

Step by Step SharePoint Disaster Recovery

Randy Williams

(Reprinted From Windows IT Pro Magazine)

It's Sunday night, and you just got an urgent call from the office: Your Microsoft SharePoint server is down. After some investigation, you find that the disk array in your only front-end web server is dead. You groan, wishing that you'd implemented a complete farm backup from within SharePoint. However, all is not lost. You know that SharePoint stores all its content in a separate SQL Server machine, and that server is fine. You spring into action, trying to get the environment back up before Monday morning. You ask yourself, What steps do I take? What settings will I lose? Will I get any sleep tonight?

This article will answer these questions and more. The recovery I discuss is based on the two-server farm I've mentioned, but the principles also apply to larger farms. The first (crashed) server is running all your SharePoint services (or roles), and the second server is a dedicated SQL Server system. For the purposes of this article, I'm assuming that you're running Microsoft Office SharePoint Server (MOSS) 2007, but most will also apply to Windows SharePoint Services (WSS). I also assume you're using Windows authentication and Active Directory (AD). Of course, your environment is likely to vary in some way, so these steps won't be applicable to all situations. Toward the end of the article, I'll also provide you with some recovery recommendations that you can use today to better protect your SharePoint investment.

Recovery Overview

SharePoint stores all content and most of its configuration in SQL Server databases. However, some configuration settings are stored only in Microsoft IIS and various web.config files. Custom code is often stored within the 12 Root (by default, C:\Program Files\Common Files\Microsoft Shared\web server extensions\12) or the global assembly cache. As you'll see, performing only a SQL Server backup isn't enough to ensure a smooth farm recovery. Perhaps the most significant drawback is that even with many configuration settings stored in a configuration database, this is not recoverable without a SharePoint-based farm backup. (To learn more about SharePoint farm backups, see "Back up a farm by using built-in tools " at technet.microsoft.com/en-us/library/cc263298.aspx.) Nonetheless, you still have recovery options, so let's start by reviewing what you'll need.

Assess Your Inventory

Let's review the items you'll need to proceed with your recovery. Here are the primary items you should identify:

- You'll need all your content databases (not including the one for central administration), your Shared Services Provider (SSP) service database, and your search database. All other databases will be re-created.
- Identify your web applications and the settings that were in use. This should include your portal web application(s), your SSP web application, and your MySites web application, if applicable. Ensure that you know which content database(s) each web application was using. This is a critical reason why basic documentation for your SharePoint environment is so important. If you don't know or have this, try to remember and document as much as you can; during the recovery, you might experience some trial and error to fit everything back together.
- Determine your farm's build version, which will tell you what service packs or other updates that have been applied. To get this information when your farm is down, open a query window on your SQL Server system. In the SharePoint config database, run a `Select * From Versions` command. In the results window, look for the highest value in the version column. Common build numbers are 12.0.0.4518 Original release (RTM), 12.0.0.6219 SP1, 12.0.0.6318 Infrastructure Update, and 12.0.0.6421 SP2.

Step by Step SharePoint Disaster Recovery

Randy Williams

(Reprinted From Windows IT Pro Magazine)

- Identify the SharePoint domain service accounts and passwords that were in use. If you're uncertain what accounts you have, you can obtain them from your SQL Server system's Logins folder. (Note that you might have other login accounts in addition to SharePoint, and you'll also need to specify which account is used for which service.) If you don't know the passwords, you can reset them in AD. Here are the domain accounts and a naming convention I often use: setup/admin account (MOSS.Admin); server farm account, aka the database access account (MOSS.Farm); application pool accounts (MOSS.PortalAppPool, MOSS.SSPAppPool); SSP Service account (MOSS.SSPService); Farm Search Service account (MOSS.Search); and Crawler account (MOSS.Crawler).
- Identify the SharePoint domain service accounts and passwords that were in use. If you're uncertain what accounts you have, you can obtain them from your SQL Server system's Logins folder. (Note that you might have other login accounts in addition to SharePoint, and you'll also need to specify which account is used for which service.) If you don't know the passwords, you can reset them in AD. Here are the domain accounts and a naming convention I often use: setup/admin account (MOSS.Admin); server farm account, aka the database access account (MOSS.Farm); application pool accounts (MOSS.PortalAppPool, MOSS.SSPAppPool); SSP Service account (MOSS.SSPService); Farm Search Service account (MOSS.Search); and Crawler account (MOSS.Crawler).
- Identify any third-party applications and SharePoint Solutions (.wsp files) that will need to be reinstalled.
- Identify the new physical or virtual server that you'll use as your front-end web server.
- Ensure that you have your MOSS installation media and license key.

Recovery Steps

Now that you've made an inventory of all the necessary components, let's proceed with the suggested recovery steps. (When you're entering the service accounts in the steps below, I recommend that you precede the accounts with the domain name—for example: domain\MOSS.Farm.)

1. Install the original OS version on your new server, and don't be tempted to upgrade the OS at this point. It's technically possible but adds another level of complexity to your recovery effort. Keep all other settings (e.g., server name, IP address) the same, if possible.
2. Add the MOSS.Admin account to the local administrators group on the new server. Make sure this account also has logon permissions to your SQL Server system and is a member of the Sysadmin server role.
3. Remove the previous computer account from AD, join the new server to the domain, and reboot.
4. Install IIS.
5. Install the same .NET Framework version that you had on the previous server. At a minimum, this would be version 3.0. If you don't know, install the latest version, which is version 3.5 SP1, as of this writing.
6. Install MOSS. Start by logging on as your administrative account (MOSS.Admin). Run the MOSS setup program from your installation media. As with all SharePoint installations, the recommendation is to use the Advanced and then Complete options. These options give you the

Step by Step SharePoint Disaster Recovery

Randy Williams

(Reprinted From Windows IT Pro Magazine)

most flexibility, letting you have this SharePoint server run any roles needed (e.g., Web Application, search) You can install a slipstreamed version provided it isn't newer than the build you had previously.

7. Before creating the farm, install all updates to match your previous build version. When doing this, make sure you apply the individual WSS update first and the MOSS update second. For example, to get to build 6318, install in this sequence: WSS SP1, MOSS SP1, WSS Infrastructure Update, MOSS Infrastructure Update. After each update, the SharePoint Products and Technologies Configuration Wizard will start. When it does, simply cancel it.
8. Once you've applied the updates, you're ready to create the server farm. Start by launching the SharePoint Products and Technologies Configuration Wizard, which you can access in the Microsoft Office Server group on the Start menu. When prompted, create a new server farm. Next, specify the name of your SQL Server system and the name of your SharePoint config database. If you're using the same database name that you used in your old farm, you must delete the old database first. For the username, enter the name of your server farm account (MOSS.Farm). Click Next, then enter the desired port for the Central Administration Web application and set the proper form of authentication (i.e., NTLM or Kerberos). When you see the summary screen, review it and click Next to create the farm.
9. Start the Search service. After the farm is created, the Central Administration web site should automatically appear. If the system prompts you to log on, use your MOSS.Admin credentials. To start the search service, first go to the Operations tab and choose Services on server. In the list of services, click Start next to Office SharePoint Server Search. In the resulting dialog box, select both check boxes at the top to make the server an index and query server. For the Farm Search Service Account, enter the appropriate account (e.g. MOSS.Search).
10. Start any additional services that are in use, such as Excel Calculation Services. For MOSS, you might not need the WSS Search service because it's used only to index the Help collection.
11. Re-create each of your Web applications. You'll need to do this for your SSP Web application, your MySites Web application (if applicable), and each additional Web application that your farm was using. For each one, follow these steps: Go to the Application Management tab, choose Create or extend Web application, then select Create a new Web application. Enter the port and host header. In most cases, you can keep the path as the default. If this web application was using SSL, specify that here. Enter the application pool credentials. In most cases, each web application should use a separate application pool with unique credentials. For example, for the SSP web application, you would use a logon such as MOSS.SSPAppPool. Finally, and most important, enter the name of your SQL Server system and one of the content databases used for this web application. SharePoint will recreate this website in IIS, register it in the new config database, and link it to your existing content database. If you previously extended any of your Web applications (e.g., configured an intranet for extranet access), you should reapply this now.
12. Associate remaining content databases with your web applications. This step is necessary only if you have multiple content databases for your web applications. Go to the Application Management tab, access Content databases, and select Add a content database. Ensure that you've selected the correct web application at the top, then specify each additional database name.
13. Restore your SSP. In navigation menu on the left inside Central Administration, click Shared Services Administration, then Restore SSP. For SSP Name, enter in the name of your SSP such as SharedServices1. For Web application, select the Web application that you just created for

Step by Step SharePoint Disaster Recovery

Randy Williams

(Reprinted From Windows IT Pro Magazine)

your SSP. If you were using a separate Web application for My Sites, clear the use existing location check box. If you get warnings here, just acknowledge them and then select the Web application used for My Sites. Next, enter in the SSP Service Credentials (e.g. MOSS.SSPService). Enter in the name of the SSP Database and then the name of the Search Database. Finally, set the desired folder for the index file location. This should be on a drive letter that has plenty of space, so the C: default is not usually a good choice.

14. Reset IIS. The easiest way to do so is to click Start, Run, and type iisreset.
15. Reinstall any third-party applications or SharePoint Solutions. These can include custom IFilters (e.g., to index PDF files), custom web parts, and so on. For more information about SharePoint Solutions, see the "Solutions Overview" at msdn.microsoft.com/en-us/library/aa543214.aspx.
16. Apply any additional configurations. This is the most problematic area because SharePoint changes might occur in a number of ways. Here are some common areas where you might need to make modifications: alternate access mappings (AAM), web.config changes to your web applications, code deployed to bin folders or global assembly cache, IIS settings (e.g., reloading and binding your SSL certificate), changes to 12 Root (e.g., Features or Site Definitions), web application policy settings, and incoming/outgoing email—in general, anything on the Operations tab in Central Administration.
17. Issue a full crawl of all your content sources, which will recreate SharePoint's search index. Because your index files were lost on the old server, you must re-crawl. Within your newly restored SSP, click Search settings, then Content sources and crawl schedules. For each content source, select Start Full Crawl from the context menu. Depending on the amount of content, the full crawl can take from minutes to days to complete.
18. Last, but definitely not least, fully test your SharePoint websites to validate your work. Errors could range from minor web-part problems on pages to full sites not displaying at all. The cause of errors is most likely configuration settings or missing files.

Recommendations

As you can see, not having a SharePoint-specific backup makes the recovery process much more painful, and you run the real risk of ending up with one or more inoperable components. Here are some recommendations that can mitigate this risk and ensure that your recovery is quick and easy.

- Perform regular SharePoint-specific farm backups. You can do this manually through Central Administration (on the Operations tab, select Perform a backup) or by using the stsadm.exe command-line utility. One advantage to stsadm.exe is that you create a Windows scheduled task to run on a recurring basis. Here's the basic syntax for a full farm backup using stsadm.exe:

```
stsadm -o backup -directory -backupmethod full
```

You must run this command from one of your SharePoint servers, preferably running as your SharePoint admin account. Also, the service account running the MSSQLServer service on your SQL Server system must have Modify permissions to this UNC share and the underlying NTFS folder.

- Because a farm backup doesn't include everything, you should also back up your inetpub\wwwroot folders, your 12 Root folder hierarchy, and IIS (for Windows Server 2003, use iisback.vbs; for Windows Server 2008, use appcmd.exe.)

Step by Step SharePoint Disaster Recovery

Randy Williams

(Reprinted From Windows IT Pro Magazine)

- For more powerful and granular recovery options, consider third-party backup software such as AvePoint's DocAve, a popular and respected app.
- When you upgrade the farm (e.g., install SP2), perform a farm backup before and after the upgrade. Creating a backup following an upgrade is recommended because you'll now be at a newer build and previous backups are more difficult to restore.
- Maintain a configuration change log. This can be a simple document that describes the updates that were made to the farm—for example, upgrading to SP2, installing a custom application, or manually changing a web.config setting. For obvious reasons, don't store this file in SharePoint.
- For environments that can't afford downtime, you should build a recovery farm and configure it through step 7 above. (For more information about building a recovery farm, see "Create a recovery farm" at technet.microsoft.com/en-us/library/cc288425.aspx.) Doing so will speed up the recovery. Also, consider an additional web front end and cluster or mirror SQL Server to add additional fault tolerance to your farm. Incidentally, SharePoint is supported in a virtual environment, and it's common to have a recovery farm in either VMware or Hyper-V.
- Perform trial restores to your test/recovery farm. Doing so will ensure that your backups are working and that you know how to perform a restore. You really don't want to learn how to perform a recovery during a disaster on a Sunday night.
- When deploying custom code to your farm, use SharePoint Solutions. SharePoint Solutions are the best way to deploy custom updates to your farm. If your organization has a development team that is building SharePoint software, insist that they also create a solution package to deploy it.
- Keep your content databases small. The larger your content databases are, the longer they will take to restore. In general, I recommend keeping each content database under 200GB.
- Use an intuitive naming convention for your databases. As you can see, you might need to map your content databases to your web applications. Using a naming convention will make that much easier.

Earn Some Rest

We've now walked through a SharePoint recovery using only SQL Server databases. Remember that you won't be able to recover all your configuration settings; however, now that you understand how this kind of recovery works, you should be able to get your farm online within a few hours. Knowing the limitations of a database-only recovery should encourage you to consider additional backup options, along with my other recommendations. Only then can you be sure to get home in time to get some sleep.