Global Knowledge™

Expert Reference Series of White Papers

SharePoint: How It's Leveraged and How It Works

SharePoint: How It's Leveraged and How It Works

Gail Pomper, Server+, MCSE, MCT, CTT, CNI, CNE

Introduction

SharePoint is Microsoft's document management technology, and has been in use under various product names for more than five years. Despite its longevity, many computer users are unaware of its existence and fewer still understand how the technology simplifies the network environment for end-users.

But every organization that generates content can benefit from using SharePoint. Some smaller organizations will require only WSS 3.0, but most organizations will get maximum benefit by implementing MOSS 2007. Some examples of how existing organizations are using SharePoint include:

Technical installation instruction databases – these implementations use Infopath forms to create documents that provide instructions on how to install all corporate software and how to configure supported hardware devices such as handheld PCs.

Information sharing amongst R&D think tanks – SharePoint fosters research and development efforts in the science and technology industry by enabling organizations to open extranet and Internet portals where scientists and researchers can coordinate their efforts and exchange information.

Project management for dispersed teams – Project managers working with remote workers can manage a project in Project Server 2006 by first clicking on a SharePoint task list. Projects can then be easily organized by site and users accessing the sites see only the data to which they have been granted SharePoint access.

Portals for school systems – For students attending in school districts that use MOSS 2007, each school has its own web application with separate site collections for students, teachers and administrative staff. Students access an Internet portal that links them with their classroom website and their own mysite.

So how do different users leverage SharePoint, and how exactly does it work? This white paper will first examine how users', managers', and network administrators' view and utilize SharePoint. It will then explore how SharePoint works for both SharePoint users and architects. Finally, this paper will list and explain six typical tasks SharePoint architects are responsible for.

What Is SharePoint?

SharePoint's use can mean different things to different users. This section will briefly cover how user's and manager's view SharePoint and then give a more in-depth look from the network administrator's view.

The User's View

In the world of computers, a product can look very different, depending on your viewpoint. For example, a SharePoint user sees the environment as an application that puts everything at their fingertips. The user opens a web browser and suddenly has access to an Access spreadsheet, a Word document, an email message, an updated task list, or data from a custom Peoplesoft application that accesses an Oracle database.

But to the user, SharePoint is more than just a document management system; it's a user environment, a file system manager, a database abstractor, a task manager, and a relational database. In short, it is a multi-faceted application whose primary task is to make data access transparent to the user.

The Manager's View

A manager might have a department of 18 employees, five projects in various stages, and a requirement to maintain the security of the information his or her workers create. SharePoint can help with all these tasks and more.

SharePoint gives choices for managing a project. The most sophisticated of these is Project Server, which uses SharePoint to access the project data stored in an SQL Server database. A less sophisticated, but still manageable, solution is to use Microsoft Project and simply assign tasks to users through SharePoint. Some of the reporting and "what if" capabilities are lost, but everything stays in the same SharePoint database. With Project Server, a separate database is used for just the project data. The task element is handled through Outlook. When using Outlook 2007, the task can be updated in Outlook and posted to SharePoint or vice versa.

SharePoint provides managers with a "security-focused" view. This means the users only see the items they have access to view. If a user does not have read-access to an item, it is not displayed in the view of the library. If a user does not have access to the library, that entire library is not displayed in any view. This keeps security simple and the user views manageable.

The Network Administrator's View

So far, we have not talked about the implications of running SharePoint in a network environment. SharePoint certainly depends on a reliable network to deliver all the services we have discussed. But given reliable network services are taken for granted in most companies, SharePoint can considerably reduce the time required to manage the file system.

In many organizations, documents are stored on a file server, in a hierarchical view, organized by project or department, and managed by network administrators. This means that the file system is secured by network administrators, backup and recovery is the purview of the data center, and access control is achieved through some change-control process—also typically handled by network administrators. SharePoint eliminates all the data management, control, and security allocation issues.

The Role of the Network Administrator

Network administrators (or the data center) are responsible for backing up the SQL database and, since most SharePoint information is stored in the SQL database, this ensures recoverability in case of a data failure. In fact, all SharePoint tasks that need to be handled by network administrators are centralized in a separate database called the Central Administration database. Administrators performing these tasks are referred to as **Farm Administrators** and, by default, have no access to the data stored in the SharePoint database.

The Role of the Site Collection Administrator

When a top-level site is created, a **Site Collection Administrator** is assigned (a **Secondary Administrator** can also be assigned) and all security for the contents of the SharePoint site resides with the **Site Collection Administrators**. Often, the site collection administrator is the department manager, so if security rights for an item or SharePoint library need to be changed, the new security assignment can be made immediately without going through a lengthy change-control process.

Security Management

The kind of security management just described is based on the idea that data creators are the most knowledgeable about the security requirements of the data. If you are managing a team of chemists, the security of the new formulations is going to be of the utmost importance. The library where those formulations are stored is going to be restricted to the few individuals who need access. In a normal administrative environment, network administrators can take ownership of most file shares, giving rise to the possibility of a security leak.

This arrangement actually has several beneficial side affects. First, in a properly designed SharePoint site, user documents get created from within SharePoint and are automatically saved to the database. This prevents data loss by keeping files on a network server and away from users' PC hard drives. Second, security can be assigned at the time the document library is created. When the library is created, a default content type can be assigned, and the appropriate groups are assigned "contribute" and "read" access.

Given that most data centers have automated backup and recovery systems, SharePoint eliminates the burden of managing file system data from the network administrators, leaving them time to focus on other more important server management tasks.

How Does SharePoint Work?

SharePoint requires a number of backend services in order to manage file content, including, network services, security services, database structure, and web services infrastructure. Network Services and some elements of Security Services have already been covered, so I will now focus on the database structure and the web services infrastructure.

How exactly does SharePoint work? Again – there is the need to look at this product from different points of view. In this case, we will look at the perspectives of the user and the SharePoint architect.

How SharePoint Works for Users

SharePoint simplifies the user environment by requiring the user to open only one application, the web browser. Top-level support is provided for Internet Explorer and Netscape Navigator. Second-level support is provided for Safari, Firefox, and Mozilla. If you are not using either IE or Netscape, this simply means that some library items will display differently, depending on the fonts and design elements used in the site. The SharePoint designer needs to test every site element meticulously to ensure a reasonable level of user acceptance.

When a user creates a "new" item, either a default application opens automatically or a list box appears where the user can choose the content type that is linked to the correct application. An example of this would be an Infopath forms library that has a number of pre-defined forms available. After an Infopath form is designed, it can be published to SharePoint either as a **library item** from a library in a specific site or a **content type**. When published as a content type, the form can be deployed to more than one site. When a user

creates a 'new" item in the form library, a drop-down list of the form types displays and the user chooses the correct form to fill out.

Another way to manage different content types is to create a separate library for each content type. This way, a library contains only one type of data. In this case, a default content type will automatically call the correct application that is assigned at library creation time. This is not limited to just forms. A content type can be any specific document format that (1) the site users have a need to recreate, and (2) can be associated with a specific application at document creation time.

For example, if you have a document library that is used to store faxes, a fax cover sheet might be the default content type specified for that library, and the library would open Microsoft Word with a blank fax cover sheet.

Again – this saves time for users because opening an application is not a separate step. When an existing document is opened, either the application was used to create the document is opened, or, if the user does not have the application installed on the PC that holds their current session, it opens in a browser view.

How SharePoint Works for the SharePoint Architect

The SharePoint architect establishes the SharePoint environment, providing a reliable and secure infrastructure for content that can originate from many different departments and organizations throughout a business enterprise.

Things become a little more complicated in this realm. First, SharePoint is a network application, so any problems in the network will be accentuated when you bring SharePoint on-line. This means that DNS, DHCP, and Active Directory need to be working flawlessly before you deploy your SharePoint implementation. If these systems are all functioning, the next step is to decide whether this will be a single server or multi-server installation. Regardless of which installation type you choose, there are two primary types of server services that must be implemented.

The first is an **SQL Server database**. SQL Server is the storage backend for SharePoint, which requires a number of databases to store specific content. Table 1 defines the databases created to support a typical SharePoint implementation.

Database Name	Purpose
Point_Config	Point configuration database
Content	database
Service_Search	configuration database
Services1_DB	service provider configuration database
ServicesContent	service provider content database
PointAdminContent	administration content database
Search_PortalName	content database

Table 1. Databases created to support a typical SharePoint implementation.

The second is the web service provided by IIS. **IIS with ASP.NET** services enabled must be installed on the SharePoint server prior to initiating the installation process. In addition, Microsoft's .NET Framework versions 2 and 3 are required, and the installation process will terminate if these services are not installed. The steps to install SharePoint can be found at several well-documented sources. One such source is:

http://mindsharpblogs.com/bill/archive/2006/06/27/1153.aspx

Although some organizations can get by with just the features provided by Windows SharePoint Services (WSS) 3.0 (a free download from Microsoft), most will want the complete set of capabilities provided by Microsoft Office SharePoint Server (MOSS) 2007. MOSS comes in two versions: Standard and Enterprise. The Enterprise version provides capabilities like the Enterprise Publishing Infrastructure.

The following Microsoft URL hosts two spreadsheets, one in Excel 2007 format, the other in Excel 2003 format, that compare the features provided by each SharePoint version:

http://office.microsoft.com/en-us/sharepointserver/HA101978031033.aspx?pid=CL100626951033

The SharePoint Architect's Tasks

A SharePoint architect typically is responsible for the following six tasks:

1. Active Directory Security Planning
2. SSL Security Planning
3. Administration of Shared Service providers
4. Enabling Farm and Web Application Features
5. Creation of Site Collections
6. Documentation of the SharePoint Configuration

1. Active Directory Security Planning

Most SharePoint users already log into the network that will support SharePoint with an Active Directory user ID and password. Each site collection created in SharePoint establishes content access security for the top-level site. When new sites are created, this security can be inherited or the site creator/administrator can decide to create a unique set of security privileges for the content in the sub-site. The easiest way to apply security in an enterprise environment is to use new or existing Active Directory global groups.

SharePoint is similar to every other Microsoft application you have ever installed. The installation, or in this case, site creation process, will automatically create default local groups. The SharePoint architect needs to ensure that Active Directory contains appropriate global groups so that SharePoint site creators/ administrators can add the correct AD groups to the SharePoint local groups associated with a sub site to secure content and make it available to the correct audience. Here's an example of how this works:

When you create a site collection called ABC Realty, a top-level site of the same name is created. If this is the first site to be created in SharePoint, it will typically be associated with an IIS web application (web site) called SharePoint – 80. If not, you can create a new web application to service this site collection. In both the standard edition of MOSS 2007 and WSS 3.0, three new SharePoint groups will be created with default permissions to secure the content planned for this site:

- ABC Realty Owners – Full Control permissions
- ABC Realty Members – Contribute permissions
- ABC Realty Visitors – Read permissions

AD global groups can be assigned to each of these SharePoint groups to enable content access and control. Your other option is to add AD users individually, but this makes site security management more time consuming.

Suppose you then add a subsite underneath ABC Realty called PasadenaBranch for the Pasadena office of ABC Realty. During site creation, you are prompted to inherit permissions from parent or create unique permissions. If you choose to create unique permissions, the parent level site permissions are copied to the sub-site, inheritance is turned off and you are presented with an option that allows you to create three new groups:

- PasadenaBranch Owners – Full Control permissions
- PasadenaBranch Members – Contribute permissions
- PasadenaBranch Visitors – Read permissions

Again, the site creator/administrator should assign AD global groups to the SharePoint local groups to establish content security for the sub-site content. In an earlier section we discussed the ability of the site administrator to assign security to a specific document library or item within the library. Although security can be assigned in this very detailed way, it leads to a complex security scheme that can make it difficult to troubleshoot rights and permissions. It is easiest to assign content security at the site level rather than at the library or item level.

If you are using the Enterprise version of MOSS 2007, the initial site collection and top-level site will actually contain a set of security groups similar to the following:

- Owners – Full Control permissions
- Visitors – Read permissions
- Designers
- Approvers
- Style Resource Readers
- Hierarchy Managers
- Quick Deploy Users
- Restricted Readers
- Viewers

When you create a sub-site in the Enterprise edition, you are still prompted to inherit permissions of the parent site or to create unique permissions. Regardless of how many groups SharePoint creates for that top-level site, if you choose to assign unique permissions, you will only be prompted to create the three groups (Members, Owners, Visitors) defined above.

The SharePoint local groups are used to ensure that content access is controlled. Once a file has been opened by a user however, it will be exposed to the network where it is possible for the file content to be seen by unauthorized users that have access to network monitoring tools. To protect against this threat, the SharePoint architect should plan for methods to secure the data while en route from the SharePoint server to the user's PC.

2. SSL Security Planning

When you create a site in SharePoint, the site can be exposed as either an intranet, extranet or Internet portal. Each of these portal types has a risk profile that increase as the content audience is enlarged. The intranet has the lowest risk profile since the exposure is limited to personnel inside the enterprise. However, all content that is exposed on traditional wiring schemes is at risk for compromise. To reduce this risk, implementing an SSL security scheme can protect data. SSL use client-server certificates to encrypt data as it traverses the network. The broader the audience the content will reach, the more important it becomes to encrypt that data during transmission. It is relatively simple to secure SharePoint content in this way because the certificate is applied at the level of the SharePoint web application. In IIS, each SharePoint web application is equivalent to a website. The certificate is applied to the IIS web site in the Directory Security tab and all content that is accessed through the corresponding SharePoint web application is automatically subject to data encryption.

The SharePoint architect should ensure that the architecture of the SharePoint hierarchy supports SSL whenever data will be accessed outside the boundaries of the enterprise and also for certain data that is generated inside the enterprise that has a high degree of risk for exposure – for example – financial data, HR content and the SharePoint Central Administration web site.

3. Administration of Shared Service Providers

The Shared Service Provider (SSP) in MOSS 2007 allows network and business connection functionality to be configured once and shared throughout the farm by site collections created in all farm web applications. Typically there will be only one SSP required and all enterprise services including the Business Data Catalog (BDC), Excel Calculation Services and the Search service are also managed by this SSP. Additional SSPs can be created, for example, if you want to crawl content and only make it accessible to a specific group of users, but only one SSP can be associated with a content database at a time so you would have to have additional content databases to support this configuration.

The Search service has dozens of configuration options and these are all configured through the SSP. The items which must be configured are as follows:

- Index Server
- Query Server
- Content sources
- Crawl Schedules
- Crawl Rules
- Scopes
- Authoritative pages and order of relevance
- File types to be crawled
- Metadata to be crawled

Once the configuration of search properties is complete, the scopes need to be activated to the appropriate site collections so the items crawled are available for users to search.

The SSP also holds the application definition files that create the entries in the BDC. The catalog contains a list of business applications that are accessible via items in a SharePoint list. This might be a view into an employee database generated in PeopleSoft, a view into an SAP database, or a table from a SQL Server database. The application definition files, which are created by an application developer, are .XML files that define how the data is accessible to SharePoint including authentication and connection information.

Excel Calculation services is configured by first identifying a "Trusted Location", a server location that hosts spreadsheets accessible to SharePoint. This allows SharePoint to expose links to Excel workbooks and named objects that exist within those workbooks to display a chart, graph or table with data that is always current.

The SSP allows services to be configured once and used throughout the farm. All Front End SharePoint servers in the farm will be able to make use of these service settings. In order for users to access services such as Excel Calculation Services and Enterprise Search, the appropriate feature set must be enabled at the farm, web application, site collection and site level.

4. Enabling Farm and Web Application Features

Your SharePoint architect will also need to determine the feature set within SharePoint that will be used in your implementation. Features need to be turned on at 4 levels in SharePoint to be accessible from a site – Farm, web application, site collection and site. Features enabled at the Farm, web application and site collection level do not have to be enabled at the site level. Features can be enabled on a site-by-site basis.

To configure farm features, open the Central Administration web site and select the Operations tab. Configuration of web application features is performed from the Applications Management tab in Central Administration. Site collection administrators and site owners will configure site collection and site features respectively. This is because farm administrators, and typically SharePoint site architects do not have access to SharePoint content. We will mention how to enable these features only because the features must be enabled for the functionality to be available at the site level where users are accessing content.

5. Create of Site Collections and Configuration of Site Collection Features

By default site collections are created by farm administrators even though farm administrators have no access to the Sharepoint content within those site collections. At creation time, the farm administrator will assign a site collection administrator from among the pool of users in Active Directory. This user will be responsible for all the content within the sites that are created in that site collection.

Site collection features are configured from the Site Actions drop-down menu in the top-level site. Under the column labeled Site Collection Administration, choose Site Collection Features. If you have deployed custom solutions in this site collection, the solution will appear in this list along with the default Microsoft features. Click the Activate button to enable each feature.

Site features are enabled by clicking on the Site Actions drop down menu and selecting Site Settings in each individual site. The option to configure site features is in the Site Administration column. This option might be used to enable a custom Help Desk web part that has been deployed in a site designed for IT personnel. Site features expand the functionality of SharePoint in an individual site.

6. Documentation of the SharePoint Configuration

It is the responsibility of the SharePoint architect to document the configuration of the SharePoint implementation. This can be accomplished by using the pre-built worksheets provided by Microsoft on the Sharepoint site. Not all worksheets are relevant to every Sharepoint implementation, however, they provide guidance to ensure that all configuration elements are considered for most implementations.

Summary

Windows Sharepoint Services 3.0 and Microsoft Office Sharepoint Server 2007 provide an impressive array of document management, collaboration, and business management tools to organize and streamline your business processes. In future white papers, we will look at how to implement some specific features of Sharepoint like on-line presence information, business dashboards and records management to meet on-going business requirements and meet government regulations.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:
Implementing Windows Sharepoint Services 3.0 and Microsoft Office Sharepoint Server 2007
Microsoft Office SharePoint Designer 2007

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Gale Pomper has over 25 years of experience installing and designing computer networks. She holds numerous certifications from Microsoft, Novell, and CompTIA, including Server+, MCT, MCSE, MCTS for Sharepoint, and MCTS for Exchange 2007. She is the principal author for an exam guide for Windows 2000 Active Directory published in December 2001, and a contributing author for Windows XP Power Pack published in March 2003. For the past 15 years, she has been an independent consultant providing network design services, customized training, and Sharepoint implementation services. She is also an instructor for Global Knowledge.