



December 1st, 2012

Antonio Maio
Microsoft SharePoint Server MVP
Senior Product Manager, TITUS

Email: Antonio.maio@titus.com
Blog: www.trustsharepoint.com
www.titus.com/blog
Twitter: @AntonioMaio2

SHAREPOINT SATURDAY
OTTAWA



December 1st, 2012

Antonio Maio
Microsoft SharePoint Server MVP
Senior Product Manager, TITUS

Email: Antonio.maio@titus.com
Blog: www.trustsharepoint.com
www.titus.com/blog
Twitter: @AntonioMaio2

SHAREPOINT SATURDAY
OTTAWA



December 1st, 2012

Antonio Maio
Microsoft SharePoint Server MVP
Senior Product Manager, TITUS

Email: Antonio.maio@titus.com
Blog: www.trustsharepoint.com
www.titus.com/blog
Twitter: @AntonioMaio2

SHAREPOINT SATURDAY
OTTAWA



December 1st, 2012

Antonio Maio
Microsoft SharePoint Server MVP
Senior Product Manager, TITUS

Email: Antonio.maio@titus.com
Blog: www.trustsharepoint.com
www.titus.com/blog
Twitter: @AntonioMaio2

SHAREPOINT SATURDAY
OTTAWA



December 1st, 2012

Antonio Maio
Microsoft SharePoint Server MVP
Senior Product Manager, TITUS

Email: Antonio.maio@titus.com
Blog: www.trustsharepoint.com
www.titus.com/blog
Twitter: @AntonioMaio2

SHAREPOINT SATURDAY
OTTAWA

TITUS Introduction



Data Security & Classification Market Leader

- Over 500 Enterprise Customers
- Over 2 Million Users Deployed
- SharePoint Security
- Email and Document Marking
- Data Loss Prevention

Introduction

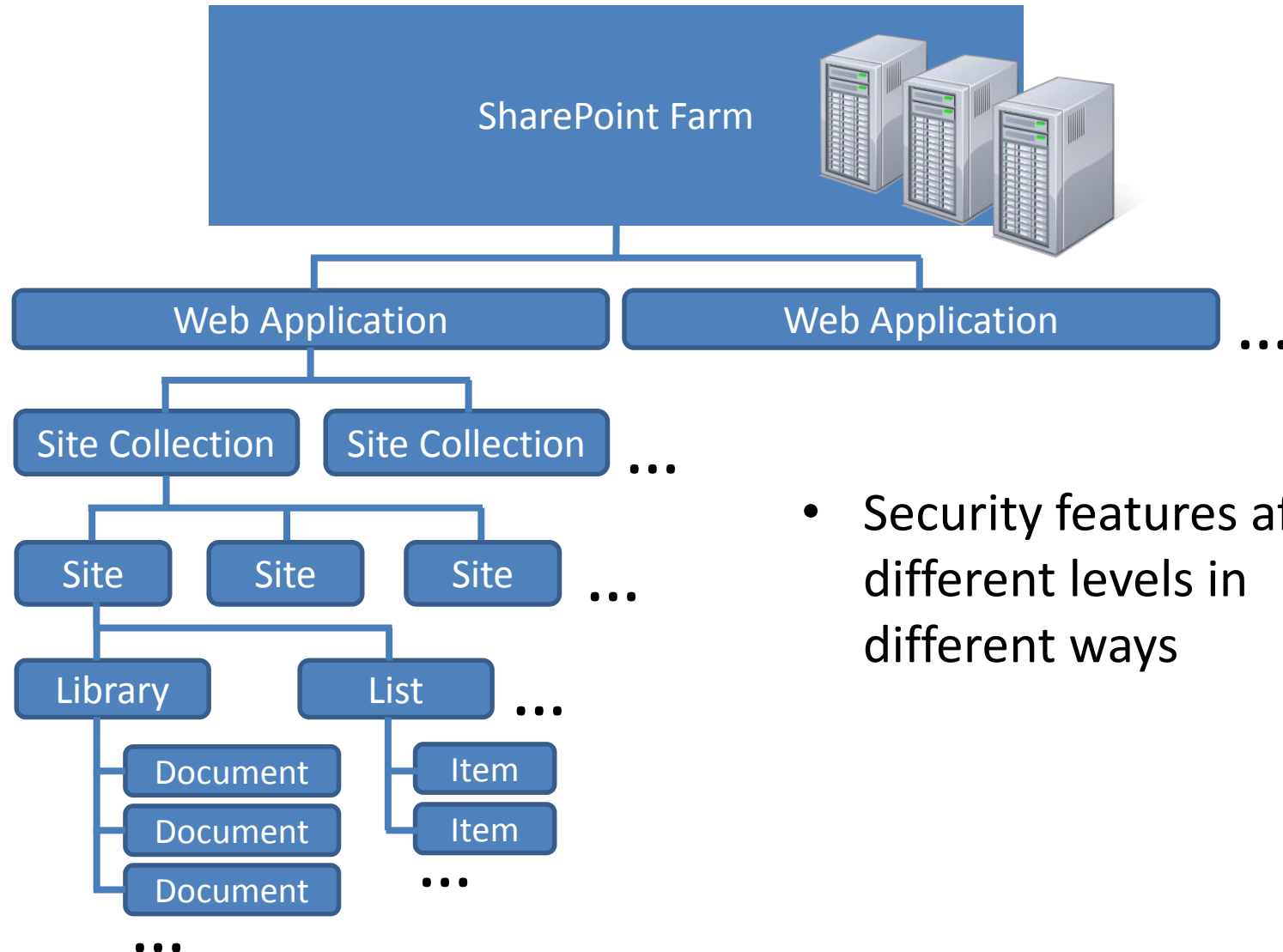
Goal - Inform and educate on key SharePoint security features

- Focus on SharePoint 2010 and SharePoint 2013
- Security is built into many aspects of SharePoint
- Sometimes an after thought for deployments... Requires good planning
- Critical consideration in government and military deployments
- Driven by Regulations & Compliance, Reporting Obligations, Secure Information Sharing...

Topics

- Deployment planning & managed accounts
- Authentication
- Web Application Policies
- Anonymous Access & Public Facing Sites
- Data Governance
- Permissions
- Other...
 - Information Rights Management
 - User License Enforcement
 - Privileged Users

SharePoint Hierarchy

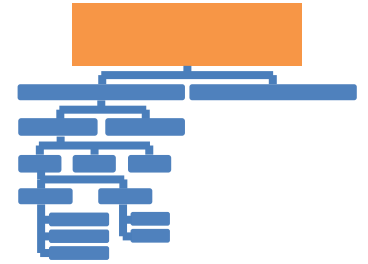


- Security features affected different levels in different ways

Deployment Planning/Managed Accounts

- SharePoint is a web application built on top of SQL Server
- Best Practice: specific managed accounts for specific purposes with least privileges... Planning required
- Benefits: Separation of Concerns
 - Separation of data
 - Multiple points of redundancy
 - Targeted auditing of account usage
 - Minimize risk of compromised accounts
 - Minimize risk of information leaks
- Review SharePoint deployment guide before you install (at least this section)

Examples of Managed Accounts



1. SQL Server Service Account

- Purpose: Assign to MSSQLSERVER and SQLSERVERAGENT services when you install SQL Server (ex: domain\SQL_service)
- No special domain permissions - given required rights on the SQL Server during setup

2. Setup User Account

- Purpose: Used to install SharePoint, run Product Config Wizard, install patches/updates
- login with this account when running setup (ex: domain\sp_setup_user)
- Must be local admin on each server in SharePoint farm (except SQL Server if different box)

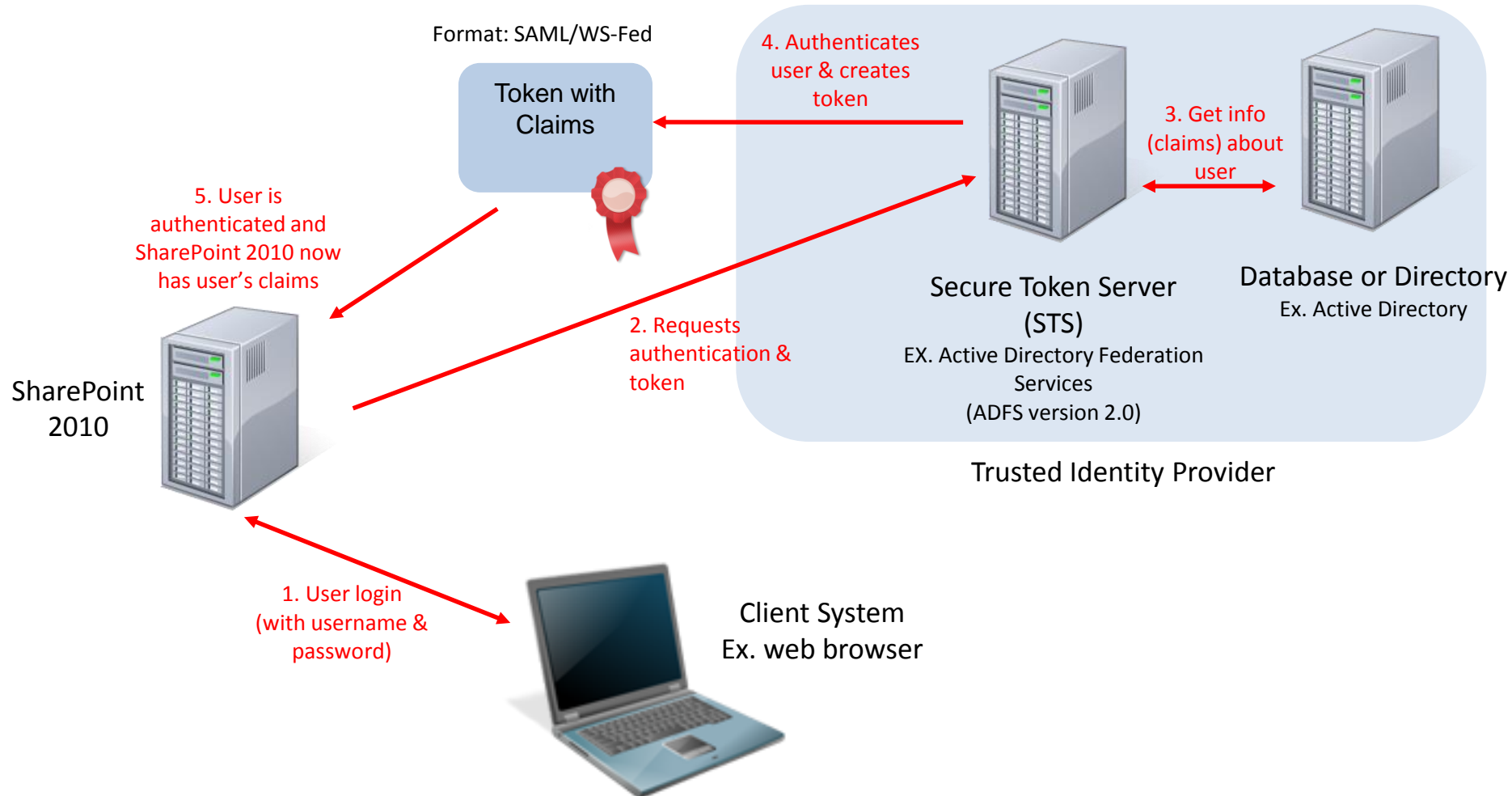
3. SharePoint Farm Account (Database Access Account)

- Purpose: the service account used to run the SharePoint farm; not just for database access (ex. domain\sp_farm_user)
- After Product Config Wizard is run, prompted to provide the Database Access Account – misnamed in UI, this is really the farm service account

- Should all be AD domain accounts
- Do not use personal admin account , especially for Farm Account
- Configure central email account for all managed accounts

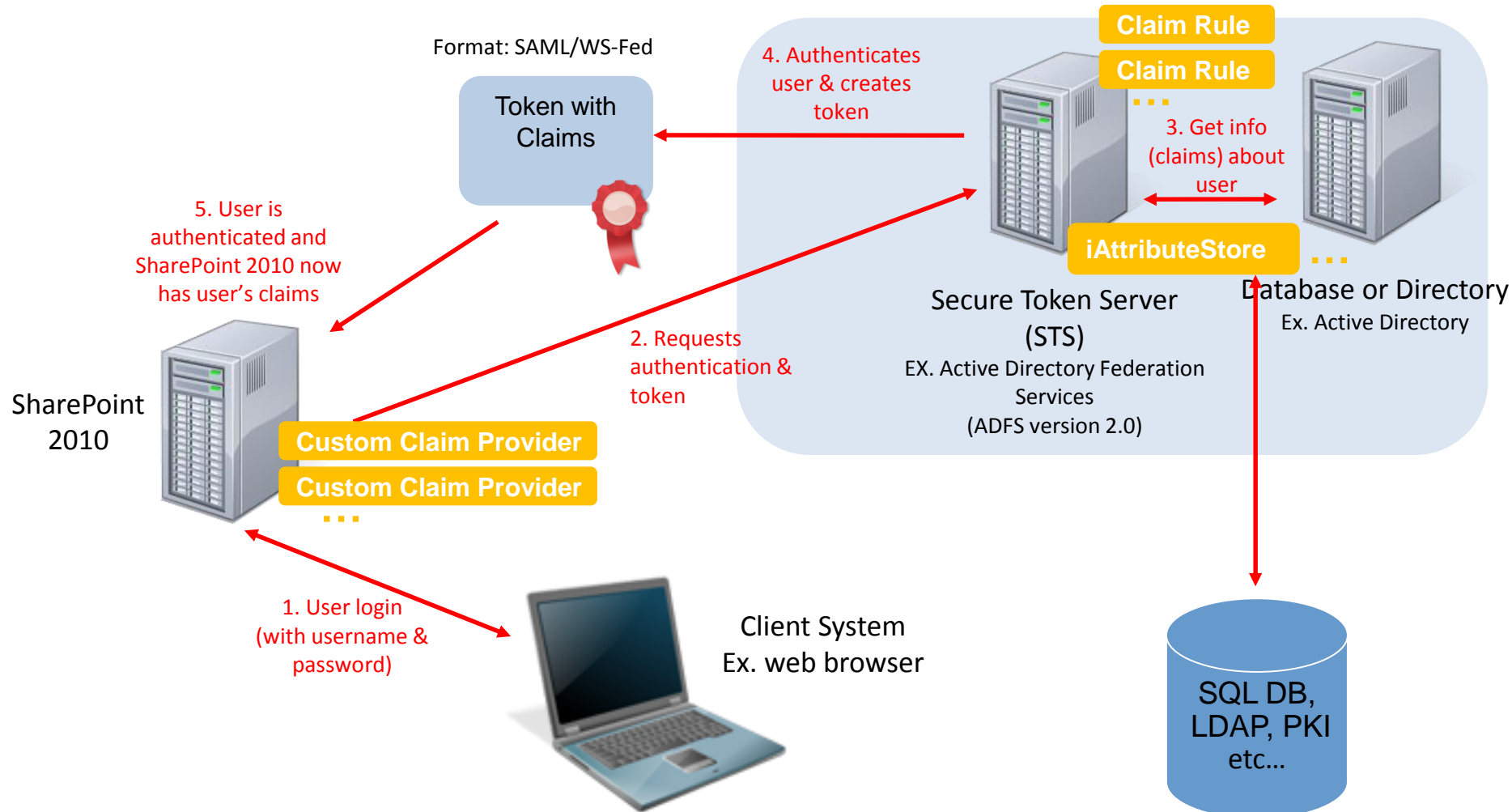
- Determine that users are who they say they are (login)
 - Configured on each web app
 - Multiple authentication methods per web app
- SharePoint 2010 Options
 - Classic Mode Authentication (Integrated Auth, NTLM, Kerberos)
 - Claims Based Authentication
 - Forms Based Authentication available- done through Claims Based Auth.
 - UI configuration only available in UI upon web app creation
 - To convert non-claims based web app to claims will require PowerShell
- SharePoint 2013 Options
 - Claims Based Authentication - default
 - Classic Mode Configuration UI has been removed – only configurable through PowerShell

Claims Based Authentication



Claims Based Authentication

Customization



```

graph TD
    A[Root] --> B[Intermediate 1]
    A --> C[Intermediate 2]
    B --> D[Leaf 1]
    B --> E[Leaf 2]
    C --> F[Leaf 3]
    C --> G[Leaf 4]
    C --> H[Leaf 5]
    C --> I[Leaf 6]
    C --> J[Leaf 7]
    C --> K[Leaf 8]
    C --> L[Leaf 9]
    C --> M[Leaf 10]
    C --> N[Leaf 11]
    C --> O[Leaf 12]
    C --> P[Leaf 13]
    C --> Q[Leaf 14]
    C --> R[Leaf 15]
    C --> S[Leaf 16]
    C --> T[Leaf 17]
    C --> U[Leaf 18]
    C --> V[Leaf 19]
    C --> W[Leaf 20]
    C --> X[Leaf 21]
    C --> Y[Leaf 22]
    C --> Z[Leaf 23]
    C --> AA[Leaf 24]
    C --> AB[Leaf 25]
    C --> AC[Leaf 26]
    C --> AD[Leaf 27]
    C --> AE[Leaf 28]
    C --> AF[Leaf 29]
    C --> AG[Leaf 30]
    C --> AH[Leaf 31]
    C --> AI[Leaf 32]
    C --> AJ[Leaf 33]
    C --> AK[Leaf 34]
    C --> AL[Leaf 35]
    C --> AM[Leaf 36]
    C --> AN[Leaf 37]
    C --> AO[Leaf 38]
    C --> AP[Leaf 39]
    C --> AQ[Leaf 40]
    C --> AR[Leaf 41]
    C --> AS[Leaf 42]
    C --> AT[Leaf 43]
    C --> AU[Leaf 44]
    C --> AV[Leaf 45]
    C --> AW[Leaf 46]
    C --> AX[Leaf 47]
    C --> AY[Leaf 48]
    C --> AZ[Leaf 49]
    C --> BA[Leaf 50]
    C --> BB[Leaf 51]
    C --> BC[Leaf 52]
    C --> BD[Leaf 53]
    C --> BE[Leaf 54]
    C --> BF[Leaf 55]
    C --> BG[Leaf 56]
    C --> BH[Leaf 57]
    C --> BI[Leaf 58]
    C --> BJ[Leaf 59]
    C --> BK[Leaf 60]
    C --> BL[Leaf 61]
    C --> BM[Leaf 62]
    C --> BN[Leaf 63]
    C --> BO[Leaf 64]
    C --> BP[Leaf 65]
    C --> BQ[Leaf 66]
    C --> BR[Leaf 67]
    C --> BS[Leaf 68]
    C --> BT[Leaf 69]
    C --> BU[Leaf 70]
    C --> BV[Leaf 71]
    C --> BW[Leaf 72]
    C --> BX[Leaf 73]
    C --> BY[Leaf 74]
    C --> BZ[Leaf 75]
    C --> CA[Leaf 76]
    C --> CB[Leaf 77]
    C --> CC[Leaf 78]
    C --> CD[Leaf 79]
    C --> CE[Leaf 80]
    C --> CF[Leaf 81]
    C --> CG[Leaf 82]
    C --> CH[Leaf 83]
    C --> CI[Leaf 84]
    C --> CJ[Leaf 85]
    C --> CK[Leaf 86]
    C --> CL[Leaf 87]
    C --> CM[Leaf 88]
    C --> CN[Leaf 89]
    C --> CO[Leaf 90]
    C --> CP[Leaf 91]
    C --> CQ[Leaf 92]
    C --> CR[Leaf 93]
    C --> CS[Leaf 94]
    C --> CT[Leaf 95]
    C --> CU[Leaf 96]
    C --> CV[Leaf 97]
    C --> CW[Leaf 98]
    C --> CX[Leaf 99]
    C --> CY[Leaf 100]
    C --> CZ[Leaf 101]
    C --> DA[Leaf 102]
    C --> DB[Leaf 103]
    C --> DC[Leaf 104]
    C --> DD[Leaf 105]
    C --> DE[Leaf 106]
    C --> DF[Leaf 107]
    C --> DG[Leaf 108]
    C --> DH[Leaf 109]
    C --> DI[Leaf 110]
    C --> DJ[Leaf 111]
    C --> DK[Leaf 112]
    C --> DL[Leaf 113]
    C --> DM[Leaf 114]
    C --> DN[Leaf 115]
    C --> DO[Leaf 116]
    C --> DP[Leaf 117]
    C --> DQ[Leaf 118]
    C --> DR[Leaf 119]
    C --> DS[Leaf 120]
    C --> DT[Leaf 121]
    C --> DU[Leaf 122]
    C --> DV[Leaf 123]
    C --> DW[Leaf 124]
    C --> DX[Leaf 125]
    C --> DY[Leaf 126]
    C --> DZ[Leaf 127]
    C --> EA[Leaf 128]
    C --> EB[Leaf 129]
    C --> EC[Leaf 130]
    C --> ED[Leaf 131]
    C --> EE[Leaf 132]
    C --> EF[Leaf 133]
    C --> EG[Leaf 134]
    C --> EH[Leaf 135]
    C --> EI[Leaf 136]
    C --> EJ[Leaf 137]
    C --> EK[Leaf 138]
    C --> EL[Leaf 139]
    C --> EM[Leaf 140]
    C --> EN[Leaf 141]
    C --> EO[Leaf 142]
    C --> EP[Leaf 143]
    C --> EQ[Leaf 144]
    C --> ER[Leaf 145]
    C --> ES[Leaf 146]
    C --> ET[Leaf 147]
    C --> EU[Leaf 148]
    C --> EV[Leaf 149]
    C --> EW[Leaf 150]
    C --> EX[Leaf 151]
    C --> EY[Leaf 152]
    C --> EZ[Leaf 153]
    C --> FA[Leaf 154]
    C --> FB[Leaf 155]
    C --> FC[Leaf 156]
    C --> FD[Leaf 157]
    C --> FE[Leaf 158]
    C --> FF[Leaf 159]
    C --> FG[Leaf 160]
    C --> FH[Leaf 161]
    C --> FI[Leaf 162]
    C --> FJ[Leaf 163]
    C --> FK[Leaf 164]
    C --> FL[Leaf 165]
    C --> FM[Leaf 166]
    C --> FN[Leaf 167]
    C --> FO[Leaf 168]
    C --> FP[Leaf 169]
    C --> FQ[Leaf 170]
    C --> FR[Leaf 171]
    C --> FS[Leaf 172]
    C --> FT[Leaf 173]
    C --> FU[Leaf 174]
    C --> FV[Leaf 175]
    C --> FW[Leaf 176]
    C --> FX[Leaf 177]
    C --> FY[Leaf 178]
    C --> FZ[Leaf 179]
    C --> GA[Leaf 180]
    C --> GB[Leaf 181]
    C --> GC[Leaf 182]
    C --> GD[Leaf 183]
    C --> GE[Leaf 184]
    C --> GF[Leaf 185]
    C --> GG[Leaf 186]
    C --> GH[Leaf 187]
    C --> GI[Leaf 188]
    C --> GJ[Leaf 189]
    C --> GK[Leaf 190]
    C --> GL[Leaf 191]
    C --> GM[Leaf 192]
    C --> GN[Leaf 193]
    C --> GO[Leaf 194]
    C --> GP[Leaf 195]
    C --> GQ[Leaf 196]
    C --> GR[Leaf 197]
    C --> GS[Leaf 198]
    C --> GT[Leaf 199]
    C --> GU[Leaf 200]
    C --> GV[Leaf 201]
    C --> GW[Leaf 202]
    C --> GX[Leaf 203]
    C --> GY[Leaf 204]
    C --> GZ[Leaf 205]
    C --> HA[Leaf 206]
    C --> HB[Leaf 207]
    C --> HC[Leaf 208]
    C --> HD[Leaf 209]
    C --> HE[Leaf 210]
    C --> HF[Leaf 211]
    C --> HG[Leaf 212]
    C --> HH[Leaf 213]
    C --> HI[Leaf 214]
    C --> HJ[Leaf 215]
    C --> HK[Leaf 216]
    C --> HL[Leaf 217]
    C --> HM[Leaf 218]
    C --> HN[Leaf 219]
    C --> HO[Leaf 220]
    C --> HP[Leaf 221]
    C --> HQ[Leaf 222]
    C --> HR[Leaf 223]
    C --> HS[Leaf 224]
    C --> HT[Leaf 225]
    C --> HU[Leaf 226]
    C --> HV[Leaf 227]
    C --> HW[Leaf 228]
    C --> HX[Leaf 229]
    C --> HY[Leaf 230]
    C --> HZ[Leaf 231]
    C --> IA[Leaf 232]
    C --> IB[Leaf 233]
    C --> IC[Leaf 234]
    C --> ID[Leaf 235]
    C --> IE[Leaf 236]
    C --> IF[Leaf 237]
    C --> IG[Leaf 238]
    C --> IH[Leaf 239]
    C --> II[Leaf 240]
    C --> IJ[Leaf 241]
    C --> IK[Leaf 242]
    C --> IL[Leaf 243]
    C --> IM[Leaf 244]
    C --> IN[Leaf 245]
    C --> IO[Leaf 246]
    C --> IP[Leaf 247]
    C --> IQ[Leaf 248]
    C --> IR[Leaf 249]
    C --> IS[Leaf 250]
    C --> IT[Leaf 251]
    C --> IU[Leaf 252]
    C --> IV[Leaf 253]
    C --> IW[Leaf 254]
    C --> IX[Leaf 255]
    C --> IY[Leaf 256]
    C --> IZ[Leaf 257]
    C --> JA[Leaf 258]
    C --> JB[Leaf 259]
    C --> JC[Leaf 260]
    C --> JD[Leaf 261]
    C --> JE[Leaf 262]
    C --> JF[Leaf 263]
    C --> JG[Leaf 264]
    C --> JH[Leaf 265]
    C --> JI[Leaf 266]
    C --> JJ[Leaf 267]
    C --> JK[Leaf 268]
    C --> JL[Leaf 269]
    C --> JM[Leaf 270]
    C --> JN[Leaf 271]
    C --> JO[Leaf 272]
    C --> JP[Leaf 273]
    C --> JQ[Leaf 274]
    C --> JR[
```

- **User Permissions**
 - Permissions available within permission levels at site collection level
- **Permission Policies**
 - Define groups of permissions (similar to permission levels)
 - Control if site collection admins have full control on any object in site col.
 - Only place with a “Deny” capability (default: deny write, deny all)
- **User Policies**
 - Assign permission policies to users and groups for the entire web app
 - Ex. Deny group from deleting items within an entire web app – applicable to public facing web app
- **Blocked File Types**
 - Prevent specific files types from being added to libraries within web app

Web Application Permission Policies

Application Management > Manage Web Applications

The screenshot shows the 'Add Permission Policy Level' dialog box, which is used to configure permissions for a web application. The dialog is divided into three main sections: 'Name and Description', 'Site Collection Permissions', and 'Permissions'.

Name and Description

Enter a name and description for this permission policy level.

Name:

Description:

Site Collection Permissions

Choose the site collection level permissions the policy level should have.

☐ Site Collection Administrator - Site collection administrators have Full Control over the entire site collection and can perform any action on any object.

☐ Site Collection Auditor - Site collection auditors have Full Read access for the entire site collection including reading permissions and configuration data.

Permissions

Choose which permissions to grant or deny in this permission policy level. Granting permissions gives users this permission. Denying permissions prevents users from ever having this permission.

Select the permission to grant or deny in this permission policy level.

Grant	Deny	
<input type="checkbox"/>	<input type="checkbox"/>	All
<input type="checkbox"/>	<input type="checkbox"/>	All
<input type="checkbox"/>	<input type="checkbox"/>	Manage Lists - Create and delete lists, add or remove columns in a list, and add or remove public views of a list.
<input type="checkbox"/>	<input type="checkbox"/>	Override Check Out - Discard or check in a document which is checked out to another user.
<input type="checkbox"/>	<input type="checkbox"/>	Add Items - Add items to lists and

The background shows the 'Central Administration' interface with the 'Application Management' section selected. The 'AMDEMO\administrator' user is logged in. A table with columns 'Port' and '34540/' is visible in the background.

Web Application User Policies

Application Management > Manage Web Applications

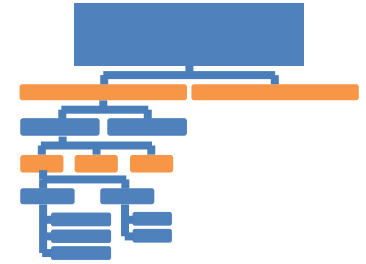
The screenshot displays the SharePoint Central Administration console. The top navigation bar includes 'Site Actions', 'Browse', and 'Web Applications'. The 'Web Applications' section is active, showing a ribbon with 'Contribute' (New, Extend, Delete), 'Manage' (General Settings, Managed Paths, Service Connections), 'Security' (Authentication Providers, Self-Service Site Creation, Web Part Security), and 'Policy' (User Policy, Anonymous Policy, Permission Policy). The 'User Policy' link is highlighted in red.

The 'Policy for Web Application' dialog box is open, showing a table of users and their permissions. The table has columns for 'Zone', 'Display Name', 'User Name', and 'Permissions'. The 'OK' button is visible at the top right of the dialog.

Zone	Display Name	User Name	Permissions
<input type="checkbox"/> (All zones)	NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\LOCAL SERVICE	Full Read
<input type="checkbox"/> (All zones)	Search Crawling Account	AMDEMO\Farm.admin	Full Read

Anonymous Access

Public Facing Sites



- Turn on or off for web application – only making available for sites
 - Central Admin> Manage Web Apps> Authentication Providers
 - Edit an Authentication Provider
 - Check on ‘Enable Anonymous Access’ for that provider
 - Select “Anonymous Policy” for the web app
 - Select zone and policy for anonymous access

The screenshot shows a dialog box titled "Anonymous Access Restrictions". It is divided into two main sections: "Select the Zone" and "Permissions".

Select the Zone: This section contains a text box with the following text: "The security policy will apply to requests made through the specified zone. To apply a policy to all zones, select '(All zones)'. All zone policies are only valid for Windows users." To the right of this text is a dropdown menu labeled "Zones:" with "Default" selected.

Permissions: This section contains a text box with the following text: "Choose the permissions you want anonymous users to have." To the right of this text is a section labeled "Anonymous User Policy:" with three radio button options: "None - No policy" (which is selected), "Deny Write - Has no write access", and "Deny All - Has no access".

At the bottom of the dialog box are two buttons: "Save" and "Cancel".

-
- The screenshot shows the 'Anonymous Access' dialog box in SharePoint. The dialog is titled 'Anonymous Access' and has a close button. It contains two main sections. The left section is titled 'Anonymous Access' and contains a paragraph: 'Specify what parts of your Web site (if any) anonymous users can access. If you select Entire Web site, anonymous users will be able to view all pages in your Web site and view all lists and items which inherit permissions from the Web site. If you select Lists and libraries, anonymous users will be able to view and change items only for those lists and libraries that have enabled permissions for anonymous users.' The right section is titled 'Anonymous users can access:' and contains three radio button options: 'Entire Web site', 'Lists and libraries', and 'Nothing'. The 'Nothing' option is selected. At the bottom of the dialog are 'OK' and 'Cancel' buttons. In the background, the 'Permission Tools' ribbon is visible, showing 'Grant Permissions', 'Create Group', 'Edit User Permissions', and 'Remove User Permissions' buttons. Below these buttons is a table with columns 'Libraries' and 'Name'. The 'Libraries' column lists 'Site Pages', 'Shared Documents', 'Lists', 'Calendar', and 'Tasks'. The 'Name' column lists 'Demos', 'Demos', 'Demos', 'System', and 'Viewers'. Each row has a checkbox in the 'Name' column.

Anonymous Access

Risks of Incorrect Configuration

- Risk: Inadvertent exposure of internal data on a public web site
- All form pages and `_vti_bin` web services are accessible - PUBLICLY
- Modify the URL of a public facing SharePoint site:
<http://www.mypublicsite.com/SitePages/Home.aspx> to
http://www.mypublicsite.com/_layouts/viewlsts.aspx
- View All Site Content page is now exposed, typically in SharePoint branding, with all site content visible
- Desired behavior: user is presented with a login page, or an HTTP error
- Accessible pages

`/_layouts/adminrecyclebin.aspx`
`/_layouts/bpcf.aspx`
`/_layouts/create.aspx`
`/_layouts/listfeed.aspx`
`/_layouts/managefeatures.aspx`
`/_layouts/mngsiteadmin.aspx`
`/_layouts/mngsubwebs.aspx`

`/_layouts/policy.aspx`
`/_layouts/policyconfig.aspx`
`/_layouts/policycts.aspx`
`/_layouts/policylist.aspx`
`/_layouts/mcontent.aspx`
`/_layouts/sitemanager.aspx`
`/_layouts/stor_man.aspx`

`/_layouts/recyclebin.aspx`
`/_layouts/wrkmg.aspx`
`/_layouts/vsubwebs.aspx`
`/_layouts/pagesettings.aspx`
`/_layouts/settings.aspx`
`/_layouts/newsbweb.aspx`
`/_layouts/userdisp.aspx`

Anonymous Access

Lockdown Feature & Web.Config

- Purpose: Removes **View Application Pages** permission & **Use Remote Interfaces** permission from Limited Access permission level (which is what's used for anonymous users)
 - Prevents anonymous users from accessing form pages
- Setting Lockdown Feature:
 - Remove all anonymous access from the site
 - open command prompt and go to the folder C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN
 - Check whether the feature is enabled or not (If ViewFormPagesLockDown is listed, it's enabled):
get-spfeature -site http://url
 - If not listed then we must enable it using:
stsadm -o activatefeature -url -filename ViewFormPagesLockDown\feature.xml
 - To disable it:
stsadm -o deactivatefeature -url -filename ViewFormPagesLockDown\feature.xml
 - Reset anonymous access on the site
- Available in MOSS2007, SharePoint 2010 and SharePoint 2013
 - On by default for Publishing Portal Site Template – for other site templates must turn it on manually

Anonymous Access

Lockdown Feature & Web.Config

- To prevent access to _layouts pages and web services we must also:

```
<add path="configuration">
  <location path="_layouts">
    <system.web>
      <authorization>
        <deny users="?" />
      </authorization>
    </system.web>
  </location>

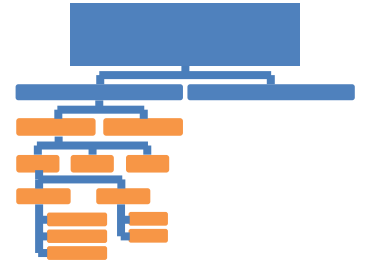
  <location path="_vti_bin">
    <system.web>
      <authorization>
        <deny users="?" />
      </authorization>
    </system.web>
  </location>

  <location path="_layouts/login.aspx">
    <system.web>
      <authorization>
        <allow users="?" />
      </authorization>
    </system.web>
  </location>
```

```
<location path="_layouts/error.aspx">
  <system.web>
    <authorization>
      <allow users="?" />
    </authorization>
  </system.web>
</location>

<location path="_layouts/accessdenied.aspx">
  <system.web>
    <authorization>
      <allow users="?" />
    </authorization>
  </system.web>
</location>
```

Permissions



- Permissions can apply to any information object or container in SharePoint
 - Determine who gets access to what information objects and what type of access
- Applying permissions include selecting a permission level (ex. Full control) and a user or group and assigning it to information object (ex. document, item, etc.)
 - Can apply to SharePoint user/group or AD user/group

Finance AD Group has Full Control on Library

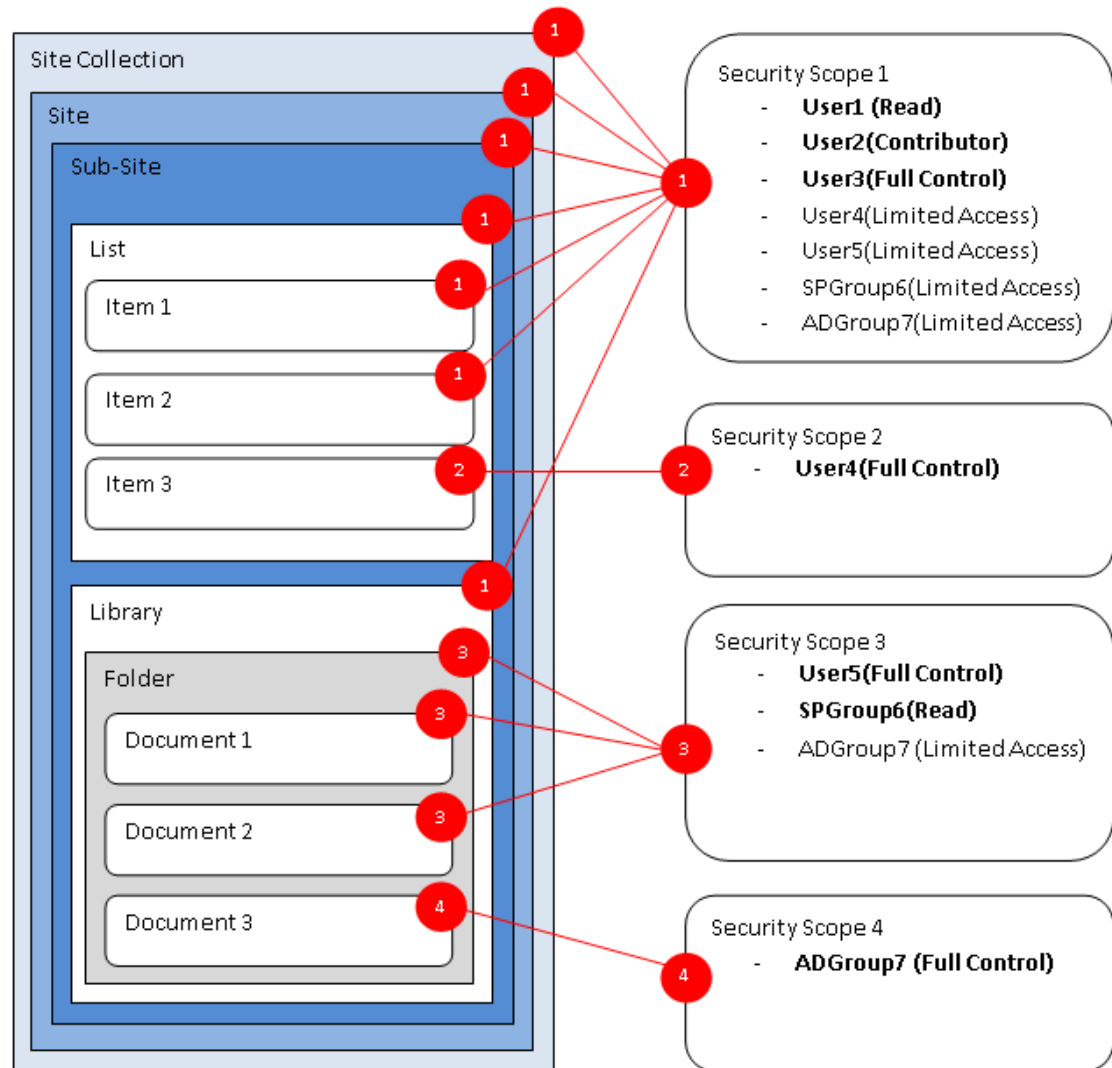
ProjectXContractor SharePoint Group has Read access on site

Antonio.Maio AD user has Contribute access on Document

- Permission Levels are created at Site Collection Level

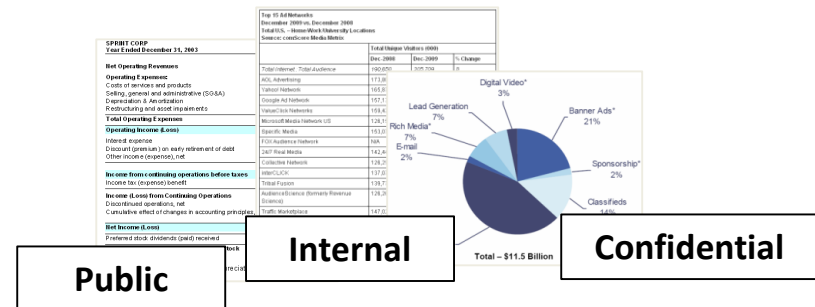
Permissions and Security Scopes

- Hierarchical permission model: permissions are inherited from level above
or
- Can break inheritance and apply unique permissions
- Breaking inheritance is a manual process
- See my detailed whitepaper on this “Effectively Manage Permissions...” at <http://www.titus.com/resources/sharepoint.php>



Fine Grained Permissions

- Trend: sensitive content sitting beside non-sensitive content
- Leads to customers exploring fine grained permissions
- Recommendation:
 - Use metadata to identify which data to protect
 - User attributes (claims) to determine who should have access
 - Implemented automated solution to manage fine-grained permissions



Other Security Features

- Information Rights Management

- ADRMS Integration - Encrypts documents when opened/saved from SharePoint (so content is still searchable)
- Sets information rights (do not print, do not forward, etc.)
- Granularity limited to library
- Supports MS Office documents (+PDF in SharePoint 2013)
- See my detailed blog: www.titus.com/blog



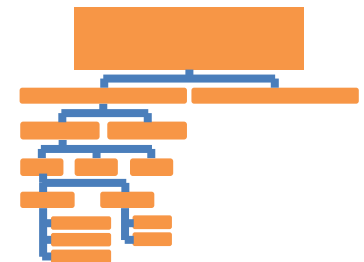
- User License Enforcement

- New in SharePoint 2013 – support for mixed mode licensing
- Some users can be on Standard and some on Enterprise
- Managed through AD Groups and PowerShell
- Elegantly deals with standard users accessing a page with an enterprise web part
- See my detailed blog: www.titus.com/blog



- Privileged Users

- What if your farm or site collection admins are consultants or not TS Cleared



TITUS Prize Giveaway



- See us at TITUS booth today
- Come to TITUS Vendor session this afternoon (Rm. 123 @ 4pm)

- TITUS SharePoint Security Suite
- More SharePoint Security, Less Effort
- Ensure the right people are accessing the Right Information
- Raise Awareness about Sensitive Data
- Promote End User Accountability for Sensitive Data



Thank you to all of our Sponsors!!



Remember to fill out your evaluation forms to win some great prizes!

&

Join us for SharePint today!

Date & Time: Dec 1st, 2012 @6:00 pm
Location: Pub Italia
Address: 434 ½ Preston Street
Parking: On street with meters \$
Site: <http://www.pubitalia.ca/>