cespeUnB

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

MINISTÉRIO DAS COMUNICAÇÕES
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES
(ANATEL)

CARGO 6: ANALISTA ADMINISTRATIVO – ESPECIALIDADE: SUPORTE E INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

PROVA DISCURSIVA
DISSERTAÇÃO

APLICAÇÃO: 14/9/2014

PADRÃO DE RESPOSTA

Espera-se que o candidato redija texto dissertativo acerca das soluções e ferramentas agregadas ao Microsoft Sql Server 2012 e voltadas para alta disponibilidade e BI, desenvolvendo os tópicos especifidacos.

***Analysis services*: objetivos e abordagens de BI (tabular, multidimensional e PowerPivot)**

Objetivo: oferecer soluções para criar e implantar bancos de dados analíticos usados para apoio à decisão.

Soluções tabulares usam construções de modelagem relacionais como tabelas e relações para modelar dados. Soluções multidimensionais e de mineração de dados usam construções de modelagem OLAP (cubos e dimensões) e armazenamento MOLAP, ROLAP ou HOLAP. O PowerPivot é uma solução de BI de autoatendimento que permite que os analistas de negócios criem um modelo de dados analíticos dentro de uma pasta de trabalho do Excel, utilizando o suplemento PowerPivot para Excel.

***Data Mining* (SSAS): objetivos e recursos integrados**

Objetivo: descobrir, por meio de princípios estatísticos pesquisados, padrões em seus dados, ajudando-o a tomar decisões inteligentes sobre problemas complexos.

Recursos integrados:

- várias fontes de dados: possibilidade de utilização de dados tabulares de provedores externos, planilhas e arquivos de texto;
- limpeza de dados integrada, gerenciamento de dados e ETL;
- algoritmos personalizáveis: além de algoritmos como *clustering*, redes neurais e árvores de decisões, a plataforma oferece suporte ao desenvolvimento de seus próprios algoritmos de *plug-in* personalizados;
- infraestrutura de testes de modelo: teste seus modelos e conjuntos de dados;
- consulta e detalhamento: crie consultas de previsão, recupere padrões modelo e estatísticas e detalhe os dados de caso;
- suporte a linguagem de *scripts* e API gerenciada: gerar *scripts* é possível por meio do MDX, XMLA ou as extensões de PowerShell para o *analysis services*;
- segurança e implantação: fornece segurança baseada em função por meio do *analysis services*;

***AlwaysOn availability groups:* objetivos e componentes**

Objetivos: fornecer alternativa em nível corporativo para espelhamento de banco de dados. Um grupo de disponibilidade oferece suporte a um ambiente de *failover* para um conjunto discreto de bancos de dados de usuário, conhecidos como bancos de dados de disponibilidade, que fazem *failover* juntos.

Componentes:

- réplica de disponibilidade – instanciação de um grupo de disponibilidade que é hospedado por uma instância específica do SQL Server e que mantém uma cópia local de cada banco de dados de disponibilidade pertencente ao grupo de disponibilidade;
- *failover* – as funções primária e secundária das réplicas de disponibilidade, normalmente, são intercambiáveis em um processo conhecido como *failover*. Durante o *failover*, o destino de *failover* assume a função primária, recupera seus bancos de dados e os coloca *online* como os novos bancos de dados primários. Existem três formas de *failover*: *failover* automático (sem perda de dados),

failover manual planejado (sem perda de dados) e failover manual forçado (com possível perda de dados), geralmente chamado de *failover* forçado;

- reparo automático de página (grupos de disponibilidade/espelhamento de banco de dados). Depois que certos tipos de erros corrompem uma página, tornando-a ilegível, um parceiro de espelhamento de banco de dados (entidade de segurança ou espelho) ou uma réplica de disponibilidade (primária ou secundária) tenta recuperar a página automaticamente.

***Log shipping e failover cluster instances*: objetivos e principais características**

Objetivos e características do *log shipping*: o envio de logs do SQL Server permite o envio automático de backups do *log* de transações de um banco de dados primário em uma instância do servidor primário para um ou mais bancos de dados secundários em outras instâncias de servidor secundário.

Objetivos e características do *failover cluster instances*: as instâncias de *cluster* de *failover* do *AlwaysOn* aproveitam a funcionalidade WSFC (*windows server failover clustering*) para fornecer alta disponibilidade local por meio de redundância na instância de nível de servidor, uma FCI (*instância de cluster de failover*) proporciona *failover* de um nó do WSFC para outro se o nó atual se tornar indisponível.

cespeUnB

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

MINISTÉRIO DAS COMUNICAÇÕES
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES
(ANATEL)

CARGO 6: ANALISTA ADMINISTRATIVO – ESPECIALIDADE: SUPORTE E INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

PROVA DISCURSIVA
QUESTÃO 1

APLICAÇÃO: 14/9/2014

PADRÃO DE RESPOSTA

Espera-se que o candidato redija texto dissertativo acerca do gerenciamento de processos no ambiente Linux, conforme as seguintes especificações.

Conceito de processo e mecanismo de envio de sinais para um processo com o comando `kill`

Processo são programas ou aplicações que estão carregados em memória para atender alguma demanda. Os processos podem, ou não, estar em estado de execução, pois um processo apresenta diferentes estados, variando de acordo com a demanda do sistema operacional ou do administrador do ambiente que pode enviar sinais modificando o seu estado.

Para enviar sinais que modifiquem o estado do processo, podem ser utilizados utilitários como o comando `kill`. Esse comando pode enviar sinais para um processo reiniciar, entrar em modo de espera, fechar abruptamente, entre outros sinais.

Exemplo do comando `kill`: `kill -9 <número do processo>` ou `kill –HUP <número do processo>`

Três estados do processo ativos no sistema operacional Linux

R = em execução
S = em espera ou *sleep*
s = líder de sessão, possui subprocessos associados a ele
D = em espera aguarda operações de entrada e saída por outro dispositivo
T = parado ou em modo trace
W = realizando paginação de memória
X = Acabou de morrer (terminou)
Z = *zombie* ou recebeu comando para morrer e está morrendo, porém ainda possui recursos em memória
< = rodando em alta prioridade
N = rodando em baixa prioridade

Funções dos comandos *`ps`*, *`nice`* e *`renice`*.

O comando `ps` consegue exibir informações dos processos em memória; exemplo de comando: `ps ax` = consegue mostrar todos os processos do sistema operacional, com os respectivos estados.

O comando `nice` modifica a prioridade do processo no momento que ele for iniciado; exemplo do comando: `nice -10` comando/programa.

O comando `renice` modifica a prioridade do processo durante a sua execução; exemplo do comando: `renice – 10 PID` (*process identification*).

cespeUnB

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

MINISTÉRIO DAS COMUNICAÇÕES
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES
(ANATEL)

CARGO 6: ANALISTA ADMINISTRATIVO – ESPECIALIDADE: SUPORTE E INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

PROVA DISCURSIVA
QUESTÃO 2

APLICAÇÃO: 14/9/2014

PADRÃO DE RESPOSTA

Espera-se que o candidato discorra sobre os ataques DDoS, abordando, necessariamente, os aspectos a seguir especificados.

Características dos principais tipos de ataques DDoS, seus modos de operação e tendências

DDoS: ataques através da rede lançados simultaneamente de vários pontos, com objetivo de exaurir os recursos, aplicações ou serviços de rede de uma organização, e, assim, impedir que os usuários legítimos acessem os recursos de interesse.

Principais tipos: ataques volumétricos, que produzem grandes quantidades de dados e consomem a banda disponível da rede/serviço alvo ou congestionam as vias de comunicação com o restante da Internet; ataques de exaustão das conexões TCP, que consomem as tabelas de estados de conexão presentes em componentes da infraestrutura como balanceadores, *firewalls* e servidores; e, os ataques de camada de aplicação, que exploram aspectos das aplicações e serviços para obstruir a comunicação. Esses ataques são perigosos porque podem ser efetivos com poucas máquinas e taxas de tráfego não muito altas. Hoje são comuns e a tendência é que sigam em aperfeiçoamento para se confundirem mais e mais com tráfego legítimo, dificultando sua detecção e mitigação.

Ações de governança, medidas, procedimentos e soluções técnicas que reduzem o impacto de tentativas de ataques DDoS e evitam a indisponibilidade dos serviços da organização na Internet

Em termos de governança, é importante: conhecer a própria rede, os tráfegos normais e típicos; estabelecer parcerias para cooperação com operadoras, consultores experientes e “vizinhos” potencialmente afetáveis; mapear o que deve ser feito em casos de ataques, prevendo-se os possíveis cenários, e incluindo-se o que deve e o que não deve ser bloqueado, em considerações funcional e política. Um plano de operação sem Internet é desejável. Tecnicamente, é importante que haja acessos redundantes à Internet, de fornecedores diferentes, e cujos contratos incluam apoio em caso de DDoS. O monitoramento do tráfego deve ocorrer em tempo integral, com alertas em alterações nos patamares predefinidos. Deve-se investir em equipamentos de monitoração que “entendam” os ataques e encaminhem medidas automáticas como bloqueios e interceptação de tráfego ruim, desvios e balanceamento entre canais.

cespeUnB

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

MINISTÉRIO DAS COMUNICAÇÕES
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES
(ANATEL)

CARGO 6: ANALISTA ADMINISTRATIVO – ESPECIALIDADE: SUPORTE E INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

PROVA DISCURSIVA
QUESTÃO 3

APLICAÇÃO: 14/9/2014

PADRÃO DE RESPOSTA

Espera-se que o candidato discorra sobre a tecnologia VoIP, abordando, necessariamente, os aspectos a seguir especificados.

Regulamentação pela ANATEL da tecnologia VoIP

O provimento do VoIP pode ocorrer de duas formas distintas: serviço de valor adicionado (art. 61, LGT) ou serviço de telecomunicações (art. 60, LGT). Fornecendo a infraestrutura e a respectiva capacidade de transmissão e recepção de informações ao usuário, a provedora de VoIP estará prestando um serviço de telecomunicações e precisará de uma autorização prévia da Anatel. Por outro lado, um usuário de um serviço de telecomunicações — como banda larga ADSL, *Cable Modem* e 3G — pode contratar uma provedora de VoIP, o que será caracterizado como serviço de valor adicionado.

Ameaças e vulnerabilidades em VoIP (citação de dois exemplos)

A infraestrutura que implementa VoIP é suscetível a diferentes tipos de ataques, entre eles: DDoS (*distributed deny of service*), SIP Flooding, SIP Sinalling Loop (repetição de sinalizações SIP), VoIP Packet Replay Attack (ataque de resposta de pacotes VoIP), QoS Modification Attack (ataque de modificação de QoS), VoIP Packet Injection (injeção de pacotes VoIP), Faked Call Teardown Message (fraude de mensagem de término de chamada).