

Sistemas Distribuídos - ESP625

Prof^a Ana Carolina Sokolonski

Bacharelado em Sistemas de Informação
Instituto Federal de Ciência e Tecnologia da Bahia
Campus de Feira de Santana

carolsoko@ifba.edu.br

September 26, 2023

DEPENDABILITY - Confiança no Funcionamento do Sistema

- 1 DEPENDABILITY - Confiança no Funcionamento do Sistema
- 2 O que é Falha, Erro e Defeito?
 - FAULT (Falha)
 - ERROR (Erro)
 - FAILURE (Defeito)
- 3 Classificação das Falhas em Sistemas Distribuídos
 - Falhas Físicas X Falhas Humanas
 - Falhas de Outras Naturezas
 - Falhas Maliciosas
 - Falhas em Sistemas Críticos
- 4 Referências

DEPENDABILITY

Confiança no Funcionamento do Sistema

DEPENDABILITY

DEPENDABILITY:

A dependabilidade surge da necessidade de se poder depender de um sistema. Devido à evolução tecnológica e à crescente dependência humana da tecnologia, de um sistema poder ter a propriedade de se poder depender do mesmo.

DEPENDABILITY

DEPENDABILITY:

A dependabilidade surge da necessidade de se poder depender de um sistema. Devido à evolução tecnológica e à crescente dependência humana da tecnologia, de um sistema poder ter a propriedade de se poder depender do mesmo.

Um pouco mais formalmente, dizemos que um componente X depende de um componente Y se a corretude do comportamento de X depende da corretude do componente Y e dizemos também que um componente é “dependável” (DEPENDABLE) na medida em que outros podem depender dele.

DEPENDABILITY

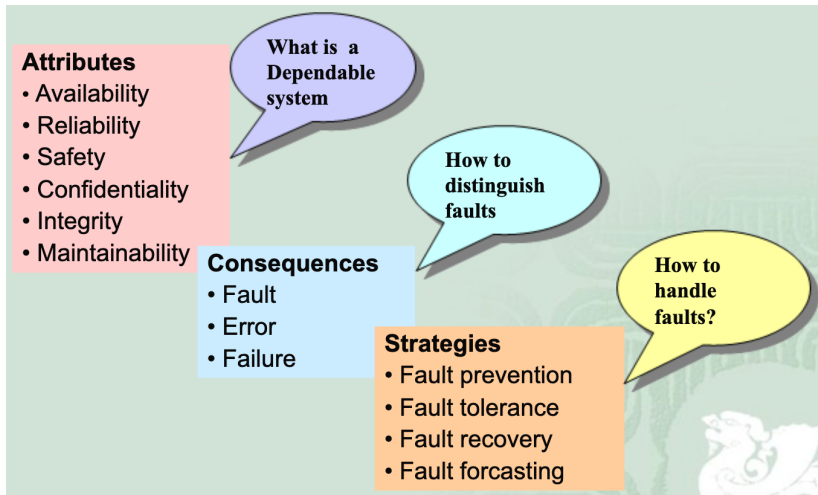
DEPENDABILITY:

A dependabilidade surge da necessidade de se poder depender de um sistema. Devido à evolução tecnológica e à crescente dependência humana da tecnologia, de um sistema poder ter a propriedade de se poder depender do mesmo.

Um pouco mais formalmente, dizemos que um componente X depende de um componente Y se a corretude do comportamento de X depende da corretude do componente Y e dizemos também que um componente é “dependável” (DEPENDABLE) na medida em que outros podem depender dele.

A dependabilidade é essencial aos componentes de Sistemas Distribuídos.

Resumindo... DEPENDABILITY



ATRIBUTOS

DEPENDABILITY:

A dependabilidade não é uma coisa só, ela engloba diferentes atributos. São eles:

- Disponibilidade (AVAILABILITY) - capacidade do sistema de estar disponível para uso, levando em conta inclusive a ocorrência de falhas que interrompam o serviço e a posterior recuperação com a retomada do serviço;
- Confiabilidade (RELIABILITY) - capacidade do sistema de oferecer o serviço correto continuamente, sem falhas e interrupções;

ATRIBUTOS

DEPENDABILITY:

A dependabilidade não é uma coisa só, ela engloba diferentes atributos. São eles:

- Segurança (SAFETY) - capacidade do sistema de evitar consequências catastróficas;
- Segurança (SECURITY) - inclui os diversos atributos clássicos de segurança, como capacidade de oferecer confidencialidade e integridade;
- Manutenibilidade (MAINTAINABILITY) - facilidade de manutenção e realizar alterações.

ATRIBUTOS

Atributo	Significado
Dependabilidade (<i>dependability</i>)	qualidade do serviço fornecido por um dado sistema
Confiabilidade (<i>reliability</i>)	capacidade de atender a especificação, dentro de condições definidas, durante certo período de funcionamento e condicionado a estar operacional no início do período
Disponibilidade (<i>availability</i>)	probabilidade do sistema estar operacional num instante de tempo determinado; alternância de períodos de funcionamento e reparo
Segurança (<i>safety</i>)	probabilidade do sistema ou estar operacional e executar sua função corretamente ou descontinuar suas funções de forma a não provocar dano a outros sistema ou pessoas que dele dependam
Segurança (<i>security</i>)	proteção contra falhas maliciosas, visando privacidade, autenticidade, integridade e irrepudiabilidade dos dados

RELIABILITY:

A confiabilidade $R(t)$ é a capacidade de atender a especificação, dentro de condições definidas, durante certo período de funcionamento e condicionado a estar operacional no início do período.

RELIABILITY:

A confiabilidade $R(t)$ é a capacidade de atender a especificação, dentro de condições definidas, durante certo período de funcionamento e condicionado a estar operacional no início do período.

Confiabilidade (Reliability) é a medida mais usada em sistemas críticos, ou seja nos seguintes tipos de sistemas: Sistemas em que mesmo curtos períodos de operação incorreta são inaceitáveis e Sistemas em que reparo é impossível.

RELIABILITY:

A confiabilidade $R(t)$ é a capacidade de atender a especificação, dentro de condições definidas, durante certo período de funcionamento e condicionado a estar operacional no início do período.

Confiabilidade (Reliability) é a medida mais usada em sistemas críticos, ou seja nos seguintes tipos de sistemas: Sistemas em que mesmo curtos períodos de operação incorreta são inaceitáveis e Sistemas em que reparo é impossível.

A definição acima implica algumas condições essenciais:

RELIABILITY:

- Especificação: sem uma especificação do sistema, não é possível determinar se o sistema está operando conforme esperado ou não, quando mais formal e completa a especificação, mais fácil estabelecer essa condição. Não é possível estabelecer se um sistema sem especificação é confiável ou não.

RELIABILITY:

- Especificação: sem uma especificação do sistema, não é possível determinar se o sistema está operando conforme esperado ou não, quando mais formal e completa a especificação, mais fácil estabelecer essa condição. Não é possível estabelecer se um sistema sem especificação é confiável ou não.
- Condições Definidas: as condições de funcionamento do sistema devem ser bem definidas. Um exemplo simples são as condições ambientais de temperatura e umidade. Outro exemplo são os dados ou estímulos de entrada que o sistema deve processar.

RELIABILITY:

- Período de Funcionamento: o tempo de missão deve ser conhecido. O tempo de missão de uma viagem espacial é diferente do tempo de missão de um voo comercial doméstico. Um sistema pode ser altamente confiável para 12 horas de operação e depois necessitar de um longo período de repouso e reparo.

RELIABILITY:

- Período de Funcionamento: o tempo de missão deve ser conhecido. O tempo de missão de uma viagem espacial é diferente do tempo de missão de um voo comercial doméstico. Um sistema pode ser altamente confiável para 12 horas de operação e depois necessitar de um longo período de repouso e reparo.
- Estado Operacional no Início do Período: não é possível falar em confiabilidade de sistemas que já partem operando com defeitos.

RELIABILITY:

Confiabilidade é uma medida de probabilidade, pois a ocorrência de falhas é um fenômeno aleatório. Confiabilidade não pode ser confundida com disponibilidade.

RELIABILITY:

Confiabilidade é uma medida de probabilidade, pois a ocorrência de falhas é um fenômeno aleatório. Confiabilidade não pode ser confundida com disponibilidade.

UM SISTEMA PODE SER DE ALTA CONFIABILIDADE E DE BAIXA DISPONIBILIDADE.

RELIABILITY:

Confiabilidade é uma medida de probabilidade, pois a ocorrência de falhas é um fenômeno aleatório. Confiabilidade não pode ser confundida com disponibilidade.

UM SISTEMA PODE SER DE ALTA CONFIABILIDADE E DE BAIXA DISPONIBILIDADE.

Um exemplo seria um avião que precisa de reparos e manutenção nos intervalos de vôo.

AVAILABILITY:

A Disponibilidade também é uma medida de probabilidade. Disponibilidade é a probabilidade do sistema estar operacional num instante de tempo determinado.

AVAILABILITY:

A Disponibilidade também é uma medida de probabilidade. Disponibilidade é a probabilidade do sistema estar operacional num instante de tempo determinado.

É o atributo mais usado em sistemas de missão crítica. Sistemas de consulta de base de dados on-line, servidores de rede, servidores de páginas web, são alguns exemplos de sistemas onde alta disponibilidade é requerida. [TANENBAUM e STEEN 2007]

AVAILABILITY:

DISPONIBILIDADE NÃO PODE SER CONFUNDIDA COM
CONFIABILIDADE.

AVAILABILITY:

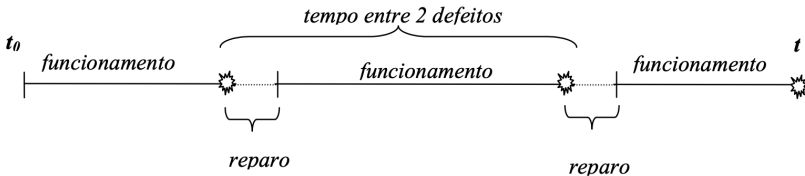
DISPONIBILIDADE NÃO PODE SER CONFUNDIDA COM CONFIABILIDADE.

Um sistema pode ser altamente disponível mesmo apresentando períodos de inoperabilidade, quando está sendo reparado, desde que esses períodos sejam curtos e não comprometam a qualidade do serviço. Disponibilidade está muito relacionada com o tempo de reparo do sistema. Diminuir o tempo de reparo resulta em um aumento de disponibilidade.

AVAILABILITY:

DISPONIBILIDADE NÃO PODE SER CONFUNDIDA COM CONFIABILIDADE.

Um sistema pode ser altamente disponível mesmo apresentando períodos de inoperabilidade, quando está sendo reparado, desde que esses períodos sejam curtos e não comprometam a qualidade do serviço. Disponibilidade está muito relacionada com o tempo de reparo do sistema. Diminuir o tempo de reparo resulta em um aumento de disponibilidade.



SAFETY:

Segurança (SAFETY) é a probabilidade do sistema ou estar operacional, e executar sua função corretamente, ou descontinuar suas funções de forma a não provocar dano a outros sistemas ou pessoas que dele dependam.

SAFETY:

Segurança (SAFETY) é a probabilidade do sistema ou estar operacional, e executar sua função corretamente, ou descontinuar suas funções de forma a não provocar dano a outros sistemas ou pessoas que dele dependam.

Segurança é a medida da capacidade do sistema de se comportar de forma livre de falhas (FAIL-SAFE).

SAFETY:

Segurança (SAFETY) é a probabilidade do sistema ou estar operacional, e executar sua função corretamente, ou descontinuar suas funções de forma a não provocar dano a outros sistemas ou pessoas que dele dependam.

Segurança é a medida da capacidade do sistema de se comportar de forma livre de falhas (FAIL-SAFE).

Um exemplo seria um sistema de transporte ferroviário onde os controles de um trem providenciam sua desaceleração e parada automática quando não mais conseguirem garantir o seu funcionamento correto. Em um sistema FAIL-SAFE, ou a saída é correta ou o sistema é levado a um estado seguro.

[Coulouris et al. 2013]

Demais Atributos:

Outros atributos importantes de um sistema são: comprometimento do desempenho (PERFORMABILITY), manutenibilidade (MANTENABILITY) e testabilidade (TESTABILITY). Todas essas medidas são igualmente representadas por uma probabilidade.

Demais Atributos:

Outros atributos importantes de um sistema são: comprometimento do desempenho (PERFORMABILITY), manutenibilidade (MANTENABILITY) e testabilidade (TESTABILITY). Todas essas medidas são igualmente representadas por uma probabilidade.

Comprometimento do desempenho (PERFORMABILITY) está relacionada à queda de desempenho provocado por falhas, onde o sistema continua a operar, mas degradado em desempenho.

Demais Atributos:

Mantenabilidade (MANTENABILITY) significa a facilidade de realizar a manutenção do sistema, ou seja, a probabilidade que um sistema com defeitos seja restaurado a um estado operacional dentro de um período determinado. Restauração envolve a localização do problema, o reparo físico e a colocação em operação.

Demais Atributos:

Mantenabilidade (MANTENABILITY) significa a facilidade de realizar a manutenção do sistema, ou seja, a probabilidade que um sistema com defeitos seja restaurado a um estado operacional dentro de um período determinado. Restauração envolve a localização do problema, o reparo físico e a colocação em operação.

Testabilidade (TESTABILITY) é a capacidade de testar certos atributos internos do sistema ou facilidade de realizar certos testes.

Demais Atributos:

Mantenabilidade (MANTENABILITY) significa a facilidade de realizar a manutenção do sistema, ou seja, a probabilidade que um sistema com defeitos seja restaurado a um estado operacional dentro de um período determinado. Restauração envolve a localização do problema, o reparo físico e a colocação em operação.

Testabilidade (TESTABILITY) é a capacidade de testar certos atributos internos do sistema ou facilidade de realizar certos testes.

Quanto maior a testabilidade, melhor a manutenabilidade, e por consequência menor o tempo que o sistema não estará disponível devido a reparos.

O que é Falha, Erro e Defeito?

Antes de mais nada, precisamos definir exatamente o que é uma “FALHA”. Poucos termos são usados na computação com tantos significados tão distintos.

O que é Falha, Erro e Defeito?

Antes de mais nada, precisamos definir exatamente o que é uma “FALHA”. Poucos termos são usados na computação com tantos significados tão distintos.

É possível generalizar, dizendo que uma falha corresponde a um comportamento incorreto, fora da especificação. Desta forma, o sistema ou não produz resultado algum, ou produz resultado que não está entre os permitidos ou desejáveis.

O que é Falha, Erro e Defeito?

Antes de mais nada, precisamos definir exatamente o que é uma “FALHA”. Poucos termos são usados na computação com tantos significados tão distintos.

É possível generalizar, dizendo que uma falha corresponde a um comportamento incorreto, fora da especificação. Desta forma, o sistema ou não produz resultado algum, ou produz resultado que não está entre os permitidos ou desejáveis.

No jargão da área de tolerância a falhas são identificados três “estágios” diferentes referentes à falha de um componente de um sistema, em inglês eles são: **Fault, Error e Failure.**

FAULT (Falha):

Tudo começa com uma falha de um componente do sistema. Pode ser uma falha de *hardware* ou um *bug de software*. Um componente pode falhar, mas esta falha não ser “ativada”.

FAULT (Falha):

Tudo começa com uma falha de um componente do sistema. Pode ser uma falha de *hardware* ou um *bug de software*. Um componente pode falhar, mas esta falha não ser “ativada”.

Por exemplo, pode ser que um procedimento específico de um programa tenha sido implementado incorretamente, mas se aquele procedimento não for executado, então a falha fica lá, dormente.

FAULT (Falha):

O termo **Fault** se refere justamente a este tipo de incorreção. Em português, a comunidade de tolerância a falhas, adotam duas palavras distintas para FAULT em português: alguns traduzem como "falta", outros como "falha" mesmo.

FAULT (Falha):

O termo **Fault** se refere justamente a este tipo de incorreção. Em português, a comunidade de tolerância a falhas, adotam duas palavras distintas para FAULT em português: alguns traduzem como "falta", outros como "falha" mesmo.

Veja que em inglês "TOLERÂNCIA A FALHAS" é "FAULT TOLERANCE", ou seja, o que se tolera é uma FAULT, que neste contexto podemos traduzir para "falha".

FAULT (Falha):

O termo **Fault** se refere justamente a este tipo de incorreção. Em português, a comunidade de tolerância a falhas, adotam duas palavras distintas para FAULT em português: alguns traduzem como "falta", outros como "falha" mesmo.

Veja que em inglês "TOLERÂNCIA A FALHAS" é "FAULT TOLERANCE", ou seja, o que se tolera é uma FAULT, que neste contexto podemos traduzir para "falha".

No fim das contas, o que importa é compreender que FAULT corresponde a uma falha latente, intrínseca de um componente, que pode ou não se manifestar.

ERROR (Erro):

Quando a falha (FAULT) se manifesta, ocorre o chamado erro (ERROR). Neste caso, em português todos concordam em traduzir como "erro".

ERROR (Erro):

Quando a falha (FAULT) se manifesta, ocorre o chamado erro (ERROR). Neste caso, em português todos concordam em traduzir como "erro".

Retomando o exemplo anterior, se o procedimento implementado incorretamente é executado e produz uma saída fora de sua especificação, então acontece um erro, que é a manifestão da falha (FAULT).

ERROR (Erro):

Veja que mesmo que o procedimento com falha seja executado, é possível que as saídas produzidas sejam (por alguma coincidência) corretas, neste caso não há erro.

ERROR (Erro):

Veja que mesmo que o procedimento com falha seja executado, é possível que as saídas produzidas sejam (por alguma coincidência) corretas, neste caso não há erro.

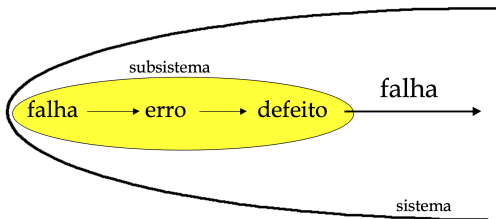
Um exemplo bastante impressionante de falha e erro é o que aconteceu com alguns modelos do processador Pentium da Intel, no começo dos anos 1990, que incrivelmente, computadores produzidos iguais davam ou não davam erro. Acontecia o erro em algumas máquinas e em outras não. Por algum motivo.

FAILURE (Defeito):

Uma falha (FAULT) pode se manifestar como um erro (ERROR) e, por sua vez, o erro produzido pelo componente com defeito pode se propagar para a saída geral do sistema, causando então seu defeito (FAILURE).

FAILURE (Defeito):

Uma falha (FAULT) pode se manifestar como um erro (ERROR) e, por sua vez, o erro produzido pelo componente com defeito pode se propagar para a saída geral do sistema, causando então seu defeito (FAILURE).



FAILURE (Defeito):

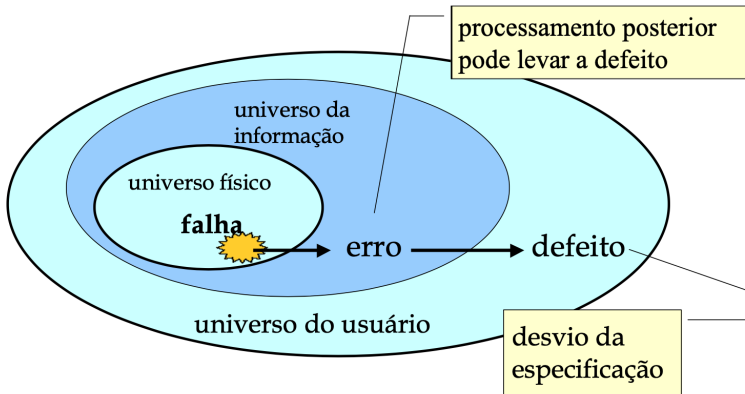
O Defeito (FAILURE) do sistema corresponde ao seu colapso: o sistema como um todo produz resultado incorreto, fora da sua especificação.

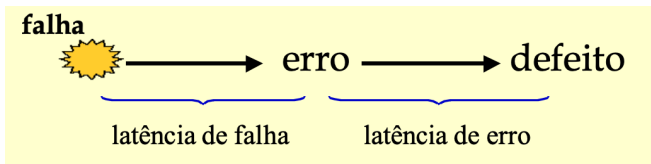
FAILURE (Defeito):

O Defeito (FAILURE) do sistema corresponde ao seu colapso: o sistema como um todo produz resultado incorreto, fora da sua especificação.

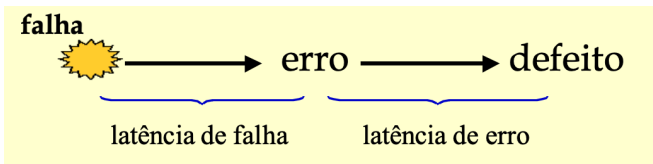
É possível que o erro de um componente não se propague até a saída do sistema. Por exemplo, se a saída de um módulo aritmético tem uma falha (FAULT) que se manifesta em erro (ERROR), mas este erro é então multiplicado por zero, o erro é neutralizado e não vai se propagar até a saída do sistema.

falha (falta) → erro → defeito



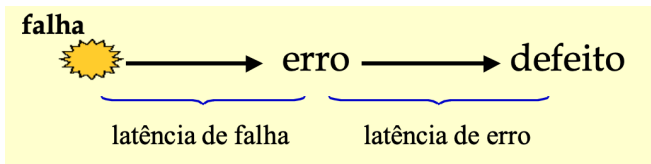


Latência de Falha e de Erro:



Latência de Falha e de Erro:

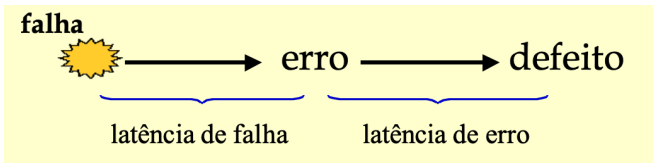
Define-se latência de falha como o período de tempo desde a ocorrência da falha até a manifestação do erro devido àquela falha.



Latência de Falha e de Erro:

Define-se latência de falha como o período de tempo desde a ocorrência da falha até a manifestação do erro devido àquela falha.

Define-se latência de erro como o período desde a ocorrência do erro até a manifestação do defeito devido àquele erro.



Latência de Falha e de Erro:

Define-se latência de falha como o período de tempo desde a ocorrência da falha até a manifestação do erro devido àquela falha.

Define-se latência de erro como o período desde a ocorrência do erro até a manifestação do defeito devido àquele erro.

Baseando-se no modelo de 3 universos, o tempo total desde a ocorrência da falha até o aparecimento do defeito é a soma da latência de falhas e da latência de erro.

Classificação das Falhas:

As falhas aparecem geralmente classificadas em falhas físicas, aquelas afetam os componentes, e falhas humanas. Falhas humanas compreendem falhas de projeto e falhas de interação.

Classificação das Falhas:

As falhas aparecem geralmente classificadas em falhas físicas, aquelas afetam os componentes, e falhas humanas. Falhas humanas compreendem falhas de projeto e falhas de interação.

As principais causas de falhas são problemas de especificação, problemas de implementação, componentes defeituosos, imperfeições de manufatura, fadiga dos componentes físicos, além de distúrbios externos como radiação, interferência eletromagnética, variações ambientais (temperatura, pressão, umidade) e também problemas de operação.

Classificação das Falhas:

Além da causa, para definir uma falha considera-se também:

- Natureza: falha de hardware, falha de software, de projeto, de operação, etc.
- Duração ou persistência: permanente ou temporária (intermitente ou transitória)
- Extensão: falha restrita a um módulo, falha global
- Valor: determinado ou indeterminado no tempo

Classificação das Falhas:

Vem crescendo a ocorrência daquelas falhas provocadas por interação humana maliciosa, ou seja, por aquelas ações que visam propositadamente provocar danos aos sistemas.

Classificação das Falhas:

Vem crescendo a ocorrência daquelas falhas provocadas por interação humana maliciosa, ou seja, por aquelas ações que visam propositadamente provocar danos aos sistemas.

Essas falhas e suas consequências são tratados por técnicas de segurança computacional (security) e não por técnicas de tolerância a falhas.

Classificação das Falhas:

Vem crescendo a ocorrência daquelas falhas provocadas por interação humana maliciosa, ou seja, por aquelas ações que visam propositadamente provocar danos aos sistemas.

Essas falhas e suas consequências são tratados por técnicas de segurança computacional (security) e não por técnicas de tolerância a falhas.

Deve ser considerado, entretanto, que um sistema tolerante a falhas deve ser também seguro a intrusões e ações maliciosas.

Classificação das Falhas:

Falhas de software e também de projeto são consideradas atualmente o mais grave problema em computação crítica.



Classificação das Falhas:

Falhas de software e também de projeto são consideradas atualmente o mais grave problema em computação crítica.

Sistemas críticos, tradicionalmente, são construídos de forma a suportar falhas físicas. Assim é compreensível que falhas não tratadas, e não previstas, sejam as que mais aborreçam, pois possuem uma grande potencial de comprometer a confiabilidade e disponibilidade do sistema.

Referências

Referências

-  COULOURIS, G. et al. *Sistemas Distribuídos: Conceitos e Projetos*. 5. ed. [S.l.]: Bookman, 2013. v. 1.
-  TANENBAUM, A.; STEEN, M. V. *Sistemas Distribuídos - Princípios e Paradigmas*. 2. ed. [S.l.]: Prentice Hall, 2007. v. 1.