

CAIO YAGO VILELA

F00JED-7

SISTEMAS DISTRIBUÍDOS

LIMEIRA - SP

2022

1.

Um sistema distribuído é aquele no qual os componentes de hardware ou software, localizados em computadores interligados em rede, comunicam-se e coordenam suas ações enviando mensagens entre si.

2.

Vantagens: Segurança: A vantagem dos sistemas centralizados é que eles possuem um único host que fornece um alto grau de segurança, concorrência e controle de cópias de segurança e recuperação. Dados: Todos os dados ficam centralizados em um único host. Desvantagem: Desempenho: O host em que o banco de dados está localizado pode ainda criar um "gargalo" (diz que um elemento é o gargalo quando limita o desempenho do sistema), dependendo da quantidade de acessos simultâneos. Disponibilidade: Podem acontecer também problemas de disponibilidade dos dados, se o host, onde os dados estão armazenados, sair do ar.

3.

Sistema de computação: São vários computadores com o mesmo objetivo trabalhando juntos, podem estar na mesma sala ou no mesmo prédio (sendo conectados por um software), compartilha recursos, comunicação por padrões

Sistema de informação: é um conjunto de processos concorrentes acessando recursos distribuídos, os quais podem ser compartilhados ou replicados, através de troca de mensagens em um ambiente de rede. O objetivo é parecer que a aplicação está sendo usada em um único sistema.

Sistema pervasivo: Obtém de ausência geral de controle administrativo humano, entre dezenas a centenas de milhares de nós relativamente pequenos, e cada sensor processa e armazena dados (comparado à banco de dados distribuídos), pode ser integrado por diversos tipos de dispositivos e não somente computadores

4.

Compartilhamento de recursos: Em nosso ambiente, teremos vários computadores e softwares trocando informações entre si e se faz necessário esse compartilhamento de informações, assim geramos mais economia em recursos.

Concorrência: É necessário que o acesso concorrente ocorra normalmente nos sistemas distribuídos, já que podem existir várias requisições de diferentes máquinas para o mesmo arquivo e/ou recurso.

Escalabilidade: Por mais que no início o sistema distribuído possa ser projetado para um ambiente pequeno, não devemos descartarmos a possibilidade de expandirmos no futuro. Pensando em um ambiente de fácil escalabilidade, pode-se gerar economias muito grandes em tempo e gastos com novos hardwares.

Tolerância a falhas: Quando acontece uma falha no sistema, todo o ambiente que está em produção NÃO deve parar e não deve afetar os demais componentes.

Transparência: A questão da transparência é deixar o usuário enxergar apenas uma única interface, ver todo o sistema como um todo.

Tudo o que acontece por trás, todas as requisições, todas as falhas, devem se manter ocultas da visão do usuário final.

5.

Como característica fundamental um sistema distribuído deve ser notado como um só sistema íntegro e robusto. Ele não deve ser percebido de forma segmentada, por uma ótica dos usuários e desenvolvedores. E uma forma de mensurar o sucesso desse sistema distribuído é dada pela sua transparência. O sistema distribuído ideal deve fornecer basicamente oito formas de transparência.

Acesso: permite o acesso a componentes remotos e locais através das mesmas operações.

Localização: permite o acesso a componentes sem conhecimento da sua localização física. Caracteriza-se pela existência de um mecanismo que determina a localização baseada em um nome.

Concorrência: permite a execução concorrente de múltiplas operações sobre o mesmo conjunto de recursos sem causar interferência entre elas.

Escala: permite a expansão do sistema e de suas aplicações sem exigir mudanças significativas na infraestrutura existente.

Migração: permite a realocação de recursos e aplicações sem afetar o seu uso.

Replicação: o usuário desconhece a existência de várias cópias de recurso, fundamental para desempenho e tolerância a falhas.

Falhas: a presença de falhas no sistema não é percebida pelos usuários. Implica na ausência de um ponto único de falha.

Desempenho: recursos adicionais são adicionados para suprir a nova demanda.

6.

O modelo cliente – servidor é usado para fornecer serviços em uma rede de computadores, como por exemplo e-mail, servidor de arquivos, web entre outros, quando um cliente faz uma solicitação ao servidor, o servidor faz o processamento da solicitação e retorna com o resultado para o cliente.

7.

Uma arquitetura cliente servidor móvel não necessariamente utilizará conexões wireless, mas em sua maioria é de se considerar como a principal forma de conexão com a rede. A segurança dos dados refere-se as camadas de privacidade (criptografia) aplicadas para integridade dos dados. Em um middleware móvel, deve-se manter sigilo sobre as credenciais de acesso ao banco de dados, evitando que invasores tenham acesso aos dados trafegados entre cliente e servidor. Em um banco de dados uma transação é um conjunto de diretivas SQL que consultam e retornam um resultado. Em um middleware móvel de acesso à dados, deve-se garantir que os comandos sejam executados ou nenhum comando permaneça na base para evitar instabilidades e não impactar no sistema como um todo. Um grande limitador de desempenho é a deficiência de conexões de dados móveis estáveis o bastante para garantirem um sistema distribuído em pleno funcionamento.

Como mencionado anteriormente, não será necessariamente conectado à uma conexão móvel o tempo todo, mas em sua maioria é a principal forma de conexão. A cada requisição que é enviada ao banco de dados tem como resposta o download de volumes de dados para o dispositivo, o que pode ocasionar queda de desempenho. Outro fator de queda de desempenho é a limitação de hardware, não muito comum hoje em dia, mas ainda presente em alguns casos. Da mesma forma que uma conexão móvel precária pode ocasionar perda de desempenho, um hardware não compatível com as requisições terá o mesmo resultado para processar requisições complexas podendo gerar um atraso na resposta para o cliente.

Técnicas de Caching que servem para armazenar dados muito utilizados ou que serão utilizados em breve em uma memória mais veloz do que a normal onde aquele dado costuma residir. Outro uso para mecanismos de caching está na arquitetura de computadores, onde existem diversos tipos e níveis de memória cache, como a memória cache existente nos processadores, que evita o tráfego desnecessário entre a unidade lógica aritmética (ULA) e o dado na memória RAM. No caso de bancos de dados, é comum que as tabelas ou combinações de dados mais comuns sejam mantidas em estruturas organizacionais

diferenciadas, como índices e visões, e as consultas mais comumente utilizadas sejam mantidas na memória RAM. Aplicando-se as três técnicas anteriores a um middleware de acesso à dados, têm-se um ganho de desempenho que embora não seja superior a implementações de acesso à banco de dados usando web services, é mais adequado e confiável ao cenário móvel

8.

Modelo de rede p2p tem como objetivo aproveitar o poder de processamento subutilizado dos nós da internet, programas torrentes e requisições www, assim buscam o nó mais próximo para verificar se ele possui o caminho para o site solicitado.

9.

Sem coordenação central.

Sem banco de dados central.

Sem local único de falha ou gargalo.

Nenhum ponto (peer) tem visão global do sistema.

Comportamento global definido por interações locais.

Todos os dados e serviços são acessíveis de qualquer ponto.

Pontos são autônomos.

Pontos e conexões não são confiáveis.

Descentralização da maior parte das funções da rede, isto é, cada nó pode realizar funções de cliente e/ou servidor.

O modelo de rede p2p possui formas de arquiteturas diferentes, podendo ser centralizadas, híbridas e somente p2p.

10.

As redes que utilizam a arquitetura centralizada, possui super nós, onde são responsáveis por indexarem informações de outros super nós, onde irá conter as localizações dos caminhos para arquivos solicitados em buscas por nós comuns, eles evitam tráfego desnecessário e dão precisão as buscas. O nó comum faz uma busca e o super nós, informa o caminho do nó que possui a informação buscada, assim evita buscas desnecessárias e ambos os nós o que buscou e o que tem a informação, estabelecem uma conexão mais rápida. A alguns desafios para redes que usam super nós, são em relação a encontrar possíveis nós comuns que podem tornar-se super nós, onde ele terá que ter alta disponibilidade e banda, assim com esses requisitos pode se tornar um super nó.

11.

Peer-to-peer (do inglês par-a-par ou simplesmente ponto a ponto) ou P2P é uma arquitetura de redes de computadores onde cada um dos pontos ou nós, da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

12.

A alguns desafios para redes que usam super nós, são em relação a encontrar possíveis nós comuns que podem tornar-se super nós, onde ele terá que ter alta disponibilidade e banda, assim com esses requisitos pode se tornar um super nó.

13.

Para o desenvolvimento de uma arquitetura de um sistema, o arquiteto/projetista terá que levantar requisitos para a funcionalidade do sistema. Tradicionalmente, os requisitos de um software são separados em requisitos funcionais (o que ele faz), e não funcionais (como ele faz). Requisitos são objetivos ou restrições estabelecidas por clientes e usuários que definem as suas diversas propriedades do sistema.

14.

A confiabilidade de software é definida como: “a probabilidade de operação livre de falhas de um programa de computador num ambiente específico durante determinado tempo” (Musa et al, 1987 in Pressman(1995)). É um dos atributos da qualidade de software, além de desempenho, portabilidade, reusabilidade, dentre outros. Desconsiderar a confiabilidade de software durante o desenvolvimento de um sistema de software implica na possível ocorrência de falhas durante a fase operacional do sistema.

Para manter altos níveis de confiança de software podem ser somente alcançados à custa do desempenho do sistema. A confiabilidade do produto de software é influenciada pelo processo de software utilizado para desenvolver o produto. Um processo orientado no sentido de evitar defeitos poderá desenvolver um sistema confiável.

A segurança de um sistema é um atributo que reflete a capacidade do sistema de operar normalmente e anormalmente, sem ameaçar as pessoas ou o ambiente. A confiabilidade e a segurança do sistema estão relacionadas, mas

são atributos de confianças distintos, os sistemas que apresentam tolerância a defeitos não são necessariamente seguros

15.

Modelo síncrono:

Vantagens: Comunicação em tempo real, as mensagens são enviadas e recebidas na mesma hora, com velocidade muito próxima, possui uma fácil utilização, possibilita feedback instantâneo e um melhor acompanhamento dos processos.

Desvantagens: A comunicação deve ocorrer na mesma velocidade, para que uma não tenha que ficar aguardando o processamento da outra, para que possibilite uma fluidez maior, existe uma limitação física, quando se pensando em comunicação por barramentos.

16.

Modelo assíncrono:

Vantagens: É mais adaptável as mudanças tecnológicas, possibilitando uma atualização de hardwares, pois não é necessário que as partes tenham a mesma velocidade de processamento, permitindo mais tempo para elaboração de uma resposta.

Desvantagens: Não possibilita interação, pois a comunicação não é feita sempre em tempo real, dificultando a troca de muitas informações, tornando as partes mais isoladas.

17.

A ordenação de mensagens deve existir para que seja garantida a exclusão mútua caso mais de uma mensagem acesse a região crítica, por isso devem ser entregues em ordem. Por exemplo, num processo de ordenação total, se uma mensagem m é entregue antes de uma mensagem m' , assegura-se que os demais processos as entregarão na mesma ordem. Exemplo de implementação: Fila de holdback. A mensagem com menor número de sequência, seja ele proposto ou de consenso, encabeça a fila. A fila é reordenada quando um número sequencial de consenso é colocado em uma mensagem. Efetivamente, reordenar somente quando o número de consenso for diferente do proposto.

18.

Hash é um algoritmo matemático que transforma qualquer bloco de dados em uma série de caracteres de comprimento fixo. Independentemente do comprimento dos dados de entrada, o mesmo tipo de hash de saída será sempre um valor hash do mesmo comprimento. O controle de acesso tem a seguinte função: Quando ocorre uma requisição para acessar um objeto, o monitor de referência verifica os direitos de acesso do remetente e toma a decisão se ele tem ou não a permissão para acessar o objeto, se o resultado for positivo, a requisição é recebida e respondida pelo objeto que foi procurado.

19.

Para garantir uma comunicação segura em sistema distribuído, é necessária uma divisão em duas etapas:

A comunicação de usuários e processos em computadores diferentes.

A autorização de acesso a recursos e serviços disponíveis.

Os mecanismos de segurança são:

Encriptação: Criptografia na troca de mensagens e armazenamento de informações sensíveis.

Autenticação: Para acessar um recurso.

Autorização: Para executar ações em um recurso.

Auditoria: Registro de atividades realizadas em logs

20.

Um Web Service é um conjunto de métodos acedidos e invocados por outros programas utilizando tecnologias Web. Aplicações que se comunicam independente de sistema operacional ou linguagem de programação o Fazendo comunicar usuário e banco de dados com traduções através de protocolos como o SOAP e o REST