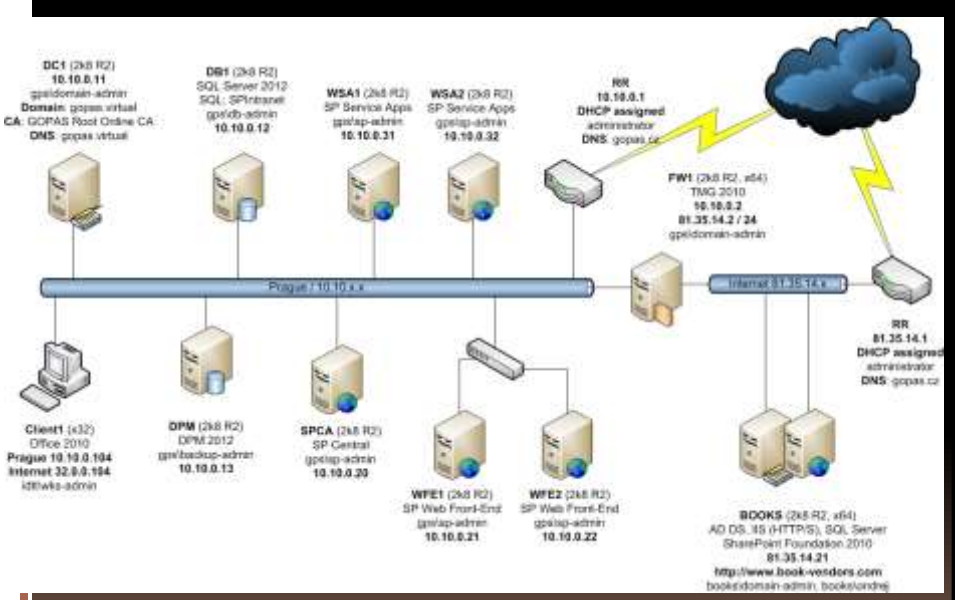
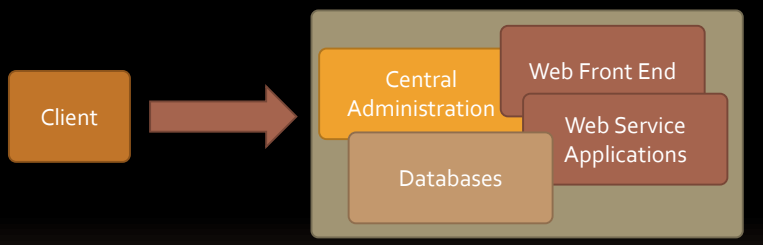
Ondřej Ševeček | PM Windows Server | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

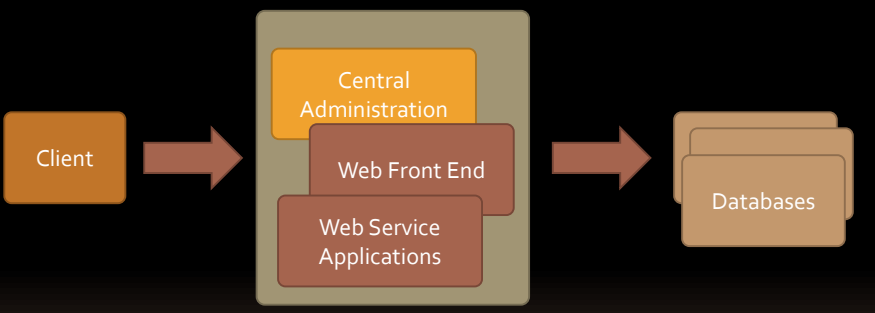
INFRASTRUCTURE OVERVIEW

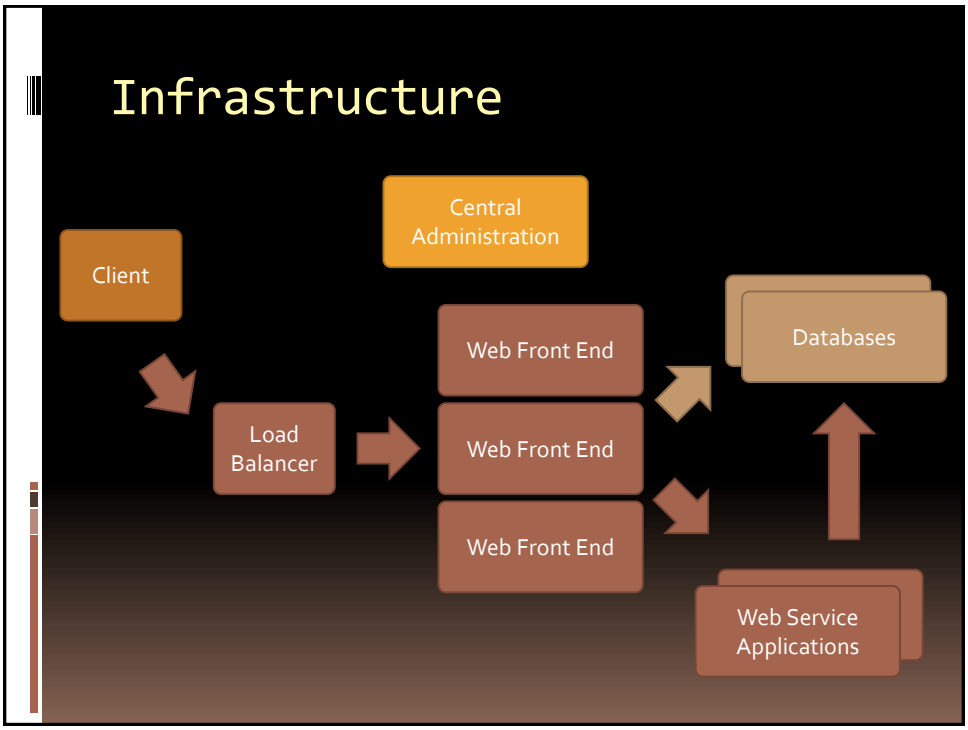


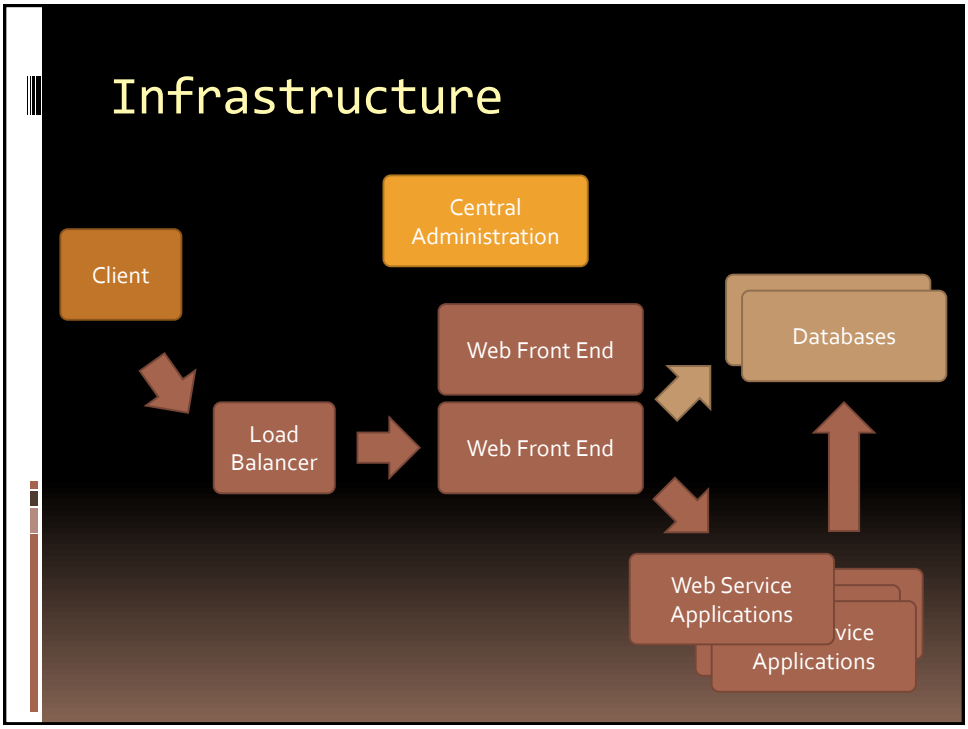
Simplest Infrastructure

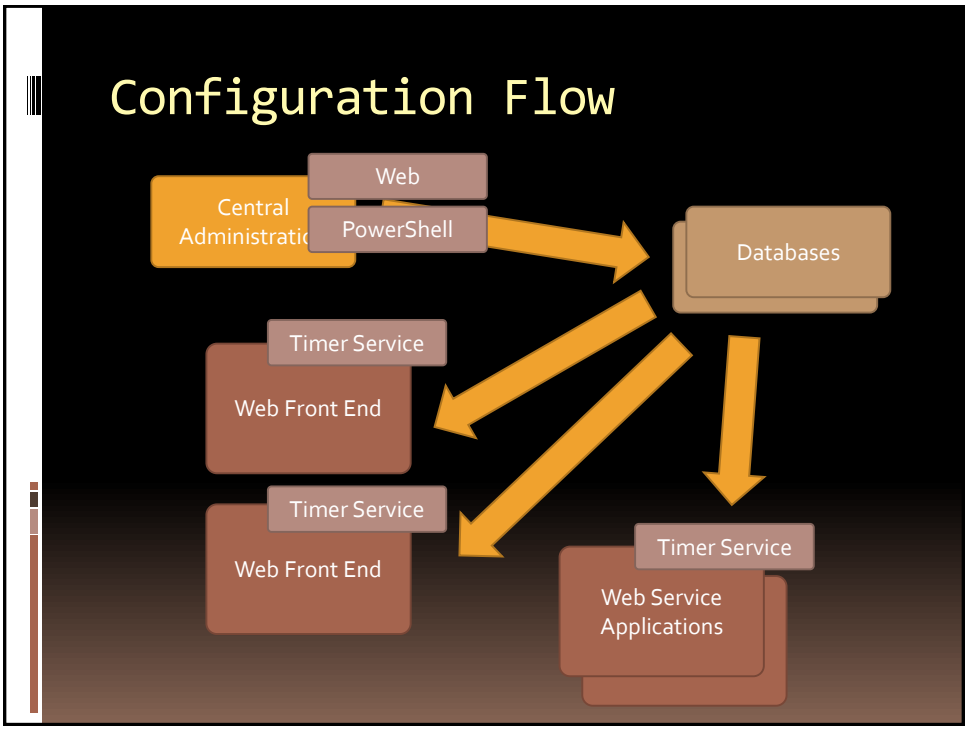


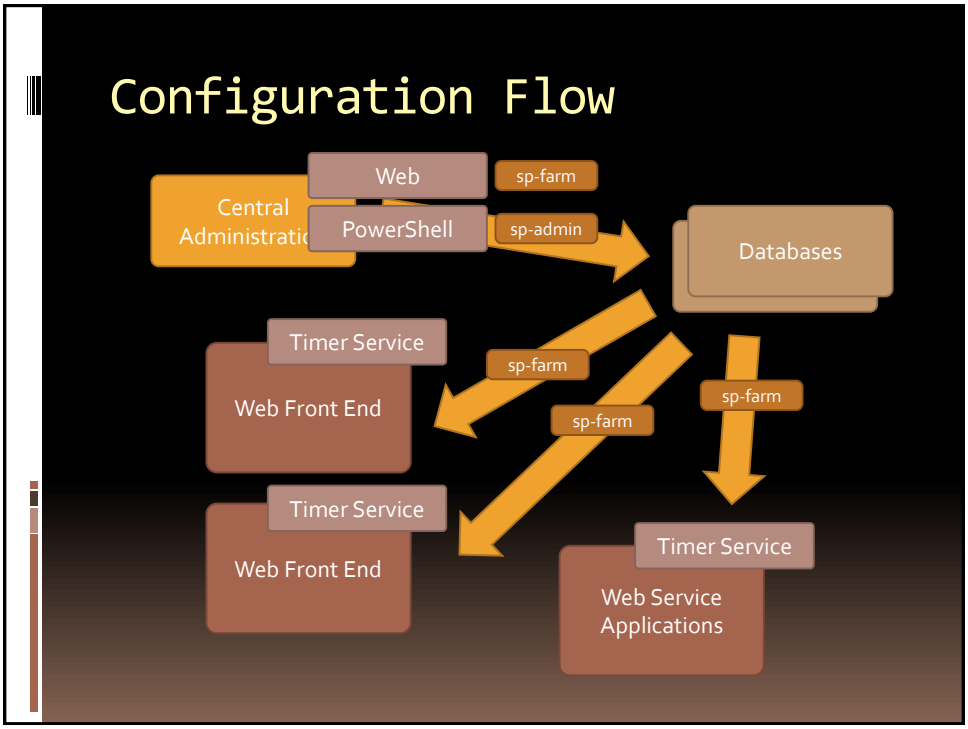
Common Simple Infrastructure




Infrastructure
Central Administration
Client
Web Front End
Databases
Load Balancer
Web Front End
Web Front End
Web Service Applications


Infrastructure
Central Administration
Client
Web Front End
Databases
Load Balancer
Web Front End
Web Service Applications
Applications


Configuration Flow
Central Administratio
Web
PowerShell
Databases
Timer Service
Web Front End
Timer Service
Web Front End
Timer Service
Web Service Applications


Configuration Flow
Central Administratio
Web
sp-farm
PowerShell
sp-admin
Databases
Timer Service
sp-farm
Web Front End
sp-farm
sp-farm
Timer Service
Web Front End
Timer Service
Web Service Applications

Software boundaries and limits for SharePoint 2013

- Max file size - 2 GB
- Web applications per farm - 20
- IIS web sites per application - 5
- Managed paths per web app - 20
- App pools per web server - 10
- Content databases per farm - 500
- Content database - 200 GB / 4 TB / archive unlimited
- Site collections per content database - 10 000 (2 000 recommended)
- Site collections per farm - 750 000
- Web sites per site collection - 250 000
- Items per content database - 60 000 000
- Documents/items per library/list - 30 000 000
- Web parts on a page - 25
- URI limit without query string - 255 characters
- File and folder name length - 123 characters
- Users per site collection - 2 000 000
- SharePoint groups per site collection - 10 000

Networking

- IPv4 and IPv6
  - static addressing
- Internet connectivity
  - NAT over TMG 2010
  - Reverse HTTPS publishing over TMG 2010 or Web Application Proxy on Windows 2012
- Windows Firewall
  - managed through GPOs

Domain Environment

- Active Directory domain
  - GPS, gopas.virtual
  - Windows 2003 Domain/Forest Functional Level
  - UPN suffix: gopas.virtual, gopas.cz
- Public DNS domain
  - gopas.cz
- Hosted domains
  - expensive-pc.com
  - sharp-bikes.com
  - training-virtuosos.com

Certificate Services

- AD CS
  - GOPAS Root Online CA
- Autoenrollment
  - Kerberos Authentication

Domain Security

- Password policies
  - complex passwords
  - minimum password age = 1
- Auditing
- Pre-Windows 2000 Compatible Access group
  - empty
- Windows Authorization Access Group
  - empty
- Service accounts

SQL Server

- SQL Server 2012
  - at least SQL Server 2005 SP3 supported by SP 2010
  - at least SQL Server 2008 R2 SP1 supported by SP 2013
- Instances
  - SPIntranet (dynamic TCP)
- Service account isolation
  - Kerberos SPN registered
- SSL Certificate
  - autoenrollment
  - script to change default private key security

Kerberos authentication to DB

- MSSQLSVC/data1.gopas.virtual:33000
  - rather use static port because of Kerberos delegation
- MSSQLSVC/data1.gopas.virtual:SPINTRANET

SQL Server Editions

- Express
  - supported
  - DB size limited to 10 GB
  - maximum RAM memory 1 GB
  - maximum one socket, maximum 4 cores
  - can do RBS without DB size limits
- Enterprise
  - backup compression
  - data encryption
  - table partitioning (for Web Analytics)
  - database snapshots (content deployment)
  - PowerPivot for SharePoint only part of SQL Enteprise Analysis Services

SQL Recommendations

- SharePoint 2013 (MUST) and older (SHOULD)
  - Max degree of parallelism (MAXDOP) = 1
- Do not enable auto create/update statistics
  - per database (AUTO_CREATE_STATISTICS, AUTO_UPDATE_STATISTICS)
  - SharePoint database maintenance job do this itself
- Limit SQL memory if sharing OS with other applications or SP itself

Lab: Infrastructure overview

- Create \\DC1\Support shared folder
- Confirm that ping www.google.com works
- Download ULS Viewer and store it into \\DC1\Support
- Explore OU=Company contents
- Use GPMC to enable Account Management advanced auditing categories in the Sec: Auditing GPO

User Groups

- SP Admins (sp-install, sp-admin)
  - local administrators on SPCA
  - DBCreator, SecurityAdmin in all SQL instances
  - DBO for all content databases
  - read/change password access over SharePoint service accounts
- Service Accounts
- Service Accounts and Admin Accounts must be able to read all others' properties

Lab: SQL Server...

- Enable Login Auditing to Both failed and successful logins for all SQL instances
- Confirm default DB location for all instances
- Confirm that sp-install is DBCreator + SecurityAdmin
- SharePoint 2013 (MUST) and older (SHOULD)
  - Max degree of parallelism (MAXDOP) = 1
  - sp_configure 'show advanced options', 1;
  - RECONFIGURE WITH OVERRIDE;
  - sp_configure 'max degree of parallelism', 8;
  - RECONFIGURE WITH OVERRIDE;

Why SQL Alias

- Simpler SQL server migration
- Simpler use
- User Profile Service (UPS) has problems with
  - named instances
  - FQDN SQL server names

Lab: SQL Clients

- Create SQL Aliases on all SPCA, WFE1, WFE2, WSA1, WSA2
  - CLICONFG and %windir%\SysWoW64\CLICONFG
  - spdb = TCP, db1\spintranet
  - use short DB1 name instead of FQDN to see some errors and be able to enjoy troubleshooting later
- Note that you could create .BAT file and store it in \\DC1\Support folder
  - REG ADD "HKLM\Software\Microsoft\MSSQLServer\Client\ConnectTo" /v "spcfg" /t REG_SZ /d "DBMSSOCN,dc1\spconfig" /f
  - REG ADD "HKLM\Software\WoW6432NodeMicrosoft\MSSQLServer\Client\ConnectTo" /v "spcfg" /t REG_SZ /d "DBMSSOCN,dc1\spconfig" /f
  - ...\SuperSocketNetLib /v Encrypt /t REG_DWORD /d 1

Lab: Prepare IIS...

- Delete Default Web Site
  - %windir%\system32\inetsrv\appcmd.exe delete site "default web site"

Lab: ...Prepare IIS...

- Enable detailed logging
  - appcmd set config /section:httpLogging /dontLog:False /selectiveLogging:LogAll
  - appcmd set config /section:sites -siteDefaults.logFile.logExtFileFlags:Date,Time,ClientIP,UserName,SiteName,ComputerName,ServerIP,Method,UriStem,UriQuery,HttpStatus,Win32Status,BytesSent,BytesRecv,TimeTaken,ServerPort,UserAgent,Cookie,Referer,ProtocolVersion,Host,HttpSubStatus
  - appcmd set config /section:sites -siteDefaults.logFile.logFormat:W3C

Lab: ...Prepare IIS

- Stop all AppPools
  - appcmd list apppool /xml | appcmd stop apppool /in
- Define NLB-Host header to return the computer name

Lab: MSI Logging

- Create new GPO
- Enable MSI Logging to v* level
  - Computer / Administrative Templates / Windows Components / Windows Installer / Logging