Pertemuan 10
FAULT TOLERANCE

Copyright © September 2022

Pokok Bahasan

- Pengertian Foult Tolerance
- Basic concepts
- Failure model
- Failure masking and redudancy
- Recovery

Copyright © September 2022

Pengertian Foult Tolerance

Fitur karakteristik dari sistem terdistribusi yang membedakannya dari sistem mesin tunggal adalah gagasan kegagalan parsial. Kegagalan parsial dapat terjadi ketika satu komponen dalam sistem terdistribusi gagal. Kegagalan ini dapat memengaruhi pengoperasian komponen lainnya dengan benar, sementara pada saat yang sama meninggalkan komponen lain yang sama sekali tidak terpengaruh. Sebaliknya, kegagalan dalam sistem tidak terdistribusi seringkali total dalam arti bahwa hal itu mempengaruhi semua komponen, dan dapat dengan mudah menjatuhkan sistem pusat.

Copyright © September 2022

Tujuan penting dalam desain sistem terdistribusi adalah untuk membangun sistem sedemikian rupa sehingga dapat secara otomatis pulih dari kegagalan parsial tanpa secara serius mempengaruhi kinerja keseluruhan. Secara khusus, setiap kali terjadi kegagalan, sistem terdistribusi harus terus beroperasi dengan cara yang dapat diterima saat perbaikan sedang dilakukan, yaitu, itu harus mentolerir kesalahan dan terus beroperasi ke beberapa orang yang ada di hadapan mereka.

 Copyright © September 2022

Dalam bahasan ini, dengan melihat lebih dekat teknik untuk membuat sistem terdistribusi toleran terhadap kesalahan. Setelah memberikan latar belakang umum tentang toleransi kesalahan, akan dilihat ketahanan proses dan multicasting yang andal. Ketahanan proses menggabungkan teknik yang satu atau lebih proses dapat gagal tanpa mengganggu sistem lainnya. Terkait dengan masalah ini adalah multicasting yang andal, dimana transmisi pesan ke kumpulan proses dijamin berhasil.

Copyright © September 2022

Basic Concepts

Untuk memahami peran toleransi kesalahan dalam sistem terdistribusi, pertama-tama perlu melihat lebih dekat apa arti sebenarnya dari sistem terdistribusi untuk mentolerir kesalahan. Menjadi toleran terhadap kesalahan sangat terkait dengan apa yang disebut sistem yang dapat diandalkan. Ketergantungan adalah istilah yang mencakup sejumlah persyaratan yang berguna untuk sistem terdistribusi termasuk yang berikut:

1. Ketersediaan
2. Keandalan
3. Keamanan
4. Maintainability

Copyright © September 2022

Ketersediaan didefinisikan sebagai properti yang sistem siap digunakan segera. Secara umum, ini mengacu pada probabilitas bahwa sistem beroperasi dengan benar. setiap saat dan tersedia untuk menjalankan fungsinya atas nama penggunanya. Dengan kata lain, sistem yang sangat tersedia adalah sistem yang kemungkinan besar akan bekerja pada saat tertentu.

Copyright © September 2022

Keandalan mengacu pada properti yang sistem dapat berjalan terus menerus tanpa kegagalan. Berbeda dengan ketersediaan, keandalan didefinisikan dalam hal interval waktu alih-alih waktu instan. Sistem yang sangat andal adalah sistem yang kemungkinan besar akan terus bekerja tanpa gangguan selama periode waktu yang relatif lama. Ini adalah perbedaan yang halus tetapi penting jika dibandingkan dengan ketersediaan.

Copyright © September 2022

Keselamatan mengacu pada situasi bahwa ketika suatu sistem sementara gagal untuk beroperasi dengan benar, tidak ada bencana yang terjadi. Misalnya, banyak sistem kontrol proses, seperti yang digunakan untuk mengendalikan pembangkit listrik tenaga nuklir atau mengirim orang ke luar angkasa, diperlukan untuk memberikan tingkat keamanan yang tinggi. Jika sistem kontrol seperti itu untuk sementara gagal hanya untuk sesaat yang sangat singkat, efeknya bisa menjadi bencana.

Copyright © September 2022

Akhirnya, rawatan mengacu pada betapa mudahnya sistem dapat diperbaiki. Sistem yang sangat terpelihara juga dapat menunjukkan tingkat ketersediaan yang tinggi, terutama jika kegagalan dapat dideteksi dan diperbaiki secara otomatis. Namun, seperti yang dapat dilihat nanti dalam pembahasan ini, secara otomatis pulih dari kegagalan lebih mudah dikatakan daripada dilakukan. Seringkali, sistem yang dapat diandalkan juga diperlukan untuk memberikan tingkat keamanan yang tinggi, terutama ketika menyangkut masalah seperti integritas. Akan dibahas keamanan dalam pembahasan berikutnya.

Copyright © September 2022

Suatu sistem dikatakan gagal ketika tidak dapat memenuhi janjinya. Khususnya, jika suatu sistem terdistribusi dirancang untuk menyediakan sejumlah layanan kepada penggunanya, sistem tersebut akan gagal ketika satu atau lebih dari layanan tersebut tidak dapat (sepenuhnya) disediakan. Kesalahan adalah bagian dari kondisi sistem yang dapat menyebabkan kegagalan. Misalnya, ketika mengirimkan paket melalui jaringan, diharapkan bahwa beberapa paket telah rusak ketika mereka tiba di penerima. Rusak dalam konteks ini berarti bahwa penerima mungkin merasakan nilai abit secara keliru (mis., Membaca 1 bukannya 0), atau bahkan mungkin tidak dapat mendeteksi bahwa sesuatu telah tiba.

Copyright © September 2022

Penyebab kesalahan disebut Fault. Jelas, mencari tahu apa yang menyebabkan kesalahan itu penting. Misalnya, media transmisi yang salah atau buruk dapat dengan mudah menyebabkan paket menjadi rusak. Dalam hal ini, relatif mudah untuk menghapus kesalahan. Namun, kesalahan transmisi juga dapat disebabkan oleh kondisi cuaca buruk seperti di jaringan nirkabel. Mengubah cuaca untuk mengurangi atau mencegah kesalahan agak sulit.

Copyright © September 2022

Failure Models

Sistem yang gagal tidak cukup menyediakan layanan yang dirancang untuknya. Jika menganggap sistem terdistribusi sebagai kumpulan server yang berkomunikasi satu sama lain dan dengan klien mereka, tidak menyediakan layanan berarti bahwa server, saluran komunikasi, atau mungkin keduanya, tidak melakukan apa yang seharusnya mereka lakukan. Namun, server yang rusak itu sendiri mungkin tidak selalu menjadi kesalahan yang dicari. Jika server seperti itu bergantung pada server lain untuk menyediakan layanannya secara memadai, penyebab kesalahan mungkin perlu dicari di tempat lain.

Copyright © September 2022

Hubungan ketergantungan seperti itu muncul dalam sistem tak terdistribusi yang berlimpah. Disk yang gagal dapat mempersulit server file yang dirancang untuk menyediakan sistem file yang sangat tersedia. Jika server file seperti itu merupakan bagian dari basis data terdistribusi, kerja yang tepat dari seluruh basis data mungkin dipertaruhkan, karena hanya sebagian dari datanya yang dapat diakses.

Copyright © September 2022

Untuk mendapatkan pemahaman yang lebih baik tentang seberapa serius kegagalan sebenarnya, beberapa skema klasifikasi telah dikembangkan yaitu:

Type of failure	Description
Crash failure	A server halts, but is working correctly until it halts
Omission failure *Receive omission* *Send omission*	A server fails to respond to incoming requests A server fails to receive incoming messages A server fails to send messages
Timing failure	A server's response lies outside the specified time interval
Response failure *Value failure* *State transition failure*	A server's response is incorrect The value of the response is wrong The server deviates from the correct flow of control
Arbitrary failure	A server may produce arbitrary responses at arbitrary times

Gambar 1. Different types of failures.

Copyright © September 2022

Kegagalan kerusakan terjadi saat server berhenti sebelum waktunya, tetapi berfungsi dengan benar hingga berhenti. Aspek penting dari kegagalan crash adalah bahwa begitu server berhenti, tidak ada lagi yang terdengar darinya. Contoh umum kegagalan kerusakan adalah sistem operasi yang berhenti bekerja, dan hanya ada satu solusi: reboot. Banyak sistem komputer pribadi sering mengalami kegagalan karena crash sehingga orang-orang mengharapkannya normal. Akibatnya, memindahkan tombol reset dari belakang kabinet ke depan dilakukan untuk alasan yang baik. Mungkin suatu hari bisa dipindahkan ke belakang lagi, atau bahkan dihilangkan sama sekali.

Copyright © September 2022

Failure Masking and Redundancy

Jika suatu sistem harus toleran terhadap kesalahan, yang terbaik yang bisa dilakukan adalah mencoba menyembunyikan terjadinya kegagalan dari proses lain. Teknik teknik untuk menutupi kesalahan adalah menggunakan redundansi. Tiga macam mungkin: redundansi informasi, redundansi waktu, dan redundansi fisik. Dengan redundansi informasi, bit tambahan ditambahkan untuk memungkinkan pemulihan dari bit yang kacau. Sebagai contoh, kode kerusakan dapat ditambahkan data yang dikirim total untuk memulihkan dari kebisingan pada saluran transmisi.

Copyright © September 2022

Dengan redundansi waktu, suatu tindakan dilakukan, dan kemudian. jika perlu, itu dilakukan lagi. Transaksi menggunakan pendekatan ini. Jika suatu transaksi dibatalkan, hal itu dapat dilakukan kembali tanpa membahayakan. Redundansi waktu sangat membantu ketika kesalahan bersifat sementara atau terputus-putus.

Dengan redundansi fisik, peralatan atau proses tambahan ditambahkan untuk memungkinkan sistem secara keseluruhan mentolerir kehilangan atau kegagalan fungsi beberapa komponen. Redundansi fisik dengan demikian dapat dilakukan baik dalam perangkat keras maupun perangkat lunak. Sebagai contoh, proses tambahan dapat ditambahkan ke sistem sehingga jika sejumlah kecil dari mereka crash, sistem masih dapat berfungsi dengan benar.

 Copyright © September 2022

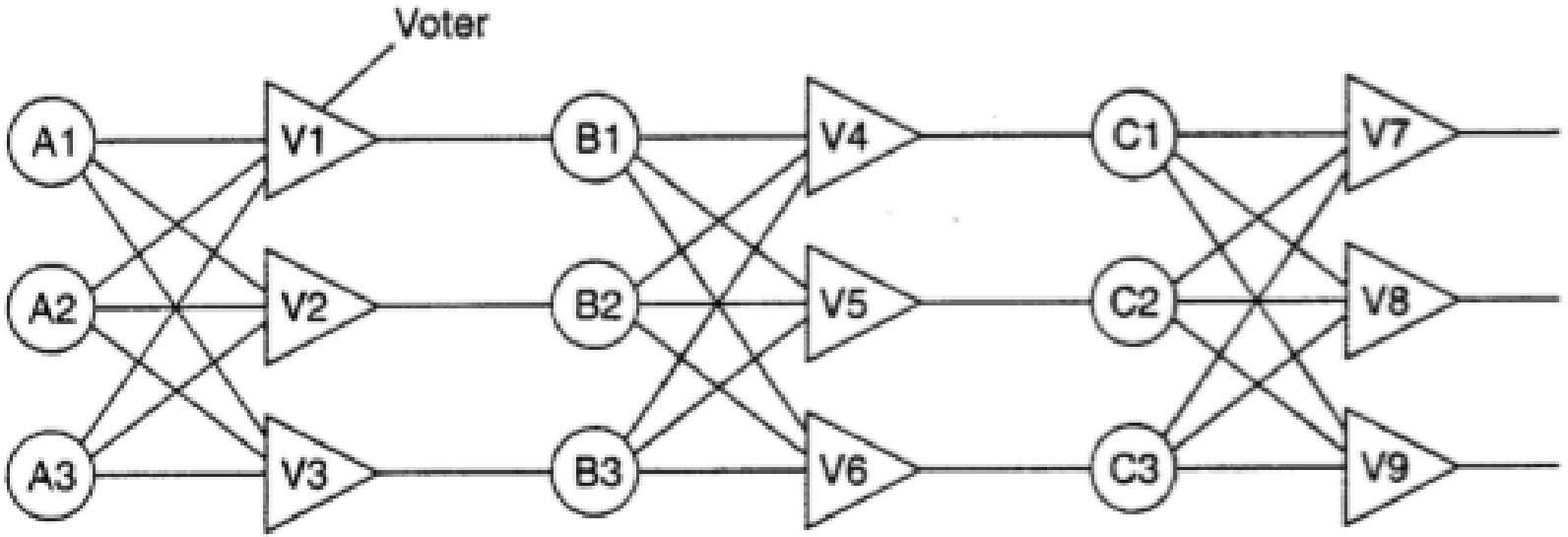
Redundansi fisik adalah teknik yang terkenal untuk memberikan toleransi kesalahan. Ini digunakan dalam biologi (mamalia memiliki dua mata, dua telinga, dua paru-paru, dll.), Pesawat terbang (747 memiliki empat mesin tetapi dapat terbang tiga), dan olahraga (beberapa wasit memunculkan satu melewatkan acara). Itu juga telah digunakan untuk toleransi kesalahan di sirkuit elektronik selama bertahun-tahun; itu ilustratif untuk melihat bagaimana itu diterapkan di sana. Pertimbangkan, misalnya, rangkaian Gambar 2. Di sini sinyal melewati perangkat A, B, dan C, secara berurutan. Jika salah satu dari mereka rusak, hasil akhirnya kemungkinan akan salah.

Gambar 2. Sequencial Circuit

 Copyright © September 2022

Di permasalahan yang berbeda, setiap perangkat direplikasi tiga kali. Setelah setiap tahap dalam sirkuit adalah pemilih rangkap tiga. Setiap pemilih adalah sirkuit yang memiliki tiga input dan satu output. Jika dua atau tiga input sama, output sama dengan input itu. Jika ketiga input berbeda, output tidak ditentukan. Jenis desain ini dikenal sebagai TMR (Triple Modular Redundancy). Misalkan elemen Az gagal. Masing-masing pemilih, Vb Vz, dan V3 mendapatkan dua input bagus (identik) dan satu input jahat, dan masing-masing dari mereka menghasilkan nilai yang benar untuk tahap kedua. Pada intinya, efek dari fail gagal sepenuhnya ditutup-tutupi, sehingga input ke BI, Bz, dan B3 persis sama seperti yang seharusnya seandainya kesalahan tidak terjadi. Perhatikan Gambar 3.

 Copyright © September 2022



Gambar 3. Triple modular redundancy.

 Copyright © September 2022

Misalkan elemen Az gagal. Masing-masing pemilih, Vb Vz, dan V3 mendapatkan dua input bagus (identik) dan satu input jahat, dan masing-masing dari mereka menghasilkan nilai yang benar untuk tahap kedua. Pada intinya, efek dari fail gagal sepenuhnya ditutup-tutupi, sehingga input ke BI, Bz, dan B3 persis sama seperti yang seharusnya seandainya kesalahan tidak terjadi. Sekarang pertimbangkan apa yang terjadi jika B3 dan C1 juga salah, selain Az · Efek ini juga sudah sama, sehingga keluaran akhir masih benar.

Copyright © September 2022

Pada awalnya mungkin tidak jelas mengapa diperlukan tiga pemilih di setiap tahap. Lagi pula, satu pemilih juga bisa mendeteksi dan melewati pandangan mayoritas. Namun, seorang pemilih juga merupakan komponen dan bisa juga salah. Anggaplah, misalnya, bahwa kerusakan fungsi pemilih VI. Input ke BI kemudian akan salah, tetapi selama semuanya bekerja, Bz dan B3 akan menghasilkan output yang sama dan V4, Vs, dan V6 semuanya akan menghasilkan hasil yang benar ke tahap tiga. Kesalahan dalam VI secara efektif tidak berbeda daripada kesalahan dalam BI.Dalam kedua kasus BI menghasilkan output yang salah, tetapi dalam kedua kasus itu dinilai lebih rendah dan hasil akhirnya masih benar.

Copyright © September 2022

Meskipun tidak semua sistem terdistribusi toleransi kesalahan menggunakan TMR, teknik ini sangat umum, dan harus memberikan perasaan yang jelas untuk apa sistem toleran-gangguan adalah, dibandingkan dengan sistem yang komponen individualnya sangat andal tetapi yang organisasinya tidak dapat mentolerir kesalahan (yaitu , beroperasi dengan benar bahkan di hadapan komponen yang salah). Tentu saja, TMR dapat diterapkan secara rekursif, misalnya, 'untuk membuat chip yang sangat andal dengan menggunakan TMR di dalamnya, tidak diketahui oleh perancang yang menggunakan chip, mungkin di sirkuit mereka sendiri yang berisi banyak salinan chip bersama dengan para pemilih.

Copyright © September 2022

RECOVERY

Toleransi mendasar untuk kesalahan adalah pemulihan dari kesalahan. Ingat bahwa kesalahan adalah bagian dari suatu sistem yang dapat menyebabkan kegagalan. Seluruh gagasan pemulihan kesalahan adalah mengganti keadaan yang salah dengan keadaan bebas kesalahan. Pada dasarnya ada dua bentuk pemulihan teror. Dalam pemulihan mundur, masalah utama adalah membawa sistem dari kondisi salah yang sekarang kembali ke keadaan yang sebelumnya benar. Untuk melakukannya, akan perlu untuk merekam keadaan sistem dari waktu ke waktu, dan mengembalikan keadaan yang direkam tersebut ketika terjadi kesalahan. Setiap kali (bagian dari) kondisi sekarang sistem dicatat, titik pencapaian dikatakan dibuat.

Copyright © September 2022

Bentuk lain dari pemulihan kesalahan adalah pemulihan ke depan. Dalam hal ini, ketika sistem telah memasuki keadaan yang salah, alih-alih pindah kembali ke keadaan sebelumnya yang telah diperiksa, suatu upaya dilakukan untuk membawa sistem dalam keadaan baru yang benar dari mana ia dapat terus dieksekusi. Masalah utama dengan mekanisme pemulihan kesalahan maju adalah bahwa hal itu harus diketahui sebelumnya kesalahan mana yang mungkin terjadi. Hanya dalam kasus itu adalah mungkin untuk memperbaiki kesalahan itu dan memindahkan keadaan baru.

Copyright © September 2022