Para que um cliente envie mensagens a um servidor, primeiro o cliente, deve necessariamente conhecer o endereço do servidor, desse modo, é preciso estabelecer um esquema de identificação. Quais são esses mecanismos?

I - Identificador único de processo quando na mesma máquina;

II - Endereçamento indicando o processo e a máquina;

III - Processos escolhem endereços que são detectados por broadcast

IV - Uso de DNS.Opção única.

Somente a I esta correta.

1. Somente I e II estão corretas.
2. Somente I, II e III estão corretas.
3. Todas estão corretas.
4. Nenhuma esta correta.

Tolerância a falha é uma questão importante no projeto de sistemas distribuídos; é definida como a característica:Opção única.

A) Pela qual um sistema pode mascarar a ocorrência e a recuperação de falhas somente quando os servidores estiverem disponíveis.

B) Pela qual um sistema chama imediatamente o suporte a fim de garantir a sua integridade física.

C) Pela qual um sistema monocamada garante o seu funcionamento durante 6 dias da semana.

D) Pela qual um sistema pode mascarar a ocorrência e a recuperação de falhas. Um sistema é tolerante a falha se puder continuar a funcionar na presença de falhas.

E) Pela qual um sistema utilizando terminais burros com processamento local garante o seu funcionamento 24 horas por dia durante os sete dias da semana, ou seja, o sistema jamais ficará fora do ar.

Em sistemas distribuídos a segurança desempenha um papel de extrema importância.

Sobre as afirmativas é possível afirmar:

I - Deve oferecer facilidades para estabelecer canais seguros entre processos. Um canal seguro fornece os meios para autenticar mutuamente as partes comunicantes e proteger mensagens contra modificação durante sua transmissão. De modo geral, um canal seguro também oferece confidencialidade, de maneira que ninguém, exceto as partes comunicantes, podem ler as mensagens que passam pelo canal.

II - A autorização trata de proteger recursos de modo tal que somente processos que tenham os direitos de acesso adequados possam realmente acessar e usar esses recursos. O controle de acesso sempre ocorre depois que um processo foi autenticado. Relacionada com o controle de acesso está a prevenção contra o ataque de recusa de serviço, que é um problema difícil para sistemas que são acessíveis pela Internet.

III - O gerenciamento de chaves inclui a distribuição de chaves criptográficas na qual os certificados emitidos por terceiros de confiança desempenham papel importante. Um aspecto relevante em relação ao gerenciamento de autorização são os certificados de atributo e delegação.

Qual das alternativas é verdadeira?

A) Somente os itens I e II são verdadeiros.

B) Somente os itens II e III são verdadeiros.

C) Somente os itens I e III são verdadeiros.

D) Os itens I, II e III são falsos.

E) Os itens I, II e III são verdadeiros.

Tolerância à falha é uma questão importante no projeto de sistemas distribuídos. Definida como a característica pela qual um sistema pode mascarar a ocorrência e a recuperação de falhas. Em outras palavras, um sistema é tolerante a falha se puder continuar a funcionar na presença de falhas. Existem vários tipos de falhas. Uma falha por queda ocorre quando um processo simplesmente para. Uma falha por omissão ocorre quando um processo não responde a requisições que chegam. Quando um processo responde muito cedo ou muito tarde a uma requisição, diz-se que ele exibe uma falha de temporização. Responder a uma requisição que chega, mas do modo errado, é um exemplo de uma falha de resposta. As falhas mais difíceis de tratar são aquelas em que um processo exibe qualquer tipo de falha, denominadas falhas arbitrárias ou bizantinas. Qual a técnica utilizada para contornar uma falha em um ambiente distribuído?

A) Redundância.

B) Confiabilidade.

C) Tolerância.

D) Disponibilidade.

E) Comunicação.

POSCOMP 2004 - Os tipos mais comuns de defeitos em sistemas distribuídos provocados por falhas físicas de componentes ou interferência eletromagnética são:

A) Perda de arquivos, colapso de servidores, captura de senhas.

B) Captura de senhas, sobrecarga de servidores, mensagens duplicadas.

C) Perda de mensagens, mensagens com vírus e mensagens órfãs.

D) Colapso de servidores, queda do enlace e perda de mensagens.

E) Páginas web com endereço errado, spam e mensagens duplicadas.

Sabemos que computadores e sistemas falham! Não é uma questão de SE eles vão falhar, mas de QUANDO! Em um falha, um computador pode devolver um resultado errado, mas, em geral, eles param antes de dar a resposta; num SD, falhas são parciais: outros componentes continuam funcionando; quais são as técnicas que podem ser usadas no tratamento desse tipo de ocorrência?

A) Resolução de falhas, mascaramento de falhas, tolerar falhas, recuperação de falhas e redundância.

B) Detecção de falhas, mascaramento de falhas, recuperação de falhas e redundância.

C) Detecção de falhas, mascaramento de falhas, tolerar falhas e recuperação de falhas.

D) Detecção de falhas, mascaramento de falhas, tolerar falhas, recuperação de falhas e redundância.

E) Detecção de falhas, mascaramento de falhas, tolerar falhas, recuperação de falhas e concordãncia.

Petrobras 2012 - Um cluster tolerante à falha assegura que todos os recursos de um sistema estão sempre disponíveis. A função de trocar aplicações e recursos de armazenamento de dados de um sistema que falhou para um sistema alternativo do cluster é denominada

A) Autorestore.

B) Autorecover.

C) Failoff.

D) Failback.

E) Failover.

Universidade Federal Fronteira Sul - Considere o seguinte conjunto de informações a respeito de conceitos de segurança em sistemas distribuídos:

1 - A assinatura digital garante as propriedades de autenticidade, integridade e confidencialidade;

2 - Uma assinatura digital é gerada usando a chave pública para cifrar o resumo digital (hash) do documento a ser assinado;

3 - O protocolo SSL usa criptografia de chave assimétrica para estabelecer uma sessão de comunicação com a criptografia de chave simétrica;

4 - A propriedade de confidencialidade garante que os usuários do sistema só podem ler informações para as quais estejam autorizados.

Assinale a alternativa correta:

A) Somente a alternativa 1 é correta.

B) Somente as alternativas 1 e 2 são corretas.

C) Somente as alternativas 3 e 4 são corretas.

D) Somente as alternativas 1, 3 e 4 são corretas.

E) Somente as alternativas 2, 3 e 4 são corretas.

Como o DNS resolve o problema da ‘disponibilidade’?

Como é resolvido o problema de atualização dos IPs dinâmicos quando usados com um servidor de DNS?

O que é paravirtualização?

Qual a diferença entre ‘emulação’ e ‘virtualização nativa’?

O que é um hypervisor bare metal?

O que é VDI (Vitual Desktop Infrastructure)?

O que é uma ACL em um sistema de arquivos?

O que é SSO? Quais vantagens ele apresenta?

O que é uma CA em um certificado digital?

Quais os dois modos de fazer a verificação de revogação de um certificado?

O que é virtualização de aplicação?

Quais as vantagens de uma máquina virtual sobre um container?

Descreva o funcionamento da estrutura de resolução de nomes de computadores na internet.

Descreva os seguintes termos relacionados à tolerância à falhas:

Disponibilidade, Confiabilidade, MTTF, MTTR, MTBF, ‘quantidade de noves’

SSDs são vendidos com uma medida de durabilidade em TBW. Considerando um uso moderado de um computador em que são gravados 30GB por dia no SSD (contando arquivo de paginação, ...), quanto tempo um SSD de 256GB com 100 TBW de durabilidade deve durar?