Technische Universität Braunschweig

Institut für Betriebssysteme und Rechnerverbund

Verteilte Systeme - 5. Übung

Dr. Jens Brandt

Sommersemester 2011

Transaktionen

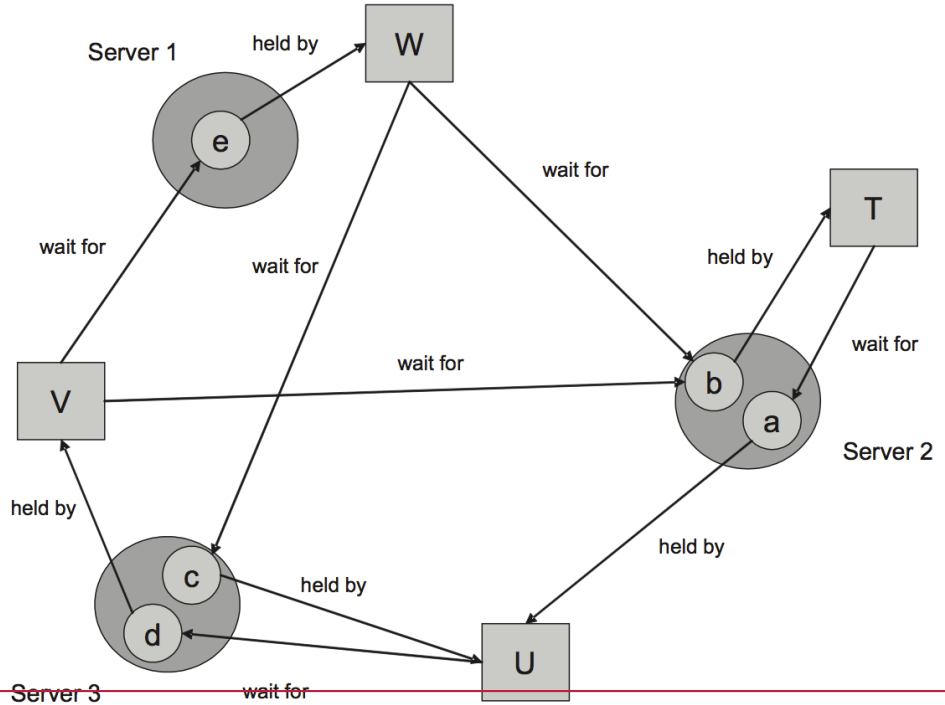
a) Erläutere was Transaktionen sind und wofür diese benötigt werden.
   - Folge von Operationen mit bestimmten Eigenschaften:
     - Atomicity
     - Consistency
     - Isolation
     - Durability
   - Schutz von Ressourcen vor gleichzeitigem Zugriff
   - Zugriff auf mehrere Ressourcen in einer atomaren Operation
   - Rückabwicklung im Fehlerfall

Transaktionen

b) Wie können Verklemmungen (Deadlocks) entstehen?

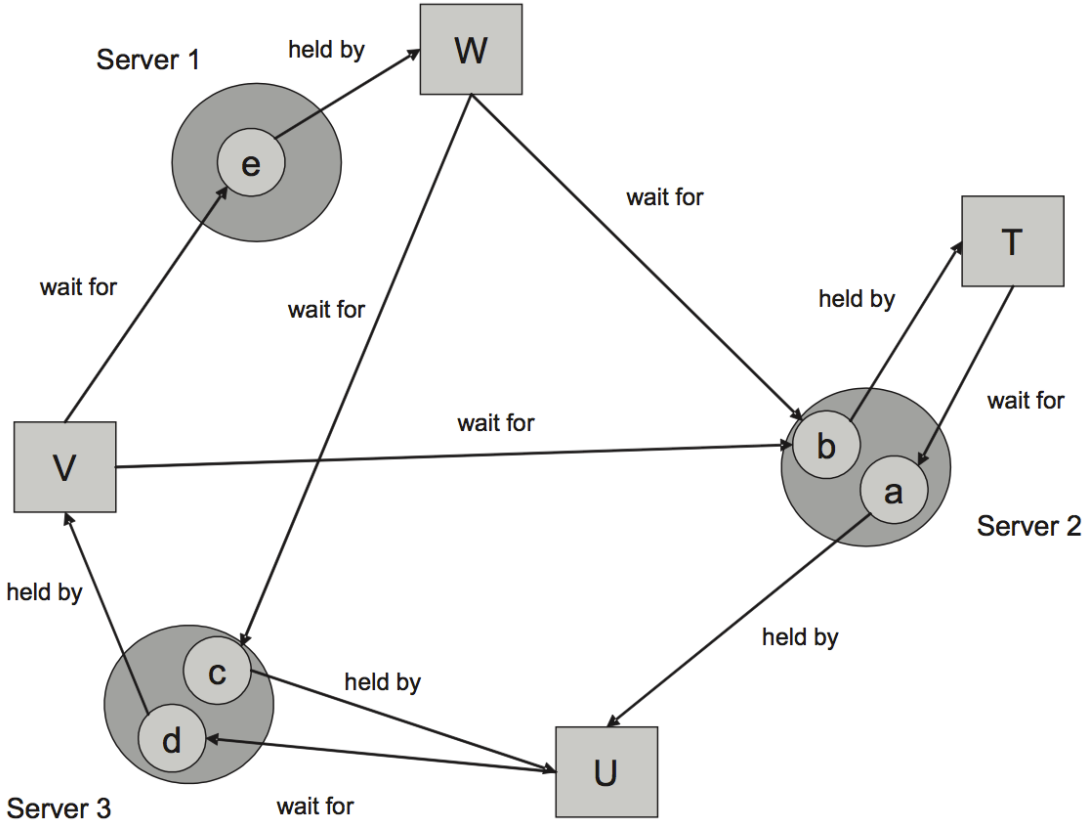
- Nebenläufigkeit
- Gegenseitiges Warten auf Lock

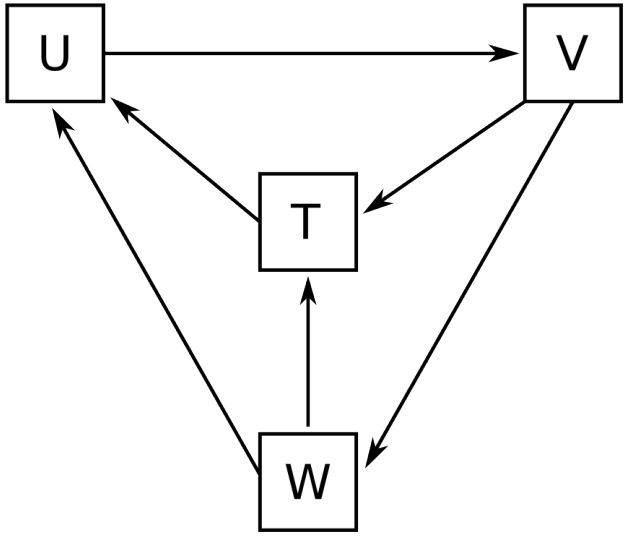
b) Bestimme den Wait-For-Graph der Transaktionen T, U, V und W für das folgende Szenario. Liegt hier eine Verklemmung vor?



Transaktionen

Wait-For-Graph der Transaktionen T, U, V





$\Rightarrow$ Deadlock

Konsistenz

a) Beschreibe, warum in verteilten Systemen schwache Konsistenz in Betracht gezogen wird. Gehe dabei auch auf die Motivation von Replikation ein.

- Replikation von Daten für Performancegewinn
- Knoten können performanter auf Daten zugreifen
- Aufwand für strikte Konsistenz ist gegenläufig zum Performancegewinn durch Replikation.

Konsistenz

b) Erläutere die behandelten datenzentrierten Konsistenzmodelle.

1. Kausale Konsistenz:
   Kausal zusammenhängende Zugriffe in gleicher Reihenfolge
2. Sequentielle Konsistenz:
   Zugriffe in gleicher Reihenfolge
3. Linearisierbarkeit:
   Zugriffe in gleicher Reihenfolge und zeitlich geordnet
4. Strikte Konsistenz:
   Absolute zeitliche Ordnung

c) Mit welcher Art von Konsistenz kann eine Plattform für Aktienhandel implementiert werden? Begründe deine Wahl.

- Kausale Konsistenz sollte ausreichen.
- Wertänderungen müssen konsistent sein.
- Unabhängige Änderungen nicht relevant

Konsistenz

d) Erläutere den Begriff der clientzentrierten Konsistenz.

- Sicht des Clients
- Weniger starke Annahmen
- keine gleichzeitigen Updates

Replikationsverwaltung

a) Erläutere die Motivation zur Erzeugung von Replikaten.

- Zuverlässigkeit
- Datensicherheit
- Zugriffsgeschwindigkeit

b) Nenne und erläutere die vorgestellten, unterschiedlichen Arten von Kopien eines Datenspeichers.

- Permanent: dauerhaft vorliegende Replikate
  (Bsp. Mirroring von Webseiten, replizierte DNS-Server)
- Serverinitiiert: bei Bedarf durch den Server veranlasst
  (Bsp. Web Hosting Services, Content Delivery Networks)
- Clientinitiiert: durch den Client erzeugt (Client Cache)

Replikationsverwaltung

c) Wie können Updates in replizierten Datenspeichern verteilt werden?

- Was wird propagiert?
  - Sende geänderte Werte
  - Sende Nachricht, dass eine Änderung erfolgt ist
  - Sende Nachricht mit ausgeführter Operation
- Wie wird propagiert? (push/pull, Uni-/Multicast)
  - Push: Updates werden aktiv verteilt
  - Pull: Updates werden aktiv abgerufen
  - Unicast: Eine Nachricht/Verbindung pro Replikat
  - Multicast: Eine Nachricht an alle Server

Fehlertoleranz

a) Beschreibe die vier Grundeigenschaften, die ein verlässliches System aufweisen sollte.
   - Verfügbarkeit
   - Zuverlässigkeit
   - Sicherheit
   - Wartbarkeit

b) Wie kann ein verteiltes System fehlertolerant gestaltet werden?
   - Reaktion auf Ausfälle
   - Einführung von Redundanz

Sicherheit

a) Welche Sicherheitsrichtlinien gibt es?

- Authentizität: Korrektheit von Identitätsbehauptungen
- Integrität: Feststellen nicht authorisierter Datenänderungen
- Vertraulichkeit: Nur legitimierte Nutzer teilen Geheimnisse
- Nicht-Anfechtbarkeit: Stattgefundene Kommunikation kann nicht geleugnet werden
- Zugriffskontrolle: Zugriff auf Ressourcen durch Authentisierung gesteuert
- Verfügbarkeit: Service steht zur Verfügung, wenn er benötigt wird

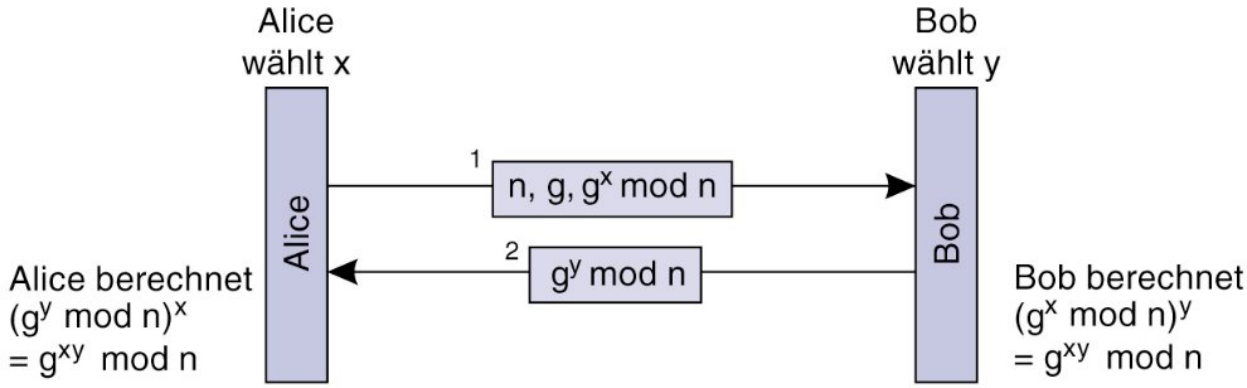
Sicherheit

b) Welche Sicherheitsrichtlinien sind für einen Online-Shops relevant? Wie können diese verletzt werden?

- Integrität: Änderung von Rechnungsbeträgen
- Authentizität: Einkaufen mit fremdem Account / auf fremden Namen
- Verfügbarkeit: Absturz des Shop-Servers
- Nicht-Anfechtbarkeit: Quasi nicht möglich (und nötig)

Sitzungsschlüssel

a) Mit Hilfe des Diffie-Hellman Schemas kann ein sicherer Sitzungsschlüssel erstellt werden:



Welche Sicherheitsrichtlinien können damit eingehalten werden?

- Authentizität: Nein
- Integrität: Nein
- Vertraulichkeit: Ja
- Nicht-Anfechtbarkeit: Nein

Sitzungsschlüssel

b) Bei PGP werden sowohl symmetrische Sitzungsschlüssel als auch asymmetrische Schlüssel für den Austausch der Sitzungsschlüssel verwendet. Warum ist dieses Vorgehen prinzipiell sinnvoll?

- Symmetrische Verschlüsselung ist performanter
- Asymmetrische Verfahren stellen Authentizität, Integrität und Nicht-Anfechtbarkeit bereit
- Symmetrisches Verfahren stellt Vertraulichkeit bereit

The Eight Fallacies of Distributed Computing

1. The network is reliable
2. Latency is zero
3. Bandwidth is infinite
4. The network is secure
5. Topology doesn't change
6. There is one administrator
7. Transport cost is zero
8. The network is homogeneous

Peter Deutsch

Fragen?

brandt@ibr.cs.tu-bs.de

Wiederholung, Fragen, Prüfungsvorbereitung:
12.07.2011 09:45 - 11:15 Uhr