



# Security And SharePoint

## From Service Accounts To Item-Level Access

Michael Noel



*michael@cco.com*

 Microsoft®  
**Office SharePoint®**  
Server 2007

# About the Presenter and Convergent Computing



- Author of SAMS Publishing titles "SharePoint 2007 Unleashed," "SharePoint 2003 Unleashed", "Teach Yourself SharePoint 2003 in 10 Minutes," "Exchange Server 2007 Unleashed", "ISA Server 2006 Unleashed", and many other titles with over 100,000 books in circulation worldwide translated into 7 languages.
- Microsoft MVP for Microsoft Office SharePoint Server
- Convergent Computing – San Francisco, U.S.A., Infrastructure/Security specialists for SharePoint, AD, Exchange.

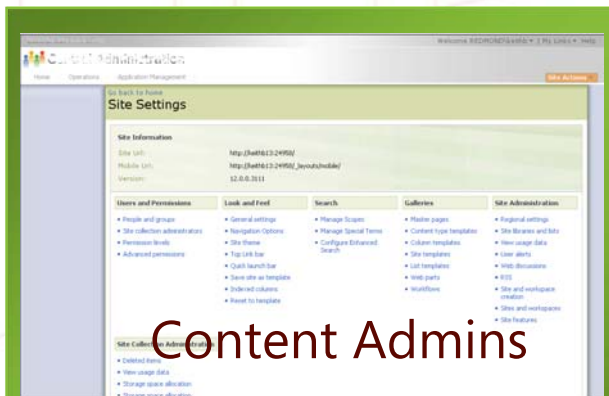


# Goals And Agenda

- Learn in this session
  - How to configure authentication
  - How to manage permissions
  - How to securely configure your web farm
- Agenda
  - Office server family
  - Windows and ASP.NET authentication
  - Managing permissions bottom to top
  - Configuring the web farm
  - ForeFront Security for SharePoint

# Administrative Architecture

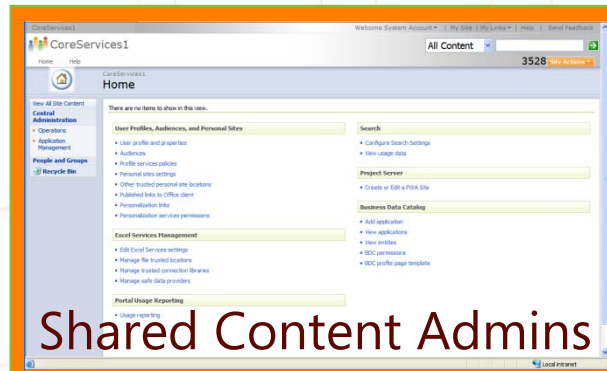
- Three Tier Admin
  - Web-based
  - Role & task delineated
  - Controlled delegation
  - Secure isolation



**Site Settings**

- Content Authorization

Content Admins



**Shared Content Admins**

**Shared Services**

- Service Authorization
- Service Configuration
- MOSS only



**IT Admins**

**Central Admin**

- Authentication
- Security Policies
- Farm Configuration

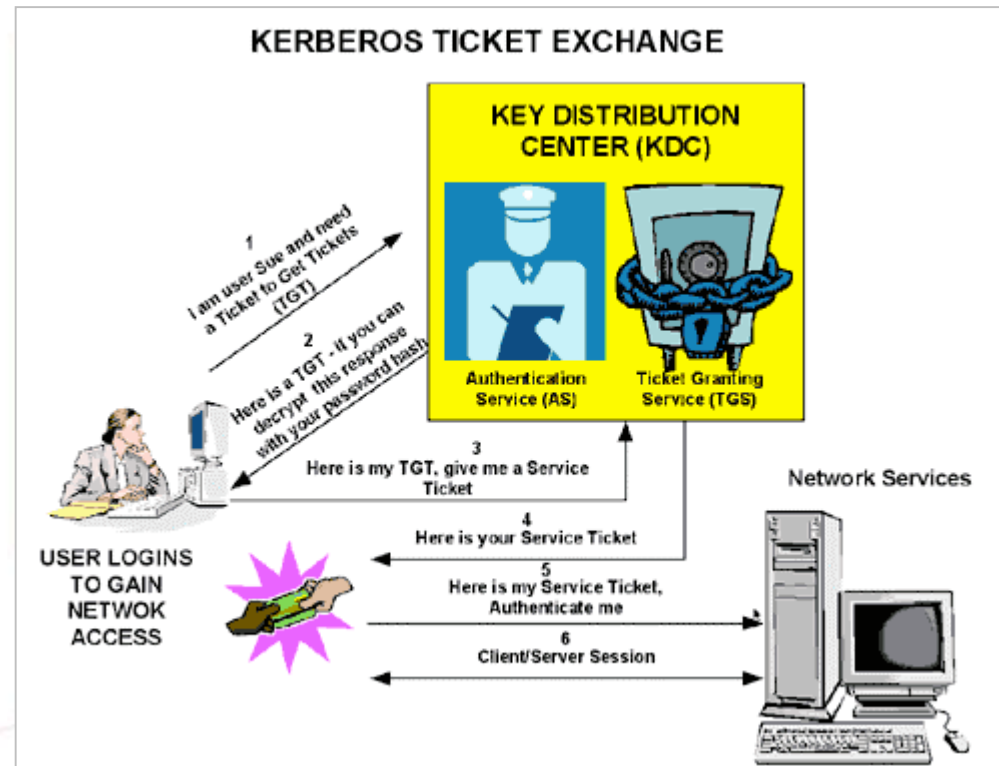
# User Authentication

- Authentication = Who are you?
  - User identity
  - User groups/roles as defined by the directory
  - Same in WSS and MOSS!
- Windows
  - Windows integrated, Basic, Digest, etc
- ASP.NET Pluggable Authentication
  - Forms – locally hosted login form
  - Web SSO – remotely hosted login form

# Windows Authentication

- Provided by IIS – SharePoint consumes
- Windows Integrated
  - Kerberos/Negotiate 
  - NTLM
- Basic
- Certificates (Must use IIS configuration UI)

# Configuring Kerberos

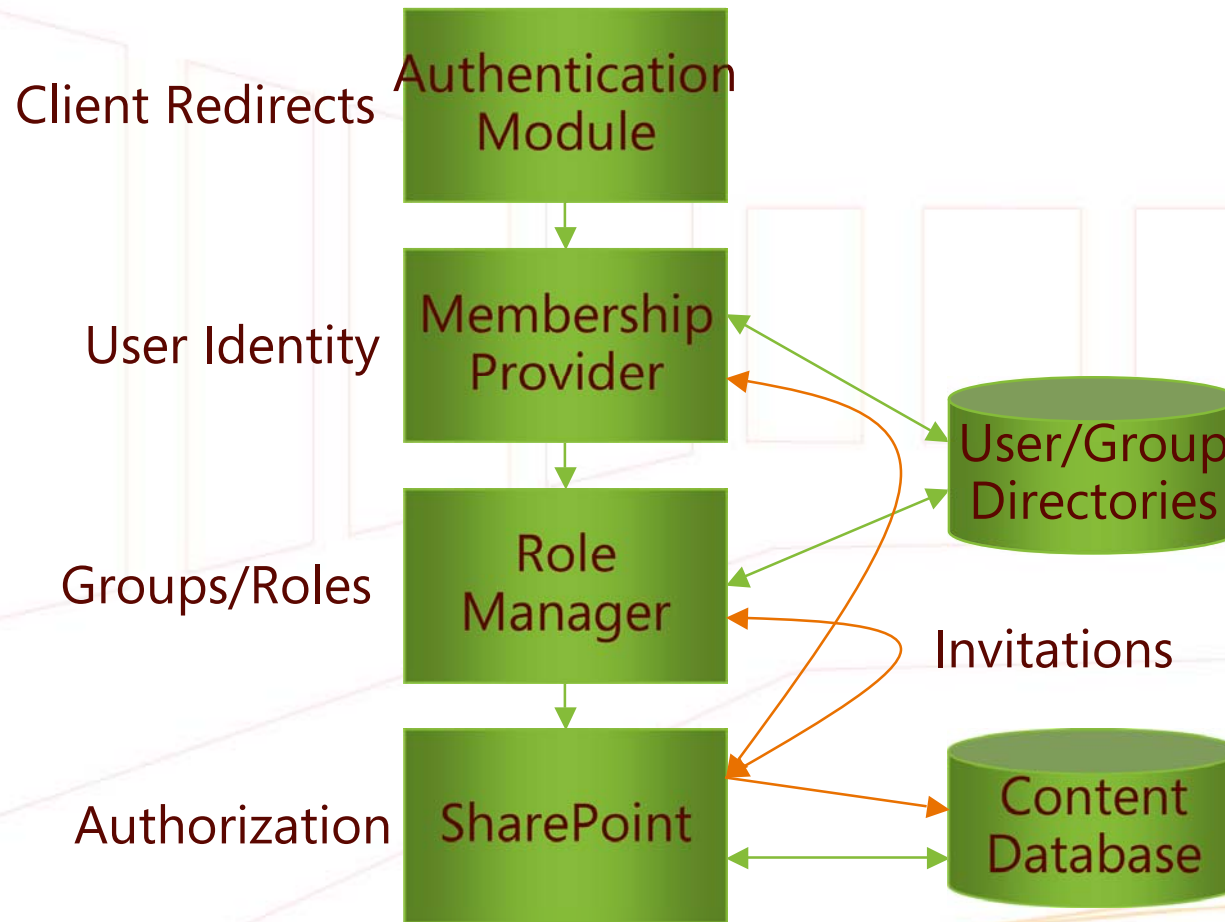


- KDC Service Principal Name **must** match SharePoint application pool account

# ASP.NET Authentication

- Pluggable authentication framework
  - User identity is independent from Operating System (OS) identity
  - Custom code to handle authentication
  - Two related providers
    - Membership – user identities
    - Role – roles/groups/attributes for a user
- Out-of-the-box providers
  - LDAP (Office Server)
  - SQL Server (ASP.NET)
  - AD – single domain only (ASP.NET)

# ASP.NET Pipeline



# Web.config

```
<membership>
  <providers>
    <add name="YourMembershipProviderName"
      connectionStringName="YourConnectionString"
      .../>
  </providers>
</membership>

<roleManager>
  <providers>
    <add name="YourRoleProviderName"
      connectionStringName="YourConnectionString"
      ... />
  </providers>
</roleManager>

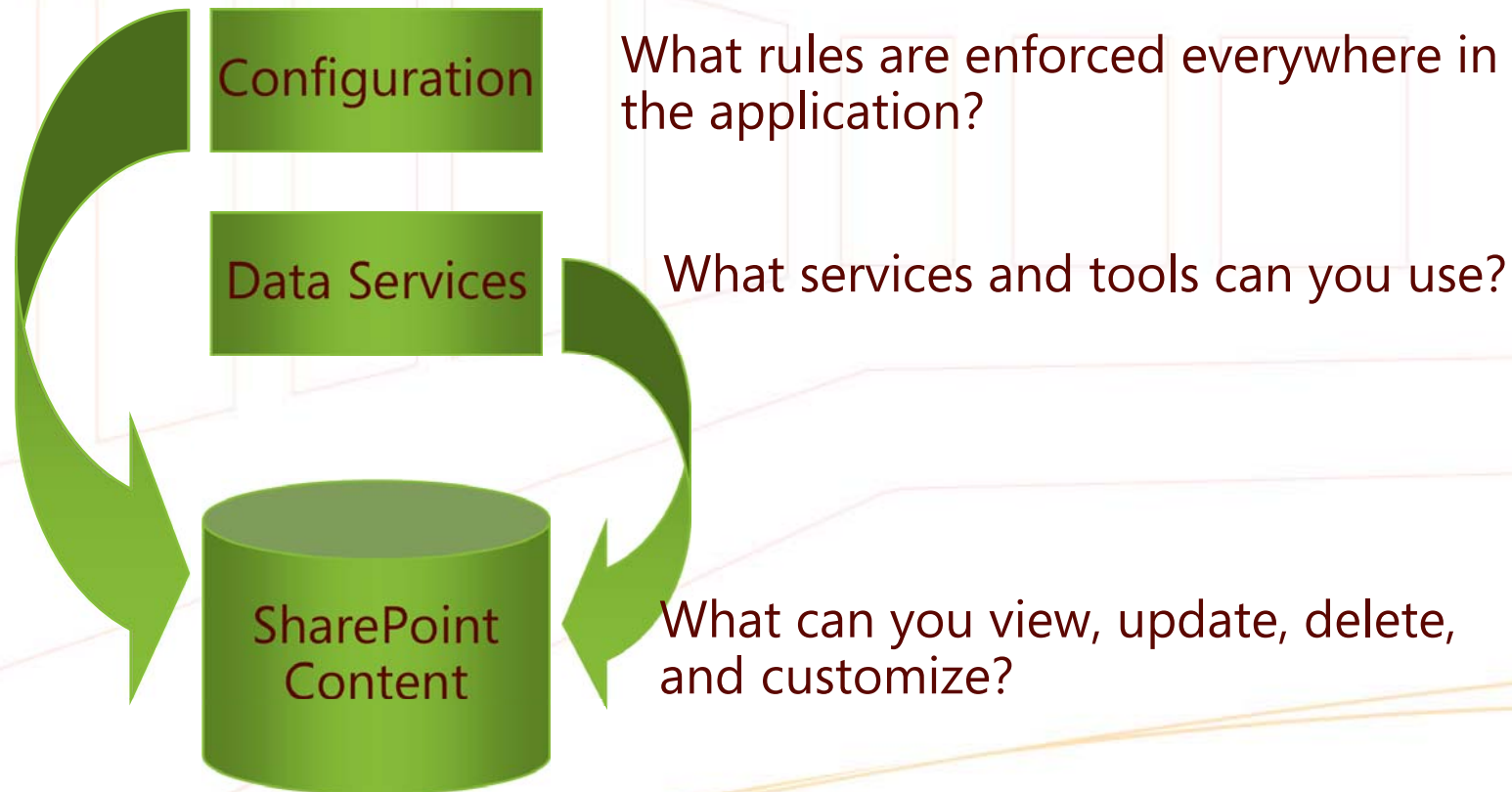
<connectionStrings>
  <add name="YourConnectionString" connectionString="data
    source=127.0.0.1;Integrated Security=SSPI;Initial Catalog=aspnetdb" />
</connectionStrings>
```

# ASP.NET Authentication Limitations

- Browser clients only
  - Search crawler must use Windows
  - Office client interaction degraded
- One authentication type per web application
  - No Windows and Forms in same domain
  - **One** provider pair per domain
- Forms over Windows accounts
  - Forms user **not** same as Windows user

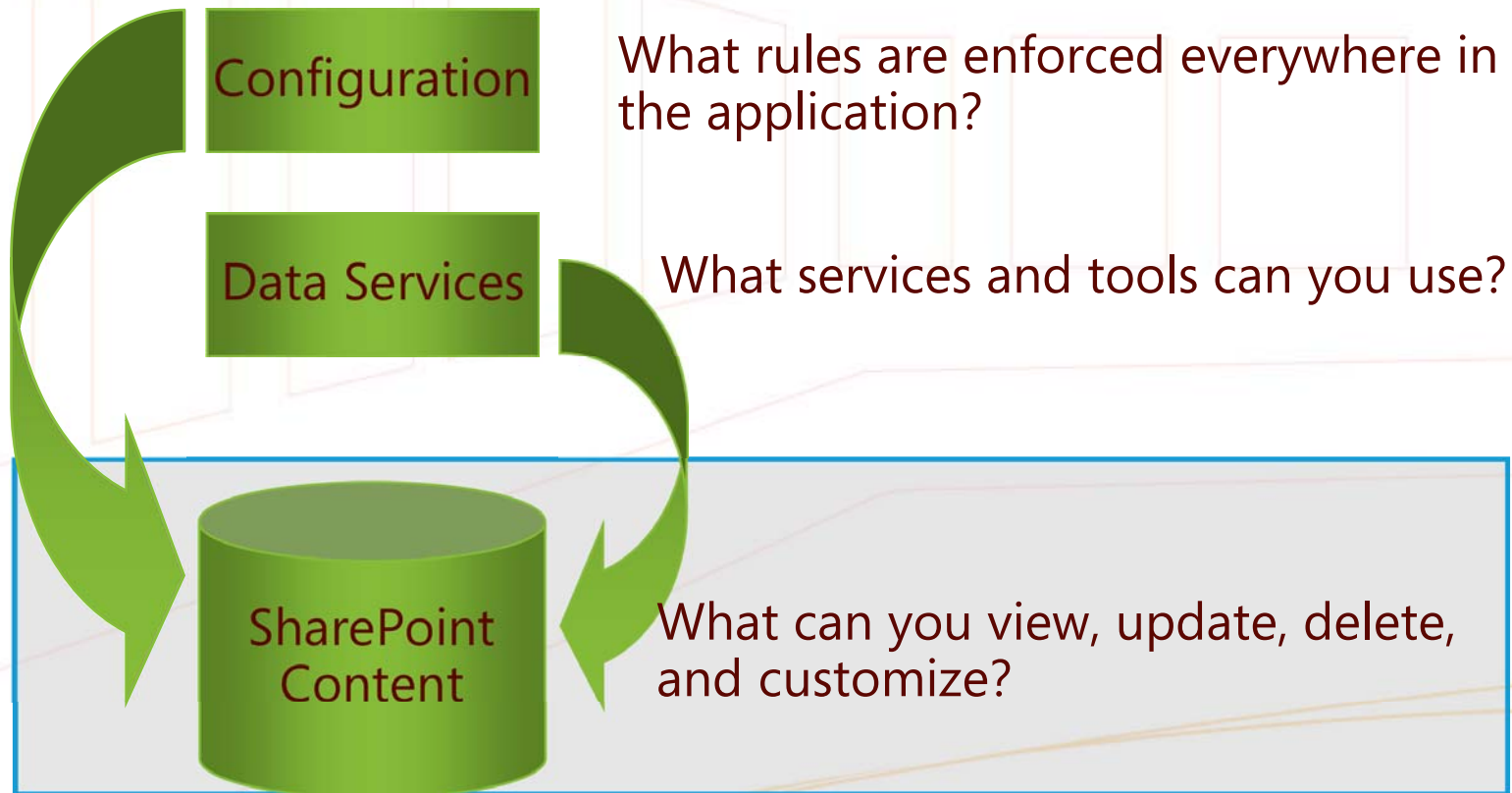
# Authorization Tools

- Authorization = What can you do?



# Authorization Tools

- Authorization = What can you do?



# Permissions Management

- Group-based permissions management
- Role-based permissions management
- Fine-grained permissions control
- List, library, folder, item, and document
- Anonymous access
- Security trimmed user interface!
- Explicit access denied experience!

# SharePoint Groups

- New permissions management experience
- Three default groups
  - Owners – full control
  - Members – contribute to existing lists and libraries
  - Visitors – read only
- Integrated with user information list
- SharePoint groups can be assigned permissions anywhere in the site collection
- Group administration **scales** better

# Permission Levels

- Collections of **rights**, not people
  - Full Control – Has full control
  - Design – Can view, add, update, delete, approve, and customize
  - Contribute – Can view, add, update, and delete
  - Read – Can view only
- Customizable
- Inheritable across site collection

# Fine Grained Permissions

- New securable objects
  - Web site
  - Lists and libraries
  - Folders within list or library
  - Document or list item
- Consistent user interface top to bottom
  - Permission levels
  - Inherit from parent or unique permissions

# Site Collection Administrators

- Users with full control over all content in the site collection
  - Fix lock out problems
  - Recover items from 2nd stage recycle bin
  - Cannot be removed from permissions

# Limited Access

- Permissions required for fine-grained perm

Navigation Bars

Shared Form

Theme

<b>Title</b>	Welcome to Jim's Site
<b>Body</b>	This is a team site for Jim
<b>Expires</b>	5/5/2006

Created at 4/25/2006 2:20 PM by James Sturms  
Last modified at 4/28/2006 2:09 PM by James Sturms

# New Permissions

- Edit User Information – display name, e-mail, etc
- Approve Items – promote minor to major version
- View Versions
- Delete Versions
- Create Alerts – separated from view items
- Manage Alerts – create alerts for other people
- Enumerate Permissions – read, but not change
- Open Items – view source of server files (ASPX)
- View Application Pages – e.g. \_layouts pages
- Use Remote Interfaces – e.g. SOAP
- Use Client Integration Features – e.g. Office

# Anonymous Access

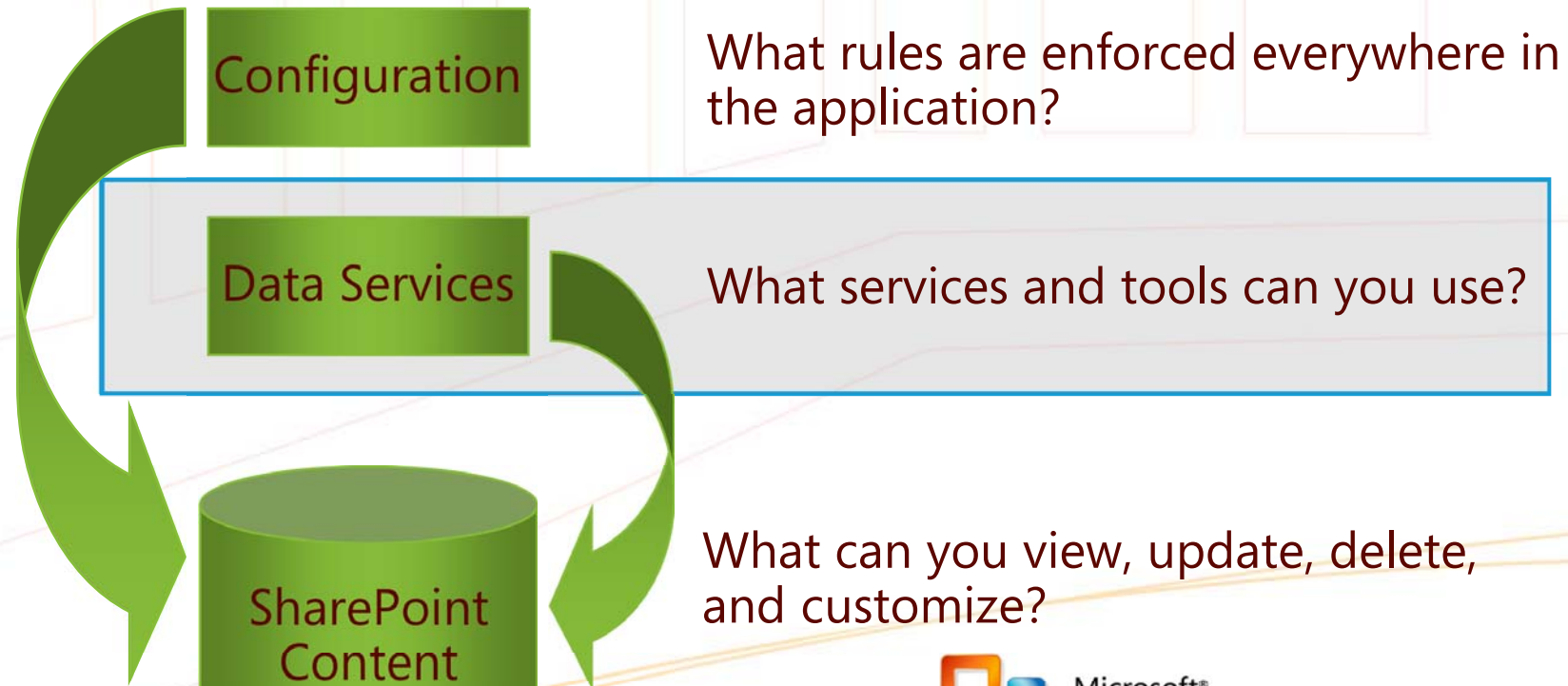
- Disabled **and** off by default
- Enable/disable in Central Administration
- Web site level control
  - On/Off
  - Allow anonymous lists (Limited access)
- List level control
  - Read, add, update, and delete
- Library level control
  - Read

# Anonymous Limitations

- Defaults to **very** reduced permissions
  - Read only
  - No remote interfaces
  - No client integration
- Configurable via object model
- No folder or item level control
- Hard coded limitations
  - No anonymous authoring of documents
  - No anonymous administration

# Authorization Tools

- Authorization = What can you do?

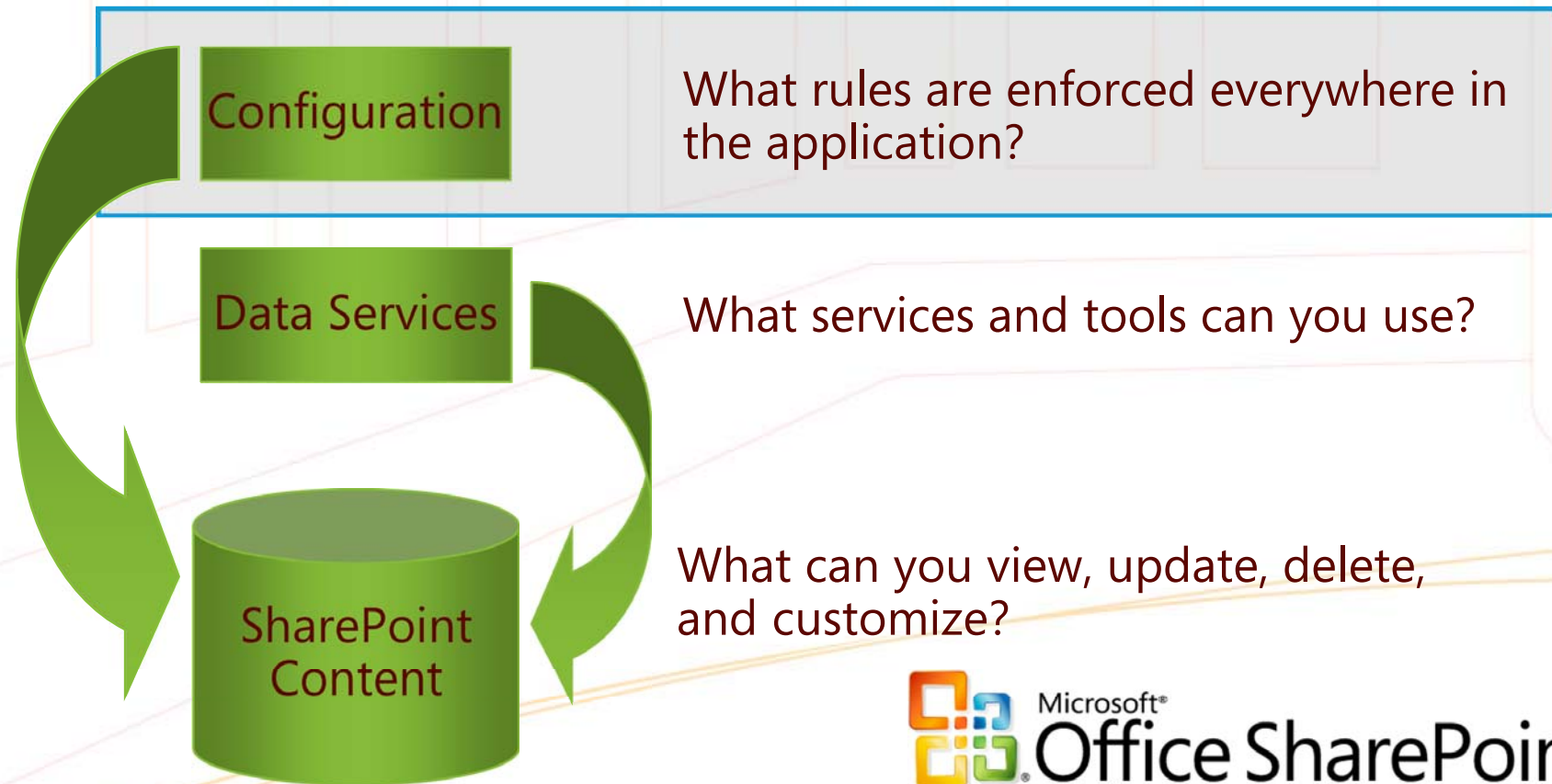


# Shared Services

- Business data catalog
- Impersonation/delegation
  - Kerberos constrained delegation
  - Office server SSO
- Trusted subsystem
- Excel trusted locations
- User profile rights
- Property visibility
- Audiences are **NOT** for security

# Authorization Tools

- Authorization = What can you do?



What rules are enforced everywhere in the application?

Configuration

What services and tools can you use?

Data Services

What can you view, update, delete, and customize?

SharePoint  
Content



Microsoft®

Office SharePoint®  
Server 2007

# Security Policy

- Central enforced permissions for **all** sites in the web application
  - GRANT and DENY
  - Bound to web application/zone
- Scenarios
  - Full read – search crawling accounts, auditors, legal compliance
  - Deny all – security control, regulatory compliance
  - Deny write – extranet lockdown

# Web Farm Configuration

- Application pool accounts
  - Full control over content
  - Act as the "SharePoint\system" account
- Timer service accounts
  - Timer
  - Admin Service – must run as Local System
- SQL Servers
  - Kerberos SPN issue applies here too!

# Security Configuration

- Rights mask
- Blocked file types
- Form digest timeout
- Safe control list
- Code access security
- Code execution paths
- Virus scanning

# Office Server SSO



- Credentials for server-to-server hop
- Unique or shared

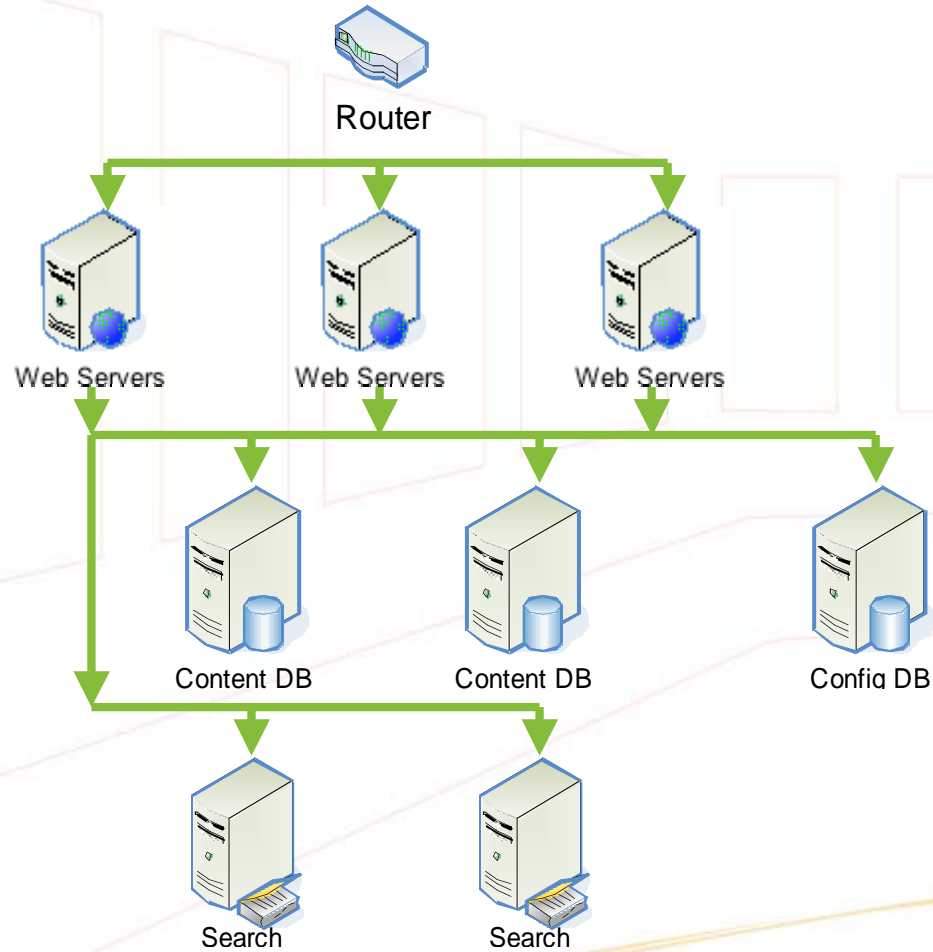
# User Account Migration

- Windows
  - Cross **domain** moves requires SharePoint migration
  - stsadm.exe -o migrateuser
    - oldlogin <DOMAIN\name>
    - newlogin <DOMAIN\name>
    - [-ignoresidhistory]
- ASP.NET
  - No SID History

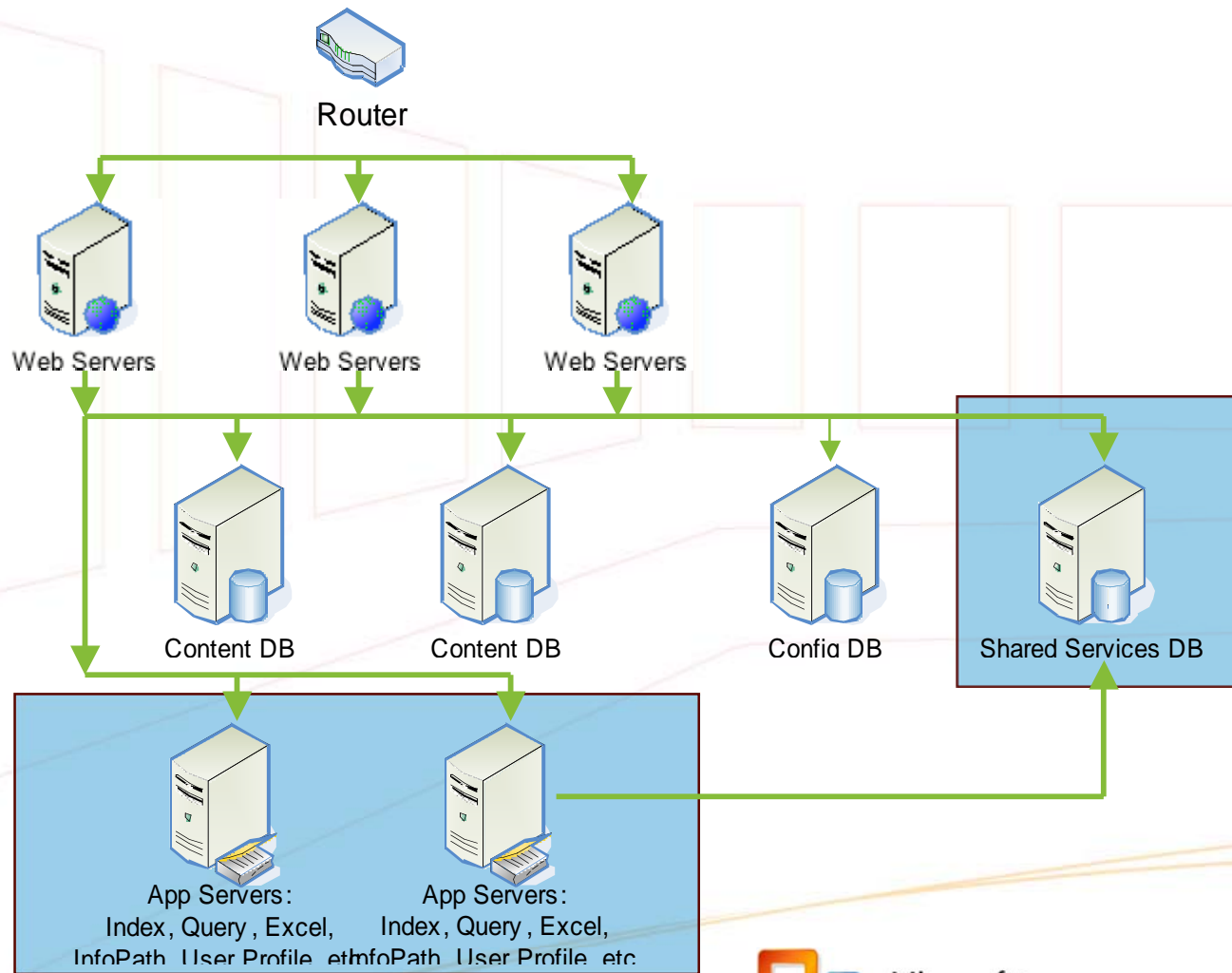
# Admin Access To Data

- Central administrators no longer have default full access to content
- Central administrators **can** grant themselves access to any content
  - Security policy
  - Site collection owners/administrators
  - Both actions are audited in NT Event Log

# WSS Topology



# MOSS Shared Services



# Configuration Best Practices

- Unique accounts
  - Central administration
  - Shared services process
  - Shared services shared web service account
  - Content app pools
- **Kerberos** on (default = NTLM)
  - Each process account must be a registered SPN to work
  - SQL 2005 defaults to Kerberos with non-system process ID!
- SSL enabled (default = off)
  - Turn on for admin sites and server to server
  - Warning provided on credentials pages if SSL is off
- SPAdmin service
  - Single server: Off  
(recommend 'On' for OSS)
  - Farm: On

# Forefront Security for SharePoint

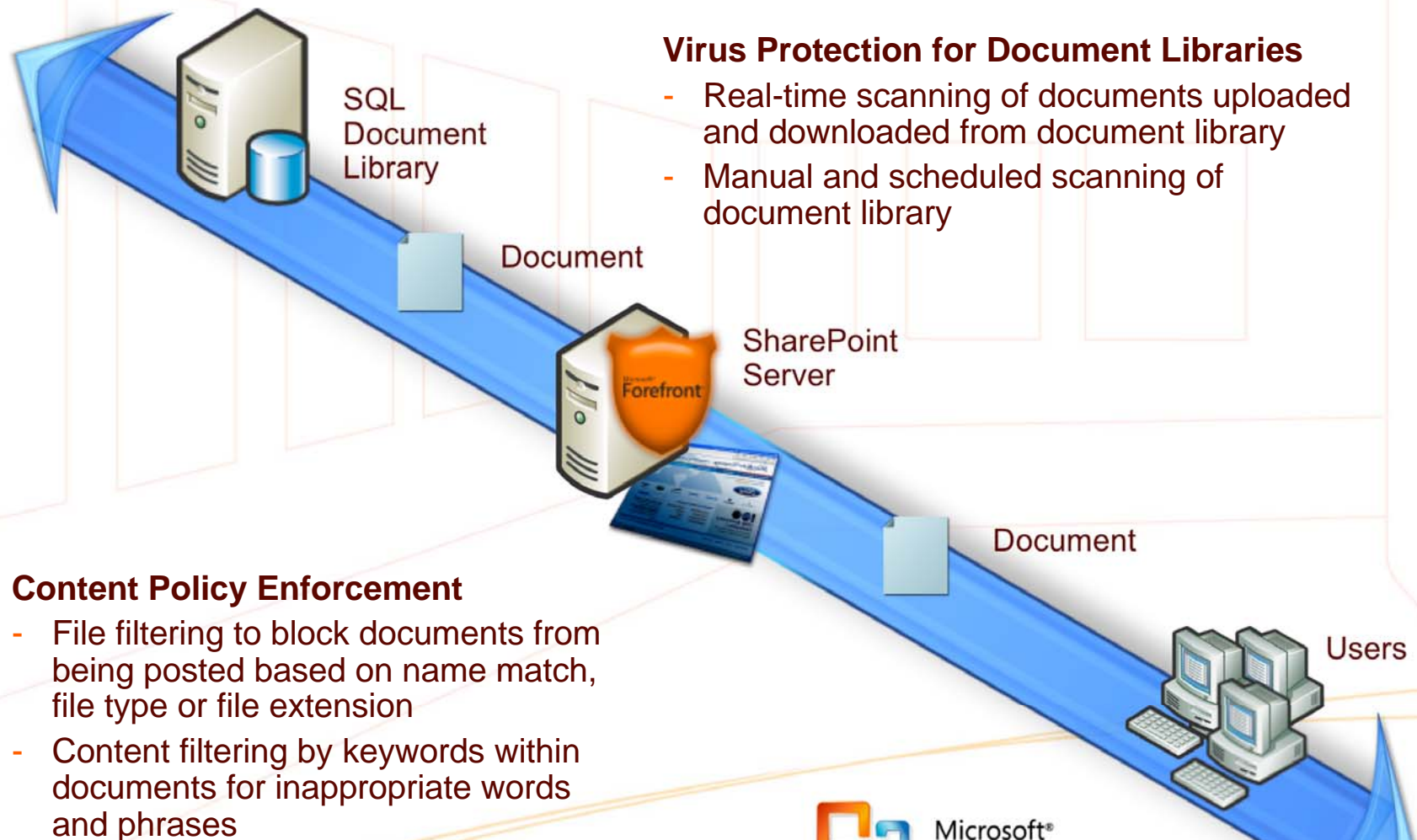
Protecting Content from Virus threats



# What's New in This Release?

- Forefront Security for SharePoint
  - Both 32-bit and 64-bit support
  - Localization (11 languages)
  - Support for SharePoint Information Rights Management Documents
  - Keyword filtering on Office XML Open Format and Excel formats
  - Access to all scan engines included with license

# Forefront Security for SharePoint



# SharePoint API integration

- Utilizes the SharePoint Virus API to scan files during upload and download
  - Optimized for performance in a SQL environment
- Files are not rescanned if engines have not been updated
- Up to ten simultaneous scanning threads to help ensure users are not delayed waiting for documents to scan
- Automatic integration with SharePoint Information Rights Management (IRM) to scan protected files on the fly

# Recap

- Pluggable authentication
  - Windows – Kerberos, NTLM, Basic
  - ASP.NET – Forms and Web SSO
- Managing permissions
  - Site settings: Site, list, folder, and item
  - Shared services
  - Central admin policies and configuration
- Web farm configuration
  - Application pool accounts
  - Other process accounts
- ForeFront Security for SharePoint

# Call To Action

- Get Kerberos working!
  - More secure than NTLM
  - Better performance than NTLM
- Evaluate custom code
  - Ready for Forms authentication?
- Evaluate content topology
  - Does folder and item level permissions change how you deploy SharePoint content?
- Model your groups

# SharePoint Conference Hands-on Labs

The following is the list of Hands-on Labs available in SAAL C (Part 1):

- HOL101 What's New in Microsoft Windows SharePoint Services 3.0 Feature Walkthrough
- HOL111 What's New in Microsoft Office SharePoint Server 2007 Feature Walkthrough
- HOL171 Synchronizing Data Between Microsoft Office Groove 2007 and Microsoft SharePoint Products and Technologies
- HOL201 Introducing Content Types for Microsoft Windows SharePoint Services 3.0
- HOL202 Microsoft Windows SharePoint Services Installation and Configuration
- HOL203 Microsoft Windows SharePoint Services 3.0 Backup and Restore
- HOL211 Microsoft Office SharePoint Server 2007 People and Permissions
- HOL212 Microsoft Office SharePoint Server 2007 Personalization
- HOL213 Microsoft Office SharePoint Server 2007 Installation and Configuration
- HOL214 Microsoft Office SharePoint Server 2007 Enterprise Features Administration
- HOL215 Microsoft Office SharePoint Server 2007 Records Management Deployment and Configuration
- HOL216 Microsoft Office SharePoint Server 2007 for Search Installation
- HOL217 Getting Started with Search in Microsoft Office SharePoint Server 2007



# SharePoint Conference Hands-on Labs (2)

The following is the list of Hands-on Labs available in SAAL C (Part 2):

- HOL241 Using Microsoft Office Excel 2007 Spreadsheets for Web Service-Based Calculations and Browser Rendering
- HOL262 Building Microsoft Office InfoPath 2007 Forms that Run as Both Rich Client and Browser Applications
- HOL301 Using Features to Provision Sites in Microsoft Windows SharePoint Services 3.0
- HOL302 ASP.NET 2.0 Interoperability with Microsoft Windows SharePoint Services 3.0 - Web Parts and Master Pages
- HOL303 Creating Workflows for Microsoft Windows SharePoint Services 3.0
- HOL304 Using List Events in Microsoft Windows SharePoint Services 3.0
- HOL305 Microsoft Windows SharePoint Services 3.0 Site Templates
- HOL311 Getting Started with the Business Data Catalog in Microsoft Office SharePoint Server 2007
- HOL312 Search Administration and Customization in Microsoft Office SharePoint Server 2007
- HOL313 Designing Content-Driven Web Sites with Microsoft Office SharePoint Server 2007
- HOL314 Microsoft Office SharePoint Designer 2007 - CSS and the Data Form Web Part

# Sweepstake

Complete your Feedback form  
and have a chance  
to win a Zune!\*



\* English US version

# Questions?

[michael@cco.com](mailto:michael@cco.com)

*Microsoft*<sup>®</sup>

*Your potential. Our passion.*<sup>™</sup>

© 2007 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

 Microsoft<sup>®</sup>  
**Office SharePoint<sup>®</sup>**  
**Server 2007**