ARQUITETURA DE SERVIDORES **DE REDE**

Esp. Geiza Caruline Costa

INICIAR

introdução

Introdução

Nesta unidade aprenderemos sobre como administrar devidamente um sistema, realizar agrupamento de NIC, executar troubleshooting e conceitos básicos de backup.

No tópico 1 falaremos sobre como deve ocorrer a administração de um sistema, descrevendo sucintamente seu funcionamento e como realizar a análise de logs.

Descreveremos sobre a lógica da estrutura de agrupamento da placa de rede NIC aplicando contingência, verificando largura de banda e averiguando tolerância a falhas, no tópico 2.

O tópico 3 tratará sobre troubleshooting, analisando devidamente os logs e atuando com ferramentas de manutenção, com o intuito de atuar em caso de falhas nos serviços de rede ou do sistema operacional de um servidor.

Por fim, no tópico 4, abordaremos o conceito e configuração de backups, analisando os princípios básicos de cópia de segurança para um servidor de rede e destacando as principais ferramentas de uso.

Administração do Sistema

Dentre as atribuições de um administrador de redes, temos a configuração de uma vasta gama de dispositivos e serviços, como servidores, switches, roteadores, firewall e todos os demais recursos necessários para as operações do negócio.

Quando a configuração de um recurso de rede é feita corretamente, como no caso de um roteador, raramente será preciso refazê-la, apenas em casos estritamente necessários, como um redimensionamento da demanda ou tratativa de incidentes.

No entanto, a monitoração da rede é um papel fundamental para a continuidade dos negócios, a qual envolve o acompanhamento dos parâmetros a fim de evitar gargalos e otimizar o desempenho do sistema. Segundo Barrett e King (2010, p. 372), “essa é uma tarefa sem fim, mas alguém precisa realizá-la”, pois o monitoramento deve ser constante e persistente. Observe o seguinte exemplo de solução de problemas baseada em monitoramento:

Às vezes, uma mudança mínima pode afetar o desempenho. Por

> *exemplo, uma empresa de pequeno porte de repente começou a experimentar um desempenho fraco na rede. A gerência contratou vários consultores e diversas mudanças foram feitas nas configurações do servidor, todas em vão. Finalmente, por sua própria conta, a administradora do sistema instalou um software de monitoração para acompanhar o tráfego na rede. Ela descobriu que um tráfego excessivo estava vindo de uma área no canto da sala. Aparentemente, o novo técnico da mesa de apoio decidiu montar sua própria rede pequena. No processo, ele usou várias placas de rede que eram antigas e geravam ruído, causando tráfego excessivo na rede. Depois que a rede própria do técnico foi desativada, o desempenho retornou ao normal para a empresa. Algo tão simples como algumas placas de rede prejudicou o desempenho e gerou custos de consultoria. (BARRETT e KING, 2010, p. 373).*

Barrett e King (2010, p. 374) explicam que o administrador de rede deve conhecer o comportamento típico da rede e de seus recursos, para ser capaz de identificar qual é o comportamento anormal. Algumas ferramentas podem auxiliar nesta tarefa. No caso de sistemas operacionais Windows, podemos citar o Monitor de Desempenho e o Visualizador de Eventos.

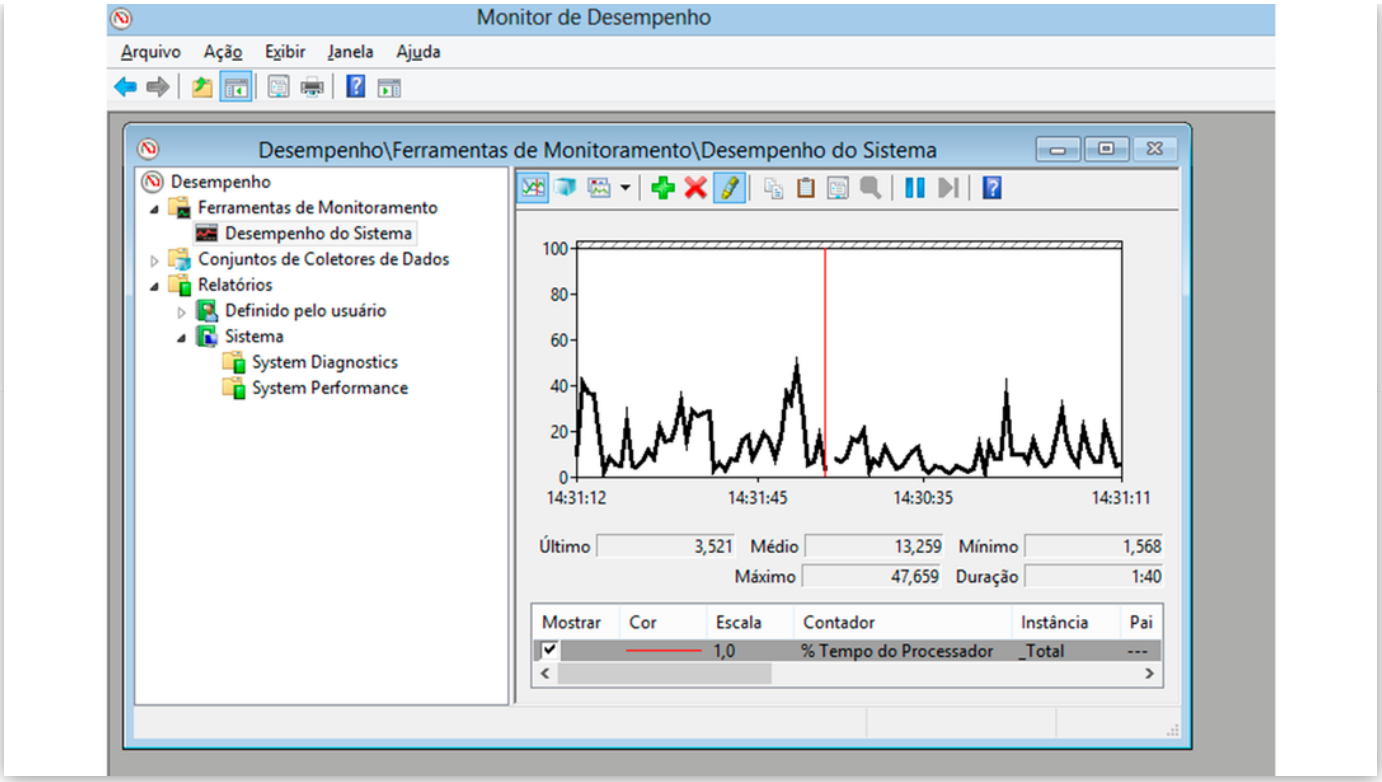


Figura 4.1 - Ferramenta Monitor de Desempenho do Windows
Fonte: Elaborado pela autora.

O Monitor de Desempenho do Windows monitora e registra continuamente os níveis do desempenho de um servidor, de tal forma que pode ser configurado para emitir relatórios e alertas caso níveis pré-determinados sejam atingidos. Um exemplo disso é o envio de um relatório quando níveis críticos de desempenho do processador forem atingidos, cabendo ao administrador da rede tomar medidas contingenciais para evitar a interrupção dos serviços. Observe que na Figura 4.1 o pico de percentual de uso do processador no período foi de aproximadamente 55%. Um alerta crítico de desempenho poderia ser emitido quando fosse detectado 75% ou mais de uso de processador.

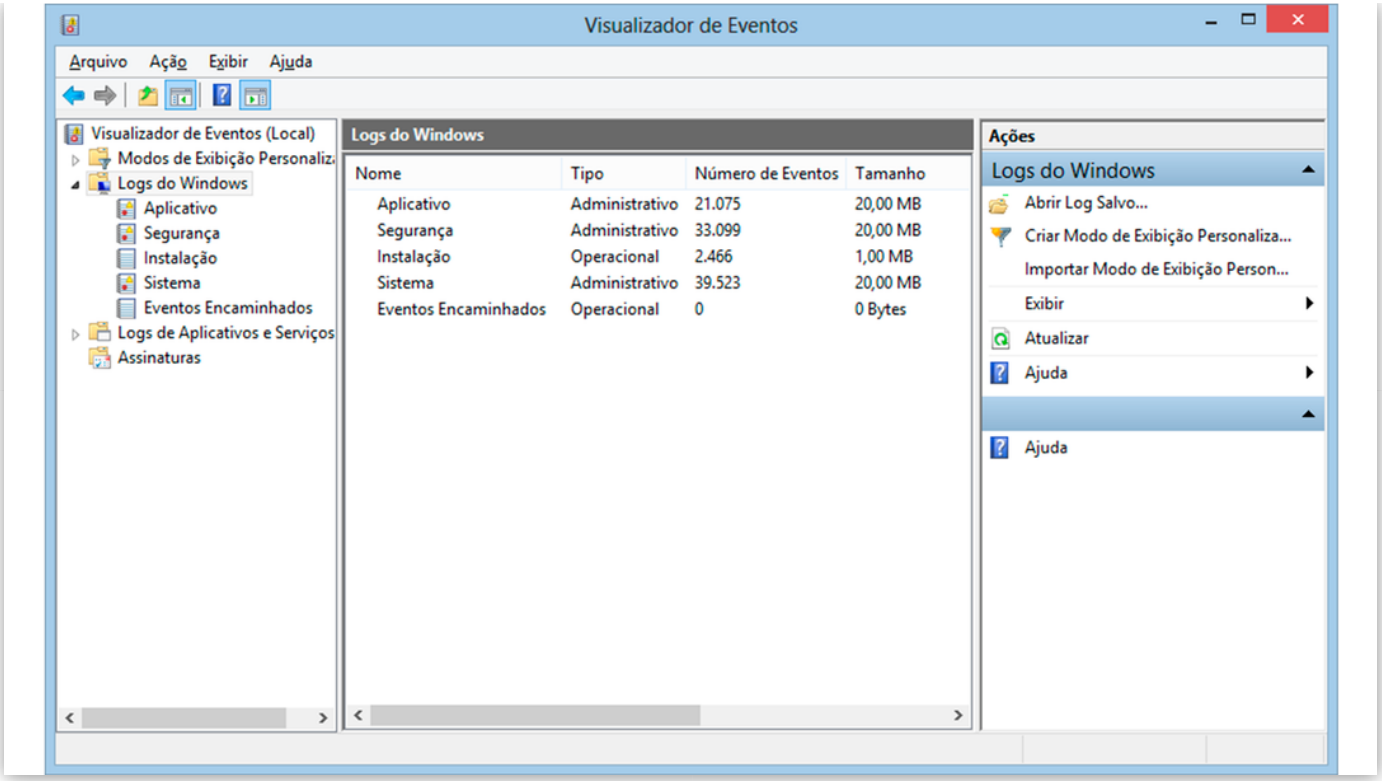


Figura 4.2 - Ferramenta Visualizador de Eventos do Windows.
Fonte: Elaborado pela autora.

O Visualizador de Eventos do sistema operacional Windows monitora as ações executadas em um computador, sejam elas ações iniciadas por um usuário, ações agendadas ou erros e alertas decorrentes de aplicativos ou do próprio sistema operacional.

O número de eventos registrados pode ser gigantesco e difícil de analisar, daí a importância de fazer o rotacionamento de logs. Se o gerenciamento dos arquivos de logs não for feito de maneira correta, inevitavelmente será ocupado um grande espaço em disco que poderia ser utilizado para salvar dados mais úteis para a organização.

> *O rotacionamento de logs permite que, de acordo com a política empregada, um arquivo possa ser segmentado, bem como seus segmentos mais antigos serem compactados (de modo a reduzir o espaço utilizado). (DIBIAZI, 2015).*

No ambiente de servidores de rede Linux também é possível configurar e gerenciar o registro de logs. Para isso é importante identificar os arquivos de logs gerados pelas aplicações, então pode ser utilizada uma ferramenta

chamada logrotate.

apt-get install logrotate

logrotate --version

/etc/logrotate.conf

/etc/logrotate.d

Quadro 4.1 - Procedimentos para a instalação e utilização do logrotate em um computador com sistema operacional Ubuntu Server
Fonte: Adaptado de Kaieski (2012).

No Quadro 4.1 é exibida uma série de comandos utilizados para a instalação, o uso e a configuração do logrotate. Na primeira linha é exibido o comando para instalar a ferramenta. A execução do comando exibido na segunda linha apresenta a versão do logrotate instalada. Antes de tentar instalar o logrotate, convém verificar se há alguma versão já instalada no servidor. A terceira linha apresenta o arquivo de configuração do logrotate (logrotate.conf). Neste arquivo são listados todos os arquivos de logs gerados pelas aplicações e é indicada a forma de rotacionar cada um deles. Na quarta linha temos o diretório logrotate.d, no qual podem ser criados arquivos com configurações específicas para determinados aplicativos. Segundo Kaieski (2012), “muitos aplicativos ao serem instalados, como por exemplo o Apache, geram um arquivo de rotacionamento de logs dentro do diretório /etc/logrotate.d”.

daily

rotate 35

compress

size 5M

mail

Quadro 4.2 - Exemplo de configuração do logrotate
Fonte: Adaptado de Kaieski (2012).

O Quadro 4.2 apresenta um sumário de configurações efetuadas para o rotacionamento de logs no arquivo logrotate.conf. A palavra daily indica que os logs serão rotacionados diariamente, esta opção poderia ser substituída por monthly ou weekly (mensal ou semanal, respectivamente). rotate 35 indica que somente 35 arquivos de log rotacionados serão mantidos. compress indica que os logs serão compactados. size 5M indica o tamanho do arquivo de log a ser rotacionado, neste caso 5 megabytes. A diretiva mail indica que, periodicamente, quando os logs forem rotacionados será enviado um email para o administrador.

saiba mais

Saiba mais

Veja mais detalhes sobre rotacionamento de logs e parâmetros adicionais no artigo de Rodrigo Telles.

Fonte: TELLES, R. Rotacionamento de logs e o desastre iminente. Rodrigo

ACESSAR

Atividade

1) Barrett e King (2010, p. 380) explicam que “quando examinarmos a correção ou a melhoria do desempenho de nossa rede, um dos primeiros fatores a considerar serão os servidores”. Analise as sentenças a seguir observando quais cenários são relevantes para o registro e a verificação dos logs de sistema. Em seguida, assinale a alternativa correta.

BARRETT, D.; KING, T. Redes de Computadores. Rio de Janeiro: LTC, 2010.

i. Quando for feito um bloqueio de tráfego de dados pelo firewall em determinada porta TCP.
ii. Quando sucessivas tentativas de login forem feitas com o mesmo nome de usuário.
iii. Quando um servidor atingir um limite crítico de espaço para armazenamento em disco.

- **a)** Somente o exposto na sentença I é relevante para o registro e a verificação nos logs de sistema.
- **b)** Somente o exposto nas sentenças I e II é relevante para o registro e a verificação nos logs de sistema.
- **c)** Somente o exposto nas sentenças I e III é relevante para o registro e a verificação nos logs de sistema.
- **d)** Somente o exposto nas sentenças II e III é relevante para o registro e a verificação nos logs de sistema.
- **e)** O exposto nas sentenças I, II e III é relevante para o registro e a verificação nos logs de sistema.

Agrupamento NIC

A placa de rede, também conhecida como NIC (Network Interface Card), é a interface de comunicação entre um computador e a rede de computadores. Através dessa interface o fluxo de bytes é enviado e recebido no dispositivo.

Algumas versões de sistemas operacionais, como Windows Server 2012 ou mais recentes, possuem uma funcionalidade que permite o agrupamento de NICs.

Segundo Thompson (2014, p. 194), o uso de vários adaptadores de rede para balancear o tráfego no servidor, ou mesmo fazer com que dois adaptadores funcionem como se fossem uma única interface com maior taxa de transferência, são funcionalidades que podem ser configuradas a partir do agrupamento NIC.

A configuração do agrupamento de NICs também confere ao servidor um nível de tolerância a falhas (failover), pois permite que, no caso de uma interface de rede apresentar problemas, a outra interface continue operando de forma a manter a disponibilidade dos sistemas e o atendimento às demandas dos usuários.

Para ambientes de servidores com o sistema operacional Windows Server 2012 ou superior, a configuração do agrupamento de NIC requer o uso da ferramenta NIC Teaming. Na prática, será criado um time com um nome, em que deverão ser indicadas as interfaces de rede (ou adaptadores) que serão membros da equipe.

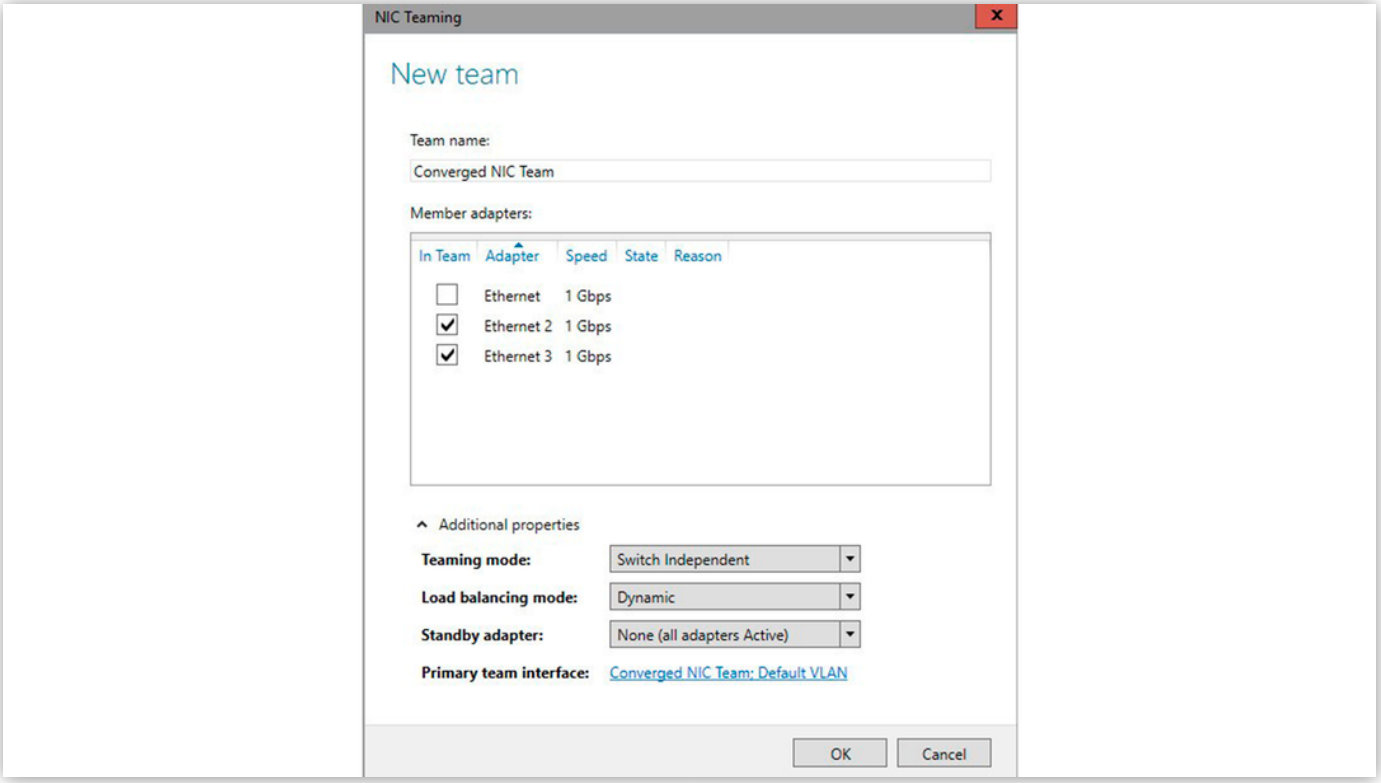


Figura 4.3 - Tela para criação do time NIC
Fonte: Windows IT Pro Center (2019).

A Figura 4.3 apresenta a tela para criação de um time de interfaces de rede considerando o cenário de um servidor que tenha 3 placas de rede: Ethernet, Ethernet 2 e Ethernet 3, cada uma com taxa de transmissão máxima de 1 Gbps (Gigabit por segundo).

Propriedades adicionais podem ser configuradas no momento da criação do time, conforme apresentado no Quadro 4.3.

Tipo de configuração de modo	Descrição
Independente de switch	Neste modo o switch ao qual o servidor está conectado não reconhece que houve a configuração de um time de NICs, desta forma, o tráfego é gerenciado internamente pelo servidor e direcionado ao membro correspondente.
Dependente de switch	Neste modo, o switch ao qual o servidor está conectado determina como o tráfego será distribuído entre os membros do time de NICs.

Quadro 4.3. - Modo de configuração do time de NIC
Fonte: Adaptado de Windows IT Pro Center (2018).

Entre os principais benefícios que o agrupamento de NIC pode oferecer estão o uso combinado de até 32 interfaces de rede e a combinação da largura de banda dessas placas, oferecendo uma largura de banda resultante maior do que qualquer NIC único.

Na opção **Load balacing mode** pode ser escolhida uma entre duas opções: **Hyper-V Port** ou **Address Hash** .

No modo de balanceamento Hyper-V Port as máquinas virtuais são tratadas pelo switch como máquinas reais, havendo endereços MAC diferentes para cada máquina virtual (WINDOWS IT PRO CENTER, 2018).

No modo Address Hash é criado um hash com base no endereço contido no cabeçalho do pacote de dados, dessa forma a carga é balanceada entre todas as interfaces de rede do grupo (WINDOWS IT PRO CENTER, 2018).

Atividade

Schaefer (2018) explica que as configurações avançadas do NIC Teaming permitem escolher como o agrupamento de NICs funcionará. Uma forma de usar mais de uma placa de rede em um servidor é manter uma delas em stand-by e ativá-la somente em caso de falha na NIC principal. Analise as sentenças a seguir e escolha a alternativa verdadeira em relação à utilização de agrupamento de NICs.

SCHAEFER, A. Configurando o agrupamento de placas de rede para Windows Server 2012 / 2012 R2 / 2016 — NIC TEAMING. **Arthur Schaefer** , 2018. Disponível em: < https://www.arthurschaefer.com.br/2018/02/configurando-o-agrupamento-de-placas-de-rede-para-windows-server-2012-2012-r2-2016-nic-teaming/ >. Acesso em: 21 abr. 2019.

- **a)** O agrupamento de NICs garante economia na aquisição de placas de rede para servidores.
- **b)** O uso combinado de NICs proporciona uma taxa de transferência inferior devido à interferência entre os adaptadores, por isso é preferível ter somente um adaptador com maior velocidade.
- **c)** Independentemente do uso de agrupamento de NICs, em caso de falhas em um adaptador de rede será necessário parar de imediato todos os serviços, desligar o servidor, trocar a placa de rede que apresentou falhas e reinicializar o sistema.
- **d)** O uso combinado de NICs proporciona maior taxa de transferência do que placas de redes isoladas.
- **e)** O administrador de rede deve considerar a necessidade de aquisição de pelo menos 6 NICs, e no máximo 12, pois estes são os limites de placas de rede utilizadas no agrupamento de NIC do Windows Server 2012 ou mais recente.

Troubleshoot

A prevenção é a melhor forma de manter os serviços de TI funcionando em níveis adequados, no entanto, mesmo com planejamento apropriado, monitoramento e auditoria, eventualmente os problemas acontecem (BARRETT e KING, 2010, p. 407).

Dentre os problemas mais comuns de rede, Barrett e King (2010, p. 407) destacam os erros dos usuários e as conexões físicas. Para estes incidentes mais simples, geralmente as soluções são rápidas e fáceis de se executar. No entanto, para problemas mais graves é preciso elaborar uma estratégia a fim de determinar o diagnóstico, a isso damos o nome de troubleshooting.

Algumas etapas para a solução de um problema relacionado a redes de computadores e seus recursos, segundo a recomendação de Barrett e King (2010, p. 408), são apresentadas a seguir:

1. **Definir o escopo:** a constatação de um problema passa pela identificação dos sintomas, que podem ser comportamentos anormais, travamento, lentidão ou interrupção de um serviço. Verificar o que exatamente está acontecendo com o serviço ou o

servidor e quais das últimas mudanças que aconteceram no ambiente de rede podem ajudar a delimitar o problema.

2. **Definir prioridade:** em certas ocorrências, um problema não surge de forma isolada, e pode afetar de um a muitos usuários. Caso um serviço crítico de um servidor esteja inoperante, ou se o problema impacta muitas pessoas, seu tratamento terá prioridade mais alta em relação às outras tarefas do administrador de rede.
3. **Verificar prováveis causas:** determinar as causas prováveis para um problema permite que possíveis soluções sejam isoladas. Se várias soluções forem testadas simultaneamente, caso o problema seja corrigido não se saberá ao fim do processo qual foi a solução específica.
4. **Consultar a documentação:** geralmente sistemas de hardware e software acompanham uma documentação ou manual de uso, alguns deles indicam problemas comuns e como resolvê-los. Um administrador de rede deve saber onde encontrar essa documentação e ser familiarizado com ela para agilizar o atendimento.
5. **Utilizar ferramentas:** um conjunto de ferramentas pode ser utilizado para a tratativa de problemas mais comuns, nesta lista são incluídas falhas relacionadas a energia elétrica e rede, para as quais podem ser usados testadores de cabos, multímetros e voltímetros. Dentre as ferramentas também podem ser destacados softwares que auxiliam na identificação de falhas, como ping, traceroute, analisadores de rede e protocolo.

A atuação assertiva e rápida do administrador de redes em caso de falha nos serviços ou no servidor de rede é crucial para o restabelecimento das operações de TI. Barrett e King (2010, p. 422) defendem que “o gerenciamento de desempenho, bem como o gerenciamento do tempo de resposta, torna-se mais difícil” em redes complexas, mas o monitoramento correto através de logs, por exemplo, pode ajudar.

Segundo os autores, as mudanças constituem a principal fonte de falhas que

podem causar um mau desempenho na rede. Portanto, o administrador de rede deve saber o que mudou na rede corporativa recentemente (BARRETT e KING, 2010, p. 422).

Outras possíveis causas para problemas de desempenho da rede corporativa estão relacionadas a atualizações de software, instalação de novos equipamentos elétricos, interferência, novos hardwares e até mesmo mudanças na demanda dos usuários (BARRETT e KING, 2010, p. 422).

saiba mais

Saiba mais

Rafael Mantovani, especialista da Microsoft TechNet apresenta em seu vídeo uma proposta de abordagem de troubleshooting para ambiente de rede com sistemas Windows.

Veja em: < https://www.microsoft.com/pt-br/videoplayer/embed/973eab5b-1267-408f-be6b-f60e6446c3d2 >. Acesso em: 8 maio 2019.

Atividade

Para Barrett e King (2010, p. 422) “você não pode resolver instantaneamente todo problema que existe. Porém, pode descobrir uma metodologia para encontrar e diagnosticar quase todo problema de uma maneira sistemática e lógica”. Assinale a única alternativa verdadeira relacionada a troubleshooting de sistemas.

BARRETT, D.; KING, T. Redes de Computadores. Rio de Janeiro: LTC, 2010.

- **a)** Deve-se testar todas as causas prováveis simultaneamente de modo a resolver rapidamente o problema.
- **b)** Quando o problema detectado tiver alto impacto não é recomendável consultar a documentação devido ao tempo gasto.
- **c)** A determinação do nível de prioridade do problema implica concentrar esforços para resolver falhas que impactam maior quantidade de usuários ou serviços mais críticos.
- **d)** Em um ambiente de rede complexo não existem causas prováveis. Falhas podem acontecer por qualquer razão.
- **e)** Um administrador de rede proativo não precisa levar em consideração as mudanças ocorridas no ambiente de rede, mas deve considerar as próximas mudanças que ocorrerão.

Backup

A cópia de dados, mais conhecida como backup, é um mecanismo de segurança que realiza a duplicação de dados com o intuito de reservar uma cópia destes por segurança, em caso de imprevistos. É como se fosse registrada uma “foto” dos dados em um particular momento, definido pela empresa, e essa “foto” ficasse guardada até sua devida utilização. Caso não utilizada, a “foto” pode ser atualizada por uma mais recente dos dados.

Faria (2017) define backup como:

> *Backup consiste em gerar dados redundantes com o propósito específico de recuperação no caso de perda dos originais. As cópias podem ser armazenadas no mesmo computador, em um dispositivo de storage ou, ainda, em outro prédio ou localização (protegendo assim os dados de ameaças físicas e lógicas locais): partindo de um nível menor de segurança para um maior, respectivamente. (FARIA, 2017, p. 1).*

O autor ressalta que, em casos de perda de dados, um backup realizado corretamente colabora com a redução do impacto, permitindo uma

restauração mais rápida do serviço, garantindo também a qualidade dos dados, conforme o nível de serviço determinado pela organização (FARIA, 2017, p. 1).

No Quadro 4.4 é possível verificar os principais fatores relativos aos procedimentos de backup:

Fatores	Descrição
Automação	Backups manuais estão mais suscetíveis a erros humanos. O processo automático contribui para um backup confiável e com menos esforço.
Controle de Qualidade	Realização de testes periódicos para verificar se o backup está corretamente configurado.
Gestão de Riscos	É importante identificar e verificar a mitigação de riscos aportados em processos de backup para minimização de falhas em procedimentos.
Aderência aos acordos operacionais/níveis de serviços	Deve estar alinhado às estratégias do cliente e formalizado com acordos operacionais ou níveis de serviços.

Quadro 4.4 - Fatores para procedimentos de backup
Fonte: Adaptado de Faria (2017, p. 2).

Existem diferentes tipos de backup que estrategicamente podem ser utilizados pelas empresas, conforme o Quadro 4.5.

Tipo de Backup	Descrição
Completo	Copia todos os arquivos desmarcando o bit de arquivamento.
Incremental	Possui as informações do último backup e desmarca o bit de arquivamento.
Diferencial	Copia todas as alterações realizadas desde o último backup e não desmarca o bit de arquivamento.
De Cópia	Copia todos os arquivos e não desmarca o bit de arquivamento.

Quadro 4.5 - Tipos de Backup
Fonte: Adaptado de Barrett e King (2010, p. 386).

Segundo Faria (2017, p. 17), há três tipos de locais de armazenamento de backups. Backups on-site são dispositivos de armazenamento em massa (conhecidos como storages) e mídias de backup armazenados no mesmo prédio ou próximo aos computadores. Backups off-site são aqueles que estão fisicamente em torno de 15 km de distância do local de armazenamento original. Backup Cloud é um tipo de cópia que fica armazenada em um servidor na nuvem e pode ser acessada remotamente de qualquer localidade através da internet.

Em ambiente de rede com servidores baseados em Linux existe uma grande variedade de aplicações voltadas para a realização de backups, como Bacula, Amanda e ZBackup (COSTA, 2016).

Reflita

O desastre das Torres Gêmeas em 11 de setembro de 2001, nos Estados Unidos, representou um marco para a Segurança da Informação. Foi constatado que várias empresas guardavam seus backups na torre vizinha, e devido à grande tragédia com as duas torres, muitos dados nunca foram recuperados. Como planejar o armazenamento seguro dos backups de dados?

Fonte: Morales (2013).

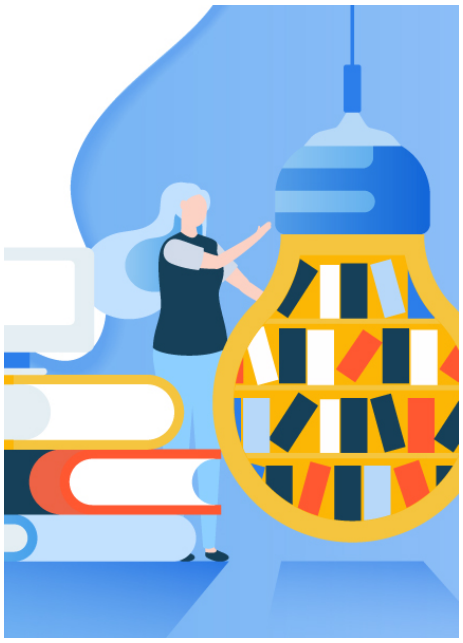
Atividade

Analise as sentenças a seguir e assinale a alternativa que identifica um fator de importância da realização de backups periódicos em uma empresa.

- **a)** Possui duplicidade de arquivos e dados desatualizados.
- **b)** Realiza controle da qualidade dos dados.
- **c)** Tem aderência aos acordos de níveis de serviço.
- **d)** Previne a empresa contra ataques de *malwares* e vírus.
- **e)** É possível recuperar dados atuais mediante imprevistos.

indicações

Material Complementar



LIVRO

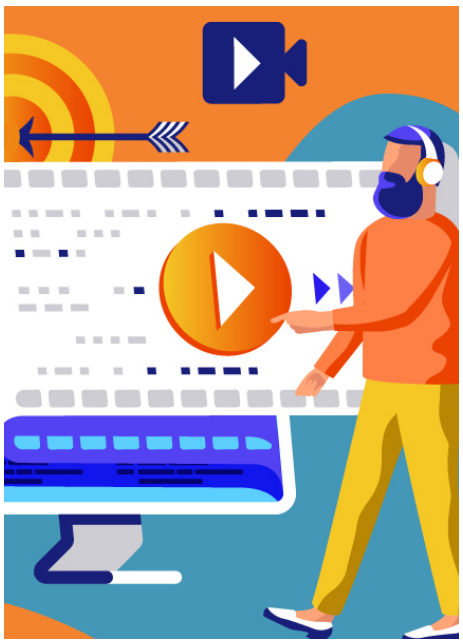
Redes com Windows Server 2016

Andrew Warren

Editora: Bookman

ISBN: 8582604645

Comentário: Com este livro você aprenderá os fundamentos da configuração de servidores de rede com Windows Server e poderá se preparar para obter uma certificação profissional.



FILME

A Rede

Ano: 1995

Comentário: Neste filme, a protagonista, interpretada por Sandra Bullock, é vítima de um complexo ataque de hacker, capaz de alterar sua identidade e seus registros nos mais variados sistemas do governo. Assista a este filme e reflita como os registros de logs poderiam ser úteis para a identificação da autoria dos crimes cibernéticos.

Para conhecer mais sobre este filme, acesse o trailer disponível em:

TRAILER

conclusão

Conclusão

Nesta unidade discutimos a importância de compreender os sistemas de logs e identificar problemas e soluções relacionados ao ambiente de TI. Através das técnicas de troubleshooting foi possível verificar possíveis problemas de um servidor e como um administrador de redes deve atuar em caso de falhas, seja no âmbito das tecnologias de comunicação de dados ou no sistema operacional de um servidor.

Foi possível também aprender sobre o uso combinado de várias placas de rede em um mesmo servidor, a lógica da estruturação de um time de NIC e como aplicar o agrupamento de NICs em contingências de rede.

Um quesito importante de segurança dos dados foi tratado no tópico 4, descrevendo o conceito e definições de backup, suas devidas configurações e as ferramentas mais utilizadas.

referências

Referências Bibliográficas

BARRETT, D.; KING, T. **Redes de Computadores** . Rio de Janeiro: LTC, 2010.

FARIA, H. M. **Bacula** : o software livre de backup. 3 ed. Rio de Janeiro: Brasport, 2017.

THOMPSON, M. A. **Microsoft Windows Server 2012** : Instalação, Configuração e Administração de Redes. 2. ed. São Paulo: Érica, 2014.

COSTA, R. F. TOP 15 ferramentas open source de backup para Linux. **Linux Descomplicado** , 2016. Disponível em: < https://www.linuxdescomplicado.com.br/2016/01/15-ferramentas-open-source-de-backup-para-linux.html >. Acesso em: 21 abr. 2019.

DIBIAZI JUNIOR, W. Auditoria e Rotacionamento de logs em Servidores de Arquivos Linux. **Profissionais de TI** , 2015. Disponível em: < https://www.profissionaisti.com.br/2015/09/auditoria-e-rotacionamento-de-logs-em-servidores-de-arquivos-linux/ >. Acesso em: 21 abr. 2019.

KAIESKI, N. Utilizando Logrotate. **Dicas-L** , 2012. Disponível em: < http://www.dicas-l.com.br/arquivo/utilizando_logrotate.php#.XLy1Athv_IU >. Acesso em: 21 abr. 2019.

MORALES, I. 11 de Setembro e a Segurança da Informação. **Security Information News** , 2013. Disponível em: < https://securityinformationnews.com/2013/09/11/11-de-setembro-e-a-seguranca-da-informacao/ >. Acesso em: 21 abr. 2019.

SCHAEFER, A. Configurando o agrupamento de placas de rede para Windows Server 2012 / 2012 R2 / 2016 — NIC TEAMING. **Arthur Schaefer** , 2018. Disponível em: < https://www.arthurschaefer.com.br/2018/02/configurando-o-agrupamento-de-placas-de-rede-para-windows-server-2012-2012-r2-2016-nic-teaming/ >. Acesso em: 21 abr. 2019.

TELLES, R. Rotacionamento de logs e o desastre iminente. **Rodrigo Telles.com** , 2014. Disponível em: < https://rodrigotelles.com/rotacionamento-de-logs-e-o-desastre-iminente/ >. Acesso em: 21 abr. 2019.

CRIAR uma nova equipe de placa de rede em um computador Host ou VM. **Windows IT Pro Center** , 2019. Disponível em: < https://docs.microsoft.com

/pt-br/windows-server/networking/technologies/nic-teaming/create-a-new-nic-team-on-a-host-computer-or-vm >. Acesso em: 21 abr. 2019.

NIC Teaming settings. **Windows IT Pro Center** , 2018. Disponível em: < https://docs.microsoft.com/en-gb/windows-server/networking/technologies/nic-teaming/nic-teaming-settings >. Acesso em: 21. abr. 2019.

IMPRIMIR