

Grupo Handbook

# Handbook de Questões de TI

comentadas para **CONCURSOS**

*Além do gabarito*

2ª Edição

Volume 1

*Analista de Suporte  
BNDES 2008  
Fundação Cesgranrio*

## **Prefácio**

Este é o primeiro volume da série *Handbook de Questões de TI Comentadas para Concursos – Além do Gabarito*, que traz para você a oportunidade de se preparar para concursos de TI por meio de estudo de provas reais. Além disso, não faltará embasamento teórico ao concurseiro, uma vez que os comentários elaborados não se limitam à simples resolução das questões.

Este volume traz a prova para Analista de Suporte do BNDES, aplicada em meados de 2008 pela Fundação Cesgranrio. São 40 questões comentadas “além do gabarito” para você se preparar não só para os concursos do BNDES, mas, também, para todos os demais concursos de alta concorrência na área de TI.

Pelo fato do BNDES oferecer salário e benefícios superiores aos da maioria das empresas públicas e órgãos governamentais, o cargo de Analista de Suporte do BNDES é um dos mais disputados no Brasil na área de TI.

Trata-se de uma prova completa, que cobre assuntos como segurança de informação, arquitetura de computadores, banco de dados, governança de TI, gerenciamento de projetos e muito mais.

Bons estudos,

*Grupo Handbook de TI*

**Direitos Autorais**

Este material é registrado no Escritório de Direitos Autorais (EDA) da Fundação Biblioteca Nacional. Todos os direitos autorais referentes a esta obra são reservados exclusivamente aos seus autores.

Os autores deste material não proíbem seu compartilhamento entre amigos e colegas próximos de estudo. Contudo, a reprodução, parcial ou integral, e a disseminação deste material de forma indiscriminada através de qualquer meio, inclusive na Internet, extrapolam os limites da colaboração. Essa prática desincentiva o lançamento de novos produtos e enfraquece a comunidade concurseira Handbook de TI.

A série *Handbook de Questões de TI Comentadas para Concursos – Além do Gabarito* é uma produção independente e contamos com você para mantê-la sempre viva.

*Grupo Handbook de TI*

### **Canais de Comunicação**

A equipe Handbook de TI disponibiliza diversos canais de comunicação para seus clientes.

#### *Loja Handbook de TI*

<http://www.handbookdeti.com.br>

#### *Serviço de Atendimento*

Comunicação direta com a Equipe Handbook de TI pode ser feita em  
<http://www.handbookdeti.com.br/contacts>

#### *Twitter do Handbook de TI*

Que acompanhar de perto o trabalho do Grupo Handbook de TI. Cadastre-se no twitter e comece a seguir o grupo Handbook de TI em <http://twitter.com/handbookdeti>

1. **Assuntos relacionados:** *Comandos UNIX, Link Simbólico, Hard Link,*

**Banca:** *CESGRANRIO*

**Instituição:** *BNDES*

**Cargo:** *Analista de Suporte*

**Ano:** *2008*

**Questão:** *31*

No Linux, que comando é utilizado para criação de links simbólicos?

- (a). `dmesg`
- (b). `rsync`
- (c). `mv -f`
- (d). `ln -s`
- (e). `chmod -l`

---

**Solução:**

(A) ERRADA

O comando `dmesg` é um comando do UNIX utilizado para imprimir as mensagens do kernel na saída padrão. Por padrão, as mensagens do kernel são salvas no arquivo `/var/log/dmesg`. O parâmetro mais comum do comando `dmesg` é o `-n`, que serve para controlar o nível de log que será enviado para a saída padrão. Usualmente, o comando `dmesg` é utilizado para diagnosticar problemas durante a etapa de inicialização do sistema.

(B) ERRADA

O `rsync` é um aplicativo UNIX que sincroniza diretórios e arquivos entre dois computadores ou dois pontos distintos em um mesmo computador. O aplicativo trabalha de forma incremental, sincronizando apenas as partes alteradas dos arquivos, poupando a rede e tornando a sincronização mais rápida. O `rsync` também é capaz de preservar links, propriedades e permissões dos arquivos, bem como as datas de criação e modificação.

(C) ERRADA

No UNIX, o comando `mv` é utilizado para renomear um arquivo ou movê-lo de um diretório para outro. Com a opção `-f`, o `mv` irá mover o arquivo sem solicitar a confirmação ao usuário, mesmo que um arquivo de mesmo nome já exista no diretório de destino.

(D) CORRETA

O comando `ln` é utilizado para criar links entre arquivos ou diretórios. Por sua vez, os links são pseudo arquivos que apontam para um arquivo real. No UNIX, existem basicamente dois tipos de links: os hard links e os links simbólicos. Os links simbólicos são criados pela opção `-s` do comando `ln`.

Um hard link é uma cópia de uma entrada do sistema de arquivos. As duas entradas contêm nomes diferentes, mas apontam para o mesmo inode, de modo que o conteúdo e as permissões sejam compartilhados. Embora os hard links não ocupem espaço útil no sistema de arquivos, eles possuem duas limitações básicas. A primeira é que o hard-link e o arquivo precisam estar no mesmo sistema de arquivos, e a segunda é que os hard links não podem

apontar para diretórios.

Os links simbólicos são pequenos arquivos que apontam para outros arquivos, que podem estar localizados em qualquer lugar, inclusive em sistemas de arquivos remotos. Ao contrário dos hard links, os links simbólicos ocupam espaço, embora pequeno, no sistema de arquivos e podem apontar para diretórios. As permissões do arquivo real são herdadas pelos links simbólicos e, caso o arquivo real seja apagado, o link simbólico torna-se um dead link, pelo fato de apontar para um arquivo ou diretório que não mais existe no sistema de arquivos.

#### (E) ERRADA

O comando `chmod` é utilizado para modificar as permissões de acesso em arquivos ou diretórios no UNIX. Com o `chmod` é possível, por exemplo, definir se um usuário ou um grupo pode ler, alterar ou executar os arquivos. No caso dos diretórios, o privilégio de execução corresponde ao direito de listar seu conteúdo.

**2. Assuntos relacionados:** *Redes de Computadores, Endereçamento IP, Protocolo ARP,***Banca:** *CESGRANRIO***Instituição:** *BNDES***Cargo:** *Analista de Suporte***Ano:** *2008***Questão:** *32*

Suponha uma rede TCP/IP formada por 3 equipamentos conectados em um mesmo switch:

Estação X, IP 192.168.10.100/24

Estação Y, IP 192.168.10.200/24

Roteador R, IP 192.168.10.1/24

Considerando-se que o default gateway (default route, rota padrão) de cada estação é R, observe as afirmativas abaixo.

- I - Caso X inicie uma conexão TCP destinada a Y, os pedidos de requisição de conexão (SYN) passarão por R.
- II - Todas as mensagens ARP Request enviadas por Y são recebidas por R.
- III - Sem que o endereçamento IP seja alterado, é possível adicionar 253 estações a essa rede.

SOMENTE está(ão) correta(s) a(s) afirmativa(s)

- (a). I
- (b). II
- (c). I e II
- (d). II e III
- (e). I, II e III

---

**Solução:**

A afirmativa I é incorreta. Como X e Y pertencem a mesma subrede, as requisições enviadas de X para Y não passarão por R. As requisições partindo de X ou Y só passarão por R caso sejam destinadas a alguma estação localizada em uma subrede diferente de 192.168.10.0/24.

A alternativa II é correta. As mensagens ARP Request (Address Resolution Protocol) tem por objetivo recuperar o endereço MAC de um outro elemento da rede, para o qual é conhecido o endereço IP. Em linhas gerais, quando Y precisa descobrir o endereço MAC de X, o processo é o seguinte:

- Y monta um pacote ARP Request com a pergunta “Quem tem o IP 192.168.10.100?”;
- Y envia o pacote para o endereço de broadcast FF:FF:FF:FF:FF:FF;
- todos os integrantes da subrede recebem o pacote ARP Request;
- ao receber o pacote, X verifica que é capaz de receber a pergunta;
- X monta um pacote ARP Response contendo seu endereço MAC e o envia diretamente a Y;
- Y recebe o ARP Response, e agora está preparado para montar o pacote e endereçá-lo com o MAC de X.

A alternativa III é incorreta. A subrede 192.168.10.0/24 contém 256 endereços. A faixa de endereçamento útil é de 192.168.10.1 até 192.168.10.254, já que os endereços 192.168.10.0 e 192.168.10.255 são os endereços de rede e de broadcast, respectivamente. Ou seja, a subrede em questão pode conter, no máximo, 254 elementos. Como X, Y e R já consumiram 3 desses endereços, podem ser adicionados, no máximo, mais 251 elementos a essa subrede.

3. **Assuntos relacionados:** *Gerenciamento de Identidades, Single Sign-On, Segurança da Informação,*

**Banca:** CESGRANRIO

**Instituição:** BNDES

**Cargo:** Analista de Suporte

**Ano:** 2008

**Questão:** 33

No âmbito de segurança, é INCORRETO afirmar que o single sign-on

- (a). permite que um usuário se autentique uma única vez para acessar múltiplos sistemas e aplicações.
- (b). é aplicável em sistemas WEB, mesmo que não se utilize certificação digital.
- (c). é implantado mais facilmente em ambientes de Infra-estrutura homogênea do que heterogênea.
- (d). reduz a complexidade da Infra-estrutura e dificulta ataques de força-bruta em senhas.
- (e). facilita a gerência e a administração centralizada de identidades.

---

**Solução:**

Single sign-on é um método de controle de acesso que habilita ao usuário a realizar o logon uma única vez e ganhar acesso a múltiplos recursos da rede sem a necessidade de se autenticar novamente. As soluções de single sign-on podem ser implementadas de várias formas, por exemplo, por meio do uso de smart cards, certificados digitais e kerberos.

Entre as principais vantagens das soluções de single sign-on estão a utilização de um método único de autenticação, o que acaba por facilitar a administração. Além disso, o single sign-on pode aumentar a produtividade e reduzir o número de problemas com a administração de senhas. A desvantagem mais clara do single sign-on refere-se a segurança das informações. Caso um atacante A venha a descobrir a senha de B, automaticamente ele terá acesso a todos os sistemas de B. Além disso, as soluções de single sign-on geralmente fazem uso de um repositório central de autenticação, o que representa um ponto único de falha e de invasão. Caso um atacante domine o repositório central, ele pode vir a comprometer a autenticação de todos os sistemas da rede.

Para contornar o problema de ponto único de falha, muitas organizações optam por implantar soluções de sincronismo de senhas, ao invés de soluções de single sign-on. Assim, os usuários precisam decorar apenas uma senha, mas continuam precisando digitá-las nos diversos sistemas da rede.

A complexidade da infraestrutura de soluções de single sign-on depende do ambiente em que se deseja realizar a implantação. Quanto maior o número de sistemas envolvidos e mais diversas forem as tecnologias, mais complexa será a implantação do single sign-on.

Além disso, em soluções de single sign-on e de sincronismo de senha, a complexidade da política de senhas geralmente é definida pelas capacidades do sistema menos restritivo. Ou seja, se um dos sistemas alvo do single sign-on só aceitar senhas alfanuméricas, a política de senha geral deverá comportar essa limitação, o que pode diminuir a segurança da rede como um todo.