

Respostas aos Recursos 0013 - ANALISTA DE TECNOLOGIA DE INFORMAÇÃO

Questão	Justificativa	Conclusão (Deferido ou Indeferido)	Resposta alterada para:
Questão 32- 1 Questão 50- 2 Questão 37- 3 Questão 42- 4	<p>Após a análise da questão, esta Banca entendeu por anular o gabarito oficial, pelos motivos apresentados abaixo:</p> <p>A questão não especificou o tipo de Cluster de Balanceamento de Carga.</p> <p>Os clusters podem ser classificados em: ■ Clusters de alta disponibilidade (High Availability – HA): os clusters de alta disponibilidade endereçam redundância com capacidade de failover automático. ■ Clusters de balanceamento de carga (Load Balancing – LB): os clusters do tipo load balancing endereçam a melhoria da capacidade para a execução da carga de trabalho (WORKLOAD). ■ Clusters de alta performance (HPC e HTC): os clusters do tipo alta performance endereçam o aumento da performance da aplicação.</p> <p>A escolha da tecnologia de cluster HA ou LB depende se os aplicativos a serem executados possuem estado de execução demorada na memória. As diferenças entre os dois tipos de clusters são que: ■ O cluster HA destina-se aos aplicativos que têm estado de execução demorada na memória ou que têm estados de dados frequentemente atualizados. Esses são denominados aplicativos com monitoração de estado e incluem aplicativos de bancos de dados e aplicativos de mensagens. A utilização típica dos clusters de failover inclui servidores de arquivos, servidores de impressão, servidores de bancos de dados e servidores de mensagens. ■ O cluster LB destina-se aos aplicativos que não têm estado de execução demorada na memória. Esses são denominados aplicativos sem monitoração de estado. Um aplicativo sem monitoração de estado trata cada solicitação do cliente como uma operação independente e, portanto, pode balancear a carga de cada solicitação de forma independente. Em geral, os aplicativos sem monitoração de estado possuem dados somente de leitura ou dados frequentemente alterados. Servidores web, VPNs, servidores FTP, firewalls e servidores proxy costumam usar o cluster LB.</p>	DEFERIDO	ANULADA

	<p>FONTE: https://www.sistemas24horas.com.br/aulas/files_semi2018/Computacao-nas-nuvens-Manoel%20Veras%20-%20Cloud%20Computing%20-%20Nova%20Arquitetura%20da%20TI.pdf</p> <p>Diante do exposto, defere-se o presente recurso, questão anulada.</p>		
<p>Questão 36- 1</p> <p>Questão 43- 2</p> <p>Questão 32- 3</p> <p>Questão 38- 4</p>	<p>Após a análise da questão, esta Banca entendeu por manter o gabarito oficial, pelos motivos apresentados abaixo:</p> <p>Questão elaborada conforme o item “Cabeamento estruturado categorias 5, 5e, 6 e 6ª; redes sem fio (wireless): padrões IEEE 802.11b/g/n, IEEE 802.1x.”, do Conteúdo Programático divulgado no Edital.</p> <p>Cat 5E A Categoria 5E é compatível com uma gama de frequências de, no máximo, 100 MHz e está desenhada para velocidades de transmissão até, no máximo, 1 gigabit por segundo (Gigabit Ethernet).</p> <p>Cat 6 A Categoria 6 é compatível com uma gama de frequências de, no máximo, 250 MHz e está desenhada para velocidades de transmissão até, no máximo, 1 gigabit por segundo (Gigabit Ethernet). Os cabos Cat 6 proporcionam um desempenho melhorado e confiabilidade na transmissão, especialmente em relação ao protocolos 1000BaseT e 1000BaseTX.</p> <p>Cat 6A Um cabo de dados de muito alto desempenho concebido para velocidades de transmissão de até 10 GB por segundo. Desenvolvido especialmente a pensar no novo protocolo de Ethernet 10GBaseT. A Categoria 6a disponibiliza uma largura de banda de 500 MHz, sendo, portanto, indicada para as aplicações mais exigentes ao nível de dados utilizadas em redes informáticas de condutores metálicos.</p> <p>Cat 7 Os cabos da Categoria 7 são cabos de dados de muito alto desempenho concebidos para velocidades de transmissão até, no máximo, 10 GB por segundo ao longo de 100 m, e com capacidade para gamas de frequências até, no máximo, 600 MHz. São retrocompatíveis com as</p>	INDEFERIDO	

	<p>categorias Cat 5e, Cat 6 e Cat 6a, e possuem blindagem individual global de forma a cumprirem requisitos exigentes em matéria de diafonia.</p> <p>FONTE: https://www.elandcables.com/pt/cables/lan-cat-5e-6-6a-cable</p> <p>Diante do exposto, indefere-se o presente recurso.</p>		
<p>Questão 43 – 1</p> <p>Questão 49 – 2</p> <p>Questão 44 – 3</p> <p>Questão 35 – 4</p>	<p>Após a análise da questão, esta Banca entendeu por manter o gabarito oficial, pelos motivos apresentados abaixo:</p> <p>Questão elaborada conforme o item “Banco de Dados NoSQL.”, do Conteúdo Programático divulgado no Edital.</p> <p>FONTE:</p> <p>Diante do exposto, indefere-se o presente recurso.</p>	INDEFERIDO	
<p>Questão 47- 1</p> <p>Questão 33- 2</p> <p>Questão 34- 3</p> <p>Questão 36- 4</p>	<p>Após a análise da questão, esta Banca entendeu por anular o gabarito oficial, pelos motivos apresentados abaixo:</p> <p>As alternativas “b” e “c” estão corretas.</p> <p>Na representação de um endereço IPv6, é permitido utilizar tanto caracteres maiúsculos quanto minúsculos.</p> <p>Além disso, regras de abreviação podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos. É permitido omitir os zeros a esquerda de cada bloco de 16 bits, além de substituir uma sequência longa de zeros por “::”.</p> <p>Por exemplo, o endereço 2001:0DB8:0000:0000:130F:0000:0000:140B pode ser escrito como 2001:DB8:0:0:130F::140B ou 2001:DB8::130F:0:0:140B. Neste exemplo é possível observar que a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrário poderá haver ambigüidades na representação do endereço.</p> <p>FONTE: https://ipv6.br/post/enderecamento/</p> <p>Diante do exposto, defere-se o presente recurso, questão anulada.</p>	DEFERIDO	ANULADA

Questão 48 – 1	Após a análise da questão, esta Banca entendeu por manter o gabarito oficial, pelos motivos apresentados abaixo:	INDEFERIDO	
Questão 47 – 2	Um IDS passivo é projetado para detectar ameaças e informar ao administrador da rede sobre a atividade maliciosa detectada. O sistema de prevenção de intrusão (em inglês, <i>Intrusion Prevention System</i> - IPS), por outro lado, representa o comportamento de um IDS ativo, ou seja, é projetado com o objetivo de bloquear automaticamente a atividade maliciosa, seja por configuração de <i>firewalls</i> e comutadores ou outras técnicas, como encerramento de conexão via envio de pacotes <i>reset</i> .		
Questão 41 – 3			
Questão 45 – 4	<p>FONTE: https://www.gta.ufri.br/grad/16_2/2016IDS/conceituacao.html</p> <p>Diante do exposto, indefere-se o presente recurso.</p>		
Questão 49- 1	Após a análise da questão, esta Banca entendeu por manter o gabarito oficial, pelos motivos apresentados abaixo:	INDEFERIDO	
Questão 32- 2	A afirmação da alternativa “E” não está correta:		
Questão 40- 3	Uma outra medida preventiva é utilizar um firewall pessoal, pois alguns firewalls podem bloquear o recebimento de programas spyware. Além disso, se bem configurado, o firewall pode bloquear o envio de informações coletadas por estes programas para terceiros, de forma a amenizar o impacto da possível instalação de um programa spyware em um computador		
Questão 39- 4	<p>FONTE: https://www.inf.ufsc.br/~bosco.sobral/ensino/ine5630/material-seg-redes/cartilha-08-malware.pdf</p> <p>Diante do exposto, indefere-se o presente recurso.</p>		