Resumen teoria.pdf

julvos

Sistemas Distribuidos

3º Grado en Ingeniería Informática

Escuela de Ingeniería y Arquitectura
Universidad de Zaragoza

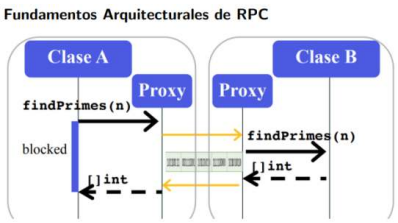
RPC

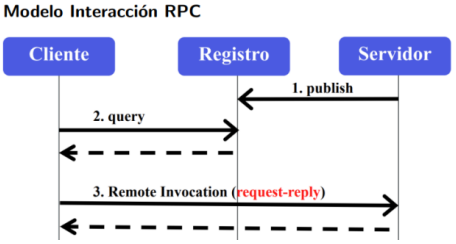
El cliente invoca un procedimiento remoto como si fuese local.

El servidor publica una interfaz

Se genera código automático para serializar los datos

Cuando un proceso A invoca a un proceso B, A se queda bloqueado.





Modelo Actor

Un Actor es un proceso. Cada proceso tiene un identificador único PID

Puede recibir y enviar mensajes de forma asíncrona

Solo tiene memoria local

Un proceso recibe los mensajes en un buzón

Ricart-Agrawala

Comportamiento en general

- N procesos se comunican por paso de mensajes en una red libre de errores. Mensajes pueden llegar fuera de orden.
- Si Pi desea acceder a la SC y recibe una petición de acceso a la SC (request) con más timestamp, la posterga (y la almacena en una cola)
- Si no desea acceder a la SC o recibe una petición de acceso a la SC (request) de menos timestamp, envía inmediatamente el ack.
- Coste -> N-1 envíos de request y N-1 esperas de ack

Preprotocol de Pi

- Pi envía request(i, Ti) a todos los procesos (N – 1)
- Pi espera las (N - 1) respuestas ack (sin estampilla)
- Cuando recibe todas las respuestas ack, accede a la SC

Postprotocol -> envía un mensaje de ack para todos los mensaje postergados

Raft

(miraré los VoF)

Algoritmo del matón

(miraré los VoF)

Contenedores

- Es un entorno de ejecución virtualizado utilizado en el desarrollo de aplicaciones.
- Se utiliza para crear, ejecutar y desplegar aplicaciones que están aisladas del hardware subyacente.
- Aislamiento de recursos
- Docker -> herramienta para automatizar el despliegue de aplicaciones en un conjunto de imágenes autosuficientes, portables y ligeros que puedan ejecutarse en una máquina.
    - Encapsulación de servicios, aplicaciones y sus dependencias.
    - Ligero de operar, mover, manipular
    - Separación entre implementación del modelo y la infraestructura.
    - Aislamiento de recursos, red y contenido entre aplicaciones.

Kubernetes

Automatizar y desplegar aplicaciones en muchas máquinas mediante contenedores.

Eficiente, robusto, escalable.

Soporte de tolerancia a fallos y monitorización.

Código de dominio público implementado en Golang

Pod

- Unidad de ejecución en Kubernetes. Se usa para ejecutar una instancia de una aplicación.
- Puede contener 1 o múltiples contenedores, aunque lo normal es que haya solo 1.
- Sistema de ficheros compartidos entre contenedores
- Cada contenedor tiene su hardware delimitado.
- Cada uno tiene su propia IP única en el cluster.
- Todos los pods pueden comunicarse entre ellos sin NAT y participar en servicios.

Kubectl para adminstrar un cluster de Kubernetes.

Tipos de aplicaciones

- Deployment -> gestión estilo Puppet de puesta en marcha de Pods o ReplicaSets. Se declara un estado de configuración a alcanzar a un determinado ritmo.
- StatefulSet -> como los deployments, pero mantiene garantías de unicidad de Pods y su orden de puesta en marcha y eliminación.
- Services -> conjunto lógico de Pods y política de acceso a ellos. IPs ligadas a Pods desaparecen con ellos, pero el servicio necesita punto de acceso estable eliminación.

Comunicación en Grupo

COMUNICACIÓN MULTICAST

Requisitos

- Cada grupo se identifica con una dirección IP
- Los grupos pueden ser de tamaño variable (dinámico)
- Los miembros de un grupo se pueden encontrar en cualquier parte de Internet
- Los miembros de un grupo pueden unirse y abandonar al grupo libremente
- La pertenencia a un grupo no se conoce a priori
- Los emisores no tienen por qué ser miembros del grupo

Los mensajes los reciben todos los miembros o ninguno (Atomic Multicast). Si los procesos se añaden o borran de un grupo se notifica el cambio a todos los miembros activos para mantener la consistencia entre ellos.

Se quiere garantizar atomicidad, uniformidad y terminación.

Los mensajes deben llegar a todos los miembros en el mismo orden. Los mensajes con relaciones de causalidad tienen que llegar en orden causal. Todos los nodos tienen el mismo orden de recepción.

IP Multicast usa UDP -> no fiable. Buena solución para una LAN controlada pero no para internet.

Alternativas a IP Multicas -> gossiping. Envía uno a varios. Esos varios envían luego a otros varios, etc.

Transacciones distribuidas

Una transacción distribuida define una secuencia de operaciones en un conjunto de servidores. Se garantiza que la secuencia es atómica, o se ejecuta completamente o no se ejecuta (comprometida al completo o se aborta). Además, pueden coexistir múltiples clientes y múltiples servidores y todos ellos pueden fallar.

ACID -> Atómica Consistente Isolation Durabilidad

Seguridad

Acceso seguro a la información y recursos -> confidencialidad, integridad y disponibilidad.

Hay que definir normas de seguridad que utilizarán mecanismos para garantizar la seguridad.

Amenazas: filtración, manipulación, vandalismo, espionaje, enmascaramiento (fishing) y denegación de servicio (inundar un canal u otro recurso con mensajes para denegar el acceso a otros).

Criptografía

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos Holandés con una garantía de hasta 100.000 euros por depositante. Consulta más información en ing.es

Que te den **10 € para gastar** es una fantasía. ING lo hace realidad.

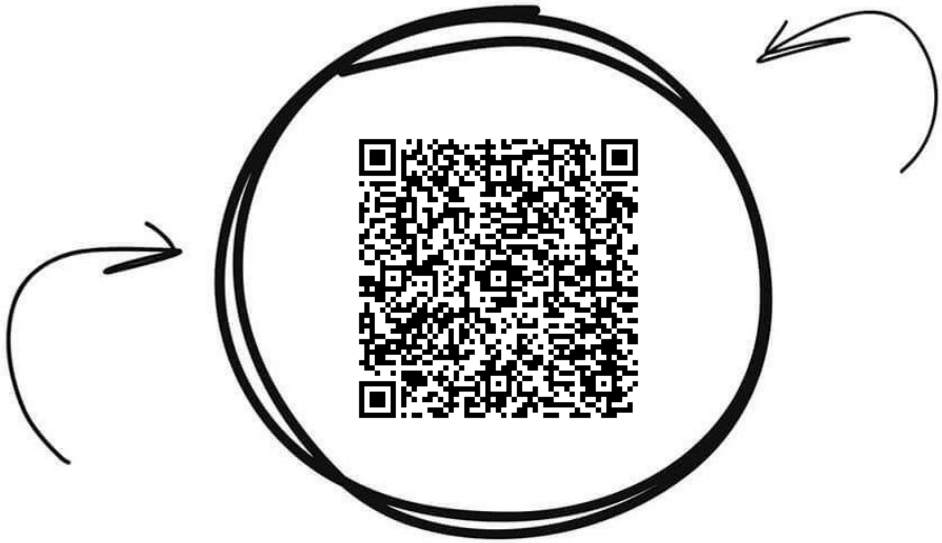
Abre la **Cuenta NoCuenta** con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Quiero el cash

Consulta condiciones **aquí**

do your thing

Sistemas Distribuidos



Banco de apuntes de la

WUOLAH

Comparte estos flyers en tu clase y consigue más dinero y recompensas

1. Imprime esta hoja
2. Recorta por la mitad
3. Coloca en un lugar visible para que tus compis puedan escanar y acceder a apuntes
4. Llévate dinero por cada descarga de los documentos descargados a través de tu QR

- De clave simétrica -> misma clave tanto para cifrar como para descifrar
- De clave pública -> se cifra y descifra con claves diferentes.
- Funciones hash -> a una secuencia de datos se le corresponde una secuencia de números.

Certificados digitales

Existe un conjunto de autoridades certificadoras para firmar certificados que puedan utilizarse en Internet.

Firma digital: cifrar(Hash(datos-certificado),Kpriv-CA). Con Kpublica CA se puede descifrar el mensaje y comprobar hash.

TLS

Constituido por 3 protocolos de nivel superior

- Protocolo de apretón de manos: negocia algoritmos de seguridad y parámetros, intercambia claves.
- Protocolo de cambio de especificación de cifrado: mensaje final que indica el acuerdo.
- Protocolo de alerta: mensajes de error.
- Protocolo de registro en el nivel inferior: fragmentación, comprensión y autentificación de mensaje y protección de integridad.

Kerberos

Servicio de autentificación y comunicación segura en ssdd. Responde a los problemas de utilización de mecanismos de cifrado como son el coste computacional de algoritmos de cifrado y el cómo distribuir las claves.

- Entidad tercera almacena claves secretas y permite autentificarse entre entidades con dificultades para intercambiar claves (Centro de Distribución de Claves, KDC). Posteriormente, KDC provee tickets para servicios de seguridad entre entidades. Estos son:
    - Autentificados y no falsificables
    - Con mecanismo para impedir ataques de reinyección
    - Contiene id, clave secreta de sesión, tiempo de vida limitado y tiempo de creación.
- Autentificación servicios de red, máquinas, usuarios.
- Servicio Single sign-on (SSO) para autentificación centralizada. Las contraseñas circulan cifradas por la red.
- Utiliza cifrado simétrica por menor coste computacional
- Mayor dificultad de implementación: compartir claves secretas.
- También puede utilizarse para comunicación confidencial e integra.

Debilidades

- Una autoridad central (KDC) distribuye y contiene todas las claves del ssdd.
- Se utiliza replicación de KDC, con consistencia eventual, para mitigar el problema del fallo.
- Un acceso no autorizado al servicio central compromete las claves.