptime: 12610 (0 days, 0 hours, 2 minutes)
Hostname: n4
Location: Nic.br
Contact: teste@teste

Ping Results
ICMP Ping Success (0.043 ms)

Devices [edit: n4]

General Host Options

Description Give this host a meaningful description.

Hostname Fully qualified hostname or IP address for this device.

Host Template Choose the Host Template to use to define the default Graph Templates and Data Queries associated with this Host.

Number of Collection Threads The number of concurrent threads to use for polling this device. This applies to the Spine poller only.

Disable Host Check this box to disable all checks for this host.

Availability/Reachability Options

Downed Device Detection The method Cacti will use to determine if a host is available for polling.

PING Method The type of ping packet to sent.

Ping Timeout Value The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings.

Ping Retry Count After an initial failure, the number of ping retries Cacti will attempt before failing.

SNMP Options

SNMP Version Choose the SNMP version for this device.

SNMP Community SNMP read community for this device.

SNMP Port Enter the UDP port number to use for SNMP (default is 161).

SNMP Timeout The maximum number of milliseconds Cacti will wait for an SNMP response (does not work with php-snmp support).

Maximum OID's Per Get Request Specified the number of OID's that can be obtained in a single SNMP Get request.

Additional Options



Ferramentas de Gerenciamento

- **Gerenciamento de Endereços**

- **IPplan**

- <http://iptrack.sourceforge.net/>
 - Última atualização em 2010
 - Suporte a IPv6 somente na versão beta

- **PhplIPAM**

- phpipam.net
 - Suporte IPv6
 - Interface amigável

Ferramentas de Gerenciamento

- **NetDot**

- Descoberta de dispositivos via SNMP
- Gerenciamento de endereços IPv4 e IPv6
- Geração de arquivos de configuração para outras ferramentas
 - Nagios
 - RANCID
 - Cacti

Ferramentas de Gerenciamento

- **GestióIP**

- <http://www.gestioip.net/>
- Descoberta da rede via SNMP
- Suporte à IPv6
- Calcula subredes

Ferramentas de Gerenciamento

The image displays three screenshots of network management tools:

- phpipam IP address management:** A web-based interface for managing subnets. It shows fields for Subnet (CIDR), Description, VLAN, Master Subnet, VRF, IP Requests, and Show as name. A search bar at the top right allows users to search for specific subnets.
- GestióIP:** A tool for creating networks. It includes fields for network (IPv4 or IPv6), BM (Broadcast/Mask), description, comment, site, and category. It also features options for Root network, include networks within automatic update, and create/calculate buttons.
- IPPlan - IP Address Management and Tracking:** A web-based application for managing users and groups. It shows a user manager interface with sections for Current Users/Groups, Create group, and Edit Users/Groups. It includes a search bar and a table for subnet management showing details like Address, Status, Description, and Utilization.

Ferramentas de Gerenciamento

- **Ntop – Network top**
 - Mostra o uso a rede de forma similar ao top
 - Acessível tanto via terminal como via web
 - No modo terminal o ntop fornece o estado da rede (forma similar a como o top mostra os processos)
 - No modo web é possível configurar o ntop para monitorar constantemente a rede e gerar relatórios

Ferramentas de Gerenciamento

- **Iperf**
 - Ferramenta para medir o throughput/ performance da rede
 - Cria streams que podem ser em TCP ou UDP
 - Analisa largura de banda, latência, jitter e perda de pacotes

Conclusão

- Para que gerenciar?
 - Para garantir uma rede funcional e clientes satisfeitos
- Como gerenciar?
 - Ferramentas de Gerenciamento
 - Logs (rsyslog, log analyzer, tenshi)
 - Alertas (Icinga, Nagios, Zabbix)
 - Performance (Cacti)
 - Tickets (trac, redmine)
 - Endereços (IPPlan, NetDot, GestióIP)
 - Configuração (SVN, Rancid)

Dúvidas?

