



INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

BOAS PRÁTICAS DA SEGURANÇA DA INFORMAÇÃO – PARTE II

Prof. Dr. Daniel Caetano

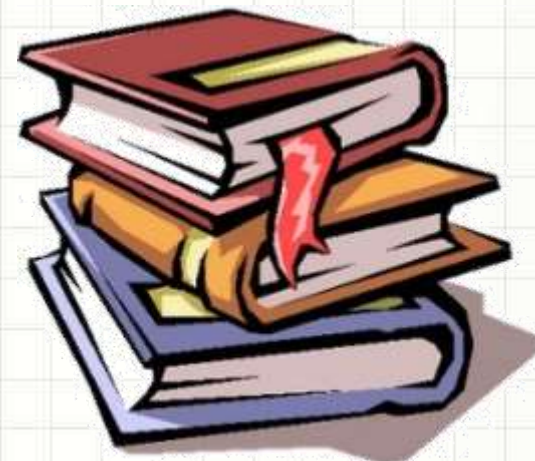
2020 - 1

Objetivos

- Recordar os mecanismos de controle de acesso e sua importância
- Conhecer os procedimentos relacionados aos registros de acesso (logs)
- Compreender a importância da sincronia de relógio dos diferentes equipamentos
- Tomar contato com o conceito de política de cópia de segurança (backup)



Material de Estudo



Material

Acesso ao Material

Notas de Aula e
Apresentação

<http://www.caetano.eng.br/>
(Segurança da Informação – Aula 8)

Material Didático

Gestão de Segurança da Informação, Cap 5.

Leitura Adicional

<http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf> (Cartilha do TCU)



CONTROLE DE ACESSO LÓGICO

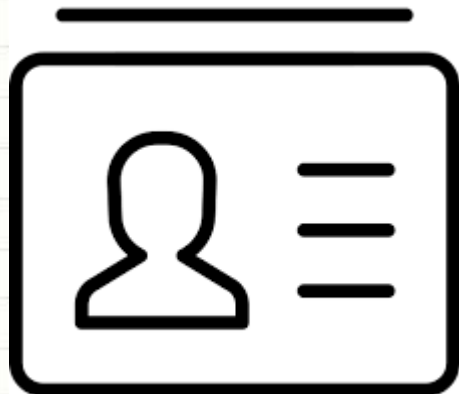
Controle de Acesso

- Segurança pressupõe controle de acesso
 - Físico x lógico
- Envolve
 - Recurso x usuário: quem pode o quê
- Regra de ouro: tudo proibido...
 - ...a menos que expressamente permitido.
 - Registrar tudo que todos fazem
 - Auditoria
 - Responsabilização



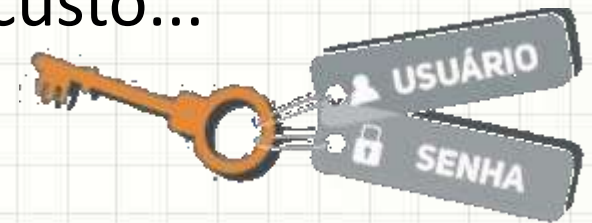
Controle de Acesso: Procedimento

- **Logon/Login:** dois processos básicos
 - Identificação: qual é o usuário e suas permissões
 - Autenticação: comprovar a identidade
- Resumindo
 - **Identificação + Algo que usuário sabe ou tem**



Dificuldades Associadas

- Processo precisa ser resistente à “invasão”:
 - Cartões: podem ser perdidos
 - UserIDs: podem ser fornecidos facilmente
 - Senhas: anotações, senhas fracas, força bruta...
 - Biometria: falsos negativos, custo...



- Recordando
 - Limitar o número de tentativas (e registrar!)
 - Exigir senhas complexas (evitar dicionários!)
 - Limitar o tempo de login (esquecimento!).

Política de Acesso Lógico

- Em geral, as permissões de acesso
 - Associadas à função do funcionário
 - Papel do funcionário dentro da empresa
 - Permissões devem ser atribuídas minuciosamente
 - Apenas o necessário...!
 - Revisões periódicas!
 - Remover excessos
 - Ex.: Estagiário



PROFESSORES



ESTUDANTES



PESQUISADORES

Controle de Acesso de Arquivos

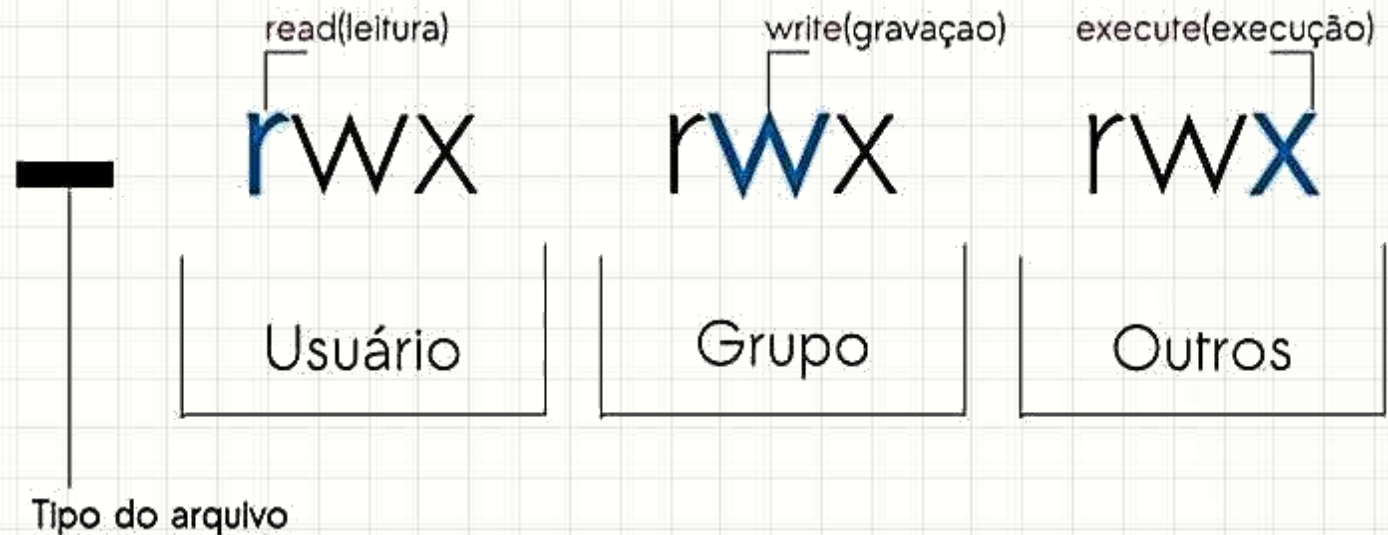
- Além do *login...* existe outro aspecto
 - Proteção de acesso no nível do sistema de arquivos



- Unix/Linux x Windows

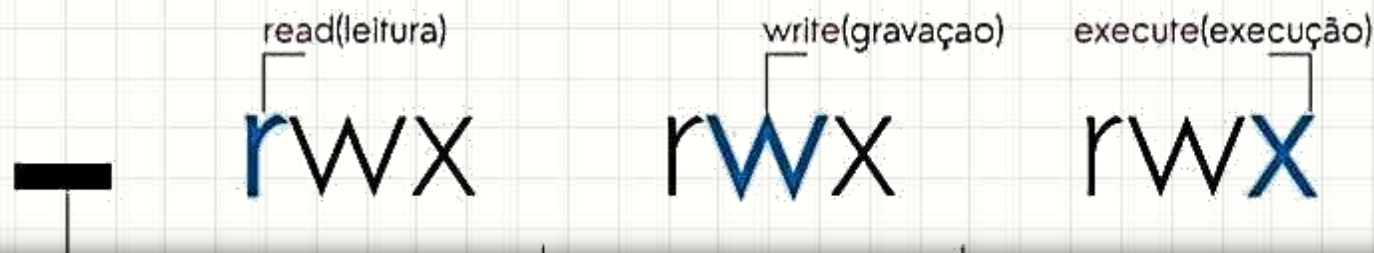
Controle de Acesso de Arquivos

- Unix/Linux
 - Permissões de execução (x), leitura (r) e escrita (w)
 - Usuário, grupo de usuários e usuários em geral



Controle de Acesso de Arquivos

- Unix/Linux
 - Permissões de execução (x), leitura (r) e escrita (w)
 - Usuário, grupo de usuários e usuários em geral



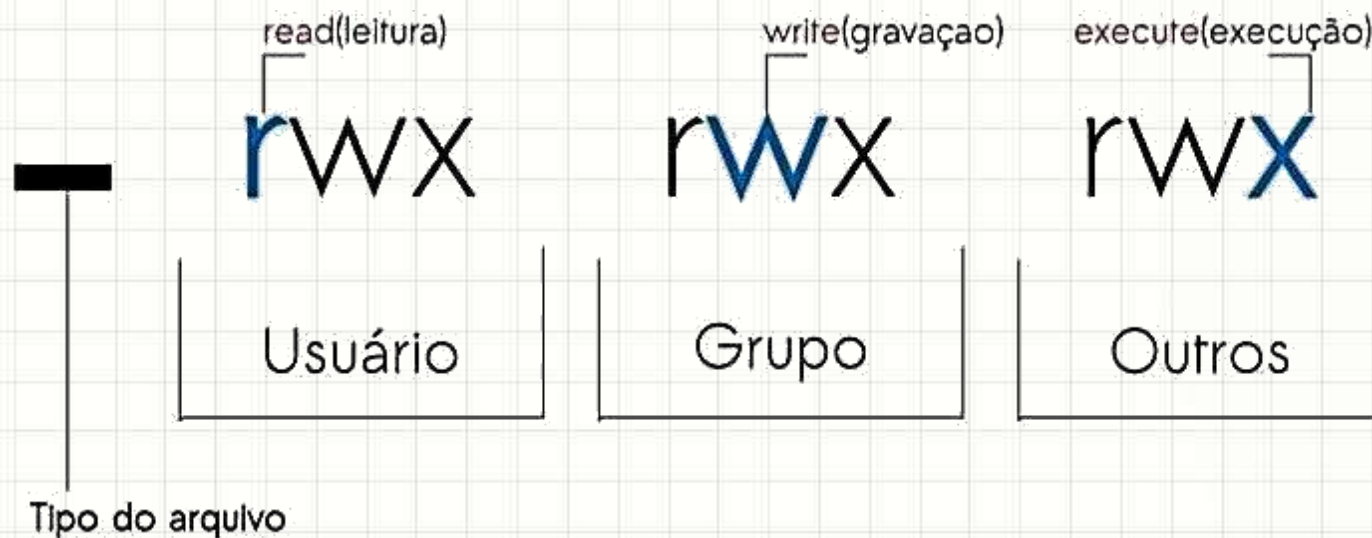
www.linuxnaweb.com

Usuário dono	Grupo dono	Outros								
-rw-	r--	r--	1	root	root	1528	Out 31 22:33	/etc/passwd		
Tipo de objeto	Permissão		Número de links	Dono	Grupo Dono	Tamanho	Data	Hora	Caminho	Nome

Controle de Acesso de Arquivos

- Unix/Linux

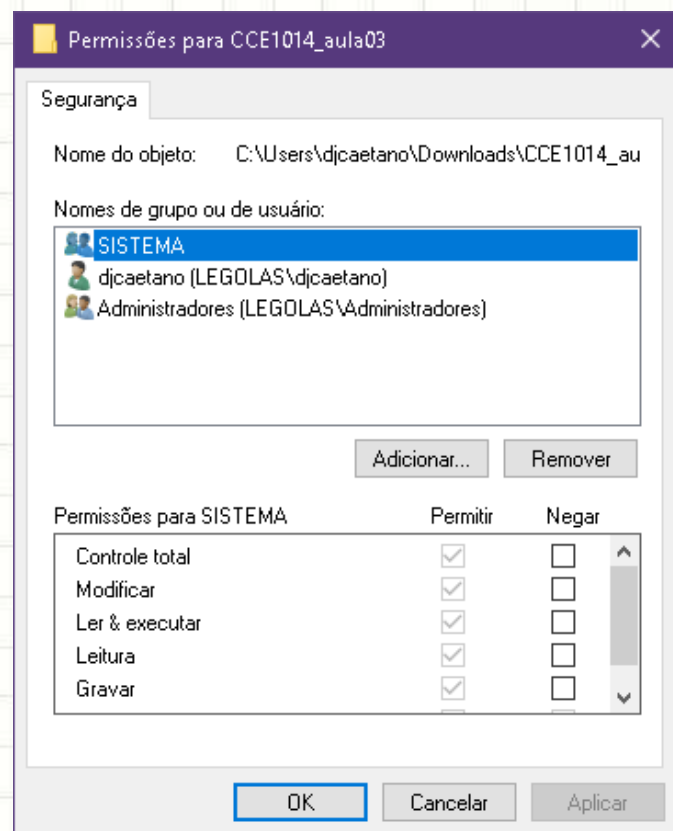
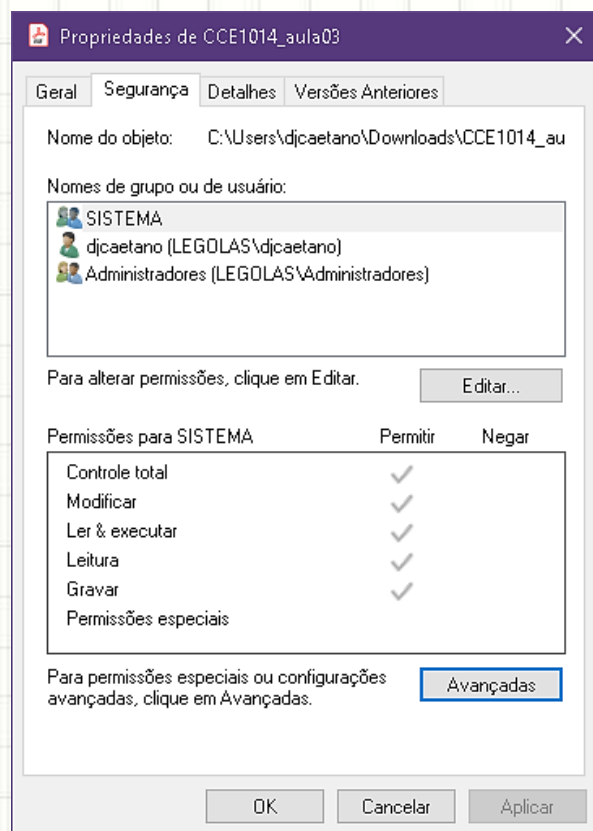
- Permissões de execução (x), leitura (r) e escrita (w)
- Usuário, grupo de usuários e usuários em geral



- Root sempre tem acesso a tudo.
 - Proteger! Nunca *login* remoto!

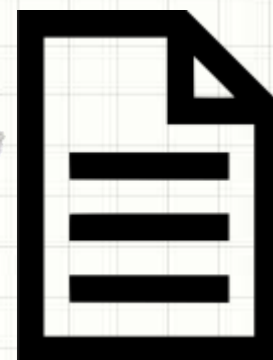
Controle de Acesso de Arquivos

- *Windows/Active Directory*
 - ACL – *Access Control Lists*
 - Permite melhor controle, mas integração limitada



Proteção com Controle de Acesso

- O que proteger?
 - Aplicativos;
 - Arquivos de dados;
 - Utilitários e S.O.;
 - Arquivos de senha;
 - Arquivos de log.



Proteção com Controle de Acesso

- Aplicativos
 - Código fonte e objetos compilado
 - Por quê?
 - Inserir as mais variadas brechas de segurança
 - Modificar o comportamento de maneira inadequada
 - Ex.: “arredondamentos” em código financeiro.



Proteção com Controle de Acesso

- Arquivos de Dados
 - Tanto arquivos propriamente ditos...
 - ...quanto em banco de dados
 - Por quê?
 - Dados de operação da empresa
 - Dados estratégicos
 - Dados de clientes...



Proteção com Controle de Acesso

- Utilitários e Sistema Operacional
 - Acesso restrito, principalmente aos mais críticos
 - Compiladores, manutenção, monitoração, diagnóstico...
 - Por quê?
 - Maiores alvos, permitem expor configurações e falhas
 - Permite abrir brechas graves e “invisíveis”.



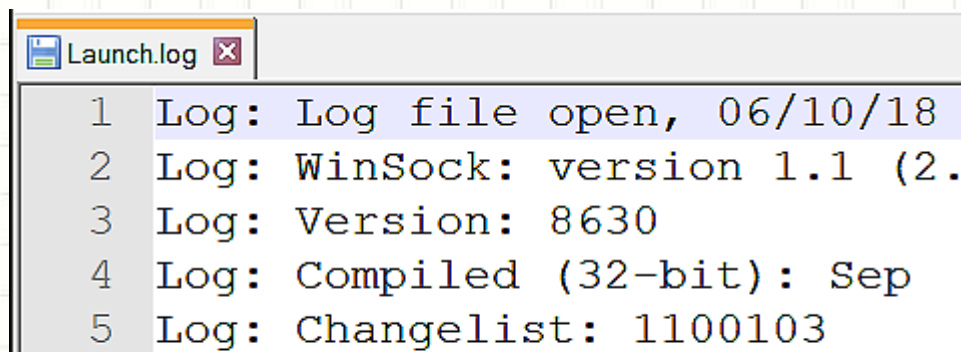
Proteção com Controle de Acesso

- Arquivos de Senha
 - Tanto do sistema operacional quanto aplicativos
 - Por quê?
 - Prejudicam completamente o controle!
 - Usuário que tenha acesso pode ser passar por outros!.



Proteção com Controle de Acesso

- Arquivos de Log
 - De acesso e operações...
 - De sistema e das aplicações!
 - Por quê?
 - É pelos logs que fazemos auditoria
 - Identificar tentativas e sucessos de ataques
 - Se eles forem alterados/apagados...
 - Ficamos no escuro!



```
Launch.log x
1 Log: Log file open, 06/10/18
2 Log: WinSock: version 1.1 (2.
3 Log: Version: 8630
4 Log: Compiled (32-bit): Sep
5 Log: Changelist: 1100103
```

O que mais Restringir?

- Além do acesso a arquivos...
 - (Permissões do sistema de arquivos e ACLs)
- Restringir funções nas aplicações
 - Opções não autorizadas não devem nem aparecer
 - Ocultar dados que não podem ser exibidos.

The screenshot shows a settings page for a menu item named 'Muay Thai'. At the top, there is a header with the name 'Muay Thai' and a 'Página' dropdown. Below this is a 'Rótulo de navegação' (Navigation Label) field containing 'Muay Thai'. A red box highlights the 'User Restrictions' section, which includes three radio buttons: 'Logged Out Users', 'Logged In Users' (which is selected), and 'All Users'. Below this, a green box highlights the 'Access Role' section, which contains a note: 'Access Role: leave all unchecked to allow all logged in users to see the menu.' and five checkboxes: 'Administrator', 'Editor', 'Author', 'Contributor', and 'Subscriber'. All five checkboxes are currently checked. At the bottom, there is a 'Mover' section with a link 'Um abaixo'.

Muay Thai Página ▲

Rótulo de navegação

Muay Thai

User Restrictions

Logged Out Users Logged In Users All Users

Access Role: leave all unchecked to allow all logged in users to see the menu.

Administrator Editor Author
 Contributor Subscriber

Mover [Um abaixo](#)



REGISTROS DE ACESSO E OPERAÇÃO: LOGS

Registros de Acesso e Operação

- O que são?
 - Registros cronológicos e detalhados de:
 - O que foi feito
 - Quem fez
 - Onde/De onde fez (se for o caso).
 - Possibilitam a reconstrução e revisão...
 - ...de uma operação, procedimento ou evento...
 - ...do início ao fim.

Foram encontrados 10320 registros.

Primeira | Anterior | **1** 2 3 4 5 6 ... | Próxima | Última

Data	Identificador	Usuário	Tipo	IP	Requisição
12/05/2010 às 09:49	aix sistemas		Outros	192.168.0.9	/webgizead/index.php?option=com_aixadministracao&view=logacesso
12/05/2010 às 09:46	aix sistemas		Outros	192.168.0.9	/webgizead/index.php?option=com_aixadministracao&view=papelpessoa
12/05/2010 às 09:46	aix sistemas		Outros	192.168.0.9	/webgizead/index.php?option=com_aixadministracao&view=papelpessoa
12/05/2010 às 09:44	aix sistemas		Outros	192.168.0.9	/webgizead/index.php?option=com_aixadministracao&view=papelpessoa
12/05/2010 às 09:44	aix sistemas		Outros	192.168.0.9	/webgizead/index.php?option=com_aixadministracao&view=papelpessoa

Registro de Acesso e Operação

- Finalidade
 - Auditoria
- Também conhecidos como
 - Logs ou Logging
- Demanda ações da administração do sistema
 - Cadastro / Comunicação de Senhas
 - Cada usuário é único no sistema (incluindo adms)
 - Gerenciamento de permissões
 - Gerenciamento dos próprios logs
 - Auditorias Frequentes.



Exemplos de Logs

- Log de acesso

```
20/01/2008 - 22:17:55 - IP: 200.178.95.16 - ddamasio logged in.  
20/01/2008 - 22:19:30 - IP: 200.192.67.112 - jsoldi logged in.  
20/01/2008 - 22:54:17 - IP: 200.178.95.16 - ddamasio logged out.  
20/01/2008 - 22:55:32 - IP: 200.192.67.112 - jsoldi logged out.  
20/01/2008 - 23:20:13 - IP: 163.102.100.17 - cabrahm logged in.  
21/01/2008 - 00:10:11 - IP: 163.102.100.17 - cabrahm logged out.
```

- Log de operações

```
20/01/2008 - 23:25:33 - IP: 163.102.100.17 - copied \\COMP3\shared\test.c to c:\work.  
20/01/2008 - 23:27:33 - IP: 163.102.100.17 - opened file c:\work\test.c.  
21/01/2008 - 00:08:25 - IP: 163.102.100.17 - saved and closed file c:\work\test.c.
```

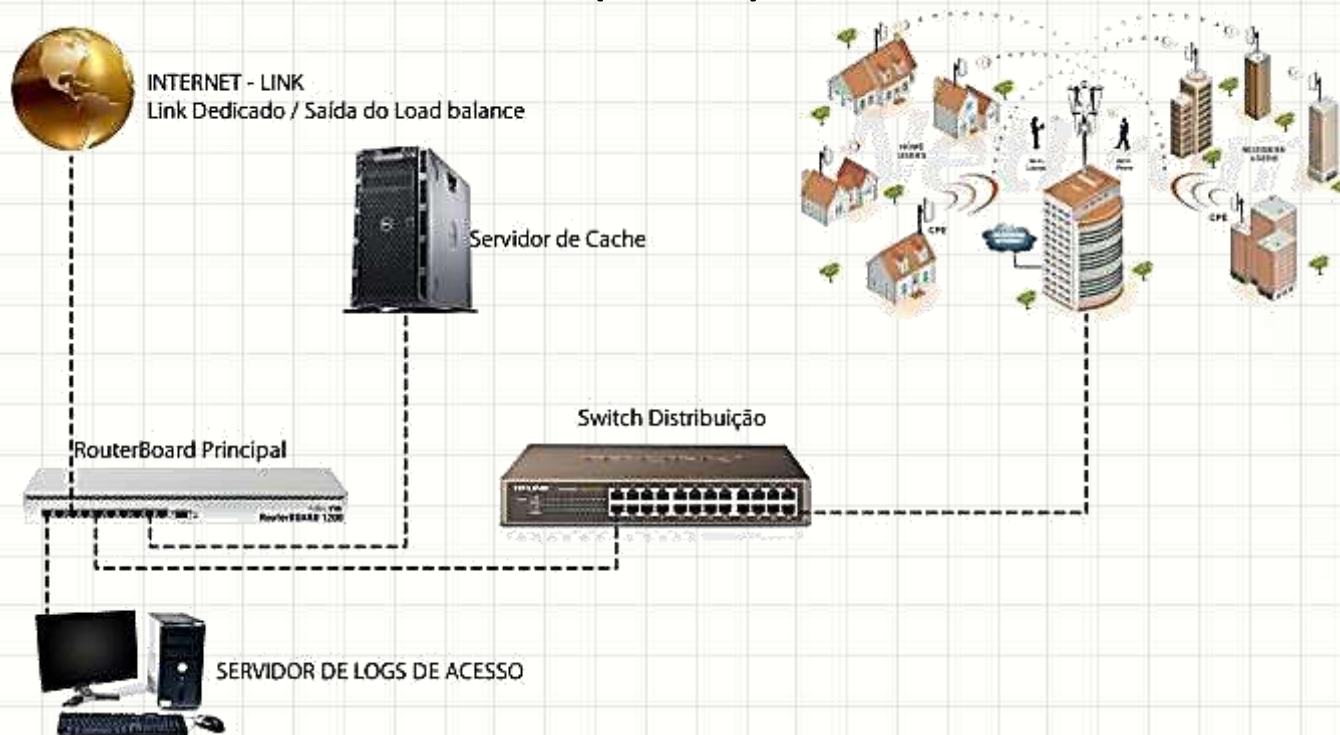

Sincronia de Relógios

- A sincronia de relógios é fundamental
- Por quê?
 - Correlacionar logs em máquinas diferentes!
 - Sistemas de Single Sign-On não funcionam sem.
- Como manter a sincronia?
 - Linux: `ntpdate -s pool.ntp.br`
 - Windows: Configuração > Hora e Idioma
 - “Definir Horário automaticamente” como ligado



Armazenamento dos Logs

- Onde armazenar os logs?
 - Em geral, existe um armazenamento local
 - Cuidado com as permissões!
 - Pode ser externo (rede) ou misto



Logs de Armazenamento Local

- Vantagens
 - Configuração mais simples
 - Baixo consumo de recursos
 - Funciona mesmo que a rede dê problemas.
- Desvantagens
 - Administração descentralizada
 - Proteção depende do sistema de arquivos e S.O.
 - Pode ser alterado/apagado, se permissões autorizarem
 - Se disco lotar por alguma outra razão...
 - O registro nos logs ficará comprometido.

Logs de Armazenamento Externo

- “Servidor de Log”
- Vantagens
 - Administração centralizada
 - Facilita a gestão de espaço em disco para log
 - Proteção maior: limitar acesso ao servidor de log
 - Limitar significativamente o poder de alterar/apagar.
- Desvantagens
 - Configuração mais complexa
 - Maior consumo de recursos
 - Se a rede cair, pode deixar de realizar registros.

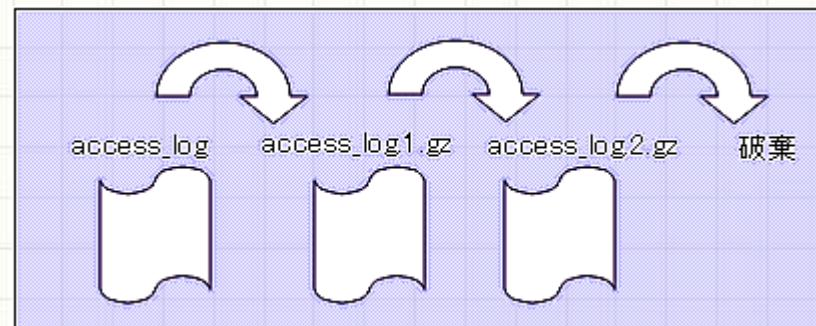
Logs de Armazenamento Misto

- Duplo registro: local e via rede
- Vantagens
 - Maior segurança geral
 - Dificilmente o invasor conseguirá apagar todas as suas pistas
 - Se rede falhar ou disco local lotar, haverá registros
 - Se os dois ao mesmo tempo... Aí não! 😊.
- Desvantagens
 - Administração complexa (espalhada + servidor de log)
 - Configuração bastante mais complexa
 - Consumo de recursos significativamente maior
 - Maior complexidade na auditoria (logs diferentes).

Rotação de Logs

- Até quando preciso guardar os logs?

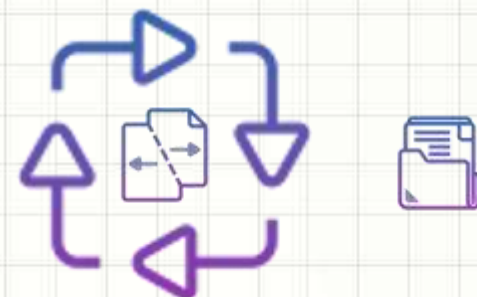
- Critérios legais
- Critérios de negócio
- Espaço.



- Liberar espaço...

- De tempos em tempos, começar um novo
- Comprimir arquivos de log mais antigos
- Apagar os que já “venceram”...
 - ...E/ou foram auditados

Rotação de Logs



Auditoria de Logs

- Reconstruir eventos
 - “Seguir as migalhas de pão”
- Monitoramento...
 - Proativo x Reativo
- Auditoria frequente
 - Tanto quanto o sistema for crítico
 - Qualquer evento estranho deve ser investigado.





CÓPIAS DE SEGURANÇA

Cópias de Segurança

- O que é isso?
 - Cópias de dados e programas relevantes...
 - ...para recuperação em caso de desastres
 - E para proteção legal.
- Também conhecidas como...



Frequência de Backup

- Com que frequência fazemos backup?
 - Sempre que possível e não prejudique os negócios.
- Limitações
 - Espaço: cópias ocupam espaço
 - Tempo: backup com sistema desligado
 - Desempenho: backup com sistema ligado.
- Resumindo: não dá pra copiar tudo sempre
 - Diária, semana, mensal... Misto
 - Depende da necessidade.



Abrangência do Backup

- Tenho que fazer backup de tudo?

- Depende!

- Estratégias comuns:

- Completa ou completa+diferencial

- O que usualmente protegemos?

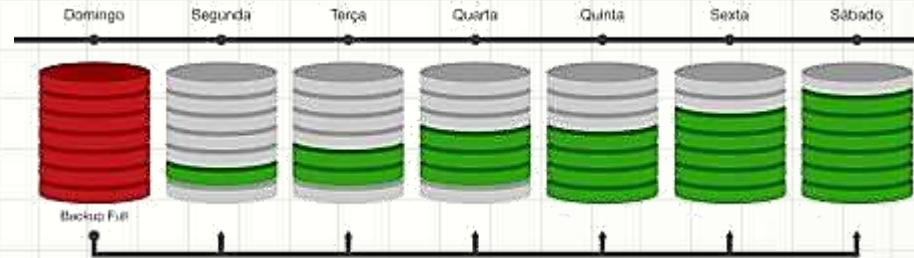
- Arquivos de dados / banco de dados

- Arquivos de configuração.

- Em sistemas complexos / máquinas virtuais

- Pode-se fazer backup de tudo, completo

- Deixa-se para o “storage” eliminar as redundâncias



Mídias/Armazenamento de Backup

- Em que meio guardar esses dados?
 - Diversos: fitas DAT, DVDs, BluRays, *storage*...
- Escolha:
 - Tipo de ameaça aos dados
 - Quantidade de dados
 - Tempo de vida do dado
 - Frequência da recuperação
 - Tempo de recuperação.





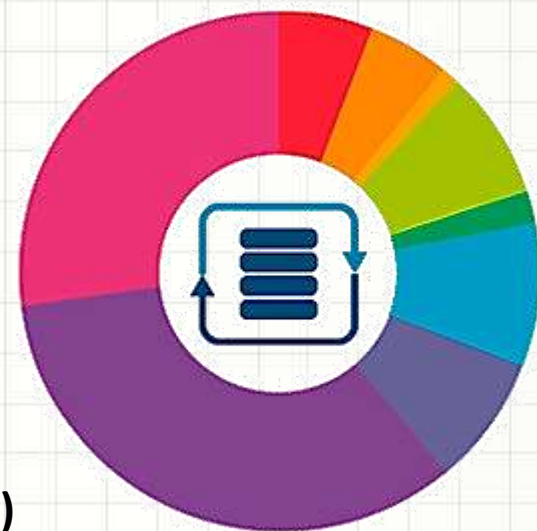
Localidades de Backup

- Onde guardar esses dados?
 - De preferência, não na mesma máquina da origem!
 - Embora mesmo essa seja melhor que nenhuma!
- Idealmente:
 - Localidade externa
 - Distante o suficiente para evitar “desastre duplo”
 - Perto o suficiente para não prejudicar recuperação
 - Quando necessária.... Qual o prazo?
 - Segurança física e lógica na localidade externa
 - Controle ambiental.



Testes de Restauração

- Os ambientes mudam...
 - Conteúdo do backup: revisar com frequência
 - Além da documentação, como saber?
- Testes de restauração
 - Simulação de desastre
 - Restabelecer estado anterior
 - Completa x arquivos específicos



Frequência de Necessidade de Recuperação (GFI Software)





QUESTÕES

Quiz

Para que a auditoria em logs possa ser feita com sucesso, marque a alternativa **INCORRETA...**

<https://kahoot.it/>



CONCLUSÕES

Resumo e Próximos Passos

- Controle de acesso lógico
 - Principais mecanismos
 - Política de controle de acesso
 - Registro e manutenção de logs
 - Políticas de backup
-
- + Boas práticas em segurança da informação
 - Continuidade de negócios
 - Enfrentando um ataque



PERGUNTAS?