Ferramentas

Artigos Gerais

A Survey on Fault Injection Techniques

Fault injection techniques and Tools

Assessing Dependability with Software Fault Injection: A Survey

A Survey on Fault Injection Techniques

Perguntas

- **Aplicação:** Qual a aplicação da ferramenta?
- **Cenário:** Em que cenário a ferramenta pode ser utilizada?
- **Disponibilidade:** A ferramenta é gratuita ou paga?
- **Nuvem:** A ferramenta pode ser utilizada em Serviços de Nuvem?
- **Comentários Adicionais:** Comentários adicionais sobre a ferramenta.

AFEX

Paper: Fast black-box testing of system recovery code

Aplicação

AFEX é uma técnica e ferramenta para automatizar o processo de injeção de falhas em sistemas de software, com o objetivo de maximizar a descoberta de bugs em um período de tempo fixo

O AFEX ajuda a gerar combinações de falhas para atender a critérios específicos, como causar perda de dados ou identificar falhas que afetam o desempenho.

A ferramenta produz conjuntos de falhas, caracterizações de qualidade e casos de teste para injetar falhas no sistema em teste e medir seu impacto.

Fornece scripts de injeção de falhas que podem ser usados diretamente para reproduzir falhas e seu impacto no sistema, economizando tempo na construção de suítes de teste de regressão

Cenário

O AFEX pode ser usado em cenários de teste de software em que é necessário um controle refinado sobre a injeção de falhas.

Ele pode se beneficiar de ferramentas de análise estática para detectar pontos de injeção vulneráveis e aumentar a eficiência na descoberta de bugs.

A ferramenta pode automatizar processos de injeção de falhas em sistemas do mundo real, como MySQL, Apache httpd, utilitários UNIX e MongoDB, descobrindo novos bugs com eficiência.

O AFEX gera conjuntos de falhas, caracterizações de qualidade e casos de teste para injetar falhas no sistema em teste e medir seu impacto.

Disponibilidade

As informações de preços da ferramenta AFEX não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

O AFEX pode ser usado em serviços em nuvem, pois automatiza o processo de injeção de falhas e pode ser aplicado a sistemas reais como MySQL, Apache httpd, utilitários UNIX e MongoDB.

A ferramenta fornece medições para cada teste e cria pastas contendo registros e outras saídas, o que pode ser benéfico para analisar resultados em ambientes de nuvem.

O AFEX foi projetado para ser flexível e extensível, permitindo a integração de novos injetores de falhas e algoritmos de pesquisa personalizados, tornando-o adaptável a diferentes ambientes do sistema, incluindo serviços em nuvem.

Comentários Adicionais

A ferramenta visa produzir um conjunto de falhas que satisfaçam critérios específicos, como perda de dados ou impacto no desempenho, reduzindo a necessidade de mão de obra humana na geração de testes.

FIAT

Paper: FIAT: A Fault Injection Tool for Distributed Systems

Aplicação

O FIAT (Teste Automatizado Baseado em Injeção de Falhas) é um ambiente experimental usado para explorar metodologias de validação para sistemas tolerantes a falhas.

Consiste em dois componentes principais: o Fault Injection Manager (FIM) e o Fault Injection Receptor (FIRE).

O FIAT permite a emulação de várias arquiteturas de sistemas distribuídos, monitorando o comportamento do sistema e injetando falhas para caracterizar e validar a confiabilidade do sistema.

Cenário

Ele permite emular arquiteturas de sistemas distribuídos, monitorar o comportamento do sistema e injetar falhas para caracterização e validação experimental.

Disponibilidade

As informações de preços da ferramenta FIAT não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

Ele permite emular arquiteturas de sistemas distribuídos, monitorar o comportamento do sistema e injetar falhas para caracterização e validação experimentais, que são aspectos essenciais nos testes de serviços em

nuvem.

FTAPE

Paper: FTAPE - A fault injection tool to measure fault tolerance

Aplicação

O FTAPE combina injeção de falhas em nível de sistema com uma carga de trabalho controlável. Um gerador de carga de trabalho é utilizado para criar condições de alto estresse para a máquina, e as falhas são injetadas com base nessa atividade da carga de trabalho para garantir um alto nível de propagação de falhas. As medidas de tolerância a falhas incluem a relação erros/falhas e a degradação de desempenho.

Cenário

A ferramenta pode ser usada para comparar computadores tolerantes a falhas, medindo a eficácia e a eficiência dos mecanismos de tolerância a falhas.

Ele pode fornecer uma medida única que caracteriza a tolerância a falhas de um computador, ajudando os compradores a avaliar diferentes projetos de tolerância a falhas e fornecendo feedback detalhado aos projetistas do sistema.

o FTAPE pode ser usado para rastrear a propagação de falhas quando ocorrem falhas no sistema e melhorar o projeto de mecanismos de contenção de falhas.

Disponibilidade

As informações de preços da ferramenta FTAPE não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

A FTAPE é projetada para injetar falhas em registros da CPU, memória e sistemas de disco, e combina a injeção de falhas em todo o sistema com uma carga de trabalho controlada para avaliar como o sistema responde às falhas. Isso significa que a ferramenta pode ser adaptada para avaliar a tolerância a falhas e o desempenho de sistemas em ambientes de nuvem, onde a confiabilidade e a tolerância a falhas são aspectos críticos.

Xception

Paper: Xception: Software Fault Injection and Monitoring in Processor Functional Units

Aplicação

O Xception utiliza recursos avançados de depuração e monitoramento de desempenho existentes na maioria dos processadores modernos para injetar falhas realistas por software e monitorar a ativação das falhas e seu impacto no comportamento do sistema-alvo.

Fornece um conjunto abrangente de gatilhos de falhas, incluindo gatilhos espaciais e temporais, bem como gatilhos relacionados à manipulação de dados na memória. Além disso,

Pode afetar qualquer processo em execução no sistema-alvo, incluindo o sistema operacional, e pode injetar falhas em aplicativos para os quais o código-fonte não está disponível.

Cenário

pode ser utilizada em cenários de avaliação de propriedades de confiabilidade de sistemas computacionais. útil para avaliar o impacto de falhas em sistemas paralelos e distribuídos, bem como para avaliar a capacidade de tolerância a falhas de algoritmos e aplicativos paralelos.

Disponibilidade

As informações de preços da ferramenta Xception não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

Xception pode afetar qualquer processo em execução no sistema-alvo, incluindo o sistema operacional, e pode injetar falhas em aplicativos para os quais o código-fonte não está disponível. Portanto, ela pode ser aplicada em ambientes de nuvem para avaliar e validar as propriedades de dependabilidade de sistemas computacionais distribuídos.

Ferrari

Paper: Faultinjection Techniques and Tools

Aplicação

A ferramenta Ferrari, também conhecida como Fault and Error Automatic Real-Time Injection (FERRARI), é uma ferramenta desenvolvida na Universidade do Texas em Austin, que consiste em componentes para injetar falhas em locais acessíveis ao usuário, como registros da CPU e subsistema de disco. Ela é utilizada para testar a detecção de erros e a eficácia da tolerância a falhas em sistemas computacionais. A ferramenta permite injetar módulos de falhas em diferentes partes do sistema, como CPU, memória e subsistema de disco, e monitorar seus efeitos. Além disso, a Ferrari é capaz de exercitar mecanismos de detecção de erros, sendo uma ferramenta valiosa para avaliar a confiabilidade e desempenho de sistemas computacionais.

Cenário

Pode ser utilizada em cenários nos quais é necessário avaliar a dependabilidade de sistemas computacionais. Ela é particularmente útil para injetar falhas em locais acessíveis ao usuário, como registros da CPU e subsistema de disco, e monitorar seus efeitos. A ferramenta pode ser empregada para testar a detecção de erros, a capacidade de recuperação de falhas e a tolerância a falhas em sistemas computacionais.

Disponibilidade

As informações de preços da ferramenta Ferrari não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

A ferramenta pode ser utilizada para testar a detecção de erros e a eficácia da tolerância a falhas em sistemas distribuídos, como os encontrados em serviços de nuvem.

Mafalda

paper: Assessment of COTS Microkernels by Fault Injection

Aplicação

A ferramenta MAFALDA (Microkernel Assessment by Fault injection AnaLysis and Design Aid) é uma ferramenta de injeção de falhas projetada para avaliar o comportamento de microkernels na presença de falhas. Ela é usada para analisar a robustez da interface do microkernel em relação a falhas externas, a cobertura de detecção de erros dos mecanismos internos de detecção de erros, os canais de propagação de erros entre os componentes internos do microkernel e o impacto de seu comportamento defeituoso em camadas superiores. A MAFALDA é executada em um ambiente Solaris e fornece recursos para a descrição de uma campanha de injeção de falhas, a execução de experimentos e a coleta de resultados observados para análise posterior. Ela utiliza a técnica de injeção de falhas de software-implementado (SWIFI) para emular falhas permanentes e transitórias, permitindo a observação de eventos como exceções, falhas de aplicativos e falhas do sistema. A ferramenta é baseada em uma arquitetura modular que corresponde à arquitetura do microkernel, e é capaz de identificar deficiências no microkernel e fornecer orientações para melhorias de design.

Cenário

fornece recursos para a descrição de uma campanha de injeção de falhas, a execução de experimentos (reinicialização, carregamento, injeção de falhas, etc.) e a coleta de resultados observados para análise posterior. Ela é particularmente útil para avaliar a adequação do uso de microkernels em sistemas críticos de segurança e para identificar deficiências no microkernel, fornecendo orientações para melhorias de design e a definição de estratégias de tolerância a falhas.

Disponibilidade

As informações de preços da ferramenta MAFALDA não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

Elas podem ser usadas para avaliar a robustez de microkernels em ambientes de nuvem, onde a confiabilidade e a tolerância a falhas são aspectos críticos.

Mefisto-C

Paper: A Comparison of Simulation Based and Scan Chain Implemented Fault Injection

Aplicação

MEFISTO-C é uma ferramenta desenvolvida na Chalmers University of Technology para conduzir experimentos de injeção de falhas usando modelos de simulação VHDL. A ferramenta é um versão melhorada da ferramenta MEFISTO que foi desenvolvida em conjunto pela LAAS-CNRS e Chalmers [10]. (Uma ferramenta semelhante chamada MEFISTO-L foi desenvolvida no LAASCNRS). MEFISTO-C usa o Vantage Optium VHDL simulador e injeta falhas por meio de comandos do simulador em variáveis e sinais definidos no modelo VHDL. Oferece ao

usuário uma variedade de modelos de falha predefinidos, bem como outros recursos para configurar e conduzir falhas automaticamente campanhas de injeção em uma rede de estações de trabalho UNIX.

Cenário

O MEFISTO-C pode ser usado para conduzir experimentos de injeção de falhas em modelos de simulação VHDL. A ferramenta injeta falhas por meio de comandos do simulador em variáveis e sinais definidos no modelo VHDL. O MEFISTO-C oferece modelos e recursos de falha predefinidos para configurar e conduzir automaticamente campanhas de injeção de falhas em estações de trabalho UNIX.

Disponibilidade

As informações de preços da ferramenta MEFISTO-C não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

Não pois é uma ferramenta de simulação VHDL.

PREFAIL

Paper: PREFAIL: A Programmable Tool for Multiple-Failure Injection

Aplicação

PREFAIL é uma ferramenta programável de injeção de falhas projetada para ajudar os testadores a escrever políticas para reduzir o espaço de várias falhas em sistemas de software em nuvem. Ele permite que os testadores especifiquem o número máximo de falhas a serem injetadas, executa o sistema com zero falhas inicialmente e, em seguida, injete falhas com base nas políticas especificadas pelo testador.

Cenário

O PREFAIL foi projetado para ajudar os testadores a escrever políticas para reduzir o espaço de várias falhas em sistemas de software em nuvem, como HDFS, Cassandra e ZooKeeper. Ele pode ser usado para testar a versão do software Hadoop e encontrar bugs de forma eficiente, gastando muito menos tempo do que testes exaustivos.A ferramenta permite que os testadores especifiquem o número máximo de falhas a serem injetadas em uma execução do sistema em teste, permitindo uma abordagem sistemática para testar várias falhas.

Disponibilidade

As informações de preços da ferramenta PREFAIL não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

O PREFAIL foi projetado para sistemas de software em nuvem como HDFS, Cassandra e ZooKeeper, tornando-o adequado para testar serviços em nuvem. A ferramenta foi usada para testar a versão do software Hadoop, indicando sua aplicabilidade em ambientes de nuvem

---

RIFLE

Paper: RIFLE: A General Purpose Pin-level Fault Injector

Aplicação

O RIFLE é um injetor de falhas no nível do pino projetado para validação de confiabilidade, capaz de injetar vários tipos de falhas nos pinos do processador. Ele pode ser adaptado a diferentes sistemas de destino e foi usado em processadores como 68000, Z80, Intel 486DX e Inmos T800. A ferramenta combina técnicas de acionamento e rastreamento para injetar falhas e registrar informações detalhadas sobre o comportamento do processador alvo após a injeção de falhas. O RIFLE redefine automaticamente o sistema alvo antes da injeção de falhas, espera 5 segundos após a injeção para detectar erros e pode definir conjuntos específicos de falhas com base nos critérios do usuário. Sua arquitetura inclui módulos de hardware e software de controle para injeção e análise de falhas, com resultados armazenados em uma planilha para posterior análise estatística.

Cenário

O RIFLE pode ser utilizado para validar a confiabilidade em diversos sistemas, injetando falhas nos pinos do processador. A ferramenta pode configurar conjuntos específicos de falhas conforme os critérios do usuário, como falhas aleatórias no espaço do programa, falhas aleatórias no tempo de execução, falhas no fluxo de controle e falhas no comportamento da memória. Ele combina técnicas de gatilho e rastreamento para injetar e analisar falhas, fornecendo informações detalhadas sobre o impacto da falha e a propagação do erro.

Disponibilidade

As informações de preços da ferramenta RIFLE não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

A adaptabilidade do RIFLE a vários sistemas de destino sugere sua potencial aplicabilidade em ambientes de serviços em nuvem. Seus recursos de injeção de falhas e mecanismos de detecção de erros podem auxiliar na avaliação da confiabilidade e resiliência de aplicativos baseados em nuvem. Além disso, a capacidade do RIFLE de definir conjuntos específicos de falhas com base nos critérios do usuário pode ser útil para simular cenários de falhas em serviços em nuvem. A abordagem determinística de injeção de falhas do RIFLE pode, ainda, ajudar a compreender o impacto das falhas no desempenho e na confiabilidade do serviço em nuvem.

PROFIPY

Paper: ProFIPy: Programmable Software Fault Injection as-a-Service

Aplicação

O ProfiPy é uma ferramenta de injeção de falhas projetada para software Python. Ele permite que os usuários especifiquem seu modelo de falha usando uma linguagem específica de domínio. A ferramenta pode injetar código defeituoso em pontos específicos do software, controlar a execução do código injetado e analisar os efeitos das falhas e da recuperação. O ProfiPy fornece um fluxo de trabalho completo de injeção de falhas, auxiliando na aplicação da injeção de falhas de software em sistemas Python.

Cenário

O ProfiPy foi projetado para realizar campanhas de injeção de falhas com cargas de falhas personalizadas no software Python, tornando-o adequado para testar os requisitos de resiliência do software. Ele auxilia os engenheiros de teste na aplicação da injeção de falhas de software em sistemas Python, gerando versões mutadas do software de destino para análise do comportamento do sistema em caso de falha.

Disponibilidade

O ProfiPy é fornecido como software como serviço, oferecendo recursos de injeção de falhas para o software Python. Os usuários podem acessar o ProfiPy para especificar seu modelo de falha usando uma linguagem específica do domínio, configurar a carga de falhas e a carga de trabalho e automatizar experimentos usando virtualização baseada em contêineres.

Nuvem

O ProfiPy é fornecido como software como serviço, tornando-o adequado para ambientes baseados em nuvem. A ferramenta oferece suporte à automação total de experimentos usando virtualização baseada em contêineres, que se alinha bem aos princípios da computação em nuvem. O ProfiPy pode executar vários experimentos paralelos em sandboxes independentes, aproveitando CPUs de vários núcleos, o que é benéfico para serviços em nuvem.

VFIT

Paper: Improvement of Fault Injection Techniques Based on VHDL Code Modification

Paper: A prototype of a VHDL-based fault injection tool: description and application

Aplicação

A ferramenta VFIT é um protótipo de uma ferramenta de injeção de falhas automática e independente de modelo projetada para plataformas IBM-PC. Ela foi construída em torno de um simulador VHDL comercial e é capaz de injetar uma ampla gama de modelos de falhas que superam os modelos clássicos como stuck-at e bit-flip. Além disso, pode injetar falhas permanentes, transitórias e intermitentes usando várias funções de distribuição de probabilidade. A ferramenta é capaz de injetar falhas nos níveis de porta, registro e chip, além de realizar a análise da síndrome de erro e a validação do FTS para melhorar a confiabilidade do sistema.

Cenário

A ferramenta VFIT pode ser utilizada em sistemas de média complexidade para realizar campanhas de injeção de falhas. Ela é capaz de injetar uma ampla gama de modelos de falhas, indo além dos modelos clássicos de stuck-at e bit-flip. Além disso, a ferramenta pode analisar os resultados obtidos das campanhas de injeção, a fim de estudar a Síndrome de Erro do modelo do sistema e/ou validar seus mecanismos de tolerância a falhas.

Disponibilidade

As informações de preços da ferramenta VFIT não são explicitamente mencionadas nas fontes fornecidas.

Nuvem

É descrita como uma ferramenta de injeção de falhas baseada em VHDL, projetada para trabalhar em um PC (ou compatível) sob WindowsTM, e é adequada para campanhas de injeção em sistemas de média complexidade.