CONHECIMENTOS ESPECÍFICOS

Julgue os itens a seguir, relacionados à instalação e configuração de servidores de *email*.

61 A macro Feature permite definir as características que serão utilizadas para a configuração de uma instalação do Sendmail.

62 Na configuração do Sendmail, o recurso `always_add_domain` tem a função de adicionar o nome do *host* local aos endereços de destino local que não sejam totalmente qualificados.

63 O `IP 127.x.x.x` estará autorizado a enviar mensagens para fora do ambiente local em que o Qmail estiver instalado, se a linha `127.:allow,RELAYCLIENT=""` for incluída no arquivo de configuração do Qmail.

64 A quantidade de tempo que o Procmail deverá ficar inativo, caso um recurso necessário não esteja disponível, pode ser configurada.

Acerca da instalação e configuração dos serviços e servidores JBOSS, Squid e LDAP, julgue os itens que se seguem.

65 Durante a configuração do LDAP, é necessário definir o `Root DN`, que é a parte do `Distinguished Name` que todos os objetos no diretório têm em comum.

66 O SquidGuard possibilita o bloqueio de acesso a páginas impróprias, a partir de listas formadas por URLs de páginas indesejáveis. Porém, uma vez instalado, o Squid deixará de funcionar se houver uma interrupção qualquer no funcionamento do SquidGuard.

67 Na pasta doc, pertencente à estrutura de pastas do JBOSS, está armazenada a documentação do próprio servidor, como o manual do usuário.

68 No Squid, se utilizada, a diretiva de configuração collapsed_forwarding faz que múltiplas requisições pela mesma URL sejam processadas como se fossem uma única requisição.

Julgue os próximos itens, relacionados à instalação e configuração de TCP/IP, NFS, NIS e DNS.

69 Na configuração do serviço NIS (*network information service*), é necessário que o nome do domínio NIS seja igual ao nome do domínio DNS.

70 Ao se instalar e configurar um DNS, é possível que um servidor dedicado que disponha de dois ou mais endereços IP assuma, ao mesmo tempo, os papéis de servidor DNS primário e secundário.

71 Os endereços definidos durante a configuração do TCP/IP são atribuídos a máquinas conectadas à rede, de forma que cada endereço localize uma máquina.

72 Em um NFS (*network file system*), é possível, por meio de configuração, negar direitos de acesso especiais aos superusuários de um *host*.

A respeito do IIS 6.0, julgue os itens subsecutivos.

73 Por padrão, a primeira página procurada pelo IIS é a `Index.asp`. Caso seja necessário, é possível configurá-lo para que ele passe a procurar por outra página.

74 O número de conexões no IIS é limitado a 1.000, por padrão, a fim de se evitar eventual sobrecarga na rede.

75 Ao instalar o IIS, é necessário que as permissões sejam ativadas manualmente para que o servidor possa executar páginas dinâmicas.

No que se refere a *terminal services*, no Windows 2000, julgue os itens seguintes.

76 Em computadores que fazem parte de uma estrutura de domínio, é possível instalar IPSec e configurar políticas como forma de otimizar a segurança nas comunicações do *terminal services*.

77 O modo de administração remota permite o gerenciamento do servidor a distância via rede, desde que seja utilizada uma conta membro do grupo administradores com licenciamento específico para esse fim.

78 O servidor de licença de domínio, modo padrão de instalação do *terminal services licensing* (TSL), deve ser usado quando se deseja manter um TSL para cada domínio.

Julgue os itens subsecutivos, referentes à instalação e configuração do Active Directory.

79 No Active Directory, a criação de contas de usuários, ou de grupos de usuários, e alterações nas contas de usuários ou políticas de segurança podem ser feitas em servidores-membros e automaticamente replicadas para todos os controladores de domínio.

80 Para que se possa instalar o Active Directory, é recomendado que haja um endereço IP dedicado.

Julgue os itens a seguir, relacionados ao serviço NFS do Unix.

81 Em um sistema de arquivos montado com a opção `intr`, quando o servidor sai do ar, as operações correspondentes a tentativas de acesso a esse servidor falham e, automaticamente, retornam mensagens de erro para o usuário.

82 Em servidores com o serviço NFS habilitado, os `deamons` denominados `mountd` e `nfsd` podem ter sua execução iniciada no momento em que acontece a inicialização do sistema e devem permanecer em execução enquanto o sistema estiver ativo.

83 O NFS adota o UDP como protocolo de transporte, em função dos algoritmos de controle de congestionamento que o UDP implementa e que são essenciais para um bom desempenho em uma rede IP de grande porte. Por esse mesmo motivo, não é possível utilizar TCP como protocolo de transporte no NFS.

84 O NFS exerce o controle sobre os identificadores de usuários e permissões de forma a impedir que um usuário seja capaz de acessar arquivos de outro usuário, sem que haja nenhum tipo de autorização explícita.

Julgue os itens que se seguem a respeito do uso compartilhado de impressoras em redes Windows Server 2003 e Unix.

85 Em uma rede Unix, quando existe mais de uma impressora conectada a uma mesma máquina, o servidor CUPS mantém uma única fila compartilhada pelas impressoras e gerencia a distribuição dos documentos que entram na fila de impressão.

86 Para fazer uso compartilhado de uma impressora física instalada em uma estação da rede, é necessário instalar o seu *software* de utilização em todas as estações que terão uso compartilhado.

87 Se um servidor de impressão for instalado em uma rede Windows Server 2003, as impressoras que forem gerenciadas por esse servidor ficarão, automaticamente, disponíveis para impressão a partir de qualquer estação dessa rede.

Em relação ao ambiente Windows Server 2003, julgue os próximos itens.

88 O Windows Server 2003 pode ser instalado em uma partição FAT ou NTFS.

89 Quando o Windows Server 2003 é instalado, a primeira conta a ser criada é a conta `Administrador` (ou `Administrator`). Essa conta não pode ser removida nem desativada.

90 O acesso remoto a servidores Windows Server 2003 pode ser feito por meio de rede local, mas, por uma questão de segurança, o acesso pela Internet é bloqueado.

91 Criado para empresas de médio a grande porte, o Windows Server 2003 Enterprise Edition pode oferecer suporte a até oito processadores.

92 O Windows Server 2003 Standard Edition fornece suporte para o compartilhamento de arquivos e impressoras e oferece conectividade segura com a Internet. Para a instalação desse sistema, a mínima capacidade de memória RAM recomendada é de 256 MB.

Julgue os itens subsequentes, a respeito do ambiente Unix.

93 Há várias ferramentas que podem ser adotadas para depurar problemas em uma rede de computadores, entre elas, o comando `traceroute <nomeDoHost>` revela a sequência de *gateways* que um pacote IP percorre para alcançar seu destino; todavia, o `<nomeDoHost>` deve ser especificado com um endereço IP.

94 O sistema operacional Unix permite que uma tarefa seja subdividida em vários processos que podem ser executados em (pseudo) paralelismo e realizar comunicação entre si.

95 O princípio básico do NFS, sistema de arquivos de rede usado pelo Unix, é permitir que um conjunto qualquer de clientes e servidores compartilhe um sistema de arquivos comum, mas, para que isso ocorra, é necessário que todos os clientes e servidores estejam na mesma LAN.

96 A característica que define uma conta `root` é o seu UID igual a 0. No Unix, há algumas chamadas de sistemas que tradicionalmente somente podem ser executadas pelo superusuário, por exemplo, modificação do diretório-raiz de um processo com `chroot`.

97 O comando `netstat` coleta informações sobre o estado do *software* de rede do computador em que esse *software* esteja instalado, inclusive estatísticas de interface, informações de roteamento e tabelas de conexão.

Em relação à instalação e ao suporte dos protocolos TCP/IP e DHCP no ambiente Windows Server 2003, julgue os itens de **98** a **101**.

98 No Windows Server 2003, na guia de Configurações Avançadas do servidor DHCP, é possível definir o número de tentativas de detecção de conflitos de endereço IP que o servidor DHCP deve realizar antes de conceder um endereço IP para um cliente. Por padrão, essa opção é habilitada em uma tentativa.

99 No DHCP, a duração de concessão especifica por quanto tempo um cliente pode usar um endereço IP. No Windows Server 2003, o tempo máximo a ser configurado para uma concessão DHCP é de 24 horas.

100 No Windows Server 2003, para se configurar o protocolo TCP/IP, é correto seguir o seguinte procedimento: abrir o Painel de Controle e aplicar um duplo clique no ícone Redes. Para realizar essa tarefa, deve-se clicar, sucessivamente: no *menu* Iniciar, Configurações, Painel de Controle e Redes. Na guia Configurações, deve-se clicar sobre o ícone do protocolo TCP/IP que estiver vinculado à placa de rede e, em seguida, clicar o botão Propriedades.

101 No Windows Server 2003, para se configurar o protocolo TCP/IP, deve-se informar o número IP destinado à estação que estiver sendo configurada e, obrigatoriamente, o número IP do roteador padrão.

Julgue os itens que se seguem, referentes à instalação e ao suporte dos protocolos DNS e FTP no ambiente Windows Server 2003.

102 No console do DNS, a partir do Windows Server 2003, é possível realizar as três seguintes tarefas: visualizar o *log* de eventos; criar, remover ou editar zonas de pesquisa direta; e criar, remover ou editar zonas de pesquisa inversa.

103 No Windows Server 2003, ao se configurar um servidor de transferência de arquivos (FTP), é possível configurar a descrição do sítio, o endereço IP a ser atribuído ao FTP, o número de conexões simultâneas a serem permitidas e a habilitação de um arquivo de *log*. Todavia, não é possível configurar a porta TCP, pois a porta 21 já é predefinida por *default* para esse serviço.

104 Por questão de segurança, no Windows Server 2003, não é possível configurar conexões anônimas ao FTP.

105 Ajustes finos e alterações na configuração do DNS, no Windows Server 2003, podem ser feitos a partir do *menu* Iniciar, clicando-se, sucessivamente, as opções Ferramentas de Sistema e DNS, ou a partir da Central de Controle do Windows Server 2003, na opção Gerenciar este Servidor DNS.

Um administrador de redes deve elaborar um relatório com indicações de possíveis soluções a serem adquiridas por sua empresa, visando modernizar a tecnologia de armazenamento de dados.

Tendo como referência o texto acima, julgue os itens seguintes, a respeito dos conceitos de NAS (*network attached storage*) e SAN (*storage area network*).

106 A solução de *storage* SAS é mais simples que a solução NAS, uma vez que sua implementação ocorre em redes já existentes.

107 Se a velocidade de acesso aos dados for um requisito primordial para a empresa, é correto que, em seu relatório, o administrador aponte como solução ideal que os dispositivos de armazenamento sejam conectados à rede NAS.

108 Em caso de necessidade de autorizar acesso a um conjunto de arquivos na rede por vários computadores, o relatório deve apontar a solução SAN.

109 Considere que, no atendimento dos usuários da rede em apreço, seja necessário um serviço de armazenamento cuja formatação, particionamento e distribuição dos dados nos discos lógicos criados no *storage* sejam de responsabilidade do sistema de gerência da infraestrutura de armazenamento. Nesse caso, para atender a essa exigência, o administrador deverá propor, em seu relatório, a solução de armazenamento SAN.

Com referência às características das arquiteturas RISC e Intel, julgue os itens que se seguem.

110 Na arquitetura Intel, para aumentar o desempenho do processador, todas as instruções usam endereçamento imediato ou de modo registrador, exceto as que endereçam memória.

111 Na arquitetura RISC, os processadores são projetados com um número elevado de registradores, pois a grande maioria das operações é do tipo registrador-registrador.

112 Um computador com a arquitetura RISC trabalha com instruções de formato simples, as quais são executadas por microcódigo.

Julgue os itens seguintes, relativos a *firewalls* e sistemas de detecção de intrusão.

113 Detecção por assinatura de tráfego é a abordagem comum em sistemas de detecção de intrusão embasados em rede.

114 Em *firewalls*, com ou sem inspeção de estado, para todos os pacotes, a decisão de encaminhamento é tomada por meio da verificação de cada pacote contra cada uma das regras de filtragem.

115 A tabela de estados contém informações sobre os fluxos de pacotes já validados pelo conjunto das regras; no entanto, a aplicação desse tipo de tabela restringe-se aos protocolos orientados a conexão.

116 A utilização de *firewalls* de camada de rede é efetiva para evitar ataques dos tipos SQL *injection* e *buffer overflow*.

117 Duas abordagens utilizadas em sistemas de detecção de intrusão embasados em *host* são a verificação de integridade e heurísticas para a detecção de comportamento anômalo.

Com relação à criptografia e suas aplicações, julgue os itens de **118** a **122**.

118 Alto nível de segurança das mensagens que trafegam em uma VPN é obtido pela cifração dessas mensagens, sem a necessidade de mecanismos de garantia de integridade.

119 A criptografia simétrica difere da assimétrica por utilizar uma chave compartilhada entre as partes, que é usada tanto na cifração, quanto na decifração.

120 VPNs são aplicações comuns de criptografia no contexto de redes de computadores, devendo incluir a autenticação das partes envolvidas, bem como o sigilo das mensagens em trânsito.

121 Uma assinatura digital consiste na cifração do resumo criptográfico de um arquivo digital com uma chave pública.

122 Um certificado digital consiste na cifração do resumo criptográfico de uma chave pública com a chave privada de uma autoridade certificadora.

Acerca de gestão de risco segundo o NIST SP 800-30, julgue os itens subsequentes.

123 Controles preventivos alertam sobre a ocorrência de violações.

124 A identificação de ameaças visa produzir a lista das vulnerabilidades que são potencialmente exploráveis.

125 Mecanismos de controle de acesso, identificação e autenticação são exemplos de controles técnicos.

126 Controles gerenciais e operacionais caracterizam os controles não técnicos.

Julgue os itens a seguir, relativos à segurança da informação.

127 O tratamento da informação refere-se a recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle tanto da informação sigilosa quanto da informação não sigilosa.

128 Gestão de segurança da informação é o conjunto de ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

129 A ocorrência de quebra de segurança restringe-se à ação ou omissão estritamente intencional que resulte no comprometimento da segurança da informação e das comunicações.

130 Confidencialidade requer que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.