

QUALITY ASSURANCE

CURS 6

AGENDA

- **Performance**
- **Security**

LOAD TESTING

LOAD TESTING

- Realizarea de cereri la un sistem sau dispozitiv si masurarea raspunsului
- Practica de a modela utilizarea asteptata/previzionata a unui sistem software prin simularea unui numar de utilizatori care acceseaza sistemul concurrent
- Relevant in cazul sistemelor multi-user, cum ar fi aplicatii web
- Cateodata denumit test ne-functional
- Lucreaza la nivel de protocol

BENEFICII

- **Reduce riscurile de downtime**
- **Creste calitatea instalabilitatii (deployment)**
- **Identifica probleme de performanta**
- **Reduce costurile defectelor si creste satisfactia clientului**
- **Ofera statistici tangibile echipei de dezvoltare**
- **Benchmark util in tot SDLC**
- **Imbunatateste scalabilitatea si reduce riscul asociat cu cerintele de performanta viitoare**

UTILIZARE

- **Smoke** – cum se comporta sistemul sub incarcare usoara pentru o durata scurta de timp
- **Stress** – pentru a determina daca sistemul va functiona corect sub incarcare mare pentru o durata mare de timp
- **Performance** – pentru a determina cat de rapid raspunde sistemul la cereri la diferite nivele de incarcare
- **Capacity** – pentru a determina cati utilizatori si/sau tranzactii poate suporta sistemul indeplinind criteriile de performanta

ABORDAREA

- **Identificarea obiectivelor de performanta**
- **Identificarea scenariilor cheie**
- **Identificarea unui model de incarcare**
- **Identificarea metricilor de colectat**
- **Design**
- **Executie – simulare load**
- **Analiza**

OBIECTIVE

- **Response time – pagina de home trebuie afisata in mai putin de 3 secunde**
- **Throughput – Sistemul trebuie sa suporte 100 de cereri pe secunda**
- **Utilizarea resurselor – CPU, RAM, disk I/O, network I/O, etc**
- **Maximum User Load – Determinarea numarului maxim de utilizatori care pot fi serviti pe o anumita configuratie hardware**

SCENARII

- **Functionalitati accesate in general de utilizatori care implica in general diferite activitati/actiuni**
- **Scenarii cheie sunt cele pentru care exista criterii specifice de performanta sau care au un impact semnificativ asupra performantei**
- **Exemple**
 - Login
 - Home
 - Browse products
 - Order

WORKLOAD

- **Identificare distributiei**
 - Web server logs
 - Research
- **User load**
 - Care este numarul maxim de utilizatori concurenti astept?

User Scenarios	% of Work distribution
Browse	50
Search	30
Place Order	20
Total	100

User Scenarios	% of users	Users
Browse	50	250
Search	30	150
Place Order	20	100
Total	100	500

METRIC

- Oferă informații despre cât de aproape este sistemul de obiectivele stabilite
- Ajută la identificarea zonelor cu probleme (bottlenecks)
- Network specific
- System specific
- Platform specific
- Application specific
- Alte exemple
 - CPU load
 - RAM load
 - Requests failed
- Sample rate depinde de durată testului

Metric	Accepted level
Request Execution time	Must not exceed 8 seconds
Request Rejected	Less than 5
Throughput	100 or more requests / second
% process time	Must not exceed 75%
Memory Available	25 % of total RAM

Load Test Duration	Recommended Sample Rate
< 1 Hour	5 seconds
1 – 8 Hours	15 seconds
8 – 24 Hours	30 seconds

CRITERII (NU SPERANTE)

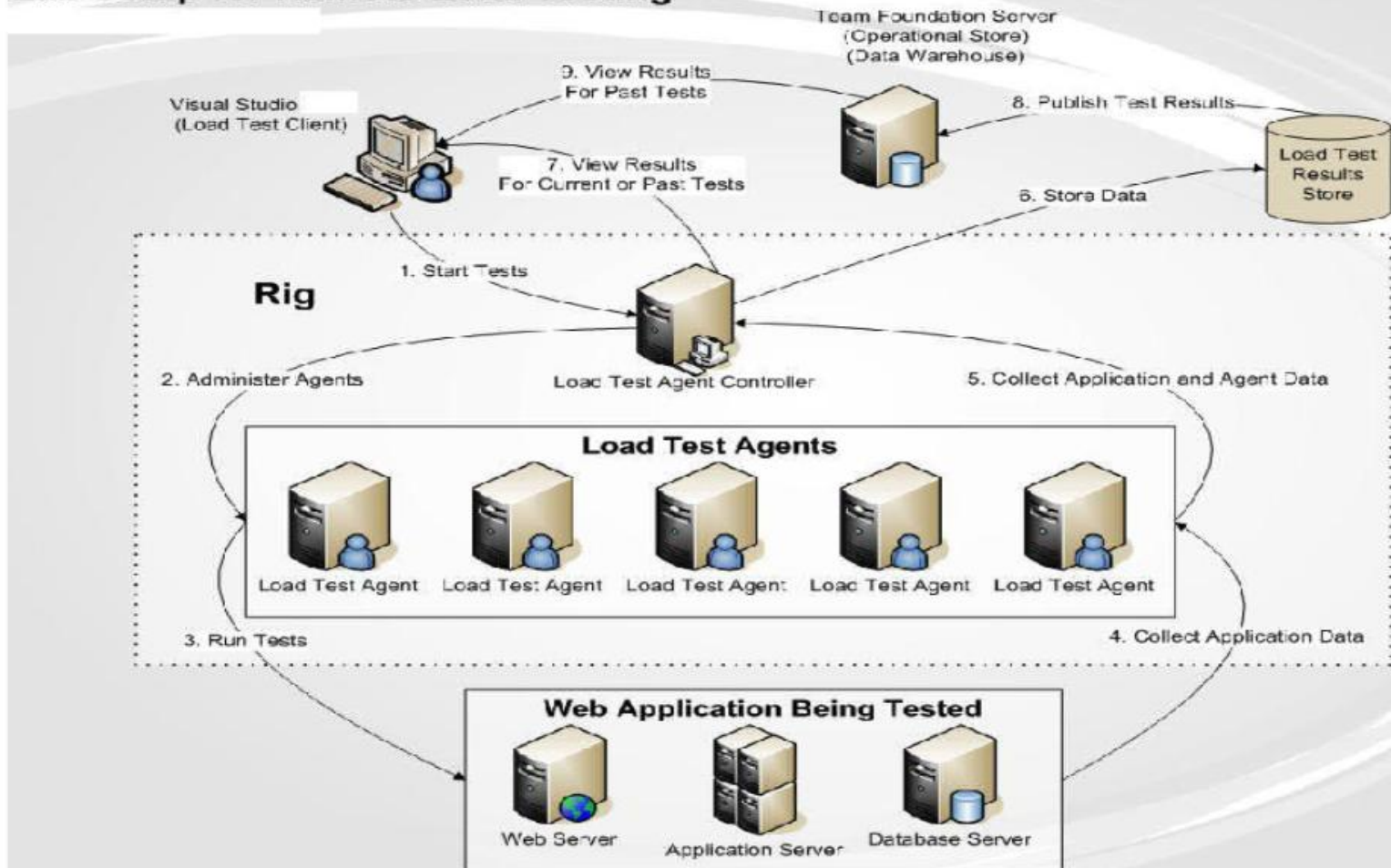
- **SLA – Service Level Agreements**
- **Transaction Response Time**
- **Throughput**
- **Availability**
- **Numar utilizatori concurenti**

MEDIUL DE EXECUTIE

- **Hardware/Platform**
 - Marime
 - Versiuni
- **Load Balancing**
- **Network simulation**
- **Infrastructura software (firewall/proxy/etc)**
- **Instrumente software (executie, monitorizare, etc)**

CUM FUNCTIONEAZA

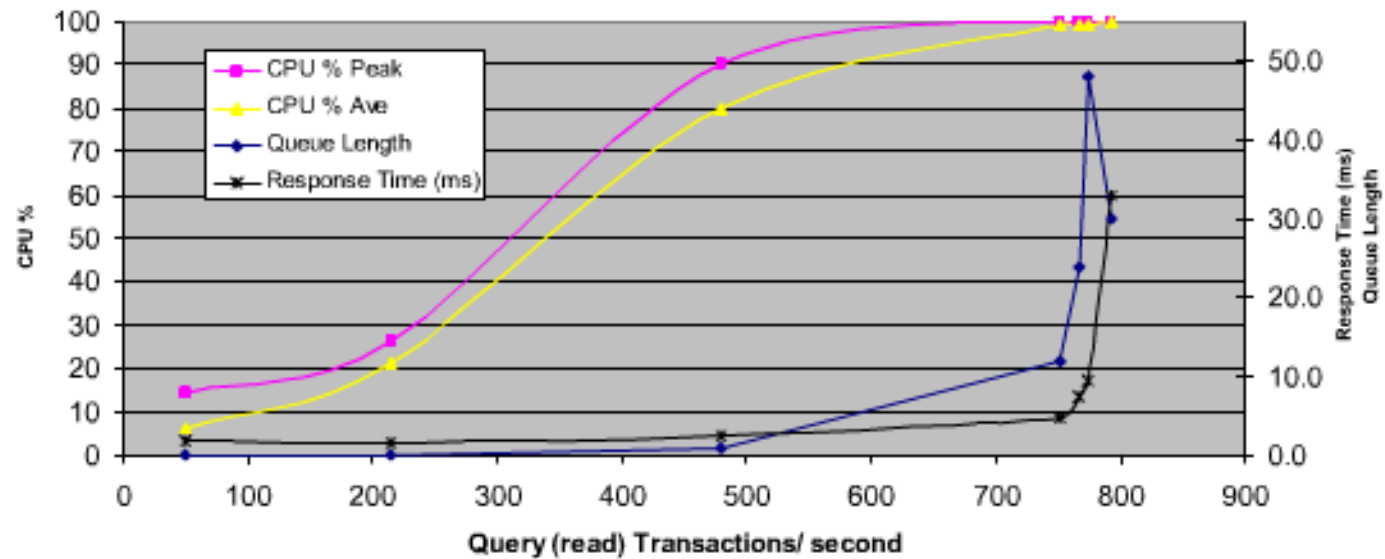
Visual Studio Team System Lab Setup for Remote Load Testing



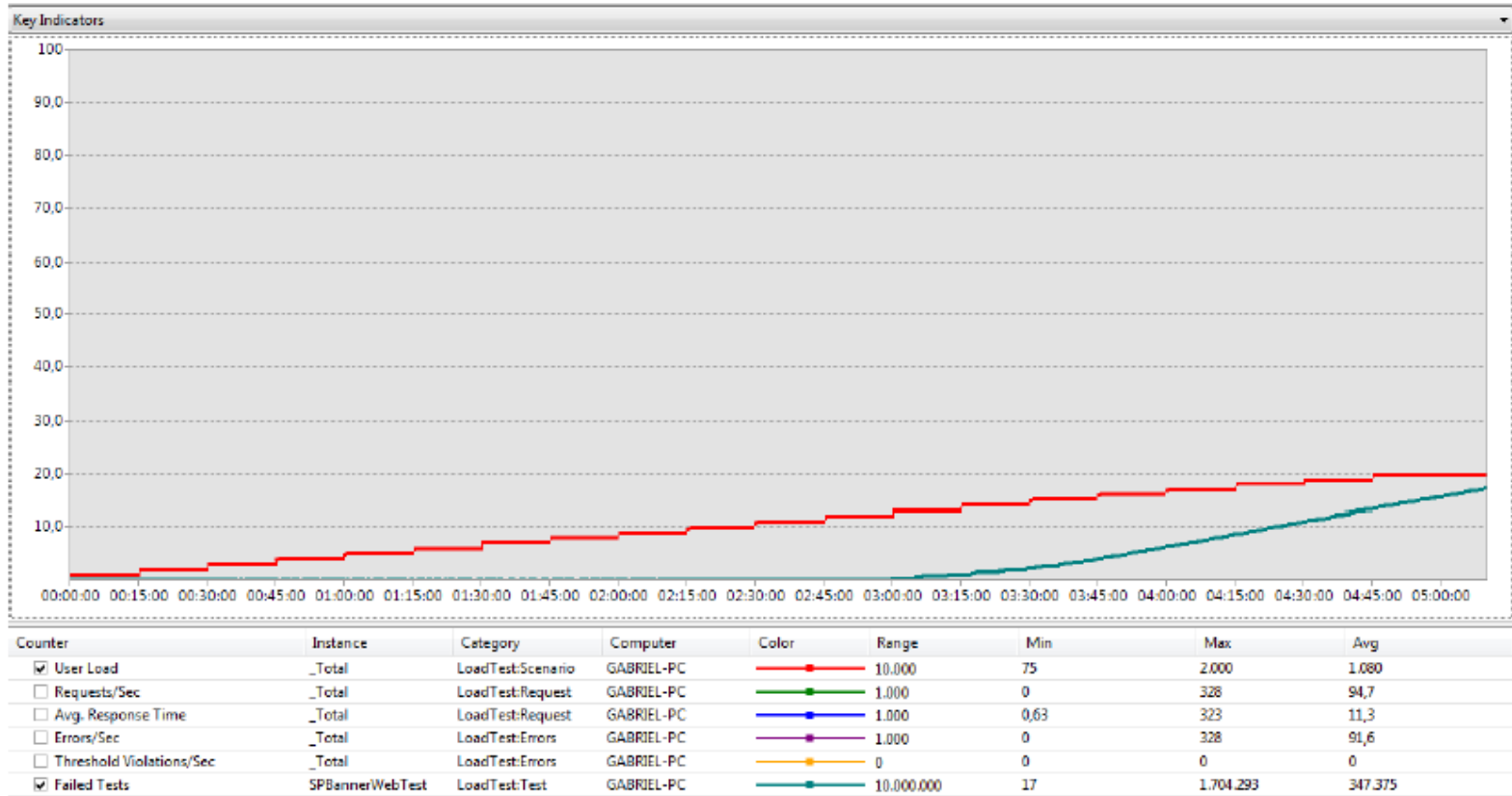
PROBLEME

- **Executia pe aceiasi masina:**
 - Viteza de transfer HDD devine un bottleneck
 - Nu se mai poate face distinctie clasa intre incarcarea agentului si a serverului
- **Executia pe doua masini**
 - LAN
 - RAM pe test agent
- **Recomandare**
 - Urmariti topologia din productie (Web + DB)
 - Cel putin 2 test agents pentru a distribui incarcarea
 - Testele trebuie sa fie de cel putin 4 ore ca durata

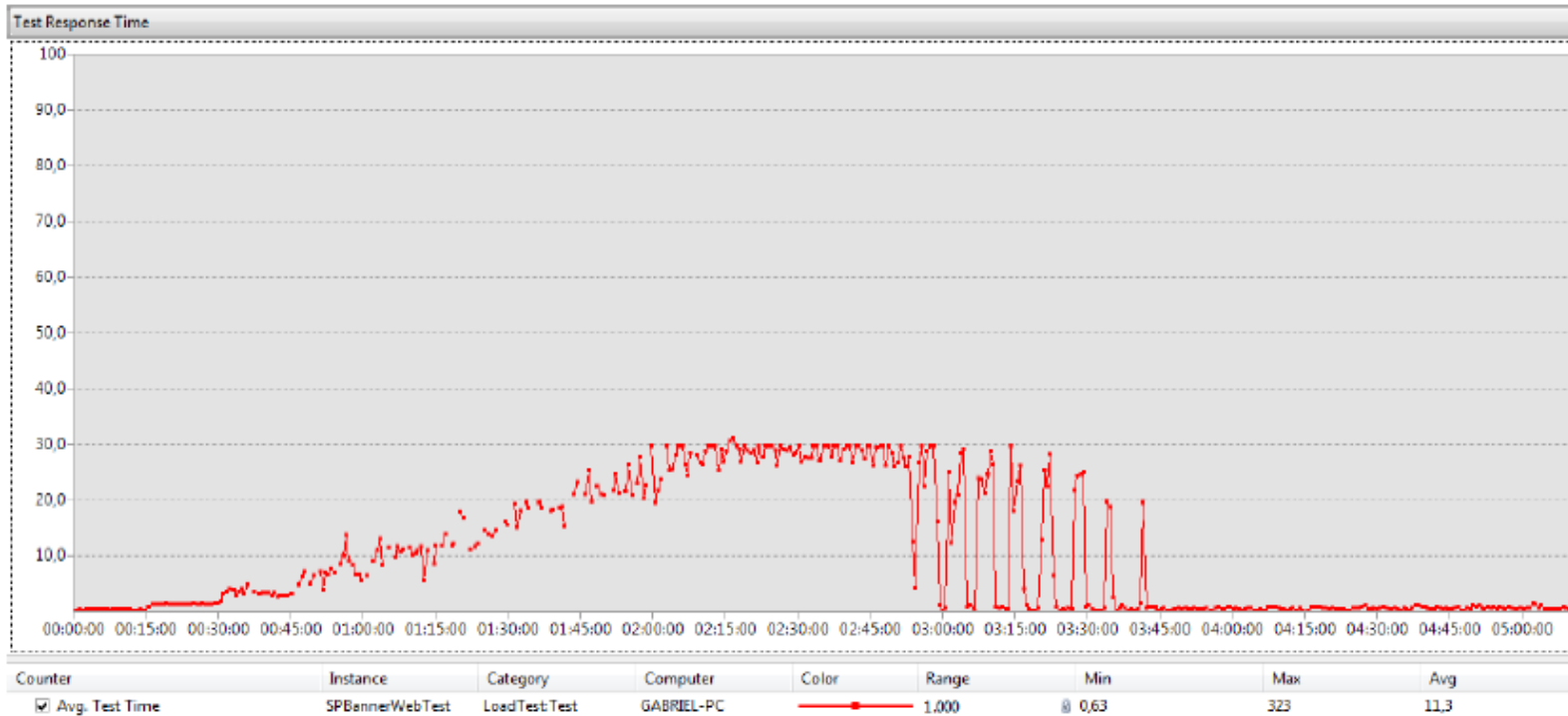
TRANZACTII/SEC VS CPU LOAD



FAILED TRX VS USER LOAD



RESPONSE TIME VS USER LOAD



STRUMENTE

- **HP Load Runner**
- **Visual Studio for Testers**
 - Unit, Manual, Web, Load
 - >3000\$
- **Webperformance**
 - 100 utilizzatori virtuali – 1500\$

SECURITY TESTING

- **OWASP – Open Web Application Security Project**
 - O comunitate “open” dedicata sa ajute organizatiile sa construiasca, cumpere si utilizeze aplicatii “secure”
- **Top 10 – Ten Most Critical Web Application Security Risks**
- **Top 10 riscuri, nu Top 10 cele mai comune probleme**

TOP 10

- **Injection**
 - Are loc atunci cand date in care nu avem incredere sunt incorporate intr-o comanda pentru a fi interpretate
 - Exemplu SQL Injection, LDAP injection
- **Cross site scripting**
 - Aplicatia preia date care nu sunt validate (si “escaped”) si le trimite la un browser
 - XSS permite unui atacator sa execute scripturi in browserul unei victime
- **Broken Application & Session management**
 - Implementarea gresita permite compromiterea de sesiune, chei, etc
- **Insecure Direct Object References**
 - Expunerea unui obiect intern (fisier, director, baza de date) fara controlul accesului sau alte protectii
- **Cross Site Request Forgery**
 - Formarea unui request HTTP fals (inclusiv sesiune, auth, etc) catre o aplicatie vulnerabila
 - Forteaza browserul sa genereze o cerere catre o aplicatie vulnerabila care apare ca si cum ar veni de la un utilizat legitim

TOP 10

- **Security Misconfiguration**
 - Software up to date
 - Nu toate sistemele vin 'locked by default'
- **Insecure Cryptographic Storage**
 - Protectia neadecvata a datelor sensibile (SSN, Credit card, etc)
- **Failure to Restrict URL Access**
 - Este necesara autentificare pentru a accesa pagina?
 - Orice user autentificat poate avea acces?
- **Insufficient Transport Layer Protection**
 - Configurarea incorecta a certificatelor sau folosirea de certificate incorect generate/expire
- **Invalidated Redirects & Forwards**
 - Utilizarea de date de la utilizator pentru a construi redirecturi

INTREBARI RASPUNSURI