Realtime publishers

The Shortcut Guide™ To

Centralized SharePoint Administration

sponsored by

AvePoint®
Unleashing the Power of SharePoint™

Wendy Henry

Copyright Statement

Chapter 2: Understanding SharePoint Administration Hierarchy

Large SharePoint enterprises often require an entire team of professionals to assure optimal usability and performance of the environment. Tasked with managing the various levels of the logical infrastructure in SharePoint, not to mention the IIS and SQL Server applications essential to SharePoint, these individuals work together to provide a stable collaboration platform. Some, or most, of the administrators may be IT personnel, but information workers may also play a role in managing their own delegated SharePoint resources. Web masters and Database Administrators responsible for all IIS and SQL Server resources on the network can influence SharePoint Web sites and databases residing on the servers they manage.

When it comes to SharePoint itself, Microsoft advocates a tiered administration model. The manufacturer recommends a 2-tier model for Windows SharePoint Services v3.0 that separates farm administration from individual site administration (see Table 2.1). This model allows companies to easily differentiate between IT support for the infrastructure and information worker empowerment for the site resources. Microsoft Office SharePoint Server 2007 can be addressed by the same 2-tier model as WSSv3 with an additional layer between farm and site administration that focuses on the MOSS Shared Services Provider (see Table 2.1).

TIER 1: Farm Administrator	Responsible for farm services layout, configuration, management and performance monitoring. Duties also include web application management, configuring email settings, backup/restore, defining external service connections, SSO and Forms Services settings, setting up logging and usage analysis, and configuring farm security.
TIER 2: SSP Administrator	Responsible for MOSS Shared Services Provider configuration and association. Duties include SharePoint user profile property management, MySites configuration, personalization settings, enterprise Search and Index management, globally-compiled audiences, and optional Excel Calculation Services and Business Data Catalog administration (MOSS Enterprise only) .
TIER 3: Site Administrator	Tasked with site administration within the farm including but not limited to optional self-service top level site creation (new site collections), top-level site inheritable permissions structure, web part management, content management, individual site object creation/administration

Table 2.1: Microsoft Office SharePoint Server 2007 Administration Model highlighting site level administration.

This chapter will examine the different responsibilities and possible configuration settings that can be managed at each tier of Microsoft's SharePoint Administration Model. Starting at the top, we will first examine global settings that affect Web applications (and thus the site collections within them). We'll then explore the MOSS Shared Service Provider management at tier two. Lastly, this chapter will divide the bottom administration tier into site collection versus individual site management. There is much to discuss, so let's get started!

Global Web Application Administration

Farm management at the top tier of Microsoft's administration model for SharePoint includes service administration as well as Web application and some site collection duties. Scaling SharePoint into a farm by assigning certain services to specific servers and configuring each of the services' properties can be accomplished in Central Administration or the CLI via stsadm.exe by a user with elevated authority (such as membership in the Farm Administrators SharePoint group in SharePoint and the local Administrators group in the Windows OS). The previous chapter outlined challenges faced when using the two native administration utilities to manage multiple farm servers concurrently.

Instead of further analyzing service administration, let's focus on the Web application management responsibilities of a tier-one administrator. To comprehend the breadth that a Web application administrator's decisions can reach, we must first understand the logical architecture of a Web application in SharePoint. What does it contain? Where does it reside? And how bad would it really be if the tier-one administrator made a mistake at the Web application level?

> **Resource**
>
> For more information on Microsoft's SharePoint Administration Model first tier, see TechNet article http://technet.microsoft.com/en-us/library/cc288765.aspx (WSS) or http://msdn.microsoft.com/en-us/library/bb447594.aspx (MOSS).

Logical Explanation of Web Applications

In SharePoint vocabulary, a Web application represents the logical container of one or more site collections. Like a parent object, Web applications bear configuration settings that influence the behavior of their associated site collections. Creating new Web applications can be accomplished by tier-one administrators. New Web applications will automatically generate a corresponding new Web site in IIS that executes the SharePoint Web application, creating a 1:1 relationship between the SharePoint Web application and its IIS Web site. Similarly, a new content database will be created in SQL Server by default during the inauguration of a new Web application (see Figure 2.1). A Web application's relationship to IIS and/or SQL can be altered, forming 1:many relationships. Why? One example is the need for an extranet site in IIS that exposes the intranet site content for partners or telecommuting employees. Another is the need to increase capacity by adding content databases in SQL Server.

Cross-Reference

For details about creating or extending SharePoint Web applications, see Microsoft TechNet articles http://technet.microsoft.com/en-us/library/cc287954.aspx and http://technet.microsoft.com/en-us/library/cc825317.aspx.

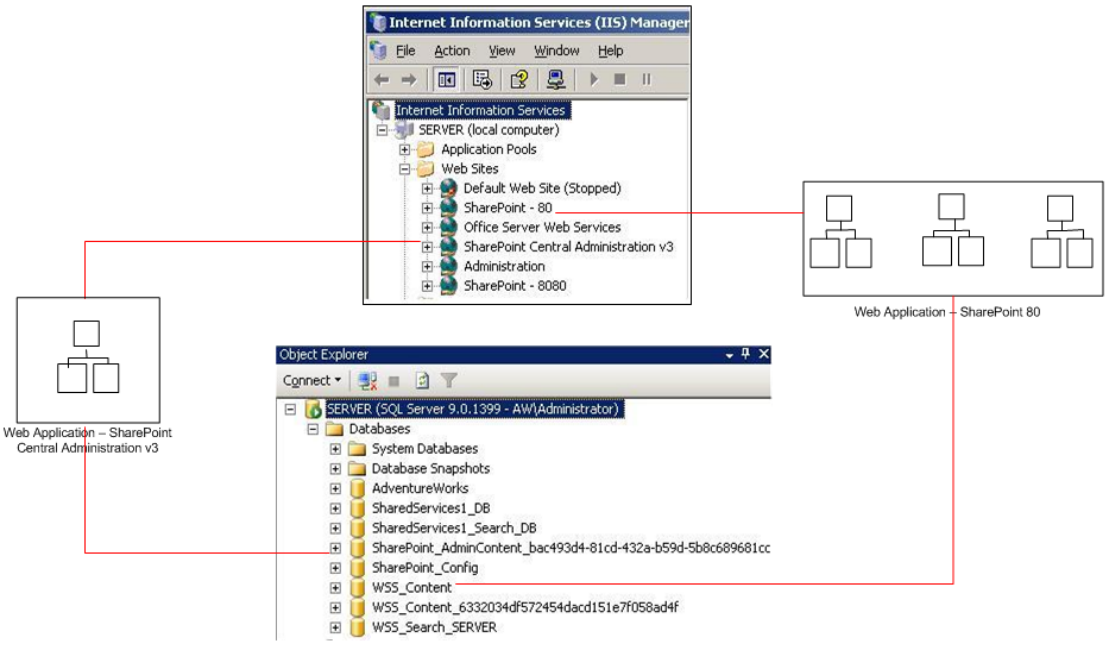

Figure 2.1: Logical mapping of SharePoint Web applications to IIS and SQL Server.

Understanding the relationships of a SharePoint Web application sheds light on one of the reasons Web application management should be restricted to a chosen few skilled tier-one administrators. Well-intentioned yet excessive Web application creation could result in superfluous SQL databases and IIS Web sites to administer. But even well-planned multiple Web applications can be a challenge to configure identically using the native SharePoint administration tools because both the Central Administration interface and stsadm.exe CLI utility operate against one Web application at a time (see Figure 2.2).

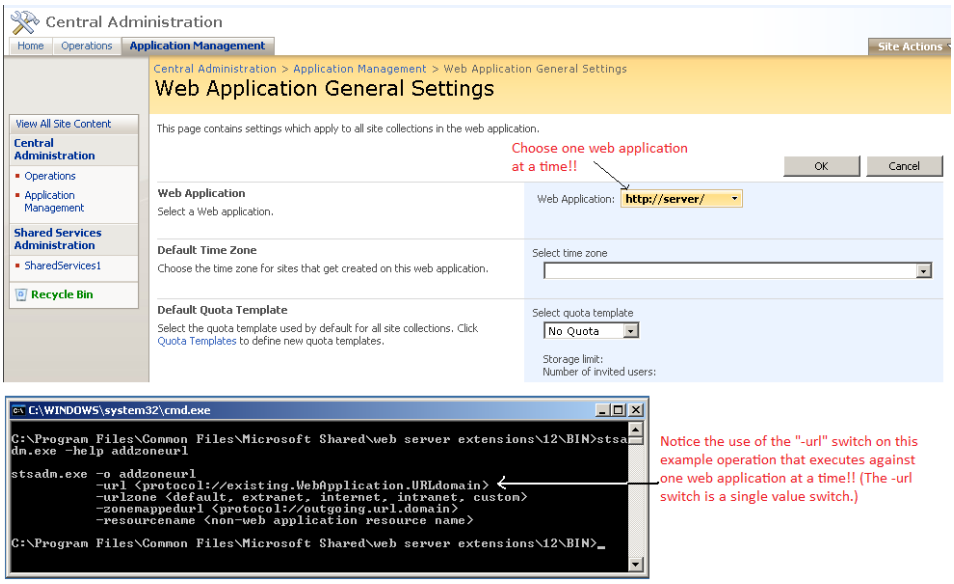

Figure 2.2: Central Administration and STSADM.EXE examples of single Web application focus.

Web Application Configuration Settings

A second reason to be selective in dubbing Web application administrators is that configuring Web applications must take into account the influence the settings will have on the behavior of all site collections within. For example, configuring a Web application to require SSL encryption will secure all SharePoint sites throughout the one or many site collections within that Web application. Configuration values set at the Web application level have a far-reaching effect on multiple sites, so attention should be paid before altering them.

Let's begin with the Web application creation process. Performed via Central Administration or stsadm.exe, Web application creation demands elevated privileges not only in SharePoint but also in the OS (for IIS site creation) and SQL Server (for content database creation).

> **Cross Reference**
>
> More about security will follow later in this section of the chapter.

To plan a new Web application, first write down the values you will provide for the configuration settings listed in Table 2.2 before accessing the Central Administration Web site.

Parameter Name	Purpose	Settings Label
IIS Web Site	Specify IIS Web site and its TCP/IP parameters	Existing Port vs. Host Header New Path
Security Configuration	Dictate authentication and TCP/IP encryption security parameters	Authentication Provider Allow Anonymous Use SSL
Load Balanced URL	Set URL domain and IE browser security zone for all sites	URL Zone
Application Pool	Define application pool for the IIS Web site	Use Existing or Create New
Reset IIS	Specify IIS reset initiation	Automatically or Manually
DB Name & Authorization	Provide SQL destination for new/existing-empty content database and access credential	Database Server Database Name Database Authentication
Search Server	Specify the Search Server the new Web application is to use	Server

Table 2.2: Web application creation values.

The Create New Web Application page in Central Administration, which can be found in the 12-hive (.....12\Template\Admin\extendvs.aspx), does a good job of aptly naming the creation parameters and labeling the settings choices. Even better, each parameter bears a description that educates the creator and even warns about possible side effects. And if you need to change the configuration of a Web application after creation, the creation settings can be altered later, though not all in one place. Web site settings (IIS Web Site, Security Configuration, Load Balanced URL, and Application Pool) can be changed in the IIS Manager console. Just be aware that SharePoint will not recognize new application pool credentials set in IIS Manager until you update the Service Accounts link on the Operations tab of Central Administration (see Figure 2.3).

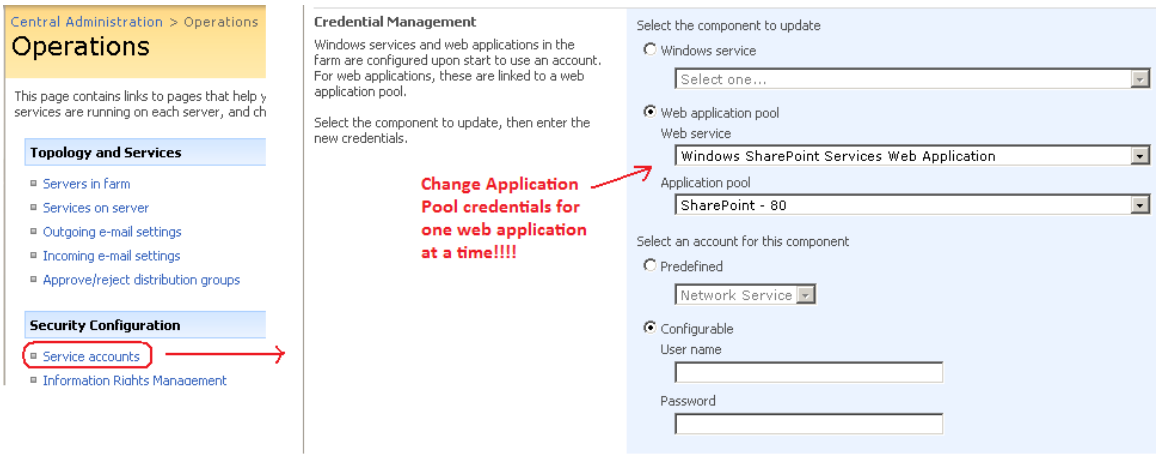

Figure 2.3: Service Accounts page (FarmCredentialManagement.aspx) from Central Administration.

Database settings (DB Name & Authorization) can be changed using the Content Databases link on the Application Management tab of Central Administration (see Figure 2.4). Just be aware that content currently stored in the existing content database will not be moved to the new content database automatically. If moving the data is your goal, a separate content migration project will be necessary and may require a robust third-party product to accomplish.

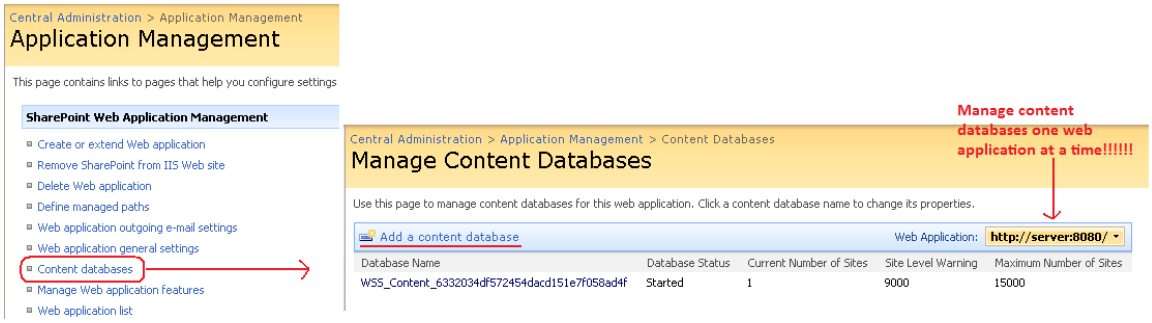

Figure 2.4: Manage Content Databases page (CNTDBADM.aspx) from Central Administration.

Configuring Web Applications in SharePoint

The scope of this guide prohibits a lengthy discussion of each individual Web application configuration setting in SharePoint. To do so would take the entire rest of the book! But there are many properties beyond those defined during Web application creation that can affect the sites within a SharePoint Web application. The following list provides a quick breakdown of Web application settings that can be configured from the Application Management page of Central Administration:

- Web Application General Settings (per web app)—Time zone, default quota template, person/presence tagging, max upload size (MB), alerts (ON/OFF & max), RSS (ON/OFF), Blog (ON/OFF & credential accept), Web page security validation (ON/OFF & expiration), user credential email notification (ON/OFF), backward-compatible event handlers (ON/OFF), change log expiration, recycle bin (ON/OFF, purge expiration)
- Managed Paths, Outgoing E-mail, & Features (per web app)—Include those Web paths to be managed by WSS, set SMTP and address choices for outbound email, activate Features
- Application Security (per web app)—Web part connections and online Web part gallery (allow/prevent), Self-Service site management (ON/OFF), User Permissions (select which permissions can be set for all sites), Policy (service accounts), Authentication Providers

Additionally, tier-one administrators are called upon to create the first new site collection into a Web application. Creating site collections can be accomplished from the Application Management page of Central Administration or stsadm.exe at the CLI. Creating a new site collection requires defining:

- Web Application—Dictate the Web application that will host the site collection
- Title and Description—Explanatory properties appearing on default page
- Web Site Address—URL for site collection top-level site
- Template—Choose from system-supplied or custom site templates
- Primary Site Collection Administrator (mandatory)—Name a SCA
- Secondary Site Collection Administrator (optional)—Name a second SCA
- Quota Template—Select a predefined quota template limiting site size throughout site collection

Security Requirements

As you can see, creating a Web application in SharePoint generates more than just a SharePoint logical object. Therefore, in order to create a new Web application, your logon account must have the necessary authority in the Windows OS to create new Web sites into IIS and new databases into SQL Server. By default, only members of the local OS group called Administrators can create new IIS Web sites. Similarly, only SQL logins with membership in the dbcreator role have the authority in SQL Server to generate new databases. Therefore, you must make sure that the user account logged onto SharePoint has the following authority to successfully create a new Web application in Central Administration:

- Farm Administrators SharePoint Group Membership—Necessary to enter Central Administration and configure logical architecture of the SharePoint farm
- Windows OS Local Administrators Group Membership—Necessary to create new IIS Web sites
- SQL Server "DBCreator" and "SecurityAdmin" Server Role Membership—Necessary to create and secure new databases

Tip

Pre-generating the IIS Web site and application pool (then choosing "Existing" Web Site and "Use Existing" Application Pool during Web application creation in Central Administration) alleviates the need for OS/IIS privileges via the Windows OS Local Administrators group during Web application creation.

Unlike site collections, each with their own distinctly named administrators, there is no setting in SharePoint that deems a user as "Web application administrator" for a specific Web application. To manage Web applications, the user must be a tier-one administrator with membership in the Farm Administrators SharePoint group, and as such, will have authority over all Web applications in the farm. Extending existing Web applications bears the same elevated authority requirements for IIS and SQL Server as creating new Web applications.

MOSS Shared Services Provider Administration

Tier-two of Microsoft's administration model for SharePoint focuses on an optional suite of services available only to MOSS 2007 licensed installations (not WSSv3-only environments) called the Shared Services Provider. SSP introduces several enterprise-class features to a MOSS environment, so management of the SSP is considered an elevated privilege, though not as critical as actual farm and Web application management performed by tier-one administrators. Mismanagement of the SSP at tier two can interrupt resource location efforts and may negatively affect productivity but does not have the same far-reaching effect as taking down the entire farm or preventing access to a bevy of site collections.

> **Resource**
>
> For more information about managing MOSS SSPs, read the TechNet article http://technet.microsoft.com/en-us/library/cc262003.aspx.

Logical Explanation of SSP

SSP can be implemented to employ enterprise-class features across a large SharePoint farm. Functionalities such as enterprise-wide searching, social networking, audience targeting, and My Sites are provided by SSP, just to name a few. Additionally, an Enterprise Edition license of MOSS includes the Business Data Catalog (BDC) and Excel Calculation Services (ECS) server products, which are also courtesy of SSP. Although all these enterprise-class features are nice, they are not mandatory. You can install and run MOSS without ever creating a single SSP if you wish. However most enterprises that invest in MOSS do so specifically to take advantage of the product's enterprise-class features, so employing an SSP ensures full advantage!

Creating an SSP in MOSS can be accomplished via Central Administration or stsadm.exe by using the *createssp* operation, one SSP at a time. Before sitting down to the keyboard, however, you must plan how many SSPs will be necessary and to which Web applications their services will be provided. The relationship between SSPs and Web applications can be 1:many but not many:1 (see Figure 2.5). Each Web application can only be configured to be associated with one SSP at a time, yet one SSP can be associated with many different Web applications. The choice to implement multiple SSPs in a single SharePoint farm is driven by a need to configure one or more of the SSP services differently per Web application(s). Also, Web application to SSP associations can be modified by clicking the *Create or Configure this farm's shared services* hyperlink in the Office SharePoint Server Shared Services section of the Application Management page in Central Administration.

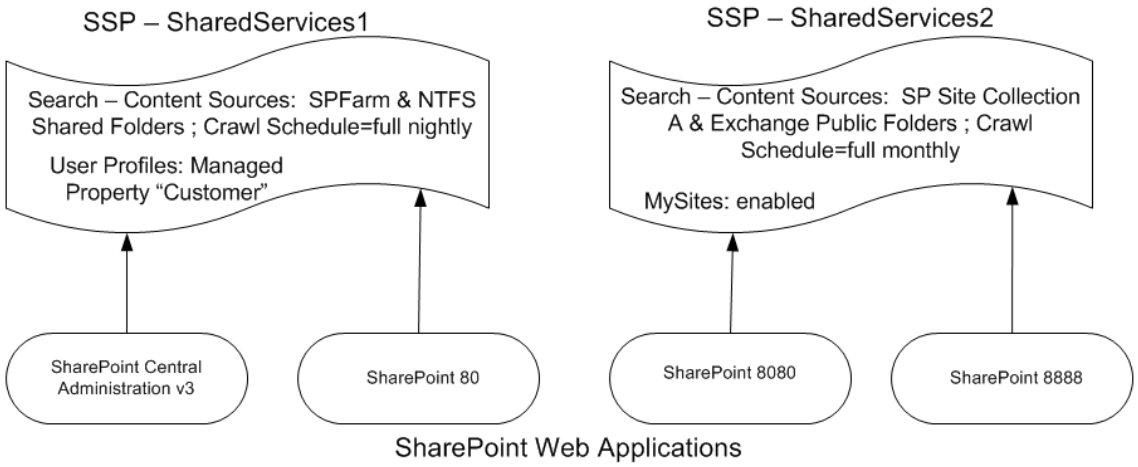

Figure 2.5: Sample logical mapping of multiple SSPs in a single farm containing four Web applications.

Creating an SSP demands Web applications to support both the administration site collection and the optional My Sites site collection. If My Sites will be employed, you must decide whether to host them in the same Web application as the administration site. Microsoft best practice recommends choosing an alternate Web application for My Sites so that they can be managed and backed up separately and to protect the SSP administration site collection from being affected by My Sites corruption should it occur. The SSP Web applications can be existing or created anew during SSP creation. Additional settings required during SSP creation are listed in Table 2.3. Keep in mind that SSP is a suite of Web services, so be generous with hardware resources such as disk storage space on the SQL Server (especially if implementing My Sites) as well as memory and network resources on the WFE servers.

Parameter Name	Purpose	Settings Label
SSP Name	Name SSP and specify Web application for admin site	SSP Name Web Application
My Site Location	Set MySite Web app and URL path	Web Application Location URL
SSP Service Credentials	Set Inter-Server/SSP-scoped timer jobs credential	User Name Password
SSP Database	Provide SQL destination for new/existing-empty SSP database and access credential	Database Server Database Name Database Authentication
Search Database	Provide SQL destination for new/existing-empty SSP Search database and access credential	Database Server Database Name Database Authentication
Index Server	Select crawler for Index builds	Index Server Path for Index file
SSL for Web Services	Dictate security	Use SSL

Table 2.3: SSP creation values.

It is possible to configure a widely scoped SSP intended to be associated with Web applications in multiple SharePoint farms. This practice is called Inter-Farm Shared Services and is described in Microsoft TechNet article cc262179. One advantage of this strategy is that a Web application in Farm "B" (child farm) can benefit from SSP Web services already defined in Farm "A" (parent farm), instead of being associated with one of the SSPs in its own farm. However, to even participate in such a design, a farm must be configured to allow Inter-Farm Shared Services (see Figure 2.6) and in doing so, is named as either a provider (parent) or consumer (child) role but not both. If named a consumer, the child farm can use services only from one named parent Inter-Farm Shared Services provider at a time. But the child farm can also support its own SSPs for its exclusive use. Inter-Farm Shared Services offers a bit of centralized management in that potentially fewer SSPs need to be created and managed, but complex designs should be documented carefully to avoid inappropriate Web services being provided to a Web application and its sites.

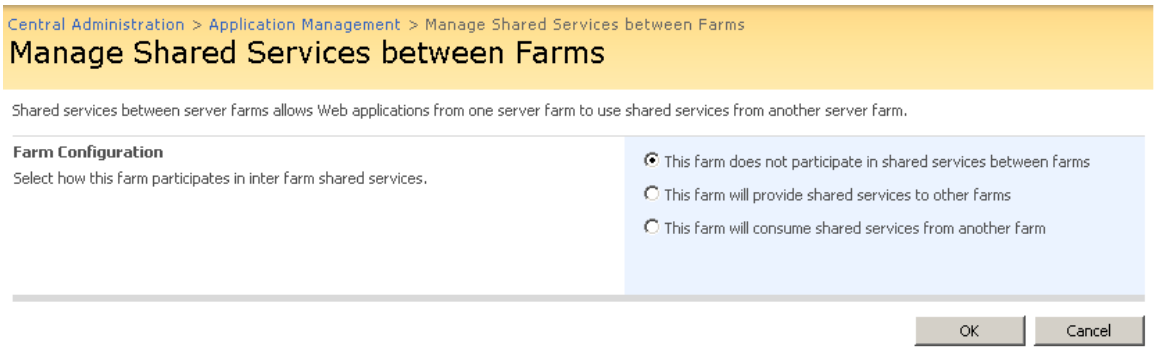

Figure 2.6: Allowing Inter-Farm Shared Services participation for a farm.

SSP Configuration Settings

The authority to create and manage SSPs in a MOSS environment should be granted astutely. Changing the behavior of any Web service in the suite impacts multiple sites throughout every Web application associated with that SSP. The native management utilities in MOSS do not allow for "one-off" SSP configurations for Web applications that require a slightly different behavior from one of the services in the SSP. Therefore, by associating a given Web application to a specific SSP, you are committing all the sites in that Web application to accepting all the services provided by that SSP in the manner by which they are configured. Period.

So exactly what are you signing up a Web application for when you associate it with an SSP? Each SSP has the ability to offer the following Web services to its Web applications:

- User Profiles—Static and/or imported user profiles consisting of system-supplied and custom properties (foundation for social networking); define profile properties, schedule/invoke/log profile imports, define privacy policies for profile information
- My Sites—Personal Web sites for SharePoint users; set search center, hosting site collection, URL location, site naming convention, localization/globalization, and default Reader site SharePoint group membership for all My Sites
- Personalization—Link and security maintenance for SSP and My Sites; publish site and destination links to My Sites and Office Suite apps, grant authority to services in SSP, and specify trusted My Site locations
- Audiences—Dynamically compiled audiences based on defined rules rather than SharePoint Group or directory role/group membership; audience rules and compilation schedule, manual compilation invocation
- Search—Settings and usage reports ; set content sources, crawl rules, logs and schedules, global scopes, content access account for crawling, metadata property mappings and authoritative pages; view system-supplied Search usage reports
- Usage Reporting—Advanced Usage Analysis processing and Search Query logging settings (ON/OFF); advanced usage analysis processing requires that WSS usage logging be enabled for the farm (Central Administration-Operations-Usage Analysis Processing—Logging Settings)

Additionally, if the Enterprise Edition license of MOSS has been purchased and installed, the SSP suite will include ECS and BDC service as well. These two enterprise features introduce line of business (LOB) data integration into SharePoint via database or Web service connections defined in the BDC and trusted Excel spreadsheets made available to ECS. Configuration of these two services takes place in the SSP Administration site GUI or the stsadm.exe CLI utility (see Figure 2.7). The architecture of the MOSS SSP makes centralized administration of multiple SSPs a challenge because the SSP administration site is unique per SSP. The design also prohibits breaking up the services in the suite, requiring a robust third-party administration tool for more granular control of SSP Web services.

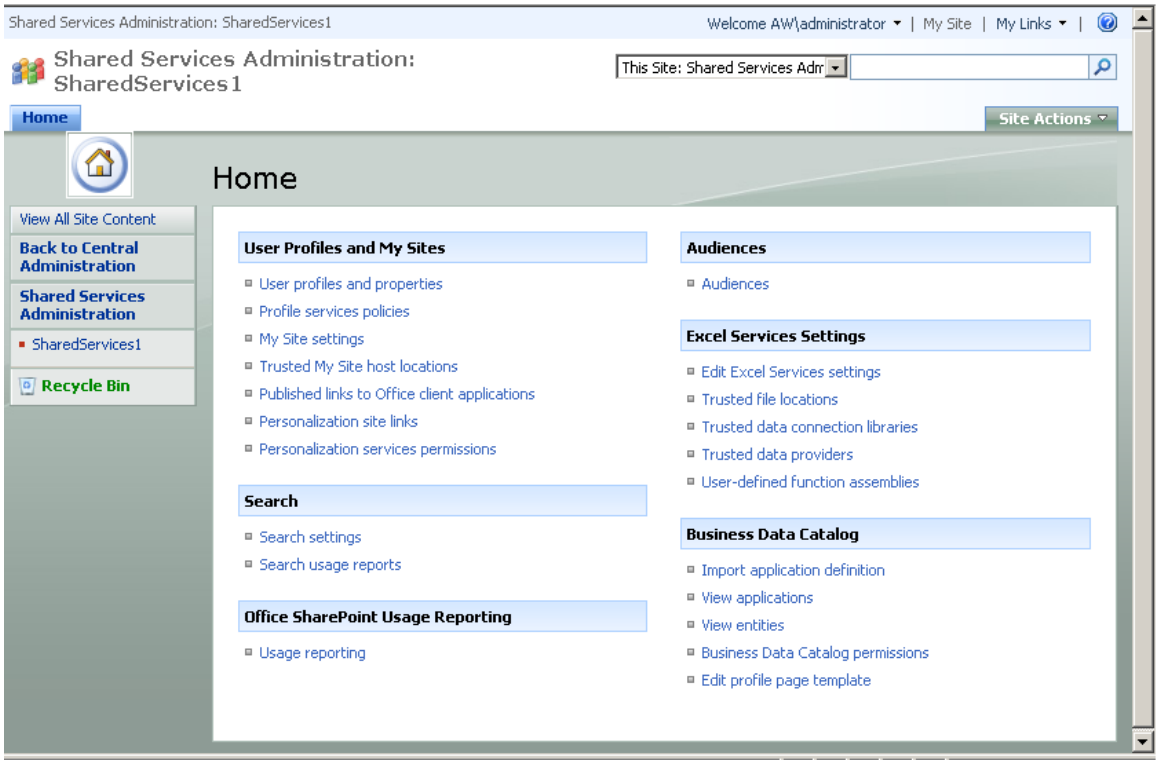

Figure 2.7: Example of SSP Administration site home page in MOSS Enterprise Edition.

Security Requirements

To create a new SSP for a SharePoint farm, the security requirements may be similar to those for Web application creators if new Web applications for the SSP administration site and My Sites will be generated on the fly during SSP creation. If, in a highly segregated IT administration model, Web application management is handled separately, then the Web applications for SSP can be created ahead of time and called as existing choices during SSP creation. In this case, the only security requirement for the creator of the new SSP is that the logon account be a member of the Farm Administrators SharePoint group. Whatever logon account creates the new SSP will gain explicitly-assigned Full Control permissions to the SSP Administration site as well as become the Primary Site Collection Administrator for the administration site collection. Additional tier-two administrators will then need to be granted permissions into the SSP administration site collection by the creator.

By default, the only security principals listed in the default SSP administration site collection's permission structure are:

- {SSP creator's logon} = Full Control
- SharePoint System Account = Limited Access
- Viewers (system-generated SharePoint Group) = View Only (0 members)

It is not necessary or advisable to give general users any permissions to the SSP administration site unless you are naming them as tier-two administrators. Though the Windows NT Authority system group called Authenticated Users is built-in to the SSP administration site collection permissions structure by default as a user (but has no initial permissions assignment), it is rare that this all-inclusive system group would require privileges to read SSP configuration settings let alone manage them. The default Viewers SharePoint group can be populated with Help desk or assistance personnel so that they may read SSP settings to detail issues being escalated to the tier-two administrator.

User rights to utilize the SSP services are instead managed through Shared Services rights and policies. Profile services policies define which profile properties and My Site information is available to whom and whether the user himself can override the security setting (see Figure 2.8) and can be set by clicking the *Profile services policies* link in the User Profiles and My Sites section of the SSP administration home page.

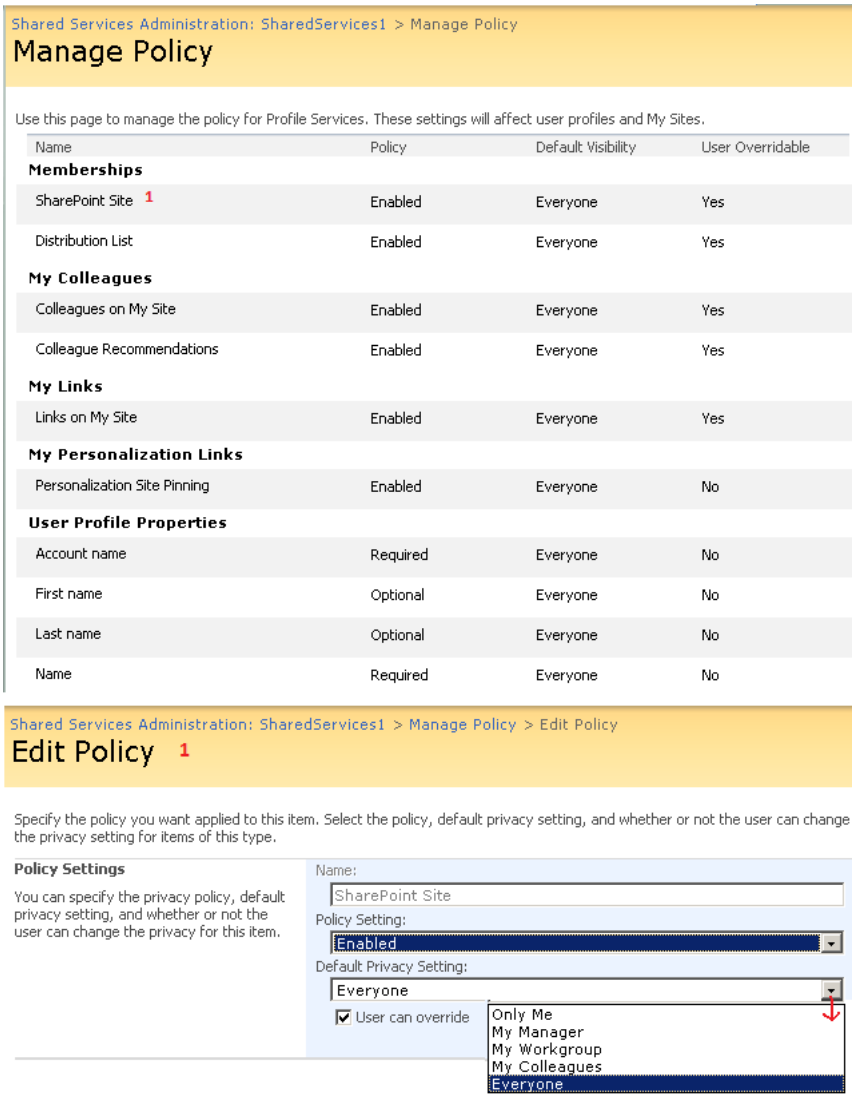

Figure 2.8: SSP profile services policies example.

Similarly, Figure 2.9 displays the default rights assigned in a new SSP garnered by clicking the *Personalization services permissions* link in the same section.

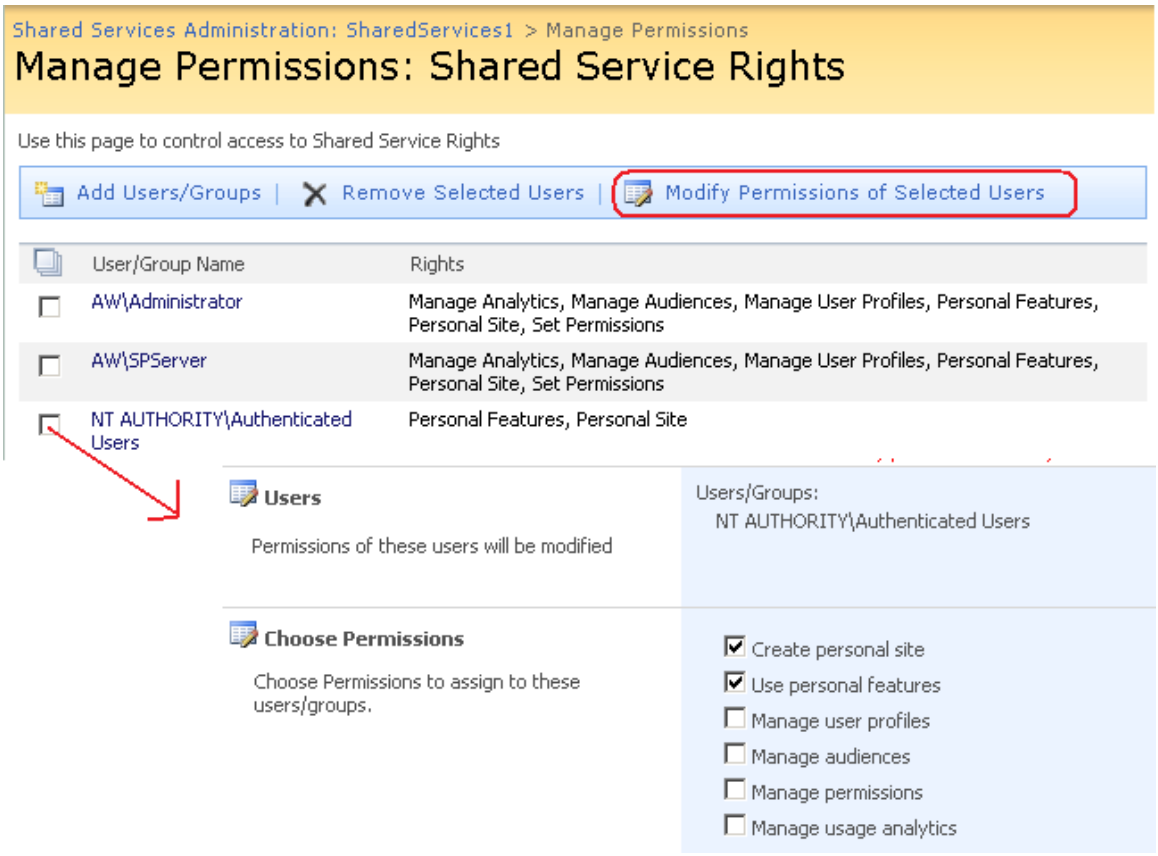

Figure 2.9: Shared Service personalization services permissions.

Site Collection Administration

Farm and Shared Services administration, the top two tiers of Microsoft's administration model for SharePoint, can affect multiple sites and demand the skill set usually found in IT personnel. However, SharePoint, as a collaboration platform uniquely equipped for community computing, is primed for empowering business information workers to manage and utilize their own data. As such, individual site maintenance and even some site collection configuration can be delegated to non-IT users in a large environment to share the administration workload and better respond to immediate content needs. Tier three of Microsoft's SharePoint Administration Model relates to these Site Collection Administrators and Site Administrators.

For now, let's focus on the Site Collection Administrators (SCAs) of tier three. The privilege to manage an entire site collection hierarchy of sites can be granted either during site collection creation or afterward. Responsibilities include enabling site collection scoped features, managing site collection level search options, perusing site collection level logs/reports, and more. The site collection administrators also have the ability to salvage content erroneously deleted by other users.

Logical Explanation of Site Collection

A site collection is a hierarchical anthology of individual SharePoint sites. Beginning at the top with a "top level site," a subsequent site created beneath the single top-level site of the site collection is referred to as a child site. The top-level site becomes a parent to one or more of these first-tier children sites who each, in turn, may be configured as parents themselves by creating subsequent children sites beneath them (see Figure 2.10). Several of these hierarchies can be hosted by a single Web application, but the first site collection created into the Web application has a special role. The top-level site of the first site collection built-in to a Web application is also that Web application's root site. It holds the Web application up, so to speak, at least as far as user access is concerned.

Caution

Microsoft best practice discourages deleting the root site of a Web application. Truncating it after relocating its content elsewhere is fine, but deleting the site itself can cause undesired behavior by the Web application due to special files residing in the root directory. For more information, visit msdn.microsoft.com.

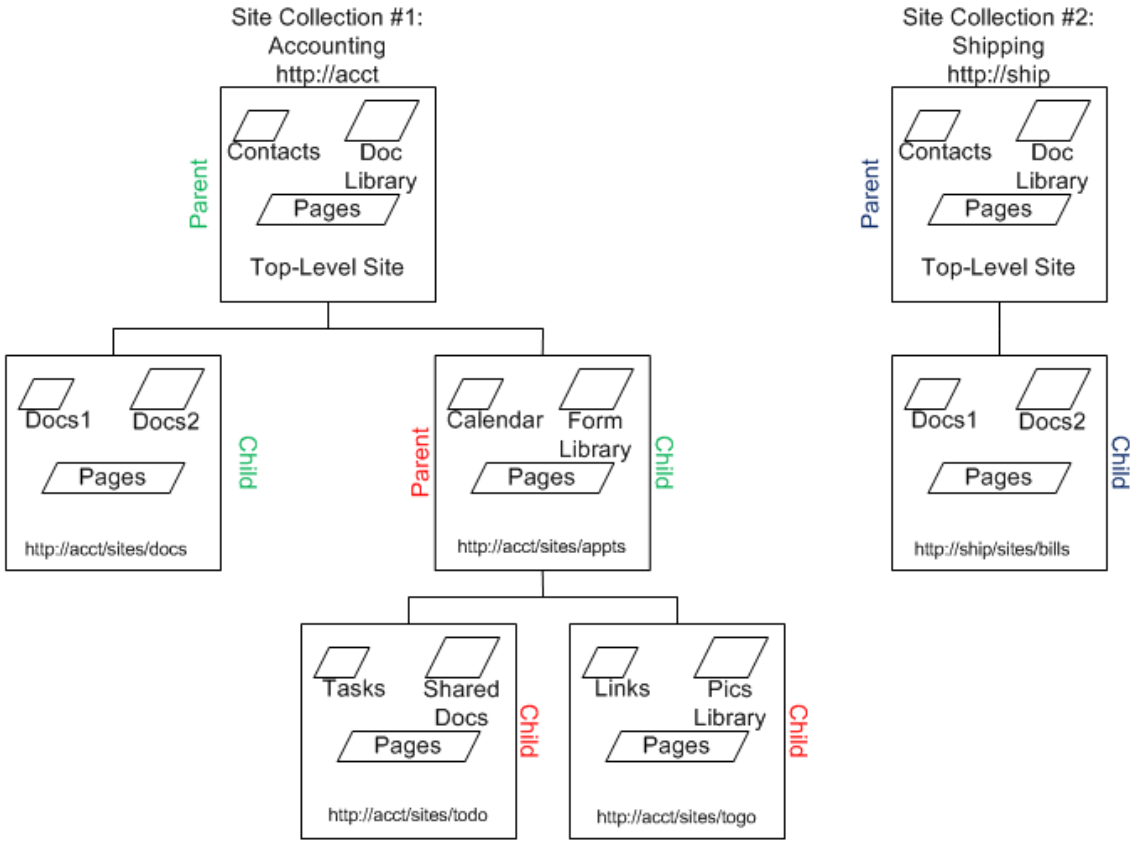

Figure 2.10: Example site collections.

Recall from earlier in this chapter that creation of the first site collection into a Web application is performed by a tier-one administrator and includes the naming of at least one Site Collection Administrator for the new site collection. Additional tier-three administrators can also be named during site collection creation (up to two total in Central Administration). Yet more SCAs can be named in Site Settings from the top-level site in the site collection, but don't go overboard. Too many SCAs can result in administration conflicts.

Thereafter, tier-three site administrators may be granted self-service site creation capabilities by the tier-one administrator (more on configuring self-service in just a bit). Once self-service has been enabled for a Web application, tier-three administrators may generate additional new hierarchies of sites that they own and manage from the top down. Tier-three site collection administrators' decisions can affect users of multiple sites, so delegate selectively.

Site Collection Configuration Settings

When a tier-one administrator enables self-service site management for a Web application via either Central Administration or the *enablessc* operation in stsadm.exe, a new item is automatically generated into the Announcements list of the Web application's root site (the top-level site of the first site collection built-in to the Web application). This announcement message contains a hyperlink to the scsignup.aspx page of the _layouts directory in the SharePoint 12 hive (see Figure 2.9). This is a different page than the Create Site Collection page accessed from Central Administration (createsite.aspx from _admin directory). Namely, the tier-three administrator engaging in self-service site creation cannot specify the host Web application for his new site collection, name SCAs, or specify a quota template.

> **Resource**
>
> To receive the auto-generated announcement, the root site of the Web application must contain an announcement-templated list entitled "Announcements." Otherwise, a custom link can be created to http://{web app URL}/_layouts/scsignup.aspx. For more information about self-service site management, see Microsoft TechNet article at http://technet.microsoft.com/en-us/library/cc287884.aspx.

Site collection administration includes configuring site collection access and behavior as well as managing galleries whose items are available site-collection wide. Three prominent columns of site settings links used by SCAs are Users and Permissions, Site Collection Administration, and Galleries (see Figure 2.11). Though galleries are site centric, the contents of a parent site's galleries are also available to its children sites. Thus, creating a new site column or content type in the top-level site of a site collection makes it possible to employ the new site column or content type at any list or library in any site throughout the collection. Defining the site gallery location of a new gallery item determines its breadth or scope of use and should be the responsibility of a tier-three administrator.

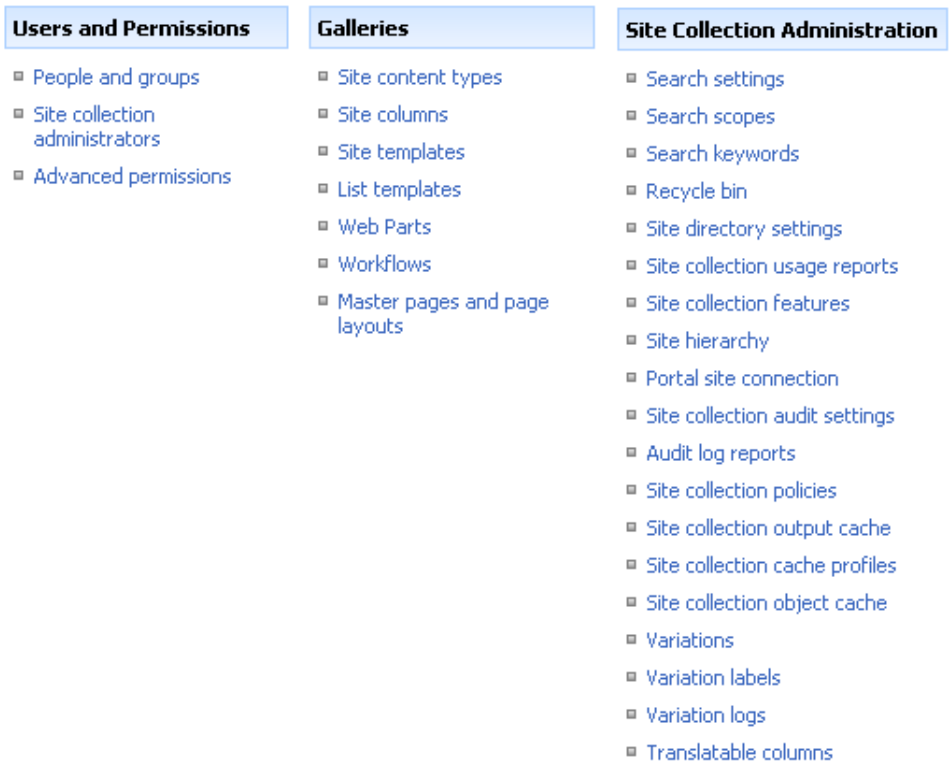

Figure 2.11: Site Collection Administrator links from Site Settings in a MOSS environment.

A common obstacle for tier-three administrators is central administration of multiple site collections. The native SharePoint tools focus on one site collection at a time. Making similar changes to multiple site collections requires repetitive administration or programmatic scripting. Luckily, there are third-party utilities on the market that offer more streamlined interfaces for multi-site-collection management.

Security Requirements

Unlike Web application or SSP creation, site collection creation does not require elevated privilege in the OS to create IIS objects or SQL Server to generate new databases. Recall that only Farm Administrators have access to Central Administration by default, so creating new site collections in this utility does require elevated SharePoint privilege. However, creation of new site collections by tier-three administrators via self-service does not require Farm Administrators membership. The site collection, its definition, and its content are all contained within the content database of the Web application hosting the site collection. A site collection can be created into a new content database for the Web application via stsadm.exe, but that distinct practice is reserved for tier-one Farm Administrators.

The user logon that creates the site collection automatically is made a member of the top-level site's Owners SharePoint group and thus has full control of the site collection. Moving forward, they can begin adding other users to the top-level site and granting permissions explicitly or through SharePoint group membership. Primarily, site collection administration of existing collections is performed via the browser GUI, except for disaster recovery, which can be implemented via stsadm.exe or Central Administration (although these tools are not commonly disseminated to tier-three administrators due to the elevated authority requirements in the OS and SharePoint).

One of the most crucial responsibilities of a tier-three site collection administrator is permissions management for content access. Because the default behavior of new sites created into the site collection will be to "Use same permissions as parent site" (inheritance), permissions assigned by a tier-three site collection administrator at the top-level site will, by default, cascade throughout the collection.

Site Administration via Delegation

The granular administration architecture of SharePoint extends to the individual site level with tier-three Site Administrators. By granting control over a single site within a site collection, responsibility for a sub-section of content can be delegated to a business information worker who best understands the content and has keen ideas regarding data taxonomy, access, and maintenance. To name a SharePoint user as a Site Administrator, a site collection administrator need only grant the user Full Control of the site either explicitly or by membership in the site's Owners SharePoint group. Tier-three site administrators have dominion over the site's permission structure (and therefore the permission assignments for inheriting child sites), the site's sub-hierarchy (child site creation and management), page design, site features, and content. Site administrators can even delete the entire site or any of its children sites.

Logical Explanation of Sites

Unlike traditional Web sites, SharePoint sites are not individual entities in IIS. Instead, a SharePoint site's very existence is courtesy of table rows constructed in the content database associated with its hosting SharePoint Web application. Although modifying the web.config file of a SharePoint Web application's associated IIS Web site may be necessary to provide custom programmatic controls on a specific SharePoint site's pages, this is more of a tier-one concept than a tier-three discussion and well beyond the scope of this guide. SharePoint sites are logical entities that are managed solely within the confines of SharePoint itself.

Creating a new site into a site collection begins by choosing its parent site. The site from which a new site is generated determines the new site's placement in the site collection hierarchy and thus its inherited permissions, features, and presentation. Positioning a new sub-site to take the best advantage of parental hierarchy all the way up to the top-level site of the site collection assures appropriate content delivery while efficiently utilizing content database space in SQL Server by reducing the need to duplicate content data. Each new site can be configured with unique regionalization and RSS settings, search visibility, anonymous user cache output settings, and more.

Site Configuration Settings

Tier-three administrators will likely perform most of their management duties in either the browser GUI or SharePoint Designer 2007. As previously mentioned for tier-three site collection administrators, site administrators will likely not be granted the OS authority to run stsadm.exe or the SharePoint authority to enter Central Administration. The primary Site Settings categories of administration links that will be utilized by tier-three site administrators include Users and Permissions (if site uses unique permissions), Look and Feel, Galleries, and Site Administration (see Figure 2.12). In fact, as the browser interface is security trimmed (that is, users only see links to locations or tools they have permission to visit or utilize), site administrators of a specific site who are not also site collection administrators of the site collection will not even see the Site Collection Administration column from Figure 2.11.

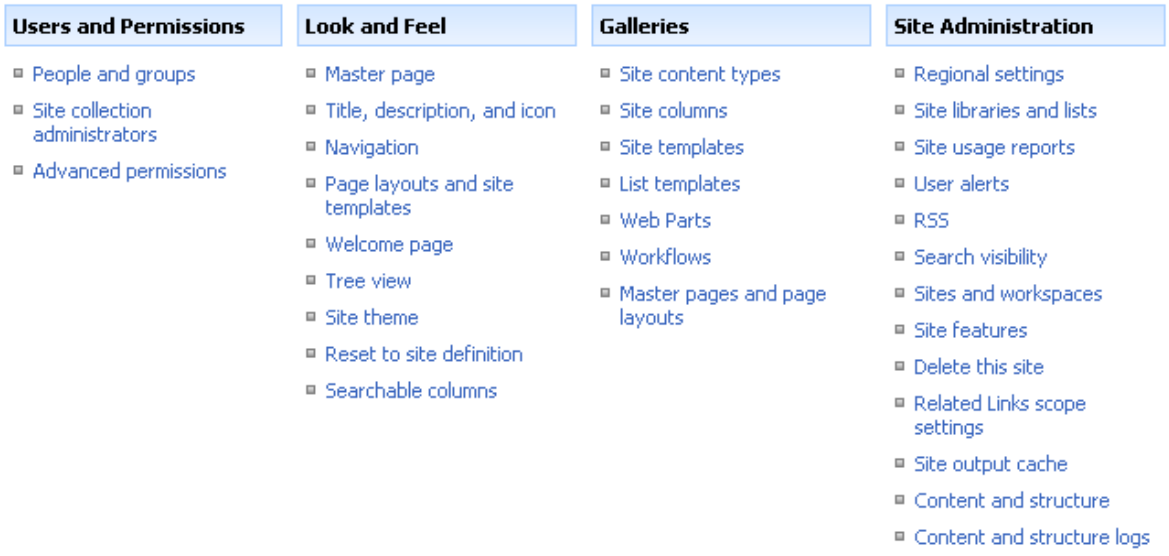

Figure 2.12: Site Administration links from Site Settings in a MOSS environment.

In many large SharePoint implementations, tier-three site administrators are tasked with customizing, or "branding," their sites to provide a look and navigation pattern specific to their site's content. Although these site administrators may not be held responsible for actually creating custom master pages or cascading style sheets, they are often held accountable for applying such tools to their sites in an effort to enforce consistency or instill marketability to the SharePoint farm. Like site collection administrators, one of the greatest challenges faced by site administrators is the site by site-centric interface of the native SharePoint administration tools. When the same change needs to be applied to multiple sites, there is no central tool in SharePoint, resulting in repetitive administrative steps or the need for a third-party solution.

Security Requirements

Any SharePoint user who has been granted the *Create Subsites* permission on one of the sites in the site collection (such as found in the Manage Hierarchy permission level) has the ability to create new sub-sites into the collection. The user logon that creates the new site will gain only Owner SharePoint group membership for the new site if they opt to *Use unique permissions* during creation. Otherwise, the creator's permission to the new child site is dictated by the parent site's security structure.

To give out full control to an existing site, a user who currently holds the *Manage Permissions* permission on the site must grant the new administrator the *Manage Web Site* permission (as found in the Full Control permission level). Ah, but here is where things get tricky. If the site uses unique permissions, adding members into the site's unique Owners group, which is assigned the Full Control permission level, isn't too difficult. But if the site is inheriting its permissions from its parent site and administration is being performed in a browser GUI focused on the site needing a new administrator, changes in SharePoint group memberships must take place at the parent site or inheritance must be disabled. Remember, inherited permissions result in changes made at the parent site affecting both that parent and its children sites! There is no way in Site Settings to define scope for a new permission assignment such as "not this parent but child sites only." Thankfully, there are third-party tools that can accomplish this without requiring dissolution of inheritance entirely.

Summary

In this chapter, we discussed the different responsibilities associated with each tier of Microsoft's SharePoint Administration Model. We discussed global settings that affect Web applications their site collections. We then examined the MOSS SSP and its management. Lastly, this chapter divided tier three of Microsoft's SharePoint Administration Model into site collection versus individual site administration.

In the remaining chapters, this guide will explore the concept of single-instance storage in a multi-location SharePoint farm and the art of managing multiple sites in various locales. It will also divulge archiving and reporting best practices for SharePoint, and the limitations of native tools for accomplishing them. So stay tuned!

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.